Analysis and Design of Quantum Secure Communication System

A thesis submitted to Indian Statistical Institute
in partial fulfillment of the thesis requirements for the degree of
Doctor of Philosophy in Computer Science

Author: **Nayana Das**

Applied Statistics Unit
Indian Statistical Institute
Kolkata - 700108, India

Supervisor: **Goutam Paul**

Cryptology and Security Research Unit
R. C. Bose Centre for Cryptology and Security
Indian Statistical Institute
Kolkata - 700108, India

August 2022

I dedicate this thesis to **my Parents**.

List of Publications

■ Included in this thesis:

1. Nayana Das and Goutam Paul. Measurement-Device-Independent Quantum Secure Direct Communication with User Authentication.
   Quantum Information Processing 21.7 (2022): 260.
   DOI: https://doi.org/10.1007/s11128-022-03572-z
   arXiv:2202.10316[quant-ph].

2. Nayana Das and Goutam Paul. Cryptanalysis of Quantum Secure Direct Communication Protocol with Mutual Authentication Based on Single Photons and Bell States.
   Europhysics Letters 138.4 (2022):48001.
   DOI: https://doi.org/10.1209/0295-5075/ac2246
   arXiv:2007.03710[quant-ph].

3. Nayana Das, Goutam Paul and Ritajit Majumdar. Quantum Secure Direct Communication with Mutual Authentication using a Single Basis.
   International Journal of Theoretical Physics 60.11 (2021): 4044–4065.
   DOI: https://doi.org/10.1007/s10773-021-04952-4.
   arXiv:2101.03577[quant-ph].

4. Nayana Das and Goutam Paul. Secure Multi-Party Quantum Conference and Xor Computation.
   Quantum Information and Computation 21.3,4 (2021): 203–0232.
   DOI: https://doi.org/10.26421/QIC21.3-4-2.
   arXiv:2101.05560[quant-ph].

5. Nayana Das and Goutam Paul. Two Efficient Measurement Device Independent Quantum Dialogue Protocols.
   International Journal of Quantum Information 18.7 (2020): 2050038.
   DOI: https://doi.org/10.1142/S0219749920500380.
   arXiv:2005.03518v2[quant-ph].

6. Nayana Das and Goutam Paul. Improving the Security of "Measurement-Device-Independent Quantum Communication without Encryption".
   Science Bulletin 65.24 (2020): 2048-2049.
   DOI: https://doi.org/10.1016/j.scib.2020.09.015.
   arXiv:2006.05263v2[quant-ph].

7. Nayana Das, Goutam Paul and Arpita Maitra. Dimensionality Distinguishers.
   Quantum Information Processing 18.6 (2019): 1-17.
   DOI: https://doi.org/10.1007/s11128-019-2279-5.
   arXiv:1904.11405[quant-ph].

■ Not included in this thesis

8. Nayana Das and Ritajit Majumdar. Comment on “Quantum Key Agreement Protocol”.
   International Journal of Quantum Information (2020): 2050039.
   DOI: https://doi.org/10.1142/S0219749920500392.
   arXiv:2003.07610[quant-ph].

Acknowledgments

My thesis becomes a reality with the kind support and help of many individuals. I would like to extend my heartiest thanks with a deep sense of gratitude and respect to all those who provide me immense help and gratitude during my Ph.D. work.

Foremost, I want to offer this endeavor to our **Almighty GOD** for the wisdom he bestowed upon me, the strength, peace of my mind, and good health to finish my Ph.D. work.

It's a genuine pleasure to express my deepest sense of thanks and gratitude to my mentor, philosopher, and guide **Dr. Goutam Paul**, Associate Professor of Cryptology and Security Research Unit, Indian Statistical Institute, for the continuous support, motivation, enthusiasm, and immense knowledge of my Ph.D. study and research. His guidance helped me in all the time of research and writing of this thesis. I could not have imagined having a better advisor and mentor for my Ph.D. study. I shall be forever obliged for his encouragement and support of my academic as well as non-academic life.

No words to thanks can sum up the gratitude that I owe to all the members of my research fellow advisory committee, especially **Prof. Bimal Kumar Roy**, **Prof. Subhamoy Maitra**, who have always been key peoples to me for their keen interest in my research and provide their guidance, timely suggestions with kindness.

I owe a deep sense of gratitude to **Prof. Guruprasad Kar**, Physics and Applied Mathematics Unit, Indian Statistical Institute, for helping me at the time of exploring the fantastic world of quantum information and computation. Whenever I ran into some confusion regarding quantum theory, he was always available for discussion.

I would like to thank **all the faculty members of the Applied Statistics Unit and the Cryptology and Security Research Unit, Indian Statistical Institute**, for their kind help and co-operation throughout my Ph.D. research.

I wish to express my warm and sincere thanks to my collaborators **Dr. Arpita Maitra**, TCG CREST, Kolkata, and **Mr. Ritajit Majumdar**, Advanced Computing & Microelectronics Unit, Indian Statistical Institute. for joining their hands and contributing and updating me in my research, and it was always has been great fun to work with them.

During my Ph.D. life, I was considering very lucky enough to be surrounded by wonderful

colleagues: **Mr. Diptendu Chatterjee, Mr. Mostafizar Rahman, Mr. Prabal Banerjee, Mr. Pritam Chattopdhayay, Mr. Avishek Majumder, Mr. Samir Kundu, Mr. Laltu Sarder, Mr. Sampriti Soor, Mr. Soumya Das, Mr. Amit Jana**, etc. I would like to thank all of you for enormously helpful and enjoyable discussions about any topic related or not related to my research works. Because of you all, I have never felt lonely in my difficult times. I will always remember the special moments we spent together over the past few years.

Finally, I take this opportunity to express my greatest regards and heartfelt thanks to my beloved parents, **Mr. Debasis Das** and **Mrs. Chhabi Das**, who always support me in all aspects of my life. I also take this opportunity to express my immense respect to all my family members, **Lt. Sadhan Das, Ms. Dipti Das, Mr. Nimai Chandra Mandal, Mrs. Mamata Mandal, Mr. Mrinal Majumder, Mr. Arun Majumder**, etc. I would also like to thank **Mr. Amit Mandal, Mrs. Tanaya Mukherjee, Mrs. Soma Dey, Mr. Bipul Roy** for their continuous support and encouragement. I am grateful to have you by my side. Thank you, **Mr. Promit Dutta**, for all the support and love you give me since we met. This thesis would not have been possible without you all.

Abstract

Quantum secure direct communication (QSDC) is an important branch of quantum cryptography, where one can transmit a secret message securely without encrypting it by a prior key. Quantum dialogue (QD) is a process of two way secure and simultaneous communication using a single channel and quantum conference (Q.Conf) is a process of securely exchanging messages between three or more parties, using quantum resources. Deterministic secure quantum communication (DSQC) is another class of quantum secure communication protocol, to transmit secret message without any shared key, where at-least one classical bit is required to decrypt the secret message. In the practical scenario, an adversary can apply detector-side-channel attacks to get some non-negligible amount of information about the secret message. Measurement-device-independent (MDI) quantum protocols can remove this kind of detector-side-channel attack, by introducing an untrusted third party (UTP), who performs all the measurements in the protocol with imperfect measurement devices. For secure communication, identity authentication is always important as it prevents an eavesdropper to impersonate a legitimate party. The celebrated Clauser, Horne, Shimony, and Holt (CHSH) game model helps to perform the security analysis of many two-player quantum protocols.

In this thesis, we perform analysis of several existing QSDC and QD protocols, and also design some new efficient protocols. We present new approaches of QSDC, QD and DSQC protocols with user authentication, some of them are MDI protocols. We analyze the security of a QSDC protocol, an MDI-QSDC protocol, and an MDI-QD protocol. We improve the previous protocols and propose some modifications of the above protocols. We also present a Q.Conf protocol by generalizing the previous MDI-QD protocol and using the algorithm of the Q.Conf protocol, we propose a quantum multi-party computation protocol to calculate the XOR value of multiple secret numbers. Next, we generalize the CHSH game, and we demonstrate how to distinguish between dimensions two and three for some special form of maximally entangled states using the generalized version of the CHSH game.

Contents

List of Figures

List of Tables

List Of Acronyms and Abbreviations

Expansion	Acronyms/ Abbreviations
Advanced Encryption Standard	AES
Data Encryption Standard	DES
Denial-of-Service	DoS
Device Independent	DI
Deterministic Secure Quantum Communication	DSQC
Left Hand Side	LHS
Local Hidden Variable Model	LHVM
Measurement Device Independent	MDI
Multi Party Computation	MPC
Orbital Angular Momentum	OAM
One Time Pad	OTP
Quantum Bit Error Rate	QBER
Quantum Conference	Q.Conf
Quantum Dialogue	QD
Quantum Key Agreement	QKA
Quantum Key Distribution	QKD
Quantum Multi Party Computation	QMPC
Quantum Secure Direct Communication	QSDC
Quantum Secret Sharing	QSS
Right Hand Side	RHS
Rivest–Shamir–Adleman	RSA
Standard Deviation	SD
Untrusted Fourth Party	UFP
Untrusted Third Party	UTP
Exclusive-OR	XOR
For example	e.g.
That is	i.e.

List of Symbols

Throughout the thesis, we use some notations and we describe those common notations here.

- Z basis $= \{|0\rangle, |1\rangle\}$ basis.
- $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.
- X basis $= \{|+\rangle, |-\rangle\}$ basis.
- $|\psi\rangle^{\perp}$ = orthogonal to $|\psi\rangle$.
- $\langle\psi|$ = conjugate transpose of $|\psi\rangle$.
- The following four unitary operators are called the Pauli operators [6]:
  1. $U_0 = I = |0\rangle\langle 0| + |1\rangle\langle 1|$.
  2. $U_1 = \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$.
  3. $U_2 = \sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|$.
  4. $U_3 = i\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|$.
- U^T = Transpose of U.
- $U^{\dagger}$ = conjugate transpose of U.
- $H = \frac{1}{\sqrt{2}}(\sigma_x + \sigma_z)$ is the Hadamard operator.
- $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|{+}{+}\rangle + |{-}{-}\rangle)$.
- $|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = \frac{1}{\sqrt{2}}(|{+}{-}\rangle + |{-}{+}\rangle)$.
- $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = \frac{1}{\sqrt{2}}(|{+}{+}\rangle - |{-}{-}\rangle)$.
- $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = \frac{1}{\sqrt{2}}(|{+}{-}\rangle - |{-}{+}\rangle)$.
- The states $|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle$ are called Bell states or EPR pairs.
- $\mathcal{B} = \{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$ is called Bell basis.

- The eight Greenberger–Horne–Zeilinger (GHZ) states are:

  $|G_1^{\pm}\rangle = \frac{1}{\sqrt{2}}(|000\rangle \pm |111\rangle)$, $\quad |G_2^{\pm}\rangle = \frac{1}{\sqrt{2}}(|001\rangle \pm |110\rangle)$,

  $|G_3^{\pm}\rangle = \frac{1}{\sqrt{2}}(|010\rangle \pm |101\rangle)$, $\quad |G_4^{\pm}\rangle = \frac{1}{\sqrt{2}}(|011\rangle \pm |100\rangle)$.

- $\mathcal{G} = \{G_1^{\pm}, G_2^{\pm}, G_3^{\pm}, G_4^{\pm}\}$ is called the GHZ basis.

- $\{S[i]\}_{i=1}^{m} = S$ is a finite sequence of length m.

- $S[i] = S_i = i$-th element of finite sequence S.

- $S_{A,i} = i$-th element of finite sequence S_A.

- $a \wedge b =$ a AND b.

- $a \oplus b =$ a XOR b.

- $a \odot b =$ a XNOR b.

- $\bar{b} =$ bit complement of b.

- $|\phi\rangle \otimes |\psi\rangle =$ $|\phi\rangle$ tensor product $|\psi\rangle$.

- $tr(A) =$ trace of a matrix A.

- $wt(v) =$ number of 1's in a binary vector v.

- $\Pr(A) =$ Probability of occurrence of an event A.

- $\Pr(A|B) =$ Probability of occurrence of an event A given that the event B has already occurred.

Chapter 1

Introduction

In this chapter, we will give a brief overview of the basics of quantum mechanics, quantum algorithms and quantum information theory, and then discuss one of its subfields that this thesis will focus on, which is quantum cryptography. Except where otherwise referenced, the following is based on information that can be found in [6, 7, 8, 9, 10], which provide a comprehensive summary for the less-experienced reader.

1.1 Quantum mechanics

Quantum mechanics is a fundamental theory in physics, which allows the calculation of properties and behavior of physical systems. We now move to cover the principles of quantum mechanics that underlie the work of this thesis and discuss the effect of quantum computers on modern cryptography. We also provide a summary of the most popular approaches for encoding information on quantum states of light.

1.1.1 Quantum states

A quantum state (specifically, a "pure state") is a unit vector of $\mathbb{C}^n$, a space of n-tuples $(z_1, z_2, \ldots, z_n)$ where each $z_i \in \mathbb{C}$. Theoretically, the dimension n can be infinite (e.g., for position or momentum state), but we consider only finite dimensional spaces.

A qubit is a two dimensional quantum state $|\psi\rangle = a|0\rangle + b|1\rangle$, where $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$,

$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, and thus $|\psi\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$. Since $|\psi\rangle$ is a unit vector of $\mathbb{C}^2$, we must have $a, b \in \mathbb{C}$ and $|a|^2 + |b|^2 = 1$. The set $\{|0\rangle, |1\rangle\}$ is called the computational basis or Z-basis, and the set $\{|+\rangle, |-\rangle\}$ is called the diagonal basis or X-basis, where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

The conjugate transpose of $|\psi\rangle$ is $\langle\psi| = a^* \langle 0| + b^* \langle 1| = (a^* \quad b^*)$ and the general representation of $|\psi\rangle$ is $\cos\theta |0\rangle + e^{i\gamma} \sin\theta |1\rangle$, where $\theta, \gamma \in \mathbb{R}$.

Let us now consider the two qubits $|\phi\rangle = a_1 |0\rangle + b_1 |1\rangle$ and $|\psi\rangle = a_2 |0\rangle + b_2 |1\rangle$. Then the inner product of $|\phi\rangle$ and $|\psi\rangle$ is defined as $\langle\phi|\psi\rangle = a_1^* b_1 + a_2^* b_2$. The two states $|\phi\rangle$ and $|\psi\rangle$ are orthogonal ($|\phi\rangle = |\psi\rangle^\perp$) if $\langle\phi, \psi\rangle = 0$. Thus for any state $|\psi\rangle$ of $\mathbb{C}^2$, the set $\{|\psi\rangle, |\psi\rangle^\perp\}$ forms an orthonormal basis of $\mathbb{C}^2$.

We now talk about multiple qubits state. The two-qubit state $|\phi\rangle |\psi\rangle$ or $|\phi\psi\rangle$ is the tensor product of the states $|\phi\rangle$ and $|\psi\rangle$, and it is defined as

$$|\phi\rangle \otimes |\psi\rangle \coloneqq a_1 a_2 |00\rangle + a_1 b_2 |01\rangle + b_1 a_2 |10\rangle + b_1 b_2 |11\rangle,$$

where $|a_1 a_2|^2 + |a_1 b_2|^2 + |b_1 a_2|^2 + |b_1 b_2|^2 = 1$. Thus the space of all two-qubit states has dimension 4 and therefore any element of this space can be expressed as a linear combination of 2^2 orthonormal vectors of $\mathbb{C}^{2^2}$. We can say a two-qubit state $a |00\rangle + b |01\rangle$ is valid if $|a|^2 + |b|^2 = 1$ holds.

Similarly, an n-qubit state is the tensor product of n single-qubit states, which can be expressed as a linear combination of 2^n orthonormal vectors of $\mathbb{C}^{2^n}$.

A qutrit is a three dimensional quantum state $|\psi\rangle = a |0\rangle + b |1\rangle + c |2\rangle$, where $|0\rangle = (1, 0, 0)^T$, $|1\rangle = (0, 1, 0)^T$, $|2\rangle = (0, 0, 1)^T$ are three orthonormal states of $\mathbb{C}^3$ and thus $|\psi\rangle = (a, b, c)^T$. Since $|\psi\rangle$ is an unit vector of $\mathbb{C}^3$, we must have $|a|^2 + |b|^2 + |c|^2 = 1$. An n-qutrit state is the tensor product of n single-qutrit states, which can be expressed as a linear combination of 3^n orthonormal vectors of $\mathbb{C}^{3^n}$.

A qudit is a d-dimensional quantum state described by a vector of $\mathbb{C}^d$. The space is spanned by a set of orthonormal basis vectors $\{|0\rangle, |1\rangle, |2\rangle, \ldots, |d-1\rangle\}$ and the state of a qudit has the general form $|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle + \alpha_2 |2\rangle + \ldots + \alpha_{d-1} |d-1\rangle = (\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_{d-1})^T \in \mathbb{C}^d$ with $|\alpha_0|^2 + |\alpha_1|^2 + |\alpha_2|^2 + \ldots + |\alpha_{d-1}|^2 = 1$ [11]. Due to the multi-level nature of a qudit,

it provides a larger state space to store and process information. It can able to do multiple control operations simultaneously, which play an important role in the reduction of the circuit complexity, the simplification of the experimental setup and the enhancement of the algorithm efficiency [12, 13, 14, 15]. The advantage of the qudit also applies to adiabatic quantum computing devices [16, 17]; topological quantum systems [18, 19, 20] and more. The qudit-based quantum computing system can be implemented on various physical platforms such as photonic systems [21, 13]; continuous spin systems [22, 23] etc.

1.1.2 Unitary operators

A linear operator U is called unitary if $U^\dagger U = UU^\dagger = I$ holds, where $U^\dagger$ denotes the conjugate transpose of U and I is the identity operator. Let us discuss some important unitary operators.

- **Pauli operators:**

  Consider the following four unitary operators

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = |0\rangle\langle 0| + |1\rangle\langle 1|, \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1|,$$

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = |0\rangle\langle 1| + |1\rangle\langle 0|, \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = i(|1\rangle\langle 0| - |0\rangle\langle 1|).$$

  These four operators form a basis of the space of all 2×2 unitary matrices and they are called the Pauli operators.

- **Hadamard operator:**

$$H = \frac{1}{\sqrt{2}}(\sigma_z + \sigma_x) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|).$$

  This unitary operator is called the Hadamard operator, and it is used to create superposition of all possible states.

These are all one-qubit unitary operators, act on single-qubit states.

- $CNOT$ **operator:**

  It is an example of two-qubit unitary operator, where the input qubits are control qubit and target qubit and

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10|.$$

  This $CNOT$ operator is used to create entanglement, which we discuss later.

1.1.3 Measurement

Let $|\psi\rangle = a|0\rangle + b|1\rangle$ be a quantum state, then measuring $|\psi\rangle$ in Z-basis gives the measurement result $|0\rangle$ with probability $|a|^2$ and $|1\rangle$ with probability $|b|^2$. More generally, if $\{|\alpha\rangle, |\beta\rangle\}$ is an orthonormal basis of $\mathbb{C}^2$, and $|\psi\rangle = a_1|\alpha\rangle + b_1|\beta\rangle$, then measuring $|\psi\rangle$ in $\{|\alpha\rangle, |\beta\rangle\}$ basis gives the measurement result $|\alpha\rangle$ with probability $|a_1|^2$ and $|\beta\rangle$ with probability $|b_1|^2$. Thus, if we measure $|\psi\rangle$ in $\{|\psi\rangle, |\psi\rangle^{\perp}\}$ basis, then we get the result $|\psi\rangle$ with probability 1.

Born rule [24]: Let $B = \{|b_1\rangle, |b_2\rangle, \ldots, |b_{2^n}\rangle\}$ be a orthonormal basis of $\mathbb{C}^n$, and $|\psi\rangle$ be an n-qubit state. Then measuring the state $|\psi\rangle$ in the orthonormal basis B gives the measurement result $|b_i\rangle$ with probability $|\langle b_i|\psi\rangle|^2$, where $1 \leq i \leq 2^n$.

Let us consider the two-qubit state $|\psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$. If we measure $|\psi\rangle$ in computational basis $Z \otimes Z$, then we get

$$\Pr(|00\rangle) = |a_{00}|^2, \ \Pr(|01\rangle) = |a_{01}|^2, \ \Pr(|10\rangle) = |a_{10}|^2 \text{ and } \Pr(|11\rangle) = |a_{11}|^2.$$

Suppose we measure only the first qubit in Z-basis. We can write $|\psi\rangle = |0\rangle(a_{00}|0\rangle + a_{01}|1\rangle) + |1\rangle(a_{10}|0\rangle + a_{11}|1\rangle)$. Then we have the outcome $|0\rangle$ with probability $|a_{00}|^2 + |a_{01}|^2$ and the state becomes $|0\rangle \otimes \frac{a_{00}|0\rangle + a_{01}|1\rangle}{\sqrt{|a_{00}|^2 + |a_{01}|^2}}$. Similarly we get the outcome $|1\rangle$ with probability $|a_{10}|^2 + |a_{11}|^2$ and the state becomes $|1\rangle \otimes \frac{a_{10}|0\rangle + a_{11}|1\rangle}{\sqrt{|a_{10}|^2 + |a_{11}|^2}}$. This is called the partial measurement rule.

General form of measurement and POVM: Let $\{M_m\}$ be a collection of measurement operators, such that $\sum_m M_m^\dagger M_m = I$, and $|\psi\rangle$ be the state of the quantum system being measured. Then the probability of getting outcome m is given by

$$p(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle ,$$

and the state becomes

$$\frac{M_m |\psi\rangle}{\sqrt{\langle\psi| M_m^\dagger M_m |\psi\rangle}}.$$

Then measuring the state $|\psi\rangle = a|0\rangle + b|1\rangle$ in Z-basis means, there are two measurement operators $M_0 = |0\rangle\langle 0|$, $M_1 = |1\rangle\langle 1|$, and $p(0) = \langle\psi| M_0^\dagger M_0 |\psi\rangle = \langle\psi| M_0 |\psi\rangle = |a|^2$, $p(1) = \langle\psi| M_1^\dagger M_1 |\psi\rangle = \langle\psi| M_1 |\psi\rangle = |b|^2$.

Denoting $E_m = M_m^\dagger M_m$, we see that each E_m is a positive operator with $\sum_m E_m = I$ and $p(m) = \langle\psi| E_m |\psi\rangle$. The set of operators $\{E_m\}$ is called Positive Operator-Valued Measure (POVM).

1.1.4 Entanglement

Consider the two-qubit state $|\psi\rangle = a|00\rangle + b|11\rangle$, where $|a|^2 + |b|^2 = 1$. Then what is the representation of each individual state? Let us assume it can be written in the form $|\alpha\rangle \otimes |\beta\rangle$ in Z-basis. So $|\alpha\rangle, |\beta\rangle$ can be written as $|\alpha\rangle = m|0\rangle + n|1\rangle$ and $|\beta\rangle = p|0\rangle + q|1\rangle$. Therefore $|\alpha\rangle \otimes |\beta\rangle = mp|0\rangle|0\rangle + mq|0\rangle|1\rangle + np|1\rangle|0\rangle + nq|1\rangle|1\rangle$. If $a, b \neq 0$, then it is not possible to write in this form. That is, this state has the property that, there exist no single qubit states $|\alpha\rangle$ and $|\beta\rangle$ such that $|\psi\rangle = |\alpha\rangle \otimes |\beta\rangle$. This property is called entanglement property quantum states. A state of a composite system having the property, that it can not be factored into a tensor product of it's component systems, is called entangled state.

In quantum entanglement, two or more quantum particles (maybe space-like separated) share their states in such a way that the state of each of the particles cannot be fully described without considering the other(s). If we change the quantum state of one particle through local unitary operations, the state of the rest of the particles changes automatically to maintain the entanglement.

Four important two-qubit entangled states are

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), \quad |\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle).$$

These states $|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle$ are called Bell states or EPR pairs and the set $\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$ is called the Bell basis.

The eight three-qubit entangled states (Greenberger–Horne–Zeilinger or GHZ states [25]) are:

$$|G_1^{\pm}\rangle = \frac{1}{\sqrt{2}}(|000\rangle \pm |111\rangle), \quad |G_2^{\pm}\rangle = \frac{1}{\sqrt{2}}(|001\rangle \pm |110\rangle),$$
$$|G_3^{\pm}\rangle = \frac{1}{\sqrt{2}}(|010\rangle \pm |101\rangle), \quad |G_4^{\pm}\rangle = \frac{1}{\sqrt{2}}(|011\rangle \pm |100\rangle),$$

and the set $\{G_1^{\pm}, G_2^{\pm}, G_3^{\pm}, G_4^{\pm}\}$ is called the GHZ basis.

Many modern quantum protocols are based on entanglement theory, such as, super-dense coding [26], quantum teleportation [27], entanglement swapping [28] etc.

1.1.5 Density matrix

Consider the two-qubit pure state $|\Psi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$. It can be easily shown that $|\Psi^+\rangle_{AB}$ is an entangled state and thus can not be expressible as a tensor product of two single-qubit states. Then how to calculate the state of each subsystem A and B? To answer this question, we now introduce the concept of the density matrix.

Let $|\psi\rangle = a|0\rangle + b|1\rangle$ be a quantum state, then another way of representing this state is $\rho = |\psi\rangle\langle\psi|$. This is called density matrix representation. Then we have

$$\rho = \begin{pmatrix} a \\ b \end{pmatrix} (a^* \quad b^*) = \begin{pmatrix} aa^* & ab^* \\ a^*b & bb^* \end{pmatrix} = \begin{pmatrix} |a|^2 & ab^* \\ a^*b & |b|^2 \end{pmatrix}.$$

Let $|\psi\rangle$ be a unit vector of $\mathbb{C}^n$, then it is called a pure state and the density matrix (or density operator) $|\psi\rangle\langle\psi|$ describes that pure state.

Now we consider a mixture of pure states $|\psi_i\rangle$, where i is an index and p_i is the probability of the state $|\psi_i\rangle$ with $\sum_i p_i = 1$. Then the density matrix for the system is $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$.

It represents the perfect description of the state of a quantum system, and we call ρ as a mixed state.

Suppose there are two mixed states $\rho_1 = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)$ and $\rho_2 = \frac{1}{2}(|+\rangle\langle +| + |-\rangle\langle -|)$. Then

$$\rho_1 = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix} = \frac{I}{2}, \qquad \rho_2 = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} + \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix} = \frac{I}{2}.$$

That is, the mixed states ρ_1 and ρ_2 are the same. The density matrix $\frac{I}{2}$ is called the maximally mixed state.

We now calculate the density matrices of the subsystems A and B of the two-qubit state $|\Psi^+\rangle_{AB}$. The density matrix of the joint state is

$$\rho_{AB} = |\Psi^+\rangle\langle\Psi^+|_{AB} = \frac{1}{2}(|01\rangle\langle 01| + |01\rangle\langle 10| + |10\rangle\langle 01| + |10\rangle\langle 10|).$$

By tracing out the subsystem B (take partial trace over B), we get the reduced density matrix ρ_A of the subsystem A. Then

$$\begin{aligned} \rho_A = tr_B(|\Psi^+\rangle\langle\Psi^+|) &= \frac{1}{2}(|0\rangle\langle 0|\langle 1|1\rangle + |0\rangle\langle 1|\langle 1|0\rangle + |1\rangle\langle 0|\langle 0|1\rangle + |1\rangle\langle 1|\langle 0|0\rangle) \\ &= \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) = \frac{I}{2}. \end{aligned}$$

Similarly, we can calculate $\rho_B = \frac{I}{2}$ by tracing out subsystem A from ρ_{AB}.

1.1.6 Maximally entangled state

Let us consider a Hilbert space H (for now, $H = \mathbb{C}^2$). There are infinitely many maximally entangled states in $H \times H$ and all are connected by a unitary. A pure bipartite state in $\mathbb{C}^2 \times \mathbb{C}^2$ is maximally entangled if the reduced density matrix is $\frac{I}{2}$ for both subsystems. Bell states are examples of two-qubit maximally entangled states.

Let $|\phi\rangle = \cos\alpha\,|0\rangle + \sin\alpha\,|1\rangle$ and $|\theta\rangle = \cos\beta\,|0\rangle + \sin\beta\,|1\rangle$. Then
$|\Psi\rangle_{AB} = \frac{1}{\sqrt{2}}[|\phi\theta\rangle + |\phi^\perp\theta^\perp\rangle] = \frac{1}{\sqrt{2}}[|0\rangle|\varphi\rangle + |1\rangle|\varphi^\perp\rangle]$, where $|\varphi\rangle = \cos(\alpha-\beta)\,|0\rangle - \sin(\alpha-\beta)\,|1\rangle$ is maximally entangled as $\rho_A = \rho_B = \frac{I}{2}$ where ρ_A and ρ_B are reduced density matrix of subsystem A and B respectively.

Again let $|\chi\rangle_{AB} = \frac{1}{\sqrt{2}}[|0\rangle|\sigma\rangle + |1\rangle|\varrho\rangle]$, where $|\sigma\rangle = \cos\gamma|0\rangle + \sin\gamma|1\rangle$ and $|\varrho\rangle = \cos\delta|0\rangle + \sin\delta|1\rangle$. To make $\rho_A = \rho_B = \frac{I}{2}$, we must have $|\varrho\rangle = |\sigma^{\perp}\rangle$.

Thus a general form of maximally entangled state in $\mathbb{C}^2$ is $\frac{1}{\sqrt{2}}[|\phi\theta\rangle + |\phi^{\perp}\theta^{\perp}\rangle]$ (we are considering real coefficients only).

A bipartite maximally entangled (pure) state in a d-dimensional Hilbert space has the Schmidt decomposition $\sum_{i=1}^{d} \frac{1}{\sqrt{d}}|i\rangle \otimes |i\rangle$ is an appropriate basis [29]. And in Hilbert space $\mathbb{C}^m \otimes \mathbb{C}^n$ (where $m < n$), a maximally entangled (pure) state is the same as that in $\mathbb{C}^m \otimes \mathbb{C}^m$.

1.1.7 Bell inequality

In 1935, Einstein, Podolsky and Rosen (EPR) showed that quantum mechanics is not complete [30]. They also claimed that there may exist some local hidden variable λ still unknown. Knowing λ, one can explain entanglement without the spooky action at a distance. In 1964, Bell proposed a test for the existence of these hidden variables and developed an inequality [31]. He showed that if the inequality were not satisfied, then a local hidden variable theory would not be possible. Inspired by Bell's paper, Clauser, Horne, Shimony and Holt (CHSH) formed a correlation inequality and Bell's theorem can be proved by using that inequality [32]. CHSH inequality gives a bound on any local hidden variable model (LHVM). A simple setting for showing the usefulness of entanglement involves a two-player game known as the CHSH game.

1.1.8 The CHSH game

In this game there are two players, namely, Alice and Bob , and a referee. Let us assume that Alice and Bob are far away from each other and not able to communicate during the game. Before the game begins, they can communicate freely to discuss their strategy. During the game, they only communicate with the referee in the following way:

- The referee chooses two independent random bits x and y uniformly (also called "questions") and sends x to Alice and y to Bob, i.e., for all $s \in \{0,1\},\ t \in \{0,1\},\ \Pr(x = s, y = t) = \Pr_{xy}(s,t) = \frac{1}{4}$.

- Alice and Bob reply to referee with bits a and b respectively.
- Referee calculates $x \wedge y$ and $a \oplus b$.
- Alice and Bob win if $x \wedge y = a \oplus b$.

Their goal is to achieve the highest winning probability together. Classically, the winning probability is 0.75. But in the quantum world, this probability is 0.85 if they follow the following strategy.

Quantum strategy: The strategy to win the game with maximum probability is to share a maximally entangled state (e.g, Bell state) between Alice and Bob. According to the referee's questions, they choose measurement bases to measure their qubits and send their answers to the referee. Details are given in the Algorithm 1.

Algorithm 1: Quantum strategy for CHSH game

---

1. Before the game starts, Alice and Bob share $|\Psi_{AB}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B)$
2. Alice takes the first qubit and Bob takes the second qubit
3. **Alice chooses:**
   - Standard basis $\{|0\rangle, |1\rangle\}$ if $x = 0$
   - Hadamard basis $\{|+\rangle, |-\rangle\}$ if $x = 1$.
4. **Bob chooses:**
   Basis $\{|\nu_0(\theta_y)\rangle, |\nu_1(\theta_y)\rangle\}$ corresponding to $y = 0, 1$, where
   $|\nu_0(\theta_y)\rangle = \cos\theta_y |0\rangle + \sin\theta_y |1\rangle$, $|\nu_1(\theta_y)\rangle = \sin\theta_y |0\rangle - \cos\theta_y |1\rangle$, and $\theta_0 = \frac{\pi}{8}$, $\theta_1 = -\frac{\pi}{8}$.
5. **Alice sends:**
   - $a = 0$ if $|0\rangle$ or $|0_x\rangle$
   - $a = 1$ otherwise
6. **Bob sends:**
   - $b = 0$ if Bob gets $|\nu_0(\theta_0)\rangle$ or $|\nu_0(\theta_1)\rangle$
   - $b = 1$ otherwise

Winning probability: Let *win* be the event that Alice and Bob win, i.e., $x \wedge y = a \oplus b$. Now the winning probability of the CHSH game can be written as:

$$\Pr(win) = \sum_{s,t} \Pr_{xy}(s,t) \Pr(win|x=s, y=t) \tag{1.1}$$

Which again implies that for $u, v, s, t \in \{0, 1\}$,

$$\Pr(win) = \sum_{s,t,u,v} \Pr_{xy}(s,t)(s \wedge t = u \oplus v)\Pr_{ab|xy}(a=u, b=v|x=s, y=t)$$

If the referee sends questions $x = 0, y = 0$, Alice and Bob win if they answer identically $a = 0, b = 0$ or $a = 1, b = 1$.

Then from Algorithm 1, the corresponding probability of winning (given $x = 0, y = 0$) is:
$\Pr(win|x=0, y=0) = |\langle 0| \otimes \langle \nu_0(\theta_0)| \Psi_{AB}\rangle|^2 + |\langle 1| \otimes \langle \nu_1(\theta_0)| \Psi_{AB}\rangle|^2 = \cos^2\theta_0$

Similarly we have,
$\Pr(win|x=0, y=1) = |\langle 0| \otimes \langle \nu_0(\theta_1)| \Psi_{AB}\rangle|^2 + |\langle 1| \otimes \langle \nu_1(\theta_1)| \Psi_{AB}\rangle|^2 = \cos^2\theta_1$
$\Pr(win|x=1, y=0) = |\langle 0_x| \otimes \langle \nu_0(\theta_0)| \Psi_{AB}\rangle|^2 + |\langle 1_x| \otimes \langle \nu_1(\theta_0)| \Psi_{AB}\rangle|^2 = \frac{1}{2}(1 + \sin 2\theta_0)$
$\Pr(win|x=1, y=1) = |\langle 0_x| \otimes \langle \nu_1(\theta_1)| \Psi_{AB}\rangle|^2 + |\langle 1_x| \otimes \langle \nu_0(\theta_1)| \Psi_{AB}\rangle|^2 = \frac{1}{2}(1 - \sin 2\theta_1)$
Hence from equation 1.1,

$$\begin{aligned} P(win) &= \frac{1}{4}(P(win|x=0,y=0) + P(win|x=0,y=1) + P(win|x=1,y=0) + P(win|x=1,y=1)) \\ &= \frac{1}{4}[\cos^2\theta_0 + \cos^2\theta_1 + \frac{1}{2}(1+\sin 2\theta_0) + \frac{1}{2}(1-\sin 2\theta_1)] \end{aligned}$$

This probability is maximum at $(\theta_0 = \frac{\pi}{8}, \theta_1 = \frac{15\pi}{8})$ and the maximum value is approximately 0.85355. This conclusively proves that the quantum correlation is different from the classical correlation.

1.1.9 No-cloning theorem

Let us consider the Hilbert space $\mathbb{C}^n$ and $|b\rangle$ be an ancillary state of $\mathbb{C}^n$. Then there does not exist any unitary operator $\mathcal{U}$ such that $\mathcal{U}(|\psi\rangle \otimes |b\rangle) = |\psi\rangle \otimes |\psi\rangle$ holds, for all arbitrary state $|\psi\rangle \in \mathbb{C}^n$. That is, it is not possible to clone an arbitrary quantum state [33].

Let us assume that there exists a unitary operator $\mathcal{U}$ which can clone two different states

$|\phi\rangle$ and $|\psi\rangle$. Let $|b\rangle$ be a fixed state. Then we must have

$$\mathcal{U}(|\phi\rangle\,|b\rangle) = |\phi\rangle\,|\phi\rangle \text{ and } \mathcal{U}(|\psi\rangle\,|b\rangle) = |\psi\rangle\,|\psi\rangle\,.$$

By taking the scaler product we have,

$$\begin{aligned}
&\langle b|\,\langle\phi|\,\mathcal{U}^{\dagger}\mathcal{U}\,|\psi\rangle\,|b\rangle = \langle\phi|\psi\rangle\,\langle\phi|\psi\rangle \\
&\Rightarrow \langle b|b\rangle\,\langle\phi|\psi\rangle = \langle\phi|\psi\rangle^{2} \\
&\Rightarrow \langle\phi|\psi\rangle = \langle\phi|\psi\rangle^{2}\,.
\end{aligned}$$

This equation holds if $|\phi\rangle = |\psi\rangle$ or $\langle\phi|\,|\psi\rangle = 0$. That is, two different states can be cloned only if they are orthogonal (Note that, the $CNOT$ operator can clone the states $|0\rangle$ and $|1\rangle$). This also implies that two non-orthogonal states are not distinguishable. This indistinguishability property of non-orthogonal quantum states plays a key role in quantum algorithms and quantum cryptography.

1.1.10 Superdense coding

Suppose Alice wishes to send Bob two classical bits of information to Bob. Superdense coding can achieve this task by sending only one qubit over a quantum channel. To initiate this task, Alice and Bob must initially share the Bell state $|\Phi^{+}_{AB}\rangle$. Alice has the first qubit and Bob has the second qubit. Then the process is as follows:

1. Alice applies U_0, U_1, U_2, U_3 on her qubit to encode the classical information $00, 01, 10, 11$ respectively.

2. Alice sends her qubit to Bob.

3. Bob measures the two qubit state AB in Bell basis and from the measurement result he gets the two classical bits from Alice. If the resultant Bell states are $|\Phi^{+}_{AB}\rangle$, $|\Phi^{-}_{AB}\rangle$, $|\Psi^{+}_{AB}\rangle$ and $|\Psi^{-}_{AB}\rangle$, then the decoded classical bits are $00, 01, 10$ and 11 respectively.

1.1.11 Quantum teleportation

Suppose Alice has a qubit $|\alpha\rangle = a|0\rangle + b|1\rangle$ with $|a|^2 + |b|^2 = 1$, and she wants to send this qubit to Bob, who is fer apart from her. To send the $|\alpha\rangle$, it would seem that Alice would either have to send the physical qubit itself, or she would have to communicate the two complex amplitudes with infinite precision. Quantum teleportation is a technique for moving quantum states around, even in the absence of a quantum communications channel linking the sender of the quantum state to the recipient. To date, the expected means of reliably transmitting a qubit is via quantum teleportation, which requires one Bell pair and two classical bit transmissions. To initiate this task, Alice and Bob must initially share the Bell state $|\Phi^+_{AB}\rangle$. Alice has the first qubit and Bob has the second qubit. Then the process is as follows:

1. The 3-qubit state possessed jointly by Alice and Bob is initially $|\alpha\rangle|\Phi^+_{AB}\rangle$. It can be written as

$$|\alpha\rangle|\Phi^+_{AB}\rangle = \frac{1}{2}|\Phi^+\rangle|\alpha\rangle + \frac{1}{2}|\Phi^-\rangle U_1(|\alpha\rangle) + \frac{1}{2}|\Psi^+\rangle U_2(|\alpha\rangle) + \frac{1}{2}|\Psi^-\rangle U_3(|\alpha\rangle).$$

2. Alice measures the first two qubits in Bell basis.

3. Based on the measurement result Alice sends two classical bits to Bob. If the resultant states are $|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle$ and $|\Psi^-\rangle$ then she sends $00, 01, 10$ and 11 respectively.

4. Bob applies unitary operator U_0, U_1, U_2 and U_3 on his qubit corresponding to the classical bits $00, 01, 10$ and 11 respectively. Since $U_i^2 = I$ for $0 \leq i \leq 3$, he gets back the state $|\alpha\rangle$.

1.2 Quantum algorithms

In this section, we discuss some quantum algorithms, which can establish that quantum computers offer an advantage over classical computers.

1.2.1 Deutsch algorithm

Let $f : \{0,1\} \to \{0,1\}$ be an unknown 1-bit function. Suppose we have a black box, which can compute the value of f. Now the problem is to find the value of $f(0) \oplus f(1)$, i.e., to know that f is balanced or constant. Classically it takes 2 queries to solve this problem. But Deutsch algorithm [34] can determine the value by making a single query to the quantum oracle for f.

1.2.2 Deutsch–Jozsa algorithm

It is a generalization of the Deutsch algorithm. Consider the unknown function $f : \{0,1\}^n \to \{0,1\}$ with a promise that f is either balanced or constant, where f is balanced means $f(x) = 0$ for half of the input strings x, and $f(x) = 1$ for the other half of the inputs. The problem is to determine whether f is constant or balanced. Classically it takes $2^{n-1} + 1$ queries to solve this problem, whereas Deutsch–Jozsa algorithm [35] makes only one query to determine this, by using the advantage of quantum superposition.

1.2.3 Simon's algorithm

Consider the unknown function $f : \{0,1\}^n \to \{0,1\}^n$ with a promise that there exists an element $a \in \{0,1\}^n$ such that $f(x) = f(x \oplus a)$ holds for all $x \in \{0,1\}^n$. The problem is to find the value of a by making queries to f. Classically, it is an exponentially hard problem. In 1994, Simon [36] exhibited a quantum algorithm that can solve this problem in linear time.

1.2.4 Grover's algorithm

Given an unknown function $f : \{0,1\}^n \to \{0,1\}$, the search problem is to find an input $x \in \{0,1\}^n$ such that $f(x) = 1$. Grover's quantum search algorithm [37] provides a polynomial speed-up over the best-known classical algorithms.

1.2.5 Shor's algorithm

In the classical domain, the factorization problem is assumed to be a hard problem, as any classical computer takes exponential time to find the prime factors of a given integer. In 1994,

Peter Shor [38] formulated a quantum algorithm that can calculate the prime factors of a large number in only polynomial time. That is, Shor's algorithm is exponentially faster than any classical algorithm for factorization. Shor's factoring algorithm uses a quantum computer to determine the period r of the function $f(x) = a^x \mod N$ (i.e., r is the smallest positive integer such that $f(x+r) = f(x)$), where N is a l digit integer whose factors we want to calculate and a is a small random integer co-prime to N. Now from the knowledge of r, N can be factorized with high probability by applying number theoretic techniques.

1.3 Quantum information theory

Information theory studies the transmission, processing, extraction, and utilization of information. In 1948, Shannon [39] first proposed the basic concept of the communication of classical information over a noisy channel. The fundamental results of Shannon are "the noiseless channel coding theorem" and "the noisy channel coding theorem". Quantum information theory is a natural generalization of the classical information theory, where the classical or quantum information is transmitted using quantum states as the medium. It includes all the static and dynamic elements of classical information theory.

Any communication system consists of an information source, an encoder, a channel (classical or quantum) and a decoder. A communication channel is a mapping from an input set $\{x_i\}$ to an output set $\{y_i\}$. More precisely, a quantum channel is a completely positive, trace-preserving, convex linear map on the set of states.

1.3.1 Shannon entropy

It is the key concept of classical information theory. The Shannon entropy of a random variable X measures the amount of uncertainty about X before knowing its value. Let X can take n distinct values and $p_1, p_2, \ldots, p_n$ be the probability distribution of X, then the Shannon entropy of X is defined as

$$H(X) = -\sum_{x=1}^{n} p_x \log p_x.$$

If $n = 2$, i.e., X has two outcomes 0 and 1 with probability p and $1 - p$, then

$$H(X) = h(p) = -p \log p - (1 - p) \log(1 - p)$$

is called the binary entropy function.

For two random variables X and Y, with probability distribution p_x and p_y respectively, and the joint distribution p_{xy}, we have the joint entropy function $H(X, Y)$ as

$$H(X, Y) = -\sum_{x,y} p_{xy} \log p_{xy},$$

and the conditional entropy $H(X|Y)$ as

$$H(X|Y) = -\sum_{x,y} p_{xy} \log \frac{p_{xy}}{p_y}.$$

The mutual information $I(X; Y)$ between two random variables X and Y is defined as

$$I(X; Y) = H(X) + H(Y) - H(X, Y).$$

1.3.2 Von Neumann entropy

This is the quantum analogue of Shannon entropy. Let ρ be the density matrix of a quantum state, then the Von Neumann entropy is defined as

$$S(\rho) = -tr(\rho \log \rho),$$

where tr denotes the trace function. Equivalently, we can say that, if the eigenvalues of ρ are $\eta_1, \eta_2, \ldots, \eta_k$, then

$$S(\rho) = -\sum_{i=1}^{k} \eta_i \log \eta_i.$$

Let A and B are two quantum systems with respective density matrix ρ_A and ρ_B. Also let the density matrix of the joint state AB be ρ_{AB}. Then the quantum mutual information between

the systems A and B is defined as

$$I(A;B) = I(\rho_A, \rho_B) = S(\rho_A) + S(\rho_B) - S(\rho_{AB}).$$

1.3.3 Holevo bound

In 1973, Holevo [40] gave an useful upper bound on the quantum accessible information. Suppose $\mathcal{E} = \{\rho_1, \rho_2, \ldots, \rho_n\}$ be an ensemble of density matrices and each ρ_x is prepared with some probability p_x. Then for any POVM $\{E_y\}$ performed on $\rho = \sum_x p_x \rho_x$, the amount of accessible information about X with measurement outcome Y is bounded above by

$$I(X;Y) \leq S(\rho) - \sum_x p_x S(\rho_x).$$

1.4 Quantum cryptography

Nowadays security is one of the basic requirements in our daily life and cryptography is a method of secure communication of our secret information over a public channel. In classical cryptography, there are two types, symmetric or private key cryptography and asymmetric or public-key cryptography. Symmetric key cryptographic algorithms use a shared secret key to encrypt (or decrypt) the plain-text (or cipher-text), whereas, in asymmetric key cryptography, a public-private key pair is used for encryption and decryption. Some famous examples of symmetric key cryptographic algorithms are One Time Pad (OTP) [41], Data Encryption Standard (DES) [42], Advanced Encryption Standard (AES) [43] etc, and some asymmetric key cryptographic algorithms are Diffie–Hellman key exchange [44], ElGamal [45], RSA [46], Elliptic-curve cryptography [47, 48, 49, 50] etc.

In the symmetric key cryptosystem, a major challenge is that the legitimate parties have to share a secret key before the information exchange process. Usually, one party generates the secret key and distributes it to the other party in a secure manner. Now the challenge is, how to distribute a secret key with perfect secrecy or without leaking any information? To solve this problem classically, asymmetric key cryptographic algorithms can be used. That is, one party, say, Alice, generates a public-private key pair (k_1, k_2) and announces the public

key k_1, and the other party, say, Bob, generates the secret key k for future communication. Then Bob encrypts k with k_1 and sends it to Alice, who decrypts k with her private key k_2. However, the security of the asymmetric key cryptosystem is based on some mathematical hardness assumptions, such as integer factorization problem, discrete log problem, etc. But due to Shor's algorithm [38], which can factorize an integer in polynomial-time, the quantum computer becomes a threat for asymmetric key cryptography. Thus we can say that the key distribution problem can not be solvable classically without assuming some mathematically hard problem.

Quantum key distribution (QKD): Quantum cryptography provides unconditional security based on the fundamental principles of quantum mechanics, such as the Heisenberg uncertainty principle [51], quantum no-cloning theory [33]. The first-ever quantum cryptographic protocol is BB84 QKD [52], proposed by Bennett and Brassard in 1984. The BB84 QKD is based on the idea of quantum conjugate coding proposed by Wiesner [53]. QKD allows two or more remote users to establish a shared secret key between themselves and the security only depends on the laws of quantum physics. In the BB84 protocol, two users, namely, Alice and Bob, use a sequence of single photons randomly prepared in the rectilinear basis (Z-basis), and the diagonal basis (X-basis) to produce a random secret key. In 2000, Shor and Preskill [54] showed that this protocol is secure and they gave a simple proof of security of the BB84 protocol. In 1991, Ekert [55] proposed another QKD protocol using entangled states. Till now, there are many variants of QKD protocols proposed by many researchers, for example, BBM92 [56], B92 [57] and many others [58, 59, 60, 61, 62, 63, 64, 65].

Quantum secure direct communication (QSDC): In classical cryptography, sending a message from Alice to Bob always requires a key. In particular, one shared secret key is required for any symmetric key protocol, and a pair of keys (one public key and one private key of the receiver Bob) is required for any asymmetric or public key protocol. Interestingly, in the quantum domain there exist some protocols for secure message transmission that does not explicitly require any key. QSDC is one such protocol. That is, in QSDC, the secret message can be transmitted directly from the sender to the receiver without any classical communication of ciphertext, or in other words, the QKD and the classical communication of the ciphertext are condensed into one single quantum communication. QSDC is fully quantum

mechanicalhas and thus it has a great potential in future. Since QSDC sends secret message directly over quantum channel, it demands more security than any QKD protocol. It must satisfy the following requirements, first the secret messages should be read out directly by the legitimate user, when he receives the quantum states, and no additional classical information is needed after the transmission of qubits. Secondly the secret messages which have been encoded already in the quantum states should not leak even though an eavesdropper may get hold of channel. That is to say, the eavesdropper can not only be detected but also obtains blind results. The intuitive idea of QSDC was first proposed by Long et al. [58] in 2002. In 2003, Deng et al. generalized the previous idea of Long et al. [58] and proposed a new QSDC protocol [66], where the sender (Alice) and the receiver (Bob) first share two-particle entangled states (namely, one of the Bell state) and each of them takes one particle from each pair. After that, Alice encodes her state with one of the four unitary operations, which are called Pauli matrices [6], I, σ_z, σ_x, and $i\sigma_y$ to encode the information 00, 01, 10, and 11 respectively and sends it to Bob. Then Bob measures the two-particle state (one from Alice and another from his own) in Bell basis to decode Alice's message. One of the famous QSDC protocols is Ping-Pong Protocol (PPP) [67], where the receiver first prepares two-qubit entangled states and ping the sender with one qubit. Then sender encodes her information by performing I or σ_z on that qubit and pong it to the receiver. Many other QSDC protocols have been proposed and analyzed in several works using different approaches [68, 69, 70, 71, 72, 73, 74]. In recent years, QSDC has gone through rapid developments [75, 76, 77, 78, 79, 2, 80, 5]. The experimental demonstration of QSDC are given in [75, 76, 77]. A practical QSDC prototype has been constructed recently [78]. QSDC is the explicit realization of Wyner's wiretap theory [79]. In particular, the measurement-device-independent QSDC have been proposed in [2, 80, 5].

Quantum Dialogue (QD): It can be thought of as a two-way QSDC protocol. Nowadays it is a very important research topic in quantum cryptography. In QD, Alice and Bob can send messages to each other simultaneously in the same channel. Quantum dialogue was first proposed by Nguyen [81] in 2004, he first found out some drawbacks in the so-called PPP [67] and improved it. Then he extended the PPP to a QD protocol such that Alice and Bob can exchange their secret message directly. At the same time, Zhang [82] also gave the idea of secure direct bidirectional communication. In 2005 Xiao et al. [83] showed that the QD protocol

proposed by Nguyen was insecure against intercept and resend attack strategy. They modified the protocol in such a way that intercept and resend attack can be detected. After that, Xia et al. [84] proposed a QD protocol using the GHZ state, which is also a modified version of Nguyen's protocol. In 2006, Xin et al. [85] proposed a QD protocol based on single-photon. Recently various research work have been done in this area [86, 87, 88, 89, 90, 91, 92, 93, 3]. QSDC protocols for more than two parties are discussed in [94, 71, 95, 96, 97, 98].

Deterministic secure quantum communication (DSQC): This is another class of quantum secure communication protocol, which is a variant of deterministic QKD plus classical communication. This can also transmit messages securely and deterministically through a quantum channel. In usual QKD, the key is agreed first quantum mechanically and then used to encrypt the message into ciphertext, which is then communicated classically. The difference between QSDC and DSQC is that in the former no additional classical information (except those for eavesdropping detection) is required for decoding the secret message, whereas in the latter, after assuring the security of the transmission of qubits, at least one bit of classical information is required to decode each qubit. The first DSQC was proposed by Beige et al. [99], where the sender first chooses a key, encrypts the message with the key using a one-time-pad into ciphertext, and then sends the ciphertext deterministically through the quantum channel to the receiver. After assuring the security of the transmission, she sends the key via a classical communication. Various DSQC protocols are proposed and discussed in [100, 101, 102, 72, 103].

Quantum key agreement (QKA): Key agreement is one of the basic requirements of cryptography, which allows two or more parties to agree on the same secret key by exchanging their information over public channels. The difference between key distribution and key agreement protocol is as follows: in key distribution protocol, one party can determine a key and distribute it to the other legitimate parties. But in a key agreement protocol, all the parties involved in the protocol contribute their information equally in order to generate a shared secret key. In 1976, Diffie and Hellman first proposed a classical key agreement protocol [44], whose security is based on the assumption that the discrete logarithm problem is computationally hard. But, in 1999, Shor proposed a quantum algorithm, which can solve the discrete logarithm problem in polynomial time [104]. Thus some key agreement protocol was in need, such that, the security of that protocol does not depend on the computation complexity of some

mathematical problem. The first two-party QKA protocol was proposed by Zhou et al. [105], who used quantum teleportation [27] protocol without the classical communication in order to generate the key bit string between the two parties. However, in 2009, Tsai et al. pointed out that the above QKA protocol [105] is not a fair key agreement protocol [106]. Also in 2020, Das et al.[107] showed that the QKA protocol [105] is not consistent with allowed physical operation in quantum mechanics. The first secure two-party QKA protocol was proposed by Chong et al. in 2010 [108] and after that many other QKA protocols have been proposed by different groups of researchers [109, 110, 111, 112].

Quantum multi-party computation (QMPC): In multi-party computation (MPC), two or more parties exchange messages over a public channel and perform some local computation to jointly compute the value of a function on their private data as inputs. The requirement is that, after the end of the computation, each party will have the output of the function, but no party will have access to the input of any other party. QMPC is an interesting research area in quantum cryptography, where the parties possess some quantum states as inputs. Quantum secret sharing (QSS) [113, 97, 114, 115, 116], QMPC protocol for summation and multiplication [117, 118], quantum private comparison [119, 120, 121] are some examples of QMPC protocols.

Device independent (DI) protocols: Security of any quantum cryptographic protocol relies on two basic assumptions. The first one is that any eavesdropper must obey the laws of quantum physics, and the second one is that there is no unwanted information leakage from the laboratories of the legitimate parties. Moreover, the security proofs also assume that the devices used in the protocols are perfect, i.e., the authorized parties have full control of the state preparation and measurement devices. In 2007, Acín et al. first proposed the DI security proof for a QKD protocol [122], where they relax the assumption about using the perfect devices. DI protocols are based on the non-local correlation properties of entanglement and use the Bell inequality to establish the security analysis. Thereafter, a lot of DI protocols are proposed by many researchers [123, 124, 125, 126, 127, 128]. In 2019, Zhou et al. proposed the first DI-QSDC protocol [129] inspired by the DI-QKD protocols. They treat the quantum apparatuses as black boxes and perform the CHSH game to check the non-locality of the entangled particles.

Measurement device independent (MDI) protocols: However in practice, due to lack of perfect measurement devices, an adversary (Eve) can take advantage of this loophole of an imperfect measurement device and tries to steal information without being detected. In order to solve this problem, Lo et al. first proposed the concept of MDI-QKD protocol [63]. In MDI protocols, a UTP performs all the measurements during the protocol using imperfect devices, and thus it removes all the detector side-channel attacks introduced by Eve [130, 131, 132, 133]. Using the same technique as MDI-QKD, Zhou et al. proposed the first MDI-QSDC protocol [5], and some other MDI-QSDC and MDI-QD protocols also proposed recently [2, 134, 135, 136, 80, 137, 3, 138]. Similar to MDI-QKD, in 2021 Yang et al. proposed the first MDI-DSQC protocol [139] based on the polarization-spatial-mode hyperencoded qudits.

Authentication: For secure communication, authentication is always important as it prevents an eavesdropper to impersonate a legitimate party. There are two types of authentication in cryptography, one is user or identity authentication, and another is message authentication. The first process is used to check the authenticity of the users of the protocol, and the second process is to check the integrity of the transmitted information. Here in the thesis, we use both classical and quantum channels and assume that the classical channel is authenticated. That means, both user and message authentications are assumed for the classical channel, or in other words, we can say that an eavesdropper can eavesdrop on the information but can not modify it. Here the concept of public announcement [52] is used throughout the thesis. In 1995, Crépeau et al. [140] proposed the first quantum identification scheme based on quantum oblivious transfer [141]. QSDC with user authentication was first proposed by Lee et al. in 2006 based on Greenberger-Horne-Zeilinger (GHZ) states [4]. However, Zhang et al. showed that this protocol is not secure against the intercept-and-resend attack and proposed a revised version of the original protocol [142]. Later on, a number of new QSDC protocols with authentication are presented [143, 144, 145, 146].

In this thesis, we specially focus on various types of QSDC protocols. We present a QSDC protocol and some MDI-QSDC, MDI-QD, MDI-DSQC protocols with user authentication. We analyze the security of a QSDC protocol, an MDI-QSDC protocol, and an MDI-QD protocol. We present these protocols using block diagrams and explain in our own language. We improve the previous protocols and propose some modifications of the above protocols. We also present

a Q.Conf protocol by generalizing the previous MDI-QD protocol and using the algorithm of the Q.Conf protocol, we propose a quantum multi-party computation protocol to calculate the XOR value of n secret numbers. There are standard algorithm available for noisy quantum channel, quantum error correction, post-processing etc. If someone wants, he/ she can add those algorithm as wrapper/ layer. Here in this thesis, we do not focus on that part. Then we generalize the CHSH game, and we demonstrate how to distinguish between dimensions 2 and 3 for a special form of maximally entangled state using the generalized version of the CHSH game.

1.5 Thesis outline

This thesis is structured as follows:

- **Chapter 1** contains the general introduction of quantum information theory, quantum algorithms, quantum communication, and quantum cryptography.

- **Chapter 2** presents the background of our works. It contains some well-known QKD protocols, a survey of QSDC, QD, Q.Conf protocols and the idea of dimensionality testing. We give a brief description of each of the protocols we have improved in the Ph.D. tenure.

- **Chapter 3** justifies a security loophole of Yan et al.'s QSDC protocol with authentication [1]. We show that the QSDC protocol is not secure against intercept-and-resend attack and impersonation attack, an eavesdropper can get the full secret message by applying these attacks. We propose a modification of this protocol, which defeats the above attacks along with all the familiar attacks.

- **Chapter 4** contains a new theoretical scheme for QSDC with user authentication. Different from the previous QSDC protocols, the new protocol uses only one orthogonal basis of single-qubit states to encode the secret message. Moreover, this is a one-time and one-way communication protocol, which uses qubits prepared in a randomly chosen arbitrary basis, to transmit the secret message. We discuss the security of the proposed

protocol against some common attacks and show that no eavesdropper can get any information from the quantum and classical channels. We have also studied the performance of this protocol under realistic device noise. We have executed the protocol in the IBMQ Armonk device and proposed a repetition code-based protection scheme that requires minimal overhead.

- **Chapter 5** explores information leakage problems in the MDI-QSDC and MDI-QD protocols proposed by Niu et al. [2]. By analyzing these protocols we find some security issues in both these protocols. We show that a third party can get half of the secret information without any active attack. We also propose suitable modifications of these protocols to improve security.

- **Chapter 6** contains a new MDI-QSDC protocol with user authentication, where both the sender and the receiver first check the authenticity of the other party and then exchange the secret message. Then we extend this to an MDI quantum dialogue (QD) protocol, where both the parties can send their respective secret messages after verifying the identity of the other party. Along with this, we also report a new MDI-DSQC protocol with user identity authentication. Theoretical analyses prove the security of our proposed protocols against common attacks.

- **Chapter 7** contains two efficient MDI-QD protocols, which are improved versions of Maitra's MDI-QD protocol [3]. In the original work [3], to make the protocol secure against information leakage, the authors have discarded almost half of the qubits remaining after the error estimation phase, whereas we propose two modified versions of the MDI-QD protocol such that the number of discarded qubits is reduced to almost one-fourth of the remaining qubits after the error estimation phase. We use almost half of their discarded qubits along with their used qubits to make our protocol more efficient in qubits count. We show that both of our protocols are secure under the same adversarial model given in the MDI-QD protocol.

- **Chapter 8** contains a Q.Conf protocol, which is a process of securely exchanging messages between three or more parties, using quantum resources. In this chapter, we show

that the MDI-QD protocol [3] is insecure against intercept-and-resend attack strategy. We first modify this protocol and generalize this MDI-QD to a three-party quantum conference and then to a multi-party quantum conference. We also propose a protocol for quantum multi-party XOR computation. None of these three protocols proposed here use entanglement as a resource and we prove the correctness and security of our proposed protocols.

- **Chapter 9** generalizes the CHSH game by considering all possible non-constant Boolean functions and all possible measurement bases (up to certain precision). Based on the success probability computation, we construct several equivalence classes and show how they can be used to generate three classes of dimension distinguishers. In particular, we demonstrate how to distinguish between dimensions 2 and 3 for a special form of maximally entangled state.

- **Chapter 10** closes this thesis with a summary of the work and a discussion on possible future works.

Chapter 2

Background

In the last chapter, we gave a brief introduction to quantum information theory, quantum algorithms, quantum communication and quantum cryptography. In this chapter, we describe some important quantum cryptographic protocols.

2.1 Quantum key distribution protocols

QKD enables two or more parties to produce a shared random secret key in a secure manner using the tools of quantum mechanics and cryptography. The shared secret key then can be used to encrypt and decrypt secret messages. There are mainly two types of QKD schemes, one is the prepare-and-measure scheme, such as BB84 [52], B92 [57] etc. The other is the entanglement-based QKD, such as Ekert91 [55], BBM92 [56]. All the QKD protocols need quantum channels and an authenticated classical channel [147, 148], such that Eve can not modify the classical information at the time of communication. We now discuss some well-known QKD protocols. Also we estimate the resources for each protocol in tabular form in Table (2.1). For that part, we consider the resources only for key generation, and we ignore the security check process, since user can decide the number of qubits which they can use for the security checking. The classical information transmission is required in every protocol and the method is pubic announcement.

2.1.1 BB84 Protocol

In 1984, Bennett and Brassard proposed the first quantum cryptographic protocol [52, 6] to share a secret key between two parties, which is called the BB84 protocol. Let the parties be Alice and Bob, who want to share a secret key among themselves. The BB84 protocol is as follows:

1. Alice randomly chooses two $4n$-bit strings a and b. She prepares a finite sequence of $4n$ qubits Q from the bit strings a and b by using the following strategy. For $1 \leq i \leq 4n$,

   (a) if $a_i = 0,\ b_i = 0$, she prepares $Q_i = |0\rangle$,

   (b) if $a_i = 1,\ b_i = 0$, she prepares $Q_i = |1\rangle$,

   (c) if $a_i = 0,\ b_i = 1$, she prepares $Q_i = |+\rangle$,

   (d) if $a_i = 1,\ b_i = 1$, she prepares $Q_i = |-\rangle$.

2. Alice sends Q to Bob, who measures each qubits of Q in the Z or X basis at random. He makes a $4n$-bit string a', if the i-th measurement result is $|0\rangle$ or $|+\rangle$ ($|1\rangle$ or $|-\rangle$), then $a'_i = 0$ (1).

3. Alice publicly announces b. After a public discussion of the choice of bases, they discard the bits of a and a', where Bob chooses a different basis than Alice. It happens with probability $\frac{1}{2}$ and thus they have $2n$ bit strings approximately. If the case is not so, then they abort the protocol.

4. Alice randomly chooses n bits from the remaining $2n$ bits of a and tells the chosen positions to Bob. To check on Eve's interference, they publicly compare the values of those n check bits and calculate the error rate. If the error rate is not in the acceptable range, they abort the protocol.

5. Alice and Bob perform information reconciliation and privacy amplification process [149] to extract an m-bit ($m < n$) secret key from the remaining n bits.

2.1.2 B92 Protocol

This is a modified version of the BB84 protocol [57, 6], proposed by Bennett in 1992, which uses only two polarization states (conventionally, $|0\rangle$ and $|+\rangle$). The B92 protocol can be summarized in the following steps.

1. Alice randomly chooses an n-bit strings a and prepares a sequence Q of n qubits corresponding to a. The i-th qubit $Q_i = |0\rangle$ ($|+\rangle$) if $a_i = 0$ (1). She sends Q to Bob.

2. Bob randomly chooses an n-bit strings a' and measures the qubits of Q according to a', i.e., if $a'_i = 0$ (1), he choses the Z (X) basis to measure the i-th qubit Q_i.

3. From the measurement result, he obtains an n-bit strings b, i.e., $b_i = 0$ (1), if the i-th measurement result is $|0\rangle$ or $|+\rangle$ ($|1\rangle$ or $|-\rangle$).

4. Bob announces the bit strings b but keeps a' secret.

5. Alice and Bob discard the i-th bits of a and a' if $b_i = 0$, i.e., the cases where $a_i = a'_i$. The remaining bits are corresponding to the value $b_i = 1$, for which $a_i = a'_i \oplus 1$.

6. Then the shared secret key of Alice and Bob is $a = a' \oplus 1$.

2.1.3 Ekert's Protocol

Ekert's QKD Protocol [55, 150], also known as E91 protocol, which uses entangled pairs of photons, is a nice application of the Bell inequality for the generation of a secret key by two parties. Let us first describe the basis Z_θ, which is the Z basis rotated by angle θ. For this QKD protocol, Alice and Bob have three choices of basis and their basis sets are $\{Z_0, Z_{\frac{\pi}{4}}, Z_{\frac{\pi}{2}}\}$ and $\{Z_{\frac{\pi}{4}}, Z_{\frac{\pi}{2}}, Z_{\frac{3\pi}{4}}\}$ respectively. Then the QKD protocol is as follows:

1. Alice and Bob share EPR pairs in $|\Phi^-\rangle_{AB}$ state. Alice has particle A and Bob has particle B.

2. They measure their respective qubits by choosing a random basis, out of the three possible bases.

3. After that, Alice and Bob announce the basis for each measurement. They use the instances, where their chosen bases are different, to check the presence of Eve. Then calculate the CHSH quantity [32]

$$E = \langle \theta_1, \phi_1 \rangle - \langle \theta_1, \phi_3 \rangle + \langle \theta_3, \phi_1 \rangle + \langle \theta_3, \phi_3 \rangle ,$$

where θ_is and ϕ_is are Alice's and Bob's choice of bases, and $\langle \theta_i, \phi_j \rangle$ is the expectation value when Alice measures using Z_{θ_i} basis and Bob measures using Z_{ϕ_j} basis.

4. If $|E| \leq 2$, then it indicates the presence of some Eve, and in that case, Alice and Bob abort the protocol. For a perfectly secure channel, $|E| = 2\sqrt{2}$, which is the maximal violation of Bell inequality.

5. Alice and Bob consider the instances, where they chose the same bases, to generate their shared secret key. As their measurement results are anti-correlated, thus for each bit of the secret key is $a = 1 \oplus b$, where a and b are the respective measurement result of Alice and Bob.

2.1.4 BBM92 Protocol

In 1992, Bennett et al. proposed this protocol [56, 150], which is aimed as a critic to the Ekert's protocol's reliance on entanglement for security. In the BBM92 protocol, Alice and Bob use two measuring basis instead of three bases of the previous protocol. Here the two bases are the same as the BB84 protocol, i.e., they use only Z and X basis to measure the qubits. The QKD protocol is as follows:

1. Alice and Bob share n EPR pairs in $|\Phi^+\rangle_{AB}$ state. Alice has particle A and Bob has particle B.

2. Alice and Bob randomly select two n-bit string b and b' respectively. They measure their respective particles corresponding to b and b'. If the i-th bit of b (b') is 0, then Alice (Bob) measures her (his) qubit in Z-basis, otherwise in X-basis.

