INFORMATICA, 2007, Vol. 18, No. 1, 115–124

Key Agreement Protocol (KAP) Using Conjugacy and Discrete Logarithm Problems in Group Representation Level

Eligijus SAKALAUSKAS, Povilas TVARIJONAS,
Andrius RAULYNAITIS

Kaunas University of Technology, Department of Applied Mathematics
Studentų 50-327, 51368 Kaunas, Lithuania
e-mail: eligijus.sakalauskas@ktu.lt

Received: May 2006

Abstract. The key agreement protocol based on infinite non-commutative group presentation and representation levels is proposed.

Two simultaneous problems in group representation level are used: the conjugator search problem (CSP) and modified discrete logarithm problem (DLP). The modified DLP in our approach is a matrix DLP and is different from that's used in other publications. The algorithm construction does not allow to perform a crypto-analysis by replacing the existing CSP solution to the decomposition problem (DP) solution.

The group presentation level serves for two commuting subgroups and invertible group's word image matrix construction. The group representation level allows reliable factors disguising in the initial word. The word equivalence problem (WEP) solution is transformed from the group presentation level to the group representation level. Hence there are not necessary to solve WEP in the group presentation level and hence there are no restrictions on the group complexity in this sense. The construction of irreducible representation of group is required. The presented protocol is a modernization of protocol declared in (Sakalauskas *et al.*, 2005).

Key words: key agreement protocol, conjugator search problem, discrete logarithm problem, group representation.

1. Introduction

New ideas in public key cryptography using infinite non-commutative groups and semigroups appeared in (Sidelnikov *et al.*, 1993). In the case of group, the main idea is based on two of three known problems, declared by M. Dehn in 1910 and related with an infinite non-commutative group $(G, \cdot)$.

1. Word equivalency problem (WEP). For given two words $\omega_1, \omega_2 \in G$ decide if

$$\omega_1 \cdot \omega_2^{-1} = 1 \in G.$$

2. Conjugator search problem (CSP). For given $\mu, \theta \in G$ find $\alpha \in G$, that satisfies relation

$$\mu = \alpha \cdot \theta \cdot \alpha^{-1}.$$

So far these problems are the main ones in the cryptographic protocols construction (including KAP) using infinite non-commutative group presentation level.

In general, the main cryptographic protocols are based on two main requirements: firstly the WEP solution must be performed algorithmically efficiently and secondly CSP solution must be intractable. For the basic group the additional requirement is that two mutual commutative subgroups must be easily determined.

During the last decade the concrete realizations of cryptosystems, that meet these requirements, were developed using braid groups. The reason of the interest concerning the braid groups is that WEP has an effective solution algorithm, i.e., it has a polynomial time complexity. The running time is quadratic with respect to the braid index. This is achieved by words' transformation to the left weighted canonical form. On the other hand there is no known deterministic solution of CSP in polynomial time yet. But this fact automatically does not mean the reliable security of that kind algorithms. The additional requirement of two mutually commutative subgroups construction is easy satisfied in braid groups.

The new cryptosystem using braid groups is presented in (Ko *et al.,* 2000). Its security is based on the complexity of CSP.

As it was pointed out in (Shpilrain and Ushakov, 2004) the intractability of CSP is not a necessary condition for a KAP security in (Ko *et al.*, 2000) algorithm. Considering the crypto-analysis of this algorithm it was found that the original CSP can be reduced to the other problem, which seems to be easier (Shpilrain and Ushakov, 2004). This problem is called a decomposition problem (DP), and can be formulated as follows: for given $\mu, \theta \in G$, find any α', $\beta' \in G_1 \subset G$, that satisfies relation

$$\mu = \alpha' \cdot \theta \cdot \beta'.$$

Beside the CSP reducibility to the DP the presented algorithm is also vulnerable to so-called "length-based" attack (Hughes and Tannenbaum, 2002).

Hence, according to Shpilrain and Ushakov the security of cryptosystems based on the single CSP seems to be insufficient. On the other hand the solution of SCP is also unnecessary since it can be replaced by the decomposition problem.

