COMMUTATOR SUBGROUP OF SYLOW 2-SUBGROUPS OF ALTERNATING GROUP AND MILLER-MORENO GROUPS AS BASES OF NEW KEY EXCHANGE PROTOCOL

A Preprint

Ruslan V. Skuratovskii
NTUU 'Igor Sikorsky Kyiv Polytechnic Institute'
r.skuratovskii@kpi.ua
ruslcomp@mail.ru

Aled Williams
School of Mathematics
Cardiff University
Cardiff, UK
williamsae13@cardiff.ac.uk

February 26, 2020

ABSTRACT

The goal of this investigation is effective method of key exchange which based on non-commutative group $G$. The results of Ko et al. [6] is improved and generalized. The size of a minimal generating set for the commutator subgroup of Sylow 2-subgroups of alternating group is found. The structure of the commutator subgroup of Sylow 2-subgroups of the alternating group $A_{2k}$ is investigated and used in key exchange protocol which based on non-commutative group.

We consider non-commutative generalization of CDH problem [4,5] on base of metacyclic group of Miller-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.

Key words: the commutator subgroup of Sylov 2-subgroups, metacyclic group, conjugacy key exchange scheme, finite group, conjugacy problem.

2000 AMS subject classifications: 20B27, 20B22, 20F65, 20B07, 20E45.
1 Introduction

In this paper a new conjugacy key exchange scheme is proposed. This protocol based on conjugacy problem in non-commutative group \[2, 3, 4, 5, 10\]. We slightly generalize Ko Lee’s \[6\] protocol of key exchange. Public key cryptographic schemes based on the new systems are established. The conjugacy search problem in a group 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 \[2\] and another due to Ko et al. \[6\]. As we know if CCP problem is tractable in \(G\) then problem of finding \(wab\) by given \(w\), \(w^a = a^{-1}wa\), \(w^b = b^{-1}wb\) for an arbitrary fixed \(w \in G\) such that is not from center of \(G\), \(wab\) 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 \[11, 2\]. 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 \((w^x, w^y, w^x y)\) and \((w^g, w^h, w^{gh})\) does not exist. Also, an efficient algorithm which recovers \(w^{x^n}\) from \(w^x\) and \(w^y\) does not exist. This group has representation

\[
G = \left\langle a, b \mid a^{p^m} = e, b^{p^n} = e, b^{-1}ab = a^{1+p^{-1}}c, m \geq 2, n \geq 1 \right\rangle.
\]

As a generators \(a, b\) can be chosen two arbitrary commuting elements \[8, 10, 7\].

Consider non-metacyclic group of Miller Moreno. This group has representation

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

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 \(b^{-1}a^j c^i b = a^{j+1}c^i, \ldots\), 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 though \(n\) 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 \[5\]. Due to the relation in metacyclic group, which define the homomorphism \(\varphi : \langle b \rangle \to \text{Aut}(\langle a \rangle)\) to the automorphism group of the \(B = \langle b \rangle\), we obtain a formula for finding a conjugated element. Using this formula, we can efficiently calculate the conjugated to 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 $\mathbb{Z}_n$ because of reducing by finite modulo $n$.

2 Proof that conjugacy problem is $\mathcal{NP}$-hard in $G$. Size of a conjugacy class

The orbit of the given base element $w \in G$ must be long enough if we want to have problem of DL or equally problem of conjugacy in non-commutative group $G$ like $\mathcal{NP}$-hard problem.

Let elements of $G$ act by conjugation on $w \in G$, where $w \notin Z(G)$.

**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 the formula $b^{-1}ab = a^{1+p^{m-1}}$. Let us recall the structure of minimal non-abelian Metacyclic group, namely $G = B \rtimes \varphi A$, where $A = \langle a \rangle$ and $B = \langle h \rangle$ are finite cyclic groups. Therefore, the formula $b^{-1}ab = a^{1+p^{m-1}}$ defines a homomorphism $\varphi$ in the subgroup of inner automorphisms Aut($\langle a \rangle$). It is well-known that each finite cyclic group is isomorphic to the correspondent additive cyclic group modulo $n$ residue $\mathbb{Z}_n$. 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 $(1 + p^{m-1})^s \equiv 1 \pmod{p^m}$ and taking into account the relation $a^{p^m} = e$. We obtain

$$1 + C_s^1 p^{m-1} + C_s^2 p^{2(m-1)} + \cdots + p^{s(m-1)} \equiv 1 \pmod{p^m}$$

only if $s \equiv p^l \pmod{p^m}$ with $l < m$ because $1 + C_s^1 p^{m-1} = 1 + sp^{m-1} \not\equiv 1 \pmod{p^s}$ if $s < p$. It means that the minimal $s$ when this congruence start to holds is equal to $p$. The prime number $p$ can be chosen as big as we need [17] which completes the proof.

