Liet. mat. rink. LMD darbai, **50**, 2009, 218–223

Asymmetric cipher protocol using conjugacy and discrete logarithm problem

Andrius RAULYNAITIS[1], Agnė VENCLOVIENĖ[2]

[1] Kaunas University of Technology, Institute of Defense Technologies
Kęstučio 27, LT-44312 Kaunas, Lithuania

[2] Communication and Information System Service under MoD
Šv. Ignoto 8/29, LT-01120 Vilnius, Lithuania

e-mail: andrius.raulynaitis@stud.ktu.lt; agne.vencloviene@gmail.com

Abstract. The paper proposes asymmetric cipher protocol based on matrix field over some field $\mathcal{F}$. The asymmetric cipher is based on two simultaneous problems: matrix conjugator search problem (MCSP) and matrix discrete logarithm problem (MDLP). The algorithm construction does not allow performing a crypto-analysis by replacing the existing MCSP solution to the matrix decomposition problem (MDP) solution. The security parameters are defined and preliminary security analysis is presented.

Keywords: asymmetric cipher, conjugator search problem, discrete logarithm problem, one-way function.

Introduction

The asymmetric cipher constructing must be based on certain one-way function. According to the general definition, OWF is a function, when computing its value for any argument is easy, but its inversion is not, i.e., this problem is intractable. Hence, the security of asymmetric cipher relies on the complexity of OWF inversion.

The security of classical asymmetric cipher protocols such as RSA, El Gamal, etc. relies on the complexity of OWFs based on the number theoretical approach. But after the significant breakthrough by P. Shor of ATT Research Labs in the field of quantum computing the situation have changed essentially. The quantum algorithms can factor integers and find discrete logarithms in probabilistic polynomial time. So the security of classical asymmetric cryptosystems may have a serious security threat in near future. Hence the there is a need of other approaches in construction of asymmetric cryptosystems to withstand the new challenge of quantum computing.

New ideas in public key cryptography using hard problems in infinite non-commutative groups and semigroups appeared in [6]. One realization of these ideas appeared in [1], using the braid group as a platform. The security of this cryptosystem was based on conjugator search problem. But according to [5], this approach is not sufficient and necessary to achieve the proper security.

The other approach to use non-commutative infinite group (e.g., braid group) representation was also used for the other kind of one way functions construction as a background of both digital signature scheme and key agreement protocol [3,4]. Construction of new asymmetric cipher using decomposition (double coset) problem in matrix semiring $\mathcal{M}$ over semiring $\mathcal{N}$ of natural numbers is presented in [2].

We proposed the idea to use two simultaneous problems for the one way function construction, presented in [4], to construct the asymmetric cipher. The idea is to use matrix group conjugacy problem together with matrix discrete logarithm problem. We will make a conjecture supported by our analysis, that these two simultaneous problems are intractable and hence proposed function is a good candidate to be an OWF.

In this paper we analyze security aspects of CSP and DLP in matrix field over some finite field. The construction of asymmetric cipher protocol with a brief mathematical background is presented in Section 2. Section 3 provides considerations on the preliminary security analysis. The main conclusions about the security analysis of proposed algorithms are outlined in Section 4.

1. Asymmetric cipher protocol

We will use the previously proposed idea to use two simultaneous problems for the key agreement protocol [4] for asymmetric cipher construction. For this we use the following algebraic structures:

- the matrix ring $\mathcal{M}$ consisting of m x m dimensional matrices over the finite field $\mathcal{Z}_q = \{0, 1, \dots, q-1\}$, where q is prime number;
- the set $\mathcal{P} = \{p_i(\,)\}$ of all polynomials over $\mathcal{Z}_q$;
- the subset $\mathcal{M}_L$ of mutually commutating m-dimensional matrices. Then for all matrices $M_{L1}, M_{L2}, \in \mathcal{M}_L$:

$$M_{L1} \cdot M_{L2} = M_{L2} \cdot M_{L1}.$$

Let these matrices have the following form:

$$M_{L1} = \begin{pmatrix} L_1 & \Theta \\ \Theta & g_1 I \end{pmatrix}, \qquad M_{L2} = \begin{pmatrix} g_2 I & \Theta \\ \Theta & L_2 \end{pmatrix},$$

where Θ is $m/2$-dimensional zero matrix; L_1 and L_2 are $m/2$ - dimensional square matrices over $\mathcal{Z}_q$; I is $m/2$-dimensional identity matrix; g_1 and g_2 are the numbers in $\mathcal{Z}_q$.

