The Conference of Young Scientists «Pidstryhach Readings – 2020», May 26–28, 2020, Lviv

UDC 512.14

AN APPLICATION OF MILLER MORENO GROUPS TO GENERALIZATION OF DIFFIE–HELLMAN PROTOCOL

Ruslan Skuratovskii[1], Volodymyr Osadchyy[1], Aled Williams[2]

[1]Igor Sikorsky Kyiv Polytechnic Institute, r.skuratovskii@kpi.ua, vo@it-gravity-vo.com

[2]Cardiff University, UK, williamsae13@cardiff.ac.uk

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 of common key in non-commutative group with 2 mutually commuting subgroups are constructed by us. The results of Ko K, Lee S are improved and generalized on base of metacyclic group G of type Millera Moreno.

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]. We know that if the CSP problem is tractable in group G, then the problem of finding w^{ab} from given w, $w^a = a^{-1}wa$, $w^b = b^{-1}wb$ is tractable too.

Metacyclic Millera Moreno group has 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. As a generators a, b can be chosen two arbitrary non commuting elements [4, 5,6].

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

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

Since the group has the structure of a semidirect product of aditive cyclic groups, their elements can be effectively represented coordinatewise. 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 item.

Find the complexity of CSP problem in this group. 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 homomophism $\varphi:\langle b\rangle \to Aut(\langle a\rangle)$ 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 $m>1$.

Let S_1, S_2 are 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 choose a random element x from the subgroup H_1 and computes w^x. She then sends it to Bob. Bob choose 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 [6] w^{xy} was successfully generated.

1. *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. 2013. – Vol 6, No. 7. – P. 912–922.
2. *J.-M. Bohli, B. Glas and R. Steinwandt.* Towards provable secure group key agreement building on group theory, Cryptology ePrint Archive: – 2006/ 79.
3. *Skuratovski R.* The Derived Subgroups of Sylow 2-Subgroups of the Alternating Group and Commutator Width of Wreath Product of Groups// Mathematics, Basel, Switzerland, – 2020. – No. 8 (4). – P. 1–19.

ЗАСТОСУВАННЯ ГРУП МІЛЛЕРА-МОРЕНО ДО УЗАГАЛЬНЕННЯ ПРОТОКОЛУ ДІФФІ -ХЕЛЛІМАНА

Ми розглядаємо некомутативне узагальнення проблеми CDH [1,2] на основі метациклічної групи типу Міллера Морено (мінімальна неабелева група). Ми доводимо, що проблема кон'югації в цій групі є нерозв'язною. В роботі показано що проблема спряженості в цій метациклічной групі є NP-складною