ISSN 1392 – 124X INFORMATION TECHNOLOGY AND CONTROL, 2005, Vol. 34, No. 1

KEY AGREEMENT PROTOCOL (KAP) REALIZATION IN GAUSSIAN GROUP PRESENTATION AND ACTION LEVELS

Eligijus Sakalauskas, Gediminas Dosinas, Arūnas Dargis, Kęstutis Lukšys, Artūras Katvickis, Andrius Raulynaitis

Kaunas University of Technology, Department of Applied Mathematics
Studentų st. 50-324, LT- 51368 Kaunas, Lithuania

Abstract. The method for a key agreement protocol (KAP) with application of a non-commutative group is presented. The method is based on the two one-way functions (OWFs) and corresponding hard problems. One hard problem is left right factors' search problem (LRFSP) in non-commutative group presentation level, and another one is a postulated hard problem in the non-commutative group representation level or, in other words, action level.

On the basis of LRFSP the first one-way function (OWF_1) is constructed.

Non-commutative group is treated as an endomorphic group of operators acting on a certain semimodule or module. In this case such semimodule is compatible with a non-commutative group and algebra generated by this non-commutative group. The requirements of semimodule compatibility to the introduced algebra are presented. On the basis of a hard problem postulation in non-commutative group action level the second OWF_2 is constructed.

Key words: Key agreement protocol, one–way function, non-commutative group, module, semimodule.

1. Indroduction

New ideas in public key cryptography appeared in 1993 when Sidelnikov, Cherepnev and Yaschenko presented a realization of a key agreement protocol in infinite non-commutative group of general type (Sidelnikov *et al.*, 1993). The main idea was to use two types of recognized hard algorithmic problems in these groups for a one-way function (OWF) construction. One of the problem is a conjugator search problem (CSP) and the other one we named a left-right factors search problem (LRFSP). The LRFSP is a generalization of CSP, when the right factor in the word is not equal to the left factor with an opposite unit power.

In (Anshel *et. al*., 1999) the ideas presented in (Sidelnikov *et al.*, 1993) were formalized and some considerations about the application of braid groups is presented. Approximately in the same time in (Ko, *et. al*., 2000) the cryptosystem based on the conjugacy search problem (CSP) in braid groups appeared. In both sources the KAP was realized using the pure braid group formalism, *i. e.* so–called group presentation level (Magnus, *et. al*., 1966).

But according to the latest publication in (Shpilrain and Zapata, 2004) it is declared that the CSP in braid group is unlikely to provide sufficient level of security. In general, according to authors, using the theoretical group formalism, one faces the following natural questions, which we slightly reformulate below.

Q1. Is there a group, or class of groups, where the public key exchange protocol would be secure enough to be used in real-life applications?

Q2. Is there another "hard" problem in combinatorial group theory that can be used, instead of the conjugacy search problem, in a public key exchange protocol?

Q3. Can one efficiently disguise an element of a given group (or semigroup) by using relations?

According to authors, without a positive answer to at least one Q1 and Q2, it is unlikely that combinatorial group theory will have a significant impact on public key cryptography, which is now dominated by methods and ideas from number theory. They also pointed out that question Q3, which has not been getting sufficient attention so far, but likely to become a focus of the future research in public key cryptography based on symbolic computation.

We would like to present the positive answers to the questions Q1-Q3 joining the combinatorial group theory with a group representation theory or equivalently considering both group presentation and representation levels. The latter we will call the group action level.

As regarding Q1 we consider a non-commutative group since we reckon that the action level of this group can allow us to construct an effective OWF.

As regarding Q2 we propose to use the other problem instead of the CSP which we named a left right factors search problem (LRFSP) which is familiar to

declared one in (Sidelnikov, *et al.*, 1993). When using this problem, it is required to use the other related hard problem in the non-commutative group action level.

As regarding Q3 we will propose a disguise procedure of left and right factors in the group word using word reversing procedure (Dehornoy and Paris, 1999). The efficiency of this procedure is based on the complexity of used group which can be chosen as complex as possible because no restrictions on its complexity are taken into account.

The idea of group or semigroup action level application was declared in (Monico, 2002). The action is defined as an action of group or semigroup elements as operators in the particular vector space. In the group theory formalism the operators in the vector space call this action a group representation or more precisely homomorphic group representation.

