ABSTRACT

Any reliable cryptography algorithm must provide the high non-linearity between ciphertext and plaintext as a primary security measure. Customarily, Error Correcting Codes are used for recovery of the original message from channel-induced errors. If channel coding theory and its error correcting properties are effectively incorporated into the construction of reliable cryptography algorithms, then such technique is called as Crypto-coding.

In this work, a novel Mixed Parity Code is constructed as Enhanced Hamming Code by considering the existing (8, 4) Extended Hamming Code. Enhanced Hamming Code is developed by randomized parity bits padding among the codeword bits of Extended Hamming Code. Our work concentrates on the designing of two novel structures for Symmetric Key-based Crypto-coding. In one structure, designing of memory-efficient cum dynamic Code-based Substitution box is proposed and in another structure, generation of Code-based round-key schedules using novel Enhanced Hamming Code is proposed. In addition, we propose two different schemes for the generation of Code-based round-keys schedules. Here, one method has separation of each key schedules into two parts as Split Key Generation Scheme, and another method is proposed as Reversible Forward Key Generation Scheme for the different application of proposed Crypto-coding in the non-split key algorithms.
We have introduced a novel key-dependent dynamic EnHC based S-box generation and Co-set leader based substitution technique to enhance the security strength of the proposed design against brute force attacks and linear attacks. The Feedback Shift Register and Permutator are used for penetrating high non-linearity between message text and ciphertext by incorporating more number of randomized functions. In the proposed design, we have suppressed the relationship between the S-box elements and round keys schedule generation in the cryptographic functions to improve the randomization at round keys scheduling. These methods would show high security strength against linear and differential cryptanalysis in the proposed design. Every proposed algorithm is designed, simulated and synthesized using Xilinx Integrated Simulation and Synthesize tool. The complexity of the proposed key schedules generation schemes is justified by the adoption of three different nonlinear techniques, namely selective key bits expansion technique, randomized round constant bits expansion technique and stipulated bit inversion technique, for optimal non-linearity dissemination on original key and round keys schedule. The security strength of the proposed S-box substitution scheme against linear and differential cryptanalysis is justified by applying shift based key schedules for each round transformation and removing the shadow of the algebraic expressions in the byte substitution technique of S-box. Security strength of our proposed design is described by the high probability functions of choice of S-box generation, choice of S-box elements selection and key-based substitution with minimum input parameters.