Abstract

There are several motivation towards designing lightweight cryptographic primitives to provide efficiency in resource-constrained environments – without compromising the confidentiality and integrity of the transmitted information. The state size of such ciphers is kept as small as possible to minimize the area occupied by the cryptographic device. Such secure ciphers are frequently exploited in designing RFID tags, smart cards, etc. The cryptographic community has designed a number of lightweight cryptographic primitives that varies from stream ciphers, block ciphers and recently to hash functions in response to these requirements. However, these primitives need to be carefully cryptanalyzed. This thesis aims towards analyzing and evaluating the security of some the recently proposed lightweight symmetric ciphers against different cryptanalytic techniques.

This thesis can be divided into two parts. In the first part we focus on analyzing various ciphers using classical cryptanalysis techniques and in the second part we focus on estimating the resources required to analyze symmetric ciphers in the quantum framework using the Grover's search algorithm.

In the classical framework we analyze a block cipher SIMON against Differential Fault Attack (DFA). We also show that a stream cipher Fountain-v1, first round candidate of NIST's LWC competition, has a weakness against Cube attack and Conditional Time-Memory-Data-Tradeoff (TMDTO) attack.

In the quantum framework we estimate the resources required to construct reversible quantum circuits for block ciphers SIMON, SPECK and TinyJAMBU and stream ciphers Grain-128-AEAD,LIZARD, and Grain-v1. Grain-128-AEAD and TinyJAMBU are second round candidate of NIST's LWC competition. We then estimate the resources required to apply Grover's search algorithm for key recovery on these ciphers. We implement Differential Cryptanalysis on SPECK and correctly recover the secret key on a SPECK like toy cipher. We also show that using proper sampling of the keystream and Grover's algorithm, states of LFSR based stream ciphers can be recovered in time less than Grover's search complexity in the quantum paradigm.