STATISTICAL INSTITUTE
Semester Examination
M. Tech. (CrS) II year (1st Sem): 2019-2020
Advanced Cryptology

Date: 02.12. 2019 Total Marks : 100 Time : 3.00 Hours

Answer as much as you can. Maximum you can score is 100.

1. (a) Define a hardcore predicate of a function f. How does one obtain a secure pseudo-random generator from a hardcore predicate?

   (b) Explain in details Shamir's (t, n) Secret Sharing Scheme. [6+10]

2. (a) Define a (cryptographic) bilinear map. When is it said to be type-I? Using a type-I bilinear map obtain Joux's three-party key agreement protocol.

   (b) Explain Bilinear Diffie-Hellman(BDH) and Decisional Bilinear Diffie-Hellman(DBDH) problems. Show that if there is an efficient algorithm for BDH then one can construct an efficient algorithm for DBDH.
   Let $e : G \times G \rightarrow G_T$ be a bilinear map. Show that the Decisional Diffie-Hellman(DDH) is easy for G.

   [(4+1+5)+(4+4+4)]

3. (a) Formally define an Identity-Based Encryption(IBE) scheme. When is it said to be IND-ID-CPA secure?

   (b) Describe Boneh-Franklin IBE scheme **BasicIdent**. Prove the correctness of the decryption algorithm.

   (c) Assuming that **BasicIdent** is IND-ID-CPA secure, how would you transform it to obtain an IND-ID-CCA IBE?

   [(5+5)+8+7]

4. (a) Describe Boneh-Boyen Hierarchical Identity-Based Encryption(HIBE) scheme. Prove the correctness of the decryption algorithm. What can you say about its security?

   (b) Describe Waters IBE scheme. Prove the correctness of the decryption algorithm. What can you say about its security?

   (c) Describe Boneh-Lynn-Shacham short signature scheme.

   [(7+3+2)+(7+3+2)+6]

5. (a) Given a basis **B** of a lattice Λ , describe the Shortest Vector Problem (SVP) for Λ.

   (b) Describe the Short Integer Solution problem $SIS_{n,m,q,\beta}$? Show that one can obtain a collision-resistant hash family from $SIS_{n,m,q,\beta}$ assumption, where $\beta = \sqrt{n}$.

   (c) Describe the decisional Learning With Errrors problem $LWE_{n,m,q,\chi}$.

   (d) Assuming decisional $LWE_{n,m,q,\chi}$, obtain a Secret-Key Encryption scheme.Give an informal proof of its security.

   [4+(4+6)+5+8]

STATISTICAL INSTITUTE
Semester Examination
M. Tech. (CrS) II year (1st Sem): 2019-2020
Advanced Cryptology
Back Paper

Date: 09.01. 2020
Answer as much as you can.

Total Marks : 100

Time : 3.00 Hours

1. (a) What is a 1-out-of-2 oblivious transfer protocol? Obtain a 1-out-of-2 oblivious transfer protocol using a public key cryptosystem.

   (b) Explain what you mean by a (t, n) secret sharing scheme? Suppose you have a secret $s \in \mathbb{Z}_p$ and want to share this secret among n participants in such a way that 3 or more participants would be able to recover s, but 2 or less participants will learn nothing. How would you set up such a scheme?

[10+10]

2. (a) When is a function said to be one-way? State one use of a one-way function.

   (b) Define a (cryptographic) bilinear map. What are the three types of bilinear maps?

   (c) Describe Bilinear Diffie-Hellman(BDH) Problem and Decisional Bilinear Diffie-Hellman (DBDH) Problem. Find a relation among them.

[6+7+12]

3. (a) Formally define an Identity Based Encryption (IBE) scheme. Describe an IBE scheme that is known to be IND-ID-CPA secure in the random oracle model.

   (b) When is an IBE scheme said to be IND-ID-CCA secure?

[12+8]

4. Describe Gentry-Silverberg Hierarchical IBE.

[10]

5. (a) Define an n-dimensional lattice of rank $k \leq n$. Describe the approximate Shortest Vector Problem SVP_{γ}.

   (b) Describe the $LWE_{n,q,\gamma}$ problem and its decisional version

   (c) Assuming the decisional LWE is hard, describe a secret key encryption scheme.

[8+10+10]

INDIAN STATISTICAL INSTITUTE
End-Semester Examination
M. Tech(CrS) II year, 1st Sem, AY 2019–2020

Computing Systems Security II

Date:- 29.11.2019 Time: 3 Hours

Total Marks: 110 Buffer Marks: 10 Maximum Marks: 100

Please try to write all the part answers of a question at the same place.

Answer the folowing questions.

