# Isonumber based Iso-Key Interchange Protocol for Network Communication

**Mamta S. Dani[1], Akshaykumar Meshram[2*], Rupesh Pohane[3] and Rupali R. Meshram[4]**

**Corresponding Author: akshaykjmeshram@gmail.com*

[1, 2,*]Department of Applied Mathematics, Yeshwantrao Chavan College of Engineering, Nagpur-441110, M.S., India

[3]Department of Applied Mathematics, Suryodaya College of Engineering and Technology, Nagpur-440027, M.S., India

[4]Department of Mathematics, Kamla Nehru Mahavidyalaya, Nagpur-440024, M.S., India

**Summary**

Key exchange protocol (KEP) is an essential setup to secure authenticates transmission among two or more users in cyberspace. Digital files protected and transmitted by the encryption of the files over public channels, a single key communal concerning the channel parties and utilized for both to encrypt the files as well as decrypt the files. If entirely done, this impedes unauthorized third parties from imposing a key optimal on the authorized parties. In this article, we have suggested a new KEP term as isokey interchange protocol based on generalization of modern mathematics term as isomathematics by utilizing isonumbers for corresponding isounits over the Block Upper Triangular Isomatrices (BUTI) which is secure, feasible and extensible. We also were utilizing arithmetic operations like Isoaddition, isosubtraction, isomultiplication and isodivision from isomathematics to build iso-key interchange protocol for network communication. The execution of our protocol is for two isointegers corresponding two elements of the group of isomatrices and cryptographic performance of products eachother. We demonstrate the protection of suggested isokey interchange protocol against Brute force attacks, Menezes et al. algorithm and Climent et al. algorithm.

***Keywords:***

*Cryptography, Block Isomatrix, Isomathematics, Isonumber, Isounit.*

## 1. Introduction

Now a days, the security is main concern in large open network. To set up a private channel among two users' needs to interchange a mutual secret key [2]. It is feasible in limited and small network but not possible in large and broad networks like internet. The public-key cryptography (PKC) offers a technique to permit secret session keys to be interchange over an unprotected network in which each user holds key pair comprising of a non-secret key and a secret key such that only non-secret keys are published in network. Diffie–Hellman offered first feasible PKC in 1976 [3]. Number theory problems are the attraction in cryptographic researcher to build prominent PKC in which at least two user, user-I utilize the user-II non-secret key and encrypts the information and then transmits to user-II. After getting the encrypted text, the user-II can decrypt the information with utilizing of his/her secret key [4].

Meshram C. [5-8] developed certain PKC schemes which are depends on solving discrete logarithm problem and integer factoring problem along with its generalization. Moreover offered specific designs for identity-based cryptography [09-15]. Blake I. and Climent J., independently study the Elliptic Curve discrete logarithm problem which is one of the main problems where PKC are constructed [16-17]. Meshram A. [18-20] proposed certain cryptographic schemes based on suzuki 2-group and dihedral group.

Recently, Meshram C. [21] introduce Quadratic Exponentiation Randomized PKC based on Partial Discrete Logarithm Problem. Meshram A. recommended $\mathcal{KEP}$ constructed on isoring isopolynomials coefficient [22]. Dani M. recommended $\mathcal{SISK}$ based $\mathcal{KEP}$ for protected transmission [23] and $\mathcal{KEP}$ based on $\mathcal{SIFK}$ [24]. Thatere A. recommended isoryptosystem constructed on $\mathcal{SIFK}$ [25].

## 2. Motivations and Organization

In this article, we have proposed an isokey interchange protocol based on isonumbers for corresponding isounits over $\mathcal{BUTI}$. The primary thought of this article is to examine, for two isointegers $\hat{a}$ and $\hat{b}$ with elements of the group of isomatrices $\hat{\mathcal{H}}_1$and $\hat{\mathcal{H}}_2$, the cryptographic performance of products of the nature $\hat{\mathcal{H}}_1^{\hat{a}}\hat{\mathcal{H}}_2^{\hat{b}}$.

The rest of the article is coordinated in various sections. In section 3, we have reviewed the prerequisite background for article. Section 4, describes the suggested isokey Interchange Protocol. Section 5, investigate the security analysis of suggested isokey Interchange Protocol. Finally, in section 6, we have concluded the article.

