symmetry

MDPI

Article

Improved Asymmetric Cipher Based on Matrix Power Function with Provable Security

Eligijus Sakalauskas [1], Aleksejus Mihalkovich [1,*] and Algimantas Venčkauskas [2]

[1] Faculty of Mathematics and Natural Sciences, Department of Applied Mathematics, Kaunas University of Technology, Studentu str. 50-324, Kaunas LT - 51368, Lithuania; eligijus.sakalauskas@ktu.lt

[2] Faculty of Informatics, Department of Computer Science, Kaunas University of Technology, Studentu str. 50-213, Kaunas LT - 51368, Lithuania; algimantas.venckauskas@ktu.lt

* Correspondence: aleksejus.michalkovic@ktu.lt; Tel.: +370-60014070

Academic Editors: Young-Sik Jeong, Laurence T. Yang and Stefanos Gritzalis
Received: 23 September 2016; Accepted: 28 December 2016; Published: 7 January 2017

Abstract: The improved version of the author's previously declared asymmetric cipher protocol based on matrix power function (MPF) is presented. Proposed modification avoids discrete logarithm attack (DLA) which could be applied to the previously declared protocol. This attack allows us to transform the initial system of MPF equations to so-called matrix multivariate quadratic (MMQ) system of equations, which is a system representing a subclass of multivariate quadratic (MQ) systems of equations. We are making a conjecture that avoidance of DLA in protocol, presented here, should increase its security, since an attempt to solve the initial system of MPF equations would appear to be no less complex than solving the system of MMQ equations. No algorithms are known to solve such a system of equations. Security parameters and their secure values are defined. Security analysis against chosen plaintext attack (CPA) and chosen ciphertext attack (CCA) is presented. Measures taken to prevent DLA attack increase the security of this protocol with respect to the previously declated protocol.

Keywords: cryptography; asymmetric encryption; embedded systems

1. Introduction

In this paper we present the improvement of the matrix power function (MPF) asymmetric cipher published in [1]. The purpose of this improvement is the prevention of discrete logarithm attack (DLA), which allows us to transform the initial system of MPF equations to the matrix multivariate quadratic (MMQ) system of equations. So far, it has not been proved that the MMQ problem is also NP -complete, but nevertheless we are making a conjecture that this problem is hard, since, in general, the corresponding system of MMQ equations is neither underdefined, nor overdefined. It is known that a certain class of underdefined or overdefined systems of MQ equations can be solved in polynomial time.

MPF was previously used to construct cryptographic primitives in [2,3]. Implementation of these primitives in computationally restricted environments was analyzed in [4,5]. The results have shown that suggested protocols can be effectively implemented in Internet of Things (IoT) systems.

Formally, MPF used in our construction can be defined as a function of matrix Q as a parameter and matrices (X, Y) as function arguments parameters denoted by $F_Q(X, Y)$ and expressed by the formula

$$F_Q(X, Y) = E$$

where E is a matrix representing the function value.

In the previous protocol, the entries of matrix Q were chosen in the specially constructed multiplicative group $\boldsymbol{Z}_n^\sharp$ of integers with multiplication operation performed modulo n. In this paper we would like discuss some aspects of this structure and present an alternative algebraic structure, which can be used to execute the proposed protocol more efficiently and prevent discrete logarithm attack.

The cryptographic protocols and algorithms constructed on the base of MPF (see [1,2]) belong to the branch of non-commutiative cryptography. The survey of non-commutative cryptography can be found in [6]. Some initial investigation in this field can be found in [7–9] where the authors investigated the so-called Sakalauskas, Tvarijonas, Raulynaitis (STR) key agreement protocol published in [3]. Moreover, in [8] it is shown that STR protocol can be effectively realized in microprocessors.

In Section 5 we present a proof of our protocol resistance to chosen plaintext attack (CPA) and chosen ciphertext attack (CCA).

The prevention of DLA attack is also presented in subsequent sections.

2. Our Previous Work

Let us recall some definitions from our previous paper.

We consider a commutative multiplicative semigroup $\boldsymbol{S}$. The multiplicative order of semigroup $\boldsymbol{S}$ is defined as the smallest integer t, such that $a^t = e, \forall a \in \boldsymbol{S}$, where e is a neutral element in $\boldsymbol{S}$. Hence the powers of elements of $\boldsymbol{S}$ can be defined in a commutative numeric ring $\boldsymbol{Z}_t$, where addition and multiplication are defined modulo t.

