Gazi University Journal of Science
GU J Sci
29(1):123-127 (2016)

Key Exchange Protocol Using Decomposition Problem In Near-Ring

D. EZHILMARAN[1,♠], V. MUTHUKUMARAN[2]

[1,2]*School of Advanced Sciences, VIT University, Tamilnadu, India-632014*

Received: 27/11/2015 *Accepted: 05/01/2016*

ABSTRACT

There are several public key cryptosystem around that use computational hardness of either conjugacy search problem or the word problem for non-abelian groups. In this paper we use decomposition problem in near-ring to construct a public key cryptosystem and improved the security of key establishment protocol based on the decomposition problem.

Keywords: *public key cryptosystem, near-ring, decomposition problem, key exchange protocol*

1. INTRODUCTION

Public key cryptography (PKC) was introduced by Diffie and Hellman [7] in 1976, many public key cryptography schemes have been proposed and broken. Today most successful PKC schemes are based on the perceived difficult of certain problem in particular large finite commutative rings. For example, the difficulty of solving the integer factoring problem defined over the ring Z_n forms the ground of the basic RSA cryptosystem[18] and its variants, such as Rabin-Williams schemes[19,20,21] and Cao's schemes[5,6]. In 1999 Anshel introduced a new key agreement scheme using non-commutative groups known as the Commutator KAP exploiting the difficulty of conjugacy search problem and Ko et al. in 2000 and Cha et al[16]. In 2001 proposed new schemes that also work over non-commutative groups. A more recent key agreement protocol that relies on solving multivariate equations on non-commutative rings has been proposed by Yagisawa[22] in 2012.The currently, the security of cryptosystems on non-abelian group G is based on any of the following problems;

♠Corresponding author, e-mail: *ezhil.devarasan@yahoo.com*

The Conjugator Search Problem (CSP). Given $(x,y)\in G\times G$, the problem is to find $z\in G$ such that $y=z^{-1}xz$.

The Decomposition Problem (DP). Given $(x,y)\in G\times G$ and $S\subseteq G$, the problem is to find $z_1,z_2\in S$ such that $y=z_1xz_2$.

The Symmetric Decomposition Problem (SDP). Given $(x,y)\in G\times G$ and $m,n\in\mathbb{Z}$, the problem is to find $z\in G$ such that $y=z^mxz^n$.

The Generalization of the Symmetric Decomposition Problem (GSDP). Given $(x,y)\in G\times G$, $S\subseteq G$ and $m,n\in\mathbb{Z}$, the problem is to find $z\in S$ such that $y=z^mxz^n$.

Several authors have used non-abelian groups for public key exchange. Below we mention a few of them without going into details. In [1, 2, 14, 15] the authors suggest to use the braid groups as platform groups for their respective protocols. In [12] the authors present a PKC based on rings. We can find some attacks on this cryptosystem in [10,11].In [17]the authors introduce the DLP for matrix rings with entries in F_q ,while a Diffie-Hellmann key exchange protocol based on matrices can be found in [8].More recently, B.Hurley and T.Hurley[13] presented a public key cryptosystem using groups rings. The main Idea of this work is design a new key exchange protocol based on decomposition problem using centralizer of near-ring.

The rest of the paper is organized as follows in Section 2 we recall the some basic definition of near-rings and centralizer of near-rings. Section 3 we introduced new protocol based on decomposition problem, Section 4 we discuss the possible attacks, and section 5 is conclusion.

2 . PRELIMINARIES

Definition 1

A near-ring N is a system with two binary operations addition and multiplication, such that:

i. The element of N from a group N^+ under addition.

ii. The element of N from a multiplicative semi-group.

iii. $x(y+z)=xy+xz$ for all $x,y,z\in N$.

Definition 2

Let $(N,+)$ be a group, not necessarily abelian, and let S be a subsemigroup of End N. The set $M_S(N)=\{f:N\to N\mid f\alpha=\alpha f \text{ for every } \alpha\in S\}$ forms a near-ring under pointwise addition and function composition and is called the centralizer near-ring determined by the pair (S,N).Since every near-ring with identity is isomorphic to an $M_S(N)$ for some pair (S,N), these near-rings are quite general and are difficult to study without some restriction on S or N

2.1 New Cryptography Assumption of Near-Rings

Suppose that $(N,+,\bullet)$ is a near-ring. For any random picked element $a\in N$, we define a set $p_a\subseteq N$ by

$$p_a\triangleq\{f(a):f(x)\in\mathbb{Z}_{>0}[x]\}.$$

Then, let us consider the new versions of GSD and CDH problems over $(N,\bullet)$ with respect to its subset P_a, and name them as polynomial symmetric decomposition (PSD) problem respectively:

The Conjugator Search Problem (CSP). Given $(x,y)\in N\times N$, the problem is to find $z\in N$ such that $y=z^{-1}xz$.

