Santilli’s isofields first-kind based key exchange protocol

Mamta S Dani\textsuperscript{1}, Akshaykumar Meshram\textsuperscript{2}\textsuperscript{*} and Chandrashekhar Meshram\textsuperscript{3}

\textsuperscript{1, 2} Department of Applied Mathematics, Yeshwantrao Chavan College of Engineering, Nagpur, M.S., 441110, India.
\textsuperscript{3} Department of PG Studies and Research in Mathematics, Jayawanti Haksar Govt. PG College, College of Chhindwara University, Betul, M.P. 460001, India.

Corresponding author e-mail: \textsuperscript{*}akshaykjmeshram@gmail.com

Abstract. The key exchange protocol (𝓀ₑ𝓅) is used to barter whatsoever keys or related information are required, so that no one can replicate it. Conventionally either a reliable courier, diplomatic bags, or some other protected network are needed. The present work put forward, a new technique for designing a 𝓀ₑ𝓅 build on Santilli’s isofields of the first kind is to use rings isopolynomials with elements called isonumbers.

Keywords. Isounit, Isonumbers, Isopolynomials, Isofields, and Diffie-Hellman Problem.

1. Introduction

The 𝓀ₑ𝓅 is a key instituting process where similar private key is persistent by either two or more than two users, where every users are connected or used as a component of data contributed by, in a perfect world such that none can foreordain the subsequent value [1, 2]. The symmetric key cryptography based protocols consist of two communicating users, who uses a commonly approved algorithm and a secret key which is identified only to these users. A few defined ways can be used by the Secret 𝓀ₑ𝓅 such as, out-of-band correspondence, for example, by telephone, via email, physical entry and a trustworthy third party key distribution center etc. The greater part required for these process require earlier secret key formation used by the protocol and the independent users.

Diffie-Hellman’s [3] 𝓀ₑ𝓅 is the pioneer of practically use asymmetric cryptographic structure where two users who have never encountered are authorized, to establish a typical secrete key over an unprotected network. The 𝓀ₑ𝓅 based on the number theory are used commonly at present. The theoretical value relies upon the structure of abelian groups. The discrete logarithm problem (DLPG) [4, 5] as well as the elliptic curve DLP [6, 7], are the prime issues for which the public key cryptosystems is constructed. In cryptography the efficiently computable groups where DLP complex plays are a vital role [8]. Most of the recommended protocols are associated to arithmetic operations on commutative algebraic structures and certain efficient attacks are constructed on the commutative property of these structures and are well recognized. Different executions of the Diffie-Hellman protocol in matrix rings, for diverse variety of matrices, are presented in [9 10].

Meshram C. [11] offered certain different cryptographic techniques based on double DLP and specific implication on cryptography protocols in [12, 13, 14, 15]. Meshram A. [16, 17, 18] suggested some different cryptographic techniques based on suzuki 2-group and dihedral group which are secure in CPA, IND-CPA, IND-CCA2. Recently, Meshram A. [19] proposed key exchange protocol based on isomathematics.
2. Motivations and Organization

The present endeavor focuses on a novel method for constructing an isep established on the Santilli’s isofields of the first kind to utilized rings isopolynomials with isonumbers coefficient. This method is much easy to apply the isep.

The paper is organized as follow. We discussed the respective background in Section 3. Santilli’s isofields of the first kind based isep is offered in Section 4. Paper is concluded in Section 5.

3. Background

The section explains, definition such as the Santilli’s isofields, Symmetrical Decomposition Problem (SDP) over ring \( \bar{F} \), Diffie-Hellman Problem (DHP) over ring \( \bar{F} \).

3.1. Santilli’s isofields first kind [20]

The \( \bar{F} = \bar{F}(\hat{z}, +, \bar{x}) \) first kind of Santilli’s isofields are the rings with isonumbers \( \hat{z} = z\hat{f}, z \in \mathbb{F} \), \( \hat{f} = \frac{1}{f} \in \mathbb{F} \) and \( \hat{g} \) is the multiplication on \( \mathbb{F} \) with \( \hat{z} + \hat{g} = (z + y)\hat{f} \) an isosum, with additive unit \( 0 = 0\hat{f} = 0, \hat{z} + 0 = 0 + \hat{z} = \hat{z} \) and isoproduct \( \hat{z} \times \hat{g} = \hat{z}\bar{f} \hat{g} = z\hat{f} y\hat{f} = (yz)\hat{f} \).

where, the left and right new unit \( \hat{f}, \hat{g} \times \hat{z} = \hat{z} \times \hat{f} = \hat{z} \) is called isounit and \( \hat{f}\hat{g} = 1, \hat{f} \) is called inverse isounit \( \hat{f} \neq 1 \).

