Journal of Applied Mathematics & Bioinformatics, vol.3, no.1, 2013, 83-97
ISSN: 1792-6602 (print), 1792-6939 (online)
Scienpress Ltd, 2013

Some aspects of group-based cryptography

Sotirios D. Hasapis[1] and Dimitrios Panagopoulos[2]

Abstract

This article was presented in Cryptography Conference 2012 of the Hellenic Military Academy. The article consists of two parts. In the first part is presented a short overview of group-based cryptography. In the second part the notions of group-based cryptography are used to present a secret sharing scheme.

Mathematics Subject Classification: 20, 94A60
Keywords: group-based cryptography; secret sharing; Dehn's problems

1 Introduction

In 1975 Diffie, Hellman and Merkle introduced public key cryptography. The basic idea is to use for encryption a so-called one way function, a function such that it is easy to compute $f(x)$ but difficult, in general, to compute $f^{-1}(y)$.

[1] e-mail: shasapis@gmail.com
[2] e-mail: dpanagop@yahoo.com

Article Info: *Received* : November 1, 2012. *Revised* : January 30, 2013
Published online : March 30, 2013

In 1976 Diffie and Hellman presented the Discrete Logarithm Key agreement protocol [7]. This protocol uses a finite cyclic group with generator g (the original implementation used the multiplicative group of integers modulo p as the basis group and a primitive root for g). A brief description of the scheme is given bellow.

Discrete Logarithm scheme

1. Alice and Bob agree, publicly, on a finite cyclic group G and a generating element g of G.
2. Alice randomly chooses an integer α and sends g^{α} to Bob.
3. Bob randomly chooses an integer β and sends g^{β} to Alice.
4. Bob computes $g^{\alpha\beta} = (g^{\alpha})^{\beta}$.
5. Alice computes $g^{\beta\alpha} = (g^{\beta})^{\alpha}$.

Since $K = g^{\alpha\beta} = g^{\beta\alpha}$, K may serve as a common key. The Discrete Logarithm Key agreement protocol is considered secure because it is, supposedly, difficult for an eavesdropper to compute $g^{\alpha\beta}$ from g^{α}, g^{β}. A problem that is connected (although not equivalent) to the discrete logarithm problem, i.e. the problem of recovering α from g and g^{α} [13, p. 6-7]. Koblitz [9] and Miller [12] independently suggested the use of the group of rational points of elliptic curves as a platform in 1985.

The most famous public key encryption protocol is RSA which was proposed by Rivest, Shamir and Adleman in 1977 [15].

RSA scheme

1. Alice chooses two primes p, q, calculates $n = pq$ and selects an integer $1 < e < \phi(n) = (p-1)(q-1)$ with $g.c.d(e, g) = 1$. She publishes n, e. Her secret key is an integer d such that $ed = 1 \mod \phi(n)$.
2. Bob encodes his message using integers $0 \leq m \leq n-1$. For every integer m, Bob sends $m^e \mod n$ to Alice.
3. Alice computes $m = m^{ed} = (m^e)^d \mod n$.

The basic mathematical tool behind RSA is Euler's theorem which states that for every integers n and a with $0 \leq a \leq n-1$, $a^{\phi(n)} = 1 \mod n$. RSA is considered secure because it is related to the integer factorization problem since the only known way to recover $m \mod n$ from $m^e \mod n$ is to calculate $m^{ed} = (m^e)^d \mod n$. And finding d, supposedly, requires knowledge of $\phi(n) = (p-1)(q-1)$ and hence the factorization of n.

Most common public key cryptosystems in use, such as presented above, are based on abelian groups. However, since computing power expands every day and new innovative lines of attack are invented, the security of many of them is questioned. For example, there exists a wide bibliography concerning attacks to the RSA cryptosystem [5]. And it is not wise to place all of one's eggs in the same basket. The wide use of only a few cryptosystems means that should a line of attack proved successful, the consequences would reach a huge number of people and certainly, the news would attract a great deal of media attention. This was the case for an announcement made by A. Shamir back in 1999 which proposed a way to break RSA [11, 19].

Therefore, research in new cryptographic methods is in demand. One such method uses the foundations of group theory, especially non-commutative structures as platforms. In section 2, after a brief overview of some basic definitions of group theory, we present a few cryptographic methods based on non-commutative groups. In section 3, we present a secret sharing scheme which was proposed by the second author [14] and it is based on group presentations and the word problem.