The Decomposition Problem (DP). Given $(x,y)\in N\times N$ and $S\subseteq N$, the problem is to find $z_1,z_2\in S$ such that $y=z_1xz_2$.

The Symmetric Decomposition Problem(SDP). Given $(x,y)\in N\times N$ and $m,n\in\mathbb{Z}$, the problem is to find $z\in N$ such that $y=z^mxz^n$.

The Generalization of the Symmetric Decomposition Problem (GSDP). Given $(x,y)\in N\times N$, $S\subseteq N$ and $m,n\in\mathbb{Z}$, the problem is to find $z\in S$ such that $y=z^mxz^n$.

Polynomial Symmetrical Decomposition (PSD) Problem over near-ring N : Given $(a,x,y)\in N^3$ and $m,n\in\mathbb{Z}$ find $z\in p_a$ such that $y=z^mxz^n$.

Polynomial Diffie-Hellman (PHD) Problem over near-ring N : Compute $x^{z_1z_2}$ $\left(x^{z_2z_1}\right)$ for given a,x,x^{z_1} and x^{z_2}, where $a,x\in N,z_1,z_2\in P_a$.

Accordingly, the PSD cryptographic assumption says that PSD problem over $(N,\bullet)$ is intractable, there does not exist probabilistic polynomial time algorithm which can solve PSD problem over $(N,\bullet)$ with non-negligible accuracy with respect to problem scale.

3. DIFFIE-HELLMAN LIKE KEY EXCHANGE PROTOCOL BASED ON DECOMPOSITION PROBLEM(DHK-DP)

Now, let take a near ring N with Decomposition Problem **(DP)** as the underlying work fundamental infrastructure for the key exchange protocol

Protocol 3.1

The decomposition search problem, which we subsequently call just the decomposition problem. The problem is given two elements α, α_1 of the platform near-ring N and two subnear-rings $P, Q \subseteq N$ find element $p \in P, q \in Q$ such that $\alpha_1 = p\alpha q$ .It's straight forward to arrange a key establishment protocol based on this problem assuming $pq = qp$ for any $p \in P, q \in Q$

Step 1: One of the parties Alice publishes a random element $\alpha \in N$

Step 2: Alice chooses $p_1, p_2 \in P$ and sends $p_1 \alpha p_2$ to Bob

Step 3: Bob chooses $q_1, q_2 \in Q$ and sends $q_1 \alpha q_2$ to Alice

Step 4: Alice computes $K_P = p_1 q_1 \alpha q p_2 q_2$ and Bob computes $K_Q = q_1 p_1 \alpha q p_2 q_2$

If $p_i q_i = q_i p_i$ then $K_P = K_Q$ in N .Thus Alice and Bob have a shared secret key.

Security of such a protocol will, of course, depend on a particular platform near-ring N .If DH-like key exchange men in middle attack present a serious threat.

3.2 Man in Middle Attack

Above protocol 3.1 is vulnerable to a man in middle attack. In this attack, an opponent, adversary, does the following

Step 1: Adversary intercepts Alice public value $p_1 \alpha p_2$ and sends $p_1' \alpha p_2'$ to Bob.

Step 2: When Bob transmits his public value $q_1 \alpha q_2$, adversary substitutes it with $p'_1 \alpha p_2'$ and sends it to Alice.

Step 3: Adversary and Alice thus agree on one shared key $K_P = p_1 p'_1 \alpha p_2' p_2$ and adversary and Bob agree on another shared key $K_Q = q_1 p'_1 \alpha p_2' q_2$.

After this exchange, adversary simply decrypts any messages sent out by Alice and Bob, and then reads and possibly modifies them before re-encrypting with the appropriate key and transmitting them to the correct party. This vulnerability is due to the fact that Diffie-Hellman-like key agreement does not authenticate the participants.

In this article, we introduce two new ideas that improve the security of Diffie Hellman-like key establishment protocols based on the decomposition problem:

- We conceal one of the subnear-rings P, Q.
- We make Alice choose her left private key p_1 from one of the subnear-rings P, Q and her right private key p_2 from the other subnear-ring. Same to Bob.

These two improvements together will obviously avoid men in middle attacks.

Let N be a near-ring $n \in N$. Denote $C_N(n)$ the centralizer of n in N, i.e., the set of elements $m \in N$ such that $mn = nm$. For $S = \{n_1, \cdots, n_k\} \subseteq N$, $C_N(n_1, \ldots, n_k)$ denotes the centralizer of S in N , which is the intersection of the centralizers $C_N(n_i), i = 1, 2 \ldots k$.

