INTERNATIONAL JOURNAL OF MATHEMATICAL MODELS AND METHODS IN APPLIED SCIENCES
DOI: 10.46300/9101.2020.14.2 Volume 14, 2020

Some approach to key exchange protocol based on non-commutative groups

Ruslan Skuratovskii, Aled Williams

Abstract —We consider non-commutative generalization of CDH problem [1,2] on base of metacyclic group G of type Millera Moreno (minimal non-abelian group). We show that conjugacy problem in this group are intractable. The algorithm of generating (desinging) of common key in non-commutative group with 2 mutually commuting subgroups are constructed by us.

Keywords — CDH and CCP problem, non-commutative cryptography, Millera Moreno group, subdirect product, generalization of CDH problem.

I. Introduction

In this investigation effective method of key exchange which based on non-commutative group G is proposed. The results of Ko K, Lee S, is improved and generalized [1,2,3]. Public key cryptographic schemes based on the new systems are established. One of them is most notable due to Anshel and Goldfeld [9], and another due to Ko Lee etc. As we know if CSP problem is tractable in group G then problem of finding w^{ab} by given w, $w^a = a^{-1}wa$, $w^b = b^{-1}wb$ is tractable too for arbitrary fixed $w \in G$ such that is not from center of G, where w^{ab} is the common key that Alice and Bob have to generate.

As well known if CCP problem is tractable in G then problem of finding w^{ab} by given w, $w^a = a^{-1}wa$, $w^b = b^{-1}wb$ is tractable too for arbitrary fixed $w \in G$ such that is not from center of G. Note that w^{ab} is the common key that Alice and Bob have to generate.

We denote by w^x the conjugated element $u = x^{-1}wx$. We show that no eficient algorithm exists that can distinguish between the two probability distributions of (w^x, w^y, w^{xy}) and (w^g, w^h, w^{gh}). Also no efficient algorithm exists to recover w^{xh} from w, w^x and w^y. Metacyclic Millera Moreno group has representation $G = \left\langle a, b \mid a^{P^m} = e, b^{P^n} = e, b^{-1}ab = a^{1+p^{m-1}}, m \geq 2, n \geq 1 \right\rangle$, where is p prime. As a generators a, b can be chosen two arbitrary non commuting elements [4, 5,6].

The authors are with the department of computer science
Kiev Polytechnic Institute, Kiev, Ukraine
The second author is also with the Department of computer science of Cardiff University, UK

For desining a key exchange algorithm based on non-commutative DH problem [3] it have to be effective algorithm for computation of conjugated elements. Due to the relation in metacyclic group, which define the homomphism $\varphi : \langle b \rangle \to Aut(\langle a \rangle)$ to the automorphism group of $A = \langle a \rangle$, we obtaint a formula for finding a conjugated element. This formula give us possibility to efficiently calculate the conjugated to a element by using the raising to the $1 + p^{m-1}$-th power, where $m > 1$. Also due to cyclic structure of groups $A = \langle a \rangle$ and $B = \langle b \rangle$ in this group G exists effectively method of cheking of equality of elements.

Indead the reducing by finite modulo n give us an effective method of checking the equality of elements in the additive group $\mathbb{Z}_n$.

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.

II. Proof that conjugacy proplem is NP-hard in G

A. Size of cojugacy class

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 $\varphi : \langle b \rangle \to \mathrm{Aut}(\langle a \rangle)$ to the automorphism group of the $A = \langle a \rangle$, we obtain a formula for finding a conjugated element. Using this formula, we can efficiently calculate the conjugated to a^i element by using the raising to the $1 + p^{(m-1)}$-th power by modulo p^m, where $m > 1$.

There is effective method of checking the equality of elements due to cyclic structure of subgroups $A = \langle a \rangle$ 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.

To problem of DL or equaletly problem of conjugancy in non-commutative group *G* be NP-hard it have to be enough long orbit of the given base element $w \in G$.
Let elements of *G* acts by conjugation on $w \in G$, where $w \notin Z(G)$.

