# Design and Analysis of Lightweight Authenticated Encryption with Associated Data


## Abstract:

The demand for lightweight cryptographic protocols has skyrocketed in the previous decade, especially for many resource-constrained devices such as IoT end nodes and RFID tags. The goal of lightweight cryptography is to use less memory, processing resources, and power to create a less secure but adequate security solution on devices with limited resources. As a result, lightweight cryptographic protocols should be easier and faster to use than traditional ones. The National Institute of Standards and Technology (NIST) began a standardization process in 2018 for lightweight cryptographic (LWC) encryption schemes that have at least one scheme with a key length of 128 bits and can achieve security against adversaries capable of making 2^{50}- 1 byte queries and 2^{112} computations. Running a good feedback loop on a specified lightweight primitive is a typical approach to designing such schemes. In more technical terms, such approaches process data input into fixed-sized chunks. Following initialization, the primitive output is passed through a suitable function with one of these partial data inputs to provide acceptable output and feedback for the primitive's subsequent execution. In this thesis, we start by looking at existing schemes that use pseudo-random permutations as the underlying primitive and can be thought of as different variations of the Sponge scheme. We give all such structures a new name Transform-then-Permute and do a security analysis. We show that we can reduce the security of such schemes to a graph theoretic security game called the "multi-chain security game," based on the underlying feedback function of the Transform-then-Permute design. Then, for various feedback functions, we employ various techniques to limit an adversary's advantage against this game. As a result, we developed some novel or significantly enhanced security bounds for popular permutation-based authenticated encryption techniques. Finally, we aim to design authenticated encryption techniques to process the most data possible in each protocol iteration. We construct and examine two generalized systems, Full-rate Transform-then-Permute and mF, which use a pseudo-random permutation and a tweakable block cipher as their underlying primitives, respectively. We illustrate how to instantiate these general structures to meet the NIST LwC requirement.



**Keywords: Lightweight cryptography, Authenticated Encryption, AEAD, Multichain, Querygraph**