ISSN 1392 – 124X INFORMATION TECHNOLOGY AND CONTROL, 2010, Vol. 39, No. 1

KEY AGREEMENT PROTOCOL OVER THE RING OF MULTIVARIATE POLYNOMIALS

Eligijus Sakalauskas, Artūras Katvickis, Gediminas Dosinas

Kaunas University of Technology, Department of Applied Mathematics,
Studentų Str. 50, LT–51368, Kaunas, Lithuania
e-mail: eligijus.sakalauskas@ktu.lt, arturas.katvickis@ktu.lt, gedinimas.dosinas@ktu.lt

Abstract. The key agreement protocol (KAP) using matrices over the ring of multivariate polynomials is presented. The compromisation of proposed KAP relies on the solution of multivariate quadratic (MQ) system of equations problem – the problem, which is reckoned as being NP-complete. The general method of solving MQ problem is Grobner basis algorithm, which is of exponential or even double exponential time in general case. For special cases such as overdefined and sparse systems, there are some special solution methods, i.e. XL and XSL algorithms. By choosing suitable security parameters for the compromisation of the proposed KAP, we obtained a random not overdefined and not sparse system of MQ equations and hence we recon that our KAP compromasation relies on the hard MQ problem.

1. Introduction

Key agreement protocol is one of the basic cryptographic protocols. KAP allows two or more parties negotiate a common secret key using insecure communications.

The first KAP was presented by Diffie and Hellman [5]. This algorithm caused rapid development of asymmetric cryptography.

In 1993 new ideas appeared in asymmetric cryptography [14] using known hard computational problems in infinite non-Abelian groups instead of hard number theory problems such as discrete logarithm or integer factorization problems to construct one-way functions.

These ideas were realized in [1] where KAP was constructed using conjugator search problem and membership problem in Braid groups. The similar result was presented in [9].

Later, in [13] it was showed that conjugator search problem in braid groups does not produce sufficient security level.

The idea to use non-commutative infinite group e.g. braid group representation was used for the one-way functions construction as a background of KAP in [11]. The other approach of hypothetical one-way function construction applied for the digital signature scheme using infinite non-commutative group representation in finite field was presented in [10].

In this paper we present KAP using matrices over the ring of multivariate polynomials. This function pretends to be a one-way function since its inversion is related with a solution of multivariate quadratic (MQ) system of equations over finite field.

2. Key agreement protocol

Now we propose the following two parties key agreement protocol.

1. Parties agree on publicly available matrices Q, L, R of order m over the multivariate polynomials ring $Z_2[t_1, \ldots, t_p]$. The set of these matrices is a non-commutative matrix ring which we denote by $\mathbf{M}$ or more formally by $\mathbf{M}(m, Z_2[t_1, \ldots, t_p])$. Let $\mathbf{M}_L$ and $\mathbf{M}_R$ are the subsets in $\mathbf{M}$ consisting of commuting matrices. This means that for any $L_1, L_2 \in \mathbf{M}_L$ and $R_1, R_2 \in \mathbf{M}_R$ the following commuting condition holds

$L_1L_2 = L_2L_1$,

$R_1R_2 = R_2R_1$.

Let $L \in \mathbf{M}_L$ and $R \in \mathbf{M}_R$ are the publicly known parameters.

2. Alice randomly generates two secret matrix polynomials represented by the randomly chosen bit sequences $\{b_{xi}\}$, $\{b_{yi}\}$, $i = 0, 1, \ldots, k$ and computes

$$X = \sum_{i=0}^{k} b_{xi} L^i = b_{x0} I + b_{x1} L + \ldots + b_{xk} L^k, \qquad (1)$$

$$Y = \sum_{i=0}^{k} b_{yi} R^i = b_{y0} I + b_{y1} R + \ldots + b_{yk} R^k. \qquad (2)$$

Then $X \in \mathbf{M}_L$ and $Y \in \mathbf{M}_R$.

