*Applied Mathematics*, 2013, 4, 1043-1049
http://dx.doi.org/10.4236/am.2013.47142 Published Online July 2013 (http://www.scirp.org/journal/am)

# New Practical Algebraic Public-Key Cryptosystem and Some Related Algebraic and Computational Aspects

**S. K. Rososhek**
Faculty of Mathematics and Mechanics, Tomsk State University, Tomsk, Russia
Email: rososhek@list.ru

Received April 26, 2013; revised May 26, 2013; accepted June 6, 2013



## ABSTRACT

The most popular present-day public-key cryptosystems are RSA and ElGamal cryptosystems. Some practical algebraic generalization of the ElGamal cryptosystem is considered-basic modular matrix cryptosystem (BMMC) over the modular matrix ring $M_2(\mathbb{Z}_n)$. An example of computation for an artificially small number $n$ is presented. Some possible attacks on the cryptosystem and mathematical problems, the solution of which are necessary for implementing these attacks, are studied. For a small number $n$, computational time for compromising some present-day public-key cryptosystems such as RSA, ElGamal, and Rabin, is compared with the corresponding time for the BMMC. Finally, some open mathematical and computational problems are formulated.

**Keywords:** Public-Key Cryptosystem; Modular Matrix Ring

## 1. Introduction

Security of some present-day public-key cryptosystems is based on computational complexity of some number-theoretical problems. Two of these problems are used most often: the integer factorization problem and the discrete logarithm problem. These problems ensure the security of the RSA and ElGamal cryptosystems, as well as of the corresponding digital signature schemes [1].

However, the true level of the computational complexity of these problems is unknown. That is to say, they are widely believed to be intractable, although no proof of this fact is known.

In [2], randomized polynomial-time algorithms for computing discrete logarithms and integer factoring were presented for the quantum computer.

Nevertheless, some alternatives should be proposed. One of possible approaches is to replace number-theoretical cryptosystems by such algebraic cryptosystems that would be resistant to an attack on a quantum computer.

Let us now consider some scheme of cryptosystems, namely, cryptosystems of group rings.

In the author's work [3,4], a scheme of group ring cryptosystems was proposed. The idea to apply group rings in cryptography is based on the fact that if we fix the cardinality of a finite ring $R$, the cardinality of the group ring $RG$ for a finite group $G$ is an exponent of the cardinality of the group $G$. Then, a legal user can perform cryptographic transformations separately in the ring $R$ and in the group $G$ using polynomial algorithms and the illegal user has to solve computationally difficult problems in the group ring $RG$.

Let us consider the standardization problem in the group ring and two its aspects. The direct standardization problem is to construct a standard automorphism $\gamma$ of the group ring $RG$ from an automorphism $\alpha$ of the group $G$ and automorphism $\beta$ of the ring $R$ in the following way: if an element $x$ of the group ring $RG$ is represented as a formal linear combination of elements $g_i$ of the group $G$ with coefficients $r_i$ from the ring $R$, then the image of the element $x$ under the action of $\gamma$ is a formal linear combination of images of the elements $g_i$ of the group $G$ under the action of $\alpha$ with coefficients that are images of the coefficients $r_i$ under the action of $\beta$.

The inverse standardization problem is formulated as follows. For a given automorphism $\gamma$ of a group ring $RG$, find an automorphism $\alpha$ of the group $G$ and an automorphism $\beta$ of the ring $R$ such that $\gamma$ can be constructed from $\alpha$ and $\beta$ by the way that was mentioned in the direct standardization problem or prove that such automorphisms $\alpha$ and $\beta$ do not exist.

It is easy to see that, in the case of an efficient specification of the automorphism $\alpha$ in the group $G$ and of the

automorphism $\beta$ in the ring $R$, one can efficiently compute the action of the automorphism $\gamma$ on any element of the group ring $RG$, *i.e.*, efficiently specify the automorphism $\gamma$ of the ring $RG$.

As for the inverse standardization problem, there are some reasons to believe that this problem is computationally difficult. However, there is no proof for this statement.

In [5] some generalization of group ring cryptosystem is considered in the case of quasigroup ring.