We construct a semigroup of square $m \times m$ matrices with entries defined in semigroup $\boldsymbol{S}$ and denote it by $\boldsymbol{M_S}$. We call this matrix semigroup *a platform semigroup*. Analogously we construct a ring of square $m \times m$ matrices $\boldsymbol{M_R}$ with entries of these matrices defined in numerical ring $R = \boldsymbol{Z}_t$. This ring is called *a power ring*.

The matrix power function (MPF) for a fixed parameter matrix $Q \in \boldsymbol{M_S}$ is a mapping $\boldsymbol{M_R} \times \boldsymbol{M_R} \to \boldsymbol{M_S}$ which is denoted as follows:

$$^XQ^Y = E, \tag{1}$$

where matrices $X = \{x_{ij}\}$ and $Y = \{y_{ij}\}$ are defined in a power ring $\boldsymbol{M_R}$ and matrix $Q = \{q_{ij}\}$ is defined in a platform semigroup $\boldsymbol{M_S}$. The entries of matrix $E = \{e_{ij}\}$ are calculated in a following way:

$$e_{ij} = \prod_{k=1}^{m}\prod_{l=1}^{m} q_{kl}^{x_{ik}y_{lj}}. \tag{2}$$

To demonstrate further clarity, let us assume that all matrices are the square of second order. The elements are then computed as follows:

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

We will refer to matrices X and Y as *matrix powers* or *power matrices*, Q as *a base matrix* and E as *a matrix power value*. Recall from our previous paper, that under chosen algebraic structures the following properties hold for MPF:

$$\left(^XQ\right)^Y = {}^X\left(Q^Y\right) = {}^XQ^Y \tag{3}$$

$${}^X\left({}^UQ^V\right)^Y = {}^{(XU)}Q^{(VY)} = {}^{XU}Q^{VY} \tag{4}$$

To define a platform semigroup we previously considered a multiplicative semigroup $\boldsymbol{Z}_n = \{0, 1, \ldots, n-1\}$, where $n = pq$ is a composite integer and p, q are distinct odd primes with $p > q$. We defined an ideal of this semigroup $Id_q(\boldsymbol{Z}_n) = \{j = i \cdot q; i = 1, ..., p-1\}$ and used it to construct a new multiplicative semigroup $\boldsymbol{Z}_n^\sharp$ in a following way:

$$\boldsymbol{Z}_n^\sharp = \boldsymbol{Z}_n^* \cup Id_q(\boldsymbol{Z}_n), \tag{5}$$

where $\boldsymbol{Z}_n^*$ is a multiplicative group consisting of elements coprime with n. It is well-known, that the multiplicative order of elements of $\boldsymbol{Z}_n^*$ is determined by Carmichael function $\lambda(n)$. For our goals we suggested to use $n = 3p$, since in this case $\lambda(n) = p - 1$ and hence

$$\lambda(n) = |Id_q(\boldsymbol{Z}_n)|,$$

where $|\cdot|$ denotes the cardinality of the set. The latter identity makes it possible to define power ring over ring $\boldsymbol{Z}_{\lambda(n)}$.

The protocol suggested in [1] is described below. We name this protocol as Matrix Power Asymmetric Cipher (MPAC) protocol.

3. Previous Asymmetric Cipher Protocol

Alice and Bob agree on the following public data:

- platform semigroup $\boldsymbol{M_S}$ and power ring $\boldsymbol{M_R}$;
- the base matrix Q;
- two non-commuting matrices Z_1 and Z_2.

Alice randomly selects non-singular secret matrix X in $\boldsymbol{M_R}$ and two sets of coefficients (not necessarily distinct) in numerical ring $\boldsymbol{R}$ to define two polynomials $\boldsymbol{P}_{a1}(\cdot)$ and $\boldsymbol{P}_{a2}(\cdot)$. To construct her private and public data she performs the following actions:

- computes a secret matrix U as a product of two polynomials of Z_1 and Z_2 i.e., $U = \boldsymbol{P}_{a1}(Z_1) \cdot \boldsymbol{P}_{a2}(Z_2)$;
- computes matrices $XZ_1X^{-1} = A_1, XZ_2X^{-1} = A_2, {}^XQ^U = E$.

