New Asymmetric Cipher Based On Matrix Power Function and Its Implementation in Microprocessors Efficiency Investigation

A. Mihalkovich[1, 2], E. Sakalauskas[1], A. Venckauskas[2]
[1]*Department of Applied Mathematics, Kaunas University of Technology, Studentų St. 50–327, LT-51368 Kaunas, Lithuania, phone: +370 37 300 300*
[2]*Department of Computer Science, Kaunas University of Technology, Studentu St. 50–213, LT-51368 Kaunas, Lithuania, phone: +370 37 300 386*
aleksejus.michalkovic@stud.ktu.lt

***Abstract*–The efficiency of realization of a new asymmetric cipher in microprocessors is presented. The cipher is based on the matrix power function and therefore to the contrary of traditional asymmetric ciphers the computation with large numbers is avoided. Since microprocessors are widely used in embedded systems such as smart-cards and have restricted computational resources the development of effectively realizable cryptographic primitives is a very actual problem. The efficiency investigation of proposed cipher showed that it has a significant superiority with respect to the traditional asymmetric ciphers such as El-Gamal and elliptic curves.**

***Index Terms*–Microprocessors, asymmetric cipher, embedded systems.**

I. INTRODUCTION

As the technological possibilities expand, embedded systems such as smartphones become common devices in our everyday life. The security of data, sent across the Internet, is very important for such devices. This requires creating cryptographic protocols, which can be implemented in computationally restricted electronic devices. However many of known protocols based on commuting cryptography, such as El-Gamal encryption, require a significant amount of computation. In recent time non-commuting cryptographic primitives such as McEliece PKC [1] are considered as a perspective trend of post quantum cryptography. One of the first sources declaring non-commuting cryptography was [2]. In 2007 the state of the art of this perspective field of investigation was presented in seminal book by Myasnikov, Spilrain and Ushakov [3]. In 2007 authors published a new key agreement protocol (see [4]) based on matrix conjugator search problem in combination with matrix discrete logarithm function. This key agreement protocol was named as STR (Sakalauskas, Tvarijonas, Raulynaitis) and was studied in detail in several sources available on web (see [5]–[7]). Continuing our research in non-commuting cryptography we present here a new asymmetric cipher based on matrix power function (MPF). MPF was previously used for key agreement protocol in [8] and asymmetric cipher construction in [9]–[11].

We expect that the proposed asymmetric cipher has an effective realization in restricted computational environments as it was shown by Ottaviani et al. in [5] for STR key agreement protocol.

Manuscript received January 09, 2013; accepted April 08, 2013.
This research was partly funded by a grant (No. VP1-3.1-ŠMM-08-K-01-018) from the EU SA.

II. PRELIMINARIES

Let $\boldsymbol{Z_n} = \{0, 1\ldots, n-1\}$ be a finite ring of integers where the multiplication and addition are performed modulo n. These operations are associative and commuting and we will take it in mind below by default. It is well known that if n is prime then $\boldsymbol{Z_n}$ is a field. Conveniently, we denote a multiplicative group in $\boldsymbol{Z_n}$ consisting of integers relatively prime to n by $\boldsymbol{Z_n}^*$. We denote the order of $\boldsymbol{Z_n}^*$ by $|\boldsymbol{Z_n}^*|$. The value of $|\boldsymbol{Z_n}^*|$ is determined by the value of Euler's totient function $\phi(n)$.

Let Q and Y and all the other matrices defined below be square matrices of order m. Let matrix $Q = \{q_{ij}\}$ powered by matrix $Y = \{y_{ij}\}$ from the right be a matrix $C = \{c_{ij}\}$, i.e.

$$C = Q^Y, \tag{1}$$

where elements of C are computed by the formula $c_{ij} = \prod_{k=1}^{m} q_{ik}{}^{y_{kj}}$.

In a similar way by powering matrix Q from the left by matrix $X = \{x_{ij}\}$ we obtain a matrix $D = \{d_{ij}\}$, i.e.

$$D = {}^X Q, \tag{2}$$

where elements of D are computed by the formula $d_{ij} = \prod_{k=1}^{m} q_{kj}{}^{x_{ik}}$.

