An application of metacyclic and Miller Moreno *p*-groups to establishment protocol

RUSLAN SKURATOVSKII
Department of computer science
Igor Sikorsky Kiev Polytechnic Institute
Kiev, UKRAINE 03056, av. Pobedy 37 and
Interregional Academy of Personnel Management

VOLODYMYR OSADCHYY
Department of computer science
IT-GRAVITY-VO, Inc. Orlando
Florida US Kiev,

ALED WILLIAMS
Cardiff University
Cardiff, UK.

Abstract: — The protocol of Ko K., Lee S., are improved and generalized on base of metacyclic and non-metacyclic *p*-groups of type Miller-Moreno (minimal non-abelian group). We show that the decomposition problem in this group is intractable. It is proved that the conjugacy problem in this group is also intractable. Further, we have constructed an algorithm of generating (designing) of common key for a non-commutative group with two mutually commuting subgroups has been constructed by us. An application of general metacyclic group to control an entropy of key space is considered.

Key-Words: - CDH and CSP problems; non-commutative cryptography; Miller-Moreno p-group, generalization of CDH problem, conjugacy problem.

Received: February 16, 2020. Revised: July 15, 2020. Accepted: July 29, 2020. Published: August 10, 2020.

1 Introduction

Multi-agent systems consist of agents and their environment. For safety communications between agents this environment have to be provided by protocols of common key generations. Typically multi-agent systems research refers to software agents. We propose an effective method persistent to the attack of a man in the middle by solving the decomposition problem [1] of the key exchange protocol which is based on non-commutative group *G*. It can be used for the formation of subject access requests. The results of Ko K., Lee S., are improved and generalized [4]. We construct an cryptographic primitives, methods and protocol are based on algebraic structures like semigroups, groups. In these protocols it would be assumed that *G* is a non-abelian group. If *w* and *a* are elements of *G* the notation w^a would indicate the element $a^{-1}wa$. A. Miasnikov and P. Schupp [5] complicated this design by using extensions of the base groups. Vladimir Shpilrain and Alexander Ushakov analyzed all kinds of attacks [1] on this protocol. The 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. We know that if CSP problem is tractable in a group *G* then problem of finding w^{ab} by given $w,\ \ w^{a}=a^{-1}wa,\ w^{b}=b^{-1}wb$ is also tractable 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. All main analytical and constructive results belong to R. V. Skuratovskii.

Alexei Miasnikov and Paul Schupp [5] improved the protocol using HNN extension of groups. We use minimal non-abelian *p*-groups [6,7] for this goal. We show that no efficient 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}.

We recall that in modular arithmetic, the integers coprime to *n* which belong to the set $\{0,1,\ldots,n-1\}$ of n non-negative integers form a group under multiplication modulo *n*, called the multiplicative group of integers modulo ***n***. The elements of this group can be thought of as the congruence classes, also known as *residues* modulo *n*, that are relatively prime to *n*.

For an effective computation in *G* this group has to satisfy to the following conditions:

1. Elements of *G* allow efficient coding and can be effectively multiplied.
2. There must be an effective algorithm for checking the equality of the elements of the group.