1. Using LiveHTTPHeader, the following GET request is used to send an HTTP request to *www.example.com* to delete a page owned by a user (only the owner of a page can delete the page).

```
http://www.example.com/delete.php?pageid=5
GET /delete.php?pageid=5
Host: www.example.com
...
```

Construct a simple malicious web page, so that when a victim visits this web page, a forged request will be launched against *www.example.com* to delete a page belonging to the user. Explain briefly how to counter such attacks. [6+4]

2. Consider the following *POST* request.

```
http://www.example.com/delete.php
POST /delete.php HTTP/1.1
Host: www.example.com...
Content-Length: 8
pageid=5
```

Construct a simple malicious web page, so that when a victim visits this web page, a forged request will be launched against *www.example.com* to delete a page belonging to the user. Why cannot a web server use the referer header to tell whether a request is cross-site or not? If a page from *www.example.com* contains an *iframe*, inside which a facebook page is displayed. If a request is sent from inside the *iframe*, is it considered as a cross-site request or not? [8+4+2]

3. Define Access Control. What is Access Control List (ACL)? How is Access Control List implemented in Unix Operating System? [4+4+8]

4. Why is Multilevel Security Policy required? Explain the Bell-LaPadula model. [6+10]

5. What do you mean by API attacks? Explain XOR-to-Null key attack or Differential Protocol attack. Briefly describe the vulnerabilities of operating systems in the context of API attacks. [4+10+4]

6. Define Emission Security. What is the significance of Red/Black separation in thrawting passive attacks. Explain different types of active attacks. [4+6+10]

7. How is *Memory Remanence* exploited to attack a cryptoprocessor? Explain how *Smart Cards* are attacked by slowing down it's execution. Briefly describe the countermeasures of such attacks. [6+6+4]

INDIAN STATISTICAL INSTITUTE

First Semester Examination: 2019-2020
M.TECH(CrS) II YEAR

CRYPTOGRAPHIC AND SECURITY IMPLEMENTATIONS

Date: 18.11.2019 Maximum marks: 100 Duration: 3.0 hours.

The paper contains 100 marks. The answers to question 7 not to be submitted now.

1. (a) Given X_1 and Z_1, it requires 6 multiplications to compute X_2, Z_2 using the following formulae:

$$\begin{aligned} X_2 &= (X_1^2 - Z_1^2)^2 \\ Z_2 &= 4X_1Z_1(X_1^2 + AX_1Z_1 + Z_1^2). \end{aligned}$$

   Rewrite these formulae so that X_2, Z_2 can be computed using 5 multiplications.

   (b) Using the modular exponentiation algorithm show how to compute the following:

   - Given $a \in \mathbb{Z}_p$, where $p \equiv 3 \bmod 4$, compute the square root of a if it exists.
   - Given a, N, and $\phi(N)$, compute the multiplicative inverse of a modulo N. Note, $\phi(.)$ is the Euler's totient function. [10]

2. We intend to multiply elements in the prime field $\mathbb{F}_p$ where $p = 2^{192} - 2^{64} - 1$. We assume a base 2^{64} representation of the elements in $\mathbb{F}_p$. Also, assume that you already have a multiplier which can multiply two 192-bit unsigned integers to give a 384-bit unsigned integer. You need to design a efficient procedure for reduction which uses only additions and shifts. Your procedure gets as input $(s_0, s_1, s_2, s_3, s_4, s_5)$ where $s_i < 2^{64}$ and the input represents the integer $s = s_5 2^{320} + s_4 2^{256} + s_3 2^{192} + s_2 2^{128} + s_1 2^{64} + s_0$. Your procedure should output $s \bmod p$. Explain your solution. [10]

3. (a) Derive the addition and doubling formulae for the points in the Montgomery curve $By^2 = x^3 + Ax^2 + x$ where A, B are elements in a field K whose characteristic is not 2 and $B(A^2 - 4) \neq 0$.

   (b) Let $\mathcal{M}$ be the set of points on the Montgomery curve described in the above problem, and ∞ be the point at infinity. Define $\mathrm{x} : \mathcal{M} \to K \cup \{\infty\}$ as $\mathrm{x}(x, y) = x$ and $\mathrm{x}(\infty) = \infty$. Let $P \in \mathcal{M}$ be such that $P \neq \infty$ and $\mathrm{x}(P)^3 + A\mathrm{x}(P)^2 + \mathrm{x}(P) \neq 0$, then (using the expressions derived for the above problem), show that

$$\mathrm{x}(2P) = \frac{(\mathrm{x}(P)^2 - 1)}{4\,(\mathrm{x}(P)^3 + A\mathrm{x}^2 + \mathrm{x}(P))}.$$

[20]

4. Consider the following algorithm for computing the Montgomery constant when given inputs N, a odd positive integer and $r = 2^w$, where w is the word length.

```
$y \leftarrow 1$;
for $i = 2$ to $w$
    if $(Ny \bmod 2^i) \neq 1$,
        $y \leftarrow y + 2^{i-1}$;
    end if
end for
return $y \leftarrow r - y$
```

Prove that the above algorithm is correct, i.e., it outputs $\mu = -N^{-1} \bmod r$.