The question "For which finite commutative rings $R$ and finite groups $G$ all automorphisms of the group ring $RG$ are standard automorphisms?" was partially answered in [6-8]. It should be noted that an inner automorphism of an integral group ring of a finite group is not a standard automorphism as a rule. This is why, together with the standard automorphisms of the group ring $\mathbb{Z}G$, where $G$ is a finite group, we use inner automorphisms. In [9] the group ring $\mathbb{Z}S_3$, where $S_3$ is the permutation group for three symbols, is represented in a matrix form as block diagonal matrices of the fourth degree with two one-dimensional blocks and one two-dimensional block. In [9,10] it is shown that the unit group of the group ring $\mathbb{Z}S_3$ is a semi-direct product of trivial units $\left(\pm S_3\right)$ and a free subgroup of rank 3. Since matrices of the fourth degree from this subgroup contain two identity one-dimensional blocks, we can restrict ourselves by a free group of matrices of the second degree with the free generators [9]:

$$A=\begin{pmatrix}1 & 0\\ 3 & 1\end{pmatrix}, B=\begin{pmatrix}1 & 3\\ 0 & 1\end{pmatrix}, C=\begin{pmatrix}-2 & 3\\ -3 & 4\end{pmatrix}.$$

If we fall outside the limits of the matrix representation of $\mathbb{Z}S_3$, we consider arbitrary matrices of the second degree from the ring $M_2\left(\mathbb{Z}\right)$ and its unit group $GL_2\left(\mathbb{Z}\right)$, which contains free rank 3 subgroups $G\left(\alpha,\beta,\gamma\right)$ with the free generators

$$A\left(\alpha\right)=\begin{pmatrix}1 & 0\\ \alpha & 1\end{pmatrix}, B\left(\beta\right)=\begin{pmatrix}1 & \beta\\ 0 & 1\end{pmatrix},$$

$$C\left(\gamma\right)=\left(\begin{array}{c|c}1-\gamma & \gamma\\ \hline -\gamma & \gamma+1\end{array}\right),$$

where $\alpha,\beta,\gamma\in\mathbb{Z}$ and $\left|\alpha\right|\geq 3,\left|\beta\right|\geq 3,\left|\gamma\right|\geq 3$ [11]. For example, if $\alpha=\beta=\gamma=3$, we obtain a free rank 3 subgroup $G=G\left(3,3,3\right)$ with the aforesaid free generators $A$, $B$, and $C$.

It should be also noted that all automorphisms of the group ring $\mathbb{Z}S_3$ are inner [12].

New practical algebraic generalization of the ElGamal cryptosystem will be given in the Section 2, some attacks on this cryptosystem—in the Section 4, new hard computational problems—in the Section 5, comparison of the security level of classical RSA, ElGamal and Rabin cryptosystems with security level of this cryptosystem for the same small number—in the Section 7, some related open mathematical and computational problems—in the Section 8. It should be noted, that some other theoretical algebraic generalizations of the ElGamal cryptosystem are given in [13,14].

## 2. Basic Modular Matrix Cryptosystem (BMMC)

### 2.1. Key Generation

User **A** does the following:

1) picks large random positive integer $n$;

2) picks the random words $W\left(X\right)$ and $W\left(U\right)$ in the alphabet $A^{\pm 1},B^{\pm 1},C^{\pm 1}$ in a free rank 3 group with free generators $A$, $B$, and $C$;

3) computes the noncommuting matrices $X_n,U_n$ by replacing the symbols $A$, $B$, and $C$ in the words $W\left(X\right)$ and $W\left(U\right)$ by the corresponding matrices

$$A=\begin{pmatrix}1 & 0\\ 3 & 1\end{pmatrix}, B=\begin{pmatrix}1 & 3\\ 0 & 1\end{pmatrix}, C=\begin{pmatrix}-2 & 3\\ -3 & 4\end{pmatrix}$$

and performing matrix computations modulo $n$, *i.e.*,

$$X_n=X\left(\mathrm{mod}\, n\right), U_n=U\left(\mathrm{mod}\, n\right);$$

If $X_n$ and $U_n$ commute, then return to 2);

4) let $f\left(n\right)$ be the cardinality of the group $GL_2\left(\mathbb{Z}_n\right)$ over $\mathbb{Z}_n$-residue ring modulo $n$, then user **A** picks the random integers

$$-f\left(n\right)<k<f\left(n\right), -f\left(n\right)<s<f\left(n\right), 1<\ell<f\left(n\right);$$

5) public key of user **A** is

$$\left(n,P_1,P_2,P_3\right)=\left(n,X_n,U_n^{-s}X_n^kU_n^s,U_n^\ell\right)$$

and its private key is

$$\left(U_n,s,k\right).$$

Remark 1. Orders of matrices

$$A=\begin{pmatrix}1 & 0\\ 3 & 1\end{pmatrix}, B=\begin{pmatrix}1 & 3\\ 0 & 1\end{pmatrix}$$

in the group $GL_2\left(\mathbb{Z}_n\right)$ are equal to $n$;

Remark 2. The cardinality of the group $GL_2\left(\mathbb{Z}_n\right)$ in the case $n=p^i$, $p$ is a prime number, $i$ is a positive integer, is equals to

$$f\left(p^i\right)=\left|GL_2\left(\mathbb{Z}_{p^i}\right)\right|=p^{4i-3}\left(p^2-1\right)\left(p-1\right)\ \text{[15].}$$