Let us consider isopolynomials with isonumbers coefficient. Initially, the notion of scale isoproduct over \( \bar{F} \) is already existing.

- If \( \hat{z} \in \mathbb{Z} > 0, \hat{f} \in \bar{F} \), then \( (\hat{z})\hat{f} = \{\hat{f} + \cdots + \hat{f}\}^{\hat{z}} \times \hat{f} \).
- If \( \hat{z} \in \mathbb{Z} < 0 \), then \( (\hat{z})\hat{f} = (-\hat{z})(-\hat{f}) = \{-\hat{f} + \cdots + (-\hat{f})\}^{\hat{z}} \times \hat{f} \).
- If \( \hat{z} = 0 \), then \( (\hat{z})\hat{f} = 0 \).

Remark-I. For every \( \hat{a}, \hat{u}, \hat{a}, \hat{b} \in \mathbb{Z} \) and \( \hat{f} \in \bar{F} \), we get \( (\hat{a})\hat{f}^\hat{a} \ast (\hat{u})\hat{f}^\hat{b} = (\hat{a}\hat{u})\hat{f}^\hat{a} \times \hat{b} \ast (\hat{v})\hat{f}^\hat{a} \).

We can conclude the above statement, by the definition of scale multiplication, the distributivity of multiplication with respect to addition, and commutativity of addition.

Remark-II. For \( \hat{f} \neq \hat{\lambda} \), we get \( (\hat{a})\hat{f} \ast (\hat{u})\hat{\lambda} = (\hat{a})\hat{\lambda} \ast (\hat{a})\hat{f} \).

We continue further to define ring isopolynomials with positive isointegral coefficient. Let \( \hat{h}(\hat{a}) = \hat{a}_{0} + \hat{a}_{1}\hat{z} + \cdots + \hat{a}_{\hat{a}}\hat{z}^{\hat{a}} \in \mathbb{Z}^{+}[\hat{z}] \) is an isopolynomial with positive isointegral coefficient. For isonumber \( \hat{f} \) in \( \bar{F} \) and get \( \hat{h}(\hat{f}) = \sum_{j=0}^{\hat{a}}(\hat{a}_{j})\hat{f}^{j} = (\hat{a}_{0}) + (\hat{a}_{1})\hat{f} + \cdots + (\hat{a}_{\hat{a}})\hat{f}^{\hat{a}} \in \bar{F} \). Additionally, if \( \hat{f} \in \bar{F} \), then \( \hat{h}(\hat{f}) \) can be isopolynomial about variable \( \hat{f} \). The set of such kinds of polynomials, encompassing all the \( \hat{h}(\hat{f}) \in \mathbb{Z}^{+}[\hat{f}] \), which can be looked upon as the extension of \( \mathbb{Z}^{+} \) with \( \ast \), referred by \( \mathbb{Z}^{+}[\hat{f}] \).

Assume that \( \hat{h}(\hat{f}) = \sum_{j=0}^{\hat{a}}(\hat{a}_{j})\hat{f}^{j} \in \mathbb{Z}^{+}[\hat{f}], \hat{h}(\hat{f}) = \sum_{k=0}^{\hat{u}}(\hat{u}_{k})\hat{f}^{k} \in \mathbb{Z}^{+}[\hat{f}] \) and \( \hat{b} \geq \hat{a} \), then \( \left( \sum_{j=0}^{\hat{b}}(\hat{a}_{j})\hat{f}^{j} \right) + \left( \sum_{k=0}^{\hat{a}}(\hat{u}_{k})\hat{f}^{k} \right) = \left( \sum_{j=0}^{\hat{b}}(\hat{a}_{j})\hat{f}^{j} \right) + \left( \sum_{k=0}^{\hat{a}}(\hat{u}_{k})\hat{f}^{k} \right) \), using Remark-I as well as the distributivity, for \( \rho_{j} = \sum_{k=0}^{\hat{b}}(\hat{a}_{j})\hat{u}_{k-k} = \sum_{k=0}^{\hat{b}}(\hat{a}_{j})\hat{u}_{k-k} \), where we have \( \left( \sum_{j=0}^{\hat{b}}(\hat{a}_{j})\hat{f}^{j} \right) = \left( \sum_{k=0}^{\hat{a}}(\hat{u}_{k})\hat{f}^{k} \right) \ast \left( \sum_{k=0}^{\hat{a}}(\hat{u}_{k})\hat{f}^{k} \right) \). So, we complete the following Remark-III conferring to Remark-I.