The other example of cryptosystem using infinite non-commutative group was presented in (Anshel *et al.*, 1999). The security of this algorithm relies on two hard problems. The first one is the simultaneous multiple CSP. The second one is the membership problem. Despite the opinion that simultaneous multiple CSP is easier than single CSP, it is reckoned that membership problem in braid groups is very hard. According to (Shpilrain and Ushakov, 2004), even if a polynomial time deterministic algorithm would be found for solving CSP in, say, braid groups, this will not be sufficient to break the (Anshel *et*

al., 1999) protocol by a deterministic attack since, in addition, this algorithm is supported by additional hard problem, i.e., membership problem.

In general, the problem of cryptosystem construction, based on the infinite non-commutative group, is to hide factors α and α^{-1} or α' and β' in the word μ (Shpilrain and Ushakov, 2004). This problem is also actual in approach presented in (Anshel *et al.*, 1999) for braid groups. Hence, it is desirable that the cryptosystem construction based on the infinite non-commutative group presentation level would be based not only on the intractability of CSP, but at the same time on some other infeasible problem in addition.

This opinion is confirmed by the latest publication (Shpilrain and Ushakov, 2005). The presented KAP lies also on the group presentation level and seems to be interesting since the one of two commuting subgroup is hidden. This approach uses the CSP, the centralizer's calculation of some subgroup and the word membership to the subgroup generated by certain word problem.

In this study we propose to use two infinite non-commutative group attributes: its presentation and representation levels. Using the similar ideas the digital signature scheme was proposed in (Sakalauskas, 2005). We will follow the general ideas presented in (Sidelnikov *et al.*, 1993) expanding this approach to the group representation level.

We are not considering here the faithfulness of group representation, since for each sufficiently complex group it requires a very deep algebraic-topological investigation. Even in the case of braid groups the faithful representation was found only recently (Krammer, 2000). In this connection we only assume, that the chosen representation is complex enough to provide a very poor representation kernel, which does not significantly influence to the security of proposed algorithm. In the case of braid groups we choose the Burau representation in finite set matrix group over the Galois field.

The ideas to use the group representation level were declared in (Monico, 2002). The example of cryptosystem based on finite semigroup action problem is there presented. It is a multidimensional generalization of modular exponentiation using finite semigroup of matrices or ring of matrix polynomials over finite vector field. As a consequence the proposed semigroup action problem is a multi-dimensional generalization of the traditional (one-dimensional) DLP and seems to be harder. This cryptosystem is used for session key agreement protocol and ElGamal type encryption. According to the author, this cryptosystem requires further investigations and first of all secure key length needs to be determined. The author also pointed out, that a suitable algebraic system for cryptosystem realization is not found yet.

We are using two simultaneous problems in group representation level: the matrix CSP and matrix DLP ones. The DLP used in our approach is different from that used in the (Monico, 2002). The CSP itself in the group representation level does not provide a sufficient security but we reckon the entire security provided by both problems pretends to be sufficient. The algorithm construction does not allow the replacing of existing CSP to the DP solution.

The group presentation level serves for two commuting subgroups and inverted group word image matrix construction. The group representation level allows a reliable factors' disguising in the initial word. The WEP solution is transformed from the group presentation level to the group representation level. Hence it is not necessary to solve WEP in

the group presentation level and no restrictions on the group complexity are made. The presented protocol is a modernization of protocol declared in (Sakalauskas *et al.*, 2005).

The mathematical background in brief is presented in Section 2. The proposed KAP is described in Section 3. Section 4 provides some considerations on the security analysis issue. The discussions on realization of proposed algorithms are outlined in Section 5.

2. Mathematical Background

The main definitions used in this section could be found in (van der Waerden, 1967).

We consider an infinite non-commutative group $(G, \cdot)$, presented by finite set of generators $\gamma_1 ..., \gamma_n$ and relations $R_1, R_2 ..., R_l$ (Magnus *et al.*, 1966). This definition constitutes group G presentation level. As a suitable example, a braid group B_n can be choosed, where $n = k$ is the index of braid group (Ko *et al.*, 2000). Further we will also call the group G as basic group.

Let F be some field. Define m-dimensional vector space F^m over the field F. We shall consider F^m as a module, which will be denoted in the following by M.

