ISSN 1392 – 1215 ELECTRONICS AND ELECTRICAL ENGINEERING 2012. No. 1(117)
ELEKTRONIKA IR ELEKTROTECHNIKA

T 120 SYSTEM ENGINEERING, COMPUTER TECHNOLOGY
SISTEMŲ INŽINERIJA, KOMPIUTERINĖS TECHNOLOGIJOS

Microprocessor Realization of Key Agreement Protocol based on Matrix Power Function

P. Vitkus, E. Sakalauskas, N. Listopadskis, R. Vitkiene
Department of Applied mathematics, Kaunas University of Technology,
Studentu str. 50, Kaunas, Lithuania, phone: +370 37 300300, e-mails: paulius.vitkus@ktu.lt, eligijus.sakalauskas@ktu.lt, narimantas.listopadskis@ktu.lt, raimonda.vitkiene@dnb.lt

crossref http://dx.doi.org/10.5755/j01.eee.117.1.1049

Introduction

Nowadays the Internet has expanded and encompasses not only regular PCs, but also a large number of small devices ranging from PDAs and cell phones to appliances and network sensors. Conventionally these systems are called embedded systems. In this connection information security becomes a very important issue [1]. Symmetric cryptography achieves information confidentiality goals. However it requires pre-distribution of secret keys, which can be done with the help of public-key cryptography. Traditional key agreement protocols (KAP) requires a significant amount of computation [2], but in restricted computational environment we are limited in computational power and memory size.

In this paper we propose a new KAP based on NP-complete problem and hence having a property of provable security. Proposed KAP can be used in low-cost systems and it should work efficiently even on 8-bit microprocessors with no dedicated cryptographic coprocessors. We also compare the realization of our KAP with classical KAPs.

Key agreement protocols

KAPs are one of the basic cryptographic protocols. KAP allows two or more parties negotiate a common secret key using insecure communications. First KAP was presented by [3] which caused a rapid development of asymmetric cryptography. Its realization in restricted computational environments is time consuming since it requires arithmetical operations with big integers.

In 1985 [4, 5] independently suggested elliptic curve cryptography. Based on that elliptic curve Diffie-Hellman (ECDH) KAP was developed. Because of the smaller key size its realization is significantly faster then that of original Diffie-Hellman (DH) protocol.

In 1993 new ideas appeared in asymmetric cryptography [6] – using known hard computational problems in infinite non-commutative groups instead of hard number theory problems such as discrete logarithm or integer factorization problems. These ideas were realized in [7, 8, 9].

Nevertheless, [10] showed that conjugator search problem in braid groups does not produce sufficient security level. Moreover, authors noticed that the main problem for construction of cryptographic primitives in infinite non-commutative groups is to reliably hide the factors in group word.

The idea to use non-commutative infinitive group (e.g. braid group) representation was also used to construct other candidate one-way function as a background of both digital signature scheme and key agreement protocol [11, 12]. The (semi)group representation level allows us to avoid a significant problem of hiding the factors in the publicly available group word when using its presentation level. Since this problem is solved in a very natural way. However, the original hard problems, such as conjugator search or decomposition problems in (semi)group presentation level are weakened when they are transformed into the representation level. Therefore using representation level these problems must be considerably strengthened by simultaneously adding the other additional hard problems. One of solution is to use matrix power function (MPF) [12].

The idea of this article is to create a new KAP based on the centralizer's application in braid groups presentation level, Burau representation and MPF and having effective realization in 8-bits microprocessors. KAP based on braid groups as platform groups in presentation level using centralizers is also presented in [9]

Proposed KAP is using matrix power function which is some matrix (semi)group S action on a matrix set M. The set M is not specified as a closed set with respect to some internal operation. Both S and M are defined over two different algebraic structures. S is defined over some finite field F and M over some finite non-cyclic group G. We will show that inversion of so defined MPF has some indications to be NP-complete. Hence the security of presented KAP relies on the complexity conjectured of NP-complete problem and its realization is based on the candidate one-way function (OWF).

Mathematical background

We consider general Artin braid group [13] as our infinite non-commutative group. Given an integer $n \geq 2$, the braid group on n strands, B_n, is defined by following presentation

$$B_n = \left\langle e, \sigma_1, \ldots, \sigma_{n-1} \middle| \begin{array}{l} \sigma_i \sigma_j = \sigma_j \sigma_i, |i-j| \geq 2 \\ \sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}, 1 \leq i \leq n-2 \end{array} \right\rangle . \quad (1)$$

Given a group B_n, the centralizer of an element $x \in B_n$ is the subgroup of B_n consisting of all elements which commute with x. We denote $C(x) = \{\gamma_{x_1}, \ldots, \gamma_{x_k}\}$ the know set of generators of the centralizer of an element x. An algorithm how to compute a generating set for the centralizer of an element in braid group and more generally in Garside group is presented by [14]. We claim that $k \geq 2$.

