IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Mathematical Modelling of Engineering Problems
Vol. 10, No. 5, October, 2023, pp. 1824-1832
Journal homepage: http://iieta.org/journals/mmep

A Novel Secure Session Key Agreement Protocol Based on Multivariate Polynomials

Sravani Jayanti, Chittibabu Kandikatla, Pragathi Chaganti, Chandra Sekhar Akkapeddi*

Department of Mathematics, Gandhi Institute of Technology and Management, Visakhapatnam 530045, India

Corresponding Author Email: cakkaped@gitam.edu

https://doi.org/10.18280/mmep.100535

Received: 13 May 2023
Revised: 7 August 2023
Accepted: 24 August 2023
Available online: 27 October 2023

Keywords:
telemedicine, multivariate polynomials, affine cipher, key agreement protocols, session key

ABSTRACT

Cryptology, a crucial discipline for safeguarding sensitive information against unauthorized access, underpins the Session Key Agreement Protocol (SKAP), which facilitates authorized access. SKAP generates unique cryptographic session keys for each session, allowing authorized users to access, share, and modify encrypted data. The current research landscape is dominated by the development of Key Agreement Protocols (KAPs) and key exchange mechanisms that are robust against known attacks and provide security to the cryptographic key. These novel KAPs leverage complex mathematical algorithms for enhanced security. This article introduces an innovative SKAP that employs Affine Transformation over Multivariate polynomials. The non-commutative and invertible nature of Affine Transformation forms the cornerstone of this protocol. The use of Multivariate polynomials augments the quantity of potential private keys, thereby amplifying security. The proposed protocol's security features are thoroughly analyzed and compared with existing key exchange mechanisms and SKAPs. Moreover, the paper encapsulates the application of the proposed SKAP in the realm of Telemedicine. This approach demonstrates the real-world implications and practical utility of this advanced SKAP.

1. INTRODUCTION

The designing of cryptosystems mainly focuses on enhancing the confidentiality of data. This is accomplished by designing complex algorithms to perform encryption. The cipher text obtained through these computations is sent to the authorized recipient to retrieve the information. Consequently, the sender and the recipient agree on a mutual key communicated over a secure channel to access, encrypt and decrypt the data. Various key exchange mechanisms are developed using mathematical concepts to safeguard the cryptographic key [1].

The sole responsibility of protecting data is on the key used to unlock the vault. In most of the developed algorithms, some information is displayed publicly while some are hidden, which in terms of cryptography, is the public and the private key. Key exchange protocols allow the users to securely share a key to access the stored information. The infeasibility to retrieve the key using the available public data makes a key exchange or agreement protocol secure. This is mainly focused on designing the key exchange mechanisms and cryptosystems.

The cryptographic key either needs to be remembered or preserved in a password vault for accessing the information in future. The strength and security of the key is compromised when an intruder tries to unlock the vault or the key is forgotten, or the memory occupancy of the key is large. To eradicate the pertaining threat, session keys are introduced. A session key unlocks the vault and provides user access only for a single session. The key is rejuvenated when the session expires. SKAPs are developed over time to generate the session keys applying mathematical and cryptographic algorithms.

In the Key exchange protocols [2-5] and Key generation mechanisms [6], multivariate polynomials, Diophantine equations, Diffie-Hellman, RSA and ElGAmal algorithms are incorporated to establish a new competent protocol. Diophantine equations in multiple variables are applied to develop secure cryptosystems [7].

KAPs are the major cryptographic primitives for establishing secure communication channels over public networks. Several real time applications like e-voting, e-commerce, Telemedicine rely on SKAPs and block chain technologies.

Some of the designed protocols are reviewed. A KAP over Sylvester Hadamard matrices is proposed in the study [8] whose security drawbacks are overcome in the study [9]. A trusted third party is involved in studies [8, 9] to develop the KAP. In the study [10], SKAP and an authentication scheme are developed applying ECC applicable in Telemedicine.

This paper proposes a SKAP inspired by studies [11-13]. The protocols developed in studies [11-13] are discussed in detail.

In the study [11], a key exchange mechanism over the Diophantine equation over n variables is proposed by Yosh. The basic idea behind the developed method in the study [11] is:

- Suppose that a key is to be exchanged between two parties, say A and B. Initially, B selects a solution set $\{\alpha_i\}_{i=1,2,\dots n}$ randomly and forms a Diophantine equation.

$$f(x_1, x_2, \dots, x_n) = 0 \ni f(\alpha_1, \alpha_2, \dots, \alpha_n) = 0 \quad (1)$$

- $f(x_1, x_2, \dots, x_n)$ is the public key and the solution set

$\{\alpha_i\}_{i=1,2,\dots n}$ is the private key.

- A defines an invertible linear transformation $T_{[a,b,c]}$ over the quotient ring $Z[x_1, x_2, \dots, x_n]/(f(x_1, x_2, \dots, x_n))$.
- A chooses an element $l(x_1, x_2, \dots, x_n) \in Z[x_1, x_2, \dots, x_n]/(f(x_1, x_2, \dots, x_n))$ and computes $T_{[a_1, b_1, c_1]}\, T_{[a_2, b_2, c_2]} \dots T_{[a_m, b_m, c_m]}(l(x_1, x_2, \dots, x_n)) = h(x_1, x_2, \dots, x_n)$.
- Since $h(x_1, x_2, \dots, x_n) \in Z[x_1, x_2, \dots, x_n]/(f(x_1, x_2, \dots, x_n))$ and can be represented in different ways, therefore any one of the representations of $h(x_1, x_2, \dots, x_n)$, $(k(x_1, x_2, \dots, x_n))$ is made public along with $l(x_1, x_2, \dots, x_n)$.
- B computes $l(\alpha_1, \alpha_2, \dots, \alpha_n)$, $k(\alpha_1, \alpha_2, \dots, \alpha_n)$ and returns $k(\alpha_1, \alpha_2, \dots, \alpha_n)$ to A.
- A computes $l(\alpha_1, \alpha_2, \dots, \alpha_n)$ by applying inverse transformation on $k(\alpha_1, \alpha_2, \dots, \alpha_n)$: $T_{[a_m, b_m, c_m]}^{-1}\, T_{[a_{m-1}, b_{m-1}, c_{m-1}]}^{-1} \dots T_{[a_1, b_1, c_1]}^{-1}(k(\alpha_1, \alpha_2, \dots, \alpha_n)) = l(\alpha_1, \alpha_2, \dots, \alpha_n)$.
- Thus, A and B share the key: $l(\alpha_1, \alpha_2, \dots, \alpha_n)$.

From the publicly available information in the above protocol, the attacker is left with two equations:

$$F(\alpha_1, \alpha_2, \dots, \alpha_n) = 0 \text{ and } k(x_1, x_2, \dots, x_n) = k(\alpha_1, \alpha_2, \dots, \alpha_n) \quad (2)$$

The insolvability of the above set of Diophantine equations of higher order is the basis for the security of the protocol. However, this protocol is safe for n>2. In the study [12], an analysis of the protocol developed in the study [11] is carried out, which states that the protocol with the same polynomial can be used at most (n-3) times.