By $Aut(M)$ we define a certain set of automorphisms $A\colon M \to M$. According to the definition, for each $A \in Aut(M)$ there exists $A^{-1} \in Aut(M)$ such that $AA^{-1} = A^{-1}A = I \in Aut(M)$, where I is an identity automorphism.

In general the representation of group G is some homomorphism $\varphi : G \to Aut(M)$. It is clear that $Aut(M) = GL(m, F)$, where $GL(m, F)$ is general linear group of all m-dimensional invertible matrices over F. Then for all $\alpha \in G$ there exists $A \in Aut(M)$ such that $\varphi(\alpha) = A$.

When m is finite we have a finite dimensional representation and when the homomorphism image is finite the finite image representation takes place. The latter occurs in the case when infinite group G is represented by finite group of matrices in $Aut(M)$.

Define two commutative subsets G_1 and G_2 in G. Assume that $\varphi(G_1) = Aut(M)_1$ and $\varphi(G_2) = Aut(M)_2$. Then if $A \in Aut(M)_1$ and $B \in Aut(M)_2$ the following commutative relation takes place

$$AB = BA.$$

The multiplication of any matrix $K \in Aut(M)$ with any element $a \in M$, which we denote by Ka, is defined using the arithmetical operations in the field F, which we denote, by Ka. This multiplication defines also a group G action on module M.

For further construction we will consider the Galois field $GF(2^k)$ (Menezes *et al.*, 1996) instead of abstract field F. Then the basic group G will be represented by m-dimensional matrices over $GF(2^k)$, or in other words, by matrices in $GL(m, GF(2^k))$.

3. Key Agreement Protocol

Consider two cryptographic entities Alice and Bob, which has two public elements $a \in M$ and $\theta \in G$. The elements θ and a can be considered also as a public key one of the parties.

The key agreement protocol is the following:

1. Alice chooses at random a secret element $\alpha \in G_1$. She forms a word

$$\omega_1 = \alpha \cdot \theta \cdot \alpha^{-1}.$$

2. Using homomorphism φ she obtains a matrix

$$U = \varphi(\omega_1) = \varphi(\alpha \cdot \theta \cdot \alpha^{-1}) = \varphi(\alpha) \cdot \varphi(\theta) \cdot \varphi(\alpha^{-1}) = AQA^{-1}.$$

   By choosing at random some secret natural number r, she calculates the matrix

$$R = U^r = (AQA^{-1})^r = AQ^rA^{-1},$$

   and sends R to Bob.
3. Bob chooses at random a secret element $\beta \in G_2$ and analogously forms a word

$$\omega_2 = \beta \cdot \theta \cdot \beta^{-1}.$$

4. Bob calculates

$$V = \varphi(\omega_2) = BQB^{-1}.$$

   By choosing at random some secret natural number s, he calculates the matrix

$$S = V^s = (BQB^{-1})^s = BQ^sB^{-1},$$

   and sends S to Alice.
5. Each party calculates the elements K_A and K_B respectively

$$K_A = AS^rA^{-1} = A(BQ^sB^{-1})^rA^{-1} = ABQ^{sr}B^{-1}A^{-1}, \tag{3.1}$$
$$K_B = BR^sB^{-1} = A(AQ^rA^{-1})^sB^{-1} = BAQ^{rs}A^{-1}B^{-1}. \tag{3.2}$$

The common secret key is $Ka = K_Aa = K_Ba$, since $AB = BA$ and $Q^{sr} = Q^{rs}$.

The motivation of group representation level application relies on the following aspects.

1. The representation level provides a good diffusion of group generators to disguise factors α, α^{-1} and β, β^{-1} in initial words ω_1 and ω_2 respectively. In the case of complicated groups without normal forms the disguising procedure can dramatically increase the length of transformed initial word. Moreover, as it is pointed out in (Shpilrain and Zapata, 2004) the amount of work needed to disguise a factors by using the defining relations is about the same as needed to recover an element from its disguised form.