As consequence in the case $n=pq,p,q$ are primes, we have

$$f\left(pq\right)=\left|GL_2\left(\mathbb{Z}_{pq}\right)\right|$$
$$=p\left(p^2-1\right)\left(p-1\right)q\left(q^2-1\right)\left(q-1\right).$$

 

### 2.2. Encryption

User **B** does the following:

1) writes the plaintext as a sequence of $N$ numbers from $\mathbb{Z}_n$, where $N$ is a multiple of 4, $\ell_1, \ell_2, \cdots, \ell_N$, adding, if necessary, numbers from the first quadruple by a cyclic permutation at the end of the sequence;

2) writes each quadruple of numbers of the obtained sequence similarly as matrix:

$$m^{(1)} = \begin{pmatrix} \ell_1 & \ell_2 \\ \ell_3 & \ell_4 \end{pmatrix} \in M_2(\mathbb{Z}_n);$$

3) picks session keys-random integers $r_i, t_i, -f(n) < r_i < f(n), -f(n) < t_i < f(n)$ for each of $N/4$ obtained matrices $m^{(i)}$;

4) computes the ciphertext block for each matrix $m^{(i)}$:

$$\left(C_1^{(i)}, C_2^{(i)}\right) = \left(P_3^{-r_i} P_1^{t_i} P_3^{r_i}, m^{(i)} P_3^{-r_i} P_2^{-t_i} P_3^{r_i}\right),$$
$$i = 1, 2, \cdots, N/4.$$

### 2.3. Decryption

Using the private key, user **A** computes for each ciphertext block $\left(C_1^{(i)}, C_2^{(i)}\right)$:

$$C_2^{(i)} U_n^{-s} \left(C_1^{(i)}\right)^k U_n^s = m^{(i)}.$$

After obtaining the sequence of matrices

$$m^{(1)}, m^{(2)}, \cdots, m^{(N/4)},$$

the sequence of numbers $\ell_1, \ell_2, \cdots, \ell_N$ and hence the plaintext can be reconstructed uniquely.

Theorem. Decryption in the BMMC is correct.

*Proof*. It is sufficiently to consider a case of one block of the ciphertext:

$$\begin{aligned} & C_2 U_n^{-s} C_1^k U_n^s \\ &= \left(m P_3^{-r} P_2^{-t} P_3^r\right) U_n^{-s} \left(P_3^{-r} P_1^t P_3^r\right)^k U_n^s \\ &= m P_3^{-r} P_2^{-t} P_3^r U_n^{-s} P_3^{-r} P_1^{kt} P_3^r U_n^s \\ &= m U_n^{-r\ell} U_n^{-s} X_n^{-kt} U_n^s U_n^{r\ell} U_n^{-s} U_n^{-r\ell} X_n^{kt} U_n^{r\ell} U_n^s \\ &= m\left(U_n^{-r\ell-s} X_n^{-kt} U_n^0 X_n^{kt} U_n^{r\ell+s}\right) \\ &= m\left(U_n^{-r\ell-s} U_n^{r\ell+s}\right) = m. \end{aligned}$$

It should be noted that algorithms of the BMMC are implemented using the algorithm of matrix modular exponentiation similar to the usual modular exponentiation algorithm in which multiplication of integers is replaced by multiplication of matrices with reduction of their elements modulo $n$. In addition parallel computations may be used in matrix multiplications to increase the computational efficiency of the cryptosystem.

Let $n$ be a large 256 bit integer, then the cardinality bit length of the group $GL_2(\mathbb{Z}_n)$ would be near 800 bits or more. For comparing in the case of the ElGamal cryptosystem the bit lengths of p and the cardinality of corresponding multiplicative group of residue field $\mathbb{Z}_p$ are equal. But one reduction modulo 1024 bit number in the ElGamal cryptosystem costs as some reductions modulo 256 bit number in the BMMC. Therefore, under corresponding choice of parameters the BMMC may be faster than the ElGamal cryptosystem with the same security level, because the gybrid problem and the transformation problem are harder than the discrete logarithm problem in the groups of the same cardinality.

## 3. Example

### 3.1. Key Generation

User **A** does the following:

1) picks two prime numbers $p = 17$ and $q = 19$ and computes $n = 17 \times 19 = 323$;

