ISSN 1392 – 124X INFORMATION TECHNOLOGY AND CONTROL, 2012, Vol. 41, No. 4

Matrix Power Cipher

Kęstutis Lukšys, Eligijus Sakalauskas

Department of Applied Mathematics, Kaunas University of Technology
Studentų str. 50-327A, LT-51368 Kaunas, Lithuania
e-mail: kestutis.luksys@ktu.lt, eligijus.sakalauskas@ktu.lt

crossref http://dx.doi.org/10.5755/j01.itc.41.4.820

Abstract. In this paper a new symmetric matrix power cipher is presented. The main component of this cipher is the key dependent S-box based on the matrix power function (MPF). We give the details of the cipher and explain how MPF can be used in multiple rounds. The matrix power cipher due to its special algebraic structure can be highly parallelized and each round can be separated into up to m2 distinct threads, where m is the order of square matrices used in the cipher. A security analysis and main security parameters are also provided.

Keywords: global optimization; finite element method; genetic algorithms; optimization of grillages.

1. Introduction

In this paper, a new symmetric cipher based on the matrix power function (MPF) is proposed. The MPF was firstly introduced in [15] and it can be used to create a key dependent S-box. We analyzed such construction in detail and presented our results in [7, 16].

The MPF is based on matrix powering by other matrix. This function is some generalization of discrete exponent function in cyclic groups by its expansion in matrix set. The security assumption of the MPF is quite different from the ordinary discrete exponent function since it does not rely on the difficulty of classical discrete logarithm problem. The MPF can be interpreted as some matrix group action in some other set of matrices. All matrices are quadratic and have the same size.

The preliminary security analysis against the linear and differential attacks of constructed S-box was considered in [7]. The algebraic degree, nonlinearity, differential uniformity, algebraic quadratic equations immunity and algebraic biaffine equations immunity characteristics were analyzed. These characteristics are not absolutely compatible with our construction since full matrix power S-box realizes an injective mapping. But nevertheless we found that they are similar to those of ordinary power functions, like Gold, Kasami, Niho etc. Deeper analysis showed that even single S-box based on the MPF with considerably small parameters can resist differential attack.

We present here a new cipher construction with improved security and flexibility. We briefly review the matrix power and S-box functions in section 2 and show some round properties of the MPF in section 3. Then, the new matrix power cipher is specified in section 4. We analyze its security properties in section 5.

2. Matrix power function

The matrix power function f is defined in the set of $m \times m$ matrices over the finite field GF(2^n), and provides the mapping from GF(2^n)$^{m \times m}$ to GF(2^n)$^{m \times m}$. The domain of f is an arbitrary subset of GF(2^n)$^{m \times m}$ consisting of matrices without zero entries which we denote by $\mathbf{M}$. We assume also for simplicity that the range of f is the same, thus f: $\mathbf{M} \to \mathbf{M}$. According to our construction, MPF represents some matrix group $\mathbf{M_G}$ action in $\mathbf{M}$. Matrix group $\mathbf{M_G}$ is a set of $m \times m$ matrices over the $\boldsymbol{Z}^*_{2^n-1} = \{1, \ldots, 2^n - 2\}$, i.e. using conventional notation we are dealing with a group GL(m, $\boldsymbol{Z}^*_{2^n-1}$). Hence the multiplication operation in $\mathbf{M_G}$ is the ordinary matrix multiplication and it consists of those matrices which have their inverses.

The MPF f is defined as a composition of two functions $f_{L\text{-}}$ and $f_{\text{-}R}$, which are called left and right MPF respectively, i.e.

$$f_{L,R} = f_{L\text{-}} \circ f_{\text{-}R}. \quad (1)$$

The left MPF $f_{L\text{-}}$ provides a mapping $f_{L\text{-}}$: $\mathbf{M_G} \times \mathbf{M} \to \mathbf{M}$ and the right MPF a mapping $f_{\text{-}R}$: $\mathbf{M} \times \mathbf{M_G} \to \mathbf{M}$. Parameters L and R represent any

matrices in matrix group $\mathbf{M_G}$ and reflect the fact that function $f_{L\text{-}}$ is defined by the left action of matrix L and $f_{\text{-}R}$ by the right action of matrix R in $\mathbf{M}$.

