International Journal of Modern Science and Technology *Vol. 1, No. 9, December 2016. Page 300-303.*
http://www.ijmst.co/ ***ISSN: 2456-0235.***

Mini-Review

A Non-abelian group Cryptography

S. Iswariya, A. R. Rishivarman
Department of Mathematics, Theivanai Ammal College for Women (Autonomous)
Villupuram - 605 401. Tamilnadu, India.

*Corresponding author's e-mail: rishivarmanar@gmail.com

Abstract

Most common public key cryptosystems and public key exchange protocols presently in use, such as the RSA algorithm, Diffie-Hellman, and elliptic curve methods are number theory based and hence depend on the structure of abelian groups. The strength of computing machinery has made these techniques theoretically susceptible to attack and hence recently there has been an active line of research to develop cryptosystems using noncommutative cryptographic platforms. This line of investigation has been given the broad title of noncommutative algebraic cryptography. This was initiated by two public key protocols that used the braid groups. The study of these protocols and the group theory surrounding them has had a large effect on research in infinite group theory. In cryptosystems, the algebraic properties of the platforms are used prominently in both devising cryptosystems and in cryptanalysis. The present paper discusses the potential non-commutative group and associate cryptosystem in detail.

Keywords: Non-abelian group; Cryptosystem; Public key; Private key.

Introduction

The word 'cryptography' was coined by combining two Greek words, 'Krypto' meaning hidden and 'graphene' meaning writing. The art of cryptography is considered to be born along with the art of writing [1]. As civilizations evolved, human beings got organized in tribes, groups, and kingdoms. This led to the emergence of ideas such as power, battles, supremacy, and politics. These ideas further fueled the natural need of people to communicate secretly with selective recipient which in turn ensured the continuous evolution of cryptography as well. The roots of cryptography are found in Roman and Egyptian civilizations.

Cryptography is the science and/or art of devising and implementing secret codes or cryptosystems. Cryptanalysis is the science and/or art of breaking cryptosystems while cryptology refers to the whole field of cryptography plus cryptanalysis [2]. In most modern literature cryptography is used synonomously with cryptology. Presently there is an increasing need for secure cryptosystems due to the use of internet shopping, electronic financial transfers and so on.

Although there have been no successful attacks on the standard protocols there is a feeling that the strength of computing machinery has made these techniques less secure. As a result of this there has been an active line of research to develop and analyze new cryptosystems and key exchange protocols based on noncommutative cryptographic platforms. This line of investigation has been given the broad title of noncommutative algebraic cryptography [3,4].

Public-key cryptosystems are essential for electronic commerce or electronic banking transactions. They assure privacy of transactions, as well as integrity of messages and senders or receivers. In 1997 it became known that the ideas of public key cryptography were developed by British Intelligience Services prior to Diffie and Hellman.

Group-based cryptography is concerned with the role of nonabelian groups in cryptography. Since its origins in the 1980s, there have been numerous cryptographic proposals based on nonabelian groups, many of which have been broken [5,6].

Cryptography

Cryptography is the study of secret (crypto)-writing (graph). It is the science of art of encompassing the principle and methods of transforming an intelligible message into one that is intelligible and then transforming the message back to its original form [7].

Received: 21.10.2016; Received after Revision: 02.11.2016; Accepted: 08.11.2016; Published: 04.12.2016

Cryptography today is assumed as the study of techniques and authenticity of transfer of information under difficult circumstances. Mainly cryptography is a study of mathematical techniques related to aspect of information security and analysis such as confidentiality, data integrity authentication and non reputation.

Group

A group is a nonempty set G on which there is defined a binary operation $(a, b) \rightarrow ab$ satisfying the following properties [8] [9].

Closure

If a and b belong to G, then ab is also in G.

Associativity

$a(bc) = (ab)c$ for all $a, b, c \in G$.

Identity

There is an element $1 \in G$ such that $a1 = 1a = a$ for all $a \; in \; G$.

Inverse

If a is in G, then there is an element $a^{-1} in \; G$ such that $aa^{-1} = a^{-1}a = 1$.

Abelian group

A group G is abelian if the binary operation is commutative, i.e., $ab = ba$ for all $a, b \; in \; G$.

Nonabelian group

A group is non-Abelian if there is some pair of elements a and b for which

$ab \neq ba$ for all $a, b \in G$.

Nonabelian group based cryptography

The noncommutative cryptographic platform has been nonabelian groups. A cryptographer has began to pay more attention towards non-commutative cryptography based on non-commutative algebraic structures. Non-commutative cryptography extends the research territory of cryptography. A large number of non-commutative algebraic structures are now waiting to be explored for new public key cryptosystems [10].

