A KEY EXCHANGE PROTOCOL
USING THE NEAR-RING
GENERATED BY THE INNER
AUTOMORPHISM OF A FINITE
SIMPLE GROUP

D. Ezhilmaran\textsuperscript{1} and M. Arunma\textsuperscript{2}
\textsuperscript{1,2} Department of Mathematics, School of Advanced Sciences,
VIT - University, Vellore -632014, India,
ezhil.devarasan@yahoo.com and arunmamkumaran@gmail.com

February 9, 2017

Abstract

In this paper we present a new key exchange protocol which works in the Near Ring generated by the Inner Automorphism of a finite simple group. We prove that the protocol meet the security of key establishment based on the conjugacy search problem.

AMS Subject Classification: 16Y30, 94A60, 94A62

Key Words: Key exchange protocol; Conjugacy search problem; Near Ring of Inner automorphism over finite simple non Abelian group

1 Introduction

A protocol which allows for a key exchange between two parties by using a secret key to use in their succeeding private communication is known to be a key exchange protocol. Diffie-Hellman introduced the first key exchange protocol in [3]. Many key exchange protocol
were developed using discrete logarithm problem. The development in quantum computing made easy to solve the discrete logarithm problem. Hence the mathematicians search for new key exchange relying on hard problem. The new key exchange protocols work over non commutative cryptography. A public key crypto system was built using finite non abelian groups. The system works under the conjugate action defined on the discrete logarithm problem in the inner automorphism groups. This public key crypto system was proposed in [10]. Diffie-Hellman key agreement using Braid group was proposed by Koetal. Cryptography based on braid group uses Conjugacy search problem. Anshel et als key exchange also uses conjugacy search problem for the secured protocol. Dima and ShpilRain proposed on authentication scheme using conjugacy search problem in non-commutative semigroup [6].

We make use of conjugacy search problem [CSP] for a new key exchange protocol which is resistant to Man-in-the-Middle attack. It is more interesting to study automorphism. As automorphism groups of non abelian groups are not simpler compared to that of abelian groups. We propose a new key exchange using inner automorphisms over a finite non abelian group. We will use CSP in our protocol so that our protocol makes the security consideration.

A brief introduction of the inner automorphisms of a finite non abelian group which generates the near ring in section 2. In section 3 we define the proposed key exchange protocol mention its enviable attributes. The security consideration of the proposal is described in section 4. The paper ends with conclusion.

2 Preliminaries

Definition 1. A near-ring is a set N together with binary operations ”+” and ”.” such that
1. \((N, +)\) is a group
2. \((N, \cdot)\) is a semigroup
3. \((n_1 + n_2)n_3 = n_1n_3 + n_2n_3 \forall n_1, n_2, n_3 \in N\)

Definition 2. Let us now define an algebraic structure of mappings.

Let \(\Omega\) be a finite non-abelian simple group whose identity is \(\omega_0\).
For any two elements \((\omega \neq \omega_0)\) and \(\omega_1\) (arbitrary) of \(\Omega\) we can find a pair of sequences \([\mu_1, \mu_2, \ldots, \mu_n] \in \Omega\) and \([\gamma_1, \gamma_2, \ldots, \gamma_n]\) being integers such that

\[
\mu_1\omega^{\gamma_1}\mu_1^{-1} \ldots \mu_n\omega^{\gamma_n}\mu_n^{-1} = \omega_1
\]

and

\[
\mu_1\sigma^{\gamma_1}\mu_1^{-1} \ldots \mu_n\sigma^{\gamma_n}\mu_n^{-1} = \omega_0, \text{ if } \sigma \neq \omega.
\]

The mapping of \(\Omega\) into itself which maps \(\omega_0\) into \(\omega_0\) is represented in the form of pair of finite sequences as indicated.

Let \(\Omega\) be the group with identity \(0\). The sum and the product of the mappings of \(\Omega\) into itself is by

\[
(\phi + \chi)\omega = \phi\omega + \chi\omega \quad \forall \omega \in \Omega
\]

\[
(\phi \chi)\omega = \phi(\chi\omega), \forall \omega \in \Omega
\]

Now we define the mappings along with the pair of sequences as

\([\mu_1, \mu_2, \ldots, \mu_n] \in \Omega\) and \([\gamma_1, \gamma_2, \ldots, \gamma_n]\) being the integers as

\[
\phi(\omega) = \mu_1 + \gamma_1\omega - \mu_1 + \ldots + \mu_n + \gamma_n\omega - \mu_n \\forall \omega \in \Omega
\]

**Definition 3.** Let \(T\) denote the algebraic structure of mappings defined above.

1. \((T, +)\) is a group.