[10]

5. Consider an instruction set architecture with 128-bit registers R1, R2, ... , R10, with the following instructions:

- XOR(R1, R2, R3) : Computes the bitwise XOR of R1 and R2 and stores the result in R3
- LSHFT(R1, k): Shifts left the contents in R1 by k bits.
- RSHFT(R1, k): Shifts right the contents in R1 by k bits.
- XMUL64(R1, R2, k,R3) : Computes the carryless product of 64 bits of R1 and 64 bits of R2 and stores it in R3 as follows. Let R1 and R2 contain a and b where a, b are both 128 bits. Let $a = a1||a0$ and $b = b1||b0$, where $a0, a1, b0, b1$ are all 64 bits then XMUL64(R1, R2, k,R3) yields the following results:

```
if k == 0, R3 = a0*b0;
if k == 1, R3 = a0*b1;
if k == 2, R3 = a1*b0;
if k == 3, R3 = a1*b1;
```

where $a*b$ represents the carryless product of a and b, i.e, consider $a =< a_{63}, a_{62}, \ldots, a_0 >$ and $b =< b_{63}, b_{62}, \ldots, b_0 >$ to represent the polynomials $a(x) = \sum_{i=0}^{63} a_i x^i$ and $b(x) = \sum_{i=0}^{63} b_i x^i$ over $GF(2)$, then $a * b$ computes $a(x)b(x)$ with additions and multiplications in $GF(2)$.

You are given two polynomials $A(x)$ and $B(x)$ of degree at most 127 with coefficients in $GF(2)$ and an irreducible polynomial $\sigma(x) = x^{128} + p(x)$ over $GF(2)$ such that the degree of $p(x)$ is at most 63. Assume the the polynomials $A(x)$, $B(x)$ and $p(x)$ are given to you stored in three different 128-bit registers. Write a program using the instructions specified above to compute $A(x)B(x) \bmod \sigma(x)$. Explain your solution.

[20]

6. You have a CPU which has specialized arithmetic units GF128ADD and GF128MUL to perform additions and multiplications respectively in $GF(2^{128})$. Both takes two 128 bit strings as inputs and outputs a 128 bit string, and they take 2 clock cycles and 4 clock cycles respectively to complete the operations. Assume that the CPU has k independent GF128ADD and GF128MUL units, i.e., you can perform k multiplications and k additions simultaneously.

   Let $f(x) = a_0x + a_1x^2 + \ldots + a_{nk}x^{nk+1}$ be a polynomial over $GF(2^{128})$. Given $b \in GF(2^{128})$, you are required to compute $f(b)$. Describe a strategy to compute $f(b)$ with exploiting the parallelism as best as you can. What would be the theoretical cycle counts required for the computation? Explain your answer.

[10]

7. **Implementation**: This question is take-home. The submission instructions can be found in www.isical.ac.in/~debrup/takeHome.html.

   (a) Consider the permutation $\Pi : \{0,1\}^{256} \rightarrow \{0,1\}^{256}$, as described in the algorithms below:

```
procedure $F_{c,b}(x)$
1. $y \leftarrow c \oplus b$;
2. $C \leftarrow$ SETR_EPI32(0x00 $\oplus y$, 0x10 $\oplus y$, 0x20 $\oplus y$, 0x30 $\oplus y$);
3. return AESENC(AESENC($x, C$), 0);

procedure $\Pi(x)$
1. $x_1||x_0 \leftarrow (x)$;
2. $b \leftarrow 2$; $c \leftarrow 1$; $R \leftarrow 15$;
3. for $r \leftarrow 0$ to $R-1$;
4.     $x_{r+1 \bmod 2} \leftarrow x_{r+1 \bmod 2} \oplus F_{c,b}(x_{r \bmod 2})$;
5.     $c \leftarrow c + 1$;
6. end for
7. return $x_1||x_0$;
```

- In the procedure $F_{c,b}(x)$, c, b are 32 bit strings and x is a 128 bit string. The procedure returns a 128 bit string. AESENC(X, Y) is one round of AES-128 with X as the state and Y the key. In particular the AESENC(X, Y) is computed as:

```
procedure AESENC($X, Y$)
1. $X \leftarrow$ SubBytes($X$);
2. $X \leftarrow$ ShiftRows($X$);
3. $X \leftarrow$ MixColumns($X$);
4. $X \leftarrow X \oplus Y$;
5. return $X$;
```

- The procedure $\Pi(x)$ takes in a string of 256 bits and outputs a string of 256 bits. In line 1 of the procedure, x is parsed as two strings x_0 and x_1, which are the least significant 128 bits and the most significant 128 bits respectively.