Alice keeps her private key $PrK_A = (X, U)$ a secret and publishes her public key $PuK_A = (A_1, A_2, E)$.

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

1. Bob chooses randomly a non-singular matrix Y in $\boldsymbol{M_R}$;
2. He selects two sets of coefficients in numerical ring $\boldsymbol{R}$ to define two polynomials $\boldsymbol{P}_{b1}(\cdot)$ and $\boldsymbol{P}_{b2}(\cdot)$ and computes a secret matrix $V = \boldsymbol{P}_{b1}(Z_1) \cdot \boldsymbol{P}_{b2}(Z_2)$. Then he takes matrices A_1 and A_2 and computes a matrix $\boldsymbol{P}_{b1}(A_1) \cdot \boldsymbol{P}_{b2}(A_2) = XVX^{-1} = W$;
3. He raises matrix ${}^XQ^U$ to the obtained power matrix $W = XVX^{-1}$ on the left and obtains ${}^{XV}Q^U$ since $WX = XV$;
4. He raises the result matrix to the power matrix Y on the right and obtains ${}^{XV}Q^{UY} = K$ and converts it to a bit string. One of the possible ways to do this is to write all the elements of matrix K in a string of the form
$$k_{11}k_{12}\ldots k_{1m}k_{21}k_{22}\ldots k_{2m}\ldots k_{mm}$$
and convert every $k_{ij} \in \boldsymbol{S}$ into its binary representation. Then bit string of matrix K is a concatenation of all binary representations of k_{ij}. The obtained bit string is used as a key to encrypt the message M and compute the ciphertext C;
5. Bob computes the ciphertext $C = K \oplus M$, where $\oplus$ is bitwise sum modulo 2 of all entries of bitstings K and M;
6. Bob computes three matrices $(Y^{-1}Z_1Y = B_1, Y^{-1}Z_2Y = B_2, {}^VQ^Y = F)$ which we denote by encryptor ε and sends it to Alice together with C.

To decrypt Bob's message Alice does the following:

1. Using given matrices B_1 and B_2 Alice computes $\boldsymbol{P}_{a1}(B_1) \cdot \boldsymbol{P}_{a2}(B_2) = Y^{-1}UY$, since $U = \boldsymbol{P}_{a1}(Z_1) \cdot \boldsymbol{P}_{a2}(Z_2)$;
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 $K = {}^{XV}Q^{UY}$ and converts it to a bitstring.
3. Alice can now decrypt a ciphertext C using encryption key K and relation

$$M = K \oplus C = K \oplus K \oplus M.$$

Since discrete logarithm can be applied to both sides of Equation (1), it can be transformed to the following matrix equation

$$X(\mathrm{ld}_g Q)Y = \mathrm{ld}_g E.$$

Security of this protocol relies on the following problem:

Definition 1. *The problem of finding matrices X and Y, satisfying the following system of equations*

$$\begin{cases} XTY = S \\ X^{-1}AX = C \\ Y^{-1}BY = D \end{cases}, \tag{6}$$

for some known values of T, S, A, B, C, D is called the matrix multivariate quadratic (MMQ) problem.

Note, that in the case of our protocol $T = \mathrm{ld}_g Q$,$S = \mathrm{ld}_g E$, $A = Z_1$, $B = A_1$, $C = Z_2$, $D = A_2$.

An example of MPAC protocol is presented in [1]. A minor modification we use in this paper is converting the obtained encryption key K to a bitstring. An example of this transformation is presented below.

Example 1. *Let us assume, that Bob has obtained the following encryption key K*

$$K = \begin{pmatrix} 1 & 2 & 2 \\ 1 & 14 & 14 \\ 14 & 1 & 14 \end{pmatrix}$$

To convert it to a bitstring we consider the string

$$1, 2, 2, 1, 14, 14, 14, 1, 14.$$

We convert each element to binary form to obtain a bitsring

$$000100100010000111101110111000011110,$$

where the first four bits represent an element 1*, next four bits represent an element* 2 *and so on.*