In the study [13], a key exchange protocol is designed over Diophantine equations over n variables, which is secure for n>1. The basic idea behind the methodological approach for exchanging key in the study [13] is:

- Suppose that the key is to be exchanged between two parties say A and B.
- A selects a random Diophantine equation $f(x_1, x_2, \dots, x_n)$ and defines an invertible operator $T_{[a,b]}$ on the Diophantine equation.
- A computes $T_{[a_1, b_1]}\, T_{[a_2, b_2]} \dots T_{[a_m, b_m]}(f(x_1, x_2, \dots, x_n)) = h(x_1, x_2, \dots, x_n)$ and publicly displays $f(x_1, x_2, \dots, x_n)$ and $h(x_1, x_2, \dots, x_n)$.
- B selects a solvable Diophantine equation $g(x_1, x_2, \dots, x_n)$ and a random solution $\{\alpha_i\}_{i=1,2,\dots n}$ of g=0.
- B computes $f(\alpha_1, \alpha_2, \dots, \alpha_n)$, $h(\alpha_1, \alpha_2, \dots, \alpha_n)$ and sends $h(\alpha_1, \alpha_2, \dots, \alpha_n)$ to A keeping $f(\alpha_1, \alpha_2, \dots, \alpha_n)$ secret.
- A computes $T_{[a_m, b_m]}^{-1}\, T_{[a_{m-1}, b_{m-1}]}^{-1} \dots T_{[a_1, b_1]}^{-1}(h(\alpha_1, \alpha_2, \dots, \alpha_n)) = f(\alpha_1, \alpha_2, \dots, \alpha_n)$.
- Thus, both parties exchange the key $f(\alpha_1, \alpha_2, \dots, \alpha_n)$.

This key exchange protocol is secure for n>1 since the publicly available information, cannot be solved to deduce $\{\alpha_i\}_{i=1,2,\dots n}$ to reach the key $f(\alpha_1, \alpha_2, \dots, \alpha_n)$ whenever n>1. This protocol can be used with the same Diophantine equation and the solution set for ut most (n-2) times.

$$h(x_1, x_2, \dots, x_n) = h(\alpha_1, \alpha_2, \dots, \alpha_n) \quad (3)$$

This paper proposes a SKAP inspired by studies [11, 13]. Our methodological approach applies the mathematical concepts of Affine cipher [14, 15] and multivariate polynomials to establish the protocol.

1.1 Affine cipher

An affine cipher is a combination of a multiplicative cipher and an additive cipher. In an Affine Cipher, over a congruence modulo n, for the values of $a, b \ni \gcd(a, n) = 1$, $a, b < n$, plaintext (P) is encrypted as Cipher text:

$$C = (a * P + b) \bmod n \quad (4)$$

and the Cipher text (C) is decrypted to Plain text:

$$P = (C - b) * a^{-1} \bmod n \text{ where } a * a^{-1} \equiv 1 \pmod n \quad (5)$$

Here, for different choices of a, b, various cipher texts are obtained for the same plain text character. The maximum possible combinations for a, b is $n * \varphi(n)$.

1.2 Multivariate polynomial

A polynomial in multiple variables is a multivariate polynomial. For example: $x_1 + 3x_2^2 + 10x_3^3$ is a polynomial in 3 variables and is a multivariate polynomial.

2. PROPOSED SESSION KEY AGREEMENT PROTOCOL

The SKAP proposed is demonstrated using the following parameters.

S=Set of multivariate polynomials in n variables

Let:

- $f, g \in S$,
- $\alpha = \{\alpha_i\}_{i=1,2,\dots,n}$, $\beta = \{\beta_i\}_{i=1,2,\dots,n}$, *where* $\alpha_i s, \beta_i s \in \mathbb{N}$,
- $[a, b] = [a_i, b_i]_{i=1,2,\dots,n}$, $[c, d] = [c_i, d_i]_{i=1,2,\dots,n}$, *where* $a_i s, b_i s, c_i s, d_i s \in \mathbb{N}$.

Define a non-commutative linear operator T on S where the inverse of T is T^{-1}.

Let:

- $h = T_{[a,b]}(f)$, $l = T_{[c,d]}(g)$,
- $u = l(\alpha)$, $v = h(\beta)$,
- $f(\beta) = T_{[a,b]}^{-1}(v)$, $g(\alpha) = T_{[c,d]}^{-1}(u)$.

The final key value, $K = f(\beta) * g(\alpha)$.

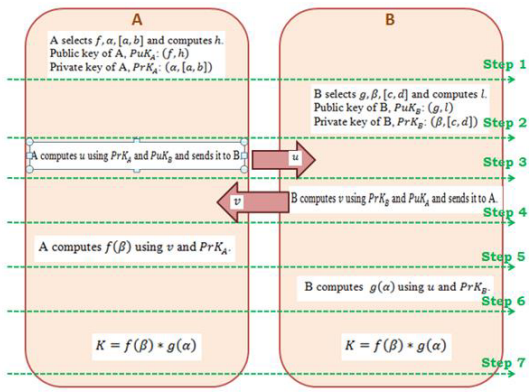


Figure 1. Methodology of SKAP proposed

The methodological approach adopted to agree on a key K by two communicating parties A and B is depicted in the Figure 1.

The methodological approach to agree on a session key demonstrated above is cryptographically implemented applying modulo congruence and an Affine operator over multivariate polynomials. The multivariate polynomials involved are polynomials in n variables over the ring of polynomials $Z[x_1, x_2, \dots, x_n]$. The Affine operator involved in the process of key exchange is:

For a multivariate polynomial function 'f' define.

$$T_{\{a,b\}}(f) = (a * f + b) \bmod p \text{ where } \gcd(a, p) = 1, b < p \quad (6)$$

$$T_{\{a,b\}}^{-1}(f) = \left((f - b) * a^{-1}\right) \bmod p \text{ where } a * a^{-1} \equiv 1 \pmod p \quad (7)$$

Here, mod p is performed over the coefficients and constant term of the polynomial.

Suppose that the communicating parties are A and B. Parameters those are public: Prime number (p).

Step 1: Public key and private key generation by A.

- Select a set of integers $\{\alpha_i\}_{i=1,2,\dots,n}$, $\alpha_i \in Z$ and $[a_i, b_i]_{i=1,2,\dots,r}$, $r \in N$.
- Select a multivariate polynomial $f(x_1, x_2, \dots, x_n)$ over the ring $Z[x_1, x_2, \dots, x_n]$.
- Compute $T_{[a_1, b_1]}\, T_{[a_2, b_2]} \dots T_{[a_r, b_r]}\left(f(x_1, x_2, \dots x_n)\right) = h(x_1, x_2, \dots, x_n)$.
- Public key of A: $\left(f(x_1, x_2, \dots, x_n), h(x_1, x_2, \dots, x_n)\right)$.
- Private key of A: $(\{\alpha_i\}_{i=1,2,\dots,n}, [a_i, b_i]_{i=1,2,\dots,r})$.