3. Analogously, Bob randomly generates two randomly chosen secret bit sequences $\{b_{ui}\}$, $\{b_{vi}\}$, $i = 0, 1, \ldots, k$ and computes

$$U = \sum_{i=0}^{k} b_{ui} L^i = b_{u0} I + b_{u1} L + \ldots + b_{uk} L^k , \quad (3)$$

$$V = \sum_{i=0}^{k} b_{vi} R^i = b_{v0} I + b_{v1} R + \ldots + b_{vk} R^k . \quad (4)$$

After these precomputations $U \in \mathbf{M}_L$ and $V \in \mathbf{M}_R$ and

$$XU = UX;\ YV = VY. \quad (5)$$

4. Alice computes intermediate value K_A and sends result to Bob:

$$K_A = XQY. \quad (6)$$

5. Bob computes intermediate value K_B and sends result to Alice:

$$K_B = UQV. \quad (7)$$

6. Since matrices X, U and Y, V are commuting, both parties compute common secret key

$$K = XK_BY = UK_AV = XUQVY = UXQYV. \quad (8)$$

The public key of the proposed KAP consists of matrices Q, L and R.

3. KAP compromisation

If adversary (Eve) could find any X', Y', satisfying commutating conditions (5) and relation

$$X'QY' = K_A, \quad (9)$$

then he (she) can determine the common secret key K in the following way

$K = X'K_BY' = X'UQVY' =$ [if commutating condition holds] $= UX'QY'V = UK_AV = K$.

Let Eve choose any matrix $Y' = Y_0 \in \mathbf{M}_R(m, Z_2[t_1, \ldots, t_p])$. Then (6) can be rewritten in the form

$$X'QY_0 = K_A.$$

By denoting the product $QY_0 = T$, we obtain the following linear matrix equation

$$X'T = K_A, \quad (10)$$

which can be easily solved with respect to the unknown matrix X'. But nevertheless there is no guarantee that solution X' of matrix equation (10) is in subring $\mathbf{M}_L(m, Z_2[t_1, \ldots, t_p])$, i.e. the commuting equation

$$X'U = UX'$$

does not necessary hold even if solution X' exists.

Hence to break the system, an adversary must solve the initial equation (9) with two unknown matrices X' and Y'.

The same compromisation equation holds for the relation (7).

Hence the security of the proposed KAP relies on the complexity of the solution of (9). This problem can be formulated in the following way: for instances Q and K_A find any matrices X' and Y', satisfying commutation conditions (5). If the functions (6), (7) and (9) are one-way, then the proposed KAP is secure. According to intuitive definition, the function is reckoned as one-way function (OWF) if the calculation of its value is easy but the calculation of its inverse values is not. More specifically a function can be treated as one-way if the effective polynomial time algorithm for its inversion is not known. We use this methodology in our investigation below to confirm our conjecture. In our case the calculation of inverse value is to find any X' and Y' in (9) satisfying commutation conditions (5).

We are making a conjecture that the function related to (6), (7) and (9) equations is one-way. We present the analysis confirming in some sense our conjecture below.

4. One-way function analysis

We rewrite the proposed candidate for OWF in a more convenient form

$$f(X, Q, Y) = XQY = A. \quad (11)$$

For investigation of the function $f(X, Q, Y)$ to be OWF we use known theorem which states that:

Theorem 1 ([8]). Pseudorandom number generators (PRNG) exist, if and only if one-way functions exist .

This result can be used to test if the proposed function is one-way. Then on the basis of this function the PRNG must be constructed and the tests for randomness must be performed. Then if the obtained PRNG output passes pseudo random bit tests, this function can be a good candidate to be an OWF. If PRNG output fails pseudo random bit tests, it will be an indication that the investigated function is not a one-way function.

One-way function used in the proposed key agreement protocol is a function of three parameters X, Q, Y, i.e. $f(X, Q, Y) = XQY$. Two of them (matrices X and Y) are chosen at random and are assumed to be fixed in our PRNG construction. Some matrix Q_0 must be chosen to define the initial value. Then the PRNG corresponding to this function can be expressed by the formula:

$$Q_i = XQ_{i-1}Y,$$

where initial value $Q_0 = Q$ is required for the generator initialization.

To test PRNG output, we have used monobit, poker, runs and long runs pseudo random bits tests described in [12].