We denote the input matrix by X and the output matrices $f_{L\text{-}}(X) = Y$ and $f_{\text{-}R}(X) = Z$, where $L, R \in \mathbf{M_G}$ and $X, Y, Z \in \mathbf{M}$. We denote matrices L, X, R, Y and Z by the indexed sets of their entries respectively, e.g. we denote the matrix X by $\{x_{ij}\}$. Then $f_{L\text{-}}$ and $f_{\text{-}R}$ can be written for the entries of result matrices in the way

$$y_{ij} = \prod_{s=1}^{m} x_{sj}^{l_{is}}, \quad (2)$$

$$z_{ij} = \prod_{t=1}^{m} x_{it}^{r_{tj}}. \quad (3)$$

The entries l_{is} and r_{tj} are in $Z^{*}_{2^n-1}$, i.e. they are integers, and x_{ij} are in GF(2^n). The power and multiplication operations are performed using GF(2^n) field arithmetic. The function $f_{L\text{-}}$ corresponds to the matrix X left powered by the matrix L and $f_{\text{-}R}$ to X right powered by the matrix R:

$$Y = f_{L\text{-}}(X) = {}^{L}X, \quad (4)$$

$$Z = f_{\text{-}R}(X) = X^{R}. \quad (5)$$

MPF cannot be used directly due to special requirements for the input data. None entry of X should be equal to zero to avoid columns and rows of matrices Y and Z, respectively, vanishing to zero. Hence the matrix X can not be an input data matrix, i.e. matrix representing plain text. If we denote the input data matrix by D, then this matrix must be transformed to input matrix X without zero entries. This problem is solved by constructing MPF based S-box function (SBF) F as an injective mapping F: GF$(2^{n-1})^{m\times m} \rightarrow$ GF$(2^n)^{m\times m}$ to guarantee the unique inverse mapping F^{-1} for decryption. The SBF F is a composition of some auxiliary function g_K and MPF $f_{L,R}$ with both defined by additional key matrix $K \in \boldsymbol{Z}_{2^{n-1}}^{m\times m}$ and matrices $L, R \in \mathbf{M_G}$ correspondingly. Then if D is an input matrix of the SBF, the output matrix C can be expressed by the relation

$$C = F(D) = f_{L,R}(g_K(D)). \quad (6)$$

Since function g_K must perform an injective affine transformation from GF$(2^{n-1})^{m\times m}$ to GF$(2^n)^{m\times m}$ we proposed to express it in the following way

$$g_K(D) = D + K + \mathbf{1} = X. \quad (7)$$

Here the addition operations are the ordinary additions of matrices. It is the additions of entries of matrices but they are defined according to the addition rules in $\boldsymbol{Z}_{2^n}$. Matrix denoted by $\mathbf{1}$ is the matrix in $\boldsymbol{Z}_{2^n}^{m\times m}$ consisting of arithmetical unity elements in all its positions.

Then the SBF F explicitly is defined by the following relations

$$F(D) = {}^{L}(g_K(D))^{R} = {}^{L}(D + K + \mathbf{1})^{R} = C. \quad (8)$$

Using the transformation defined in (7), we obtain a matrix $X \in \mathbf{M}$ which does not contain zero entries, despite the presence of zero entries in the matrix D. The smallest possible entry of $\{x_{ij}\}$ is 1 and the largest one can be coded in numerical form being equal to $2^n - 1$. This condition must be necessarily satisfied since the presence of at least one zero entry among $\{x_{ij}\}$ will cause to gain the zero ciphertext matrix C.

Single entry c_{ij} of the ciphertext matrix can be expressed for $i, j = 1, 2, \ldots, m$ by the formula:

$$\prod_{t=1}^{m}\prod_{s=1}^{m}(d_{st} + k_{st} + 1)^{l_{is}r_{tj}} = \prod_{t=1}^{m}\prod_{s=1}^{m} x_{st}^{l_{is}\cdot r_{tj}} = c_{ij}, \quad (9)$$

where 1 is a unity in $\boldsymbol{Z}_{2^n}$.