Proof of NP-hardness of the conjugacy problem in *G*. Size of a conjugacy class.

Let elements of G acts by conjugation on $w \in G$, where $w \notin Z(G)$. To problem of DL or equivalent problem of conjugacy in non-commutative group *G* be NP-hard, the orbit of the given base element $w \in G$ must be enough long if we want to have stability of DL problem or equally problem of conjugacy in non-commutative group *G* like NP-hard problem.

Theorem 1. The length of conjugacy class of non-central element *w* is equal to *p*.

Proof. Recall the inner automorphism in G is determined by formula $b^{-1}ab = a^{(1+p^{(m-1)})}$. Let us recall the structure of minimal non-abelian Metacyclic group:

$G = B\beta_{\varphi} A$, where $A=\langle a\rangle$ and $B=\langle b\rangle$ are finite cyclic groups. Therefore formula $b^{(-1)}ab = a^{(1+p^{(m-1)})}$ define a homomorphism φ in the subgroup of inner automorphisms Aut(⟨a⟩). As well-known each finite cyclic group is isomorphic to the correspondent additive cyclic group modulo n residue $\mathbb{Z}_n$ (or Z_n). In this group equality of elements can be checked effectively due to reducing the elements of the module group.

Consider the orbit of element w under action by conjugation. The length of such orbit can be found from equality $w^{(1+p^{(m-1)})^s} = w$ as minimal power *s* for which this equality will be true. We apply Newton binomial formula to the expression $(1+p^{(m-1)})^s \equiv 1(modp^m)$ and taking into account the relation $a^{p^m} = e.$ We obtain $1+C_s^1 p^{(m-1)} + C_s^2 p^{(2(m-1))} + ... + p^{(s(m-1))} \equiv 1(modp^m)$, $l < m$ bec ause of $1+C_s^1 p^{(m-1)} = 1+sp^{(m-1)} \equiv 1(modp^s)$ if $s < p$. It means that minimal *s* when this congruence start to holds is equal to *p*. The prime number *p* can be chosen as big as we need [7]. The proof is fully completed.

Consider non-metacyclic group of Millera Moreno.

Theorem 2. The length of conjugacy class of non-central element *w* is equal to *p* ш non-metacyclic group of Millera Moreno.

This group has representation

$$G = \left\langle a,b \middle| |c| = p,\ |a| = p^m,\ |a| = p^n,\ m,\ n \geq 1,\ b^{-1}ab = ac,\ b^{-1}cb = c. \right\rangle$$

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*.

B. Key exchange protocol

Let S_1, S_2 are subsets from *G* sonsisting of mutually commutative elements. We consider subgroups $H_1 = \langle S_1 \rangle$ and $H_2 = \langle S_2 \rangle$. Due to mutually commutative generating sets this subgroups are mutually commutative too.

Consider base steps of protocol.

Input: Elements *w*, w^x and w^y.

Alice chose random element *x* from the subgroup H_1 and compute w^x. After she sents it to Bob.

Bob chose random element *y* from the subgroup H_2 and compute w^x. After he sents it to Alice.

Bob computes $\left(w^x\right)^y = w^{xy}$ and Alice computes $\left(w^y\right)^x = w^{yx}$. Taking into consideration that H_1 and H_2 are mutually commutative groups we obtain that $xy = yx$.

Therefore we have $w^{xy} = w^{yx}$. Thus, common key [6] w^{xy} was successfully generated.

Resistance to a cryptanalysis. But if we will use for cryptoanalysys solving of conjugacy search problem the method of reduction to solving of decomposition problem [8] then it leads us to solving of discrete logarithm problem in the group that have structure of semidirect product ot multiplicative group Z_{p^n} and Z_{p^m}. This problem is NP-hard even in multiplicative group Z_{p^m} for enough big *p* or for essentially big *m*.

