ORIGINAL PAPER

NEW KEY AGREEMENT PROTOCOL BASED ON FACTOR PROBLEM IN CENTRALIZER NEAR-RING

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

Manuscript received: 10.06.2017; Accepted paper: 02.02.2018;
Published online: 30.06.2018.

Abstract. *Non-abelian structure is attracted by the cryptographers to build public key cryptosystem. In this article we proposed a new key agreement protocol based non-abelian near-rings. We show that our protocol meet the security attribute under the assumptions factor problem in centralizer near-rings and security issues also discussed.*

Keywords: *Factor problem, key exchange protocol, non-abelian near-rings, centralizer near-rings.*

1. INTRODUCTION

Public key cryptography (PKC) was introduced by Diffie and Hellman [1] 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. In 2007 P. Vasudeva Reddy and M. Padmavathamma proposed new authenticated key agreement protocol based on factor problem and the security attribute of the protocol based on elliptic curve over finite field [3]. Structural attacks and linearization equations attacks are working vulnerable based on BKT-B cryptosystem and BKT-FO cryptosystem in factorization problem [2]. In 2016 Haibo Hong et al proposed new public key encryption scheme established on lie group in integer factorization problem and secure the random oral modal [4]. In 2013 Lize Gu et al. proposed a two public encryption scheme established on non-abelian factor problem in random oral modals and resolve Shor's quantum attacks [6]. In 2016 Haibo Hong et al design a new public key encryption established on non-abelian factorization problem in lie groups and they proved his protocol secure IND-CCA2 and random oracle models [5]. Lize Gu and Shihui Zheng proposed Conjugacy Systems based on factorization in non-abelian groups and improved the signature scheme [7]. Srinivas kotyada et al proposed factorization established on three different non-abelian groups GLn(Fq), UTn(Fq) and the Braid Groups[9].In this article we proposed new key agreement protocol based on factor problem in centralizer near-rings.

This article is organised as follows, In section 2, we recall the some basic definition of near-rings, factor problem and centralizer of near-rings. In section 3, proposed a new key exchange protocol based on factor problem in near-rings. In section 4, discussed security issues and section 5 conclude the article.

[1] VIT University, Department of Mathematics, 632014 Vellore, India. E-mail: muthu.v2404@gmail.com; ezhil.devarasan@yahoo.com.

2. PRELIMINARIES

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
$(n_1 + n_2).n_3 = n_1.n_3 + n_2.n_3$

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

Definition 2:

i. N is called the additive- abelian near-ring then $n_1 + n_2 = n_2 + n_1$ for all $n_1, n_2 \in N.$

ii. N is called the multiplicative abelian near-ring then $n_1.n_2 = n_2.n_1$ for all $n_1, n_2 \in N.$

iii. N is called a multiplicative non-abelian near-ring with respect to multiplication then $n_1.n_2 \neq n_2.n_1$ for all $n_1, n_2 \in N.$

iv. N is satisfied the distributive property then the near-ring is called distributive near-rings.

v. If N is called a Idempotent near-ring then satisfying this conditions $n_1 \bullet n_1 = n_1 \;\&\; n_2 \bullet n_2 = n_2.$

Definition 3:

For an element $n \in N$ let $C(n)$ be the set of elements that commute with $n.,$ i.e., $C(n) = \{r \in N \setminus nr = rn\}$. $C(n)$ is called the **centralizer of near-ring** in $N.$

For a subset $R = \{n_1, n_2, \ldots, n_k\}$ of $N,$ define as follows $C(R) = C(n_1, n_2, \ldots, n_k)$ to be the set of elements in N that commute with all n_i *for* $i = 1, 2, \ldots, k$ where $C(R) = C(n_1) \cap \ldots \cap C(n_k).$

Factor problem in non-abelian near-rings

Given an element ω of non-abelian near-rings N and two subnear-rings $\mathrm{N}_1, \mathrm{N}_2 \subseteq N,$ find any two elements $x \in N_1, y \in N_2$ that would satisfy $\omega = x \bullet y.$

3. DIFFI-HELLMAN LIKE KEY AGREEMENT PROTOCOL BASED ON FACTOR PROBLEM

Let N be non-abelian near-rings with two subnear-rings of $\mathrm{N}_1, \mathrm{N}_2 \in N$ that are finitely generated and the user publishes the generator of subnear-rings. The element of above subnear-rings satisfies the commutative conditions for any $x \in N_1, y \in N_2, x \bullet y = y \bullet x.$

3.1. PROTOCOL

1. Alice chooses two random element $x_1, x_2 \in N_1$.
2. Alice computes $\omega_1 = x_1 \bullet x_2$ and send to Bob.
3. Bob chooses two random element $y_1, \mathrm{y}_2 \in N_2$.
4. Alice computes $\omega_2 = y_1 \bullet y_2$ and send to Alice.
5. On knowing x_1 and x_2, Alice computes $K_X = x_1 \omega_2 x_2 = x_1 y_1 x_2 y_2$.
6. On knowing y_1 and y_2, Alice computes $K_Y = y_1 \omega_1 y_2 = x_1 y_1 x_2 y_2$.