Remark-III. For every \( \hat{h}(\hat{f}), \hat{h}(\hat{f}) \in \mathbb{Z}^{+}[\hat{f}] \), we get \( \hat{h}(\hat{f}) \ast \hat{h}(\hat{f}) = \hat{h}(\hat{f}) \ast \hat{h}(\hat{f}) \).
In general, if \( \phi \neq \lambda \), then \( \bar{h}(\phi) \neq \bar{h}(\lambda) \). Consider ring isopolynomial with isonumber coefficient \( (\phi, +, \times) \). In case of any randomly select isonumber \( \bar{g} \in \bar{F} \), we define a set \( \bar{W}_{\bar{g}} \subseteq \bar{F} \) by \( \bar{W}_{\bar{g}} = \{ \bar{h}(\bar{g}) : \bar{h}(\phi) \in \mathbb{Z}^+[\bar{F}] \} \).

3.2 SDP over Ring \( \bar{F} \) with isopolynomial
For given \((\bar{\ell}, \phi, \delta) \in \bar{F}^3 \) and \( \bar{a}, \bar{b} \in \mathbb{Z}^+ \), find \( \bar{w} \in \bar{W}_{\bar{g}} \) such that \( \delta = \bar{w}^{\bar{a}} \phi \bar{w}^{\bar{b}} \).

3.3 DHP over Ring \( \bar{F} \) with isopolynomial
Compute \( \phi \bar{w}_1 \bar{w}_2 \) for given \( \phi, \phi \bar{w}_1 \) and \( \phi \bar{w}_2 \), where \( \phi \in \bar{F}, \bar{w}_1, \bar{w}_2 \in \bar{W}_{\bar{g}} \).

4. Santilli’s Isofields First-kind based kep
At this instant, let us consider the ring isopolynomial with the isonumber coefficient as an primary work and vital infrastructure to create a kep, where two users, say Mamta and Minal, who agree to share a secret session key via a public, insecure unreliable network.

The procedure is described as stated below:

i. Mamta refers two arbitrary small, positive isointegers \( \bar{a}, \bar{b} \in \mathbb{Z}^+ \) and two arbitrary elements
\( \bar{w}, \bar{a} \in \bar{F} \) to Minal.

ii. Mamta choose a randomly isopolynomial \( \bar{h}(\phi) \in \mathbb{Z}^+[\phi] \) such that \( \bar{h}(\phi) \neq 0 \) and then takes \( \bar{h}(\phi) \) as her secret key.

iii. Minal choose a randomly isopolynomial \( \hat{h}(\phi) \in \mathbb{Z}^+[\phi] \) such that \( \hat{h}(\phi) \neq 0 \) and then takes \( \hat{h}(\phi) \) as her secret key.

iv. Mamt computes \( M_A = \bar{h}(\phi)\bar{a} \times \hat{h}(\phi)\hat{b} \) and refers \( M_A \) to Minal.

v. Minal computes \( M_L = \hat{h}(\phi)\hat{a} \times \bar{h}(\phi)\bar{b} \) and refers \( M_L \) to Mamta.

vi. Minal computes \( R_{Mamta} = \bar{h}(\phi)\bar{a} \times M_L \times \hat{h}(\phi)\hat{b} \) as the shared session key.

vii. Minal computes \( R_{Minal} = \hat{h}(\phi)\hat{a} \times M_A \times \hat{h}(\phi)\hat{b} \) as the shared session key.

