ADV MATH SCI JOURNAL
Advances in Mathematics: Scientific Journal **9** (2020), no.3, 1389–1395
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.9.3.85 Spec. Issue on ICNTMMA

A SECURE AND ENHANCED PUBLIC KEY CRYPTOSYSTEM USING DOUBLE CONJUGACY SEARCH PROBLEM NEAR-RING

V. MUTHUKUMARN[1], M. ADHIYAMAN, AND D. EZHILMARAN

ABSTRACT. The recent advancement in modern communication systems leads to the requirement of secure cryptosystems for efficient data transfer processes. The public key cryptosystem (PKC) is a well-known method of asymmetric encryption technique which is most prevalent across several domains of application. In such type of systems, the process of key management remains to be a highly difficult issue. The main impartial of the paper is to deliver a secure and enhanced PKC using near-ring for double conjugacy search problem. It secures the public key cryptosystem with non-commutative algebraic structure. The proposed approach presents a novel public key cryptosystem through which the cryptographic keys are generated, stored and used in a more secure manner. The safety analysis of the proposed approach is established on double conjugacy over near-ring and the results state that it is highly secure and resistant against chosen ciphertext attack and brute-force attack.

1. INTRODUCTION

The tremendous growths of computer and communication systems lead to the development of the new generation of advanced cryptosystems. In general, "PKC" likewise named asymmetric system makes use for two different keys such as public key and private keys for exchange procedure. The public keys are

[1]*corresponding author*

2010 *Mathematics Subject Classification.* 68M12, 49M27, 16Y30.

Key words and phrases. Public key crypto system, Conjugacy Search Problem, Near-ring, Discrete Logarithmic Problem (DLP).

distributed athwart scheme persons reserved confidential. The facts translated by the "PKC" technique canister remain decrypted using the appropriate private key. In general, the data to be shared across a channel is translated by a public key and a receiver decrypts the translated files through the use of their private key. Thus, through a procedure of the public key encryption process, only the authorized users could be able to decrypt the data [1, 2]. In comparison to "PKC" encryption systems is needs higher computation such that this method is difficult to be applied across the large volume of the data [3]. Conventional technique of "PKC" systems includes Diffie-Hellman, Elliptic curve cryptography (ECC) and RSA cryptosystems. In the year 1976 Diffie and Hellman first hosted the perception of "PKC" across the internet systems [1]. It stands a secure way on exchange keys across the open network. It enables two unknown entities to secretly exchange data across the public network. Such, that the secret is given in the form $A = g^a mod p$. Thus, tranquil for the attacker to calculate g, p and hard to find g^a. Even though Diffie-Hellman is a non-authenticated key treaty procedure it's basis of development of several other authenticates public key cryptosystem protocols. Further, it preserves the property of forward security [4,5,6].

Followed by Diffie-Hellman approach the next evolved "PKC" stands the "RSA" process [7]. RSA is an asymmetric cryptographic system. The term asymmetric represent that the algorithm can work in two different ways such as using a public and private key. In general, the "public key" covers binary facts someplace unique is the multiplicative result of binary huge primary facts and other is the private key derived from the equivalent dual primary facts. Thus, if someone is able to find the factorization of two large prime numbers they can easily compromise the private key of the user. Hence, the increase in the size of the secret key increases the security of the system. The key concept behind RSA cryptosystems is that it is hard to factorize a huge numeral integer. Thus increasing the key dimension to double or triple size increases the security of the system. In general, RSA key size can be a maximum length of 1024 or 2048 bits [8, 9].

Elliptic curve cryptography (ECC) and "PKC" all arranged the beginning of algebraic structures over the finite fields [10]. ECC system requires only smaller cryptographic keys and provides a comparatively equivalent level of security features to the non-ECC systems. ECC model is widely used across various domains such as digital signatures, key agreement, pseudorandom generators, etc. [11].

The two major drawbacks in existing public key cryptosystems are the establishment of a secure communication channel and key management processes. Further, asymmetric cryptographic systems are highly expensive and require more computation resources for implementation. An encryption scheme with public key cryptosystem has to fulfill several requirements. Among them, a secure and privacy-preserving key exchange process play a predominant role. Thus, trendy these effort, we existing a secure and enhanced "PKC" by near-ring. The suggested method is extremely vulnerable and provides an efficient solution to double conjugacy problem over near-ring. Further, it prevents chosen ciphertext attack and brute force attack across public key encryption techniques.

