Group Theory in Cryptography

Maeve Dunne, Catherine Fraser and Ariea McDaid

Introduction

In the last few years, many papers have proposed cryptosystems based on group theoretic concepts. The idea of group-based cryptosystems is interesting and the different perspective leads to some worthwhile group theory. This poster aims to introduce the use of group theory in public key and symmetric key cryptography systems, with emphasis on **Braid Group Theory** and the **Diffie-Hellman Key Exchange**.

Basics of Cryptography

- Plain text: the original message
- Cipher text: the coded message
- Encryption: the process used for converting the plain text into the cipher text
- Decryption: restoring the plain text from the cipher text

The main technique used in cryptography is based on encryption and decryption. The methods of encryption/decryption fall into two categories: public key and symmetric key. In symmetric key algorithms, the encryption and decryption keys are known to both A and B. In public key cryptography, the encryption key is made public, but it is computationally infeasible to find the decryption key without information known only to B.

Braid Groups

In the last two decades a number of public key cryptosystems based on combinatorial group theoretic problems in braid groups have been proposed. Based on braid groups and its underlying problems, two cryptosystems were suggested by Anshel, Anshel and Goldfeld in 1999 and by Ko, Lee, Cheon, Han, Kong and Park in 2000. These cryptosystems initiated a wide discussion about the possibilities of cryptography in the braid group.

Those underlying problems were as follows:

. Conjugacy decision problem
. Conjugacy search problem
. Multiple simultaneous conjugacy search problem
. Decomposition problem

Some notable key exchange protocols come to mind when on the topic of braid groups:

1. The **Anshel-Anshel-Goldfeld** key exchange protocol which assumes that the conjugacy search problem is difficult. They used the images of braids under the coloured Burau representation of the braid group defined by Marton, instead of the braids themselves.
2. The **Diffie-Hellman** key exchange protocol which is based on the braid group and some commutative property of some of its elements. We will talk more about Diffie-Hellman later.

Although braid groups are not commutative, we can find large subgroups such that each element of the first subgroup commutes with each element of the second and indeed it is true that braids involving disjoint sets of strands commute.

Braid Groups

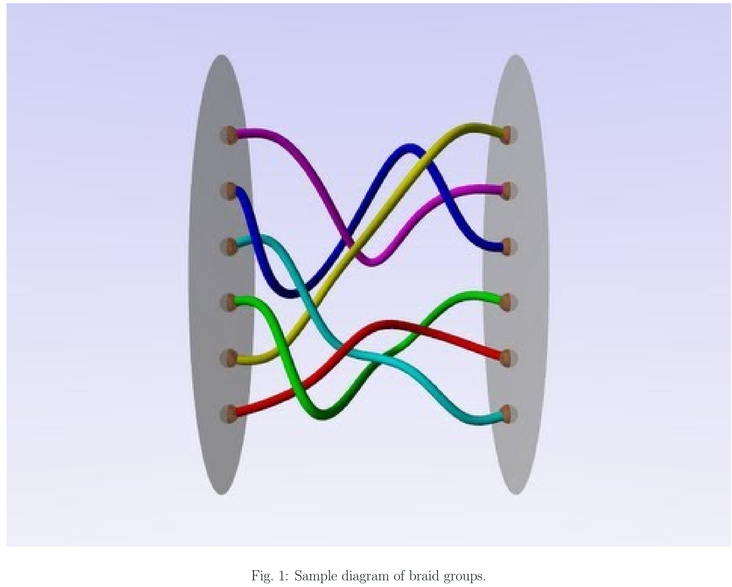

Fig. 1: Sample diagram of braid groups.

Anshel–Anshel–Goldfeld Key Exchange Protocol

Let G be a non-abelian group, and let elements $a_1, ..., a_k, b_1, ..., b_m \in G$ be public.

- Alice picks a private word x in $a_1, ..., a_k$ and sends $b_1^x, ..., b_m^x$ to Bob.
- Bob picks a private word y in $b_1, ..., b_m$ and sends $a_1^y, ..., a_k^y$ to Alice.
- Alice computes x^y and Bob computes y^x.
- The secret key is $[x, y] = x^{-1}y^{-1}xy$.