To perform a modelling, we selected some toy example of PRNG by choosing multivariate polynomials rings $Z_2[t_1, t_2, t_3]$ and $Z_2[t_1, t_2, t_3, t_4]$ with matrices of dimensions ranging from 3 to 20.

Modelling results are presented in Table 1 and showed that PRNG output fits the tests with matrices dimension equal to or higher than 12. Hence we can make a conjecture that for the bigger multivariate polynomials rings results will be similar and, referencing to Theorem 1, the function $f(X, Q, Y) = XQY$ pretends to be a one-way function. The further step to investigate the one-wayness of the proposed function is to perform its security analysis based on the function inversion.

Table 1. Percentage of "bad" bit blocks in PRNG output

Matrix dimension	3	4	5	6	7	8	9	10	11
$Z_2[t_1, t_2, t_3]$	100,0%	100,0%	100,0%	100,0%	51,7%	26,2%	9,9%	5,1%	2,7%
$Z_2[t_1, t_2, t_3, t_4]$	100,0%	100,0%	100,0%	67,6%	43,0%	8,1%	2,9%	2,0%	0,5%

Matrix dimension	12	13	14	15	16	17	18	19	20
$Z_2[t_1, t_2, t_3]$	0,5%	0,5%	0,5%	0,5%	0,5%	0,5%	0,5%	0,5%	0,5%
$Z_2[t_1, t_2, t_3, t_4]$	0,5%	0,5%	0,5%	0,5%	0,5%	0,5%	0,5%	0,5%	0,5%

5. Security analysis

We define the following security parameters: matrix dimension d, number of variables p in polynomials ring and secret length k of sequences in (1) – (4). They must be large enough to prevent brute force attack. To compromise the key K, the adversary must solve the (9) type of matrix equations to find any matrices X', Y' (or U', V') with known instances Q, K_A (Q, K_B), i.e. find inverse function of either $f(X, Q, Y)$ or $f(U, Q, V)$. Then commutation conditions (5) will be satisfied.

To determine the matrices X and Y from (6) it is required to find the unknown binary sequences $b_{x0}, \ldots, b_{xk}$ and $b_{y0}, \ldots, b_{yk}$ in (1), (2). Hence, equation (6) can be rewritten as follows:

$$\left(\sum_{i=0}^{k} b_{xi} L^i\right) Q \left(\sum_{j=0}^{k} b_{yj} R^j\right) = \\ = \sum_{i=0}^{k}\sum_{j=0}^{k} b_{xi} b_{yj} L^i Q R^j = A, \qquad (12)$$

where L, Q, R and A are known matrices over the multivariate polynomial ring. Then the system of equations (12) will be a MQ system of equations over the field Z_2 with respect to the unknown binary variables $b_{x0}, \ldots, b_{xk}$ and $b_{y0}, \ldots, b_{yk}$.

It is known that MQ problem over any field is NP-complete [6]. Moreover, it is believed that this problem is NP-Hard not only in worst case but in average case as well [15].

The general method for the MQ problem solution is the Grobner basis algorithm and its modifications. In the case of overdefined sparse system of equations the special ad hock methods are introduced such as XL, XSL and others [2], [4].

In our case we can obtain an underdefined or overdefined MQ problem near to the equaldefined case by choosing suitable parameters m, p, k.

As we see from (12), in general case when the order of matrices is m, the system consists of m^2 polynomial equations and can be rewritten to $m^2 2^p$ multivariate quadratic equations with $2(k+1)$ unknown variables. Depending on parameters m, p, k we will obtain different cases: underdefined ($m^2 2^p < 2k+2$), overdefined ($m^2 2^p > 2k+2$) or equaldefined systems ($m^2 2^p = 2k+2$).

In all cases when parameters $\{b_{xi}\}$ and $\{b_{yj}\}$ are chosen at random in (1), (2), the constructed MQ system of type (12) is not sparse and has a general form. Hence, so far no special methods except the Grobner bases algorithm can be applied.