2) picks the words in the free group:

$$W(U) = C^{-4} A^3 B, W(X) = B^{-1} C;$$

3) computes matrices modulo $n$:

$$\begin{aligned} U_n &= U \pmod n \\ &= \left[\left(\begin{array}{c|c} 321 & 3 \\ \hline 320 & 4 \end{array}\right)^{-4} \left(\begin{array}{c|c} 1 & 0 \\ \hline 3 & 1 \end{array}\right)^3 \left(\begin{array}{c|c} 1 & 3 \\ \hline 0 & 1 \end{array}\right)\right] (\mathrm{mod}\, 323) \\ &= \left(\begin{array}{c|c} 228 & 26 \\ \hline 236 & 51 \end{array}\right), \end{aligned}$$

$$\begin{aligned} X_n &= X \pmod n \\ &= \left[\left(\begin{array}{c|c} 1 & 3 \\ \hline 0 & 1 \end{array}\right)^{-1} \left(\begin{array}{c|c} 321 & 3 \\ \hline 320 & 4 \end{array}\right)\right] (\mathrm{mod}\, 323) \\ &= \left(\begin{array}{c|c} 7 & 314 \\ \hline 320 & 4 \end{array}\right); \end{aligned}$$

matrices $U_n$ and $X_n$ do not commute and, therefore, the user passes to the next step;

4) picks the integers $k = s = 1, \ell = 2$;

5) the public key is

$$\begin{aligned} & (n, P_1, P_2, P_3) \\ &= \left(n = 323, \left(\begin{array}{c|c} 7 & 314 \\ \hline 320 & 4 \end{array}\right), \left(\begin{array}{c|c} 227 & 39 \\ \hline 101 & 107 \end{array}\right), \left(\begin{array}{c|c} 303 & 148 \\ \hline 275 & 16 \end{array}\right)\right); \end{aligned}$$

the private key is $\left(\left(\begin{array}{c|c} 228 & 26 \\ \hline 236 & 51 \end{array}\right), k = s = 1\right)$.

### 3.2. Encryption

User **B** does the following:

 

1) writes the plaintext as a sequence of numbers from $\mathbb{Z}_n$. The length of this sequence is multiple of 4. If necessary, some numbers are added. For example, let the plaintext be

$$4\|5\|7\|8\|17\|15\|10\|;$$

here, a number should be added to the last block by shifting the first number cyclically, the user obtains two quadruples of numbers from $\mathbb{Z}_n$:

$$4\|5\|7\|8,17\|15\|10\|4;$$

2) writes the plaintext as two matrices from $M_2(\mathbb{Z}_n)$:

$$m^{(1)} = \left(\begin{array}{c|c} 4 & 5 \\ \hline 7 & 8 \end{array}\right), m^{(2)} = \left(\begin{array}{c|c} 17 & 15 \\ \hline 10 & 4 \end{array}\right);$$

3) encrypts each block (matrix) separately choosing different session keys. For example, the first block is encrypted as follows;

4) picks the session key for the first block $r_1 = 2$, $t_1 = 1$;

5) computes the ciphertext of the first block modulo $n = 323$:

$$C_1^{(1)} = P_3^{-2} P_1 P_3^2 \bmod n = \left(\begin{array}{c|c} 303 & 148 \\ \hline 275 & 16 \end{array}\right)^{-2} \left(\begin{array}{c|c} 7 & 314 \\ \hline 320 & 4 \end{array}\right) \left(\begin{array}{c|c} 303 & 148 \\ \hline 275 & 16 \end{array}\right)^2 (\bmod n) = \left(\begin{array}{c|c} 220 & 245 \\ \hline 105 & 114 \end{array}\right)$$

$$C_2^{(1)} = m^{(1)} \cdot P_3^{-2} P_2^{-1} P_3^2 = \left(\begin{array}{c|c} 4 & 5 \\ \hline 7 & 8 \end{array}\right) \left(\begin{array}{c|c} 303 & 148 \\ \hline 275 & 16 \end{array}\right)^{-2} \left(\begin{array}{c|c} 107 & 284 \\ \hline 202 & 227 \end{array}\right) \left(\begin{array}{c|c} 303 & 148 \\ \hline 275 & 16 \end{array}\right)^2 (\bmod n) = \left(\begin{array}{c|c} 217 & 206 \\ \hline 205 & 13 \end{array}\right).$$

The ciphertext of the second block $m^{(2)}$ is computed similarly with the choice of another session key $r_2, t_2$.

### 3.3. Decryption

User **A**, having obtained the ciphertext from user **B**, does the following: using its private key, for each *i*th block, computes

$$C_2^{(i)} U_n^{-1} C_1^{(i)} U_n;$$

in particular, for the first block, he obtains

$$C_2^{(1)} U_n^{-1} C_1^{(1)} U_n = \left[\left(\begin{array}{c|c} 217 & 206 \\ \hline 205 & 13 \end{array}\right)\left(\begin{array}{c|c} 51 & 297 \\ \hline 87 & 228 \end{array}\right)\left(\begin{array}{c|c} 220 & 245 \\ \hline 105 & 114 \end{array}\right)\left(\begin{array}{c|c} 228 & 26 \\ \hline 236 & 51 \end{array}\right)\right] \bmod n$$

$$= \left(\begin{array}{c|c} 217 & 206 \\ \hline 205 & 13 \end{array}\right)\left(\begin{array}{c|c} 248 & 97 \\ \hline 90 & 86 \end{array}\right) \bmod n = \left(\begin{array}{c|c} 4 & 5 \\ \hline 7 & 8 \end{array}\right) = m^{(1)}.$$