Since $\mathbf{M_G}$ is a group of matrices, there exist the inverse matrices R^{-1} and L^{-1} such that $RR^{-1} = R^{-1}R = \boldsymbol{I} = LL^{-1} = L^{-1}L$, where $\boldsymbol{I}$ is the identity diagonal matrix in $Z_{2^n-1}^{m\times m}$.

Decryption operation can be written in a similar formal way as in (8):

$$F^{-1}(C) = g_K^{'}\left({}^{L^{-1}}C^{R^{-1}}\right) = {}^{L^{-1}}C^{R^{-1}} - K - \mathbf{1} = D. \quad (10)$$

Function $g_K^{'}$ performs bijective affine transformation from the subset of GF$(2^n)^{m\times m}$ to GF$(2^{n-1})^{m\times m}$.

The security of the S-box based on the matrix power function does not rely on classical DLP problem since the orders of the finite fields are considerable small and hence DLP is reckoned to be feasible. It is rather linked with so called generalized matrix decomposition problem (MDP). According to our knowledge, the first idea to use the most general form of MDP for the public key cryptography in abstract non-commuting groups is presented in [18]. One kind of decomposition problem is used in the asymmetric cryptosystems based on the hard problems in infinite non-commutative groups, e.g. braid groups [17]. The other kind of decomposition problem is used also in digital signature scheme construction and key agreement protocols [12-14].

This kind of MPF and SBF construction allows efficient implementation using parallel computing. Multiplication and powering operations can be implemented efficiently using lookup tables. The size of lookup tables depends on the chosen field size n. All output entries can be calculated separately as it is clearly seen from (9). Thus every MPF operation can be separated to m^2 threads. Each thread should perform m^2 multiplications in $\boldsymbol{Z}^{*}_{2^n-1}$, m^2 powering and m^2 multiplication operations in GF(2^n), i.e. $3m^2$ table lookup operations, and $2m^2$ sum operations in $\boldsymbol{Z}_{2^n}$. If we regard sum and table lookup operations as computationally equivalent, then for the whole output matrix calculation we will need $5m^4$ operations in total.

This number of total operations can be reduced by omitting repeated sums, i.e. input matrix would be

summed with key K only once and then used in the MPF. This would lead to $3m^4 + 2m^2$ operations or $3m^2 + 2$ per thread.

Greater improvement in operations count can be achieved by separating the MPF to the left and the right functions. The number of sum operations remains the same (2 per one thread). But there will not be any multiplications in $\boldsymbol{Z}^*_{2^n-1}$. In the left (right) MPF there are m power operations and $m-1$ multiplications according to (2)–(3). Thus one thread should perform only $4m$ operations for calculation of one output matrix entry. And it would be needed $4m^3$ operations for the whole matrix. The drawback of this approach is that all threads must be synchronized twice, i.e. they must share their results after summation and the left MPF operation.

3. Round properties of the matrix power function

It is known that the left and the right MPFs are associative and hence satisfying the following identities [7]

$$ {}^{L_1}\left({}^{L_2}X\right) = {}^{(L_1L_2)}X, \tag{11}$$

$$ \left(X^{R_1}\right)^{R_2} = X^{(R_1R_2)}, \tag{12}$$

$$ {}^{L}\left(X^{R}\right) = \left({}^{L}X\right)^{R} = {}^{L}X^{R}. \tag{13}$$

We can interpret the last identity as mutually associative property. The single MPF is not applicable for the round function of the iterated cipher according to these identities. Due to (11)–(13) the round functions have a group property. We show this by the contrary assumption.

Assume that the cipher is constructed using t rounds with the S-box represented by the MPF and with t different round key pairs (L_1, R_1), (L_2, R_2), … (L_t, R_t). Let the input of the first round be the matrix X. Then after t rounds we obtain the following ciphertext matrix C

$$ \left({}^{L_t\ldots}\left({}^{L_2}\left({}^{L_1}X\right)^{R_1}\right)^{R_2\ldots}\right)^{R_t} = C. \tag{14}$$

Lemma 1. *If the ciphertext is expressed by (14), then t-round ciphering is equivalent to one round ciphering with a pair of matrices (L_0, R_0) satisfying the following relations*

$$L_0 = L_tL_{t-1} \ldots L_1 \text{ and } R_0 = R_1R_2 \ldots R_t.$$

▼**Proof**. Using identities (11)–(13), we can express the powers in (14) by the matrices L_0 and R_0. Then using association identities (11)–(13) and after substitution of power matrices we obtain

$$ {}^{L_tL_{t-1}\ldots L_1}X^{R_1R_2\ldots R_t} = {}^{L_0}X^{R_0} = C. $$ ▲

Corollary 1. For the S-box round function construction, MPF must be combined with the other functions providing that this composition cannot satisfy the associative identities (11)–(13) and does not yield the matrices with zero entries for the same reasons mentioned above.

