Using the Hill's a Modified Algorithm for Construction the Tweakable block algorithm.

Zurab Kochladze
zurab.kochladze@tsu.ge
Department of computer sciences, Faculty of exact and natural sciences,
Iv. Djavaxishvili Tbilisi State University
No 1. I.Chavchavadaze ave. Tbilisi, Ceorcia

Keywords: symmetric algorithms, tweakable block cipher, Hill modified algorithm.

Hill's famous algorithm moves the open text to the number vector and then multiplied by invertible matrix. The main advantages of this algorithm compared to other algorithms is that in the elaboration of one symbol of the encrypted text, the number of open text characters participated, that make difficult cryptanalyzis of the cipher.
The author of the article [1] proposing the modification of the algorithm in a way that instead of transforming to the vector, the open text will directly transformed to a square matrix, and then multiplied by invertable matrix. It also shows, that the algorithm retain its basic properties.
The report describes the use of the method toconstruct the tweakable block algorithm.
This algorithm works with 128 bits in length blocks and uses 256-bit key. Before the begining of the round, the initial key's first (head) 128 bit and open text are gathered through XOR operation. After the operation, the obtained 128 bit text enters under the first round for processing.

The first operation of the round is to add to the obtained text the tweak parameters through XOR. Tweak parameter is used only in odd rounds. The result of the addition, the 128-byte text is converted 4X4 matrix and it is multiplied by self-invertible matrix. The obtained matrix again transformed to 128 bite and added to the round key. After that, the matrix enters to S block. The S block scheme taken from AES standard, which is known as a specifically constructed to withstand the differential and linear attacks.

Key schedule and Tweake parameters generationcan be done also through usage of Hill's modified algorithm. Initial key will be in the form of a matrix and the matrix is multiplied self-invertable matrix.That represent the key for second round. The previous round keys participate in calculation of the next round keys. The procedure of obtaining of parameters is similar of getting the round keys.
The application of the Hill's modified algorithm makes possible to reduce the amount of rounds that significantly speeds up the execution time of the algorithm.

1. Z. Kochladze Modified Version of the Hill's Algorithm. GESJ: Comutere Science and Telecommunication No3 (43) 2014.