## 4. Some Attacks on BMMC

### 4.1. Find the Private Key $(U_n, s, k)$ by the Public Key $(n, P_1, P_2, P_3)$

1) Let the cardinality of the group $GL_2(\mathbb{Z}_n)$ be

$$\left|GL_2(\mathbb{Z}_n)\right| = f(n);$$

Since $P_3 = U_n^{\ell}$, the cryptanalyst can try to solve the equation with two unknowns *Y* and *x*:

$$Y^x = P_3,$$

where $Y, P_3 \in GL_2(\mathbb{Z}_n), -f(n) < x < f(n)$.

2) Since

$$P_2 = U_n^{-s} P_1^k U_n^s,$$

the cryptanalyst can try to solve the equation with two unknowns *Z* and *x*:

$$Z P_2 Z^{-1} = P_1^x,$$

where $Z \in GL_2(\mathbb{Z}_n), -f(n) < x < f(n)$, what leads to the private key by applying 1) to each solution $\mathbb{Z}_0$ (which we call the transforming matrix).

### 4.2. Find the Private Key $(U_n, s, k)$ by the Ciphertext $(C_1, C_2)$

Since the private key is applied in the ciphertext $(C_1, C_2)$ not directly but only via the public key, the knowing of only the ciphertext does not yield additional possibilities to the attacks from 4.1 for the attack on the private key.

### 4.3. Find the Session Key $(r, t)$ by the Ciphertext $(C_1, C_2)$

1) Since $C_1 = P_3^{-r} P_1^t P_3^r$, the cryptanalyst can try to solve the equation with two unknowns *Z* and *y*:

$$Z C_1 Z^{-1} = P_1^y,$$

where $Z \in GL_2(\mathbb{Z}_n), -f(n) < y < f(n)$.

2) For any solution $(Z_0, y_0)$ of the equation from 1), the cryptanalyst can try to solve the equation with two unknowns *Y* and *x*:

 

$$Y^x = Z_0,$$

where $Y, Z_0 \in GL_2(\mathbb{Z}_n), -f(n) < x < f(n)$

### 4.4. Find the Corresponding Plaintext *m* or the Session Key $(r,t)$ by a Chosen Ciphertext $(C_1,C_2)$

Cryptanalyst chooses the random $\tilde{m} \in GL_2(\mathbb{Z}_n)$ and computes $\tilde{m}C_2$, then send it to user **A** for decryption. User **A** computes:

$$(\tilde{m}C_2)U_n^{-s}C_1^{-k}U_n^s = \tilde{m}(C_2U_n^{-s}C_1^{-k}U_n^s) = \tilde{m}m.$$

and send the result to cryptanalyst, which computes the plaintext:

$$\tilde{m}^{-1}(\tilde{m}m) = m.$$

Hence for protecting cryptosystem the modification of encryption algorithm is:

$$C_2P_3^{-r}P_2^{-t}P_3^r mP_3^{-r}P_2^{-t}P_3^r,$$

the modification of decryption algorithm is:

$$U_n^{-s}C_1^kU_n^sC_2U_n^{-s}C_1^kU_n^s = m.$$

## 5. Computational Problems in Ensuring BMMC Security

From the consideration of attacks 4.1-4.4 one can formulate some problems, the solution of which is necessary to implement the corresponding attacks.

### 5.1. The Transformation Problem

Let a matrix $P_2$ be conjugated with an unknown integral power of a matrix $P_1$ for two given matrices $P_1, P_2 \in GL_2(\mathbb{Z}_n)$. Find all solutions of the equation with two unknowns *Z* and *y*:

$$ZP_2Z^{-1} = P_1^y,$$

where $Z \in GL_2(\mathbb{Z}_n), -f(n) < y < f(n)$.

Let us consider a particular case of Problem 5.1.

1) The conjugation problem.

For two given conjugated matrices $P_2$ and $P_1^{y_0}$ from the group $GL_2(\mathbb{Z}_n)$, find a transforming matrix $T \in GL_2(\mathbb{Z}_n)$, *i.e.*, matrix *T* such that

$$T^{-1}P_2T = P_1^{y_0}.$$

### 5.2. The Hybrid Problem

Find all solutions of the equation with two unknowns *Y* and *x*

$$Y^x = Z_0,$$

where $Y, Z_0 \in GL_2(\mathbb{Z}_n), -f(n) < x < f(n)$ in the group $GL_2(\mathbb{Z}_n)$.

Let us also consider two particular cases of Problem 5.2.