Furthermore we can use a combination of both functions to define a *two-sided matrix power function* or MPF by powering matrix Q from the left and right by matrices X and

Y respectively. Denoting the result matrix by $E = \{e_{ij}\}$ we have the following MPF definition

$$E = {}^{X}Q^{Y}, \tag{3}$$

For more clarity let us assume that all matrices are square of second order. The elements e_{ij} are then computed in a following way:

$$\begin{cases} q_{11}^{x_{11}y_{11}} & q_{12}^{x_{11}y_{21}} & q_{21}^{x_{12}y_{11}} & q_{22}^{x_{12}y_{21}} = e_{11} \\ q_{11}^{x_{11}y_{12}} & q_{12}^{x_{11}y_{22}} & q_{21}^{x_{12}y_{12}} & q_{22}^{x_{12}y_{22}} = e_{12} \\ q_{11}^{x_{21}y_{11}} & q_{12}^{x_{21}y_{21}} & q_{21}^{x_{22}y_{11}} & q_{22}^{x_{22}y_{21}} = e_{21} \\ q_{11}^{x_{21}y_{12}} & q_{12}^{x_{21}y_{22}} & q_{21}^{x_{22}y_{12}} & q_{22}^{x_{22}y_{22}} = e_{22} \end{cases}. \tag{4}$$

Consider (3) and assume, that matrices Q and E are given, while matrices X and Y are unknown. We name the problem of finding matrices X and Y, which satisfy (3), as MPF problem.

If elements of matrix Q are from $\boldsymbol{Z_n^*}$, then, referencing to the Euler theorem, we can see, that the elements of matrices Q, X and Y are not in the same algebraic structures. Let matrix Q be from some matrix semigroup $\boldsymbol{M_S}$ over some abstract semigroup $\boldsymbol{S}$. In this case matrices X and Y should be chosen from some ring $\boldsymbol{M_R}$ over some commuting numerical ring $\boldsymbol{R}$, since their elements are powers of elements of matrix Q. It is clear that characterization of $\boldsymbol{R}$ depends on the properties of semigroup $\boldsymbol{S}$. We will name matrix semigroup $\boldsymbol{M_S}$ as a *platform semigroup*, and the matrix ring $\boldsymbol{M_R}$ as a *power ring*. Hence according to (3) and (4), matrices $X, Y \in \boldsymbol{M_R}$ and matrices $Q, E \in \boldsymbol{M_S}$.

Let us now present two lemmas, which indicate important properties of MPF useful for cryptographic protocols construction [9] (Sakalauskas, Luksys, 2007). We denote the ordinary matrix multiplication by XY.

Lemma 1. If $\boldsymbol{R}$ is commuting numerical semiring and $\boldsymbol{S}$ is commuting semigroup, then MPF satisfies the following associative law

$$\left({}^{X}Q\right)^{Y} = {}^{X}\left(Q^{Y}\right) = {}^{X}Q^{Y}. \tag{5}$$

Lemma 2. If $\boldsymbol{R}$ is commuting numerical semiring and $\boldsymbol{S}$ is commuting semigroup, then MPF defined by (4) is an action of $\boldsymbol{M_R} \times \boldsymbol{M_R}$ in $\boldsymbol{M_S}$ satisfying the following identity

$${}^{X}\left({}^{U}Q^{V}\right)^{Y} = {}^{(XU)}Q^{(VY)}. \tag{6}$$

Now we can turn to asymmetric cipher construction.

III. Asymmetric Cipher

The construction of suggested asymmetric cipher is based on the conjecture that MPF is a candidate one-way function (OWF). This means that direct computation of MPF value i.e. computation of matrix E for given instances Q, X and Y in (3) is algorithmically effective while the computation of the inverse value i.e. finding any matrices X and Y for instances Q and E is infeasible.

Let Bob be the sender and let Alice be the receiver. Bob is willing to encrypt a message M using Alice's public key. The message M can be decrypted by Alice's private key.

Alice and Bob agree on the following public matrices: matrix Q, selected from platform semigroup $\boldsymbol{M_S}$ and matrix A selected from power ring $\boldsymbol{M_R}$. Alice randomly selects non-singular secret matrix X in $\boldsymbol{M_R}$ and computes a secret matrix U as a polynomial of A i.e. $U = \boldsymbol{P}_U(A)$, when polynomial $\boldsymbol{P}_U(\ )$ is secret and chosen at random. Alice's private key PrK_A is a pair of matrices (X, U), i.e. $PrK_A = (X, U)$. Her public key is a pair of matrices B and E, i.e. $PuK_A = (XAX^{-1} = B, {}^{X}Q^{U} = E)$.

