ADV MATH SCI JOURNAL
Advances in Mathematics: Scientific Journal **10** (2021), no.2, 1131–1139
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.10.2.39

AN EFFICIENT KEY EXCHANGE SCHEME USING SANTILLI'S ISOFIELDS SECOND-KIND FOR SECURE COMMUNICATION

Mamta S. Dani, Akshaykumar Meshram[1], Chandrashekhar Meshram, and N. M. Wazalwar

ABSTRACT. We intend to bring out a unique method for constructing key exchange scheme (KES) using Santilli's isofields second kind for safe transmission. The substantial idea of our offer KES is to utilized isopolynomials with general isonumber coefficient. Suggested KES is an unusual advantage for afore application as Santilli's isofields second kind framework permutable permutation of isocongruence and isoarirthmetic progressions.

1. INTRODUCTION, MOTIVATIONS AND ORGANIZATION

The framework for KES introduced by Diffie–Hellman, permits two users to simultaneously build a mutual private key over an unconfident mechanism [1]. At present, most of KES build on the number theory. The primary concerns on that the public key cryptography is design are discrete logarithm problem (DLP) [2, 3] along with the elliptic curve DLP [4, 5]. The methodically enumerable groups in which DLP structure plays are a fundamental part in cryptosystem [6]. Various implementations of the Diffie-Hellman procedure in matrix rings and diversity of matrices are suggested in [7, 8]. Various cryptographic schemes constructed on DLP and double DLP proposed in [9–12,

[1]*corresponding author*

2020 *Mathematics Subject Classification.* 16L30, 94A60.

Key words and phrases. Isopolynomials, isoproduct, isofields and diffie-hellman problem.

Submitted: 01.02.2021; *Accepted:* 20.02.2021; *Published:* 27.02.2021.

16]. Dihedral group and Suzuki-2 group based cryptosystem which are secure against chosen-plaintext-attack, ciphertext-indistinguishability-attack and adaptive-chosen-ciphertext-attack in random oracle model offered in [13–15]. Lately, Meshram A. [17] presented KES based on isonumbers.

The current work concentrate on a particular procedure for design a KES build on the Santilli's isofields of the second kind to make use of isounit is an element of the original field. This paper is structured as follow. In part 3, we confer the relevant background. In part 4, we present Santilli's isofields of the second kind based KES. Lastly, paper is accomplished in part 5.

2. Mathematical Definitions and Associated Data

In this part, we describes mathematical definitions such as arthmatic operation in morden mathematics, arthmatic operation in Santilli's isomathematics, Santilli's isofields of the second kind, Diffie-Hellman Problem (DHP), Symmetrical Decomposition Problem (SDP) over ring $\widehat{\mathcal{F}}$.

2.1. **Modern Mathematics:** Arithmetic operations with "0" an additive unity and "1" an multiplicative unity define as:

$\alpha + 0 = 0 + \alpha = \alpha$, $\alpha - 0 = \alpha, 0 - \alpha = -\alpha$, $\alpha \times 1 = 1 \times \alpha = \alpha$,

$\alpha \times \beta = \alpha\beta$, $\alpha \div 1 = \alpha$, $1 \div \alpha = \frac{1}{\alpha}$, $\alpha \div \beta = \frac{\alpha}{\beta}$,

with $\alpha^{(0)} = 1$ and $\alpha^{(1)} = \alpha$.

2.2. **Santilli's Iso - mathematics:** The structure for iso - mathematics presented by Jiang [17] as follows:

- Iso-addition $(\widehat{+})$: $\alpha\widehat{+}\beta = \alpha + \widehat{0} + \beta$.
- Iso-subtraction $(\widehat{-})$: $\alpha\widehat{-}\beta = \alpha - \widehat{0} - \beta$.
- Iso-multiplication $(\widehat{\times})$: $\alpha\widehat{\times}\beta = \alpha\widehat{\Upsilon}\beta$.
- Iso-division $(\widehat{\div})$: $\alpha\widehat{\div}\beta = \left(\frac{\alpha}{\beta}\right)\widehat{\hbar}$.

Here, $\widehat{0}$ is called isozero and $\widehat{\Upsilon}$ is called inverse of isounit $\widehat{\hbar} \neq 1$ such that $\widehat{\Upsilon}\widehat{\hbar} = 1$.