2 Non-commutative Algebraic Cryptography

2.1 Group presentations and normal forms

Some prerequisites for the use of a group as a platform, are the presentation of a group and the possibility to obtain a normal form for an element of the group with a specific presentation.

A **generator** g of a group G is any element of a subset $S \subset G$, called **generating set**, such that any other element of the group can be expressed in terms of S. The generators of a group G could be connected by some **relations**.

For example, the cyclic group of order 2 C_2 could be defined by an element g, as the generator of C_2, which is related to the identity element of G by the relation $g^2 = e$. A **presentation of a group** G consists of a generating set and some relations between those generators. Of course, for any group there is not a unique presentation. For example the next two presentations define the cyclic group of order 6:

$$(a : a^6 = 1)$$

$$(a, b : a^2 = 1, b^3 = 1, aba^{-1}b^{-1} = 1)$$

Although there is a way to pass from one presentation to another for isomorphic groups, using the Tietze transformations for example, this is not always trivial. A useful property of a group is the possibility of writing any element in a standard way that becomes easy for us to choose and manipulate elements. This is the notion of **normal form**. The existence of a normal form is a characteristic of free groups for example [16]. There are two necessary principles that need to be held by a normal form. The first one is uniqueness; every object must have exactly one normal form of a given type, as the second principle states that two objects of the same normal form have to be equal. For instance, in the additive group of integers it is known that every integer has a unique decomposition as a product of prime numbers, not taking in consideration the order of the product. This is a good way for representing an integer, with all the advantages described above.

Another extra, useful property of a group is the capability of effectively rewriting an element in normal form. In Thompson's Group, for example, there is such a rewriting system, that converts a given word to its normal form. Another such example is the braid group where there is not only one type of normal form, but different types of normal forms, each one useful for another reason. The early use of braid groups in cryptography is partly due to the development of different types of normal forms. Thus, the existence of a normal form is crucial for a platform group in cryptosystems. But what are other useful properties for a group to be chosen as the base of a cryptosystem? We will discuss this question in section 2.4. Let us see first the underlying problems in group-based cryptography.

2.2 Decision and Search problems in Group Theory

Fundamental decision problems formulated by Max Dehn [6] in 1911, being used for implementing a one-way function are presented below [10]. Let G be a group which presentation is given. Then:

- **The Word Problem**: for a word W given in terms of generators of G, find in a finite number of steps whether $W = 1$ or not.
- **The Conjugacy Problem**: for two given words W_1, W_2 on the generators of G, decide in a finite number of steps whether

$$W_1 = g^{-1}W_2g,\ for\ g \in G.$$

- **The Isomorphism Problem**: for two presentations G, G', decide in a finite number of steps whether the groups G, G' are isomorphic or not.

These problems are not solvable in general. The word problem is solvable in the following classes of groups: finite, polycyclic, one relator negative curvature, Coxeter, Braid, residually finite, finitely generated groups and others. The conjugacy problem expands the word problem, as the latter comes from the first one, just by substituting the word $W_1 = 1$. The isomorphism problem is believed to be the most difficult of Dehn's problems.

The important fact is that even though in some cases one od the problems stated above can be solved in a finite number of steps, it might be a difficult problem from a cryptographic point of view. So, one should know whether the problem could be solved in polynomial or subexponential time. In this way **search problems** emerge: Given a property P, known that there are objects with this property, try to find such an object.

2.3 Key Agreement Protocols based on non commutative groups

An analogue of Discrete Logarithm Problem (DLP) in group theory is the Conjugacy Search Problem (CSP): If G is a non-abelian group and $g, h \in G$ such that g and h are conjugate, find an element $y \in G$ so that the next equality occurs: $h = y^{-1}gy$. The CSP seems to be a really hard problem given an appropriate choice of a platform group. This choice is going to be discussed later on.