3. Alice obtains a n-bit string a, if the i-th measurement result is $|0\rangle$ or $|+\rangle$ ($|1\rangle$ or $|-\rangle$), then $a_i = 0$ (1). Similarly Bob obtains a'.

4. They compare the bit strings b and b' over public classical channel and discard the bits of a and a' for which the corresponding bits of b and b' are not equal. Then the shared secret key is the remaining bits of a and a' (for this case $a = a'$).

Note that in this protocol, the secret key is generated by both parties, and it is undetermined until at least one party performs a measurement on its particle.

2.1.5 SARG04 Protocol

Currently, the perfect single-photon sources are not available, and this causes photon number splitting attack [151]. In this attack model, when the sender Alice sends some photons to the receiver Bob through a quantum channel, then Eve measures the number of photons in the optical pulse. If it contains more than one photon, then Eve stole one photon and keeps it until post-processing, to listen to the communication between Alice and Bob, and thus she can learn all the information about the key without being detected. In 2004, Scarani et al. proposed a different kind of QKD protocol [152], called SARG04, to defeat the photon number splitting attack. Let us now describe this protocol.

1. Alice randomly chooses two n-bit strings a and b. She prepares a finite sequence of n qubits Q from the bit strings a and b by using the following strategy. For $1 \leq i \leq n$,

   (a) if $a_i = 0,\ b_i = 0$, she prepares $Q_i = |0\rangle$,

   (b) if $a_i = 1,\ b_i = 0$, she prepares $Q_i = |1\rangle$,

   (c) if $a_i = 0,\ b_i = 1$, she prepares $Q_i = |+\rangle$,

   (d) if $a_i = 0,\ b_i = 1$, she prepares $Q_i = |-\rangle$.

2. Alice sends Q to Bob, who measures each qubits of Q in the Z or X basis at random. For each i, he notes down the the i-th measurement basis and result as b'_i and $\mathcal{M}_i$ respectively.

3. Bob publicly announces that he has received and measured the qubits of Q.

4. For each i, Alice publicly announces the pair of states (Q_i^1, Q_i^2), where $Q_i^1 \in \{|0\rangle, |1\rangle\}$, $Q_i^2 \in \{|+\rangle, |-\rangle\}$ and $Q_i \in \{Q_i^1, Q_i^2\}$.

5. If $\mathcal{M}_i \in \{Q_i^1, Q_i^2\}$, then Bob can not distinguish between the two candidate states, and thus he announces the i-th bit is invalid.

6. If $\mathcal{M}_i \notin \{Q_i^1, Q_i^2\}$, then Bob surely knows that he has chosen the wrong basis and he can guess the correct state of Q_i. In this case the he announces the i-th bit is valid and the corresponding secret bit is $b_i = b_i' \oplus 1$.

2.1.6 QKD with user authentication

User identity authentication is one of the basic tasks of cryptography that can defeat the impersonation attack. In 2000, Ljunggren et al. proposed some QKD schemes with user identity authentication with the help of a trusted third party Trent [153]. Here we present one of those schemes, where Alice and Bob want to share a secret key using quantum methods.

1. Trent and Alice (BOB) use the BB84 protocol [52] to generate a secret key K_A (K_B).

2. Trent sends the key K to Alice (Bob) encrypted with the secret key K_A (K_B).

3. Alice and Bob can send each other the secret message encrypted with the key K.

Note that, since Trent knows the shared secret key K, he can also listen to the encrypted communication. In the same paper, the authors also propose some QKD with authentication using entangled particles.

In 2001, Shi et al. [154] proposed a scheme that allows the simultaneous realization of QKD and quantum authentication based on entangled states. However, Wei et al. [155] points out a weakness in Shi et al.'s scheme [154], in which a malicious user can impersonate a legitimate participant without being detected. Furthermore, they proposed an improved scheme to avoid this weakness. There are many other protocols in this domain, and some of them are discussed in [156, 157, 158, 159, 160, 161]

2.1.7 Device independent QKD

Quantum cryptography promises unconditional security based on the law of physics. Security proofs of the QKD protocols assume that the legitimate parties have perfect control of the state preparation and of the measurement devices, which is difficult to follow in practical life. In actual implementations, if a QKD protocol does not follow one of the above two assumptions, then it compromises the security, and Eve can get the secret key without introducing any error in the channel. These types of attacks are called side-channel attacks [162, 163, 164, 165]. Now the question is, can this security be guaranteed to the users, who may not trust the quantum devices used to implement the protocol? In 1998, Mayers et al. [166] approach to this question in the form of a new security paradigm called device independence. The term "device independence" (DI) was only introduced much later, in 2007 by Acín et al., who proposed a DI security proof [122] of the protocol [167] based on CHSH inequality. The protocol [122] is as follows.

1. Alice and Bob share EPR pairs in $|\Phi^+\rangle_{AB}$ state.

2. Alice measures her qubits randomly in basis $\mathcal{B}_{A_0}$, $\mathcal{B}_{A_1}$ and $\mathcal{B}_{A_2}$, where $\mathcal{B}_{A_j} = \{|0\rangle + e^{iA_j}|1\rangle, |0\rangle - e^{iA_j}|1\rangle\}$ and $j \in \{0,1,2\}$ with $A_0 = \frac{\pi}{4}, A_1 = 0, A_2 = \frac{\pi}{2}$. Bob measures his qubits randomly in basis $\mathcal{B}_{B_1}$ and $\mathcal{B}_{B_2}$, where $\mathcal{B}_{B_j} = \{|0\rangle + e^{iB_j}|1\rangle, |0\rangle - e^{iB_j}|1\rangle\}$ and $j \in \{1,2\}$ with $B_1 = \frac{\pi}{4}, B_2 = -\frac{\pi}{4}$. All the measurement results a_0, a_1, a_2, b_1, b_2 have binary outcomes labeled by ± 1.

3. Alice and Bob reveal their measurement basis and calculate the value of the CHSH polynomial $S = \langle a_1 b_1\rangle + \langle a_2 b_1\rangle + \langle a_1 b_2\rangle - \langle a_2 b_2\rangle$, where $\langle a_i b_j\rangle = \Pr(a = b \mid ij) - \Pr(a \neq b \mid ij)$.

4. If $S > 2$, then they consider the measurement outcomes corresponding to the bases $\mathcal{B}_{A_0}$ and $\mathcal{B}_{B_1}$ as the secret key.

Some other DI-QKD protocols are discussed in [125, 127, 168, 169, 126, 128, 170].

2.1.8 Measurement device independent QKD

This approach of DI-QKD is conceptually very powerful, but unfortunately, it is difficult to implement with current technology. In 2012, Lo et al. [63] first proposed the idea of MDI-QKD to solve the problem of all detector side-channel attacks [132, 171, 163, 162]. In MDI-QKD protocol, both legitimate parties, namely, Alice and Bob send quantum signals to an untrusted third party (UTP), with the assumption that Alice and Bob have almost perfect state preparation. The detail protocol [63] is as follows.

1. Alice (Bob) randomly chooses two n-bit strings a and a' (b and b'). She (he) prepares a finite sequence of n qubits Q_A (Q_B) from the bit strings a and a' (b and b') by using the strategy of BB84 protocol. For $1 \leq i \leq n$,

   (a) if a_i $(b_i) = 0$, a'_i $(b'_i) = 0$, she (he) prepares Q_{A_i} $(Q_{B_i}) = |0\rangle$,

   (b) if a_i $(b_i) = 1$, a'_i $(b'_i) = 0$, she (he) prepares Q_{A_i} $(Q_{B_i}) = |1\rangle$,

   (c) if a_i $(b_i) = 0$, a'_i $(b'_i) = 1$, she (he) prepares Q_{A_i} $(Q_{B_i}) = |+\rangle$,

   (d) if a_i $(b_i) = 0$, a'_i $(b'_i) = 1$, she (he) prepares Q_{A_i} $(Q_{B_i}) = |-\rangle$.

2. They send their sequences Q_A and Q_B to an UTP.

3. Alice and Bob randomly chose some qubits, and apply decoy state techniques [61, 62, 172] to estimate the gain and quantum bit error rate (QBER) for this transmission.

4. The UTP measures each pair of qubits (Q_{A_i}, Q_{B_i}) in Bell basis and announces the result $\mathcal{M}_i$, where $1 \leq i \leq n$.

5. Alice and Bob announce the bit strings a' and b' respectively, i.e., the preparation bases corresponding to their qubits. They keep the i-th measurement result $\mathcal{M}_i$ only when the bases are same, i.e., $a'_i = b'_i$, and otherwise they discard $\mathcal{M}_i$.

6. They get the shared secret key from the remaining measurement results and the bases as follows:

   - $a'_i = b'_i = Z$:

- $\mathcal{M}_i = |\Phi^+\rangle$ or $|\Phi^-\rangle \Rightarrow \ a_i = b_i$.
- $\mathcal{M}_i = |\Psi^+\rangle$ or $|\Psi^-\rangle \Rightarrow \ a_i = b_i \oplus 1$.

- $a'_i = b'_i = X$:
  - $\mathcal{M}_i = |\Phi^+\rangle$ or $|\Psi^+\rangle \Rightarrow \ a_i = b_i$.
  - $\mathcal{M}_i = |\Phi^-\rangle$ or $|\Psi^-\rangle \Rightarrow \ a_i = b_i \oplus 1$.

After that many MDI-QKD protocols were proposed by different group of researchers [173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188].

2.1.9 Multi-party QKD

In 2007, Matsumoto proposed the first multi-party QKD protocol [189] without using entanglement and we now discuss the protocol. Let Alice, Bob and Charlie be the three legitimate parties who want to generate a shared secret key among themselves.

1. Alice prepares two identical sequences Q_1 and Q_2 of single qubits states, where the qubits are randomly chosen from Z and X bases. She sends the Q_1 (Q_2) to Bob (Charlie).

2. Bob (Charlie) measures each received qubit in Z or X basis randomly.

3. Alice publicly announces the preparation bases of the qubits, and Bob, Charlie announces the measurement bases of the qubits. They keep the qubits only when these three basis are equal and otherwise discard these.

4. Among the remaining qubits, let there be $2n$ number of qubits prepared in Z-basis. Define three $2n$-bit strings a, b, c, and for $1 \leq i \leq 2n$,
   - $a_i = 0$ (1) if Alice prepared the i-th qubit as $|0\rangle$ ($|1\rangle$),
   - $b_i = 0$ (1) if Bob's measurement outcome for the i-th qubit is $|0\rangle$ ($|1\rangle$),
   - $c_i = 0$ (1) if Charlie's measurement outcome for the i-th qubit is $|0\rangle$ ($|1\rangle$).

5. Also let there be $2n'$ number of qubits prepared in X-basis. Define three $2n'$-bit strings α, β, γ, and for $1 \leq i \leq 2n'$,

- $\alpha_i = 0$ (1) if Alice prepared the i-th qubit as $|+\rangle$ ($|-\rangle$),
- $\beta_i = 0$ (1) if Bob's measurement outcome for the i-th qubit is $|+\rangle$ ($|-\rangle$),
- $\gamma_i = 0$ (1) if Charlie's measurement outcome for the i-th qubit is $|+\rangle$ ($|-\rangle$).

6. Alice randomly chooses a subset S of $\{1, 2, \ldots, 2n\}$ such that $|S|$ = cardinality of the set $S = n$. She announces the subset S, and for each $i \in S$, they publicly compare the bits a_i, b_i, c_i to compute the error rate q_1, where

$$q_1 = \max\left\{\frac{|\{i \in S : a_i \neq b_i\}|}{|S|}, \frac{|\{i \in S : a_i \neq c_i\}|}{|S|}\right\}.$$

7. Alice randomly chooses a subset S' of $\{1, 2, \ldots, 2n'\}$ such that $|S'| = n'$. She announces the subset S', and for each $i \in S'$, they publicly compare the bits $\alpha_i, \beta_i, \gamma_i$ to compute the error rate q_2, where

$$q_2 = \frac{|\{i \in S' : \alpha_i = \beta_i \neq \gamma_i \text{ or } \alpha_i = \gamma_i \neq \beta_i\}|}{|S'|}.$$

8. Alice, Bob and Charlie decide a linear code C_1 of length n and parity check matrix H, such that the decoding error probability of C_1 is sufficiently small over all the binary symmetric channel whose crossover probability is close to q_1.

9. For $i \in S$, they discard the i-th bit from a, b, c and relabel the bit strings. Then each bit string contains n bits.

10. Alice chooses a subspace C_2 of C_1 of dimension $nh(q_2)$, where h is the binary entropy function.

11. Alice publicly announces the syndrome Ha of the linear code C_1 and subspace C_2. The final shared secret key is the coset $a + C_2$.

Other multi-party QKD protocols are discussed in [190, 191, 192].

Table 2.1: Resource estimation of the discussed QKD protocols

Protocol	**No. of Single Qubit**	**No. of Entangled Qubit**	**Measurement Basis**	**Qubit Transmission**	**Length of the Key**
BB84 [52]	$2n$	0	Z, X	$2n$	n
B92 [57]	$2n$	0	Z, X	$2n$	n
E91 [55]	0	n EPR pairs	$Z_0, Z_{\frac{\pi}{4}}, Z_{\frac{\pi}{2}}, Z_{\frac{3\pi}{4}}$	No	$2n/9$
BBM92 [56]	0	n EPR pairs	Z, X	No	$n/2$
SARG04 [152]	n	0	Z, X	n	$n/2$
DI-QKD [122]	0	n	$\mathcal{B}_{\frac{\pi}{4}}, \mathcal{B}_0, \mathcal{B}_{\frac{\pi}{2}}, \mathcal{B}_{-\frac{\pi}{4}}$	No	$n/6$
MDI-QKD [63]	$2n$	0	Bell basis	$2n$	$n/2$
3-Party QKD [189]	$2n$	0	Z, X	$2n$	$n/8$

2.2 Quantum secure direct communication protocols

QSDC can send a secret message through a quantum channel, without any previously shared key. Each of the legitimate parties encodes and decodes the message using some predefined encoding and decoding rules. Now we discuss some QSDC protocols. Also we estimate the resources for those protocols in tabular form in Table (2.4). For that part, we consider the resources only for message transmission, and we ignore the security and integrity check processes, since user can decide the number of qubits which they can use for those checking. The classical information transmission is required in every protocol and the method is pubic announcement.

2.2.1 The first QSDC protocol

In 2002, Long and Liu [58] proposed a theoretical QKD scheme using EPR pairs. Although it was designed for key distribution, but in this protocol, the key was prepared before it was sent, which is a clear indication that it is a QSDC protocol.

The protocol is as follows.

1. The message bits are encoded in EPR pairs by using the following rule: $00 \rightarrow |\Phi^+\rangle$, $01 \rightarrow |\Phi^-\rangle$, $10 \rightarrow |\Psi^+\rangle$ and $11 \rightarrow |\Psi^-\rangle$.

2. Alice prepares EPR pairs corresponding to her message bits and she takes one qubit from each EPR pair to form a sequence Q_A. The remaining partner qubit of each EPR pair forms another sequence Q_B and she sends it to Bob.

3. Bob chooses some qubits of Q_B and measures those qubits randomly in Z basis or X basis. Then he tells the positions and the measurement bases of those qubits to Alice, who measures the partner qubits from Q_A in proper bases. They compare the measurement results publicly to check eavesdropping.

4. If there is no eavesdropper, then Alice sends Q_A to Bob and he measures each pair of qubits (one from Q_A and another from Q_B) in Bell basis. From the measurement result, Bob gets the message.

5. They choose some random positions of the message bits to check the integrity of the message.

2.2.2 Two-step QSDC protocol using EPR pair

The two-step QSDC scheme [66] generalizes the basic idea of the previous QKD protocol [58]. It is the first secure model for quantum direct communication and can be described in brief as follows.

1. Alice and Bob agree on the message encoding rule as: $11 \rightarrow |\Phi^+\rangle$, $10 \rightarrow |\Phi^-\rangle$, $01 \rightarrow |\Psi^+\rangle$ and $00 \rightarrow |\Psi^-\rangle$.

2. Alice prepares N EPR pairs in $|\psi^-\rangle$ states and she takes one qubit from each EPR pair to form a sequence Q_A. The remaining partner qubit of each EPR pair forms another sequence Q_B and she sends it to Bob.

3. Bob chooses some qubits of Q_B and measures those qubits randomly in Z basis or X basis. Then he tells the positions and the measurement bases of those qubits to Alice, who measures the partner qubits from Q_A in proper bases. They compare the measurement results publicly to check eavesdropping.

4. If there is no eavesdropper, then Alice encodes her message bits by applying the Pauli operators on the qubits of Q_A. She applies the unitary U_0, U_1, U_2, U_3 to encode the bits $00, 01, 10, 11$ respectively.

5. Alice sends Q_A to Bob and he measures each pair of qubits (one from Q_A and another from Q_B) in Bell basis. From the measurement result, Bob gets the message.

6. They choose some random positions of the message bits to check the integrity of the message.

2.2.3 Ping-pong protocol

In 2002, Boström and Felbinger [67] proposed a quasi-secure direct communication scheme based on entangled pair of qubits, i.e, an eavesdropper may be able to gain a small amount of secret information before her presence is detected. Let Alice be the sender and Bob be the receiver of the secret message $x = (x_1, x_2, \ldots, x_n)$, where $x_i \in \{0, 1\}$ for $1 \leq i \leq n$. Then the protocol is as follows:

1. Protocol is initialized and $i = 0$.

2. $i = i + 1$. Bob first prepares an EPR pair AB in $|\Psi^+\rangle$ state and sends the qubit A to Alice.

3. After receiving the qubit, Alice chooses either control mode or message mode with probabilities c and $1 - c$ respectively.

   (a) Control mode: Alice measures the qubit A in Z-basis and sends the measurement result to Bob classically. Then Bob measure his qubit B in Z-basis and compares the measurement result with Alice's measurement result. If both the measurement results are same, then presence of Eve is detected and they abort the protocol. Else $i = i - 1$ and go to the step 2.

   (b) Message mode: Alice encodes her i-th message bit on qubit A by applying the unitary U_0 and U_1 corresponding to the value 0 and 1 respectively. She sends it back to Bob and he measures the two-qubit state AB in Bell basis. Bob decodes the message bit from the measurement result. The final state $|\Psi^+\rangle$ ($|\Psi^-\rangle$) implies the message bit is 0 (1).

4. If $i < n$, goto step 2, else the message is transmitted successfully.

But in 2003, Wójcik [193] analyzed the security of the ping-pong protocol and showed that this is not secure in the case of considerable quantum channel losses. Also in 2004, Cai [194] showed that an eavesdropper can apply the denial of service attack on the ping-pong protocol, which causes transmission of a random string instead of a useful message. In the same year, Nguyen [81] pointed out a drawback of the ping-pong protocol and then improved it towards a quantum dialogue (QD) protocol, where both the legitimate parties can exchange their secret message simultaneously.

In 2004, Cai and Li [195] improved the capacity of the ping-pong protocol by introducing two additional unitary operations U_2 and U_3 to encode two bits of information in each message mode. They proved the security of their protocol against Wójcik [193] eavesdropping scheme by using two conjugate bases for measurement in the control mode. Also, they discussed that a message authentication method can protect their protocol against the denial of service attack [194].

Again in 2007, Deng et al. [196] showed that if there is a non-zero error rate introduced due to channel noise, then the ping-pong protocol can eavesdrop freely.

2.2.4 QSDC with quantum teleportation

In 2004, Yan et. al. [100] proposed a QSDC scheme based on EPR pairs and teleportation [27] between the legitimate parties. The protocol is described below where Bob wants to send a message to Alice.

1. Alice and Bob share a set of EPR pairs in $|\Phi^+\rangle_{AB}$ states.

2. Bob prepares a qubit $|\Psi\rangle_C$ in the state $|+\rangle$ or $|-\rangle$ corresponding to 0 or 1 respectively.

3. Bob measures the particles B and C in Bell basis and announces the measurement outcome. Then the state of Alice's particle becomes $|\Psi\rangle_A$ after applying a fixed unitary transformation to complete the teleportation process [27].

4. Alice measures $|\Psi\rangle_A$ in X-basis and gets the secret message of Bob.

2.2.5 Controlled quantum teleportation and QSDC

In 2004, Gao et. al. [197] proposed controlled QSDC based on controlled quantum teleportation protocol. In this protocol, Alice, the sender of the secret message, encodes her message by preparing qubits in X-basis ($|+\rangle$ and $|-\rangle$ for 0 and 1 respectively) and transmits them to Bob supervised by the controller Charlie. The controlled QSDC scheme works as follows.

1. Alice, Bob and Charlie share a set of triplets of qubits in $|\xi\rangle_{ABC}$ states, where

$$|\xi\rangle_{ABC} = \frac{1}{2}(|000\rangle + |110\rangle + |101\rangle + |011\rangle). \tag{2.1}$$

2. Alice wants to teleport the state $|\phi\rangle_M = \frac{1}{\sqrt{2}}(|0\rangle + b\,|1\rangle)$, where $b = 1$ and -1 corresponding to message bit 0 and 1. The quantum state of the whole system

$$|\phi\rangle_M\,|\xi\rangle_{ABC} = \frac{1}{\sqrt{2}}(|0\rangle + b\,|1\rangle) \otimes \frac{1}{2}(|000\rangle + |110\rangle + |101\rangle + |011\rangle). \tag{2.2}$$

3. If Charlie allows the communication, then he measures the C-particle in Z-basis and publicly announces the result.

4. Alice measures her particles M and A in Bell basis and announces the result.

5. Bob recovers the signal state $|\phi\rangle_B = \frac{1}{\sqrt{2}}(|0\rangle + b\,|1\rangle)$ by applying appropriate unitary. He measures the B-particle in X-basis and reads out Alice's messages.

Another controlled qsdc scheme was proposed by Gao [198] by using GHZ state and controlled teleportation [199]. In 2007, Xia et. al. proposed a controlled QSDC protocol [200] by using a 2-dimensional GHZ entangled state and a 3-dimensional Bell-basis state via high-dimension quantum superdense coding [201, 27, 202], local collective unitary operations and entanglement swapping.

2.2.6 QSDC using entanglement swapping

In 2004, Gao et. al. [203] proposed a QSDC scheme based on entanglement swapping [204] of EPR pairs and GHZ basis measurement. Here, Alice, is the sender and Bob is the receiver

of the secret message. The unitary operators used to encode the secret message are $\sigma_{00} = U_0, \sigma_{01} = U_2, \sigma_{10} = U_3, \sigma_{11} = U_1$ and $\sigma_0 = U_0, \sigma_1 = U_2$. The steps of the protocol are as follows.

1. Alice and Bob share enough number of EPR pairs to initiate the protocol. They randomly divide all the EPR pairs into N ordered groups $\{\xi(1)_{12}, \eta(1)_{34}, \zeta(1)_{56}\}$, $\{\xi(2)_{12}, \eta(2)_{34}, \zeta(2)_{56}\}, \ldots, \{\xi(N)_{12}, \eta(N)_{34}, \zeta(N)_{56}\}$, where $\xi(n)_{12}, \eta(n)_{34}, \zeta(n)_{56}$ $(1 \leq n \leq N)$ are EPR pairs and Alice (Bob) has the 1st, 3rd and 5th (2nd, 4th and 6th) particles.

2. Alice applies σ_{ij} and σ_k on her 1st and 3rd particles to encode the message bits ij and k respectively.

3. Alice jointly measures her three qubits in the GHZ basis and informs Bob that she has made the measurement.

4. Bob measures his three qubits in GHZ basis and from his measurement outcome he infers Alice's outcome.

5. Alice announces her measurement result publicly and from the result, Bob gets the secret message.

2.2.7 QSDC with quantum one-time-pad

In 2003, Deng and Long [68] proposed the first QSDC protocol using single qubits and claimed that their scheme is unconditionally secure even in a noisy channel. Here the message receiver, namely Bob, first initiates the communication by preparing single-qubit states randomly in Z and X bases, and then sends these states to the sender Alice. The details of the protocol are as follows:

1. Bob prepares a sequence Q of single-qubit states, where each Q_i is randomly chosen from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and sends the sequence Q to Alice.

2. Alice chooses some qubits of Q and randomly measures in Z and X bases. Then they publicly discuss the positions and the measurement results to calculate the error rate in the channel. A higher error rate implies the presence of some eavesdroppers and then

they abort. Otherwise, Alice applies the unitary U_0 and U_3, on the remaining qubits, to encode her message bit 0 and 1 respectively. Note that U_0 does not change the states and U_3 flips the states, i.e., $U_3|0\rangle = |1\rangle$, $U_3|1\rangle = |0\rangle$, $U_3|+\rangle = |-\rangle$ and $U_3|-\rangle = |+\rangle$.

3. Alice sends those encoded qubits to Bob, who measures those qubits in proper bases and gets the secret message.

In 2005, Hoffmann et. al. [205] showed that the above QSDC protocol [68] is not unconditionally secure for the case of a noisy channel by giving an undetectable attack scheme. As a reply to the comment of Hoffmann et. al. [205], the authors of [68] showed that the QSDC protocol is secure against the attack strategy described in [205] by using quantum privacy amplification directly [206, 207].

2.2.8 QSDC using multi-particle GHZ state

In 2005, Wang et.al [70] proposed a multi-step QSDC protocol using blocks of maximally entangled three-particle GHZ states. Before describing the protocol, let us first relabel the eight independent GHZ-states as:

$$|\psi_1\rangle = |G_1^+\rangle\,; \qquad |\psi_2\rangle = |G_1^-\rangle\,; \qquad |\psi_3\rangle = |G_4^+\rangle\,; \qquad |\psi_4\rangle = |G_4^-\rangle\,;$$
$$|\psi_5\rangle = |G_3^+\rangle\,; \qquad |\psi_6\rangle = |G_3^-\rangle\,; \qquad |\psi_7\rangle = |G_2^-\rangle\,; \qquad |\psi_8\rangle = |G_2^-\rangle\,.$$

Next, eight unitary operations, which are used to encode the secret message are:

$$O_1 = U_1 \otimes U_1; \qquad O_2 = U_0 \otimes U_1; \qquad O_3 = U_3 \otimes U_1; \qquad O_4 = U_2 \otimes U_1;$$
$$O_5 = U_0 \otimes U_2; \qquad O_6 = U_1 \otimes U_2; \qquad O_7 = U_2 \otimes U_2; \qquad O_8 = U_3 \otimes U_2,$$

where for $1 \leq k \leq 8$, $\quad O_k|\psi_1\rangle = |\psi_k\rangle$.

Now, each of the states $|\psi_k\rangle$ represents a three-bit binary number corresponding to the decimal number $(k-1)$. The protocol is as follows:

1. Alice prepares N GHZ states, each of them is in state $|\psi_1\rangle_{ABC}$. Alice takes the C-particle from each GHZ state and sends the C-sequence to Bob.

2. After Bob receives the C-sequence, then Alice and Bob check the security of the channel by measuring the particles.

3. Alice encodes her message on the AB-particles by applying the above unitary operators and sends the sequence of B-particles to Bob. Again they do a security check, and if the channel is secure then Alice sends the A-sequence to Bob.

4. Bob measures ABC-particles in GHZ basis and reads Alice's message.

2.2.9 QSDC with W state

In 2006, Jing et. al. [208] proposed a theoretical QSDC scheme based on four-qubit W states and Bell measurements. The four-qubit symmetric W state can be written as

$$\begin{aligned} |W_4\rangle &= \frac{1}{2}(|1000\rangle + |0100\rangle + |0010\rangle + |0001\rangle)_{1234} \\ &= \frac{1}{2}[|\Psi^+\rangle_{12}(|\Phi^+\rangle + |\Phi^-\rangle)_{34} + (|\Phi^+\rangle + |\Phi^-\rangle)_{12}|\Psi^+\rangle_{34}]. \end{aligned} \tag{2.3}$$

Suppose Alice wants to transmit a message to Bob, then the steps of the protocol are as follows:

1. Alice prepares N number of symmetric W state $|W_4\rangle$. She makes two sequences of qubits A and B, where A contains the 1st and 2nd particles of each W state, whereas B contains the 3rd and 4th particles of each W state, and sends the B sequence to Bob.

2. After Bob receives the B sequence, they check the security of the channel by measuring some randomly chosen qubits in Z or X bases randomly.

3. If the channel is secure, Alice measures the 1st and 2nd particles of each W state in Bell basis. She encodes her message by using the following rule: $|\Psi^+\rangle \rightarrow 0, \quad |\Phi^\pm\rangle \rightarrow 1$. If the measurement result is the same as her message bit, then she sends the classical information 0 to Bob, and otherwise sends 1.

4. Bob performs Bell measurement on 3rd and 4th particles, and from the result and the classical information of Alice, Bob reads the secret message of Alice.

However, Jun et. al. [209] pointed out a security loophole of the above QSDC protocol [208] and showed that an eavesdropper can get the full secret message by applying the intercept-and-resend attack strategy. They also proposed an improvement to fix this security issue.

2.2.10 QSDC with quantum encryption

In 2007, Han et.al [73] presented a QSDC scheme with quantum encryption using controlled-not (CNot) gate. Here Alice has a secret message, which she wants to send to Bob. The two-qubit pure entangled states $|\Psi\rangle_{AB} = \frac{1}{\sqrt{2}}(a|0\rangle|0\rangle + b|1\rangle|1\rangle)$ and $|\Phi\rangle_{AB} = U_2^A \otimes U_2^B |\Psi\rangle_{AB}$ are used in this protocol. Now, let us describe the QSDC scheme in detail as follows.

1. Bob prepares n two-qubit entangled pairs randomly from $\{|\Psi\rangle_{AB}, |\Phi\rangle_{AB}\}$ and sends the sequence of A-particles, with some decoy qubits in some random positions of the sequence, to Alice. They use those decoy photons to check the security of the channel.

2. Alice prepares a sequence of qubits $S_T = \{\gamma_i\}_{i=1}^n$, where $\gamma_i = |0\rangle$ or $|1\rangle$ according to her secret message bit 0 or 1 respectively.

3. For $1 \leq i \leq n$, Alice applies a $CNOT$ gate with control qubit A_i and target qubit γ_i. Alice sends S_T, with some decoy photon inserted in some random positions, to Bob.

4. After ensuring the security of the channel, Bob applies a $CNOT$ gate with control qubit B_i and target qubit γ_i $(1 \leq i \leq n)$. Then he measures each γ_i in Z-basis and gets the secret message of Alice.

2.2.11 QSDC with χ-type entangled states

In 2008, Lin et. al. [74] proposed an efficient QSDC protocol based on four-qubit χ-type entangled state [210, 211], where

$$|\chi^{00}\rangle_{3214} = \frac{1}{2\sqrt{2}}(|0000\rangle - |0011\rangle - |0101\rangle + |0110\rangle + |1001\rangle + |1010\rangle + |1100\rangle + |1111\rangle)_{3214}, \quad (2.4)$$

where the subscripts denote different qubits. The sender Alice applies the unitary U_0, U_1, U_2, U_3 to encode the 2-bit classical information $00, 11, 01, 10$ respectively. An explicit description of the protocol is as follows.

1. Alice prepares n number of χ-type four-particle entangled states $|\chi^{00}\rangle_{3214}$ and she makes four sequences $S_1 = \{P_1^1, P_1^2, \ldots, P_1^n\}$, $S_2 = \{P_2^1, P_2^2, \ldots, P_2^n\}$, $S_3 = \{P_3^1, P_3^2, \ldots, P_3^n\}$

and $S_4 = \{P_4^1, P_4^2, \ldots, P_4^n\}$. Here, the subscripts $1, 2, 3, 4$ represent four different particles in each χ-type state $|\chi^{00}\rangle_{3214}^i$, for $1 \leq i \leq n$. She keeps sequences S_1 and S_3, and sends the sequences S_2 and S_4 to Bob.

2. After Bob receives the sequences, they measure some randomly chosen qubits to check the security of the channel.

3. Alice applies the unitary operators on her remaining particles corresponding to her message. Then she sends S_1 and S_3 to Bob.

4. Bob measures each four-particle state in the basis $\{|\chi^{ij}\rangle_{3214} = U_1^i U_2^j |\chi^{00}\rangle_{3214} | \ i, j = 0, 1, 2, 3\}$ and gets the secret message of Alice.

2.2.12 QSDC with user authentication

In 2005, Lee et al. [4] proposed the first QSDC protocol with user authentication using GHZ states and one-way hash functions. A one-way hash function h is defined as $h : \{0,1\}^* \times \{0,1\}^c \to \{0,1\}^l$, where $*$ denotes an arbitrary length, c is a counter and l is a fixed number. Let the users Alice and Bob have their secret identities and one-way hash functions Id_A, h_A and Id_B, h_B respectively. Before sending the secret message, the users authenticate each other with the help of a trusted third party Trent, who knows Id_A, h_A and Id_B, h_B. Suppose Alice wants to send a message to Bob, then the protocol is as follows.

1. Trent generates N GHZ tripartite states $|\Psi\rangle = |\psi_1\rangle \ldots |\psi_N\rangle$ where $|\psi_i\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ATB}$ for $1 \leq i \leq N$ and the subscripts A, T and B correspond to Alice, Trent, and Bob, respectively.

2. Trent encodes Alice's and Bob's particles with their authentication keys $h_A(Id_A, c_A)$ and $h_B(Id_B, c_B)$ respectively, where $c_A(c_B)$ is the counter call of Alice's (Bob's) hash function. If the i-th bit of $h_A(Id_A, c_A)$ $(h_B(Id_B, c_B))$ is 0, then Trent applies I, and otherwise he applies H on Alice's (Bob's) particle.

3. Trent sends the A-particles to Alice and the B-particles to Bob. He keeps the T-particles.

4. Alice and Bob apply the same unitary operators as Trent on the received qubits corresponding to their authentication keys.

5. Alice and Bob measure some randomly chosen qubits and compare the results publicly. If the error rate is high, then they abort the protocol. Otherwise, they can confirm that the other party is legitimate and the channel is secure.

6. Alice inserts some check bits on random positions of the secret message m. Then she encodes the new bit-string m' on the qubits which are not measured in the previous step. Alice applies H if the corresponding bit of m' is 0. Otherwise, she first applies σ_x and then H.

7. Alice sends the encoded A-particles to Bob, who makes Bell measurements on the pair of particles AB.

8. Trent measures his particles in X-basis and announces the results. From Bob's measurement results, and the announced results by Trent, Bob decodes the secret message of Alice using Table 2.2.

Table 2.2: Decoding rule of the QSDC protocol [4]

Secret bit of Alice	**Encoding operation**	**Measurement result of Trent**	**Measurement result of Bob**	**Decoded bit**
0	H	$\|+\rangle$	$\|\Phi^-\rangle$	0
			$\|\Psi^+\rangle$	0
		$\|-\rangle$	$\|\Phi^+\rangle$	0
			$\|\Psi^-\rangle$	0
1	HX	$\|+\rangle$	$\|\Phi^+\rangle$	1
			$\|\Psi^-\rangle$	1
		$\|-\rangle$	$\|\Phi^-\rangle$	1
			$\|\Psi^+\rangle$	1

The authors also proposed another protocol [4], where Alice sends the encoded qubits to Trent, who makes Bell measurements on the AT-particles pairs and announces the results. Bob measures his B-particles in X-basis and decodes the secret message bits of Alice.

However, Zhang et al. showed that these protocols are not secure against the intercept-and-resend attack and proposed revised versions of the original protocols [142]. Later on, a

number of new QSDC protocols with authentication are presented [212, 213, 214, 215, 143, 216, 217, 218, 219, 220, 144, 145, 146, 221].

2.2.13 Device independent QSDC

In 2019, Zhou et. al. [129] proposed the first device-independent quantum secure direct communication (DI-QSDC) protocol, where the legitimate parties, namely, Alice and Bob require to perform the Bell CHSH test [31, 32] to check the security of the protocol. The violation of the Bell CHSH inequality proves that the device-independent protocol is secure. The encoding rule for this DI-QSDC is: the Bell states $|\Phi^+\rangle$, $|\Phi^-\rangle$, $|\Psi^+\rangle$, $|\Psi^-\rangle$ represents the two-bits classical information $00,\ 01,\ 10,\ 11$ respectively. The DI-QSDC protocol is described as follows.

1. Alice prepares N EPR pairs in $|\Phi^+\rangle$ state and makes two sequences of single qubits C, M containing the partner qubits of those EPR pairs. She sends the C sequence to Bob through the quantum channel.

2. To check the security of the channel, Alice announces some random positions of the M sequence. She measures the selected qubits randomly in basis $\mathcal{B}_{A_0}$, $\mathcal{B}_{A_1}$ and $\mathcal{B}_{A_2}$, where $\mathcal{B}_{A_j} = \{|0\rangle + e^{iA_j}|1\rangle, |0\rangle - e^{iA_j}|1\rangle\}$ and $j \in \{0,1,2\}$ with $A_0 = \frac{\pi}{4}, A_1 = 0, A_2 = \frac{\pi}{2}$. Bob measures the corresponding partner qubits from the C sequence randomly in basis $\mathcal{B}_{B_1}$ and $\mathcal{B}_{B_2}$, where $\mathcal{B}_{B_j} = \{|0\rangle + e^{iB_j}|1\rangle, |0\rangle - e^{iB_j}|1\rangle\}$ and $j \in \{1,2\}$ with $B_1 = \frac{\pi}{4}, B_2 = -\frac{\pi}{4}$. All the measurement results a_0, a_1, a_2, b_1, b_2 have binary outcomes labeled by ± 1. They reveal their measurement basis and results and calculate the value of the CHSH polynomial [32] $S_1 = \langle a_1 b_1\rangle + \langle a_2 b_1\rangle + \langle a_1 b_2\rangle - \langle a_2 b_2\rangle$, where $\langle a_i b_j\rangle = \Pr(a = b \mid ij) - \Pr(a \neq b \mid ij)$. If $S_1 \leq 2$, then they abort the protocol and else continue it.

3. They discard the measured qubits from the sequences M and C. Then Alice encodes her message by applying the Pauli operators on the remaining qubits of M and sends the encoded qubits to Bob. She applies U_0, U_1, U_2, U_3 to encode the message bits $00, 01, 10, 11$ respectively.

4. Bob checks the security of the channel by estimating the value of the CHSH polynomial, and if he finds the value less or equal to 2, then abort the protocol.

5. Bob measures the qubit pairs of (M, C) in Bell basis and reads out the secret message of Alice.

2.2.14 Measurement device independent QSDC

In 2018 Zhou et. al. [5] proposed a MDI-QSDC protocol based on single photons and EPR pairs. Let Alice be the message sender and Bob be the receiver and Charlie is an untrusted third party (UTP), who performs all the measurements. The protocol is as follows.

1. Alice prepares $(n+t_0)$ EPR pairs in $|\Psi^-\rangle$ state and makes two sequences of single qubits S_{Ah}, S_{At} containing the partner qubits of those EPR pairs. She also prepares t_1 number of decoy qubits randomly from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and inserts these qubits in random positions of S_{At}. Let the new sequence be P_A which contains $(n + t_0 + t_1)$ single qubit states. She sends P_A to Charlie.

2. Bob prepares a sequence P_B which contains $(n + t_0 + t_1)$ single qubit states randomly from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and sends it to Charlie.

3. For $1 \leq i \leq (n+t_0+t_1)$, Charlie measures each pair (P_{A_i}, P_{B_i}) in Bell basis and announces the result $\mathcal{M}_i$. If $P_{A_i} \in S_{At}$, then due to this measurement P_{B_i} is almost teleported to Alice, apart from a unitary operation u_{T_i}. They check the security of the channel from the other measurement results where $P_{A_i} \notin S_{At}$, this security check process is identical to that in the MDI-QKD [63].

4. If the channel is secure, Bob announces the preparing bases of the states of P_B. Then Alice encodes her message by applying the unitary operator $U = u_m u_T$ on the qubits of S_{Ah} and sends those to Charlie, where $u_m = U_0$ (U_3) if the message bit is 0 (1) and $u_T = U_0, U_1, U_3$ depending on basis announced by Bob and the Bell measurement results (see Table 2.3).

5. Charlie measures the qubits of S_{Ah} in Z or X basis depending upon the basis information of Bob and announces the results. From these measurement results, Bob gets the secret message of Alice.

Table 2.3: Alice's unitary operators [5]

Bob's basis	**Measurement result** $\mathcal{M}_i$	**Unitary** u_{T_i}
Z	$\|\Phi^{\pm}\rangle$	U_3
	$\|\Psi^{\pm}\rangle$	U_0
X	$\|\Phi^{+}\rangle, \|\Psi+\rangle$	U_1
	$\|\Phi^{-}\rangle, \|\Psi-\rangle$	U_0

2.2.15 Quantum dialogue using EPR pairs

In 2004, Nguyen [81] proposed an entanglement-based QSDC protocol for two people to simultaneously exchange their messages. They first pointed out a loophole of ping-pong-protocol [67] and then improve it towards a quantum dialogue protocol.

Suppose Alice and Bob have their $2N$-bit secret messages a and b respectively, where $a = \{(i_1, j_1), (i_2, j_2), \ldots, (i_N, j_N)\}$, $b = \{(k_1, l_1), (k_2, l_2), \ldots, (k_N, l_N)\}$ and $i_n, j_n, k_n, l_n \in \{0, 1\}$ for $1 \leq n \leq N$. To securely exchange their messages, Bob first prepares a large number of entangled pairs in $|\Psi^{+}\rangle_{ht}$ state. Then Bob and Alice proceed as follows.

1. Set $n = 0$.

2. Set $n = n + 1$. Bob encodes his bits (k_n, l_n) by applying the unitary $C^t_{k_n,l_n}$ on the t qubit of $|\Psi^{+}\rangle_{h_n t_n}$, where $C^t_{0,0}$, $C^t_{0,1}$, $C^t_{1,0}$, $C^t_{1,1}$ denote U_0, U_2, U_3, U_1 respectively. He sends the qubit t_n to Alice and keeps h_n with him.

3. Alice encodes her secret (i_n, j_n) by applying the unitary $C^t_{i_n,j_n}$ on the t_n and sends it back to Bob.

4. Bob measures the two qubit h_n, t_n jointly on Bell basis and gets the result $|\Psi_{x_n y_n}\rangle$, where $|\Psi_{x_n y_n}\rangle = C^t_{x_n y_n} |\Psi^{+}\rangle_{h_n t_n}$ and $x_n, y_n \in \{0, 1\}$.

5. Alice tells Bob that the run is message mode (MM) or control mode (CM).

   (a) If it is a MM run, then Bob publicly announces the value of (x_n, y_n). Both the parties decode the secret bits from the relations $x_n = i_n \oplus k_n$ and $y_n = j_n \oplus l_n$. If $n < N$, then they goto the Step 2 and else goto the Step 6.

   (b) If it is a CM run, then Alice publicly reveals the value of (i_n, j_n) for Bob to check the eavesdropping by using the relation same as MM mode. If there is no eavesdropper,

they Bob sets $n = n - 1$ and goes to the Step 2. Otherwise he reinitializes the process by going Step 2.

6. This completes the protocol.

In 2005, Zhong-Xiao et. al. first showed that the above QD protocol [81] is insecure against intercept and resend attack strategy and then they proposed a modified version of the protocol [83]. Also in 2006, Xia et. al. proposed a QD protocol using the GHZ state [84] by modifying Nguyen's QD protocol [81]. Nguyen proposed another QD protocol [222] by introducing two control modes for the security check process, where one relies on single-qubit measurements [67], and the other relies on two-qubit Bell analyses [81].

At that time, Cai [223] pointed out that all the deterministic and direct two-way quantum communication protocols, also known as ping-pong (PP) type protocols, are insecure against invisible photon eavesdropping scheme, and proposed a possible improvement as a remedy.

2.2.16 Quantum dialogue based on single-photon

Xin et. al. [85] proposed a QD protocol in 2006 by using N batches of single photons. The legitimate parties, namely, Alice and Bob agree that the two unitary operations U_0 and U_3 are apply to encode the information 0 and 1 respectively. Suppose Alice and Bob have n-bit secret messages to share. The protocol is as follows.

1. Bob prepares N batches of single photons, where each batch contains n photons randomly from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Bob encodes the same message on N batches by applying U_0 and U_3 and sends them to Alice.

2. Then Alice and Bob choose $(N-1)$ batches randomly to check the security of quantum channels by measuring them randomly in Z or X bases.

3. If the channel is secure, then Alice encodes her message on the remaining batch of photons. Bob announces the initial states and preparation bases of the photons. Alice measures those photons and gets Bob's message. She announces the measurement results and from those Bob gets the message of Alice.

In 2008, Gao et. al. [90] analyzed the security of the QSDC and QD protocols [81, 83, 85, 224, 225, 84, 71, 226, 227] and showed that the transmitted secret information is partially leaked out from the public annunciations of the legal users. Also, Tan et. al. [88] independently pointed out the insecurity of QD protocol [81] and showed that fifty percent of the secret information is leaked through the classical channel. In 2010, shi et. al. proposed some QD protocols via single photons, which can overcome the drawback of information leakage [92, 228]. In the same year, Shi also proposed another QD protocol by introducing the auxiliary particle and utilizing the special character of Bell state, "correlation extractability" [229]. A QD protocol by using a non-symmetric quantum channel was proposed by Bang et. al. [230]. Gan et. al. [231] proposed a QD protocol by using the idea of the entanglement swapping of genuine four-particle entangled states, the "two-step" transmission and the block transmission.

2.2.17 Multi-party QSDC using quantum entanglement-swapping

In 2005, Gao et. al. [94] presented a simultaneous QSDC scheme between a central party Charlie, and other two parties Alice and Bob, where Alice and Bob send their secret message to Charlie by using entanglement swapping. Alice applies the unitary operators U_0, U_1, U_2, U_3 to encode her message bits $00, 11, 01, 10$ respectively, and Bob applies U_0, U_2 to encode message bit $0, 1$ respectively. The protocol is as follows:

1. Alice, Bob and Charlie share N ordered pairs of GHZ triplets $\{\xi(1)_{123}, \eta(1)_{456}\}$, $\{\xi(2)_{123}, \eta(2)_{456}\}, \ldots, \{\xi(N)_{123}, \eta(N)_{456}\}$, where Alice has the 1st and 4th particles, Bob has the 2nd and 5th particles, and Charlie has 3rd and 6th particles of each pair of GHZ state $\{\xi(i)_{123}, \eta(i)_{456}\}$, $1 \leq i \leq N$.

2. Alice and Bob encode their message bits by applying corresponding unitary operators on the 1st and 2nd particles respectively.

3. Alice (Bob) measures the 1st and 4th (2nd and 5th) particles in the Bell basis and they inform Charlie that the Bell measurement is done.

4. Charlie measures the 3rd and 6th particles in Bell basis and deduces the two possible outcomes of Alice and Bob's measurements.

5. Alice and Bob announce their measurement results publicly and from those information and Charlie's measurement results, he can read the secret messages.

In 2005, Ting et. al. [95] generalize the QSDC scheme [94] and proposed a simultaneous QSDC scheme between the central party and other M parties by using $(M+1)$-particle GHZ states and entanglement swapping between communicating parties. In 2006, Xiao et. al. [232] proposed a QSDC scheme with one sender and N receivers by using $(N+1)$-particle GHZ states. However, Fei et. al. [233] analyse the security of the QSDC protocol [232] and showed that an eavesdropper can utilize a special property of GHZ states to get the whole secret message without being detected. They also proposed an improved version of this QSDC protocol, which can resist this kind of attack.

2.2.18 Three-party QSDC based on GHZ states

In 2006, Jin et. al. [71] presented a three-party simultaneous QSDC scheme by using GHZ states, where the three parties Alice, Bob and Charlie can exchange their secret messages among them. This QSDC protocol can be directly generalized to multi-party QSDC by using n-particle GHZ states.

For the three-party QSDC scheme, the encoding rules and are as follows:

- Alice encodes her two-bits message $00, 01, 10, 11$ by applying the unitary U_0, U_2, U_3, U_1 respectively.
- Bob and Charlie perform the unitary operations U_0, U_3 to encode their one-bit message $0, 1$ respectively.

The protocol is described below.

1. Alice prepares N groups three-particle GHZ states randomly from $\{G_1^{\pm}, G_2^{\pm}, G_3^{\pm}, G_4^{\pm}\}$ and send the sequence of 2nd particles to Bob and the sequence of 3rd particles to Charlie.
2. They choose some particles to check the security of the channel. If there is a negligible error rate then they continue the protocol and encode their message bits on their remaining particles by applying the corresponding unitary.

3. Bob and Charlie send their qubits to Alice, who measures each 3-qubit state in the GHZ basis $\mathcal{G}$. She publicly announces the measurement result and the initial GHZ state, and from this information, each of them gets others' secret messages.

In 2007 Zhong et. al. [226] pointed out a security loophole of the above three-party QSDC protocol [71] and showed that one bit of Alice's message is always leaked out without any active attack. They also proposed an improved version of the same. However, in 2008, Gao et. al. [234] analyzed the security of the QSDC protocols [71, 226] and showed that both the protocols have an information leakage problem.

2.2.19 Three-party QSDC with EPR pairs

In 2007, Wang et. al. [235] presented a three-party simultaneous QSDC scheme by using EPR pairs, where each party can obtain the N-bit secret messages of the other two parties. Let the secret message of Alice, Bob and Charlie be $\{i_1, i_2, \ldots, i_N\}$, $\{j_1, j_2, \ldots, j_N\}$ and $\{k_1, k_2, \ldots, k_N\}$ respectively. Bob and Charlie apply the unitary operators C_{j_n} and C'_{k_n} to encode their message bits j_n and k_n respectively, where

$$C_{j_n} = \begin{cases} U_0, \text{ if } j_n = 0, \\ U_2, \text{ if } j_n = 1; \end{cases} \qquad \text{and} \qquad C'_{j_n} = \begin{cases} U_0, \text{ if } k_n = 0, \\ U_1, \text{ if } k_n = 1. \end{cases}$$

To initiate the QSDC protocol, Alice first prepares enough number of EPR pairs all in the $|\Psi^+\rangle_{ht}$ state, where the h and t denote home particle and travel particle respectively. Then Alice, Bob and Charlie proceed as follows:

1. Set $n = 0$.

2. Set $n = n + 1$. Alice sends the qubit t_n to Bob and keeps h_n with her.

3. Bob either measures the received qubit to check eavesdropping or encodes it.

(a) Eavesdropping check: Bob measures the qubit t_n in Z or X basis randomly and ask Alice to measure the qubit h_n in the same basis. They compare the results to calculate the error rate.

(b) If Bob wants to encode the qubit t_n, he chooses either message mode(MM) or control mode (CM). In MM he applies C_{j_n} on t_n and in CM he does nothing. Then Bob sends t_n to Charlie.

4. When Charlie received the qubit, Bob announces the running mode MM or CM.

(a) If it was a CM, then Alice and Charlie check the security of the channel as procedure in Step 3a.

(b) If it was a MM, then Charlie choose a running mode either MM or CM for himself. In MM, he encodes the qubit t_n by applying C'_{k_n} and sends it to Alice. In CM, he prepares a decoy qubit randomly from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and sends it to Alice.

5. After Alice receives the qubit, Charlie announces the mode of communication.

(a) If it was CM, then he announces the state of the decoy qubit and Alice measures the qubit to check the security of the channel.

(b) If it was MM, then Alice measures (h_n, t_n) in Bell basis and gets the value of j_n and k_n. Then she announces the values $i_n \oplus j_n$ and $i_n \oplus k_n$, and from these information Bob and Charlie get other two messages.

6. If $n < N$, then goto Step 2, else the protocol is completed.

In 2010, Chong et al. [236] proposed an enhancement on Wang et al.'s scheme [235] such that the communications process changes from sequential to parallel. In this protocol, Alice sends h_n (t_n) qubit of each EPR pair to Bob (Charlie), then they encode their message bits and send back those qubits to Alice.

However, in 2011, Wang et al. [237] pointed out that both of the above schemes [235, 236] have the information leakage problem and any eavesdropper can directly get some information about the secret messages without any active attack.

Table 2.4: Resource estimation of the discussed QSDC protocols

Protocol	**No. of Single Qubit**	**No. of Entangled Qubit**	**Measurement Basis**	**Qubit Transmission**	**Encoding, Decoding Operators**	**Length of the message**
Ref [58]	0	n EPR pairs	Z, X, Bell basis	$2n$	0	$2n$
Ref [66]	0	n EPR pairs	Z, X, Bell basis	$2n$	U_0, U_1, U_2, U_3	$2n$
Ref [67]	0	n EPR pairs	Z, Bell basis	$2n$	U_0, U_1	n
Ref [100]	n	n EPR pairs	X, Bell basis	No	U_0, U_1, U_2, U_3	n
Ref [197]	n	n triplets	Z, X, Bell basis	No	U_0, U_1, U_2, U_3	n
Ref [203]	0	$3n$ EPR pairs	GHZ basis	No	U_0, U_1, U_2, U_3	$3n$
Ref [68]	n	0	Z, X	$2n$	U_0, U_3	n
Ref [70]	0	n GHZ states	Z, X, GHZ basis	$3n$	$U_1 \otimes U_1, U_0 \otimes U_1,$ $U_3 \otimes U_1, U_2 \otimes U_1,$ $U_0 \otimes U_2, U_1 \otimes U_2,$ $U_2 \otimes U_2, U_3 \otimes U_2$	$3n$
Ref [208]	0	n W states	Z, X, Bell basis	$2n$	–	n
Ref [73]	n	n two-qubit entangled pairs	Z	$2n$	CNot	n
Ref [74]	0	n four qubit χ- type states	Z, X, Bell, χ-basis	$4n$	U_0, U_1, U_2, U_3	$2n$
Ref [129]	0	n EPR pairs	$\mathcal{B}_\theta$ $(\theta = 0, \pm\frac{\pi}{4}, \frac{\pi}{2})$, Bell basis	$2n$	U_0, U_1, U_2, U_3	$2n$
Ref [5]	n	n EPR pairs	Z, X, Bell basis	$3n$	U_0, U_1, U_3	n
Ref [81]	0	n EPR pairs	Bell basis	$2n$	U_0, U_1, U_2, U_3	$4n$
Ref [85]	n	0	Z, X	n	U_0, U_3	$2n$
Ref [94]	0	$2n$ GHZ states	Bell basis	No	U_0, U_1, U_2, U_3	$3n$
Ref [71]	0	n GHZ states	GHZ basis	$4n$	U_0, U_1, U_2, U_3	$3n$
Ref [235]	0	n EPR pairs	Bell basis	$3n$	U_0, U_1, U_2	$3n$

2.3 Details of the QSDC and QD protocols which we improved

In this section, we briefly describe all the protocols which we analyzed. First, we discuss a QSDC protocol with user authentication [1], then an MDI-QSDC protocol [2], thereafter an MDI-QD protocol [3].

2.3.1 Yan et al.'s QSDC protocol with mutual authentication [1]

In 2020, Yan et al. proposed a QSDC protocol with mutual authentication. For simplicity, we call this protocol as YZCSS protocol. There are two parties, namely, Alice and Bob with their corresponding pre-shared N-bit secret identities ID_A and ID_B respectively, where $ID_A,\ ID_B \in \{0,1\}^N$. Alice wants to send a secret message $M \in \{0,1\}^N$ to Bob by using single photons and Bell states. The steps of the protocol are as follows:

1. Alice and Bob have their previously shared identities ID_A and ID_B, they used some QKD to exchange ID_A and ID_B. Alice prepares two ordered sets of two-qubit states S_M and S_A corresponding to the message M and her own identity ID_A, each ordered set contains N qubit pairs. For $1 \leq i \leq N$, let the i-th bit of M (or ID_A or ID_B) be M_i (or $ID_{A,i}$ or $ID_{B,i}$) and the i-th qubit of S_M (or S_A) be $S_{M,i}$ (or $S_{A,i}$). She prepares the qubits by using the following rule:

   (a) if M_i (or $ID_{A,i}$) $= 0$, then $S_{M,i}$ (or $S_{A,i}$) $= |01\rangle$ or $|10\rangle$ with equal probability,

   (b) if M_i (or $ID_{A,i}$) $= 1$, then $S_{M,i}$ (or $S_{A,i}$) $= |\Phi^+\rangle$ or $|\Phi^-\rangle$ with equal probability.

   The qubit pairs of the ordered set S_A are called decoy states. Now Alice inserts these decoy states into the ordered set S_M according to the following rule:

   (a) if $ID_{B,i} = 0$, then she inserts $S_{A,i}$ before $S_{M,i}$, and

   (b) if $ID_{B,i} = 1$, then she inserts $S_{A,i}$ after $S_{M,i}$.

   Let the new ordered set be S containing $2N$ qubit pairs. Then Alice sends S to bob using a quantum channel. Let us take an example.

   Example 1. *Let* $M = 10110$, $ID_A = 01101$ *and* $ID_B = 01001$.
   Then $S_M = \{|\Phi^+\rangle, |01\rangle, |\Phi^+\rangle, |\Phi^-\rangle, |01\rangle\}$, $S_A = \{|10\rangle, |\Phi^-\rangle, |\Phi^-\rangle, |01\rangle, |\Phi^+\rangle\}$ *and*
   $S = \{|10\rangle, |\Phi^+\rangle, |01\rangle, |\Phi^-\rangle, |\Phi^-\rangle, |\Phi^+\rangle, |01\rangle, |\Phi^-\rangle, |01\rangle, |\Phi^+\rangle\}$.

2. After Bob receives S, he knows the exact positions of the decoy photons corresponding to his identity ID_B. Bob measures those decoy photons in proper bases according to ID_A. If $ID_{A,i} = 0$, then he chooses $Z \times Z$ basis, where $Z = \{|0\rangle, |1\rangle\}$, thus $Z \times Z = \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, and if $ID_{A,i} = 1$, then he chooses the Bell basis $= \{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$ to measure $S_{A,i}$. Bob also measures the qubit pairs of S_M in $Z \times Z$ basis or Bell basis randomly. He notes the measurement results.

3. Bob asks Alice to announce the initial states of the qubit pairs of S_A for security check. They compare the initial states and the measurement results of the decoy photons, and calculate the error rate. If the error rate exceeds some pre-defined threshold value, then they terminate the protocol, else they continue.

Figure 2-1: Block diagram of the Yan et al.'s QSDC protocol with mutual authentication [1]

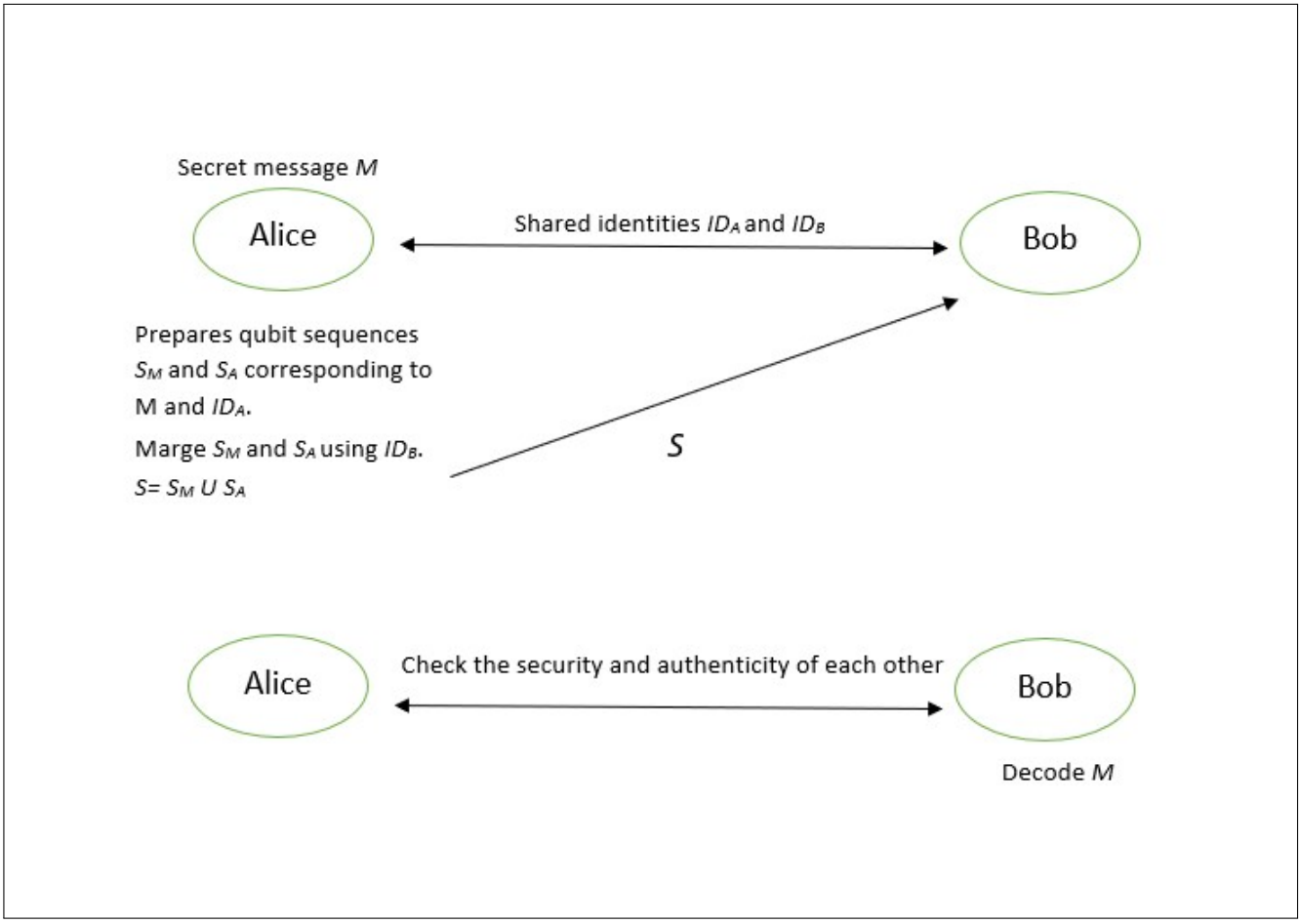


Table 2.5: Different cases of the YZCSS protocol [1]

Secret message bit of Alice M_i	**Encoded qubit $S_{M,i}$**	**Basis chosen by Bob**	**measurement result of Bob**	**Decoded secret bit**
0	$\|01\rangle$	$Z \times Z$ basis	$\|01\rangle$	0
		Bell basis	$\|\Psi^+\rangle$ or $\|\Psi^-\rangle$	0
	$\|10\rangle$	$Z \times Z$ basis	$\|10\rangle$	0
		Bell basis	$\|\Psi^+\rangle$ or $\|\Psi^-\rangle$	0
1	$\|\Phi^+\rangle$	$Z \times Z$ basis	$\|00\rangle$ or $\|11\rangle$	1
		Bell basis	$\|\Phi^+\rangle$	1
	$\|\Phi^-\rangle$	$Z \times Z$ basis	$\|00\rangle$ or $\|11\rangle$	1
		Bell basis	$\|\Phi^-\rangle$	1

4. Bob gets all the secret message bits from the measurement results of the qubit pairs of S_M. The relation between the measurement results and the secret message bits are given in Table 2.5. To check the integrity of the secret message Alice and Bob publicly compare some parts of the message.

The authors of [1] have shown that the YZCSS protocol is secure against various kinds of attacks, such as the impersonation attack, the intercept-and-resend attack, man-in-the-middle attack, entangle-measure attack.

2.3.2 Niu et al.'s MDI-QSDC Protocol [2]

In this section, we briefly describe the MDI-QSDC and MDI-QD protocols proposed by Niu et al. in 2018.

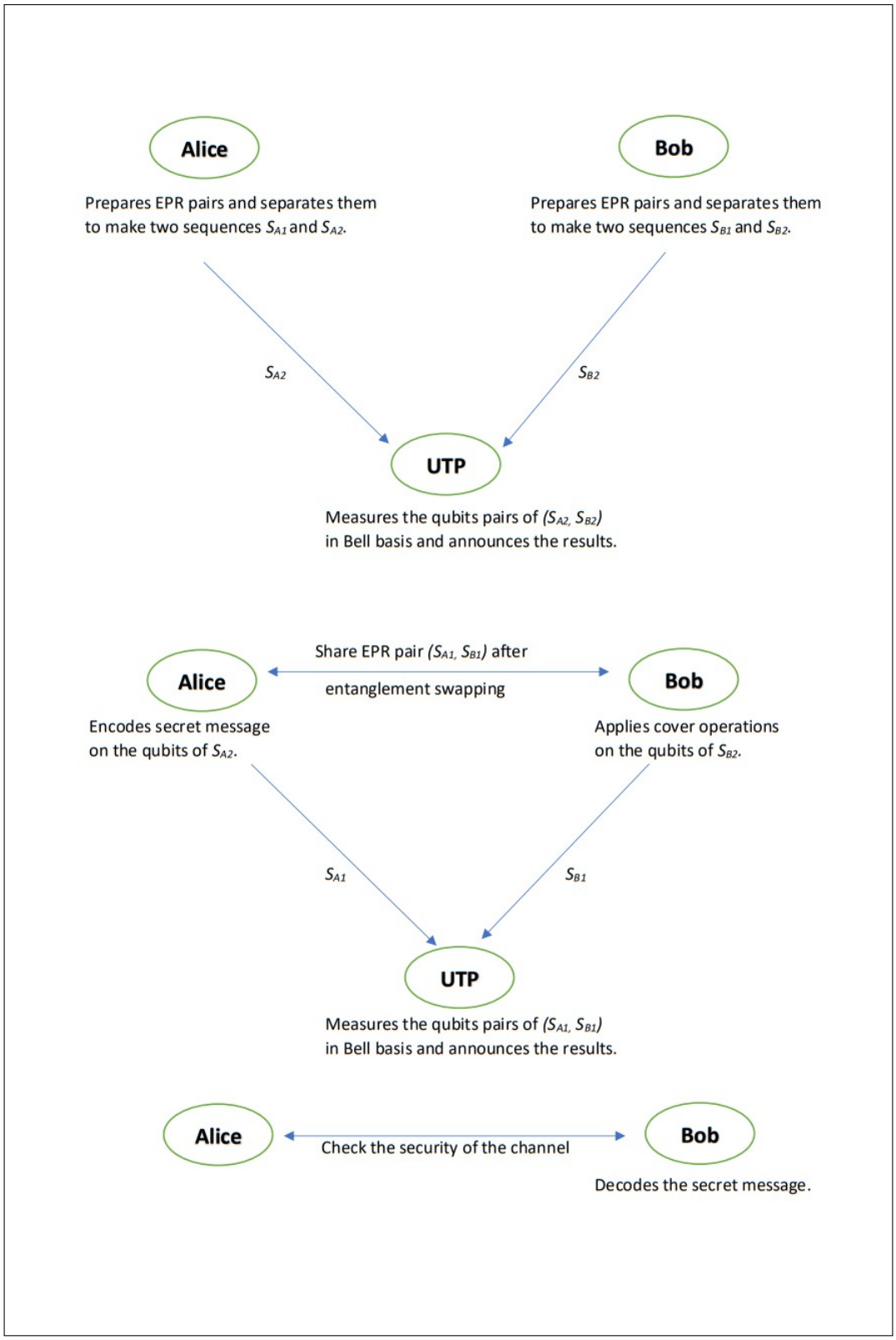
MDI-QSDC protocol

There are three parties in this protocol, namely, Alice, Bob and Charlie, where Alice wants to send some message to Bob, and Charlie is an untrusted third party, who performs all the measurements. They use the EPR pairs $|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle$ for sending the message bits.

The steps of the protocol are as follows:

1. Alice prepares n EPR pairs randomly in $|\Psi^+\rangle$ and $|\Psi^-\rangle$ states and creates two sequences S_{A_1} and S_{A_2} of single photons, such that for $1 \leq i \leq n$, the i-th qubits of S_{A_1} and S_{A_2} are partners of each other in the i-th EPR pair. Similarly, Bob also prepares S_{B_1} and S_{B_2}

Figure 2-2: Block diagram of Niu et al.'s MDI-QSDC Protocol [2]



from his n EPR pairs randomly chosen from $|\Psi^+\rangle$ and $|\Psi^-\rangle$. Alice (Bob) also chooses m single qubit states randomly from $\{|0\rangle, |1\rangle, |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$ and inserts these qubits in random positions of S_{A_2} (S_{B_2}), and let the new sequence be C_{A_2} (C_{B_2}) containing $(n+m)$ single qubit states.

2. Alice (Bob) sends the sequence C_{A_2} (C_{B_2}) to Charlie and keeps S_{A_1} (S_{B_1}) in her (his) lab.

3. Charlie makes Bell measurement on each pair of C_{A_2} and C_{B_2} (i.e., the i-th Bell measurement on the i-th qubit of C_{A_2} and the i-th qubit of C_{B_2}, $1 \leq i \leq n+m$) and announces the results.