2. The WEP solution from group presentation level is transformed to its solution in representation level. It is easy to perform this for every group having the representation. The accuracy of WEP depends on the amount of representation kernel elements. But we assume that the kernel is poor and that the probability of collision is negligible.
3. The group presentation is used to provide the existence of random chosen inverse matrices.

4. Security Analysis and Implementation

The security of proposed KAP relies on two simultaneous problems in group representation level: the matrix conjugator search problem (CSP) and matrix discrete logarithm problem (DLP).

Let us consider both these problems separately.

The matrix CSP can be formulated as follows: for given Q and R find the conjugator matrix A from the equation

$$R = AQA^{-1}.$$

The matrix CSP alone in matrix group $GL(m, F)$ does not provides a sufficient security since its solution can be performed in polynomial time. The unknown matrix A can be found by solving the following homogenous matrix equation

$$RA - AQ = 0.$$

The matrix DLP is to find r for given m-dimensional matrices Q and P, satisfying 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 matrix DLP can be splited to several l_i-dimensional matrix DLP where $l_1, \ldots, l_k$ are dimensions of corresponding k blocks. The complexity in this case corresponds to the complexity of k, l_i-dimensional matrix DLP. Hence it is required to build a matrix Q without lower dimension invariant spaces or in other words the irreducible representation of basic group must be used.

When we are considering the cryptanalysis of proposed KAP, we are facing with the following problem: find matrix A and natural r for given matrices R and Q satisfying relation

$$R = AQ^rA^{-1}. \tag{4.1}$$

Let us formulate and prove the proposition concerning the security of proposed KAP.

PROPOSITION 1. The security of KAP relies on the simultaneous solution of two hard problems: matrix conjugator search problems (CSP) and matrix discrete logarithm problem (DLP).

Proof. Let us try to split the solution of matrix CSP and matrix DLP separately trying to obtain the secret key either K_A or K_B as in (3.1), (3.2).

Let us construct the first attack by solving the CSP firstly. Since the matrix Q^r is not known due to the fact that r is unknown, we can choose the arbitrary natural number k and having matrix Q calculate the corresponding matrix

$$P = Q^k.$$

Then instead of (4.1) we have the following relation with known R and P

$$R = A'PA'^{-1}.$$

The matrix *A'* can be determined by solving matrix CSP in polynomial time. As a result, we obtain a matrix A' instead of A.

Then having A', S and k we can try to obtain the secret key

$$K_{A'} = A'S^kA'^{-1} = A'BQ^{sk}B^{-1}A'^{-1}.$$

But this cryptanalysis fails since $K_{A'} \neq K_A$.

In the similar way the compromising of K_A fails if we apply the second attack by trying to solve the matrix DLP at first step separately. Then by guessing some conjugator *A"* we can find r from the relation

$$A''^{-1}RA'' = Q^r,$$

having known R and Q. This problem corresponds to the matrix DLP and is conjectured to be hard since the classical DLP is reckoned hard. Even if r could be computed, the obtained key

$$K_{A''} = A''S^rA''^{-1} = A''BQ^{sr}BA''^{-1}$$

is not equal to the K_A from (3.1).

Hence we proved that both the matrix CSP and matrix DLP can not be solved separately avoiding a total scan. Nor A' neither A'' can provide a valid session key determination if they are not equal to the actual matrix A. Analogously the adversary must find the actual value r instead of choosing arbitrary value k.

We prove now that the CSP can not be replaced by the possible easier decomposition problem solution. Assume that in order to reduce the computation time in first attack the adversary is trying to choose the suitable matrices A_1, A_2 satisfying relation

$$R = A_1Q^kA_2 = A_1PA_2,$$

for some selected k. But this attempt fails since the calculated key

$$K_{12} = A_1 S^k A_2$$

does not equal to the K_A or K_B. Moreover in this case the main conjugation identity is also not valid, i.e., if $A_2 \neq A_1^{-1}$

$$(A_1 Q A_2)^s \neq A_1 Q^s A_2.$$

Hence the replacement of matrix CSP by matrix DP does not facilitate the attack.