Now, given a public $\alpha \in N$, Alice privately selects $p_1 \in N$ and publishes a subnear-rings $Q \subseteq C_N(p_1)$. Similarly, Bob privately selects $p_2 \in N$ and publishes a subnear-ring $P \subseteq C_N(q_1)$. Alice then select $p_2 \in P$ and sends $\alpha_1 = p_1 \alpha p_2$ to Bob, Bob selects $q_1 \in Q$ and sends $\alpha_2 = q_1 \alpha q_2$ to Alice.

Thus, in the first transmission, say, the adversary faces the problem of finding p_1, p_2 such that $\alpha_1 = p_1 \alpha p_2$, where $p_2 \in P$, but there is no explicit indication of where to choose p_1 from. Therefore, before arranging something like a man in middle attack the adversary would have to compute the centralizer $C_N(Q)$ first (because $p_1 \subseteq C_N(P)$), which is usually a hard problem by itself.

4. NEW DIFFIE HELLMAN-LIKE KEY EXCHANGE PROTOCOLS BASED ON NORMAL FORM IN CENTRALIZER OF NEAR-RING

Protocol 4.1

In this section we introduce new normal form $N(x)$ which is sequence of symbols uniquely defined for a given n. A specific way of constructing such a sequence depends, of course, on a particular platform near-ring N which we discuss in subsequent sections of paper.

Step1: Alice chooses an element $p_1 \in N$ chooses subnear-ring of $C_N(p_1)$ and publishing its generators $P = \{\varphi_1, \ldots, \varphi_n\}$

Step 2: Bob Choose an element $q_2 \in N$ chooses a subnear-ring of $C_N(q_2)$, and publishes its generators $Q = \{\psi_1, \ldots, \psi_m\}$

Step 3: Alice chooses a random element p_2 from $\langle \psi_1, \ldots, \psi_m \rangle$ and sends the normal form $W_p = N(p_1 \alpha p_2)$ to bob

Step 4: Bob chooses a random element q_2 from $\langle \varphi_1,\ldots,\varphi_n \rangle$ and sends the normal form $W_Q = N(q_1 \alpha q_2)$ to Alice

Step 5: Alice computes $K_p = p_1 W_Q p_2$

Step 6: Bob compute $K_Q = q_1 W_P q_2$

Since $p_1 q_1 = q_1 p_1$ and $p_2 q_2 = q_2 p_2$ we have $K = K_P = K_Q$ the shared secret key.

4.2 Attacks on the Protocol

Attacks on Alice's private key

Find an element $p_1^{'}$ which commutes with every element of the subnear-ring $\langle p \rangle$ and an element $p_2^{'} \in \langle Q \rangle$, such that $W_P = N(p_1^{'} \alpha p_2^{'})$. The pair $(p_1^{'}, p_2^{'})$ is equivalent to (p_1, p_2). (That means, $p_1^{'} \alpha p_2^{'} = p_1 \alpha p_2$, and therefore the pair $(p_1^{'}, p_2^{'})$ can be used by the adversary to get the shared secret key.)

Attacks on Bob's private key

Find an element $q_1^{'}$ which commutes with every element of the subnear-ring $\langle q \rangle$ and an element $q_1^{'} \in \langle P \rangle$, such that $W_Q = N(q_1^{'} \alpha q_2^{'})$. The pair $(q_1^{'}, q_2^{'})$. is equivalent to (p_1, p_2). (That means, $q_1^{'} \alpha q_2^{'} = q_1 \alpha q_2$, and therefore the pair $(q_1^{'}, q_2^{'})$ 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.

1. Compute the centralizer $C_N(P)$.
2. Solve the search version of the membership problem in the double coset $C_N(P) \circ \alpha \circ \langle Q \rangle$

To make the protocol secure. We want both problems to be computationally hard. For the problems (2) to be hard, it's necessary for the centralizer $C_N(P)$ to be large. Otherwise the adversary can use the "Brute force" attack. i.e., enumerate all elements of $C_N(P)$ and find candidates for $p_2^{'}$.

4.3 Requirements on the Platform of Near-Ring N

i. N should be a near-ring which is non-commutative.

ii. There should be an efficiently computable normal form for elements of N.

iii. It should be computationally easy to perform near-ring operations on normal forms.

iv. It should be computationally easy to generate pairs $(p, \{p_1,\ldots,p_n\})$ such that $pp_i = p_i p$ for each $i = 1,\ldots,k$.

v. Multiplication and inversion of elements should be computationally easy with the representation.

vi. For a generic set $\{n_1,\ldots,n_k\}$ of elements of N it should be difficult to compute

vii. $C(n_1,\ldots,n_m) = C(n_1) \cap \cdots \cap C(n_k)$.

viii. Even if $R = C(n_1,\ldots,n_{k1})$ are computed, it should be hard to find $p \in R$ and $q \in R_1$ (where R_1 is some fixed subnear-ring given by a generating set) such that $p \alpha q = \alpha^{'}$, i.e., to solve the membership search problem for a double coset.