4. Alice and Bob announce the positions of the single qubit states in the sequences C_{A_2} and C_{B_2} respectively. For $1 \leq i \leq n+m$, four cases may arise.

   (a) If the i-th qubit of C_{A_2} and the i-th qubit of C_{B_2} are from S_{A_2} and S_{B_2} respectively, then as a result of quantum entanglement swapping [204], the Bell measurement causes the corresponding partner qubits of S_{A_1} and S_{B_1} become an EPR pair, which is shown in Equation (2.5).

$$
\begin{aligned}
|\Psi^+\rangle_{A_1A_2}|\Psi^+\rangle_{B_1B_2} &= \frac{1}{2}(|\Psi^+\rangle_{A_1B_1}|\Psi^+\rangle_{A_2B_2} - |\Psi^-\rangle_{A_1B_1}|\Psi^-\rangle_{A_2B_2} + \\
&\quad |\Phi^+\rangle_{A_1B_1}|\Phi^+\rangle_{A_2B_2} - |\Phi^-\rangle_{A_1B_1}|\Phi^-\rangle_{A_2B_2}), \\
|\Psi^-\rangle_{A_1A_2}|\Psi^+\rangle_{B_1B_2} &= \frac{1}{2}(|\Psi^-\rangle_{A_1B_1}|\Psi^+\rangle_{A_2B_2} - |\Psi^+\rangle_{A_1B_1}|\Psi^-\rangle_{A_2B_2} + \\
&\quad |\Phi^-\rangle_{A_1B_1}|\Phi^+\rangle_{A_2B_2} - |\Phi^+\rangle_{A_1B_1}|\Phi^-\rangle_{A_2B_2}), \\
|\Psi^+\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2} &= \frac{1}{2}(|\Psi^+\rangle_{A_1B_1}|\Psi^-\rangle_{A_2B_2} - |\Psi^-\rangle_{A_1B_1}|\Psi^+\rangle_{A_2B_2} + \\
&\quad |\Phi^-\rangle_{A_1B_1}|\Phi^+\rangle_{A_2B_2} - |\Phi^+\rangle_{A_1B_1}|\Phi^-\rangle_{A_2B_2}), \\
|\Psi^-\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2} &= \frac{1}{2}(|\Psi^-\rangle_{A_1B_1}|\Psi^-\rangle_{A_2B_2} - |\Psi^+\rangle_{A_1B_1}|\Psi^+\rangle_{A_2B_2} + \\
&\quad |\Phi^+\rangle_{A_1B_1}|\Phi^+\rangle_{A_2B_2} - |\Phi^-\rangle_{A_1B_1}|\Phi^-\rangle_{A_2B_2}).
\end{aligned}
\tag{2.5}
$$

   (b) If the i-th qubit of C_{A_2} is from S_{A_2} and the i-th qubit of C_{B_2} is any single qubit from the set $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, then Alice and Bob discard the i-th Bell measurement

result.

(c) If the i-th qubit of C_{A_2} is a single qubit from the set $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and the i-th qubit of C_{B_2} is from S_{B_2}, then also Alice and Bob discard the i-th Bell measurement result.

(d) If both the i-th qubits of C_{A_2} and C_{B_2} are from the set $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, then Alice and Bob exchange the basis information of their single qubits. If the bases are different, then they discard the i-th Bell measurement result. Else it is used for security checking. A pair of single qubits with identical bases can be written as:

$$\begin{aligned}
|0\rangle_{A_2}|0\rangle_{B_2} &= \frac{1}{\sqrt{2}}(|\Phi^+\rangle_{A_2B_2} + |\Phi^-\rangle_{A_2B_2}),\\
|1\rangle_{A_2}|1\rangle_{B_2} &= \frac{1}{\sqrt{2}}(|\Phi^+\rangle_{A_2B_2} - |\Phi^-\rangle_{A_2B_2}),\\
|0\rangle_{A_2}|1\rangle_{B_2} &= \frac{1}{\sqrt{2}}(|\Psi^+\rangle_{A_2B_2} + |\Psi^-\rangle_{A_2B_2}),\\
|1\rangle_{A_2}|0\rangle_{B_2} &= \frac{1}{\sqrt{2}}(|\Psi^+\rangle_{A_2B_2} - |\Psi^-\rangle_{A_2B_2});
\end{aligned} \tag{2.6}$$

and

$$\begin{aligned}
|+\rangle_{A_2}|+\rangle_{B_2} &= \frac{1}{\sqrt{2}}(|\Phi^+\rangle_{A_2B_2} + |\Psi^+\rangle_{A_2B_2}),\\
|-\rangle_{A_2}|-\rangle_{B_2} &= \frac{1}{\sqrt{2}}(|\Phi^+\rangle_{A_2B_2} - |\Psi^+\rangle_{A_2B_2}).\\
|+\rangle_{A_2}|-\rangle_{B_2} &= \frac{1}{\sqrt{2}}(|\Phi^-\rangle_{A_2B_2} - |\Psi^-\rangle_{A_2B_2}),\\
|-\rangle_{A_2}|+\rangle_{B_2} &= \frac{1}{\sqrt{2}}(|\Phi^-\rangle_{A_2B_2} + |\Psi^-\rangle_{A_2B_2}).
\end{aligned} \tag{2.7}$$

Using the relations (2.6) and (2.7), Alice and Bob estimate the error in the channel and decide to continue the protocol or not.

5. Alice and Bob discard the qubits, which are not entangled, from their sequences S_{A_1} and S_{B_1}, and make the new sequences M_A and M_B respectively. Let the number of discarded qubits from each set be δ, and then each new sequence contains $(n - \delta)$ single qubits. Alice performs the unitary operation σ_z [6], on the qubits of M_A, whose initial states were $|\Psi^+\rangle$. This process is equivalent to the fact that Alice prepared all the initial EPR pairs in $|\Psi^-\rangle$ state. Now, only Bob knows the actual state of the qubit pairs (M_{Ai}, M_{Bi})

for $1 \leq i \leq n - \delta$, where M_{Ai} and M_{Bi} are the i-th qubits of the sequences M_A and M_B respectively. Due to quantum entanglement swapping, (M_{Ai}, M_{Bi}) is in a Bell state (see Equation (2.5)).

6. Message encoding: Alice puts some random checking bits on random positions of her message. She applies one of the four unitary operators (Pauli matrices [6]), I, σ_x, $i\sigma_y$ and σ_z, on the qubits of M_A, to encode the information 00, 01, 10, and 11 respectively. To make the protocol secure against the intercept-and-resend attack, Bob randomly applies I or σ_z on the qubits of M_B.

7. Alice (Bob) sends the sequence M_A (M_B) to Charlie, who measures each pair of qubits of M_A and M_B on Bell basis and announces the results. From the measurement results, Bob decodes the message of Alice. Then Alice announces the positions and value of the random checking bits, and from this information, they can check the integrity of the message. A non-negligible error implies the existence of some eavesdropper in the channel.

MDI-QD protocol

This is a simple generalization of the previous MDI-QSDC protocol. The first five steps are the same as above. To encode their messages, Alice and Bob divide the pair of sequence (M_A, M_B) into two disjoint parts (M_A^1, M_B^1) and (M_A^2, M_B^2). One part is used for sending the message from Alice to Bob and another part is used for sending a message from Bob to Alice.

2.3.3 Maitra's MDI-QD Protocol [3]

In this section, we shortly describe the MDI-QD protocol proposed in [3], where two legitimate parties, namely Alice and Bob, can simultaneously exchange their messages. The proposal in [3] is a composition of two different protocols, one is the BB84 QKD protocol [52] and another is a modified version of Lo et al.'s MDI-QKD protocol [63]. In the first part, Alice and Bob perform BB84 QKD [52] to generate a shared key k between themselves. In the second part, they prepare their sets of qubits Q_A and Q_B, corresponding to k and their respective messages a and b. The qubits preparation procedure is given in Algorithm 2.

Algorithm 2: Algorithm for encoding

Let the key be $k = k_1k_2 \dots k_n$, Alice's message be $a = a_1a_2 \dots a_n$ and Bob's message be $b = b_1b_2 \dots b_n$.

Then for $1 \leq i \leq n$, Alice and Bob prepare their qubits according to the following strategy:

1. if a_i (b_i)$= 0$ and $k_i = 0$, prepares $|0\rangle$.
2. if a_i (b_i)$= 1$ and $k_i = 0$, prepares $|1\rangle$.
3. if a_i (b_i)$= 0$ and $k_i = 1$, prepares $|+\rangle$.
4. if a_i (b_i)$= 1$ and $k_i = 1$, prepares $|-\rangle$.

Alice and Bob send Q_A and Q_B to an untrusted third party or UTP (who may be an Eavesdropper, Eve). Then the UTP measures the two-qubit states in Bell basis (i.e, $\mathcal{B}_2$) and announces the result. From the result, Alice and Bob decode the messages of each other (see Table 2.6). Details are given in Figure 3.

Table 2.6: Different cases in MDI QD [3]

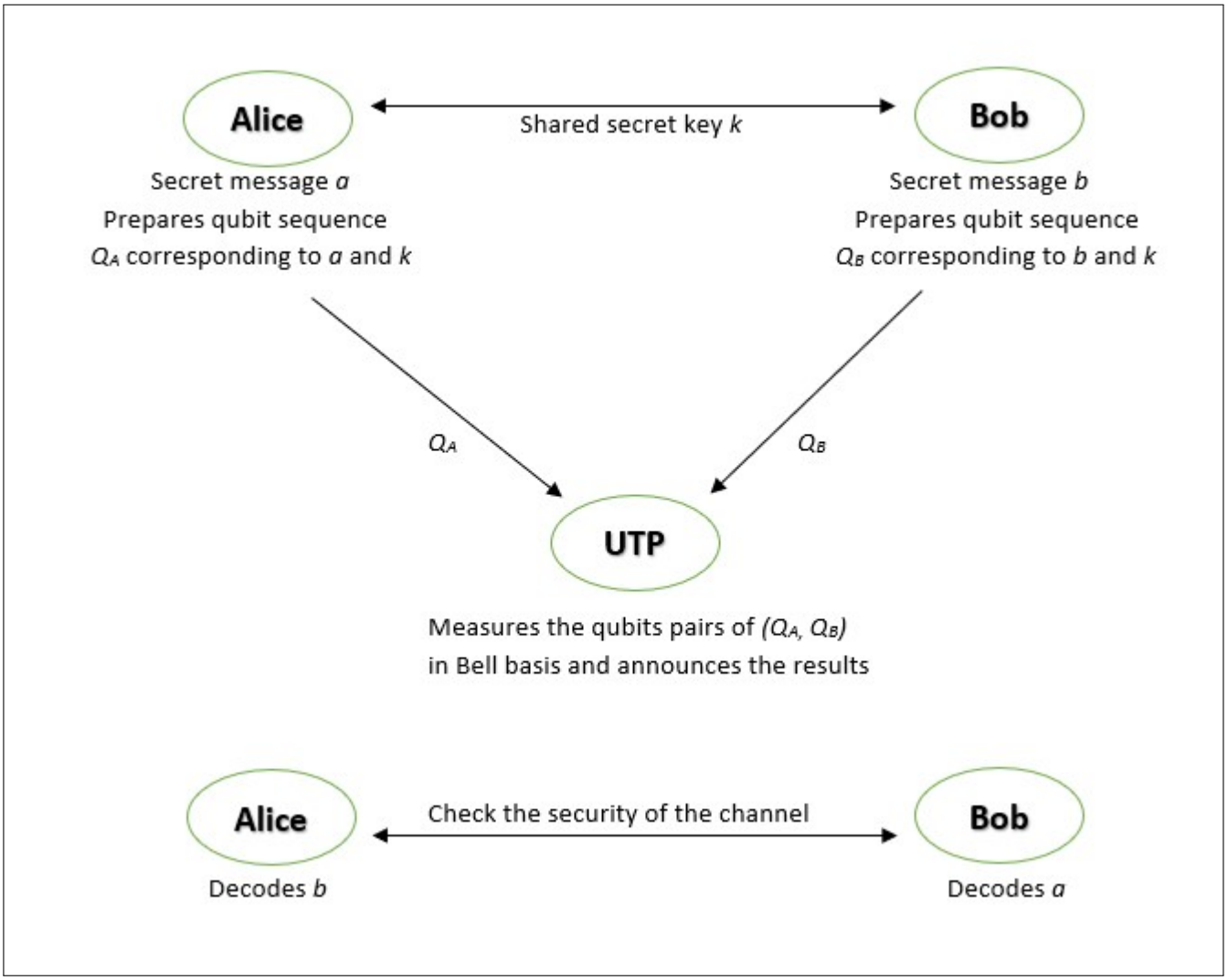
Bits to communicate by		Qubits prepared by		Probabilities of measurement results at UTP's end			
Alice	Bob	Alice (Q_{Ai})	Bob (Q_{Bi})	$\|\Phi^+\rangle$	$\|\Phi^-\rangle$	$\|\Psi^+\rangle$	$\|\Psi^-\rangle$
0	0	$\|0\rangle$	$\|0\rangle$	1/2	1/2	0	0
0	1	$\|0\rangle$	$\|1\rangle$	0	0	1/2	1/2
1	0	$\|1\rangle$	$\|0\rangle$	0	0	1/2	1/2
1	1	$\|1\rangle$	$\|1\rangle$	1/2	1/2	0	0
0	0	$\|+\rangle$	$\|+\rangle$	1/2	0	1/2	0
0	1	$\|+\rangle$	$\|-\rangle$	0	1/2	0	1/2
1	0	$\|-\rangle$	$\|+\rangle$	0	1/2	0	1/2
1	1	$\|-\rangle$	$\|-\rangle$	1/2	0	1/2	0

It is clear from Table 2.6 that,

- if the prepared qubit of Alice is $|0\rangle(|1\rangle)$, then Alice guesses message bit of Bob with probability 1 as follows:

$$\text{Measurement result} = \begin{cases} |\phi^+\rangle \text{ or } |\phi^-\rangle \Rightarrow & \text{message bit of Bob is 0 (1)}, \\ |\psi^+\rangle \text{ or } |\psi^-\rangle \Rightarrow & \text{message bit of Bob is 1 (0)}, \end{cases}$$

Figure 2-3: Block diagram of the Maitra's MDI-QD Protocol [3]



Algorithm 3: Maitra's MDI-QD Protocol [3]

1. Alice and Bob share an n-bit key stream ($k = k_1k_2 \dots k_n$) between themselves using BB84 protocol.
2. Let the n-bit message of Alice (Bob) be $a = a_1a_2 \dots a_n$ ($b = b_1b_2 \dots b_n$).
3. For $1 \leq i \leq n$, Alice (Bob) prepares the qubits $Q_A = Q_{A_1}Q_{A_2} \dots Q_{A_n}$ ($Q_B = Q_{B_1}Q_{B_2} \dots Q_{B_n}$) at her (his) end according to Algorithm 2.
4. Alice (Bob) sends her (his) prepared qubits Q_A (Q_B) to an untrusted third party (UTP).
5. For $1 \leq i \leq n$, the UTP measures each two qubits Q_{A_i} and Q_{B_i} in Bell basis (i.e., $\mathcal{B}_2 = \{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$) and announces the measurement result $\mathcal{M}_i \in \{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$ publicly. Table 2.6 shows the possible measurements results with their occurring probabilities.
6. For $1 \leq i \leq n$, Alice and Bob consider the i-th measurement result $\mathcal{M}_i$, if $\mathcal{M}_i = |\Phi^-\rangle$ or $|\Psi^+\rangle$ and discard the other cases.
7. They randomly choose δn number of measurement results to estimate the error, where $\delta \ll 1$ is a small fraction.
8. Alice and Bob guess the message bits of other, corresponding to their chosen δn number of measurement results using Table 2.7 and Table 2.8.
9. For the above-mentioned δn rounds, they disclose their respective guesses.
10. If the estimated error is greater than some predefined threshold value, then they abort. Else they continue and go to the next step.
11. For the remaining measurement results, Alice and Bob guess the message bits of each other, using Table 2.7 and Table 2.8.

- if the prepared qubit of Alice is $|+\rangle(|-\rangle)$, then Alice guesses message bit of Bob with probability 1 as follows:

$$\text{Measurement result} = \begin{cases} |\phi^+\rangle \text{ or } |\psi^+\rangle \Rightarrow & \text{message bit of Bob is 0 (1),} \\ |\phi^-\rangle \text{ or } |\psi^-\rangle \Rightarrow & \text{message bit of Bob is 1 (0).} \end{cases}$$

From the above discussion and Table 2.6, let us construct two more tables, namely Table 2.7

and Table 2.8, containing the information of Alice's guess and Bob's guess about other's message bits for different cases.

Table 2.7: Alice's guess about Bob's message bit for different cases of MDI-QD [3]

Key bit k_i	Alice's bit a_i	Alice's qubit Q_{Ai}	Alice's guess about b_i when $\mathcal{M}_i$			
			$\|\phi^+\rangle$	$\|\phi^-\rangle$	$\|\psi^+\rangle$	$\|\psi^-\rangle$
0	0	$\|0\rangle$	0	0	1	1
0	1	$\|1\rangle$	1	1	0	0
1	0	$\|+\rangle$	0	1	0	1
1	1	$\|-\rangle$	1	0	1	0

Table 2.8: Bob's guess about Alice's message bit for different casesof MDI-QD [3]

Key bit k_i	Bob's bit b_i	Bob's qubit Q_{Bi}	Bob's guess about a_i when $\mathcal{M}_i$			
			$\|\phi^+\rangle$	$\|\phi^-\rangle$	$\|\psi^+\rangle$	$\|\psi^-\rangle$
0	0	$\|0\rangle$	0	0	1	1
0	1	$\|1\rangle$	1	1	0	0
1	0	$\|+\rangle$	0	1	0	1
1	1	$\|-\rangle$	1	0	1	0

Hence from Table 2.7 and Table 2.8, we can say that both Alice and Bob can exchange their message simultaneously.

Now we can see from Table 2.6, if the measurement result is $|\phi^+\rangle$ or $|\psi^-\rangle$, then Eve knows the XOR of the communicated bits between Alice and Bob. In that case, Eve has 1 bit information among 2 bits. To avoid the information leakage, Alice and Bob discard the measurement result when it is $|\phi^+\rangle$ or $|\psi^-\rangle$.

After that, Alice and Bob estimate the error between the channel. If the UTP cheats, that can also be detected from this checking. If the error lies between a tolerable range they continue the protocol, else they abort.

2.4 Deterministic secure quantum communication

DSQC is a type of quantum communication, in which the parties need to exchange classical information to decode the secret message after the security check process. Since the classical resource is much cheaper than a quantum resource, secure DSQC protocols have attracted

continuous attention. In 1999, Shimizu et al. [238] proposed the first DSQC protocol, where the cipher-texts are encoded using entangled photon pairs. The sender Alice sends the encoded qubits through a quantum channel to the receiver Bob. After the security checking process, Bob measures the entangled pairs in Bell bases and Alice announces the classical information about the encoding bases. From this announcement and his measurement results, Bob decodes the secret message of Alice.

In 2002, Beige et al. [239] proposed the first DSQC scheme using single photons, but the authors themselves pointed out that the scheme is insecure against teleportation attack in erratum.

After that, Yan et al. [100] and Man et al. [240] proposed several DSQC schemes based on quantum teleportation [241] and entanglement swapping [242]. Lucamarini et al. [243] presented a protocol for DSQC without using entanglement. Cai et al. [244] proposed a DSQC protocol using single qubit in a mixed state. Li et al. [102] proposed two DSQC schemes using non- maximally entangled states and single-photon measurements, the protocols are based on pure entangled states and d-dimensional single-photon states respectively. Yuan et al. [245] proposed a novel efficient DSQC scheme with cluster state [246]. Liu et al. [247] proposed a universal and general DSQC protocol in which unitary operations are not required. Subsequently, various DSQC protocols have been proposed [248, 249, 250, 251, 252, 139], based on the symmetric W state [248], multi-particle GHZ states [249, 250, 251], photons' polarization-spatial-mode DOFs [139], and so on.

2.5 Dimensionality testing

For a physical system, we generally assume that it has a particular dimension. Any practical application that uses entangled quantum systems has some predefined dimensional entangled states. In information theory, the dimensionality of quantum systems is a resource. In cryptographic applications, the security level scheme depends on the dimension. So testing dimensionality or distinguishing dimensionality of the underlying state-space are important pre-processing tasks before executing the actual protocol.

A higher dimension implies more degrees of freedom. For example, consider QKD protocol

with the qubit. In this case, the legitimate parties use only the polarization of a photon for encoding. However, they have to fix the values for the other degrees of freedom such as spectral line, spatial mode or temporal mode, etc. Lack of knowledge of any of these parameters may cause a security back-door. Recently, Maitra et al. [253] showed that if the honest party measures only the polarization of a photon and remains ignorant about the *Orbital Angular Momentum* (OAM), then by changing the value of OAM one can steal more information than what he/she is entitled to in a certain type of QKD protocol. This strengthens the motivation of dimensionality testing.

The dimension witness gives a bound on the dimension of an unknown system based on measurement statistics. It was first introduced for quantum systems in the context of non-local correlations by Brunner et al. [254] and further developed in [255, 256, 257, 258, 259, 260, 261, 123, 262]. Various experiments have been recently proposed about the implementation of such witnesses [124, 263].

Some theory of dimensional detection of an unknown quantum system is based on the set of conditional probabilities. It is based on the analysis of the probabilities of observing an outcome after creating and measuring the system for a given set of possibilities. It has become a prominent research area in recent times [261, 123, 262]. Experimental tests for testing the dimension of a quantum system have been explored [263, 124] and it has produced successful results. A simple and general dimension witnesses for quantum systems of arbitrary Hilbert space dimension was proposed by Brunner (2013) [264]. Their proposed work can distinguish between classical and quantum systems of the same dimension. A simple method for generating nonlinear dimension witnesses for systems of arbitrary dimension has been proposed by Bowles (2014) [265]. It has been shown in this paper that this witness can be used to certify the presence of randomness.

Chapter 3

Analysis and Design of QSDC Protocol

Yan et al. proposed a QSDC protocol with authentication using single photons and EPR pairs (YZCSS protocol) [1], which we discussed in Chapter 2. Here, in this chapter, we show that the YZCSS protocol is secure neither against intercept-and-resend attack, nor against impersonation attack. If an eavesdropper applies any one of these attacks, then it can get the complete secret message, i.e., not only a portion of the message is revealed, but also the entire message is compromised. Moreover, for impersonation attack, the legitimate parties can not detect the presence of the eavesdropper. Here we present a modification of the YZCSS protocol to improve its security, where we assume that the classical channel is authenticated, and we achieve authentication of the quantum channel within our protocol [146].

3.1 Security loophole of the YZCSS protocol

We now show that the YZCSS protocol discussed in Section 2.3.1 of the previous chapter, is not secure against intercept-and-resend attack and impersonation attack, an eavesdropper (Eve) can get the whole secret message M and Alice's authentication identity ID_A by adopting these attacks.

3.1.1 Intercept-and-resend attack

In this attack strategy, when Alice sends the quantum states to Bob, *Eve* intercepts those from the quantum channel, she measures the states and resend those to Bob. However, to attack the YZCSS protocol, *Eve* follows a special strategy while resending the quantum states to Bob. The process of the attack is as follows.

1. *Eve* intercepts the ordered set S and measures each two-qubit state randomly in $Z \times Z$ basis or Bell basis and note down the measurement results. For $1 \leq i \leq 2N$, if she chooses $Z \times Z$ basis to measure the i-th qubit pair of S and the measurement result is either $|01\rangle$ or $|10\rangle$, then she simply sends this state to Bob. But if the measurement result is either $|00\rangle$ or $|11\rangle$, *Eve* definitely knows that she chooses wrong basis and the initial state was either $|\Phi^+\rangle$ or $|\Phi^-\rangle$. Then she randomly prepares $|\Phi^+\rangle$ or $|\Phi^-\rangle$ and sends it to Bob. Similarly if *Eve* chooses Bell basis and gets $|\Phi^+\rangle$ or $|\Phi^-\rangle$, then sends them. Otherwise she randomly sends $|01\rangle$ or $|10\rangle$ to Bob.

2. *Eve* constructs a $2N$-bit string m from the measurement results by using Table 3.1.

Table 3.1: Rule of construction of m by *Eve*

Basis chosen by *Eve*	***Eve*'s measurement result**	**Corresponding bit of** m
$Z \times Z$ basis	$\|01\rangle$ or $\|10\rangle$	0
	$\|00\rangle$ or $\|11\rangle$	1
Bell basis	$\|\Psi^+\rangle$ or $\|\Psi^-\rangle$	0
	$\|\Phi^+\rangle$ or $\|\Phi^-\rangle$	1

3. *Eve* splits the $2N$-bit string $m = m_1 m_2 \ldots m_{2N}$ into N number of 2-bit strings $\mathcal{M}_1, \mathcal{M}_2, \ldots, \mathcal{M}_N$, and for $1 \leq i \leq N$, $\mathcal{M}_i = m_{2i-1} m_{2i}$. Now from the construction procedure of the ordered set S, *Eve* exactly knows that each $\mathcal{M}_i$ contains the i-th bit of secret message M and the i-th bit of Alice's authentication identity ID_A. If both the bits of $\mathcal{M}_i$ are equal, i.e., $\mathcal{M}_i = bb$, where $b \in \{0, 1\}$, then she concludes $M_i = b$ and $ID_{A,i} = b$. Again if $\mathcal{M}_i = b\bar{b}$, where $\bar{b}$ = bit complement of b, then she waits for Alice's announcement about the initial states of the decoy photons. If Alice announces $|01\rangle$ or $|10\rangle$, then *Eve* concludes $ID_{A,i} = 0$ and $M_i = 1$, otherwise she concludes $ID_{A,i} = 1$ and $M_i = 0$. Thus *Eve* can successfully attack the protocol and gets the complete secret message.

Now Alice and Bob can detect this intercept-and-resend attack at the time of security check, but it has no impact on the attack result as one of the main requirement of a QSDC protocol is: "the secret messages which have been encoded already in the quantum states should not leak even though an eavesdropper may get hold of channel" [66].

3.1.2 Impersonation attack

By analyzing the YZCSS protocol, we find that the authentication procedure of this QSDC protocol is unidirectional, i.e., only Bob can verify Alice's identity. Here we show that how *Eve* impersonate Bob to acquire the secret message of Alice. The process is as follows:

1. Alice prepares the ordered set S and sends it to *Eve*.
2. After receiving S, *Eve* measures all the qubit pairs randomly in $Z \times Z$ or Bell basis and generates a $2N$-bit string m from the measurement results by using Table 3.1.
3. *Eve* asks Alice to declare the initial state of the decoy photons and from this information, she gets the whole secret message (by using the same process as in Step 3 of the intercept-and-resend attack).

In this case, Alice can not detect *Eve*, or in other words, only one-way authentication is possible in the YZCSS protocol. Moreover, without knowing the exact position of the decoy photons, *Eve* can get the whole secret message.

Let us take an example of this attack.

Example 2. *Let* $M = 10110$*,* $ID_A = 01101$ *and* $ID_B = 01001$*.*
Then $S_M = \{|\Phi^+\rangle, |01\rangle, |\Phi^+\rangle, |\Phi^-\rangle, |01\rangle\}$*,* $S_A = \{|10\rangle, |\Phi^-\rangle, |\Phi^-\rangle, |01\rangle, |\Phi^+\rangle\}$ *and*
$S = \{|10\rangle, |\Phi^+\rangle, |01\rangle, |\Phi^-\rangle, |\Phi^-\rangle, |\Phi^+\rangle, |01\rangle, |\Phi^-\rangle, |01\rangle, |\Phi^+\rangle\}$*.*

1. *Eve has the ordered set* S*.*
2. *Let* $\mathcal{B} = \{Z, Z, Bell, Z, Bell, Bell, Bell, Z, Z, Bell\}$ *be a sequence of bases which Eve choses to measure the qubit pairs of* S*.*
3. *Let the ordered set of measurement results be*
   $\{|10\rangle, |00\rangle, |\Psi^-\rangle, |11\rangle, |\Phi^-\rangle, |\Phi^+\rangle, |\Psi^+\rangle, |11\rangle, |01\rangle, |\Phi^+\rangle\}$.

4. *Then* $m = 0101110101$ *and* $\mathcal{M}_1 = 01$, $\mathcal{M}_2 = 01$, $\mathcal{M}_3 = 11$, $\mathcal{M}_4 = 01$, $\mathcal{M}_5 = 01$. *Eve concludes* $M_3 = 1$ *and* $ID_{A,3} = 1$.

5. *Alice announces* $S_A = \{|10\rangle, |\Phi^-\rangle, |\Phi^-\rangle, |01\rangle, |\Phi^+\rangle\}$ *and then Eve concludes*

   - $ID_{A,1} = 0$ *and* $M_1 = 1$,
   - $ID_{A,2} = 1$ *and* $M_2 = 0$,
   - $ID_{A,4} = 0$ *and* $M_4 = 1$,
   - $ID_{A,5} = 1$ *and* $M_5 = 0$.

   Thus Eve gets the whole secret message $M = 10110$.

In the next section we propose a remedy to these security problems of the YZCSS protocol.

3.2 Proposed modification

In this section, first we describe how authentication is perform, and then our modified protocol, followed by its security analysis.

For the quantum channel we do not assume any authentication, but both the user authentication and message authentication are incorporated with the modified protocol (see Table 3.2 for more details).

Table 3.2: Channel authentication (assumptions and achievements)

Type of the channel	**User authentication**		**Message authentication**	
	Protocol assumes	**Protocol achieves**	**Protocol assumes**	**Protocol achieves**
Classical	Yes	–	Yes	–
Quantum	No	Yes	No	Yes

Now we discuss how to modify this YZCSS protocol so that it can provide mutual authentication and stand against the intercept-and-resend attack. In the original protocol, the length of ID_A and ID_B are equal to the length of the message, which may vary. However, in our improved version, we fix the length of ID_A and ID_B, and the fixed-length is k. Here we use some techniques of the authentication protocol proposed by Fei et al. [266]. Our modified protocol is given below:

1. Qubits preparation to encode secret message:

   (a) Alice and Bob have their previously shared k-bit identities ID_A and ID_B, where ID_A and ID_B are unknown to everybody other than Alice and Bob.

   (b) Suppose Alice has an n-bit secret message m which she wants to send to Bob through a quantum channel. She chooses c random check bits and inserts those in random positions of m. Let the new message string be M of length $N = n + c$.

   (c) Alice prepares a sequence of N qubit pairs S_M corresponding to her N-bit message M. For $1 \leq i \leq N$, let the i-th pair of S_M be $S_{M,i} = (S^1_{M,i}, S^2_{M,i})$ and she prepares $S_{M,i}$ by using the following rule:

$$S_{M,i} = \begin{cases} |01\rangle \text{ or } |10\rangle \text{ with equal probability, if } M_i = 0, \\ |\Phi^+\rangle \text{ or } |\Phi^-\rangle \text{ with equal probability, if } M_i = 1. \end{cases} \tag{3.1}$$

   (d) Alice takes one qubit from each qubit pair $S_{M,i}$ to form an ordered qubit sequence $Q^1_M = \{S^1_{M,1}, S^1_{M,2}, \ldots, S^1_{M,N}\}$. The remaining partner qubits of $S_{M,i}$ compose another qubit sequence $Q^2_M = \{S^2_{M,1}, S^2_{M,2}, \ldots, S^2_{M,N}\}$.

   (e) Alice prepares the first sequence of decoy photons S_A, for authentication, corresponding to her own identity ID_A as follows: for $1 \leq i \leq k$,

$$S_{A,i} = \begin{cases} |0\rangle \text{ or } |1\rangle \text{ with equal probability, if } ID_{A,i} = 0, \\ |+\rangle \text{ or } |-\rangle \text{ with equal probability, if } ID_{A,i} = 1, \end{cases} \tag{3.2}$$

   where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Now she inserts these decoy states into the first sequence Q^1_M according to the following rule: for $1 \leq i \leq k$,

      i. if $ID_{B,i} = 0$, then she inserts $S_{A,i}$ before $Q^1_{M,\lambda i-\lambda+1}$,

      ii. if $ID_{B,i} = 1$, then she inserts $S_{A,i}$ after $Q^1_{M,\lambda i}$,

   where $\lambda = [N/k]$, $[x]$ = greatest integer not greater than x and $k \leq N$. Let the first sequence become S containing $N + k$ qubits. For better understanding, let us take an example,

Example 3. *Let* $M = 1011010$, $ID_A = 011$ *and* $ID_B = 010$.

i. $S_M = \{|\Phi^+\rangle, |01\rangle, |\Phi^+\rangle, |\Phi^-\rangle, |01\rangle, |\Phi^+\rangle, |10\rangle\}$ *and let the i-th pair of* S_M *be* $(S^1_{M,i}, S^2_{M,i})$.

ii. $Q^1_M = \{S^1_{M,1}, S^1_{M,2}, \ldots S^1_{M,7}\}$, $Q^2_M = \{S^2_{M,1}, S^2_{M,2}, \ldots S^2_{M,7}\}$.

iii. $S_A = \{|0\rangle, |-\rangle, |-\rangle\}$.

iv. $\lambda = [7/3] = 2$.

v. $S = \{|0\rangle, S^1_{M,1}, S^1_{M,2}, S^1_{M,3}, S^1_{M,4}, |-\rangle, |-\rangle, S^1_{M,5}, S^1_{M,6}, S^1_{M,7}\}$.

(f) She also prepares a second set of decoy photons D_A randomly from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and inserts them in random positions of S. Let the new sequence be S'.

2. First sequence of qubits transmission: Alice sends the new sequence S' to Bob using a quantum channel. She keeps the sequence Q^2_M with her.

3. Security check: After Bob receives S', Alice announces the positions and the bases of the second set of decoy photons. Bob measures those decoy photons and they calculate the error rate in the channel by comparing the measurement results with the initial states. If the error rate is low, then they continue the protocol, otherwise they terminate this.

4. Authentication procedure:

   (a) Bob knows the exact positions of the decoy photons of S_A corresponding to his identity ID_B. He measures those decoy photons in proper bases according to ID_A. If $ID_{A,i} = 0$, then he chooses the Z basis and if $ID_{A,i} = 1$, then he chooses the $X = \{|+\rangle, |-\rangle\}$ basis to measure $S_{A,i}$.

   (b) For $1 \leq i \leq k$, Alice and Bob construct an k-bit string $info(S_A)$ such that, if $S_{A,i} = |0\rangle$ or $|+\rangle$, then $info(S_{A,i}) = 0$, else $info(S_{A,i}) = 1$.

   (c) They randomly choose $k/2$ (approximate) positions and Alice announces the values of the corresponding bits of $info(S_A)$. Bob compares these values with his corresponding measurement results to authenticate Alice's identity. Similarly Bob announces the remaining bits of $info(S_A)$ for his identity authentication. If any of them finds intolerable error rate, then he or she aborts this protocol.

5. Second sequence of qubits transmission: Alice prepares a third set of decoy photons D'_A randomly from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and inserts them in random positions of Q_M^2. Let the new sequence be S'' and she sends the new sequence S'' to Bob using a quantum channel.

6. Security check: After Bob receives S'', Alice announces the positions and the bases of the third set of decoy photons. Bob measures those decoy photon and they calculate the error rate in the channel by comparing the measurement results with the initial states. If the error rate is low, then they continue the protocol, otherwise they terminate this protocol.

7. Message decoding:

   (a) Bob discards all the decoy photons and gets back the sequences Q_M^1 and Q_M^2.

   (b) He measures the qubit pairs of S_M in $Z \times Z$ basis or Bell basis randomly and notes the measurement results.

   (c) Bob gets all the secret message bits from the measurement results of the qubit pairs of S_M. The relation between the measurement results and the secret message bits are given in Table 2.5.

   (d) To check the integrity of the secret message, Alice and Bob publicly compare values of the random check bits. Bob discards these check bits from M and gets back m.

Note that, though quantum memories are still at the early development stage, many states of the art quantum communication protocols use quantum memory [58, 66, 68, 71, 2, 137, 267]. Here in this work we also follow a similar approach. The possible realizations of quantum memory are discussed in [268, 269, 76, 270, 271].

3.3 Security analysis of the modified protocol

We now show that our modified protocol is secure against some common attacks. First, we discuss the intercept-and-resend attack and the impersonation attack as the original YZCSS protocol was proven to be insecure against these two attacks. Then we also discuss Denial-of-

Alice (Identity Id_A)		Bob (Identity Id_B)
1. Message Encoding		
Message: M of length N.		
• Prepares qubit pairs seq. S_M.		
$*$ $M_i = 0 \Rightarrow S_{M,i} = \|01\rangle$ or $\|10\rangle$,		
$*$ $M_i = 1 \Rightarrow S_{M,i} = \|\Phi^+\rangle$ or $\|\Phi^-\rangle$.		
• Devides S_M, makes Q_M^1, Q_M^2.		
• Prepares S_A from ID_A.		
$*$ $ID_{A,i} = 0 \Rightarrow S_{A,i} = \|0\rangle$ or $\|1\rangle$,		
$*$ $ID_{A,i} = 1 \Rightarrow S_{A,i} = \|+\rangle$ or $\|-\rangle$,		
• Inserts S_A in Q_M^1 according to ID_B.		
• Inserts decoy D_A, new seq.S'.	Sends S' ⇢	
2. Security check	Position and bases of D_A →	Measures qubits of D_A.
Checks eavesdropping.	← Announces states of D_A	
3. Authentication process		Measures qubits of S_A
		Construct $info(S_A)$ from S_A.
Checks ID_B from $info(S_A)$.	$info(S_A)$ ↔	Checks ID_A from $info(S_A)$.
2. Security check		
Inserts decoy photons D'_A in Q_M^2.	Sends Q_M^2 ⇢	
	Position and bases of D_A →	Measures qubits of D_A.
Checks eavesdropping.	← Announces states of D_A	
4. Decoding process		
		Measures qubits of S_M in $Z \times Z$ or Bell basis.
		Decodes message using Table 2.5.

⇢ denotes quantum channel

⟶ denotes classical channel

Figure 3-1: Modified QSDC with authentication based on single photons and Bell states

Service attack, man-in-the-middle attack, entangle-measure attack and Trojan horse attack. We assume that *Eve* has infinite resources and unbounded computation power.

1. **Intercept-and-resend attack:** Let *Eve* intercept the sequence S' from the quantum channel. Since S' contains only the first qubit of each pair of qubits corresponding to the secret message bits, it is impossible for *Eve* to gain any information by measuring those qubits. At most *Eve* can do is to measure the qubits of S' in Z or X basis and resend those measured qubits to Bob. In that case, she does not get any useful information about the secret message, and also Alice and Bob detect her and terminate the protocol at the time of security checking (Step 3 of the modified protocol). Let the second set of decoy photons D_A contain l number of qubits.

   We now calculate the probability that Alice and Bob can detect *Eve*. Let the i-th qubit of D_A be d_i prepared in basis $\mathcal{B}_i \in \{Z, X\}$, and suppose *Eve* chooses the basis $\mathcal{B}'_i$ to measure d_i and gets d'_i. At the time of security checking, Bob measures d'_i in $\mathcal{B}_i$ and gets the result d''_i. Thus the winning probability of *Eve* for the i-th decoy qubit is

$$\begin{aligned}
&\Pr(d''_i = d_i) \\
&= \Pr(d''_i = d_i |\ \mathcal{B}_i = \mathcal{B}'_i) \Pr(\mathcal{B}i = \mathcal{B}'_i) + \Pr(d''_i = d_i |\ \mathcal{B}_i \neq \mathcal{B}'_i) \Pr(\mathcal{B}_i \neq \mathcal{B}'_i) \\
&= \frac{1}{2}\{\Pr(d''_i = d_i |\ \mathcal{B}_i = \mathcal{B}'_i) + \Pr(d''_i = d_i |\ \mathcal{B}_i \neq \mathcal{B}'_i)\} \\
&= \frac{1}{4}\left(1 + \frac{1}{2}\right) = \frac{3}{4}.
\end{aligned}$$

   Thus the probability that Alice and Bob can detect the existence of *Eve* is $1 - \left(\frac{3}{4}\right)^l > 0$. Again if *Eve* intercept the sequence S'' from the quantum channel in the second phase of transmission, then also she can not get any information about M as S'' contains only one qubit of each qubit pair. In this case, also Alice and Bob detect her with probability $1 - \left(\frac{3}{4}\right)^{l'} > 0$, where l' is the number of decoy qubits in the set D'_A, and terminate the protocol at the time of second security checking (Step 6 of the modified protocol).

2. **Impersonation attack:** In the YZCSS protocol, only Alice announces the exact states of the decoy photons corresponding to ID_A and Bob compares them with his measurement results to check the authenticity of Alice. In the modified version, both Alice and

Bob have to announce the information about the initial states of the decoy photons of S_A, they do not announce the exact states to keep ID_A secret. If Eve impersonating any one of Alice and Bob, then the other one can detect her and aborts this protocol. Let Eve impersonate Alice, then in the authentication procedure (Step 4) Eve has to construct a k-bit string as $info'(S_A)$. Then she needs to announce the bit values of $info'(S_A)$ for $k/2$ random positions jointly chosen by Bob and her. Since Eve does not know the value k and the positions of the qubits corresponding to ID_A, she just randomly guesses the bit values of $info'(S_A)$. Thus the winning probability of Eve is $(1/2)^{k/2}$ and hence Bob can detect her with probability $1-(1/2)^{k/2} > 0$. Similarly, when Eve impersonates Bob, Alice can detect her with probability $1-(1/2)^{k/2} > 0$.

3. **Denial-of-Service (DoS) attack:** The motivation of Eve, for adopting the DoS attack, is to tamper the secret message [194]. Let Eve capture the sequence S' (or S'') and make a certain operation $\mathcal{U}$ to every qubit of S'. However, this action will be detected by the legitimate parties at the security checking procedure in Step 3 and as a result, Alice and Bob terminate this protocol. Since the Pauli matrices I, σ_x, $i\sigma_y$ and σ_z form a basis for the space of all 2×2 Hermitian matrices [6], $\mathcal{U}$ can be expressed as a linear combination of these basis vectors. Let $\mathcal{U} = w_1 I + w_2\sigma_x + w_3 i\sigma_y + w_4\sigma_z$ where $\sum_{j=1}^{4} w_j^2 = 1$ as $\mathcal{U}$ is unitary.

   Now we calculate the winning probability of Eve for each decoy qubit $d \in D_A$ (or $d \in D'_A$). First we individually calculate the winning probabilities p_1, p_2, p_3 and p_4 of Eve if she applies the Pauli matrices I, σ_x, $i\sigma_y$ and σ_z respectively. We obtain $p_1 = 1$, as I applied on d does not change its state; $p_2 = 1/2$, as σ_x changes the state of a decoy qubit d only if $d \in \{|0\rangle, |1\rangle\}$; $p_3 = 0$, as $i\sigma_y$ always changes the state of a decoy qubit; and $p_4 = 1/2$, as σ_z changes the states in X-basis. Therefore the winning probability of Eve is $p = \sum_{j=1}^{4} p_j w_j^2 < 1$, unless $\mathcal{U} = I$ (which is equivalent to no attack by Eve). Hence in the security check processes (Step 3 and Step 6 of the modified protocol) Alice and Bob find this eavesdropping with probability $1 - p^l > 0$ (or with $1 - p^{l'} > 0$).

4. **Man-in-the-middle attack:** When Alice sends the sequence S' (or S'') to Bob, Eve intercepts S' (or S'') and keep this with her. She prepares another set of qubits T' (or

T'') and sends it to Bob. In this case, also Alice and Bob can realize the existence of *Eve* and abort the protocol in Step 3 (or Step 6) and terminate the protocol. We now calculate the detection probability of *Eve* when she intercepts S'. Let the i-th decoy qubit of D_A be d_i and suppose it is the j-th qubit of S'. Also let *Eve* prepare t_j as the j-th qubit of T'. Let the preparation bases of d_i and t_j be $\mathcal{B}_1$ and $\mathcal{B}_2$ respectively. In the security check process, Bob measures t_j in basis $\mathcal{B}_1$ and gets t'_j. Thus the winning probability of *Eve* for the i-th decoy qubit is as follows:

$$\begin{aligned}
&\Pr(t'_j = d_i) \\
&= \Pr(t'_j = d_i|\ \mathcal{B}_1 = \mathcal{B}_2)\Pr(\mathcal{B}_1 = \mathcal{B}_2) + \Pr(t'_j = d_i|\ \mathcal{B}_1 \neq \mathcal{B}_2)\Pr(\mathcal{B}_1 \neq \mathcal{B}_2) \\
&= \frac{1}{2}\{\Pr(t'_j = d_i|\ \mathcal{B}_1 = \mathcal{B}_2) + \Pr(t'_j = d_i|\ \mathcal{B}_1 \neq \mathcal{B}_2)\} \\
&= \frac{1}{2}[\Pr(t'_j = d_i|\ \mathcal{B}_1 = \mathcal{B}_2,\ t_j = d_i)\Pr(t_j = d_i) + \\
&\qquad\qquad \Pr(t'_j = d_i|\ \mathcal{B}_1 = \mathcal{B}_2,\ t_j \neq d_i)\Pr(t_j \neq d_i) + 1/2] \\
&= \frac{1}{2}\left[1 \times \frac{1}{2} + 0 \times \frac{1}{2} + \frac{1}{2}\right] = \frac{1}{2}.
\end{aligned}$$

Hence Alice and Bob detect *Eve* with probability $1 - (1/2)^l > 0$. Similar argument follows for the second transmission phase also.

5. **Entangle-measure attack:**

In order to steal partial information, *Eve* may apply this attack [151]. She first intercepts the qubits of the sequence S' and prepares some ancillary state $|E\rangle$, then applies an unitary U_E to the joint states of qubits of S' and $|E\rangle$ such that the composite system become entangled. Let the i-th decoy state in D_A be d_i and after applying U_E suppose it becomes d'_i. However, the effect of the unitary operation U_E on the second set of decoy photons are as follows:

$$\begin{aligned}
U_E\,|0\rangle\,|E\rangle &= \alpha_0\,|0\rangle\,|E_{00}\rangle + \beta_0\,|1\rangle\,|E_{01}\rangle\,, \\
U_E\,|1\rangle\,|E\rangle &= \alpha_1\,|0\rangle\,|E_{10}\rangle + \beta_1\,|1\rangle\,|E_{11}\rangle\,.
\end{aligned} \tag{3.3}$$

Since U_E is unitary, we must have

$$\begin{aligned} |\alpha_0|^2 + |\beta_0|^2 &= 1, \\ |\alpha_1|^2 + |\beta_1|^2 &= 1, \\ \alpha_0\alpha_1^* + \beta_0\beta_1^* &= 0. \end{aligned} \tag{3.4}$$

Thus when the decoy state d_i is prepared in Z basis, the error rate is $e = |\beta_0|^2 = |\alpha_1|^2$.

Further, we get

$$\begin{aligned} U_E |+\rangle |E\rangle &= \frac{1}{\sqrt{2}}(|+\rangle |E_{++}\rangle + |-\rangle |E_{+-}\rangle), \\ U_E |-\rangle |E\rangle &= \frac{1}{\sqrt{2}}(|+\rangle |E_{-+}\rangle + |-\rangle |E_{--}\rangle), \end{aligned} \tag{3.5}$$

where

$$\begin{aligned} |E_{++}\rangle &= \tfrac{1}{\sqrt{2}}(\alpha_0 |E_{00}\rangle + \beta_0 |E_{01}\rangle + \alpha_1 |E_{10}\rangle + \beta_1 |E_{11}\rangle), \\ |E_{+-}\rangle &= \tfrac{1}{\sqrt{2}}(\alpha_0 |E_{00}\rangle - \beta_0 |E_{01}\rangle + \alpha_1 |E_{10}\rangle - \beta_1 |E_{11}\rangle), \\ |E_{-+}\rangle &= \tfrac{1}{\sqrt{2}}(\alpha_0 |E_{00}\rangle + \beta_0 |E_{01}\rangle - \alpha_1 |E_{10}\rangle - \beta_1 |E_{11}\rangle), \\ |E_{--}\rangle &= \tfrac{1}{\sqrt{2}}(\alpha_0 |E_{00}\rangle - \beta_0 |E_{01}\rangle - \alpha_1 |E_{10}\rangle + \beta_1 |E_{11}\rangle). \end{aligned}$$

Thus if the decoy state d_i is prepared in X basis, then Bob measures the first qubit d_i' of the entangled state $U_E |+\rangle |E\rangle$ or $U_E |-\rangle |E\rangle$ in X basis. Therefore he gets the correct result with probability 1/2, and hence the error rate is 1/2. Hence from the error rate introduced by *Eve* in the communication process, Alice and Bob detect this eavesdropping in Step 3. Furthermore, if *Eve* applies this attack on the second stage of transmission, then also in a similar way Alice and Bob can detect her.

6. **Trojan horse attack:** Both the YZCSS protocol and its modified version are one-way quantum communication protocols, i.e., only Alice prepares qubits and sends them to Bob. Thus these protocols have immunity to the Trojan horse attack.

3.4 Discussion

In this chapter, we analyze the security of a QSDC protocols with authentication (YZCSS protocol) and demonstrate that this protocol is vulnerable to two specific attacks, namely, intercept-and-resend attack and impersonation attack. An eavesdropper adopting any one of these two attacks gets the whole secret message. The authentication process in the YZCSS protocol is unidirectional, which causes the impersonation attack. To address these concerns, we propose a modification of the YZCSS protocol, where a mutual authentication process is suggested, and the modified protocol resists the intercept-and-resend attack. We also prove that it is secure against several familiar attack strategies.

Chapter 4

A New Approach of QSDC Design using a Single Basis

Almost every quantum cryptographic protocol uses either entangled states or single qubit states randomly prepared in a pair of orthogonal bases, to transmit information securely. This chapter is based on the work [221], where for the first time, we propose a QSDC protocol, which also provides mutual identity authentication of the participants by using only one orthogonal basis, chosen randomly from a predefined finite set of bases, of single qubit states for encoding the secret message. In the present protocol, the message sender Alice prepares a sequence of single-qubit states corresponding to her message in a randomly chosen arbitrary basis and sends it to the receiver Bob through a quantum channel. Then Alice publicly announces some classical information and they check the security of the channel. If they find any eavesdropper in the channel, then they terminate the protocol. However, in this case the eavesdropper can not get any information about the secret message. After the security check process is passed, then Bob uses the information of Alice to measure the received qubits and to get the secret message. Furthermore, in this protocol, we use only one orthogonal basis to encode all the secret information. But since the basis is chosen arbitrarily, any eavesdropper can not guess the basis of the encoded qubits and therefore the protocol remains secure. Although this protocol requires hardware that can operate a gate $U(\theta)$ for any $\theta \in \mathbb{Z}_{360}$, modern quantum hardware such as the IBM Quantum Device allows the creation of such operators using the parameterized U_1 and U_2 gates [272]. Furthermore, as described later in detail, the measurement is always

in $\{|0\rangle, |1\rangle\}$ basis only, and does not require hardware ability to measure in arbitrary bases. Therefore, it is possible to execute this protocol in available quantum hardware, and we have shown the results of such execution in Section 4.

Execution of the protocol in real devices makes them susceptible to the channel noise - in particular decoherence, calibration and readout error. We have executed this protocol in the IBMQ Armonk Device [273] to study the behaviour of it in the presence of noise. We show that the effect of noise is equivalent to a bit-flip error in the case of this protocol. We further show from our execution results that the effect of noise does not depend on the choice of basis. In order to account for the non-instantaneous nature of any quantum channel, we model an ideal quantum channel as a series of identity gates without any Eavesdropper. However, in a realistic scenario, these gates are susceptible to noise, and the channel no longer behaves as identity. Our execution results show that a minimal overhead of a 3-qubit repetition code is sufficient to protect this protocol against noise as long as the number of identity gates (i.e. the length of the quantum channel) is below a certain threshold.

4.1 QSDC protocol with mutual authentication

In this section, we propose the new QSDC protocol with a mutual identity authentication process. We use the basic idea of quantum identity authentication scheme [274] to verify the identity of the message sender.

Without loss of generality, let Alice be the sender and Bob be the receiver. Also, let Alice and Bob have their previously shared k-bit authentication identities (we assume k is even) Id_A and Id_B respectively (using some secured QKD). Alice wants to send a message $M = M_1 M_2 \dots M_n$ to Bob. Let Θ be a predefined ordered set of angles with finite cardinality N. For each $\theta \in \Theta$, the unitary matrix U_θ is defined as

$$U_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

Then $U_\theta |0\rangle = \cos\theta |0\rangle + \sin\theta |1\rangle = |x\rangle$ (say), and $U_\theta |1\rangle = -\sin\theta |0\rangle + \cos\theta |1\rangle = |y\rangle$ (say).

For simplicity, in our protocol, we take $\Theta = \{x^\circ : x \text{ is an integer and } 1 \leq x \leq 360\}$. Thus

here, $N = 360$. Note that, one can use an ordered set of real angles instead of integer angles, i.e., $\Theta = \{x_1^\circ, x_2^\circ, \ldots, x_N^\circ\}$, where each $x_i \in \mathbb{R}$ for $1 \leq i \leq N$. In either case, to encode $\theta = x_i^\circ$, Alice just encodes the $\lceil log_2 N \rceil$ bit binary representation of i in Step (1f) of the following protocol, where $\lceil log_2 N \rceil$ denotes the smallest integer no smaller than $log_2 N$.

1. Encoding process:

   (a) Alice puts some random check bits in random positions of her n-bit message M. Let the new bit string be M', which contains $n' = n + c$ bits, where c is the number of check bits.

   (b) She prepares a sequence Q_A^1 containing n' number of single qubits in $\{|0\rangle, |1\rangle\}$ basis corresponding to M'. She prepares $|0\rangle$ and $|1\rangle$ corresponding to message bit 0 and 1 respectively.

   (c) Alice randomly chooses an angle $\theta \in \Theta$ and applies the unitary operator U_θ on all the qubits of Q_A^1. Thus all the qubits of Q_A^1 are now in $\{|x\rangle, |y\rangle\}$ basis.

   (d) She prepares a sequence of single qubits I_A corresponding to her authentication identity Id_A. For $1 \leq i \leq k/2$ (as k is even), she chooses the i-th qubit of I_A as $|0\rangle, |1\rangle, |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, according to the values $00, 01, 10$ and 11 of the $(2i-1)$-th and the $2i$-th bits of Id_A. She randomly inserts the qubits of I_A into Q_A^1 and let the new sequence be Q_A^2 containing $n' + k/2$ number of qubits.

   (e) Alice chooses a k-bit random number r and prepares a sequence of single qubits I_B corresponding to the bit strings $Id_B^1 = Id_B \oplus r$ and Id_B. For $1 \leq i \leq k$, let the i-th bit of Id_B (Id_B^1) be $Id_{B,i}$ ($Id_{B,i}^1$),

      i. if $Id_{B,i}^1 = 0$ (1) and $Id_{B,i} = 0$, then the i-th qubit of I_B is $|0\rangle$ ($|1\rangle$),

      ii. if $Id_{B,i}^1 = 0$ (1) and $Id_{B,i} = 1$, then the i-th qubit of I_B is $|+\rangle$ ($|-\rangle$).

      She randomly inserts the qubits of I_B into Q_A^2 and let the new sequence be Q_A^3 containing $n' + 3k/2$ number of qubits.

   (f) She also encodes the value of θ by preparing a sequence of single qubits Q_θ corresponding to the binary representation of $\theta = \theta_1\theta_2 \ldots \theta_{k'}$ containing k' bits. Note

that since θ is an integer, whose value lies between 0 to 360, $k' \leq 9$. We assume $k \geq k'$ and then the encoding strategy, for $1 \leq i \leq k'$, is:

i. if $\theta_i = 0$ (1) and $Id_{B,i} = 0$, then prepares $|0\rangle$ ($|1\rangle$),

ii. if $\theta_i = 0$ (1) and $Id_{B,i} = 1$, then prepares $|+\rangle$ ($|-\rangle$).

She puts these single qubits in random positions of Q_A^3 and let the new sequence be Q_A^4 containing $n' + 3k/2 + k'$ number of qubits.

(g) Finally she chooses a sequence D_A of m number of decoy photons randomly from $\{|0\rangle, |1\rangle,$
$|+\rangle, |-\rangle\}$ and inserts them in random positions of Q_A^4. Let the new sequence be Q_A^5 containing $l = n' + 3k/2 + k' + m$ single qubits. Alice sends Q_A^5 to Bob through a quantum channel.

2. Security check: After Bob receives Q_A^5, they check if there is any eavesdropper in the channel. Alice announces the positions and bases of the decoy photons. Bob measures the decoy photons and announces the results. By comparing these measurement results and the initial states of the decoy photons, Alice calculates the error in the channel. If the estimated error is greater than some threshold value, then it proves the existence of some eavesdropper in the channel. In that case, they abort the task; otherwise, they continue the protocol.

3. Authentication procedure:

(a) Alice tells the positions of the single qubits of I_A and Bob measures those qubits in the proper bases corresponding to Id_A, i.e., he chooses $\{|0\rangle, |1\rangle\}$ basis if the corresponding bits of Id_A are 00 or 01; otherwise he chooses $\{|+\rangle, |-\rangle\}$ basis if the corresponding bits of Id_A are 10 or 11. Bob compares his measurement results with the bits of Id_A and calculates the error rate. Low error rate implies that there is no eavesdropper impersonating Alice, then he continues the process, otherwise terminates it.

(b) Alice tells the positions of the single qubits of I_B and Bob measures those qubits in the proper bases corresponding to Id_B, i.e., he chooses $\{|0\rangle, |1\rangle\}$ ($\{|+\rangle, |-\rangle\}$) basis

if the corresponding bit of Id_B is 0 (1). Then from the measurement results, Bob gets Id_B^1 and announces $r = Id_B \oplus Id_B^1$. Alice checks the value of r to confirm Bob's authenticity and decides to continue or abort the communication.

4. Decoding process:

   (a) Alice tells Bob the positions of the qubits of Q_θ and Bob measures those qubits on proper bases corresponding to Id_B, i.e., if the i-th bit Id_B is 0 (1), then he chooses $\{|0\rangle, |1\rangle\}$ ($\{|+\rangle, |-\rangle\}$) basis to measure the i-th qubit of Q_θ. After measuring all the qubits of Q_θ, he gets the value of θ_i, for $1 \leq i \leq k'$. Bob calculates the decimal representation of $\theta_1\theta_2 \ldots \theta_{k'}$ to get the actual value of θ. One can note that, since Id_B is a secret key, nobody except Bob can decode the value of θ.

   (b) Bob discards all the measured qubits and gets back the sequence Q_A^1 (since all the qubits of the set $(Q_A^5 \setminus Q_A^1)$ are already measured in the previous steps). As Bob knows the value of θ, he applies the unitary operator ${U_\theta}^{-1}$ to all the qubits of Q_A^1. Thus all the qubits of Q_A^1 are now in $\{|0\rangle, |1\rangle\}$ basis. Now Bob measures these qubits in $\{|0\rangle, |1\rangle\}$ basis. If the i-th measurement result is $|0\rangle$, then Bob concludes ${M'}_i = 0$, else ${M'}_i = 1$, i.e., he decodes the classical bit M'_i of the string M'.

   (c) To check the integrity of the secret message, they publicly compare the random check bits and calculate the error rate. If it is negligible, then by discarding the check bits from M', Bob gets M. Otherwise, they abort the protocol.

Example 4. *Let us take an example of the above discussed QSDC protocol.*
$\Theta = \{x^\circ : x$ *is an integer and* $1 \leq x \leq 8\}$, $Id_A = 1100$, $Id_B = 0111$ *and the secret message* $M = 011101$.

1. *Encoding process:*

   (a) Alice inserts check bits 1 *and* 0 *after the* 1*st and* 3*rd bits of* M*, i.e.,* $M' = 0\mathbf{1}11\mathbf{0}101$. *(Bold numbers are check bits.)*

   (b) $Q_A^1 = |0\rangle |1\rangle |1\rangle |1\rangle |0\rangle |1\rangle |0\rangle |1\rangle$.

Alice (Identity Id_A)		Bob (Identity Id_B)
1. Message Encoding		
Message M, chooses θ and r.		
• Inserts check bits in M.		
• Encodes: $0 \rightarrow U_\theta \left\|0\right\rangle,\ 1 \rightarrow U_\theta \left\|1\right\rangle$.		
• Prepares sequence Q_A^1		
• Inserts $I_A,\ I_B,\ Q_\theta,\ D_A$ in Q_A^1.		
Prepared sequence Q_A^5	Sends Q_A^5 ⇢	
2. Security check		
	Position and bases of D_A →	Measures qubits of D_A.
Checks eavesdropping.	← Announces states of D_A	
3. Authentication process		
	Positions of I_A →	Measures qubits of I_A
		Checks Id_A
	Positions of I_B →	Calculates $r = Id_B \oplus Id_B^1$.
Checks Id_B	← Sends r	
4. Decoding process		
	Positions of Q_θ →	• Measures qubits of Q_θ, gets θ
		• Discards measured qubits.
		• Applies ${U_\theta}^{-1}$.
		• Measures in $\{\left\|0\right\rangle, \left\|1\right\rangle\}$.
	Check bits →	Checks eavesdropping and Get M.

⇢ denotes quantum channel

⟶ denotes classical channel

Notations: $\theta \in \Theta$, $r \in \{0,1\}^k$, Q_θ : qubits corresponding to θ, D_A : decoy qubits,
I_A : qubits corresponding to Id_A and I_B : qubits corresponding to Id_B^1, $Id_B^1 = Id_B \oplus r$.

Figure 4-1: Proposed QSDC protocol with mutual authentication

(c) *Alice chooses* $\theta = 7^\circ$ *and applies* U_θ *on the qubits of* Q_A^1. *Then* $Q_A^1 = |x\rangle\,|y\rangle\,|y\rangle\,|y\rangle\,|x\rangle\,|y\rangle\,|x\rangle\,|y\rangle$, *where* $|x\rangle = U_\theta\,|0\rangle$, $|y\rangle = U_\theta\,|1\rangle$.

(d) $I_A = |-\rangle\,|0\rangle$ *and* $Q_A^2 = |x\rangle\,|y\rangle\,\boxed{|-\rangle}\,|y\rangle\,\boxed{|0\rangle}\,|y\rangle\,|x\rangle\,|y\rangle\,|x\rangle\,|y\rangle$, *where the boxed qubits are randomly added from* I_A.

(e) *Alice chooses* $r = 1001$, *then* $Id_B^1 = Id_B \oplus r = 0111 \oplus 1001 = 1110$, $I_B = |1\rangle\,|-\rangle\,|-\rangle\,|+\rangle$ *and* $Q_A^3 = |x\rangle\,\boxed{|1\rangle}\,|y\rangle\,|-\rangle\,\boxed{|-\rangle}\,|y\rangle\,|0\rangle\,|y\rangle\,\boxed{|-\rangle}\,|x\rangle\,|y\rangle\,|x\rangle\,\boxed{|+\rangle}\,|y\rangle$, *where the boxed qubits are randomly added from* I_B.

(f) $Q_\theta = |1\rangle\,|-\rangle\,|-\rangle$ *and* $Q_A^4 = |x\rangle\,|1\rangle\,|y\rangle\,|-\rangle\,|-\rangle\,|y\rangle\,\boxed{|1\rangle}\,|0\rangle\,\boxed{|-\rangle}\,|y\rangle\,|-\rangle\,|x\rangle\,|y\rangle\,\boxed{|-\rangle}\,|x\rangle\,|+\rangle\,|y\rangle$, *where the boxed qubits are randomly added from* Q_θ.

(g) *Decoy photons* $D_A = |0\rangle\,|1\rangle\,|+\rangle\,|0\rangle$ *and* $Q_A^5 = |x\rangle\,\boxed{|0\rangle}\,|1\rangle\,\boxed{|1\rangle}\,|y\rangle\,|-\rangle\,|-\rangle\,|y\rangle\,|1\rangle\,|0\rangle\,|-\rangle\,|y\rangle\,|-\rangle\,|x\rangle\,\boxed{|+\rangle}\,|y\rangle\,|-\rangle\,|x\rangle\,\boxed{|0\rangle}\,|+\rangle\,|y\rangle$, *where the boxed qubits are randomly added from* D_A.

(h) *Alice sends* $Q_A^5 = |x\rangle\,|0\rangle\,|1\rangle\,|1\rangle\,|y\rangle\,|-\rangle\,|-\rangle\,|y\rangle\,|1\rangle\,|0\rangle\,|-\rangle\,|y\rangle\,|-\rangle\,|x\rangle\,|+\rangle\,|y\rangle\,|-\rangle\,|x\rangle\,|0\rangle\,|+\rangle\,|y\rangle$ *to Bob.*

2. *Security check: After Bob receives* Q_A^5, *Alice announces the positions* (2*nd*, 4*th*, 15*th and* 19*th*) *and bases* ($\{|0\rangle, |1\rangle\}$, $\{|0\rangle, |1\rangle\}$, $\{|+\rangle, |-\rangle\}$, $\{|0\rangle, |1\rangle\}$) *of the decoy photons. Bob measures the decoy photons and announces the results* ($|0\rangle, |1\rangle, |+\rangle, |0\rangle$). *Alice calculates the error in the channel. Here, we assume a noiseless channel. Hence, Bob discards all the measured qubits and gets back the sequence* Q_A^4.

3. *Authentication procedure:*

(a) *Alice announces the positions* (4*th and* 8*th*) *of the qubits of* I_A *and Bob chooses the bases* ($\{|+\rangle, |-\rangle\}$, $\{|0\rangle, |1\rangle\}$ *to measure those qubits and gets* $|-\rangle\,|0\rangle$, *which is equivalent to* Id_A.

(b) *Alice tells the positions* (2*nd*, 5*th*, 11*th and* 16*th*) *of the single qubits of* I_B *and Bob chooses the bases* ($\{|0\rangle, |1\rangle\}$, $\{|+\rangle, |-\rangle\}$, $\{|+\rangle, |-\rangle\}$) *and* $\{|+\rangle, |-\rangle\}$) *to measure those qubits and gets* $|1\rangle\,|-\rangle\,|-\rangle\,|+\rangle$. *He gets* $Id_B^1 = 1110$ *announces* $r = 1110 \oplus 0111 = 1001$. *Alice confirms Bob's identity.*

4. Decoding process:

(a) Alice tells Bob the positions (7th, 9th and 14th) of the qubits of Q_θ and Bob chooses the bases ($\{|0\rangle, |1\rangle\}$, $\{|+\rangle, |-\rangle\}$, $\{|+\rangle, |-\rangle\}$) to measure those qubits and obtains θ.

(b) He discards all the measured qubits to get Q_A^1 and applies ${U_\theta}^{-1}$ to all the qubits of Q_A^1. Bob measures these qubits in $\{|0\rangle, |1\rangle\}$ basis and gets $M' = 01110101$.

(c) They publicly compare the random check bits (2nd and 5th bit of M') and Bob discards those bits to obtain $M = 011101$.

This completes the QSDC protocol.

4.2 Security analysis

We now discuss the security of the proposed protocol against some familiar attack strategies such as the impersonation attack, intercept-and-resend attack, entangle-and-measure attack, DoS attack, man-in-the-middle attack, information leakage attack, and Trojan horse attack. We assume that *Eve* has infinite resources and unbounded computation power.

1. **Impersonation attack:** Let us first discuss this attack model, where an eavesdropper (*Eve*) is impersonating a legitimate party. First, we assume *Eve* impersonates Alice to send a wrong message to Bob. Since *Eve* has no knowledge about Id_A, she prepares the qubits of I'_A randomly from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. As Bob knows Id_A, he chooses the corresponding bases to measure the qubits of I'_A. According to the value of the bits $Id_{A,(2i-1)}Id_{A,2i}$, let the i-th qubit of I_A be $I_{A,i}$ prepared in basis $\mathcal{B}$, where $\mathcal{B} = \{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$. Also let *Eve* prepare the i-th qubit $I'_{A,i}$ in $\mathcal{B}'$ basis. Since Bob knows the exact state of $I_{A,i}$, he measures $I'_{A,i}$ in $\mathcal{B}$ basis and let the measurement result be $I''_{A,i}$. Now the probability that Bob can not find this eavesdropping is $\Pr(I''_{A,i} = I_{A,i})$. Now,

   - If $\mathcal{B} = \mathcal{B}'$ and $I_{A,i} = I'_{A,i}$, then $I''_{A,i} = I_{A,i}$ with probability 1.
   - If $\mathcal{B} = \mathcal{B}'$ and $I_{A,i} \neq I'_{A,i}$, then $I''_{A,i} = I_{A,i}$ with probability 0.
   - If $\mathcal{B} \neq \mathcal{B}'$, then $I''_{A,i} = I_{A,i}$ with probability 1/2.

