Abstract

Cryptology consists of cryptography and cryptanalysis, which, in a broad aspect, deals with the design and breaking of cryptographic algorithms. In this thesis, we study and cryptanalysis some of the primitives of symmetric-key ciphers. Additionally, we utilize the random evolution of Cellular Automata (CA) as a countermeasure of a few existing attacks. The techniques that we use for the cryptanalysis exploit the attacks on scan-chain and the cube attacks based on the division property. The fundamental idea of the scan-chain-based attacks is to extract the secret information from the knowledge of controlling and observing the cipher properties. We first mount this attack on an existing prevention scheme and validate this attack on one eSTREAM cipher. Then, we augment the existing design to enhance the security of the new design with the proposed countermeasure. In addition, we estimate the minimum resources that are required to implement the prevention algorithm on hardware platforms. On the other hand, the cube attack is a powerful cryptanalytic technique and is especially powerful against stream ciphers. The idea of the cube attack is to solve a system of nonlinear equations resulting from modifying the equations by assigning arbitrary values to their public variables. Later, this attack is strengthened by using the division property technique. In a class of ciphers, nonlinear feedback shift registers (NLFSRs) are utilized in the initialization phase. The security analysis of the initialization phase establishes resistance to attacks targeting the nonlinear feedback-based state initialization. In this regard, we follow the concept of these cryptanalytic techniques to examine the security of the stream cipher WG-7 (an eSTREAM submission candidate) and the authenticated encryption scheme WAGE (a Round-2 candidate of NIST lightweight competition submissions). Ciphers that offer reasonable security and also hardware efficiency are crucial in cryptographic applications. In this regard, we propose a cellular automata-based counter mode of authenticated encryption scheme. We show that the CA-based scheme removes some constant factors from the expression of the upper bound ad-

vantage of the adversary of one NIST standard authenticated encryption scheme, AES-GCM. This makes the CA-based scheme strong against message forgery attack. The hardware efficiency comes from the usage of CA for its simple and regular structure, which is also verified by implementing the proposed scheme on the FPGA platform.

Keywords: Symmetric Ciphers, Stream Cipher, Authenticated Encryption, Scan-chain-based Attack, Cellular Automata, Cube Attack, Division Property, Mixed Integer Linear Programming.