The illustration of the protocol is shown in the following table.

| Table 4.1. Santilli’s Isofields First-kind based kep |
|-----------------|-----------------|
| **Pass** | **Mamta** | **Minal** |
|-----------------|-----------------|
| Choose at randomly \( \bar{a}, \bar{b} \in \mathbb{Z}^+ \) | \( \bar{w}, \bar{a} \in \bar{F} \) | \( \bar{w}, \bar{a} \in \bar{W}_{\bar{g}} \) |
| Choose at randomly \( \bar{a}, \bar{b} \in \mathbb{Z}^+ \) | \( \bar{w}, \bar{a} \in \bar{F} \) | \( \bar{w}, \bar{a} \in \bar{W}_{\bar{g}} \) |
| Choose at randomly \( \bar{h}(\phi) \in \mathbb{Z}^+[\phi] \) | \( \bar{w}, \bar{a} \in \bar{F} \) | \( \bar{w}, \bar{a} \in \bar{W}_{\bar{g}} \) |
| \( \bar{a}, \bar{b}, \bar{a}, \bar{b}, \bar{h}(\phi)\bar{a} \bar{h}(\phi)\hat{b} \rightarrow \) | \( \bar{w}, \bar{a} \in \bar{F} \) | \( \bar{w}, \bar{a} \in \bar{W}_{\bar{g}} \) |
| Selects at arbitrary \( \hat{h}(\phi) \in \mathbb{Z}^+[\phi] \) | \( \bar{w}, \bar{a} \in \bar{F} \) | \( \bar{w}, \bar{a} \in \bar{W}_{\bar{g}} \) |
| \( \bar{h}(\phi)\bar{a} \hat{h}(\phi)\hat{b} \rightarrow \) | \( \bar{w}, \bar{a} \in \bar{F} \) | \( \bar{w}, \bar{a} \in \bar{W}_{\bar{g}} \) |
| \( R_{Mamta} = \bar{h}(\phi)\bar{a} \hat{h}(\phi)\hat{b} \rightarrow \) | \( \bar{w}, \bar{a} \in \bar{F} \) | \( \bar{w}, \bar{a} \in \bar{W}_{\bar{g}} \) |
| \( R_{Minal} = \hat{h}(\phi)\hat{a} M_A \hat{h}(\phi)\hat{b} \rightarrow \) | \( \bar{w}, \bar{a} \in \bar{F} \) | \( \bar{w}, \bar{a} \in \bar{W}_{\bar{g}} \) |
| \( \bar{w}, \bar{a} \in \bar{F} \) | \( \bar{w}, \bar{a} \in \bar{W}_{\bar{g}} \) |

\[
R_{Mamta} = \bar{h}(\phi)\bar{a} \hat{h}(\phi)\hat{b} \hat{h}(\phi)\hat{b} \hat{h}(\phi)\hat{b} = \hat{h}(\phi)\hat{a} \hat{h}(\phi)\hat{b} \hat{h}(\phi)\hat{b} = R_{Minal}
\]
4.1 Examples
Santilli’s Isofields First-kind based $\mathcal{KEP}$ using Matrix Rings.

Example I. Let an integer $\mathcal{N} = 17 \ast 19$, isounit $\hat{I} = \begin{bmatrix} 5 \\ 7 \\ 8 \end{bmatrix}$ and inverse of isounit $\hat{T} = \begin{bmatrix} -4 & 3 \\ 3,5 & -2.5 \end{bmatrix}$.
Suppose that Mamta chooses $\hat{a} = 2, \hat{b} = 3,$ $\hat{v} = \begin{bmatrix} 2 \\ 5 \\ 8 \end{bmatrix}, \hat{u} = \begin{bmatrix} 2 \\ 4 \\ 1 \end{bmatrix}$, and $\hat{\mathcal{K}}(\hat{\mathcal{R}}) = 3\hat{\mathcal{R}}^3 + 2\hat{\mathcal{R}}^2 + \hat{\mathcal{R}} + \hat{2}$.
She computes
$$\hat{\mathcal{K}}(\hat{v}) = 3\left[ \begin{array}{ccc} 3 & 5 \\ 7 & 8 \end{array} \right]^3 + 2\left[ \begin{array}{ccc} 3 & 5 \\ 7 & 8 \end{array} \right]^2 + \left[ \begin{array}{cc} 1 & 0 \\ 1 & 1 \end{array} \right] = \left[ \begin{array}{cc} 352 & 157 \\ 347 & 509 \end{array} \right] \mod 323 = \left[ \begin{array}{cc} 29 & 157 \\ 24 & 186 \end{array} \right]$$
And
$$\mathcal{M}_A = \hat{\mathcal{K}}(\hat{v})^\hat{a} * \hat{u} * \hat{\mathcal{K}}(\hat{v})^\hat{b}$$
$$\mathcal{M}_A = \left[ \begin{array}{cc} 29 & 157 \\ 24 & 186 \end{array} \right] * \left[ \begin{array}{cc} 2 & 4 \\ 6 & 1 \end{array} \right] * \left[ \begin{array}{cc} 29 & 157 \\ 24 & 186 \end{array} \right] = \left[ \begin{array}{cc} 20 & 236 \\ 30 & 105 \end{array} \right]$$
Then, she refers $\hat{a}, \hat{b}, \hat{v}, \hat{u}$ and $\mathcal{M}_A$ to Minal.