Thus for each qubit of I'_A the winning probability of Eve is

$$\begin{aligned}
&\Pr(I''_{A,i} = I_{A,i}) \\
&= \Pr(I''_{A,i} = I_{A,i} |\ \mathcal{B} = \mathcal{B}') \Pr(\mathcal{B} = \mathcal{B}') + \Pr(I''_{A,i} = I_{A,i} |\ \mathcal{B} \neq \mathcal{B}') \Pr(\mathcal{B} \neq \mathcal{B}') \\
&= \frac{1}{2}[\Pr(I''_{A,i} = I_{A,i} |\ \mathcal{B} = \mathcal{B}') + \Pr(I''_{A,i} = I_{A,i} |\ \mathcal{B} \neq \mathcal{B}')] \\
&= \frac{1}{2}[\Pr(I''_{A,i} = I_{A,i} |\ \mathcal{B} = \mathcal{B}',\ I_{A,i} = I'_{A,i}) \Pr(I_{A,i} = I'_{A,i}) + \\
&\qquad \Pr(I''_{A,i} = I_{A,i} |\ \mathcal{B} = \mathcal{B}',\ I_{A,i} \neq I'_{A,i}) \Pr(I_{A,i} \neq I'_{A,i}) + 1/2] \\
&= \frac{1}{2}\left[1 \times \frac{1}{2} + 0 \times \frac{1}{2} + \frac{1}{2}\right] = \frac{1}{2}.
\end{aligned}$$

Hence in the authentication process, Bob can detect Eve with probability $1 - (1/2)^{k/2}$.

On the other hand, now let Eve impersonate Bob to get the secret message from Alice. Then Eve has no idea about the preparation bases of the qubits of I_B and thus she randomly chooses basis $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$ to measure those qubits. From the measurement results, she correctly guesses the value of Id_B^1 with probability $(3/4)^k$. Since $Id_B^1 = Id_B \oplus r$ and Id_B is unknown to Eve, from the security notion of "One-Time-Pad", r is completely random to her and she correctly guesses r with probability $(1/2)^k$. Therefore, when Eve announces the random number r, Alice detects her with probability $1 - (1/2)^k$.

So for both cases, the legitimate party can detect the eavesdropping with a high probability.

2. **Intercept-and-resend attack:** In this attack model, Eve intercepts the qubits from the quantum channel from Alice to Bob, then she measures those qubits and resends to Bob. In our proposed protocol, let Eve intercept the sequence Q_A^5 from the quantum channel. Note that the qubits corresponding to M' are encoded in an arbitrary basis $\{|x\rangle, |y\rangle\}$ and those are in random positions of Q_A^5. Let Eve choose a random $\theta_0 \in \Theta$ and measure all the qubits in $\{|x_0\rangle, |y_0\rangle\}$ basis, where,

$$
\begin{aligned}
|x_0\rangle = U_{\theta_0}|0\rangle &= \cos\theta_0|0\rangle + \sin\theta_0|1\rangle \\
&= \frac{1}{\sqrt{2}}[(\cos\theta_0 + \sin\theta_0)|+\rangle + (\cos\theta_0 - \sin\theta_0)|-\rangle]
\end{aligned}
\tag{4.1}
$$

and

$$
\begin{aligned}
|y_0\rangle = U_{\theta_0}|1\rangle &= -\sin\theta_0|0\rangle + \cos\theta_0|1\rangle \\
&= \frac{1}{\sqrt{2}}[(\cos\theta_0 - \sin\theta_0)|+\rangle - (\cos\theta_0 + \sin\theta_0)|-\rangle].
\end{aligned}
\tag{4.2}
$$

Then,

$$
\begin{aligned}
|0\rangle &= \cos\theta_0|x\rangle - \sin\theta_0|y\rangle, \\
|1\rangle &= \sin\theta_0|x\rangle + \cos\theta_0|y\rangle
\end{aligned}
\tag{4.3}
$$

and

$$
\begin{aligned}
|+\rangle &= \frac{1}{\sqrt{2}}[(\cos\theta_0 + \sin\theta_0)|x\rangle + (\cos\theta_0 - \sin\theta_0)|y\rangle], \\
|-\rangle &= \frac{1}{\sqrt{2}}[(\cos\theta_0 - \sin\theta_0)|x\rangle - (\cos\theta_0 + \sin\theta_0)|y\rangle].
\end{aligned}
\tag{4.4}
$$

Table 4.1: Effects of Eve's measurement on decoy photons

Original state $D_{A,i}$	**After Eve's measurement: $D'_{A,i}$**		**After Bob's measurement: $D''_{A,i}$**	
	State	**Probability**	**State**	**Probability**
$\|0\rangle$	$\|x_0\rangle$	$\cos^2\theta_0$	$\|0\rangle$	$\cos^2\theta_0$
	$\|y_0\rangle$	$\sin^2\theta_0$		$\sin^2\theta_0$
$\|1\rangle$	$\|x_0\rangle$	$\sin^2\theta_0$	$\|1\rangle$	$\sin^2\theta_0$
	$\|y_0\rangle$	$\cos^2\theta_0$		$\cos^2\theta_0$
$\|+\rangle$	$\|x_0\rangle$	$\frac{1}{2}(\cos\theta_0 + \sin\theta_0)^2$	$\|+\rangle$	$\frac{1}{2}(\cos\theta_0 + \sin\theta_0)^2$
	$\|y_0\rangle$	$\frac{1}{2}(\cos\theta_0 - \sin\theta_0)^2$		$\frac{1}{2}(\cos\theta_0 - \sin\theta_0)^2$
$\|-\rangle$	$\|x_0\rangle$	$\frac{1}{2}(\cos\theta_0 - \sin\theta_0)^2$	$\|-\rangle$	$\frac{1}{2}(\cos\theta_0 - \sin\theta_0)^2$
	$\|y_0\rangle$	$\frac{1}{2}(\cos\theta_0 + \sin\theta_0)^2$		$\frac{1}{2}(\cos\theta_0 + \sin\theta_0)^2$

Eve's measurement affects the decoy photons as well. Let the i-th decoy photon be $D_{A,i}$ prepared in basis $\mathcal{B}$, where $\mathcal{B} = \{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$, and after *Eve* measures in

$\{|x_0\rangle, |y_0\rangle\}$ basis the state becomes $D'_{A,i}$. When Alice announces the preparation basis of $D_{A,i}$, then Bob measures $D'_{A,i}$ in basis $\mathcal{B}$ and gets $D''_{A,i}$. We now calculate the probability that $D_{A,i} = D''_{A,i}$. From Table 4.1 we get,

$$
\begin{aligned}
&\Pr(D''_{A,i} = D_{A,i}) \\
&= \sum_{|b\rangle \in \{|0\rangle, |1\rangle\}} \Pr(D''_{A,i} = |b\rangle, D_{A,i} = |b\rangle) + \sum_{|b\rangle \in \{|+\rangle, |-\rangle\}} \Pr(D''_{A,i} = |b\rangle, D_{A,i} = |b\rangle) \\
&= \sum_{|b\rangle \in \{|0\rangle, |1\rangle\}} \Pr(D''_{A,i} = |b\rangle \mid D_{A,i} = |b\rangle) \Pr(D_{A,i} = |b\rangle) + \\
&\qquad \sum_{|b\rangle \in \{|+\rangle, |-\rangle\}} \Pr(D_{A,i} = |b\rangle \mid D''_{A,i} = |b\rangle) \Pr(D_{A,i} = |b\rangle) \\
&= \frac{1}{4}\left[\sum_{|b\rangle \in \{|0\rangle, |1\rangle\}} \Pr(D''_{A,i} = |b\rangle \mid D_{A,i} = |b\rangle) + \sum_{|b\rangle \in \{|+\rangle, |-\rangle\}} \Pr(D''_{A,i} = |b\rangle \mid D_{A,i} = |b\rangle) \right] \\
&= \frac{1}{4}\left[2\left(\cos^4\theta_0 + \sin^4\theta_0\right) + 2\left\{ \frac{1}{4}\left(\cos\theta_0 + \sin\theta_0\right)^4 + \frac{1}{4}\left(\cos\theta_0 - \sin\theta_0\right)^4 \right\} \right] \\
&= \frac{1}{2}\left[\left(\cos^4\theta_0 + \sin^4\theta_0\right) + \frac{1}{2}\left(1 + sin^2 2\theta_0\right) \right] \\
&= \frac{1}{2}\left(sin^2\theta_0 + cos^2\theta_0\right)^2 + \frac{1}{4} = \frac{3}{4}.
\end{aligned}
$$

Thus the probability that Alice and Bob can realize the existence of *Eve* is $1 - \left(\frac{3}{4}\right)^m$, where m is the number of decoy photons. However, in this case the legitimate parties detect her and terminates the protocol.

Now, let us calculate the probability p_{corr}, that *Eve* guesses the original n-bit message M of Alice correctly. If *Eve* chooses $\theta_0 = \theta$ and measures the qubits of the sequence Q_A^5 in $\{|x\rangle, |y\rangle\}$ basis, then she have to choose the correct n positions corresponding to the message bits among $l = n' + 3k/2 + k' + m$ positions. Thus the winning probability of *Eve* is:

$$p_{corr} = \frac{1}{N \times \binom{l}{n}}.$$

For positive integers n and l with $1 \leq n \leq l$, we know that, $\left(\frac{l}{n}\right)^n \leq \binom{l}{n}$, which implies

$$p_{corr} \leq \frac{1}{N}\left(\frac{n}{l}\right)^n \leq \left(\frac{1}{2}\right)^{\lfloor log_2 N \rfloor} \times \left(\frac{n}{l}\right)^n \leq \left(\frac{1}{2}\right)^n, \text{ if } l \geq 2n\left(\frac{1}{2}\right)^{\lfloor log_2 N \rfloor / n},$$

where $\lfloor log_2 N \rfloor$ denotes the greatest integer less than or equal to $log_2 N$. So for our case $p_{corr} \leq \left(\frac{1}{2}\right)^n$, if $l \geq 2n\left(\frac{1}{2}\right)^{8/n}$. Since p_{corr} is negligible, our protocol is secure against this attack strategy.

3. **Entangle-and-measure attack:** In addition to the above discussed attacks, there is a different kind of attack, called entangle-and-measure attack, which *Eve* can apply to get a partial information about M. For this purpose, *Eve* prepares a set of ancilla qubits whose initial states are $|\chi\rangle_e$. When Alice sends Q_A^5 to Bob, *Eve* performs a unitary operation $\mathcal{U}_e$ on the qubits of Q_A^5 and $|\chi\rangle_e$ to make them entangled, where $\mathcal{U}_e$ is defined as [151]:

$$\begin{aligned} \mathcal{U}_e |0\rangle |\chi\rangle_e &= \alpha_0 |0\rangle |\chi_{00}\rangle_e + \beta_0 |1\rangle |\chi_{01}\rangle_e , \\ \mathcal{U}_e |1\rangle |\chi\rangle_e &= \alpha_1 |0\rangle |\chi_{10}\rangle_e + \beta_1 |1\rangle |\chi_{11}\rangle_e , \end{aligned} \tag{4.5}$$

where the four pure states $|\chi_{00}\rangle_e$, $|\chi_{01}\rangle_e$, $|\chi_{10}\rangle_e$ and $|\chi_{11}\rangle_e$ are orthonormal and they belong to Eve's Hilbert space. They are uniquely determined by the unitary operation $\mathcal{U}_e$ and the following conditions hold,

$$\begin{aligned} |\alpha_0|^2 + |\beta_0|^2 = 1,\ |\alpha_1|^2 + |\beta_1|^2 = 1, \\ |\alpha_0|^2 = |\beta_1|^2 = \mathcal{F},\ |\alpha_1|^2 = |\beta_0|^2 = \mathcal{D}. \end{aligned} \tag{4.6}$$

If Alice sends $|b\rangle$, $b \in \{0, 1\}$, then after measurement Bob gets the correct result with probability $\mathcal{F}$. Here $\mathcal{F}$ is the fidelity and $\mathcal{D}$ is the quantum bit error rate (QBER).

Further, we get

$$\begin{aligned} \mathcal{U}_e |+\rangle |\chi\rangle_e &= \frac{1}{\sqrt{2}} (\mathcal{U}_e |0\rangle |\chi\rangle_e + \mathcal{U}_e |1\rangle |\chi\rangle_e) \\ &= \frac{1}{\sqrt{2}} [\alpha_0 |0\rangle |\chi_{00}\rangle_e + \beta_0 |1\rangle |\chi_{01}\rangle_e + \alpha_1 |0\rangle |\chi_{10}\rangle_e + \beta_1 |1\rangle |\chi_{11}\rangle_e] \\ &= \frac{1}{\sqrt{2}} [\ |+\rangle (\alpha_0 |\chi_{00}\rangle_e + \beta_0 |\chi_{01}\rangle_e + \alpha_1 |\chi_{10}\rangle_e + \beta_1 |\chi_{11}\rangle_e)/\sqrt{2} + \\ &\qquad |-\rangle (\alpha_0 |\chi_{00}\rangle_e - \beta_0 |\chi_{01}\rangle_e + \alpha_1 |\chi_{10}\rangle_e - \beta_1 |\chi_{11}\rangle_e)/\sqrt{2}\ ] \\ &= \frac{1}{\sqrt{2}} (|+\rangle |\chi_{++}\rangle_e + |-\rangle |\chi_{+-}\rangle_e) \end{aligned} \tag{4.7}$$

and

$$\begin{aligned}
\mathcal{U}_e \left|-\right\rangle \left|\chi\right\rangle_e &= \frac{1}{\sqrt{2}} \left(\mathcal{U}_e \left|0\right\rangle \left|\chi\right\rangle_e - \mathcal{U}_e \left|1\right\rangle \left|\chi\right\rangle_e\right) \\
&= \frac{1}{\sqrt{2}} \left[\alpha_0 \left|0\right\rangle \left|\chi_{00}\right\rangle_e + \beta_0 \left|1\right\rangle \left|\chi_{01}\right\rangle_e - \alpha_1 \left|0\right\rangle \left|\chi_{10}\right\rangle_e - \beta_1 \left|1\right\rangle \left|\chi_{11}\right\rangle_e\right] \\
&= \frac{1}{\sqrt{2}} [\ \left|+\right\rangle \left(\alpha_0 \left|\chi_{00}\right\rangle_e + \beta_0 \left|\chi_{01}\right\rangle_e - \alpha_1 \left|\chi_{10}\right\rangle_e - \beta_1 \left|\chi_{11}\right\rangle_e\right)/\sqrt{2} + \\
&\qquad \left|-\right\rangle \left(\alpha_0 \left|\chi_{00}\right\rangle_e - \beta_0 \left|\chi_{01}\right\rangle_e - \alpha_1 \left|\chi_{10}\right\rangle_e + \beta_1 \left|\chi_{11}\right\rangle_e\right)/\sqrt{2}\ ] \\
&= \frac{1}{\sqrt{2}} (\left|+\right\rangle \left|\chi_{-+}\right\rangle_e + \left|-\right\rangle \left|\chi_{--}\right\rangle_e).
\end{aligned} \tag{4.8}$$

If Alice sends $\left|b\right\rangle$, $b \in \{+, -\}$, then after measurement Bob gets the correct result with probability 1/2.

Now in the present protocol Alice prepares decoy states randomly from $\{\left|0\right\rangle, \left|1\right\rangle, \left|+\right\rangle, \left|-\right\rangle\}$. So for a particular decoy state $\left|b\right\rangle$, Bob gets the correct state with probability $p = \frac{1}{2}(\mathcal{F} + 1/2)$, where $\mathcal{F}$ is the fidelity when the decoy state is in $\{\left|0\right\rangle, \left|1\right\rangle\}$ and 1/2 is the fidelity when the decoy state is in $\{\left|+\right\rangle, \left|-\right\rangle\}$. Moreover, both of these cases occur with probability 1/2. Hence in security check Alice and Bob can detect *Eve* with probability $1 - p^m$, where m is the number of decoy states.

However we now show that, by applying this attack strategy, *Eve* gets no information about the secret message. From Equation (4.5) we have,

$$\begin{aligned}
\mathcal{U}_e \left|x\right\rangle \left|\chi\right\rangle_e &= \mathcal{U}_e(cos\theta \left|0\right\rangle + \sin\theta \left|1\right\rangle) \left|\chi\right\rangle_e \\
&= \left|0\right\rangle (\alpha_0 \cos\theta \left|\chi_{00}\right\rangle_e + \alpha_1 \sin\theta \left|\chi_{10}\right\rangle_e) + \left|1\right\rangle (\beta_0 \cos\theta \left|\chi_{01}\right\rangle_e + \beta_1 \sin\theta \left|\chi_{11}\right\rangle_e) \\
&= (\cos\theta \left|x\right\rangle - \sin\theta \left|y\right\rangle)(\alpha_0 \cos\theta \left|\chi_{00}\right\rangle_e + \alpha_1 \sin\theta \left|\chi_{10}\right\rangle_e) + \\
&\qquad (\sin\theta \left|x\right\rangle + \cos\theta \left|y\right\rangle)(\beta_0 \cos\theta \left|\chi_{01}\right\rangle_e + \beta_1 \sin\theta \left|\chi_{11}\right\rangle_e)
\end{aligned} \tag{4.9}$$

and

$$\begin{aligned}\mathcal{U}_e\left|y\right\rangle\left|\chi\right\rangle_e &= \mathcal{U}_e(-\sin\theta\left|0\right\rangle+\cos\theta\left|1\right\rangle)\left|\chi\right\rangle_e \\ &= \left|0\right\rangle(-\alpha_0\sin\theta\left|\chi_{00}\right\rangle_e+\alpha_1\cos\theta\left|\chi_{10}\right\rangle_e)+\left|1\right\rangle(-\beta_0\sin\theta\left|\chi_{01}\right\rangle_e+\beta_1\cos\theta\left|\chi_{11}\right\rangle_e) \\ &= (\cos\theta\left|x\right\rangle-\sin\theta\left|y\right\rangle)(-\alpha_0\sin\theta\left|\chi_{00}\right\rangle_e+\alpha_1\cos\theta\left|\chi_{10}\right\rangle_e)+ \\ &\quad (\sin\theta\left|x\right\rangle+\cos\theta\left|y\right\rangle)(-\beta_0\sin\theta\left|\chi_{01}\right\rangle_e+\beta_1\cos\theta\left|\chi_{11}\right\rangle_e).\end{aligned} \tag{4.10}$$

From Equation (4.9) and (4.10) it follows that, *Eve* gains no useful information by measuring the ancilla qubit $\left|\chi\right\rangle_e$ entangled with the qubits corresponding to the secret message.

4. **DoS attack:** In this attack model, Eve's aim is not to get secret information but to tamper with the original message [194]. To execute this attack strategy, *Eve* intercepts the qubits from the quantum channel and randomly applies I and U with probability $1/2$, where U is a random unitary operator. Since *Eve* does not know the positions of the decoy state, the unitary operation also affects those qubits.

   As the Pauli matrices [6] I, σ_x, $i\sigma_y$ and σ_z form a basis for the space of all 2×2 Hermitian matrices, thus the unitary matrix U can be represented as a linear combination of the Pauli matrices. Let

$$U = w_1 I + w_2\sigma_x + iw_3\sigma_y + w_4\sigma_z,$$

   since U is unitary, we must have $\sum_{i=1}^{4} w_i^2 = 1$, we consider only real coefficients. To calculate the winning probability of Eve, let us first discuss the effects of the Pauli operators on the decoy qubits.

   I is the identity operator, so it does not change the state of any qubit. Hence if *Eve* applies I on a decoy state, then after measurement Bob gets the correct result with probability $p_1 = 1$.

$$\sigma_x\left|0\right\rangle = \left|1\right\rangle,\ \sigma_x\left|1\right\rangle = \left|0\right\rangle,\ \sigma_x\left|+\right\rangle = \left|+\right\rangle,\ \sigma_x\left|-\right\rangle = -\left|-\right\rangle, \tag{4.11}$$

i.e., if *Eve* applies σ_x on a decoy state, then after measurement Bob gets the correct result with probability $p_2 = 1/2$, as σ_x changes the state of a decoy qubit $|d\rangle$ only if $|d\rangle \in \{|0\rangle, |1\rangle\}$.

Similarly,

$$i\sigma_y |0\rangle = -|1\rangle,\ i\sigma_y |1\rangle = |0\rangle,\ i\sigma_y |+\rangle = |-\rangle,\ i\sigma_y |-\rangle = -|+\rangle, \tag{4.12}$$

and

$$\sigma_z |0\rangle = |0\rangle,\ \sigma_z |1\rangle = -|1\rangle,\ \sigma_z |+\rangle = |-\rangle,\ \sigma_z |-\rangle = |+\rangle, \tag{4.13}$$

i.e., if *Eve* applies $i\sigma_y$ (or σ_z) on a decoy state, then after measurement Bob gets the correct result with probability $p_3 = 0$ (or $p_4 = 1/2$). Thus when *Eve* applies U on the decoy qubits, then the winning probability of *Eve* is

$$p' = \sum_{i=1}^{4} p_i w_i^2 < 1 \text{ as } U \neq I.$$

Now *Eve* chooses I and U with probability $1/2$ and thus the probability that Bob gets the correct result is $p'' = (1 + p')/2$. Hence in the security check process Alice and Bob find this eavesdropping with probability $1 - p''^m > 0$, where m is the number of decoy states. Moreover, this attack can also be found when they publicly compare the random check bits to check the integrity of the message.

5. **Man-in-the-middle attack:** When *Eve* follows this attack strategy, she intercepts the sequence Q_A^5 from the quantum channel and keeps this. She prepares another set Q_E of single qubit states and sends Q_E to Bob instead of Q_A^5. Since *Eve* does not know the position and exact states of the decoy qubits, she prepares all the single qubits in $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$ bases to reduce the detection probability in the security check process. Let the i-th decoy photon be $D_{A,i}$, which is the j-th qubit of the sequence Q_A^5, prepared in basis $\mathcal{B}$. Also let the j-th qubit of Q_E be $D'_{A,i}$ prepared in basis $\mathcal{B}'$, where $\mathcal{B}$ and $\mathcal{B}'$ are $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$. In the security check process when Alice

announces the preparation basis of $D_{A,i}$, then Bob measures $D'_{A,i}$ in basis $\mathcal{B}$ and gets $D''_{A,i}$. We now calculate the probability that $D''_{A,i} = D_{A,i}$.

- If $\mathcal{B} = \mathcal{B}'$ and $D_{A,i} = D'_{A,i}$, then $D''_{A,i} = D_{A,i}$ with probability 1.
- If $\mathcal{B} = \mathcal{B}'$ and $D_{A,i} \neq D'_{A,i}$, then $D''_{A,i} = D_{A,i}$ with probability 0.
- If $\mathcal{B} \neq \mathcal{B}'$, then $D''_{A,i} = D_{A,i}$ with probability 1/2.

Thus for each decoy qubit, the winning probability of *Eve* is

$$\begin{aligned}
&\Pr(D''_{A,i} = D_{A,i}) \\
&= \Pr(D''_{A,i} = D_{A,i} |\ \mathcal{B} = \mathcal{B}') \Pr(\mathcal{B} = \mathcal{B}') + \Pr(D''_{A,i} = D_{A,i} |\ \mathcal{B} \neq \mathcal{B}') \Pr(\mathcal{B} \neq \mathcal{B}') \\
&= \frac{1}{2}[\Pr(D''_{A,i} = D_{A,i} |\ \mathcal{B} = \mathcal{B}') + \Pr(D''_{A,i} = D_{A,i} |\ \mathcal{B} \neq \mathcal{B}')] \\
&= \frac{1}{2}[\Pr(D''_{A,i} = D_{A,i} |\ \mathcal{B} = \mathcal{B}',\ D_{A,i} = D'_{A,i}) \Pr(D_{A,i} = D'_{A,i}) + \\
&\qquad \Pr(D''_{A,i} = D_{A,i} |\ \mathcal{B} = \mathcal{B}',\ D_{A,i} \neq D'_{A,i}) \Pr(D_{A,i} \neq D'_{A,i}) + 1/2] \\
&= \frac{1}{2}\left[1 \times \frac{1}{2} + 0 \times \frac{1}{2} + \frac{1}{2}\right] = \frac{1}{2}.
\end{aligned}$$

Hence Alice and Bob can detect this eavesdropping and terminate the protocol with probability $1 - 2^{-m}$, where m is the number of decoy states. Furthermore, since *Eve* has no idea about the value of the parameter θ and the exact position of the qubits corresponding to the secret message M, so without the classical information from Alice, *Eve* can not get any useful information by measuring the qubits of Q_A^5 in some random basis.

6. **Information leakage attack:** It refers to the information about the secret message obtained by analyzing the classical channels by Eve. In other words, it is a measure of the information which *Eve* can get from the classical channel. Since in the present protocol, no measurement outcome corresponding to the secret bits is discussed by the classical channel, therefore *Eve* can not get any secret information from the communications in the classical channel.

7. **Trojan horse attack:** In the present protocol, only Alice prepares all the qubits required for secure communication, and then she sends these qubits to Bob at once. Therefore this

protocol is a one-way quantum communication protocol and hence Eve can not adopt the Trojan horse attack strategy to get any information about M.

We have shown that our proposed protocol is secure against all the above-discussed attacks as in each case the legitimate parties can detect the presence of Eve with non-negligible probability.

In the following section, we study the performance of this protocol in a realistic noisy quantum computer and illustrate results from IBM Quantum Computer.

4.3 Implementation in a noisy quantum device

The operations in our proposed protocol can be broadly represented as $U_B U_{Channel} U_A$ where U_A and U_B are the operations at the two ends (Alice and Bob respectively), and $U_{Channel}$ captures the action of the channel. Since Bob should receive the exact bit sent by Alice, if $|q\rangle$ is the qubit sent by Alice, we expect that in an ideal (noiseless and absence of eavesdropper) scenario

$$U_B U_{Channel} U_A |q\rangle = |q\rangle . \tag{4.14}$$

Now in an ideal scenario our protocol requires $U_B = U_A^{-1}$. If $U_{channel} \propto I$, then this requirement suffices. Without loss of generality, we consider $U_{Channel} = nI$, where $n \in \mathbb{Z}^+$. The scalar n also captures the finite time duration of the channel.

In reality, the channel is usually noisy and is no longer $\propto I$. If p_{error} is the probability of error, then the noisy channel can be represented as

$$U_{Channel}^{noisy} = (1 - p_{error})nI + p_{error} \sum_{i=1}^{n} I_{e_i}, \tag{4.15}$$

where I_{e_i} is some noisy version of the i^{th} identity gate. Note that I_{e_i} may not be equal to I_{e_j} for $i \neq j$, and it is possible that for some i, $I_{e_i} = I$, i.e., some of the n identity gates may be noise-free as well.

In such a scenario, the ideal operation of Bob should be $U_B = (U_{Channel}^{noisy})^{-1} U_A^{-1}$. However, since the action of the noise is unknown, it is not possible for Bob to apply this required operation in a realistic scenario. Furthermore, our protocol requires the preparation of U_θ gate

for $\theta \in \Theta$. In near-term devices, which are noisy, this technique can be a victim of calibration error, i.e., the applied operation maybe $U_{(\theta+\delta\theta)}$ for some small $\delta\theta \in \mathbb{R}$.

Let us assume that the density matrix of the original state to be transmitted is $|q\rangle \langle q|$, $q \in \{0, 1\}$. Let U_A and U_B be the actual operations of Alice and Bob respectively, where $U_B = U_A^{-1}$. However, due to noise, the operators U_A and U_B may change to U'_A and U'_B with probabilities p_A and p_B respectively. Therefore, the density matrix of the transmitted qubit is

$$\begin{aligned}(1-p_A)(1-p_B)U_B \cdot U_A |q\rangle \langle q| U_A \cdot U_B + p_A(1-p_B)U_B \cdot U'_A |q\rangle \langle q| U'^{\dagger}_A \cdot U^{\dagger}_B \\ +(1-p_A)p_B U'_B \cdot U_A |q\rangle \langle q| U^{\dagger}_A \cdot U'^{\dagger}_B + p_A p_B U'_B \cdot U'_A |q\rangle \langle q| U'^{\dagger}_A \cdot U'^{\dagger}_B\end{aligned}$$

Now, both U_A and U_B are single qubit gates, and can be implemented using a single U_3 gate in IBM Quantum devices (as discussed in detail in subsections henceforth). The probability of error of a single qubit gate in IBM Quantum devices is $\mathcal{O}(10^{-2})$. Therefore, from the above form, the probability of correction transmission is ~ 0.98. Furthermore, even when a qubit is affected by noise due to incorrect gate operations, post measurement, Bob will receive either q or $q \oplus 1$ as the measurement outcome. Therefore, it doesn't hamper the protocol if Bob received the correct outcome q even when the gate operations may have incorporated some errors on the system. Therefore, the probability of correct transmission post gate error only is greater than 98%. However, gate error is not the only error acting on the qubits. Other errors, such as relaxation, measurement etc. also affect the outcome. So, in real scenario, we expect to have a lower success probability (as shown in later subsections).

Here, we execute this protocol on the IBM Quantum Computer (Armonk device). We assume different lengths of the quantum channel (i.e., various values of the scalar n). As discussed before, noise in this device deviates the realization of the quantum channel from $U_{Channel}$ to $U^{noisy}_{Channel}$. We execute this protocol for different values of θ as well and show that the protocol is robust against various sources of errors and the integrity of the protocol can be guaranteed with minimum overhead in a noisy scenario as long as the time duration of the ideal channel (i.e., the value of n) is below a certain threshold.

4.3.1 Equivalence with Bit Flip Channel

Prior to further discussion on errors, we want to mention explicitly a property of this QSDC protocol. Unlike general error correction scheme, in this protocol, it is not of urgency to preserve the exact state that is being sent from Alice to Bob. The ultimate goal is to ensure that Bob receives the exact bit that Alice has sent him with high probability. In other words, suppose Alice wants to send a qubit $|q\rangle$ to Bob corresponding to a classical bit q. However, in a realistic scenario, if the noisy operations of Alice, Bob and the channel are U'_A, U'_B and $U'_{channel}$ respectively, then instead of the required $U_B U_{Channel} U_A |q\rangle$, we obtain $U'_B U'_{Channel} U'_A |q\rangle$. We do not care how the transmitted state $|q\rangle$ is being tampered with by the errors as long as $\langle q| U'_B U'_{Channel} U'_A |q\rangle > 1 - \epsilon$ for some small $\epsilon > 0$.

Furthermore, let $|q\rangle$ be the original qubit transmitted by Alice, whereas Bob received $|q'\rangle$ which may not be the same as the original transmitted message. However, since $q \in \{0, 1\}$, when Bob measures $|q'\rangle$ in the $\{|0\rangle, |1\rangle\}$ basis, he either receives q or $q \oplus 1$. Therefore, although the underlying channel may incorporate any error to the transmitted qubit, it is eventually equivalent to a single bit flip. Therefore, the overhead required for the error induced by the channel is the overhead to correct bit-flip errors.

4.3.2 Simulation of the protocol in IBM quantum device

In this subsection, we compute our protocol in the IBM Quantum Computer. However, for this computation, we have ignored the authentication portion. Rather we have only computed the communication portion, i.e., for each message qubit $|q\rangle$, we have computed the operation $U_B U_{Channel} U_A |q\rangle$, and shown the action of noise on it. The effect of noise can be mitigated using error correction. We aim to use the minimum overhead for error correction, which we discuss in the following subsection, followed by the computation results henceforth.

Overhead for error correction

To account for the imperfection of the channel, it is necessary to introduce error correction. However, for this protocol, we intend to introduce the minimum possible resource for error correction. Classically, a 3-bit repetition code is sufficient to correct a single bit flip error. The

repetition code is, in general, not extendable to the quantum domain, since (i) errors on qubits are not simple bit flips [275], and (ii) No Cloning Theorem prohibits cloning of any arbitrary quantum state [33]. However, we have already argued that the effective error on this protocol is indeed a simple bit flip. Furthermore, the qubits transmitted by Alice are either $|0\rangle$ or $|1\rangle$. Therefore, No Cloning Theorem does not restrict the use of repetition code in this scenario. The use of a distance 3 repetition code ensures that to send N qubits through a noisy channel, a total of $3N$ qubits are sufficient for error-free transmission as long as the error probability is below a particular threshold, which we now elaborate.

A distance-3 repetition code fails when at least two errors occur on the codeword. Therefore, if p_{err} is the probability of error, then we should have

$$\binom{3}{2} p_{err}^2 < p_{err},$$

which yields $p_{err} < \frac{1}{3}$.

In the following subsection, we show empirically that the action of noise is similarly for any angle θ selected for this protocol. However, the time duration of the channel restricts the distance of the code. We have represented a noisy quantum channel as $U_{Channel}^{noisy}$. We show that for the usual time duration of an identity gate in the IBMQ device, a distance 3 repetition code can protect this protocol from error as long as $n < 350$. For higher values of n, the noise in the device will lead to more than one error on expectation, and larger distance codes will be required for error-free transmission.

Results of simulation in IBM Quantum Device

In our protocol, once a θ is decided upon, each bit is encoded independently and sequentially by Alice. Similarly each qubit is decoded and measured independently and sequentially by Bob. Therefore, a single qubit quantum computer is sufficient to perform these operations. We have computed the encoding by Alice and the decoding by Bob, followed by measurement in the IBMQ Armonk device [273] for various values of θ and various lengths (n) of the channel. IBMQ Armonk is a single qubit quantum computer with specifications shown in Fig. 4-2.

Computation on this device exposes our protocol to various device noise. Calibration error signifies the inaccuracy in the gate operation (denoted as H error rate in Fig. 4-2). Readout

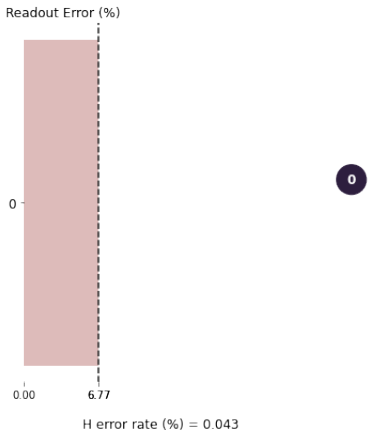


Figure 4-2: Specifications of the IBMQ Armonk quantum device as provided by IBM

error, on the other hand, encapsulates the inaccuracy in measurement. If the measurement device is noisy, then it is possible that although the original output was m, due to measurement inaccuracy, it was noted down as $m \oplus 1$. Readout error is one of the most dominating sources of errors in current quantum devices (as shown in Fig. 4-2 where the readout error rate is 6.7% as compared to calibration error rate of 0.04%). We shall discuss about the channel noise (particularly the T_1 error) later.

Qiskit [272] has its own gate sets which are computed on their device. Such a gate is the $U3(\theta, \phi, \lambda)$ gate whose matrix form is

$$U3(\theta, \phi, \lambda) = \begin{pmatrix} cos(\frac{\theta}{2}) & e^{-i\lambda}sin(\frac{\theta}{2}) \\ e^{i\phi}sin(\frac{\theta}{2}) & e^{i(\phi+\lambda)}cos(\frac{\theta}{2}) \end{pmatrix},$$

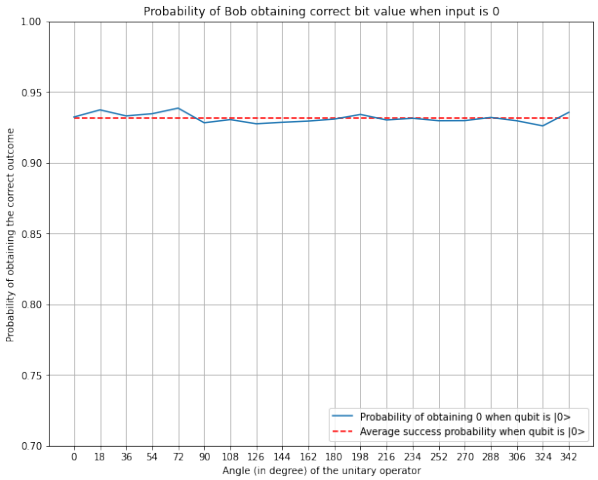
where $0 \leq \theta, \phi, \lambda < 2\pi$ are the parameters. Different quantum gates can be generated by varying this parameter. Note that our required operation $U_\theta = U3(2\theta, 0, 0)$.

Effect of choice of angle

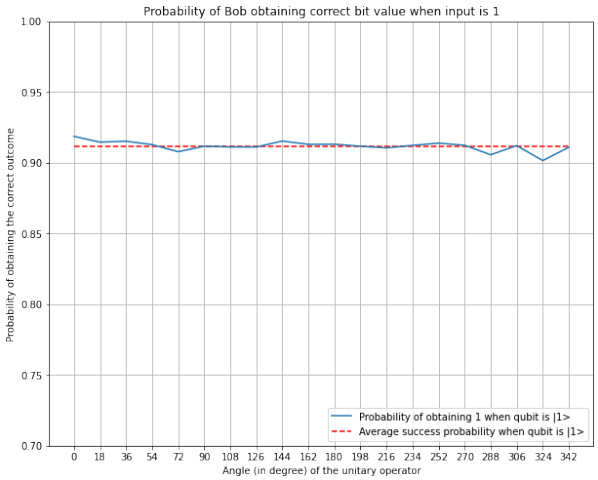
First, we show the effect of the angle θ on the performance of the protocol in a realistic noisy scenario. For this portion, we do not consider the presence of channel. We have executed our protocol on the quantum device of Fig. 4-2 for 20 equally spaced values of θ ranging from 0° to 360°. We show the circuit for one such θ in Fig. 4-3. This figure shows the exact

circuit that is being executed on the IBMQ Armonk device. The two gates are respectively the U_θ applied by Alice, and the U_θ^{-1} applied by Bob. Qiskit tends to optimize their circuit to reduce the execution overhead. Since we are applying two inverse operations sequentially, the optimization module of qiskit would lead to an identity operation. Therefore, we have forcefully introduced the barrier between the two gates which ensures that both the operations are executed as they are.

Figure 4-3: Circuit diagram of the QSDC protocol executed on the IBMQ Armonk device



(a) Performance when Alice sends 0



(b) Performance when Alice sends 1

Figure 4-4: Action of noise in real quantum device

We have executed the protocol for the two scenarios - when the original bit is 0 or 1. Fig 4-4a and Fig. 4-4b shows the action of noise in real quantum device on the performance of the protocol. We see that Bob no longer obtains the original bit sent by Alice with certainty. However, it is evident from the figures that the choice of angle does not have any significant effect on the performance of the noisy protocol. For each value of the angle, we have taken an average over 20 random instances. In Table 4.2 we show how the standard deviation of the average values from the mean tends to 0 as the number of trials is increased from 5-20. The

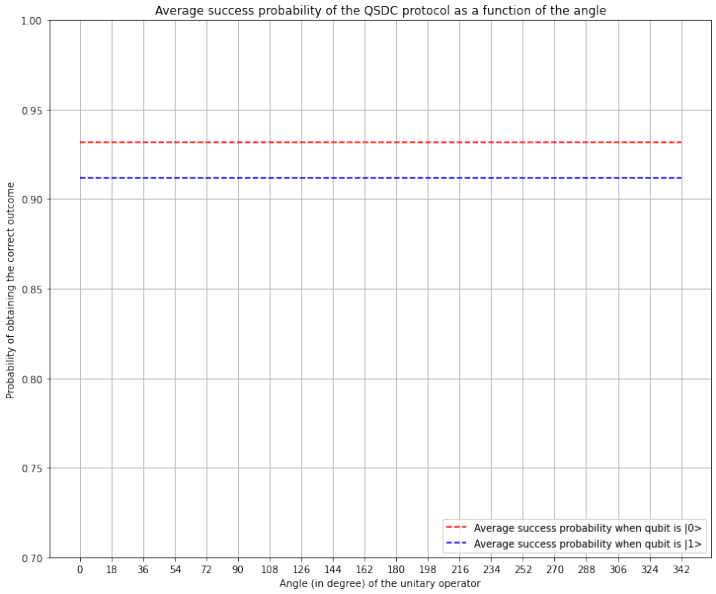


Figure 4-5: Average success probability for different bit values

mean more or less remains same. Therefore, it is evident that if the averaging is done over even larger trials, whatever little jaggedness is still observable in 20 trials, will be removed as well. Furthermore, we see that the average success probability for $|0\rangle$ and $|1\rangle$ are ~ 0.93 and ~ 0.91 respectively. We argued earlier that the presence of gate error alone leads to a success probability of ~ 0.98. These results from real IBMQ hardware reconfirms it, since these values are lower than the theoretical value obtained using only gate error (here other errors are present as well), but not significantly apart.

Table 4.2: Variation in Standard Deviation (SD) with the number of trials

Number of trials	**Transmitted bit 0**		**Transmitted bit 1**	
	Mean	**SD**	**Mean**	**SD**
5	0.9343	0.00539	0.9116	0.00498
10	0.9354	0.00444	0.9122	0.00477
15	0.9345	0.00358	0.9123	0.00353
20	0.9337	0.00317	0.9118	0.00308

We note from Fig. 4-5 that the average performance is better when the qubit is $|0\rangle$ than when the qubit is $|1\rangle$. This can be explained by the T_1 error. The natural tendency of any

quantum state is to retain its lowest energy state ($|0\rangle$), or ground state. When a qubit is elevated to its excited state ($|1\rangle$), it has a natural tendency to release the excess energy to return to its ground state. This noise model [6] is parameterized by T_1. In general, the probability that a qubit, prepared in the state $|1\rangle$, remains in that state after a certain time t is given by

$$\text{Prob}(|1\rangle) = exp(-\tfrac{t}{T_1}),$$

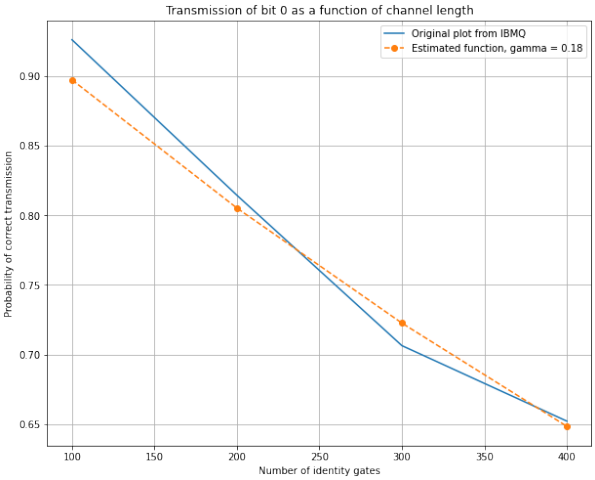
The qubits which are prepared in the state $|1\rangle$ are exposed to this error along with the other device noise. Therefore, naturally, the average probability of observing $|1\rangle$ is lower than that of $|0\rangle$. However, we note that for no value of θ, the probability of correct transmission goes below 0.9.

Effect of the length of the channel

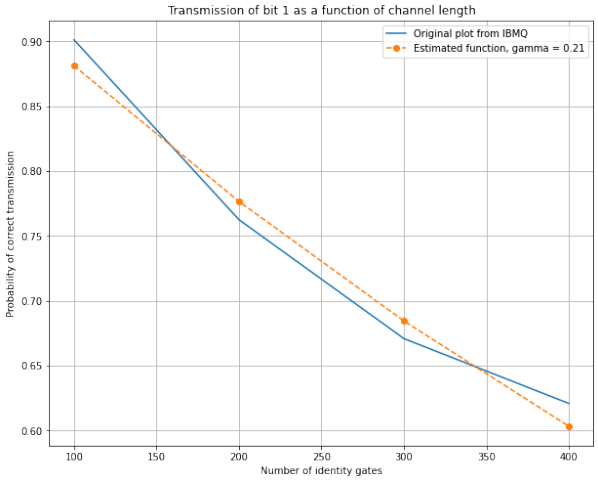
Now, we incorporate the presence of a quantum channel. A quantum channel is not instantaneous. In order this simulate the finite time duration, we execute the circuit of Fig. 4-3, with $100 \leq n \leq 400$ identity gates in between the two U_3 operators. Each identity gate in the IBMQ Armonk device requires 142 ns to execute, and the error probability of each identity gate is $p_{error} = 0.001$. The probability that the channel remains error-free is $(1 - p_{error})^n$. However, when we execute this circuit, it is subjected to other sources of errors apart from the channel noise only (e.g. calibration error, readout error). In order to account for these, we hypothesize that the probability of no error is

$$(1 - p_{error})^{\gamma n}, \tag{4.16}$$

for some scalar γ. In Fig. 4-6a and 4-6b, we show the probability of correct transmission as a function of the length of the channel. We estimate the value of γ in each case through curve fitting and observe $\gamma = 0.18$ for the transmission of bit 0, and $\gamma = 0.21$ for the transmission of bit 1. The estimated functions are plotted in Fig. 4-7 to show a comparison of the variation in probability for the bits 0 and 1. We see that, similar to Fig. 4-5, the transmission of 1 is more prone to error than that of 0. This can be similarly explained as before via the T_1 error. This is, in fact, the reason for obtaining two different values of γ for the two bits.



(a) Performance variation with channel length when Alice sends 0



(b) Performance variation with channel length when Alice sends 1

Figure 4-6: Action of noise in real quantum device for different channel length

We have already argued that a distance 3 repetition code is applicable for correcting errors only when the probability of no error is $\geq \frac{2}{3} = 0.66$. We note from Fig. 4-7 that when the number of identity gates is ~ 350, the estimated success probability of both 0 and 1 goes below the required threshold. Therefore, in order to use the minimum overhead of 3 qubit repetitions, it is necessary that the channel length is < 350 identity gates. Nevertheless, in case the channel length is greater, then higher distance repetition codes can be used for error-free transmission.

4.4 Discussion

In this chapter, we propose a QSDC protocol with user authentication using single qubits prepared on a randomly chosen arbitrary basis. In this protocol, before starting the communication process, Alice and Bob share their secret identities through a secure QKD to authenticate each other. In the proposed QSDC protocol, Alice, the message sender, prepares all the single qubits and sends them to the receiver Bob, i.e., this is a one-step one-way quantum communication protocol. After receiving the qubits, Bob only performs measurement and applies unitary operations to the received particles to get the secret message of Alice. Moreover, the present protocol does not use entanglement as a resource. We discuss the security of the protocol and show that our proposed protocol defeats all the familiar attack strategy

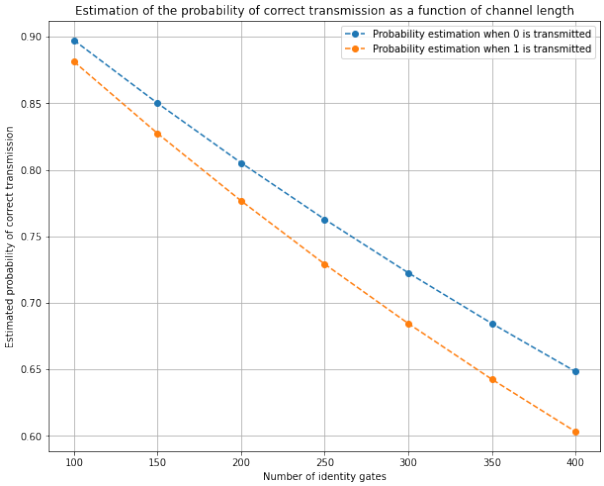


Figure 4-7: Estimated functions for success probability for varying channel length

and the eavesdropper could not get on any information about the secret message. The curse of executing such protocols in near-term devices is that they become susceptible to noise in the device. We have computed the protocol in the IBMQ Armonk device which is a single qubit device, and therefore perfectly captures the sequential structure of the protocol. We find that our protocol is quite robust to error, and a simple distance 3 repetition code is sufficient for reliable transmission as long as the length of the quantum channel is less than 350 identity gates. Therefore, in order to transmit N qubits in such a noisy scenario, $3N$ qubits are sufficient, and it does not require any complex gate operations for preparing logical qubits as well.

Chapter 5

Analysis and Design of MDI-QSDC

Recently, Niu et al. [2] proposed a measurement-device-independent (MDI) QSDC protocol using Einstein-Podolsky-Rosen (EPR) pairs. Then they generalized this one-way communication to a bidirectional one and proposed an MDI-QD protocol. In their protocols, the two legitimate parties prepare two sets of EPR pairs in their place, and send the partner qubits of their EPR pairs to an untrusted third party, since the condition for being an MDI protocol is that, all the measurements during the communication process should be performed by an untrusted third party (who may be an eavesdropper). Here we analyze these protocols and point out that the secret messages are not transmitted securely for both the protocols. We show that fifty percent of the information about the secret message bits is leaked out in both the protocols. In other words, in the perspective of information theory and cryptography, these protocols are not secure. This type of security loophole of information leakage in various QSDC and QD protocols are discussed in [226, 234, 90, 88, 276, 237, 277, 146]. We also propose modifications of these protocols to improve their security. This work presented in the paper [137].

5.1 Security loophole of the MDI-QSDC protocol [2]

In this section, we explicitly analyze the MDI-QSDC protocol of [2] discussed in Section 2.3.2. After Charlie has done the first set of Bell measurements of the qubits pairs of S_{A_2} and S_{B_2} in Step 3, the qubits pairs of S_{A_1} and S_{B_1} become entangled due to entanglement swapping (Step 4a). Now from Equation (2.5), we can see that, if the Bell measurement results of the

qubits pairs of S_{A_2} and S_{B_2} are $|\Phi^+\rangle_{A_2B_2}$ or $|\Phi^-\rangle_{A_2B_2}$, then also the states of the qubit pairs of S_{A_1} and S_{B_1} are $|\Phi^+\rangle_{A_1B_1}$ or $|\Phi^-\rangle_{A_1B_1}$. Similarly, the state of the qubit pair $(A_2, B_2) = |\Psi^\pm\rangle_{A_2B_2}$ implies the state of the qubit pair $(A_1, B_1) = |\Psi^\pm\rangle_{A_1B_1}$ or $|\Psi^\mp\rangle_{A_1B_1}$.

After security checking, Alice and Bob discard the qubits, which are not entangled, from their sequences S_{A_1} and S_{B_1}, and make the new sequences M_A and M_B respectively. So, from the Bell measurement results of the qubit pairs (A_2, B_2), Charlie knows the states of the qubit pairs (A_1, B_1), are either $|\Phi^\pm\rangle_{A_1B_1}$ or $|\Psi^\pm\rangle_{A_1B_1}$. That is, for $1 \leq i \leq n - \delta$, Charlie exactly knows that the qubit pairs (M_{Ai}, M_{Bi}) are in set $\Phi = \{|\Phi^+\rangle, |\Phi^-\rangle\}$ or in set $\Psi = \{|\Psi^+\rangle, |\Psi^-\rangle\}$.

Now Alice applies σ_z on the qubits of M_A, whose corresponding initial states were $|\Psi^+\rangle$. It is easy to check that, if Alice applies σ_z on M_{A_i} for some i, then the state of the qubit pair (M_{Ai}, M_{Bi}) changes from either $|\Phi^\pm\rangle$ to $|\Phi^\mp\rangle$ or $|\Psi^\pm\rangle$ to $|\Psi^\mp\rangle$. Thus Charlie's knowledge about the state of (M_{Ai}, M_{Bi}) remains same.

Then Alice encodes her message on the qubits of M_A by using the unitary operations I, σ_x, $i\sigma_y$ and σ_z corresponding the message bits 00, 01, 10, and 11 respectively. That is, the unitary operators I and σ_z are used to encode the message bits bb, and the unitary operators σ_x and $i\sigma_y$ are used to encode the message bits $b\bar{b}$, where $b \in \{0, 1\}$ and $\bar{b}$ = bit complement of b. Bob also randomly applies I or σ_z on the qubits of M_B. They send M_A and M_B to Charlie, who measures each pair of qubits (M_{Ai}, M_{Bi}) in Bell basis, and announces the results. All the different cases are given in Table 5.1.

We now show that, in the MDI-QSDC protocol [2], the untrusted third party Charlie (or any eavesdropper) can get partial information about the secret without any active attack. For this, we need to discuss the effects of the encoding rules in this MDI-QSDC protocol. Without loss of generality, suppose the joint state of M_{Ai}, M_{Bi} before encoding is $|\Phi^+\rangle$, then Charlie knows that the joint state is in the set Φ.

After Charlie measures (M_{Ai}, M_{Bi}) in Bell basis, if the measurement result is in the set Φ, then from Table 5.1, Charlie concludes that, the secret information is either 00 or 11. Again if the measurement result is in the set Ψ, then from Table 5.1, Charlie concludes that, the secret information is either 01 or 10. Similarly, for the other cases, Charlie exactly knows that the secret information is bb or $b\bar{b}$. For both the cases, Charlie can get the exact secret information with probability 1/2, thus the Shannon entropy, which measures the amount of uncertainty, is

Table 5.1: Different cases of MDI-QSDC [2].

State of (M_{A_i}, M_{B_i}) before encoding	**Message bits of Alice**	**Alice's unitary operation on M_{A_i}**	**Bob's unitary operation on M_{B_i}**	**State of (M_{A_i}, M_{B_i}) after encoding**
$\|\Phi^+\rangle$	00	I	I	$\|\Phi^+\rangle$
			σ_z	$\|\Phi^-\rangle$
	01	σ_x	I	$\|\Psi^+\rangle$
			σ_z	$\|\Psi^-\rangle$
	10	$i\sigma_y$	I	$\|\Psi^-\rangle$
			σ_z	$\|\Psi^+\rangle$
	11	σ_z	I	$\|\Phi^-\rangle$
			σ_z	$\|\Phi^+\rangle$
$\|\Phi^-\rangle$	00	I	I	$\|\Phi^-\rangle$
			σ_z	$\|\Phi^+\rangle$
	01	σ_x	I	$\|\Psi^-\rangle$
			σ_z	$\|\Psi^+\rangle$
	10	$i\sigma_y$	I	$\|\Psi^+\rangle$
			σ_z	$\|\Psi^-\rangle$
	11	σ_z	I	$\|\Phi^+\rangle$
			σ_z	$\|\Phi^-\rangle$
$\|\Psi^+\rangle$	00	I	I	$\|\Psi^+\rangle$
			σ_z	$\|\Psi^-\rangle$
	01	σ_x	I	$\|\Phi^+\rangle$
			σ_z	$\|\Phi^-\rangle$
	10	$i\sigma_y$	I	$\|\Phi^-\rangle$
			σ_z	$\|\Phi^+\rangle$
	11	σ_z	I	$\|\Psi^-\rangle$
			σ_z	$\|\Psi^+\rangle$
$\|\Psi^-\rangle$	00	I	I	$\|\Psi^-\rangle$
			σ_z	$\|\Psi^+\rangle$
	01	σ_x	I	$\|\Phi^-\rangle$
			σ_z	$\|\Phi^+\rangle$
	10	$i\sigma_y$	I	$\|\Phi^+\rangle$
			σ_z	$\|\Phi^-\rangle$
	11	σ_z	I	$\|\Psi^+\rangle$
			σ_z	$\|\Psi^-\rangle$

equal to $-\sum_{j=1}^{2} \frac{1}{2} \log \frac{1}{2} = 1$ bit. That means, only one bit among two bits of secret information is unknown to Charlie. One may note that, from the viewpoint of information theory, this is equivalent to the event that, among two bits of secret information, Charlie knows the exact value of one bit and does not have any knowledge about the other bit. Thus we can say that, here in this MDI-QSDC protocol, only fifty percent of the secret message communicated securely.

By the same argument, we can say that the MDI-QD protocol proposed in [2] is also not secure against information leakage, and in this protocol, only fifty percent of the secret messages communicated securely.

Now, we find the root of this information leakage problem in these protocols. Let for some i, $M_{A_i} \in M_A$ and $M_{B_i} \in M_B$, and after Alice and Bob apply their unitary operators, the states M_{A_i} and M_{B_i} become N_{A_i} and N_{B_i} respectively. If the joint state $(M_{A_i}, M_{B_i}) \in \Phi$ or Ψ, then after applying I or σ_z on M_{A_i} (or M_{B_i}), the joint state (N_{A_i}, M_{B_i}) (or (M_{A_i}, N_{B_i})) remains in the same set Φ or Ψ respectively. In other words, both I and σ_z are applied on M_{A_i} or M_{B_i} or both M_{A_i} and M_{B_i}, map the set Φ to Φ, and Ψ to Ψ. That is, for both the mappings, the domain and the range sets are same, and if both the joint states (M_{A_i}, M_{B_i}) and (N_{A_i}, N_{B_i}) belong to the same subset of the Bell states Φ or Ψ, then Charlie concludes that the message bits are bb. Otherwise, when (M_{A_i}, M_{B_i}) and (N_{A_i}, N_{B_i}) belong to two different subsets Φ or Ψ, then Charlie concludes that the message bits are $b\bar{b}$ (i.e., Alice applies σ_x or $i\sigma_y$ on M_{A_i}). So, the main problem in this encoding rule is, Bob's random unitary operations can not lower down the information of Charlie about the secret message. In the next section, we propose a remedy to overcome this security flaw.

5.2 Proposed modification of MDI-QSDC protocol

In this section, we modify the MDI-QSDC protocol, to make it secure against information leakage. To resolve the problem discussed in Section 5.1, Bob needs to apply some random unitary operators on M_{B_i} such that the the union of the range sets, of his unitary operators, becomes the whole set of Bell states, i.e., for each $(M_{A_i}, M_{B_i}) \in \Phi$ or Ψ and $(N_{A_i}, N_{B_i}) \in \Phi \cup \Psi$, there exist all the four possibilities of Alice's two bits message $b_1 b_2$ $(b_1, b_2 \in \{0, 1\})$.

The modified protocol is almost same as the original one. In our modified MDI-QSDC protocol, Step 1 to Step 5 and Step 7 are same as the MDI-QSDC protocol discussed in Section 2.3.2. In Step 6, the encoding process of Alice is the same as the previous one, and Bob randomly applies σ_x and I on the qubits of M_B (instead of σ_z and I in the original one). All the different cases, of the states of the qubit pairs of M_A and M_B, before and after encoding are given in Table 5.2.

We will now show that this modified protocol is secure against information leakage. Again without loss of generality, suppose the joint state of M_{Ai}, M_{Bi} before encoding is $|\Phi^+\rangle$, then Charlie knows that the joint state is either $|\Phi^+\rangle$ or $|\Phi^-\rangle$. From Table 5.2, it is easy to check that, before encoding, if the joint state is $|\Phi^\pm\rangle$, then all the four Bell states can arise after encoding any two message bits b_1b_2. Thus Charlie's knowledge, about the joint state before encoding, does not help him to extract any information about the secret bits. Similarly for the other cases also Charlie can not get any secret information about the message bits.

We can also modify the MDI-QD protocol of [2], with a similar approach, i.e., the receiver applies the unitary I and σ_x randomly on his (her) state at the time of encoding.

5.2.1 Other Pauli operators to fix the issue

One can ask, what happen if Bob chooses any other pair of Pauli matrices as his random unitary operators. To check this, we consider two sets of linear transformations $\mathcal{F}_1 = \{I, \sigma_z\}$ and $\mathcal{F}_2 = \{\sigma_x, i\sigma_y\}$ (note that, every matrix is a linear transformation), where both the domain and range of these linear transformations are Φ and Ψ. Then, $f \in \mathcal{F}_1$ implies that f maps the set Φ to Φ and the set Ψ to Ψ (ignoring the global phase of the Bell states). Again, $f \in \mathcal{F}_2$ implies that f maps the set Φ to Ψ and the set Ψ to Φ. Let for any mapping f, $\mathcal{D}(f)$ and $\mathcal{R}(f)$ be the domain and range of f respectively. If Bob uses both his unitary operators from the same set $\mathcal{F}_1$ or $\mathcal{F}_2$ (i.e., Bob's unitary operator f_1, $f_2 \Longrightarrow \mathcal{D}(f_1) = \mathcal{D}(f_2) = \mathcal{D}$ (say) and $\mathcal{R}(f_1) = \mathcal{R}(f_2) = \mathcal{R}$ (say), where both $\mathcal{D}$ and $\mathcal{R}$ are either Φ or Ψ), then $(N_{A_i}, N_{B_i}) \in \mathcal{R} \Longrightarrow \ (N_{A_i}, M_{B_i}) \in \mathcal{D}$. As Charlie knows exactly the set Φ or Ψ in which the state (M_{A_i}, M_{B_i}) belongs, thus from the knowledge that $(N_{A_i}, M_{B_i}) \in \mathcal{D}$, Charlie gets the information that "both the bits of Alice's two bits message are equal or not".

Now let the two unitary operators of Bob be f_1 and f_2, where $f_1 \in \mathcal{F}_1$ and $f_2 \in \mathcal{F}_2$.

• When UTP measures the qubit pairs of (S_{A_2}, S_{B_2}), then the qubit pairs of (S_{A_1}, S_{B_1}) became entangled due to entanglement swapping.

Figure 5-1: Modified MDI-QSDC protocol

Table 5.2: Different cases of modified MDI-QSDC.

State of (M_{A_i}, M_{B_i}) before encoding	**Message bits of Alice**	**Alice's unitary operation on M_{A_i}**	**Bob's unitary operation on M_{B_i}**	**State of (M_{A_i}, M_{B_i}) after encoding**
$\|\Phi^+\rangle$	00	I	I	$\|\Phi^+\rangle$
			σ_x	$\|\Psi^+\rangle$
	01	σ_x	I	$\|\Psi^+\rangle$
			σ_x	$\|\Phi^+\rangle$
	10	$i\sigma_y$	I	$\|\Psi^-\rangle$
			σ_x	$\|\Phi^-\rangle$
	11	σ_z	I	$\|\Phi^-\rangle$
			σ_x	$\|\Psi^-\rangle$
$\|\Phi^-\rangle$	00	I	I	$\|\Phi^-\rangle$
			σ_x	$\|\Psi^-\rangle$
	01	σ_x	I	$\|\Psi^-\rangle$
			σ_x	$\|\Phi^-\rangle$
	10	$i\sigma_y$	I	$\|\Psi^+\rangle$
			σ_x	$\|\Phi^+\rangle$
	11	σ_z	I	$\|\Phi^+\rangle$
			σ_x	$\|\Psi^+\rangle$
$\|\Psi^+\rangle$	00	I	I	$\|\Psi^+\rangle$
			σ_x	$\|\Phi^+\rangle$
	01	σ_x	I	$\|\Phi^+\rangle$
			σ_x	$\|\Psi^+\rangle$
	10	$i\sigma_y$	I	$\|\Phi^-\rangle$
			σ_x	$\|\Psi^-\rangle$
	11	σ_z	I	$\|\Psi^-\rangle$
			σ_x	$\|\Phi^-\rangle$
$\|\Psi^-\rangle$	00	I	I	$\|\Psi^-\rangle$
			σ_x	$\|\Phi^-\rangle$
	01	σ_x	I	$\|\Phi^-\rangle$
			σ_x	$\|\Psi^-\rangle$
	10	$i\sigma_y$	I	$\|\Phi^+\rangle$
			σ_x	$\|\Psi^+\rangle$
	11	σ_z	I	$\|\Psi^+\rangle$
			σ_x	$\|\Phi^+\rangle$

Then $\mathcal{D}(f_1) = \mathcal{D}(f_2) = \mathcal{D}$ (say) implies $\mathcal{R}(f_1)$ and $\mathcal{R}(f_2)$ are disjoint. Since Φ and Ψ make a partition of the set of all the two qubits Bell states, thus $\mathcal{R}(f_1) \cup \mathcal{R}(f_2)$ contains all the Bell states. As Bob randomly chooses between f_1 and f_2, therefore from the exact state of (N_{A_i}, N_{B_i}), Charlie does not know the exact set of the state (N_{A_i}, M_{B_i}). For example, if Charlie knows $(M_{A_i}, M_{B_i}) \in \Phi$, then for Alice's message $b_1 b_2$, all the four Bell state can occur as the state of (N_{A_i}, N_{B_i}). So in this case, the protocol is secure against information leakage.

Hence the collection of all possible choices of Bob's random unitary operators pairs, from the set of Pauli matrices, is $\{(f_1, f_2) : f_1 \in \mathcal{F}_1 \text{ and } f_2 \in \mathcal{F}_2\}$, i.e., there are four options for Bob to choose his pair of unitary operators and they are: I and σ_x; I and $i\sigma_y$; σ_z and σ_x; σ_z and $i\sigma_y$. One can easily check that, if Bob uses any one pair from the above set as his random unitary operators, then both the protocols prevent the information leakage problem.

5.3 Discussion

In this chapter, we analyze Niu et al.'s MDI quantum communication protocols and observe some security issues in both the protocols. We show that these protocols are not secure against information leakage, and one bit among two bits of information is always leaked without any active attack. Then we propose a modification of these protocols, which are secure against such information leakage problem. We also characterize the set of Pauli operators, which can alternatively be used to bypass the security flaws.

Chapter 6

A New Approach of MDI-QSDC Design with User Authentication

In this chapter, we put forward an MDI-QSDC protocol with user identity authentication, where both the sender and the receiver first check the authenticity of the other party and then exchange the secret message. Then we extend this to an MDI quantum dialogue (QD) protocol, where both the parties can send their respective secret messages after verifying the identity of the other party. Along with this, we also report an MDI-DSQC protocol with user identity authentication. Theoretical analyses prove the security of our proposed protocols against common attacks.

6.1 Proposed MDI-QSDC protocol with user authentication

In this section, we propose our new MDI-QSDC protocol with user identity authentication process.

Suppose Alice has an n-bit secret message m, which she wants to send Bob through a quantum channel with the help of some untrusted third-party (UTP), who performs all the measurements during the protocol. Alice and Bob have their secret user identities Id_A and Id_B (each of $2k$ bits) respectively, which they have shared previously by using some secured

QKD. The protocol is as follows:

1. Alice chooses c check bits and inserts those bits in random positions of m. Let the new bit string be m' of length $n + c$. We assume this length to be even, i.e., $n + c = 2N$ for some integer N.

2. **Bob:**

   (a) Prepares $(N + k)$ EPR pairs randomly in $|\Phi^+\rangle$, $|\Phi^-\rangle$, $|\Psi^+\rangle$ and $|\Psi^-\rangle$ states. He separates the entangled qubit pairs into two particle sequences S_A and S_B each of length $(N+k)$, where S_A is formed by taking out one qubit from each pair, and the remaining partner qubits form S_B.

   (b) He also prepares k EPR pairs according to his identity Id_B. For $1 \leq i \leq k$, the i-th qubit pair I_i is prepared as one of $|\Phi^+\rangle$, $|\Phi^-\rangle$, $|\Psi^+\rangle$ and $|\Psi^-\rangle$, if the value of $Id_{B,(2i-1)}Id_{B,2i}$ is one of 00, 01, 10 and 11 respectively. He creates two sequences I_A and I_B of single photons, such that for $1 \leq i \leq k$, the i-th qubits of I_A and I_B are partners of each other in the i-th EPR pair I_i.

   (c) Bob chooses two sets D_A and D_B, each of d many decoy photons randomly prepared in Z-basis or X-basis. Then he randomly interleaves the qubits of $I_A(I_B)$ and $D_A(D_B)$ and $S_A(S_B)$ (maintaining the relative ordering of each set) to get a new sequence of single qubits $Q_A(Q_B)$ (i.e., $Q_P = S_P \cup I_P \cup D_P$, $P = A, B$).

   (d) Bob retains the Q_B-sequence and sends the Q_A-sequence to Alice through a quantum channel.

   (e) After Alice receives Q_A-sequence, Bob announces the positions of the qubits of I_A and D_A.

3. **Alice:**

   (a) She separates the qubits of S_A, I_A and D_A from Q_A. Then from the sequence S_A, she randomly chooses N qubits to encode the secret message and the remaining k qubits (say, the set C_A) are used to encode her secret identity Id_A. The encoding processes for m' and Id_A are the same. Alice encodes two bits of classical information into

one qubit by applying an unitary operator. To encode $00, 01, 10$ and 11, she applies the Pauli operators [6] I, σ_x, $i\sigma_y$ and σ_z respectively. After encoding the classical information, let S_A become S'_A.

(b) Alice randomly applies I, σ_x, $i\sigma_y$ and σ_z on the qubits of I_A and resulting in a new sequence I'_A. She randomly inserts the qubits of I'_A into random positions of S'_A and the new sequence be Q'_A.

(c) She randomly applies cover operations from $\{I, i\sigma_y, H, i\sigma_y H\}$ on the qubits of D_A, resulting in a new new sequence D^1_A.

