A secure public key cryptosystem based medical records using non-commutative group

A Ramamoorthy and P Jayagowri

Department of mathematics, Sudharsan College of Arts and Science, Pudukkottai, Tamilnadu, India – 622 104.
E-mail: *gowrimullaimani@gmail.com

Abstract. Tolerant records, including specialists' conclusions of illnesses, hint of medicines and patients' conditions, nursing activities, and assessment results from united wellbeing calling offices, are the main clinical records of patients in clinical frameworks. With understanding records, clinical staff can comprehend the whole clinical data of a patient so that, as indicated by the patient's conditions, more exact analyses and more fitting top to bottom medicines can be given. By and by, in such a cutting-edge society with blasting data advances, customary paper-based understanding records have confronted a great deal of issues, for example, absence of uniform organizations, low information versatility, slow information move, indecipherable penmanship styles, tremendous and inadequate capacity space, trouble of preservation, being handily harmed, and low adaptability. In this article we propose new public key cryptosystem for securing medical record based on non-commutative group. The securities of our key exchange protocol based on hybrid of group root extraction problem and Conjugacy Search Problem in non-commutative group implement our key exchange protocol in special matrix group.

1. Introduction

Today individuals are utilized to get to a wide scope of information and applications utilizing public versatile correspondence organizations. In such omnipresent correspondence conditions, it's anything but an unexpected that there is a developing need to empower the versatile crisis clinical groups to have a persistent and secure admittance to quiet clinical records. The additional advantage of continuous admittance to patients' clinical records while giving portable crisis care is self-evident and has been featured in various ongoing distributions [4 & 5]. Synopsis Care Records by NHS England and Emergency Care Summary by NHS Scotland empower clinicians in emergency clinics mishap and crisis offices to access, with quiet assent, significant clinical data on recommended prescriptions and hypersensitivities 24 hours per day [1 & 2].

The patient clinical records are put away at the patient's clinical focus and the versatile crisis unit which is at the crisis spot has no admittance to the patient's clinical record. Consequently, the crisis unit is an obscure and un-confided in element for the clinical focus to share delicate data. Building up trust exchange on touchy patient clinical records between two substances for a brief timeframe (during the crisis care) is a long way from basic. The primary test is the need to safeguard the protection of the individual clinical data while giving a straightforward and snappy technique for secure admittance to the clinical information, which won't defer the conveyance of crisis care. The crisis clinical group must be confirmed and trusted by the supplier of the individual clinical records before the information download is approved. During the download, the information must be encoded to shield it from likely
assaults. When the information is utilized during the crisis care it ought to be wrecked to forestall against any future information dissemination and abuse.

This paper gives a novel security system that can be utilized to trade clinical information in a crisis situation. This is accomplished via cautious conveyance of trust between the central participants all the while: (a) the clinical information supplier putting away the clinical records and (b) the cell phone at the crisis clinical unit. Trust must be arranged and assigned between these players to feel sure to trade information. In the interim, this paper presents a Trust Granting Server (TGS) which builds up the association between the two obscure gatherings.

With the headway of web innovations, valuable commitment of innovation in medical care administrations is additionally expanded, despite the fact that it likewise brings a few difficulties. The greater part of the current medical care frameworks are wellbeing suppliers driven and have low interoperability. All things considered, situation, patients don't restrict themselves to one emergency clinic or specialist. They may visit various centres or specialists for clinical perception and treatment, or they might be alluded starting with one clinic then onto the next, and in such circumstances sharing patient's clinical information for better treatment is obligatory.

EMRs of one clinical organization are not generally accessible to another clinical establishment. These issues of care coordination are notable in medical care and should be tended to. Likewise, in these frameworks patients have no control of their clinical records. There clinical records might be tempered taken or imparted to others without their assent. Along these lines, basic security and protection issues likewise emerges. Improving the security, protection, the executives and proficient sharing of clinical records is the principle focal point of our work depicted in this article Figure.1.

![Figure 1. Authentication Scheme for medical record](image)

In 1976 Diffie and Hellman introduced the concept of Public Key Cryptography (PKC), using a trapdoor one-way function, many PKC’s have been proposed and broken [1]. Currently most outstanding PKC schemes are based on the recognized challenging of convinced problem in special large finite commutative rings. For example, (R.L. Rivest et al 1978) solving the integer factoring problem defined over the ring $\mathbb{Z}_n$ forms the ground of the basic RSA cryptosystem [6, 7, 8]. In 1993 Iris Lee Anshel and Michael Anshel proposed PKC’s based on word problem in group theory. In 2000 Ko et al described a new public key cryptosystem established on braid groups [9, 10, and 11]. In 2016 Ezhilmaran and Muthukumaran proposed new PKC system established on decomposition problem in non-abelian near-ring and implement his scheme in centralizer of near-ring. In 2007 Kao et al introduced new PKC system based on non-commutative ring [12]. In 2006 Vladimir Shpilrain and Gabriel Zapata describe the subgroup membership search problem in PKC system [13,17,18]. In 2017 Ezhilmaran and Muthukumaran introduce PKC system based on triple decomposition problem in non-commutative near-ring [14, 15, and 16]. In this article we proposed new public key cryptosystem-based combination of CSP and NREP in non-commutative near-ring.
The rest of the manuscript organized as follows. In Section 2 we recall some basic definition of cryptography assumption over non-commutative group. In Section 3 we construct new Public key cryptosystem for securing medical records protocol based on combination of root extraction problem and conjugacy problem in non-commutative group. In section 4 we implement protocol in matrix group and security issues are also discussed, and in section 5 we conclude the paper.

