Lietuvos matematikos rinkinys
Proc. of the Lithuanian Mathematical Society, Ser. A
Vol. **53**, 2012, 135–140

ISSN 0132-2818
www.mii.lt/LMR/

Security analysis of key agreement protocol based on matrix power function

Paulius Vitkus, Eligijus Sakalauskas

Department of Applied Mathematics, Kaunas University of Technology
Studentų str. 50, LT-51368 Kaunas
E-mail: paulius.vitkus@ktu.lt, eligijus.sakalauskas@ktu.lt

Abstract. Key agreement protocol (KAP) using Burau braid groups representation and matrix power function (MPF) is analyzed. MPF arguments are Burau representation matrices defined over finite field or ring. It is shown that KAP security relies on the solution of matrix multivariate quadratic system of equations over the ring with additional commutation constraints for matrices to be found. We are making a conjecture that proposed KAP is a candidate one-way function since its inversion is related with the solution of known multivariate quadratic problem which is NP-complete over any field. The one of advantages of proposed KAP is its possible effective realization even in restricted computational environments by avoiding arithmetic operations with big integers.

Keywords: cryptography, key agreement protocol, multivariate quadratic problem, one-way function.

1 Introduction

In general key agreement protocol (KAP) allows two or more parties negotiate a common secret key using insecure communications. Traditional KAPs are time consuming especially in restricted computational environments since they require arithmetical operations with big integers. They are based on the discrete exponent function and there security relies on the difficulty of solving discrete logarithm problem (DLP). In [12] it was shown that DLP is solvable by quantum algorithms in polynomial time both in the case of numerical cyclic groups and elliptic curve groups.

In 1993 new ideas appeared in asymmetric cryptography [15] – using known hard computational problems in infinite non-commutative groups instead of hard number theory problems such as discrete logarithm or integer factorization problems.

Nevertheless, [13] 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 [8, 11]. 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.

In this paper we present security analysis of KAP proposed in [16]. It is based on the centralizer's application in braid groups presentation level using Burau repre-

sentation and MPF. KAP based on braid groups as platform groups in presentation level using centralizers is also presented in [14].

Our proposed KAP is using matrix power function which is some matrix (semi)-group $\boldsymbol{S}$ action on a matrix set $\boldsymbol{M}$. The set $\boldsymbol{M}$ is not specified as a closed set with respect to some internal operation. Both $\boldsymbol{S}$ and $\boldsymbol{M}$ are defined over two different algebraic structures. $\boldsymbol{S}$ is defined over some finite ring $\boldsymbol{R}$ and $\boldsymbol{M}$ over some finite (semi)group $\boldsymbol{G}$. We will show that inversion of so defined MPF has some indications to be a hard problem and hence it can be a candidate one-way function (OWF). The security of presented KAP relies on the complexity of inversion of this OWF.

2 Mathematical backgroud

For our construction we consider infinite non-commutative general Artin braid group [5]. Given an integer $n \geqslant 2$, the braid group on n strands, B_n, is defined by following presentation:

$$B_n = \left\langle e, \sigma_1, \ldots, \sigma_{n-1} \;\middle|\; \begin{array}{ll} \sigma_i\sigma_j = \sigma_j\sigma_i, & |i-j| \geqslant 2 \\ \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}, & 1 \leqslant i \leqslant n-2 \end{array} \right\rangle.$$

How to generate random words in braid group B_n is explained in [4].

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 it by $C(x) = \{\gamma_1, \ldots, \gamma_k\}$ 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 [2]. For security reasons of our protocol we claim that $k \geqslant 2$.

Our protocol is based on braid group reduced Burau representation [5]. To transform braid groups to matrix groups we denote representation by $\beta : B_n \to GL(n-1, Z_m)$ as follows:

$$\sigma_i \mapsto I_{i-2} \oplus \begin{pmatrix} 1 & t & 0 \\ 0 & -t & 0 \\ 0 & 1 & 1 \end{pmatrix} \oplus I_{n-i-2}.$$

Where $\oplus$ is a direct matrix sum and t is an integer in Z_m. Hence, our matrix group $\boldsymbol{S}$ corresponds to $GL(n-1, Z_m)$ and the finite ring $\boldsymbol{R}$ is Z_m.

