Transactions of A. Razmadze
Mathematical Institute
Vol. **173** (2019), 101–104

PUBLIC KEY EXCHANGE USING CROSSED MODULES OF GROUPS

N. INASSARIDZE[1,2] AND E. KHMALADZE[1,3]

Abstract. A notion of one-way crossed module of groups is introduced and a new general public key exchange protocol based on one-way crossed modules of groups is described.

1. Introduction

There are many attempts to use modern algebraic structures in different cryptographic constructions (see [1, 3, 8–12, 16] and related references therein). Some typical cryptosystems based on non-commutative groups (semigroups, algebras) described in recent papers are the best understood as various generalizations of the classical Diffie–Hellman scheme [5]. In the Diffie–Hellman case the underlying algorithmic problem is the famous discrete logarithm problem for the platform group. Other group based schemes the underlying algorithmic problems could be different such as the conjugacy search problem, the membership search problem, the decomposition and factorization problems and so on.

In this note we propose a new general public key exchange protocol based on one-way crossed modules of groups, that is, one-way functions having an additional algebraic structure. Here, we only give some well-known examples of crossed modules of groups, whose computing algorithms have the cryptographic nature, which will be demonstrated in the forthcoming paper suggesting candidates of one-way crossed modules.

1.1. Basic notions and notations.

We proceed with recalling some basic notions and notations. Let G and H be the groups. By *an action* of H on G we mean a left action written by ${}^{h}g$, for $h \in H$ and $g \in G$. It is always understood that a group H acts on its normal subgroup H' by conjugation: ${}^{h}h' = hh'h^{-1}$, for $h \in H$, $h' \in H'$. Moreover, given a group G, it is always understood that the group of automorphisms $\mathrm{Aut}(G)$ acts on G in the following natural way:

$$ {}^{\phi}g = \phi(g), \quad \text{for } \phi \in \mathrm{Aut}(G),\ g \in G. $$

Given an action of a group H on a group G, *the semi-direct product* of G and H is defined to be the group $G \rtimes H$ with the underlying set $G \times H$ and the multiplication

$$ (g,h)(g',h') = (g\,{}^{h}g', hh'), \quad \text{for all } g,g' \in G,\ h,h' \in H. $$

In particular, the product of elements in $G \rtimes \mathrm{Aut}(G)$ is given by

$$ (g,\phi)(g',\psi) = (g\phi(g'), \phi\psi), \quad \text{for all } g,g' \in G,\ \phi,\psi \in \mathrm{Aut}(G). $$

2. One-way Crossed Modules of Groups

The general concept of a crossed module takes its origin in the work of Whitehead in the late 40s of the past century [15]. The crossed modules of groups are algebraic models for the path-connected CW-spaces whose homotopy groups are trivial in dimensions > 2. Since their introduction, crossed modules played an important role in the homotopy theory.

Definition 2.1. A *crossed module of groups* is a group homomorphism $\mu\colon G \to P$ together with an action of P on G such that

$$ \mu({}^{p}g) = p\mu(g)p^{-1}, \quad {}^{\mu(g)}g' = gg'g^{-1}, $$

for all $g, g' \in G$ and $p \in P$, denoted by (G, P, μ).

2010 *Mathematics Subject Classification.* 94A60, 94A62, 16S34.

Key words and phrases. Crossed module of groups; Group of authomorphisms; Key exchange protocol.

Now we give examples of crossed modules of groups which are useful in cryptographic sense for constructing candidates of one-way crossed modules.