In (Monico, 2002) an example of cryptosystem based on finite semigroup action problem (SAP) is 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 SAP is a multi–dimensional generalization of the traditional (one–dimensional) discrete logarithm problem (DLP) and is more hard. 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 pointed out also that a suitable algebraic system for cryptosystem realization is still not found except the ones mentioned in his paper.

We would like to present one solution based on the non-commutative group action on the certain module or semimodule. The general way to construct a cryptosystem using a sufficiently complicated and therefore secure algebraic system presented by the set of generators and relations (group, semigroup, ring, *etc.*) is to choose the system itself and to select a suitable module over this system. The algebraic system elements must be almost automorphic, *i. e.* endomorphic operators acting in a module. Then it can be said that the module and algebraic system are compatible. We present here the main compatibility requirements for algebraic systems and construct the KAP using this background.

2. Preliminaries

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

We consider some semimodule $(M, +)$ over the non-commutative group $(G, \cdot)$. According to the classical definition the module is an additive Abelian group over some set of operators. It is a generalization of vector space. Instead of a module we consider its generalization, *i. e.* semimodule M which is an additive Abelian semigroup. In our case we do not require that for any $m \in M$ there exists an unique element $(-m)$ such that

$$m + (-m) = 0 .$$

We assume only that there exists a zero element 0 such that

$$m + 0 = 0 + m = m.$$

So the semimodule M is an additive Abelian monoid.

We consider the Gaussian class atomic infinite non-commutative group G (Dehornoy and Paris, 1999). This group is treated as a set of endomorphic operators acting in semimodule M and is finitely presented by the set of generators called atoms and relations, *i. e.*

$$G = < \varepsilon_1 , \varepsilon_2 \ldots \varepsilon_n ; r_1 , r_1 \ldots, r_m > .$$

The latter definition constitutes a group G presentation level.

The set $\{ \varepsilon_1 , \varepsilon_2 \ldots \varepsilon_n \}$ is a set of atoms and $\{ r_{12} , r_{13} \ldots, r_m \}$ is a set of relations. This defines a non-commutative group presentation level.

Each element of G we call a word (Magnus, *et al.*, 1966). Every finite word $w \in G$ can be expressed as a product of atoms with a positive or negative unit power in the form

$$w = \varepsilon_i^{\pm 1} \cdot \varepsilon_j^{\pm 1} \ldots \cdot \varepsilon_k^{\pm 1} . \quad (1)$$

In general, word consists of either finite or infinite products of atoms. For each word w in G, there exists an inverse element w^{-1} satisfying the trivial group relation

$$w \cdot w^{-1} = w^{-1} \cdot w = 1_G,$$

where 1_G is the unity element (empty word) of the group.

Similarly to (Sakalauskas, 2003 - 2004) we define two mutually commutative subsets $S_1, S_2 \subset G$ such that

$$\alpha \cdot \beta = \beta \cdot \alpha ,$$

when $\alpha \in S_1, \beta \in S_2$.

According to Gaussian group definition, the monoid M_G associated with a Gaussian group G admits so–called right complement presentation (Dehornoy and Paris, 1999)

$$\varepsilon_i \cdot f(\varepsilon_j, \varepsilon_i) = \varepsilon_j \cdot f(\varepsilon_i, \varepsilon_j), \quad i, j \in I, \quad (2)$$

where I is an index set.

This presentation allows us to perform the following transformations in G

$$\varepsilon_i^{-1} \cdot \varepsilon_j = f(\varepsilon_j, \varepsilon_i) \cdot f(\varepsilon_i, \varepsilon_j)^{-1} ; \quad (3)$$

$$\varepsilon_j^{-1} \cdot \varepsilon_i = f(\varepsilon_i, \varepsilon_j) \cdot f(\varepsilon_j, \varepsilon_i)^{-1} , \quad (4)$$

which can be used for construction of our KAP. The latter transformations are used also for a reversing procedure as a tool to construct normal forms in Garside groups because it is proved that Garside groups are biautomatic groups (Dehornoy and Paris, 1999). This means that there exists a finite state automaton that computes the normal forms.

In the case of Gaussian groups it is unlikely that a general automaticity result holds for even particular groups, *i. e.* closed Gaussian groups. Hence the word problem solution is not available in these groups and, therefore, Gaussian groups can not be directly applied for the cryptographic primitive construction.