Our protocol is based on braid group reduced Burau representation [15]. To transform braid groups to matrix groups we denoted representation by $\rho : B_n \to GL(n-1, Z_p)$ as follows

$$\sigma_i \mapsto I_{i-2} \oplus \begin{pmatrix} 1 & -t & 0 \\ 0 & -t & 0 \\ 0 & -1 & 1 \end{pmatrix} \oplus I_{n-i-2}, \quad (2)$$

where the $-t$ in the middle of the 3×3 matrix is always in the $(i,i)^{th}$ spot and $t \in Z_p$. Hence, our matrix group S is $GL(n-1, Z_p)$ and the finite field F that it is defined over is Z_p. Regular Burau representation [15] can also be used.

As non-cyclic group G we consider non-cyclic multiplicative group Z_m^* of integers modulo m. It is a set of congruence classes relatively prime to modulus m under multiplication. It is also called the group of primitive residue classes modulo m.

We can define left matrix X on matrix Q action yielding the matrix $A = {}^X Q$. All matrices are of the m-th order and formula relating the elements of these matrices

$$a_{ij} = \prod_{k=1}^{m} q_{kj}^{x_{ik}} . \quad (3)$$

Analogously, we can define right matrix Y on matrix Q action which is matrix $B = Q^Y$ and there elements satisfy equation

$$a_{ij} = \prod_{k=1}^{m} q_{ik}^{y_{kj}} . \quad (4)$$

These left and right actions are called matrix power functions. To illustrate them let us assume that matrices A, B, Q, X and Y are of the 2-nd order. Then $m = 2$ and (3), (4) can be can be written:

$$A = {}^{\begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix}} \begin{pmatrix} q_{11} & q_{12} \\ q_{21} & q_{22} \end{pmatrix} = \begin{pmatrix} q_{11}^{x_{11}} q_{21}^{x_{12}} & q_{12}^{x_{11}} q_{22}^{x_{12}} \\ q_{11}^{x_{21}} q_{21}^{x_{22}} & q_{12}^{x_{21}} q_{22}^{x_{22}} \end{pmatrix}, \quad (5)$$

$$B = Q^Y = \begin{pmatrix} q_{11} & q_{12} \\ q_{21} & q_{22} \end{pmatrix}^{\begin{pmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{pmatrix}} = \begin{pmatrix} q_{11}^{y_{11}} q_{12}^{y_{21}} & q_{11}^{y_{12}} q_{12}^{y_{22}} \\ q_{21}^{y_{11}} q_{22}^{y_{21}} & q_{21}^{y_{12}} q_{22}^{y_{22}} \end{pmatrix}. \quad (6)$$

Matrix power function is explained in more detail by [16, 17]. There is also shown that following equations are correct:

$$^{XY}Q = {}^{(XY)}Q = {}^X\left({}^Y Q\right), \quad (7)$$

$$Q^{XY} = Q^{(XY)} = \left(Q^X\right)^Y, \quad (8)$$

$$^X Q^Y = \left({}^X Q\right)^Y = {}^X\left(Q^Y\right). \quad (9)$$

Proposed protocol

Now we propose the following key agreement protocol for two parties – Alice and Bob.

1. Parties agree on publicly available braid group B_n order n, prime number p, modulo m of the group G, element $t \in S$ and matrix $Q \in M$ of the (n–1)-th order;

2. Alice randomly generates braid group word $x \in B_n$. After calculating $C(x)$, $X = \rho(x)$ and $C(X) = \rho(C(x))$ she stores X as her private key and makes $C(X)$ publicly available as her public key;

3. Bob randomly generates braid group word $y \in B_n$. After calculating $C(y)$, $Y = \rho(y)$ and $C(Y) = \rho(C(y))$ he stores Y as his private key and makes $C(Y)$ publicly available as his public key;