4. Improvements of the Asymmetric Cipher Protocol

Let the parameter n of multiplicative group $\boldsymbol{Z}_n^*$ be a composite integer (factors of this number are irrelevant) and let $\lambda(n)$ be of the form $\lambda(n) = pq$ where p is prime and $\gcd(p, q) = 1$. According to the Sylow theorem [10] the Sylow subgroup of the prime order p exists in $\boldsymbol{Z}_n^*$. We denote this subgroup as $\boldsymbol{\Gamma}_{p,n}$. Since, according to the Lagrange theorem, the order of the element γ has to divide p, the only orders possible in group $\boldsymbol{\Gamma}_{p,n}$ are 1 and p. Therefore, every non-identity element γ is the generator of $\boldsymbol{\Gamma}_{p,n}$. We can use this group to ensure the maximum entropy of the entries of the result matrix E. However,

it can be shown (see Section 5) that using a cyclic group as the platform makes MPF vulnerable to algebraic cryptanalysis. Consequently we have to construct a structure similar to $\boldsymbol{Z}_n^\sharp$.

Let j be an idempotent of semigroup $\boldsymbol{Z}_n$. Since the order of the element is a multiplicative function, we can multiply each element of group $\boldsymbol{\Gamma}_{p,n}$ by j to obtain a new cyclic group $\boldsymbol{J}_{p,n} = j\boldsymbol{\Gamma}_{p,n}$. The identity of this group is j and the order of every non-identity element is p. We construct a semigroup $\boldsymbol{\Gamma}_{p,n}^\sharp$ as a union of $\boldsymbol{\Gamma}_{p,n}$ and $\boldsymbol{J}_{p,n}$ i.e.,

$$\boldsymbol{\Gamma}_{p,n}^\sharp = \boldsymbol{\Gamma}_{p,n} \cup \boldsymbol{J}_{p,n} \tag{7}$$

We can use this semigroup to avoid direct application of a discrete logarithm function to MPF, since $\boldsymbol{J}_{p,n}$ is the ideal of $\boldsymbol{\Gamma}_{p,n}^\sharp$. Note that no additional constraints for parameter n and the entries of Q are needed as compared to $\boldsymbol{Z}_n^\sharp$.

The main advantage of $\boldsymbol{\Gamma}_{p,n}^\sharp$ is the prime order of non-idempotent elements. Since the order of $\boldsymbol{\Gamma}_{p,n}^\sharp$ determines the modulo of entries of matrices of power ring $\boldsymbol{M_R}$, we obtain a power ring defined over the field $\boldsymbol{Z}_p$. Therefore, conjugation constrains

$$XZ_1X^{-1} = A_1, XZ_2X^{-1} = A_2 \tag{8}$$

are defined over the field $\boldsymbol{Z}_p$. Furthermore, this semigroup also provides security against chosen cipertext and chosen plaintext attacks (see Section 5) since entries of matrix exponent are uniformly distributed either in $\boldsymbol{\Gamma}_{p,n}$ or in $\boldsymbol{J}_{p,n}$ depending on the entries of power matrices.

Note, that the set of solutions of the latter equations depends on the canonical Jordan form of matrices Z_1 and Z_2 . More precisely we have to consider Jordan blocks of Jordan matrix J_1 and J_2, which are similar to matrices Z_1 and Z_2 respectively. It was shown in [1], that if a Jordan matrix J is defined over the field $\boldsymbol{Z}_p$ and has the form

$$\begin{pmatrix} \mu & 1 & 0 & \dots & 0 & 0 \\ 0 & \mu & 1 & \dots & 0 & 0 \\ 0 & 0 & \mu & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \mu & 1 \\ 0 & 0 & 0 & \dots & 0 & \mu \end{pmatrix},$$

i.e., it consists of a single Jordan block of size m with eigenvalue μ, then each equation in (8) has exactly $p^{m-1}(p-1)$ solutions.

To construct $\boldsymbol{\Gamma}_{p,n}^\sharp$ we have to consider finding a suitable value of parameter n; and finding an idempotent j in the semigroup $\boldsymbol{Z}_n$.