Step 2: Public key and private key generation by B.

- Select a set of integers $\{\beta_i\}_{i=1,2,\dots,n}$, $\beta_i \in Z$ and $[c_i, d_i]_{i=1,2,\dots,s}$, $s \in N$.
- Select a multivariate polynomial $g(x_1, x_2, \dots, x_n)$ over the ring $Z[x_1, x_2, \dots, x_n]$.
- Compute $T_{[c_1, d_1]}\, T_{[c_2, d_2]} \dots T_{[c_s, d_s]}\left(g(x_1, x_2, \dots x_n)\right) = l(x_1, x_2, \dots, x_n)$
- Public key of B: $\left(g(x_1, x_2, \dots, x_n), l(x_1, x_2, \dots, x_n)\right)$.
- Private key of B: $(\{\beta_i\}_{i=1,2,\dots,n}, [c_i, d_i]_{i=1,2,\dots,s})$.

Step 3: Key exchange.

- A computes $l(\alpha_1, \alpha_2, \dots, \alpha_n) \bmod p = u$ and sends it to B. Similarly, B computes $h(\beta_1, \beta_2, \dots, \beta_n) \bmod p = v$ and sends it to A.
- A computes $f(\beta_1, \beta_2, \dots, \beta_n) \bmod p = T_{[a_r, b_r]}^{-1} \dots T_{[a_1, b_1]}^{-1}\, T_{[a_1, b_1]} \dots T_{[a_r, b_r]}^{-1}(v) = y$ and $g(\alpha_1, \alpha_2, \dots, \alpha_n) \bmod p = z$.
- B computes $g(\alpha_1, \alpha_2, \dots, \alpha_n) \bmod p = T_{[c_s, d_s]}^{-1} \dots T_{[c_1, d_1]}^{-1}\, T_{[c_1, d_1]} \dots T_{[c_s, d_s]}(u) = z$ and $f(\beta_1, \beta_2, \dots, \beta_n) \bmod p = y$.
- Finally, A and B agree on the key: $y * z$.

The proposed methodology is explained through Figure 2.

- $P_A(f) = T_{[a_1, b_1]}\, T_{[a_2, b_2]} \dots T_{[a_r, b_r]}\left(f(x_1, x_2, \dots x_n)\right)$,
- $P_B(g) = T_{[c_1, d_1]}\, T_{[c_2, d_2]} \dots T_{[c_s, d_s]}\left(g(x_1, x_2, \dots x_n)\right)$,
- $P_A^{-1}\left(h(\beta_1, \beta_2, \dots, \beta_n)\right) = T_{[a_r, b_r]}^{-1} \dots T_{[a_1, b_1]}^{-1}\left(h(\beta_1, \beta_2, \dots, \beta_n)\right) = f(\beta_1, \beta_2, \dots, \beta_n)$,
- $P_B^{-1}\left(l(\alpha_1, \alpha_2, \dots, \alpha_n)\right) = T_{[c_s, d_s]}^{-1} \dots T_{[c_1, d_1]}^{-1}\left(l(\alpha_1, \alpha_2, \dots, \alpha_n)\right) = g(\alpha_1, \alpha_2, \dots, \alpha_n)$.

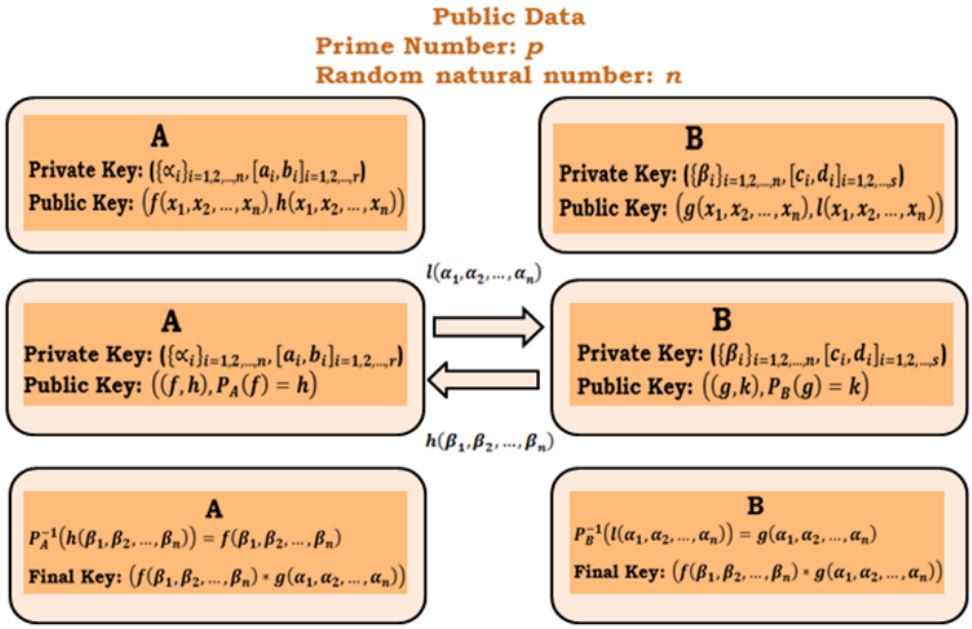


Figure 2. Key exchange process: (a) Public and private key generation of A and B; (b) Exchange of information by both A and B to retrieve the key; (c) Deducing the exchanged key

The application of a non-commutative invertible linear operator in the proposed protocol is a necessary condition for retaining the security and efficiency of the protocol. If the operator is commutative, then it is easy for an intruder to deduce the key. This is explained below:

T is commutative $\Rightarrow T_{[a,b]}\, T_{[c,d]}(u) = T_{[c,d]}\, T_{[a,b]}(u) = T_{[e,f]}(u)$ for some e, f.

The values of $[a, b]$, $[c, d]$ are private to the party but it is computationally feasible to trace e, f values and therefore

$T^{-1}_{[e,f]}(u)$ could be calculated to retrieve $g(\alpha)$. Similarly, $f(\beta)$ could be retrieved. Whereas if T is non-commutative then the intruder needs access to $[a,b]$, $[c,d]$ and the order of applying the transformations $T_{[a,b]}$, $T_{[c,d]}$ to reach $g(\alpha)$. Therefore, non-commutative nature of the operator plays a major role in retaining the security of the protocol.

If the operator is non-invertible, it is impossible for the communicating parties to retrieve $f(\beta)$ and $g(\alpha)$. Thus, the operator needs to be invertible.

Public keys of A and B assist the communicating parties to send signals to each other to initiate the process of key agreement. Private keys of A and B permit the parties to access the key confidentially.

Affine transformation is invertible, non-commutative, and easy to comprehend and implement thus making it the best fit for the protocol. The prime number p chosen increases the number of possibilities for the $a_i s$ and $c_i s$ as $\gcd(a_i, p) = 1$ and $\gcd(c_i, p) = 1$ is required. All the computations in the protocol are performed over modulo p thus the parameter p is declared publicly.