Note that Alice and Bob can both compute the secret commutator: Alice can premultiply x^y by x^{-1} and Bob can premultiply y^x by y^{-1} and then compute the inverse: $[x, y] = (y^{-1}y^x)^{-1}$.

References

1. "Use of Group Theory in Cryptography" Priya Arora; Assistant Professor, Department of Mathematics, S.D. (P.G) College,Panipat. Vol-2 Issue-6 2016
2. "Group Theory in Cryptography" Simon R. Blackburn, Carlos Cid and Ciaran Mullan. Department of Mathematics, Royal Holloway, University of London. January 25, 2010
3. "Diffie-Hellman Key Exchange Protocol, Its Generalization and Nilpotent Groups" Ayan Mahalanobis, Florida Atlantic University. August 2005
4. "New Directions in Cryptography" Whitfield Diffie and Martin E. Hellman, IEEE Transactions on Information Theory Vol. IT-22, No. 6, November 1976

Diffie-Hellman Key Exchange Protocol

"We stand today on the brink of a revolution in cryptography". This was the opening line of a paper published in 1979 by Whitfield Diffie and Martin Hellman, in which they proposed the first publicly known example of a public key cryptosystem; a system now known as the Diffie-Hellman key exchange. It stems from the Discrete Logarithm Problem, namely the complex problem of finding n when given g^n and g. The Diffie-Hellman key exchange can be explained nicely in terms of finite cyclic groups.
We take there to be two parties with no prior knowledge of each other, Alice and Bob, who wish to establish a shared secret key. The steps are as follows below, and a simple example has been included in blue.

1. Alice and Bob agree on a finite cyclic group G with a generating element g, and order n. For our example, let's take $G = (\mathbb{Z}/23\mathbb{Z})^X$, the multiplicative group of integers modulo 23, and the generating element $g = 5$ of this group.
2. Alice chooses a value for a, where a is a natural number and $a < n$, and computes g^a. She sends this value to Bob. Let's say she chooses $a = 4$, then g^a is $5^4 \bmod 23 = 4$. (It is a coincidence that in this case $g^a = a$).
3. Similarly, Bob chooses a natural number b, $b < n$, and computes g^b. He sends this value on to Alice. Bob chooses $b = 3$, so g^b is $5^3 \bmod 23 = 10$.
4. Alice computes $(g^b)^a$, Bob computes $(g^a)^b$, and now both parties are in possession of the shared private key g^{ab}. In our example, Alice computes $(10)^4 \bmod 23 = 18$ and Bob computes $(4)^3 \bmod 23 = 18$. The key is 18.

The choice of group G and generating element g, and the values of g^a and g^b are public knowledge, hence why the Diffie-Hellman key exchange is known as a public key exchange. However the numbers a and b are private and so, thanks to the Discrete Logarithm Problem, it is very difficult for an attacker to obtain the private key g^{ab}.

Logarithmic signatures

There is an *alternative* approach to generalising the Diffie–Hellman scheme: to find a more direct generalisation of the Discrete Logarithm Problem for groups that are not necessarily abelian.

Let G be a finite group, $S \subseteq G$ a subset of G and s a positive integer. For all $1 \leq i \leq s$, let $A_i = [\alpha_{i1}, ..., \alpha_{ir_i}]$ be a finite sequence of elements of G of length $r_i > 1$ and let $\alpha = [A_i, ..., A_s]$ be the ordered sequence of A_i.

We say that α is a *cover* for S if any $h \in S$ can be written as a product $h = h_1...h_s$, where $h_i = \alpha_{ik_i} \in A_i$. If such a decomposition is unique for every $g \in S$, then α is said to be a *logarithmic signature* for S.

One natural way to construct a logarithmic signature for a group G is to take a subgroup chain $1 = G_0 < G_1 < ... < G_n = G$, and let A_i be a complete set of coset representatives for G_{i-1} in G_i. Then $\alpha = [A_i, ..., A_n]$ is a logarithmic signature for G.