2. PRELIMINARIES

Conjugacy Search Problem (CSP)

Instance: $(r, s) \in N^2$ such that $\varphi = rsr^{-1}$for some $\varphi \in N$.
Objective: Find $\varphi_1 \in N$ such that $\psi = \varphi_1 s \varphi_1^{-1}$.
Discrete Logarithmic Problem (DLP)
Instance: Assumed a prime q a generator a of $Z_*^q$and an element $r \in Z_q^*$ where Z_*^q is a cyclic group.
Objective: Discovery an integer $0 \leq r \leq q-1$ such that$r^a = n(modp)$.
Double Conjugacy Search Problem (DCSP)
Instance: Assumed $r, s \in N$ and $c \in Z_q^*$.
Objective: Find $1 \leq r \leq q-1$and$2 \leq s \leq q-1$ such that $\varphi = c^r d^s a^{-r} \,(mod\, q)$

3. NEAR-RING PUBLIC KEY ENCRYPTION SCHEME

Key generation: The persons Alice and Bob randomly select the public parameters $d \in R$ and $c \in Z_q^*$ from a Blum prime of the arrangement$q = 7k + 1$. Alice arbitrarily selects the private key $r, s \in Z$ such that $1 \leq r \leq q-1$ and $2 \leq s \leq q-1$then calculate $\varphi = c^r d^s c^{-r} \,(mod\, q)$and distributes her public key (φ, d, c, q).

Encryption: Given a message $m \in N$ and Alice's public key (φ, d, c, q) Bob chooses randomly $w, k \in Z$ such that $1 \leq w \leq q-1$ and$2 \leq k \leq q-1$ then calculates $C_1 = c^w d^k c^{-w} \,(mod\, q)$, $C_2 = m.c^w \varphi^s c^{-w} \,(mod\, q)$ and to finish harvests the ciphertext (C_1, C_2).

Decryption: On received of the ciphertext(C_1, C_2)Alice performs the decryption of ciphertext by her private key:

$$\left[C_2 \left(c^r C_1^s c^{-r}\right)^{-1}\right] (mod\, q) = m.$$

Correctness: Correctness of the scheme is verified as follows

$$\begin{aligned}
&\left[C_2 \left(c^r C_1^k a^{-r}\right)^{-1}\right] (mod\, q)\\
&\left[m.c^w \varphi^k c^{-w} \left(c^r C_1^s c^{-r}\right)^{-1}\right] (mod\, q)\\
&\left[m. \left(c^w \varphi^k c^{-w}\right) \left(c^r (c^w d^k c^{-w})^s c^{-r}\right)^{-1}\right] (mod\, q)\ \cdot\\
&\left[m. \left(c^w \varphi^k c^{-w}\right) \left(c^w (c^r d^s c^{-r})^k c^{-w}\right)^{-1}\right] (mod\, q)\\
&= m
\end{aligned}$$

Toy Example for Proposed Public Key Cryptosystem: The proposed method is briefly demonstrated with a matrix $M_2\left(Z_n\right)$, where n to be a huge sheltered prime.

Initial setup: Let take

$$c = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, d = \begin{bmatrix} 1 & 5 \\ 0 & 1 \end{bmatrix} \in M_2(Z_n)$$

Key generation: The entity Alice arbitrarily picks dual usual numbers $r = 3, s = 5$ r and s denote the private key of Alice.

$$\begin{aligned}
\varphi &= c^r d^s c^{-r} (mod\, q)\\
&= \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}^3 \begin{bmatrix} 1 & 5 \\ 0 & 1 \end{bmatrix}^5 \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}^{-3}\\
&= \begin{bmatrix} 1 & 6 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 20 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -6 \\ 0 & 1 \end{bmatrix} mod 23\\
&= \begin{bmatrix} 1 & 20 \\ 0 & 1 \end{bmatrix}
\end{aligned}$$

and declare(y, z, a, q).

Encryption: To transfer a message $m = \begin{bmatrix} 1 & 4 \\ 0 & 1 \end{bmatrix} \in M_2(Z_n)$ toward Alice, Bob picks $w = 2$ and $k = 3$. He formerly arrangements Let

$$\begin{aligned} C_1 &= c^w d^s c^{-w} mod 23 \\ &= \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}^2 \begin{bmatrix} 1 & 5 \\ 0 & 1 \end{bmatrix}^3 \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}^{-4} mod 23 \\ &= \begin{bmatrix} 1 & 10 \\ 0 & 1 \end{bmatrix} \end{aligned}$$

$$\begin{aligned} C_2 &= m.c^w \varphi^s c^{-w} mod 23 \\ C_1 &= \begin{bmatrix} 1 & 4 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}^2 \begin{bmatrix} 1 & 20 \\ 0 & 1 \end{bmatrix}^3 \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}^{-2} mod 23 \\ &= \begin{bmatrix} 1 & 10 \\ 0 & 1 \end{bmatrix} \end{aligned}$$

Decryption: Once received of the ciphertext(C_1, C_2) is received Alice decrypts ciphertext using her private key .

$$\begin{aligned} &\left[C_2 \left(c^r C_1^k a^{-r}\right)^{-1}\right] mod 23 \\ &= \left[\begin{bmatrix} 1 & 10 \\ 0 & 1 \end{bmatrix} \left[\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}^3 \begin{bmatrix} 1 & 10 \\ 0 & 1 \end{bmatrix}^5 \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}^{-3}\right]^{-1}\right] mod 23 \\ &= \begin{bmatrix} 1 & 23 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -21 \\ 0 & 1 \end{bmatrix} mod\, 23 \\ &= \begin{bmatrix} 1 & 4 \\ 0 & 1 \end{bmatrix} \\ &= m \end{aligned}$$

4. Security Analysis

Chosen ciphertext attack: In the proposed approach, the value of decrypting the ciphertexts $C_1 = c^w d^k c^{-w} \,(mod\, q)$ into the plain text m is comparable toward perceptive $\left[m.\left(c^w d^k c^{-w}\right)\left(c^w (c^r d^s c^{-r})^s c^{-w}\right)^{-1}\right] (mod\, q)$. The adversary randomly select a message $\overline{m} \in N$ and calculates $\overline{m} C_2$ formerly forwards it toward Alice

aimed at decryption process. Formerly, Alice calculates $\overline{m}C_2\left(c^rC_1^sc^{-r}\right)^{-1}$. Such that, the opponent can recuperate the message m uncertainty he acquires $\overline{m}m$.