2.3.1 Ko et al. Key Agreement Protocol [8]

Suppose G is a non-abelian group chosen and $A, B \leq G$ commuting subgroups and let $g \in G$ be an element, all the above publicly known. A secret common key is developed by Alice and Bob, procceding as follows:

1. Alice selects $a \in A$, calculates $g^a = a^{-1}ga$ and sends g^a to Bob.

2. Bob selects $b \in B$, calculates $g^b = b^{-1}gb$ and sends g^b to Alice.

3. Each one computes $K_a = (g^b)^a$, $K_b = (g^a)^b = K$ which stands for the common secret key, as $ab = ba$ and hence $K_a = g^{ab} = g^{ba} = K_b$.

The platform group G chosen in this scheme is a very critical point. The authors Ko et al. used for instance the Braid group B_n. The real reason about that is that a good normal form for the elements of Braid groups exists.

2.3.2 Anshel et al. Key Agreement Protocol [1]

A non-abelian group G is used for this protocol too, but the need of any commuting subgroups is overtaken. So, except the group G, also elements $a_1, \ldots, a_k, b_1, \ldots, b_m \in G$ are made publicly known. The key establishment comes as follows:

1. Alice computes a private word $x = x(a_1, \ldots, a_k)$ on $a_1, \ldots, a_k$ and sends Bob $b_1^x, \ldots, b_m^x$, where b_i^x stands for the conjugate $x^{-1}b_ix$.

2. Bob computes a private word $y = y(b_1, \ldots, b_m)$ on $b_1, \ldots, b_m$ and sends Alice $a_1^y, \ldots, a_k^y$.

3. Then Alice computes $x(a_1^y, \ldots, a_k^y) = x^y = y^{-1}xy$ and Bob computes $y(b_1^x, \ldots, b_m^x) = y^x = x^{-1}yx$. The commutator $[x, y]$ stands for the common secret key K, as: $[x, y] = x^{-1}x^y$ and $[x, y] = (y^{-1}y^x)^{-1} = (y^{-1}x^{-1}yx)^{-1} = x^{-1}y^{-1}xy$ respectively.

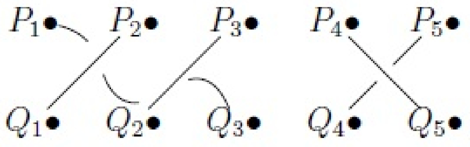

Figure 1: A 5-braid

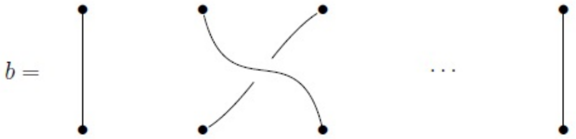

Figure 2: A n-braid b

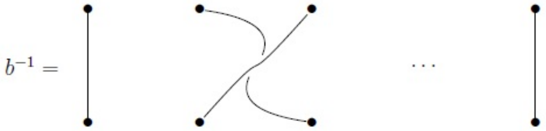

Figure 3: The inverse n-braid b^{-1}

An interesting implementation involves the braid groups. In particular, the n-braid group B_n is defined by the following group presentation.

$$B_n = \left\langle \sigma_1, \ldots, \sigma_{n-1} \left| \begin{array}{ll} \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j, & if\ |i-j| = 1 \\ \sigma_i\sigma_j = \sigma_j\sigma_i, & if\ |i-j| \geq 2 \end{array} \right. \right\rangle$$

Each element of B_n is called an n-braid. A n-braid can be displayed as a set of disjoint n strands all of which are attached to two horizontal bars at the top and at the bottom, so as each strand always heads downwards as one "walks" along the strand from the top to the bottom. The braid index is the number of strings. The multiplication ab of two braids σ_1 and σ_2 is the braid obtained by positioning σ_1 on top of σ_2. The identity e is the braid consisting of n straight vertical strands and the inverse of a is the reflection of a with respect to a horizontal line.

Let us see why braid groups are a good candidate as a platform groups. First of all, a braid group has solvable word problem and there exists a canonical form (in fact there exist more than one [3]) for its elements such that braids are easily compared. Also the best known algorithm to solve the conjugacy problem is of exponential time. Finally, the membership decision problem in a braid group $B_n,\ n > 6$ is algorithmically unsolvable, because such a group contains subgroups isomorphic to the free group product $F_2 \times F_2$, where the membership decision problem (determining whether or not a given $x \in G$ belongs to a subgroup of G generated by given $a_1, a_2, \dots a_n$) is algorithmically unsolvable [13, p.48]. This is important because an adversary would have to know the x, y elements above not simply as a word in G, but as a word in public elements used $a_1, a_2, \dots a_n$ or $b_1, b_2, \dots b_m$ in order to reveal the secret key K [13].

