Scientific Journal Impact Factor (SJIF): 1.711

e-ISSN: 2349-9745
p-ISSN: 2393-8161

International Journal of Modern Trends in Engineering and Research
www.ijmter.com

CAMINA GROUP FOR THE MOR CRYPTOSYSTEM

Akshaykumar Meshram[1], Dr. N.W.Khobragade[2]
Ph.D Scholar[1], Professor[2]
[1, 2]Department of Mathematics, R.T.M. Nagpur University, Nagpur (M.S.), India

Abstract— In this paper we study of the MOR cryptosystem using camina group**.** We show that using the automorphism of the camina group one can build a secure MOR cryptosystem.

Keywords- MOR cryptosystem, Camina group, Discrete Logarithm Problem, Diffie- Hellman problem**,** ElGamal cryptosystem.

I. INTRODUCTION

The digital system has brought revolutionary changes in every walk of life. The data storage, its processing and the outcome are the major stages in it. Naturally security of the same is a quite concern in this matter.

Cryptography, which basically writing codes and solving codes, has worked out justifiable solution to the problem of security of the digital data.
A Principal Goal of (Public Key) Cryptography is to allow two people to exchange confidential information, even if they have never met and can communicate only viaa channel that is being monitored by an adversary.

There are three cryptosystems widely in use today:
1) RSA(Ron Rivest, Adi Shamir and Leonard Adleman).
2) The El-Gamal or the Diffie-Hellman key exchange protocol over the multiplication group of a finite field.
3) The El-Gamal or the Diffie -Hellman key exchange protocol over the group of points on an Elliptic curve over a finite field.

The security type of the 1st and 2nd is the same. The best known attack against them, the index calculus method, is sub-exponential in nature. On the other hand, the best known attack against 3rd is exponential in nature. Today, some cryptographers try to build public key cryptosystems based on non-abelian groups with the security expected at least as secure as Elliptic curve cryptosystems.

Discrete Logarithm Problem (DLP) is the famous problem in cryptography. It is the complexity of DLP, which is the base of most commonly, used cryptosystem like the ElGamal cryptosystems over finite field or Elliptic curve cryptosystems. The algebraic groups used in such cryptosystems are abelian (commutative). There are many ones based on DLP other than ElGamal and Elliptic cryptosystems. Among them, we studied the MOR cryptosystem over the automorphism group Aut(G) of a non-abelian group G.

II. PRELIMINARIES

Most of the definition used in these papers is standard.

2.1 Discrete Logarithm Problem {DLP}:

The (discrete) exponentiation problem is as follows: Given a base a, an exponent b and a modulus p, calculate c such that $a^b \equiv c \pmod p$ and $0 \leq c < p$.

It turns out that this problem is fairly easy and can be calculated "quickly" using fast-exponentiation.
The discrete log problem is the inverse problem:
Given a base a, a result c ($0 \leq c < p$) and a modulus p, calculate the exponent b such that
$a^b \equiv c \pmod p$.
It turns out that no one has found a quick way to solve this problem. To get an intuition as to why this is the case, try picking different values of a and p, and listing out each successive power of a mod p. What you will find is that there is no discernable pattern for the list of numbers created. Thus, given a number on the list, it's very difficult to predict where it appears on the list.

2.2 ElGamal Cryptosystem:

Let q be a prime such that the discrete logarithm problem in $(Z_q,)$ is infeasible and let $\alpha \in Z_q$ be a primitive element. Let $P=Z_q$, $C=Z_q \times Z_q$, and define

$$K=\{(q, \alpha, X_B, Y_B): Y_B=\alpha^{X_B} \bmod q\}.$$

The values q, α and Y_B are the public key and X_B is the private key.

For $K= (q,\alpha, X_B, Y_B)$, and for a (secret) random number $k \in Z_{q-1}$, define

$$e_k(x, k)=(C_1, C_2)$$

Where

$$C_1=\alpha^k \bmod q$$

$$C_2= x Y_B^{\,k} \bmod q$$

For C_1 and $C_2 \in Z_q$, define

$$\alpha^k (C_1, C_2)=C_2 (C_1^{X_B})^{-1} \bmod q$$

2.2 Camina Group:

A group G is called a Camina group if $G' \neq G$, and for each $x \in G \setminus G'$ the following equation holds:

$$x^G = x\{G'\},$$

where $x^G = \{x^g \setminus g \in G\}$ is the conjugacy class of x in G and $x\{G'\}$ denotes the set $\{x^{g'} / g' \in G'\}$.

It is well know that,

1) In Camina group the equality

$$x^G = x\{G'\}$$

2) In an arbitrary group $x^G \subseteq x\{G'\}$ for each $x \in G$.

III. THE MOR CRYPTOSYSTEM

In this section we discuss the MOR cryptosystem. The concept of the MOR cryptosystem was first proposed in Crypto2001 by Paeng et al[2]. There are two different security concepts used in [2].
a) The discrete logarithm problem in the group of inner automorphisms.
b) Membership problem in a finite cyclic group.

The MOR cryptosystem is a generalization of ElGamal cryptosystem, where the discrete logarithm problem works in the automorphism group of a group G, instead of the group G itself.

Later in same year, Paeng et al [3], they generalized the MOR cryptosystem and study this new system for non abelian group.

