

KEY EXCHANGE PROTOCOL BASED ON TRIPLE DECOMPOSITION PROBLEM USING NON-ABELIAN NEAR-RING STRUCTURE

D.Ezhilmaran¹ and V.Muthukumaran²

^{1,2} Department of Mathematics, School of Advanced Sciences,
VIT - University, Vellore -632014, India,
ezhil.devarasan@yahoo.com and muthu.v2404@gmail.com

February 8, 2017

Abstract

Non-abelian structure have attracted by the cryptographer to build the public key cryptographic protocols. In this article we proposed a new key exchange protocol based on triple decomposition problem which work in non-abelian near-ring. We have prove that our protocol meet the security attribute based on centralizer near-ring.

AMS Subject Classification: 68M12, 49M27, 16Y30

Key Words: Key agreement protocol, triple decomposition problem, non-abelian near-ring, centralizers of near-rings

1 Introduction

Public key cryptography (PKC) was introduced by [3], many public key cryptography schemes have been proposed most of them broken. Currently most outstanding PKC schemes are based on the

recognized challenging of convinced problem in special large finite commutative rings. For example, [10] solving the integer factoring problem defined over the ring Z_n forms the ground of the basic RSA cryptosystem.

PKC presently in use, such as the RSA algorithm, Diffie-Hellman, and elliptic curve methods are number theory based on the structure of abelian groups. Although there have been Most common no successful attacks on the standard protocol there is a feeling that the courage of computing machinery has made these techniques less secure. As a result of this there has been an active line of research to develop and analyses the new cryptosystems and key exchange protocols based on non-commutative cryptographic platforms its more useful for cryptographer to build the PKC system.

In [1] introduced a new key agreement scheme using non-commutative groups known as the Commutator KAP exploiting the difficulty of conjugacy search problem. In [7] proposed a new key exchange primitive based on the Triple Decomposition Problem in non-commutative monoid and he implement our protocol based on the braid groups. [6] proposed a new key exchange protocol established on Discrete Heisenberg group they form a two layers security based on triple decomposition problem and twisted conjugacy problem. In [11] used decomposition problem in braid groups and reducing the length based attacks. [12] proposed new platform key exchange in elliptic curve cryptography based on decomposition problem and improved security condition of Shpilrain and Ushakov key exchange protocol. [4] proposed new key exchange protocol based on decomposition problem in centralizer near-rings and secure the men-in-middle attacks. In this article we proposed new triple decomposition problem based on centralizer of near-rings.

This paper is organised Section 2 we recall the some basic definition of near-rings and centralizer of near-rings. Section 3 we construct new key exchange protocol based on triple decomposition in non-commutative near-ring 4 Implementation of our key exchange protocol based on centralizer of near-rings, and section 5 we conclude the paper.

2 Preliminaries

In algebraic systems with two binary operations such as addition and multiplication, satisfying the entire ring axioms except possibly one of the distributive laws and the commutativity of addition, such systems are called near rings.

Definition 1: A triplet $(N, +, \bullet)$ is called a near-ring if

- i The ordered pair $(N, +)$ is a group (not necessarily abelian)
- ii The ordered pair $(N, \bullet)$ a semi group
- iii For every element $n_1, n_2, n_3 \in N$ then $(n_1 + n_2) \cdot n_3 = n_1 \cdot n_3 + n_2 \cdot n_3$

To be more precise, they right near-rings because the right distributive law is satisfied.

Definition 2:

- i N is called a abelian near-ring with respect to addition then $n_1 + n_2 = n_2 + n_1$ for all $n_1, n_2 \in N$.
- ii N is called a abelian near-ring with respect to multiplication then $n_1 \cdot n_2 = n_2 \cdot n_1$ for all $n_1, n_2 \in N$.
- iii N is called a non-abelian near-ring with respect to multiplication then $n_1 \cdot n_2 \neq n_2 \cdot n_1$ for all $n_1, n_2 \in N$.

Definition 3: For an element $n \in N$ let $C(n)$ be the set of elements that commute with n , i.e., $C(n) = \{r \in N \mid nr = rn\}$. $C(n)$ is called the centralizer of near-ring in N . For a subset $R = \{n_1, n_2, \dots, n_k\}$ of N , define as follows $C(R) = C(n_1, n_2, \dots, n_k)$ to be the set of elements in N that commute with all n_i for $i = 1, 2, \dots, k$ where $C(R) = C(n_1) \cap \dots \cap C(n_k)$.