(d) Alice sends D^1_A sequence to UTP to check the security of the channel from Bob to Alice.

4. After the UTP receives the sequence D^1_A, Bob announces the preparation bases of the qubits of D_A and Alice announces the corresponding cover operations which she applies on those qubits.

5. UTP measures the qubits of D^1_A in proper bases and announces the measurement result. Note that if the cover operation belongs to the set $\{H, i\sigma_y H\}$, then UTP changes the basis to measure the corresponding qubit. For example, let the i-th qubit of D_A be prepared in Z-basis and the i-th cover operation be $i\sigma_y H$, then UTP measures the ith qubit of D^1_A in X-basis. From the measurement results, Alice and Bob calculate the error in the channel from Bob to Alice, and decide to continue or abort the protocol.

6. Alice inserts a new set of d' decoy photons D'_A into random positions of Q'_A, resulting in a new sequence Q''_A. Alice sends Q''_A-sequence to UTP.

7. Alice announces the positions and the preparation bases of the decoy qubits of D'_A. UTP measures the decoy qubits and publishes the measurement results, and from that Alice calculates the error in the quantum channel between Alice and UTP. If the estimated error is greater than some threshold value, then they terminate the protocol and otherwise go to the next step.

8. Bob sends the sequence Q_B to UTP and when all the qubits of Q_B are reached to UTP, Bob announces the positions and the preparation bases of the decoy qubits of D_B. UTP

measures those qubits in proper bases and discloses the measurement results, and Bob calculates the error in the quantum channel between Bob and UTP. If the estimated error is greater than some threshold value, then they terminate the protocol and otherwise go to the next step.

9. **Authentication process:**

   (a) Alice announces the positions of the qubits of I'_A and Bob announces the positions of the qubits of I_B. For $1 \leq i \leq k$, UTP measures the i-th qubit pair $(I'_{A,i}, I_{b,i})$ in Bell basis and announces the result. As Alice knows Id_B, she knows the exact state of each I_i, which is the joint state $I_{A,i}I_{B,i}$. Since she randomly applies Pauli operators on $I_{A,i}$, the joint state changes to $I'_{A,i}I_{B,i}$. Alice compares the measurement result with $I'_{A,i}I_{B,i}$ to confirm Bob's identity. If she finds a non-negligible error then she aborts the protocol.

   (b) Alice announces the positions of the qubits of C_A corresponding to her identity Id_A and UTP measures those qubits with their partner qubits from S_B (say, the set C_B) in Bell bases and announces the measurement result. Since Bob knows Id_A, he compares the measurement results with Id_A and checks if Alice is a legitimate party or not. If he finds a non-negligible error, he aborts the protocol.

10. The UTP measures each qubit pair from (S'_A, S_B) in Bell basis and announces the measurement result. From the knowledge of (S_A, S_B) and (S'_A, S_B), Bob decodes the classical bit string m' using Table (6.1).

11. Alice and Bob publicly compare the random check bits to check the integrity of the messages. If they find an acceptable error rate then Bob gets the secret message m and the communication process is completed.

Figure 6-1 represents the block diagram of the proposed MDI-QSDC with user authentication protocol. We also present it in the form of an algorithm in figure 6-2, where we use the following notations.

- $X \rightarrow Y$: X changes to Y.

Table 6.1: Encoding and decoding rules of our proposed MDI-QSDC.

Bob prepares (S_A, S_B)	**Secret message bits of Alice**	**Alice's unitary** S_A **to** S'_A	**Final joint state** (S'_A, S_B)	**Decoded message bits**
$\|\Phi^+\rangle$	00	I	$\|\Phi^+\rangle$	00
	01	σ_x	$\|\Psi^+\rangle$	01
	10	$i\sigma_y$	$\|\Psi^-\rangle$	10
	11	σ_z	$\|\Phi^-\rangle$	11
$\|\Phi^-\rangle$	00	I	$\|\Phi^-\rangle$	00
	01	σ_x	$\|\Psi^-\rangle$	01
	10	$i\sigma_y$	$\|\Psi^+\rangle$	10
	11	σ_z	$\|\Phi^+\rangle$	11
$\|\Psi^+\rangle$	00	I	$\|\Psi^+\rangle$	00
	01	σ_x	$\|\Phi^+\rangle$	01
	10	$i\sigma_y$	$\|\Phi^-\rangle$	10
	11	σ_z	$\|\Psi^-\rangle$	11
$\|\Psi^-\rangle$	00	I	$\|\Psi^-\rangle$	00
	01	σ_x	$\|\Phi^-\rangle$	01
	10	$i\sigma_y$	$\|\Phi^+\rangle$	10
	11	σ_z	$\|\Psi^+\rangle$	11

- $\mathcal{P}(Q)$: Positions of the qubits of Q.
- $\mathcal{C}(Q)$: Cover operations on the qubits of Q.
- $\mathcal{B}(Q)$: Bases of the qubits of Q.
- $\mathcal{M}(Q)$ & $\mathcal{A}$: Measures the qubits of Q in proper bases and announces the results.
- $\mathcal{BM}(Q_1, Q_2)$ & $\mathcal{A}$: Measures the qubit pairs of (Q_1, Q_2) in Bell bases and announces the results.
- Sec.chk (A, B): Checks the security of the channel from A to B.
- Cov. op.: Cover operation.
- Ins.: Inserts.

Figure 6-1: Block diagram of the proposed MDI-QSDC with user authentication protocol

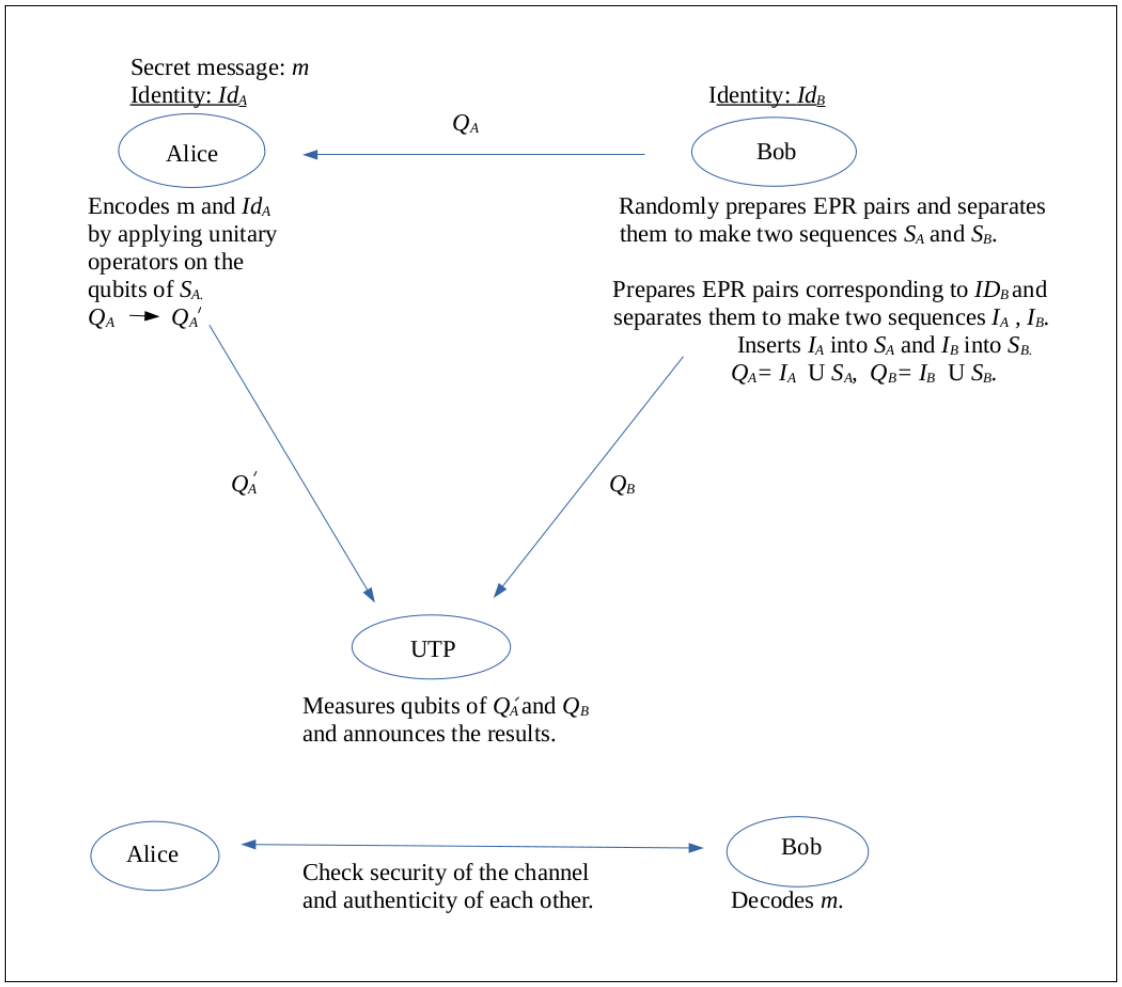
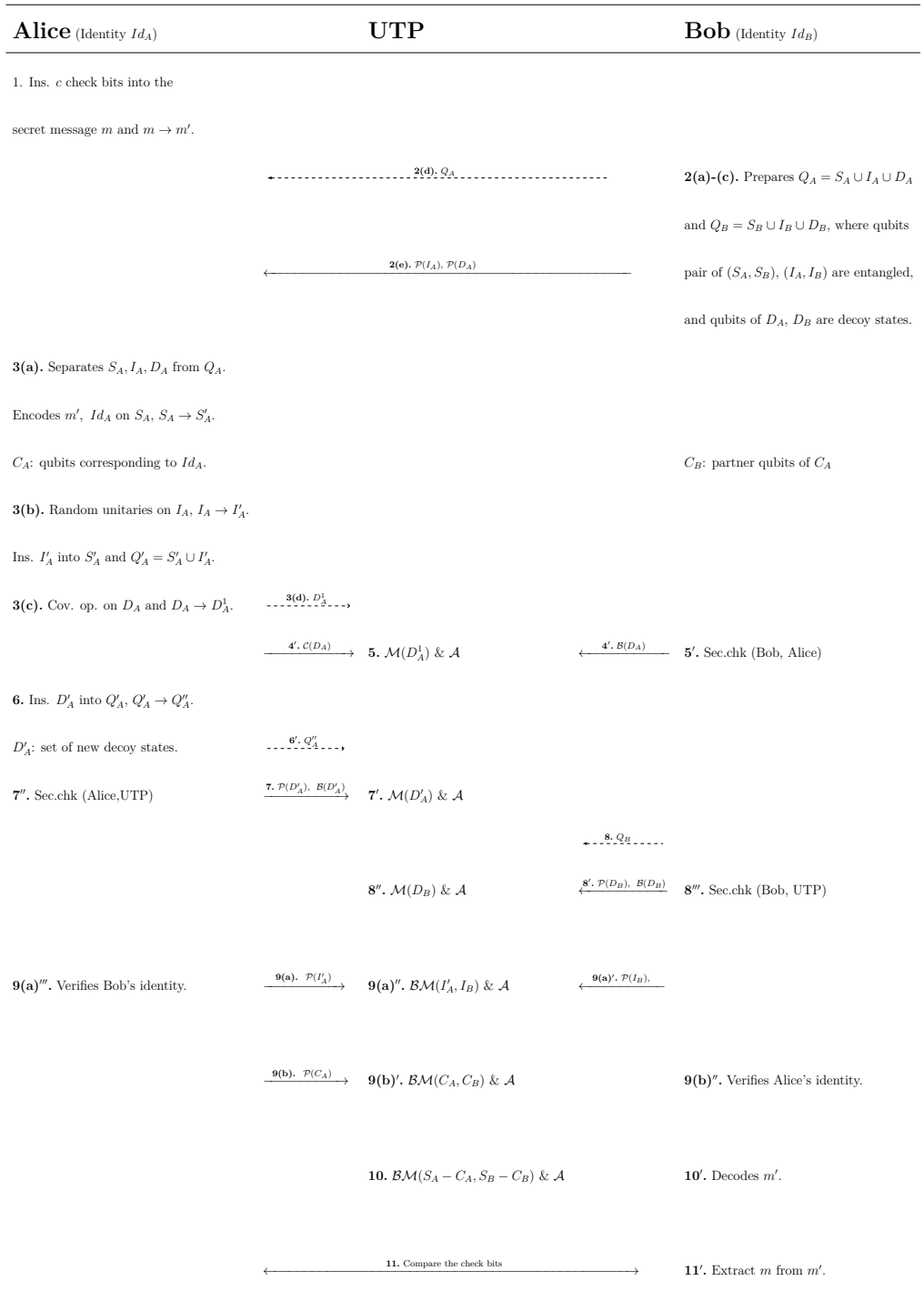


Figure 6-2: Proposed MDI-QSDC with user authentication protocol



6.1.1 Example of our MDI-QSDC protocol

Let us now take an example of the above discussed MDI-QSDC with user authentication protocol, where we assume all channels are noiseless.

Suppose Alice has a 6-bit secret message $m = 011010$ and the secret identities of Alice and Bob are $Id_A = 1011$ and $Id_B = 0111$ respectively, i.e., $n = 6$ and $k = 2$. Then the protocol is as follows.

1. Alice chooses $c = 4$ check bits 1001 and inserts those bits in random positions of m. Let the new bit string be $m' = 0\mathbf{1}011\mathbf{0}0\mathbf{1}\mathbf{1}0$ (bold numbers are check bits, i.e., the 2nd, 3rd, 7th and 9th bits) of length $n + c = 10 = 2N$, i.e., $N = 5$.

2. **Bob:**

   (a) Randomly prepares $N + k = 7$ EPR pairs

   $$|\Psi^+\rangle_{a_1b_1}, |\Phi^+\rangle_{a_2b_2}, |\Phi^+\rangle_{a_3b_3}, |\Psi^-\rangle_{a_4b_4} |\Phi^-\rangle_{a_5b_5}, |\Psi^-\rangle_{a_6b_6}, \text{ and } |\Psi^+\rangle_{a_7b_7}.$$

   He separates the entangled qubit pairs into two particle sequences

   $$S_A = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7\} \text{ and } S_B = \{b_1, b_2, b_3, b_4, b_5, b_6, b_7\},$$

   each of length 7.

   (b) He also prepares 2 EPR pairs $I_1 = |\Phi^-\rangle_{a_1'b_1'}$ and $I_2 = |\Psi^-\rangle_{'a_2b_2'}$ corresponding to his identity $Id_B = 0111$, and creates two single-qubit sequences $I_A = \{a_1', a_2'\}$ and $I_B = \{b_1', b_2'\}$ by separating the EPR pairs.

   (c) Bob chooses two sets $D_A = \{|+\rangle, |1\rangle, |0\rangle, |+\rangle\}$ and $D_B = \{|-\rangle, |0\rangle, |1\rangle, |0\rangle\}$, each of $d = 4$ many decoy photons randomly prepared in Z-basis or X-basis. Then he randomly interleaves the qubits of $I_A(I_B)$ and $D_A(D_B)$ and $S_A(S_B)$ (maintaining the relative ordering of each set) to get a new sequences of single qubits $Q_A(Q_B)$. Let

   $$Q_A = \{a_1, a_2, a_1', |+\rangle, a_3, |1\rangle, a_2', a_4, a_5, |0\rangle, a_6, a_7, |+\rangle\}$$

and $Q_B = \{b_1, b_1', b_2, b_3, b_4, |-\rangle, |0\rangle, b_2', b_5, |1\rangle, b_6, b_7, |0\rangle\}$.

(d) Bob retains the Q_B-sequence and sends the Q_A-sequence to Alice through a quantum channel.

(e) After Alice receives Q_A-sequence, Bob announces the positions of the qubits of I_A (3rd and 7th) and D_A (4th, 6th, 10th and 13th).

3. **Alice:**

(a) She separates the qubits of S_A, I_A and D_A from Q_A, i.e., she has

$$S_A = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7\}, I_A = \{a_1', a_2'\} \text{ and } D_A = \{|+\rangle, |1\rangle, |0\rangle, |+\rangle\}.$$

She randomly chooses 5 qubits a_1, a_3, a_4, a_6 and a_7 from S_A to encode $m' = 0101100110$ and the remaining 2 qubits a_2 and a_5 (say, the set $C_A = \{a_2, a_5\}$) are used to encode $Id_A = 1011$. After encoding the classical information, let S_A become S_A', then

$$S_A' = \{\sigma_x(a_1), i\sigma_y(a_2), \sigma_x(a_3), i\sigma_y(a_4), \sigma_z(a_5), \sigma_x(a_6), i\sigma_y(a_7)\}.$$

(b) Alice randomly applies σ_z and I on the qubits of I_A and the resulting new sequence is $I_A' = \{\sigma_z(a_1'), I(a_2')\}$. She randomly inserts the qubits of I_A' into random positions of S_A' and the new sequence is

$$Q_A' = \{\sigma_x(a_1), \sigma_z(a_1'), i\sigma_y(a_2), \sigma_x(a_3), I(a_2'), i\sigma_y(a_4), \sigma_z(a_5), \sigma_x(a_6), i\sigma_y(a_7)\}.$$

(c) She randomly applies cover operations from $\{I, i\sigma_y, H, i\sigma_y H\}$ on the qubits of D_A and the resulting new sequence is

$$D_A^1 = \{H(|+\rangle), i\sigma_y H(|1\rangle), i\sigma_y(|0\rangle), I(|+\rangle)\} = \{|0\rangle, |+\rangle, |1\rangle, |+\rangle\}.$$

(d) Alice sends D_A^1 to UTP to check the security of the channel from Bob to Alice.

4. After the UTP receives the sequence D_A^1, Bob announces the preparation bases (X, Z, Z and X) of the qubits of D_A and Alice announces the corresponding cover operations ($H, i\sigma_y H, i\sigma_y$ and I).

5. UTP measures the qubits of D_A^1 in proper bases (Z, X, Z and X) and announces the measurement results $|0\rangle, |+\rangle, |1\rangle, |+\rangle$. Since there is no error, Alice and Bob continue the protocol.

6. Alice prepares a new set of $d' = 4$ decoy photons $D'_A = \{|0\rangle, |+\rangle, |-\rangle, |1\rangle\}$. She inserts the decoy qubits into random positions of Q'_A and sends the resulting new sequence Q''_A to UTP, where

$$Q''_A = \{\sigma_x(a_1), \sigma_z(a'_1), i\sigma_y(a_2), |0\rangle, \sigma_x(a_3), I(a'_2), |+\rangle, i\sigma_y(a_4), |-\rangle, \sigma_z(a_5), \sigma_x(a_6), |1\rangle, i\sigma_y(a_7)\}.$$

7. Alice announces the positions (4th, 7th, 9th and 12th) and the preparation bases (Z, X, X and Z) of the decoy qubits of D'_A. UTP measures the decoy qubits and publishes the measurement results $|0\rangle, |+\rangle, |-\rangle, |1\rangle$. Since there is no error, Alice and Bob continue the protocol.

8. Bob sends the sequence Q_B to UTP and when all the qubits of Q_B are reached to UTP, Bob announces the positions (6th, 7th, 10th and 13th) and the preparation bases (X, Z, Z and Z) of the decoy qubits of D_B. UTP measures those qubits in proper bases and discloses the measurement results $|-\rangle, |0\rangle, |1\rangle, |0\rangle$. Then Bob calculates the error rate (which is zero for this example) in the quantum channel between Bob and UTP and goes to the next step.

9. **Authentication process:**

(a) Alice announces the positions (2nd and 6th) of the qubits of I'_A in the sequence Q''_A and Bob announces the positions (2nd and 8th) of the qubits of I_B in the sequence Q_B. UTP measures the i-th qubit pairs $(\sigma_z(a'_1), b'_1)$ and $(I(a'_2), b'_2)$ in Bell basis and announces the results $|\Phi^+\rangle$ and $|\Psi^-\rangle$. As Alice knows $Id_B = 0111$, she knows the exact states of $I_1 = |\Phi^-\rangle$ and $I_2 = |\Psi^-\rangle$. Since she randomly applied Pauli operators σ_z, I on a'_1, a'_2 respectively, the joint state changes to $|\Phi^+\rangle, |\Psi^-\rangle$. Alice confirms Bob's identity and continues the protocol.

(b) Alice announces the positions (2nd and 5th) of the qubits of C_A in the sequence S'_A and UTP measures those qubits with their partner qubits from S_B (say, the set $C_B = (b_2, b_5)$) in Bell bases and announces the measurement results $|\Psi^-\rangle, |\Phi^+\rangle$. Since the initial states of the EPR pairs are $|\Phi^+\rangle, |\Phi^-\rangle$, Bob decodes the identity of Alice as $Id_A = 1011$ and confirms Alice as a legitimate party and continues the protocol.

10. The UTP measures each qubit pair from (S'_A, S_B) in Bell basis and announces the measurement result $|\Phi^+\rangle, |\Psi^+\rangle, |\Phi^+\rangle, |\Phi^-\rangle, |\Phi^-\rangle$. From these results, Bob decodes the classical bit string $m' = 0101100110$.

11. Alice and Bob publicly compare the random check bits (2nd, 3rd, 7th and 9th bits of m') to check the integrity of the messages. Bob discards those bits to obtain the secret message $m = 011010$ and the communication process is completed.

6.1.2 Security analysis of our MDI-QSDC protocol

In our proposed MDI-QSDC with user authentication, the secret message is transmitted between two legitimate parties, and the potential adversary is kept ignorant of the content. There are also broadcast channels between Alice, Bob and UTP, for the necessary classical information, to execute the protocol. First, we show the security of our proposed MDI-QSDC protocol for user authentication by establishing the security against impersonation attack. Then we prove the security of the message transmission part. We assume that *Eve* has infinite resources and unbounded computation power.

Security for user authentication

Let us now discuss the security of our proposed MDI-QSDC protocol against impersonation attacks. An eavesdropper, Eve, may try to impersonate Alice in order to send a fake message to Bob. But since Eve does not know the pre-shared key Id_A, Bob can easily detect Eve with a very high probability. In the proposed MDI-QSDC protocol, suppose Eve may intercept the sequence Q_A sent from Bob to Alice in Step 2d. However, without knowing the pre-shared key Id_A, Eve applies Pauli operators randomly on k qubits of C_A, instead of performing the correct unitary to encode Id_A. She sends it to UTP, who measures these qubits with their partner qubits from C_B on the Bell basis and announces the results. Since Bob knows the initial state of those k EPR pairs (C_A, C_B) and the value of Id_A, he compares the measurement results with the expected EPR pairs and detects Eve. Since Eve applies Pauli operators randomly on each qubit, she applies correct unitary with probability $\frac{1}{4}$ and hence the detection probability of Bob is $1 - (\frac{1}{4})^k$.

On the other hand, Eve may try to impersonate Bob to get the secret message from Alice. In the proposed MDI-QSDC protocol, suppose Eve initiates the protocol and generates the sequences of qubits Q_A and Q_B, which contain the sequences I_A and I_B respectively, by following the process described in Step 2. Now, since Eve does not know the value of Id_B, she prepares each I_i $(1 \leq i \leq k)$ as one of the EPR pairs randomly with probability $\frac{1}{4}$. After Alice applies cover operations on the qubits of I_A, the set becomes I'_A. In the authentication process (Step 9a), UTP measures the joint states of (I'_A, I_B) in proper bases and announces the results. As Alice knows the value of Id_B, she compares the measurement results with the expected results and detects Eve with probability $1 - (\frac{1}{4})^k$.

Security for message transmission

In our MDI-QSDC protocol, we are ignorant of the measurement process and strategy that an adversary may exploit, hence we focus on the system after Bob sends the sequence Q_A to Alice, where a joint state ρ_{AB}^{jnt}, consisting of maximally entangled photon pairs shared between Alice and Bob. We consider a situation where an adversary Eve attacks the system with an auxiliary system and performs a coherent attack. Here, in our protocol, Alice and Bob use

decoy states to obtain the gain and quantum bit error rate (QBER) after each transmission of qubits sequences where both of them send single qubits to the UTP. Now we use the concept of virtual qubits [278, 63] and the proof technique of [135] to establish the security of our protocol against this type of attack. The idea of virtual qubit is that, instead of preparing a single qubit decoy state from $\{|0\rangle, |1\rangle, |+\rangle\ |-\rangle\}$, Alice (Bob) prepares EPR pair, which is a combined system of her (his) virtual qubit and the qubit she (he) is sending to the UTP. Subsequently, they measure their virtual qubits to decide to continue or abort the protocol. For simplicity, let us assume that initially Bob prepares all the EPR pairs in $|\Phi^+\rangle$ and he applies the cover operations $I, \sigma_z, \sigma_x, i\sigma_y$ on the qubits of S_B while sending this sequence Q_B to the UTP. Note that this step is equivalent to the fact that Bob prepares EPR pairs randomly from the set of all Bell states.

Let the system of Alice, Bob and *Eve* be A, B and E respectively. Then from Csiszár–Körner theory [279], the secrecy capacity between Alice and Bob is C_S,

$$C_S = \max[I(A:B) - I(A:E)], \tag{6.1}$$

where $I(X:Y)$ stands for mutual information of two random variables X and Y. Now if $C_S > 0$, then there is a forward encoding scheme with a capacity less than C_S, which can be used to transmit the message reliably and securely from Alice to Bob.

According to quantum De Finetti representation theorem [280], the joint state ρ_{AB}^{jnt} can be asymptotically approximated as a direct product of independent and identically distributed (i.i.d.) subsystems $\rho_{AB}^{\otimes N}$, if a randomized permutation is applied to the system. Thus *Eve* attacks each qubit separately by using a separate probe $|E\rangle$ and then the coherent attack model can be considered as the collective attack by Eve.

According to [281], ρ_{AB} can be written as a linear combination of the Bell states as follows,

$$\rho_{AB} = \delta_1 |\Phi^+\rangle \langle\Phi^+| + \delta_2 |\Phi^-\rangle \langle\Phi^-| + \delta_3 |\Psi^+\rangle \langle\Psi^+| + \delta_4 |\Psi^-\rangle \langle\Psi^-|, \tag{6.2}$$

where $\sum_{i=1}^{4} \delta_i = 1$. Let $|\Phi_{ABE}\rangle$ be a purification of the mixed state ρ_{AB}. Then it can be written

as

$$|\Phi_{ABE}\rangle = \sum_{i=1}^{4} \sqrt{\delta_i}\, |\Psi_i\rangle\, |E_i\rangle\,, \tag{6.3}$$

where $|\Psi_1\rangle = |\Phi^+\rangle$, $|\Psi_2\rangle = |\Phi^-\rangle$, $|\Psi_3\rangle = |\Psi^+\rangle$, $|\Psi_4\rangle = |\Psi^-\rangle$ are the entangled pairs shared by Alice and Bob, and $|E_i\rangle$, $1 \leq i \leq 4$, are the orthonormal states of the system $|E\rangle$.

After Bob sends the sequence Q_A to Alice, they calculate the bit error rate ϵ_z and phase error rate ϵ_x by measuring the virtual qubits by Bob and their partner qubits by Alice. They choose the same bases, either (Z, Z) or (X, X) with probability $\frac{1}{2}$, and measure their respective qubits. If no error occurs, then they should get the same outcomes as $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|{+}{+}\rangle + |{-}{-}\rangle)$. If they get different outcomes while measuring in Z-basis, i.e., the shared entangled state is either $|\Psi^+\rangle$ or $|\Psi^-\rangle$, then bit flip error occurs and thus $\epsilon_z = \delta_3 + \delta_4$. Similarly, when they measure in X-basis and get different outcomes, phase error occurs and thus $\epsilon_x = \delta_2 + \delta_4$. If both the error rates are less than some predefined threshold value, then they continue the process and Alice encodes her message by applying proper unitary operators U_ζ's on the qubits of S_A and Bob applies random cover operations from the set of all Pauli operators on the qubits of S_B, and send their respective sequences to the UTP. Then the shared state becomes

$$\begin{aligned} \rho^{\zeta}_{ABE} &= \frac{1}{4} U_\zeta (|\Phi_{ABE}\rangle \langle\Phi_{ABE}| + \sigma_z^B |\Phi_{ABE}\rangle \langle\Phi_{ABE}| \sigma_z^B \\ &\quad + \sigma_x^B |\Phi_{ABE}\rangle \langle\Phi_{ABE}| \sigma_x^B - \sigma_y^B |\Phi_{ABE}\rangle \langle\Phi_{ABE}| \sigma_y^B) U_\zeta^\dagger \\ &= U_\zeta \rho^c_{ABE} U_\zeta^\dagger, \end{aligned} \tag{6.4}$$

where $\zeta \in \{00, 01, 10, 11\}$ and $U_{00} = I$, $U_{01} = \sigma_x$, $U_{10} = i\sigma_y$, $U_{11} = \sigma_z$ are the message encoding operations of Alice, and $\rho^c_{ABE} = \frac{1}{4}(|\Phi_{ABE}\rangle \langle\Phi_{ABE}| + \sigma_z^B |\Phi_{ABE}\rangle \langle\Phi_{ABE}| \sigma_z^B + \sigma_x^B |\Phi_{ABE}\rangle \langle\Phi_{ABE}| \sigma_x^B - \sigma_y^B |\Phi_{ABE}\rangle \langle\Phi_{ABE}| \sigma_y^B)$.

Let the $2N$-bit message of Alice be $m' = \zeta_1 \zeta_2 \ldots \zeta_N$, where for $1 \leq i \leq N$, ζ_i is a two-bit binary number randomly chosen from $\mathcal{B} = \{00, 01, 10, 11\}$ and the probability distribution of each ζ_i is $\frac{1}{4}$. For $1 \leq i \leq N$, Alice encodes ζ_i by applying U_{ζ_i} on ρ^c_{ABE} and the state becomes $\rho^{\zeta_i}_{ABE}$. We now calculate the maximum amount of accessible information of Eve about ζ_i. Then from Holevo theorem [40], we see the mutual information $I(A : E)$ is bounded above as,

$$I(A:E) \leq S\left(\sum_{\zeta\in\mathcal{B}} p_\zeta \rho^\zeta_{ABE}\right) - \sum_{\zeta\in\mathcal{B}} p_\zeta S(\rho^\zeta_{ABE}) \tag{6.5}$$

where $p_\zeta = \frac{1}{4}$, the probability of randomly selecting one element from $\mathcal{B}$, and $S(\cdot)$ is the Von Neumann entropy.

One can see that Alice's encoding and Bob's cover operations make a maximal mixture of the subsystems A and B. Thus we have $S(\rho^\zeta_{ABE}) = 2$ for $\zeta \in \mathcal{B}$, and

$$I(A:E) \leq S\left(\sum_{\zeta} p_\zeta \rho^\zeta_{ABE}\right) - 2, \tag{6.6}$$

and

$$\begin{aligned}\sum_{\zeta} p_\zeta \rho^\zeta_{ABE} &= \rho^{mix}_{AB} \otimes Tr_{AB}(|\Phi_{ABE}\rangle \langle\Phi_{ABE}|) \\ &= \rho^{mix}_{AB} \otimes \sum_{j=1}^{4} \delta_j |E_j\rangle \langle E_j|,\end{aligned} \tag{6.7}$$

where $\rho^{mix}_{AB} = \frac{I}{4}$ is the maximally mixed state of the system AB. Now we have from Equation (6.7),

$$\begin{aligned}S\left(\sum_{\zeta} p_\zeta \rho^\zeta_{ABE}\right) &= S\left(\rho^{mix}_{AB} \otimes \sum_{j=1}^{4} \delta_j |E_j\rangle \langle E_j|\right) \\ &= S(\rho^{mix}_{AB}) + S\left(\sum_{j=1}^{4} \delta_j |E_j\rangle \langle E_j|\right) \\ &= S\left(\frac{I}{4}\right) + \sum_{j=1}^{4} \delta_j \log \frac{1}{\delta_j} \\ &= 2 + H(\delta_j),\end{aligned} \tag{6.8}$$

where $H(\cdot)$ represents the Shannon entropy function.

Lemma 1: For a probability distribution $\{\delta_i, 1 \leq i \leq 4\}$, $-\sum_{i=1}^{4} \delta_i log \delta_i \leq h(\delta_2 + \delta_4) + h(\delta_3 + \delta_4)$, where $h(\cdot)$ represents the binary entropy function. (See appendix for proof.)

Then from Equation (6.6) and Equation (6.8),

$$\begin{aligned} I(A:E) \leq H(\delta_j) &= \sum_{j=1}^{4} \delta_j \log \frac{1}{\delta_j} \\ &\leq h(\delta_3 + \delta_4) + h(\delta_2 + \delta_4) \text{ (by Lemma 1)} \\ &= h(\epsilon_z) + h(\epsilon_x), \end{aligned} \tag{6.9}$$

Let ϵ_e be the error rate calculated after message decoding step, and if there is a discrete symmetric channel between Alice and Bob, then the secrecy capacity is

$$\begin{aligned} C_S &\geq I(A:B) - I(A:E) \\ &\geq H(A) - H(A|B) - h(\epsilon_z) - h(\epsilon_x) \\ &= 2 - h(\epsilon_e) - h(\epsilon_z) - h(\epsilon_x). \end{aligned}$$

For our protocol to be secure, we need $C_S > 0$, i.e., $2 - h(\epsilon_e) > h(\epsilon_z) + h(\epsilon_x)$.

6.1.3 Comparison with existing works

We compare the efficiency of our proposed MDI-QSDC protocol with the existing works (see Table 6.2). In [5], authors proposed an MDI-QSDC protocol based on the idea of quantum teleportation, where the sender prepares a Bell state and the receiver prepares a single qubit state. First, they do a Bell measurement, by UTP, to teleport the receiver's qubit to the sender, and then the sender encodes its secret message. To decode the secret message they do a single qubit measurement on Z basis by UTP. Therefore the protocol [5] requires three qubits and two measurements to communicate a single-bit message. In [2], the authors proposed an MDI-QSDC protocol using entanglement swapping. To share a two-bit secret message, both the sender and the receiver prepare Bell states and perform entanglement swapping with the help of a third party. After that, the sender encodes the secret message. This protocol requires two Bell states and two Bell measurements for sending a two-bit message. In [137], authors found a security loophole in [2] and proposed a modification over that. The modified version also requires the same resource as before. In [80], the authors proposed a long-distance MDI-

QSDC protocol by using ancillary entangled photon-pair sources and relay nodes. To transmit a single-bit message, they use two Bell states and a single qubit state. The protocol also requires two Bell measurements and a Z-basis measurement. Here in our present protocol, to send a two-bit message, we only use a Bell state and a Bell measurement. Therefore, on average it requires a qubit and half measurement to transfer a single-bit message. Also, none of the above existing works provide the user authentication feature before transferring the secret information.

Table 6.2: Comparison between existing MDI-QSDC and our work

Paper	**No. of qubits per message bit**	**No. of Bell Meas. per message bit**	**No. of S.B. Meas. per message bit**	**User authentication**
Zhou et al. [5]	3	1	1	No
Neu et al. [2]	2	1	0	No
Gao et al. [80]	5	2	1	No
Das et al. [137]	2	1	0	No
Present protocol	1	1/2	0	Yes

*Bell Meas.: Bell basis measurement, S.B. Meas.: Single basis measurement.

In the next two sections, we propose MDI-QD and MDI-DSQC protocols with mutual identity authentication respectively.

6.2 Proposed MDI-QD protocol with user authentication

In this section, we generalize the MDI-QSDC protocol into an MDI-QD protocol, which also provides mutual user authentication. Here, both Alice and Bob send their n-bit secret message to each other simultaneously after confirming the authenticity of the other user. They use one EPR pair to exchange one-bit messages from each other. Bob randomly prepares $(n+c)$ EPR pairs $|\Phi^+\rangle$ or $|\Psi^+\rangle$ ($|\Phi^-\rangle$ or $|\Psi^-\rangle$) corresponding to his secret message bit 0 (1), where c is the number of check bits. He also randomly prepares k EPR pairs from $\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$ for encoding the secret identity of Alice and inserts these into the previously prepared EPR sequence. After Alice receives the qubit sequence, he announces the positions of randomly prepared EPR pairs. Alice randomly applies Pauli operator I or σ_z (σ_x or $i\sigma_y$) to encode

her message bit 0 (1) (see Table (6.3)). The rest of the procedure is the same as the above MDI-QSDC protocol described in Section 4.1. The security of this protocol directly follows from the above MDI-QSDC protocol.

Table 6.3: Encoding rules of our proposed MDI-QD.

Message bit		**Bob prepares**	**Alice's unitary**	**Final joint state**
Alice	**Bob**	(S_A, S_B)	S_A **to** S'_A	(S'_A, S_B)
0	0	$\|\Phi^+\rangle$	I	$\|\Phi^+\rangle$
			σ_z	$\|\Phi^-\rangle$
		$\|\Psi^+\rangle$	I	$\|\Psi^+\rangle$
			σ_z	$\|\Psi^-\rangle$
0	1	$\|\Phi^-\rangle$	I	$\|\Phi^-\rangle$
			σ_z	$\|\Phi^+\rangle$
		$\|\Psi^-\rangle$	I	$\|\Psi^-\rangle$
			σ_z	$\|\Psi^+\rangle$
1	0	$\|\Phi^+\rangle$	σ_x	$\|\Psi^+\rangle$
			$i\sigma_y$	$\|\Psi^-\rangle$
		$\|\Psi^+\rangle$	σ_x	$\|\Phi^+\rangle$
			$i\sigma_y$	$\|\Phi^-\rangle$
1	1	$\|\Phi^-\rangle$	σ_x	$\|\Psi^-\rangle$
			$i\sigma_y$	$\|\Psi^+\rangle$
		$\|\Psi^-\rangle$	σ_x	$\|\Phi^-\rangle$
			$i\sigma_y$	$\|\Phi^+\rangle$

6.2.1 Example of our MDI-QD protocol

Let us now take an example of the above discussed MDI-QD with user authentication protocol, where we assume all channels are noiseless.

Suppose Alice (Bob) has the 3-bit secret message $m_a = 011$ ($m_b = 100$) and 4-bit secret identity $Id_A = 1011$ ($Id_B = 0111$), i.e., $n = 3$ and $k = 2$. Then the protocol is as follows.

1. Alice (Bob) chooses $c = 2$ check bits 10 (01) and inserts those bits in random positions

of m_a (m_b). Let the new bit string be $m'_a = \mathbf{1}0\mathbf{1}0\mathbf{1}$ ($m'_b = 1\mathbf{0}0\mathbf{1}0$) of length 5, where the bold numbers represent the check bits.

2. **Bob:**

   (a) Prepares 5 EPR pairs corresponding to m'_b and those are

   $$|\Psi^-\rangle_{a_1b_1}, |\Phi^+\rangle_{a_3b_3}, |\Psi^+\rangle_{a_4b_4}, |\Phi^-\rangle_{a_6b_6}, \text{ and } |\Phi^+\rangle_{a_7b_7}.$$

   He separates the entangled qubit pairs into two particle sequences

   $$S_A = \{a_1, a_3, a_4, a_6, a_7\} \text{ and } S_B = \{b_1, b_3, b_4, b_6, b_7\},$$

   each of length 5.

   (b) He also randomly prepares 2 EPR pairs $|\Phi^+\rangle_{a_2b_2}$ and $|\Phi^-\rangle_{a_5b_5}$ and separates into two particle sequences $C_A = \{a_2, a_5\}$ and $C_B = \{b_2, b_5\}$. He inserts the qubits of C_A and C_B into the sequences S_A and S_B to form two new sequences

   $$S'_A = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7\} \text{ and } S'_B = \{b_1, b_2, b_3, b_4, b_5, b_6, b_7\}$$

   respectively.

   (c) Then he prepares 2 EPR pairs $I_1 = |\Phi^-\rangle_{a'_1b'_1}$ and $I_2 = |\Psi^-\rangle_{'a_2b'_2}$ corresponding to his identity $Id_B = 0111$, and creates two single-qubit sequences $I_A = \{a'_1, a'_2\}$ and $I_B = \{b'_1, b'_2\}$ by separating the EPR pairs.

   (d) Bob chooses two sets $D_A = \{|+\rangle, |1\rangle, |0\rangle, |+\rangle\}$ and $D_B = \{|-\rangle, |0\rangle, |1\rangle, |0\rangle\}$, each of $d = 4$ many decoy photons randomly prepared in Z-basis or X-basis. Then he randomly interleaves the qubits of $I_A(I_B)$ and $D_A(D_B)$ and $S'_A(S'_B)$ (maintaining the relative ordering of each set) to get a new sequences of single qubits $Q_A(Q_B)$. Let

   $$Q_A = \{a_1, a_2, a'_1, |+\rangle, a_3, |1\rangle, a'_2, a_4, a_5, |0\rangle, a_6, a_7, |+\rangle\}$$

   $$\text{and } Q_B = \{b_1, b'_1, b_2, b_3, b_4, |-\rangle, |0\rangle, b'_2, b_5, |1\rangle, b_6, b_7, |0\rangle\}.$$

(e) Bob retains the Q_B-sequence and sends the Q_A-sequence to Alice through a quantum channel.

(f) After Alice receives Q_A-sequence, Bob announces the positions of the qubits of C_A (2nd and 9th), I_A (3rd and 7th) and D_A (4th, 6th, 10th and 13th).

3. **Alice:**

(a) She separates the qubits of S_A, C_A, I_A and D_A from Q_A, i.e., she has

$$S_A = \{a_1, a_3, a_4, a_6, a_7\}, C_A = \{a_2, a_5\}, I_A = \{a'_1, a'_2\} \text{ and } D_A = \{|+\rangle, |1\rangle, |0\rangle, |+\rangle\}.$$

She encodes $m'_a = 10101$ and $Id_A = 1011$ on the qubits of S_A and C_A respectively. After encoding the classical information, let S_A and C_A become S_A^1 and C_A^1 respectively. Then

$$S_A^1 = \{\sigma_x(a_1), \sigma_z(a_3), i\sigma_y(a_4), I(a_6), i\sigma_y(a_7)\}$$

and

$$C_A^1 = \{i\sigma_y(a_2), \sigma_z(a_5)\}.$$

Then she randomly inserts the qubits of C_A^1 into the S_A^1 and let the new sequence be

$$S''_A = \{\sigma_x(a_1), i\sigma_y(a_2), \sigma_z(a_3), i\sigma_y(a_4), \sigma_z(a_5), I(a_6), i\sigma_y(a_7)\}.$$

(b) Alice randomly applies σ_z and I on the qubits of I_A and the resulting new sequence is $I'_A = \{\sigma_z(a'_1), I(a'_2)\}$. She randomly inserts the qubits of I'_A into random positions of S''_A and the new sequence is

$$Q'_A = \{\sigma_x(a_1), \sigma_z(a'_1), i\sigma_y(a_2), \sigma_z(a_3), I(a'_2), i\sigma_y(a_4), \sigma_z(a_5), I(a_6), i\sigma_y(a_7)\}.$$

(c) She randomly applies cover operations from $\{I, i\sigma_y, H, i\sigma_y H\}$ on the qubits of D_A and the resulting new sequence is

$$D_A^1 = \{H(|+\rangle), i\sigma_y H(|1\rangle), i\sigma_y(|0\rangle), I(|+\rangle)\} = \{|0\rangle, |+\rangle, |1\rangle, |+\rangle\}.$$

(d) Alice sends D_A^1 to UTP to check the security of the channel from Bob to Alice.

4. After the UTP receives the sequence D_A^1, Bob announces the preparation bases (X, Z, Z and X) of the qubits of D_A and Alice announces the corresponding cover operations ($H, i\sigma_y H, i\sigma_y$ and I).

5. UTP measures the qubits of D_A^1 in proper bases (Z, X, Z and X) and announces the measurement results $|0\rangle, |+\rangle, |1\rangle, |+\rangle$. Since there is no error, Alice and Bob continue the protocol.

6. Alice prepares a new set of $d' = 4$ decoy photons $D'_A = \{|0\rangle, |+\rangle, |-\rangle, |1\rangle\}$. She inserts the decoy qubits into random positions of Q'_A and sends the resulting new sequence Q''_A to UTP, where

$$Q''_A = \{\sigma_x(a_1), \sigma_z(a'_1), i\sigma_y(a_2), |0\rangle, \sigma_z(a_3), I(a'_2), |+\rangle, i\sigma_y(a_4), |-\rangle, \sigma_z(a_5), I(a_6), |1\rangle, i\sigma_y(a_7)\}.$$

7. Alice announces the positions (4th, 7th, 9th and 12th) and the preparation bases (Z, X, X and Z) of the decoy qubits of D'_A. UTP measures the decoy qubits and publishes the measurement results $|0\rangle, |+\rangle, |-\rangle, |1\rangle$. Since there is no error, Alice and Bob continue the protocol.

8. Bob sends the sequence Q_B to UTP and when all the qubits of Q_B are reached to UTP, Bob announces the positions (6th, 7th, 10th and 13th) and the preparation bases (X, Z, Z and Z) of the decoy qubits of D_B. UTP measures those qubits in proper bases and discloses the measurement results $|-\rangle, |0\rangle, |1\rangle, |0\rangle$. Then Bob calculates the error

rate (which is zero for this example) in the quantum channel between Bob and UTP and goes to the next step.

9. **Authentication process:**

   (a) Alice announces the positions (2nd and 6th) of the qubits of I'_A in the sequence Q''_A and Bob announces the positions (2nd and 8th) of the qubits of I_B in the sequence Q_B. UTP measures the i-th qubit pairs $(\sigma_z(a'_1), b'_1)$ and $(I(a'_2), b'_2)$ in Bell basis and announces the results $|\Phi^+\rangle$ and $|\Psi^-\rangle$. As Alice knows $Id_B = 0111$, she knows the exact states of $I_1 = |\Phi^-\rangle$ and $I_2 = |\Psi^-\rangle$. Since she randomly applied Pauli operators σ_z, I on a'_1, a'_2 respectively, the joint state changes to $|\Phi^+\rangle, |\Psi^-\rangle$. Alice confirms Bob's identity and continues the protocol.

   (b) Alice announces the positions (2nd and 5th) of the qubits of C'_A in the sequence S''_A and UTP measures those qubits with their partner qubits from $C_B = (b_2, b_5)$ in Bell bases and announces the measurement results $|\Psi^-\rangle, |\Phi^+\rangle$. Since the initial states of the EPR pairs are $|\Phi^+\rangle, |\Phi^-\rangle$, Bob decodes the identity of Alice as $Id_A = 1011$ and confirms Alice as a legitimate party and continues the protocol.

10. The UTP measures each qubit pair from (S'_A, S_B) in Bell basis and announces the measurement result $|\Phi^-\rangle, |\Phi^-\rangle, |\Phi^-\rangle, |\Phi^-\rangle, |\Psi^-\rangle$. From these results, Alice (Bob) decodes the classical bit string $m'_b = 10010$ ($m'_a = 10101$).

11. Alice and Bob publicly compare the random check bits to check the integrity of the messages. They discard those bits to obtain the secret message $m_a = 011$ and $m_b = 100$. This completes the communication process.

6.3 Proposed MDI-DSQC Protocol with user authentication

In this section, we propose our new MDI-DSQC protocol with user identity authentication process.

Let Alice has an n-bit secret message m, which she wants to send Bob through a quantum channel with the help of some UTP, who performs all the measurements during the protocol. Alice and Bob have their $2k$-bit secret user identities Id_A and Id_B respectively which they have shared previously by using some secured QKD. The protocol is as follows:

Steps 1, 2, 3(a) are the same as before in the MDI-DSQC protocol of Section 4.1.

3. **Alice:**

   (a) She separates the qubits of S_A, I_A and D_A from Q_A. Then from the sequence S_A she randomly chooses N qubits to encode the secret message and the remaining k qubits are used to encode her secret identity Id_A. The encoding processes for m' and Id_A are the same. Alice encodes two bits of classical information into one qubit by applying an unitary operator. To encode $00, 01, 10$ and 11 she applies the Pauli operators [6] I, σ_x, $i\sigma_y$ and σ_z respectively. After encoding the classical information, suppose S_A becomes S'_A.

   (b) Alice randomly applies I, σ_x, $i\sigma_y$ and σ_z on the qubits of I_A to get, say, I'_A. She randomly inserts the qubits of I'_A and D_A into random positions of S'_A and let the new sequence be Q'_A.

   (c) She randomly applies cover operations from $\{I, i\sigma_y, H, i\sigma_y H\}$ on the qubits of Q'_A and inserts a new set of d' decoy photons D'_A into random positions of Q'_A, to obtain, say, Q''_A, which Alice sends to UTP.

4. After UTP receives the sequence Q''_A, Alice announces the positions and the preparation bases of the decoy qubits of D'_A. UTP measures the decoy qubits and publishes the measurement results, and Alice calculates the error in the quantum channel between Alice and UTP. If the estimated error is greater than some threshold value, then they terminate the protocol and otherwise go to the next step.

5. Bob sends the sequence Q_B to UTP and when all the qubits of Q_B are reached to UTP, Bob announces the positions and the preparation bases of the decoy qubits of D_B. UTP measures those qubits in proper bases and discloses the measurement results, and Bob calculates the error in the quantum channel between Bob and UTP. If the estimated error

is greater than some threshold value, then they terminate the protocol and otherwise go to the next step.

6. To check the security of the quantum channel from Bob to Alice, Bob announces the preparation bases of the qubits of D_A and Alice announces the corresponding positions and the cover operations which she applies on those qubits. UTP measures those qubits, from the announced measurement results Alice and Bob calculate the error in the channel and decide to continue or stop the protocol.

7. UTP discards all the measured qubits and Alice announces all cover operations for the remaining qubits.

8. **Authentication process:** Same as before in the MDI-DSQC protocol of Section 4.1.

9. UTP measures each qubit pair from (S'_A, S_B) in Bell basis and announces the measurement result. From the knowledge of (S_A, S_B) and (S'_A, S_B), Bob decodes the classical bit string m'.

10. Alice and Bob publicly compare the random check bits to check the integrity of the messages. If they find an acceptable error rate then Bob gets the secret message m and the communication process is completed.

Using similar arguments as in Section 6.1.2, we can prove the security of our proposed MDI-DSQC Protocol with user authentication.

6.3.1 Example of our MDI-DSQC protocol

Let us now take an example of the above discussed MDI-DSQC with user authentication protocol, where we assume all channels are noiseless.

Suppose Alice has a 6-bit secret message $m = 011010$ and the secret identities of Alice and Bob are $Id_A = 1011$ and $Id_B = 0111$ respectively, i.e., $n = 6$ and $k = 2$. Then the protocol is as follows.

1. Alice chooses $c = 4$ check bits 1001 and inserts those bits in random positions of m. Let the new bit string be $m' = 0\mathbf{1}011\mathbf{0}0\mathbf{1}1\mathbf{0}$ (bold numbers are check bits, i.e., the 2nd, 3rd, 7th and 9th bits) of length $n + c = 10 = 2N$, i.e., $N = 5$.

2. **Bob:**

   (a) Randomly prepares $N + k = 7$ EPR pairs

   $$|\Psi^+\rangle_{a_1b_1}, |\Phi^+\rangle_{a_2b_2}, |\Phi^+\rangle_{a_3b_3}, |\Psi^-\rangle_{a_4b_4} |\Phi^-\rangle_{a_5b_5}, |\Psi^-\rangle_{a_6b_6}, \text{ and } |\Psi^+\rangle_{a_7b_7}.$$

   He separates the entangled qubit pairs into two particle sequences

   $$S_A = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7\} \text{ and } S_B = \{b_1, b_2, b_3, b_4, b_5, b_6, b_7\},$$

   each of length 7.

   (b) He also prepares 2 EPR pairs $I_1 = |\Phi^-\rangle_{a_1'b_1'}$ and $I_2 = |\Psi^-\rangle_{'a_2b_2'}$ corresponding to his identity $Id_B = 0111$, and creates two single-qubit sequences $I_A = \{a_1', a_2'\}$ and $I_B = \{b_1', b_2'\}$ by separating the EPR pairs.

   (c) Bob chooses two sets $D_A = \{|+\rangle, |1\rangle, |0\rangle, |+\rangle\}$ and $D_B = \{|-\rangle, |0\rangle, |1\rangle, |0\rangle\}$, each of $d = 4$ many decoy photons randomly prepared in Z-basis or X-basis. Then he randomly interleaves the qubits of $I_A(I_B)$ and $D_A(D_B)$ and $S_A(S_B)$ (maintaining the relative ordering of each set) to get a new sequences of single qubits $Q_A(Q_B)$. Let

   $$Q_A = \{a_1, a_2, a_1', |+\rangle, a_3, |1\rangle, a_2', a_4, a_5, |0\rangle, a_6, a_7, |+\rangle\}$$

   $$\text{and } Q_B = \{b_1, b_1', b_2, b_3, b_4, |-\rangle, |0\rangle, b_2', b_5, |1\rangle, b_6, b_7, |0\rangle\}.$$

   (d) Bob retains the Q_B-sequence and sends the Q_A-sequence to Alice through a quantum channel.

   (e) After Alice receives Q_A-sequence, Bob announces the positions of the qubits of I_A (3rd and 7th) and D_A (4th, 6th, 10th and 13th).

3. **Alice:**

(a) She separates the qubits of S_A, I_A and D_A from Q_A, i.e., she has

$$S_A = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7\}, I_A = \{a'_1, a'_2\} \text{ and } D_A = \{|+\rangle, |1\rangle, |0\rangle, |+\rangle\}.$$

She randomly chooses 5 qubits a_1, a_3, a_4, a_6 and a_7 from S_A to encode $m' = 0101100110$ and the remaining 2 qubits a_2 and a_5 (say, the set $C_A = \{a_2, a_5\}$) are used to encode $Id_A = 1011$. After encoding the classical information, let S_A become S'_A, then

$$S'_A = \{\sigma_x(a_1), i\sigma_y(a_2), \sigma_x(a_3), i\sigma_y(a_4), \sigma_z(a_5), \sigma_x(a_6), i\sigma_y(a_7)\}.$$

(b) Alice randomly applies σ_z and I on the qubits of I_A and the resulting new sequence is $I'_A = \{\sigma_z(a'_1), I(a'_2)\}$. She randomly inserts the qubits of I'_A and D_A into random positions of S'_A and the new sequence is

$$Q'_A = \{\sigma_x(a_1), |+\rangle, \sigma_z(a'_1), i\sigma_y(a_2), |1\rangle, |0\rangle, \sigma_x(a_3), I(a'_2), i\sigma_y(a_4), |+\rangle, \sigma_z(a_5), \sigma_x(a_6), i\sigma_y(a_7)\}.$$

(c) She randomly applies cover operations from $\{I, i\sigma_y, H, i\sigma_y H\}$ on the qubits of Q'_A and the resulting new sequence is

$$Q'^{1}_A = \{i\sigma_y H\sigma_x(a_1), H(|+\rangle), I\sigma_z(a'_1), Hi\sigma_y(a_2), I(|1\rangle), i\sigma_y(|0\rangle), H\sigma_x(a_3),$$
$$HI(a'_2), i\sigma_y Hi\sigma_y(a_4), I(|+\rangle), i\sigma_y\sigma_z(a_5), i\sigma_y H\sigma_x(a_6), Hi\sigma_y(a_7)\}.$$

Alice choses a set $D'_A = \{|-\rangle, |1\rangle, |0\rangle\}$ of $d' = 3$ decoy qubits randomly prepared in Z-basis or X-basis. Then she inserts those decoy qubits into some random positions

of Q'_A and the resulting new sequence is

$$Q''_A = \{|-\rangle, i\sigma_y H\sigma_x(a_1), H(|+\rangle), I\sigma_z(a'_1), Hi\sigma_y(a_2), I(|1\rangle), |1\rangle, i\sigma_y(|0\rangle), H\sigma_x(a_3),$$
$$HI(a'_2), i\sigma_y Hi\sigma_y(a_4), I(|+\rangle), i\sigma_y\sigma_z(a_5), i\sigma_y H\sigma_x(a_6), |0\rangle, Hi\sigma_y(a_7)\}.$$

Alice sends Q''_A to UTP.

4. After the UTP receives the sequence Q''_A, Alice announces the positions (1st, 7th and 15th) and the preparation bases (X, Z and Z) of the decoy qubits of D'_A. UTP measures the decoy qubits and publishes the measurement results $|-\rangle, |1\rangle, |0\rangle$. Since there is no error, the quantum channel between Alice and UTP is secure and they continue the protocol.

5. Bob sends the sequence Q_B to UTP and when all the qubits of Q_B are reached to UTP, Bob announces the positions (6th, 7th, 10th and 13th) and the preparation bases (X, Z, Z and Z) of the decoy qubits of D_B. UTP measures those qubits in proper bases and discloses the measurement results $|-\rangle, |0\rangle, |1\rangle, |0\rangle$. Then Bob calculates the error rate (which is zero for this example) in the quantum channel between Bob and UTP and goes to the next step.

6. Bob announces the preparation bases (X, Z, Z and X) of the qubits of D_A and Alice announces the corresponding positions (3rd, 6th, 8th and 12th) in the sequence Q''_A and the cover operations ($H, I, i\sigma_y$ and I) which she applies on those qubits. UTP measures those qubits and from the announced measurement results, Alice and Bob find the channel is secure. They decide to continue the protocol.

7. UTP discards all the measured qubits from Q''_A and Q_B, then UTP has the following sequences

$$Q^1_A = \{i\sigma_y H\sigma_x(a_1), I\sigma_z(a'_1), Hi\sigma_y(a_2), H\sigma_x(a_3), HI(a'_2), i\sigma_y Hi\sigma_y(a_4),$$
$$i\sigma_y\sigma_z(a_5), i\sigma_y H\sigma_x(a_6), Hi\sigma_y(a_7)\}$$

and

$$Q_B^1 = \{b_1, b_1', b_2, b_3, b_4, b_2', b_5, b_6, b_7\}.$$

Alice announces all cover operations ($i\sigma_y H, I, H, H, H, i\sigma_y H, i\sigma_y, i\sigma_y H$ and H) for the qubits of Q_A^1. Then UTP applies the inverse of the cover operation on the corresponding qubits and gets back

$$Q_A^2 = \{\sigma_x(a_1), \sigma_z(a_1'), i\sigma_y(a_2), \sigma_x(a_3), I(a_2'), i\sigma_y(a_4), \sigma_z(a_5), \sigma_x(a_6), i\sigma_y(a_7)\}.$$

8. **Authentication process:**

   (a) Alice announces the positions (2nd and 5th) of the qubits of I_A' in the sequence Q_A^2 and Bob announces the positions (2nd and 6th) of the qubits of I_B in the sequence Q_B^1. UTP measures the qubit pairs $(\sigma_z(a_1'), b_1')$ and $(I(a_2'), b_2')$ in Bell basis and announces the results $|\Phi^+\rangle$ and $|\Psi^-\rangle$. As Alice knows $Id_B = 0111$, she knows the exact states of $I_1 = |\Phi^-\rangle$ and $I_2 = |\Psi^-\rangle$. Since she randomly applied Pauli operators σ_z, I on a_1', a_2' respectively, the joint state changes to $|\Phi^+\rangle, |\Psi^-\rangle$. Alice confirms Bob's identity and continues the protocol.

   (b) Alice announces the positions (2nd and 5th) of the qubits of C_A in the sequence S_A' and UTP measures those qubits with their partner qubits from S_B (say, the set $C_B = (b_2, b_5)$) in Bell bases and announces the measurement results $|\Psi^-\rangle, |\Phi^+\rangle$. Since the initial states of the EPR pairs are $|\Phi^+\rangle, |\Phi^-\rangle$, Bob decodes the identity of Alice as $Id_A = 1011$ and confirms Alice as a legitimate party and continues the protocol.

9. The UTP discards the measured qubits and measures the remaining qubit pairs from (S_A', S_B) in Bell basis and announces the measurement result $|\Phi^+\rangle, |\Psi^+\rangle, |\Phi^+\rangle, |\Phi^-\rangle, |\Phi^-\rangle$. From these results, Bob decodes the classical bit string $m' = 0101100110$.

10. Alice and Bob publicly compare the random check bits (2nd, 3rd, 7th and 9th bits of

m') to check the integrity of the messages. Bob discards those bits to obtain the secret message $m = 011010$ and the communication process is completed.

6.4 Discussion

In this chapter, we discuss an MDI-QSDC which provides mutual identity authentication of the users. Here, both the parties have their previously shared secret identity keys, and the sender first verify the authenticity of the receiver and then sends the secret message with the help of a UTP, who performs all the measurements. Similarly, the receiver also verify the sender's identity before receiving the message. Then we extend it to an MDI-QD protocol, where both the parties check the authenticity of the other party before exchanging their secret messages. Next we also present an MDI-DSQC protocol with user authentication and analyses the security of these protocols

Chapter 7

Analysis and Design of MDI Quantum Dialogue Protocols

This chapter is based on the paper [138], where we propose two efficient MDI-QD protocols which are modifications of [3]. In our protocols, after the key generation step as [3], let the shared key between two legitimate parties Alice and Bob be $k = k_1 k_2 \dots k_n$. They calculate the bit $c = \oplus k_i$, $1 \leq i \leq n$. Then both of our protocols are the same as [3] up-to the step where the UTP announces the measurement results. In the next step, Alice and Bob estimate the error in the channel (process is also same as [3]). If the estimated error lies between a tolerable range they continue the protocol, else they abort. In the original protocol [3], Alice and Bob discard almost half of the measurement results to avoid information leakage problem. We reduce the number of discarded measurement results by generating some sequences and computing some functions of the sequences.

7.1 Our first efficient MDI-QD protocol

After the error estimation phase, let the number of remaining measurement results be n', Alice and Bob make a finite sequence $\{M[i]\}_{i=1}^{n'}$ containing the measurement results. i.e., $M[i]$ is the i-th measurement result announced by the UTP, for $1 \leqslant i \leqslant n'$ and $M[i] \in \{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$. They keep all the measurement results $M[i]$s where $M[i] \in \{|\phi^-\rangle, |\psi^+\rangle\}$. Among the remaining measurement results, they choose some of them to keep and discard the

others. For $1 \leq i \leq n'$, if $M[i] \in \{|\phi^+\rangle, |\psi^-\rangle\}$ and $k_i = c$, then Alice and Bob keep that $M[i]$. Else they discard that $M[i]$. Using Table 2.7 and Table 2.8, they guess the message bit of each other corresponding to all the measurement results $M[i]$ which they kept. Details are given in the following section.

7.1.1 Proposed protocol

1. Alice and Bob share a n-bit key stream ($k = k_1 k_2 \dots k_n$) between themselves using BB84 protocol.

2. They calculate $c = \oplus k_i$, $1 \leq i \leq n$.

3. Let n-bit message of Alice and Bob be $a = a_1 a_2 \dots a_n$ and $b = b_1 b_2 \dots b_n$ respectively.

4. For $1 \leq i \leq n$, Alice (Bob) prepares the qubits Q_A (Q_B) at her (his) end according to the following strategy:

   (a) if a_i (b_i)$= 0$ and $k_i = 0$, set Q_{A_i} (Q_{B_i}) $= |0\rangle$;

   (b) if a_i (b_i)$= 1$ and $k_i = 0$, set Q_{A_i} (Q_{B_i}) $= |1\rangle$;

   (c) if a_i (b_i)$= 0$ and $k_i = 1$, set Q_{A_i} (Q_{B_i}) $= |+\rangle$;

   (d) if a_i (b_i)$= 1$ and $k_i = 1$, set Q_{A_i} (Q_{B_i}) $= |-\rangle$.

5. Alice (Bob) sends Q_A (Q_B) to the third party (TP).

6. For $1 \leq i \leq n$, the UTP measures the two qubits Q_{A_i} and Q_{B_i} in Bell basis and announces the result.

7. Alice and Bob make a finite sequence $\{M[i]\}_{i=1}^{n}$ containing the measurement results, i.e., for $1 \leqslant i \leqslant n$, $M[i]$ is the i-th measurement result announced by the UTP, where $M[i] \in \{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$.

8. They randomly choose γn number of measurement results $M[i]$ from the sequence $\{M[i]\}_{i=1}^{n}$ to estimate the error, where $\gamma < 1$ is a small fraction.

9. Alice and Bob guess the message bit of other, corresponding to their chosen γn number of measurement results using Table 2.7 and Table 2.8.

10. They reveal their respective guesses for these rounds.

11. If estimated error is greater than some predefined threshold value, then they abort. Else continue and goto next step.

12. Their remaining sequence of measurement results is relabeled as $\{M[i]\}_{i=1}^{n'}$, where $n' = (1-\gamma)n$.

13. They update their n-bit key to an n'-bit key by discarding γn number of key bits corresponding to above γn rounds. The updated key is relabeled as $k = k_1 k_2 \dots k_{n'}$.

14. They generate a finite sequence $\{X[i]\}_{i=1}^{n'}$ such that

$$X[i] = \begin{cases} 1, & \text{if } M_i = |\phi^-\rangle \text{ or } |\psi^+\rangle; \\ 0, & \text{otherwise.} \end{cases}$$

15. Then they generate another finite sequence $\{Y[i]\}_{i=1}^{n'}$ such that

$$Y[i] = \begin{cases} 0, & \text{if } X[i] = 1; \\ k_j, & \text{if } c = 1 \text{ and } X[i] \text{ is the } j\text{-th zero of the sequence } \{X[q]\}_{q=1}^{n'}; \\ \bar{k_j}, & \text{if } c = 0 \text{ and } X[i] \text{ is the } j\text{-th zero of the sequence } \{X[q]\}_{q=1}^{n'}. \end{cases}$$

16. For $1 \leq i \leq n'$:

    - if $X[i] \oplus Y[i] = 1$, then Alice and Bob consider the i-th measurement result $M[i]$ and guess others message bit using Table 2.7 and Table 2.8.
    - Else they discard $M[i]$.

This completes the protocol.

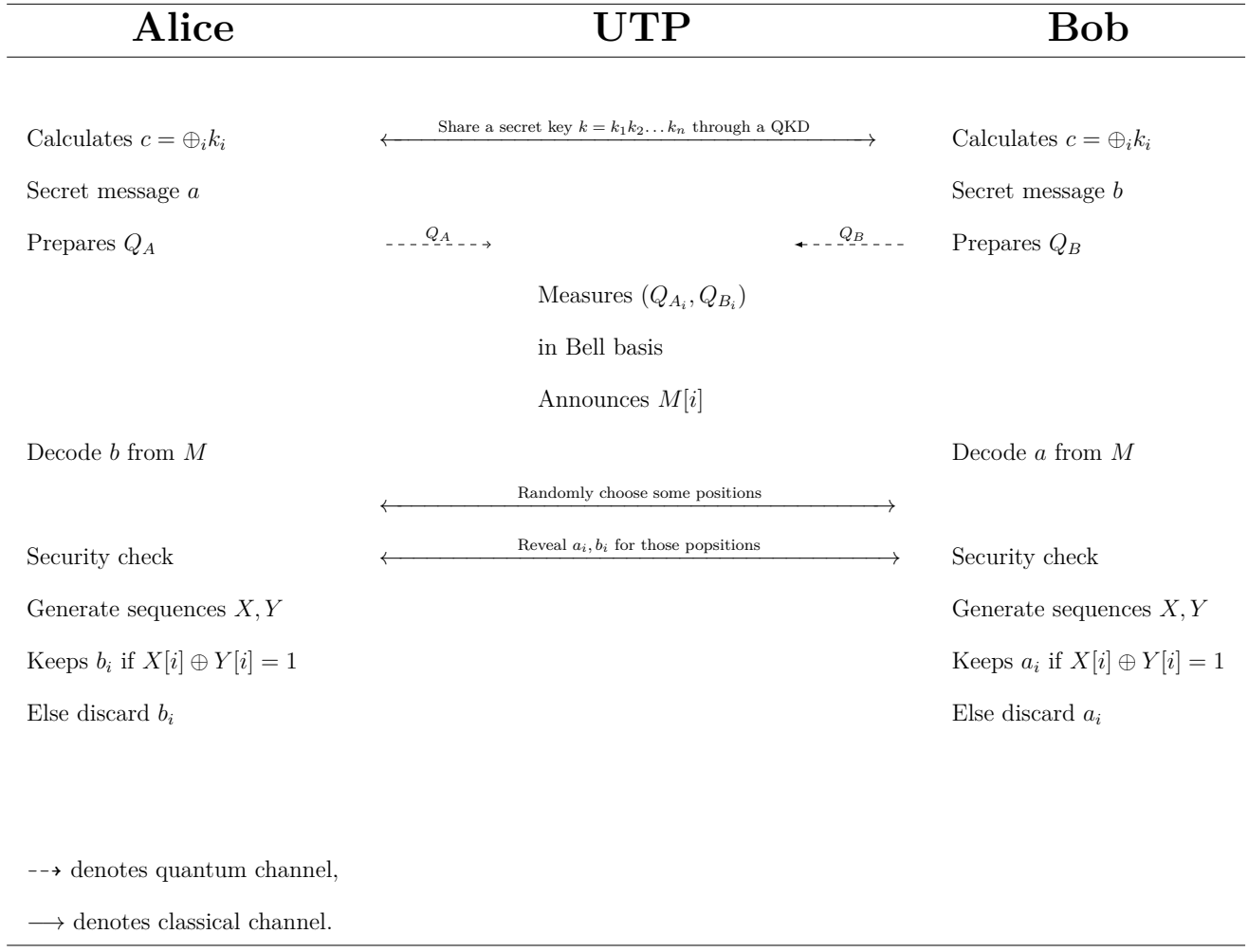


Figure 7-1: Proposed MDI-QD (first protocol)

Example 5. *Let us take an example to understand the protocol more clearly. Here we skip the error estimation phase.*

1. *Let* $k = 10011101101001010010$ *be the shared key between Alice and Bob, then* $c = \oplus k_i = 0$.