2.3. **Santilli's isofields of the second kind $\widehat{\mathcal{F}} = \widehat{\mathcal{F}}(\alpha, +, \times)$.**

For all $\alpha \in \mathcal{F}$ not lifted to $\widehat{\alpha} = \alpha\widehat{\hbar}$ verify all the axioms of a field if and only if the isounit is an element of the original field, i.e. $\widehat{\hbar} = \frac{1}{\widehat{\Upsilon}} \in \mathcal{F}$. Then isoproduct is defined as $\alpha\widehat{\times}\beta = \alpha\widehat{\Upsilon}\beta \in \widehat{\mathcal{F}}$.

We then have the following isoproduct operations of second kind as:

•$\alpha^{\widehat{\hbar}} = \alpha, \alpha^{-\widehat{\hbar}} = \alpha^{-1}\widehat{\hbar}^2,\ \alpha^{\widehat{\hbar}} \mathbin{\widehat{\times}} \alpha^{-\widehat{\hbar}} = \alpha^{\widehat{0}} = \widehat{\hbar} = \widehat{\Upsilon}^{-1} \neq 1.$

•$\alpha^{\widehat{2}} = \alpha^2\widehat{\Upsilon}, \alpha^{-\widehat{2}} = \alpha^{-2}\widehat{\hbar}^3,\ \alpha^{\widehat{2}} \mathbin{\widehat{\times}} \alpha^{-\widehat{2}} = \alpha^{\widehat{0}} = \widehat{\hbar} = \widehat{\Upsilon}^{-1} \neq 1$, and so on.

In general,

•$\alpha^{\widehat{n}} = \alpha^n\widehat{\Upsilon}^{n-1}, \alpha^{-\widehat{n}} = \alpha^{-n}\widehat{\hbar}^{n+1},\ \alpha^{\widehat{n}} \mathbin{\widehat{\times}} \alpha^{-\widehat{n}} = \alpha^{\widehat{0}} = \widehat{\hbar} = \widehat{\Upsilon}^{-1} \neq 1.$

•$\alpha^{\widehat{1/2}} = \alpha^{1/2}(\widehat{\hbar})^{1/2}, \alpha^{-\widehat{1/2}} = \alpha^{-1/2}(\widehat{\hbar})^{3/2},\ \alpha^{\widehat{1/2}} \mathbin{\widehat{\times}} \alpha^{-\widehat{1/2}} = \alpha^{\widehat{0}} = \widehat{\hbar} = \widehat{\Upsilon}^{-1} \neq 1.$

•$\alpha^{\widehat{1/3}} = \alpha^{1/3}(\widehat{\hbar})^{2/3}, \alpha^{-\widehat{1/3}} = \alpha^{-1/3}(\widehat{\hbar})^{4/3},\ \alpha^{\widehat{1/3}} \mathbin{\widehat{\times}} \alpha^{-\widehat{1/3}} = \alpha^{\widehat{0}} = \widehat{\hbar} = \widehat{\Upsilon}^{-1} \neq 1,$ and so on.

In general,

•$\alpha^{\widehat{1/n}} = \alpha^{1/n}(\widehat{\hbar})^{1-\frac{1}{n}}, \alpha^{-\widehat{1/n}} = \alpha^{-1/n}(\widehat{\hbar})^{1+\frac{1}{n}},\ \alpha^{\widehat{1/n}} \mathbin{\widehat{\times}} \alpha^{-\widehat{1/n}} = \alpha^{\widehat{0}} = \widehat{\hbar} = \widehat{\Upsilon}^{-1} \neq 1.$

•$\alpha^{\widehat{\gamma/\beta}} = \alpha^{\gamma/\beta}(\widehat{\hbar})^{1-\frac{\gamma}{\beta}}, \alpha^{-\widehat{\gamma/\beta}} = \alpha^{-\gamma/\beta}(\widehat{\hbar})^{1+\frac{\gamma}{\beta}},\ \alpha^{\widehat{\gamma/\beta}} \mathbin{\widehat{\times}} \alpha^{-\widehat{\gamma/\beta}} = \alpha^{\widehat{0}} = \widehat{\hbar} = \widehat{\Upsilon}^{-1} \neq 1.$

•$\alpha^{\widehat{\beta}} = \alpha^{\beta}(\widehat{\hbar})^{1-\beta} = \alpha^{\beta}(\widehat{\Upsilon})^{1-\beta}, \alpha^{-\widehat{\beta}} = \alpha^{-\beta}(\widehat{\hbar})^{1+\beta},\ \alpha^{\widehat{\beta}} \mathbin{\widehat{\times}} \alpha^{-\widehat{\beta}} = \alpha^{\widehat{0}} = \widehat{\hbar} = \widehat{\Upsilon}^{-1} \neq 1.$

