Abstract

A cryptographic hash function is a mechanism producing a fixed-length output of a message of arbitrary length. It fullfils a collection of security requirements guaranteeing that a hash function does not introduce any weakness into the system to which it is applied. The example applications of cryptographic hash functions include digital signatures and message authentification codes. This thesis analyzes cryptographic hash functions and studies the design principles in the construction of secure cryptographic hash functions.

We investigate the problem of building hash functions from block ciphers and the security properties of different structures used to design compression functions. We show that we can build open-key differential distinguishers for Crypton, Hierocrypt-3, SAFER++ and Square. We know that our attack on SAFER++ is the first rebound attack with standard differentials. To demonstrate the efficiency of proposed distinguishers, we provide formal proof of a lower bound for finding a differential pair that follows a truncated differential in the case of a random permutation. Our analysis shows that block ciphers used as the underlying primitive should also be analyzed in the open-key model to prevent possible collision attacks.

We analyze the `IDEA`-based hash functions in a variety of cipher *modes*. We present practical complexity collision search attacks and preimage attacks, where we exploit a null weak-key and a new non-trivial property of IDEA. We prove that even if a cipher is considered secure in the secret-key model, one has to be very careful when using it as a building block in the hashing *modes*.

We investigate the recent rotational analysis. We show how to extend the rotational analysis to subtractions, shifts, bit-wise Boolean functions, multi additions

and multi subtractions. In particular, we develop formulae for calculation of probabilities of preserving the rotation property for multiple modular additions and subtractions. We examine S-functions and its application to the rotational analysis. The findings are applied to BMW and SIMD. We also propose a new shift distinguisher and apply it to Shabal.

Finally, we introduce chained additions in context of the rotational analysis. We argue that Markov chain assumtion does not always hold and rotational probability of an ARX primitive depends not only on the number of modular additions but also on their positions. We present an explicit formulae for the probability of such chained additions. The findings are applied to `BLAKE2`, `Skein` and SIMD.