Metacyclic Miller-Moreno *p*-group has structure $\langle a\rangle\rtimes\langle b\rangle$ and the following representation $G=\left\langle a,b\ \middle|\ a^{P^{m}}=e,b^{P^{n}}=e,\ b^{-1}ab=a^{1+p^{m-1}},\ m\geq 2,\ n\geq 1\right\rangle$, where is p prime. The generators a,b can be chosen as two arbitrary non commuting elements [6,7,8]. Since the group has the structure of a semidirect product of additive cyclic groups, their elements can be effectively represented coordinatewise that is (g,h), where $g\in Z_{p^{m}}$ and $h\in Z^{*}_{p^{n}}$. Notice that Metacyclic Miller-Moreno *p*-group is a **minimal non abelian group** in the class of metacyclic groups. Recall that a **metacyclic group** is a group *G* having a cyclic normal subgroup *N*, such that the quotient *G*/*N* is also cyclic. Metacyclic group has the presentation $G=\left\langle a,b\ \middle|\ a^{P^{l}}=b^{P^{m}}=e,\ b^{-1}ab=a^{1+p^{k}},1\leq k,\ m-k\leq l\right\rangle$. In each coordinate, there is an additive group of residues modulo finite. Analogously, $Aut(Z_{p^{m}})\simeq Z^{*}{}_{p^{m}}$, where $Z^{*}{}_{p^{m}}$ is the multiplicative subgroup of group $Z_{p^{m}}$. Thus, condition (1) is satisfied. The fulfillment of condition 2) will be shown in the Complexity of CSP problem section. The main reason of effectiveness of computation in $Z_{p^{m}}$ is quick reduction by modulo p that is $\log_{2}^{2}p^{m}=m\log_{2}^{2}p$. Analogously in the multiplicative group $Z^{*}_{p^{n}}$ one operation takes $2\log_{2}^{2}p^{\varphi(n)}=2\varphi(n)\log_{2}^{2}p$.

For designing a key exchange algorithm based on non-commutative DH problem [4] it have to be an effective algorithm for the computation of conjugated elements. Due to the relation in metacyclic group, which define the homomorphism $\varphi:\langle b\rangle\rightarrow Aut(\langle a\rangle)$ to the automorphism group of $A=\langle a\rangle$, we obtain 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 for checking of equality of elements.

Indeed, 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*.

We consider non-commutative generalization of CDH problem [1,2] on base of metacyclic group *G* 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.

2. Problem Solution

A. Computation of conjugacy class size

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 [4]. Due to the relation in metacyclic group, which define the homomorphism φ:⟨*b*⟩→Aut(⟨*a*⟩) 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 an effective method of checking the equality of elements due to cyclic structure of subgroups *A*=⟨*a*⟩ and *B*=⟨*b*⟩ 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* is quick operation. It is well-known that each finite cyclic group is isomorphic to the correspondent additive cyclic group modulo *n* residue $\mathbb{Z}_n$ (or Z_n). In this group, the equality of elements can be checked effectively by reducing the elements of the module group. The main reason of effectiveness of computation in Z_{p^m} is quick reduction by modulo p that is $\log_2^2 p^m = m\log_2^2 p$. Analogously in the multiplicative group $Z^*_{p^n}$ one operation takes $2\log_2^2 p^{\varphi(n)} = 2\varphi(n)\log_2^2 p$.

For crypto stability (NP-hardness) of DL or equivalent conjugacy problem in a non-commutative group *G* it have to be enough large length of conjugacy class of the given base element $w\in G$. As greater a number of conjugacy classes $N_G(w_i)$ for base elements w_i as greater be key-space of such system. To construct the key-space, two subsets of mutually commuting elements S_1 and S_2 are selected that give as many pairs of mutually commuting elements as possible. To key-space be enough big sizes of S_1 and S_2 be as grater as possible. Therefore, the orders of the subsets S_1 and S_2 should be as large as possible in comparison with the order of the group, i.e. index of the subgroups $H_1=\langle S_1\rangle, H_2=\langle S_2\rangle$ have to be as minimal as possible in G. The metacyclic and non-metacyclic Miller-Morreno groups have this property. Notice that metacyclic group of Miller-Moreno has order p^{n+m} [6,7], and the order of its center is p^{n+m-2}. Hence, we can choose subgroups subgroups $H_1=\langle S_1\rangle, H_2=\langle S_2\rangle$, where $S_1\cap S_2=e$, with an order of about $L=\frac{p^{n+m-2}}{2}$ and generate $(C_L^1)^2$ pairs of private keys.