As it is known, the classical DLP in cyclic group Z_p* (Menezes, 1996) is hard and the security of algorithms based on modular exponent, relies on it. It is sensible to expect that the complexity of DLP in matrix group $Aut(M)$ is more (or at least no less) complex than in Z_p* since for the transformation of matrix DLP to the multiple classical DLPs it is required to transform the matrix to the diagonal form. But this can not be performed if the basic group representation is irreducible.

The possible hardest DLP in matrix ring is introduced in (Monico, 2002). Hence we can conclude that the complexity of considered matrix DLP is intermediate between the DLP in Z_p* and possible hardest DLP declared in (Monico, 2002).

Taking into account that in our case the total complexity is composed by both matrix CSP and DLP, we can expect that proposed approach for KAP construction is promising.

Let the basic group be a braid group B_n of index n (Ko *et al.*, 2000), and $n = 32$. To code the 31 generator $\sigma_1 ..., \sigma_{31}$ and its inverses in B_{32}, the 6 bits is required. Assume the public element θ as a word in B_{32} can contain 128 generators in average. Then we have $6 \times 128 = 4096$ bits to code the parameter θ.

For the braid groups a faithful Krammer representation is known (Krammer, 2000). This representation is of order $n(n-1)/2 = 496$ and is comparatively complex to realize. Moreover, the faithfulness of basic group representation is not important since we will consider the finite image representation.

The other kind of representation is the Burau representation of order n (Long, 1994). This representation is not faithful for $n \geqslant 6$ and is defined by matrixes over the ring $Z[t, t^{-1}]$ (Long and Paton, 1993). The kernel and the image structure of this representation is unknown yet. In general, even to determine the kernel element is a very hard problem. Some kernel elements in Burau representation are known for $n = 5, 6$ (Turaev, 2000). The obtained kernel elements are very complex and do not facilitate the WEP solution in group representation level.

For a proposed KAP realization we can choose the modified irreducible Burau type representation. The irreducible Burau representation can be found in (Dian-Min Tong *et al.*, 1994). In this case B_n has the $(n-1)$-dimensional representation. Our modification relies on the substitution of representation matrices over the $Z[t, t^{-1}]$ with ones over the $GF(2^k)[t, t^{-1}]$. In this case we have a finite image, irreducible Burau representation by matrices in $GL((n-1),\ GF(2^k))$. Hence we have $m = n - 1 = 31$ and the module M is a vector space $GF^m(2^k)$ over $GF(2^k)$. According to (Birman *et al.*, 1992) the deeper investigation of finite image representations are probably very interesting.

Let $k = 64$. Then the public parameter $a \in GF^{31}(2^{64})$ and a can be coded by 1984 bits.

In total the public parameters θ and a can be coded by 4096 + 1984 = 6080 bits.

The storage requirement for the matrices used in KAP is $31 \times 31 \times 64 = 61504$ bits.

We have chosen these public parameters intuitively seeking to provide a better security than the other known KAP. In some recent cryptosystems using Diffie–Hellman KAP the modular exponent in Z_p* is computed for module p of order 2^{4096}. As we see the number expressed in 4096 bits is comparable with our one having 6080 bits.

We think 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.

We estimate now a computation time, required to perform the KAP.

To calculate the K_A and K_B the only matrix multiplications are required. The creation of matrices A and A^{-1} requires the 128 matrix multiplications each. These calculations are simple and can be produced in $\mathcal{O}(m)$ time algorithm. The same is valid for matrices B and B^{-1}. To compute the matrix K_A it is required $2 + r + 2 + s$ matrix multiplications in $\mathcal{O}(m^2)$ time. The key *Ka* calculation can be performed in $\mathcal{O}(m)$ time.

Hence the KAP realization has $\mathcal{O}(m^2)$ time complexity. This complexity has the same order as the complexity of modular exponent $\mathcal{O}(\lg p)$, when $m = 31$ and p is of order 2^{4096}.

References

Anshel, A., M. Anshel and D. Goldfeld (1999). An algebraic method for public-key cryptography. *Mathematical Research Letters*, **6**, 1–5.

Birman, J.S., D.D. Long and J.A. Moody (1992). Finite-dimensional representation of Artin's braid groups. *Contemporary Mathematics*, **169**, Amer. Math. Soc.