To find a suitable value of n we can consider all odd square-free integers of the form $n = p_1p_2$, where p_1 and p_2 are primes. It is known from the definition of the Carmichael function $\lambda(\cdot)$, that

$$\lambda(p_1p_2) = \mathrm{lcm}(p_1 - 1, p_2 - 1).$$

According to Sylow theorem, the multiplicative group $\boldsymbol{Z}_n^*$ has a Sylow group of the fixed size p, if p divides $\lambda(p_1p_2)$ and p^2 does not divide $\lambda(p_1p_2)$. To satisfy this condition it is enough to find the value of p_1 such, that

$$p_1 = kp + 1,$$

where k is the least possible even number for p_1 to be prime. To minimize the value of n we can set $p_2 = 3$. The idempotent j can be obtained by solving the following system of congruences:

$$\begin{cases} j \equiv 1 \bmod p_1 \\ j \equiv 0 \bmod 3 \end{cases}.$$

The main parameters of the semigroup $\mathbf{\Gamma}^{\sharp}_{p,n}$ are the following:

- Size of the Sylow group $\mathbf{\Gamma}_{p,n}$ p;
- Parameter n, which defines the multiplicative semigroup $\boldsymbol{Z}_n$;
- The prime factor p_1 of the parameter n;
- Generator of the Sylow group $\mathbf{\Gamma}_{p,n}$ γ;
- Idempotent $j \in \boldsymbol{Z}_n$;

Values of the main parameters of $\mathbf{\Gamma}^{\sharp}_{p,n}$ for a fixed value of p are presented in Table 1.

Table 1. Values of main parameters of $\mathbf{\Gamma}^{\sharp}_{p,n}$.

p	n	p_1	γ	j
5	33	11	4	12
7	87	29	7	30
13	159	53	10	54
17	309	103	13	207
19	573	191	25	192
23	141	47	4	48
29	177	59	4	60
31	933	311	7	312

The newly defined multiplicative semigroup $\mathbf{\Gamma}^{\sharp}_{p,n}$ can be used to define a platform semigroup $\boldsymbol{M_S}$. MPAC protocol is executed as presented in Section 3.

5. Security Analysis

As it was pointed out above, by preventing DLA application to MPAC protocol [1] we are forcing an adversary to deal with the initial MPF system of Equation (2) to break our protocol. Hence the security of the improved version of the MPAC protocol relies on the complexity of the MPF problem, which is defined in the following way:

Definition 2. *The problem of finding matrix powers X and Y, satisfying Equation (1), when Q and E are given, is called an MPF problem.*

In our research we are considering MPF problem with two conjugation constrains, i.e., the following system of matrix equations:

$$\begin{cases} {}^{X}Q^{Y} = E \\ X^{-1}AX = C \\ Y^{-1}BY = D \end{cases}, \tag{9}$$

where matrices Q and E are in a platform semigroup and matrices A, B, C, D are in a power ring. These matrices are publicly known. The only unknown matrices are X and Y.

The NP-hardness of MPF problem in (9) can be proved using the polynomial-time reduction of of known NP-hard problem to MPF problem. In previuos paper [11] author proved that the so-called multivariate quadratic power problem is NP-complete. The reduction is provided using randomly generated MQ problem, which is NP-complete. Referencing to this result and the fact that MMQ problem is conceptually related to MPF problem the NP-completeness of MPF problem can be proved by proving that MMQ problem is NP-complete. Then reduction from MMQ to MPF problem can be constructed automatically referencing to [11].

Unfortunately, the NP-completeness of MMQ problem remains an open question yet. We are making a conjecture, that the MPF problem is at least no less complex than the MMQ problem. Hence avoidance of transformation of MPF equations in protocol, presented here, should increase its

security, since at this time well-known Grobner bases and other algorithms can be applied to try to solve MMQ system of equation and so far we have no knowledge of how to deal with the system of MPF equations. In this case unknowns are also multivariate quadratic monomials, but they are presented in the powers of entries of certain known matrix.

We provide the security considerations by proving that the proposed algorithm is secure against chosen ciphertext attack (CCA) and chosen plaintext attack (CPA). This analysis is performed by considering entropy of entries of matrix exponent E. For this purpose we use generators of some cyclic group $\boldsymbol{G}$. In this case we can estimate the statistical security of MPF using the following known propositions:

Proposition 1. *For any generator g of group $\boldsymbol{G}$ and $\alpha \in \boldsymbol{Z}_{|\boldsymbol{G}|}$ chosen at random, the power term g^{α} has the same distribution in G as α in $\boldsymbol{Z}_{|\boldsymbol{G}|}$ [10].*

Proposition 2. *Let $a \in \boldsymbol{Z}_{|\boldsymbol{G}|}$ be an arbitrary element. Choosing at random $b \in \boldsymbol{Z}_{|\boldsymbol{G}|}$ and setting $c = ab$ gives the same distribution for c as choosing random c [10].*

We can now formulate the following corollary.