The non-commutative algebraic structures can increase the hardness of some mathematical problems significantly [11]. For instance, we already know that how to design efficient quantum algorithms for solving hidden subgroup problems in any abelian group, but we are still unable to construct efficient algorithms for dealing hidden subgroup problem in non-abelian groups [12].

Most of cryptosystems in non-commutative cryptography are derived from combinatorial group theory, but they are mainly theoretical or have certain limitations in wider and general practice [13]. The properties of non-commutative cryptography is that it can take the advantage of intractable problems in quantum computing, combinatorial group theory and computational complexity theory to constructing cryptographic platforms [14].

Cryptosystem

A cryptosystem is an implementation of cryptographic techniques and their accompanying infrastructure to provide information security services. A cryptosystem is also referred to as a cipher system.

Types of cryptosystems

There are two types of cryptosystems based on the manner in which encryption-decryption is carried out in the system

- Symmetric Key Encryption
- Asymmetric Key Encryption

The main difference between these cryptosystems is the relationship between the encryption and the decryption key.

Symmetric key encryption

The encryption process where same keys are used for encrypting and decrypting the information is known as Symmetric Key Encryption. The study of symmetric cryptosystems is referred to as symmetric cryptography. Symmetric cryptosystems are also sometimes referred to as secret key cryptosystems.

Asymmetric key encryption

The encryption process where different keys are used for encrypting and decrypting the information is known as Asymmetric Key Encryption. Though the keys are different, they are mathematically related and hence, retrieving the plaintext by decrypting cipher text is feasible.

Public key cryptosystem

Modern cryptography is usually separated into classical or symmetric key cryptography and public key cryptography. In public key cryptography the encryption method is public knowledge but only the receiver knows how to decode. In a classical cryptosystem once the encrypting algorithm is known the decryption algorithm can be implemented in approximately the same order of magnitude of time. In a public the decryption algorithm is much more difficult to implement. This difficulty depends on the type of computing machinery used and as

computers get more powerful, new and more secure public key cryptosystems become necessary.

The basic idea in a public key cryptosystem is to have a one-way function. That is a function which is easy to implement but very hard to invert. Hence it becomes simple to encrypt a message but very hard, unless you know the inverse, to decrypt.

Public-key cryptography, or asymmetric cryptography, is an encryption scheme that uses two mathematically related, but not identical, keys - a public key and a private key are shown in fig 1. Unlike symmetric key algorithms that rely on one key to both encrypt and decrypt, each key performs a unique function. The public key is used to encrypt and the private key is used to decrypt [15].

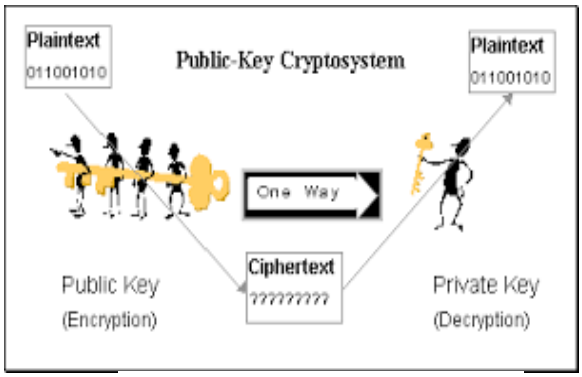

Fig. 1. Public key cryptosystem

Algorithm

Let *G* be a non-abelian finite group, $a, b \in G$ such that$ab \neq ba$. Let n_1 be the order of the element a and n_2 be the order of the element$b$. Suppose that B and A want to exchange a secret key [13]. The following steps will be executed for this purpose:

(1) B randomly chooses natural numbers r and s with $0 < r < n_1, 0 < s < n_2$. r and s are kept secret. He then forms $c = a^r b^s$ and submits this result to A.

(2) A randomly chooses natural numbers v and w with $0 < v < n_1, 0 < w < n_2$. v and w are kept secret. She then forms $d = a^v b^w$ and submits this result to B. The latter variant does not need verification by means of a zero knowledge poof. We will now briefly analyze the possibility of forgery of the latter variant of the signature system. Suppose 'A' wants to provide 'B' with a forged signature. She then has to deliver group elements $g_1$and g_2 such that $db^{-y}g_1a^{-x}d = a^r g_2 b^s$ holds. This is impossible, as long as r, x and s, y are not known to 'A'.

