International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 2, Issue 12, December 2015

Camina Group-Based MOR Cryptosystem using Isodual Mathematics

[1] Akshaykumar Meshram,[2] N.W.Khobragade
[1] Department of Mathematics & Humanities,,[2] Department of Mathematics,
[1] Yeshwantrao Chavan College of Engineering, [2] R.T.M. Nagpur University,
Nagpur (M.S.), India
[1] akj.meshram@gmail.com, [2] khobragadenw@gmail.com

Abstract:- In this paper we extend the concept of Meshram etal [1] and analysis the security of MOR public key Cryptosystem using Isodual mathematics. Finally we claim that the security of proposed system is highly depending on the presentation of groups.

Keywords:-ElGamal Cryptosystem, Discrete Logarithm Problem, Camina Group, MOR Cryptosystem, Conjugacy Problem,Finite Non-Abelian Group, Isodual Mathematics.

I.INTRODUCTION

In the days where most of the transactions and calculation are done online, the importance and need of the security of the digital data is of huge concern. Cryptography, a practice for secure communication, is a decisive mark for data security. The modern cryptography which is highly based on mathematical theory and computer science is opening new and dynamic avenues for the standardized security of data.

The framework 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.

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

II.PRELIMINARIES

A.ElGamal Cryptosystem:

In 1985 an algorithm was proposed by ElGamal. It, like Diffie-Hellman, is based upon the discrete logarithm problem.The (public) parameters required for the ElGamal cryptosystemare a prime p and an integer g. The powers of g modulo p should generate a large number of elements (though not necessary all).

Alice has a private key a and a public key e, where e = ga mod p, which is where we see the assumption that the private key is difficult to obtain from the public key.

If Bob wants to send a plaintext message, m, to Alice he must first generate a random number k < p. He then computes c1 = gk mod p and c2 = ekm mod p, and sends the pair (c1, c2) to Alice. To decrypt the message, Alice computes c1-a c2 modp.

This is equal to m, since c1-a c2 = g-akek m = e-k ek m =m mod p[4].

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 ab ≡ c (mod p) and 0 ≤ 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 ≤ c < p) and a modulus p, calculate the exponent b such that

ab ≡ c (mod p) [4].

B.Camina group:

Camina groups were introduced by A.R.Camina in [5] and it is defined as follows:

A group G is called a Camina group if G′ ≠ G, and for each x ∈ G \ G′ the following equation holds:

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

Where xG = {xg \ g ∈ G} is the conjugacy class of x in G and x{G'} denotes the set {xg′/g′ ∈ G′}.

C.The Mor cryptosystem:

Let G be a group and ∅ : G → G be an automorphism.

Alice's keys are as follows:
Public Key: ∅ and ∅m, m ∈ ℕ.

Private Key: m.

D.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 $(\emptyset_r, \emptyset_{mr}(a))$.

E.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 orderof 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.

F.MOR cryptosystem for camina group:

In [1], Meshram et al said that on using automorphism ofcamina group, one can make secure MOR cryptosystem. In [6],Meshram et al construct MOR cryptosystem for camina group G as follows:

Let the following sequence;

$$G \xrightarrow{q} \frac{G}{N} \xrightarrow{\emptyset} \mathrm{Aut}(G'),$$

Where N is a normal subgroup of G, q is a quotient map toG/N and $\emptyset$ is a homomorphism from G/N to Aut G′ , where $G' \neq G$.

Alice's keys are as follows:

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

Private Key: m.

G.Encryption

a) To send a message $g \in G$. In camina grpup $x \in \frac{G}{G'}$ and $a \in G'$ then $xa = x_g$ for some $g \in G$.

b) Bob computes $\emptyset(x_g)_r$ and $\emptyset(x_g)_{mr}$ for a random $r \in \mathbb{N}$.

c) The ciphertext is $(\emptyset(x_g)_r, \emptyset(x_g)_{mr})$.

H.Decryption

Alice knows m, so if she receives the ciphertext $(\emptyset(x_g)_r, \emptyset(x_g)_{mr})$. she computes $\emptyset_{mr}$ from $\emptyset_r$ and then $\emptyset_{-mr}$ and then from $\emptyset(x_g)_{mr}$ computes 'g'.

III. OUR MAIN CONTRIBUTIONTION,

The concept of isodual mathematics was first proposed by Rugger Maria Santilli [7] in which he introduced the two kinds namely- Isofield of kind-I and Isofield of kind-II.