Answer the following questions (look for the submission instructions in the webpage specified above):

i. Write an algorithm for Π^{-1}.

ii. Implement both Π and Π^{-1}. Your implementation should use SIMD instructions and the AES-NI instructions, as required, through Intel intrinsics.

iii. Compute the values of $\Pi(0^{256})$ and $\Pi(1^{256})$.

(b) Let p be the largest prime less than 2^{127}.

i. Find p;

ii. Write efficient programs for addition and multiplication in Z_p.

[20]

INDIAN STATISTICAL INSTITUTE
Semestral Examination
M. Tech. (CrS) II year (1st Sem): 2019–2020
Topics in Cryptology

Date: 25.11.2019 Maximum Score: 100 Time: 3.5 Hours

Answer all the questions. The maximum you can score is 100.

1. Answer in one or two sentences.

   (a) What is *round efficient* zero knowledge proof?

   (b) Give one example of passive and one example of active non-invasive physical attack.

   (c) If a language L has a unidirectional zero knowledge proof, then $L \in \mathcal{BPP}$. How would you justify the fact that graph hamilonian is an $\mathcal{NP}$-complete problem and it has a non-interactive zero knowledge proof?

   (d) Mention two countermeasures for resisting side-channel attacks.

   (e) What is the power of the adversary in Integral and Boomerang attack?

   (f) In a zero knowledge proof, if a simulator can prove without witness, why can't the prover?

   (g) Mention two limitations of Homomorphic encryption.

   (h) Why AES-128 would not be used for practical purposes in quantum paradigm?

   (i) How can you use MILP in impossible differential cryptanalysis?

   (j) What is circular security of an encryption scheme?

   $[10 \times 2 = 20]$

2. Answer the following questions with proper justifications.

   (a) Suppose, Alice has a software that given the revenue, past income and manpower of a company can predict its future stock price. Now, Bob wants to know the future stock of his company without disclosing the confidential information and Alice also does not want to give her software containing the secret formulas. Can you suggest a cryptographic tool that can solve the issue?

(b) An S-box is called *Almost Perfect Non-linear* (APN) if all the entries in it's DDT belongs to $\{0, 2\}$. Show that, a 5×5 S-Box defined as $S(0) = 0$, $S(x) = x^{-1}$ $\forall x \neq 0$ is APN.

(c) What is the necessity of having both *perfectly hiding* as well as *perfectly binding* commitment scheme in the round-efficient ZKP for Graph 3-coloring?

(d) Why would you prefer *sponge mode* in *Encrypt-then-MAC* paradigm while designing side-channel attack resistant authenticated encryption schemes?

(e) How homomorphic encryption can be used in a zero-knowledge proof protocol for every language $L \in NP$?

(f) How many times you should run the Grover operator to search an element from an unordered set of 16 elements? If you execute it just once, what will be the success probability?

$[6 \times 5 = 30]$

3. (a) Given a plaintext pair which are equal at all bytes but one, show that the ciphertexts of 4-round (last round without Mix-Column) AES cannot be equal in any of the diagonals (i.e. the combinations of bytes: $(1, 6, 11, 16)$, $(2, 7, 12, 13)$, $(3, 8, 9, 14)$, $(4, 5, 10, 15)$).

   (b) Mount a distinguishing attack on 4-round AES using the above impossible differential result. Find the complexity of the attack.

   (c) Prove that 5-round AES is Boomerang attack resistant. The minimum number of active S-Boxes in AES after 1/2/3/4/5 rounds are 1/5/9/25/26 respectively.

[8+6+6=20]

4. (a) Explain the following properties of a homomorphic encryption: (i) compact, (ii) multi-hop, (iii) circuit privacy.

   (b) What is the basic difference between obfuscation and homomorphic encryption? Note that, in obfuscation, you give the cloud an encrypted program $E(P)$. For any input x, the cloud can compute $E(P(x)) = P(x)$, but learns nothing about P except $\{x_i, P(x_i)\}$.

   (c) Describe a somewhat homomorphic encryption scheme capable of both addition and multiplication. Prove the correctness of the scheme.

(d) How can you construct a public-key strongly homomorphic encryption scheme from a secret-key strongly homomorphic encryption? What happens in case the underlying homomorphic encryption is *not strong*?

[3+2+5+5=15]

5. (a) Consider a block cipher AES$^-$ which is identical to AES except that we remove the shift row operation. Mount an Integral attack on general r round AES$^-$.

   (b) Describe a deterministic fault attack on AES, where a random byte fault is injected at the begining of the 9^{th} round.

   (c) How much can you improve the attack if you are allowed to (i) inject faults on at most 4 bytes, and (ii) choose the byte positions of the faults?