If $x_i \bullet y_i = y_i \bullet x_i$ then $K = K_X = K_Y$ in N .Thus Alice and Bob have a shared secret key. If D-H-like key exchange protocol man in middle attack present a serious threat.

3.2. MEN IN MIDDLE ATTACK

Above protocol 3.1 is susceptible to a Man in middle attack.

1. Adversary intercepts Alice public value $\omega_1 = x_1 \bullet x_2$ and sends $\overline{\omega}_1 = \overline{x}_1 \bullet \overline{x}_2$ to Bob.
2. When Bob transmits his public value $\omega_2 = y_1 \bullet y_2$, adversary substitutes it with $\overline{\omega}_2 = \overline{y}_1 \bullet \overline{y}_2$ and sends it to Alice.
3. Adversary and Alice thus agree on one shared key $K_X = x_1 \overline{y}_1 \overline{y}_2 x_2$ and adversary and Bob agree on another shared key $K_Y = y_1 \overline{x}_1 \overline{x}_2 y_2$.

After this exchange, adversary simply decrypts any messages sent out by Alice and Bob, and find the secrete key.

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

i. We conceal one of the subnear-rings N_1, N_2.

ii. We make Alice pick her left private key x_1 from one of the subnear-rings N_1, N_2 and her right private key x_2 from the other subnear-ring. Same to Bob.

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

Let N be a non-abelian near-ring $r \in N$. Denote $C_N(r)$ the centralizer of r in N, i.e., the set of elements $s \in N$ such that $r \bullet s = s \bullet r$. For $P = \{r_1, \cdots, r_k\} \subseteq N$, $C_N(r_1, \ldots, r_k)$ denotes the centralizer of P in N, which is the intersection of the centralizers $C_N(r_i), i = 1, 2 \ldots k$.

Now, given a public $\omega \in N$, Alice privately selects $x_1 \in N$ and publishes a subnear-rings $N_2 \subseteq C_N(x_1)$. Similarly, Bob privately selects $y_2 \in N$ and publishes a subnear-ring $N_1 \subseteq C_N(y_2)$. Alice then select $x_2 \in N_1$ and sends $\omega_1 = x_1 \bullet x_2$ to Bob, Bob selects $y_1 \in N_2$ and sends $\omega_2 = y_1 \bullet y_2$ to Alice.

Thus, in the first transmission, say, the adversary faces the problem of finding x_1, x_2 such that $\omega_1 = x_1 \bullet x_2$ where $x_2 \in N_1$, but there is no explicit indication of where to choose x_1 from. Therefore, before arranging something like a man in middle attack the adversary would have to compute the centralizer $C_N\left(N_1\right)$ first (because $x_1 \subseteq C_N\left(N_1\right)$), this is usually a hard problem by itself.

3.3. NEW FACTOR PROBLEM BASED ON NORMAL FORM IN CENTRALIZER NEAR-RINGS.

In this section we introduced new normal form $\mathbb{N}\left(x\right)$ based on centralizer of near-rings and the protocol following steps are required.

1. Alice chooses an element $x_1 \in N$ chooses subnear-ring of $C_N\left(x_1\right)$ and publishing its generators $N_1 = \{\eta_1, \ldots, \eta_r\}$
2. Bob Choose an element $y_2 \in N$ chooses a subnear-ring of $C_N\left(y_2\right)$, and publishes its generators $N_2 = \{\sigma_1, \ldots, \sigma_s\}$
3. Alice chooses a random element x_2 from $\{\sigma_1, \ldots, \sigma_s\}$ and sends the normal form $W_{N_1} = \mathbb{N}\left(x_1 x_2\right)$ to bob
4. Bob chooses a random element y_2 from $\{\eta_1, \ldots, \eta_r\}$ and sends the normal form $W_{N_2} = \mathbb{N}\left(y_1 y_2\right)$ to Alice
5. Alice computes $K_{N_1} = x_1 W_{N_2} x_2$
6. Bob compute $K_{N_2} = y_1 W_{N_1} y_2$

Since $x_1 \bullet y_1 = y_1 \bullet x_1$ and $x_2 \bullet y_2 = y_2 \bullet x_2$ we have $K = K_{N_1} = K_{N_2}$ the shared secret key.