Corollary 1. *For any two generators of group G g_1 and g_2 and two uniformly chosen elements $\alpha, \beta \in \boldsymbol{Z}_{|\boldsymbol{G}|}$ the element z, computed by the expression*

$$z = g_1^{\alpha} g_2^{\beta}$$

is uniformly distributed in $\boldsymbol{G}$.

The latter corallary implies that element z as a function of α, β is strongly universal$_2$ as defined by authors in [12] (notation of strongly universal function is taken from the same paper), i.e., g_1^{α} and g_1^{β} are two independent elements uniformly distributed in $\boldsymbol{G}$. This result can also be generalized for any entry of the matrix exponent E in (1), i.e., each entry of this matrix is a strongly universal function. In [13] this property is defined as a perfect m^2-wise decorrelation (as denoted by the author).

The statistical security of MPF in case of $S = \boldsymbol{Z}_n^*$ and $R = \boldsymbol{Z}_{\lambda(n)}$ is also considered in [14]. The parameter n is selected as a composite number of the form $n = 3p$, where $p = 2s + 1$ and both p and s are prime numbers. The main outcome of that paper is the following proposition:

Proposition 3. *If a base matrix $Q \in \boldsymbol{M_G}$ implying power matrices $X, Y \in \boldsymbol{M_R}$ where $R = \boldsymbol{Z}_{|\boldsymbol{G}|}$, and if the entries of power matrices are chosen at random with uniform distribution, then the system (9) yields the matrix E which entries are also uniformly distributed.*

Note also, that the last step of our protocol is similar to the Vernam cipher. According to [13] this cipher has perfect 1-wise decorrelation. Due to Proposition 3 if matrices X and Y are chosen randomly with uniform distribution of their entries then the key matrix K has perfect m^2-wise decorrelation. It was shown in [13], that in this case our cipher is secure against CCA and CPA respectively (Theorem 7).

Corollary 2. *MPAC protocol is CPA and CCA secure.*

However, using a cyclic group $\boldsymbol{G}$ to define a platform semigroup does not provide any security against a specific algebraic attack. This so-called discrete logarithm attack (DLA) is based on a ordinary discrete logarithm function, which can be generalized to matrix semigroups. This generalization is performed as follows:

$$\mathrm{ld}_g Q = P, \quad \text{if} \quad \forall i, j = 1, 2, \ldots, m \quad p_{ij} = \mathrm{ld}_g q_{ij}, \tag{10}$$

where $\mathrm{ld}_g(\cdot)$ is the discrete logarithm function, g is a generator of a semigroup $\boldsymbol{S}$ and Q, P are square $m \times m$ matrices in $\boldsymbol{M_S}$. Note, that we do not consider both ordinary and matrix discrete logarithm problems (DLP) as hard, since we will not use a large semigroup $\boldsymbol{S}$ to define the platform semigroup and hence $\mathrm{ld}_g Q$ can be obtained easily if $\boldsymbol{S} = \boldsymbol{G}$.

The generalized discrete logarithm function can be applied to MPF Equation (1) to obtain

$$\mathrm{ld}_g \left({}^{X}Q^{Y} \right) = X \cdot \left(\mathrm{ld}_g Q \right) \cdot Y = XTY = \mathrm{ld}_g E, \tag{11}$$

where $T = \mathrm{ld}_g Q$.

The way to break the presented asymmetric cipher specification is to solve either system of matrix Equation (9) or an MMQ problem corresponding to an MPF problem with the same conjugation constrains, i.e., the system (6), where all equations are defined in a power ring.

Despite the fact that a MMQ problem is a subclass of well-known multivariate quadratic (MQ) problems, which is NP-complete, the NP-completeness of MMQ problem has thus far not been proved. However, it was shown in [11] that MQ power problem is NP-complete over any semigroup $\boldsymbol{Z}_n$.

Note, that choosing $\boldsymbol{S} = \boldsymbol{Z}_n^*$, where $n = pq$ does not provide security against DLA as well, since Chinese Remainder Theorem (CRT) can be used to define the following mapping:

$$\varphi : \left(g_p^a ; g_q^b \right) \to (a; b), \tag{12}$$

where g_p and g_q are generators of multiplicative cyclic groups $\boldsymbol{Z}_p^*$ and $\boldsymbol{Z}_q^*$ respectively.