2. *Let Alice's message be* $a = 10110100111010110011$,

3. *Let Bob's message be* $b = 01101000101001101011$.

4. *Alice's encrypted message*
   $Q_A = |-\rangle\,|0\rangle\,|1\rangle\,|-\rangle\,|+\rangle\,|-\rangle\,|0\rangle\,|+\rangle\,|-\rangle\,|1\rangle\,|-\rangle\,|0\rangle\,|1\rangle\,|+\rangle\,|1\rangle\,|-\rangle\,|0\rangle\,|0\rangle\,|-\rangle\,|1\rangle$.

5. *Bob's encrypted message*
   $Q_B = |+\rangle\,|1\rangle\,|1\rangle\,|+\rangle\,|-\rangle\,|+\rangle\,|0\rangle\,|+\rangle\,|-\rangle\,|0\rangle\,|-\rangle\,|0\rangle\,|0\rangle\,|-\rangle\,|1\rangle\,|+\rangle\,|1\rangle\,|0\rangle\,|-\rangle\,|1\rangle$.

6. *Alice and Bob send their respective sequences of qubits* Q_A *and* Q_B *to the UTP and the UTP measures the two qubits (one from Alice and one from Bob) in Bell basis and announces the results.*

7. *Let* M *be the sequence*
   $|\phi^-\rangle, |\psi^+\rangle, |\phi^+\rangle, |\psi^-\rangle, |\psi^-\rangle, |\phi^-\rangle, |\phi^-\rangle, |\phi^+\rangle, |\psi^+\rangle, |\psi^-\rangle, |\phi^+\rangle, |\phi^+\rangle, |\psi^-\rangle,$
   $|\phi^-\rangle, |\phi^-\rangle, |\phi^-\rangle, |\psi^+\rangle, |\phi^-\rangle, |\phi^+\rangle, |\phi^-\rangle$

8. X *is the sequence* $1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1$.

9. Y *is the sequence* $0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0$.

10. *Then* $X \oplus Y$ *is the sequence* $1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1$.

11. *Alice and Bob consider the* i*-th message bit pair* (a_i, b_i) *if* $X[i] \oplus Y[i] = 1$. *That is, they consider* $a' = 10101010011001$ *as Alice's message and* $b' = 01010010110101$ *as Bob's message.*

7.1.2 Correctness of our proposed protocol

In our proposed protocol, Alice and Bob first prepare qubits corresponding to their messages and shared key and then send those qubits to the UTP. After that, the UTP measures each two qubit state (one from Alice and one from Bob) in Bell basis and announces the result. Now, there may arise four cases and from help of Table 2.6 we can say the followings:

- if the prepared qubit of Alice is $|0\rangle(|1\rangle)$, then Alice guesses message bit of Bob with probability 1 as follows:

$$\text{Measurement result} = \begin{cases} |\phi^+\rangle \text{ or } |\phi^-\rangle \Rightarrow & \text{message bit of Bob is 0 (1)} \\ |\psi^+\rangle \text{ or } |\psi^-\rangle \Rightarrow & \text{message bit of Bob is 1 (0)} \end{cases}$$

- if the prepared qubit of Alice is $|+\rangle(|-\rangle)$, then Alice guesses message bit of Bob with probability 1 as follows:

$$\text{Measurement result} = \begin{cases} |\phi^+\rangle \text{ or } |\psi^+\rangle \Rightarrow & \text{message bit of Bob is 0 (1)} \\ |\phi^-\rangle \text{ or } |\psi^-\rangle \Rightarrow & \text{message bit of Bob is 1 (0)} \end{cases}$$

From the above knowledge, we construct Table 2.7, which contents the information of Alice's guess about Bob's message for different cases.

Similar thing happens for Bob too. So we construct Table 2.8, which contents the information of Bob's guess about Alice's message for different cases.

From Table 2.7 and Table 2.8, we see that for all cases Alice and Bob can conclude the communicated bit of the other party with probability 1. That is, always they can guess the correct message bit of the other party with probability 1. Hence our proposed protocol is giving the correct results.

7.1.3 Security analysis of our proposed protocol

The proposed MDI-QD protocol is a modification of the MDI-QD protocol given in [3]. In their protocol they have considered only the cases where the measurement results were $|\phi^-\rangle$ or

$|\psi^+\rangle$ and discard the cases for $|\phi^+\rangle$ and $|\psi^-\rangle$. But in our protocols, we have used all the cases where the measurement results are $|\phi^-\rangle$, $|\psi^+\rangle$ and also some cases where the measurement results are $|\phi^+\rangle$, $|\psi^-\rangle$. We have done some classical computation to choose which results to take. Since in [3], the authors had done the security analysis of the protocol for the cases where the measurement results were $|\phi^-\rangle$ or $|\psi^+\rangle$, so it is sufficient for us to analyze the security of rest of the part of the protocols.

Before we proceed, let us first define the advantage of an adversary. It measures the success of an attack by an adversary on a cryptographic scheme. The advantage distinguishes the output of a cryptographic algorithm from that of a uniformly random source. If the advantage of an adversary for an algorithm is negligible, i.e., it is less than some predefined threshold value, then the algorithm is said to be secure. The word "negligible" usually means "within $O(2^{-p})$" where p is a security parameter associated with the algorithm.

Definition 1. *(Advantage): For our purpose, the advantage of an adversary A is the absolute value of the differences between the probabilities of the events A_0 and A_1, where A_0 = Guessing a random message "m" from the message space, and A_1 = Guessing the same message "m" from the message space using our algorithm. That is, $Adv(A) = |\Pr(A_0) - \Pr(A_1)|$.*

Our protocol is said to be secure if $Adv(A) < \epsilon$, where ϵ is the security parameter.

We have an n bit key $k = k_1k_2 \dots k_n$ and $c = \oplus k_i$, $1 \leq i \leq n$. Alice's n bit message is a and Bob's n bits message is b. Let there be l number of zeros in the finite sequence $\{X[q]\}_{q=1}^{n}$. The UTP knows the value of $a_j \oplus b_j$ if $X[j] = 0$ (when $X[j] = 0$, the UTP knows that the communicated bits of Alice and Bob are same or different). Let us consider the following.

- $k' = k'_1k'_2 \dots k'_l$, where $k'_i = k_j$ if $X[j]$ is i-th zero in the finite sequence $\{X[q]\}_{q=1}^{n}$.
- $e = l$ bit substring of a, where $e_i = a_j$, if $X[j]$ is the i-th zero of the sequence $\{X[q]\}_{q=1}^{n}$.
- $f = l$ bit substring of b, where $f_i = b_j$, if $X[j]$ is the i-th zero of the sequence $\{X[q]\}_{q=1}^{n}$.
- The UTP knows $e \oplus f$.

We keep the i-th $(1 \leqslant i \leqslant l)$ message pair (e_i, f_i) if $k'_i = c$ and discard the others. Let c_1 = Number of cases where $k'_i = c$, $1 \leqslant i \leqslant l$. Let us define some events first.

- E_0 = Keeping the i-th message bit pair (e_i, f_i).
- E_1 = Knowing our new message pair.
- E_2 = Guessing a random message pair (e, f) of length c_1.

So, $\Pr(E_0) = \frac{1}{2}$, $\Pr((e_i, f_i)|e_i \oplus f_i) = \frac{1}{2}$.

Thus, $\Pr(E_1) = \left(\frac{1}{2}\right)^l \left(\frac{1}{2}\right)^{c_1}$. Again, $\Pr(E_2) = \left(\frac{1}{4}\right)^{c_1}$.

Now the expected value of $c_1 = \frac{l}{2}$. Substituting this in the above expression, we get $\Pr(E_1) \approx \left(\frac{1}{2}\right)^{\frac{3l}{2}}$ and $\Pr(E_2) \approx \left(\frac{1}{4}\right)^{\frac{l}{2}}$.

Hence the advantage is, $Adv(A) = |\Pr(E_2) - \Pr(E_1)| \approx |\left(\frac{1}{4}\right)^{\frac{l}{2}} - \left(\frac{1}{2}\right)^{\frac{3l}{2}}| = \left(\frac{1}{2}\right)^l \left[1 - \left(\frac{1}{2}\right)^{\frac{l}{2}}\right]$.

Now $Adv(A) < \epsilon$

$\Leftrightarrow \left(\frac{1}{2}\right)^l \left[1 - \left(\frac{1}{2}\right)^{\frac{l}{2}}\right] < \epsilon$

$\Rightarrow \left(\frac{1}{2}\right)^{\frac{3l}{2}} \leqslant \left(\frac{1}{2}\right)^l \left[1 - \left(\frac{1}{2}\right)^{\frac{l}{2}}\right] < \epsilon$ (assuming that $\left(\frac{1}{2}\right)^{\frac{l}{2}} < 1 - \left(\frac{1}{2}\right)^{\frac{l}{2}} \Leftrightarrow \left(\frac{1}{2}\right)^{\frac{l}{2}-1} < 1 \Leftrightarrow \frac{l}{2} - 1 > 0 \Leftrightarrow l > 2$.)

$\Rightarrow \left(\frac{1}{2}\right)^{\frac{3l}{2}} < \epsilon \Leftrightarrow -\frac{3l}{2} < log(\epsilon) \Leftrightarrow l > \frac{2}{3} log(\frac{1}{\epsilon})$.

So for a predefined security parameter ϵ, if $l >$max$\{2, \frac{2}{3} log(\frac{1}{\epsilon})\}$, then $Adv(A) < \epsilon$, i.e., our protocol is secure. We can also adjust the value of l by padding some random message bits.

7.2 Our second efficient MDI-QD protocol

After the error estimation phase, let the number of remaining measurement results be n', Alice and Bob make a finite sequence $\{M[i]\}_{i=1}^{n'}$ containing the measurement results. i.e., $M[i]$ is the i-th measurement result announced by the UTP, for $1 \leqslant i \leqslant n'$ and $M[i] \in \{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$. They keep all the measurement results $M[i]$s where $M[i] \in \{|\phi^-\rangle, |\psi^+\rangle\}$. Among the remaining measurement results, they choose some to keep and discard other.

To choose the measurement results for Alice's message, they will do the following:
for $1 \leq i \leq n'$, if $M[i] \in \{|\phi^+\rangle, |\psi^-\rangle\}$ and $k_i = c$, then Alice and Bob keep that $M[i]$. Else they discard that $M[i]$. Using Table 2.8, Bob guesses the message bit of Alice corresponding to all the measurement results $M[i]$ which they kept.

To choose the measurement results for Bob's message, they will do the following:
for $1 \leq i \leq n'$, if $M[i] \in \{|\phi^+\rangle, |\psi^-\rangle\}$ and $k_i = \bar{c}$, then Alice and Bob keep that $M[i]$. Else

they discard that $M[i]$. Using Table 2.7, Alice guesses the message bit of Bob corresponding to all the measurement results $M[i]$ which they kept. In this case the length of final messages of Alice and Bob may differ. Details are given in the following section.

7.2.1 Proposed protocol

1. Alice and Bob share a n-bit key stream ($k = k_1 k_2 \dots k_n$) between themselves using BB84 protocol.

2. They calculate $c = \oplus k_i$, $1 \leq i \leq n$.

3. Let n bit message of Alice and Bob be $a = a_1 a_2 \dots a_n$ and $b = b_1 b_2 \dots b_n$ respectively.

4. For $1 \leq i \leq n$, Alice (Bob) prepares the qubits Q_A (Q_B) at her (his) end according to the following strategy:

   (a) if a_i (b_i)$= 0$ and $k_i = 0$, set Q_{A_i} (Q_{B_i}) $= |0\rangle$;

   (b) if a_i (b_i)$= 1$ and $k_i = 0$, set Q_{A_i} (Q_{B_i}) $= |1\rangle$;

   (c) if a_i (b_i)$= 0$ and $k_i = 1$, set Q_{A_i} (Q_{B_i}) $= |+\rangle$;

   (d) if a_i (b_i)$= 1$ and $k_i = 1$, set Q_{A_i} (Q_{B_i}) $= |-\rangle$.

5. Alice (Bob) sends Q_A (Q_B) to the third party (TP).

6. For $1 \leq i \leq n$, the UTP measures the two qubits Q_{A_i} and Q_{B_i} in Bell basis and announces the result.

7. Alice and Bob make a finite sequence $\{M[i]\}_{i=1}^{n}$ containing the measurement results, i.e., for $1 \leqslant i \leqslant n$, $M[i]$ is the i-th measurement result announced by the UTP, where $M[i] \in \{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$.

8. They randomly choose γn number of measurement results $M[i]$ from the sequence $\{M[i]\}_{i=1}^{n}$ to estimate the error, where $\gamma < 1$ is a small fraction.

9. Alice and Bob guess the message bit of other, corresponding to their chosen γn number of measurement results using Table 2.7 and Table 2.8.

10. They reveal their respective guesses for these rounds.

11. If estimated error is greater than some predefined threshold value, then they abort. Else continue and goto next step.

12. Their remaining sequence of measurement results is relabeled as $\{M[i]\}_{i=1}^{n'}$, where $n' = (1-\gamma)n$.

13. They update their n-bit key to an n'-bit key by discarding γn number of key bits corresponding to above γn rounds. The updated key is relabeled as $k = k_1 k_2 \dots k_{n'}$.

14. They generate a finite sequence $\{X[i]\}_{i=1}^{n'}$ such that

$$X[i] = \begin{cases} 1, & \text{if } M_i = |\phi^-\rangle \text{ or } |\psi^+\rangle; \\ 0, & \text{otherwise.} \end{cases}$$

15. Then they generate another two finite sequence $\{Y[i]\}_{i=1}^{n'}$ and $\{Z[i]\}_{i=1}^{n'}$ such that

$$Y[i] = \begin{cases} 0, & \text{if } X[i] = 1; \\ k_j, & \text{if } c = 1 \text{ and } X[i] \text{ is the } j\text{-th zero of the sequence } \{X[q]\}_{q=1}^{n'}; \\ \bar{k_j}, & \text{if } c = 0 \text{ and } X[i] \text{ is the } j\text{-th zero of the sequence } \{X[q]\}_{q=1}^{n'}. \end{cases}$$

$$Z[i] = \begin{cases} 0, & \text{if } X[i] = 1; \\ k_j, & \text{if } c = 0 \text{ and } X[i] \text{ is the } j\text{-th zero of the sequence } \{X[q]\}_{q=1}^{n'}; \\ \bar{k_j}, & \text{if } c = 1 \text{ and } X[i] \text{ is the } j\text{-th zero of the sequence } \{X[q]\}_{q=1}^{n'}. \end{cases}$$

16. For Alice's message ($1 \leq i \leq n'$):

    - if $X[i] \oplus Y[i] = 1$, then Alice and Bob consider the i-th measurement result $M[i]$. Bob guesses Alice's message bit a_i using Table 2.8.
    - Else they discard $M[i]$.

17. For Bob's message ($1 \leq i \leq n'$):

- if $X[i] \oplus Z[i] = 1$, then Alice and Bob consider the i-th measurement result $M[i]$. Alice guesses Bob's message bit b_i using Table 2.7
- Else they discard $M[i]$.

This completes the protocol.

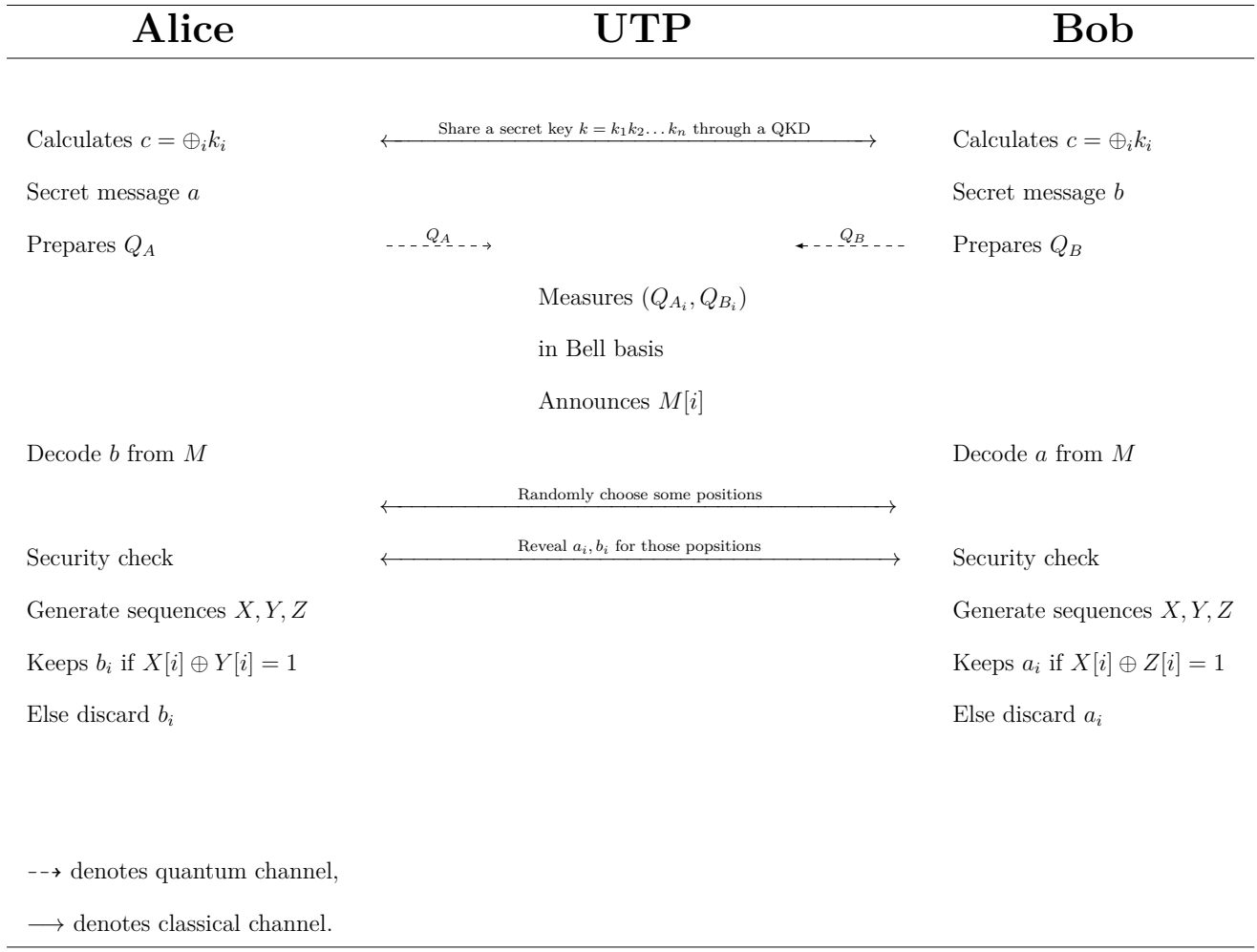


Figure 7-2: Proposed MDI-QD (second protocol)

Example 6. *Let us take an example to understand our protocol more clearly. Here we skip the error estimation phase.*

1. *Let* $k = 10011101101001010010$ *be the shared key between Alice and Bob, then* $c = \oplus k_i = 0$.

2. *Let Alice's message be* $a = 10110100111010110011$,

3. *Let Bob's message be* $b = 01101000101001101011$.

4. *Alice's encrypted message*
   $Q_A = |-\rangle\,|0\rangle\,|1\rangle\,|-\rangle\,|+\rangle\,|-\rangle\,|0\rangle\,|+\rangle\,|-\rangle\,|1\rangle\,|-\rangle\,|0\rangle\,|1\rangle\,|+\rangle\,|1\rangle\,|-\rangle\,|0\rangle\,|0\rangle\,|-\rangle\,|1\rangle$.

5. *Bob's encrypted message*
   $Q_B = |+\rangle\,|1\rangle\,|1\rangle\,|+\rangle\,|-\rangle\,|+\rangle\,|0\rangle\,|+\rangle\,|-\rangle\,|0\rangle\,|-\rangle\,|0\rangle\,|0\rangle\,|-\rangle\,|1\rangle\,|+\rangle\,|1\rangle\,|0\rangle\,|-\rangle\,|1\rangle$.

6. *Alice and Bob send their respective sequences of qubits* Q_A *and* Q_B *to the UTP and the UTP measures the two qubits (one from Alice and one from Bob) in Bell basis and announces the results.*

7. *Let* M *be the sequence*
   $|\phi^-\rangle, |\psi^+\rangle, |\phi^+\rangle, |\psi^-\rangle, |\psi^-\rangle, |\phi^-\rangle, |\phi^-\rangle, |\phi^+\rangle, |\psi^+\rangle, |\psi^-\rangle, |\phi^+\rangle, |\phi^+\rangle, |\psi^-\rangle,$
   $|\phi^-\rangle, |\phi^-\rangle, |\phi^-\rangle, |\psi^+\rangle, |\phi^-\rangle, |\phi^+\rangle, |\phi^-\rangle$

8. X *is the sequence* $1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1$.

9. Y *is the sequence* $0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0$.

10. Z *is the sequence* $0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0$.

11. *Then* $X \oplus Y$ *is the sequence* $1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1$ *and*

12. $X \oplus Z$ *is the sequence* $1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1$.

13. *For Alice's message, Alice and Bob consider the* i*-th* ($1 \leq i \leq 20$) *measurement result* $M[i]$ *only when* $X[i] \oplus Y[i] = 1$ *and discard other cases. That is, they consider* $a' = 10101010011001$ *as Alice's message.*

14. *For Bob's message, Alice and Bob consider the* i*-th* ($1 \leq i \leq 20$) *measurement result* $M[i]$ *only when* $X[i] \oplus Z[i] = 1$ *and discard other cases. That is, they consider* $b' = 01100010101101011$ *as Bob's message.*

7.2.2 Correctness of our proposed protocol

Using the similar argument as the first protocol in Section 7.1.2, we can say that our second protocol also gives the correct results.

7.2.3 Security analysis of our proposed protocol

Our protocol is said to be secure if $Adv(A) < \epsilon$, where ϵ is the security parameter.

We have an n bit key $k = k_1k_2 \dots k_n$ and $c = \oplus k_i$, $1 \leq i \leq n$. Alice's n bit message is a and Bob's n bits message is b. Let there be l number of zeros in the finite sequence $\{X[q]\}_{q=1}^{n}$. The UTP knows the value of $a_j \oplus b_j$ if $X[j] = 0$ (when $X[j] = 0$, the UTP knows that the communicated bits of Alice and Bob are same or different). Let us consider the following.

- $k' = k'_1k'_2 \dots k'_l$, where $k'_i = k_j$ if $X[j]$ is i-th zero in the finite sequence $\{X[q]\}_{q=1}^{n}$.
- $e = l$ bit substring of a, where $e_i = a_j$, if $X[j]$ is the i-th zero of the sequence $\{X[q]\}_{q=1}^{n}$.
- $f = l$ bit substring of b, where $f_i = b_j$, if $X[j]$ is the i-th zero of the sequence $\{X[q]\}_{q=1}^{n}$.
- The UTP knows $e \oplus f$.

In our second protocol, we keep the i-th bit of Alice's message e_i if $k'_i = c$, the i-th bit of Bob's message f_i if $k'_i = \bar{c}$, $1 \leqslant i \leqslant l$ and discard the rest.

Let c_1 = Number of cases where $k'_i = c$, $1 \leqslant i \leqslant l$. Let us define some events first.

- E_0 = Keeping e_i, the i-th message bit of Alice.
- E_1 = Keeping f_i, the i-th message bit of Bob.
- E_2 = Knowing Alice's and Bob's new message e' and f' respectively.
- E_4 = Guessing two random message e and f of length c_1 and $l - c_1$ respectively.

So, $\Pr(E_0) = \frac{1}{2}$ and $\Pr(E_1) = \frac{1}{2}$.

Using the expectation of c_1 calculated earlier, we have $\Pr(E_3) = \left(\frac{1}{2}\right)^{l} \left(\frac{1}{2}\right)^{c_1} \left(\frac{1}{2}\right)^{l-c_1} \approx \left(\frac{1}{2}\right)^{2l}$. Again, $\Pr(E_4) = \left(\frac{1}{2}\right)^{c_1} \left(\frac{1}{2}\right)^{l-c_1} \approx \left(\frac{1}{2}\right)^{l}$.

Thus, the advantage of the UTP is, $Adv(A) = |\Pr(E_4) - \Pr(E_3)| \approx |\left(\frac{1}{2}\right)^l - \left(\frac{1}{2}\right)^{2l}| = \left(\frac{1}{2}\right)^l \left[1 - \left(\frac{1}{2}\right)^l\right]$.

Now $Adv(A) < \epsilon$

$\Leftrightarrow \left(\frac{1}{2}\right)^l \left[1 - \left(\frac{1}{2}\right)^l\right] < \epsilon$

$\Rightarrow \left(\frac{1}{2}\right)^{2l} < \left(\frac{1}{2}\right)^l \left[1 - \left(\frac{1}{2}\right)^l\right] < \epsilon$ (assuming that $\left(\frac{1}{2}\right)^l < 1 - \left(\frac{1}{2}\right)^l \Leftrightarrow \left(\frac{1}{2}\right)^{l-1} < 1 \Leftrightarrow l > 1$.)

$\Rightarrow \left(\frac{1}{2}\right)^{2l} < \epsilon \Leftrightarrow -2l < log(\epsilon) \Leftrightarrow l > \frac{1}{2} log(\frac{1}{\epsilon})$.

So for a predefined security parameter ϵ, if $l >$max$\{1, \frac{1}{2} log(\frac{1}{\epsilon})\}$, then $Adv(A) < \epsilon$, i.e., our protocol is secure. We can also adjust the value of l by padding some random message bits.

7.2.4 Difference with the first protocol

Both of our proposed protocols for quantum dialogue are modifications of the quantum dialogue protocol given in [3]. In these protocols, the UTP measures each two qubit state (one from Alice and one from Bob) in Bell basis and announces the result. Alice and Bob make a finite sequence $\{M[i]\}_{i=1}^{n}$ containing the measurement results. That is, $M[i]$ is the i-th ($1 \leqslant i \leqslant n$) measurement result announced by the UTP and $M[i] \in \{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$. After the error estimation phase, the remaining sequence of measurement results is relabeled as $\{M[i]\}_{i=1}^{n'}$. For $1 \leqslant i \leqslant n$, if $M[i] \in \{|\phi^-\rangle, |\psi^+\rangle\}$, then we keep those results for both the protocols. But if $M[i] \in \{|\phi^+\rangle, |\psi^-\rangle\}$, then we use some technique to decide whether we keep those results or discard them.

The basic difference between our two protocols is the technique of choosing $M[i]$ when $M[i] = |\phi^+\rangle$ or $|\psi^-\rangle$, $1 \leq i \leq n'$. From our first protocol, we get a synchronized message pair of Alice and Bob. Here by synchronized message, we mean that if we keep the i-th message bit of Alice, then we also keep the i-th message bit of Bob. For this protocol, we consider the i-th message bit pair (a_i, b_i), if $X[i] \oplus Y[i] = 1$ holds ($1 \leq i \leq n'$), where $\{X[i]\}_{i=1}^{n'}$ and $\{Y[i]\}_{i=1}^{n'}$ are defined in Algorithm 1.

But for the second protocol, we do not get any synchronized message pair of Alice and Bob. In this protocol, if $M[i] = |\phi^+\rangle$ or $|\psi^-\rangle$, then, for some cases we keep the corresponding message bit of Alice and discard Bob's message bit, or the converse. For $1 \leq i \leq n'$, the condition for keeping Alice's message bit a_i is $X[i] \oplus Y[i] = 1$, i.e., when $X[i] \oplus Y[i] = 1$, we

keep a_i and discard b_i. Also for $1 \leq i \leq n'$, the condition for keeping Bob's message bit b_i is $X[i] \oplus Z[i] = 1$, i.e., when $X[i] \oplus Z[i] = 1$, we keep b_i and discard a_i, where $\{X[i]\}_{i=1}^{n'}$, $\{Y[i]\}_{i=1}^{n'}$ and $\{Z[i]\}_{i=1}^{n'}$ are defined in Algorithm 2.

So for each i, we are keeping a_i or b_i or both. The performance of our second protocol is better, when $c_1 < \frac{l}{2}$ (these are defined in Section 7.1.3). In that case, we can keep more message bits using our second protocol than the first one. One may note that synchronization is not an issue if only message transmission is considered. But if Alice and Bob use the synchronized messages to define something else, then our second protocol cannot be used (as the length of their final message may differ from each other). For this case, they have to use our first protocol.

7.3 Discussion

In this chapter, we propose two protocols for quantum dialogue such that two legitimate parties Alice and Bob can securely communicate their messages simultaneously. Both of our proposed protocols are modifications of MDI-QD [3] protocol. In their protocol they have used only half of the qubits. But in our protocols we have used almost three fourth of the qubits. So our protocols are more efficient than the previous one in terms of number of qubits. We show that our QD protocols are secure as advantages of adversary are negligible for both the cases. Also we have discussed about the difference between our two protocols.

Chapter 8

Analysis and Design of Quantum Conference Protocols

Quantum conference is a process of securely exchanging messages between three or more parties, using quantum resources. In this chapter, we first generalize the MDI-QD protocol [3] to a three-party Q.Conf protocol with the help of an untrusted fourth party. Next, we generalize our three-party Q.Conf protocol to a multi-party version. We show that both these conference protocols are correct and secure against intercept-and-resend attack, entangle-and-measure attack, DoS attack and man-in-the-middle attack. As the fourth and final contribution, we show how to use part of our multi-party Q.Conf protocol to compute multi-party XOR function, and establish it's correctness and security. None of these three protocols proposed here use entanglement as a resource and we prove the correctness and security of our proposed protocols [282].

Before describing our protocol, let us first define the basis $\mathcal{B}_N$ for the Hilbert space $\mathbb{C}^N$.

$$\mathcal{B}_N = \{|\Phi_0^+\rangle, |\Phi_0^-\rangle, |\Phi_1^+\rangle, |\Phi_1^-\rangle, \ldots, |\Phi_{2^{(N-1)}-1}^+\rangle, |\Phi_{2^{(N-1)}-1}^-\rangle\},$$

where $|\Phi_i^{\pm}\rangle = \frac{1}{\sqrt{2}}(|i\rangle \pm |2^N - 1 - i\rangle)$ for $i \in \{0, 1, \ldots, 2^{(N-1)} - 1\}$. For example :

1. $\mathcal{B}_2 = \{|\Phi_0^+\rangle, |\Phi_0^-\rangle, |\Phi_1^+\rangle, |\Phi_1^-\rangle\}$ is called Bell basis; where

   - $|\Phi_0^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\Phi^+\rangle$, $|\Phi_0^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = |\Phi^-\rangle$

- $|\Phi_1^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = |\Psi^+\rangle$, $|\Phi_1^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = |\Psi^-\rangle$

2. $\mathcal{B}_3 = \{|\Phi_0^+\rangle, |\Phi_0^-\rangle, |\Phi_1^+\rangle, |\Phi_1^-\rangle, |\Phi_2^+\rangle, |\Phi_2^-\rangle, |\Phi_3^+\rangle, |\Phi_3^-\rangle\}$ basis; where

- $|\Phi_0^+\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$, $|\Phi_0^-\rangle = \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)$
- $|\Phi_1^+\rangle = \frac{1}{\sqrt{2}}(|001\rangle + |110\rangle)$, $|\Phi_1^-\rangle = \frac{1}{\sqrt{2}}(|001\rangle - |110\rangle)$
- $|\Phi_2^+\rangle = \frac{1}{\sqrt{2}}(|010\rangle + |101\rangle)$, $|\Phi_2^-\rangle = \frac{1}{\sqrt{2}}(|010\rangle - |101\rangle)$
- $|\Phi_3^+\rangle = \frac{1}{\sqrt{2}}(|011\rangle + |100\rangle)$, $|\Phi_3^-\rangle = \frac{1}{\sqrt{2}}(|011\rangle - |100\rangle)$;

8.1 Three party Q.Conf

We extend the QD protocol of [3] from two to three parties, thus leading to a protocol of Q.Conf. Our proposed conference protocol is divided into two parts. Let Alice, Bob and Charlie be three participants of the conference. Also let Alice's, Bob's and Charlie's m bit messages be a, b and c respectively, where $a = a_1a_2 \dots a_m$, $b = b_1b_2 \dots b_m$ and $c = c_1c_2 \dots c_m$.

In the first part, Alice, Bob, and Charlie perform a Multi-party QKD protocol [189] to establish a secret key $k = k_1k_2 \dots k_m$ of m bits between themselves. Then each of them uses the key to encode one's own message M into the corresponding state Q, according to Subroutine 1. The details of the three party Q.Conf protocol are given in Protocol 1.

Subroutine 1 Message Encoding Strategy for Three Party Q.Conf

Inputs: Own message $M = M_1M_2 \dots M_m$; key $k = k_1k_2 \dots k_m$.

Output: Sequence of qubits $Q = Q_1Q_2 \dots Q_m$.

The subroutine:

For $1 \leqslant i \leqslant m$,

1. if $M_i = 0$ and $k_i = 0$, prepares $Q_i = |0\rangle$.
2. if $M_i = 1$ and $k_i = 0$, prepares $Q_i = |1\rangle$.
3. if $M_i = 0$ and $k_i = 1$, prepares $Q_i = |+\rangle$.
4. if $M_i = 1$ and $k_i = 1$, prepares $Q_i = |-\rangle$.

8.1.1 Protocol 1: Three party Q.Conf

The steps of the protocol is as follows:

1. Alice, Bob and Charlie perform any multi-party QKD protocol (e.g., [189]) to establish an m-bit secret key $k = k_1k_2 \dots k_m$ between themselves.

2. Let the m-bit messages of Alice, Bob and Charlie be a, b and c respectively, where $a = a_1a_2 \dots a_m$, $b = b_1b_2 \dots b_m$ and $c = c_1c_2 \dots c_m$.

3. For $1 \leqslant i \leqslant m$, Alice, Bob and Charlie prepare the sequences of qubits $Q_A = \{Q_A[i]\}_{i=1}^m = (Q_{A1}, Q_{A2}, \dots, Q_{Am}), Q_B = \{Q_B[i]\}_{i=1}^m = (Q_{B1}, Q_{B2}, \dots, Q_{Bm})$ and $Q_C = \{Q_C[i]\}_{i=1}^m = (Q_{C1}, Q_{C2}, \dots, Q_{Cm})$ respectively at their end by using Subroutine 1.

4. Alice, Bob, and Charlie choose some random permutation and apply those on their respective sequences of qubits Q_A, Q_B, and Q_C and get new sequences of qubits q_A, q_B and q_C.

5. They send the prepared sequences of qubits q_A, q_B, and q_C to an untrusted fourth party (UFP).

6. Alice, Bob, and Charlie randomly choose δm number of common positions on sequences Q_A, Q_B and Q_C to estimate the error in the channel, where $\delta \ll 1$ is a small fraction. Corresponding to these δm rounds, they do the following:

   (a) Each participant tells the positions and preparation bases of those qubits for those rounds to the UFP.

   (b) The UFP measures each single-qubit state in proper basis and announces the results.

   (c) They reveal their respective qubits for these rounds and compare them with the results announced by the UFP.

   (d) If the estimated error is greater than some predefined threshold value, then they abort. Else they continue and go to the next step.

7. The UFP asks Alice, Bob, and Charlie to tell the permutations which they have applied to their sequences.

8. The UFP applies the inverse permutations, corresponding to the permutations chosen by Alice, Bob, and Charlie, on q_A, q_B, and q_C to get Q_A, Q_B and Q_C respectively.

9. They discard the qubits corresponding to the above δm positions. Their remaining sequence of prepared qubits are relabeled as $Q_A = \{Q_A[i]\}_{i=1}^{m'}$, $Q_B = \{Q_B[i]\}_{i=1}^{m'}$ and $Q_C = \{Q_C[i]\}_{i=1}^{m'}$, where $m' = (1-\delta)m$.

10. They update their m-bit key to an m'-bit key by discarding δm number of key bits corresponding to the above δm rounds. The updated key is relabeled as $k = k_1 k_2 \dots k_{m'}$.

11. For $1 \leqslant i \leqslant m'$, the UFP measures the each three qubits state $(Q_{A_i}, Q_{B_i}, Q_{C_i})$ in basis $\mathcal{B}_3$ and announces the result.

12. Alice, Bob and Charlie make a finite sequence $\{\mathcal{M}[i]\}_{i=1}^{m'}$ containing the measurement results, i.e., for $1 \leqslant i \leqslant m'$, $\mathcal{M}[i] \in \{|\Phi_0^+\rangle, |\Phi_0^-\rangle, |\Phi_1^+\rangle, |\Phi_1^-\rangle, |\Phi_2^+\rangle, |\Phi_2^-\rangle, |\Phi_3^+\rangle, |\Phi_3^-\rangle\}$ is the i-th measurement result announced by the UFP .

13. They randomly choose $\gamma m'$ number of measurement results $\mathcal{M}[i]$ from the sequence $\{\mathcal{M}[i]\}_{i=1}^{m'}$ to estimate the error (may be introduced by the UFP), where $\gamma \ll 1$ is a small fraction.

    (a) They reveal their respective message bits for these rounds.

    (b) If the estimated error is greater than some predefined threshold value, then they abort. Else they continue and go to the next step.

14. Their remaining sequence of measurement results is relabeled as $\{\mathcal{M}[i]\}_{i=1}^{n}$, where $n = (1-\gamma)m'$.

15. They update their m'-bit key to an n-bit key by discarding $\gamma m'$ number of key bits corresponding to the above $\gamma m'$ rounds. The updated key is relabeled as $k = k_1 k_2 \dots k_n$.

16. Each of Alice, Bob, and Charlie applies Algorithm 4 to get others' messages.

Note that in this protocol, there are two error estimation phases. The first one checks if there is any adversary (other than the UFP) in the channel who tries to get some information about the messages or change the messages. In this case, if the 1st error estimation phase does not pass, then Alice, Bob, and Charlie abort the protocol. Thus, in this step, the motivation of the UFP being correct is that there is no information gain for him/her if the parties abort the protocol. The next error estimation phase is to check if there is any error introduced by the UFP .

8.1.2 Correctness of three party Q.Conf protocol

In our proposed protocol, Alice, Bob and Charlie first prepare qubits corresponding to their messages and shared key and then send those qubits to the fourth party (UFP). After that, UFP measures each of the three qubits state (one from Alice, one from Bob and one from Charlie) in basis $\mathcal{B}_3 = \{|\Phi_0^+\rangle, |\Phi_0^-\rangle, |\Phi_1^+\rangle, |\Phi_1^-\rangle, |\Phi_2^+\rangle, |\Phi_2^-\rangle, |\Phi_3^+\rangle, |\Phi_3^-\rangle\}$ and announces the result. Now, we can say the following from Table 8.1:

- If the prepared qubit of Alice is $|0\rangle(|1\rangle)$, then Alice guesses message bit of Bob and

Algorithm 4: Three Party Message Reconstruction Algorithm.

Input: Own message , measurement results $\{\mathcal{M}[i]\}_{i=1}^{n}$, key k.
Output: Others' messages.

1. For $1 \leqslant i \leqslant n$, if $k_i = 0$, then each participant can learn the i-th bit of others' messages from the measurement result $\mathcal{M}[i]$ and their own message (see Table-8.1).

2. For $1 \leqslant i \leqslant n$, if $k_i = 1$, then from the measurement result $\mathcal{M}[i]$ and their own message each participant can learn the i-th bit of others messages are same or different (see Table-8.1). Let $c = wt(k)$.

   (a) Alice, Bob and Charlie prepare ordered sets of qubits S_A, S_B and S_C respectively, corresponding to their message bit where the key bit is 1. They prepare the qubits at their end according to the following strategy. Each of S_A, S_B and S_C contain c number of qubits. For $1 \leqslant j \leqslant c$ and if $k_i = 1$ is the j-th 1 in k, then

   - if a_i (b_i, c_i)= 0 and i is even, prepares $S_A[j]$ $(S_B[j],\ S_C[j])\ = |0\rangle$.
   - if a_i (b_i, c_i)= 1 and i is even, prepares $S_A[j]$ $(S_B[j],\ S_C[j])\ = |1\rangle$.
   - if a_i (b_i, c_i)= 0 and i is odd, prepares $S_A[j]$ $(S_B[j],\ S_C[j])\ = |+\rangle$.
   - if a_i (b_i, c_i)= 1 and i is odd, prepares $S_A[j]$ $(S_B[j],\ S_C[j])\ = |-\rangle$.

   (b) Alice, Bob and Charlie prepare sets of d decoy photons D_A, D_B and D_C respectively, where the decoy photons are randomly chosen from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. They randomly insert their decoy photons into their prepared qubits sets and make new ordered sets S'_A, S'_B and S'_C. They also choose random permutations R_A, R_B, R_C and apply those on their respective sets S'_A, S'_B, S'_C to get the sets S''_A, S''_B, S''_C respectively.

   (c) Each of them sends its set to the next participant in a circular way. That is, Alice sends S''_A to Bob, who sends S''_B to Charlie, who in turn sends S''_C to Alice.

   (d) After receiving the qubits from the previous participant, each of them announces the random permutations and the positions, states of their decoy photons.

   (e) They apply the inverse permutations and verify the decoy photons to check eavesdropping. If there exists any eavesdropper in the quantum channel, they abort the protocol, else they go to the next step.

   (f) Now everyone knows the basis of the qubits of S_A, S_B and S_C. So they can measure those qubits to get the exact message bits of the previous participant from whom they got those qubits.

Table 8.1: Different cases in the three party Q.Conf.

Bits to Communicate			Qubits prepared by			Probabilities of measurement results $\mathcal{M}[i]$ at UFP's end							
Alice	Bob	Charlie	Alice (Q_{Ai})	Bob (Q_{Bi})	Charlie (Q_{Ci})	$\|\Phi_0^+\rangle$	$\|\Phi_0^-\rangle$	$\|\Phi_1^+\rangle$	$\|\Phi_1^-\rangle$	$\|\Phi_2^+\rangle$	$\|\Phi_2^-\rangle$	$\|\Phi_3^+\rangle$	$\|\Phi_3^-\rangle$
0	0	0	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	1/2	1/2	0	0	0	0	0	0
0	0	1	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	0	0	1/2	1/2	0	0	0	0
0	1	0	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	0	0	0	0	1/2	1/2	0	0
0	1	1	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	0	0	0	0	0	0	1/2	1/2
1	0	0	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	0	0	0	0	0	0	1/2	1/2
1	0	1	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	0	0	0	0	1/2	1/2	0	0
1	1	0	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	0	0	1/2	1/2	0	0	0	0
1	1	1	$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	1/2	1/2	0	0	0	0	0	0
0	0	0	$\|+\rangle$	$\|+\rangle$	$\|+\rangle$	1/4	0	1/4	0	1/4	0	1/4	0
0	0	1	$\|+\rangle$	$\|+\rangle$	$\|-\rangle$	0	1/4	0	1/4	0	1/4	0	1/4
0	1	0	$\|+\rangle$	$\|-\rangle$	$\|+\rangle$	0	1/4	0	1/4	0	1/4	0	1/4
0	1	1	$\|+\rangle$	$\|-\rangle$	$\|-\rangle$	1/4	0	1/4	0	1/4	0	1/4	0
1	0	0	$\|-\rangle$	$\|+\rangle$	$\|+\rangle$	0	1/4	0	1/4	0	1/4	0	1/4
1	0	1	$\|-\rangle$	$\|+\rangle$	$\|-\rangle$	1/4	0	1/4	0	1/4	0	1/4	0
1	1	0	$\|-\rangle$	$\|-\rangle$	$\|+\rangle$	1/4	0	1/4	0	1/4	0	1/4	0
1	1	1	$\|-\rangle$	$\|-\rangle$	$\|-\rangle$	0	1/4	0	1/4	0	1/4	0	1/4

Charlie (b_i and c_i) with probability 1 as follows:

$$\text{Measurement result} = \begin{cases} |\Phi_0^+\rangle \text{ or } |\Phi_0^-\rangle \Rightarrow & b_i = 0(1) \text{ and } c_i = 0(1); \\ |\Phi_1^+\rangle \text{ or } |\Phi_1^-\rangle \Rightarrow & b_i = 0(1) \text{ and } c_i = 1(0); \\ |\Phi_2^+\rangle \text{ or } |\Phi_2^-\rangle \Rightarrow & b_i = 1(0) \text{ and } c_i = 0(1); \\ |\Phi_3^+\rangle \text{ or } |\Phi_3^-\rangle \Rightarrow & b_i = 1(0) \text{ and } c_i = 1(0). \end{cases}$$

- If the prepared qubit of Alice is $|+\rangle(|-\rangle)$, then Alice guesses the XOR function of message bits of Bob and Charlie with probability 1 as follows:

$$\text{Measurement result} = \begin{cases} |\Phi_0^+\rangle \text{ or } |\Phi_1^+\rangle \text{ or } |\Phi_2^+\rangle \text{ or } |\Phi_3^+\rangle \Rightarrow & b_i \oplus c_i = 0(1); \\ |\Phi_0^-\rangle \text{ or } |\Phi_1^-\rangle \text{ or } |\Phi_2^-\rangle \text{ or } |\Phi_3^-\rangle \Rightarrow & b_i \oplus c_i = 1(0). \end{cases}$$

  In this case, Charlie sends her encoded qubit to Alice (the encoding process is given in Step 2a of Algorithm 4). Since Alice knows the basis of the received qubit from Charlie, by measuring the qubit in the proper basis, Alice can know the message bit c_i of Charlie. Then from $b_i \oplus c_i$, she can get b_i also.

A similar thing happens for Bob and Charlie too. From the above discussion, we see that for all the cases Alice, Bob, and Charlie can conclude the communicated bit of the other parties with probability 1. Hence our protocol is giving the correct result.

8.1.3 Security analysis of the three party Q.Conf protocol

In this section, we discuss the security of our proposed three-party Q.Conf protocol against the common known attacks which $\mathcal{A}$ can adopt. If there exists some adversary in the channel and the legitimate parties can detect her with a non-negligible probability, then we call our protocol as secure. We assume that $\mathcal{A}$ has infinite resources and unbounded computation power.

We first show that if the UFP does some cheating, it can be detected by the players at the error estimation phase of the protocol (Step 13 of Protocol 1). Let UFP measure each

Table 8.2: Different cases when UFP is dishonest in the three party Q.Conf.

UFP choses	UFP's measurement results			Probability that UFP guesses $\mathcal{M}'[i]$							
measurement basis	Alice (Q_{A_i}')	Bob (Q_{B_i}')	Charlie (Q_{C_i}')	$\|\Phi_0^+\rangle$	$\|\Phi_0^-\rangle$	$\|\Phi_1^+\rangle$	$\|\Phi_1^-\rangle$	$\|\Phi_2^+\rangle$	$\|\Phi_2^-\rangle$	$\|\Phi_3^+\rangle$	$\|\Phi_3^-\rangle$
Z	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	1/2	1/2	0	0	0	0	0	0
	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	0	0	1/2	1/2	0	0	0	0
	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	0	0	0	0	1/2	1/2	0	0
	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	0	0	0	0	0	0	1/2	1/2
	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	0	0	0	0	0	0	1/2	1/2
	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	0	0	0	0	1/2	1/2	0	0
	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	0	0	1/2	1/2	0	0	0	0
	$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	1/2	1/2	0	0	0	0	0	0
X	$\|+\rangle$	$\|+\rangle$	$\|+\rangle$	1/4	0	1/4	0	1/4	0	1/4	0
	$\|+\rangle$	$\|+\rangle$	$\|-\rangle$	0	1/4	0	1/4	0	1/4	0	1/4
	$\|+\rangle$	$\|-\rangle$	$\|+\rangle$	0	1/4	0	1/4	0	1/4	0	1/4
	$\|+\rangle$	$\|-\rangle$	$\|-\rangle$	1/4	0	1/4	0	1/4	0	1/4	0
	$\|-\rangle$	$\|+\rangle$	$\|+\rangle$	0	1/4	0	1/4	0	1/4	0	1/4
	$\|-\rangle$	$\|+\rangle$	$\|-\rangle$	1/4	0	1/4	0	1/4	0	1/4	0
	$\|-\rangle$	$\|-\rangle$	$\|+\rangle$	1/4	0	1/4	0	1/4	0	1/4	0
	$\|-\rangle$	$\|-\rangle$	$\|-\rangle$	0	1/4	0	1/4	0	1/4	0	1/4

of the three qubits $Q_{A_i}, Q_{B_i}, Q_{C_i}$ in a randomly chosen basis (Z or X) instead of measuring $(Q_{A_i}, Q_{B_i}, Q_{C_i})$ in $\mathcal{B}_3$ basis. Now UFP checks the individual measurement results and decides to announce an $\mathcal{M}'[i] \in \{|\Phi_0^+\rangle, |\Phi_0^-\rangle, |\Phi_1^+\rangle, |\Phi_1^-\rangle, |\Phi_2^+\rangle, |\Phi_2^-\rangle, |\Phi_3^+\rangle, |\Phi_3^-\rangle\}$ corresponding to the states which can arrive if he measures in the correct basis (see Table 8.2). For example, if UFP measures in Z-basis and gets the result $|0\rangle|0\rangle|1\rangle$ then he announces $\mathcal{M}'[i]$ from the set $\{|\Phi_1^+\rangle, |\Phi_1^-\rangle\}$. Again if he measures in X-basis and gets the result $|-\rangle|+\rangle|+\rangle$ then he announces $\mathcal{M}'[i]$ from the set $\{|\Phi_0^-\rangle, |\Phi_1^-\rangle, |\Phi_2^-\rangle, |\Phi_3^-\rangle\}$.

We now calculate the winning probability p of UFP for correctly guessing the i-th measurement result $\mathcal{M}[i]$. Let the preparation basis for the initial qubits $Q_{A_i}, Q_{B_i}, Q_{C_i}$ be $\mathcal{B}$ and UFP chooses the basis $\mathcal{B}'$. Then we have,

$$
\begin{aligned}
p &= \Pr(\mathcal{M}'[i] = \mathcal{M}[i]) \\
&= \Pr(\mathcal{M}'[i] = \mathcal{M}[i] |\ \mathcal{B} = \mathcal{B}') \Pr(\mathcal{B} = \mathcal{B}') + \Pr(\mathcal{M}'[i] = \mathcal{M}[i] |\ \mathcal{B} \neq \mathcal{B}') \Pr(\mathcal{B} \neq \mathcal{B}') \\
&= \frac{1}{2}\{\Pr(\mathcal{M}'[i] = \mathcal{M}[i] |\ \mathcal{B} = \mathcal{B}') + \Pr(\mathcal{M}'[i] = \mathcal{M}[i] |\ \mathcal{B} \neq \mathcal{B}')\} \\
&= \frac{1}{2}\{\Pr(\mathcal{M}'[i] = \mathcal{M}[i] |\ \mathcal{B} = \mathcal{B}') + \Pr(\mathcal{M}'[i] = \mathcal{M}[i] |\ \mathcal{B} = X, \mathcal{B}' = Z) + \\
&\qquad\qquad \Pr(\mathcal{M}'[i] = \mathcal{M}[i] |\ \mathcal{B} = Z, \mathcal{B}' = X)\} \\
&= \frac{1}{2}\left(1 + \frac{1}{2} + \frac{1}{4}\right) = \frac{7}{8}.
\end{aligned}
$$

Therefore the legitimate parties can detect this eavesdropping with probability $1 - p^{\gamma m'}$, which is a non-negligible probability for large $\gamma m'$.

Next, we consider four types of attacks (intercept-and-resend attack, entangle-and-measure attack, DoS attack, man-in-the-middle attack) and show that our protocol is secure against these attacks.

1. **Intercept-and-resend attack**

   Here we consider the intercept-and-resend attack by an adversary $\mathcal{A}$ (other than the UFP). In this attack model, $\mathcal{A}$ intercepts the qubits from the quantum channel, then she measures those qubits and resends to the receiver. First let us assume that $\mathcal{A}$ intercepts q_A, measures the qubits in randomly chosen bases (Z or X) and notes down the measurement results. Due to the measurements by $\mathcal{A}$, let the sequence q_A changes

to q'_A and she resends q'_A to UFP. After receiving the sequence q'_A, Alice tells UFP some random positions of the sent qubits and their preparation bases, then UFP measures those qubits and announces the results. Let the i-th qubit q_{A_i} prepared in basis $\mathcal{B}_{A_i}$, and $\mathcal{A}$ chooses basis $\mathcal{B}'_{A_i}$ to measure q_{A_i}. At the time of security checking, UFP measures q'_{A_i} in $\mathcal{B}_{A_i}$ and gets the result q''_{A_i}.

Thus the winning probability of $\mathcal{A}$ is

$$\begin{aligned}
p_1 &= \Pr(q''_{A_i} = q_{A_i}) \\
&= \Pr(q''_{A_i} = q_{A_i} |\ \mathcal{B}_{A_i} = \mathcal{B}'_{A_i}) \Pr(\mathcal{B}_{A_i} = \mathcal{B}'_{A_i}) + \Pr(q''_{A_i} = q_{A_i} |\ \mathcal{B}_{A_i} \neq \mathcal{B}'_{A_i}) \Pr(\mathcal{B}_{A_i} \neq \mathcal{B}'_{A_i}) \\
&= \frac{1}{2}\{\Pr(q''_{A_i} = q_{A_i} |\ \mathcal{B}_{A_i} = \mathcal{B}'_{A_i}) + \Pr(q''_{A_i} = q_{A_i} |\ \mathcal{B}_{A_i} \neq \mathcal{B}'_{A_i})\} \\
&= \frac{1}{4}\left(1 + \frac{1}{2}\right) = \frac{3}{4}.
\end{aligned}$$

Similarly, when $\mathcal{A}$ intercepts q_B and q_C, then the winning probability of $\mathcal{A}$ is $p_2 = \frac{3}{4}$ and $p_3 = \frac{3}{4}$ respectively. Note that Alice, Bob, and Charlie apply random permutations on their respective sequences of qubits, and those permutations are announced only if the error estimation phase is passed after the qubits arrive at their destinations. So at the time of sending those sequences, $\mathcal{A}$ can not just guess a key bit and measure the qubits in the corresponding bases. Even if she gets some of the key bits, she can not guess the corresponding bases for sequences of qubits q_A, q_B, q_C. Therefore measuring the qubits of q_A, q_B, q_C are independent events to $\mathcal{A}$ and thus the winning probability of $\mathcal{A}$ for this attack is $p_1 p_2 p_3 = (\frac{3}{4})^3$. Alice, Bob, and Charlie randomly choose δm number of rounds to estimate the error in the channel (Step 6 of Protocol 1), where $\delta \ll 1$ is a small fraction. Corresponding to these rounds, they tell the positions and preparation bases of the qubits to the UFP . Next, the UFP measures each single qubit state in proper basis and announces the result. Alice, Bob, and Charlie reveal their respective qubits for these rounds and compare them with the results announced by UFP and calculate the error rate in the quantum channel. Thus the probability that they can detect the existence of $\mathcal{A}$ is $1 - \left(\frac{3}{4}\right)^{3\delta m}$, and in this case the legitimate parties terminate the protocol.

Next we consider $\mathcal{A}$ tries to eavesdrop in the second phase of transmission of qubits (Step 2 of Algorithm 4). Suppose $\mathcal{A}$ intercepts the sequences S''_A, S''_B, S''_C from the quan-

tum channel, measures them in Z or X basis and then resends those sequences to the receivers. Since each of S''_A, S''_B, S''_C contains d decoy photons, then these intermediate measurements change the states of those decoy photons. Let the i-th decoy photon of Alice be D_{A_i} prepared in basis $\mathcal{B}$, where $\mathcal{B} = Z$ or X, and after $\mathcal{A}$ measures in $\mathcal{B}'$ basis the state becomes D'_{A_i}. When Alice announces the preparation basis of D_{A_i}, then Bob measures D'_{A_i} in basis $\mathcal{B}$ and gets D''_{A_i}. We now calculate the probability that $D_{A_i} = D''_{A_i}$ as follows,

$$\begin{aligned}
&\Pr(D''_{A_i} = D_{A_i}) \\
&= \Pr(D''_{A_i} = D_{A_i} |\ \mathcal{B} = \mathcal{B}') \Pr(\mathcal{B} = \mathcal{B}') + \Pr(D''_{A_i} = D_{A_i} |\ \mathcal{B} \neq \mathcal{B}') \Pr(\mathcal{B} \neq \mathcal{B}') \\
&= \frac{1}{2}[\Pr(D''_{A_i} = D_{A_i} |\ \mathcal{B} = \mathcal{B}') + \Pr(D''_{A_i} = D_{A_i} |\ \mathcal{B} \neq \mathcal{B}')] \\
&= \frac{1}{2}\left[1 + \frac{1}{2}\right] = \frac{3}{4}.
\end{aligned}$$

Thus the probability that Alice and Bob can detect the existence of $\mathcal{A}$ is $1 - \left(\frac{3}{4}\right)^d$, where d is the number of decoy photon. Similarly for the other sequences of qubits.

2. **Entangle-and-measure attack**

Let us discuss another attack, called entangle-and-measure attack, by an adversary $\mathcal{A}$. For this attack, $\mathcal{A}$ does the following: when Alice sends her sequence of qubits q_A to the UFP , then $\mathcal{A}$ takes each qubit q_{A_i}, $1 \leqslant i \leqslant m$, from the channel and takes an ancillary qubit $|b\rangle$, which is in state $|0\rangle$, from her own. $\mathcal{A}$ applies a CNOT gate with control q_{A_i} and target $|b\rangle$, and then she sends q_{A_i} to the UFP . The joint state becomes $|00\rangle$, $|11\rangle$, $|\Phi^+\rangle$ and $|\Phi^-\rangle$, corresponding to the state of q_{A_i}, which are $|0\rangle$, $|1\rangle$, $|+\rangle$ and $|-\rangle$ respectively. Also $\mathcal{A}$ does the same thing with the qubits of Bob and Charlie. After the UFP receives all the qubits, Alice, Bob and Charlie randomly choose δm number of rounds to estimate the error in channel (Step 6 of Protocol 1), where $\delta \ll 1$ is a small fraction. Corresponding to these rounds, they tell the positions and preparation bases of the qubits to the UFP , who then measures each of the single qubit state in proper basis and announces the result. Alice, Bob and Charlie reveal their respective qubits for these rounds and compare with the results announced by the UFP.

Let UFP get the measurement result q'_{A_i} by measuring the state q_{A_i} prepared in basis $\mathcal{B}$. Now if the original state of q_{A_i} is $|0\rangle$ or $|1\rangle$, then no error occurs. But if the original state of q_{A_i} is $|+\rangle$ or $|-\rangle$, then an error will occur with probability 1/2, as $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle)$ and $|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = \frac{1}{\sqrt{2}}(|++\rangle - |--\rangle)$. Thus Alice, Bob and Charlie abort the protocol. Let us calculate the probability of the event $q'_{A_i} = q_{A_i}$.

$$\begin{aligned} p_1 &= \Pr(q'_{A_i} = q_{A_i}) \\ &= \Pr(q'_{A_i} = q_{A_i} |\ \mathcal{B} = Z) \Pr(\mathcal{B} = Z) + \Pr(q'_{A_i} = q_{A_i} |\ \mathcal{B} = X) \Pr(\mathcal{B} = X) \\ &= \frac{1}{2}[q'_{A_i} = q_{A_i} |\ \mathcal{B} = Z) + \Pr(q'_{A_i} = q_{A_i} |\ \mathcal{B} = X)] \\ &= \frac{1}{2}\left[1 + \frac{1}{2}\right] = \frac{3}{4}. \end{aligned}$$

Similarly we can calculate $p'_2 = \Pr(q'_{B_i} = q_{B_i}) = \frac{3}{4}$, $p'_3 = \Pr(q'_{C_i} = q_{C_i}) = \frac{3}{4}$. Thus for $1 \leqslant i \leqslant m$, the winning probability of $\mathcal{A}$ is $p'_1 p'_2 p'_3 = \left(\frac{3}{4}\right)^3$ and the legitimate party can detect him at the time of security checking with probability $1 - \left(\frac{3}{4}\right)^{3\delta m}$. Similar argument follows for the second round of communication.

3. **DoS attack**

In this attack model, $\mathcal{A}$ applies a random unitary operator $\mathcal{U} \neq I$ on the qubits to tamper the original message and introduce noise in the channel. This attack can also be detected in the same way as discussed above. Let $\mathcal{U} = \sum_{j=1}^{4} w_j P_j$, where P_js are the Pauli matrices I, σ_x, $i\sigma_y$ and σ_z for $1 \leq j \leq 4$ respectively [6], and they form a basis for the space of all 2×2 Hermitian matrices. Since $\mathcal{U}$ is unitary, $\sum_{j=1}^{4} w_j^2 = 1$. Now the winning probability of $\mathcal{A}$ is $p_4 = \sum_{j=1}^{4} h_j w_j^2$, where h_js are the winning probabilities of $\mathcal{A}$ when she applies P_js respectively. Thus $h_1 = 1$, $h_2 = 1/2$, $h_3 = 0$ and $h_4 = 1/2$ as I does not change any state, σ_x changes the states in Z-basis, $i\sigma_y$ changes the states in both Z-basis and X-basis, and σ_z changes the states in X-basis. Hence in the security check process Alice, Bob and Charlie find this eavesdropping with probability $1 - {p_4}^{3\delta m} > 0$. Similarly for the second phase of communication, the legitimate parties can detect $\mathcal{A}$ with probability $1 - {p_4}^{3d} > 0$, where d is the number of decoy states.

4. **Man-in-the-middle attack**

For this attack, $\mathcal{A}$ prepares three finite sequences of length m, of single qubit states q'_A, q'_B and q'_C, whose elements are randomly selected between $|0\rangle, |1\rangle, |+\rangle$ and $|-\rangle$. When Alice, Bob, and Charlie send their prepared sequences of qubits q_A, q_B and q_C to the UFP , then $\mathcal{A}$ intercepts q_A, q_B, q_C and keeps those with her. Instead of q_A, q_B and q_C, she sends q'_A, q'_B and q'_C to the UFP . Note that Alice, Bob, and Charlie apply random permutations on their respective sequences of qubits, and those permutations are announced only if the error estimation phase is passed after the qubits arrive at their destinations. So at the time of sending those sequences, $\mathcal{A}$ can not just guess a key bit and prepare her qubits. Even if she gets some of the key bits, she can not guess the corresponding bases for the sequences of qubits q_A, q_B, q_C. Alice, Bob, and Charlie randomly choose δm number of rounds to estimate the error in channel (Step 6 of Protocol 1), where $\delta \ll 1$ is a small fraction. Corresponding to these rounds, they tell the positions and preparation bases of the qubits to the UFP. Next, the UFP measures each single qubit state in proper basis and announces the result. Alice, Bob, and Charlie reveal their respective qubits for these rounds and compare them with the results announced by UFP. Since the elements of q'_A, q'_B, and q'_C are randomly chosen by $\mathcal{A}$, thus they introduce error in the channel. Let us calculate the probability that Alice, Bob and Charlie can detect this eavesdropping and so they abort the protocol.

For each i, let the i-th qubit of Alice be q_{A_i} prepared in basis $\mathcal{B}_{A_i}$, and $\mathcal{A}$ prepare q'_{A_i} in basis $\mathcal{B}'_{A_i}$. At the time of security checking, UFP measures q'_{A_i} in $\mathcal{B}_{A_i}$ and gets the result q''_{A_i}. Now three cases may arise,

- If $\mathcal{B}_{A_i} = \mathcal{B}'_{A_i}$ and $q_{A_i} = q'_{A_i}$, then $q''_{A_i} = q_{A_i}$ with probability 1.

- If $\mathcal{B}_{A_i} = \mathcal{B}'_{A_i}$ and $q_{A_i} \neq q'_{A_i}$, then $q''_{A_i} = q_{A_i}$ with probability 0.

- If $\mathcal{B}_{A_i} \neq \mathcal{B}'_{A_i}$, then $q''_{A_i} = q_{A_i}$ with probability 1/2.

Thus the winning probability of $\mathcal{A}$ is

$$\begin{aligned}
&\Pr(q''_{A_i} = q_{A_i}) \\
&= \Pr(q''_{A_i} = q_{A_i} |\ \mathcal{B}_{A_i} = \mathcal{B}'_{A_i}) \Pr(\mathcal{B}_{A_i} = \mathcal{B}'_{A_i}) + \Pr(q''_{A_i} = q_{A_i} |\ \mathcal{B}_{A_i} \neq \mathcal{B}'_{A_i}) \Pr(\mathcal{B}_{A_i} \neq \mathcal{B}'_{A_i}) \\
&= \frac{1}{2}\{\Pr(q''_{A_i} = q_{A_i} |\ \mathcal{B}_{A_i} = \mathcal{B}'_{A_i}) + \Pr(q''_{A_i} = q_{A_i} |\ \mathcal{B}_{A_i} \neq \mathcal{B}'_{A_i})\} \\
&= \frac{1}{2}[\Pr(q''_{A_i} = q_{A_i} |\ \mathcal{B} = \mathcal{B}',\ q_{A_i} = q'_{A_i}) \Pr(q_{A_i} = q'_{A_i}) + \\
&\qquad \Pr(q''_{A_i} = q_{A_i} |\ \mathcal{B} = \mathcal{B}',\ q_{A_i} \neq q'_{A_i}) \Pr(q_{A_i} \neq q'_{A_i}) + 1/2] \\
&= \frac{1}{2}\left[1 \times \frac{1}{2} + 0 \times \frac{1}{2} + \frac{1}{2}\right] = \frac{1}{2}.
\end{aligned}$$

We can calculate the winning probabilities for q_{B_i} and q_{C_i} in a similar way. Hence Alice, Bob and Charlie can detect this eavesdropping with probability $1 - \left(\frac{1}{2}\right)^{3\delta m} > 0$. Again, if $\mathcal{A}$ tries to eavesdrop in the second phase of transmission of qubits (Step 2 of Algorithm 4), Alice, Bob and Charlie can detect it in the error estimation phase (Step 2e of Algorithm 4) and abort the protocol.

Hence our protocol is secure against a dishonest UFP , intercept-and-resend attack, entangle-and-measure attack, DoS attack and man-in-the-middle attack.

8.2 Multi-party Q.Conf

In this section, we generalize our three-party Q.Conf protocol to a multi-party Q.Conf protocol. Suppose there are N ($\geqslant 3$) parties $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_N$; each of them wants to send one's message to the other $N-1$ parties by taking help from an untrusted $(N+1)$-th party $\mathcal{P}_{(N+1)}$, who may be an eavesdropper. Let the m-bit messages of $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_N$ be $M_1 = M_{1,1}M_{1,2}\ldots M_{1,m}$; $M_2 = M_{2,1}M_{2,2}\ldots M_{2,m}$; $\ldots$; $M_N = M_{N,1}M_{N,2}\ldots M_{N,m}$ respectively, where $M_{i,j}$ is the j-th message bit of the i-th party $\mathcal{P}_i$. To do this task, first, they have to share an m-bit key $k = k_1k_2\ldots k_m$ and according to the key, they prepare their sequence of qubits to encode their message bits. The encoding algorithm is the same as the three-party case, i.e., Subroutine 1. Then they send their qubit sequences to $\mathcal{P}_{(N+1)}$, who measures each N-qubit states in $\mathcal{B}_N$ basis and announces the result publicly. Depending on the measurement results, one's message bits and key bits,

each of them prepares another sequence of qubits, which contains some encoded message bits and some decoy photons, and sends it to the next party circularly. By measuring these qubits on appropriate bases, each of them gets the message bits of the previous party, but the states of the qubits corresponding to the message bits remain the same. Each adds some decoy photons to the message qubits sequence of the previous party and send it to their next party circularly and repeat this process for $N-2$ times. From the previous measurement results announced by $\mathcal{P}_{(N+1)}$, each can get other $N-1$ messages from the other $N-1$ parties. Details are given in Section 8.2.1. Note that for $N=3$, the protocol is given in Section 8.2.1 reduces to the three-party protocol of Section 8.1.1.