3 Diffie Hellman-like Key Exchange protocol based on triple decomposition problem

In this section we construct new key exchange protocol based on triple decomposition in non-commutative near-ring

The protocol

The system requires a non-commutative near-ring with identity elements and two sequences containing 5 subsets of N each, say $P = \{P_1, P_2, P_3, Y_1, Y_2\}$ and $Q = \{Q_1, Q_2, Q_3, Z_1, Z_2\}$ satisfying the invertibility and commutativity conditions:

- i The element of Y_1, Y_2, Z_1, Z_2 are invertible (invertibility conditions).
- ii $[P_2, Z_1] = 1, [P_3, Z_2] = 1, [Q_1, Y_1] = 1, [Q_2, Y_2] = 1$ (commutativity conditions).

Setting the private and the public keys

Suppose a near-ring N and the subsets $P = \{P_1, P_2, P_3, Y_1, Y_2\}$ and $Q = \{Q_1, Q_2, Q_3, Z_1, Z_2\}$ satisfying i and ii above are fixed. Alice and Bob carry out the following steps:

Step 1 Alice and Bob agree on who will use which set of subsets; say Alice uses P and Bob uses Q .

Step 2 Alice randomly chooses $p_1 \in P_1, p_2 \in P_2, p_3 \in P_3, y_1 \in Y_1, y_2 \in Y_2$, and computes: $c = p_1 y_1, d = y_1^{-1} p_2 y_2$ and $e = y_2^{-1} p_3$. Her private key is (p_1, p_2, p_3) and her public key is (c, d, e) .

Step 3 Bob randomly chooses $q_1 \in Q_1, q_2 \in Q_2, q_3 \in Q_3, z_1 \in Z_1, z_2 \in Z_2$, and computes: $u = q_1 z_1, v = z_1^{-1} q_2 z_2$ and $w = z_2^{-1} q_3$. Her private key is (q_1, q_2, q_3) and her public key is (u, v, w) .

Key exchange protocol

Alice and Bob want to agree key exchange by the following steps follows

Step 1 Alice sends Bob her public key (c, d, e) .

Step 2 Bob sends Alice his public key (u, v, w) .

Step 3 Alice computes $p_1 u p_2 v p_3 w$.

Step 4 Bob computes $q_1 c q_2 d q_3 e$.

Step 5 Alice computes $p_1 u p_2 v p_3 w = p_1 q_1 z_1 p_2 z_1^{-1} q_2 z_2 p_3 z_2^{-1} q_3 = p_1 q_1 p_2 q_2 p_3 q_3$.

Step 6 Bob computes $q_1 c q_2 d q_3 e = q_1 p_1 y_1 q_2 y_1^{-1} p_2 y_2 q_3 y_2^{-1} p_3 = p_1 q_1 p_2 q_2 p_3 q_3$.

Shared key is $p_1 q_1 p_2 q_2 p_3 q_3$

The idea is to hide the private key by multiplying each component by some elements from the non-commutative near-ring. These elements are chosen from subsets satisfying the invertibility and

commutativity conditions so that both parties compute the same key.

Note: The following case should be avoided because, they allow immediate computation from public key to the shared key.

Case1: If $[Y_1, Z_1] = 1$, $[Y_2, Z_1] = 1$, and $[Y_2, Z_2] = 1$ then shared key can be computed from the public keys by

$$\text{shared key} = (p_1 y_1)(q_1 z_1)(y_1^{-1} p_2 y_2)(y_2 p_3)(z_2 b_3) = cudvew$$

Case2: If $[P_2, Q_1] = 1$, $[P_3, Q_2] = 1$, and $[P_3, Q_1] = 1$, then shared key can be computed from the public keys by

$$\text{shared key} = (p_1 p_2 p_3)(q_1 q_2 q_3) = cdeuvw$$

4 Implementation of key agreement protocol based on triple decomposition problem in centralizer of near-rings

Let N be non-abelian near-rings with two sets of subnear-rings S_{y1}, S_{y2} and S_{z1}, S_{z2} that are finitely generated and the user publishes the generators of subnear-rings. The elements of the above subnear-rings satisfy the commutative condition the elements of the above subsets commute with each other.