•$\alpha^{\widehat{\hbar}} \mathbin{\widehat{\times}} \alpha^{\widehat{\hbar}} = \alpha\widehat{\Upsilon}\beta,\ \alpha^{\widehat{\hbar}} \mathbin{\widehat{\times}} \alpha^{-\widehat{\hbar}} = \alpha\beta^{-1}\widehat{\hbar}.$

In the first instance, scale isomultiplication notion over $\widehat{\mathcal{F}}$ define as follows:

I. $(\widehat{\lambda})\widehat{\mu} \triangleq (-\widehat{\lambda})(-\widehat{\mu}) = \underbrace{(-\widehat{\mu}) + (-\widehat{\mu}) + (-\widehat{\mu}) + ... + (-\widehat{\mu})}_{-\widehat{\lambda} \text{ times}}, \widehat{\lambda} \in \mathbb{Z} < \widehat{0}.$

II. $(\widehat{\lambda})\widehat{\mu} \triangleq \underbrace{\{\widehat{\mu} + \widehat{\mu} + \widehat{\mu} + ... + \widehat{\mu}\}}_{\widehat{\lambda} \text{ times}}, \widehat{\lambda} \in \mathbb{Z} < \widehat{0}.$

III. $(\widehat{\lambda})\widehat{\mu} = \widehat{0},\ \widehat{\lambda} = \widehat{0}.$

Case-I: For isonumber $\widehat{\amalg}, \overset{\frown}{\surd}, \widehat{\sqcup}, \widehat{\int} \in \mathbb{Z}$, we have $(\widehat{\amalg})\ \widehat{\mu}^{\widehat{\sqcup}} * (\overset{\frown}{\surd})\ \widehat{\mu}^{\widehat{\int}} = (\widehat{\amalg}\ \overset{\frown}{\surd})\ \widehat{\mu}^{\widehat{\sqcup}+\widehat{\int}} = (\overset{\frown}{\surd})\widehat{\mu}^{\widehat{\int}} * (\widehat{\amalg})\ \widehat{\mu}^{\widehat{\sqcup}}, \forall\ \widehat{\mu} \in \widehat{\mathcal{F}}.$

By utilizing definition of scale isomultiplication, the distributivity of isomultiplication with respect to isoaddition, and commutativity of isoaddition, we can conclude the above statement.

Case-II: For distinct $\widehat{\lambda}$ and $\widehat{\mu}$ we have $(\widehat{\amalg})\ \widehat{\mu} * (\overset{\frown}{\surd})\ \widehat{\lambda} \neq (\overset{\frown}{\surd})\ \widehat{\lambda} * (\widehat{\amalg})\ \widehat{\mu}.$

Let us define for isonumber $\widehat{\mu}$ in $\widehat{\mathcal{F}}$, we have $\widehat{\mathfrak{h}}(\widehat{\mu}) = \sum_{|=0}^{\widehat{\int}}(\widehat{\amalg_|})\widehat{\mu}^| = (\widehat{\amalg_0}) + (\widehat{\amalg_1})\widehat{\mu} + ... + (\widehat{\amalg_{\widehat{\int}}})\widehat{\mu}^{\widehat{\int}} \in \widehat{\mathcal{F}}$ for an isopolynomial with positive isointegral coefficient $\widehat{\mathfrak{h}}(\widehat{\updownarrow}) = \widehat{\amalg_0} + \widehat{\amalg_1}\widehat{\updownarrow} + ... + \widehat{\amalg_J}\widehat{\updownarrow}_J \in \mathbb{Z}^+[\widehat{\updownarrow}]$. Furthermore, $\widehat{\mathfrak{h}}(\widehat{\mu})$ is an isopolynomial about variable $\widehat{\mu}, \forall\ \widehat{\mu} \in \widehat{\mathcal{F}}$ then $\widehat{\mathfrak{h}}(\widehat{\mu}) \in \mathbb{Z}^+[\widehat{\mu}]$. Where $\mathbb{Z}^+[\widehat{\mu}]$ is an extension of $\mathbb{Z}^+$ with $\widehat{\mu}$. Consider $\widehat{\mathfrak{h}}(\widehat{\mu}) = \sum_{|=0}^{\widehat{\int}}(\widehat{\amalg_|})\widehat{\mu}^| \in \mathbb{Z}^+[\widehat{\mu}]$, $\widehat{\mathfrak{f}}(\widehat{\mu}) = \sum_{\|=0}^{\widehat{\sqcup}}(\overset{\frown}{\surd})\widehat{\mu}^| \in \mathbb{Z}^+[\widehat{\mu}]$ and $\widehat{\int} \geq \widehat{\sqcup}$,