Let H: $\mathrm{GF}(2^n)^{m\times m} \to \mathrm{GF}(2^n)^{m\times m}$ be a function which is not mutually associative with the MPF. This means that

$$H\left({}^{L}X^{R}\right) \neq {}^{L}\left(H(X)\right)^{R} \text{ or}$$

$$H\left({}^{L}X^{R}\right) \neq {}^{L'}\left(H(X)\right)^{R'}. \tag{15}$$

We propose the S-box function F to be chosen in the following way

$$F(X) = H\left({}^{L}X^{R}\right). \tag{16}$$

Ciphering function of t rounds can be expressed in the way

$$ {}^{L_t}\left(H\left(\ldots{}^{L_2}\left(H\left({}^{L_1}\left(H(X)\right)^{R_1}\right)\right)^{R_2}\ldots\right)\right)^{R_t} = C. \tag{17}$$

Referencing to Lemma 1 and inequalities (15), this construction allows us to formulate the following result: if the function H is not mutually associative with the MPF, then t-rounds cipher functions cannot be expressed with the equivalent one round function with a key pair (L_0, R_0).

Further we will consider H function as a concatenation of m^2 component functions h_{ij} which are the mappings from $\mathrm{GF}(2^n)$ to $\mathrm{GF}(2^n)$, i.e. they work exclusively with the single entry of the matrix. For the simplicity and efficiency, we choose that all h_{ij} are the same and denote them simply by h.

Theorem 1. *If a component function h is distributive over multiplication in GF(2^n), then the function H is mutually associative with the MPF.*

▼**Proof**. Let us consider only one entry of the output matrix. After the single MPF operation this entry is computed as a product of all entries of the input matrix according to (9). When the function H is applied after the MPF, then one output entry can be expressed by

$$\left\{H\left({}^{L}X^{R}\right)\right\}_{ij} = h\left(\prod_{t=1}^{m}\prod_{s=1}^{m}x_{st}^{l_{is}r_{tj}}\right).$$

If h is distributive over multiplication, then it can be applied not only before multiplication operation but also before powering operation. Thus we obtain

$$h\left(\prod_{t=1}^{m}\prod_{s=1}^{m}x_{st}^{l_{is}r_{tj}}\right) = \prod_{t=1}^{m}\prod_{s=1}^{m}h\left(x_{st}\right)^{l_{is}r_{tj}} = \left\{{}^{L}H(X)^{R}\right\}_{ij}.$$

This leads us to conclusion that if function h is distributive over multiplication then

$$H\left({}^{L}X^{R}\right) = {}^{L}\left(H(X)\right)^{R}.$$ ▲

Corollary 2. To make the functions H and the MPF mutually non associative, the component function h should not be distributive over multiplication, i.e. they should not be equivalent to power mappings.

4. Matrix power cipher

The matrix power cipher (MPC) is a t-round symmetric cipher whose main round function is the MPF. Plaintext data are the $m \times m$ matrices denoted by D over GF(2^{n-1}) and corresponding ciphertext data are the $m \times m$ matrices denoted by C over GF(2^n). MPF uses the key matrices L_i and R_i randomly chosen from the group $\mathbf{M_G}$. There are totally $2t$ such matrices in the MPC. In addition, there is one key matrix K randomly chosen from $\boldsymbol{Z}_{2^{n-1}}^{m \times m}$ and used in function g_K.

4.1. Encryption

The first round of MPC is a composition of the function g_K and MPF:

$$F_1(D) = {}^{L_1}(D + K + \mathbf{1})^{R_1} = X_1. \qquad (18)$$

After the first round, the size of each entry of the data matrix is increased by one bit. This does not take place for the next rounds.