[6+4+5=15]

6. (a) Let E be an elliptic curve over $\mathbb{F}_q$, where q is a power of any prime number p. Prove that, E is supersingular if and only if $\#E(\mathbb{F}_q) \equiv 1 \mod p$.

   (b) Prove that, if $p \geq 5$ be any prime and $p \equiv 2 \mod 3$, then the elliptic curves with j-invariant 0 are supersingular over $\mathbb{F}_p$ using the following steps:

      i. Let E be an elliptic curve defined over $\mathbb{F}_p$. Show that, E is supersingular if and only if $\#E(\mathbb{F}_p) = p + 1$.

      ii. Let $\psi : \mathbb{F}_p^\times \to \mathbb{F}_p^\times$ be the homomorphism defined by $\psi(x) = x^3$. Prove, that ψ is bijective.

      iii. Let $B \in \mathbb{F}_p^\times$, $E : y^2 = X^3 + B$ be an elliptic curve. Show that $E(\mathbb{F}_p) = p + 1$.

   (c) Let p be any large prime. Let E be any supersingular elliptic curve defined over $\mathbb{F}_{p^2}$. Let $\ell < p$ be any prime. Let $P, Q \in E$ such that $E[\ell] =< P, Q >$. Define an ℓ-degree isogeny $\phi : E \to E'$ where $E' := \frac{E}{<P+xQ>}$ for some fixed $x \in \mathbb{Z}_\ell$. Let $\hat{\phi}$ be the dual of ϕ. Find an $R \in E'$ such that $ker(\hat{\phi}) =< R >$.

[4+6+5=15]

7. Consider COLM authenticated encryption depicted in Fig 1.

(a) Describe the following properties of COLM: (i) parallel, (ii) rate, (iii) inverse-free, (iv) efficient static AD processing.

(b) How can you mount a statistical fault attack on COLM?

(c) Mount a forgery attack on COLM in quantum paradigm. Can you suggest a small modification in COLM to invalidate the attack?

[4+5+6=15]

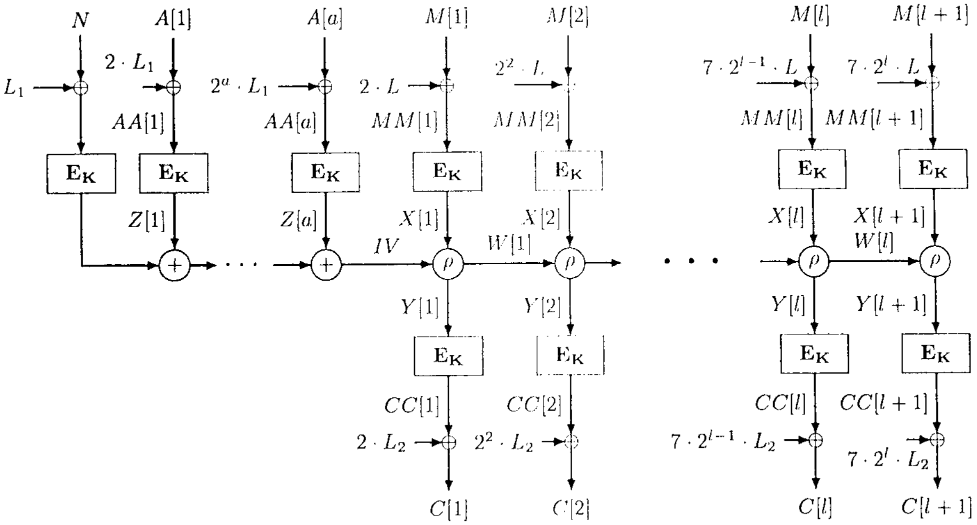

Figure 1: COLM Authenticated Encryption Mode with nonce N, Associated data A and message M. Assume $L = E_K(0)$, $L_1 = 2 \cdot L$, $L_2 = 3 \cdot L$. $M[l+1]$ is defined as the checksum of all the message blocks. The function ρ is defined as $\rho(X[i], W[i-1]) = (Y[i] := X[i] \oplus 3 \cdot W[i-1],\ W[i] := X[i] \oplus 2 \cdot W[i-1])$.

INDIAN STATISTICAL INSTITUTE

First Semester Examination: 2019-2020
M.TECH(CrS) II YEAR

Machine Learning For Security

Date: 21.11.2019 Maximum marks: 100 Duration: 3.0 hours.

1. State with short explanations whether the following statements are TRUE or FALSE.

   (a) The convex hull of a set of vectors $\boldsymbol{x}_i, i = 1, \ldots, n$ is the set of all vectors of the form $\boldsymbol{x} = \sum_{i=1}^{n} \alpha_i \boldsymbol{x}_i$ where the coefficients α_i are non-negative and sum to 1. Let X_1 and X_2 be two sets of vectors which are linearly separable. Then the convex hulls of X_1 and X_2 have a non empty intersection.