   Let \(\phi, \chi \in T\) with the pair of sequences \([\mu_1, \mu_2, \ldots, \mu_n] \in \Omega\) and \([\gamma_1, \gamma_2, \ldots, \gamma_n]\) being integers as

   \[
   (\phi + \chi)\omega = \phi(\omega) + \chi(\omega).
   \]

   \[
   \phi(\omega) + \chi(\omega) = \mu_1 + r_1\omega - \mu_1 + \ldots + \mu_n + r_n\omega - \mu_n + \gamma_1 + t_1\omega - \gamma_1 + \ldots + \gamma_n + t_n\omega - \gamma_n
   \]

   \[
   = (\mu_1 + \gamma_1) + (r_1 + t_1)\omega - (\mu_1 + \gamma_1) + \ldots + (\mu_n + \gamma_n) + (r_n + t_n)\omega - (\mu_n + \gamma_n)
   \]

   \[
   = (\phi + \chi)\omega
   \]

   The additive identity of \(T\) is 0 which is the additive identity of \(\Omega\).

2. Clearly \((T, \cdot)\) is a semigroup under multiplication \((\phi \chi)\omega = \phi(\chi\omega)\) [By definition of product]

3. Right Distributive law
Let $\phi, \chi, \tau, \epsilon \in T$

$$(\phi + \chi) \tau = \phi \tau + \chi \tau.$$ 

$$(\phi + \chi) \tau \omega = (\mu_1 + \gamma_1) + (r_1 + t_1) \tau \omega - (\mu_1 + \gamma_1) + ... + (\mu_n + \gamma_n)$$

$$+ (r_n + t_n) \tau \omega - (\mu_n + \gamma_n)$$

$$= (\mu_1 + ... + \mu_n) + r_1 (\tau \omega) + ... + r_n (\tau \omega) - (\mu_1 + ... + \mu_n)$$

$$+ (\gamma_1 + ... + \gamma_n) + t_1 (\tau \omega) + ... + t_n (\tau \omega) - (\gamma_1 + ... + \gamma_n)$$

$$= \mu_1 + r_1 (\tau \omega) - \mu_1 + ... + \mu_n + r_n (\tau \omega) - \mu_n$$

$$+ \gamma_1 + t_1 (\tau \omega) - \gamma_1 + ... + \gamma_n + t_n (\tau \omega) - \gamma_n$$

$$= \phi (\tau \omega) + \chi (\tau \omega)$$

$$= (\phi \tau) \omega + (\chi \tau) \omega. \text{ Hence } T \text{ satisfies Right Distributive Law.}$$

4. T does not holds left distributive law.

Hence T is a right near-ring. i.e T the set of mappings of $\Omega$ into itself is a right near-ring.

The endomorphism of T

For $\omega \in \Omega$ Let $L(\omega)$ denote the intersection of all the left ideals $L(\omega')$ where $\omega' \neq \omega$. The non-zero elements of $\Omega : \omega_1, \omega_2, ..., \omega_n$. The element of $L(\omega)$ for $i, j = 1, ..., n$ define $e_{ij}$ for which $e_{ij} \omega_j = \omega_i$.

$T$ contains an element $e_{ij}$ such that $e_{ij} \omega_k = \delta_{jk} \omega_i$ where $\delta_{jk}$ is the Kronecker symbol.

$\Gamma$ be the multiplicative semigroup of endomorphism of $\Omega$. Define $\chi_j$ by $\chi_j x = (\chi x) e_j$. For every element $x$ in $\Gamma$ can be uniquely represented as $x = x_1 + x_2 + ... + x_n, x \in L(\omega_j)$.

We have $\chi$ to be uniquely determined by the components $x_j$. i.e $\chi x = \sum_{j=1}^{n} \chi_j x$. Now, If $\chi_j$ is any homomorphism of $T^+$ into $Te_j$ then $\chi_j x = a_j x e_{A(j),j} \in \Gamma$.

Therefore $\chi x = \sum_{j=1}^{n} a_j x e_{A(j),j}$

Theorem:

The near- ring automorphism of T is an inner automorphism. i.e. $y \rightarrow \varphi y \varphi^{-1}$ Where $\varphi$ is a non-zero element in $\Gamma$.

Proof : Let $\chi$ be an automorphism of $T$ for all $y$ we have $\chi y = \sum_{j=1}^{n} a_j y e_{A(j),j} \in \Gamma$. $\chi$ is an automorphism hence $\chi(e_k) \neq 0$ and $\exists j$ such that $A(j) = k$. Thus there is a permutation $j \rightarrow A(j)$. Since
\(\chi(e_{A(j)}) \neq 0; a_i \neq 0\), Let \(a_i'\) be the inverse permutation.

Now \(\chi\) permutes the \(T e_j\) and transforms idempotents into idempotents. i.e. \(\chi e_j = a_{i'} e_j e_{ja_i'}\) which is an idempotent in \(T e_{a_i'}\) and so.

\[
\chi(e_j) = e_{a_j'} \\
\Rightarrow \chi(e_{ij}) = e_{a_{i},a_{j}'} \\
   = a_{a_j'} e_{ij} e_{ja_i'}
\]

Hence \(a_{a_j} e_{i,a_{j}'} = e_{a_{i}a_{j}'}\).