Let us consider some initial word w_0 consisting of left, middle and right factors, α, θ and β correspondingly:

$$w_0 = \alpha \cdot \theta \cdot \beta . \quad (5)$$

The reversing procedure corresponds to some reversing operator R which transforms any word w_0 to the word w_1 of the form

$$w_1 = u\, v^{-1} , \quad (6)$$

where u and v are positive words, *i. e.* consists of atoms with positive powers. Then w_1 is equivalent to w_0 which we denote as $w_1 \sim w_0$.

Then joining (5) and (6) we obtain

$$R(w_0) = w_1 = u \cdot v^{-1}. \quad (7)$$

We apply the reversing operator to construct the first OWF in the Gaussian group G presentation level based on the LRFSP, which we denote as OWF_1. We formulate now the corresponding hard problem in G.

Problem 1. Left – right factors' search problem (LRFSP): having $w, \theta \in G$, find any other words $\alpha', \beta' \in G$, satisfying equation

$$w = \alpha' \cdot \theta \cdot \beta' . \quad (8)$$

In the case when θ is known and $\beta = \alpha^{-1}$ we have a well-known conjugator search problem (CSP). During the decades there was proclaimed a computational difficulty of CSP in some particular groups, e.g. braid groups. The CSP has been used in some group-based cryptosystems, most notably in (Anshel, et al., 1999), (Ko et al., 2000). However according to the recent sources (Shpilrain, 2004) it is asserted now that the CSP in a braid group cannot provide sufficient level of security.

By treating G as a group of operators in module M we can define the group G representation level or, in other words, its action level. So the non-commutative group G has its presentation and action levels.

One kind of algebraic systems' action level is presented in (Monico, 2002). There is an example of cryptosystem based on the finite semigroup action problem (SAP). On the base of this problem the OWF is postulated. It is a multidimensional generalization of modular exponentiation. The semigroup is defined as a semigroup of matrices. The ring of matrix polynomials over finite vector field is also useful for this technique. As a consequence the proposed SAP is a multi–dimensional generalization of traditional (one–dimensional) discrete logarithm problem (DLP) and is more hard than the prototype. 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.

According to the assumption that the group G is a group of endomorphic operators acting in M, this means that to all $\alpha \in G$ corresponds some function α: $M \to M$ and for all $a \in A$ there exists some $b \in A$ such that the following relation takes place

$$\alpha (a + b) = \alpha (a) + \alpha (b). \quad (9)$$

For further considerations we introduce some action operation (function) denoted by $\circ$ and providing a mapping $\circ : G \times M \to M$. Then the expression $\alpha(a)$ can be replaced by the equivalent expression $\alpha \circ a$, and the last equation can be rewritten in the form

$$\alpha \circ (a + b) = (\alpha \circ a) + (\alpha \circ b) = \alpha \circ a + \alpha \circ b . \quad (10)$$

This means that according to endomorphic property definition, $\circ$ is a right distributive with respect to + operations in M.

Analogously in terms of $\circ$ operation, we can deduce, that for all $w \in G$ and $a \in M$, there exists some $b \in M$ satisfying relation

$$w \circ a = b . \quad (11)$$

The word w we will call an operator and a an operand.

We postulate now the second problem and corresponding OWF_2 defined in the Gaussian group action level.

Problem 2. Operand and operator search problem (OOSP): having known element b satisfying (6) find any other operand a' and operator w' satisfying relation

$$w' \circ a' = b. \quad (12)$$

Postulate 1. The OWF_2 based on the OOSP is a weak OWF.

The weak OWF is an opposite term of strong OWF introduced in (Rabi and Sherman, 1993), where weak OWF is simply called an OWF.

The main idea for KAP construction is to transfer the word problem solution from the group presentation level to the group action level. Then the factors' hiding procedure can be done by arbitrary transformation not requiring the unique property to be maintained. Some additional requirement for the action operation $\circ$ must be postulated in this case.

Definition 1. The word w is called a reduced word if it does not contain subwords w_s of the following type

$$w_s = \varepsilon_i^{e1} \cdot \theta \cdot \varepsilon_i^{-e2} , \quad (13)$$

where $e1, e2$ are integers and ε_i commutes with θ.

This definition is some generalization of reduced word definition in free groups (Magnus *et al.*, 1966).

