Cryptanalysis of Selected Block Ciphers

The focus of this dissertation is to present cryptanalytic results on selected block ciphers. Block ciphers are the mathematical structure that will take a plaintext message and convert it into a ciphertext one block at a time using a secret key. They play an essential role in many cryptographic architectures and frameworks. For a long time they were known as the main building block that will provide confidentiality in an information system. They would also be able to represent a full spectrum of cryptographic services as many block ciphers can be used to construct stream ciphers, hash functions, pseudorandom number generators, and authenticated encryption designs.

For this reason a multitude of initiatives over the years has been established to provide a secure and sound designs for block ciphers as in the calls for Data Encryption Standard (DES) and Advanced Encryption Standard (AES), lightweight ciphers initiatives, and the Competition for Authenticated Encryption: Security, Applicability, and Robustness (CAESAR).

In this thesis, we first present cryptanalytic results on different ciphers. We propose attack named the Invariant Subspace Attack. It is utilized to break the full block cipher PRINTcipher for a significant fraction of its keys. This new attack also gives us new insights into other, more well-established attacks. In addition, we also show that for weak keys, strongly biased linear approximations exists for any number of rounds.

Furthermore, we provide variety of attacks on the family of lightweight block cipher SIMON that was published by the U.S National Security Agency (NSA). The ciphers are developed with optimization towards both hardware and software in mind. While the specification paper discusses design requirements and performance of the presented lightweight ciphers thoroughly, no security assessment is given. We present a series of observations on the presented construction that, in some cases, yield attacks, while in other cases may provide basis of further analysis by the cryptographic community. Specifically. The attacks obtained are using classical- as well as truncated differentials. In addition to that, we also investigate the security of SIMON against different linear cryptanalysis methods, i.e., classic linear, and linear hull attacks. We present a connection between linear characteristic and differential characteristic, multiple linear and differential and linear hull and differential, and employ it to adapt the current known results on differential cryptanalysis of SIMON to linear cryptanalysis results.

Finally, we investigate links between different methods of cryptanalysis and how they can be utilized for block cipher cryptanalysis. We consider the known results on the links among integral, impossible differential and zero-correlation linear hulls in order to prove that constructing a zero-correlation linear hull always implies the existence of an integral distinguisher. Moreover, we show that constructing zero-correlation linear hull on a Feistel structure with SP-type round functions, where P is a binary matrix, is equivalent to constructing impossible differential on the same structure except that P is substituted by the transposed matrix PT. We present an integral distinguishers of 5-round Feistel structure with bijective round functions and 3-round Feistel structure with round functions not necessarily being bijective. In addition to an integral distinguishers of Camellia so far, i.e., 7-round integral distinguishers of Camellia with FL/FL−1 layer and 8-round integral distinguishers of Camellia without FL/FL−1 layer.