then $\big(\sum_{|=0}^{\widehat{\int}}(\widehat{\amalg}_{|})\widehat{\mu}^{|}\big)+\big(\sum_{\|=0}^{\widehat{\sqcup}}(\widehat{\bigvee}^{\|})\widehat{\mu}^{\|}\big)=\big(\sum_{|=0}^{\widehat{\sqcup}}(\widehat{\amalg}_{|}+\widehat{\bigvee}^{|})\widehat{\mu}^{|}\big)+\big(\sum_{|=\widehat{\sqcup}+1}^{\widehat{\int}}(\widehat{\amalg}_{|})\widehat{\mu}^{|}\big)$, by utilizing case-I along with isodistributivity and $\widehat{\exists}_{|}=\sum_{\|=0}^{\widehat{|}}\widehat{\amalg}_{|}\widehat{\bigvee}^{|-\|}=\sum_{\|+\lambda=|}\widehat{\amalg}_{|}\widehat{\bigvee}^{\lambda}$, we get $(\sum_{|=0}^{\sqcup+1}\widehat{\exists}_{|}\widehat{\mu}^{|})=(\sum_{|=0}^{\int}(\widehat{\}}_{|})\widehat{\mu}^{|})*(\sum_{\|=0}^{\sqcup}(\widehat{\bigvee}^{\|})\widehat{\mu}^{|})$ Consequently, we accomplish the successive case-III conferring to case-I.

Case-III: We have $\widehat{\mathfrak{b}}(\widehat{\mu})*\widehat{\mathfrak{f}}(\widehat{\mu})=\widehat{\mathfrak{f}}(\widehat{\mu})*\widehat{\mathfrak{b}}(\widehat{\mu}),\forall\,\widehat{\mathfrak{b}}(\widehat{\mu}),\widehat{\mathfrak{f}}(\widehat{\mu})\in\mathbb{Z}^{+}[\widehat{\mu}]$.
As usual, $\widehat{\mathfrak{b}}(\widehat{\mu})*\widehat{\mathfrak{f}}(\widehat{\lambda})\neq\widehat{\mathfrak{f}}(\widehat{\lambda})*\widehat{\mathfrak{b}}(\widehat{\mu})$ for $\widehat{\mu}\neq\widehat{\lambda}$. Assume ring isopolynomial with isonumber coefficient $(\widehat{\mathcal{F}},+,*)$, for each conjecturally select isonumber $\widehat{\dagger}\in\widehat{\mathcal{F}}$, we define a set $\widehat{\mathcal{D}\dagger}\subseteq\widehat{\mathcal{F}}$ by $\widehat{\mathcal{D}\dagger}\triangleq\{\widehat{\mathfrak{b}}(\widehat{\dagger}):\widehat{\mathfrak{b}}(\widehat{\mu})\in\mathbb{Z}^{+}[\widehat{\mu}]\}$

2.4. **SDP over Ring $\widehat{\mathcal{F}}$ with isopolynomial :** Numerate $\widehat{\xi}\in\widehat{\mathcal{D}\dagger}$ such that $\widehat{\updownarrow}=\widehat{\xi}^{\widehat{\sqcup}}\,\widehat{\mu}\,\widehat{\xi}^{\widehat{\int}}$ for $\widehat{\sqcup},\widehat{\int}\in\mathbb{Z},(\widehat{\sqcup},\widehat{\mu},\widehat{\updownarrow})\in\widehat{\mathcal{F}}^{3}$.

2.5. **DHP over Ring $\widehat{\mathcal{F}}$ with isopolynomial :** For given $\widehat{\mu},\widehat{\mu}^{\widehat{\xi}_1}$ and $\widehat{\mu}^{\widehat{\xi}_2}$, numerate $\widehat{\mu}^{\widehat{\xi}_1\widehat{\xi}_2}$ (or $\widehat{\mu}^{\widehat{\xi}_2\widehat{\xi}_1}$), $\widehat{\mu}\in\widehat{\mathcal{F}},\ \widehat{\xi}_1,\widehat{\xi}_2\in\widehat{\mathcal{D}\dagger}$.