2. Proposed Public Key Cryptosystem for Medical Records

Key exchange
A casually chooses two real number \( h \geq 2 \) and \( g \geq 2 \). The pair \((h, g)\) PK \( S_A \) of A.

Next A ways

\[
L_A = (j_1)^h(j_2)^g
\]

and announces her PK \( M_A = (j_1, j_2, L_A) \).

Encoding
Toward deliver a letter \( m \in N \) to A, B chooses casually \( d \geq 2 \) and \( f \geq 2 \). Then he calculates \((j_1)^d, (j_2)^f\) after that performs subsequent stages.

i. \( t = (j_1)^h(j_2)^g \)

ii. \( C_1 = K_A^u \)

iii. \( C_2 = K_A^{u^{-1}} \)

iv. \( B = C_1 \cdot m \cdot C_2 \)

v. \( B' = (a_1)^uK_A(a_2)^v \)

They send \((B, B')\).

Decryption
A gets the ciphertext

i. \( E = ((j_1)^h)^{-1}B'(j_1)^{-1} \)

ii. \( E_1 = (L_A^{-1})^E \)

iii. \( E_2 = (L_A^{-1})^E^{-1} \)

iv. \( T = E_1 \cdot m \cdot E_2 \)

2.1 Example for Proposed Public Key Cryptosystem

Initial setup: Let

\[
j_1 = \begin{pmatrix} 1 & 8 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad j_2 = \begin{pmatrix} 1 & 7 \\ 0 & 1 \end{pmatrix}
\]

Key Exchange:
A casually chooses two pure number \( h = 2, g = 3 \).

\( r \) and \( s \) are private keys of Alice. She then forms

\[
L_A = (j_1)^r(j_2)^s
\]

\[
= (a_1)^3(a_2)^3 \mod 23
\]

\[
= (1 \ 8)(1 \ 7)^4 \mod 23
\]

\[
= (1 \ 8) \mod 23
\]
and says $M_A = (J_1, J_2, L_A)$.

**Encoding:**

Toward transmit a message $m = \begin{pmatrix} 1 & 21 \\ 0 & 1 \end{pmatrix}$ to A and B selects $d = 3$ and $f = 2$.

He then forms

1) $t = (j_1)^d(j_2)^f = (j_1)^3(j)^2 \mod 23$

$$= \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \mod 23$$

(11)

2) $C_1 = K_A^a = (a^{-1}K_A a) \mod 23$

$C_1 = \begin{pmatrix} 1 & 8 \\ 0 & 1 \end{pmatrix} \mod 23$

(12)

3) $C_2 = K_A^{a^{-1}} = (aK_A a^{-1}) \mod 23$

$C_2 = \begin{pmatrix} 1 & 8 \\ 0 & 1 \end{pmatrix} \mod 23$

(13)

4) $R = C_1 m C_2 \mod 23$

$$= \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix} \mod 23$$

(14)

5) $R = (a_i)^r K_A (a_j)^r \mod 23$

$$= \begin{pmatrix} 1 & 11 \\ 0 & 1 \end{pmatrix} \mod 23$$

(15)

The Ciphertext

1) $E = E = \left( (j_1)^h \right)^{-1} B' \left( (j_1)^g \right)^{-1}$

$$= \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \mod 23$$

2) $E_1 = (K_A^{a^{-1}})^E = E^{-1} M_A^{-1} E \mod 23$

$$= \begin{pmatrix} 1 & 8 \\ 0 & 1 \end{pmatrix} \mod 23$$

3) $E_2 = (K_A^{a^{-1}})^{E^{-1}} = E M_A^{-1} E^{-1} \mod 23$

$$= \begin{pmatrix} 1 & 9 \\ 0 & 1 \end{pmatrix} \mod 23$$

4) $m = \begin{pmatrix} 1 & 21 \\ 0 & 1 \end{pmatrix}$

(16)

3. Security analysis

In this section we discuss some good feature for our proposed cryptosystem.
Matrix conjugation attack
The matrices $E_1$ and $E_2$ associated with encryption are the lattice formation of the framework by the private grid. The significant issue of networks is the conjugacy search issue. For directing framework formation assaults, an enemy need to track down the obscure grids.