The next rounds ($1 < i \le t$) are the composition of the function H and MPF:

$$F_i(X_{i-1}) = {}^{L_i}(H(X_{i-1}))^{R_i} = X_i. \qquad (19)$$

The output X_t of the last round is the ciphertext C. The function H consists of component functions h which are not equivalent to power mappings as defined in Sect. 3. All functions h are chosen to be permutations of GF(2^n) to ensure valid decryption and they are not equivalent to power mappings. To increase the security of the cipher, these permutations should be cryptographically strong, i.e. they must have high nonlinearity [3], low differential uniformity [9] and high algebraic degree [8]. Some new functions satisfying these criteria can be found in [1, 4, 5].

Schematically MPC encryption is presented in Fig. 1.

MPC can be parallelized to m^2 threads in the same manner as we mentioned in Sect. 2. One thread would perform around $4m$ operations in a single round. And it would take $4tm^3$ operations to calculate the whole ciphertext matrix on m^2 threads. After each round, all threads must synchronize their results.

4.2. Decryption

For the decryption of the cipher text C, all key matrices L_i , R_i must be inverted and inverse function of H must be calculated as well. Inverse matrices can be found using ordinary matrix arithmetic over Z_{2^n-1}

$$L_i' = L_i^{-1},\ R_i' = R_i^{-1},\ 1 \le i \le t.$$

All these matrices must exist since L_i and R_i are chosen from the group $\mathbf{M_G}$. For the valid decryption, these matrices must be used in reverse order. H^{-1} can be easily found by inversion of component function h. The first $t - 1$ rounds are the compositions of the MPF with inversed keys and H^{-1} ($1 \le i < t$) in the following order:

$$F_i'(X_{i-1}) = H^{-1}\left({}^{L'_{t+1-i}}X_{i-1}^{R'_{t+1-i}}\right) = X_i, \qquad (20)$$

where $X_0 = C$.

The last round of MPC decryption is a composition of the MPF and the modified function g_K':

$$F_t'(X_{t-1}) = g_K'\left({}^{L_1'}X_{t-1}^{R_1'}\right) = {}^{L_1'}X_{t-1}^{R_1'} - K - \mathbf{1} = D. \qquad (21)$$

Subtraction of matrices' entries is performed in $\boldsymbol{Z}_{2^n}$. If all key matrices are true, then all entries of D are in GF(2^{n-1}).

Schematically MPC decryption is presented in Fig. 2.

MPC decryption can be parallelized to m^2 threads, too.

5. Security assumptions

The security of the MPC relies on the MPF inversion complexity, since it is the main element of the system. We have studied the security of the MPF in other publications [7, 16]. Hence we will briefly overview those results in case of the MPC and will present more detailed analysis against differential attack.

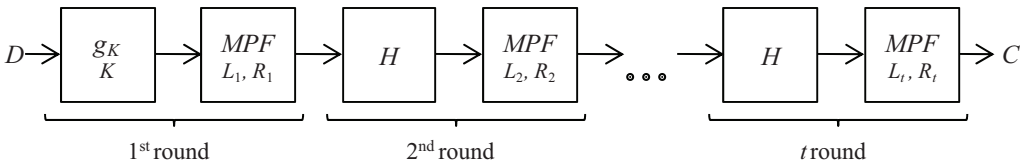

Figure 1. Encryption of t rounds matrix power cipher

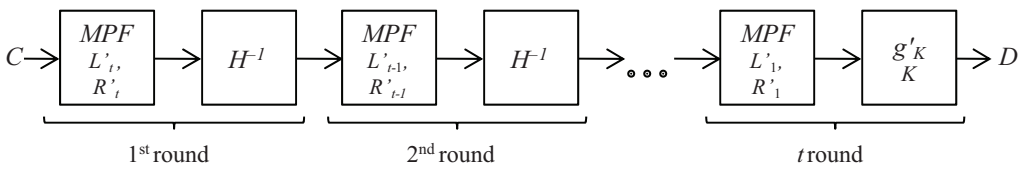

Figure 2. Decryption of t rounds matrix power cipher

5.1. Algebraic cryptanalysis

The matrix power function has rigorous mathematical structure, thus algebraic cryptanalysis of this functions becomes sensible. We understand algebraic cryptanalysis as a construction and solution of the system of algebraic equations which relates plaintext and ciphertext data bits with unknown key bits. The solution of such system in reasonable time completely breaks the cipher.