The complexity of Grobner bases algorithm can vary from the polynomial time algorithm with respect to p up to double exponential algorithm, e.g. $\mathbf{O}\left(2^{2^p}\right)$. Recall that the polynomial time algorithms can be applied in very special cases [3].

Hence we can make a conjecture that the complexity of our general MQ problem is at least an exponential time since it has no special structure.

As we see, the number of MQ equations depends exponentially with respect to the number of variables $t_1, \ldots, t_p$. The greater number of equations the harder is the solution of obtained MQ system of equations.

According to this investigation, we can define the following security parameters: m, p and k. It is believed that the solution of randomly generated MQ system is hopeless when system consists of $n \geq 80$ equations with $s \geq 80$ variables [7] when the system is near to equaldefined case. Hence, the values of security parameters can be chosen according to these figures. We propose the security parameters values to be $m = 4$, $p = 5$, $k = 255$. Then we obtain the MQ system with 512 equations and 512 variables. In this case, the total scan area consists of 2^{256} elements and hence the brute force attack is prevented. Then the bit length of public key matrices Q, L and R is of 512 bits each, and the total public key length is of 1536 bits.

6. Conclusions

- The new KAP over the ring of multivariate polynomials is presented.
- According to the preliminary investigations, based on mathematical modelling, we can make a conjecture that KAP based on constructed matrix function over multivariate polynomial ring pretends to be a one-way function.
- The compromisation of the proposed KAP relies on the solution of system of multivariate quadratic (MQ) polynomial equations, which is an NP-complete problem over any field.
- The security parameters are defined and their values are presented.

References

[1] **I. Anshel, M. Anshel, D. Goldfeld.** An algebraic method for public key cryptography. *Mathematical Research Letters* 6, 1999, 287–293.

[2] **N. Courtois, L. Goubin, W. Meier, J.-D. Tacier.** Solving Underdefined Systems of Multivariate Quadratic Equations. *Public Key Cryptography, Lect. Notes Comput. Sci. Vol.* 2274, 2002, 211-227.

[3] **N. Courtois, A. Klimov, J. Patarin, A. Shamir.** Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations. *Eurocrypt* 2000, *Lect. Notes Comput. Sci. Vol.*1807, 2000, 392-407.

[4] **N. Courtois, J. Patarin.** About the XL Algorithm over GF(2). *Cryptographers' Track RSA* 2003, *Lect. Notes Comput. Sci. Vol.*2612, 2003,141-157.

[5] **W. Diffie, M. Hellman.** New Directions in Cryptography. *IEEE Transaction on Information Theory*, 22, 1976, 644-654.

[6] **M.R. Garey, D.S. Johnson.** Computers and Intractability: *A Guide to the Theory of NP-Completeness. W. H. Freeman and Company*, 1979.

[7] **J.-C. Faugere, A. Joux.** Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems Using Grobner Bases. *Crypto* 2003, *Lect. Notes Comput. Sci., Vol.*2729, 2003, 44-60.

[8] **J. Hastad, R. Impagliazzo, L.A. Levin, M. Luby.** A pseudorandom generator from any one-way function. *Siam Journal on Computing*, 28(4), 1999, 1364–1396.

[9] **K. H. Ko, S. J. Lee, J. H. Cheon, J.W. Han, J.S. Kang, C. Park.** New Public key Cryptosystem Using Braid Groups. *Advances in Cryptology, Proc. Crypto* 2000, *Lect. Notes Comput. Sci., Vol.*1880, 2000, 166–183.

[10] **E. Sakalauskas.** One Digital Signature Scheme in Semimodule over Semiring. *Informatica*, *Vol.*16, *No*.3, 2005, 383-394.

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

[12] Security Requirements For Cryptographic Modules. *http://csrc.nist.gov/publications/fips/fips140-2/fips 1402.pdf*.

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

[14] **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), 1993, 566-567.

[15] **R. Steinfeld.** The Current Status in Design of Efficient Provably Secure Cryptographic Pseudorandom Generators. *In: Li Y. (Ed.) Proceedings of the First International Workshop on Coding and Cryptology, China*, 233-255, 2007.

Received September 2009.

DOI: 10.5755/j01.itc.39.1.12087