Thus
\[
a_{a_j'} \omega_i = a_{a_j'} e_{i,a_{j}'} \omega_{a_i'} \\
   = e_{a_{i}a_{j}' \omega_{a_i'}} \\
   = \omega_{a_i'}
\]

which is true for all \(i\) and all \(j\). i.e \(a_{k} \omega_{i} = a_{k} \omega_{i}\) for all \(i, k, l\).

Thus \(a_1 + a_2 + ... + a_n = \varphi \epsilon T\). Put \(e_{A(1),1} + ... + e_{A(n),n} = \mu\). Therefore \(\chi(y) = \varphi y \mu, \forall y \epsilon T\).

Take \(y = e\).

\[
\chi(e) = \varphi e \mu \\
e = \varphi \mu \\
\Rightarrow \mu = \varphi^{-1}
\]

Therefore \(\chi(y) = \varphi y \varphi^{-1}\). Hence the near ring automorphism of \(T\) is of the form \(\varphi y \varphi^{-1}\).

### 3 Key Agreement Protocol based on Conjugacy Search Problem

**The Conjugacy Search Problem (CSP):**

The Conjugacy Search Problem is to find \(\chi \epsilon T\) satisfying \(\phi \rightarrow \chi \phi \chi^{-1}\) for some \(\chi \epsilon T\). CSP asks to locate at least one exacting element \(\chi \epsilon T\). It is measured infeasible to solve CSP and is to be hard. The random conjugate of \(\phi\) to be equal to \(\chi\) is insignificant. Hence the probability is negligible.

Let \(T\) be the Near-ring of Inner Automorphism.

Let \(x \epsilon T\);

\(\phi \epsilon T\) be A’s long term private key.
$X_A = \phi x \phi^{-1}$ is A’s long term public key.

$\chi \epsilon T$ be B’s long term private key.

$X_B = \chi x \chi^{-1}$ B’s long term public key.

**Key Exchange:**

S1 A chooses $\tau \epsilon T$ and computes

$Y_A = \tau x \tau^{-1}$.

If $Y_A = I$ (Identity), the protocol terminates otherwise A sends $Y_A$ to B.

S2 After receiving $Y_A$, B chooses $\omega \epsilon T$ and computes $K_B = \chi X_A \chi^{-1}$
and $Y_B = K_B \omega Y_A \omega^{-1} K_B^{-1}$

S3 If $Y_B$ or $K_B = I$ then the protocol terminate else B sends $Y_B$ to A.

S4 After receiving $Y_B$, A computes

$K_A = \phi X_B \phi^{-1}$.

The shared key for A is $KEY_A = \tau K_A^{-1} Y_A K_A \tau^{-1}$.

S5 B computes the shared key $KEY_B = \omega Y_A \omega^{-1}$.

S6 If $KEY_A$ or $KEY_B$ is I then termination of protocol run occurs.

S7 If A and B share the Secret Key after a regular protocol running

$K = KEY_A = KEY_B$

### 4 Security Consideration

As by our assumption that the CSP is hard our protocol meets the following desirable attributes.

*Security of Known-Key*: It is clearly known that A and B share their unique session key K if they follow the Key exchange protocol as proposed above.

*Forward Secrecy*: For each entity, the random elements $\tau$ and $\omega$ act on the session key K during the computation. For an intruder who knows the private keys of A or B i.e $\phi$ or $\chi$ could extract $K_A$ or
$K_B$ from $Y_A$ and $Y_B$ to know the previous or next session keys. He
has to compute $\chi X_A \chi^{-1}$ which is impossible as the CSP is well secured and hence our key exchange protocol has the forward secrecy.

Key Compromise Impersonation: If an adversary $E$ wants to impersonate $A$ by knowing $A$’s long-term private key $\phi$, but it is not possible for him to impersonate $B$ to $A$ without knowing $B$’s long term private key $\chi$. In order to impersonate successfully $E$ should know the ephemeral key $\tau$ of $A$ for this he should extract $\tau$ from $A$’s ephemeral public value $Y_A = \tau x \tau^{-1}$ which is not possible as the CSP is hard.

Unknown Key-share: An adversary $E$ should try to make $A$ believe that the session key is shared with $B$, where $B$ believes that the session key shared with $E$. For this he set his public key to be certified by using the public keys of $A$ and $B$ that is $X_A, X_B$ and $x$. However after simple calculation we come to know that the unknown key share attack fails.

Key Control: The key control can be possible only by the key agreeing parties and no third party can have a key control. Hence the key control attack may happen only by the key exchanging party of the protocol $B$. For this $B$ should solve the following $K = \omega Y_A \omega^{-1}$. Again it is impossible because of the hardness of CSP.

5 Conclusion

In this paper we proposed a new key exchange protocol using near ring generated by inner automorphism. For the security consideration of the protocol we rely on the conjugacy search problem in a near ring generated by inner automorphism. The way we have focused on the inner automorphism of a finite simple group meets the desirable attribute of our protocol. Our protocol makes use of the fact that the CSP is hard in the described structure. We prove that our key exchange protocol is secure against many well-known attacks.
References