Now, suppose that Minal, after receiving $\hat{a}, \hat{b}, \hat{v}, \hat{u}$ and $\mathcal{M}_A$ from Mamta, choose a different isopolynomial $\hat{\mathcal{F}}(\hat{\mathcal{R}}) = 2\hat{\mathcal{R}}^2 + \hat{\mathcal{R}} + \hat{2}$ and compute
$$\hat{\mathcal{F}}(\hat{v}) = 2\left[ \begin{array}{ccc} 3 & 5 \\ 7 & 8 \end{array} \right]^2 + \left[ \begin{array}{cc} 1 & 0 \\ 1 & 1 \end{array} \right] = \left[ \begin{array}{cc} 93 & 115 \\ 161 & 208 \end{array} \right]$$
And
$$\mathcal{M}_L = \hat{\mathcal{F}}(\hat{v})^\hat{a} * \hat{u} * \hat{\mathcal{F}}(\hat{v})^\hat{b}$$
$$\mathcal{M}_L = \left[ \begin{array}{cc} 93 & 115 \\ 161 & 208 \end{array} \right] * \left[ \begin{array}{cc} 2 & 4 \\ 6 & 1 \end{array} \right] * \left[ \begin{array}{cc} 93 & 115 \\ 161 & 208 \end{array} \right] = \left[ \begin{array}{cc} 210 & 310 \\ 124 & 188 \end{array} \right]$$
Then, she refers $\mathcal{M}_L$ to Mamta.

At the end, Mamta derived the session key as
$$\hat{\mathcal{K}}_{\text{Mamta}} = \hat{\mathcal{K}}(\hat{v})^\hat{a} * \mathcal{M}_L * \hat{\mathcal{K}}(\hat{v})^\hat{b}$$
$$\hat{\mathcal{K}}_{\text{Mamta}} = \left[ \begin{array}{cc} 29 & 157 \\ 24 & 186 \end{array} \right] * \left[ \begin{array}{cc} 210 & 310 \\ 124 & 188 \end{array} \right] * \left[ \begin{array}{cc} 29 & 157 \\ 24 & 186 \end{array} \right] = \left[ \begin{array}{cc} 138 & 240 \\ 110 & 295 \end{array} \right]$$
While Minal derives the session key as
$$\hat{\mathcal{K}}_{\text{Minal}} = \hat{\mathcal{F}}(\hat{v})^\hat{a} * \mathcal{M}_A * \hat{\mathcal{F}}(\hat{v})^\hat{b}$$
$$\hat{\mathcal{K}}_{\text{Minal}} = \left[ \begin{array}{cc} 93 & 115 \\ 161 & 208 \end{array} \right] * \left[ \begin{array}{cc} 20 & 236 \\ 30 & 105 \end{array} \right] * \left[ \begin{array}{cc} 93 & 115 \\ 161 & 208 \end{array} \right] = \left[ \begin{array}{cc} 138 & 240 \\ 110 & 295 \end{array} \right]$$
Seemingly, $\hat{\mathcal{K}}_{\text{Mamta}} = \hat{\mathcal{K}}_{\text{Minal}}$ holds.

