International Journal of Pure and Applied Mathematics

Volume 58 No. 1 2010, 21-23

APPLICATIONS OF GROUP THEORY IN CRYPTOGRAPHY

Delaram Kahrobaei[1 §], Michael Anshel[2]

[1,2]Department of Mathematics (City Tech.)
Doctoral Program in Computer Science (CUNY Graduate Center)
City University of New York
365, Fifth Avenue, New York, NY 10016, USA
e-mail: dkahrobaei@gc.cuny.edu

[2]Department of Computer Science
City College of New York
138-th Street and Convent Ave., New York, NY 10031, USA
e-mail: csmma@cs.ccny.cuny.edu

Abstract: The paper presents an exposition of applications of non-Abelian groups in cryptography.

AMS Subject Classification: 20-02
Key Words: polycyclic groups, cryptography

*

One of the important problems in cryptology is the key exchange problem. The basic aim of key exchange problems is that two people who can only communicate via an insecure channel want to find a common secret key. Key exchange methods are usually based on one-way functions; that is, functions which are easy to compute (with polynomial complexity), while their inverses are difficult to determine (with exponential complexity). Most of the practical one-way functions have a common problem, i.e. it is often easy to find a one-way function with a polynomial complexity, but showing that there is no inverse function with similar complexity or practicality is usually the difficult part of the project,

Received: November 13, 2009

[§] Correspondence author

since the best inverse function might just not have been discovered yet. Hence it is of interest to investigate new one-way functions. The well-known key exchange problems are Diffie-Hellman (was found in 1976) and El-Gamal (was found in 1984) key exchange problems. The security of these problems are based on the discrete logarithm problem as well as DDH the decision Diffie-Hellman and the platform groups are cyclic groups of large prime order (finite fields). The Discrete lo Logarithm Assumption (DL) is the following: given $g^x \bmod q$, it is hard to compute x. The Decisional Diffie Hellman Assumption (DDH) is the following: It is hard to distinguish triples of the form (g^x, g^y, g^z) for random x, y, z in Z_q (finite field of order q) from triples of the form (g^x, g^y, g^{xy}) for random x, y in Z_q. Note that the DDH is at least as strong as strong as the DL. New one-way functions which employ the complexity of certain decision and search problems in non-Abelian combinatorial group theory was introduced in [1] (by two group theorists and a number theorists!). Particularly, algebraic key establishment protocols based on the difficulty of solving equations over algebraic structures are described as a theoretical basis for constructing public-key cryptosystems. They particularly proposed Braid groups for a new platform for cryptology. The decision problems they used for this purpose are word problem (WP) and the search conjugacy problem (SCP). The WP: Let G be a group given by a finite presentation. Does there exist an algorithm to determine if an arbitrary word w in the generators of G whether or not $w_G = 1$? More specifically they used that every word in a Braid group has a normal form. The SCP: Let G be a group given by a finite presentation. Does there exist an algorithm to determine z in G given the fact that an arbitrary pair of words u and v in the generators of G defines conjugate elements of G via conjugator z in G? One can show easily that SCP is always at least as difficult as the WP, and this could be used for creating new one-way functions. By the celebrated result of Novikov and Boone, there are groups for which these questions are undecidable in general: they cannot be answered algorithmically. The decision problems in combinatorial group theory have shown much potential for this purpose [4]. Another reason is for welcoming new one-way functions and new platform groups, using Shor's algorithm the discrete log problem and prime factorization problem admit polynomial-time quantum algorithm. That leaves the current cryptosystem in danger if the quantum computers are to be built! Non-commutative group theorists have been working in the field of non-commutative cryptography for about ten years, but a class of groups which provides a provably secure basis for the non-commutative protocols is not known yet. In 2004, Kahrobaei (one of the authors) together with Bettina Eick proposed polycyclic groups for new platform for cryptology [2]. These are natural generalizations of cyclic groups but are much more complex in their structure. Hence their algorithmic theory is more difficult. In 2006 Kahrobaei and Khan, proposed a non-commutative key-exchange scheme which generalizes the classical ElGamal Cipher to polycyclic groups [3].

References

[1] Iris Anshel, Michael Anshel, Dorian Goldfeld, An algebraic method for public-key cryptography, *Math. Res. Lett.*, **6** (1999), 287-291.

[2] Bettina Eick, Delaram Kahrobaei, Polycyclic groups: A new platform for cryptology?, *Math.GR/0411077* (2004), 1-7.

[3] Delaram Kahrobaei, Bilal Khan, A non-commutative generalization of the elgamal key exchange using polycyclic groups, *Proceeding of IEEE* (2006), 1–5.

[4] A. Myasnikov, V. Shpilrain, A. Ushakov, *Group-Based Cryptography*, Birkhäuser (2008).