By having matrices M_{L1} and M_{L2} and some polynomials p_{X1}, p_{X2} we calculate secret matrix X in the following way:

$$\begin{aligned} X &= p_{X1}(M_{L1}) \cdot p_{X2}(M_{L2}) \\ &= \left(a_{10}I + a_{11}M_{L1}^1 + \cdots + a_{1n}M_{L1}^n\right) \cdot \left(a_{20}I + a_{21}M_{L2}^1 + \cdots + a_{2n}M_{L2}^n\right), \end{aligned} \quad (1)$$

where polynomials p_{X1}, $p_{X2} \in \mathcal{P}$ are secret and chosen at random, i.e., coefficients of polynomial are secret and randomly generated. The main condition for matrix X is that there must exist inverse matrix X^{-1}. Then there must exist $p_{X1}(\,)^{-1}$, $p_{X2}(\,)^{-1}$:

$$\begin{aligned} p_{X1}(M_{L1})^{-1} \cdot p_{X1}(M_{L1}) = p_{X1}(M_{L1}) \cdot p_{X1}(M_{L1})^{-1} = 1, \\ p_{X2}(M_{L2})^{-1} \cdot p_{X2}(M_{L2}) = p_{X2}(M_{L2}) \cdot p_{X2}(M_{L2})^{-1} = 1. \end{aligned}$$

This means that for certain subset $\mathcal{P}_F \in \mathcal{P}$, there exist some subring $\mathcal{M}_F$ of matrices in $\mathcal{M}$, which is a field. For the protocol construction let us choose at random any matrix Q in $\mathcal{M}$ not equal to M_{L1} and M_{L2}. We choose also at random secret integer number $r \in \mathcal{N}$. By having instances X, Q and r, we compute the matrix A as follows:

$$A = XQ^r X^{-1}. \tag{2}$$

The asymmetric cipher we declare the following public parameters: sets $\mathcal{M}$ and $\mathcal{P}$; subset $\mathcal{M}_L$ and matrices M_{L1}, M_{L2}, Q. For the public key (PuK) we can define the matrices A and Q and for the private key (PrK) – matrix X and secret integer number r. In brief, these keys are denoted by $PuK = \{A, Q\}$ and $PrK = \{X, r\}$ correspondingly. Instead of storage matrix X, it is possible to store the coefficients of polynomial p_{X1}, p_{X2}. Then for the ciphering procedure matrix Xmust be computed using (1). This has some sense since PrK must be carefully stored in some memory restricted electronic device. Then instead of storing matrix X with m^2 matrix elements in $\mathcal{Z}_q$, we can store the only $2(n+1)$ numbers in $\mathcal{Z}_q$, representing the coefficients of polynomial p_{X1}, p_{X2}.

Since $PuK = \{A, Q\}$ is publicly available, it can be stored without the significant concern to reduce its bit length.

The example of key lengths is presented below in Section 3.

To describe the ciphering processes we need to introduce the definition of encryptor and decryptor operators, using randomly chosen secret matrix $Y \in \mathcal{M}_F$. This matrix is calculated analogously as matrix X, but using some random polynomials $p_{Y1}(\ )$, $p_{Y2}(\ ) \in \mathcal{P}$, secret coefficients $b_1 = (b_{10}, b_{11}, \ldots, b_{1n})$, $b_2 = (b_{20}, b_{21}, \ldots, b_{2n})$:

$$\begin{aligned} Y &= p_{Y1}(M_{L1}) \cdot p_{Y2}(M_{L2}) \\ &= \big(b_{10}I + b_{11}M_{L1}^1 + \cdots + b_{1n}M_{L1}^n\big) \cdot \big(b_{20}I + b_{21}M_{L2}^1 + \cdots + b_{2n}M_{L2}^n\big). \end{aligned} \tag{3}$$

Of course, the same condition, as for matrix X, must be satisfied: there must exist inverse matrix Y^{-1}, i.e., there must exist $p_{Y1}(\ )$ and $p_{Y2}(\ )^{-1}$.

Definition 1. Encryptor ε is an element in $\mathcal{M}$, which is calculated by following equation by choosing secret random number $s \in \mathcal{N}$:

$$\varepsilon = YA^s Y^{-1}. \tag{4}$$

Definition 2. Decryptor δ is an element in $\mathcal{M}$, which is calculated by following equation by choosing secret random number $s \in \mathcal{N}$:

$$\delta = YQ^s Y^{-1}. \tag{5}$$

Since the finite elements of $\mathcal{Z}_q$ can be transformed to the binary form, we define the bitwise XOR operation in $\mathcal{Z}_q$ for any finitely presented numbers.

