ASYMMETRIC CIPHER PROTOCOL USING DECOMPOSITION PROBLEM

Andrius Raulynaitis, Saulius Japertas

Abstract: The asymmetric cipher protocol based on decomposition problem in matrix semiring M over semiring of natural numbers N is presented. The security parameters are defined and preliminary security analysis is presented.

Keywords: asymmetric cipher, decomposition problem.

ACM Classification Keywords: E.3 Data Encryption, F.2.1 Numerical Algorithms and Problems.

Conference: The paper is selected from Sixth International Conference on Information Research and Applications – i.Tech 2008, Varna, Bulgaria, June-July 2008

Introduction

Main object of asymmetric cipher constructing is one way function, which must be based on hard mathematical problems. For example traditional cryptosystems is based either the problem of factoring large integer number or on the discrete logarithm problem (DLP).

New ideas in public key cryptography using hard problems in infinite non-commutative groups and semigroups appeared in [Sidelnikov et. al., 1993]. The realization of these ideas appeared in [Ko et al., 2000], using the braid group as a platform. The security of this cryptosystem was based on conjugator search problem. But according [Shpilrain and Ushakov, 2004] the approach is not sufficient and necessary.

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 [Sakalauskas, 2005], [Sakalauskas et al., 2007]. The (semi)group representation level allows us to avoid the significant problem to hide the factors in the publicly available group (braid group) word when using its presentation level. The hiding factors in representation level are achieved in a very natural way. However, the original hard problems, such as conjugator search or decomposition problems in (semi)group presentation level, are considerably weakened when transferred to the representation level. Hence these problems must be considerably strengthened by simultaneously adding the other additional hard problems in representation level.

Lately the idea to use matrix group conjugacy problem together with matrix discrete logarithm problem for the one way function construction is presented in [Sakalauskas et al., 2007]. Another approach is based on so called matrix power operation for a matrix power S-box construction, is introduced in [Sakalauskas and Luksys, 2007].

In this study we propose new asymmetric cipher using decomposition (double coset) problem in matrix semiring $\mathcal{M}$ over semiring $\mathcal{N}$ of natural numbers.

Preliminaries

We consider an infinite multiplicative matrix semiring $\mathcal{M}$ over the semiring at natural numbers $\mathcal{N}$. We assume $\mathcal{N}$ = {0, 1, 2, ...}. The elements of $\mathcal{M}$ are *m*-dimensional square matrices with entries in $\mathcal{N}$. Let us choose two distinct matrices M_L and M_R in $\mathcal{M}$ and define the set of all possible polynomials P= $\{p_i(\ )\}$ over $\mathcal{N}$. Then the set $\mathcal{P}_L$ we define as a set of all matrices of all polynomial functions in P with argument M_L and $\mathcal{P}_R$ as a set of all polynomials functions with arguments M_R. In other words $\mathcal{P}_L$ =$\{p_i(M_L)\}$ and $\mathcal{P}_R$ = $\{p_i(M_R)\}$. It is evident, that all matrices in $\mathcal{P}_L$ and all matrices in $\mathcal{P}_R$ are commuting.

To choose, for example, some matrices X, U in $\mathcal{P}_L$ and Y, V in $\mathcal{P}_R$ we can select two pairs of polynomials p_X, p_U and p_Y, p_V in $\mathcal{P}$ and using the addition and multiplication operations in $\mathcal{N}$ find the following matrices:

$$X = p_X(M_L), Y = p_Y(M_R) \tag{1}$$

$$U = p_U(M_L), V = p_V(M_R) \tag{2}$$

As we can see, the matrices X, U and Y, V are commuting, i.e.:

$$XU = UX; YV = VY \tag{3}$$

Asymmetric cipher

On the bases of presented above formalism we can construct an asymmetric ciphering algorithm. Let's choose distinct matrices M_{L1} and M_{L2} from $\mathcal{P}_L$ and M_{R1} and M_{R2} from $\mathcal{P}_R$ to calculate polynomial matrices X and Y by (2.1) in the following way:

$$X = p_{X1}(M_{L1}) \cdot p_{X2}(M_{L2}) \tag{4}$$

$$Y = p_{Y1}(M_{R1}) \cdot p_{Y2}(M_{R2}) \tag{5}$$

$$U = p_{U1}(M_{L1}) \cdot p_{U2}(M_{L2}) \tag{6}$$

$$V = p_{V1}(M_{R1}) \cdot p_{V2}(M_{R2}) \tag{7}$$

where all polynomials are in P.