Step 1 Alice chooses two elements $y_1, y_2 \in N$ and computes the centralizers of y_1 and y_2 its gives $C(y_1)$ and $C(y_2)$ published her choice of subsets S_{y1} of $C(y_1)$ and S_{y2} of $C(y_2)$.

Step 2 Bob chooses two elements $z_1, z_2 \in N$ and computes the centralizers of z_1 and z_2 its gives $C(z_1)$ and $C(z_2)$ published her choice of subsets S_{z1} of $C(z_1)$ and S_{z2} of $C(z_2)$.

Step 3 Alice chooses random elements $p_1 \in N, p_2 \in S_{z1}, p_3 \in S_{z2}$. (p_1, p_2, p_3) as her private key and She sends Bob her public key (c, d, e) where $c = p_1 y_1, d = y_1^{-1} p_2 y_2$ and $e = y_2^{-1} p_3$

Step 4 Bob chooses random elements $q_1 \in S_{y1}, q_2 \in S_{y2}, q_3 \in N$. (q_1, q_2, q_3) as his private key. He sends Alice her public key (u, v, w) where $u = q_1 z_1, v = z_1^{-1} q_2 z_2$ and $w = z_2^{-1} q_3$

Step 5 Alice computes $K_P = p_1 u p_2 v p_3 w = p_1 q_1 p_2 q_2 p_3 q_3$.

Step 6 Bob computes $K_Q = q_1 c q_2 d q_3 e = p_1 q_1 p_2 q_2 p_3 q_3$.

Where $K_P = K_Q = p_1 q_1 p_2 q_2 p_3 q_3$ key agreement is successful. The following discussion directs us to some necessary conditions for the system to truly rely on the triple decomposition problem.

$$c = p_1 y_1 \quad (1)$$

$$d = y_1^{-1} p_2 y_2 \quad (2)$$

$$e = y_2^{-1} p_3 \quad (3)$$

Solving (2) that is decomposing d as a three elements y_1^{-1}, p_2, y_2 known as triple decomposition problems. In order to apply the triple decomposition problem in near-ring must satisfy the following properties.

- i N should be a non-abelian near-ring with identity element.
- ii It should be computationally easy to perform near-rings operations multiplication and inversion.
- iii It should be computationally easy to generate pairs $(p, \{p_1, \dots, p_k\})$ such that $pp_i = p_i p$ for each $i = 1, \dots, k$
- iv For a generic set $\{n_1, \dots, n_k\}$ of element of N it should be difficult to compute $C(n_1) \cap \dots \cap C(n_k) = C(n_1, \dots, n_k)$.
- v Even if $R_1 = C(n_1, \dots, n_k)$, $R_2 = C(\bar{n}_1, \dots, \bar{n}_k)$ are computed it should be hard to find $y_1 \in R_1, y_2 \in R_2$ and $p \in R$ and such that $d = y_1 p y_2$ where R is some fixed subnear-ring of given by its generating set.

4.1 Security analysis of protocol

The adversary break the protocol it is sufficient to find either Alices or Bobs private key which may be accomplished as follows

Possible attacks on Alice private key

Find an element $\bar{q}_1$ and $\bar{q}_2$ which commutes with every element of the subnear-rings of S_{y_1}, S_{y_2} and an element $\bar{q}_3 \in N$ such that $K_P = p_1 \bar{u} p_2 \bar{v} p_3 \bar{w}$. The triples $(\bar{u}, \bar{v}, \bar{w})$ is equivalent to (u, v, w) (That means, $p_1 \bar{u} p_2 \bar{v} p_3 \bar{w} = p_1 u p_2 v p_3 w$ where $\bar{u} = \bar{q}_1 \bar{z}_1, \bar{v} = \bar{z}_1^{-1} \bar{q}_2 \bar{z}_2$, and $\bar{w} = \bar{z}_2^{-1} \bar{q}_3$ therefore the triples $(\bar{u}, \bar{v}, \bar{w})$ can be used by the adversary to get the shared secret key).