Definition 3. The bitwise XOR operation $\oplus$ of numbers in $\mathcal{Z}_q$ is a sum modulo 2 of bits of these numbers presented in binary form.

Suppose Alice wants to send Bob a message t, encrypted by asymmetric cipher. For encryption Alice uses Bob's public key PuK. The decryption is provided by Bob's private key PrK.

At first, to encrypt a message t Alice must perform an encoding of message t by the set of numbers in $\mathcal{Z}_q$ and to form a m-dimension encoded matrix T, corresponding to t.

The asymmetric cipher encryption algorithm is the following.

Step 1: Alice takes M matrix, chooses polynomials $p_{Y1}()$ and $p_{Y2}()$ in P with secret random generated coefficients, and using (2), calculates secret matrix Y which has inverse matrix Y^{-1}.

Step 2: Alice takes Bob's PuK and using (3) calculates encryptor ε.

Step 3: Alice calculates decryptor δ using (4) in a similar way.

Step 4: Alice obtains the cyphertext C computed by the formula:

$$C = \varepsilon \oplus T = YA^sY^{-1} \oplus T. \tag{6}$$

Step 5: Alice sends to Bob the following data $D = \{C, \delta\}$, which is ciphertext for T.

Decryption algorithm:

Bob gets data $D = \{C, \delta\}$ and using his private key PrK calculates the encoded plaintext T by equation:

$$X\delta^r X^{-1} \oplus = T. \tag{7}$$

The last equation is valid since the following identities hold $XY = YX$ and $X^{-1}Y^{-1} = Y^{-1}X^{-1}$. Indeed using these commutation identities we obtain the following:

$$\begin{aligned} X\delta^r X^{-1} \oplus C &= X\big(YQ^sY^{-1}\big)^r X^{-1} \oplus YA^sY^{-1} \oplus T \\ &= XYQ^{sr}Y^{-1}X^{-1} \oplus Y\big(XQ^rX^{-1}\big)^s Y^{-1} \oplus T \\ &= XYQ^{sr}Y^{-1}X^{-1} \oplus YXQ^{rs}X^{-1}Y^{-1} \oplus T \\ &= XYQ^{sr}Y^{-1}X^{-1} \oplus XYQ^{sr}Y^{-1}X^{-1} \oplus T. \end{aligned} \tag{8}$$

Then Bob, using the known decoding procedure, recovers the initial message t from T.

2. Preliminary security analysis

The security of proposed asymmetric cipher relies on OWF, which is based on two simultaneous problems: the matrix conjugator search problem (MCSP) and matrix discrete logarithm problem (MDLP).

DEFINITION 4. The MCSP is for given instances Q and A to find the conjugator matrix X from the following equation:

$$A = XQX^{-1}. \tag{9}$$

The MCSP alone in matrix field does not provides a sufficient security since its solution can be performed by polynomial time algorithm. The unknown matrix X

from (9) can be found by solving the following homogenous matrix equation, which corresponds to the homogenous system of linear equations:

$$AX - XQ = 0.$$

DEFINITION 5. The MDLP is to find a natural r for given m-dimensional matrices Q and P, satisfying the following equation:

$$P = Q^r.$$

This problem can be reduced to the multiple ordinary DLP when Q can be transformed to the diagonal form. If Q has a block diagonal form, the initial m-dimensional MDLP can be spitted to several l_i-dimensional matrix DLP where $l_1 \ldots, l_k$ are dimensions of corresponding k blocks.

To break the proposed cipher, the adversary must find the $PrK = (X, r)$. Then he/she must solve the following system of the following matrix equations:

$$\begin{cases} AX = XP, \\ P = Q^r. \end{cases}$$

The first matrix equation could be transformed into multivariate quadratic equation with $2(n+1)$ unknowns.

The second one corresponds to the MDLP. We have no known algorithms suitable to solve this system except the brute force attack, i.e., the total scan of solution.

The preliminary analysis shows, that MCSP and MDLP in this case can not be solved separately. Since the total complexity is composed by both matrix MCSP and MDLP, we can make a conjecture that proposed asymmetric cipher security level is sufficient at this time if the cipher parameters are chosen in such way that they prevent the brute force attack.