The rest of the paper is organized as follows: Section 3 illustrates the proposed method with an Example. Section 4 displays a comparative analysis of the proposed SKAP with studies [10, 11, 13]. Section 5 presents a mathematical model of the proposed SKAP in Telemedicine. Section 6 concludes the presented work in the paper, and the future scope of the work is presented in Section 7.

3. ILLUSTRATION

The illustration of the proposed SKAP is explained through the example below.

Suppose that the key is shared between two parties, A and B. For the following choices of n=3, p=13, r=2 and s=2, the protocol works as:

Step 1: Public and private key generation of A

Let $(\alpha_1, \alpha_2, \alpha_3) = (2, 3, 5)$ be any random solution set, $f(x_1, x_2, x_3) = x_1^2 + x_2 + 3x_3^2 + 5$ be any multivariate polynomial in 3 variables and $[a_1, b_1] = [5, 6]$, $[a_2, b_2] = [2, 3]$.

Then $h(x_1, x_2, x_3) = T_{[a_1,b_1]}\, T_{[a_2,b_2]}\big(f(x_1, x_2, x_3)\big) = T_{[5,6]}\, T_{[2,3]}(x_1^2 + x_2 + 3x_3^2 + 5) = T_{[5,6]}\big((2.(x_1^2 + x_2 + 3x_3^2 + 5) + 3) \bmod 13\big) = (5.(2x_1^2 + 2x_2 + 6x_3^2) + 6) \bmod 13 = 10x_1^2 + 10x_2 + 4x_3^2 + 6.$

From Eq. (6), $T_{[5,6]}(x) = (5.x + 6)\ mod\ 13$ and $T_{[2,3]}(x) = (2.x + 3)\ mod\ 13$.

Public key of A: $(x_1^2 + x_2 + 3x_3^2 + 5, 10x_1^2 + 10x_2 + 4x_3^2 + 6)$.

Private key of A: $\big((2, 3, 5), ([5, 6], [2, 3])\big)$.

Step 2: Public and private key generation of B

Let $(\beta_1, \beta_2, \beta_3) = (3, 5, 7)$ be any random solution set, $g(x_1, x_2, x_3) = 2x_1 + 3x_2^2 + x_3 + 6$ be any multivariate polynomial in 3 variables and $[c_1, d_1] = [5, 6]$, $[c_2, d_2] = [1, 2]$.

Then $l(x_1, x_2, x_3) = T_{[c_1,d_1]}\, T_{[c_2,d_2]}\big(g(x_1, x_2, x_3)\big) = T_{[5,6]}\, T_{[1,2]}\big(2x_1 + 3x_2^2 + x_3 + 6\big) = T_{[5,6]}\Big(\big(\big(2x_1 + 3x_2^2 + x_3 + 6\big) + 2\big) \bmod 13\Big) = \big(5.\big(2x_1 + 3x_2^2 + x_3 + 8\big) + 6\big) \bmod 13 = 10x_1 + 2x_2^2 + 5x_3 + 7.$

From Eq. (6), $T_{[5,6]}(x) = (5.x + 6)\ mod\ 13$ and $T_{[1,2]}(x) = (1.x + 2)\ mod\ 13$.

Public key of B: $\big(2x_1 + 3x_2^2 + x_3 + 6, 10x_1 + 2x_2^2 + 5x_3 + 7\big)$.

Private key of B: $\big((3, 5, 7), ([5, 6], [2, 3])\big)$.

Step 3: Key exchange

A computes $g(\alpha_1, \alpha_2, \alpha_3) = 42 \bmod 13 = 3$, $l(\alpha_1, \alpha_2, \alpha_3) = 70 \bmod 13 = 5$ and sends $l(\alpha_1, \alpha_2, \alpha_3)$ to B.

B computes $f(\beta_1, \beta_2, \beta_3) = 166 \bmod 13 = 10$, $h(\beta_1, \beta_2, \beta_3) = 342 \bmod 13 = 4$ and sends $h(\beta_1, \beta_2, \beta_3)$ to A.

A retrieves the value of $f(\beta_1, \beta_2, \beta_3) = T_{[a_2,b_2]}^{-1}\, T_{[a_1,b_1]}^{-1}\big(f(\beta_1, \beta_2, \beta_3)\big) = T_{[2,3]}^{-1}\, T_{[5,6]}^{-1}(4) = T_{[2,3]}^{-1}\big((4 - 6).8 \bmod 13\big) = (10 - 3).7 \bmod 13 = 10.$

From Eq. (7), $T^{-1}_{[5,6]}(x) = \big((x - 6).8\big)\ mod\ 13$ as $5.8 \equiv 1\ (mod\ 13)$.
Similarly, $T^{-1}_{[2,3]}(x) = \big((x - 3).7\big)\ mod\ 13$ as $2.7 \equiv 1\ (mod\ 13)$.

B retrieves the value of $g(\alpha_1, \alpha_2, \alpha_3) = T_{[c_2,d_2]}^{-1}\, T_{[c_1,d_1]}^{-1}\big(l(\alpha_1, \alpha_2, \alpha_3)\big) = T_{[1,2]}^{-1}\, T_{[5,6]}^{-1}(5) = T_{[1,2]}^{-1}\big((5 - 6).8 \bmod 13\big) = (5 - 2).1 \bmod 13 = 3.$

From Eq. (7), $T^{-1}_{[5,6]}(x) = \big((x - 6).8\big)\ mod\ 13$ as $5.8 \equiv 1\ (mod\ 13)$.
Similarly, $T^{-1}_{[1,2]}(x) = \big((x - 2).1\big)\ mod\ 13$ as $1.1 \equiv 1\ (mod\ 13)$.

Final Key: $f(\beta_1, \beta_2, \beta_3) * g(\alpha_1, \alpha_2, \alpha_3) = 10 * 3 = 30$.

4. COMPARATIVE ANALYSIS

The proposed SKAP is analyzed on the following security aspects and is compared with some existing methods [10, 11, 13] of safeguarding the cryptographic key:

4.1 Methodological approach

Diophantine equations serve as the building block of the protocol in studies [10, 13]. In study [11], Elliptic Curve Cryptography (ECC) is applied to design the protocol. The methodology adopted in designing the SKAP proposed applies two multivariate polynomials, f and g, and Affine transformation T. The non-commutative and invertible nature of the Affine operator serves as the base for the working of the protocol.

4.2 Number of secure rounds in a single session

This section demonstrates the maximum number of times the protocol is secure with the same choice of public and private keys chosen by the communicating parties. In short, it

discovers the number of times a generated key through the SKAP could be used to encrypt data demonstrated in the Figure 3.

In the study [13], a Linear Diophantine equation:

$$f(x_1, x_2, \dots, x_n) = 0 \ni f(\propto_i) = 0 \quad (10)$$

is selected by the recipient which facilitates the working of the protocol that is secure for at most $(n-2)$ times with the same LDE and the solution set. In the $(n-1)^{th}$ round, the recipient needs to change the solution set of the chosen equation.

$$f(x_1, x_2, \dots, x_n) = 0 \quad (11)$$

to retain the security of the protocol.

