An Arithmetic Technique for Non-Abelian Group Cryptosystem

S. Iswariya
Research Scholar,
Mathematics
Theivanai Ammal
College for Women
Villupuram 605 401,
T.N, India

A. R. Rishivarman
Professor, Mathematics
Theivanai Ammal C
ollege for Women
Villupuram 605 401,
T.N, India

ABSTRACT
Most public key cryptosystems have been constructed based on abelian groups. It possible to a cryptosystem based on non-commutative properties of groups. It propose a new public key cryptosystem built on finite non abelian groups in this paper. It is convertible to a scheme in which the encryption and decryption are much faster than other well-known public key cryptosystems.

Keywords
Non- Abelian Group, Public key, Encryption, Decryption

1. INTRODUCTION
Cryptography is an interdisciplinary field of great practical importance. The subfield of public key cryptography has notable applications, such as digital signatures. The security of a public key cryptosystem depends on the difficulty of certain computational problems in mathematics [6]. A deep understanding of the security and efficient implementation of public key cryptography requires significant background in algebra, number theory and geometry [7].

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 and key exchange protocols 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, one by Ko, Lee et.al.and one by Anshel, Anshel and Goldfeld [1]. The study of these protocols and the group theory surrounding them has had a large effect on research in infinite group theory [9]. By using a non abelian group G for a public key cryptosystem, it needs to consider the following problems related to the word problem:1. Expressing a message as an element of G. 2.Elementsof G be represented in a unique way.

If an element of G is not represented in a unique way, then a plaintext and a cipher text may not be the same. Therefore the second problem is very important by using a non abelian group for a public key system. Matrix groups and semi-direct product of abelian groups are examples of non abelian groups which have such expressions [10].

In this article, it suggests a new cryptosystem based on such a finite non-abelian group G.

3. 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.

3.1 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 [2].

3.1.1 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.

3.1.2 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.

4. PUBLIC KEY CRYPTOSYSTEM
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. Digital signatures are used to sign electronic documents [8, 11, 14]. They are also mostly based on public-key techniques.

A lot of popular public-key encryption systems are based on number-theoretic problems such as factoring of integers or finding discrete logarithms (Discrete Logarithm Problem, DLP) [4, 5]. The underlying algebraic structures very often are abelian groups. This is especially true for Diffie-Hellman-methods. Since computational power permanently increases, the required key length for a desired level of security needs to be enlarged permanently. It is therefore desirable, to look for techniques in more complex algebraic settings [23, 24].

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.

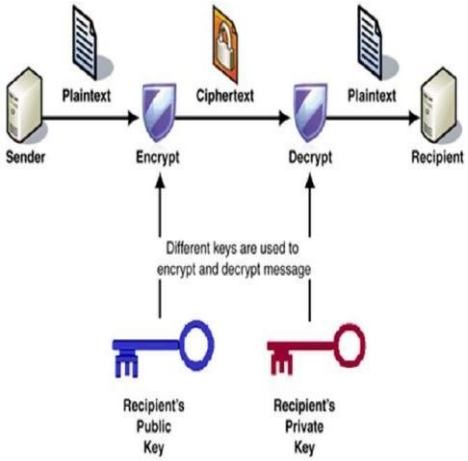

Fig 1: Public key cryptosystem

The basic idea in a public key cryptosystem is to have a one-way function [25]. 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 (see 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.

5. GROUP

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

5.1 Closure

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

5.2 Associativity

$a(bc) = (ab)c$ for all

$a, b, c \in G$.

5.3 Identity

There is an element $1 \in G$ such that

$a1 = 1a = a$ for all $a \; in \; G$.

5.4 Inverse

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

6. ABELIAN GROUP

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

7. NONABELIAN GROUP

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

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

8. DISCRETE LOGARITHM PROBLEM

Let g be a primitive root for F_p and let h be a non-zero element of F_p. The Discrete logarithm problem (DLP) is the problem of finding an exponent x such that $g^x \equiv h \; (mod \; p)$.The number x is called discrete logarithm problem of h to the base g and is denoted by $\log_g(h)$.

9. 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 [16]. 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.

The non-commutative algebraic structures can increase the hardness of some mathematical problems significantly [17]. For instance, it already know that how to design efficient quantum algorithms for solving hidden subgroup problems in any abelian group, but it is still unable to construct efficient algorithms for dealing hidden subgroup problem in non-abelian group [18, 21].

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. 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 [19, 22].