Our proposed MOR Cryptosystem for Camina group using isodual mathematics:

If G is any group with binary operation $< \hat{G}+, \hat{X} >$ and identity element e (particular e=1) then $\hat{1} = \frac{1}{T}, T \in G.$

If $a, b \in G$ then

$$\hat{a}\hat{x}\hat{b} = \frac{1}{T}aT\frac{1}{T}b = \frac{1}{T}ab = \widehat{ab}$$

Where

$$\hat{a} = \frac{1}{T}a,\ \hat{b} = \frac{1}{T}b$$

So,

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 $g \in G$. In camina grpup $x \in \frac{G}{G'}$ and $a \in G'$ then $xa = x^g$ for some $g \in G$

$$\text{then } \widehat{xa} = \frac{1}{T}x^g\,T \in G$$

b) Bob computes $\emptyset(\frac{1}{T}x^g)^r$ and $\emptyset(\frac{1}{T}x^g)^{mr}$ for a random $r \in \mathbb{N}$.

c) The ciphertext is $(\emptyset(\frac{1}{T}x^g)^r, \emptyset(\frac{1}{T}x^g)^{mr})$.

Decryption

Alice knows m, so if she receives the ciphertext $(\emptyset(\frac{1}{T}x^g)^r, \emptyset(\frac{1}{T}x^g)^{mr})$. she computes $\emptyset^{mr}$ from $\emptyset^r$ and then $\emptyset^{-mr}$ and then from $\emptyset(\frac{1}{T}x^g)^{mr}$ computes 'g' where $\frac{1}{T} = \hat{e}$, an identity element of G.

IV. THE SECURITY OF THE PROPOSED MOR CRYPTOSYSTEM

For security analysis of proposed cryptosystem we study Seong-Hun Paeng [8] shows that there are sub exponential timealgorithms to solve the DLP in inner automorphism groups forsome non-abelian groups, Lee et al [9] and Christian Tobias[10]. If we consider MOR cryptosystem for camina groupusing isodual mathematics with proposed automorphisms is broken for an arbitrary r.

But in camina group, $x, xa \in \frac{G}{G'}$ implies $< xa > = < \frac{1}{T}x^g >^g$ for some $g \in G$ and $xa = (\frac{1}{T}x^g)^r$ for some integer r and send message $g \in G$ is impossible to recover even knowing arbitrary r as $x \in \frac{G}{G'}$ is unknown and $xG' = (xa)G' = (\frac{1}{T}x^g)^r G' = (x\frac{1}{T}[x, g])^r G' = \frac{1}{T}x^r G'$ and from $|x| = p$ that $r \equiv 1(\mathrm{mod}\, p)$, where p is prime.

For center commutator attack,

In [8], For $x \in G$ define $\tau x : G \to G$ by

$\tau x(y) = x\text{-}1y\text{-}1xy$, $(y \in G)$. Then

$G/Z(G)$ has nontrivial center if and only if there exists $x \in G\backslash Z(G)$ such

that $\tau x(G) \subseteq Z(G)$.

V. CONCLUSION

In this paper we construct the MOR cryptosystem forcamina group using isodual mathematics and show that thesecurity of proposed cryptosystem same as ELGamal cryptosystem in finite filed. The MOR public key cryptosystem and DLP depend on the presentation of group. Thus, the above mentioned cryptosystem is nullify central commutator attack. It is shown that by using structure of camina group using isodual mathematics provide lot of security but more work need to bedone related with security for MOR cryptosystem.

REFERENCES

(1)Akshaykumar Meshram, N.W.Khobragade, Camina Group For The Mor Cryptosystem, IJMTER Volume:1 Issue:5, Nov'2014,(144-148)

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

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

[6] Akshaykumar Meshram, N.W.Khobragade,On The Security Analysis of MOR Public Key Cryptosystem For Camina Group, Mathematical Sciences,Volume:4,Issue1(2015)111-113.

[7] Rugger Maria Santilli,Elements of Hadronic Mechanics-volume-1(second edition),Naukova Dumka Publications KIEV-1995

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

[9] Lee et al, On the Security of MOR Public Key Cryptosystem, ASIACRYPT 2004, LNCS 3329, pp. 387-400

[10] Christian Tobias, Security Analysis of the MOR