The semigroup $\boldsymbol{\Gamma}_{p,n}^{\sharp}$ however does not have this flaw, i.e it cannot be split into two multiplicative cyclic groups and therefore the isomorphism φ cannot be used to define the discrete logarithm. To demonstrate this we present the following example:

Example 2. *Let us consider the multiplicative group* $Z_{33}^* = \{a | gcd(a, 33) = 1\}$. *The isomorphism implied by Chinese reminder theorem is as follows:*

$$\varphi : \boldsymbol{Z}_{33}^* \to \boldsymbol{Z}_3^* \times \boldsymbol{Z}_{11}^*.$$

Let $\boldsymbol{\Gamma}_{5,33}^{\sharp} = \{1, 3, 4, 9, 12, 15, 16, 25, 27, 31\}$. *Evidently this semigroup has no non-trivial isomorphism, which can be used to split this semigroup into a direct product of two or more separate (semi)groups. Therefore, the discrete logarithm function is not defined in* $\boldsymbol{\Gamma}_{5,33}^{\sharp}$.

However semigroup $\boldsymbol{\Gamma}_{p,n}^{\sharp}$ has a non-trivial isomorphism

$$\psi : \boldsymbol{\Gamma}_{p,n} \to \boldsymbol{J}_{p,n}.$$

The latter isomorphism can be used to perform reduction of the initial MPF problem to an MMQ problem. This can be done by defining a mapping

$$\psi' = \begin{cases} a & \text{if} \quad a \in \boldsymbol{\Gamma}_{p,n} \\ \psi^{-1}(a) & \text{if} \quad \boldsymbol{J}_{p,n} \end{cases}$$

and using it on each entry of MPF value matrix E in (1), thus transforming it into an MMQ problem

$$X\psi'(Q)Y = \psi'(E). \tag{13}$$

However, we found that under the certain conditions, the obtained MMQ problem is not equivalent to the initial MPF problem, i.e., solutions X' and Y' of Equation (13) do not satisfy the initial Equation (1). This happens if an entry of base matrix Q, which is chosen from an ideal is raised to zeroth power. In this case not all entries of MPF value matrix E are in the ideal $\boldsymbol{J}_{p,n}$. To demonstrate this we present an example:

Example 3. *Let us consider the multiplicative semigroup* $\boldsymbol{S} = \boldsymbol{\Gamma}^{\sharp}_{5,33}$. *Entries of power matrices X and Y have to be selected from* $\boldsymbol{Z}_5$. *Define matrices Q, X and Y in a following way:*

$$Q = \begin{pmatrix} 4 & 31 & 25 \\ 16 & 4 & 9 \\ 31 & 16 & 25 \end{pmatrix}, X = \begin{pmatrix} 2 & 3 & 4 \\ 1 & 0 & 1 \\ 1 & 2 & 3 \end{pmatrix}, Y = \begin{pmatrix} 3 & 1 & 2 \\ 4 & 1 & 1 \\ 3 & 2 & 2 \end{pmatrix}$$

Then MPF value represented by matrix E is the following:

$$E = \begin{pmatrix} 27 & 9 & 9 \\ 4 & 1 & 25 \\ 27 & 3 & 9 \end{pmatrix}$$

We can see, that entries of the second row are not contained in the ideal $\boldsymbol{J}_{5,33} = \{3, 9, 12, 15, 27\}$ and therefore mapping ψ' is not one-to-one. Therefore the mapping ψ' cannot be used to reduce MPF problem to MMQ problem in general case and hence multiplicative semigroup $\boldsymbol{\Gamma}^{\sharp}_{p,n}$ provides efficient security against DLA attack.

6. Discussion

We presented enhanced Matrix Power Asymmetric Cipher (MPAC) protocol regarding previously published prototype suggested in [1].

We have proved that enhanced MPAC is resistant to Chosen Plaintext Attack and Chosen Ciphertext Attack.

The improved security measures were proposed for preventing DLA based on application of logarithm function directly to MPAC equations and consequently avoiding initial MPF equations transformation to MMQ system of equations. Despite the lack of proof that the complexity of randomly generated MMQ system is NP-complete as it is proved for randomly generated MQ system of equations over any field [15], we are making a conjecture that the complexity of MMQ problem is high.

So far we do not know the methods of the solution of systems defined by initial MPF equations, since they are not custom systems of algebraic equations. It is rather a system of power equations, where unknown variables are the powers of certain elements in the semigroup.