   (b) Consider a two class classification problem into classes c_1 and c_2, the class conditional probability distributions for the two classes are multivariate normals with different means but the same variance-covariance matrix. The prior probabilities are the same. The Bayesian discriminant function for this problem will be quadratic.

   (c) Consider that the 1-nearest neighbor rule (or the nearest neighbor rule) is being used to classify points. Say, for two different test points $\boldsymbol{x}_1$ and $\boldsymbol{x}_2$ the nearest neighbor in the training set is the same and so they are classified into the same class c. Let $\boldsymbol{x}_3$ be any point on the line joining $\boldsymbol{x}_1$ and $\boldsymbol{x}_2$. $\boldsymbol{x}_3$ will be classified in class c.

   (d) We are given a data set $X = \{1, 2, 3, 4, 5\}$. I want to find two clusters in this data. I start with the following two cluster centers: $z_1^0 = 3$ and $z_2^0 = 10$. The k-means algorithm will work in this case.

   (e) Let $K_i, i = 1, 2, \ldots n$ be n Mercer Kernels and $a_i, i = 1, 2, \ldots n$ be n positive real numbers. Then $\sum_{i=1}^{n} a_i K_i$ is always a Mercer Kernel.

[25]

2. Suppose we are given a training set $\{(\boldsymbol{x}^{(1)}, y^{(1)}), \ldots, (\boldsymbol{x}^{(m)}, y^{(m)})\}$, where $\boldsymbol{x}^{(1)} \in \mathbb{R}^{(n+1)}$ and $y^{(i)} \in \mathbb{R}$. We would like to find a hypothesis of the form $h_{\boldsymbol{w},b}(x) = \boldsymbol{w}^T x + b$ with a small value of $\boldsymbol{w}$. Our (convex) optimization problem is:

$$\min_{\boldsymbol{w},b} \quad \tfrac{1}{2}||\boldsymbol{w}||^2$$

$$\text{such that} \quad \begin{array}{l} y^{(i)} - \boldsymbol{w}^T\boldsymbol{x}^{(i)} - b \leq \epsilon \quad \forall i = 1, 2, \ldots, m \\ \boldsymbol{w}^T\boldsymbol{x}^{(i)} + b - y^{(i)} \leq \epsilon \quad \forall i = 1, 2, \ldots, m \end{array}$$

Where $\epsilon > 0$ is a given fixed value.

(a) Write down the Lagrangian for the above optimization problem. Note that we will require two Lagrange multipliers for the two inequality constraints.

(b) Derive the dual optimization problem.

(c) Show that this algorithm can be kernelized. For this, you have to show that (i) the dual optimization objective can be written in terms of inner-products of training examples; and (ii) at test time, given a new $\boldsymbol{x}$ the hypothesis $h_{w,b}(\boldsymbol{x})$ can also be computed in terms of inner products.

[8+12+5]

3. (a) Let $\mathcal{H}$ be a collection of subsets of a given set S and let $B \subset S$. When is $\mathcal{H}$ said to shatter B?

(b) Let $\mathcal{H}$ be a collection of subsets of $\mathbb{R}$ defined as $\mathcal{H} = \{A \subset \mathbb{R} : |A| < \infty\}$, i.e., $\mathcal{H}$ contains all finite subsets of $\mathbb{R}$. Find the VC dimension of $\mathcal{H}$.

(c) Consider $\mathcal{A}$ to be the set of all convex polygons in $\mathbb{R}^2$. Define $\mathcal{H} = \{h_P : P \in \mathcal{A}\}$, where

$$h_P(x) = \begin{cases} 1 & \text{if } x \text{ lies within polygon } P \\ 0 & \text{otherwise} \end{cases}$$

Note points on the vertices and edges of the polygons are considered to be points within the polygon. Find the VC dimension of $\mathcal{H}$.

[5+5+8]

4. Suppose we have an estimation problem in which we have a training set $\{\boldsymbol{x}^{(1)}, ..., \boldsymbol{x}^{(m)}\}$ consisting of m independent examples. We wish to fit the parameters of a model $p(\boldsymbol{x}, z; \theta)$ to the data, where the likelihood is given by

$$\ell(\theta) = \sum_{i=1}^{m} \log \sum_{z} p(\boldsymbol{x}, z; \theta).$$

As discussed in class a way to do this is to use the EM algorithm where the following two steps are repeated until convergence:

(E- Step): Set for all $i = 1, 2, \ldots m$,

$$Q_i(z^{(i)}) \leftarrow p(z^{(i)} | \boldsymbol{x}^{(i)}; \theta)$$

(M- Step): Set

$$\theta \leftarrow \arg\max_{\theta} \sum_{i} \sum_{z^{(i)}} Q_i(z^{(i)}) \log \frac{p(x^{(i)}, z^{(i)}; \theta)}{Q^{(i)}(z^{(i)})}$$

Prove that these update rules indeed maximizes the likelihood and it converges. [20]

5. We have a data set $\{\boldsymbol{x}^{(1)}, ..., \boldsymbol{x}^{(m)}\}$ with zero mean and unit variance. We wish to project these data points along an unit vector $\boldsymbol{u}$ such that the variance of the projected data is maximized. Formulate this optimization problem and comment on its solution.