In case of the matrix power S-box, we obtain an underdefined system of multivariate quadratic (MQ) equations over the ring. It is known that general MQ system is NP-complete problem over any field [11]. Our case is even more complicated than for example AES system of algebraic equations, which is overdefined. In underdefined case even if one knows how to solve the system, there will be more than one solution and an attacker will have to find the right one from the set of all solutions. The solution of the obtained system becomes intractable when $m \geq 4$ [16]. Together with the parameter $n \geq 8$ the matrix power S-box becomes resistant against guess and determine attack when any two key matrices are guessed and the third one can be determined from the system of linear equations [16].

Since matrix power S-box is the first round of the MPC, the whole cipher with the same parameters $m \geq 4$ and $n \geq 8$ gains even greater resistance against algebraic and guess and determine attacks.

5.2. Differential cryptanalysis

The differential cryptanalysis was proposed by Biham and Shamir [2] and so far is an effective cryptanalytic tool against general symmetric block ciphers. The most important security measure against this attack is the number of plaintext-ciphertext pairs needed for the cryptanalysis. The number of these pairs is estimated by inverse of the maximum differential probability (DP) [6], i.e. the probability that given fixed input difference α will force to obtain desired output difference β.

The other expression of this probability is the function's uniformity. A function f is called differentially k-uniform if there are at most k solutions of x satisfying equation $f(x) \oplus f(x \oplus \alpha) = \beta$ [10]. Thus DP of k-uniform function can be expressed by the following equation

$$DP_f = \frac{k}{2^u}, \tag{22}$$

where 2^u is the cardinality of function's domain.

The lower differential probability is the more known plaintext-ciphertext pairs are needed for differential cryptanalysis.

It can be shown that the upper bound of the matrix power S-box (the 1st round of MPC) expected DP (EDP_{SBF}) can be expressed in the following way

$$EDP_{SBF} < EDP_P^{m^2}, \tag{23}$$

where EDP_P denotes the expected DP of random power function with injective affine transformation similar to function g_K. In case of $n = 3$, $EDP_P = 2.75/4$, and for $n = 8$, $EDP_P = 13.4/128 \approx 2^{-3.25}$.

We have analyzed the expected DP of the MPC for the low dimension case when $m = 2$ and $n = 3$. In this case, MPC gives us a mapping from $GF(2^2)^4$ to $GF(2^3)^4$, or 8 bit input block is mapped to 12 bit output block. We have used a randomly generated 3-bit vectorial Boolean function which can be expressed by the truth table (0, 5, 6, 7, 2, 1, 3, 4) as a function h.

In this case, EDP of one round MPC or of the single SBF according to (23) is bounded by $2^{-2.16}$, i.e.

$$EDP_{SBF} < \left(\frac{2.75}{4}\right)^4 \approx 2^{-2.16}. \tag{24}$$

It is also possible to calculate the exact DP of the S-box or entire cipher with 8 bit input and 12 bit output. We have to calculate DP with different keys to evaluate the EDP of this function. If $m = 2$ and $n = 3$, then there are 1080 distinct power matrices (L and R) which are invertible and have no zero entries. There are 256 distinct affine transformations corresponding to the different key matrices K. Thus we obtain around 2^{28} combinations of the key matrices L, R and K for the first round of MPC and around 2^{20t+8} combinations for the whole t-round MPC.

We have analyzed about 2^{19} random variants for the MPC from 1 to 4 rounds to get the clear view of differential uniformity distributions which are presented in Table 1.

