ON THE SECURITY ANALYSIS OF MOR PUBLIC KEY CRYPTOSYSTEM FOR CAMINA GROUP

AKSHAYKUMAR J MESHRAM, N.W.KHOBRAGADE

Abstract: In this paper we extend the concept of Meshram et al [1] and analysis the security of MOR public key Cryptosystem using camina group. Finally we claim that the security of proposed system is equivalent to the ELGamal cryptosystem over finite filed.

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

Introduction:

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 via channel that is being monitored by an adversary.

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.

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

Preliminaries:

Most of the definitions used in these papers are standard [5].

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 $ab \equiv c \pmod p$ and $0 \le c < p$.

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 ($0 \le c < p$) and a modulus p, calculate the exponent b such that $ab \equiv c \pmod p$.

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.

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 cryptosystem are 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 $e = g^a \bmod p$, 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 $c_1 = g^k \bmod p$ and $c_2 = e^k m \bmod p$, and sends the pair (c_1, c_2) to Alice. To decrypt the message, Alice computes $c_1^{-a} c_2 \bmod p$.

This is equal to m, since $c_1^{-a} c_2 = g^{-ak} e^k m = e^{-k} e^k m = m \bmod p$.

The MOR Cryptosystem:

Description of the MOR cryptosystem:

Let G be a group and $\emptyset : G \to G$ be an automorphism.
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.
Proposed Mor Cryptosystem For Camina Group:
For a group G to be used in the MOR public key cryptosystem, it is necessary that the DLP over the inner automorphism group Inn(G) of G must be computationally hard to solve and there must be an efficient way to represent group elements as products of the specified generators of G [2]. Here we used camina group for MOR public key cryptosystem.
Camina groups were introduced by A.R.Camina in [6] and it is defined as follows:
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 $xG = \{xg \setminus g \in G\}$ is the conjugacy class of x in G and x{G'} denotes the set $\{x^{g'}/g' \in G'\}$.

In [1], Meshram et al said that on using automorphism of camina group, one can make secure MOR cryptosystem.
Here now we are going to construct MOR cryptosystem for camina group G.
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 to G/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.
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 $r \in \mathbb{N}$.
b) The ciphertext is $(\emptyset(x^g)^r, \emptyset(x^g)^{mr})$.
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'.
The Security Of The Proposed MOR Cryptosystem:
For security analysis of proposed cryptosystem we study papers of Christian Tobias [7] and Lee et al [8]. If we consider MOR cryptosystem using camina group with proposed automorphisms is broken for an arbitrary r.
But in camina group, $x, xa \in \frac{G}{G'}$ implies $< xa >=< x >^g$ for some $g \in G$ and $xa = (x^g)^r$ 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 $xG' = (xa)G' = (x^g)^r G' = (x[x,g])^r G' = x^r G'$ and from $|x| = p$ *that* $r \equiv 1(modp)$, where p is prime.
We are thankful to professor Ol'shanskii for this this important information.This is clear from the action of the automorphisms on eliments as described above claim that the security of proposed system is equivalent to the ELGamal cryptosystem over finite filed.
For center commutator attack,
In [8], For $x \in G$ define $\tau x : G \to G$ by
$\tau x(y) = x^{-1}y^{-1}xy$, $(y \in G)$.

Then $\frac{G}{Z(G)}$ has nontrivial center if and only if there exists $x \in G \setminus Z(G)$ such that $\tau x(G) \subseteq Z(G)$.

The MOR public key cryptosystem and DLP depend on the presentation of group. Due to representation of camina group defined above gives that there is no effect on said cryptosystem using such attack.
The advantage of selecting camina group as group for MOR cryptosystem is that it is reduced to p-group and offer security as same as ELGamal cryptosystem [9].

Conclusion:

In this paper we construct the MOR cryptosystem using camina group and show that the security of proposed cryptosystem same as ELGamal cryptosystem in finite filed. The aim of this paper is to analysis the security of MOR public key cryptosystem which used camina group. It is shown that by using structure of camina group provide lot of security but more work need to be done related with security for MOR cryptosystem.

References:

1. *Md Sirajul Huque, Ismatha Begum,* A Detail Study on Various Security Threats ...; Mathematical Sciences International Research Journal ISSN 2278 – 8697 Vol 2 Issue 1 (2013), Pg 93-96
2. Akshaykumar Meshram, N.W.Khobragade, Camina Group For The Mor Cryptosystem, IJMTER Volume:1 Issue:5, Nov'2014,(144-148)
3. 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.
4. *Chinnu R, Maria Joy,* Triple Protection for Web Documents Using the ; Mathematical Sciences International Research Journal ISSN 2278 – 8697 Vol 2 Issue 2 (2013), Pg 442-447
5. S.-H. Paeng, D. Kwon, K.-C. Ha, J. Kim, Improved public key cryptosystem using finite non abelian groups, IACR ePrint 2001/066.
6. Ganga Ram Gautam, Jaydev Dabas, Existence and Stability Results of the Impulsive; Mathematical Sciences International Research Journal ISSN 2278 – 8697 Vol 3 Issue 1 (2014), Pg 57-60
7. Seong-Hun Paeng ,On the security of cryptosystem using automorphism groups, Information Processing Letters 88 (2003) 293–298
8. Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman, An introduction to mathematical
9. cryptography, Springer, 2008.
10. A.R. Camina, Some conditions which almost characterize Frobenius groups, Israel J. Math 31 (1978), 153–160.
11. KR. Nithyakalyani, Dr. K. Subramanian, Bold Signed total Domination for **Km,N,P** , **Cm,N** and **Wn** Graphs; Mathematical Sciences international Research Journal ISSN 2278 – 8697 Vol 3 Issue 2 (2014), Pg 688-690
12. Christian Tobias, Security Analysis of the MOR Cryptosystem, PKC 2003, LNCS 2567,pp. 175-186.
13. Lee et al, On the Security of MOR Public Key Cryptosystem, ASIACRYPT 2004, LNCS 3329, pp. 387-400.
14. Aayn Mahalanobis, A note on using finite non-abelian p-groups in the MOR cryptosystem ,
15. arXiv:cs/0702095v1[cs:CR] 16 Feb 2007.
16. *S. Nageswara Rao,* Eigenvalues for Iterative Systems of Nonlinear Third Order Boundary ; Mathematical Sciences International Research Journal ISSN 2278 – 8697 Vol 2 Issue 2 (2013), Pg 218-222

* * *

Assistant Professor[1], Department of Mathematics & Humanities, Y.C.C.E, Nagpur (M.S.), India
akj.meshram@gmail.com
Professor[2], Department of Mathematics, R.T.M. Nagpur University, Nagpur (M.S.), India
khobragadenw@gmail.com