Bob takes Alice's public key PuK_A and performs a following encryption protocol:

1) Bob randomly chooses a secret non-singular matrix Y in the power ring $\boldsymbol{M_R}$;
2) He selects a random secret polynomial $\boldsymbol{P}_V(\ )$ and computes a secret matrix $V = \boldsymbol{P}_U(A)$. Then he takes matrix B and computes $\boldsymbol{P}_V(B) = XVX^{-1}$;
3) He raises matrix ${}^{X}Q^{U}$ to the obtained matrix power XVX^{-1} on the left and obtains ${}^{XV}Q^{U}$;
4) He raises the result matrix to the power matrix Y on the right and obtains ${}^{XV}Q^{UY} = K$. The obtained matrix K is used as a key to encrypt a message M and compute a ciphertext C.
5) Bob computes the ciphertext $C = K \oplus M$, where $\oplus$ is bitwise sum modulo 2 of entries of matrices K and M.
6) Bob computes matrices $Y^{-1}AY$ and ${}^{V}Q^{Y}$ which we denote by ε i.e. $\varepsilon = (Y^{-1}AY, {}^{V}Q^{Y})$.
7) He sends the enctyptor ε to Alice together with C.

To decrypt Bob's message Alice does the following:

1) Using $Y^{-1}AY$ Alice computes $\boldsymbol{P}_U(Y^{-1}AY) = Y^{-1}UY$, since $U = \boldsymbol{P}_U(A)$.
2) Alice raises matrix ${}^{V}Q^{Y}$ to the power $Y^{-1}UY$ on the right and then raises the result matrix to the power X on the left and hence obtains a matrix ${}^{XV}Q^{UY}$ which is the encryption key K.
3) Alice can now decrypt a ciphertext C using encryption key K and relation

$$M = K \oplus C = K \oplus K \oplus M. \tag{7}$$

Note that only matrices U and V are commuting. This is the main advantage of the suggested protocol as compared with the protocols based on CSP. Note also, that, since Alice and Bob compute their matrices U and V as polynomials of A, only the coefficients of polynomials must be stored. This shortens private key lengths.

IV. Security Parameters Definition and their Secure Values Determination

The suggested protocol has two main security parameters: parameter n, defining group $\boldsymbol{Z_n^*}$, and the matrix order m. The choice of these parameters is based on a fact, that no information about a private key could be recovered from a public key. The recovery implies the solution of the following system of equations with respect to unknown matrices X and U:

$${}^{X}Q^{U} = E, \tag{8}$$

$$XAX^{-1} = B, \tag{9}$$

$$AU = UA, \tag{10}$$

where matrices *Q*, *E*, *A* and *B* are given.

We are making a conjecture that solution of this system of equations is infeasible.

We consider a simplest case of (8), when elements $q_{ij} \in \boldsymbol{Z}_n^*$. Then the discrete logarithm of both sides of (8) can be taken and (8) is transformed to matrix MQ problem. This problem is defined as solving an equation with respect to unknown matrices *X* and *U*

$$XPU = D, \tag{11}$$

where *P* and *D* are discrete logarithms of matrices *Q* and *E* respectively.

It was shown in [12], that if matrix *A* is similar to a Jordan matrix

$$J_A(\lambda) = \begin{pmatrix} \lambda & 1 & & & 0 \\ & \lambda & 1 & & \\ & & \lambda & \ddots & \\ & & & \ddots & 1 \\ 0 & & & & \lambda \end{pmatrix}, \tag{12}$$

then all solutions of (10) can be expressed as polynomials of matrix *A*. Hence (10) has n^m solutions. Equation (9) can be considered in a similar way since it is equivalent to (10) if we consider only invertible matrices. Hence it can be shown, that this equation has $n^{(m-1)}\varphi(n)$ solutions.

Since we obtain commutating matrices using polynomials, while non-singular matrix *X* can be chosen freely, to determine main security parameters we are referring to the following facts:

1. The number of matrices, commuting with a public matrix *A*, defined over a power ring, should be at least 2^{80}. Every commuting matrix should be obtained using polynomials of matrix *A*;
2. The number of matrices, conjugating with a public matrix *A*, defined over a power ring, should be at least 2^{80}.