Manuscript received February 5, 2022
Manuscript revised February 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.2.27

## 3. Mathematical Background and Material

In this section, we have describes the definition such as Isomathematics, arithmetic operations in modern mathematics, arithmetic operations in Santilli's isomathematics, $\mathcal{BUTJ}$ and order of the elements.

### 3.1 Santilli's Isomathematics [26]

Isomathematics is a generalization of arithmetic operations in modern mathematics. Utilizing isomathematics, we have shown that, two multiplied by two is equal to twenty-eight (for inverse of isounit $\hat{\mathcal{T}} = 7$).

### 3.2 Operations in Modern Mathematics

Addition, subtraction, multiplication and division are arithmetic operations in modern mathematics. In modern mathematics, "0" and "1" are additive unity and multiplicative unity respectively such that

$\rho + 0 = \rho,$
$\rho - 0 = \rho,$
$\rho^0 = 1,$
$\rho \times 1 = 1 \times \rho = \rho,$
$\rho \div 1 = \rho,$
$1 \div \rho = \frac{1}{\rho},$
$\rho \times \sigma = \rho\sigma,$
$\rho \div \sigma = \frac{\rho}{\sigma}$ etc.

### 3.3 Operations in Santilli's Isomathematics

Isoaddition $\hat{+}$ , isosubtraction $\hat{-}$ , isomultiplication $\hat{\times}$ and isodivision $\hat{\div}$ are arithmetic operations in isomathematics and describe as follows;

$\rho \,\hat{+}\, \sigma = \rho + \hat{\mathcal{K}} + \sigma,$
$\rho \,\hat{-}\, \sigma = \rho - \hat{\mathcal{K}} - \sigma,$
$\rho \,\hat{\times}\, \sigma = \rho\hat{\mathcal{T}}\sigma,$ and
$\rho \,\hat{\div}\, \sigma = \left(\frac{\rho}{\sigma}\right)\hat{\mathcal{J}}.$

Where, $i)$ $\hat{\mathcal{T}}\hat{\mathcal{J}} = 1, \hat{\mathcal{T}}$ is called inverse of isounit $\hat{\mathcal{J}} \neq 1$ and ii) $\hat{\mathcal{K}}$ is called isozero.

### 3.4 $\mathcal{BUTJ}$

An isomatrices $\hat{\mathcal{H}}_{\hat{v}}(\mathcal{Z}_{\hat{q}})$ of size $v \,\hat{\times}\, v$, $\hat{\mathcal{H}}_{\hat{u}}(\mathcal{Z}_{\hat{q}})$ of size $u \,\hat{\times}\, u$ and $\hat{\mathcal{H}}_{\hat{u}\times\hat{v}}(\mathcal{Z}_{\hat{q}})$ of size $u \,\hat{\times}\, v$ for isoprime number $\hat{q}$ , isonumbers $\hat{u}, \hat{v} \in \mathcal{N}\left(\mathcal{Z}_{\hat{q}}\right)$ and invertible isomatrices $\mathcal{L}_{\hat{u}}(\mathcal{Z}_{\hat{q}})$ of size $u \,\hat{\times}\, u$ , $\mathcal{GL}_{\hat{v}}(\mathcal{Z}_{\hat{q}})$ of size $v \,\hat{\times}\, v$.

Define isomatrix $\hat{\mathrm{H}} = \left\{\begin{matrix} \hat{\alpha} & \hat{\gamma} \\ \hat{0} & \hat{\beta} \end{matrix}\right\},$

$$\hat{\alpha} \in \hat{\mathcal{H}}_{\hat{u}}(\mathcal{Z}_{\hat{q}}), \hat{\beta} \in \hat{\mathcal{H}}_{\hat{v}}(\mathcal{Z}_{\hat{q}}), \hat{\gamma} \in \hat{\mathcal{H}}_{\hat{u}}\, \hat{\mathcal{H}}_{\hat{u}\times\hat{v}}(\mathcal{Z}_{\hat{q}}),$$

with subset $\hat{\Theta} = \left\{\begin{matrix} \hat{\alpha} & \hat{\gamma} \\ \hat{0} & \hat{\beta} \end{matrix}\right\},$

$$\hat{\alpha} \in \mathcal{GL}_{\hat{u}}(\mathcal{Z}_{\hat{q}}) , \hat{\beta} \in \mathcal{GL}_{\hat{v}}(\mathcal{Z}_{\hat{q}}), \hat{\gamma} \in \hat{\mathcal{H}}_{\hat{u}}\, \hat{\mathcal{H}}_{\hat{u}\times\hat{v}}(\mathcal{Z}_{\hat{q}})$$

By utilizing property [28], we have compute isopowers of these $\mathcal{BUTJ}$ to find the order of the subgroup generated by a isomatrix $\hat{\mathcal{H}} \in \hat{\Theta}$.