Let us evaluate the size of subsets $S_1, S_2$ with mutually commutative elements. Each of this subset of generated by them subgroups $H_1, H_2$ can be chosen as the subgroups of center of group $G$. It is well-known that the semidirect product is closely related to wreath product. The center of the wreath product with non-faithful action were recently studied [11].

**Proposition 1.** As it was proved by the author a center of the restricted wreath product with $n$ non-trivial coordinates $(A, X) \wr B$ is direct product of normal closure of center of diagonal of $Z(B^n)$, i.e. $(E \times Z(\Delta(B^n)))$, trivial an element, and intersection of $(K) \times E$ with $(A)$. In other words,

$$Z((A, X) \wr B = \langle (1; h, \ldots, h), e(Z(A) \cap Z(K, X)) \wr E \rangle \simeq \langle Z(A) \cap K \rangle \times Z(\Delta(B^n))$$

where $h \in Z(B), |X| = n$. 

3
Commutator subgroup of Sylow 2-subgroups of alternating group and Miller-Moreno groups as bases of new Key Exchange Protocol

Taking into consideration that a semidirect product is the partial case of wreath product the diagonal of $B^n$ degenerates in $B$. Thus, we obtain such formula for the center of semidirect product:

$$Z((A, X) \rtimes B) = \langle Z(1; h), e, (Z(A) \cap K, X) \rtimes E \rangle \simeq \langle Z(A) \cap K \rangle \times Z(\Delta(B^n)) \rangle.$$

This structure lead to constructive method of finding elements of the center. As it was noted above the elements $x$ and $y$ are parts of elements of secret key. Therefore as greater a size of center of a considered group as greater a size of a key space of this protocol.

Also commutator subgroup of Sylow 2-subgroup of alternating groups can be used as a support of CSP problem [12, 13, 15].

**Definition 2.1.** For an arbitrary $k \in \mathbb{N}$ we call a $k$-coordinate subgroup $U < G$ a subgroup, which is determined by $k$-coordinate sets $[U]_l$, $l \in \mathbb{N}$, if this subgroup consists of all Kaloujnine’s tableaux $a \in I$ for which $[a]_l \in [U]_l$.

We denote by $G_k(l)$ a level subgroup of $G_k$, which consists of the tuples of v.p. from $X^l$, $l < k - 1$ of any $\alpha \in G_k$.

As a sets $S_1$ and $S_2$ consisting of mutually commutative elements we can use the set of elements of $l$-coordinate subgroup of $G_k$, where $l < k$, or the elements of $G_k(l)$ that is isomorphic to this subgroup. As it was proved by the author [12] the order of $Syl_2A_{2k}$ is $2^{2k-2}$. Therefore the growth of mutually commutative sets of elements $S_1$ and $S_2$ is exponential function has.

According to [9] index of center of metacyclic group has index $|G : Z(G)| = p^2$, therefore the order of $Z(G) = p^{k-2}$. Thus, we have $p^2 - 1$ possibilities to choose an element $w$ as an element of the open key, which is in the protocol of key exchange.

### 3 Key exchange protocol

Let $S_1, S_2$ be subsets from $G$ consisting of mutually commutative elements. We make a generalisation of CDH by taking into consideration the subgroups $H_1 = \langle S_1 \rangle$ and $H_2 = \langle S_2 \rangle$ instead of using $S_1, S_2$. We can do this because the groups $H_1$ and $H_2$ have generating sets $S_1$ and $S_2$ which commute. Because of these mutually commutative generating sets, we know that the subgroups are additionally mutually commutative.

### 4 Consideration of base steps of the protocol

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

Alice selects a private $x$ as the random element $x$ from the subgroup $H_1$ and computes $w^x = x^{-1}wx$. The she sends it to Bob. Bob selects a private $y$ as the random element $y$ from the subgroup $H_2$ and computes $w^y$. Then he sends it to Alice. Bob computes $(w^x)^y = w^{xy}$ and Alice computes $(w^y)^x = w^{yx}$. Taking into consideration that $H_1$ and $H_2$ are mutually commutative groups we obtain that $xy = yx$. Therefore, we have that $w^{xy} = w^{yx}$.
Output: $w^{xy}$ that is the common key of Alice and Bob.