4. Alice randomly generates matrix $V \in C(Y)$, calculates K_a and sends it to Bob

$$K_a = {}^X Q^V ; \quad (10)$$

5. Bob randomly generates matrix $U \in C(X)$, calculates K_b and sends it to Alice

$$K_b = {}^U Q^Y ; \quad (11)$$

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

$$K = {}^X K_b^V = {}^{XU} Q^{YV} = {}^{UX} Q^{VY} = {}^U K_a^Y . \quad (12)$$

Preliminary security analysis

To compromise the secret key K one must find any matrices X, V in (10) or U, Y in (11) for given instances Q, K_a and Q, K_b correspondingly. Let us consider the case of finding any matrices X, V in (10). Let the elements of X, V, Q and K_a be $\{x_{ij}\}$, $\{v_{ij}\}$, $\{q_{ij}\}$ and $\{a_{ij}\}$ correspondingly. For more clarity the matrix equation (10) we will write in a form of system of equations for the matrices of 2-nd order, i.e. when $n = 3$:

$$\begin{cases} q_{11}^{x_{11}v_{11}} \cdot q_{21}^{x_{12}v_{11}} \cdot q_{12}^{x_{11}v_{21}} \cdot q_{22}^{x_{12}v_{21}} = a_{11}, \\ q_{11}^{x_{11}v_{12}} \cdot q_{21}^{x_{12}v_{12}} \cdot q_{12}^{x_{11}v_{22}} \cdot q_{22}^{x_{12}v_{12}} = a_{12}, \\ q_{11}^{x_{21}v_{11}} \cdot q_{21}^{x_{22}v_{11}} \cdot q_{12}^{x_{21}v_{21}} \cdot q_{22}^{x_{22}v_{21}} = a_{21}, \\ q_{11}^{x_{21}v_{12}} \cdot q_{21}^{x_{22}v_{12}} \cdot q_{12}^{x_{21}v_{22}} \cdot q_{22}^{x_{22}v_{22}} = a_{22}. \end{cases} \tag{13}$$

At the first sight it seems that the problem of finding any $X = \{x_{ij}\}$ and $V = \{v_{ij}\}$ can be performed by applying a discrete logarithm function to all equations in (13). This is known as discrete logarithm problem (DLP). If it is the case then due to Fermat's theorem we obtain a system of multivariate quadratic (MQ) equations over the ring. As it is known [18, 19] the solution of MQ system is NP-complete over any field. We can assume that MQ system solution over the ring is no less complex since the arithmetic operations in the ring are more complex since not all elements have their inverses.

But, since MPF system is defined over non-cyclic group, there are no generators in this group and hence to apply a discrete logarithm is impossible. So we must deal with a system (13) as it is.

Then the problem how to find mutually commuting matrices in another way remains open. We don't know yet how to formulate this new problem to try to find matrices X, V (or U, Y) in the set of images of Burau representation of braid groups. To solve this problem, we must know how to recover the braid word having its Burau image. So far we don't know any means on how to solve this problem.

Implementation and determination values

As we said before matrix set M is over some finite non-cyclic group G. Suggested group G is Z_{21}^*. This group has 12 elements. Also it has cyclic subgroups at most of 6-th order. Seeing that for group Z_{21}^* we don't need powers greater than 6 we define $p = 7$ and field F is Z_7. Field Z_7 is considered because all its elements can be encoded with 3 bits and using almost all possible bit combinations.

We perform secure key values determination using the analogy with MQ problem. According to our conjecture cryptanalysis of equations of proposed KAP is not less complex that of the MQ problem represented by similar number of equations and variables. Moreover it seems a far more complex problem according to consideration presented in previous section.

In [20] it is stated that it is impossible to solve MQ problem of equally defined equations with more than 80 variables. In our case if the DLP would be solved one would obtain under-defined MQ problem which is considered even harder to solve. Keeping this in mind we choose $n = 10$ in which case matrices would be of the 9-th order and obtainable MQ problem would have 81 equations.

Private keys used by two parties are 243 bit long. Public key lengths depend on the number of generators of the centralizer what we are able to find. Public key lenghts and are presented in Table 1.

Table 1. Public key lengths

Number of generators	Public key length
2	486
3	729
4	972
5	1215
6	1458

Further investigations are required to determine the length of braid words used in 1-st step of the protocol.

We consider the protocol's implementation in ordinary 8-bits microprocessor.

Implementing the protocol for operations in group Z_{21}^* and field Z_7 variables of 8 bits are more then enough. To speed up the algorithm we can pre-compute tables of values of multiplication and exponentiation and store them in memory [21]. To look-up the values in these tables the algorithm implemented in assembly requires to perform only simple multiplications used to compute the locations in tables. Total count of multiplications is 5994.