Our protocol works over the public keys, multivariate polynomials $f(x_1, x_2, \dots, x_n)$, $g(x_1, x_2, \dots, x_n)$ and the private keys, set of integers $\{\propto_i\}_{i=1,2,\dots,n}$, $\{\beta_i\}_{i=1,2,\dots,n}$, $[a_i, b_i]_{i=1,2,\dots,r}$ and $[c_i, d_i]_{i=1,2,\dots,s}$. The designed protocol is secure with the same polynomials and the set of integers for at most (n-2) rounds. After (n-2) rounds, either of the communicating parties needs to change the chosen polynomial or the set of integers alternately which would work for the next 2(n-2) rounds. Hence, both the communicating parties share the responsibility of changing public or private keys after each session. Although the system needs a change of polynomial or the set of integers after every (n-2) rounds, the individual communicating party needs to change the polynomial or the set of integers after 2(n-2) rounds.

The SKAP consists of a maximum of 2(n-2) rounds in a single session. The diagram below represents the changes required in the protocol after (n-2) rounds which are incorporated alternately by both the communicating parties A and B individually after 2(n-2) rounds.

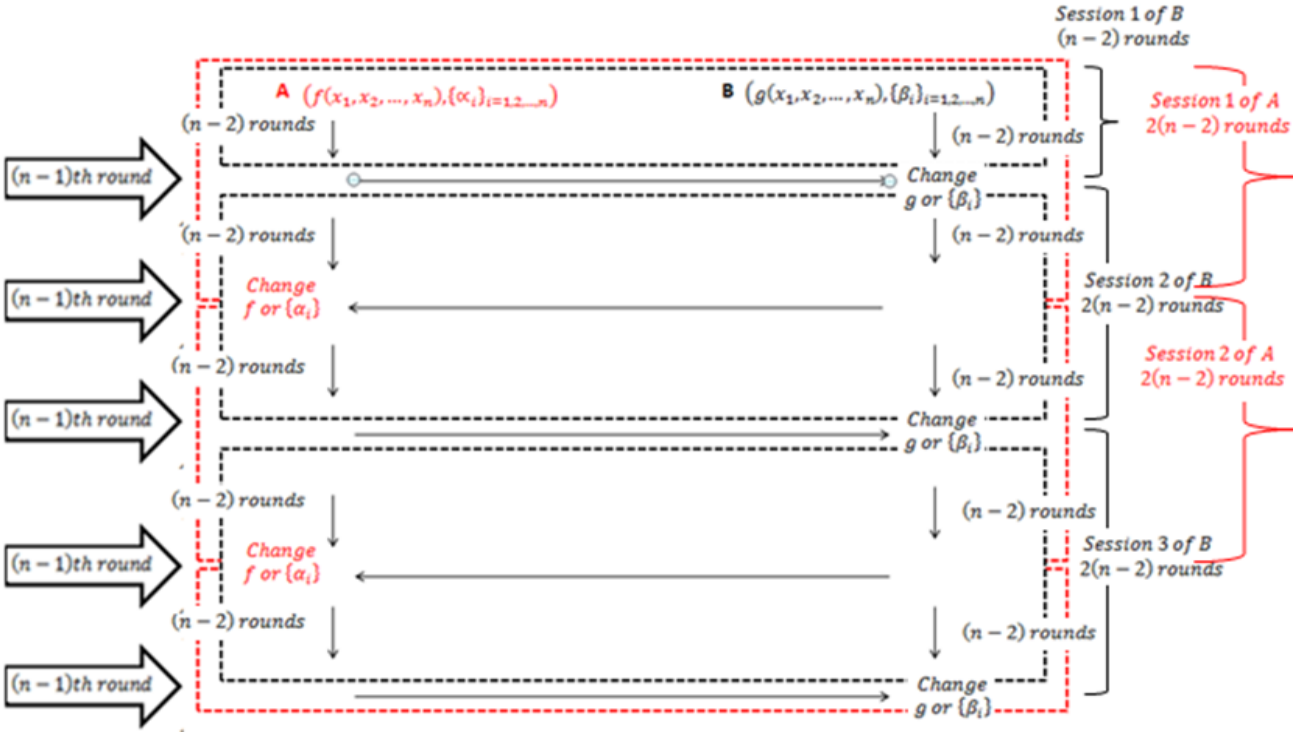


Figure 3. Required change in the chosen multivariate polynomial or the set of integers in the $(n-1)^{th}$ round

In the $(n-1)^{th}$ step, the intruder has access to a set of n equations in n variables, which are:

$$h(\beta_i) = v_j;\ l(\propto_i) = u_j, i, j = 1,2, \dots, n \quad (12)$$

The above set of equations can be solved to retrieve the values of $\{\propto_i\}_{i=1,2,\dots,n}$ and $\{\beta_i\}_{i=1,2,\dots,n}$.

As depicted in the diagram above, on changing the set of integers $\{\beta_i\}_{i=1,2,\dots,n}$ in $(n-1)^{th}$ round, the values of $\{\propto_i\}_{i=1,2,\dots,n}$ can be traced from the system of equations.

$$l(\propto_i) = u_j, i, j = 1,2, \dots, n \quad (13)$$

But $\{\beta_i\}_{i=1,2,\dots,n}$ is unknown.

If the polynomial g is changed then the values of $\{\beta_i\}_{i=1,2,\dots,n}$ can be traced from the system of equations.

$$h(\beta_i) = v_j, i, j = 1,2, \dots, n \quad (14)$$

But the values of $\{\propto_i\}_{i=1,2,\dots,n}$ is unknown for the next (n-2) rounds because of the change in the polynomial g. Therefore, the protocol is secure with the same set of integers and the polynomials chosen by both the communicating parties for at most (n-2) rounds but the individual communicating party can travel with the same polynomial or set of integers chosen for at most 2(n-2) rounds. Hence, the responsibility of changing the chosen polynomial or set of integers is divided equally among both the communicating parties in the protocol.

4.3 Session key

Session Key is a key that permits the users to access information for a single session. Once the session ends, the key expires and a new key is generated mutually among the authorized users to access the information and enhance the

security.

The protocol developed in the study [11] generates Session key whereas the protocols in studies [10, 13] emphasis on exchanging a single cryptographic key and no discussion regarding the session key is encapsulated. The SKAP proposed in this paper generates a Session Key discussed in detail in section 4.7.

4.4 Session key confidentiality

Session Key Confidentiality (SKC) refers to accessibility of the generated session key to the authorized users only such that no intruder can intercept it. This feature is achieved by the study [11] and the proposed SKAP. The non-commutative and invertible nature of the Affine operator helps in achieving the SKC in our protocol. The mathematical explanation of the security of the protocol is explained in section 2. The order of applying the Affine operators to obtain 'h' and 'g' is private to the authorized users only, which is required for retrieving the key from the public information. Hence the generated Session Key is confidential.

4.5 Known key security

Known key security is a feature where the knowledge of the current session key reveals no information about the next session key. This feature is possessed by the protocol in the study [11].

