Abstract

In this thesis, we introduce one new variant of algebraic attack based on the general decomposition of a boolean function. We also apply our attack technique on other attack methods on stream ciphers. We discuss about the theoretical complexity of this attack technique for LFSR based stream cipher.

In the eSTREAM competition, Grain-v1 is one of the finalists, which is a stream cipher based on linear feedback shift register and nonlinear feedback shift register. Grain family of stream ciphers includes: Grain v1, Grain-128, Grain-128a. As this cipher is based on nonlinear feedback shift register, it is secure against several attacks like classical algebraic cryptanalysis, linear cryptanalysis and correlation attack etc. In this thesis, we introduce one new type of probabilistic algebraic attack on this Grain family of stream ciphers. We extend our probabilistic algebraic attack on Sprout stream cipher, which is Grain type stream cipher. The design specification of Sprout was proposed at FSE, 2015. In this attack technique, we first separate out the LFSR and NFSR part by using a probabilistic technique. We generate some equations involving the state bits of the LFSR and then solve that system to get back the probabilistic state bits of the LFSR. The probability of matching of these obtained bits with the original state bits has been discussed in this thesis. We also discuss about the solving complexity of the final system of equations and also implement to obtain the probabilistic state bits.

Further, we propose a fault attack on Sprout. We implement the fault attack on this cipher by injecting the single bit fault into the NFSR of the cipher in the keystream generation phase. After injecting single bit fault into the NFSR, we recover the secret key bits by observing the normal and faulty keystream bits. We also obtain two weak key-IV pairs of this cipher. If we start the key-IV initialization phase of the cipher with these two weak key-IV pairs then the cipher will generate a same state after 40 rounds of key-IV initialization phase. We also show that, depending upon several conditions, this collision may continue for several clockings, which helps us to prove that the key-IV initialization phase of this cipher has a very poor period.

In 2003, Klimov and Shamir introduced the cryptographic primitive, T-function. This primitive has very good potential in designing boolean function or S-box with good cryptographic properties. In this thesis, we demonstrate one new construction of T-function. Our T-function is more general than the recent construction of Hong et al. We also discuss about several cryptographic properties of our new construction.

In this thesis, we study ACORN, which is a competitor of the CAESAR competi-

tion. We find that there exists a probabilistic linear relation between the message and ciphertext bits of ACORN, and the relation holds with probability greater than $\frac{1}{2}$.

Keywords: Algebraic cryptanalysis, Authenticated encryption, ACORN, Boolean function, Bent function, Decomposition of boolean function, Fault attack, Grain family, Nonlinearity, Probabilistic algebraic attack, Sprout, T-function.