Definition 2. The length $|w|$ of a reduced word is the number of atoms being in w. Let us consider some subset $S_0 \subset G$ consisting of words with bounded length L.

$$S_0 = \{w \mid w \in G\,;\ |w| \le L\}. \qquad (14)$$

In general S_0 contains subsets of equivalent words. Taking one representator from each equivalency class in S_0 we obtain a new subset $S \subset S_0$ having less elements and consisting of non-equivalent elements in G.

Assume the cardinality of subset S and module M is comparable.

Postulate 2. For all $w \in S$ the mapping $w : M \to M$ is near to bijective.

Conclusion 1. The set of operator's S acting in M is almost automorphic.

Consider two elements w_1, $w_2 \in S$ and two corresponding mappings $w_1 : M \to M$ and $w_2 : M \to M$ with domains $D(w_1) = D(w_2) = M$, and images $Im(w_1) = M$, $Im(w_2) = M$. Let us construct a direct product of the sets $D(\cdot)$ and $Im(\cdot)$ for each operator w_1 and w_2 in S.

$$D(w_1) \times Im(w_1) = \{(m_{11}, m_{12}) \in M \times M \mid w_1(m_{11}) = m_{12}\},$$

$$D(w_2) \times Im(w_2) = \{(m_{21}, m_{22}) \in M \times M \mid w_2(m_{21}) = m_{22}\}.$$

Conclusion 2. The intersection of the following sets

$$D(w_1) \times Im(w_1) \cap D(w_2) \times Im(w_2)$$

is, with a very high probability, an empty set.

Conclusion 3. If any $w_1 \in S$ satisfies equation

$$w_1(a) = w_1 \circ a = b, \qquad (15)$$

then there is infeasible to guess the other word $w_1' \in S$ such that

$$w_1'(a) = w_1' \circ a = b, \qquad (16)$$

for all $a \in G$ and $b \in Im(w_1)$.

The declared Postulate 2 is a basis of words' equivalence problem solution in S. In general, it is hard to prove the Postulate 2 theoretically. But for concrete realizations there is possible to obtain mathematical modeling results indirectly confirming its validity. For further considerations we assume that the suitable module M is constructed as a domain and image of the operators in G, that the set $S \subset G$ is defined and that Postulate 2 is valid.

3. Key agreement protocol

1. Alice chooses at random one public element $\eta \in S$, and two secret elements $\alpha_1 \in S_1$, $\alpha_2 \in S_2$, and forms a word ω_{A0} by the concatenation of α_1, η, α_2

$$\omega_{A0} = \alpha_1 \cdot \eta \cdot \alpha_2 .$$

2. Using two stage random transformations τ_A, Alice obtains a new equivalent word

$$\omega_A = \tau_A(\omega_{A0}) ,$$

and sends ω_A and η to Bob.

3. Bob chooses at random two elements $\beta_1 \in S_1$, $\beta_2 \in S_2$, and analogously forms a word

$$\omega_{B0} = \beta_2 \cdot \eta \cdot \beta_1 .$$

4. Bob transforms an element ω_{B0} to ω_B with a random transformation τ_B

$$\omega_B = \tau_B(\omega_{B0})$$

and sends it to Alice.

5. Each party calculates an element k_A and respectively k_B

$$k_A = \alpha_1 \cdot \omega_B \cdot \alpha_2 \circ a = \alpha_1 \cdot \beta_2 \cdot \eta \cdot \beta_1 \cdot \alpha_2 \circ a$$

$$k_B = \beta_1 \cdot \omega_A \cdot \beta_2 \circ a = \beta_2 \cdot \alpha_1 \cdot \eta \cdot \alpha_2 \cdot \beta_1 \circ a$$

6. The common secret key k, is the following

$$k = k_A = \alpha_1 \cdot \beta_2 \cdot \eta \cdot \beta_1 \cdot \alpha_2 \circ a = \beta_2 \cdot \alpha_1 \cdot \eta \cdot \alpha_2 \cdot \beta_1 \circ a = k_B . \qquad (17)$$

since the commutativity of pairs α_1, β_2 and α_2, β_1 takes place.

4. Security analysis

The security of proposed KAP depends on the security of OWF_1 and OWF_2.

The security of OWF_1 in turn depends on the efficiency of disguising of factors α_1, β_1 and α_2, β_2 in the word ω_A and ω_B, correspondingly. Referencing to insolvability of the word equivalence problem in the considered Gaussian group we claim that OWF_1 is secure according to following considerations.