All polynomials in (4), (5) are represented by the following vectors $a_L = (a_1, a_2, \ldots, a_n)$, $b_L = (b_1, b_2, \ldots, b_n)$, $a_R = (c_1, c_2, \ldots, c_n)$, $b_R = (d_1, d_2, \ldots, d_n)$ with components in $\mathcal{N}$. Let the matrices M_{R1}, M_{L1}, M_{R2}, and M_{L2} are at the form:

$$M_{L1} = \begin{pmatrix} L_1 & \Theta \\ \Theta & h_1 I \end{pmatrix}, M_{L2} = \begin{pmatrix} h_2 I & \Theta \\ \Theta & L_2 \end{pmatrix}, M_{R1} = \begin{pmatrix} R_1 & \Theta \\ \Theta & r_1 I \end{pmatrix}, M_{R2} = \begin{pmatrix} r_2 I & \Theta \\ \Theta & R_2 \end{pmatrix} \tag{8}$$

where Θ are $m/2$-dimensional zero matrix, L_1, L_2, R_1 and R_2 are $m/2$-dimensional square matrix over $\mathcal{N}$, I is $m/2$-dimensional identity matrix, h_1, h_2, r_1 and r_2 are numbers in $\mathcal{N}$. Let's choose any matrix Q in $\mathcal{M}$ not equal M_{L1}, M_{L2} and M_{R1}, M_{R2} and calculate matrix, using the matrices X and Y calculated by (4) and (5)

$$A = XQY \tag{9}$$

Assymmetric cipher public parameters we declare $\mathcal{M}$, $\mathcal{R}$ and matrices $M_{L1}, M_{L2}, M_{R1}, M_{R2}$. The private key is $\mathrm{PrK} = \{X, Y\}$ and public key $\mathrm{PuK} = \{Q, A\}$. When vectors a_L, a_R, b_L, b_R are unknown, matrices X and Y are also unknown. Using (2) and PuK we define encryptor and decryptor operators.

Definition 1: Encryptor ε is an element in $\mathcal{M}$ which is calculated by following equation:

$$\varepsilon = UAV \tag{10}$$

Definition 2: Decryptor δ is an element in $\mathcal{M}$ satisfying following equation:

$$\delta = UQV \tag{11}$$

It is clear that the elements of $\mathcal{N}$ can be transformed in the binary form.

Definition 3: The bitwise XOR operation $\oplus$ of the elements (numbers) in $\mathcal{N}$ is a sum modulo 2 of bits of numbers presented in binary form.

Let Alice intents to encrypt her message *t* with Bob's public key $\mathrm{PuK_B} = \{Q, A\}$ obtaining a ciphertext *C*. Then Bob decrypts received *C* using his private key $\mathrm{PrK_B} = \{X, Y\}$. For the ciphering message *t* Alice must perform encoding *t* by the numbers in $\mathcal{N}$ and to form a *m*-dimension matrix *T*, corresponding *t*.

Then the encryption algorithm is following:

Step 1. Alice takes $M_{L1}, M_{L2}, M_{R1}, M_{R2}$ matrices, chooses at random vectors of polynomials coefficients a_L, a_R, b_L and b_R and using (6), (7) calculates matrices *U* and *V*.

Step 2. Alice calculates encryptor ε using (10).

Step 3. Alice calculates decryptor δ using (11).

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

$$C = \varepsilon \oplus T = UAV \oplus T \tag{12}$$

Step 5. Alice sends to Bob the following data $D = (C, \delta)$.

Decryption algorithm:

Bob gets data $D = (C, \delta)$ and using his private key $\mathrm{PrK_B}$ calculates the decoded plaintext *T*:

$$X\delta Y \oplus C = T \tag{13}$$

The last equation is valid since using (3) the following identities take place:

$$X\delta Y \oplus C = X(UQV)Y \oplus C = X(UQV)Y \oplus UAV \oplus T = XUQVY \oplus UXQYV \oplus T = T \tag{14}$$