In the proposed SKAP, the change in the solution sets after every session is responsible for the rejuvenation of the session key. The choice of solution sets is private to the respective parties. Hence, the generated session keys are independent of the previous session keys retaining the Known-Key Security feature.

4.6 Brute-force attack

Brute-force attack is the attack carried out by an intruder to discover the cryptographic key used in encryption by trying all the possible keys. Thus, a large set of possible keys is desirable to prevent a cryptosystem from Brute-force attack.

In the proposed SKAP, the maximum possible values for $f(\beta)$ is p and for $g(\alpha)$ is p. Therefore, the number of possible keys $f(\beta) * g(\alpha)$ is p^2. Therefore, the attacker has to try p^2 number of keys, which are $\{1, 2, \dots, p^2 - 1, p^2\}$ to reach the exchanged key. Thus, by sufficiently increasing the value of p, the number of possible keys can be increased to improve security.

4.7 Passive attack

A cryptographic protocol displays some information publicly and conceals some for attaining efficiency and security respectively. Adversaries attack the protocols through the available public information and such attacks are categorized as passive attacks.

The developed SKAP's resistance to passive attacks is discussed as:

The intruder can use the publicly available information in the protocol in two ways to trace the key. One way is to reach the private keys $[a_i, b_i]_{i=1,2,\dots,r}$ of A and $[c_i, d_i]_{i=1,2,\dots,s}$ of B. The other way is to trace the values of $\{\propto_i\}_{i=1,2,\dots,n}$ and $\{\beta_i\}_{i=1,2,\dots,n}$ from the publicly available information:

$$f(x_1, x_2, \dots, x_n), h(\beta_1, \beta_2, \dots, \beta_n) = v \quad (8)$$

$$g(x_1, x_2, \dots, x_n), l(\alpha_1, \alpha_2, \dots, \alpha_n) = u \quad (9)$$

4.7.1 Infeasible to trace the private keys $[a_i, b_i]_{i=1,2,\dots,r}$ of A and $[c_i, d_i]_{i=1,2,\dots,s}$ of B

Although the composition of Affine operators is Affine, but the composition of operators cannot be confined to a single operator due to the multivariate polynomial function used in the process. In the example discussed above, let us consider that $T_{[a_1, b_1]}\, T_{[a_2, b_2]}(f(x_1, x_2, x_3)) = T_{[m,n]}(f(x_1, x_2, x_3))$.

Then,

$T_{[m,n]}(f(x_1, x_2, x_3)) = 10{x_1}^2 + 10x_2 + 4{x_3}^2 + 6$

$\Rightarrow (m.({x_1}^2 + x_2 + 3{x_3}^2 + 5) + n) \bmod 13 = 10{x_1}^2 + 10x_2 + 4{x_3}^2 + 6$

$\Rightarrow m = 10,\ n = 5,\ m^{-1} = 4.$

Now, ${T_{[m,n]}}^{-1}(h(\beta_1, \beta_2, \beta_3)) = {T_{[m,n]}}^{-1}(4) = 9$, which is not the required value of $f(\beta_1, \beta_2, \beta_3)$.

Therefore, it is not possible to use a single value in place of $[a_i, b_i]_{i=1,2,\dots,r}$ or $[c_i, d_i]_{i=1,2,\dots,s}$ by the intruder.

4.7.2 Infeasible to retrieve the set of integers $\{\propto_i\}_{i=1,2,\dots,n}$ and $\{\beta_i\}_{i=1,2,\dots,n}$ for n>1 for a single round

Through the available information, it is possible to retrieve the key only when the chosen f and g are polynomials in one variable i.e., n=1. Thus, the key exchange protocol is secure for n>1.

4.8 Computation and implementation

The proposed SKAP is easy to implement because choosing multivariate polynomials and selecting $[a_i, b_i]_{i=1,2,\dots,r}$ or $[c_i, d_i]_{i=1,2,\dots,s}$, solution sets $\{\propto_i\}_{i=1,2,\dots,n}$, $\{\beta_i\}_{i=1,2,\dots,n}$ are independent of each other. The methodology applies Affine operator to compute the key, which is computationally efficient. The initial step in protocols [10, 13] is to choose Diophantine equation $f(x_1, x_2, \dots, x_n) = a_1x_1 + a_2x_2 + \dots + a_nx_n = b \ni f(\alpha_1, \alpha_2, \dots, \alpha_n) = b$. This choice is suitable, provided $\gcd(a_1, a_2, \dots, a_n)$ divides b. Tracing such solution sets for a Diophantine equation with large coefficients is computationally complex and difficult to implement in real-time

4.9 Application

The developed SKAP is implementable in real-time applications where a secure online platform is to be constructed for sharing information and communication. One of the applications is Telemedicine which is discussed in detail in Section 5 of this paper.

The comparative analysis of the protocol is summarized in Table 1.

Thus, the developed SKAP is resistant to Brute-force and passive attacks. Also, the session key generated through the proposed SKAP retains confidentiality and known-key security feature. The number of secure rounds in a single session of the key agreement protocol is (n-2) which is extendable to 2 (n-2) as discussed in section 4.2. The protocol is easily implementable and computationally efficient whose application in Telemedicine is explored in section 5. Hence, the proposed protocol is ideal than the protocols developed in studies [10, 11, 13].

Table 1. Comparison of the proposed SKAP with studies [10, 11, 13]

Key Agreement or Key Exchange Protocol	Ref. [10]	Ref. [11]	Ref. [13]	Proposed Work
Method	Based on higher order Diophantine equations	Based on ECC	Based on linear Diophantine equations	Based on multivariate polynomials and affine transformation
Number of secure rounds in a single session	NM	NM	Y	Y
Session key	NM	Y	NM	Y
Session key confidentiality	NM	Y	NM	Y
Known key security	NM	Y	NM	Y
Brute-force attack	Y	Y	Y	Y
Passive attack	Y	NM	Y	Y
Computation and implementation	Hard	Y	Hard	Easy
Application	N	Y	N	Y

Note: Y: Resistant to attacks or holds the property or incorporated in the work; N: Doesn't hold the property; NM: Not incorporated in the work.

5. MATHEMATICAL MODEL OF THE PROPOSED SKAP IN TELEMEDICINE

Telemedicine has focused on the comfort of patients and doctors in remote areas for medical needs by providing a secure and efficient online platform for mutual communication [10, 16]. The medical information of a patient is at risk of manipulation for seeking undue advantage in terms of claiming insurance and personal grudges. The medical data hence needs to be safeguarded while transferring. During the COVID-19 pandemic, the mobility of patients was not recommended to halt the risk of infection with the life-threatening Corona virus. Telemedicine played an essential role in the times of the COVID-19 pandemic in curbing the spread of the virus and saving doctors' time [17]. Identifying the illness through the symptoms and prescribing necessary remedies needs mere communication between the patient and the doctor, which could be performed on an online platform. In fact, a patient suffering from cardio-vascular disease is more prone to infections whose treatment through Telemedicine Services is preferable to diminish the spread of the virus during the pandemic [10].