1) The discrete logarithm problem in a cyclic subgroup of the group $GL_2(\mathbb{Z}_n)$.

Let $H = \langle Y_0 \rangle$ be a fixed cyclic subgroup of order *j* of the group $GL_2(\mathbb{Z}_n)$ with the generator $Y_0$, $M \in H$ be an arbitrary element. Find the unique solution $x = x_0$ of the equation

$$Y_0^x = M,$$

where *x* is an integer such that $0 \le x < j$.

2) The problem of extracting a root of the *i*th power in the group $GL_2(\mathbb{Z}_n)$ (the matrix RSA problem).

Let $M \in GL_2(\mathbb{Z}_n)$ be an arbitrary element, $i_0$ be a fixed integer satisfying the condition $0 \le i_0 < f(n)$ and $GCD(i_0, f(n)) = 1$.

Find all solutions of the equation with a single unknown *Y*:

$Y^{i_0} = M, Y \in GL_2(\mathbb{Z}_n)$.

According to the Problem 2), in turn, one can also discern the following problem.

The problem of square-root extraction in $GL_2(\mathbb{Z}_n)$.

Find all solutions of the equation with a single unknown *Y*:

$$Y^2 = M,$$

where $Y, M \in GL_2(\mathbb{Z}_n)$.

## 6. Computational Complexity of Problems 5.1, 5.2

If the order $O(P_1) = O(P_2) = j$ is a large number, then, the fact that the generators in a cyclic group are indistinguishable and random choice of *k* in the key generation show, on the one hand, that the identification of matrices $P_1^y$ in Problem 5.1 is a hard problem and, on the other hand, the impossibility to implement the exhausting search in practice for a large number *j*.

Considering Problem 5.1 1), it should be noted that this problem is solvable in the free subgroup $G = G(3,3,3)$ of the group $GL_2(\mathbb{Z})$ (see [16]). The possibility to extend this algorithm for a subgroup of the group $GL_2(\mathbb{Z}_n)$ depends on the solution of the following problem: for a given matrix $X_n \in G_n \subset GL_2(\mathbb{Z}_n)$, find the word $W(X)$ and matrix $X \in G$ whose reduction modulo *n* yields the matrix $X_n$.

Nevertheless, even in the case of a solved problem of extension, the problem about the existence of an efficient algorithm for solving Problem 5.1 1) remains open.

Let us now consider Problem 5.2. As it is a problem with two unknowns, this problem is more complicated in the general case than its particular cases, the discrete logarithm problem and the problem of extracting a matrix root modulo *n*. It is worth to note that the square-root extracting problem is computationally difficult for large

 

number $n = pq$, $p$ and $q$ are primes.

Let us now turn to the discussion of the cardinality of the set of secret keys for BMMC. Note that, for classical cryptosystems, the uniqueness of the secret key can be reached by fitting of parameters. For BMMC, the situation is other. Indeed, if a matrix $T_0$ transforms the matrix $P_1^i$ into the matrix $P_2$, *i.e.*,

$$T_0^{-1} P_1^i T_0 = P_2,$$

then the matrix $Z_0 T_0$ also transforms $P_1^i$ into $P_2$ for any matrix $Z_0 \in C(P_1)$, where $C(P_1)$ is a centralizer of $P_1$ in $GL_2(\mathbb{Z}_n)$, because

$$\left(T_0^{-1} Z_0^{-1}\right) P_1^i \left(Z_0 T_0\right) = T_0^{-1}\left(Z_0^{-1} Z_0\right) P_1^i T_0 = T_0^{-1} P_0^i T_0 = P_2.$$

Thus, if the secret key $(U_n, s, k)$ is considered as initial, the cryptanalyst can compromise the BMMC by any real key of the form $\left(Z_0 U_n^s, k\right)$, where $Z_0 \in C(P_1)$. Then, for the cardinality of the set of real keys $W_0$, we have

$$W_0 \geq \left|C(P_1)\right|$$

and when generating a key it is necessary to choose matrix $P_1$ so that

$$W_1 = \frac{W_0}{\left|GL_2(\mathbb{Z}_n)\right|}$$

was negligibly small, e.g.,

$$W_1 < 2^{-80}.$$

This protects from random guessing of the private key.

## 7. Comparison of Computational Security of Classical RSA, ElGamal, and Rabin Cryptosystems with BMMC

For demonstrativeness, we compare the cryptosystems for a very small number $n = 35$.

### 7.1. RSA Cryptosystem

Let the public key be $(n = 35, e = 19)$.