8.2.1 Protocol 2: N-party Q.Conf

The steps of the protocol are as follows:

1. $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_N$ perform a Multi-party QKD protocol (e.g., [109]) to establish an m bit secret key $k = k_1 k_2 \ldots k_m$ between themselves.

2. Let the m-bit message of $\mathcal{P}_i$ be $M_i = M_{i,1} M_{i,2} \ldots M_{i,m}$ for $i = 1, 2, \ldots, N$.

3. For $i = 1, 2, \ldots, N$, the i-th party $\mathcal{P}_i$ prepares the sequence of qubits $Q_i = \{Q_i[j]\}_{j=1}^{m} = (Q_{i,1}, Q_{i,2}, \ldots, Q_{i,m})$ at its end by using the Subroutine 1.

4. $\mathcal{P}_i$ chooses some random permutation and applies on its respective sequence of qubits Q_i and get new sequence of qubits q_i, for $i = 1, 2, \ldots, N$.

5. They send the prepared qubits $q_1, q_2, \ldots, q_N$ to $\mathcal{P}_{(N+1)}$.

6. $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_N$ randomly choose δm number of common positions on the sequences $Q_1, Q_2, \ldots, Q_N$ to estimate the error in the channel, where $\delta \ll 1$ is a small fraction. Corresponding to these rounds, they do the followings:

   (a) Each participant tells the positions and the preparation bases of those qubits for those rounds to $\mathcal{P}_{(N+1)}$.

   (b) $\mathcal{P}_{(N+1)}$ measures each single qubit states in proper bases and announces the results.

(c) $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_N$ reveal their respective qubits for these rounds and compare with the results announced by $\mathcal{P}_{(N+1)}$.

(d) If the estimated error is greater than some predefined threshold value, then they abort. Else they continue and go to the next step.

7. $\mathcal{P}_{(N+1)}$ asks $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_N$ to tell the permutations which they have applied to their sequences.

8. $\mathcal{P}_{(N+1)}$ applies the inverse permutations, corresponding to the permutations chosen by $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_N$, on $q_1, q_2, \ldots, q_N$ to get $Q_1, Q_2, \ldots, Q_N$ respectively.

9. They discard the qubits corresponding to the above δm positions. Their remaining sequences of prepared qubits are relabeled as $Q_1 = \{Q_1[i]\}_{i=1}^{m'}$, $Q_2 = \{Q_2[i]\}_{i=1}^{m'}$, ..., $Q_N = \{Q_N[i]\}_{i=1}^{m'}$, where $m' = (1-\delta)m$.

10. They update their m-bit key to an m'-bit key by discarding δm number of key bits corresponding to the above δm rounds. The updated key is relabeled as $k = k_1 k_2 \ldots k_{m'}$.

11. For $1 \leqslant i \leqslant m'$, $\mathcal{P}_{(N+1)}$ measures each N qubit states $Q_{1,i}, Q_{2,i}, \ldots, Q_{N,i}$ in basis $\mathcal{B}_N$ and announces the result.

12. $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_N$ make a finite sequence $\{\mathcal{M}[i]\}_{i=1}^{m'}$ containing the measurement results, i.e., for $1 \leqslant i \leqslant m'$, $\mathcal{M}[i] \in \{|\Phi_0^+\rangle, |\Phi_0^-\rangle, |\Phi_1^+\rangle, |\Phi_1^-\rangle, \ldots, |\Phi_{2^{(N-1)}-1}^+\rangle, |\Phi_{2^{(N-1)}-1}^-\rangle\}$ is the i-th measurement result announced by $\mathcal{P}_{(N+1)}$.

13. They randomly choose $\gamma m'$ number of measurement results $\mathcal{M}[i]$ from the sequence $\{\mathcal{M}[i]\}_{i=1}^{m'}$ to estimate the error, where $\gamma \ll 1$ is a small fraction.

(a) They reveal their respective message bits for these rounds.

(b) If the estimated error is greater than some predefined threshold value, then they abort. Else they continue and go to the next step.

14. Their remaining sequence of measurement results is relabeled as $\{\mathcal{M}[i]\}_{i=1}^{n}$, where $n = (1-\gamma)m'$.

15. They update their m'-bit key to an n-bit key by discarding $\gamma m'$ number of key bits corresponding to the above $\gamma m'$ rounds. The updated key is relabeled as $k = k_1 k_2 \dots k_n$.

16. For $1 \leqslant \alpha \leqslant N$, $\mathcal{P}_\alpha$ uses the Algorithm 5 to recover others' messages.

Note that in this protocol, there are two error estimation phases. The first one checks if there is any adversary (other than $\mathcal{P}_{(N+1)}$) in the channel, who tries to get some information about the messages or change the messages. In this case, if the 1st error estimation phase does not pass, then the participants abort the protocol. Thus in this step, the motivation of $\mathcal{P}_{(N+1)}$ being correct is, there is no information gain if the parties abort the protocol. The next error estimation phase is to check, if there is any error introduced by $\mathcal{P}_{(N+1)}$.

8.2.2 Correctness and security analysis of N-party Q.Conf protocol

In our proposed protocol, for $1 \leqslant \alpha \leqslant N$, each $\mathcal{P}_\alpha$ first prepares qubits corresponding to his (her) message and shared key and then send those qubits to $\mathcal{P}_{(N+1)}$. After that, $\mathcal{P}_{(N+1)}$ measures each N-qubit state (one from each $\mathcal{P}_\alpha$) in basis $\mathcal{B}_N = \{|\Phi_0^+\rangle, |\Phi_0^-\rangle, |\Phi_1^+\rangle, |\Phi_1^-\rangle, \dots, |\Phi_{2^{(N-1)}-1}^+\rangle, |\Phi_{2^{(N-1)}-1}^-\rangle\}$ and announces the result.

Now for $1 \leqslant i \leqslant m$, if $k_i = 0$ (i.e preparation basis of each ${Q^\alpha}_i$ is $\{|0\rangle, |1\rangle\}$) and the N-qubit state is $|j\rangle = |j_1\rangle |j_2\rangle \dots |j_N\rangle$ or $|2^N - 1 - j\rangle = |j'\rangle = |j'_1\rangle |j'_2\rangle \dots |j'_N\rangle$, then after measurement, $\mathcal{P}_{(N+1)}$ will get $|\Phi_j^+\rangle$ and $|\Phi_j^-\rangle$ with probability $1/2$.

Again if $k_i = 1$ (i.e., the preparation basis of each ${Q^\alpha}_i$ is $\{|+\rangle, |-\rangle\}$) and there are even number of α, such that $Q_{\alpha,i} = |-\rangle$, then $\mathcal{P}_{(N+1)}$ will get $|\Phi_j^+\rangle$ ($j \in \{0, 1, \dots, 2^{(N-1)} - 1\}$) with probability $1/2^{(N-1)}$.

Else if $k_i = 1$ (i.e., preparation basis of each ${Q^\alpha}_i$ is $\{|+\rangle, |-\rangle\}$) and there are odd number of α, such that $Q_{\alpha,i} = |-\rangle$, then $\mathcal{P}_{(N+1)}$ will get $|\Phi_j^-\rangle$ ($j \in \{0, 1, \dots, 2^{(N-1)} - 1\}$) with probability $1/2^{(N-1)}$.

For better understanding, we write the table for $N = 4$ (Table 8.3 in Appendix A).

Now for $1 \leqslant i \leqslant m$ and $1 \leqslant \alpha \leqslant N$, if $k_i = 0$, we can say the following: if the prepared qubit of $\mathcal{P}_\alpha$ is $|0\rangle$ or $|1\rangle$, then $\mathcal{P}_\alpha$ guesses message bit of other parties with probability 1 as follows: $\mathcal{M}[i] = |\Phi_j^+\rangle$ or $|\Phi_j^-\rangle \Rightarrow$ the N-qubit state was $|j\rangle$ or $|2^N - 1 - j\rangle$. Since $|2^N - 1 - j\rangle = |\bar{j_1}\rangle |\bar{j_2}\rangle \dots |\bar{j_N}\rangle$, from his/her own message bit, $\mathcal{P}_\alpha$ can get the others' message bits.

If the prepared qubit of $\mathcal{P}_\alpha$ is $|+\rangle$ or $|-\rangle$, then $\mathcal{P}_\alpha$ guesses the XOR function of message bits of all parties with probability 1 as follows:

$$\text{Measurement result} = \begin{cases} |\Phi_j^+\rangle \Rightarrow & M_{1,i} \oplus M_{2,i} \oplus \ldots \oplus M_{N,i} = 0; \\ |\Phi_j^-\rangle \Rightarrow & M_{1,i} \oplus M_{2,i} \oplus \ldots \oplus M_{N,i} = 1. \end{cases}$$

for some $j \in \{0, 1, \ldots, 2^{(N-1)} - 1\}$.

In this case, $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_{(\alpha-1)}, \mathcal{P}_{(\alpha+2)}, \ldots, \mathcal{P}_{(N-1)}, \mathcal{P}_N$ send their encoded qubits to $\mathcal{P}_\alpha$ (encoding algorithm is given in Step 2a of Algorithm 5). Since $\mathcal{P}_\alpha$ knows the basis of the received qubits, by measuring the qubits in the proper basis, $\mathcal{P}_\alpha$ can know the message bits $M_{1,i}, M_{2,i}, \ldots, M_{(\alpha-1),i}, M_{(\alpha+2),i}, \ldots, M_{N,i}$. Then from the XOR value, $\mathcal{P}_\alpha$ can get $M_{(\alpha+1),i}$ also.

From the above discussion, we see that for all cases, all parties can conclude the communicated bits of the other parties with probability 1. Hence our protocol is giving the correct result.

The security analysis is the same as the three-party Q.Conf protocol and so we will not repeat it here.

8.3 Multi-party XOR computation

In this section, we present a protocol for multi-party XOR computation. Suppose there are N parties $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_N$; each of them has an m-bit number. Let m-bit numbers of $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_N$ be $M_1 = M_{1,1}M_{1,2}\ldots M_{1,m}$; $M_2 = M_{2,1}M_{2,2}\ldots M_{2,m}$; $\ldots$; $M_N = M_{N,1}M_{N,2}\ldots M_{N,m}$ respectively, where $M_{i,j}$ is the j-th bit of the i-th party $\mathcal{P}_i$'s message. They want to compute $M_1 \oplus M_2 \oplus \ldots \oplus M_N$ securely, such that their numbers remain private. To execute this protocol, they will take help from an untrusted $(N+1)$-th party (or $\mathcal{P}_{(N+1)}$). Also, one participant among $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_N$, must be semi-honest (i.e., it follows the protocol properly), who have to play a vital role in this computation. Let $\mathcal{P}_1$ be the semi-honest participant. Other participants are only allowed to prepare and send the states corresponding to their numbers. If other participants do not follow the protocol properly (i.e., they will prepare states corresponding

Algorithm 5: N-Party Message Reconstruction Algorithm for $\mathcal{P}_\alpha$.

Input: Own message M_α, key k, joint measurement results $\{\mathcal{M}[i]\}_{i=1}^{n}$ announced by $\mathcal{P}_{(N+1)}$.
Output: Others' messages $M_1, M_2, \ldots, M_{(\alpha-1)}, M_{(\alpha+1)}, \ldots, M_N$.

1. For $1 \leqslant i \leqslant n$, if $k_i = 0$,
   $\mathcal{P}_\alpha$ can learn the i-th bit of others' messages from the measurement result $\mathcal{M}[i]$ and his(her) own message (same as three party Q.Conf, e.g., see Table 8.3 for $N = 4$).

2. For $1 \leqslant i \leqslant n$, if $k_i = 1$,
   from the measurement result $\mathcal{M}[i]$ and his (her) own message, $\mathcal{P}_\alpha$ can learn the XOR value of the i-th bit of all N messages. If $\mathcal{M}[i] = |\Phi_l^+\rangle$ for some $l \in \{0, 1, \ldots, 2^{(N-1)} - 1\}$, then the value of $\chi_i = M_{1,i} \oplus M_{2,i} \oplus \ldots \oplus M_{N,i}$ becomes 0, else $\chi_i = 1$. Let $c = wt(k)$.

   (a) $\mathcal{P}_\alpha$ prepares an ordered set of c qubits S_α, corresponding to his (her) message bit where the key bit is 1. He (she) prepares the qubits at his (her) end according to the following strategy. For $1 \leqslant j \leqslant c$ and if $k_i = 1$ is the j-th 1 in k, then

   - if $M_{\alpha,i} = 0$ and i is even, prepares $S_\alpha[j] = |0\rangle$.
   - if $M_{\alpha,i} = 1$ and i is even, prepares $S_\alpha[j] = |1\rangle$.
   - if $M_{\alpha,i} = 0$ and i is odd, prepares $S_\alpha[j] = |+\rangle$.
   - if $M_{\alpha,i} = 1$ and i is odd, prepares $S_\alpha[j] = |-\rangle$.

   (b) There are $N - 2$ rounds.

   - **1st round:**

     1-1. $\mathcal{P}_\alpha$ prepares a set of decoy photons $D_{\alpha,1}$, where the decoy photons are randomly chosen from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. He (she) randomly inserts his (her) decoy photons into S_α and makes new ordered sets ${S_\alpha}^1$. $\mathcal{P}_\alpha$ sends ${S_\alpha}^1$ to $\mathcal{P}_{(\alpha+1)(Mod\ N)}$ and receives $S^1_{(\alpha-1)(Mod\ N)}$ from $\mathcal{P}_{(\alpha-1)(Mod\ N)}$.

     1-2. After $\mathcal{P}_{(\alpha+1)(Mod\ N)}$ receives ${S_\alpha}^1$, $\mathcal{P}_\alpha$ sends the positions and states of $D_{\alpha,1}$ to $\mathcal{P}_{(\alpha+1)(Mod\ N)}$ through a public channel. Also $\mathcal{P}_\alpha$ receives the positions and states of $D_{(\alpha-1)(Mod\ N),1}$.

     1-3. Then $\mathcal{P}_\alpha$ verifies the decoy photons to check eavesdropping. If there exists any eavesdropper in the quantum channel it aborts the protocol, else it goes to the next step.

     1-4. $\mathcal{P}_\alpha$ measures the qubits of $S_{(\alpha-1)(Mod\ N)}$ in proper bases and knows the corresponding message bits of $\mathcal{P}_{(\alpha-1)(Mod\ N)}$. Also after measurements in the proper bases, the states of the qubits of $S_{(\alpha-1)(Mod\ N)}$ remain unchanged.

   - **l-th round ($2 \leqslant l \leqslant N - 2$):**

     l-1. $\mathcal{P}_\alpha$ prepares a set of decoy photons $D_{\alpha,l}$, where the decoy photons are randomly chosen from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. He (she) randomly inserts his (her) decoy photons into $S_{(\alpha-l+1)(Mod\ N)}$ and makes new ordered sets ${S_\alpha}^l$. $\mathcal{P}_\alpha$ sends ${S_\alpha}^l$ to $\mathcal{P}_{(\alpha+1)(Mod\ N)}$ and receives ${S_{(\alpha-1)(Mod\ N)}}^l$ from $\mathcal{P}_{(\alpha-1)(Mod\ N)}$.

     l-2. After $\mathcal{P}_{(\alpha+1)(Mod\ N)}$ receives ${S_\alpha}^l$, $\mathcal{P}_\alpha$ sends the positions and states of $D_{\alpha,l}$ to $\mathcal{P}_{(\alpha+1)(Mod\ N)}$ through a public channel. Also $\mathcal{P}_\alpha$ receives the positions and states of $D_{(\alpha-1)(Mod\ N),l}$.

     l-3. Then $\mathcal{P}_\alpha$ verifies the decoy photons to check eavesdropping. If there exists any eavesdropper in the quantum channel, it aborts the protocol. Else it goes to the next step.

     l-4. $\mathcal{P}_\alpha$ measures the qubits of $S_{(\alpha-l+1)(Mod\ N)}$ in proper bases and knows the corresponding message bits of $\mathcal{P}_{(\alpha-l+1)(Mod\ N)}$. Also after measurements in the proper bases, the states of the qubits of $S_{(\alpha-l+1)(Mod\ N)}$ remain unchanged.

   (c) $\mathcal{P}_\alpha$ gets all the message bits of previous $N - 2$ participants. As $\mathcal{P}_\alpha$ knows χ_i and its own message bit, it gets all the other $N - 1$ message bits.

to a number other than their own numbers), then the computed value will be incorrect, which they definitely do not want.

To compute $M_1 \oplus M_2 \oplus \ldots \oplus M_N$, first $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_N$ have to share an $2m$-bit key $k = k_1 k_2 \ldots k_{2m}$ and according to the key they prepare their sequence of qubits to encode their numbers. The encoding algorithm is almost similar to conference cases. Then they send their qubit sequences to $\mathcal{P}_{(N+1)}$, who measures each N-qubit states in $\mathcal{B}_N$ basis and announces the result publicly. Then from this announcement and the key, they get the XOR value of their numbers. Details of this protocol are given in Section 8.3.1.

8.3.1 Protocol 3: Multi-party XOR computation

Input: The m-bit numbers $M_1 = M_{1,1} M_{1,2} \ldots M_{1,m}$; $M_2 = M_{2,1} M_{2,2} \ldots M_{2,m}$; $\ldots$; $M_N = M_{N,1}$ $M_{N,2} \ldots M_{N,m}$ of N parties $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_N$ respectively.

Output: $M_1 \oplus M_2 \oplus \ldots \oplus M_N$.

The steps of the protocol are as follows:

1. $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_N$ perform a Multi-party QKD protocol [109] to establish an $2m$ bit secret key $k = k_1 k_2 \ldots k_{2m}$ between themselves.

2. (a) If $wt(k) = m$, then calculate $c = \oplus k_i$, $1 \leq i \leq 2m$.

   (b) Else if $wt(k) > m$, then $c = 1$.

   (c) Else $c = 0$.

3. $\mathcal{P}_1$ prepares an m-bit random number $k' = k'_1 k'_2 \ldots k'_m$ and sends it to $\mathcal{P}_2, \ldots, \mathcal{P}_N$ by using Algorithm 6 with the inputs k' and k.

4. $\mathcal{P}_1$ calculates $M_{1_\Delta} = M_1 \oplus k'$ and uses M_{1_Δ} as his/her number.

5. $\mathcal{P}_1$ generates a $2m$ bit string M'_1 from his/her number and the key in such a way that, for $1 \leq i \leq 2m$ and $1 \leq j \leq m$:

   (a) if $k_i = c$ and $j < m$, then $M'_{1,i} = M_{1_\Delta,j}$, $i = i + 1$, $j = j + 1$;

   (b) else, $M'_{1,i} = x$, where $x \in \{0, 1\}$ is random and $i = i + 1$.

6. For $2 \leqslant \alpha \leqslant N$: $\mathcal{P}_\alpha$ generates $2m$ bit string M'_α from his/her own number as follows. For $1 \leq i \leq 2m$ and $1 \leq j \leq m$:

   (a) if $k_i = c$ and $j < m$, then $M'_{\alpha,i} = M_{\alpha,j}$, $i = i + 1$, $j = j + 1$;

   (b) else, $M'_{\alpha,i} = x$, where $x \in \{0, 1\}$ is random and $i = i + 1$.

7. Each $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_N$ prepares the sequence of qubits $Q_1 = \{Q_1[i]\}_{i=1}^{2m} = (Q_{1,1}, Q_{1,2}, \ldots, Q_{1,2m})$; $Q_2 = \{Q_2[i]\}_{i=1}^{2m} = (Q_{2,1}, Q_{2,2}, \ldots, Q_{2,2m})$; $\ldots$; $Q_N = \{Q_N[i]\}_{i=1}^{2m} = (Q_{N,1}, Q_{N,2}, \ldots, Q_{N,2m})$ at their end by using Algorithm 7.

8. $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_N$ choose some random permutations and apply those on their respective sequences of qubits $Q_1, Q_2, \ldots, Q_N$ and get new sequences of qubits $q_1, q_2, \ldots, q_N$. They send their prepared sequences of qubits $q_1, q_2, \ldots, q_N$ to $\mathcal{P}_{(N+1)}$.

9. $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_N$ randomly choose $2\delta m$ number of common positions on sequences $Q_1, Q_2, \ldots, Q_N$ to estimate the error in the channel, where $\delta \ll 1$ is a small fraction. Corresponding to these rounds, they do the followings:

   (a) Each participant tells the positions and preparation bases of those qubits for those rounds to $\mathcal{P}_{(N+1)}$.

   (b) $\mathcal{P}_{(N+1)}$ measures each single qubit states in proper bases and announces the results.

   (c) $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_N$ reveal their respective qubits for these rounds and compare with the results announced by $\mathcal{P}_{(N+1)}$.

   (d) If the estimated error is greater than some predefined threshold value, then they abort. Else they continue and go to the next step.

10. $\mathcal{P}_{(N+1)}$ asks $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_N$ to tell the permutations which they have applied to their sequences.

11. $\mathcal{P}_{(N+1)}$ applies the inverse permutations, corresponding to the permutations chosen by $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_N$, on $q_1, q_2, \ldots, q_N$ to get $Q_1, Q_2, \ldots, Q_N$ respectively.

12. They discard the qubits corresponding to the above $2\delta m$ positions. Their remaining sequences of prepared qubits are relabeled as $Q_1 = \{Q_1[i]\}_{i=1}^{2m'}$, $Q_2 = \{Q_2[i]\}_{i=1}^{2m'}$, ..., $Q_N = \{Q_N[i]\}_{i=1}^{2m'}$ where $m' = (1-\delta)m$.

13. They update their $2m$-bit key to an $2m'$-bit key by discarding $2\delta m$ number of key bits corresponding to the above $2\delta m$ rounds. The updated key is relabeled as $k = k_1 k_2 \ldots k_{2m'}$.

14. For $1 \leqslant i \leqslant 2m'$, $\mathcal{P}_{(N+1)}$ measures each N qubit states $Q_{1,i}, Q_{2,i}, \ldots, Q_{N,i}$ in basis $\mathcal{B}_N$ and announces the result.

15. $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_N$ make a finite sequence $\{\mathcal{M}[i]\}_{i=1}^{2m'}$ containing the measurement results, i.e., for $1 \leqslant i \leqslant 2m'$, $\mathcal{M}[i] \in \{|\Phi_0^+\rangle, |\Phi_0^-\rangle, |\Phi_1^+\rangle, |\Phi_1^-\rangle, \ldots, |\Phi_{2^{(N-1)}-1}^+\rangle, |\Phi_{2^{(N-1)}-1}^-\rangle\}$ is the i-th measurement result announced by $\mathcal{P}_{(N+1)}$.

16. They randomly choose $2\gamma m'$ number of measurement results $\mathcal{M}[i]$ from the sequence $\{\mathcal{M}[i]\}_{i=1}^{2m'}$ to estimate the error, where $\gamma \ll 1$ is a small fraction.

    (a) For these rounds, they reveal respective bits of their numbers.

    (b) If the estimated error is greater than some predefined threshold value, then they abort. Else they continue and go to the next step.

17. Their remaining sequence of measurement results is relabeled as $\{\mathcal{M}[i]\}_{i=1}^{2n}$, where $n = (1-\gamma)m'$.

18. They update their $2m'$-bit key to an $2n$-bit key by discarding $2\gamma m'$ number of key bits corresponding to the above $2\gamma m'$ rounds. The updated key is relabeled as $k = k_1 k_2 \ldots k_{2n}$.

19. For $1 \leqslant i \leqslant 2n$,

    (a) if $k_i = \bar{c}$, then each participant can learn i-th bit of others' number from the measurement result $\mathcal{M}[i]$ and their own number (see Algorithm 8.2.1).

    (b) Else, from the measurement result $\mathcal{M}[i]$, each participant can learn the XOR value of the i-th bit of all N numbers. If $\mathcal{M}[i] = |\Phi_l^+\rangle$ for some $l \in \{0, 1, \ldots, 2^{(N-1)} - 1\}$, then the value of $\chi_i = M_{1_\Delta,i} \oplus M_{2,i} \oplus \ldots \oplus M_{N,i}$ becomes 0, else $\chi_i = 1$.

20. Combining the knowledges from Step-19b and the key, they can get $M_{1_\Delta} \oplus M_2 \oplus \ldots \oplus M_N$.

21. $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_N$ calculate $M_1 \oplus M_2 \oplus \ldots \oplus M_N = k' \oplus M_{1_\Delta} \oplus M_2 \oplus \ldots \oplus M_N$.

Algorithm 6: Algorithm for Sending a Number to $(N-1)$-Participant.

Input: Random number $k' = k'_1 k'_2 \ldots k'_m$ chosen by $\mathcal{P}_1$, key $k = k_1 k_2 \ldots k_{2m}$.
Output: For $2 \leqslant \alpha \leqslant N$, $\mathcal{P}_\alpha$ has k'.

1. To encode random number k', $\mathcal{P}_1$ prepares $N-1$ sets of qubits $Q_\alpha = Q_{\alpha,1} Q_{\alpha,2} \ldots Q_{\alpha,m}$ for $\mathcal{P}_\alpha$ $(2 \leqslant \alpha \leqslant N)$, by using the following strategy: for $1 \leqslant i \leqslant m$ and $2 \leqslant \alpha \leqslant N$,
   (a) if $k'_i = 0$ and $k_i = 0 \Rightarrow Q_{\alpha,i} = |0\rangle$
   (b) if $k'_i = 1$ and $k_i = 0 \Rightarrow Q_{\alpha,i} = |1\rangle$
   (c) if $k'_i = 0$ and $k_i = 1 \Rightarrow Q_{\alpha,i} = |+\rangle$
   (d) if $k'_i = 1$ and $k_i = 1 \Rightarrow Q_{\alpha,i} = |-\rangle$
2. For $2 \leqslant \alpha \leqslant N$, $\mathcal{P}_1$ chooses a set of decoy photons D_α and randomly inserts those decoy photons into Q_α and gets new set of qubits q_α.
3. $\mathcal{P}_1$ sends q_α to $\mathcal{P}_\alpha$.
4. All $\mathcal{P}_\alpha$ inform $\mathcal{P}_1$ that they receive q_α.
5. $\mathcal{P}_1$ announces the positions and states of the decoy photons.
6. Each $\mathcal{P}_\alpha$ measures the decoy photons in their appropriate bases and calculate the error in the channel (or check that if there is any eavesdropper).
7. If the error rate is in a tolerable range, then $\mathcal{P}_\alpha$ measures the qubits of Q_α in their appropriate bases (determined by the key) and get k'.

8.3.2 Correctness and security analysis of the quantum protocol for multi-party XOR computation

The correctness of this protocol directly follows from the previous one (i.e., multi-party Q.Conf protocol). Also, we can say this protocol is secure against intercept-and-resend attack, disturbance attack, entangle-and-measure attack, and dishonest $\mathcal{P}_{(N+1)}$, as this is a part of the previous protocol discussed in the last section.

Now, we only have to prove that, no one can get the computed XOR-value other than the legitimate parties.

Algorithm 7: Message Encoding Algorithm for Multi-party XOR Computation.

Input: $M'_\alpha = 2m$-bit message of $\mathcal{P}_\alpha$, key $k = k_1 k_2 \dots k_{2m}$.
Output: Sequence of qubits $Q_\alpha = \{Q_\alpha[i]\}_{i=1}^{2m} = (Q_{\alpha,1}, Q_{\alpha,2}, \dots, Q_{\alpha,2m})$.

1.

1. (a) If $wt(k) = m$, then calculate $c = \oplus k_i$, $1 \leq i \leq 2m$.
   (b) Else if $wt(k) > m$, then $c = 1$.
   (c) Else $c = 0$.

2. For $1 \leqslant i \leqslant 2m$,

   (a) if $M'_{\alpha,i} = 0$ and $k_i = \bar{c}$, set $Q_{1,i}$ (or $Q_{2,i} \dots$ or $Q_{N,i} = |0\rangle$;
   (b) if $M'_{\alpha,i} = 1$ and $k_i = \bar{c}$, set $Q_{1,i}$ (or $Q_{2,i} \dots$ or $Q_{N,i} = |1\rangle$;
   (c) if $M'_{\alpha,i} = 0$ and $k_i = c$, set $Q_{1,i}$ (or $Q_{2,i} \dots$ or $Q_{N,i} = |+\rangle$;
   (d) if $M'_{\alpha,i} = 1$ and $k_i = c$, set $Q_{1,i}$ (or $Q_{2,i} \dots$ or $Q_{N,i} = |-\rangle$.

Let an adversary A constructs a $2m$-bit string $\tau = \tau_1 \tau_2 \dots \tau_{2m}$, from the measurement results in such a way that, if $\mathcal{M}[i] = |\Phi_l^+\rangle$ for some $l \in \{0, 1, \dots, 2^{(N-1)} - 1\}$, then $\tau_i = 0$, else if $\mathcal{M}[i] = |\Phi_l^-\rangle$ for some $l \in \{0, 1, \dots, 2^{(N-1)} - 1\}$, then $\tau_i = 1$. Now m-bit string $\eta = M_{1_\Delta} \oplus M_2 \oplus \dots \oplus M_N$ is a subsequence of τ. If A can guess η from τ with some low probability, then also it can not get any information about $\mu = M_1 \oplus M_2 \oplus \dots \oplus M_N$ as $\mu = \eta \oplus k'$, where k' is unknown to him/her. Then from the notion of security of the famous "one time pad" protocol [283], we can say that our proposed protocol is secure.

It is to be noted that, if $\mathcal{P}_1$ is dishonest, then he/she can cheat and get the exact XOR value, whereas the other participants get some random value instead of the exact XOR value. This thing happens in the following way: $\mathcal{P}_1$ calculates $M_{1_\Delta} = M_1 \oplus R$, where $R \neq k'$ is a random m-bit number and it is used instead of k'. Then $\mathcal{P}_1$ follows all the next steps of the protocol. At the end of the protocol, everyone get $M_{1_\Delta} \oplus M_2 \oplus \dots \oplus M_N$. Then $\mathcal{P}_2, \dots, \mathcal{P}_N$ calculate $M_1 \oplus M_2 \oplus \dots \oplus M_N = k' \oplus M_{1_\Delta} \oplus M_2 \oplus \dots \oplus M_N$, which is not true as $R \neq k'$. But, $\mathcal{P}_1$ calculates $M_1 \oplus M_2 \oplus \dots \oplus M_N = R \oplus M_{1_\Delta} \oplus M_2 \oplus \dots \oplus M_N$, which is correct. That is, after executing the protocol, $\mathcal{P}_1$ has the exact value of $M_1 \oplus M_2 \oplus \dots \oplus M_N$ and other participants have the value of $k' \oplus R \oplus M_1 \oplus M_2 \oplus \dots \oplus M_N$, which is nothing but a random number.

Thus here we are assuming that $\mathcal{P}_1$ is semi-honest, that is, follows the protocol properly.

Hence each participant gets the computed XOR-value exactly, but no other party can not get any information about the value.

8.4 Discussion

In this chapter, first we present three protocols, two of them for the Q.Conf, i.e., securely and simultaneously exchanging secret messages between the participants. The first protocol is for three parties and then we generalize it to a multi-party scenario, i.e., for N-parties (where $N \geqslant 3$). Another protocol presented in this paper is for multi-party XOR computation, where N-parties can compute the XOR function of their own numbers, but their numbers remain private. All the protocols discussed above are proven to be correct and secure.

Table 8.3: Different cases in Four Party Q.Conf.

Qubits sent by				Probability (Eve's end)															Communicated Bits			
$\mathcal{P}_1$	$\mathcal{P}_2$	$\mathcal{P}_3$	$\mathcal{P}_4$	$\|\phi_0^+\rangle$	$\|\phi_0^-\rangle$	$\|\phi_1^+\rangle$	$\|\phi_1^-\rangle$	$\|\phi_2^+\rangle$	$\|\phi_2^-\rangle$	$\|\phi_3^+\rangle$	$\|\phi_3^-\rangle$	$\|\phi_4^+\rangle$	$\|\phi_4^-\rangle$	$\|\phi_5^+\rangle$	$\|\phi_5^-\rangle$	$\|\phi_6^+\rangle$	$\|\phi_6^-\rangle$	$\|\phi_7^+\rangle$	$\|\phi_7^-\rangle$	by $\mathcal{P}_1$	by $\mathcal{P}_2$	by $\mathcal{P}_3$	by $\mathcal{P}_4$
$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	1/2	1/2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	0	0	1/2	1/2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	0	0	0	0	1/2	1/2	0	0	0	0	0	0	0	0	0	0	0	0	1	0
$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	0	0	0	0	0	0	1/2	1/2	0	0	0	0	0	0	0	0	0	0	1	1
$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	0	0	0	0	0	0	0	0	1/2	1/2	0	0	0	0	0	0	0	1	0	0
$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	0	0	0	0	0	0	0	0	0	0	1/2	1/2	0	0	0	0	0	1	0	1
$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	0	0	0	0	0	0	0	0	0	0	0	0	1/2	1/2	0	0	0	1	1	0
$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1/2	1/2	0	1	1	1
$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1/2	1/2	1	0	0	0
$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	0	0	0	0	0	0	0	0	0	0	0	0	1/2	1/2	0	0	1	0	0	1
$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	0	0	0	0	0	0	0	0	0	0	1/2	1/2	0	0	0	0	1	0	1	0
$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	0	0	0	0	0	0	0	0	1/2	1/2	0	0	0	0	0	0	1	0	1	1
$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	0	0	0	0	0	0	1/2	1/2	0	0	0	0	0	0	0	0	1	1	0	0
$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	0	0	0	0	1/2	1/2	0	0	0	0	0	0	0	0	0	0	1	1	0	1
$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	0	0	1/2	1/2	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0
$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	1/2	1/2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1
$\|+\rangle$	$\|+\rangle$	$\|+\rangle$	$\|+\rangle$	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	0	0	0	0
$\|+\rangle$	$\|+\rangle$	$\|+\rangle$	$\|-\rangle$	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	0	0	1
$\|+\rangle$	$\|+\rangle$	$\|-\rangle$	$\|+\rangle$	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	0	1	0
$\|+\rangle$	$\|+\rangle$	$\|-\rangle$	$\|-\rangle$	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	0	0	1	1
$\|+\rangle$	$\|-\rangle$	$\|+\rangle$	$\|+\rangle$	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1	0	0
$\|+\rangle$	$\|-\rangle$	$\|+\rangle$	$\|-\rangle$	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	0	1	0	1
$\|+\rangle$	$\|-\rangle$	$\|-\rangle$	$\|+\rangle$	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	0	1	1	0
$\|+\rangle$	$\|-\rangle$	$\|-\rangle$	$\|-\rangle$	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1	1	1
$\|-\rangle$	$\|+\rangle$	$\|+\rangle$	$\|+\rangle$	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	1	0	0	0
$\|-\rangle$	$\|+\rangle$	$\|+\rangle$	$\|-\rangle$	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1	0	0	1
$\|-\rangle$	$\|+\rangle$	$\|-\rangle$	$\|+\rangle$	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1	0	1	0
$\|-\rangle$	$\|+\rangle$	$\|-\rangle$	$\|-\rangle$	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	1	0	1	1
$\|-\rangle$	$\|-\rangle$	$\|+\rangle$	$\|+\rangle$	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1	1	0	0
$\|-\rangle$	$\|-\rangle$	$\|+\rangle$	$\|-\rangle$	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	1	1	0	1
$\|-\rangle$	$\|-\rangle$	$\|-\rangle$	$\|+\rangle$	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	1	1	1	0
$\|-\rangle$	$\|-\rangle$	$\|-\rangle$	$\|-\rangle$	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1/8	0	1	1	1	1

Chapter 9

Dimensionality Distinguisher

In this chapter, we present the work [284], where we generalize the CHSH game and define two classes of new games which are similar to the CHSH game. The first one is for 2-variables and the second one is for 3-variables. In this class of new games we change the winning condition of CHSH game. Instead of a particular Boolean function in CHSH game, we use all Boolean functions and find equivalence class for functions pair and bases such that, all the elements of the same class have the same winning probability of the game. We also consider all possible measurements subject to a precision parameter. For both the games, we optimize the winning probabilities. Finally, we show how our results can be used to devise three classes of dimensionality distinguishers, particularly between dimensions 2 and 3.

The efficiency of a distinguisher depends on the number of samples (for a given success probability) and that in turn depends on the gap between the probabilities. This issue has been discussed in detail in [285]. Moreover, there are some works [286] on how to deal with finite number of samples. For the time being, we are not focusing on these types of analysis. Rather, our main goal is to identify the distinguishing events with a significant probability gap and that is what we report here.

9.1 Generalized version of CHSH game

We generalize the well known CHSH game to produce two types of new games. The first type of games are for 2-variables (i.e., each question has 2 options to answer). The other type of

games are for 3-variables (i.e., each question has 3 options to answer).

Here also we assume that Alice and Bob are far away from each other and not able to communicate during the game. Before the game begins, they can communicate freely to discuss their strategy. During the game, they only communicate with the referee.

9.1.1 New games for 2-variables (Game-1)

Our new games are similar to the CHSH game. The only exception is in the winning condition. Here the winning condition is $f(x, y) = g_2(a, b)$, where f and g_2 are any two variable Boolean functions other than the constant functions (the subscript 2 in g_2 is for 2-variables). For 2 variables, there are $(2^2)^2 = 16$ possible Boolean functions. Among them 2 are constant functions. So we are playing this game with $14 \times 14 = 196$ pairs of functions where in CHSH game there is only one pair.

Rules of Game-1

For a fixed pair of two variable Boolean functions (f, g_2) we define Game-1 as follows:

• The referee chooses two independent random bits x and y uniformly (also called "questions") and sends x to Alice and y to Bob, i.e., for all $s \in \{0, 1\},\ t \in \{0, 1\},\ \Pr(x = s, y = t) = \Pr_{xy}(s, t) = \dfrac{1}{4}$.

• Alice and Bob reply to referee with bits a and b respectively.

• Referee calculates $f(x, y)$ and $g_2(a, b)$.

• Alice and Bob win if $f(x, y) = g_2(a, b)$.

Quantum strategy for Game-1

Alice and Bob follow the following strategy Algorithm 8 to play Game-1. Here also they share a maximally entangled state and choose measurement bases according to the referee's questions. They measure their qubits and send their answers to the referee. Alice's choice of measurement basis is only depends on referee's question. But for each pair (f, g_2), Bob chooses the basis

for which they can achieve maximum winning probability. Bob's bases are dependent on the parameters θ_0 and θ_1. So for different pairs of functions (f, g_2), the values of θ_0 and θ_1 change. For example, CHSH game is a special case of Game-1, where $f = AND$, $g_2 = XOR$, and Bob chooses $\theta_0 = \frac{\pi}{8}$ and $\theta_1 = \frac{15\pi}{8}$.

Algorithm 8: Quantum strategy for Game-1

1. Before the game starts, Alice and Bob share $|\Psi_{AB}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B)$
2. Alice takes the first qubit and Bob takes the second qubit
3. **Alice chooses:**
   - Standard basis $\{|0\rangle, |1\rangle\}$ if $x = 0$
   - Hadamard basis $\{|0_x\rangle, |1_x\rangle\}$ if $x = 1$, where $|0_x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|1_x\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
4. **Bob chooses:**
   Basis $\{|\nu_0(\theta_y)\rangle, |\nu_1(\theta_y)\rangle\}$ corresponding to $y = 0, 1$,
   where $|\nu_0(\theta_y)\rangle = \cos\theta_y |0\rangle + \sin\theta_y |1\rangle$, $|\nu_1(\theta_y)\rangle = \sin\theta_y |0\rangle - \cos\theta_y |1\rangle$, $0 \leqslant \theta_0, \theta_1 \leqslant 2\pi$
5. **Alice sends:**
   - $a = 0$ if $|0\rangle$ or $|0_x\rangle$
   - $a = 1$ otherwise
6. **Bob sends:**
   - $b = 0$ if Bob gets $|\nu_0(\theta_0)\rangle$ or $|\nu_0(\theta_1)\rangle$
   - $b = 1$ otherwise

Success probabilities of Game-1

We find the success probability of the game for each f and g_2 by using Equation (1.1), when the players follow the above strategy with changes in the chosen bases of Bob. Here Bob does not fix the value of θ_0 and θ_1. For different pairs of function (f, g_2) the value of the pair $(\theta_0$,

θ_1) changes as the expression of the winning probability changes.

For simplicity, we write an n-variable Boolean function as a 2^n-length binary vector consisting of the last column of the truth table in lexicographical order, e.g., for a two variable function, we write

$$f(x,y) = [f(0,0), f(0,1), f(1,0), f(1,1)] \text{ and } g_2(a,b) = [g_2(0,0), g_2(0,1), g_2(1,0), g_2(1,1)].$$

The results are in the following Table 9.1. The first two columns of Table 9.1 represent the functions of inputs and outputs (i.e., $f(x,y)$ and $g_2(a,b)$)respectively, and corresponding success probabilities are given in third column. The number of such function pair (f, g_2) having same success probabilities are in the last column.

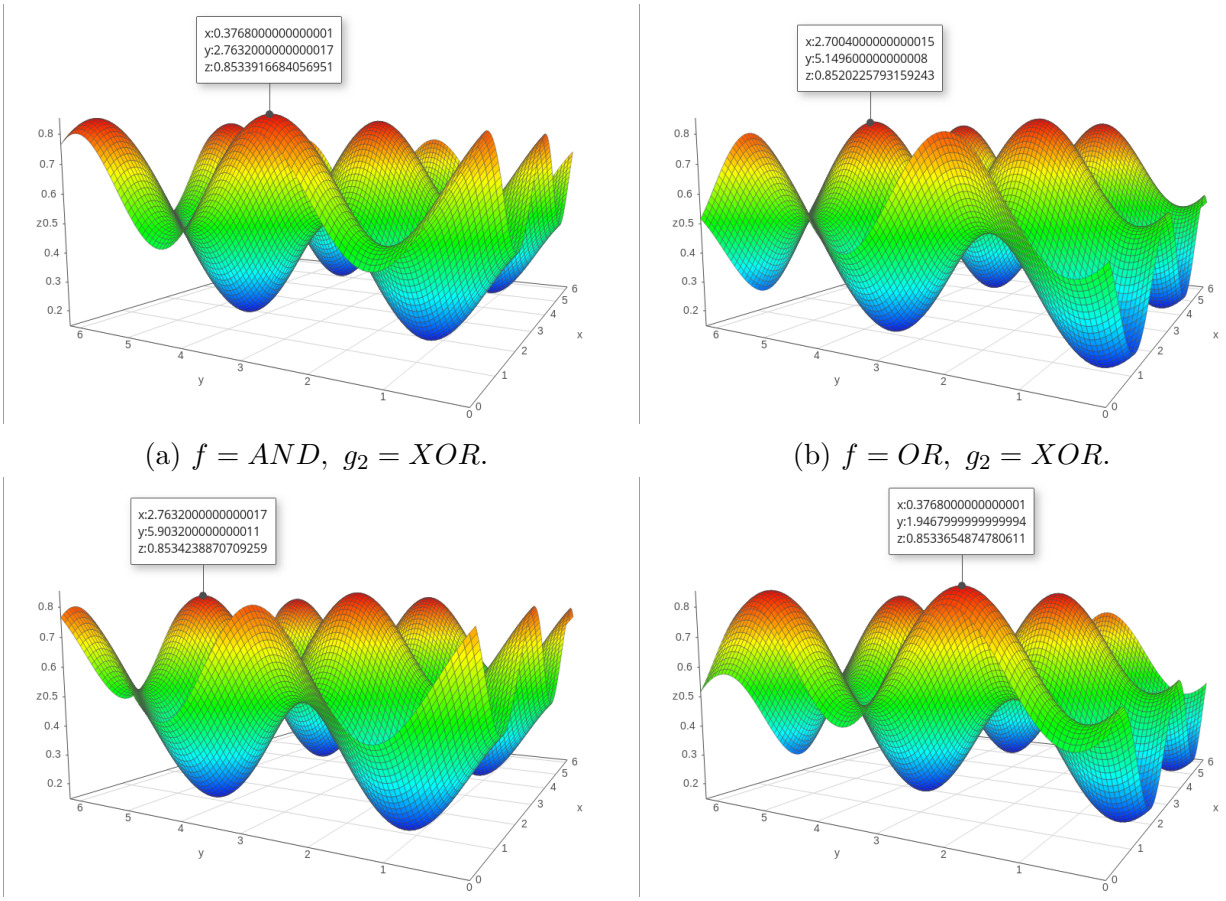
Table 9.1: Success probabilities of Game-1 with any non-constant 2 variables Boolean functions f and g

LHS of winning condition $f(x,y)$	RHS of winning condition $g_2(a,b)$	Success probability	Number of such function pair (f, g_2)
any non constant f	XOR, XNOR	0.85	28
$f(x,y)$ contains one 0	$g_2(a,b)$ contains one 0	0.80	32
$f(x,y)$ contains one 1	$g_2(a,b)$ contains one 1	0.80	32
$f(x,y)$ contains two 0	$g_2(a,b)$ contains either exactly one 1 or 0	0.67	48
$f(x,y)$ contains one 1	$g_2(a,b)$ contains one 0	0.55	16
$f(x,y)$ contains one 0	$g_2(a,b)$ contains one 1	0.55	6
Any non-constant f	$g_2(a,b) = a,\ b,\ \bar{a},\ \bar{b}$	0.5	56

Observation

From Table 9.1, we observe that the winning probability is maximum when $g_2(a,b) = a \oplus b$ and $a \odot b$, i.e., for any non-constant 2 variables Boolean function f, if $g_2 = XOR$ or $g_2 = XNOR$ then by playing the Game-1 we can win the game with probability 0.85.

The reason behind this is that the probability graph of these 28 cases are almost similar. To illustrate this, we show some probability graphs in Figure 9-1. In these graphs we plot θ_0 (x-axis) vs. θ_1(y-axis) vs. success probability expression (z-axis). From these graphs we can see that for each case the success probabilities are periodic functions of (θ_0, θ_1) and achieve



(a) $f = AND,\ g_2 = XOR.$ (b) $f = OR,\ g_2 = XOR.$

(c) $f = x,\ g_2 = XOR.$ (d) $f = y,\ g_2 = XOR.$

Figure 9-1: Success probability graphs for 4 different cases of Game-1 with non-constant 2 variables Boolean functions f and g_2.

maximum value 0.85 at more than one points.

• The first graph in Figure 9-1(a) represents the success probability $\frac{1}{4}[1+cos^2\theta_0+cos^2\theta_1+\frac{1}{2}sin2\theta_0-\frac{1}{2}sin2\theta_1]$ corresponding to the function pair $(f = AND,\ g_2 = XOR)$ and one of its maximum point is at $\left(\theta_0 = \frac{\pi}{8}, \theta_1 = \frac{15\pi}{8}\right)$.

• The second graph in Figure 9-1(b) represents the success probability $\frac{1}{4}[1+cos^2\theta_0+sin^2\theta_1-\frac{1}{2}sin2\theta_0-\frac{1}{2}sin2\theta_1]$ corresponding to the function pair $(f = OR,\ g_2 = XOR)$ and one of its maximum point is at $\left(\theta_0 = \frac{7\pi}{8}, \theta_1 = \frac{5\pi}{8}\right)$.

• The third graph in Figure 9-1(c) represents the success probability $\frac{1}{4}[1+cos^2\theta_0+cos^2\theta_1-\frac{1}{2}sin2\theta_0-\frac{1}{2}sin2\theta_1]$ corresponding to the function pair $(f = x,\ g_2 = XOR)$, where $f = x$ means $f(x, y) = x\ \forall\ x, y \in \{0, 1\}$, and one of its maximum point is at $\left(\theta_0 = \frac{7\pi}{8}, \theta_1 = \frac{7\pi}{8}\right)$.

• The fourth graph in Figure 9-1(d) represents the success probability $\frac{1}{4}[1+cos^2\theta_0+sin^2\theta_1+$

$\frac{1}{2}sin2\theta_0 - \frac{1}{2}sin2\theta_1]$ corresponding to the function pair $(f = y,\ g_2 = XOR)$, where $f = y$ means $f(x, y) = y\ \forall\ x, y \in \{0, 1\}$, and one of its maximum point is at $\left(\theta_0 = \frac{9\pi}{8}, \theta_1 = \frac{5\pi}{8}\right)$.

9.1.2 New games for 3-variables (Game-2)

In this game there are two players, namely, Alice and Bob (they are far away from each other and not able to communicate) and a referee. Let us define the sets $S = \{0, 1, 2\}$, $\mathcal{G} = \{g : S \times S \to \{0, 1\}\}$ and $\mathcal{F} = \{f : f\ is\ a\ 2\ variable\ Boolean function\}$.

Rules of Game-2

For a particular pair (f, g_3), where $f \in \mathcal{F}$ and $g_3 \in \mathcal{G}$ (the subscript 3 in g_3 is for 3-variables), we define Game-2 as follows:

• The referee chooses two independent random bits x and y uniformly (also called "questions") and sends x to Alice and y to Bob. That is, for all $s \in \{0, 1\},\ t \in \{0, 1\},\ Pr(x = s, y = t) = P_{xy}(s, t) = \frac{1}{4}$.

• Alice and Bob send their answers a and b $(a, b \in \{0, 1, 2\})$ to the referee.

• Referee calculates $f(x, y)$ and $g_3(a, b)$.

• Alice and Bob win if $f(x, y) = g_3(a, b)$.

Quantum strategy for Game-2

Now let Alice and Bob play the game with the following strategy given in Algorithm 9. Before the game starts, they share a maximally entangled bipartite state: $|\Psi_{AB}\rangle = \frac{1}{\sqrt{3}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B + |2\rangle_A \otimes |2\rangle_B)$ in the Hilbert space $\mathbb{C}^3 \otimes \mathbb{C}^3$. According to the referee's questions, they choose measurement bases to measure their qubits and send their answers to the referee. Alice's choice of measurement basis is only depends on referee's question. But for each pair (f, g_3), Bob choose the basis for which they can achieve maximum winning probability. Bob's bases are dependent on the parameters θ_0 and θ_1.

Algorithm 9: Quantum strategy for Game-2

1. Before the game starts, Alice and Bob share
   $|\Psi_{AB}\rangle = \frac{1}{\sqrt{3}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B + |2\rangle_A \otimes |2\rangle_B)$
2. Alice takes the first qubit and Bob takes the second qubit
3. **Alice chooses:**
   - Standard basis $\{|0\rangle, |1\rangle, |2\rangle\}$ if $x = 0$
   - Fourier basis $\{|0_x\rangle, |1_x\rangle, |2_x\rangle\}$ if $x = 1$, where
     $|0_x\rangle = \frac{1}{\sqrt{3}}(|0\rangle + |1\rangle + |2\rangle)$, $|1_x\rangle = \frac{1}{\sqrt{3}}(|0\rangle + \omega|1\rangle + \omega^2|2\rangle)$,
     $|2_x\rangle = \frac{1}{\sqrt{3}}(|0\rangle + \omega^2|1\rangle + \omega|2\rangle)$ and $\omega = e^{2\pi i/3}$
4. **Bob chooses:**
   - Basis $\{|\psi_0\rangle, |\psi_1\rangle, |\psi_2\rangle\}$ if $y = 0$,
     $|\psi_0\rangle = \cos\theta_0|0\rangle + \sin\theta_0\cos\theta_1|1\rangle + \sin\theta_0\sin\theta_1|2\rangle$
     $|\psi_1\rangle = \sin\theta_0|0\rangle - \cos\theta_0\cos\theta_1|1\rangle - \cos\theta_0\sin\theta_1|2\rangle$
     $|\psi_2\rangle = \sin\theta_1|1\rangle + \cos\theta_1|2\rangle$ and
     $0 \leqslant \theta_0, \theta_1 \leqslant 2\pi$
   - Basis $\{|\phi_0\rangle, |\phi_1\rangle, |\phi_2\rangle\}$ if $y = 1$,
     $|\phi_0\rangle = \cos\theta_1|0\rangle + \sin\theta_1\cos\theta_0|1\rangle + \sin\theta_1\sin\theta_0|2\rangle$
     $|\phi_1\rangle = \sin\theta_1|0\rangle - \cos\theta_1\cos\theta_0|1\rangle - \cos\theta_1\sin\theta_0|2\rangle$
     $|\phi_2\rangle = \sin\theta_0|1\rangle + \cos\theta_0|2\rangle$ and
     $0 \leqslant \theta_0, \theta_1 \leqslant 2\pi$
5. **Alice sends:**
   - $a = 0$ if Alice gets $|0\rangle$ or $|0_x\rangle$
   - $a = 1$ if she gets $|1\rangle$ or $|1_x\rangle$
   - $a = 2$ otherwise
6. **Bob sends:**
   - $b = 0$ if Bob gets $|\psi_0\rangle$ or $|\phi_0\rangle$
   - $b = 1$ if he gets $|\psi_1\rangle$ or $|\phi_1\rangle$
   - $b = 2$ otherwise

Example of Game-2

Let us take an example. Let $f(x, y) = x \wedge y$ and $g_3(a, b) = a\ Embedded\ XOR\ b$ (i.e., $g_3(a, b) = 0\ if\ a = b\ and\ g_3(a, b) = 1\ otherwise$). If we play the above game with these f and g_3 then the success probability is 0.76 at $\theta_0 = \frac{17\pi}{16}, \theta_1 = \frac{\pi}{16}$.

9.1.3 Maximum winning probability

In this Game-2 the maximum winning probability is 0.86 only for 8 pair of functions (f, g_3).

Now the functions pairs, with the highest winning probability and corresponding bases are shown in Table 9.2.

Table 9.2: Functions pairs with maximum success probabilities of Game-2

f	g_3	θ_0	θ_1
[0, 1, 0, 0]	[0, 1, 0, 1, 0, 0, 0, 0, 1]	$33\pi/32$	$19\pi/32$
[0, 1, 0, 0]	[1, 0, 0, 0, 0, 1, 0, 1, 0]	$29\pi/32$	$29\pi/32$
[0, 1, 1, 1]	[0, 1, 1, 1, 1, 0, 1, 0, 1]	$29\pi/32$	$15\pi/32$
[0, 1, 1, 1]	[1, 0, 1, 0, 1, 1, 1, 1, 0]	$19\pi/32$	$33\pi/32$
[1, 0, 0, 0]	[0, 1, 0, 1, 0, 0, 0, 0, 1]	$19\pi/32$	$33\pi/32$
[1, 0, 0, 0]	[1, 0, 0, 0, 0, 1, 0, 1, 0]	$29\pi/32$	$15\pi/32$
[1, 0, 1, 1]	[0, 1, 1, 1, 1, 0, 1, 0, 1]	$15\pi/32$	$29\pi/32$
[1, 0, 1, 1]	[1, 0, 1, 0, 1, 1, 1, 1, 0]	$33\pi/32$	$19\pi/32$

9.1.4 Equivalence classes

From the results of these two games we observe that, if we introduce some equivalence relations to make partition of the set of data in each game result, then we will take only one element of each equivalence class to play these games. It will reduce the time and space complexity of these games. Also if some measurement setup will be unavailable then we can use any other setup from the same class to continue the games. Here we take three equivalence relations to make three different types of partitions of the results.

1. We can make an equivalence class of the bases of Bob for a fixed function pair (f, g_i), $(i = 2, 3)$, such that all elements of the same class give the same success probability.

For simplicity, we only write the value of the pair (θ_1, θ_2) as a basis (i.e., we represent a basis as a point (θ_1, θ_2) in $\mathbb{R}^2$) in a class and we take the values in *radian* (i.e., $0 \leqslant \theta_1, \theta_2 \leqslant 2\pi$) and as a multiple of $\frac{\pi}{32}$.

For example, if we fix $f = AND$ and $g_2 = XOR$ in Game-1, then there are 8 equivalence classes of bases (up to 1 significant digit). Now in the previous example, if we consider the success probabilities up to 2 significant digits, then there are 4 elements in the class of highest winning probability 0.85 and the class is

$$\left\{\left(\frac{\pi}{8}, \frac{7\pi}{8}\right), \left(\frac{\pi}{8}, -\frac{\pi}{8}\right), \left(-\frac{7\pi}{8}, \frac{7\pi}{8}\right), \left(-\frac{7\pi}{8}, -\frac{\pi}{8}\right)\right\}.$$

Again in Game-2, let $f = AND$ and $g_3 = Embedded\ XOR$ (i.e. $g_3(a, b) = 0\ if\ a = b\ and\ g_3(a, b) = 1\ otherwise$) , then there are 7 equivalence classes of bases (up to 1 significant digit). Now in the previous example, if we consider the success probabilities up to 2 significant digits, then there are 4 elements in the class of highest winning probability 0.76 and the class is

$$\left\{\left(\frac{33\pi}{32}, \frac{\pi}{32}\right), \left(\frac{33\pi}{32}, \frac{2\pi}{32}\right), \left(\frac{34\pi}{32}, \frac{\pi}{32}\right), \left(\frac{34\pi}{32}, \frac{2\pi}{32}\right)\right\}.$$

2. Secondly, we fix the bases of Bob and vary the function pairs to make the equivalence classes. Here also all the elements of the same class have the same winning probability.

   For example, in Game-1, if we fix $\left(\theta_1 = \frac{\pi}{8}, \theta_2 = -\frac{\pi}{8}\right)$, then $(f = [0, 0, 0, 1],\ g_2 = [0, 1, 0, 1])$, $(f = [0, 0, 1, 0],\ g_2 = [0, 1, 0, 1])$, $(f = [0, 0, 1, 1],\ g_2 = [0, 1, 0, 1])$, $(f = [0, 1, 1, 1],\ g_2 = [0, 1, 0, 1])$ etc. are all belong to the same class with success probability 0.5.

3. At last, we vary both functions pairs and Bob's bases and the tuples which have the same winning probability are belong to the same class. E.g., in Game-2, each row of Table 9.2 have the same success probability 0.86 and thus they belong to the same class.

9.2 Dimensionality testing

We observe the winning probabilities of various cases in Game-1 and Game-2.

By using the above two games we can make device independent dimension distinguisher to distinguish between the states $|\Psi_{AB}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B)$ and $|\Phi_{AB}\rangle = \frac{1}{\sqrt{3}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B + |2\rangle_A \otimes |2\rangle_B)$. For example:

• In Game-1, if we take $f(x, y) = x \wedge y$ and $g_2(a, b) = a \oplus b$ and $\theta_0 = \frac{\pi}{8}$, $\theta_1 = -\frac{\pi}{8}$, then the winning probability of this game is 0.85.

• In Game-2, if we take $f(x, y) = x \wedge y$ and $g_3 = Embedded\ XOR$ and $\theta_0 = \frac{\pi}{8}$, $\theta_1 = -\frac{\pi}{8}$, then winning probability of this game is 0.76.

So by playing these games and observing winning probabilities we can easily distinguish between $|\Psi_{AB}\rangle$ and $|\Phi_{AB}\rangle$. In other words, we can say the dimension of the given maximally state is two or three.

We can think this whole process as a union of two black boxes. An initial black box is the state preparatory which prepares states of form either $|\Psi_{AB}\rangle$ or $|\Phi_{AB}\rangle$. the prepared state is then sent to a second black box, the measurement device. In this box, if the states are $|\Psi_{AB}\rangle$, it will follow the process of Game-1 and if the states are $|\Phi_{AB}\rangle$, it will follow the process of Game-2.

From the outputs of this measurement device we will calculate the winning probability of the game played in this box and compare this probability with the success probabilities of Game-1 and Game-2. So we have a dimension distinguisher. The protocol is described in Algorithm 10.

Following the above process and by changing the functions pairs in the games we can devise many distinguishers (for each, we use the function pair (f, g_3) in Game-2 and the function pair (f, g_2') in Game-1 (where, g_2' is the restriction of g_3 in 2 variables, i.e., $g_2'(a, b) = [g_3(0, 0), g_3(0, 1), g_3(1, 0), g_3(1, 1)]$). We divide the set of all distinguisher into 3 classes according to the winning probabilities of the games.

Algorithm 10: Dimension distinguisher of maximally entangled state

Input: n number of maximally entangled bipartite state $|\Psi_{AB}\rangle$ in an Hilbert space $\mathbb{C}^d \times \mathbb{C}^d$ which is of the form $\sum_{i=1}^{d} \frac{1}{\sqrt{d}} |i\rangle \otimes |i\rangle$, where $\{|i\rangle\}$ is the standard basis of $\mathbb{C}^d$ and $d \in \{2, 3\}$ is fixed but unknown.

Output: The value of d.

1. For rounds $i \in \{1, \ldots, n\}$

   (a) Referee chooses $x_i \in \{0, 1\}$ and $y_i \in \{0, 1\}$ uniformly at random.

   (b) • If $x_i = 0$, Alice measures the first particle of the entangled state in the standard basis $\{|0\rangle, |1\rangle, |2\rangle\}$
   • If $x_i = 1$, she measures that in the Fourier basis $\{|0_x\rangle, |1_x\rangle, |2_x\rangle\}$, where
   $|0_x\rangle = \frac{1}{\sqrt{3}}(|0\rangle + |1\rangle + |2\rangle)$,
   $|1_x\rangle = \frac{1}{\sqrt{3}}(|0\rangle + \omega |1\rangle + \omega^2 |2\rangle)$,
   $|2_x\rangle = \frac{1}{\sqrt{3}}(|0\rangle + \omega^2 |1\rangle + \omega |2\rangle)$
   and $\omega = e^{2\pi i/3}$. (if $d = 2$ it will be the Hadamard basis).

   (c) Similarly,
   • if $y_i = 0$, Bob measures the second particle of the entangled state in $\{|\psi_0\rangle, |\psi_1\rangle, |\psi_2\rangle\}$ basis , where
   $|\psi_0\rangle = \cos\theta_0 |0\rangle + \sin\theta_0 \cos\theta_1 |1\rangle + \sin\theta_0 \sin\theta_1 |2\rangle$
   $|\psi_1\rangle = \sin\theta_0 |0\rangle - \cos\theta_0 \cos\theta_1 |1\rangle - \cos\theta_0 \sin\theta_1 |2\rangle$ and
   $|\psi_2\rangle = \sin\theta_1 |1\rangle + \cos\theta_1 |2\rangle$.
   If $d = 2$, $\theta_0 = \frac{\pi}{8}, \theta_1 = 0$ and if $d = 3$, $\theta_0 = \frac{\pi}{8}, \theta_1 = -\frac{\pi}{8}$.
   • And if $y_i = 1$, he measures that in $\{|\phi_0\rangle, |\phi_1\rangle, |\phi_2\rangle\}$ basis, where
   $|\phi_0\rangle = \cos\theta_1 |0\rangle + \sin\theta_1 \cos\theta_0 |1\rangle + \sin\theta_1 \sin\theta_0 |2\rangle$
   $|\phi_1\rangle = \sin\theta_1 |0\rangle - \cos\theta_1 \cos\theta_0 |1\rangle - \cos\theta_1 \sin\theta_0 |2\rangle$ and
   $|\phi_2\rangle = \sin\theta_0 |1\rangle + \cos\theta_0 |2\rangle$.
   If $d = 2$, $\theta_0 = 0, \theta_1 = \frac{\pi}{8}$ and if $d = 3$, $\theta_0 = \frac{\pi}{8}, \theta_1 = -\frac{\pi}{8}$.

   (d) The output is recorded as $a_i(b_i) \in \{0, 1, 2\}$ for the first (second) particle. The encoding for $a_i(b_i)$ is as follows.
   • For the first particle of each pair, $a_i = i$ if the measurement result is $|i\rangle$ or $|i_x\rangle$.
   • For the second particle of each pair, $b_i = 0$ if the measurement result is $|\psi_0\rangle$ or $|\phi_0\rangle$;
   $b_i = 1$ if the measurement result is $|\psi_1\rangle$ or $|\phi_1\rangle$;
   and $b_i = 2$ if the measurement result is $|\psi_2\rangle$ or $|\phi_2\rangle$.

   (e) For the test round i, define

$$Y_i = \begin{cases} 1 & \text{if } x_i \wedge y_i = g(a_i, b_i) \text{ where g=Embedded XOR} \\ 0 & \text{if otherwise} \end{cases}$$

2. Referee calculates $S = \frac{1}{n} \sum Y_i$.

3. If $S \approx 0.85$ return $d = 2$ and if $S \approx 0.76$ return $d = 3$.

9.2.1 First class of distinguishers (D_1)

In this set, we put all the distinguishers where we choose functions pairs (f, g_3) such that the functions pair (f, g_2') has the highest winning probability in Game-1 (i.e., 0.85) which is greater than the winning probability of corresponding Game-2.

If we choose $f = [0, 1, 0, 0], g_3 = [0, 1, 1, 1, 0, 1, 1, 1, 0]$, thus $g_2' = [0, 1, 1, 0]$ (or $f = [0, 1, 1, 1], g_3 = [1, 0, 0, 0, 1, 0, 0, 0, 1]$, thus $g_2' = [0, 1, 1, 0]$), then the winning probabilities of the Game-1 and Game-2 are 0.85 and 0.58. Therefore the difference of these probabilities is 0.27, which is quite good.

There are many distinguishers in this class. We put some of them into the following Table 9.3. Here we take the winning probability for $d = 3$ at that point where the corresponding winning probability for $d = 2$ is maximum.

Table 9.3: Table for D_1

f	g_2'	g_3	W.P. if $d = 2$	W.P. if $d = 3$	Difference
[0, 0, 0, 1]	[0, 1, 1, 0]	[0, 1, 0, 1, 0, 0, 0, 1, 1]	0.85	0.53	0.32
[0, 0, 0, 1]	[0, 1, 1, 0]	[0, 1, 0, 1, 0, 0, 1, 1, 1]	0.85	0.51	0.34
[0, 0, 0, 1]	[1, 0, 0, 1]	[1, 0, 1, 0, 1, 1, 1, 1, 1]	0.85	0.45	0.4
[0, 0, 1, 0]	[1, 0, 0, 1]	[1, 0, 0, 0, 1, 1, 1, 0, 1]	0.85	0.41	0.44
[0, 0, 1, 1]	[0, 1, 1, 0]	[0, 1, 0, 1, 0, 0, 0, 0, 1]	0.85	0.39	0.46
[0, 1, 0, 0]	[0, 1, 1, 0]	[0, 1, 1, 1, 0, 1, 1, 1, 1]	0.85	0.42	0.43
[0, 1, 0, 1]	[0, 1, 1, 0]	[0, 1, 1, 1, 0, 1, 0, 1, 0]	0.85	0.46	0.39
[0, 1, 1, 1]	[0, 1, 1, 0]	[0, 1, 0, 1, 0, 1, 0, 1, 0]	0.85	0.45	0.4
[1, 0, 0, 1]	[1, 0, 0, 1]	[1, 0, 1, 0, 1, 0, 1, 0, 1]	0.85	0.53	0.32
[1, 0, 1, 0]	[1, 0, 0, 1]	[1, 0, 0, 0, 1, 0, 1, 0, 1]	0.85	0.46	0.39
[1, 0, 1, 1]	[0, 1, 1, 0]	[0, 1, 0, 1, 0, 1, 0, 0, 0]	0.85	0.44	0.41
[1, 1, 0, 0]	[1, 0, 0, 1]	[1, 0, 1, 0, 1, 1, 1, 1, 0]	0.85	0.39	0.46
[1, 1, 1, 0]	[0, 1, 1, 0]	[0, 1, 1, 1, 0, 0, 0, 0, 0]	0.85	0.41	0.44

**W.P denotes winning probability.*

9.2.2 Second class of distinguishers (D_2)

In this set, we put all the distinguishers where we choose functions pairs (f, g_3) such that it has the highest winning probability in Game-2 (i.e., 0.86) which is greater than the winning probability of corresponding Game-1 with functions pair (f, g_2'). Here we take the winning probability for $d = 2$ at that point where the corresponding winning probability for $d = 3$ is

maximum.

For example, let $f = [0, 1, 0, 0], g_3 = [1, 0, 0, 0, 0, 1, 0, 1, 0]$ then if $d = 2$ success probability is 0.80 and if $d = 3$ success probability is 0.86. We put all distinguishers in Table 9.4.