4. SECURITY ANALYSIS OF THE PROTOCOL

In this section we discussed the possible attack on the protocol described in the previous section.

Attacks on Alice's private key

Find an element $\overline{x_1}$ which commutes with every element of the subnear-ring $\langle N_1 \rangle$ and an element $\overline{x_2} \in \langle N_2 \rangle$, such that $W_{N_1} = \mathbb{N}\left(\overline{x}_1 \bullet \overline{x}_2\right)$.The pair $\left(\overline{x}_1, \overline{x}_2\right)$ is equivalent to $\left(x_1, x_2\right)$. That means, $x_1 \bullet x_2 = \overline{x}_1 \bullet \overline{x}_2$ and therefore the pair $\left(\overline{x}_1, \overline{x}_2\right)$ can be used by the adversary to get the shared secret key.

Attacks on Bob's private key

Find an element $\overline{y_1}$ which commutes with every element of the subnear-ring $\langle N_2 \rangle$ and an element $\overline{y_2} \in \langle N_1 \rangle$, such that $W_{N_2} = \mathbb{N}\left(\overline{y}_1 \bullet \overline{y}_2\right)$.The pair $\left(\overline{y}_1, \overline{y}_2\right)$ is equivalent to $\left(y_1, y_2\right)$.

That means, $y_1 \bullet y_2 = \overline{y}_1 \bullet \overline{y}_2$ and therefore the pair $\left(\overline{y}_1, \overline{y}_2\right)$ 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 $C_N\left(N_1\right)$.
2. Solve the search version of the membership problem in the double coset $C_N\left(N_1\right) \circ \left\langle N_2 \right\rangle$

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 $C_N\left(N_1\right)$ to be large. Otherwise the adversary can use the "Brute force" attack. i.e., enumerate all elements of $C_N\left(N_1\right)$ and find candidates for $\overline{x_2}$.

4.1. REQUIREMENTS ON THE PLATFORM OF NEAR-RING-N

i. N should be a non-abelian near-ring with identity elements.

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 $\left(x, \left\{x_1, \dots, x_k\right\}\right)$ such that $xx_i = x_i x$ for each $i = 1, \dots, k.$

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

vi. For a generic set $\left\{r_1, \dots, r_k\right\}$ of elements of N it should be difficult to compute $C\left(r_1, \dots, r_k\right) = C\left(r_1\right) \cap \cdots \cap C\left(r_k\right).$

vii. Even if $R = C\left(r_1, \dots, r_k\right)$ are computed, it should be hard to find $x \in R$ and $y \in R_1$ (where R_1 is some fixed subnear-ring given by a generating set) such that $x \bullet y = \overline{\omega},$ i.e., to solve the membership search problem for a double coset.

5. CONCLUSION

In this article we discussed new Diffie-Hellman like key agreement protocol based on non-abelian near-ring in factor problem. The security of our key agreement protocol describs on normal form in centralizer near-rings. The attacker want break the protocol he/she want to solve this problem in two phases. In first phase, to find the common centralizer of a finite number of elements and second phase, to solve the factor problem in non-abelian near-rings.

REFERENCES

[1] Diffie, W., Hellman, M.E., *IEEE Transactions on Information Theory*, **22**, 644, 1976.

[2] Liu, J., Fan, A., Jia, J., Zhang, H., Wang, H., Mao, S., *Tsinghua Science and Technology*, **21**(3), 344, 2016.

[3] Reddy, P.V., Padmavathamma, M., *Journal of Discrete Mathematical Sciences and Cryptography*, **10**(5), 697-705, 2007.

[4] Hong, H., Shao, J., Wang, L., Ahmad, H., Yang, Y., *arXiv preprint arXiv:1605.06608*, 2016.

[5] Hong, H., Wang, L., Shao, J., Ahmad, H., Yang, Y., *arXiv preprint arXiv:1605.07168*, 2016.

[6] Gu, L., Wang, L., Ota, K., Dong, M., Cao, Z., Yang, Y., *Security and Communication Networks*, **6**(7), 912, 2013.

[7] Gu, L., Zheng, S., *Journal of Applied Mathematics*, **2014**, 630607, 2014.

[8] Ferrero, G., *Near-rings: some developments linked to semigroups and groups*, Springer Science & Business Media, 2013.

[9] Baba, S., Kotyad, S., Teja, R., *IACR Cryptology ePrint Archive*, **2011**, 048, 2011.

[10] Myasnikov A., Shpilrain V., Ushakov A., *Non-Commutative Cryptography and Complexity of Group-Theoretic Problems*, American Mathematical Society, Providence, RI, USA, 2011.