ABSTRACT

In this dissertation, we have presented a new block cipher. The proposed block cipher is a Substitution-Permutation network cryptosystem with a block length of 128 bits and key length of 256 bits. With the increased key length and block size, the proposed block cipher has greater security over DES. A modular design approach was applied. The cipher has three major building blocks and their interaction has been carefully chosen to achieve better security and performance. Algorithmic S-Boxes are used to provide confusion and nonlinearity in the cipher. The proposed cipher uses a highly diffusive diffusion layer, which is a combination of linear mixers, to ensure that fewer rounds are required to achieve avalanche effect. In addition, we use SP network as the structure of the block cipher. Unlike Feistel cipher where only half of the bits are transformed in each round transformation, SP network has a uniform round structure that allows all bits to be transformed in every round. This contributes to the overall avalanche effect of the proposed cipher. The linear mixers are byte-oriented. This makes the proposed cipher suitable for both hardware and software implementations. Nonlinear and highly diffusive key schedule is used to maximize avalanche in the subkeys. This immunizes the key schedule against related-key attacks. The algorithm utilizes identical functions for encryption and decryption, except for the reversal of the key schedule. This saves memory, space and cost since the same module can be reused for both encryption and decryption. This is achieved despite Feistel structure is not used. The round transformation has been designed such that the algorithm uses the same function for both encryption and decryption.