Thus, the common key $[3, 6, 2, 1] w^{xy}$ was successfully generated.

**Resistance to a cryptanalysis.** But if an analytic use for a cryptanalysis will use for cryptoanalysys solving of conjugacy search problem the method of reduction to solving of decomposition problem [16], then it lead us to solving of discrete logarithm problem in the multiplicative cyclic group $Z_p$. This problem is NP-hard for big $p$.

5 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 [8] $Z(G) = p^{n+m-2}$ so size of key-space is $O(p^{n+m-2})$. It should be noted that the 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 $w \neq e$, because the size of orbit in result of action of inner automorphism $\phi$ is always not less than $p$.

References

[1] Iris Anshel, Michael Anshel, Benji Fisher, and Dorian Goldfeld. New key agreement protocols in braid group cryptography. In Cryptographers’ Track at the RSA Conference, pages 13–27. Springer, 2001.

[2] Iris Anshel, Michael Anshel, and Dorian Goldfeld. An algebraic method for public-key cryptography. *Mathematical Research Letters*, 6(3):287–291, 1999.

[3] Jens-Matthias Bohli, Benjamin Glas, and Rainer Steinwandt. Towards provably secure group key agreement building on group theory. Cryptology ePrint Archive, Report 2006/079, 2006. [https://eprint.iacr.org/2006/079](https://eprint.iacr.org/2006/079).

[4] Lize Gu, Licheng Wang, Kaoru Ota, Mianxiong Dong, Zhenfu Cao, and Yixian Yang. New public key cryptosystems based on non-abelian factorization problems. *Security and Communication Networks*, 6(7):912–922, 2013.

[5] Lize Gu and Shihui Zheng. Conjugacy systems based on nonabelian factorization problems and their applications in cryptography. *Journal of Applied Mathematics*, 2014, 2014.

[6] Ki Hyoung Ko, Sang Jin Lee, Jung Hee Cheon, Jae Woo Han, Ju-sung Kang, and Choonsik Park. New public-key cryptosystem using braid groups. In Mihir Bellare, editor, *Advances in Cryptology — CRYPTO 2000*, pages 166–183, Berlin, Heidelberg, 2000. Springer Berlin Heidelberg.

[7] Ayoub Otmani, Jean-Pierre Tillich, and Léonard Dallot. Cryptanalysis of two mceliece cryptosystems based on quasi-cyclic codes. *Mathematics in Computer Science*, 3(2):129–140, 2010.
[8] I Raievska, M Raievska, and Ya Sysak. Finite local nearrings with split metacyclic additive group. *Algebra and discrete mathematics*, 22(22, 1):129–152, 2016.

[9] László Rédei. Das “schiefe produkt” in der gruppentheorie. *Commentarii Mathematici Helvetici*, 20(1):225–264, 1947.

[10] Ruslan Viacheslavovich Skuratovskii. Employment of minimal generating sets and structure of sylow 2-subgroups alternating groups in block ciphers. In *Advances in Computer Communication and Computational Sciences*, pages 351–364. Springer, 2019.

[11] Ruslan Viacheslavovich Skuratovskii and Aled Williams. Minimal generating set and a structure of the wreath product of groups, and the fundamental group of the orbit morse function. *Bulletin of Donetsk National University. Series A: Natural Sciences*, 0(1-2):76–96, 2019.

[12] Skuratovskii R., Commutators subgroups of sylow subgroups of alternating and symmetric groups their minimal generating sets. The XII International Algebraic Conference in Ukraine (2019) Vinnytsia, p. 75.

[13] Skuratovskii R.V., Generating set of wreath product non faithful action. International Journal of Analysis and Applications Volume 18, No. 1 (2020), pp. 104–116.

[14] R. V. Skuratovskii. Structure of commutant and centralizer, minimal generating sets of. Sylow 2-subgroups $Syl_2 A_n$ of alternating and symmetric groups. International conference in Ukraine, ATA12. (2017). https://www.imath.kiev.ua/topology/.../skuratovskiy.pdf

[15] Skuratovskii R. V., Structure and minimal generating sets of Sylow 2-subgroups of alternating groups. Source: https://arxiv.org/abs/1702.05784v2

[16] V Shpilrain, A. Ushakov The Conjugacy Search Problem in Public Key Cryptography: Unnecessary and Insufficient. Applicable Algebra in Engineering, Communication and Computing. (2006), volume 17, p. 285 - 289.

[17] Ivan Matveevich Vinogradov. *Elements of number theory*. Courier Dover Publications, 2016.