[12]

INDIAN STATISTICAL INSTITUTE

BACKPAPER EXAMINATION
M.TECH(CS) IIYEAR

Machine Learning For Security

Date: 10.01.2020 Maximum marks: 100 Duration: 3 hours.

1. Write short notes on the following: (a) Supervised Learning (b)Unsupervised Learning (c) Semi-supervised Learning (d) Feature selection.

[4 × 5 = 20]

2. Given a training set $\{(\boldsymbol{x}^{(1)}, y^{(1)}), (\boldsymbol{x}^{(2)}, y^{(2)}), \ldots, (\boldsymbol{x}^{(m)}, y^{(m)})\}$, consider the cost function for linear regression:

$$J(\theta) = \frac{1}{2m} \sum_{i=1}^{m} \left(h_\theta(\boldsymbol{x}^{(i)}) - y^{(i)}\right)^2,$$

where $h_\theta(\boldsymbol{x}) = \theta^T \boldsymbol{x}$. Find the Hessian of this cost function and prove that J is convex.

[20]

3. Suppose we are given a training set $\{(\boldsymbol{x}^{(1)}, y^{(1)}), \ldots, (\boldsymbol{x}^{(m)}, y^{(m)})\}$, where $\boldsymbol{x}^{(i)} \in \mathbb{R}^{(n+1)}$ and $y^{(i)} \in \mathbb{R}$. We would like to find a hypothesis of the form $h_{w,b}(x) = \boldsymbol{w}^T x + b$ with a small value of $\boldsymbol{w}$. Our (convex) optimization problem is:

$$\begin{array}{ll} \min_{\boldsymbol{w},b} & \frac{1}{2}||\boldsymbol{w}||^2 \\ \text{such that} & y^{(i)} - \boldsymbol{w}^T\boldsymbol{x}^{(i)} - b \leq \epsilon \quad \forall i = 1, 2, \ldots, m \\ & \boldsymbol{w}^T\boldsymbol{x}^{(i)} + b - y^{(i)} \leq \epsilon \quad \forall i = 1, 2, \ldots, m \end{array}$$

Where $\epsilon > 0$ is a given fixed value.

(a) Write down the Lagrangian for the above optimization problem. Note that we will require two Lagrange multipliers for the two inequality constraints.

(b) Derive the dual optimization problem.

(c) Show that this algorithm can be kernelized. For this, you have to show that (i) the dual optimization objective can be written in terms of inner-products of training examples; and (ii) at test time, given a new $\boldsymbol{x}$ the hypothesis $h_{w,b}(\boldsymbol{x})$ can also be computed in terms of inner products.

[8+12+5=25]

4. Briefly discuss the mixture of Gaussian model. What are the underlying assumptions in the model. Write the expectation maximization algorithm to compute the parameters of the model.

[5+5+10=20]

5. (a) What is principal component analysis. Why is it used?

   (b) We have a data set $\{\boldsymbol{x}^{(1)}, ..., \boldsymbol{x}^{(m)}\}$ with zero mean and unit variance. We wish to project these data points along an unit vector $\boldsymbol{u}$ such that the variance of the projected data is maximized. Formulate this optimization problem and comment on its solution.

[5+10=15]

Indian Statistical Institute

M.Tech (CRS) II

Blockchains and Cryptocurrencies

Semester Examination 2019

Maximum Marks: 100

Date: 27^{th} November, 2019 Time: 3 hours

The question paper contains **5 questions**. Total marks is **115**. Maximum you can score is **100**.

1. Explain briefly. **Answer any 5** out of 7. $(4 \times 5 = 20)$

   a. Wormhole Attack

   b. Benefits of Layer 2 technology in Blockchain

   c. Gossip data dissemination protocol

   d. World State

   e. Bitcoin Mixing (Centralized)

   f. Endorsement Policy

   g. Broken Channel protection mechanism in Lightning Network (in context of HTLC)

2. Answer the following: $(5 + 5 + 5 + 5 = 20)$

   a. Compare and contrast between order-execute paradigm and execute-order-validate paradigm.

   b. Consider the following pseudocode:

```
function increment(){
    a = a + 1
}
function reset(){
    a = 0
}
```

   Suppose client A creates a transaction by calling `increment()` function and client B creates another transaction by calling `reset()`. Suppose both the transactions are initiated at the same time and let the value of a at that time instant be 10. Explain the possible values of a after both the transactions are on the blockchain.
   [Assume the platform to be Hyperledger Fabric]

   c. A major criticism faced by Hyperledger Fabric is that its ordering service, as of now, is centralized. Discuss the pros and cons of such an approach.
   [Refute the claim if you disagree with the criticism. Note that existing ordering services like Solo, Kafka, Raft are not byzantine fault tolerant.]

   d. On Ethereum, the concept of gas enabled the platform to filter malicious code executions like infinite loops. How does Hyperledger Fabric eliminate such a scenario? Provide a minimal example and explain.