2.3.3 Other protocols

There is an easy way to implement other protocols not based on the conjugacy search problem. Besides, the first naive scheme on group based cryptography by Wagner and Magyarik (1985) [18], was depended on the word problem, although it was not really a cryptosystem [2]. The basic idea is that we could have a defining relation anything like:

$$g^a = f(a)ga, \qquad f : G \to G$$

where f is a function in group G. In the case of conjugacy search problem f is defined as:

$$\begin{aligned} f : G \ &\to \ G \\ x \ &\mapsto \ f(x) = x^{-1} \end{aligned}$$

On the other hand f could be also the identity map, inducing the **decomposition problem protocols**. An extended reference on such themes can be found in [13].

2.4 Choosing the group and the problem

As noted above the construction of a group-based cryptosystem has two parts. The first one is choosing the platform group and the second one is the underlying problem. Concerning the group-based underlying problem it is not really clear, at the present, which is the best choice. For example, the conjugacy search problem may not provide a sufficient security level in braid groups, although it could be adopted in special cases [13].

On the other hand the choice of the platform group is believed that has to meet specific standards, such as mentioned below. The first one is the existence of an effective normal form, so that the word problem is solvable in real time. The normal form is also useful in hiding the message parts that could be obvious to recover; i.e. the part elements $x, y \in G$ in the product xy. Another, high priority, requirement is the size of the group. It is needed to be of super-polynomial growth, that means the elements of length n, growing faster than any polynomial in n so that a direct attack could not be implemented. Finally, all the above contribute to the choice of a well known group. Among groups meeting the above criteria and used so far are: braid groups, Thompson's group, Artin groups, solvable groups and others. Research in this context is open and has many potential.

3 Secret sharing

3.1 General description

A secret sharing scheme answers to the problem of distributing a secret among a group of n persons in such a way that it can be reconstructed only if at least t of them combine their shares. Such a scheme is called a (n, t) threshold scheme. This problem was first solved independently by A. Shamir [17] and G. Blakley [4] in 1979. In what follows we, briefly, present Shamir's scheme for creating a (n, t) threshold scheme.

Shamir's secret sharing scheme

Suppose that the secret is encoded by a number D.

1. Choose at random $t-1$ coefficients $a_1, \ldots, a_{t-1}$ and calculate the values $D_i = p(i)$ for $i = 1, \ldots, n$ of the polynomial $p(x) = D + a_1 x + \cdots + a_{t-1}x^{t-1}$. D_i are the distributed pieces of the key.

2. Given any subset of t of these D_i values we can find the coefficients of $p(x)$ by interpolation, and then evaluate $D = p(0)$. Knowledge of $t-1$ (or fewer) of these values, on the other hand, does not suffice to calculate D. Knowing $t-1$ (or fewer) shares provide no advantage over knowing no pieces (i.e. this is a perfect threshold scheme).

Shamir's solution to the secret sharing problem (as well as several other solutions) has some interesting properties. For example:

- its security is theoretical, it is not based on the hardness of a specific problem. Not knowing at least $t-1$ pieces makes it not hard but impossible to find D,

- the keys are easy to change without changing the original secret information D,

- we can have a hierarchial scheme in which important persons have more pieces of the key,

- if t is fixed, then any of the pieces D_i can be dynamically added or deleted without this affecting the other pieces.

In the following subsection we present a secret sharing scheme which was proposed by the second author [14] and it is based on group presentations and the word problem.

3.2 A secret sharing scheme

3.2.1 Description of the scheme

Suppose that a binary sequence must be distributed among n persons in such a way that at least t of them must cooperate in order to obtain the whole sequence. The secret sharing scheme consists of the following steps:

1. A group G with finite presentation $G =< x_1, x_2, \ldots, x_k / r_1, \ldots, r_m >$ and soluble word problem is chosen. We require that $m = \begin{pmatrix} n \\ t-1 \end{pmatrix}$.