For non negative isointeger $\hat{p}$ and isomatrix $\hat{\mathcal{H}} = \begin{bmatrix} \hat{\alpha} & \hat{\gamma} \\ \hat{0} & \hat{\beta} \end{bmatrix} \in \hat{\Theta},$

Define $\hat{\mathcal{H}}^{\hat{p}} = \begin{bmatrix} \hat{\alpha}^{\hat{p}} & \hat{\gamma}^{(\hat{p})} \\ \hat{0} & \hat{\beta}^{\hat{p}} \end{bmatrix}$, where

$$\hat{\gamma}^{(\hat{p})} = \begin{cases} 0 & if\ \hat{p}=0 \\ \sum_{j=1}^{\hat{p}} \hat{\alpha}^{\hat{p}-j}\hat{\gamma}\hat{\beta}^{j-1} & if\ \hat{p} \geq 1. \end{cases}$$

i) If $\hat{0} \leq \hat{d} \leq \hat{p}$ then $\hat{\gamma}^{(\hat{p})} - \hat{\alpha}^{\hat{d}}\hat{\gamma}^{(\hat{p}-\hat{d})} + \hat{\gamma}^{(\hat{d})}\hat{\beta}^{\hat{p}-\hat{d}}\hat{\gamma}^{(\hat{p})} = \hat{\alpha}^{(\hat{p}-\hat{d})}\hat{\gamma}^{(\hat{p})} + \hat{\gamma}^{(\hat{p}-\hat{d})}\hat{\beta}^{\hat{d}}$

ii) If $\hat{d} = 1$ then $\hat{\gamma}^{(\hat{p})} = \hat{\alpha}\hat{\gamma}^{(\hat{p}-1)} + \hat{\gamma}\hat{\beta}^{\hat{p}-1}$ or

$$\hat{\gamma}^{(\hat{p})} = \hat{\alpha}^{\hat{p}-1}\hat{\gamma} + \hat{\gamma}^{(\hat{p}-1)}\hat{\beta}$$

For isointegers $\hat{c}, \hat{e}$; define $\hat{c} + \hat{e} \geq \hat{0}$,

$$\hat{\gamma}^{(\hat{c}+\hat{e})} = \hat{\alpha}^{\hat{c}}\hat{\gamma}^{(\hat{e})} + \hat{\gamma}^{(\hat{c})}\hat{\beta}^{\hat{e}}.$$

### 3.5 Order of the elements

In this subsection [28-29], we have define the way to guarantee the maximum order of group generated by the isomatrix $\hat{\mathcal{H}} = \begin{bmatrix} \hat{\alpha} & \hat{\gamma} \\ \hat{0} & \hat{\beta} \end{bmatrix} \epsilon\ \hat{\Theta}$.

Suppose that monic isopolynomial

$$\hat{h}(\hat{y}) = \hat{c}_0 + \hat{c}_1\hat{y} + \cdots . + \hat{c}_{\hat{w}-1}\hat{y}^{\hat{w}-1} + \hat{y}^{\hat{w}} \in \mathcal{Z}_{\hat{q}}[\hat{\gamma}].$$

i) If $\hat{h} \in \mathcal{Z}_{\hat{q}}$ is an irreducible isopolynomial, then the order of the isomatrix $\overline{\hat{\alpha}}$ is identical to the order of any root of $\hat{h}$ in $\mathrm{F}_{\hat{q}^{\hat{w}}}$ and the order of $\overline{\hat{\alpha}}$ divides $\hat{q}^{\hat{w}} - 1$.

ii) If $\hat{h} \in \mathcal{Z}_{\hat{q}}$ is a primitive isopolynomial, the order of $\overline{\hat{\alpha}}$ is precisely $\hat{q}^{\hat{w}} - 1$.