3. KES USING SANTILLI'S ISOFIELDS SECOND - KIND

Promptly, We contemplate the ring isopolynomial with the isonumber coefficient as an fundamental structure to set up a KES where two clients, say Hirabai and Aakansha, who come to an agree to share a classified session key over the unsecured unstable channel.

The algorithm is stated as follow:

(i) Hirabai specify pair of two random positive isointegers $\widehat{\sqcup},\widehat{\int}\in\mathbb{Z}^{+}$ and pair of two random elements $\widehat{\amalg},\widehat{\bigvee}\in\widehat{\mathcal{F}}$ to Aakansha.
(ii) Hirabai prefer a conjecturally isopolynomial $\widehat{\mathfrak{b}}(\widehat{\mu})\in\mathbb{Z}^{+}[\widehat{\mu}]$ such that $\widehat{\mathfrak{b}}(\widehat{\amalg})\neq\widehat{0}$ and then proceed $\widehat{\mathfrak{b}}(\widehat{\amalg})$ as her classified key.
(iii) Aakansha prefer a conjecturally isopolynomial $\widehat{\mathfrak{f}}(\widehat{\mu})\in\mathbb{Z}^{+}[\widehat{\mu}]$ such that $\widehat{\mathfrak{f}}(\widehat{\amalg})\neq\widehat{0}$ and then proceed $\widehat{\mathfrak{f}}(\widehat{\sqcup})$ as her classified key.
(iv) Hirabai numerate $\mathcal{H}=\widehat{\mathfrak{b}}(\widehat{\amalg})^{\widehat{\sqcup}}*\widehat{\amalg}*\widehat{\mathfrak{b}}(\widehat{\amalg})^{\widehat{\int}}$ and refers $\mathcal{H}$ to Aakansha.
(v) Aakansha numerate $\mathcal{A}=\widehat{\mathfrak{f}}(\widehat{\amalg})^{\widehat{\sqcup}}*\widehat{\bigvee}*\widehat{\mathfrak{f}}(\widehat{\amalg})^{\widehat{\int}}$ and refers $\mathcal{A}$ to Hirabai.
(vi) Hirabai numerate $\widehat{\mathcal{K}}_{Hirabai}=\widehat{\mathfrak{b}}(\widehat{\amalg})^{\widehat{\sqcup}}*\mathcal{A}*\widehat{\mathfrak{b}}(\widehat{\amalg})^{\widehat{\int}}$ as the shared session key.
(vii) Aakansha numerate $\widehat{\mathcal{K}}_{Aakansha}=\widehat{\mathfrak{f}}(\widehat{\amalg})^{\widehat{\sqcup}}*\mathcal{H}*\widehat{\mathfrak{f}}(\widehat{\amalg})^{\widehat{\int}}$ as the shared session key.

The interpretation of the scheme is demonstrate in the following table.

Table. KES using Santilli's Isofields Second - Kind.

Pass	Hirabai $\rightleftharpoons$ Aakansha
	Pair of isointegers $\hat{t}, \hat{s} \in \hat{\mathbb{Z}}^{+}$ Pair of elements $\hat{q}, \hat{p} \in \hat{\mathcal{F}}$ Conjecturally isopolynomial $\hat{\mathfrak{h}}(\hat{\mu}) \in \hat{\mathbb{Z}}^{+}[\hat{\mu}]$
I	$\hat{t}, \hat{s}, \hat{q}, \hat{p}, \hat{\mathfrak{h}}(\hat{q})^{\hat{t}} \hat{p} \hat{\mathfrak{h}}(\hat{q})^{\hat{s}} \rightarrow$
	Choose at randomly $\hat{\mathfrak{f}}(\hat{\mu}) \in \hat{\mathbb{Z}}^{+}[\hat{\mu}]$
II	$\leftarrow \hat{\mathfrak{f}}(\hat{q})^{\hat{t}} \hat{p} \hat{\mathfrak{f}}(\hat{q})^{\hat{s}}$
	$\hat{\mathcal{K}}_{\text{Hirabai}} = \hat{\mathfrak{h}}(\hat{q})^{\hat{t}} \hat{\mathfrak{f}}(\hat{q})^{\hat{t}} \hat{p} \hat{\mathfrak{f}}(\hat{q})^{\hat{s}} \hat{\mathfrak{h}}(\hat{q})^{\hat{s}}$ $= \hat{\mathfrak{f}}(\hat{q})^{\hat{t}} \hat{\mathfrak{h}}(\hat{q})^{\hat{t}} \hat{p} \hat{\mathfrak{h}}(\hat{q})^{\hat{s}} \hat{\mathfrak{f}}(\hat{q})^{\hat{s}} = \hat{\mathcal{K}}_{\text{Aakansha}}$