4. Security analysis

To break this asymmetric cipher, Bob's $\mathrm{PrK_B}$ must be compromised, i. e. to find any *X'* and *Y'*, satisfying (9) and commutativity conditions (3). Hence for compromising $\mathrm{PrK_B}$ it is not required to find the true values of *X* and *Y*. The required matrices *X'* and *Y'*, must satisfy equation:

$$X'QY' = A \tag{15}$$

It is easy to notice, if (15) is satisfied, then

$$X'\delta Y' \oplus C = X'(UQV)Y' \oplus C = U(X'QY')V \oplus UAV \oplus T = UAV \oplus UAV \oplus T = T \tag{16}$$

Definition 4. The computational decomposition (or double coset) problem (DP) in $\mathcal{M}$ is to find any matrices *X'* and *Y'* in $\mathcal{M}$ when given *A* and *Q* satisfying equation (15).

Definition 5. The decisional (YES/NO) DP is to get an answer, if there are there any matrices *X'* and *Y'* in $\mathcal{M}$ satisfying (15) for given *Q* and *A*.

Definition 6. The DP is strong one way function (OWF) if determination of any *X'* and *Y'* is infeasible when given *A* and *Q*.

On the complexity of formulated computational DP relies on security of proposed cipher algorithm. So formulated DP is equivalent to task find any coefficients of polynomials p_{X1}, p_{X2} and p_{Y1}, p_{Y2} in (4) and (5) when the matrices *X'* and *Y'* computed using these equations satisfies (15). Let

$$\begin{aligned} X' &= p'_{X1}(M_{L1}) \cdot p'_{X2}(M_{L2}) = \\ &= \left(a'_0 M^0_{L1} + a'_1 M^1_{L1} + \ldots + a'_n M^n_{L1}\right) \cdot \left(b'_0 M^0_{L2} + b'_1 M^1_{L2} + \ldots + b'_n M^n_{L2}\right) \end{aligned} \tag{17}$$

$$\begin{aligned} Y' &= p'_{Y1}(M_{R1}) \cdot p'_{Y2}(M_{R2}) = \\ &= \left(c'_0 M^0_{R1} + c'_1 M^1_{R1} + \ldots + c'_n M^n_{R1}\right) \cdot \left(d'_0 M^0_{R2} + d'_1 M^1_{R2} + \ldots + d'_n M^n_{R2}\right) \end{aligned} \tag{18}$$

Then the DP according the Definition 4 is equivalent to find any vectors $a'_L = (a'_0, a'_1, \ldots, a'_n)$, $a'_R = (b'_1, b'_2, \ldots, b'_n)$, $b'_L = (c'_0, c'_1, \ldots, c'_n)$ and $b'_R = (d'_0, d'_1, \ldots, d'_n)$, satisfying (15), when *X'* and *Y'* are computed using ((17) and (18).

The set of possible values of vectors a'_L, a'_R, b'_L and b'_R must be large enough to prevent the total scan (i.e. *brutal force* attack), to find solution. If this is done the other way is to try to solve the matrix equation (15), using some more advanced algorithm. We can write (17) (18) in following way:

$$X' = \sum_{i,j} \left(a'_i b'_j M^i_{L1} M^j_{L2} \right) \tag{19}$$

$$Y' = \sum_{k,l} \left(c'_k d'_l M^k_{R1} M^l_{R2} \right) \tag{20}$$

Then (15) can be rewritten as:

$$X'QY' = \sum_{i,j,k,l} \left(a'_i b'_j c'_k d'_l M^i_{L1} M^j_{L2} Q M^k_{R1} M^l_{R2} \right) \tag{21}$$

This matrix equation corresponds to the *m*x*m* system of polynomial equation with fourth order monomials $a'_i b'_j c'_k d'$. But nevertheless this system allows a direct linearization. To linearize this system, let us introduce a set of new variables $\{z_{ijkl}\}$, when $z_{ijkl} = a'_i b'_j c'_k d'_l$, then (21) can be rewritten in the form:

$$\sum_{i,j,k,l} \left(z_{ijkl} M^i_{L1} M^j_{L2} Q M^k_{R1} M^l_{R2} \right) = A \tag{22}$$

As we see there are m^2 equations and $(n+1)^4$ unknowns in every equation. Depending on m^2 and $(n+1)^4$ ratio, this system is:

a) Under defined, when $m^2 > (n+1)^4$;

b) Equal defined, when $m^2 = (n+1)^4$;

c) Over defined, when $m^2 < (n+1)^4$;

We conjecture that greatest computational complexity of (22) can be achieved when the cases a) and b) are near the equal defines case. We do not know the algorithmically affective methods, how to find z_{ijkl} in semiring $\mathcal{N}$ of natural numbers Hence we can make a conjecture that private key computed by (9) represents the one-way function.