5. CONCLUSIONS

Recently, some promising build public-key cryptosystem have been constructed on non-commutative groups, such as braids groups, Thompson's groups, etc. In this article we described totally different method for designing a new public key cryptosystem based on near-ring structure. The security of our scheme is depending upon the decomposition problem in near-ring.

CONFLICT OF INTEREST

No conflict of interest was declared by the authors.

REFERENCES

[1] Anshel, I., Anshel, M., Fisher, B. and Goldfeld, D., " New key agreement protocols in braid group cryptography", In D. Naccache (editor), Topics in Cryptology – CTRSA 2001, volume 2020 of Lecture Notes in Computer Science, SpringerVerlag, Berlin, 13–27, (2001).

[2] Anshel, I., Anshel M. and Goldfeld D., "An algebraic method for public-key cryptography", Mathematical Research Letters, 1–5, (1999).

[3] Bell, Howard E., and Steve Ligh, "Some decomposition theorems for periodic rings and near-rings", Math. J. Okayama Univ 31, (1989), 93-99.

[4] Cannon, Alan G., "Centralizer near-rings determined by End *G*, Springer Netherlands", (1995).

[5] Cao Z., "Conic analog of RSA cryptosystem and some improved RSA cryptosystems", Journal of Natrual Science of Heilongjiang University, (1999).

[6] Cao Z., "A threshold key escrow scheme based on public key cryptosystem", Science in China , 441-448, (2001).

[7] Diffie W. and Hellman M.E., "New directions in cryptography", IEEE Transactions on Information Theory 22, 644-654, (1976).

[8] Eftekhari, Mohammad, "A Diffie–Hellman key exchange protocol using matrices over noncommutative rings", Groups-Complexity-Cryptology 4.1, 167-176, (2012).

[9] Ferrero, Giovanni, "Near-rings*:* some developments linked to semigroups and groups", Springer Science & Business Media, (2013).

[10] Gentry C. and Szydlo M., "Cryptanalysis of the revised NTRU signature scheme", In L. Knudsen (editor), Advances in Cryptology – EUROCRYPT 2002, volume 2332 of Lecture Notes in Computer Science, Springer-Verlag, Berlin, 299–320 ,(2002).

[11] Gentry C., "Key recovery and message attacks on NTRU-composite", In B. Pfitzmann (editor), Advances in Cryptology – EUROCRYPT 2001, volume 2045 of Lecture Notes in Computer Science, Springer-Verlag, Berlin, 182–194, (2001).

[12] Hoffstein J., Pipher J. and Silverman J. H, "NTRU: a ring-based public key cryptosystem", In J. P. Buhler (editor), Algorithmic Number Theory, volume 1423 of Lecture Notes in Computer Science, Springer-Verlag, Berlin, 267–288 ,(1998).

[13] Hurley, Barry, and Ted Hurley, "Group ring cryptography", arXiv preprint, (2011).

[14] Ko K.H, Lee S.J, Cheon J.H, Han J.W, Kang J.s and Park C., "New public-key cryptosystem using braid groups", In M. Bellare (editor), Advances in Cryptology – CRYPTO 2000, volume 1880 of Lecture Notes in Computer Science, Springer-Verlag, Berlin, 166–183, (2000).

[15] Ko K.H, Lee J.W, and Thomas T., "Towards generating secure keys for braid cryptography. Designs", Codes and Cryptography, 317–333, (2007),.

[16] Ko, Ki Hyoung, "New public-key cryptosystem using braid groups", Advances *in* cryptology—CRYPTO 2000. Springer Berlin Heidelberg, (2000).

[17] Odoni R. W. K., Varadharajan V. and Sanders P. W., "Public key distribution in matrix rings", Electronics Letters, 20, 386–387, (1984).

[18] Rivest R.L., Shamir A. and Adleman L., "A method for obtaining digital signatures and public key cryptosystems", Communications of the ACM 21, 120- 126, (1978).

[19] Rabin M.O., "Digitized signatures and public-key functions as intractable as factorization", MIT Laboratory for Computer Science Technical Report, LCS/TR-212 (1979).

[20] Williams H.C., "A Modification of the RSA Public-Key Encryption Procedure", IEEE Transactions on Information Theory, IT No.6 (26), 726-729, (1980).

[21] Williams H.C., "Some public-key crypto-funtions as intractible as factorization", In G.R. Blakley and D.Chaum (Eds): CRYPTO'84, LNCS 196, Springer-Verlag, 66-70, (1985).

[22] Yagisawa, Masahiro, "Key Agreement Protocols Using Multivariate Equations on Non-commutative Ring", IACR Cryptology ePrint Archive (2010).