3.1. **Example: KES using Santilli's Isofields Second - Kind.**

Select an integer $\mathcal{N} = 17 * 19$, isounit $\hat{\hbar} = \begin{bmatrix} 1 & 7 & 5 \\ 8 & 6 & 2 \\ 3 & 5 & 9 \end{bmatrix}$ and its inverse of isounit $\hat{\Upsilon} = \begin{bmatrix} \frac{-1}{7} & \frac{19}{154} & \frac{4}{77} \\ \frac{3}{14} & \frac{3}{154} & \frac{-19}{154} \\ \frac{-1}{14} & \frac{-4}{77} & \frac{25}{154} \end{bmatrix}$. Presume that Hirabai prefer $\hat{\square} = \hat{\in}, \hat{\int} = \hat{\ni}$, $\hat{\amalg} = \begin{bmatrix} 5 & 6 & 3 \\ 2 & 5 & 9 \\ 7 & 1 & 8 \end{bmatrix}, \hat{\surd} = \begin{bmatrix} 1 & 6 & 9 \\ 7 & 9 & 5 \\ 2 & 4 & 3 \end{bmatrix}$ and $\hat{\mathfrak{h}}(\hat{\mu}) = \hat{3}\hat{\mu}^{3} + \hat{2}\hat{\mu}^{2} + \hat{\mu} + \hat{2}$. She numerate: $\hat{\mathfrak{h}}(\hat{\amalg}) = \hat{3} \begin{bmatrix} 5 & 6 & 3 \\ 2 & 5 & 9 \\ 7 & 1 & 8 \end{bmatrix}^{\hat{3}} + \hat{2} \begin{bmatrix} 1 & 6 & 9 \\ 7 & 9 & 5 \\ 2 & 4 & 3 \end{bmatrix}^{\hat{2}} + \begin{bmatrix} 5 & 6 & 3 \\ 2 & 5 & 9 \\ 7 & 1 & 8 \end{bmatrix} + \hat{2} \begin{bmatrix} 5 & 6 & 3 \\ 2 & 5 & 9 \\ 7 & 1 & 8 \end{bmatrix} \hat{\mathfrak{h}}(\hat{\amalg}) = \begin{bmatrix} 36578 & 61046 & 63334 \\ 41198 & 71962 & 73626 \\ 41428 & 68656 & 68428 \end{bmatrix} \mod 323$, $\hat{\mathfrak{h}}(\hat{\amalg}) = \begin{bmatrix} 79 & 322 & 26 \\ 177 & 256 & 305 \\ 84 & 180 & 275 \end{bmatrix}$ and $\mathcal{H} = \hat{\mathfrak{h}}(\hat{\amalg})^{\hat{\square}} * \hat{\surd} * \hat{\mathfrak{h}}(\hat{\amalg})^{\hat{\int}}$,

$$\mathcal{H} = \begin{bmatrix} 79 & 322 & 26 \\ 177 & 256 & 305 \\ 84 & 180 & 275 \end{bmatrix}^{\widehat{2}} * \begin{bmatrix} 1 & 6 & 9 \\ 7 & 9 & 5 \\ 2 & 4 & 3 \end{bmatrix} * \begin{bmatrix} 79 & 322 & 26 \\ 177 & 256 & 305 \\ 84 & 180 & 275 \end{bmatrix}^{\widehat{3}} = \begin{bmatrix} 165 & 38 & 279 \\ 304 & 194 & 67 \\ 159 & 249 & 218 \end{bmatrix}.$$