2. Let $A_1, \ldots, A_m$ be an enumeration of the subsets of $\{1, \ldots, n\}$ with t-1 elements. Let $R_1, \ldots, R_n$ be n subsets of the relators set $\{r_1, \ldots, r_m\}$ where $r_j \in R_i$ if and only if $i \notin A_j$, $j = 1, \ldots, m$, $i = 1, \ldots, n$.

   Another way of viewing the sets $R_1, \ldots, R_n$ is the following: each set R_i is created from the relators set $\{r_1, \ldots, r_m\}$ after deleting the relations r_k for those k for which i belongs to A_k.

   Thus, for every $j = 1, \ldots, m$, r_j is not contained in exactly t-1 of the subsets $R_1, \ldots, R_n$. It follows that r_j is contained in any union of t of them whereas if we take any t-1 of the $R_1, \ldots, R_n$ there exists a j such that r_j is not contained in their union.

3. Distribute to each of the n persons one of the sets $R_1, \ldots, R_n$. The set $\{x_1, \ldots, x_k\}$ is known to all of them.

4. If the binary sequence to be distributed is $a_1 \cdots a_l$ construct and distribute a sequence of elements $w_1, \ldots, w_l$ of G such that $w_i =_G 1$ if and only if $a_i = 1$, $i = 1, \ldots, l$. The word w_i must involve most of the relations $r_1, \ldots, r_m$ if $w_i = 1$. Furthermore, all of the relations must be used at some point in the construction of some element.

Any t of the n persons can obtain the sequence $a_1 \cdots a_l$ by taking the union of the subsets of the relations of G that they possess and thus obtaining the presentation $G =< x_1, x_2, \ldots, x_k / r_1, r_2, \ldots, r_m >$ and solving the word problem $w_i =_G 1$ in G for $i = 1, \ldots, l$.

A coalition of fewer than t persons cannot decode correctly the message since the union of fewer than t of the sets $R_1, \ldots, R_n$ contains some but not all of the relations $r_1, \ldots, r_m$. Thus, such a coalition can only obtain a group presentation $G' =< x_1, \ldots, x_k / r_{j_1}, \ldots, r_{j_p} >$ with $p < m$ and $G \neq G'$, where $w_i =_G 1$ is not equivalent to $w_i =_{G'} 1$ in general.

For example, suppose that we would like to share a secret to three persons in such a way that at least two of them should combine their pieces in order to reconstruct the secret. We could use the Coxeter group

$$G =< x_1, x_2, x_3 / x_1^2 = x_2^2 = x_3^2 = 1, (x_1x_2)^2 = 1, (x_1x_3)^2 = 1, (x_2x_3)^3 = 1 > .$$

Note that here, since it is known that all the generators of a Coxeter group have order two the relations $x_1^2 = x_2^2 = x_3^2 = 1$ are considered public. An enumeration of the one element subsets of $\{1, 2, 3\}$ is $\{1\}, \{2\}, \{3\}$. Hence we would set

$$R_1 = \{x_1^2 = x_2^2 = x_3^2 = 1, (x_1x_3)^2 = 1, (x_2x_3)^3 = 1\}$$

$$R_2 = \{x_1^2 = x_2^2 = x_3^2 = 1, (x_1x_2)^2 = 1, (x_2x_3)^3 = 1\}$$

$$R_3 = \{x_1^2 = x_2^2 = x_3^2 = 1, (x_1x_2)^2 = 1, (x_1x_3)^2 = 1\}.$$

If we would like to share the binary digit 1, then could send the word

$$w = (x_1x_2)^2(x_2x_3)^2(x_1x_3)^2(x_2x_3).$$

Any two of the three persons could combine their pieces, thus obtaining the whole relator set of G and then finding out whether $w = 1$ or not.

In [14] it was proposed that Coxeter or polycyclic groups could be used for the implementation of the scheme. In the same article some more remarks were made on possible attacks to the scheme and ways to protect from them.

3.2.2 Some interesting remarks

The aforementioned scheme has several interesting properties. For example, contrary to other schemes (e.g. Shamir's, Blakley's scheme), the secret sequence to be shared is not needed until the final step. It is possible for someone to distribute the sets $R_1, \ldots, R_n$ and decide at a later time what the sequence will be. In that way the scheme can also be used so that t of the n persons can verify the authenticity of a message. In particular the binary sequence in step 4 could contain a predetermined subsequence (signature) along with the normal message. Then t persons may check whether this predetermined sequence is contained in the encoded message thus validating it.

