CORR 2000-22

Cryptanalysis of the "Augmented Family of Cryptographic Parity Circuits" proposed at ISW'97

A.M. Youssef

Abstract At Crypto '90, Koyama and Terada proposed a family of cryptographic functions for application to symmetric block ciphers. Youssef and Tavares showed that this family is affine and hence it is completely insecure. In response to this, Koyama and Terada modified their design, by including a data dependent operation between layers. The modified family of circuits was presented in the first international security workshop (ISW'97). In this paper, we show that the modified circuit can be easily broken by a differential-like attack. More explicitly, we show that after d rounds, and for any specific key k, the input X can be partitioned into $M \leq 2^d$ sets such that the ciphertext Y of each set is related to the plaintext X by an affine relation. In the average case, $M << 2^d$. Our attack enables us to explicitly recover these linear relations. We were able to break an 8-round 64-bit version of this family in few minutes on a workstation using less than 2^{20} chosen plaintext-ciphertext pairs.

Keywords Block cipher, cryptanalysis, augmented parity circuits.