Possible attacks on Bob private key

Find an element $\bar{p}_2$ and $\bar{p}_3$ which commutes with every element of the subnear-rings of S_{z_1}, S_{z_2} and an element $\bar{p}_1 \in N$ such that

$K_Q = q_1 \bar{c} q_2 \bar{d} q_3 \bar{e}$. The triples $(\bar{c}, \bar{d}, \bar{e})$ is equivalent to (c, d, e) (That means, $q_1 \bar{c} q_2 \bar{d} q_3 \bar{e} = q_1 c q_2 d q_3 e$ where $\bar{c} = \bar{p}_1 \bar{y}_1$, $\bar{d} = \bar{y}_1^{-1} \bar{p}_2 \bar{y}_2$, and $\bar{e} = \bar{y}_2^{-1} \bar{p}_3$ therefore the triples $(\bar{c}, \bar{d}, \bar{e})$ can be used by the adversary to get the shared secret key). Consider the attack on Alice and Bob private Key. The most obvious way to carry out such an attack is the followings.

- i Given $n_1, \dots, n_k$ and compute $C(n_1, \dots, n_k)$.
Suppose $S_{y_1} = \langle n_1, \dots, n_k \rangle$ an adversary trying to find y_1 does not know where to choose y_1 from in the beginning. He knows that it commutes with all elements in S_{y_1} . This implies that $y_1 = C(n_1) \cap \dots \cap C(n_k) = C(n_1, \dots, n_k)$. Similarly he knows that $y_2 = C(\bar{n}_1, \dots, \bar{n}_k)$ where $S_{y_2} = \langle \bar{n}_1, \dots, \bar{n}_k \rangle$. So if the problem stated above is solved then the subnear-rings that y_1 and y_2 belong to can be computed. Now the adversary knows where to take y_1 and y_2 from.
- ii Given $d = y_1^{-1} p_2 y_2$ find $y_1 \in R, p_2 \in P$ and $y_2 \in \bar{R}$ where $R = C(n_1, \dots, n_k)$, $\bar{R} = C(\bar{n}_1, \dots, \bar{n}_k)$ and P is a subnear-rings of N given by its generators.

These two problems become hard because the adversary is unable to break the protocol.

5 Conclusions

This paper, we proposed a new key agreement protocol based on triple decomposition problem in centralizer of near-rings. This protocol has two major advantages over all key exchange protocols. There are two way an intruder has to solve the situation. The first way is to find the common centralizer of a finite number of elements and the second way is to solve the triple decomposition problem. The main security guard is to find the common centralizer of a finite number of elements then we have not yet found a way to make sure that triple decomposition problem is hard.

References

- [1] I. Anshel, M. Anshel, D. Goldfeld, An algebraic method for public key cryptography, *Math. Res. Lett.*, (1999), 15.

- [2] G.A.Cannon, *Centralizer near-rings determined by End G*, Springer Netherlands (1995).
- [3] W. Diffie, M.E. Hellman, New directions in cryptography, *IEEE Trans. Inf. Theory*, **22** (1976), 644-654.
- [4] D. Ezhilmaran, V. Muthukumaran, Key Exchange Protocol Using Decomposition Problem In Near-Ring, *GUJS*, **29(1)** (2016), 123-127.
- [5] G. Ferrero, *Near-rings: some developments linked to semi-groups and groups*, Springer Science and Business Media (2013).
- [6] T. Isaiyarasi, K. Sankarasubramanian, A new key exchange protocol using two layers of security, *J. Discrete Math. Sci. Cryptography*, **15** (2012) 125-133.
- [7] Y. Kurt, *A New Key Exchange Primitive Based on the Triple Decomposition Problem*, IACR Cryptology ePrint Archive (2006).
- [8] A. Mahalanobis, The Diffie-Hellman key exchange protocol and non-abelian nilpotent groups, *Israel J. Math.*, **165(1)** (2008), 161-187.
- [9] Y.K. Peker, A new key agreement scheme based on the triple decomposition problem, *Int. J. Netw. Secur.*, **16(6)** (2014), 426-436.
- [10] R.L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public key cryptosystems, *Commun. ACM*, **21** (1978), 120- 126.
- [11] V. Shpilrain, A. Ushakov, *A new key exchange protocol based on the decomposition problem*, arXiv preprint math/0512140 (2005).
- [12] H.H. Zazali, W.A.M. Othman, Key Exchange in Elliptic Curve Cryptography Based on the Decomposition Problem, *Sains Malays.*, **41(7)** (2012), 907-910.

