THE APPROACH TO KEY EXCHANGE PROTOCOL BASED ON METACYCLIC GROUP

R. V. Skuratovskii, I.V. Baklan (1), Aled Williams (2),

(1)NTUU "Igor Sikorsky Kyiv Polytechnic Institute"
(2)Cardiff University

The goal of this investigation is effective method of key exchange which based on non-commutative group G. The results of Ko K, Lee S, is improved and generalized.

We consider non-commutative generalization of CDH problem [1,2] on base of metacyclic group G of Miller's Moreno type (minimal non-abelian group). We show that conjugacy problem in this group is intractable. Effectivity of computation is provided due to using groups of residues by modulo n. The algorithm of generating (designing) common key in non-commutative group with 2 mutually commuting subgroups is constructed by us.

Introduction. In this paper new conjugacy key exchange scheme is proposed. This protocol based on conjugacy problem in non-commutative group [1, 2, 3, 5, 9]. We slightly generalize Ko Lee's [8] protocol of key exchange. Public key cryptographic schemes based on the new systems are established. The conjugacy search problem in a group G is the problem of recovering an $(a \in G)$ from given $(w \in G)$ and $h = a^{-1}wa$. This problem is in the core of several recently suggested public key exchange protocols. One of them is most notably due to Anshel, Anshel, and Goldfeld [9], and another due to Ko Lee et al. As we know if CCP problem is tractable in G then problem of finding w^{ab} by given w, $w^a = a^{-1}wa$, $w^b = b^{-1}wb$ for arbitrary fixed $w \in G$ such that is not from center of G, w^{ab} is the common key that Alice and Bob have to generate.

Recently, a novel approach to public key encryption based on the algorithmic difficulty of solving the word and conjugacy problems for finitely presented groups has been proposed in [9, 10]. The method is based on having a canonical minimal length form for words in a given finitely presented group, which can be computed rather rapidly, and in which there is no corresponding fast solution for the conjugacy problem. A key example is the braid group.

We denote by w^x the conjugated element $u = x^{-1}wx$. We show that efficient algorithm that can distinguish between two probability distributions of $\left(w^x, w^y, w^{xy}\right)$ and $\left(w^g, w^h, w^{gh}\right)$ doesn't exist. Also, efficient algorithm that recovers w^{xh} from w, w^x and w^y. doesn't exist. This group has representation $\left\langle G = a, b \middle| a^{P^m} = e,\, b^{P^n} = e,\, b^{-1}ab = a^{1+p^{m-1}},\, m \geq 2,\, n \geq 1 \right\rangle$. As a generators a, b can be chosen two arbitrary non commuting elements [4, 5, 6].

Consider non-metacyclic group of Millera Moreno. This group has representation $\left\langle G = a, b \middle\| c \right| = p,\, |a| = p^m,\, |a| = p^n,\, m \geq 1,\, n \geq 1,\, b^{-1}ab = ac,\, b^{-1}cb = c \rangle$.

To find a length of orbit of action by conjugation by b we consider the class of conjugacy of elements of form $a^j c^i$. This class has length p because of action $b^{-1}a^j c^i b = a^{j+1}c^i$, … , as well as $b^{-1}a^j c^{i+p-1} b = a^j c^{i+p} = a^j c^i$ increase the power of c on 1. Thus, the first repetition of initial power j in $a^j c^i$ occurs through n conjugations of this word by b, where $1 \leq j \leq p$. Therefore, the length of the orbit is p.

We need to have an effective algorithm for computation of conjugated elements, if we want to design a key exchange algorithm based on non-commutative DH problem [3]. Due to the relation in metacyclic group, which define the homomorphism $\varphi : b \to Aut(a)$ to the automorphism group of the $B = \langle b \rangle$, we get a formula for finding a conjugated element. Using this formula, we can efficiently calculate the conjugated to a element by using the raising to the $1 + p^{m-1}$-th power, where $m > 1$.

There is effective method of checking the equality of elements due to cyclic structure of group $A = \langle a \rangle$ and $B = \langle b \rangle$ in this group G.

We have an effective method of checking the equality of elements in the additive group Z_n, because of reducing by finite modulo n.

Conclusion. We can choose mutually commutative H_1, H_2 as subgroups of $Z(G)$. As we said above, x, y are chosen from H_1, H_2, as components of key. According to [4] $Z(G) = p^{n+m-2}$ so size of key-space is $O(p^{(n+m-2)})$. Note that size of key-space can be chosen as arbitrary big number by choosing the parameters p, n, m. As an element for exponenting we can choose an arbitrary element $w \in A$ but $\boldsymbol{w} \neq \boldsymbol{e}$, because the size of orbit in result of action of inner automorphism φ is always not less then p.

References

1. Gu L, Wang L, Ota K, Dong M, Cao Z and Yang Y 2013 New public key cryptosystems based on non-abelian factorization problem Sec. Com. Netw. 6, P. 912–22
2. Bohli J, Glas B and Steinwandt R 2006 Towards provable secure group key agreement building on group theory Cryptology ePrint Archive: Report 2006/079
3. Gu L and Zheng S 2014 Conjugacy systems based on nonabelian factorization problems and their applications cryptography J. Appl. Math. Article ID 630607
4. Raievska I, Raievska M and Sysak Y 2016 Finite local nearrings with split metacyclic additive group Algebra Discrete Math. 22, P. 129-52
5. Skuratovskii R 2019 Employment of Minimal Generating Sets and Structure of Sylow 2-Subgroups Alternating Groups in Block Ciphers. Springer, Advances in Computer Comm. Comp. Sciences P. 351-64
6. Otmani A, Tillich J and Dallot L 2010 Cryptanalysis of two McEliece cryptosystems based on quasi-cyclic codes Math.Comput.Sci. 3, P. 129–40
7. Vinogradov I 2016 Elements of number theory Courier Dover Publications.
8. Ko K, Lee S, Cheon J, Han J, Kang J, Park C 2000 New public-key cryptosystem using braid groups Advances in cryptology — CRYPTO 2000 1880, P. 166–83
9. Anshel I, Anshel M and Goldfeld D 1999 An algebraic method for public-key cryptography Math. Res. Lett. 6, P. 287–91
10. Anshel I, Anshel M, Fisher B and Goldfeld D 2001 New key agreement protocol in braid group cryptography In Topics in Cryptology – CT-RSA2001 2020, P. 13-27

 ISSN-online 2708-0102