To compare our KAP to classical algorithms of DH and ECDH we used data from [22]. There elliptic curve cryptography (ECC) is compared to RSA on 8-bit Atmel ATmega128 processor clocked at 8 MHz. ECC is implemented with 160, 192 and 224 bit keys. ECC-160 provides comparable security to RSA-1024 and ECC-224 provides comparable security to RSA-2048 and DH-2048. By recommendations of [23] the suggested exponent of DH-2048 is 320 bits. Assuming exponentiations time is linear to exponents bit size and knowing RSA-2048 execution time with public key $2^{16} + 1$ (17 bits) we say that DH-2048 should take at least about 19 times longer. After evaluating operations in our KAP when calculating keys using MPF we expect that on the stated processor execution time would be about 7ms. Detailed comparison date is shown in Table 2.

Table 2. Comparison of KAPs execution times

Algorithm	Execution time in seconds
ECC-160	0.81
ECC-192	1.24
ECC-224	2.19
RSA-2048 public key 2^{16}+1	1.94
DH-2048	~37
Our KAP	~0.007

Conclusions

In this paper we present new KAP using matrix power function which is some matrix (semi)group S action on a matrix set M. We showed that inversion of so defined

MPF has some indications to be NP-complete. Hence the security of presented KAP relies on the complexity conjectured of NP-complete problem.

The comparison results with known KAPs are presented and show a considerable computation time reduction in about 100 times compared to DH and ECDH. It shows that our KAP can be effectively realized in low-cost restricted computational environments such as microprocessors and embedded systems, e.g. in 8-bits microcontrollers.

References

1. **Toldinas J., Štuikys V., Damaševičius R., Ziberkas G., Banionis M.** Energy Efficiency Comparison with Cipher Strength of AES and Rijndael Cryptographic Algorithms in Mobile Devices // Electronics and Electrical Engineering. – Kaunas: Technologija, 2011. – No. 2(108). – P. 11–14. http://dx.doi.org/10.5755/j01.eee.108.2.134.
2. **Dumčius A., Gužauskas N.** Data Encryption System Overview // Electronics and Electrical Engineering. – Kaunas: Technologija, 2002. – No. 1(36). – P. 48–51.
3. **Diffie W., Hellman M.** New Directions in Cryptography // IEEE Transaction on Information Theory. – IEEE, 1976. – Vol. IT–22. – P. 644–654.
4. **Miller V.** Use of elliptic curves in cryptography // Advances in Cryptology, CRYPTO 85, LNCS. – Springer–Verlag, 1985. – Vol. 218. – P. 417–426.
5. **Koblitz N.** Elliptic curve cryptosystems // Mathematics of Computation. – American Mathematical Society, 1987. – Vol. 48. – P. 203–209.
6. **Sidelnikov V., Cherepnev M., Yaschenko V.** Systems of open distribution of keys on the basis of noncommutative semigroups // Doklady Mathematics. – Russian Academy of Sciences, 1993. – Vol. 48(2). – P. 384–386.
7. **Anshel I., Anshel M. and Goldfeld D.** An algebraic method for public–key cryptography // Mathematical Research Letters. – International Press, 1999. – Vol. 6. – P. 287–291.
8. **Ko K. H., Lee S. J., Cheon J. H., Han J. W., Kang J. S., Park C.** New Public–key Cryptosystem Using Braid Groups // Advances in Cryptology, CRYPTO 2000, LNCS. – Springer–Verlag, 2000. – Vol. 1880. – P. 166–183.
9. **Shpilrain V., Ushakov A.** A new key exchange protocol based on the decomposition problem. – 2005. – 7 p. Online: http://eprint.iacr.org/2005/447/.
10. **Shpilrain V., Ushakov A.** The conjugacy search problem in public key cryptography: unnecessary and insufficient, 2004. – 5 p. Online: http://eprint.iacr.org/2004/321/.
11. **Sakalauskas E.** One Digital Signature Scheme in Semimodule over Semiring // Informatica. – Lithuanian Academy of Sciences, 2005. – Vol. 16. – P. 383–394.
12. **Sakalauskas E., Tvarijonas P., and Raulinaitis A.** Key Agreement Protocol (KAP) Using Conjugacy and Discrete Logarithm Problems in Group Representation Level // Informatica. – Lithuanian Academy of Sciences, 2007. – Vol. 18. – P. 115–124.
13. **Artin E.** Theory of braids // Annals of Mathematics. – Princeton University, 1946. – Vol. 48. – P. 101–126.
14. **Franco N., González–Meneses J.** Computation of centralizers in braid groups and Garside groups // Revista Matemática Iberoamericana. – European Mathematical Society, 2003. – Vol. 19. – P. 367–384.
15. **Birman J. S., Brendle T. E.** Braids: A survey. – 2004. – 91 p. Online: http://arxiv.org/pdf/math/0409205v2.
16. **Sakalauskas E., Lukšys K.** Matrix Power S–Box Construction. – 2007. – 10 p. – Online: http://eprint.iacr.org/2007/214.
17. **Sakalauskas E., Listopadskis N., Tvarijonas P.** Key agreement protocol (KAP) based on matrix power function // Advanced Studies in Software and Knowledge Engineering. – ITHEA, 2008. – No. 4. – Vol. 2. – P. 92–96.
18. **Garey M., Johnson D.** Computers and Intractability: a Guide to the Theory of NP–Completeness. – W. H. Freeman and Company, New York, 1979. – 340 p.
19. **Patarin J., Goubin L.** Trapdoor One–Way Permutations and Multivariate Polynomials // Information and Communications Security, LNCS. – Springer, 1997. – Vol. 1334. – P. 356–368.
20. **Faugere J.–C., Joux A.** Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems Using Grobner Bases // Crypto 2003, LNCS. – Springer, 2003. – Vol. 2729. – P. 44–60.
21. **Damaševičius R., Štuikys V., Toldinas J.** Embedded Program Specialization for Multiple Criteria Trade–offs // Electronics and Electrical Engineering. – Kaunas: Technologija, 2008. – No. 8(88). – P. 9–14.
22. **Gura N., Patel A., Wander A., Eberle H., Shantz S. C.** Comparing Elliptic Curve Cryptography and RSA on 8–bit CPUs // Cryptographic Hardware and Embedded Systems, LNCS. – Springer, 2004. – Vol. 3156. – P. 119–132. http://dx.doi.org/10.1007/978-3-540-28632-5_9.
23. **Kivinen T., Kojo M.** More Modular Exponential (MODP) Diffie–Hellman groups for Internet Key Exchange (IKE). – 2003. – 11 p. Online: http://www.ietf.org/rfc/rfc3526.