Suppose now, 'B' claims that 'A' has signed the message e. B may choose $g_1 \in G$. Then he may compute a suitable g_2 such that the above equation holds. But $g_2 = a^v e b^w$ needs to hold too. This is virtually impossible, if the exponents v and w are not known to him and g_1 cannot be formed properly. A can immediately prove the fosrgery by publishing *v* and *w*. Assume finally, that A has provided two correctly formed group elements g_1 and g_2 to B such that the above equation $db^{-y}g_1a^{-x}d = a^r g_2 b^s$ holds. She cannot deny this signature later. In case of dispute she may have to publish *v* and *w*. This would prove the correctness of the signature.

Conclusion

The present report presented a novel public key cryptosystem (based on a finite non abelian groups) and suggested some examples of finite non abelian groups. There may be other non abelian groups to be used in our system. However we must be careful in applying a non abelian group to our cryptosystem in order that the cryptosystem is secure. An idea of crypto primitives have been presented, which can be implemented in non-abelian groups and may be viewed as generalization of Diffie-Hellman methods. Non-commutative group based cryptosystems may be generalized existing commutative group-based cryptosystems. In fact, the MOR cryptosystem is a natural generalization of the El-Gamal cryptosystem. There are many interesting problems in non-commutative groups could be strong candidates in construction of a cryptosystem, but not all could be developed successfully. Moreover, some problems could be converted to others in polynomial time. There are many non-commutative groups could be promising candidates for building a cryptosystem. But we must be careful in choosing the function together the group for real applications, namely, the basic idea is to study the behavior of products $a^v b^w$ where *a* and *b* are elements of sufficiently high order of a non-abelian group *G*.

Acknowledgment

The authors are thankful to referees for their valuable comments and suggestions for improving the present paper.

Conflict of interest

Authors declare there are no conflicts of interest.

References

[1] Buchmann JA. *Introduction to Cryptography*. 2nd ed. Springer: 2004.

[2] Bresson E, Chevassut O, Pointcheval D. The Group Diffie-Hellman Problems. Nyberg K, Heys H. (Eds.). *Selected Areas in Cryptography*. LNCS 2595. Springer: 2003 325-338.

[3] Myasnikov AG, Shpilrain V, Ushakov A. Group-Based Cryptography Advanced Courses in Mathematics. CRM Barcelona; Birkhäuser: 2007.

[4] Myasnikov A, Shpilrain V, Ushakov A. A Practical Attack on a Braid Group Based Cryptographic Protocols. *Advances in Cryptology*. 2005;3621:86-96.

[5] Arzhanseva GN, Yu Ol'shanskii A. Generosity of the Class of Groups in Which Subgroups with a Lesser Number of Generators are Free is Generic. *Matematicheskie Zametki*. 1996;59:489-496.

[6] Koblitz N. *Algebraic Methods of Cryptography*. Springer: 1998.

[7] Myasnikov A, Shpilrain V, Ushakov A. Non-commutative Cryptography and Complexity of Group theoretic Problems. *Mathematical Surveys and Monographs*. American Mathematical Society: 2011.

[8] Boaz T. Polynomial-time solutions of computational problems in noncommutative-algebraic cryptography. *Journal of Cryptology*. 2015;28:601-622.

[9] Grigoriev D, Ponomarenko I. Homomorphic Public-Key Cryptosystems over Groups and Rings Quaderni di Matematica. 2005.

[10] Baumslag Y, Brjukhov B, Rosenberger G. Some Cryptoprimitives for Noncommutative Algebraic Cryptography Aspects of Infinite Groups, World Scientific Press: 2009.

[11] Batty M, Braunstein S, Duncan A, Rees S. Quantum algorithms in group theory. *Cont. Math*. 2003;349:1-62.

[12] Wang L, Gu L, Ota K, Dong M, Cao Z, Yang Y. New public key cryptosystems based on non-Abelian factorization problems. *Security and Communication Network*. 2013;6(7):912-922.

[13] Magliveras SS, Stinson DR. New approaches to designing public key cryptosystem using one-way functions and trapdoors infinite group. *Journal of Cryptology*. 2002;15(4)285-297.

[14] Baumslag G, Fine B, Xu X. Cryptosystems Using Linear Groups Appl. Based Cryptographic Primitives. In: Desmedt Y. G: Public Key Cryptography – PKC, Springer: 2003.

[15] Zhang H, Liu J, Jia J, Mao S, Wu W. A survey on applications of matrix decomposition in cryptography. *Journal of Cryptologic Research*. 2014;9(1):341-357.

****