The online Health Service platforms permit the patient to consult the doctor remotely and share sensitive medical information for further treatment as depicted in Figure 4. This communication occurs in multiple sessions unless the patient is relieved from illness. The data is shared in an encrypted format for better security. Mutual Session keys are generated, which allow the patient and the doctor to access the encrypted data. These session keys expire after every session, and a new session key is rejuvenated to rescue the data from an intruder, which needs multiple computations.

Cryptography is an aid to implement the advancement in Telemedicine [18-21]. The Electronic Health Service platform designed should be efficient enough to support user mobility, patient privacy, mutual authentication, data confidentiality, and integrity.

- User Mobility refers to accessing and lending medical diagnosis by a patient and doctor respectively from a remote location.
- Patient's privacy refers to concealing the health status and details of the patient.
- Mutual authentication verifies the identity of the patient and the doctor.
- Data confidentiality refers to protecting the data from illegitimate access and integrity is to retain the accuracy of the data.

Researchers are thriving to develop competent real-time online Heath Service platforms that apply strong mathematical models in programming. In the study [22], several secure and efficient symmetric key exchange protocols are designed to assist in Telemedicine, supporting user mobility, patient privacy, and anonymity.

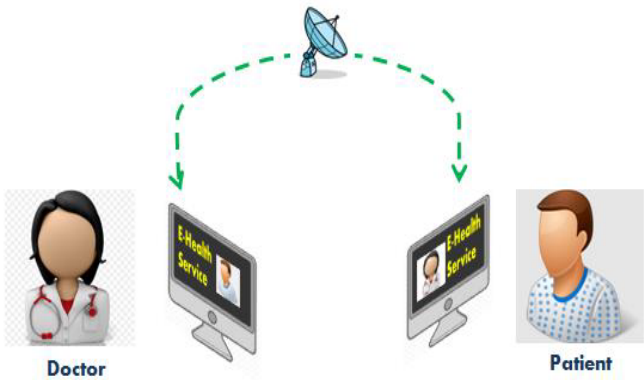


Figure 4. Remote diagnosis of patient through e-health service

5.1 Proposed online e-health service model

The proposed model of an e-Health Service Platform depicted in the Figure 5 relies on a key agreement protocol has the following main components:

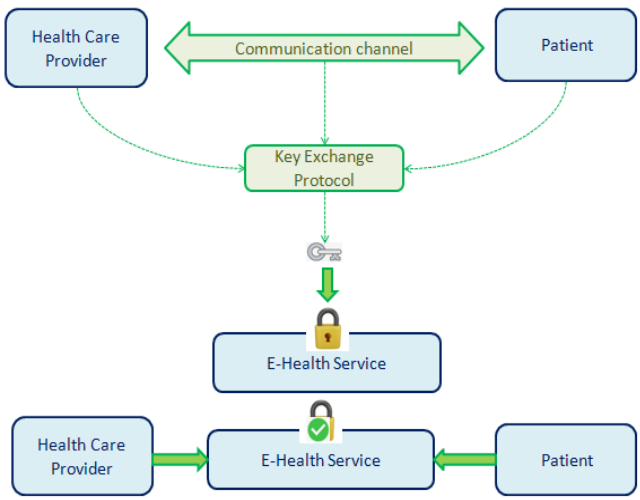


Figure 5. Proposed model of an e-health service platform

- Health Care Provider (HCP): One who diagnoses the illness of the patient and provides medical treatment.

- Patient: One who suffers from illness and needs medical diagnosis.
- Online Health Service Platform: An authenticated online platform that would connect the health care provider and the patient for medical consultation.
- Key Agreement Protocol: A passive attack-resistant protocol to agree on a key between two communicating parties.

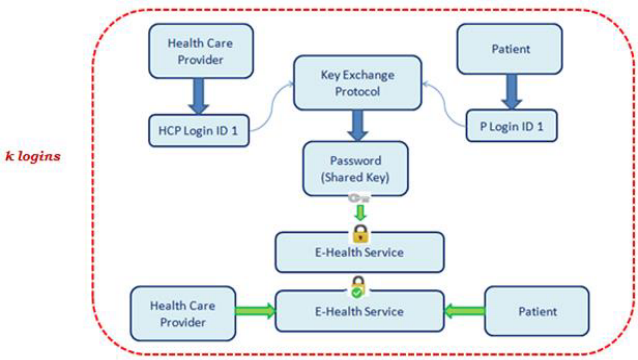
The proposed model permits communication between the Health Care provider and the patient to agree on a password that unlocks the Online Health Service platform to continue the medical treatment. The privacy of the patient's health record is retained in the developed model by providing a remote diagnosis.

5.2 Working of the proposed online e-health service platform

The Online e-Health Service platform is accessible to the HCP and the patient by using their respective credentials, which constitute a valid Login Id and a password. The Health Care Provider and the patient choose their Login Ids randomly, which are applied to generate a shared password to unlock the Health Service platform. The chosen Login Ids and the generated password are valid for a finite number (k) of logins. After k logins, a request to change the Login Id is sent to the HCP initially. This reflects a change in the shared password which is valid for the subsequent k logins. Subsequently, a request to the patient is sent to change the Login Id to create a new password. The proposal to change Login Ids is communicated to both the HCP and the patient alternatively after every k number of logins to retain security.

The password generated is secure from passive attacks for k logins. To provide authenticity, the password is stored in a vault to verify it against the input login Id and password. An intruder can attack the vault to trace the password set. Session passwords are a solution to the mentioned threat which expire after every session and are rejuvenated for every single session.

The passive attack-resistant SKAP proposed in Section 2 of this paper is applicable to develop the proposed Online Health Service Model. The protocol is secure with the same choice of polynomials, solution sets and the transformations for a maximum of (n-2) logins where n is the number of variables in the chosen polynomial. The number of secure logins is extendable to 2(n-2) logins with an alternate change in the solution sets or the chosen polynomials or the transformations after (n-2) rounds. To generate Session passwords, the solution sets are changed after every session which is randomly input by the user. The working of the proposed online e-health service platform is demonstrated in the Figure 6.