Table 1. Differential uniformity distributions of the matrix power cipher for $m = 2$ and $n = 3$

Uniformity	Frequencies, %			
	1 round	2 rounds	3 rounds	4 rounds
4	-	$4{,}8 \cdot 10^{-4}$	0,38	0,73
6	1,79	23,86	91,92	94,98
8	19,87	47,23	7,47	4,27
10	2,49	19,39	0,22	0,03
12	47,92	6,54	0,01	$2{,}4 \cdot 10^{-4}$
14	3,38	1,60	$1{,}3 \cdot 10^{-3}$	-
16	22,16	0,74	$3{,}7 \cdot 10^{-4}$	-
18	-	0,25	$1{,}2 \cdot 10^{-4}$	-
20	1,91	0,18	-	-
22	-	0,09	-	-
24	-	0,05	-	-
26	0,16	0,03	-	-
28	0,16	0,02	-	-
30	0,16	0,01	-	-
32	-	$5{,}5 \cdot 10^{-3}$	-	-
34	-	$2{,}7 \cdot 10^{-3}$	-	-
36	-	$1{,}4 \cdot 10^{-3}$	-	-
38	-	$1{,}3 \cdot 10^{-3}$	-	-
40	-	$6{,}4 \cdot 10^{-4}$	-	-
42	-	$6{,}4 \cdot 10^{-4}$	-	-
52	-	$3{,}2 \cdot 10^{-4}$	-	-

One round cipher with different keys can have only 10 distinct values of uniformity. After two rounds, the set of possible values expands to 22. It is highly possible that there may be even more values, but they may be very rare, i.e. probability of gaining them is less than 2^{-19}.

The expanded set may be explained by the nature of the uniformity of two functions composition. The input difference given to this composition determines the output difference of the first function. The distribution of this difference is predetermined and thus the input difference of the second function is not uniform. Thus the output difference of the second function and of the whole composition differs from difference of the single second function.

The uniformity of the composition depends on the both functions and may be higher or even lower than the uniformities of both functions used in it. Despite the more values of uniformity, the tendency after two rounds is positive. More than 97% of values are not higher than 12. Situation gets even better after 3 and 4 rounds. Uniformity of these ciphers is equal to 6 or lower in more than 90% of cases, and the number of possible values significantly decreases, too. Summarized results of expected uniformity are given in Table 2.

Table 2. Summarized results of the uniformity distributions of the matrix power cipher for $m = 2$ and $n = 3$

Rounds	Uniformity		
	Average	Min	Max
1	12,231±0,014	6	30
2	8,409±0,008	4	52
3	6,151±0,002	4	18
4	6,072±0,002	4	12

Increasing the number of rounds, the expected uniformity of the MPC decreases, i.e. expected DP decreases, too.

More detailed analysis of MPC with higher dimensions is infeasible. In more practical cases when $n = 8$ EDP of the SBF, i.e. one round MPC, for $m = 4$ is bounded as follows

$$EDP_{SBF} < 2^{-52}. \tag{25}$$

This bound does not mean that differential cryptanalysis is not applicable. But as in low dimension case, even maximal DP is lower than the bound given by (24). Thus we concluded that the actual EDP of matrix power S-box is much lower. If we take $m = 5$, then EDP of SBF is bounded by $2^{-81.25}$ and this ensures that differential cryptanalysis is infeasible.

However, the classical differential cryptanalysis cannot be directly applied to the matrix power cipher due to its key dependent nonlinear structure. Practical complexity of such type attack would be even higher than the order of needed known plaintext-ciphertext pairs.

Thus we can make a conjecture that presented MPC with chosen parameters $m \geq 4$, $n \geq 8$ and $t \geq 3$ is sufficiently immune against the differential cryptanalysis.

6. Conclusions

The new cipher based on the matrix power function is presented. The additional round function is introduced since direct iterated application of the MPF is equivalent to the single MPF with adequate keys. The requirements for this function are presented and it is proved that under these conditions, iterated cipher cannot be transformed to the single equivalent MPF.

The security of the MPC is based on the MPF security. Algebraic equations relating input, output and key data bits can be transformed to an underdefined system of multivariate quadratic equations over the ring. The solution of such system becomes intractable with the proper parameters. Thus MPC is resistant against algebraic cryptanalysis and guess and determine attacks. The direct differential analysis cannot be applied to the cipher due to key dependent S-box construction. Thus we derived the theoretical estimation of expected differential probability for a single S-box. According to theoretical results and mathematical modeling, we can make a conjecture that, using multiple rounds, the expected DP is improved. The MPC with chosen parameters $m \geq 4$, $n \geq 8$ and $t \geq 3$ is sufficiently immune against cryptanalysis.

Matrix power cipher due to its special algebraic structure can be highly parallelized and each round can be separated up to m^2 distinct threads.