Examples 2.2. i) A normal inclusion $N \trianglelefteq G$ is a crossed module, where G acts on its normal subgroup N by conjugation.

ii) Let G be a group. There is a homomorphism

$$\alpha : G \to \mathrm{Aut}(G)$$

given by $\alpha(g) = \phi_g$, where ϕ_g is the inner automorphism defined by $g \in G$, i.e., $\phi_g(g') = gg'g^{-1}$. It is easy to check that α together with the action of $\mathrm{Aut}(G)$ on G described above, is a crossed module.

iii) Let G and H be groups acting on each other compatibly, that is, the following conditions:

$$^{({}^{g}h)}(g') = {}^{g}({}^{h}({}^{g^{-1}}g')) \ , \qquad ^{({}^{h}g)}(h') = {}^{h}({}^{g}({}^{h^{-1}}h')) \ ,$$

hold for all $g, g' \in G$ and $h, h' \in H$. Let us denote by $G \bowtie H$ the quotient group $(G \rtimes H)/L$, where L is the normal subgroup of the semi-direct product $G \rtimes H$ generated (as a group) by all elements of the form $(g^h g^{-1}, h^g h^{-1})$, $g \in G$, $h \in H$. As a consequence of the compatibility conditions, the canonical maps

$$\mu : G \to G \bowtie H \quad \text{and} \quad \nu : H \to G \bowtie H$$

are the crossed modules (see [6]).

Now we introduce our main (cryptographic) notion, which will in the sequel be the subject of our investigation and applications in a key exchange protocol.

Definition 2.3. A crossed module of groups $\mu : G \to P$ is called a *one-way crossed module* if it is a one-way function (OWF) by its cryptographic nature, i. e., intuitively saying, a function that is easy to compute, but computationally hard to invert.

Having in mind that the existence of OWFs is not proven yet, we may follow the common practice for the proposition of new candidates of OWFs for cryptographic applications. Consequently, the following two necessary (but not sufficient) conditions may be required for the maps to be candidates of OWFs:

(1) The computation of direct value of the map is computationally easy;

(2) A certain hard problem without a known polynomial time algorithm is reducible, in polynomial time, to inverting problem of the map.

General one-wayness assumption. In this subsection we address the general question of one-wayness of a crossed module.

By the Peiffer identity in Definition 2.1, knowing $\mu(x)$ for some $x \in G$, one can compute

$$^{\mu(x)}g = xgx^{-1} \quad \text{for any} \quad g \in G.$$

So, we arrive at the computation problem which we call the *total conjugacy search problem* (TCSP). It has the form:

> given a group G, a map $f : G \to G$ given by some polynomial algorithm and the information that $f(g) = {}^{x}g$ for some x and any $g \in G$, find at least one particular element x with this property.

This problem is related to the known problem, called the k-simultaneous conjugacy search problem (k-SCSP) for a fixed $k \in \mathbb{N}$:

> given a group G and two k-tuples of elements in G, $(g_1, \dots, g_k), (h_1, \dots, h_k)$, and the information that ${}^{x}g_i = h_i$ for all $1 \le i \le n$ and some $x \in G$, find at least one particular element x with this property.

Namely, we have the following theorem.

Theorem 2.4. *Let G be a finitely generated group with k generators $g_1, \dots, g_k$. Then TCSP is polynomial-time equivalent to the k-SCSP for generators, i.e. to the problem:*

given a k-tuple of elements in G, $(h_1, \dots, h_k)$, and information that ${}^{x}g_i = h_i$ for all $1 \leq i \leq n$ and some $x \in G$, find at least one particular element x with this property.

We note that simultaneous conjugacy decision problem turns out to be quite hard in many groups, and even unsolvable in some cases. This problem was studied for various classes of groups (see [7,13,14]). It is shown that the solvability of the conjugacy problem does not imply the solvability of simultaneous conjugacy problem [4]. More recently, in [2], the examples of finitely presented groups are constructed, where the ordinary conjugacy problem is solvable, but the k-simultaneous conjugacy problem is unsolvable for every $k \geq 2$.