Then, she indicate $\widehat{\square}, \widehat{f}, \widehat{\amalg}, \widehat{\surd}$ and $\mathcal{H}$ to Aakansha. Now, assume that Aakansha, after getting $\widehat{\square}, \widehat{f}, \widehat{\amalg}, \widehat{\surd}$ and $\mathcal{H}$ from Hirabai, select a another isopolynomial $\widehat{\mathfrak{f}}(\widehat{\mu}) = \widehat{2}\widehat{\mu}^2 + \widehat{\mu} + \widehat{2}$ and numerate

$$\widehat{\mathfrak{f}}(\widehat{\amalg}) = \widehat{2} \begin{bmatrix} 5 & 6 & 3 \\ 2 & 5 & 9 \\ 7 & 1 & 8 \end{bmatrix}^{\widehat{2}} + \begin{bmatrix} 5 & 6 & 3 \\ 2 & 5 & 9 \\ 7 & 1 & 8 \end{bmatrix} + \widehat{2} \begin{bmatrix} 5 & 6 & 3 \\ 2 & 5 & 9 \\ 7 & 1 & 8 \end{bmatrix}, \quad \widehat{\mathfrak{f}}(\widehat{\amalg}) = \begin{bmatrix} 275 & 173 & 27 \\ 286 & 309 & 189 \\ 94 & 175 & 16 \end{bmatrix}.$$

Further,

$$\mathcal{A} = \widehat{\mathfrak{f}}(\widehat{\amalg})^{\widehat{\square}} * \widehat{\surd} * \widehat{\mathfrak{f}}(\widehat{\amalg})^{\widehat{f}} = \begin{bmatrix} 275 & 173 & 27 \\ 286 & 309 & 189 \\ 94 & 175 & 16 \end{bmatrix}^{\widehat{2}} * \begin{bmatrix} 1 & 6 & 9 \\ 7 & 9 & 5 \\ 2 & 4 & 3 \end{bmatrix} * \begin{bmatrix} 275 & 173 & 27 \\ 286 & 309 & 189 \\ 94 & 175 & 16 \end{bmatrix}^{\widehat{3}}$$

$$\mathcal{A} = \begin{bmatrix} 53 & 267 & 173 \\ 264 & 187 & 27 \\ 37 & 251 & 82 \end{bmatrix}.$$

Then, she indicate $\mathcal{A}$ to Hirabai. At the end, Hirabai numerate the session key as

$$\widehat{\mathcal{K}}_{Hirabai} = \widehat{\mathfrak{h}}(\widehat{\amalg})^{\widehat{\square}} * \mathcal{A} * \widehat{\mathfrak{h}}(\widehat{\amalg})^{\widehat{f}}$$

$$\widehat{\mathcal{K}}_{Hirabai} = \begin{bmatrix} 79 & 322 & 26 \\ 177 & 256 & 305 \\ 84 & 180 & 275 \end{bmatrix}^{\widehat{2}} * \begin{bmatrix} 53 & 267 & 173 \\ 264 & 187 & 27 \\ 37 & 251 & 82 \end{bmatrix} * \begin{bmatrix} 79 & 322 & 26 \\ 177 & 256 & 305 \\ 84 & 180 & 275 \end{bmatrix}^{\widehat{3}}$$

$$= \begin{bmatrix} 138 & 218 & 167 \\ 294 & 127 & 282 \\ 317 & 29 & 153 \end{bmatrix},$$

while Aakansha numerate the session key as

$$\widehat{\mathcal{K}}_{Aakansha} = \widehat{\mathfrak{f}}(\widehat{\Pi})^{\widehat{\square}} * \mathcal{H} * \widehat{\mathfrak{f}}(\widehat{\Pi})^{\widehat{f}}$$

$$\widehat{\mathcal{K}}_{Aakansha} = \begin{bmatrix} 275 & 173 & 27 \\ 286 & 309 & 189 \\ 94 & 175 & 16 \end{bmatrix}^{\widehat{2}} * \begin{bmatrix} 165 & 38 & 279 \\ 304 & 194 & 67 \\ 159 & 249 & 218 \end{bmatrix} * \begin{bmatrix} 275 & 173 & 27 \\ 286 & 309 & 189 \\ 94 & 175 & 16 \end{bmatrix}^{\widehat{3}}$$

$$= \begin{bmatrix} 138 & 218 & 167 \\ 294 & 127 & 282 \\ 317 & 29 & 153 \end{bmatrix}.$$

Allegedly, $\widehat{\mathcal{K}}_{Hirabai} = \widehat{\mathcal{K}}_{Aakansha}$ holds.

4. Conclusion

In recent times few promising KES have been design on braid groups, Thompson's groups, etc. In this artical, we have proposed the unique KES which is based on Santilli's isofields of the second - kind is to utilized isopolynomials with general isonumber coefficient. It benefit ahead perusal in view of Santilli's isofields of the second - kind framework like permutable permutation of isonumber.

References

[1] W. D. Diffie and M. E. Hellman: *New directions in cryptography*, IEEE Transactions on Information Theory, **22(6)**(1976), 644—654.