To design of block isomatrices $\overline{\hat{\alpha}} = \begin{bmatrix} \overline{\hat{\alpha}_1} & \hat{0} & \hat{0} \\ \hat{0} & \overline{\hat{\alpha}_2} & \hat{0} \\ \hat{0} & \hat{0} & \overline{\hat{\alpha}_k} \end{bmatrix}$ suggested by Odoni et al. [30], for different primitive isopolynomials in $\mathcal{Z}_{\hat{q}}$ of degree $\hat{w}_j$ and $\overline{\hat{\alpha}}_j$ is the companion matrix of $\hat{h}_j$, and $\hat{h}_j$, for $j = 1, 2, \ldots, k$.

Since, order of each block $\overline{\hat{\alpha}}_{\mathrm{i}}$ is $\hat{q}^{\hat{w}_j} - 1$, so the order of $\overline{\hat{\alpha}}$ is lcm($\hat{q}^{\hat{w}_1} - 1, \hat{q}^{\hat{w}_2} - 1$ ,...., $\hat{q}^{\hat{w}_k} - 1$).

For companion isomatrices $\overline{\overline{\hat{\alpha}}, \overline{\hat{\beta}}}$ and

$\hat{h}(\hat{y}) = \hat{c}_0 + \hat{c}_1\hat{y} + \cdots . + \hat{c}_{\hat{u}-1}\hat{y}^{\hat{u}-1} + \hat{y}^{\hat{u}}$ ,
$\hat{f}(\hat{y}) = \hat{e}_0 + \hat{e}_1\hat{y} + \cdots . + \hat{e}_{\hat{v}-1}\hat{y}^{\hat{v}-1} + \hat{y}^{\hat{v}}$ be two primitive polynomials in $\mathcal{Z}_{\hat{q}}[\hat{\gamma}]$ . For two invertible

isomatrices $\hat{\mathcal{R}}$ and $\hat{\mathcal{S}}$ , define $\hat{\alpha} = \hat{\mathcal{R}}^{-1}\bar{\hat{\alpha}}\,\hat{\mathcal{R}}$ and $\hat{\beta} = \hat{\mathcal{S}}^{-1}\bar{\hat{\beta}}\,\hat{\mathcal{S}}$ such that the order of $\hat{\mathcal{H}}$ is lcm$(\hat{q}^{\hat{u}} - 1, \hat{q}^{\hat{v}} - 1)$.

## 4. Suggested Isonumber based Isokey Interchange Protocol

Suppose that $\hat{\mathcal{H}}_1 = \begin{bmatrix} \hat{\alpha}_1 & \hat{\gamma}_1 \\ \hat{0} & \hat{\beta}_1 \end{bmatrix} \in \hat{\Theta}$ with orders $\hat{z}_1$ and $\hat{\mathcal{H}}_2 = \begin{bmatrix} \hat{\alpha}_2 & \hat{\gamma}_2 \\ \hat{0} & \hat{\beta}_2 \end{bmatrix} \in \hat{\Theta}$ with orders $\hat{z}_2$, are two isometrix. For isonumbers $\hat{m}$; $\hat{n} \in \mathcal{N}$, define the following notation; $\hat{\alpha}_{\hat{m}\hat{n}} = \hat{\alpha}_1^{\hat{m}}\hat{\alpha}_2^{\hat{n}}$, $\hat{\beta}_{\hat{m}\hat{n}} = \hat{\beta}_1^{\hat{m}}\hat{\beta}_2^{\hat{n}}$, and
$\hat{\psi}_{\hat{m}\hat{n}} = \hat{\alpha}_1^{\hat{m}}\hat{\gamma}_2^{(\hat{n})} + \hat{\gamma}_1^{(\hat{m})}\hat{\beta}_2^{\hat{n}}$.

If two clients Taylor and Eileen wish to interchange an isokey, they may implement the following algorithm:

1) Taylor and Eileen consent on isounit $\hat{\mathcal{J}}$, $\hat{q} \in \mathcal{N}$, $\hat{\mathcal{H}}_1 \in \hat{\Theta}$ with orders $\hat{z}_1$ and $\hat{\mathcal{H}}_2 \in \hat{\Theta}$ with orders $\hat{z}_2$.

2) Taylor select two arbitrary isonumber $\hat{u}$; $\hat{v} \in \mathcal{N}$ such that $1 \leq \hat{u} \leq \hat{z}_1 - 1$ , $1 \leq \hat{v} \leq \hat{z}_2 - 1$.