Table 9.4: Table for D_2

f	g_2'	g_3	W.P. if $d = 2$	W.P. if $d = 3$	Difference
[0, 1, 0, 0]	[0, 1, 1, 0]	[0, 1, 0, 1, 0, 0, 0, 0, 1]	0.46	0.86	0.4
[0, 1, 0, 0]	[1, 0, 0, 0]	[1, 0, 0, 0, 0, 1, 0, 1, 0]	0.64	0.86	0.22
[0, 1, 1, 1]	[0, 1, 1, 1]	[0, 1, 1, 1, 1, 0, 1, 0, 1]	0.63	0.86	0.23
[0, 1, 1, 1]	[1, 0, 0, 1]	[1, 0, 1, 0, 1, 1, 1, 1, 0]	0.48	0.86	0.38
[1, 0, 0, 0]	[0, 1, 1, 0]	[0, 1, 0, 1, 0, 0, 0, 0, 1]	0.48	0.86	0.38
[1, 0, 0, 0]	[1, 0, 0, 0]	[1, 0, 0, 0, 0, 1, 0, 1, 0]	0.63	0.86	0.23
[1, 0, 1, 1]	[0, 1, 1, 1]	[0, 1, 1, 1, 1, 0, 1, 0, 1]	0.64	0.86	0.22
[1, 0, 1, 1]	[1, 0, 0, 1]	[1, 0, 1, 0, 1, 1, 1, 1, 0]	0.46	0.86	0.4

**W.P denotes winning probability.*

9.2.3 Third class of distinguishers (D_3)

Similarly, we can make dimension distinguisher using other functions pairs for which the difference between the optimal winning probabilities of the two games is non-negligible. Here we take functions pair (f, g_3) and corresponding pair (f, g_2') such that both the games with respective pairs do not achieve the highest winning probabilities. we put all these distinguishers in this set. The cardinality of this set depends on the difference value between winning probabilities.

Let (f, g_3) be a function pair and the highest winning probability of Game-2 with (f, g_3) being p_2 at point (s_2, t_2) and the same of Game-1 with (f, g_2') is p_1 at point (s_1, t_1). We compare p_1, p_2 and take the best (say, $p_1 > p_2$). Then we find the winning probability p of Game-2 at (s_1, t_1) and difference value $p_1 - p$. We make a list of these distinguishers for which the difference value is greater than 0.44 in Table 9.5.

9.3 Discussion

Dimensionality of the states act as a resource in quantum information processing tasks. For many protocols, the performance as well as security depends on the particular value of the

dimension. For this reason, dimensionality testing is very important. There have been several works on dimension witness. We take a different route by constructing dimension distinguishers based on our generalized version of the CHSH game. We demonstrate several classes of practical distinguishers between 2 and 3 dimensions.

Table 9.5: Table for D_3

f	g_2'	g_3	W.P. if $d = 2$	W.P. if $d = 3$	Difference
[0, 0, 0, 1]	[1, 0, 1, 1]	[1, 0, 0, 1, 1, 0, 0, 0, 0]	0.29	0.76	0.47
[0, 0, 0, 1]	[1, 0, 1, 1]	[1, 0, 0, 1, 1, 0, 0, 0, 1]	0.29	0.77	0.48
[0, 0, 0, 1]	[1, 0, 1, 1]	[1, 0, 0, 1, 1, 0, 0, 1, 0]	0.29	0.77	0.48
[0, 0, 0, 1]	[1, 0, 1, 1]	[1, 0, 0, 1, 1, 0, 0, 1, 1]	0.29	0.77	0.48
[0, 0, 0, 1]	[1, 0, 1, 1]	[1, 0, 1, 1, 1, 0, 0, 0, 0]	0.29	0.76	0.47
[0, 0, 0, 1]	[1, 0, 1, 1]	[1, 0, 1, 1, 1, 0, 0, 0, 1]	0.29	0.75	0.46
[0, 0, 0, 1]	[1, 0, 1, 1]	[1, 0, 1, 1, 1, 0, 0, 1, 0]	0.29	0.77	0.48
[0, 0, 0, 1]	[1, 0, 1, 1]	[1, 0, 1, 1, 1, 0, 0, 1, 1]	0.29	0.76	0.47
[0, 0, 1, 0]	[1, 0, 1, 1]	[1, 0, 0, 1, 1, 0, 0, 0, 0]	0.21	0.76	0.55
[0, 0, 1, 0]	[1, 0, 1, 1]	[1, 0, 0, 1, 1, 0, 0, 0, 1]	0.21	0.77	0.56
[0, 0, 1, 0]	[1, 0, 1, 1]	[1, 0, 0, 1, 1, 0, 0, 1, 0]	0.21	0.77	0.56
[0, 0, 1, 0]	[1, 0, 1, 1]	[1, 0, 0, 1, 1, 0, 0, 1, 1]	0.21	0.77	0.56
[0, 0, 1, 0]	[1, 0, 1, 1]	[1, 0, 1, 1, 1, 0, 0, 1, 1]	0.21	0.76	0.55
[0, 0, 1, 1]	[1, 0, 1, 1]	[1, 0, 0, 1, 1, 0, 0, 1, 1]	0.36	0.81	0.45
[0, 0, 1, 1]	[1, 0, 1, 1]	[1, 0, 1, 1, 1, 0, 0, 1, 1]	0.36	0.84	0.48
[1, 1, 0, 0]	[0, 1, 0, 0]	[0, 1, 0, 0, 0, 1, 1, 0, 0]	0.36	0.84	0.48
[1, 1, 0, 0]	[0, 1, 0, 0]	[0, 1, 1, 0, 0, 1, 1, 0, 0]	0.36	0.81	0.45
[1, 1, 0, 1]	[0, 1, 0, 0]	[0, 1, 0, 0, 0, 1, 1, 0, 0]	0.21	0.76	0.55
[1, 1, 0, 1]	[0, 1, 0, 0]	[0, 1, 0, 0, 0, 1, 1, 0, 1]	0.21	0.77	0.56
[1, 1, 0, 1]	[0, 1, 0, 0]	[0, 1, 0, 0, 0, 1, 1, 1, 0]	0.21	0.75	0.54
[1, 1, 0, 1]	[0, 1, 0, 0]	[0, 1, 0, 0, 0, 1, 1, 1, 1]	0.21	0.76	0.55
[1, 1, 0, 1]	[0, 1, 0, 0]	[0, 1, 1, 0, 0, 1, 1, 0, 0]	0.21	0.77	0.56
[1, 1, 0, 1]	[0, 1, 0, 0]	[0, 1, 1, 0, 0, 1, 1, 0, 1]	0.21	0.77	0.56
[1, 1, 0, 1]	[0, 1, 0, 0]	[0, 1, 1, 0, 0, 1, 1, 1, 0]	0.21	0.77	0.56
[1, 1, 0, 1]	[0, 1, 0, 0]	[0, 1, 1, 0, 0, 1, 1, 1, 1]	0.21	0.76	0.55
[1, 1, 1, 0]	[0, 1, 0, 0]	[0, 1, 0, 0, 0, 1, 1, 0, 0]	0.29	0.76	0.47
[1, 1, 1, 0]	[0, 1, 0, 0]	[0, 1, 0, 0, 0, 1, 1, 0, 1]	0.29	0.77	0.48
[1, 1, 1, 0]	[0, 1, 0, 0]	[0, 1, 0, 0, 0, 1, 1, 1, 0]	0.29	0.75	0.46
[1, 1, 1, 0]	[0, 1, 0, 0]	[0, 1, 0, 0, 0, 1, 1, 1, 1]	0.29	0.76	0.47
[1, 1, 1, 0]	[0, 1, 0, 0]	[0, 1, 1, 0, 0, 1, 1, 0, 0]	0.29	0.77	0.48
[1, 1, 1, 0]	[0, 1, 0, 0]	[0, 1, 1, 0, 0, 1, 1, 0, 1]	0.29	0.77	0.48
[1, 1, 1, 0]	[0, 1, 0, 0]	[0, 1, 1, 0, 0, 1, 1, 1, 0]	0.29	0.77	0.48
[1, 1, 1, 0]	[0, 1, 0, 0]	[0, 1, 1, 0, 0, 1, 1, 1, 1]	0.29	0.76	0.47

**W.P. denotes winning probability.*

Chapter 10

Conclusion

The major topic in this thesis is QSDC protocols. The main results are presented in Chapters 3, 4, 5, 6, 7, 8, and 9.

10.1 Summary of work done

Our contributory works start with a simple security analysis of the YZCSS QSDC protocol [1] and we have shown that the protocol is insecure and an adversary can get the full secret message by applying intercept-and-resend or impersonation attack strategy. We have proposed a modified version of this protocol, which is secure against all the common attacks.

Then we have presented a new QSDC protocol with user authentication using single qubits prepared on a randomly chosen arbitrary basis from a pre-defined set of bases and established its security. We also have executed the protocol in the IBMQ Armonk device and shown that a simple distance 3 repetition code is sufficient for reliable transmission using this protocol.

We have also analyzed an MDI-QSDC protocol [2] and shown that half of the information is always leaked without any active attack. Then we have proposed a modification of these protocols, which are secure against such information leakage problems.

Next, we have proposed a new MDI-QSDC protocol with user authentication and proved its security. Then we extend it to an MDI-QD protocol and an MDI-DSQC protocol with user authentication.

After that, we have proposed two MDI-QD protocols, which are modified versions of the

MDI-QD protocol by Maitra [3]. Without compromising the security, our protocols are more efficient in the qubit counts than the previous one. Next, we have generalized the two-party MDI-QD protocol [3] to a three-party Q.Conf and N-party Q.Conf protocols and used the part of the N-party Q.Conf protocol to produce a QMPC protocol for XOR computation.

In our last contributory Chapter, we have generalized the CHSH game and used the new games to construct the dimensionality distinguisher to distinguish between 2 and 3 dimensional maximally entangled states.

10.2 Open problems and future work

In the future, we want to analyze the security of our proposed protocols and other protocols from the viewpoint of quantum information theory. We have given the theoretical analyses of these protocols. In contrast, the practical implementations of these protocols will be exciting, and the theoretical thresholds may differ in those cases due to unavoidable channel noise. Also, the security analyses of the protocols with a realistic noise model will be interesting extensions of our work.

In chapter 9, we have shown that the maximum winning probability of Game-1 is 0.85, which occurs in 28 cases. These probabilities were calculated through simulation. In that case, it looks like to be a mathematically provable result, but the proof remains open. A similar argument holds for the results of Game-2 also. Also, in the future, we want to use dimensionality testing in other quantum information tasks.

Till now, there is no DI-QSDC with user authentication protocol and we will try to propose it in the recent future. Another interesting open problem is, whether it is possible to have a generic reduction from arbitrary QKD protocol to a suitable QSDC protocol. Also, we want to explore the other directions of quantum cryptography, like authenticated QKD, QSS, QKA, and so on.

Appendix A

Proof of Lemma 1

Lemma 1: For a probability distribution $\{\delta_i, 1 \leq i \leq 4\}$, $-\sum_{i=1}^{4} \delta_i log \delta_i \leq h(\delta_2+\delta_4)+h(\delta_3+\delta_4)$, where $h(\cdot)$ represents the binary entropy function.

Proof: Let X be a random variable such that

$$X = \begin{cases} 00 & \text{with probability } \delta_1, \\ 01 & \text{with probability } \delta_2, \\ 10 & \text{with probability } \delta_3, \\ 11 & \text{with probability } \delta_4. \end{cases}$$

Let Y and Z be the following events,

$$Y = \begin{cases} 1, & \text{if the least significant bit of } X = 1 \ , \\ 0, & \text{otherwise.} \end{cases}$$

$$Z = \begin{cases} 1, & \text{if the most significant bit of } X = 1 \ , \\ 0, & \text{otherwise.} \end{cases}$$

In other words,

$$Y = \begin{cases} 1 & \text{with probability } \delta_2 + \delta_4 \ , \\ 0 & \text{with probability } \delta_1 + \delta_3. \end{cases}$$

and

$$Z = \begin{cases} 1 & \text{with probability } \delta_3 + \delta_4 \ , \\ 0 & \text{with probability } \delta_1 + \delta_2. \end{cases} \tag{A.1}$$

Then the entropy of the events Y and Z are as follows

$$H(Y) = -\sum_{y \in \{0,1\}} \Pr(Y = y) log[\Pr(Y = y)] = h(\delta_2 + \delta_4).$$

$$H(Z) = -\sum_{z \in \{0,1\}} \Pr(Z = z) log[\Pr(Z = z)] = h(\delta_3 + \delta_4).$$

The joint entropy $H(Y, Z)$ of the events Y and Z is

$$\begin{aligned} H(Y,Z) &= -\sum_{y \in \{0,1\}} \sum_{z \in \{0,1\}} \Pr(Y = y, Z = z) log[\Pr(Y = y, Z = z)] \\ &= -\sum_{x \in \{00,01,10,11\}} \Pr(X = x) log[\Pr(X = x)] \\ &= -\sum_{i=1}^{4} \delta_i log \delta_i. \end{aligned}$$

Now using sub-additivity property of entropy, i.e., the fact that the joint entropy of a set of variables is less than or equal to the sum of the individual entropies of the variables in the set. Therefore,

$$H(Y,Z) \leq H(Y) + H(Z)$$

$$\text{or, } -\sum_{i=1}^{4} \delta_i log \delta_i \leq h(\delta_2 + \delta_4) + h(\delta_3 + \delta_4).$$

Bibliography

[1] Lili Yan, Shibin Zhang, Yan Chang, Zhibin Sun, and Zhiwei Sheng. Quantum secure direct communication protocol with mutual authentication based on single photons and Bell states. *Computers, Materials & Continua*, 63(3):1297–1307, 2020.

[2] Peng-Hao Niu, Zeng-Rong Zhou, Zai-Sheng Lin, Yu-Bo Sheng, Liu-Guo Yin, and Gui-Lu Long. Measurement-device-independent quantum communication without encryption. *Science Bulletin*, 63(20):1345–1350, 2018.

[3] Arpita Maitra. Measurement device-independent quantum dialogue. *Quantum Information Processing*, 16(12):305, 2017.

[4] Hwayean Lee, Jongin Lim, and HyungJin Yang. Quantum direct communication with authentication. *Physical Review A*, 73(4):042305, 2006.

[5] ZengRong Zhou, YuBo Sheng, PengHao Niu, LiuGuo Yin, GuiLu Long, and Lajos Hanzo. Measurement-device-independent quantum secure direct communication. *Science China Physics, Mechanics & Astronomy*, 63(3):1–6, 2020.

[6] Michael A Nielsen and Isaac Chuang. Quantum computation and quantum information, 2002.

[7] John Preskill. Lecture notes for physics 229: Quantum information and computation. *California Institute of Technology*, 16(1), 1998.

[8] John Watrous. Quantum computation lecture course cpsc 519/619. *University of Calgary URL: http://www. cs. uwaterloo. ca/watrous/lecture-notes. html*, 2006.

[9] Phillip Kaye, Raymond Laflamme, Michele Mosca, et al. *An introduction to quantum computing*. Oxford University Press on Demand, 2007.

[10] Scott Aaronson. Introduction to quantum information science lecture notes. *URL: https://www.scottaaronson.com/qclec.pdf*, 2018.

[11] Yuchen Wang, Zixuan Hu, Barry C Sanders, and Sabre Kais. Qudits and high-dimensional quantum computing. *Frontiers in Physics*, page 479, 2020.

[12] Bin Li, Zu-Huan Yu, and Shao-Ming Fei. Geometry of quantum computation with qutrits. *Scientific reports*, 3(1):1–6, 2013.

[13] Hsuan-Hao Lu, Zixuan Hu, Mohammed Saleh Alshaykh, Alexandria Jeanine Moore, Yuchen Wang, Poolad Imany, Andrew Marc Weiner, and Sabre Kais. Quantum phase estimation with time-frequency qudits in a single photon. *Advanced Quantum Technologies*, 3(2):1900074, 2020.

[14] MingXing Luo and XiaoJun Wang. Universal quantum computation with qudits. *Science China Physics, Mechanics & Astronomy*, 57(9):1712–1717, 2014.

[15] Ming-Xing Luo, Xiu-Bo Chen, Yi-Xian Yang, and Xiaojun Wang. Geometry of quantum computation with qudits. *Scientific reports*, 4(1):1–5, 2014.

[16] Mohammad HS Amin, Neil G Dickson, and Peter Smith. Adiabatic quantum optimization with qudits. *Quantum information processing*, 12(4):1819–1829, 2013.

[17] VE Zobov and AS Ermilov. Implementation of a quantum adiabatic algorithm for factorization on two qudits. *Journal of Experimental and Theoretical Physics*, 114(6):923–932, 2012.

[18] Alex Bocharov, Shawn X Cui, Martin Roetteler, and Krysta M Svore. Improved quantum ternary arithmetics. *arXiv preprint arXiv:1512.03824*, 2015.

[19] Shawn X Cui, Seung-Moon Hong, and Zhenghan Wang. Universal quantum computation with weakly integral anyons. *Quantum Information Processing*, 14(8):2687–2727, 2015.

[20] Shawn X Cui and Zhenghan Wang. Universal quantum computation with metaplectic anyons. *Journal of Mathematical Physics*, 56(3):032202, 2015.

[21] Xiaoqin Gao, Manuel Erhard, Anton Zeilinger, and Mario Krenn. Computer-inspired concept for high-dimensional multipartite quantum gates. *Physical Review Letters*, 125(5):050501, 2020.

[22] Mark RA Adcock, Peter Høyer, and Barry C Sanders. Quantum computation with coherent spin states and the close hadamard problem. *Quantum Information Processing*, 15(4):1361–1386, 2016.

[23] Stephen D Bartlett, Hubert de Guise, and Barry C Sanders. Quantum encodings in spin systems and harmonic oscillators. *Physical Review A*, 65(5):052316, 2002.

[24] Max Born. Quantenmechanik der stoßvorgänge. *Zeitschrift für Physik*, 38(11):803–827, 1926.

[25] Daniel M Greenberger, Michael A Horne, and Anton Zeilinger. Going beyond bell's theorem. In *Bell's theorem, quantum theory and conceptions of the universe*, pages 69–72. Springer, 1989.

[26] Charles H Bennett and Stephen J Wiesner. Communication via one-and two-particle operators on Einstein-Podolsky-Rosen states. *Physical review letters*, 69(20):2881, 1992.

[27] Charles H Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical review letters*, 70(13):1895, 1993.

[28] Sougato Bose, Vlatko Vedral, and Peter L Knight. Multiparticle generalization of entanglement swapping. *Physical Review A*, 57(2):822, 1998.

[29] M Enríquez, I Wintrowicz, and Karol Życzkowski. Maximally entangled multipartite states: a brief survey. In *Journal of Physics: Conference Series*, volume 698, page 012003. IOP Publishing, 2016.

[30] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical review*, 47(10):777, 1935.

[31] John S Bell. On the Einstein Podolsky Rrosen paradox. *Physics Physique Fizika*, 1(3):195, 1964.

[32] John F Clauser, Michael A Horne, Abner Shimony, and Richard A Holt. Proposed experiment to test local hidden-variable theories. *Physical review letters*, 23(15):880, 1969.

[33] William K Wootters and Wojciech H Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 1982.

[34] David Deutsch. Quantum theory, the church–turing principle and the universal quantum computer. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, 400(1818):97–117, 1985.

[35] David Deutsch and Richard Jozsa. Rapid solution of problems by quantum computation. *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences*, 439(1907):553–558, 1992.

[36] Daniel R Simon. On the power of quantum computation. *SIAM journal on computing*, 26(5):1474–1483, 1997.

[37] Lov K Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 212–219, 1996.

[38] Peter W Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. Ieee, 1994.

[39] Claude Elwood Shannon. A mathematical theory of communication. *The Bell system technical journal*, 27(3):379–423, 1948.

[40] Alexander Semenovich Holevo. Bounds for the quantity of information transmitted by a quantum communication channel. *Problemy Peredachi Informatsii*, 9(3):3–11, 1973.

[41] Gilbert S Vernam. Cipher printing telegraph systems: For secret wire and radio telegraphic communications. *Journal of the AIEE*, 45(2):109–115, 1926.

[42] Alex Biryukov and Christophe De Cannière. Data encryption standard (des). *Encyclopedia of Cryptography and Security*, pages 295–301, 2011.

[43] NIST-FIPS Standard. Announcing the advanced encryption standard (aes). *Federal Information Processing Standards Publication*, 197(1-51):3–3, 2001.

[44] Whitfield Diffie and Martin Hellman. New directions in cryptography. *IEEE transactions on Information Theory*, 22(6):644–654, 1976.

[45] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE transactions on information theory*, 31(4):469–472, 1985.

[46] Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[47] Darrel Hankerson, Alfred J Menezes, and Scott Vanstone. *Guide to elliptic curve cryptography*. Springer Science & Business Media, 2006.

[48] Neal Koblitz, Alfred Menezes, and Scott Vanstone. The state of elliptic curve cryptography. *Designs, codes and cryptography*, 19(2):173–193, 2000.

[49] Julio Lopez and Ricardo Dahab. An overview of elliptic curve cryptography. 2000.

[50] Joppe W Bos, J Alex Halderman, Nadia Heninger, Jonathan Moore, Michael Naehrig, and Eric Wustrow. Elliptic curve cryptography in practice. In *International Conference on Financial Cryptography and Data Security*, pages 157–175. Springer, 2014.

[51] Werner Heisenberg. Über den anschaulichen inhalt der quantentheoretischen kinematik und mechanik. In *Original Scientific Papers Wissenschaftliche Originalarbeiten*, pages 478–504. Springer, 1985.

[52] Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, 1984.

[53] Stephen Wiesner. Conjugate coding. *ACM Sigact News*, 15(1):78–88, 1983.

[54] Peter W Shor and John Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Physical review letters*, 85(2):441, 2000.

[55] Artur K Ekert. Quantum cryptography based on Bell's theorem. *Physical review letters*, 67(6):661, 1991.

[56] Charles H Bennett, Gilles Brassard, and N David Mermin. Quantum cryptography without Bell's theorem. *Physical review letters*, 68(5):557, 1992.

[57] Charles H Bennett. Quantum cryptography using any two nonorthogonal states. *Physical review letters*, 68(21):3121, 1992.

[58] Gui-Lu Long and Xiao-Shu Liu. Theoretically efficient high-capacity quantum-key-distribution scheme. *Physical Review A*, 65(3):032302, 2002.

[59] Peng Xue, Chuan-Feng Li, and Guang-Can Guo. Conditional efficient multiuser quantum cryptography network. *Physical Review A*, 65(2):022317, 2002.

[60] Fu-Guo Deng and Gui Lu Long. Bidirectional quantum key distribution protocol with practical faint laser pulses. *Physical Review A*, 70(1):012311, 2004.

[61] Won-Young Hwang. Quantum key distribution with high loss: toward global secure communication. *Physical Review Letters*, 91(5):057901, 2003.

[62] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy state quantum key distribution. *Physical review letters*, 94(23):230504, 2005.

[63] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. Measurement-device-independent quantum key distribution. *Physical review letters*, 108(13):130503, 2012.

[64] Jonathan Barrett, Lucien Hardy, and Adrian Kent. No signaling and quantum key distribution. *Physical review letters*, 95(1):010503, 2005.

[65] Frédéric Grosshans, Gilles Van Assche, Jérôme Wenger, Rosa Brouri, Nicolas J Cerf, and Philippe Grangier. Quantum key distribution using gaussian-modulated coherent states. *Nature*, 421(6920):238–241, 2003.

[66] Fu-Guo Deng, Gui Lu Long, and Xiao-Shu Liu. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. *Physical Review A*, 68(4):042317, 2003.

[67] Kim Boström and Timo Felbinger. Deterministic secure direct communication using entanglement. *Physical Review Letters*, 89(18):187902, 2002.

[68] Fu-Guo Deng and Gui Lu Long. Secure direct communication with a quantum one-time pad. *Physical Review A*, 69(5):052319, 2004.

[69] Chuan Wang, Fu-Guo Deng, Yan-Song Li, Xiao-Shu Liu, and Gui Lu Long. Quantum secure direct communication with high-dimension quantum superdense coding. *Physical Review A*, 71(4):044305, 2005.

[70] Chuan Wang, Fu Guo Deng, and Gui Lu Long. Multi-step quantum secure direct communication using multi-particle Green–Horne–Zeilinger state. *Optics communications*, 253(1-3):15–20, 2005.

[71] Xing-Ri Jin, Xin Ji, Ying-Qiao Zhang, Shou Zhang, Suc-Kyoung Hong, Kyu-Hwang Yeon, and Chung-In Um. Three-party quantum secure direct communication based on GHZ states. *Physics Letters A*, 354(1-2):67–70, 2006.

[72] Gui-lu Long, Fu-guo Deng, Chuan Wang, Xi-han Li, Kai Wen, and Wan-ying Wang. Quantum secure direct communication and deterministic secure quantum communication. *Frontiers of Physics in China*, 2(3):251–272, 2007.

[73] Li Xi-Han, Li Chun-Yan, Deng Fu-Guo, Zhou Ping, Liang Yu-Jie, and Zhou Hong-Yu. Quantum secure direct communication with quantum encryption based on pure entangled states. *Chinese Physics*, 16(8):2149, 2007.

[74] Song Lin, Qiao-Yan Wen, Fei Gao, and Fu-Chen Zhu. Quantum secure direct communication with χ-type entangled states. *Physical Review A*, 78(6):064304, 2008.

[75] Jian-Yong Hu, Bo Yu, Ming-Yong Jing, Lian-Tuan Xiao, Suo-Tang Jia, Guo-Qing Qin, and Gui-Lu Long. Experimental quantum secure direct communication with single photons. *Light: Science & Applications*, 5(9):e16144, 2016.

[76] Wei Zhang, Dong-Sheng Ding, Yu-Bo Sheng, Lan Zhou, Bao-Sen Shi, and Guang-Can Guo. Quantum secure direct communication with quantum memory. *Physical review letters*, 118(22):220501, 2017.

[77] Feng Zhu, Wei Zhang, Yubo Sheng, and Yidong Huang. Experimental long-distance quantum secure direct communication. *Science Bulletin*, 62(22):1519–1524, 2017.

[78] Ruoyang Qi, Zhen Sun, Zaisheng Lin, Penghao Niu, Wentao Hao, Liyuan Song, Qin Huang, Jiancun Gao, Liuguo Yin, and Gui-Lu Long. Implementation and security analysis of practical quantum secure direct communication. *Light: Science & Applications*, 8(1):1–8, 2019.

[79] Jiawei Wu, Zaisheng Lin, Liuguo Yin, and Gui-Lu Long. Security of quantum secure direct communication based on Wyner's wiretap channel theory. *Quantum Engineering*, 1(4):e26, 2019.

[80] Zikai Gao, Tao Li, and Zhenhua Li. Long-distance measurement-device–independent quantum secure direct communication. *EPL (Europhysics Letters)*, 125(4):40004, 2019.

[81] Ba An Nguyen. Quantum dialogue. *Physics Letters A*, 328(1):6–10, 2004.

[82] Zhanjun Zhang. Deterministic secure direct bidirectional communication protocol. *arXiv preprint quant-ph/0403186*, 2004.

[83] Man Zhong-Xiao, Zhang Zhan-Jun, and Li Yong. Quantum dialogue revisited. *Chinese Physics Letters*, 22(1):22, 2005.

[84] Yan Xia, Chang-Bao Fu, Shou Zhang, Suc-Kyoung Hong, Kyu-Hwang Yeon, and Chung-In Um. Quantum dialogue by using the GHZ state. *arXiv preprint quant-ph/0601127*, 2006.

[85] Ji Xin and Zhang Shou. Secure quantum dialogue based on single-photon. *Chinese Physics*, 15(7):1418, 2006.

[86] Xia Yan, Song Jie, Nie Jing, and Song He-Shan. Controlled secure quantum dialogue using a pure entangled ghz states. *Communications in Theoretical Physics*, 48(5):841, 2007.

[87] YuGuang Yang and QiaoYan Wen. Quasi-secure quantum dialogue using single photons. *Science in China Series G: Physics, Mechanics and Astronomy*, 50(5):558–562, 2007.

[88] Yong-gang Tan and Qing-Yu Cai. Classical correlation in quantum dialogue. *International Journal of Quantum Information*, 6(02):325–329, 2008.

[89] Li Dong, Xiao-Ming Xiu, Ya-Jun Gao, and Feng Chi. A controlled quantum dialogue protocol in the network using entanglement swapping. *Optics communications*, 281(24):6135–6138, 2008.

[90] Fei Gao, Fen-Zhuo Guo, Qiao-Yan Wen, and Fu-Chen Zhu. Revisiting the security of quantum dialogue and bidirectional quantum secure direct communication. *Science in China Series G: Physics, Mechanics and Astronomy*, 51(5):559–566, 2008.

[91] Gan Gao. Two quantum dialogue protocols without information leakage. *Optics communications*, 283(10):2288–2293, 2010.

[92] Guo-Fang Shi, Xiao-Qiang Xi, Ming-Liang Hu, and Rui-Hong Yue. Quantum secure dialogue by using single photons. *Optics communications*, 283(9):1984–1986, 2010.

[93] Chun-Wei Yang and Tzonelih Hwang. Quantum dialogue protocols immune to collective noise. *Quantum information processing*, 12(6):2131–2142, 2013.

[94] Ting Gao, Feng-Li Yan, and Zhi-Xi Wang. Deterministic secure direct communication using GHZ states and swapping quantum entanglement. *Journal of Physics A: Mathematical and General*, 38(25):5761, 2005.

[95] Gao Ting, Yan Feng-Li, and Wang Zhi-Xi. A simultaneous quantum secure direct communication scheme between the central party and other *M parties.* Chinese Physics Letters*, 22(10):2473, 2005.*

[96] Xiaoqing Tan, Xiaoqian Zhang, and Cui Liang. Multi-party quantum secure direct communication. pages 251–255, 2014.

[97] Zhan-jun Zhang, Yong Li, and Zhong-xiao Man. Multiparty quantum secret sharing. Physical Review A*, 71(4):044301, 2005.*

[98] Anindita Banerjee, Kishore Thapliyal, Chitra Shukla, and Anirban Pathak. Quantum conference. Quantum Information Processing*, 17(7):1–22, 2018.*

[99] Almut Beige, Berthold-Georg Englert, Christian Kurtsiefer, and Harald Weinfurter. Secure communication with single-photon two-qubit states. Journal of Physics A: Mathematical and General*, 35(28):L407, 2002.*

[100] *FL Yan and XQ Zhang. A scheme for secure direct communication using epr pairs and teleportation.* The European Physical Journal B-Condensed Matter and Complex Systems, *41(1):75–78, 2004.*

[101] *Jian Wang, Quan Zhang, and Chao-jing Tang. Quantum secure direct communication based on order rearrangement of single photons.* Physics Letters A, *358(4):256–258, 2006.*

[102] *Xi-Han Li, Fu-Guo Deng, Chun-Yan Li, Yu-Jie Liang, Ping Zhou, and Hong-Yu Zhou. Deterministic secure quantum communication without maximally entangled states.* arXiv preprint quant-ph/0606007, *2006.*

[103] *Xiao-Ming Xiu, Hai-Kuan Dong, Li Dong, Ya-Jun Gao, and Feng Chi. Deterministic secure quantum communication using four-particle genuine entangled state and entanglement swapping.* Optics communications, *282(12):2457–2459, 2009.*

[104] *Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer.* SIAM review, *41(2):303–332, 1999.*

[105] *Nanrun Zhou, Guihua Zeng, and Jin Xiong. Quantum key agreement protocol.* Electronics Letters, *40(18):1149–1150, 2004.*

[106] *C Tsai and T Hwang. On quantum key agreement protocol.* NCKU, Taiwan, *2009.*

[107] *Nayana Das and Ritajit Majumdar. Comment on "quantum key agreement protocol".* International Journal of Quantum Information, *page 2050039, 2020.*

[108] *Song-Kong Chong and Tzonelih Hwang. Quantum key agreement protocol based on bb84.* Optics Communications, *283(6):1192–1195, 2010.*

[109] *Bin Liu, Fei Gao, Wei Huang, and Qiao-Yan Wen. Multiparty quantum key agreement with single particles.* Quantum information processing, *12(4):1797–1805, 2013.*

[110] *Wei Huang, Qiao-Yan Wen, Bin Liu, Fei Gao, and Ying Sun. Quantum key agreement with epr pairs and single-particle measurements.* Quantum information processing, *13(3):649–663, 2014.*

[111] *Guang-Bao Xu, Qiao-Yan Wen, Fei Gao, and Su-Juan Qin. Novel multiparty quantum key agreement protocol with ghz states.* Quantum Information Processing, *13(12):2587–2594, 2014.*

[112] *Dong-Su Shen, Wen-Ping Ma, and Li-li Wang. Two-party quantum key agreement with four-qubit cluster states.* Quantum information processing, *13(10):2313–2324, 2014.*

[113] *Mark Hillery, Vladimír Bužek, and André Berthiaume. Quantum secret sharing.* Physical Review A, *59(3):1829, 1999.*

[114] *Zhan-Jun Zhang. Multiparty quantum secret sharing of secure direct communication.* Physics Letters A, *342(1-2):60–66, 2005.*

[115] *Daniel Gottesman. Theory of quantum secret sharing.* Physical Review A*, 61(4):042311, 2000.*

[116] *Guo-Ping Guo and Guang-Can Guo. Quantum secret sharing without entanglement.* Physics Letters A*, 310(4):247–251, 2003.*

[117] *Run-hua Shi, Yi Mu, Hong Zhong, Jie Cui, and Shun Zhang. Secure multiparty quantum computation for summation and multiplication.* Scientific reports*, 6(1):1–9, 2016.*

[118] *Xiu-Bo Chen, Gang Xu, Yi-Xian Yang, and Qiao-Yan Wen. An efficient protocol for the secure multi-party quantum summation.* International Journal of Theoretical Physics*, 49(11):2793–2804, 2010.*

[119] *Wenjie Liu, Chao Liu, Haibin Wang, and Tingting Jia. Quantum private comparison: a review.* IETE Technical Review*, 30(5):439–445, 2013.*

[120] *Wei-Wei Zhang and Ke-Jia Zhang. Cryptanalysis and improvement of the quantum private comparison protocol with semi-honest third party.* Quantum information processing*, 12(5):1981–1990, 2013.*

[121] *Wen Liu, Yong-Bin Wang, and Xiao-Mei Wang. Quantum multi-party private comparison protocol using d-dimensional bell states.* International Journal of Theoretical Physics*, 54(6):1830–1839, 2015.*

[122] *Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. Device-independent security of quantum cryptography against collective attacks.* Physical Review Letters*, 98(23):230501, 2007.*

[123] *Rodrigo Gallego, Nicolas Brunner, Christopher Hadley, and Antonio Acín. Device-independent tests of classical and quantum dimensions.* Physical review letters*, 105(23):230501, 2010.*

[124] *Johan Ahrens, Piotr Badziag, Adán Cabello, and Mohamed Bourennane. Experimental device-independent tests of classical and quantum dimensions.* Nature Physics*, 8(8):592–595, 2012.*

[125] *Umesh Vazirani and Thomas Vidick. Fully device independent quantum key distribution.* Communications of the ACM*, 62(4):133–133, 2019.*

[126] *Nicolas Gisin, Stefano Pironio, and Nicolas Sangouard. Proposal for implementing device-independent quantum key distribution based on a heralded qubit amplifier.* Physical review letters*, 105(7):070501, 2010.*

[127] *Stefano Pironio, Antonio Acin, Nicolas Brunner, Nicolas Gisin, Serge Massar, and Valerio Scarani. Device-independent quantum key distribution secure against collective attacks.* New Journal of Physics*, 11(4):045021, 2009.*

[128] *Charles Ci Wen Lim, Christopher Portmann, Marco Tomamichel, Renato Renner, and Nicolas Gisin. Device-independent quantum key distribution with local bell test.* Physical Review X*, 3(3):031006, 2013.*

[129] *Lan Zhou, Yu-Bo Sheng, and Gui-Lu Long. Device-independent quantum secure direct communication against collective attacks.* Science Bulletin, *65(1):12–20, 2020.*

[130] *Vadim Makarov* and Dag R Hjelme. Faked states attack on quantum cryptosystems.* Journal of Modern Optics, *52(5):691–705, 2005.*

[131] *Vadim Makarov, Andrey Anisimov, and Johannes Skaar. Effects of detector efficiency mismatch on security of quantum cryptosystems.* Physical Review A, *74(2):022313, 2006.*

[132] *Bing Qi, Chi-Hang Fred Fung, Hoi-Kwong Lo, and Xiongfeng Ma. Time-shift attack in practical quantum cryptosystems.* arXiv preprint quant-ph/0512080, *2005.*

[133] *Vadim Makarov. Controlling passively quenched single photon detectors by bright light.* New Journal of Physics, *11(6):065003, 2009.*

[134] *Xu-Dong Wu, Lan Zhou, Wei Zhong, and Yu-Bo Sheng. High-capacity measurement-device-independent quantum secure direct communication.* Quantum Information Processing, *19(10):1–14, 2020.*

[135] *Peng-Hao Niu, Jia-Wei Wu, Liu-Guo Yin, and Gui-Lu Long. Security analysis of measurement-device-independent quantum secure direct communication.* Quantum Information Processing, *19(10):1–14, 2020.*

[136] *Zi-Kang Zou, Lan Zhou, Wei Zhong, and Yu-Bo Sheng. Measurement-device–independent quantum secure direct communication of multiple degrees of freedom of a single photon.* EPL (Europhysics Letters), *131(4):40005, 2020.*

[137] *Nayana Das and Goutam Paul. Improving the security of "Measurement-device-independent quantum communication without encryption".* Science Bulletin, *65(24):2048–2049, 2020.*

[138] *Nayana Das and Goutam Paul. Two efficient measurement device independent quantum dialogue protocols.* International Journal of Quantum Information, *page 2050038, 2020.*

[139] *Yu-Guang Yang, Jing-Ru Dong, Yong-Li Yang, Jian Li, Yi-Hua Zhou, and Wei-Min Shi. High-capacity measurement-device-independent deterministic secure quantum communication.* Quantum Information Processing, *20(6):1–19, 2021.*

[140] *Claude Crépeau and Louis Salvail. Quantum oblivious mutual identification. In* International Conference on the Theory and Applications of Cryptographic Techniques, *pages 133–146. Springer, 1995.*

[141] *Charles H Bennett, Gilles Brassard, Claude Crépeau, and Marie-Hélene Skubiszewska. Practical quantum oblivious transfer. In* Annual international cryptology conference, *pages 351–366. Springer, 1991.*

[142] *Zhan-jun Zhang, Jun Liu, Dong Wang, and Shou-hua Shi. Comment on "quantum direct communication with authentication".* Physical Review A, *75(2):026301, 2007.*

[143] *Liu Dan, Pei Chang-Xing, Quan Dong-Xiao, and Zhao Nan. A new quantum secure direct communication scheme with authentication.* Chinese Physics Letters*, 27(5):050306, 2010.*

[144] *Yan Chang, Chunxiang Xu, Shibin Zhang, and Lili Yan. Controlled quantum secure direct communication and authentication protocol based on five-particle cluster state and quantum one-time pad.* Chinese science bulletin*, 59(21):2541–2546, 2014.*

[145] *Tzonelih Hwang, Yi-Ping Luo, Chun-Wei Yang, and Tzu-Han Lin. Quantum authencryption: one-step authenticated quantum secure direct communications for off-line communicants.* Quantum information processing*, 13(4):925–933, 2014.*

[146] *Nayana Das and Goutam Paul. Cryptanalysis of quantum secure direct communication protocol with mutual authentication based on single photons and bell states.* Europhysics Letters*, DOI: https://doi.org/10.1209/0295-5075/ac2246(arXiv preprint arXiv:2007.03710), 2020.*

[147] *J Lawrence Carter and Mark N Wegman. Universal classes of hash functions.* Journal of computer and system sciences*, 18(2):143–154, 1979.*

[148] *Mark N Wegman and J Lawrence Carter. New hash functions and their use in authentication and set equality.* Journal of computer and system sciences*, 22(3):265–279, 1981.*

[149] *Charles H Bennett, François Bessette, Gilles Brassard, Louis Salvail, and John Smolin. Experimental quantum cryptography.* Journal of cryptology*, 5(1):3–28, 1992.*

[150] *Stefano Pirandola, Ulrik L Andersen, Leonardo Banchi, Mario Berta, Darius Bunandar, Roger Colbeck, Dirk Englund, Tobias Gehring, Cosmo Lupo, Carlo Ottaviani, et al. Advances in quantum cryptography.* Advances in Optics and Photonics*, 12(4):1012–1236, 2020.*

[151] *Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography.* Reviews of modern physics*, 74(1):145, 2002.*

[152] *Valerio Scarani, Antonio Acin, Grégoire Ribordy, and Nicolas Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations.* Physical review letters*, 92(5):057901, 2004.*

[153] *Daniel Ljunggren, Mohamed Bourennane, and Anders Karlsson. Authority-based user authentication in quantum key distribution.* Physical Review A*, 62(2):022305, 2000.*

[154] *Bao-Sen Shi, Jian Li, Jin-Ming Liu, Xiao-Feng Fan, and Guang-Can Guo. Quantum key distribution and quantum authentication based on entangled state.* Physics letters A*, 281(2-3):83–87, 2001.*

[155] *Toung-Shang Wei, Chia-Wei Tsai, and Tzonelih Hwang. Comment on "quantum key distribution and quantum authentication based on entangled state".* International Journal of Theoretical Physics*, 50(9):2703–2707, 2011.*

[156] *Guihua Zeng and Xinmei Wang. Quantum key distribution with authentication.* arXiv preprint quant-ph/9812022*, 1998.*

[157] *Tzonelih Hwang, Kuo-Chang Lee, and Chuan-Ming Li. Provably secure three-party authenticated quantum key distribution protocols.* IEEE Transactions on Dependable and Secure Computing*, 4(1):71–80, 2007.*

[158] *Song Lin, Chuan Huang, and Xiao-Fen Liu. Multi-user quantum key distribution based on bell states with mutual authentication.* Physica Scripta*, 87(3):035008, 2013.*

[159] *Dah-Jyh Guan, Yuan-Jiun Wang, and ES Zhuang. A practical protocol for three-party authenticated quantum key distribution.* Quantum information processing*, 13(11):2355–2374, 2014.*

[160] *Kun-Fei Yu, Chun-Wei Yang, Ci-Hong Liao, and Tzonelih Hwang. Authenticated semi-quantum key distribution protocol using bell states.* Quantum Information Processing*, 13(6):1457–1465, 2014.*

[161] *Song Lin, Hui Wang, Gong-De Guo, Guo-Hua Ye, Hong-Zhen Du, and Xiao-Fen Liu. Authenticated multi-user quantum key distribution with single particles.* International Journal of Quantum Information*, 14(01):1650002, 2016.*

[162] *Ilja Gerhardt, Qin Liu, Antia Lamas-Linares, Johannes Skaar, Christian Kurtsiefer, and Vadim Makarov. Full-field implementation of a perfect eavesdropper on a quantum cryptography system.* Nature communications*, 2(1):1–6, 2011.*

[163] *Lars Lydersen, Carlos Wiechers, Christoffer Wittmann, Dominique Elser, Johannes Skaar, and Vadim Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination.* Nature photonics*, 4(10):686–689, 2010.*

[164] *Henning Weier, Harald Krauss, Markus Rau, Martin Fürst, Sebastian Nauerth, and Harald Weinfurter. Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors.* New Journal of Physics*, 13(7):073024, 2011.*

[165] *Feihu Xu, Bing Qi, and Hoi-Kwong Lo. Experimental demonstration of phase-remapping attack in a practical quantum key distribution system.* New Journal of Physics*, 12(11):113026, 2010.*

[166] *Dominic Mayers and Andrew Yao. Quantum cryptography with imperfect apparatus. In* Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No. 98CB36280)*, pages 503–509. IEEE, 1998.*

[167] *Antonio Acin, Serge Massar, and Stefano Pironio. Efficient quantum key distribution secure against no-signalling eavesdroppers.* New Journal of Physics*, 8(8):126, 2006.*

[168] *Lluis Masanes, Stefano Pironio, and Antonio Acin. Secure device-independent quantum key distribution with causally independent measurement devices.* Nature communications*, 2(1):1–7, 2011.*

[169] *Cyril Branciard, Eric G Cavalcanti, Stephen P Walborn, Valerio Scarani, and Howard M Wiseman. One-sided device-independent quantum key distribution: Security, feasibility, and the connection with steering.* Physical Review A, *85(1):010301, 2012.*

[170] *Gláucia Murta, Suzanne B van Dam, Jérémy Ribeiro, Ronald Hanson, and Stephanie Wehner. Towards a realization of device-independent quantum key distribution.* Quantum Science and Technology, *4(3):035011, 2019.*

[171] *Yi Zhao, Chi-Hang Fred Fung, Bing Qi, Christine Chen, and Hoi-Kwong Lo. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems.* Physical Review A, *78(4):042333, 2008.*

[172] *Xiang-Bin Wang. Beating the photon-number-splitting attack in practical quantum cryptography.* Physical review letters, *94(23):230503, 2005.*

[173] *Yang Liu, Teng-Yun Chen, Liu-Jun Wang, Hao Liang, Guo-Liang Shentu, Jian Wang, Ke Cui, Hua-Lei Yin, Nai-Le Liu, Li Li, et al. Experimental measurement-device-independent quantum key distribution.* Physical review letters, *111(13):130502, 2013.*

[174] *Marcos Curty, Feihu Xu, Wei Cui, Charles Ci Wen Lim, Kiyoshi Tamaki, and Hoi-Kwong Lo. Finite-key analysis for measurement-device-independent quantum key distribution.* Nature communications, *5(1):1–7, 2014.*

[175] *Hua-Lei Yin, Teng-Yun Chen, Zong-Wen Yu, Hui Liu, Li-Xing You, Yi-Heng Zhou, Si-Jing Chen, Yingqiu Mao, Ming-Qi Huang, Wei-Jun Zhang, et al. Measurement-device-independent quantum key distribution over a 404 km optical fiber.* Physical review letters, *117(19):190501, 2016.*

[176] *Feihu Xu, Marcos Curty, Bing Qi, and Hoi-Kwong Lo. Practical aspects of measurement-device-independent quantum key distribution.* New Journal of Physics, *15(11):113007, 2013.*

[177] *Xiongfeng Ma and Mohsen Razavi. Alternative schemes for measurement-device-independent quantum key distribution.* Physical Review A, *86(6):062319, 2012.*

[178] *Xiongfeng Ma, Chi-Hang Fred Fung, and Mohsen Razavi. Statistical fluctuation analysis for measurement-device-independent quantum key distribution.* Physical Review A, *86(5):052305, 2012.*

[179] *Zhengyu Li, Yi-Chen Zhang, Feihu Xu, Xiang Peng, and Hong Guo. Continuous-variable measurement-device-independent quantum key distribution.* Physical Review A, *89(5):052301, 2014.*

[180] *Yan-Lin Tang, Hua-Lei Yin, Si-Jing Chen, Yang Liu, Wei-Jun Zhang, Xiao Jiang, Lu Zhang, Jian Wang, Li-Xing You, Jian-Yu Guan, et al. Measurement-device-independent quantum key distribution over 200 km.* Physical review letters, *113(19):190501, 2014.*

[181] *Chao Wang, Xiao-Tian Song, Zhen-Qiang Yin, Shuang Wang, Wei Chen, Chun-Mei Zhang, Guang-Can Guo, and Zheng-Fu Han. Phase-reference-free experiment of measurement-device-independent quantum key distribution.* Physical review letters*, 115(16):160502, 2015.*

[182] *Yan-Lin Tang, Hua-Lei Yin, Qi Zhao, Hui Liu, Xiang-Xiang Sun, Ming-Qi Huang, Wei-Jun Zhang, Si-Jing Chen, Lu Zhang, Li-Xing You, et al. Measurement-device-independent quantum key distribution over untrustful metropolitan network.* Physical Review X*, 6(1):011024, 2016.*

[183] *Yi-Heng Zhou, Zong-Wen Yu, and Xiang-Bin Wang. Making the decoy-state measurement-device-independent quantum key distribution practically useful.* Physical Review A*, 93(4):042324, 2016.*

[184] *Chao Wang, Zhen-Qiang Yin, Shuang Wang, Wei Chen, Guang-Can Guo, and Zheng-Fu Han. Measurement-device-independent quantum key distribution robust against environmental disturbances.* Optica*, 4(9):1016–1023, 2017.*

[185] *Zheng-Xia Cui, Wei Zhong, Lan Zhou, and Yu-Bo Sheng. Measurement-device-independent quantum key distribution with hyper-encoding.* Science China Physics, Mechanics & Astronomy*, 62(11):1–10, 2019.*

[186] *Yuan Cao, Yu-Huai Li, Kui-Xing Yang, Yang-Fan Jiang, Shuang-Lin Li, Xiao-Long Hu, Maimaiti Abulizi, Cheng-Long Li, Weijun Zhang, Qi-Chao Sun, et al. Long-distance free-space measurement-device-independent quantum key distribution.* Physical Review Letters*, 125(26):260503, 2020.*

[187] *Kejin Wei, Wei Li, Hao Tan, Yang Li, Hao Min, Wei-Jun Zhang, Hao Li, Lixing You, Zhen Wang, Xiao Jiang, et al. High-speed measurement-device-independent quantum key distribution with integrated silicon photonics.* Physical Review X*, 10(3):031030, 2020.*

[188] *Yu-Fei Yan, Lan Zhou, Wei Zhong, and Yu-Bo Sheng. Measurement-device-independent quantum key distribution of multiple degrees of freedom of a single photon.* Frontiers of Physics*, 16(1):1–11, 2021.*

[189] *Ryutaroh Matsumoto. Multiparty quantum-key-distribution protocol without use of entanglement.* Physical Review A*, 76(6):062316, 2007.*

[190] *Nan-Run Zhou, Kong-Ni Zhu, and Xiang-Fu Zou. Multi-party semi-quantum key distribution protocol with four-particle cluster states.* Annalen der Physik*, 531(8):1800520, 2019.*

[191] *Changhua Zhu, Feihu Xu, and Changxing Pei. W-state analyzer and multi-party measurement-device-independent quantum key distribution.* Scientific reports*, 5(1):1–10, 2015.*

[192] *Kun-Fei Yu, Jun Gu, Tzonelih Hwang, and Prosanta Gope. Multi-party semi-quantum key distribution-convertible multi-party semi-quantum secret sharing.* Quantum Information Processing*, 16(8):1–14, 2017.*

[193] *Antoni Wójcik. Eavesdropping on the "ping-pong" quantum communication protocol.* Physical Review Letters*, 90(15):157901, 2003.*

[194] *Qing-yu Cai. The ping-pong protocol can be attacked without eavesdropping.* arXiv preprint quant-ph/0402052*, 2004.*

[195] *Qing-Yu Cai and Bai-Wen Li. Improving the capacity of the boström-felbinger protocol.* Physical Review A*, 69(5):054301, 2004.*

[196] *Fu-Guo Deng, Xi-Han Li, Chun-Yan Li, Ping Zhou, and Hong-Yu Zhou. Eavesdropping on the "ping-pong" quantum communication protocol freely in a noise channel.* arXiv preprint quant-ph/0507143*, 2005.*

[197] *Gao Ting, Yan Feng-Li, and Wang Zhi-Xi. Controlled quantum teleportation and secure direct communication.* Chinese Physics*, 14(5):893, 2005.*

[198] *Ting Gao. Controlled and secure direct communication using GHZ state and teleportation.* Zeitschrift für Naturforschung A*, 59(9):597–601, 2004.*

[199] *Jindong Zhou, Guang Hou, Shenjun Wu, and Yongde Zhang. Controlled quantum teleportaion.* arXiv preprint quant-ph/0006030*, 2000.*

[200] *Yan Xia and He-Shan Song. Controlled quantum secure direct communication using a non-symmetric quantum channel with quantum superdense coding.* Physics Letters A*, 364(2):117–122, 2007.*

[201] *Nicolas J Cerf. Pauli cloning of a quantum bit.* Physical review letters*, 84(19):4497, 2000.*

[202] *XS Liu, GL Long, DM Tong, and Feng Li. General scheme for superdense coding between multiparties.* Physical Review A*, 65(2):022304, 2002.*

[203] *Ting Gao, Feng-Li Yan, and Zhi-Xi Wang. Quantum secure direct communication by einstein-podolsky-rosen pairs and entanglement swapping.* arXiv preprint quant-ph/0406083*, 2004.*

[204] *Marek Zukowski, Anton Zeilinger, Michael A Horne, and Aarthur K Ekert. "Event-ready-detectors" Bell experiment via entanglement swapping.* Physical Review Letters*, 71:4287–4290, 1993.*

[205] *Holger Hoffmann, Kim Bostroem, and Timo Felbinger. Comment on "secure direct communication with a quantum one-time pad".* Physical Review A*, 72(1):016301, 2005.*

[206] *David Deutsch, Artur Ekert, Richard Jozsa, Chiara Macchiavello, Sandu Popescu, and Anna Sanpera. Quantum privacy amplification and the security of quantum cryptography over noisy channels.* Physical review letters*, 77(13):2818, 1996.*

[207] *Fu-Guo Deng and Gui Lu Long. Reply to "comment on 'secure direct communication with a quantum one-time-pad'".* Physical Review A*, 72(1):016302, 2005.*

[208] *Cao Hai-Jing and Song He-Shan. Quantum secure direct communication with w state.* Chinese Physics Letters, *23(2):290, 2006.*

[209] *Liu Jun, Liu Yi-Min, Cao Hai-Jing, Shi Shou-Hua, and Zhang Zhan-Jun. Revisiting quantum secure direct communication with w state.* Chinese Physics Letters, *23(10):2652, 2006.*

[210] *Ye Yeo and Wee Kang Chua. Teleportation and dense coding with genuine multipartite entanglement.* Physical review letters, *96(6):060502, 2006.*

[211] *Xin-Wen Wang and Guo-Jian Yang. Generation and discrimination of a type of four-partite entangled state.* Physical Review A, *78(2):024301, 2008.*

[212] *Yang Yu-Guang, Wen Qiao-Yan, and Zhu Fu-Chen. An efficient quantum secure direct communication scheme with authentication.* Chinese Physics, *16(7):1838, 2007.*

[213] *Wang Min-Jie and Pan Wei. Quantum secure direct communication based on authentication.* Chinese Physics Letters, *25(11):3860, 2008.*

[214] *Liu Wen-Jie, Chen Han-Wu, Li Zhi-Qiang, and Liu Zhi-Hao. Efficient quantum secure direct communication with authentication.* Chinese Physics Letters, *25(7):2354, 2008.*

[215] *Yang Jing, Wang Chuan, and Zhang Ru. Quantum secure direct communication with authentication expansion using single photons.* Communications in Theoretical Physics, *54(5):829, 2010.*

[216] *Yu-Guang Yang, Xin Jia, Juan Xia, Lei Shi, and Hua Zhang. Comment on "quantum secure direct communication with authentication expansion using single photons".* International Journal of Theoretical Physics, *51(12):3681–3687, 2012.*

[217] *Chang Yan, Zhang Shi-Bin, Yan Li-Li, and Sheng Zhi-Wei. A multiparty controlled bidirectional quantum secure direct communication and authentication protocol based on epr pairs.* Chinese Physics Letters, *30(6):060301, 2013.*

[218] *Chun-Wei Yang, Tzonelih Hwang, and Tzu-Han Lin. Modification attack on qsdc with authentication and the improvement.* International Journal of Theoretical Physics, *52(7):2230–2234, 2013.*

[219] *Dongsu Shen, Wenping Ma, Xunru Yin, and Xiaoping Li. Quantum dialogue with authentication based on bell states.* International Journal of Theoretical Physics, *52(6):1825–1835, 2013.*

[220] *Yan Chang, ChunXiang Xu, ShiBin Zhang, and LiLi Yan. Quantum secure direct communication and authentication protocol with single photons.* Chinese science bulletin, *58(36):4571–4576, 2013.*

[221] *Nayana Das, Goutam Paul, and Ritajit Majumdar. Quantum secure direct communication with mutual authentication using a single basis.* International Journal of Theoretical Physics, *(arXiv preprint arXiv:2101.03577), 2021.*

[222] Nguyen Ba An. Secure dialogue without a prior key distribution. Journal-Korean Physical Society, *47(4):562, 2005.*

[223] Qing-Yu Cai. Eavesdropping on the two-way quantum communication protocols with invisible photons. Physics Letters A, *351(1-2):23–25, 2006.*

[224] Zhong-Xiao Man, Yun-Jie Xia, and Nguyen Ba An. Quantum secure direct communication by using GHZ states and entanglement swapping. Journal of Physics B: Atomic, Molecular and Optical Physics, *39(18):3855, 2006.*

[225] Man Zhong-Xiao and Xia Yun-Jie. Controlled bidirectional quantum direct communication by using a GHZ state. Chinese Physics Letters, *23(7):1680, 2006.*

[226] Man Zhong-Xiao and Xia Yun-Jie. Improvement of security of three-party quantum secure direct communication based on GHZ states. Chinese Physics Letters, *24(1):15, 2007.*

[227] Chen Yan, Man Zhong-Xiao, and Xia Yun-Jie. Quantum bidirectional secure direct communication via entanglement swapping. Chinese Physics Letters, *24(1):19, 2007.*

[228] Guo-Fang Shi and Xiu-Lao Tian. Quantum secure dialogue based on single photons and controlled-not operations. Journal of Modern Optics, *57(20):2027–2030, 2010.*

[229] Guo-Fang Shi. Bidirectional quantum secure communication scheme based on bell states and auxiliary particles. Optics communications, *283(24):5275–5278, 2010.*

[230] Zhan You-Bang, Zhang Ling-Ling, Wang Yu-Wu, and Zhang Qun-Yong. Quantum dialogue by using non-symmetric quantum channel. Communications in Theoretical Physics, *53(4):648, 2010.*

[231] Gao Gan and Wang Li-Ping. A protocol for bidirectional quantum secure communication based on genuine four-particle entangled states. Communications in Theoretical Physics, *54(3):447, 2010.*

[232] Man Zhong-Xiao and Xia Yun-Jie. Efficient one-sender versus N-receiver quantum secure direct communication. Chinese Physics Letters, *23(8):1973, 2006.*

[233] Gao Fei, Lin Song, Wen Qiao-Yan, and Zhu Fu-Chen. A special eavesdropping on one-sender versus n-receiver QSDC protocol. Chinese Physics Letters, *25(5):1561, 2008.*

[234] Fei Gao, Su-Juan Qin, Qiao-Yan Wen, and Fu-Chen Zhu. Comment on:"Three-party quantum secure direct communication based on GHZ states" [Phys. Lett. A 354 (2006) 67]. Physics Letters A, *372(18):3333–3336, 2008.*

[235] Wang Mei-Yu and Yan Feng-Li. Three-party simultaneous quantum secure direct communication scheme with epr pairs. Chinese Physics Letters, *24(9):2486, 2007.*

[236] Song-Kong Chong and Tzonelih Hwang. The enhancement of three-party simultaneous quantum secure direct communication scheme with EPR pairs. Optics communications, *284(1):515–518, 2011.*

[237] *Lian-Ying Wang, Xiu-Bo Chen, Gang Xu, and Yi-Xian Yang. Information leakage in three-party simultaneous quantum secure direct communication with EPR pairs.* Optics Communications*, 284(7):1719–1720, 2011.*

[238] *Kaoru Shimizu and Nobuyuki Imoto. Communication channels secured from eavesdropping via transmission of photonic bell states.* Physical Review A*, 60(1):157, 1999.*

[239] *Almut Beige, Berthold-Georg Englert, Christian Kurtsiefer, and Harald Weinfurter. Secure communication with a publicly known key.* arXiv preprint quant-ph/0111106*, 2001.*

[240] *Man Zhong-Xiao, Zhang Zhan-Jun, and Li Yong. Deterministic secure direct communication by using swapping quantum entanglement and local unitary operations.* Chinese Physics Letters*, 22(1):18, 2005.*

[241] *Lev Vaidman. Teleportation of quantum states.* Physical Review A*, 49(2):1473, 1994.*

[242] *Jian-Wei Pan, Dik Bouwmeester, Harald Weinfurter, and Anton Zeilinger. Experimental entanglement swapping: entangling photons that never interacted.* Physical review letters*, 80(18):3891, 1998.*

[243] *Marco Lucamarini and Stefano Mancini. Secure deterministic communication without entanglement.* Physical review letters*, 94(14):140501, 2005.*

[244] *Cai Qing-Yu and Li Bai-Wen. Deterministic secure communication without using entanglement.* Chinese Physics Letters*, 21(4):601, 2004.*

[245] *Hao Yuan, Jun Song, Xiaoyuan Hu, and Kui Hou. An efficient deterministic secure quantum communication scheme with cluster state.* International Journal of Quantum Information*, 7(03):689–696, 2009.*

[246] *Hans J Briegel and Robert Raussendorf. Persistent entanglement in arrays of interacting particles.* Physical Review Letters*, 86(5):910, 2001.*

[247] *ZhiHao Liu, HanWu Chen, WenJie Liu, Juan Xu, and ZhiQiang Li. Deterministic secure quantum communication without unitary operation based on high-dimensional entanglement swapping.* Science China Information Sciences*, 55(2):360–367, 2012.*

[248] *Chia-Wei Tsai and Tzonelih Hwang. Deterministic quantum communication using the symmetric w state.* Science China Physics, Mechanics and Astronomy*, 56(10):1903–1908, 2013.*

[249] *Hao Yuan, Qin Zhang, Liang Hong, Wen-jie Yin, Dong Xu, and Jun Zhou. Scheme for deterministic secure quantum communication with three-qubit ghz state.* International Journal of Theoretical Physics*, 53(8):2558–2564, 2014.*

[250] *Yong-Gang Hu. Deterministic secure quantum communication with four-qubit ghz states.* International Journal of Theoretical Physics*, 57(9):2831–2842, 2018.*

[251] *Hao Yuan, Jun Song, Xiang-Yuan Liu, and Xiao-Feng Yin. Deterministic secure four-qubit ghz states three-step protocol for quantum communication.* International Journal of Theoretical Physics, *58(11):3658–3666, 2019.*

[252] *Tarek A Elsayed. Deterministic secure quantum communication with and without entanglement.* Physica Scripta, *96(2):025101, 2020.*

[253] *Arpita Maitra, Bibhas Adhikari, and Satyabrata Adhikari. Proposal for dimensionality testing in quantum private query.* arXiv preprint arXiv:1805.08172, *2018.*

[254] *Nicolas Brunner, Stefano Pironio, Antonio Acin, Nicolas Gisin, André Allan Méthot, and Valerio Scarani. Testing the dimension of Hilbert spaces.* Physical review letters, *100(21):210503, 2008.*

[255] *Károly F Pál and Tamás Vértesi. Efficiency of higher-dimensional hilbert spaces for the violation of Bell inequalities.* Physical Review A, *77(4):042105, 2008.*

[256] *David Pérez-García, Michael M Wolf, Carlos Palazuelos, Ignacio Villanueva, and Marius Junge. Unbounded violation of tripartite Bell inequalities.* Communications in Mathematical Physics, *279(2):455–486, 2008.*

[257] *Tamás Vértesi, Stefano Pironio, and Nicolas Brunner. Closing the detection loophole in Bell experiments using qudits.* Physical review letters, *104(6):060401, 2010.*

[258] *T Vértesi and KF Pál. Generalized Clauser-Horne-Shimony-Holt inequalities maximally violated by higher-dimensional systems.* Physical Review A, *77(4):042106, 2008.*

[259] *Marius Junge, Carlos Palazuelos, David Pérez-García, Ignacio Villanueva, and Michael M Wolf. Operator space theory: a natural framework for Bell inequalities.* Physical review letters, *104(17):170405, 2010.*

[260] *Jop Briët, Harry Buhrman, and Ben Toner. A generalized Grothendieck inequality and nonlocal correlations that require high entanglement.* Communications in mathematical physics, *305(3):827–843, 2011.*

[261] *Stephanie Wehner, Matthias Christandl, and Andrew C Doherty. Lower bound on the dimension of a quantum system given measured data.* Physical Review A, *78(6):062112, 2008.*

[262] *Marius Junge and Carlos Palazuelos. Large violation of Bell inequalities with low entanglement.* Communications in Mathematical Physics, *306(3):695–746, 2011.*

[263] *Martin Hendrych, Rodrigo Gallego, Michal Mičuda, Nicolas Brunner, Antonio Acín, and Juan P Torres. Experimental estimation of the dimension of classical and quantum systems.* Nature Physics, *8(8):588–591, 2012.*

[264] *Nicolas Brunner, Miguel Navascués, and Tamás Vértesi. Dimension witnesses and quantum state discrimination.* Physical review letters, *110(15):150501, 2013.*

[265] *Joseph Bowles, Marco Túlio Quintino, and Nicolas Brunner. Certifying the dimension of classical and quantum systems in a prepare-and-measure scenario with independent devices.* Physical review letters*, 112(14):140407, 2014.*

[266] *Gao Fei, Qin Su-Juan, Guo Fen-Zhuo, and Wen Qiao-Yan. Cryptanalysis of quantum secure direct communication and authentication scheme via Bell states.* Chinese Physics Letters*, 28(2):020303, 2011.*

[267] *Ai-Dong Zhu, Yan Xia, Qiu-Bo Fan, and Shou Zhang. Secure direct communication based on secret transmitting order of particles.* Physical Review A*, 73(2):022338, 2006.*

[268] *SA Moiseev and MI Noskov. The possibilities of the quantum memory realization for short pulses of light in the photon echo technique.* Laser Physics Letters*, 1(6):303, 2004.*

[269] *K Jensen, W Wasilewski, H Krauter, T Fernholz, BM Nielsen, M Owari, Martin B Plenio, A Serafini, MM Wolf, and ES Polzik. Quantum memory for entangled continuous-variable states.* Nature Physics*, 7(1):13–16, 2011.*

[270] *CE Bradley, J Randall, MH Abobeih, RC Berrevoets, MJ Degen, MA Bakker, M Markham, DJ Twitchen, and TH Taminiau. A ten-qubit solid-state spin register with quantum memory up to one minute.* Physical Review X*, 9(3):031045, 2019.*

[271] *N Jiang, Y-F Pu, W Chang, C Li, S Zhang, and L-M Duan. Experimental realization of 105-qubit random access quantum memory.* npj Quantum Information*, 5(1):1–6, 2019.*

[272] *Héctor Abraham et al. Qiskit: An open-source framework for quantum computing, 2019.*

[273] *IBM Quantum team. ibmq_armonk v1.1.5, 2020. Retrieved from https://quantum-computing.ibm.com.*

[274] *Chang ho Hong, Jino Heo, Jin Gak Jang, and Daesung Kwon. Quantum identity authentication with single photon.* Quantum Information Processing*, 16(10):236, 2017.*

[275] *Daniel Gottesman. Stabilizer codes and quantum error correction.* arXiv preprint quant-ph/9705052*, 1997.*

[276] *Gao Fei, Wen Qiao-Yan, and Zhu Fu-Chen. Teleportation attack on the QSDC protocol with a random basis and order.* Chinese Physics B*, 17(9):3189, 2008.*

[277] *Gan Gao. Information leakage in quantum dialogue by using the two-qutrit entangled states.* Modern Physics Letters B*, 28(12):1450094, 2014.*

[278] *Daniel Gottesman, H-K Lo, Norbert Lutkenhaus, and John Preskill. Security of quantum key distribution with imperfect devices. In* International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings.*, page 136. IEEE, 2004.*

[279] *Imre Csiszár and Janos Korner. Broadcast channels with confidential messages.* IEEE transactions on information theory*, 24(3):339–348, 1978.*

[280] *Renato Renner. Symmetry of large physical systems implies independence of subsystems.* Nature Physics, *3(9):645–649, 2007.*

[281] *Barbara Kraus, Nicolas Gisin, and Renato Renner. Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication.* Physical review letters, *95(8):080501, 2005.*

[282] *Nayana Das and Goutam Paul. Secure multi-party quantum conference and xor computation.* Quantum Information and Computation, *21(3 & 4):0203–0232, 2021.*

[283] *Claude E Shannon. Communication theory of secrecy systems.* The Bell system technical journal, *28(4):656–715, 1949.*

[284] *Nayana Das, Goutam Paul, and Arpita Maitra. Dimensionality distinguishers.* Quantum Information Processing, *18(6):1–17, 2019.*

[285] *Goutam Paul and Souvik Ray. On data complexity of distinguishing attacks versus message recovery attacks on stream ciphers.* Designs, Codes and Cryptography, *86(6):1211–1247, 2018.*

[286] *Jyotirmoy Basak and Subhamoy Maitra. Clauser-Horne-Shimony-Holt versus three-party pseudo-telepathy: On the optimal number of samples in device-independent quantum private query.* Quantum Information Processing, *17(4):1–14, 2018.*