[2] K. McCurley : *The discrete logarithm problem, Cryptology and Computational Number Theory*, Proceedings of Symposia in Applied Mathematics, **42**(1990), 49—74.

[3] T. ElGamal : *A public key cryptosystem and a signature scheme based on discrete logarithms*, IEEE Transactions on Information Theory, **31**(1985), 469—472.

[4] Blake, G. Seroussi and N. Smart : *Elliptic Curves in Cryptography*, London Mathematical Society, Lecture Notes. Series, Cambridge University, **265**(1999).

[5] D. Coppersmith, A. Odlyzko and R. Schroeppel : *Discrete logarithms in GF(p)*, Algorithmica, **265**(1986), 1–15.

[6] R. Alvarez, L. Tortosa, J. F. Vicent and A. Zamora : *Analysis and design of a secure key exchange scheme*, Information Sciences, **179**(2009), 2014–2021.

[7] J. Climent, F. Ferrandez, J. Vicent and A. Zamora : *A nonlinear elliptic curve cryptosystem based on matrices*, Applied Mathematics and Computation, **174**(2006), 150–164.

[8] R. ALVAREZ, L. TORTOSA, J. F. VICENT AND A. ZAMORA : *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, pages. Springer-Verlag, Berlin, **5527**(2009), 117–126.

[9] C. MESHRAM : *A Cryptosystem based on Double Generalized Discrete Logarithm Problem*, International Journal of Contemporary Mathematical Sciences, **6(6)**(2011), 285 – 297.

[10] C. MESHRAM AND S. A. MESHRAM: *A Public Key Cryptosystem based on IFP and DLP*, International Journal of Advanced Research in Computer Science, **2 (5)**(2011), 616-619.

[11] C. MESHRAM AND S. S. AGRAWAL: *Enhancing the security of A Public key cryptosystem based on DLP* $\gamma \equiv \alpha a \beta b(modp)$, International Journal of Research and Reviews in Computer Science, **1 (4)**(2010), 67-70.

[12] C. MESHRAM AND S. A. MESHRAM: *PKC Scheme Based on DDLP*, International Journal of Information & Network Security (IJINS), **2 (2)**(2013), 154-159.

[13] A. MESHRAM, C. MESHRAM AND N. W. KHOBRAGADE : *An IND-CPA secure PKC technique based on dihedral group*, Indian Journal of Computer Science and Engineering (IJCSE), **8(2)**(2017), 88-94.

[14] A. MESHRAM, C. MESHRAM AND N. W. KHOBRAGADE : *An IND-CCA2 secure public key cryptographic protocol using suzuki 2-group*, Indian Journal of Science and Technology, **10(12)**(2017), 01-08.

[15] A. MESHRAM, C. MESHRAM AND N. W. KHOBRAGADE : *Public key cryptographic technique based on suzuki 2-group*, International Journal of Advanced Research in Computer Science, **8 (03)**(2017), 300-305.

[16] C. MESHRAM, M. S. OBAIDAT AND S. A. MESHRAM : *New efficient QERPKC based on partial discrete logarithm problem*, International Conference on Computer, Information and Telecommunication Systems (CITS), Hangzhou, China, (2020), 1-5,doi: 10.1109/CITS49457.2020.9232533.

[17] A. MESHRAM, C. MESHRAM, S. D. BAGDE AND R. R. MESHRAM : *RIPIC based key exchange protocol*, Advances in Mathematics: Scientific Journal, **9 (12)** (2020),11169–11177.
doi: https://doi.org/10.37418/amsj.9.12.97 (2020).

[18] C. X. JIANG : *Foundations of Santillis Isonumber Theory with Applications*, ISBN, Hadronic Press, (2002), 1-57485-056-3.

Department of Applied Mathematics,
Yeshwantrao Chavan College of Engineering,
Nagpur, M.S. 441110, India.
Email address: milinddandale@gmail.com

Department of Applied Mathematics,
Yeshwantrao Chavan College of Engineering,
Nagpur, M.S. 441110, India.
Email address: akshaykjmeshram@gmail.com

Department of Post Graduate Studies and Research in Mathematics,
Jayawanti Haksar Government Post Graduation College,
College of Chhindwara University, Betul, M.P. 460001, India
Email address: cs_meshram@rediffmail.com

Department of Statistics,
Rashtrasant Tukadoji Maharaj Nagpur University,
Nagpur, M.S., India.
Email address: neha-wazalwar@yahoo.co.in