Example II. Let an integer $\mathcal{N} = 17 \ast 19$, isounit $\hat{I} = \begin{bmatrix} 1 & 7 & 5 \\ 8 & 6 & 2 \\ 3 & 5 & 9 \end{bmatrix}$ and inverse of isounit
$$\hat{T} = \begin{bmatrix} -1 & 19 \\ 7 & 154 \\ 3 & 3 \\ 3 & 3 \\ 14 & 154 \\ -1 & -4 \\ 14 & 154 \\ 77 & 154 \end{bmatrix}.$$ 
Suppose that Mamta chooses $\hat{a} = 2, \hat{b} = 3,$
\( \vec{v} = \begin{bmatrix} 5 & 6 & 3 \\ 2 & 5 & 9 \\ 7 & 1 & 8 \end{bmatrix}, \vec{u} = \begin{bmatrix} 1 & 6 & 9 \\ 7 & 9 & 5 \\ 2 & 4 & 3 \end{bmatrix} \) and \( \hat{K}(\vec{r}) = 3\vec{r}^3 + 2\vec{r}^2 + \vec{r} + \vec{2} \).

She computes,
\[
\hat{\mathcal{K}}(\vec{v}) = 3 \begin{bmatrix} 5 & 6 & 3 \\ 2 & 5 & 9 \\ 7 & 1 & 8 \end{bmatrix} + 2 \begin{bmatrix} 1 & 6 & 9 \\ 7 & 9 & 5 \\ 2 & 4 & 3 \end{bmatrix} = \begin{bmatrix} 165 & 38 & 279 \\ 304 & 194 & 67 \\ 159 & 249 & 218 \end{bmatrix}
\]

\( \hat{\mathcal{M}}_{\vec{a}} = \hat{\mathcal{K}}(\vec{v})^\vec{a} * \vec{u} * \hat{\mathcal{K}}(\vec{v})^\vec{b} \)

Then, suppose that Minal, after receiving \( \vec{a}, \vec{b}, \vec{v}, \vec{u} \) and \( \hat{\mathcal{M}}_{\vec{a}} \) from Mamta, choose a different isopolynomial \( \hat{\mathcal{F}}(\vec{r}) = 2\vec{r}^2 + \vec{r} + \vec{2} \) and compute
\[
\hat{\mathcal{F}}(\vec{v}) = 2 \begin{bmatrix} 5 & 6 & 3 \\ 2 & 5 & 9 \\ 7 & 1 & 8 \end{bmatrix} + \begin{bmatrix} 5 & 6 & 3 \\ 2 & 5 & 9 \\ 7 & 1 & 8 \end{bmatrix} = \begin{bmatrix} 286 & 309 & 189 \\ 94 & 175 & 16 \end{bmatrix}
\]

\( \hat{\mathcal{M}}_{\vec{L}} = \hat{\mathcal{F}}(\vec{v})^\vec{a} * \vec{u} * \hat{\mathcal{F}}(\vec{v})^\vec{b} \)

Then, she refers \( \hat{\mathcal{M}}_{\vec{L}} \) to Minal.

At the end, Mamta derived the session key as
\[
\hat{R}_{\text{Mamta}} = \hat{\mathcal{K}}(\vec{v})^\vec{a} * \hat{\mathcal{M}}_{\vec{L}} * \hat{\mathcal{K}}(\vec{v})^\vec{b} = \begin{bmatrix} 138 & 218 & 167 \\ 294 & 127 & 282 \\ 317 & 29 & 153 \end{bmatrix}
\]

While Minal derives the session key as
\[
\hat{R}_{\text{Minal}} = \hat{\mathcal{F}}(\vec{v})^\vec{a} * \hat{\mathcal{M}}_{\vec{a}} * \hat{\mathcal{F}}(\vec{v})^\vec{b} = \begin{bmatrix} 275 & 173 & 27 \\ 94 & 175 & 16 \end{bmatrix}
\]

Seemingly, \( \hat{R}_{\text{Mamta}} = \hat{R}_{\text{Minal}} \) holds.
5. Conclusion

Lately certain promising $\mathcal{K}ep$ have been created on non-commutative groups like; braid groups, Thompson’s groups, etc. In present endeavor we have suggested the new $\mathcal{K}ep$ which is based on Santilli’s isofields of the first kind is to use rings isopolynomials. It promotes further study due to isomathematical structure such as permutable permutation of the ring isopolynomials with the isonumber coefficient.