References

[1] **J. Bierbrauer.** New semifields, PN and APN functions. *Designs, Codes and Cryptography*, 54(3), 2010, pp. 189–200, http://dx.doi.org/10.1007/s10623-009-9318-7.

[2] **E. Biham, A. Shamir.** Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, Vol. 4, No. 1, 1991, pp. 3–72, http://dx.doi.org/10.1007/BF00630563.

[3] **C. Carlet.** Boolean models and methods in mathematics, computer science, and engineering. In: Crama Y., Hammer P.L. (eds.) Boolean Functions for Cryptography and Error Correcting Codes. Cambridge University Press, 2010, 257–397.

[4] **C. Carlet, K. Feng.** An Infinite Class of Balanced Vectorial Boolean Functions with Optimum Algebraic Immunity and Good Nonlinearity. *Proc. of Second International Workshop on Coding and Cryptology*, *Lecture Notes in Computer Science*, Vol. 5557, 2009, 1-11.

[5] **J. Dillon.** APN polynomials: an update. *Fq9*, invited talk (2009). Also available at: http://mathsci.ucd.ie/~gmg/Fq9Talks/Dillon.pdf [accessed: 2011-10-03].

[6] **X. Lai, J. L. Massey, S. Murphy.** Markov Ciphers and Differential Cryptanalysis. *Proceedings of*

EUROCRYPT'91, *Lecture Notes in Computer Science*, Vol. 547, 1991, 17–38.

[7] **K. Luksys, P. Nefas.** Matrix Power S-Box Analysis. Information Science And Computing, book 4 „*Advanced Studies in Software and Knowledge Engineering*", 2008, 97–102.

[8] **W. Meier, E. Pasalic, C. Carlet.** Algebraic attacks and decomposition of Boolean functions. *Proc. of EUROCRYPT 2004*, *Lecture Notes in Computer Science*, Vol. 3027, 2004, 474–491.

[9] **K. Nyberg.** Differentially uniform mappings for cryptography. *Proceedings of EUROCRYPT'93*, *Lecture Notes in Computer Science*, Vol. 765, 1993, 55–64.

[10] **K. Nyberg, L.R. Knudsen.** Provable security against a differential attack. *Journal of Cryptology*, Vol.8, No.1, 1995, 27–37, http://dx.doi.org/10.1007/BF00204800.

[11] **J. Patarin, L. Goubin.** Trapdoor one-way permutetions and multivariate polynomials. *Proceedings of Information and Communication Security, First International Conference, Lecture Notes in Computer Science*, Vol.1334, 1997, 356–368.

[12] **E. Sakalauskas.** One Digital Signature Scheme in Semimodule over Semiring. *Informatica*, Vol. 16, No. 3, 2005, 383-394.

[13] **E. Sakalauskas, A. Katvickis, G. Dosinas.** Key Agreement Protocol over the Ring of Multivariate Polynomials. *Information Technology and Control*, Vol. 39, No. 1, 2010, 51-54.

[14] **E. Sakalauskas, N. Listopadskis, P. Tvarijonas.** Key Agreement Protocol (KAP) Based on Matrix Power Function. *Information Science And Computing*, book 4 „*Advanced Studies in Software and Knowledge Engineering*", 2008, 92–96.

[15] **E. Sakalauskas, K. Luksys.** Matrix Power S-Box Construction. *Cryptology ePrint Archive*: No. 214 (2007), http://eprint.iacr.org/2007/214, 2007.

[16] **E. Sakalauskas, K. Luksys.** The Matrix Power Function and its Application to Block Cipher S-box Construction. *International Journal of Innovative Computing, Information and Control*, Vol. 8, No. 4, 2012, 2655–2664.

[17] **V. Shpilrain, A. Ushakov.** A new key exchange protocol based on the decomposition problem. *Cryptology ePrint Archive*: No. 447 (2005), http://eprint.iacr.org/2005/447.

[18] **V. Sidelnikov, M. Cherepnev, V. Yaschenko.** Systems of open distribution of keys on the basis of noncommutative semigroups. *Russian Acad. Sci. Dokl. Math.* Vol. 48, No. 2, 1993, 566–567.

Received October 2011.