The proposed cipher's algorithm depends on the following parameters:

– the dimension of matrices m;

– the order q of finite field $\mathcal{Z}_q$;

– the order n of polynomials;

– the magnitude of secret integer numbers (r, s).

The greater values q, n and (r, s) are, the higher security against the brute force attack can be achieved. The PrK and PuK lengths depend on the values of these parameters. Hence can be treated as security parameters of proposed cipher algorithm.

Let us, for example, choose the values $q = 61$, $n = 12$, $m = 10$, $r = 2^{128}$, then the total scan set number of verification consist of operations about $\eta = 2^{256}$. Since the matrix $X$of private key $PrK = \{X, k\}$ can be represented by the vectors of polynomials' coefficients, then the length of PrK is 256 *bits*. The representation of $PuK = \{A, Q\}$ requires *4608 bits*. Hence, the PrK compromitation by applying the brute force attack has 2^{256} complexity.

According to the choosen parameters the ciphering procedure will take about $\log_2 r$ m-dimensional matrix multiplications. In total it is required to perform the $m^2 \log_2 r$ multiplication operations in the small field, e.g., in the field of order 61. These operations can be performed using the table. In our parameters collection this takes about 10,000 multiplications with multiplication table of order 61 × 61.

For example, for the RSA asymmetric cipher with key length of 4096 bits it is required to perform several thousands multiplications to calculate the exponent in the ring of order 2^{4096}.

As we see the amount of calculations in our system is similar to the amount of calculations in RSA. Furthermore, the private key length in our system is ten times shorter than is classical systems.

3. Conclusions

This paper presents the new asymmetric cipher scheme based on new one way function (OWF). The new OWF is constructed using two simultaneous problems: the matrix conjugator search problem (MCSP) and matrix discrete logarithm problem (MDLP) over the finite field $\mathcal{Z}_q$.

So far, there are no known deterministic algorithms allowing to solve simultaneously the MCSP and MDLP. Since nor MCSP neither MDLP can not be solved separately, the security of proposed asymmetric cipher relies on the brute force attack prevention. The paper presents the secure parameters values, which shows that the private key length in our system is ten times shorter than is classical systems. The computation amount of presented system is comparable to the classical systems.

References

1. K.H. Ko, S.J. Lee, J.H. Cheon, J.W. Han, J. Kang, C. Park. New public key cryptosystem using braid groups. In: *Advances in Cryptology*, *Proc. Crypto 2000. LNCS*, Vol. 1880. Springer-Verlag, Berlin/Heidelberg, 2009, 166–183.
2. A. Raulynaitis, S. Japertas. Asymmetric cipher protocol using decomposition problem. In: *Information Research and Applications*, *i.Tech 2008*. Varna, Bulgaria, 107–111, 2008.
3. E. Sakalauskas. One digital signature scheme in semimodule over semiring. *Informatica*, 16(3):383–394, 2005.
4. E. Sakalauskas, P. Tvarijonas, A. Raulynaitis. Key agreement protocol (KAP) using conjugacy and discrete logarithm problems in group representation level. *Informatica*, 18(1):115–124, 2007.
5. V. Shpilrain, A. Ushakov. The conjugacy search problem in public key cryptography: Unnecessary and insufficient. In: *Applicable Algebra in Engineering, Communication and Computing*, 2004.
6. V. Sidelnikov, M. Cherepnev, V. Yaschenko. Systems of open distribution of keys on the basis of noncommutative semigroups. *Russian Acad. Sci. Dokl. Math.*, 48(2):566–567, 1993.

REZIUMĖ

A. Raulynaitis, A. Venclovienė. Asimetrinio šifravimo algoritmas, paremtas jungtinumo ir diskretaus logaritmo problemomis

Šiame straipsnyje yra pasiūlytas asimetrinis šifravimo algoritmas, kuris realizuojamas matricos lauke. Asimetrinio šifravimo mechanizmas turi būti konstruojamas, naudojant vienkryptę funkciją. Pateiktas algoritmas yra paremtas vienkrypte funkcija, kuri sukonstruota naudojant iš karto dvi skaičiavimo problemas: jungtinuko suradimo problemą (JPS) ir modikuotą diskrečiojo algoritmo problemą (DAP). Algoritmo konstrukcija neleidžia atlikti kriptoanalizę, išskaidant skaičiavimo problemas JSP ir DAP bei jas sprendžiant atskirai.

Raktiniai žodžiai: asimetrinis šifravimo algoritmas, jungtinuko suradimo problema, diskretaus logaritmo problema, vienkryptė funkcija.