B. Proof of NP-hardness of the conjugacy problem in G

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 [4]. Due to the relation in metacyclic group, which define the homomorphism φ:⟨*b*⟩→Aut(⟨*a*⟩) 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*=⟨*a*⟩ and *B*=⟨*b*⟩ in this group *G*. We also have an effective method of checking the equality of elements in the additive group Z_n because of reducing by finite modulo *n*.

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 it has to be enough long orbit of the given base element $w\in G$.

In metacyclic group G that has structure of a semidirect product $G=B\ltimes_\varphi=\langle b\rangle\ltimes_\varphi\langle a\rangle$ elements of *G* act by inner automorphism φ:⟨*b*⟩→Aut(⟨*a*⟩) on an element $h\in A$ such that $h\notin Z(A)$. The element h is on second coordinate of an presentation of element $w\in G$ which has the form $w=(g,h)$, where $w\notin Z(G)$. Let h be equal to a or to a^k, where k is coprime with p^m. For the problem of of conjugacy in non-commutative group G to be NP-hard, the orbit of the given base element $w \in G$ (or length of conjugacy class of w) must be big enough, for stability of this problem.

Theorem 1. The length of conjugacy class of described above an element *w* of *G* is equal to *p*.

Proof. Recall that the inner automorphism in *G* is determined by the formula $b^{-1}ab = a^{(1+p^{(m-1)})}$. We recall the structure of minimal non-abelian Metacyclic group, namely, $G = B \ltimes_{\varphi} A$, where A=⟨a⟩ and B=⟨b⟩ are finite cyclic groups. Therefore, the formula $b^{(-1)}ab = a^{(1+p^{(m-1)})}$ defines a homomorphism φ 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 $\mathbb{Z}_n$ (or Z_n). In this group, the equality of elements can be checked effectively by reducing the elements of the module group.

Consider the orbit of element *w* under action by the conjugation. The length of such orbit can be found from the 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 $(1+p^{(m-1)})^s \equiv 1(mod p^m)$ and taking into account the relation $a^{p^m} = e$ and

$$C_s^2 p^{(2(m-1))} + ... + p^{(s(m-1))} =$$
$$= p^m \left(C_s^2 p^{m-2} + ... + p^{(s-1)m-s} \right) \equiv 0(mod p^m),$$

we obtain that

$$1 + C_s^1 p^{(m-1)} + C_s^2 p^{(2(m-1))} + ... + p^{(s(m-1))} \equiv 1(mod p^m),$$

where $s \le p$. Taking into the consideration

$$1 + C_s^1 p^{(m-1)} = 1 + sp^{(m-1)} \equiv 1(mod p^m)$$

holds if and only if $s = p^j, \ j \in N$ we obtain such minimal s. In light of this, we notice that the minimal s when the congruence $w^{(1+p^{(m-1)})^s} \equiv w(mod p^m)$ 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.

According to F. Menegazzo [19] in each metacyclic group G splitting over $N_p = \langle a \rangle$ an order of subgroup generated by such automorphism is equal to p^{m-s} we can choose $k = m-2$ therefore $p^{m-(m-2)} = p^2$.

Using of greater set of generated common key increases entropy of key space because distribution of keys became to be more uniform. Thus, we have proven that CSP problem in the group G (with efficiently solvable word problem) is intractable. A solution of the word problem in the minimal non-abelian Metacyclic group follows from embedding of multiplicative group $Z^*_{p^m} \simeq Aut(Z_{p^m})$ in Z_{p^m}. It is known that the problem of words in Z_{p^m} is tractable. Taking into account the structure of metacyclic *p*-group of Miller-Moreno $G = B \ltimes_{\varphi} A$ and orders of its subgroups A and B which are p^m and p^n [6,7] we have order of G is p^{n+m}.

Consider non-metacyclic *p*-group of Miller-Moreno.

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

This group has the structure $G = (\langle a \rangle \times \langle c \rangle) \rtimes \langle b \rangle$ and the following representation $G = \left\langle a, b \middle| a^{p^n} = b^{p^m} = c^p = e, \ [a,b] = c, \ b^{-1}cb = c \right\rangle.$

To find a length of orbit of action by the 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 $a^j c^j$ occurs through *n* conjugations of this word by b, where $1 \le j \le p$. Therefore, the length of the orbit is p.