In this case, the cryptanalyst instantaneously compromises RSA by factorization $n = 35 = 5 \times 7$, from which finds $\varphi(n) = 4 \times 6 = 24$, and computation of the secret key $d = \mathrm{e}^{-1} \left(\mathrm{mod}\, \varphi(n)\right)$ either by the extended Euclid's algorithm or by exhaustive search. Then the cryptanalyst finds the secret key:

$$d = 19^{-1} \left(\mathrm{mod}\, 24\right) = 19.$$

### 7.2. Modified ElGamal Cryptosystem

In the unit group $\mathbb{Z}_{35}^*$ of the ring $\mathbb{Z}_{35}$ one has to choose an element of the maximal order. For this purpose, $n = 35$ is factorized as $35 = 5 \times 7$, and the generators are chosen in the groups $\mathbb{Z}_5^*$ and $\mathbb{Z}_7^*$, e.g.,

$$\mathbb{Z}_5^* = \langle 2 \rangle \text{ and } \mathbb{Z}_7^* = \langle 3 \rangle.$$

Then the element of maximal order in $\mathbb{Z}_{35}^*$ is obtained from the solution of the following simultaneous congruences either by inspection or by the Chinese reminder theorem:

$$\begin{cases} x \equiv 2 \left(\mathrm{mod}\, 5\right), \\ x \equiv 3 \left(\mathrm{mod}\, 7\right). \end{cases}$$

It follows that $x = 17$ and its order is $0(17) = 12$.

Let one of cyclic subgroups of order 12, for example, $G = \langle 17 \rangle$ be chosen in the group $\mathbb{Z}_{35}^*$. In the group $G$, another generator may be chosen, e.g., $G = \langle 3 \rangle$.

Let the modified ElGamal cryptosystem be considered in a cyclic group $G$ of order 12 with a generator $\alpha = 3$ and let the public key be

$$\left(n = 35, \alpha = 3, \beta = \alpha^a \bmod 35 = 33\right).$$

In this case, the cryptanalyst instantaneously compromises the modified ElGamal cryptosystem using exhaustive search in the cyclic group of order 12 finding the secret key $a = 5$ since $3^5 \left(\mathrm{mod}\, 35\right) = 33$.

Remark. In the case of choice $n$ as $n = p$, where $p$ is a prime number, we compare BMMC with classical ElGamal cryptosystem.

### 7.3. Rabin Cryptosystem

Let the public key be $(n = 35)$, then the cryptanalyst instantaneously compromises the Rabin cryptosystem in this case by factorizing the number by prime multipliers $n = 5 \times 7$.

One can see that, in all three cases, the cryptanalyst instantaneously compromises these classical cryptosystems for $n = 35$. Let us now the case of the BMMC cryptosystem for $n = 35$.

### 7.4. BMMC

Let the public key be

$$\left(n = 35, P_1 = \left(\begin{array}{c|c} 23 & 33 \\ \hline 12 & 34 \end{array}\right), P_2 = \left(\begin{array}{c|c} 31 & 0 \\ \hline 31 & 26 \end{array}\right), P_3 = \left(\begin{array}{c|c} 31 & 5 \\ \hline 15 & 16 \end{array}\right)\right),$$

$$(C_1, C_2) = \left(\left(\begin{array}{c|c} 14 & 12 \\ \hline 18 & 8 \end{array}\right), \left(\begin{array}{c|c} 5 & 18 \\ \hline 30 & 18 \end{array}\right)\right)$$

be the ciphertext of a certain matrix $m$.

Compromising BMMC in this case needs essentially more efforts than for the classical cryptosystems and exhausting search in the space of the search containing 775,760 matrices gives $m = \left(\begin{array}{c|c} 7 & 8 \\ \hline 2 & 3 \end{array}\right)$; secret key—

 

$U_n = \left(\begin{array}{c|c} 33 & 32 \\ \hline 26 & 21 \end{array}\right), k = 17, s = 5, \ell = 3$ ; session key— $r = 1$, $t = -1$.

## 8. Some Open Mathematical and Computational Problems

1) For which finite groups $G$ and rings $R$ the unit group of group ring $RG$ is a semi-direct product of trivial units and a free subgroup of a finite rank?

2) For which groups $G$ and rings $R$ every automorphism of the group ring $RG$ has a standard form?

3) For which subgroups of the group $GL_2(\mathbb{Z}_n)$ it takes place the property of small centralizers *i.e.* every element has a cyclic centralizer?

Remark. It is well-known [16] that in the free group of finite rank centralizer of any element is a cyclic subgroup.

4) Is there a polynomial-time algorithm for constructing cyclic centralizer of any element in a free group of finite rank?

5) Is there a polynomial-time algorithm for solving the membership problem for cyclic subgroup of the a) free group of finite rank, b) subgroup $G = G(3,3,3)$ by modulo $n$ in a group $GL_2(\mathbb{Z}_n)$?

6) Is there a polynomial-time algorithm for solving the modular factorization problem, *i.e.* to represent every matrix from the subgroup $G = G(3,3,3)$ by modulo $n$ in a group $GL_2(\mathbb{Z}_n)$ as a word in an alphabet of $A^{\pm 1}, B^{\pm 1}, C^{\pm 1}$ by modulo $n$?

