DOI: https://doi.org/10.30837/csitic52021232176

Hard problems for non-abelian group cryptography

Yevgen Kotukh[1]
Gennady Khalimov[2]

[1]Sumy State University, 2 Rimskogo-Korsakova street, Sumy, 40000, Ukraine, yevgenkotukh@gmail.com
[2]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, hennadii.khalimov@nure.ua

Abstract. *The security of the DH key exchange protocol and many other public key cryptosystems such as RSA, ElGamal and ECC is based on the assumption that complex mathematical problems such as factorization (FP), discrete logarithm over finite fields (DLP), or elliptical curves (ECDLP) are intractable. The implementation of Shor and Grover's algorithms reduces the security of cryptosystems based on the intractability of these problems.*

Keywords: *intractable problems, search problem, conjugacy problem, non-abelian groups, Shor algorithm.*

I. INTRODUCTION

Modern results in solving the problem of quantum computer construction motivate cryptoscientists to review existing approaches and define the most effective ones for post-quantum cryptography demands. One of such promising research priority is the study of the cryptosystems based on non-abelian groups. In 1985, the innovative design of public key cryptosystem based on non-abelian was proposed by Wagner and Magyarik [1]. For almost two decades, multiple non-Abelian groups have been discussed to develop effective cryptographic systems.

Presumptions about the intractability of some cryptographic problems do not mean the security of real cryptosystems based on these problems. Instead, they must be embedded in the implementation of certain cryptographic primitives. In fact, security is a composite concept and can be divided into several different properties.

Many encryption schemes have now been proposed based on FP or DLP / ECDLP insolubility assumptions. Some designs further use two-line interface to increase functionality and performance, but the security of these designs is also based on the assumption that ECDLP is insoluble. Unfortunately, FP and DLP, as well as ECDLP, can be effectively solved by Shore's quantum algorithms and its extensions.

Thus, the actual task is to develop new encryption schemes with the mathematically proven security in terms of application of quantum realization of Shor and Grover algorithms. Although two lattice-based encryption schemes have recently been announced that have advantages in counteracting known quantum algorithms and attacks, there is still room for more efficient cryptosystems. Non-Abelian group cryptography with a public key is a relatively new and promising area of research for the construction of post-quantum solutions. In recent decades, new cryptographic solutions based on braid groups and factorization in finite permutation groups have been proposed, as well as cryptosystems based on multiparameter groups and logarithmic signatures for the entire group in [2–6].

This paper provides an overview of potentially complex problems for non-Abelian groups, the insolvability of which underlies their implementation.

II. HARD PROBLEMS OF NON-ABELIAN CRYPTOGRAPHY

In this section, we'll look at potentially hard problems for non-abelian groups. Cryptographic systems that can be built on the basis of these hard problems can be considered as candidates for post-quantum public key cryptosystems.

Definition 1. (**Diffie Problem-Hellman, DHP**). Let G be a group. If $g, g^x, g^y \in G$ find the value g^{xy}.

Definition 2. (**The discrete logarithm problem, DLP**). Let G be a group. If $g, h \in G$ such that $h = g^x$ and g, h are known. Find the integer x.

Definition 3. (**Conjugacy Search Problem, CSP**). Let G be a non-abelian group. Let $g, h \in G$ such that $h = g^x$ for some $x \in G$. Find x with conditions that g^x denotes $x^{-1}gx$.

The DH and DLP problems are computationally complex for a classic computer, but the security of cryptosystems that are based on these problems was significantly reduced through the implementation of quantum attacks using the Shor and Grover algorithms.

Definition 4. (**Factorization Problem, FP**). Let G be any non-abelian finite group with identity e. Let $g, h \in G$ be two random elements, so that $\langle g \rangle \cap \langle h \rangle = \{e\}$. The factorization problem with respect to G, g, h is denoted as $FP^G_{g,h}$, is to divide this product $g^x h^y \in G$ into a pair $\left(g^x, h^y\right) \in G^2$, where are x and y are arbitrary integers chosen randomly.

Definition 5. (**Computational Diffie-Hellman Problem, CDH**). Let G be any non-abelian finite group with identity e. Let $g, h \in G$ be two random elements, so that $\langle g \rangle \cap \langle h \rangle = \{e\}$. The CDH problem (denoted as $CDH^G_{g,h}$) is to recover $g^{a+c}h^{b+d}$ from the pair of $\left(g^a h^b, g^c h^d\right) \in G^2$ where a, b, c, d are arbitrary integers chosen randomly.

Definition 6. (**Diffie-Hellman Decision, DDH**). Let G be any non-abelian finite group with identity e. Let $g, h \in G$ be two random elements, so that $\langle g \rangle \cap \langle h \rangle = \{e\}$.

The DDH problem (denoted as $DDH^G_{g,h}$) with respect to G, g, h is to distinguish the following distribution

$$\Delta_0 \triangleq \left\{\left(g^a h^b, g^c h^d, g^z h^y\right) : a, b, c, d, z, y \in_R \mathrm{Z}\right\}$$

with the next one

$$\Delta_1 \triangleq \left\{\left(g^a h^b, g^c h^d, g^{a+c} h^{b+d}\right) : a, b, c, d \in_R \mathrm{Z}\right\}$$

Definition 7. (**Gap Computational Diffie-Hellman Problem, Gap-CDH**). Let G be any non-abelian finite group with identity e. Let $g,h \in G$ be two random elements, so that $\langle g \rangle \cap \langle h \rangle = \{e\}$. The Gap-CDH problem (denoted as $gap-CDH_{g,h}^{G}$) with respect to G,g,h is to solve the $CDH_{g,h}^{G}$ problem, given access to the oracle, which solves the $DDH_{g,h}^{G}$ problem.