Assume the adversary obtains a word ω_A in the form of (6) and tries to find some α' and β' from the equation

$$\omega_A = u\, v^{-1} = \alpha' \cdot \theta \cdot \beta'$$

with given u, v and θ.

But since we can choose a Gaussian group as complex as possible due to avoiding a word problem solution in its presentation level, this problem is infeasible for the adversary.

The security of the OWF_2 is based on almost automorphic property of the operators defined in the Gaussian group G acting in the module M.

***Theorem* 1**. If the OWF_1 is secure then it is sufficient for the OWF_2 to be a weak OWF.

Proof. Assume the OWF_1 is secure. Then it is infeasible to obtain the factors α_1, α_2 and β_1, β_2 in the transmitted words ω_A and ω_B, correspondingly. From (17) we can obtain the following equation

$$\beta_1^{-1} \cdot \alpha_2^{-1} \cdot \eta^{-1} \cdot \alpha_1^{-1} \cdot \beta_2^{-1} \circ k = a, \qquad (18)$$

where both elements $w = \beta_1^{-1} \cdot \alpha_2^{-1} \cdot \eta^{-1} \cdot \alpha_1^{-1} \cdot \beta_2^{-1}$ and k are unknown. Then the adversary for given a must find k when w is unknown. This means that both elements w and k must be obtained. According to the weak OWF definition, the OWF_1 is a weak OWF.

The theorem is proved.

5. Discussions

Referencing to the questions Q1, Q2 and Q3 from introduction we present here the corresponding answers A1, A2 and A3 in brief.

A1. We reckon that there exists a class of groups where the public key exchange protocol would be secure enough to be used in real-life applications.

This class of groups consists of infinite non-commutative groups where word equivalence problem and CSP are as complex as possible or insolvable at all. In the proposed KAP the word equivalence problem solution in the group presentation level is replaced by the solution in the group representation or action level.

A2. There is another "hard" problem in combinatorial group theory that can be used, instead of the conjugacy search problem, in a public key exchange protocol.

This problem is LRFSP and this is a generalization of CSP. In some cases the LRFSP can be even simpler than the CSP. Using braid groups, the KAP is mainly constructed on the basis of CSP but nevertheless the agreed key compromitation can be achieved by solving LRFSP (Shpilrain and Ushakov, 2004). Hence we are considering LRFSP, because using CSP does not add an extra security. Both problems LRFSP and CSP are infeasible if the word equivalence problem is infeasible in the considered group.

A3. One can efficiently disguise an element of a given group (or semigroup) by using relations, in the case when word equivalence problem solution is infeasible in the considered group. This can be achieved by using the reversing algorithm described above.

References

[1] **I. Anshel, M. Anshel, D. Goldfeld.** An algebraic method for public–key cryptography. *Mathematical Research Letters* 6, 1999, 1–5.

[2] **P. Dehornoy, L. Paris.** Gaussian groups and Garside groups: two generalizations of Artin groups. *Proc. London Math. Soc*. 79(3), 1999, 569 – 604.

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

[4] **W. Magnus, A. Karrass, D. Solitar.** Combinatorial Group Theory. *Interscience Publishers, NY*, 1966.

[5] **M. Rabi, A. Sherman.** Associative one-way function: A new paradigm for secret key agreement and digital signatures. *Univ. of Maryland. Comp. Sci. Dep*., 1993.

[6] **E. Sakalauskas, T. Burba.** Basic semigroup primitive for cryptographic Session Key Exchange Protocol (SKEP). *Information Technology and Control*. ISSN 1392-124X. 2003, *No*.3(28), 76-80.

[7] **E. Sakalauskas, T. Burba.** Digital signature scheme based on action of infinite ring. *Information Technology and Control.* ISSN 1392-124X, 2004, *No*.2 (31), 60-64.

[8] **E. Sakalauskas.** New Digital Signature Scheme in Gaussian Monoid. *Informatica*. ISSN 0868-4952, 2004, *No*.(3).

[9] **V. Shpilrain, G. Zapata.** Combinatorial group theory and public key cryptography, 2004. *www.iacr.org.*

[10] **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.

[11] **B.L. van der Waerden.** Algebra. *Springer-Verlag*, 1967.