If these requirements are satisfied, then total scan of matrices *X* and *U* is infeasible. Keeping this in mind the choice of parameters is as follows:

1. For the platform group definition we seek to minimize the group order and to maximize the maximal orders of group elements. In this case the optimal solution is to choose $n = 3p$ with a prime number $p = 2q + 1$, where s is also prime. This yields $r = 2q$.
2. Since we consider (9) and (10) defined in $\boldsymbol{Z}_{\lambda(n)} = \boldsymbol{Z}_{2q}$ the number $\left(\alpha(n)\right)^{m-1} \cdot (q-1)$ must be greater than or equal to 2^{80}. Since $q - 1 = (n-9)/6$ and $\alpha(n) = (n-3)/3$ we get

$$\left(\frac{n-3}{3}\right)^{m-1}\left(\frac{n-9}{6}\right) \geq 2^{80}. \tag{13}$$

We can now apply a natural logarithm to both sides of (13) to obtain

$$m \geq \left\lceil \frac{81\ln 2 + \ln(n-3) - \ln(n-9)}{\ln(n-3) - \ln 3} \right\rceil, \tag{14}$$

where $\lceil\ \rceil$ is the ceiling function.

3. Since we want to make this ciphering algorithm usable in systems with limited resources we must choose parameters values reducing memory and computation resources. In the proposed algorithm the following information should be stored:

a) Multiplication and exponential tables to perform actions with matrices in $\boldsymbol{M_S}$;
b) Addition and multiplication tables to perform actions with matrices in $\boldsymbol{M_R}$;
c) Public matrix $Q \in \boldsymbol{M_S}$;
d) Public matrix $A \in \boldsymbol{M_R}$;
e) Private matrix $X \in \boldsymbol{M_R}$ and a set of coefficients defined in $\boldsymbol{R}$ (private key);
f) Public matrices ${}^XQ^U \in \boldsymbol{M_S}$ and $XAX^{-1} \in \boldsymbol{M_R}$ (public key);

Since addition and multiplication of two matrix elements are commuting it is not necessary to store all elements of these tables. Hence we can store $\varkappa(n)\cdot\left(\varkappa(n)+1\right)/2$ elements for multiplication in a platform semigroup and $\alpha(n)\cdot\left(\alpha(n)+1\right)/2$ elements for actions over a power ring. The exponential table consists of $\varphi(n) \cdot \lambda(n)$ elements. Each matrix consists of m^2 elements and each element consists of $\lceil \log_2 n \rceil$ or $\lceil \log_2 \alpha(n) \rceil$ bits depending on an algebraic structure considered. Let us consider the first five suitable values of *n*: 15, 21, 33, 69 and 141. A presentation of the influence of parameter *n* on keys lengths and memory requirements is available in Table I.

TABLE I. INFLUENCE OF PARAMETER *N* ON KEYS LENGTHS AND MEMORY REQUIREMENTS.

n	m	λ(n)	Key length of bits		Memory requirements
			Private key	Public key	
15	41	4	3444	10086	23928 bits
21	32	6	3168	8192	20428 bits
33	25	10	2600	6520	18000 bits
69	19	22	1900	4332	26800 bits
141	15	46	1440	3150	88792 bits

Since introduced protocol has two security parameters, which have to satisfy the inequality (14), one of them must be chosen for other reasons. Therefore we advice that parameter *n* must be chosen taking the compromise between the available memory and required computation time.

Based on data of Table I we can see that the total amount of bits to store information is the smallest if $n = 33$. This yields $m = 25$ and $\lambda(n) = 10$. However the length of keys is the smallest if $n = 141$, which yields $m = 15$ and $\lambda(n) = 46$.

V. COMPARISON WITH OTHER ASYMMETRIC CIPHERS

We consider the implementation of the suggested protocol on 32 bit microprocessor. Since all arithmetic operations are performed using pre-calculated look-up tables, we can consider them as elementary operations. We estimated the upper bound of number of elementary operations to perform

the asymmetric ciphering which is no more than 8.0×10^5 if $n = 33$ and 1.04×10^5 if $n = 141$. As we can see amount of elementary operations is reduced 8 times in case of $n = 141$ as compared to the case of $n = 33$.

To compare the efficiency of our algorithm with other known algorithms we introduce a term of computational cost defined by the number of elementary operations executed in the custom microprocessor. Since our algorithm uses less elementary operations in the case of $n = 141$ as compared to the case of $n = 33$, we compare its computation cost to a classical El-Gamal-2048 bits asymmetric encryption scheme and elliptic curve ECC-521 asymmetric encryption scheme on 32 bit microprocessor.

In average multiplication of 2048 bit integer requires 8191 elementary operations. The same is true for squaring. Total average amount of elementary operations for Alice to perform asymmetric encryption is about 23.5×10^6. As we can see the minimum average number of operations performed in case of El-Gamal encryption is at least 235 times greater than in our case.