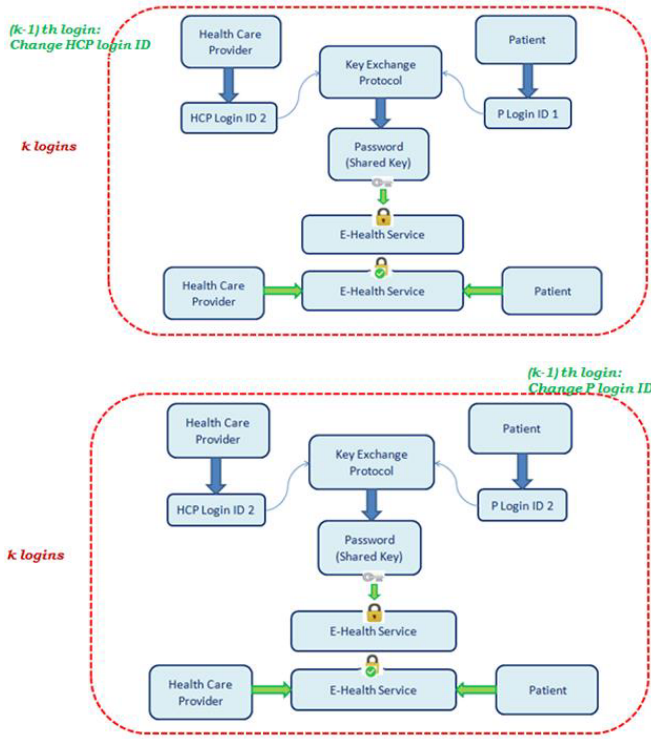


Figure 6. Working of an e-health care system

6. CONCLUSIONS

A robust and efficient Session Key Agreement Protocol (SKAP) based on Affine transformations over multivariate polynomials has been proposed. This protocol's methodology was derived from the classical Affine cipher, facilitating ease of understanding and implementation. The protocol is designed to generate a session key, thereby enhancing security. Notably, it delineates the number of possible secure rounds within a single session, given a consistent selection of public and private keys. Resistance to brute-force and passive attacks is inherent to the protocol, which operates independently of a trusted third party.

The developed SKAP is suitable for secure two-party communication, permitting information access and privacy for the participating entities. Telemedicine, characterized by remote diagnostics and treatment, presents an appropriate application scenario. In this context, the protocol's application in Telemedicine is elucidated, underscoring the practical value of SKAP in real-world settings.

7. FUTURE SCOPE

The communicating parties in the SKAP lack mutual authentication. Hence, competent authentication schemes are required to enhance the security of the developed SKAP.

ACKNOWLEDGMENT

This work is supported by GITAM Deemed to be University in the form of Dr. M.V.V.S Murthi Research Fellowship for which we are grateful.

REFERENCES

[1] Diffie, W., Hellman, M. (1976). New directions in cryptography. IEEE Transactions on Information Theory, 22(6): 644-654. https://doi.org/10.1109/TIT.1976.1055638

[2] Bérczes, A., Hajdu, L., Hirata-Kohno, N., Kovács, T., Pethő, A. (2014). A key exchange protocol based on diophantine equations and s-integers. JSIAM Letters, 6: 85-88. https://doi.org/10.14495/jsiaml.6.85

[3] Kameswari, P.A., Kumar, L.P. (2014). A method for recovering a key in the key exchange cryptosystem by diophantine equations. International Journal of Computer Applications, 100: 11-13. https://doi.org/10.5120/17592-8302

[4] Okumura, S. (2015). A public key cryptosystem based on diophantine equations of degree increasing type. Pacific Journal of Mathematics for Industry, 7(1): 1-13. https://doi.org/10.1186/s40736-015-0014-4

[5] Ben Slimane, Y., Ben Ahmed, K. (2017). Efficient end-to-end secure key management protocol for internet of things. International Journal of Electrical and Computer Engineering (IJECE), 7(6): 3622-3631. https://doi.org/10.11591/ijece.v7i6.pp3622-3631

[6] Chen, C.L., Li, C.T. (2008). Dynamic session-key generation for wireless sensor networks. EURASIP Journal on Wireless Communications and Networking, 2008: 1-10. https://doi.org/10.1155/2008/691571

[7] Osipyan, V.O., Litvinov, K.I. (2018). A mathematical model of the cryptosystem based on the linear diophantine equation. In Proceedings of the 11th International Conference on Security of Information and Networks, pp. 1-4. https://doi.org/10.1145/3264437.3264464

[8] Choe, C.H., Lee, M.H. (2011). Key agreement protocol using sylvester hadamard matrices. Journal of Communications and Networks, 13(3): 211-213. https://doi.org/10.1109/JCN.2011.6157429

[9] Zaghian, A., Hashemi, M.J., Majlessi, A. (2014). Improving the key agreement protocol security based on hadamard matrices. Journal of Mathematics and Computer Science, 12: 316-319. https://doi.org/10.22436/jmcs.012.04.07

[10] Dey, J., Bhowmik, A., Sarkar, A., Karforma, S., Chowdhury, B. (2022). Cryptographic engineering on COVID-19 telemedicine: an intelligent transmission through recurrent relation based session key. Wireless Personal Communications, 122(4): 3167-3204. https://doi.org/10.1007/s11277-021-09045-3

[11] Yosh, H. (2011). The key exchange cryptosystem used with higher order diophantine equations. International Journal of Network Security & Its Applicatons, 3(2): 43-50. https://doi.org/10.5121/ijnsa.2011.3204

[12] Hirata-Kohno, N., Petho, A. (2013). On a key exchange protocol based on diophantine equations. Infocommunications Journal, 5(3): 17-21.

[13] Kameswari, P.A., Sriniasarao, S.S., Belay, A. (2021). An application of linear diophantine equations to cryptography. Advanced in Mathematics: Scientific Journal, 10: 2799-2806. https://doi.org/10.37418/amsj.10.6.8

[14] Forouzan, B.A., Mukhopadhyay, D. (2015). Cryptography and network security, Third Edition. Mc Graw Hill Education.

[15] Stinson, D.R., Paterson, M. (2005). Cryptography: theory and practice. Fourth Edition, CRC Press, Taylor & Francis Group.

[16] Aslam, M.U., Derhab, A., Saleem, K., Abbas, H., Orgun, M., Iqbal, W., Aslam, B. (2017). A survey of authentication schemes in telecare medicine information systems. Journal of Medical Systems, 41: 1-26. https://doi.org/10.1007/s10916-016-0658-3

[17] Kadir, M.A. (2020). Role of telemedicine in healthcare during COVID-19 pandemic in developing countries. Telehealth and Medicine Today, 5(2). https://doi.org/10.30953/tmt.v5.187

[18] Xu, X., Zhu, P., Wen, Q.Y., Jin, Z.P., Zhang, H., He, L. (2014). A secure and efficient authentication and key agreement scheme based on ECC for telecare medicine information systems. Journal of Medical Systems, 38. https://doi.org/10.1007/s10916-013-9994-8

[19] Thabit, R. (2019). Review of cryptography applications in ehealth security systems. International Journal of Science and Engineering Investigations, 8(89): 110-116.

[20] Jnr, B.A. (2020). Use of telemedicine and virtual care for remote treatment in response to COVID-19 pandemic. Journal of Medical Systems, 44(7): 132. https://doi.org/10.1007/s10916-020-01596-5

[21] Oduor, X.F., Omariba, Z.B. (2022). Application of cryptography in enhancing privacy of personal data in medical services. International Journal of Communication and Information Technology, 3(1): 16-21. https://doi.org/10.33545/2707661X.2022.v3.i1a.41

[22] Rezaeibagha, F., Mu, Y. (2018). Practical and secure telemedicine systems for user mobility. Journal of Biomedical Informatics, 78: 24-32. https://doi.org/10.1016/j.jbi.2017.12.011