3. Online fantasy games are gaining popularity. In these games, participants submit teams containing real-life players before start of a match and get prizes based on the players' real world performances. For example, consider a football match between team A and B. Before the team sheets are released, participants submit a team containing a total of 11 players, each player being either from team A or B. If the players on their team perform well during the match, they earn points. Participants with highest points are rewarded.
   Many participants often complain about the lack of transparency because the online platform can manipulate data and cheat them. Design such a platform on blockchain which provides transparency. Provide smart-contract pseudocode of the core functionalities and a design outline.
   [Marks will be based on design choices, clarity, completeness and use of tools discussed during the course. You may choose your own team sport and define your own competition rules if you want.] (30)

4. Answer the following - (3 + 4 + 5 + 13 = 25)

a. Define Ring Signature.

b. Suppose Dave wants to send a payment to Charlie. How will he construct a one-time receiver address in CryptoNote Protocol to ensure unlinkability of transaction, given that Charlie has public key (A, B) whose corresponding private key is (a, b) : $A = a.\mathbb{G}, B = b.\mathbb{G}$, $\mathbb{G}$ is group of large prime order ? How will Charlie check whether he is the intended recipient of the incoming transaction ?

c. In order to prevent double spending, a key image is used in the construction of One-Time Ring Signature. Dave sends transactions T_1 and T_2 to Charlie by generating two one-time address using Charlie's public key. If Charlie has to spend the output of these two transaction the it has to retrieve the private key. He uses a different method to construct the key-images I_1 and I_2 of the two new transactions T_1 and T_2. It is defined as

$$I = x.\mathbb{G}, \qquad x \text{ is the private key}$$

State how can Dave link the signature of T_1 and T_2.

d. Consider a ring R of size n with public keys $P_1, P_2, \ldots, P_n$. Suppose a participant with public key $P_i = x_i.\mathbb{G}, i \in [1, n]$ wants to launch double spending attack. It generates a signature $\sigma = (I_i', c_1, \ldots, c_n, r_1, \ldots, r_n)$ for message $\mathcal{M}$ using key image $I_i' = \tilde{x}.H_p(P_i)$, where $\tilde{x} \neq x_i$, in order to avoid linkability. Verifier checks the following -

$$L_m = r_m.\mathbb{G} - c_m.P_m, \quad m \in [1, n]$$

$$R_m = r_m.H_p(P_m) + c_m.I_i', \quad m \in [1, n]$$

$$\Sigma_{m=1}^{n} c_m \stackrel{?}{=} H_s(\mathcal{M}, L_1, \ldots, L_n, R_1, \ldots, R_n). \ H_s \text{ is a random oracle}$$

Justify "P_i succeeds in convincing verifier 'with negligible probability"
Note - P_i follows the same procedure for construction of the response c_m, r_m, $m \in [1, n]$ as an honest signer would have done.

5. Answer the following - (4 + 6 + 10 = 20)

a. During creation of micropayment channel between two parties, how to create an *unsigned funding transaction* ? Explain why the parties do not exchange signatures for the Funding Transaction until they have created spends from this funding transaction output ?

b. Explain the role of *RSMC* and *Breach Remedy Transaction* for revoking/invalidating older commitment transaction before creating a new commitment transaction ?
Alice forms a payment channel with Bob with each party depositing 0.5 BTC. Sets a lock time of 100 blocks for first commitment transaction. Now Alice creates a new transaction transferring 0.1 BTC to Bob, revoking the former. Sets a lock time of 96 blocks. What happens if Alice still tries to broadcast the first transaction ? (Explain both the cases - Bob complains about the event within the timeperiod 100 blocks. Bob remains silent and doesn't report the event)

c. Consider five participants: Alice, Bob, Carol, Diana and Eric. Alice has a payment channel with Bob. Bob has a payment channel with Carol. Carol has a payment channel with Diana and Diana has a payment channel with Eric. Each party deposits 2 BTC in a given channel i.e. balance of 2 BTC on every side of every channel. How will Alice transfer 1 BTC to Eric using Hashed Timelock Contract (HTLC), considering that Bob charges a processing fee of 0.01 BTC, Carol and Diana each charge a processing fee of 0.02 BTC ? Explain in details.