Hughes, J., and A. Tannenbaum (2002). Length based attacks for certain group based encryption rewriting system. In *Workshop SECI02 Securite de la Communication sur Internet*. Tunis, Tunisia.

Ko, K.H., S.J. Lee, J.H. Cheon, J.W. Han, J.-S. Kang and C. Park (2000). New public-key cryptosystem using braid groups. *Advances in Cryptology, Proc. Crypto 2000*, *LNCS*, **1880**. Springer-Verlag. pp. 166–183.

Krammer, D. (2000). Braid groups are linear. *Preprint*, Basel.
Available at: `www.math.unibas.ch`

Long, D. (1994). Constructing representations of braid groups. *Comm. Anal. Geom.*, **2**, 217–238.

Long, D., and M. Paton (1993). The Burau representation is not faithful for $n \geqslant 6$. *Topology*, **32**, 439–447.

Magnus, W., A. Karrass, D. Solitar (1966). *Combinatorial Group Theory*. Interscience Publishers, NY.

Menezes, A., P. van Oorschot and S. Vanstone (1996). *Handbook of Applied Cryptography*. CRC Press.

Monico, C. (2002). Semirings and semigroup actions in public-key cryptography. *PhD thesis*, University of Notre Dame.

Sakalauskas, E. (2005). One digital signature scheme in semimodule over semiring. *Informatica*, **16**(3), 383–394.

Sakalauskas, E., G. Dosinas, A. Dargis, K. Lukšys, A. Katvickis, (2005). Key agreement protocol (KAP) realization in Gaussian group presentation and action levels. *Information Technology and Control*, **1**(34).

Shpilrain, V., and G. Zapata (2004). Combinatorial group theory and public key cryptography.
Available at: `http://eprint.iacr.org/2004/242`

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

Shpilrain, V., and A. Ushakov (2005). A new key exchange protocol based on the decomposition problem. // Available at: http://eprint.iacr.org/2005/447

Sidelnikov, V., 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), 566–567.

D.-M. Tong, D.-M., S.-D. Yang and Z.-Q. Ma (1994). N-dimensional representations of the braid groups B_n. *Commun.Theor. Phys.*, **18**, 1–6.

Turaev, V. (1999). Faithful linear representations of the braid groups. In *Seminaire BOURBAKI*, 52 eme, annee, **878**.

van der Waerden, B.L. (1967). *Algebra*. Springer-Verlag.

E. Sakalauskas received PhD degree from Kaunas University of Technology in 1983. Currently he is an associate professor in Department of Applied Mathematics and a senior reseacher in Institute of Defence Technology in Kaunas University of Technology. The scope of scientific interests is a system theory, identification and cryptography. In these fields there were published about 50 papers. In recent time his research interest is focused mainly in the cryptography. There were obtained some results in the following fields: one way function construction based on the hard problems in infinite non-commutative groups representation level, digital signature schemes, key exchange protocols and pseudorandom number generation. The obtained recent research results in cryptography were published in 10 papers.

P. Tvarijonas is a lecturer at the Department of Applied Mathematics of Kaunas University of Technology, member of Mathematicians Society of Lithuania. In 1979 he graduated from Vilnius University. His scientific interests include probability theory and cryptography.

A. Raulynaitis is PhD student of informatics engineering of Kaunas University of Technology. His current research interests are cryptography and asymmetric ciphering algorithms.

Raktų apsikeitimo protokolas (RAP), panaudojant jungtinumo ir diskretinio logaritmo problemas grupės įvaizdžio lygmenyje

Eligijus SAKALAUSKAS, Povilas TVARIJONAS, Andrius RAULYNAITIS

Jungtinuko suradimo ir diskretinio logaritmo problemos yra apibrėžiamos begalinės nekomutatyvios grupės įvaizdžio lygmenyje ir yra panaudojamos raktų apsikeitimo protokolo (RAP) realizacijai. Pasiūlytas RAP turi didesnį kriptografinį saugumą nei kriptosistemos, paremtos diskretinio logaritmo problma, nes ši problema pakeičiama sunkesne matricinio diskrertinio logaritmo problema, ją sujungiant kartu su jungtinuko suradimo problema.