Matrix power function is defined using left and right $\boldsymbol{S}$ action on $\boldsymbol{M}$ [9, 10]. Let $X, Y \in \boldsymbol{S}$ and $Q \in \boldsymbol{M}$. Also all matrices are square and are of order r. Then left matrix X action on matrix Q yields matrix $A = {}^{X}Q$. The elements $\{a_{ij}\}$ of matrix A are computed by formula:

$$a_{ij} = \prod_{k=1}^{r} q_{kj}^{x_{ik}}. \tag{1}$$

Analogously the right matrix Y action on matrix Q can be defined yielding the matrix $B = Q^{Y}$ with elements $\{b_{ij}\}$ satisfying formula:

$$b_{ij} = \prod_{k=1}^{r} q_{ik}^{y_{kj}}. \tag{2}$$

MPF is defined by both left and right actions in the following way

$$ {}^{X}Q^{Y} = D. $$

In [9, 10] the following properties of MPF are proven:

$$ {}^{XY}Q = {}^{(XY)}Q = {}^{X}\big({}^{Y}Q\big), \tag{3} $$

$$ Q^{XY} = Q^{(XY)} = \big(Q^{X}\big)^{Y}, \tag{4} $$

$$ {}^{X}Q^{Y} = \big({}^{X}Q\big)^{Y} = {}^{X}\big(Q^{Y}\big). \tag{5} $$

3 Protocol

Let the protocol be executed between two parties – Alice and Bob.

1. Parties agree on the following public parameters: braid group B_n of order n, finite ring $\boldsymbol{R}$, finite (semi)group $\boldsymbol{G}$, element $t \in \boldsymbol{R}$ and matrix $Q \in \boldsymbol{M}$ of the $(n-1)$-th order.

2. Alice randomly generates braid group word $x \in B_n$. After calculating $C(x)$, $X = \beta(x)$ and $C(X) = \beta(C(x))$ 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 $C(y)$, $Y = \beta(y)$ and $C(Y) = \beta(C(y))$ 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.

$$ K_a = {}^{X}Q^{V}. \tag{6} $$

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

$$ K_b = {}^{U}Q^{Y}. \tag{7} $$

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

$$ K = {}^{X}K_b^{V} = {}^{XU}Q^{YV} = {}^{UX}Q^{VY} = {}^{U}K_a^{Y}. \tag{8} $$

4 Security analysis

To compromise the secret key K one must find any matrices X, V in (6) or U, Y in (6) satisfying commutation identities

$$ XU = UX \quad \text{and} \quad YV = VY \tag{9} $$

for given instances Q, K_a and Q, K_b respectively. Let us consider the case of finding such matrices X, V in (6). 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 (6) is written in a form of system of equations for the matrices of second order, i.e. when $n = 3$ $(r = 2)$:

$$ \begin{cases} q_{11}^{x_{11}v_{11}} \cdot q_{21}^{x_{12}v_{11}} \cdot q_{12}^{x_{11}v_{21}} \cdot q_{22}^{x_{12}v_{21}} = a_{11} \\ q_{11}^{x_{11}v_{12}} \cdot q_{21}^{x_{12}v_{12}} \cdot q_{12}^{x_{11}v_{22}} \cdot q_{22}^{x_{12}v_{12}} = a_{12} \\ q_{11}^{x_{21}v_{11}} \cdot q_{21}^{x_{22}v_{11}} \cdot q_{12}^{x_{21}v_{21}} \cdot q_{22}^{x_{22}v_{21}} = a_{21} \\ q_{11}^{x_{21}v_{12}} \cdot q_{21}^{x_{22}v_{12}} \cdot q_{12}^{x_{21}v_{22}} \cdot q_{22}^{x_{22}v_{12}} = a_{22}. \end{cases} \tag{10} $$

We will show that in our case solving (10) type system of equations is equivalent to solving matrix equation

$$X\tilde{Q}V = \tilde{A}, \tag{11}$$

that can be written in a form of system of multivariate quadratic (MQ) equations which we name further as the matrix MQ (MMQ) problem.

It is obvious that if we apply a discrete logarithm function to all equations in (10), then in the case if $\boldsymbol{G}$ is a cyclic group and due to Fermat's theorem we obtain a system of multivariate quadratic (MQ) equations (11).

Let us consider algebraic structures $\boldsymbol{R}$ and $\boldsymbol{G}$. They both must be commutative in order for MPF to satisfy (3), (4) and (5) properties. If $\boldsymbol{R}$ is finite ring Z_m then m must be equal to the highest order of elements in $\boldsymbol{G}$. Then the elements in matrix Q will be raised by every possible power.

Let $\boldsymbol{G}$ be non-cyclic group. It is known that every finite abelian group can be expressed as a direct sum of additive cyclic subgroups [7]. This allows us to transform (10) type system to the several corresponding (11) type equations. This way we obtain more equations but with the same amount of variables.

We don't know how to construct MMQ equations directly when algebraic structure $\boldsymbol{G}$ is a semigroup. But it is known that every finite semigroup has a minimal ideal which is a group [1]. Then matrix Q would have to have at least one element from semigroups $\boldsymbol{G}$ minimal ideal $\boldsymbol{I}$. In this case from equations (1) and (2) it is obvious that protocol matrixes K_a, K_b and K will consist only from elements from group $\boldsymbol{I}$. The attacker posing as Bob and knowing matrixes K_a, K_b and K can transform matrix equation (6) to matrix MQ system of equations and try to find Alice's matrices X and V in the same way as we earlier discussed in the case of groups.