It should be mentioned here that the signature mentioned above can be created in such a way that only a certain subset of n persons can verify it. This can be done by using only the relations that appear in the pieces of this particular subset of key holders. In general it can be arranged that only a specific subset of the key holders will be able to correctly decrypt a message. It can even be arranged that two different subsets of key holders will end up with entirely different messages after decryption. Properties like this will be studied in a forthcoming paper.

Like Shamir's scheme the security is theoretical. Any of the pieces can be added or deleted without this affecting the others and we can have a hierarchial scheme in which important persons have more pieces of the key. On the other hand, contrary to Shamir's scheme, it is not obvious how to add a share. It is not clear, also, if a key can be changed. For example, we could use Tietze transformations to change a relation in a set R_i but that might affect our ability to solve the word problem.

4 Conclusion

This ends our brief encounter of group-based cryptography. We would like to stress that the use of group theory to cryptography is a very active multidisciplinary research area. Group-based cryptography is a relatively new field with many interesting, far reaching open problems. The authors hope that the article gives a glimpse in this exciting field.

Acknoledgements. The authors would like to thank the Hellenic Military Academy for organizing the 2012 Cryptography Conference which gave researchers the opportunity meet and exchange their views and results.

References

[1] I. Anshel, M. Anshel and D. Goldfeld, An algebraic method for public-key cryptography, *Math.Res.Lett.*, **6**, (1999), 287–291.

[2] J.C. Birget, S.S. Magliveras and M. Sramka, On public key cryptosystems based on combinatorial group theory, *Tatra Mt. Publ.*, **33**, (2006), 137–148.

[3] J.S. Birman, Braids, links and mapping class groups, *Annals of Math. Study*, **82**, (1974).

[4] G.R. Blakley, Safeguarding cryptographic keys, *Proceedings of AFIPS*, **48**, (1979), 313–317.

[5] D. Boneh, Twenty Years of Attacks on the RSA Cryptosystem, *Notices of the AMS*, **46**(2), (1999), 203–213.

[6] B. Chandler and W. Magnus, *The History of Combinatorial Group Theory: A Case Study in the History of Ideas*, Springer-Vedag, New York, 1982.

[7] W. Diffie and M. Hellman, New directions in cryptography, *IEEE Transaction on Information Theory*, **22**, (1976), 644–654.

[8] K.H. Ko, S.J. Lee, J.H. Cheon, J.W. Han, J.s. Kang and C. Park, New public-key cryptosystem using braid group, *Advances in Cryptology - CRYPTO 2000, Lecture Notes in Computer Science*, Springer, Berlin, (2000), 166–183.

[9] N. Koblitz, Elliptic curve cryptosystems, *Mathematics of Computation*, **48**(177), (1987), 203–209.

[10] W. Magnus, A. Karrass and D. Solitar, *Combinatorial Group Theory*, Dover Publications Inc, 1976.

[11] J. Markoff, Israeli Scientist Reports Discovery of Advance in Code Breaking, *The NY Times*, May 02, 1999.

[12] V. Miller, Use of elliptic curves in cryptography, *Advances in Cryptology Proceedings of CRYPTO '85*, Springer, Berlin, (1985), 417–426.

[13] A.G. Myasnikov, V. Shpilrain and A. Ushakov, *Group-based cryptography*, Birkhäuser Verlag, 2008.

[14] D. Panagopoulos, A secret sharing scheme using groups, *Arxiv*, http://arxiv.org/abs/1009.0026, (2010).

[15] R. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signatures and pulic-key cryptosystems, *Communications of the ACM*, **21**, (1978), 120–126.

[16] D.J.S. Robinson, *A Course in the Theory of Groups*, Springer Verlag, 2nd edition, 1996.

[17] A. Shamir, How to share a secret, *Communications of the ACM*, **22**, (1979), 612–613.

[18] N.R. Wagner and M.R. Magyarik, A public key cryptosystem based on the word problem, *Advances in Cryptology - CRYPTO '84, Lecture notes in Computer Science*, Springer, Berlin, (1985), 19–36.

[19] Wire magazine, Cryptography workshop makes news *The Wire online*, **13**(1), (1999).