Ciphertext attack
Assume a foe knows just the ciphertext $(E', E)$ as given in articulations (15) and (14), individually. In (3.14) the obscure frameworks are included. To realize a foe needs to discover the arrangement of

$$aC_1 = K_a a, C_2 a = aK_a,$$  \hspace{1cm} (16)

where the lattice is obscure. For the hidden construction lattice gathering, framework (16) will prompt huge arrangement of condition for the decision of adequately large. Likewise, the NREP of networks and is engaged with the articulation (15) of $E'$. Because of all these explanations, this kind of assault.

Plaintext attack
Let be the ciphertext relating to the plaintext known to the enemy. From this data, he needs to track down the following plaintext from the comparing ciphertext In our circumstance, this sort of assault can be made infeasible by utilizing various examples in the encryption of each new message. So, the information on past plaintext-ciphertext sets gives no sufficient data to track down the following plaintext.

Latency is a key issue with these systems, so we combined category based and user-based approaches for that with clustering offline giving scalability. The information about MAE and Precision were there in. Also, information about contextual precision and its effect on recommenders was valuable. Also, the future scope for analysis expression and signal analysis.

4. Conclusion
Paper-based patient records have for a long while been used with weights of wasting tremendous space, being viably hurt or then again lost, not being conveniently kept, not having the choice to recuperated by a couple of experts for joined treatment, a great deal of the board cost, not adequately recuperating patient records, successfully deferring medications, conveying inconvenience of patient record information, inconvenience in gathering of patient records, and countless patient records. With the progression of the time, paper-based patient records and traditional clinical exercises have been changed into mechanized constructions to impel the clinical efficiency and information instantaneousness. In this article we portrayed an entirely unexpected strategy for planning PKC dependent on broad non-commutative gathering. The security parts of our proposed plot dependent on half breed of GREP and CSP. We give the toy model for conspire. The potential assaults are likewise examined.

References
[1] Diffie W and Hellman M 1976 IEEE transactions on Information Theory 22(6) pp 644-654.
[2] Rivest R L, Shamir A and Adleman, L 1978 A method for obtaining digital signatures and public-key cryptosystems Communications of the ACM 21(2) pp 120-6.
[3] Anshel I L and Anshel M 1993 The American Mathematical Monthly 100(9) pp 835-44.
[4] Ko K H, Lee S J, Cheon J H, Han J W, Kang J S and Park C 2000 In Annual International Cryptology Conference. 166-183.
[5] Krishnamoorthy S, Muthukumaran V, Yu J, Balamurugan B 2019 In Proceedings of the 2019 the International Conference on Pattern Recognition and Artificial Intelligence, ACM. pp 27–32.
[6] Manikandan G, Perumal R and Muthukumaran V 2020 AIP Conference Proceedings 2277.
[7] Manikandan G, Perumal R and Muthukumaran V 2021 *Journal of Computational and Theoretical Nanoscience*. 18(2) pp 516–21.
[8] Muthukumaran V, Ezhilmaran D, Anjaneyulu G S G N 2018 *Advances in Algebra and Analysis* pp 37–42.
[9] Ezhilmaran D and Muthukumaran V 2016 *Gazi University Journal of Science*. 29(1).
[10] Ezhilmaran D and Muthukumaran V 2017 *Wuhan University Journal of Natural Sciences*. 22(6) pp 472–76.
[11] Muthukumaran V and Ezhilmaran D 2017 *Materials Science and Engineering Conference Series* 042137.
[12] Muthukumaran V, Ezhilmaran D, Muchtadi-Alamsyah I and Udhayakumar R 2020 *Journal of Xi’an University of Architecture and Technology*. 12(3) pp 4534–39.
[13] Muthukumaran V and Ezhilmaran D 2020 *International Journal of Information Technology and Web Engineering (IJITWE)*. 15(4) pp 18-36.
[14] Ganesh Gopal Deverajan, Muthukumaran V, Ching-Hsien Hsu, Marimuthu Karuppihah, Yeh-Ching Chung and Ying-Huei Chen 2021 *Transactions on Emerging Telecommunications Technologies*.
[15] Muthukumarn V, Adhiyaman M and Ezhilmaran D 2020 *Advances in Mathematics: Scientific Journal* pp 1389–95.
[16] Muthukumaran V and Ezhilmaran D 2018 *Journal of Science and Arts*. 18(2) pp 375-80.
[17] Ezhilmaran D and Muthukumaran V 2014 *Int. J. pure and applied mathematics*. 16(6) pp 426-36.
[18] Muthukumaran V and Ezhilmaran D 2017 *International Journal of Pure and Applied Mathematics*. 117(14) pp 247-52.