Hence the security of proposed KAP relies on the complexity of solution of matrix MQ problem. We can expect that this problem is easier then randomly generated MQ problem which is NP-complete [3, 6]. But we can make a conjecture that matrix MQ problem together with additional constraints of commutation (9) is a hard problem.

So far we haven't found the complexity status of (11) equation over the finite field. Moreover we haven't found results concerning the complexity proof of (11) together with commutation constraints (9).

5 Conclusions

In this paper we present security analysis of KAP using matrix power function defined over the Burau image of infinite non-commutative braid group.

We showed that cryptanalysis of proposed KAP is based on the solution of matrix multivariate quadratic (MQ) system of equations over the ring with additional constrain equations represented by matrix commutation equation. Hence we are making a conjecture that the system of matrix MQ equations together with commutation equations is a candidate one-way function.

Possible choices of underlying algebraic structures are also discussed. This will lead to effective realization even in restricted computational environments. Because our KAP is not based on DLP and underlying algebraic structures can be small.

References

[1] A.H. Clifford and G.B. Prestom. *The Algebraic Theory of Semigroups,* vol. 1. American Mathematical Society, 1977.

[2] N. Franco and J. Gonzalez-Meneses. Computation of centralizers in braid groups and Garside groups. *Rev. Mat. Iber.*, **19**:367–384, 2003.

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

[4] V. Gebhardt and J. Gonzalez-Meneses. Generating random braids, pp. 1–22, 2011. Available from Internet: http://arxiv.org/abs/1112.5485.

[5] C. Kassel and V. Turaev. *Braid Groups.* Springer, 2010.

[6] J. Patarin and L. Goubin. Trapdoor one-way permutations and multivariate polynomials. *Inf. Comm. Sec.*, **1334**:356–368, 1997.

[7] S. Roman. *Fundamentals of Group Theory: An Advanced Approach.* Birkhäuser, 2012.

[8] E. Sakalauskas. One digital signature scheme in semimodule over semring. *Informatica*, **15**:383–394, 2005.

[9] E. Sakalauskas, N. Listopadskis and P. Tvarijonas. Key agreement protocol (KAP) based on matrix power function. *Adv. Stud. Softw. Knowl. Eng.*, **2**(4):92–96, 2008.

[10] E. Sakalauskas and K. Lukšys. Matrix power S-box construction, pp. 1–10, 2007. Available from Internet: http://eprint.iacr.org/2007/214.

[11] E. Sakalauskas, P. Tvarijonas and A. Raulinaitis. Key agreement protocol (KAP) using conjugacy and discrete logarithm problems in group representation level. *Journal*, **18**:115–124, 2007.

[12] P. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comp.*, **26**(5):1484–1509, 1997.

[13] V. Shpilrain and A. Ushakov. The conjugacy search problem in public key cryptography: unnecessary and insufficient, pp. 1–5, 2004. Available from Internet: http://eprint.iacr.org/2004/321/.

[14] V. Shpilrain and A. Ushakov. A new key exchange protocol based on the decomposition problem, pp. 1–7, 2005. Available at: http://eprint.iacr.org/2005/447/.

[15] V. Sidelnikov, M. Cherepnev and V. Yaschenko. Systems of open distribution of keys on the basis of noncommutative semigroups. *Dokl. Math.*, **48**(2):384–386, 1993.

[16] P. Vitkus, E. Sakalauskas, N. Listopadskis and R. Vitkienė. Microprocessor realization of key agreement protocol based on matrix power function. *Electr. Electr. Eng.*, **117**(1):33–36, 2012.

REZIUMĖ

Raktų apsikeitimo protokolo, paremto matricinio laipsnio funkcija, saugumo analizė

P. Vitkus, E. Sakalauskas

Analizuojamas raktų apsikeitimo protokolas (RAP) naudojant braid grupių Burau vaizdavimą ir matricų laipsnio funkciją (MLF). MLF argumentai yra Burau vaizdavimo matricos, sudarytis iš baigtinio lauko ar žiedo elementų. Parodyta, kad RAP saugumas yra paremtas matricinės kelių kintamųjų kvadratinių lygčių sistemos sprendimo uždaviniu tam tikrame žiede. Ieškomoms matricoms taip pat yra taikomi papildomi komutatyvumo apribojimai. Teigiama, kad pasiūlytas RAP yra galima vienkryptė funkcija, nes jos apvertimas yra susijęs su kelių kintamųjų kvadratinių lygčių sistemos sprendimo uždaviniu. Šis uždavinys yra NP pilnasis bet kuriame lauke. Vienas iš pateikto

RAP privalumų yra tas, kad jį galima efektyviai realizuoti net ribotų skaičiavimo resursų aplinkose išvengiat aritmetinių operacijų su dideliais sveikaisiais skaičiais.

Raktiniai žodžiai: kriptografija, raktų apsikeitimo protokolas, kelių kintamųjų kvadratinių lygčių sistema, vienkryptė funkcija.