In a natural way we can choose the following security parameters for our cipher:

- dimension of matrices *m*;
- maximum order of matrices' $(M_{L1}, M_{L2}, M_{R1}, M_{R2}, Q)$ elements *r*;
- maximum order of polynomials *n*;
- maximum order of polynomials' coefficients *s*;

We need to define optimal limits of these parameters to prevent the brute force attack, qualitatively estimate the security of the cipher and minimize needs of computer's memory for matrix storage. The total scan to find a coefficients of the polynomials requires to perform the number of verification operations η:

$$\eta = s^{4n+4} \tag{23}$$

The number of bits β required to store the matrix *A* is:

$$\beta = m^2 \log_2 \left(\left(m/2 \right)^{2n} r^{4n+1} s^4 \right) \tag{24}$$

For example, consider such case: let $n = 2$, $s = 2^8$, $r = 2^4$, $m = 8$. Then $\eta = \left(2^8\right)^{4\cdot 2+4} = 2^{96}$ and the number of bits representing matrix A is $\beta = 8^2 \log_2\left((8/2)^{2\cdot 2} \cdot \left(2^4\right)^{4\cdot 2+1}\left(2^8\right)^4\right) = 64 \cdot 76 = 4864$ bits.

It is clear that under these parameters we prevent the brute force attack. In this case we have 64 equations and 81 monoms corresponding to (22). Hence our system is under defined. If we use linearization method to compromise cipher, we should freely choose 17 monoms values and then we need to solve system of 64 equations over semiring of natural number $\mathcal{N}$. We reckon this problem is hard enough to compromise a private key. Even if suitable variables z_{ijkl} will be found the problem of restoring the coefficients of polynomials remains hard.

Conlusions

In this paper we proposed one asymmetric cipher protocol using decomposition problem in matrix semiring $\mathcal{M}$ over semiring of natural numbers $\mathcal{N}$. We showed that the compromisation of cipher relies on the intractability of solution of system of linear equation over the semiring $\mathcal{N}$. After that the other problem is to restore the coefficients of polynomials which we reckon to be also hard task. The complexity estimation requires further investigations in order to find the estimates of security parameters and their relation to the other security parameters of known cryptographic primitives.

Bibliography

[Sidelnikov et. al., 1993] V. Sidelnikov, M. Cherepnev and V. Yaschenko (1993). Systems of open distribution of keys on the basis of noncommutative semigroups. // Russian Acad. Sci. Dokl. Math., 48(2), 566567.

[Ko et al., 2000] Ki Hyoung Ko , Sang Jin Lee , Jung Hee Cheon, Jae Woo Han, Ju–sung Kang, and Choonsik Park (2000). New Public–key Cryptosystem Using Braid Groups. // Advances in Cryptology, Proc. Crypto 2000, LNCS 1880, Springer–Verlag (2000), 166–183

[Shpilrain and Ushakov, 2004] V. Shpilrain and A. Ushakov (2004). The conjugacy search problem in public key cryptography: unnecessary and insufficient. // Available at: http://eprint.iacr.org/2004/321

[Sakalauskas, 2005] E. Sakalauskas, One Digital Signature Scheme in Semimodule over Semiring, Informatica. ISSN: 0868-4952, vol. 16, no. 3(2005), pp. 383-394.

[Sakalauskas et al., 2007] E. Sakalauskas, P. Tvarijonas and A. Raulynaitis, Key Agreement Protocol (KAP) Using Conjugacy and Discrete Logarithm Problems in Group Representation Level, Informatica, Vol. 18, No. 1, 2007, pp. 115-124.

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

Author's Information

Andrius Raulynaitis – PhD student in Institute of Defense Technologies of Kaunas University of Technology, Kęstučio g. 27, LT-44312 Kaunas, Lithuania, e-mail: Andrius.Raulynaitis@stud.ktu.lt

Saulius Japertas – associated professor in Department of Telecommunications, Kaunas University of Technology, Studentų str. 50, LT-51368 Kaunas, Lithuania, e-mail: Saulius.Japertas@ktu.lt