We suppose that the simultaneous conjugacy search problem for generators will have at least the same hardness, than the k-simultaneous conjugacy search problem. We also note that if there is an algorithm for solving the simultaneous conjugacy search problem for generators which calculates some $g'' \in G$ such that

$$ {}^{\mu(g)}g' = g''g'g''^{-1} \quad \text{for any} g' \in G, $$

there is no guarantee that $g = g''$. Indeed, it means that $g^{-1}g'' \in Z(G)$ (center of G). Hence if the center of the group is large enough, it will be unfeasible to recover g from g'' by simple multiplications on center elements of the group G.

3. Key Exchange Protocol

In this section, we give a new general key exchange protocol using the idea of one-wayness of crossed modules. Then choosing a platform crossed module of groups, we give practical instances of these protocols.

Protocol. Let (G, P, μ) be a one-way crossed module of groups. The group G is considered to be a set of possible public keys, i.e., elements $g, g' \in G$ are chosen and made public. Both Alice and Bob are going to work with the crossed module (G, P, μ) if they wish to create a shared key. Then, for creating a shared key, Alice and Bob can proceed as follows:

1. Alice selects at random a private key $m \in \mathbb{N}$. Then she computes the element
$$ a = g^m \cdot g' \cdot g^{-m}, $$
applies the one-way crossed module μ to the element a and sends $\mu(a)$ to Bob.
2. Bob selects at random a private key $n \in \mathbb{N}$. Then he computes the element
$$ b = g^n \cdot g' \cdot g^{-n}, $$
applies the one-way crossed module μ to the element b and sends $\mu(b)$ to Alice.
3. Alice computes her key as follows:
$$ K_A = (g^m) \cdot \left({}^{\mu(b)} \left(g^{-m} \cdot g' \cdot g^m \right) \right) \cdot (g^{-m}). $$
Bob computes his key as follows:
$$ K_B = (g^n) \cdot \left({}^{\mu(a)} \left(g^{-n} \cdot g' \cdot g^n \right) \right) \cdot (g^{-n}). $$
Using the crossed module structure, namely, the Peiffer identity of Definition 2.1, we have the following equalities:
$$ \begin{aligned} K_A &= (g^m) \cdot \left(g^n \cdot g' \cdot g^{-n} \right) g^{-m} \cdot g' \cdot g^m \cdot \left(g^n \cdot g'^{-1} \cdot g^{-n} \right) \cdot (g^{-m}) \\ &= (g^n) \cdot \left(g^m \cdot g' \cdot g^{-m} \right) g^{-n} \cdot g' \cdot g^n \cdot \left(g^m \cdot g'^{-1} \cdot g^{-m} \right) \cdot (g^{-n}) = K_B. \end{aligned} $$
So, Alice and Bob have the shared key $K = K_A = K_B$.

Remark 3.1. Note that the publicly known elements g and g' of G should be chosen in such a way that $gg' \neq g'g$. Otherwise, the scheme will become trivial. Moreover, as in the Habeeb-Kahrobaei-Shpilrain key exchange protocol [8,11] and in contrast to the “standard” Diffie–Hellman key exchange, the correctness here is based on the equality $g^m \cdot g^n = g^n \cdot g^m = g^{m+n}$, rather than on the equality $(g^m)^n = (g^n)^m = g^{mn}$.

Security assumptions. Since the shared secrete key in the Protocol is

$$K = g^{m+n} \cdot g' \cdot g^{-(m+n)} \cdot g' \cdot g^{m+n} \cdot g'^{-1} \cdot g^{-(m+n)},$$

our security assumption is that it is computationally hard to retrieve the key K from the quadruple $(g, g', \mu(g^m \cdot g' \cdot g^{-m}), \mu(g^n \cdot g' \cdot g^{-n}))$. If the adversary chooses a "direct" attack by trying to recover the private keys a, she will have to invert one-way function μ on $\mu(a)$, then to solve the conjugacy problem for $g^m \cdot g' \cdot g^{-m}$ and, finally, to solve the discrete logarithm problem for g^m.