If one try to solve conjugacy search problem in *G* using the method of Barrett [9, 10] then complexity of the complexity of solving this problem by enumerating options for conjugating (mating) elements is $O\left(p2\log_2(p^{m-1}+1)m\log_2^2 p\right)$. Indeed, one conjugation of *a* calculated as $b^{-1}ab = a^{1+p^{m-1}}$. To compute the power $a^{1+p^{m-1}}$ my modulo p^m the method of Barrett uses $2\log_2(p^{m-1}+1)$ multiplications. Also the complexity of one such multiplication by modulo p^m is $\log_2^2 p^m = m\log_2^2 p$. Since the length of the orbit under the action of conjugation of the active group as proved in Theorem 1 is equal to *p*. Since the length of the orbit under the action of conjugation of the active group as proved in Theorem 1 is equal to *p*.

C. Conclusion

We can chose mutually commutative H_1, H_2 as a subgroups of $Z(G)$. As we said above *x*, *y* as components of key a chosen from H_1, H_2. According to [4] $Z(G) = p^{n+m-2}$ so size of key-space is $O\left(p^{n+m-2}\right)$. Note that size of key-space can be chosen as arbitrary big number by choice of parameters *p*, *n*, *m*.

REFERENCES

[1] L. Gu, L. Wang, K. Ota, M. Dong, Z. Cao and Y. Yang, New public key cryptosystems based on non-abelian factorization problems, Secur. Commun. Netw. Vol 6, 2013, no. 7, pp. 912–922.

[2] J.-M. Bohli, B. Glas and R. Steinwandt, Towards provable secure group key agreement building on group theory, Cryptology ePrint Archive: Report 2006/079, 2006.

[3] L. Gu and S. Zheng, Conjugacy systems based on nonabelian factorization problems and their applications cryptography, J. Appl. Math. 2014 (2014), Article ID 630607.

[4] I. Raievska M. Raievska, Y. P. Sysak. Finite local nearrings with split metacyclic additive group. Algebra Discrete Math., 22, no. 1, 2016, pp. 129-152.

[5] G. A. Miller "Groups which contain an abelian subgroup of prime index" National academy of sciences. Biographical memoirs. 1936. pp. 21-32.

[6] R. V. Skuratovskii, Employment of Minimal Generating Sets and Structure of Sylow 2-Subgroups Alternating Groups in Block Ciphers. Springer, Advances in Computer Communication and Computational Sciences, 2019, pp. 351-364.

[7] A. Otmani,. J. P. Tillich, l Dallot. Cryptanalysis of two McEliece cryptosystems based on quasi-cyclic codes, Math.Comput.Sci.3, 2010, pp. 129–140.

[8] Vladimir Shpilrain And Alexander Ushakov. The conjugacy search problem in public key cryptography: unnecessary and insufficient

[9] Barrett, P. Implementing the Rivest Shamir and Adleman Public Key Encryption Algorithm on a Standard Digital Signal Processor. Advances in Cryptology — CRYPTO' 86. Lecture Notes in Computer Science (1986). volume 263, pp. 311–323.

[10] Hasenplaugh, W.; Gaubatz, G.; Gopal, V. "Fast Modular Reduction" (PDF). 18th IEEE Symposium on Computer Arithmetic(ARITH'07). (2007). pp. 225–229.

[11] R. V. Skuratovskii, Involutive irreducible generating sets and structure of sylow 2-subgroups of alternating groups. ROMAI J., 13, Issue 1, (2017), pp. 117-139.

[12] R. Skuratovskii, "Corepresentation of a Sylow *p*-subgroup of a group S*n*". Cybernetics and systems analysis, (2009), N. 1, pp. 27-41.

[13] Runovski, K., Schmeisser, H.-J. On the convergence of Fourier means and interpolation means. J Comput. Analysis Applic. 2004, 6, pp. 211-227.