Brute force attack: An enemy who knows public parameters such as public key $\varphi = c^rd^sc^{-r}$ makes an attempt to find the key values in Z_*^q. In such case, if the refuge restrictions are larger than double near-ring conjugacy then it is difficult to disruption the near-ring. Trendy order to break the secret key using "Brute force attacks" $r, s \in Z$ it requires 2^{320} attempts.

Key recovers attacks: The proposal, the public key is defined as $\varphi = c^rd^sc^{-r}$. If the opponent knows $s \in Z$ he can try to recover a conjugator Z_*^p. If we select a suitably huge leading p over Z_*^q it is comparable to decipher "CSP" aboveZ_*^q. The other probable scenario if the opponent distinguishes$s \in Z$ formerly he can resolve DLP overZ_*^q.

5. CONCLUSION

The proposed approach presents a secure and efficient technique of PKC by near-ring. It works on the basis of double conjugacy problem. From the analysis it is observed that the active implementation of non-commutative near-ring in proposed approach enables secure key exchange and management process. Thus, the suggested method is extremely efficient and it is cryptographically hard to break. The refuge analysis of this approach is established on double conjugacy over near-ring. The recital of the PKC scheme needs around $O\left(k^3p^3\right)$ bit processes to key generation, encryption and decryption.

REFERENCES

[1] T. ELGAMAL: *A public key cryptosystem and a signature scheme based on discrete logarithms*, IEEE transactions on information theory, **31**(4) (1985), 469-472.

[2] R. J. MCELIECE: *A public-key cryptosystem based on algebraic*, Coding Thv, (1978), 114–116.

[3] V. MUTHUKUMARAN, D. EZHILMARAN, I. MUCHTADI-ALAMSYAH, R. UDHAYAKUMAR, A. MANICKAM: *New public key cryptosystem based on combination of NREP and CSP in non-commutative near-ring*, Journal of Xi'an University of Architecture and Technology, **12**(3) (2020), 4534–4539.

[4] S. KRISHNAMOORTHY, V. MUTHUKUMARAN, J. YU, B. BALAMURUGAN: *A Secure Privacy Preserving Proxy re-encryption Scheme for IoT Security using Near-ring*, In Proceedings

of the 2019 the International Conference on Pattern Recognition and Artificial Intelligence, ACM, (2019), 27–32.

[5] V. MUTHUKUMARAN, D. EZHILMARAN: *Authenticated Group Key Agreement Protocol Based on Twisted Conjugacy Root Extraction Problem in Near-Ring*, Journal of Computational and Theoretical Nanoscienc., **15**(6-7) (2018), 2023–2026.

[6] D. BONEH: *Authenticated Twenty years of attacks on the RSA cryptosystem*, Notices of the AMS, **46**(2) (1999), 203–213.

[7] D. N. MOLDOVYAN: *Non-commutative finite groups as primitive of public key cryptosystems*, Quasigroups and Related Systems, **18** (2010), 165–176.

[8] V. MUTHUKUMARAN, D. EZHILMARAN, G. S. G. N. ANJANEYULU: *Efficient Authentication Scheme Based on the Twisted Near-Ring Root Extraction Problem*, Advances in Algebra and Analysis, **5** (2018), 37–42.

[9] D. EZHILMARAN, V. MUTHUKUMARAN: *Key Exchange Protocol Using Decomposition Problem In Near-Ring*, Advances in Algebra and Analysis, **29**(1) (2016), 123–127.

[10] D. EZHILMARAN, V. MUTHUKUMARAN: *Authenticated group key agreement protocol based on twist conjugacy problem in near-rings*, Wuhan University Journal of Natural Sciences, **22**(6) (2017), 472–476.

[11] V. MUTHUKUMARAN, D. EZHILMARAN: *Efficient authentication scheme based on near-ring root extraction problem*, Materials Science and Engineering Conference Series, **15** (2017), 042137.

DEPARTMENT OF MATHEMATICS
SREE ABIRAAMI ARTS AND SCIENCE COLLEGE FOR WOMEN, INDIA
Email address: muthu.v2404@gmail.com

COLLEGE OF COMPUTER SCIENCE AND SOFTWARE ENGINEER
SHENZHEN UNIVERSITY, CHINA
Email address: adhimsc2013@gmail.com

DEPARTMENT OF MATEMATICS
VELLORE INSTITUTE OF TECHNOLOGY, INDIA
Email address: ezhil.devarasan@yahoo.com