Point addition in ECC-521 can be performed with 9 multiplication and 5 squaring operations [13]. Total amount of elementary operations in average is 8078. Point doubling requires 4 multiplications and 4 squaring operations, which can be computed using 4616 elementary operations. Total amount of elementary operations to perform asymmetric encryption for Alice in average is about 6.9×10^6. This means that this algorithm uses at least 69 times more elementary operations than our algorithm.

The objective results of obtained comparison are presented in Table II.

TABLE II. COMPARISON OF COMPUTATIONAL COSTS OF ASYMMETRIC ENCRYPTION SCHEMES.

Algorithm	**Computational cost**
El-Gamal-2048	23.5×10^6
ECC-521	6.9×10^6
Our algorithm, $n = 33$	8.0×10^5
Our algorithm, $n = 141$	1.04×10^5

The explanation of the obtained results can be based on the fact that the realization of both El-Gamal-2048 and ECC-521 relies on the usage of arithmetic operations with large integers. Despite the fact that integers in ECC-521 are 4 times shorter than in El-Gamal-2048, the cost of each operation of ECC-521 is longer since these operations themselves are more complicated.

VI. CONCLUSIONS

1. We expect that compromisation of the suggested asymmetric cipher is more complex than of other compared and widely distributed ciphers since its security relies on the solution of matrix MQ problem which is related with an NP-complete MQ problem.
2. As we see from computation efficiency estimation results, the proposed cipher has a more effective realization as compared with El-Gamal and especially with widely distributed ECC-521 cipher.
3. If the parameter n increases the computational cost of the proposed algorithm reduces, but memory requirements increase. This means that parameter n must be chosen taking into consideration also memory requirements.
4. On this base an even more secure cipher can be constructed by avoiding the cryptanalysis equation transformation to matrix MQ problem, but with approximately same efficiency of computations.

REFERENCES

[1] R. J. McEliece, "Public key cryptosystem based on algebraic coding theory", The Deep Space Network. Progress Report 42-44, Jet Propulsion Laboratory, California Institute of Technology, 1978, pp. 114–116

[2] V. Sidelnikov, M. Cherepnev, V. Yaschenko, "Systems of open distribution of keys on the basis of non-commutative semigroups", *Doklady Mathematics*, Russian Academy of Sciences, vol. 48, no. 2, pp. 384–386, 1993.

[3] A. Myasnikov, V. Spilrain, A. Ushakov, "Group-based cryptography", *Centre De Recerca Matematica*, 2007.

[4] E. Sakalauskas, P. Tvarijonas, A. Raulinaitis "Key agreement protocol (KAP) using conjugacy and discrete logarithm problems in group representation level", *Informatica, Lithuanian Academy of Sciences*, vol. 18, pp. 115–124, 2007.

[5] V. Ottaviani, A. Zanoni, M. Regoli, "Conjugation as public key agreement protocol in mobile cryptography", 2011, p. 6. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5741660&tag=1

[6] K. Jacobs, *A Survey of Modern Mathematical Cryptology*. 2011, p. 13. [Online]. Available: http://trace.tennessee.edu/utk_chanhonoproj/1406.

[7] M. Sracic, *Quantum Circuits for Matrix Multiplication*, 2011, p. 18 [Online]. Available: http://www.math.ksu.edu/reu/sumar/Quantum Algorithms.pdf

[8] E. Sakalauskas, N. Listopadskis, P. Tvarijonas, "Key agreement protocol (KAP) based on matrix power function", *Advanced Studies in Software and Knowledge Engineering*, vol. 2, no. 4, pp. 92–96, 2008.

[9] E. Sakalauskas, K. Lukšys, "Matrix power s-box construction", 2007, p. 10. [Online]. Available: http://eprint.iacr.org/2007/214.pdf.

[10] E. Sakalauskas, K. Lukšys, "Matrix power function and its application to block cipher s-box construction", *Int. Journal of Innovative Computing, Information and Control*, vol. 8, no. 4, pp. 2655–2664, 2012.

[11] K. Lukšys, E. Sakalauskas, A. Venčkauskas, "Implementation analysis of matrix power cipher in embedded systems", *Elektronika ir Elektrotechnika (Electronics and Electrical Engineering)*, no. 2, pp. 95–98, 2012.

[12] F. Gantmacher, *The Theory of Matrices*, Nauka: Moscow, 1966. (in Russian).

[13] N. Gura, A. Patel, A. Wander, H. Eberle, S. C. Shantz, "Comparing Elliptic Curve Cryptography and RSA on 8–bit CPUs", *Cryptographic Hardware and Embedded Systems, LNCS*, Springer, vol. 3156, pp. 119–132, 2004.