10. PUBLIC KEY CRYPTOSYSTEM USING FINITE NON ABELIAN GROUP

10.1 A Finite Non Abelian group

1. Let r, s be integers > 0
2. $d = (r, s) = GCD \; \{r, s\} > 1$
3. It can be defined a non- abelian group G such that $|G| = r.s.d$ as follows

$$G = \langle a, b, c : a^r = 1, \quad b^s = 1, \quad c = b^{-1}a^{-1}ba, ac = ca, bc = cb \rangle$$

4. Observations

(i) c^i commutes with every elements $c = b^{-1}a^{-1}ab \; implies \; cb^{-1} = b^{-1}a^{-1}a$

(ii) $O(a) = 1, O(b) = 1, O(c) = d(r, s) > 1$

(iii) Every element of G can be represented by the word $a^{\alpha}b^{\beta}c^{\gamma}$

Where $0 \le \alpha < r, 0 \le \beta < s, 0 \le \gamma < d$

(iv) The multiplication rule for G is as follows :

$$(a^{\alpha_1}b^{\beta_1}c^{\gamma_1}) \otimes (a^{\alpha_2}b^{\beta_2}c^{\gamma_2}) = (a^{\alpha_3}b^{\beta_3}c^{\gamma_3})$$

Where $\alpha_3 = \alpha_1 + \alpha_2 (\text{mod } r)$

$$\beta_3 = \beta_1 + \beta_2 (\text{mod } s)$$

$$(\gamma_3 = \alpha_2\beta_1 + \gamma_1 + \gamma_2 \text{mod } d)$$

$$(a^{\alpha_1}b^{\beta_1}c^{\gamma_1}) \otimes (a^{\alpha_2}b^{\beta_2}c^{\gamma_2})$$
$$= (a^{\alpha_1+\alpha_2 (\text{mod } r)}b^{\beta_1+\beta_2 (\text{mod } s)}c^{\alpha_2\beta_1+\gamma_1+\gamma_2 (\text{mod } d)})$$

Therefore, this binary operations tells clearly, that G is non-abelian

(v) In fact the set of words $\{a^{\alpha}b^{\beta}c^{\gamma} : 0 \le \alpha < r, 0 \le \beta < s, 0 \le \gamma < d\}$ forms non-abelian group G under the multiplication rule (1) with $|G| = r.s.d$

Now, let us do some computation in the non- abelian group G

$$(a^{\alpha_1}b^{\beta_1}c^{\gamma_1}) \otimes (a^{\alpha_2}b^{\beta_2}c^{\gamma_2}) = (a^{x}b^{y}c^{z})$$

Where $x = \alpha_1 + \alpha_2 (\text{mod } r)$

$$y = \beta_1 + \beta_2 (\text{mod } s)$$

$$z = \alpha_2\beta_1 + \gamma_1 + \gamma_2 (\text{mod} d)$$

$$(a^{\alpha_1}b^{\beta_1}c^{\gamma_1}) \otimes (a^{\alpha_2}b^{\beta_2}c^{\gamma_2}) \otimes (a^{\alpha_3}b^{\beta_3}c^{\gamma_3} =$$
$$(a^{\alpha_1+\alpha_2 (\text{mod } r)}b^{\beta_1+\beta_2 (\text{mod } s)}c^{\alpha_2\beta_1+\gamma_1+\gamma_2 (\text{mod } d)})$$
$$\otimes (a^{\alpha_3}b^{\beta_3}c^{\gamma_3}) = a^{\sum_{i=1}^{3}\alpha_i (mod\ r)}$$
$$b^{\sum_{i=1}^{3}\beta_i (mod\ s)}c^{\sum_{i=1}^{3}[\alpha_3\sum_{j=1}^{2}\beta_j + \alpha_2\beta_1 + \sum_{j=1}^{2}\gamma_j] (mod\ d)}$$

Now, the general formula is,

$$(a^{\alpha_1}b^{\beta_1}c^{\gamma_1}) \otimes (a^{\alpha_2}b^{\beta_2}c^{\gamma_2}) \otimes \ldots \otimes (a^{\alpha_3}b^{\beta_3}c^{\gamma_3})$$
$$= a^{\sum_{i=1}^{n}\alpha_i (mod\ r)}b^{\sum_{i=1}^{n}\beta_i (mod\ s)}$$
$$c^{\sum_{i=1}^{n}[\alpha_n\sum_{j=1}^{n-1}\beta_j + \alpha_{n-1}\sum_{j=1}^{n-2}\beta_j + \cdots + \alpha_2\beta_1 + \sum_{j=1}^{n}\gamma_j] (mod\ d)}$$

For any positive integer $N > 3$, we have $(a^{\alpha}b^{\beta}c^{\gamma})^{N} =$

$$a^{N\alpha (\text{mod } r)}b^{N\beta (\text{mod } s)}c^{(\frac{N(N-1)}{2}\alpha\beta + N\gamma) (\text{mod } d)}$$

10.2 Public Key Cryptography Using the Non-abelian Group G

1. Select very large positive integer r, s, d with $d = (r, s) > 1$
2. This non-abelian group G is given to public, i.e integer r, s, d are known to public
3. Represent a message $m = a^{\alpha}b^{\beta}c^{\gamma} \in G \text{ where } 0 \le \alpha < r, 0 \le \beta < s, 0 \le \gamma < d$
4. Select a secret very large odd prime *'p'* such that (x_0, y_0) is the least positive integral solution of $y_0^2 - px_0^2 = 1$
5. $y_0$is given to public
6. x_0, p are private keys
7. Encryption of the message

