ABSTRACT

A cryptographic hash function takes an input of arbitrary length and returns a hash value of fixed length while satisfying the properties of preimage resistance, second preimage resistance, and collision resistance. These properties make hash function a valuable cryptographic primitive. Cryptographic hash functions are used in many security constructions such as digital signatures, message authentication codes, and encryption schemes. In this thesis, first we give basics of cryptographic hash functions and different security properties followed by their applications. Then we discuss the compression functions and different construction methods. These two are basic components of a cryptographic hash function. We also give survey of various attack methods on cryptographic hash functions.

Several hash functions have been proposed, but most of them have been shown to be cryptographically weak. The most widespread hash functions are MD5 and SHA-1. Both the hash functions are built by iterating a compression function according to the Merkle-Damgård method. Since their publications both hash functions have spread as cryptographic hash standards and have been deployed in a wide variety of security applications. Security of both hash functions have been damaged by recent dedicated attacks against internal structure of these hash functions and generic attacks against Merkle-Damgård construction. This necessitates the transition to newer more secure hash functions that replace today’s weak hash functions.

In this work we present two new serial iterative hash function proposals MDA-192 and DSHA-1. Both hash functions are based on the design principle of SHA-1. The main goal of work is to enhance the security of SHA-1 and NewFORK-256 against recently proposed attacks. MDA-192 encodes a message into a 192-bit hash value. MDA-192 is based on Merkle-Damgård transformation. Message expansion, data dependent rotations and the increased use of input message word in the step operation are the outstanding features of the proposed hash function. Message expansion of the algorithm expands 16 32-bit words to 96 32-bit words. The main motive of such expansion mechanism is to provide higher minimum distance between similar words, high randomness, good mixing of bits and lesser control over the propagation of difference in the words. By using message words heavily in variable bit rotations and
computation of step operations, we introduce the redundancy in the round functions of MDA-192. The algorithm is more secure and complicated for linear and differential cryptanalysis. DSHA-1 generates 160-bit output. DSHA-1 incorporates the idea of dither construction. Dither construction overcomes intrinsic limitations of the Merkle-Damgård approach. It provides strong resistance to multicollision attacks, long second preimage attacks, and herding attack. The compression function of DSHA-1 takes three inputs. An extra input to a compression function is generated through a fast pseudo-random function.

Parallel branch structure of a compression function is robust against the differential patterns. So we propose a parallel iterative hash function MNF-256. MNF-256 is also designed using the dither construction because it shows strong resistance against major generic and other cryptanalytic attacks. MNF-256 based on the principle of NewFORK-256. It follows parallel structure i.e. its compression function uses three parallel branches to update chaining variables. It takes 512-bit message blocks and generates 256-bit hash value. A random sequence is added as an additional input to the compression function of MNF-256.

We have also analyzed the security level of proposed hash function through various statistical tests. These tests have checked the randomness, onewayness and collision resistance of all proposals. We have measured the impact on the digest bits by changing input message bits through the bit variance test and statistical diffusion test. Results show that all the proposed hash functions have attained maximum performance and achieved avalanche criterion. Statistics related to mean changed bit number, mean changed probability and their standard deviations are considered for inspecting the diffusion quality of all proposals. From the results it is found that for proposed designs standard deviations are very small and mean changed bit number and probability are well above the ideal values \{96, 80, 128\} and 50% respectively. This indicates stable diffusion capability for proposals. In order to investigate the collision resistance capability of the proposed hashing approaches, we have performed collision tests which concentrate on the possibility of colliding between every two hash pair. Results shows that the all the proposals possess a strong collision resistance capability. Simulation results and rigorous analysis of the hash functions indicate that proposed algorithms have good randomness and collision resistance which provide high security against different cryptanalytic attacks.