Corollary 1. A non-abelian special and extra-special *p*-group [15] P of order p^3 having presentation:

$$P = \left\langle a,b \middle| a^p = b^p = c^p = e, [a,b] = c, b^{-1}cb = c \right\rangle$$

has the same length of conjugacy class of non-central element *w, where exist such* $u \in G$ *that* wu^{-1} belonging to **focal subgroup** of G.

Corollary 2. The length of conjugacy class of described above an element *w* of metacyclic group is equal to p^{m-k}.
The proof is similar as in Theorem 1 but we consider the congruence $w^{(1+p^{(m-k)})^s} = w$.
For instance another metacyclic group with inner automorphism $b^{(-1)}ab = a^{(1+p^{(m-2)})}$ having length of conjugacy class p^2 can be applied for generating greater number of common keys [18] instead of Miller Moreno groups are described in [6].

3. Key establishment protocol

Let S_1, S_2 denote subsets from G consisting 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, these subgroups are mutually commutative too.

Consider base steps of protocol

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

Alice chooses a random element x from the subgroup H_1 and computes w^x. She then sends it to Bob.

Bob chooses random element y from the subgroup H_2 and computes w^x. He then sends 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, the common key [8, 9] w^{xy} was successfully generated.

Note that it is not sufficient to solve an apparently easier problem of finding elements $u, v \in G$ such that $uwv = x^{-1}wx = h$ or another words solve **decomposition problem** [1] in this group. After, apply it for man in the middle attack during key exchange steps. But such groups are not divisible, therefore, equation $uwv = h$ is not solvable in polynomial time [7, 8, 14, 16, 17] in *G*.

4. Complexity of CSP problem in the Metacyclic group

But if an analytic will use for cryptoanalysis solving of conjugacy search problem the method of reduction to solving of decomposition problem [1] then it leads us to solving of discrete logarithm problem in the group that have structure of a semidirect product ot multiplicative group Z_{p^n} and Z_{p^m}. Due to the properties of a semidirect product the solution to this problem reduces to solving the discrete logarithm problem in the automorphism group $Aut(Z_{p^m}) \simeq Z^*_{p^m}$, where $Z^*_{p^m}$ is the multiplicative group of group Z_{p^m}. This problem is NP-hard even in the *p*-group 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 $O\left(2p\log_2(p^{m-1}+1)m\log_2^2 p\right)$. 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 $\log_2^2 p^m = m\log_2^2 p$. Thus, condition 2) is satisfied. Since the length of the element conjugacy class under the action of conjugation of the active group as proved in

Theorem 1 is equal to *p*. Since the number of all possible pairs keys of private keys is p^{n+m-1}.

Note that it is not sufficient to solve an apparently easier problem of finding elements $u,v \in G$ such that $uwv = x^{-1}wx = h$ or another words solve **decomposition problem** [1] in this group. If one apply it for providing the man in the middle attack during key exchange steps. More details, if one try to solve the decomposition problem instead of solving the CSP $x^{-1}gx = h$, then we have to take into account that G is not divisible group [1]. To solve the decomposition problem we need to solve the algebraic expressions $uhv = g$ using the properties of groups. If we denote uh by a, then choosing v we transform decomposition problem to solving equation $av = g$ over group *G*. This problem is equivalent to DLP in *G* that has structure of semidirect product with inner automorphism $b^{-1}ab = a^{1+p^{m-1}}$, which is computationally complex operation. Thus, our protocol it not vulnerable for the attack of the man in the middle by solving the decomposition problem [1] of key exchange.