Received 2011 06 07
Accepted after revision 2011 10 10

P. Vitkus, E. Sakalauskas, N. Listopadskis, R. Vitkiene. Microprocessor Realization of Key Agreement Protocol based on Matrix Power Function // Electronics and Electrical Engineering. – Kaunas: Technologija, 2012. – No. 1(117). – P. 33–36.

Key agreement protocol (KAP) using Burau braid groups representation and matrix power function (MPF) is presented. MPF is based on matrix semigroup action on some matrix set. All matrices are defined over finite field or ring. These functions pretend to be one-way functions since they are linked with multivariate quadratic (MQ) problems over some field. It is known that MQ problems are NP-complete over any field. We show that cryptanalysis of equations of our KAP is not less complex than those of MQ problem and moreover they seem far more complex. The one of advantages of proposed KAP is its effective realization in restricted computational environments by avoiding arithmetic operations with big integers. Bibl. 23, tabl. 2 (in English; abstracts in English and Lithuanian).

P. Vitkus, E. Sakalauskas, N. Listopadskis, R. Vitkienė. Raktų apsikeitimo protokolo, paremto matricų laipsnio funkcija, realizacija mikroprocesoriuose // Elektronika ir elektrotechnika. – Kaunas: Technologija, 2012. – Nr. 1(117). – P. 33–36.

Pateiktas raktų apsikeitimo, naudojant braid grupių Burau vaizdavimą ir matricų laipsnio funkciją (MLF), protokolas (RAP). MLF yra paremta matricų pusgrupės veiksmu su tam tikra matricų aibe. Visos matricos yra nusakytos baigtiniais laikais ir žiedais. Tokias funkcijas galima vadinti vienkryptėmis, nes jos yra susijusios su kelių kintamųjų kvadratinių lygčių sistemos sprendimo uždaviniu tam tikrame lauke. Yra žinoma, kad bet kuriame lauke uždavinys yra NP pilnasis. Mūsų nuomone, pateikto RAP kriptografinė analizė yra ne tokia sudėtinga kaip kelių kintamųjų kvadratinių lygčių sistemos uždavinio sprendimas. Ši analizė gali būti daug sudėtingesnė. Vienas iš pateikto RAP pranašumų yra tas, kad jį galima efektyviai naudoti ribotų skaičiavimo išteklių aplinkose, nes yra išvengiama aritmetinių operacijų su dideliais sveikaisiais skaičiais. Bibl. 23, lent. 2 (anglų kalba; santraukos anglų ir lietuvių k.).