Acknowledgement

The authors were partially supported by Ministerio de Economía y Competitividad (Spain), grant MTM2016-79661-P. The first author was also supported by STCU-2016-08/MTCU 6321.

References

1. I. Anshel, M. Anshel, D. Goldfeld, An algebraic method for public-key cryptography. *Math. Res. Lett.* **6** (1999), no. 3-4, 287–291.
2. M. R. Bridson, J. Howie, Conjugacy of finite subsets in hyperbolic groups. *Internat. J. Algebra Comput.* **15** (2005), no. 4, 725–756.
3. E. Chida, T. Nishizeki, M. Ohmori, H. Shizuva, On the one-way algebraic homomorphism. *IEICE Trans. Fundamentals, Communications and Computer Sciences* **79** (1996), no. 1, 54–60.
4. D. E. Collins, Conjugacy and the Higman embedding theorem. *Word problems, II* (*Conf. on Decision Problems in Algebra, Oxford,* 1976), pp. 81–85, Stud. Logic Foundations Math., 95, North-Holland, Amsterdam-New York, 1980.
5. W. Diffie, M. E. Hellman, New directions in cryptography. *IEEE Trans. Information Theory* **IT-22** (1976), no. 6, 644–654.
6. N. D. Gilbert, P. J. Higgins, The nonabelian tensor product of groups and related constructions. *Glasgow Math. J.* **31** (1989), no. 1, 17–29.
7. F. Grunewald, D. Segal, Some general algorithms. I. Arithmetic groups. *Ann. of Math. (2)* **112** (1980), no. 3, 531–583.
8. M. Habeeb, D. Kahrobaei, Ch. Koupparis, V. Shpilrain, Public key exchange using semidirect product of (semi) groups. *International Conference on Applied Cryptography and Network Security*, pp. 475-486. Springer, Berlin, Heidelberg, 2013.
9. N. Inassaridze, T. Kandelaki, M. Ladra, Categorical interpretations of some key agreement protocols. Translated from Sovrem. Mat. Prilozh., vol. 83, 2012. *J. Math. Sci. (N.Y.)* **195** (2013), no. 4, 439–444.
10. N. Inassaridze, M. Khazaradze, E. Khmaladze, B. Mesablishvili, On one-way ring homomorphisms. *Journal Math. Sci.*, 2019 (to appear).
11. D. Kahrobaei, V. Shpilrain, Using semidirect product of (semi) groups in public key cryptography. *Pursuit of the universal*, 132–141, Lecture Notes in Comput. Sci., 9709, Springer, [Cham], 2016.
12. D. Pavlovic, Chasing diagrams in cryptography. *Categories and types in logic, language, and physics*, 353–367, Lecture Notes in Comput. Sci., 8222, Springer, Heidelberg, 2014.
13. R. A. Sarkisyan, The conjugacy problem for collections of integral matrices. (Russian) *Mat. Zametki* **25** (1979), no. 6, 811–824, 956.
14. E. A. Scott, A finitely presented simple group with unsolvable conjugacy problem. *J. Algebra* **90** (1984), no. 2, 333–353.
15. J. H. C. Whitehead, Combinatorial homotopy. II. *Bull. Amer. Math. Soc.* **55** (1949), 453–496.
16. N. Yanai, E. Chida, M. Mambo, A secure structured multisignature scheme based on a non-commutative ring homomorphism. *IEICE transactions on fundamentals of electronics, communications and computer sciences* **94** (2011), no. 6, 1346–1355.

[1]A. Razmadze Mathematical Institute of I. Javakhishvili Tbilisi State University, 6 Tamarashvili Str., Tbilisi 0177, Georgia

[2]Georgian Technical University, Kostava Str., 77, Tbilisi 0175, Georgia

[3]The University of Georgia, Kostava Str., 77a, Tbilisi 0171, Georgia
E-mail address: niko.inas@gmail.com
E-mail address: e.khmal@gmail.com