5. Results

The key exchange protocol based the effective computation in *G* group has been constructed. The key exchange protocol was upgraded by applying the effective computational *G* group in the base of the protocol. We additionally extend the key space by constructing the group closure of the sets S_1 and S_2, which were used by the authors [2–4]. Due to our improvements, this protocol is not vulnerable for such attacks as the man in the middle and brute force. Since the order of metacyclic group of Miller-Moreno is p^{n+m} with the index $[G:Z(G)] = p^2$ [6, 7, 18], then the order of its center is p^{n+m-2}. Therefore, the size of key space of the protocol based on metacyclic group is p^{n+m-2}. By analogous reasons size of key space of the protocol based on metacyclic group is p^{n+m-1}. The constructed algorithm could be used in multi agent-based system for securing of campus and big areas [20].

6. Conclusion

We can chose mutually commutative H_1, H_2 as a commutative subgroups of $Z(G)$. As outlined above x, y as components of key a chosen from H_1, H_2. According to [6] we have $Z(G) = p^{n+m-2}$ so size of key-space is $O\left(p^{n+m-2}\right)$. Note that size of key-space can be chosen as some arbitrary large number through the choice of parameters *p*, *n*, *m*.

References

[1] Vladimir Shpilrain And Alexander Ushakov.: The conjugacy search problem in public key cryptography: Unnecessary and Insufficient.. *Applicable Algebra in Engineering*. 22 (17), pp. 285–289, (2006).

[2] Gu, L. Wang, L., Ota, K., Dong, M., Cao Z. and Yang, Y.: New public key cryptosystems based on non-abelian factorization problems, *Secur. Commun. Netw*. 6 (7), pp. 912–922, 2013.

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

[4] L. Gu and S. Zheng.: Conjugacy systems based on nonabelian factorization problems and their applications cryptography, *J. Appl. Math*. 6 pp. 1–10. 2014.

[5] Miasnikov A., Schupp P.: Computational complexity and the conjugacy problem. *Computability* 6(4), pp. 307-318, 2017.

[6] Raievska, I., Raievska, M. Sysak. Y. P.: Finite local nearrings with split metacyclic additive group. *Algebra Discrete Math*., 22 (1), pp. 129–152. (2016). F.: Contribution title. In: 9th International Proceedings on Proceedings, pp. 1–2, 2010.

[7] Miller, G. A.: Groups which contain an abelian subgroup of prime index. In: *Biographical memoirs*. National academy of sciences. 1936, pp. 21–32.

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

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

[10] 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 263, pp. 311–323, 1986.

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

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

[13] Skuratovskii, R.: Corepresentation of a Sylow p-subgroup of a group S_n. *Cybernetics and systems analysis*, 1, pp. 27–41, 2009.

[14] Skuratovskii, R.: The Derived Subgroups of Sylow 2-Subgroups of the Alternating Group and Commutator Width of Wreath Product of Groups. *Mathematics*, Basel, Switzerland, № 8(4), pp. 1–19, 2020.

[15] Ward, D.: *Special p-groups: Homology Groups, Pi-product Graphs, Wreath Products*. Manchester Institute for Mathematical Sciences School of Mathematics. July, 2015.

[16] Skuratovskii, R. V., Osadchyy V. Order of Edwards and Elliptic Curves Over Finite Field. *WSEAS Transactions on Mathematics*, Volume 19, pp. 253-264, 2020.

[17] Gnatyuk, V. A. Mechanism of laser damage of transparent semiconductors. Physica B: *Condensed Matter*,. pp. 308-310, 2001.

[18] Baginski, C., Malinowska, I., On groups of order p^n with automorphisms of order p^{n-2}. *Demonstratio Mathematica*. 29 (3), pp. 565–575, 1996.

[19] Federico Menegazzo. Automorphisms of p-groups with cyclic commutator subgroup Rendiconti del Seminario Matematico della Università di Padova, tome 90 (1993), p. 81-101

[20] A Multi Agent-Based System for Securing University Campus: *Design and Architecture - IEEE Conference* Publication. 2019-12-17. doi:10.1109/ISMS.2010.25.