Definition 8. (**Subgroup Conjugator Search Problem, SCSP**). Let G be any non-abelian finite group with identity e. Let $g,h \in G$ be two random elements, so that $\langle g \rangle \cap \langle h \rangle = \{e\}$. The SCSP problem (denoted as $SCSP_{g,h}^{G}$) with respect to G,g,h is to recover g^x from the given pair $\left(h^y, g^x h^y g^{-x}\right) \in G^2$ where x,y are arbitrary integers chosen randomly.

Definition 9. (**Subgroup Conjugacy Deciding Problem, SCDP**). Let G be any non-abelian finite group with identity e. Let $g,h \in G$ be two random elements, so that $\langle g \rangle \cap \langle h \rangle = \{e\}$. The SCDP problem (denoted as $SCDP_{g,h}^{G}$) with respect to G,g,h is to distinguish the following distribution:

$$\Delta_2 \triangleq \left\{\left(h^b, g^a h^b g^c\right) : a,b,c \in_R \mathrm{Z}\right\}$$

with the next one

$$\Delta_3 \triangleq \left\{\left(h^b, g^a h^b g^{-a}\right) : a,b \in_R \mathrm{Z}\right\}$$

Definition 10. (**Conjugated Computational DH Problem, CCDH**). Let G be any non-abelian finite group with identity e. Let $g,h \in G$ be two random elements, so that $\langle g \rangle \cap \langle h \rangle = \{e\}$. The CCDH problem (denoted as $CCDH_{g,h}^{G}$) with respect to G,g,h is to recover $g^{a+c}h^b g^{-a-c}$ from the given triple $\left(h^b, g^a h^b g^{-a}, g^c h^b g^{-c}\right) \in G^3$, where a,b,c,d are arbitrary integers chosen randomly.

Definition 11. (**Conjugated Decisional Diffie-Hellman's Problem, CDDH**). Let G be any non-abelian finite group with identity e. Let $g,h \in G$ be two random elements, so that $\langle g \rangle \cap \langle h \rangle = \{e\}$. The CDDH problem (denoted as $CDDH_{g,h}^{G}$)with respect to G,g,h is to distinguish the following distribution

$$\Delta_4 \triangleq \left\{\left(h^b, g^a h^b g^{-a}, g^c h^b g^{-c}, g^d h^b g^{-d}\right) : a,b,c,d \in_R \mathrm{Z}\right\}$$

with the next one

$$\Delta_5 \triangleq \left\{\left(h^b, g^a h^b g^{-a}, g^c h^b g^{-c}, g^{a+c} h^b g^{-a-c}\right) : a,b,c \in_R \mathrm{Z}\right\}$$

Definition 12. (**Gap Conjugated Computational Diffie-Hellman, Gap-CCDH**). Let G be any non-abelian finite group with identity e. Let $g,h \in G$ be two random elements, so that $\langle g \rangle \cap \langle h \rangle = \{e\}$. The Gap-CCDH problem (denoted as $gap-CCDH_{g,h}^{G}$) with respect to G,g,h is to solve the problem $CCDH_{g,h}^{G}$, given access to the oracle that solves the $CDDH_{g,h}^{G}$ problem.

The most frequently discussed non-abelian cryptographic proposals include matrix groups, braid groups, logarithmic signatures (LS) and algebraic erasers (AE). In addition to common hard problems and setting the conditions to solving them, there are a number of problems for these cryptographic proposals that need to be addressed and discussed in further research.

III. CONCLUSION

The use of non-abelian groups as a basis for post-quantum cryptosystems has a great research interest. The use and application of quantum attacks on classical intractable problems can be significantly reduced in the class of non-abelian group cryptography. A big practical interest is observed to construct encryption/decryption and electronic signature ready post-quantum cryptosystem within a basis of non-abelian cryptography.

REFERENCES

[1] N. R. Wagner, M. R. Magyarik, "A public key cryptosystem based on the word problem," in Advances in Cryptology (CRYPTO'84), Lecture Notes in Computer Science, vol. 196, pp. 19-36, 1985

[2] Tzu-Chun Lin. "A Study of Non-Abelian Public Key Cryptography" International Journal of Network Security, Vol.20, No.2, PP.278-290, Mar. 2018

[3] Haibo Hong1⋆, Jun Shao1, Licheng Wang2, Haseeb Ahmad2 and Yixian Yang "Public Key Encryption in Non-Abelian Groups" https://arxiv.org/abs/1605.06608v1

[4] G. Khalimov, Y. Kotukh, S.Khalimova "MST3 cryptosystem based on the automorphism group of the hermitian function field" // IEEE International Scientific-Practical Conference: Problems of Infocommunications Science and Technology, PIC S and T 2019 - Proceedings, 2019, pp. 865–868.

[5] G. Khalimov, Y. Kotukh, S.Khalimova "MST3 cryptosystem based on a generalized Suzuki 2 - Groups" // CEUR Workshop Proceedings, 2020, 2711, pp. 1–15.

[6] G. Khalimov, Y. Kotukh, S.Khalimova "Encryption scheme based on the automorphism group of the Ree function field" 2020 7th International Conference on Internet of Things: Systems, Management and Security, IOTSMS 2020, 2020, 9340192