By preventing initial MPF transformation to MMQ problem and referencing to these considerations we are making a conjecture that the proposed MPAC is secure against DLA since discrete logarithm functions cannot be defined for algebraic structures introduced in this paper.

It is determined in [16] that MPAC has significant computation efficiency advantage over other algorithms considered in the paper. Since we improved our protocol in this paper, MPAC can be efficiently applied in the IoT.

Author Contributions: Eligijus Sakalauskas and Aleksejus Mihalkovich conceived and designed the experiments; Aleksejus Mihalkovich and Algimantas Venčkauskas performed the experiments; Eligijus Sakalauskas and Aleksejus Mihalkovich analyzed the data; Algimantas Venčkauskas contributed analysis tools; Aleksejus Mihalkovich wrote the paper.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Sakalauskas, E.; Mihalkovich, A. New asymmetric cipher of non-commuting cryptography class based on matrix power function. *Informatica* **2014**, *25*, 283–298.
2. Sakalauskas, E.; Luksys, K. Matrix power function and its application to block cipher s-box construction. *Int. J. Innov. Comput.* **2012**, *8*, 2655–2664.
3. Sakalauskas, E.; Tvarijonas, P.; Raulynaitis, A. Key agreement protocol (KAP) using conjugacy and discrete logarithm problems in group representation level. *Informatica* **2007**, *18*, 115–124.

4. Luksys, K.; Sakalauskas, E.; Venčkauskas, A. Implementation analysis of matrix power cipher in embedded systems. *Elektron. Elektrotech.* **2012**, *2*, 95–98.
5. Vitkus, P.; Sakalauskas, E.; Listopadskis, N.; Vitkiene, R. Microprocessor realization of key agreement protocol (KAP) based on matrix power function. *Elektron. Elektrotech.* **2012**, *117*, 33–36.
6. Myasnikov, A.; Shpilrain, V.; Ushakov, A. *Group-Based Cryptography*; Birkhäuser Verlag: Basel, Switzerland, 2008.
7. Jacobs, K. A Survey of Modern Mathematical Cryptology. University of Tennessee Honors Thesis Projects: Knoxville, TN, USA; April 2011. Available online: http://trace.tennessee.edu/cgi/viewcontent.cgi?article=2422&context=utk_chanhonoproj (accessed on 5 December 2016).
8. Ottaviani, V.; Zanoni, A.; Regoli, M. Conjugation as Public Key Agreement Protocol in Mobile Cryptography. In Proceedings of the 2010 International Conference on Security and Cryptography, University of Piraeus, Athens, Greece, 26–28 July 2010; pp. 1–6.
9. Sracic, M. Quantum Circuits for Matrix Multiplication. July, 2011. Available online: https://www.math.ksu.edu/reu/sumar/QuantumAlgorithms.pdf (accessed on 5 December 2016).
10. Hall, M. *The Theory of Groups*; Macmillan: New York, NY, USA, 1959.
11. Sakalauskas, E. The multivariate quadratic power problem over Zn is NP-Complete. *Inf. Technol. Control* **2012**, *41*, 33–39.
12. Wegman, M.N.; Carter, J.L. New hash functions and their use in authentication and set equality. *J. Comput. Syst. Sci.* **1981**, *22*, 265–279.
13. Vaudenay, S. Decorrelation: A theory for block cipher security. *J. Cryptol.* **2003**, *16*, 249–286.
14. Sakalauskas, E.; Mihalkovich, A. Candidate One-Way Function Based on Matrix Power Function with Conjugation Constraints. In Proceedings of the Bulgarian Cryptography Days 2012, Sofia, Bulgaria, 20–21 September 2012; pp. 29–37.
15. Patarin, J.; Goubin, L. Trapdoor One-Way Permutations and Multivariate Polynomials. In Proceedings of the First International Conference (ICICS'97), Beijing, China, 11–14 November 1997; pp. 356–368.
16. Mihalkovich, A.; Toldinas, J.; Venčkauskas, A. The Analysis of the Performance of Matrix Power Asymmetric Cipher Protocol. In Proceedings of the GV-Global Virtual Conference, Žilina, Slovakia, 6–10 April 2015; EDIS-Publishing Institution of the University of Žilina: Žilina, Slovakia, 2015; pp. 149–153.