7) How to compute the number $f(n)$ for arbitrary positive integers $n$? More exactly, is there a polynomial-time algorithm for computing $f(n)$?

8) Is there a polynomial-time algorithm for computing maximal order elements in a subgroup $G = G(3,3,3)$ by modulo $n$ in the group $GL_2(\mathbb{Z}_n)$? What is a cardinality of this subgroup $G_n$?

## 9. Conclusion

The practicality of the BMMC is provided by the absence of the necessity in the computer algebra systems used for computer realization of cryptosystem algorithms and efficient matrix computations by modulo number of essentially less bit length than that are usually used in classical cryptosystems under the same security level.

## REFERENCES


[1] A. Menezes, P. van Ooshot and S. Vanstone, "Handbook of Applied Cryptography," CRC Press, Waterloo, 1996. doi:10.1201/9781439821916

[2] P. W. Shor, "Algorithms for Quantum Computation: Discrete Logarithm and Factoring," *Proceedings of the IEEE 35th Communications Annual Symposium on Foundations of Computer Science*, Santa Fe, 20-22 November 1994, pp. 124-134.

[3] S. K. Rososhek, "Cryptosystems in Automorphism Groups of Group Rings of Abelian Groups," *Fundamentalnaya I prikladnaya matematica*, Vol. 13, No. 8, 2007, pp. 157-164 (in Russian).

[4] S. K. Rososhek, "Cryptosystems in Automorphism Groups of Group Rings of Abelian Groups," *Journal of Mathematical Sciences*, Vol. 154, No. 3, 2008, pp. 386-391. doi:10.1007/s10958-008-9168-2

[5] A. N. Gribov, P. A. Zolotykh and A. V. Mikhalev, "A Construction of Algebraic Cryptosystem over the Quasigroup Ring," *Mathematical Aspects of Cryptography*, Vol. 1, No. 4, 2010, pp. 23-32 (in Russian).

[6] K. N. Ponomarev, "Automorphically Rigid Group Algebras I. Semisimple Algebras," *Algebra and Logic*, Vol. 48, No. 5, 2009, pp. 654-674. doi:10.1007/s10469-009-9064-y

[7] K. N. Ponomarev, "Automorphically Rigid Group Algebras II. Modular Algebras," *Algebra and Logic*, Vol. 49, No. 2, 2010, pp. 216-237.

[8] K. N. Ponomarev, "Rigid Group Rings," In: A. G. Pinus and K. N. Ponomarev, Eds., *Algebra and Model Theory*, 6, Novosobirsk Technical University Press, Novosibirsk, 2007, pp. 73-83 (in Russian). doi:10.1007/s10469-010-9086-5

[9] A. Popova and E. Poroshenko, "Units Group of Integral Group Rings of Finite Groups," In: A. G. Pinus and K. N. Ponomarev, Eds., *Algebra and Model Theory*, 4, Novosibirsk Technical University Press, Novosibirsk, 2003, pp. 99-106 (in Russian).

[10] A. Dooms and E. Jespers, "Normal Complements of the Trivial Units in the Unit Group of Some Integral Group Rings," *Communications in Algebra*, Vol. 31, No. 1, 2003, pp. 475-482. doi:10.1081/AGB-120016770

[11] Y. I. Merzlyakov, "Matrix Representations of Free Groups," *Doklady Akademii Nauk*, Vol. 238, No. 3, 1978, pp. 527-533 (in Russian).

[12] A. Popova, "Group of Automorphisms of the Ring $\mathbb{Z}S_3$," In: A. G. Pinus and K. N. Ponomarev, Eds., *Algebra and Model Theory*, 6, Novosibirsk Technical University Press, Novosibirsk, 2007, pp. 84-90 (in Russian).

[13] A. Mahalanobis, "A Simple Generalization of the ElGamal Cryptosystem to Non-Abelian Groups," *Communications in Algebra*, Vol. 36, No. 10, 2008, pp. 3878-3889. doi:10.1080/00927870802160883

[14] S.-H. Paeng, K.-C. Ha, J. N. Kim, S. Chee and C. Park, "New Public Key Cryptosystem Using Finite Non-Abelian Groups," *Proceedings of the Crypto* 2001, *Lecture Notes in Computer Sciences*, Santa Barbara, 19-23 August 2001, pp. 470-485.

[15] M. I. Kargapolov and Y. I. Merzlyakov, "Foundations of Group Theory," Nauka, Moscow, 1977 (in Russian).

[16] R. C. Lyndon and P. E. Schupp, "Combinatorial Group Theory," Springer-Verlag, Berlin, Heidelberg, New York, 1977.


 