6. References

[1] Menezes A, Oorschot P, Van, and Vanstone S., 1997, “Handbook of Applied Cryptography”, Boca Raton, FL: CRC.
[2] Xiao D, Liao X, and Deng S, 2007, “A novel key agreement protocol based on chaotic maps”, Information Sciences, vol. 177, pp. 136-1142.
[3] Diffie W D and Hellman M E, 1976, “New directions in cryptography”, IEEE Transactions on Information Theory, vol. 22(6), pp. 644-654.
[4] McCarley K, 1990, “The discrete logarithm problem, Cryptology and Computational Number Theory”, Proceedings of Symposia in Applied Mathematics, vol. 42, pp.49-74.
[5] ElGamal T., 1985, “A public key cryptosystem and a signature scheme based on discrete logarithms”, IEEE Transactions on Information Theory, vol. 31, pp.469-472.
[6] Blake. Seroussi G, Smart N, 1999, “Elliptic Curves in Cryptography”, London Mathematical Society”, Lecture Notes. Series, 265, Cambridge University.
[7] Coppersmith D, Odlyzko A., Schroeppel R, 1986, “Discrete logarithms in GF(p)”, Algorithmica, pp.1-15.
[8] Alvarez R, Tortosa L, Vicent J F and Zamora A, 2009, “Analysis and design of a secure key exchange scheme”, Information Sciences, vol. 179, pp. 2014-2021.
[9] Climent J, Ferrandez F, Vicent J and Zamora A, 2006, “A nonlinear elliptic curve cryptosystem based on matrices”, Applied Mathematics and Computation, vol. 174, pp. 150-164.
[10] Alvarez R, Tortosa L, Vicent J F and Zamora A, 2009, “A non-abelian group basedon block upper triangular matrices with cryptographic applications”, Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes, Lecture Notes in Computer Science, Springer-Verlag, Berlin, vol. 5527, pp. 117-126.
[11] Meshram C, 2011, “A Cryptosystem based on Double Generalized Discrete Logarithm Problem”, International Journal of Contemporary Mathematical Sciences, vol. 6(6), pp. 285 – 297.
[12] Meshram C and Meshram S A, 2011, “A Public Key Cryptosystem based on IFP and DLP”; International Journal of Advanced Research in Computer Science, vol. 2(5), pp. 616-619.
[13] Meshram C and Agrawal S S, 2010, “Enhancing the security of A Public key cryptosystem based on DLP $\gamma \equiv a\alpha b\beta (mod\ p)$”, International Journal of Research and Reviews in Computer Science vol.1(4), pp.67-70.
[14] Meshram C and Meshram S A, 2013, “ PKC Scheme Based on DDLP”; International Journal of Information & Network Security (IJINS), vol.2 (2), pp. 154-159.
[15] Meshram C, Obaidat M S and Meshram A, 2020, “New efficient QERPKC based on partial discrete logarithm problem”, International Conference on Computer, Information and Telecommunication Systems (CITS), Hangzhou, China, pp. 1-5, doi: 10.1109/CITS49457.2020.9232533.
[16] Meshram A, Meshram C and Khobragade N. W., 2017, “An IND-CPA secure PKC technique based on dihedral group”, Indian Journal of Computer Science and Engineering (ICSE), vol. 8(2), pp.88-94.
[17] Meshram A, Meshram C and Khobragade N. W., 2017, “An IND-CCA2 secure public key cryptographic protocol using suzuki 2-group”, Indian Journal of Science and Technology, vol. 10(12), pp.01-08.
[18] Meshram A, Meshram C and Khobragade N. W., 2017, “Public key cryptographic technique based on suzuki 2-group”, International Journal of Advanced Research in Computer Science, vol. 8 (03), pp.300-305.
[19] Meshram A, Meshram C, Bagde S D and Meshram R R, 2020, “RIPIC based key exchange protocol”, Advances in Mathematics: Scientific Journal, vol. 9 (12), pp. 11169–11177. doi: https://doi.org/10.37418/amsj.9.12.97
[20] Jiang C X, 2002, “Foundations of Santillis Isonumber Theory with Applications”, ISBN 1-57485-056-3, Hadronic Press.