In 2003, Seong-Hun Paeng [4] shows that there are subexponential time algorithms to solve the DLP in inner automorphism groups for some non-abelian groups.

3.1 Description of the MOR cryptosystem:

Alice's keys are as follows:

Public Key: $\emptyset$ and $\emptyset^m$, $m \in \mathbb{N}$.
Private Key: m.

Encryption
a) To send a message $a \in G$ Bob computes $\emptyset^r$ and $\emptyset^{mr}$ for a random $r \in \mathbb{N}$.
b) The ciphertext is ($\emptyset^r$, $\emptyset^{mr}$ (a)).

Decryption
Alice knows m, so if she receives the ciphertext ($\emptyset^r$, $\emptyset^{mr}$ (a)), she computes $\emptyset^{mr}$ from $\emptyset^r$ and then $\emptyset^{-mr}$ and then from $\emptyset^{mr}$(a) computes 'a'.

Alice can compute $\emptyset^{-mr}$ in two ways,
a) If she has the information necessary to find out the order of the automorphism $\emptyset$ then she can use the identity $\emptyset^{t-1} = \emptyset^{-1}$whenever $\emptyset^t = 1$.
b) She can find out the order of some subgroup in which $\emptyset$ belongs and use the same identity.

IV. The MOR cryptosystem using Camina group

Camina groups were introduced by A.R.Camina in [5]. The standard definition of camina group mention above and this group had been extensively studied R. Dark, C.M. Scoppola in [6]. Aayn Mahalanobis elaborately explained that the currently group for the MOR cryptosystem [2] is $SL(2,\mathbb{z}_p) \times \mathbb{z}_p$.The automorphisms proposed is inner autotomorphism. It is shown in [4] that the DLP in the group of inner autotomorphism of $SL(2,\mathbb{z}_p) \times \mathbb{z}_p$ in the same as the DLP in $SL(2,\mathbb{z}_p)$. So here we consider map $\emptyset: G \to G$ be an automorphism of camina group and the map $\emptyset: \frac{G}{\emptyset(G)} \to \frac{G}{\emptyset(G)}$.

Theorem: A finite non abelian group G is a Camina group if and only if G is a Camina p-group of nilpotance class.

In 2010, Marcel Herzog [7], shows that if G is non abelian polycyclic by finite camina group, then $\frac{G}{G'}$ is finite and if G is non abelian locally finite camina group, then the of the following hold

a) $\frac{G}{G'}$ is a p-group, for suitable prime p.

b) G' is a nilpotent group, and either G' is p-group or $\frac{G}{G'}$ is a localy cyclic group.

Also if G is non-abelian camina group, then if $\frac{G}{z(G)}$ is finite then G is finite and if $\frac{G}{z(G)}$ is a locally finite p-group, then G is a locally finite p-group.

In 2007 Aayn Mahalanobis[8], show that MOR cryptosystem over finite p-group is only as secure as the ELGamal have cryptosystem over finite field.
On using automorphism of camina group, we can make secure MOR cryptosystem as this group can reduce into p-group and using fact that,
If G is a camina group,

$x \in \frac{G}{G'}$ and $a \in G'$ then $xa = x^g$ for some $g \in G$.
$xG' = (xa)G' = (x^g)^n G' = (x[x,g])^n G' = x^n G'$ and from $|x| = p\ that\ n \equiv 1(modp)$
Since,
$x, xa \in \frac{G}{G'}$ implies $< xa > = < x >^g$ for some $g \in G$ and $xa = (x^g)^n$ for some integer n.

Using above fact one can build secure MOR cryptosystem using camina group as it can be reduce to p-group and it is depending upon the value of $a \in G'$ which is very difficult to break such cryptosystem.

V. Conclusion

The objective of this paper is to study camina group for the MOR cryptosystem. It is prove that by using camina group one can build secure MOR cryptosystem. The security of any proposed cryptosystem matter of challenge and more work need to be done for security of the given system.

Acknowledgements

The authors would like to thank anonymous reviewers of International Journal of Modern Trends in Engineering and Research for their careful and helpful comments.

Reference

[1] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman, An introduction to mathematical cryptography, Springer, 2008.

[2] S.-H. Paeng, K.-C. Ha, J. Kim, S. Chee, C. Park, New public key cryptosystem using finite non abelian groups, in: Advances in Cryptology-Crypto, 2001, pp. 470–485.

[3] S.-H. Paeng, D. Kwon, K.-C. Ha, J. Kim, Improved public key cryptosystem using finite non abelian groups, IACR ePrint 2001/066.

[4] Seong-Hun Paeng ,On the security of cryptosystem using automorphism groups, Information Processing Letters 88 (2003) 293–298

[5] A.R. Camina, Some conditions which almost characterize Frobenius groups, Israel J. Math 31 (1978), 153–160.

[6] R. Dark, C.M. Scoppola, On Camina groups of prime power order, J. Algebra 181 (1996), 787–802.

[7] Marcel Herzog, on infinite Camina groups, Tel-aviv university 2010

[8] Aayn Mahalanobis, A note on using finite non-abelian p-groups in the MOR cryptosystem , arXiv:cs/0702095v1[cs:CR] 16 Feb 2007.