$m = a^{\alpha}b^{\beta}c^{\gamma} \in G$ as follows

$$E_G^m = (a^{\alpha}b^{\beta}c^{\gamma})^{y_0^2} \in G$$

8. $a^{\alpha'}b^{\beta'}c^{\gamma'} = E_G^m = (a^{\alpha}b^{\beta}c^{\gamma})^{y_0^2} \in G$

Where $\alpha' = \alpha y_0^2 (mod\ r)$

$$\beta' = \beta y_0^2 (mod\ s)$$

$$\gamma' = (\frac{y_0^2(y_0^2-1)}{2}\alpha\beta + y_0^2\gamma) (\text{mod } d)$$

It is important to note that, given α', β', γ' and r, s, d solving (uniquely) for α, β, γ is very difficult computation.

9. Decryption ;

Using the private keys x_0, p compute

$$(a^{\alpha'}b^{\beta'}c^{\gamma'}) \otimes (a^{\alpha}b^{\beta}c^{\gamma})^{-px_0^2} (mod\ G)$$
$$= a^{\alpha}b^{\beta}c^{\gamma}$$

In this way, we hope one can construct an effective, implementable and highly secure cryptosystem using non-Abelian groups in the directions suggested in this paper. It is concluded with the remark that one can define a non-Abelian analogue of most of the protocols using the DLP in Abelian groups.

11. CONCLUSION

In this article, it is presented a novel public key cryptosystem (based on a finite non abelian groups). There may be other non abelian groups to be used in our system. However it must be careful in applying a non abelian group to our cryptosystem in order that the cryptosystem is secure. The existence of abelian normal subgroup reduces the security of the cryptosystems. So any abelian normal subgroup must be of small order. The proposed algorithm to express an element of G must be efficient.

12. ACKNOWLEDGMENT

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

13. REFERENCES

[1] I. Anshel, M. Anshel, D. Goldfeld, An algebraic method for public-key cryptography, Mathematical Research Letters 6 (1999) 1-5.

[2] S. Blackburn, S. Galbraith, Cryptanalysis of two cryptosystems based on group actions, Proc. ASIACRYPT' 99 (2000) 52-61.

[3] A. E. Brower, R. Pellikaan, E. R. Verheul, Doing more with fewer bits, Proc. ASIACRYPT' 99 (2000) 321-332.

[4] D. Coopersmith, A. M. Odlzyko, R. Schroeppel, Discrete logarithms in GF(p), Algorithmica 1 (1986) 1-15.

[5] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Transactions and Information Theory 31 (1985), 469-472.

[6] S. Flannery, Cryptography: An investigation of a new algorithm vs. the RSA,http://cryptome.org/°annery-p.pdf, 1999.

[7] T. W. Hungerford, Algebra, Springer Verlag

[8] A. K. Lenstra, E. R. Verheul, The XTR Public key system, Proc. Crypto (2000) 1-20.

[9] A. J. Menezes, P. C. Van Oorshot, S. A. Vanstone, Handbook of applied cryptography, CRC press, 1997.

[10] R. Lidl, H. Niederreiter, Introduction to finite fields and their application, Cambridge University press, 1986.

[11] K. H. Ko, S. J. Lee, J. H. Cheon, J. W. Han, J. -S. Kang, C. Park, New public-key cryptosystem using braid groups, Proc. Crypto 2000 (2000) 166-184.

[12] N. Koblitz, Elliptic curve cryptosystems, Mathematics of Computation, 48 (1987) 203-209.

[13] V. Miller, Use of elliptic curves in cryptography, Proc. Crypto 85 (1986) 417-426

[14] K. Nyberg, R. Rueppel, A new signature scheme based on DSA giving message recovery, 1st ACM Conference on Computer and Communications Security, (1993) 58-61.

[15] S.-H. Paeng, J.-W. Han, B. E. Jung, The security of XTR in view of the determinant, preprint, 2001.

[16] S.-H. Paeng, A provably secure public key cryptosystem using finite non abelian groups, preprint, 2001.

[17] A Myasnikov, V Shpilrain, A Ushakov , Noncommutative Cryptography and Complexity of Group theoretic Problems. American Mathematical Society, 2011.

[18] T Boaz, Polynomial-time solutions of computational problems in noncommutative-algebraic cryptography. Journal of Cryptology (2015) 601–622.

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

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

[21] M Batty, S Braunstein, A Duncan, S Rees, Quantum algorithms in group theory. Cont. Math. 349 (2003) 1–62.

[22] LGuL Wang, K Ota, M Dong, Z Cao, Y Yang, public key cryptosystems based on non-Abelian factorization problems, Security and Communication Network (2013) 912–922.

[23] G Baumslag, B Fine, X Xu, Cryptosystems using Linear Groups Appl. based cryptographic Primitives. Desmedt YG. Public Key Cryptography – PKC, Springer (2003) 187-198.

[24] G Baumslag, B Fine, X Xu, A Proposed Public Key Cryptosystem Using the Modular Group. Cont.Math. 421 (2007) 35-44.

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