And numerate $\hat{\alpha}_{\hat{u}\hat{v}}$ , $\hat{\beta}_{\hat{u}\hat{v}}$ , $\hat{\psi}_{\hat{u}\hat{v}}$ for constructing $\hat{\psi} = \begin{bmatrix} \hat{\alpha}_{\hat{u}\hat{v}} & \hat{\psi}_{\hat{u}\hat{v}} \\ \hat{0} & \hat{\beta}_{\hat{u}\hat{v}} \end{bmatrix}$.

(3) Taylor refers $\hat{\psi}$ to Eileen.

(4) Eileen select two arbitrary isonumber $\hat{a}, \hat{b} \in \mathcal{N}$ such that $1 \leq \hat{a} \leq \hat{z}_1 - 1$ , $1 \leq \hat{b} \leq \hat{z}_2 - 1$.

And numerate $\hat{\alpha}_{\hat{a}\hat{b}}$ , $\hat{\beta}_{\hat{a}\hat{b}}$ , $\hat{\psi}_{\hat{a}\hat{b}}$ for constructing $\hat{\chi} = \begin{bmatrix} \hat{\alpha}_{\hat{a}\hat{b}} & \hat{\psi}_{\hat{a}\hat{v}} \\ \hat{0} & \hat{\beta}_{\hat{a}\hat{b}} \end{bmatrix}$.

(5) Eileen refers $\hat{\chi}$ to Taylor.

(6) Then the isomatrices $\hat{\psi}$ is non-secret keys for Taylor and the isomatrices $\hat{\psi}$ is non-secret keys for Eileen.

(7) Taylor numerate $\hat{K}_{\text{Taylor}} = \hat{\alpha}_1^{\hat{u}}\hat{\alpha}_{\hat{a}\hat{b}}\hat{\gamma}_2^{(\hat{v})} + \hat{\alpha}_1^{\hat{u}}\hat{\psi}_{\hat{a}\hat{b}}\hat{\beta}_2^{\hat{v}} + \hat{\gamma}_1^{(\hat{u})}\hat{\beta}_{\hat{a}\hat{b}}\hat{\beta}_2^{\hat{v}}$.

(8) Eileen numerate $\hat{K}_{\text{Eileen}} = \hat{\alpha}_1^{\hat{a}}\hat{\alpha}_{\hat{u}\hat{v}}\hat{\gamma}_2^{(\hat{b})} + \hat{\alpha}_1^{\hat{a}}\hat{\psi}_{\hat{a}\hat{u}}\hat{\beta}_2^{\hat{b}} + \hat{\gamma}_1^{(\hat{a})}\hat{\beta}_{\hat{u}\hat{v}}\hat{\beta}_2^{\hat{b}}$.

Following proof shows that $\hat{K}_{\text{Taylor}} = \hat{K}_{\text{Eileen}}$.

If $\hat{K}_{\text{Taylor}} = \hat{\alpha}_1^{\hat{u}}\hat{\alpha}_{\hat{a}\hat{b}}\hat{\gamma}_2^{(\hat{v})} + \hat{\alpha}_1^{\hat{u}}\hat{\psi}_{\hat{a}\hat{b}}\hat{\beta}_2^{\hat{v}} + \hat{\gamma}_1^{(\hat{u})}\hat{\beta}_{\hat{a}\hat{b}}\hat{\beta}_2^{\hat{v}}$ and $\hat{K}_{\text{Eileen}} = \hat{\alpha}_1^{\hat{a}}\hat{\alpha}_{\hat{u}\hat{v}}\hat{\gamma}_2^{(\hat{b})} + \hat{\alpha}_1^{\hat{a}}\hat{\psi}_{\hat{a}\hat{u}}\hat{\beta}_2^{\hat{b}} + \hat{\gamma}_1^{(\hat{a})}\hat{\beta}_{\hat{u}\hat{v}}\hat{\beta}_2^{\hat{b}}$, then $\hat{K}_{\text{Taylor}} = \hat{K}_{\text{Eileen}}$.

As, $\hat{\psi} = \begin{bmatrix} \hat{\alpha}_{\hat{u}\hat{v}} & \hat{\psi}_{\hat{u}\hat{v}} \\ \hat{0} & \hat{\beta}_{\hat{u}\hat{v}} \end{bmatrix} = \hat{\mathcal{H}}_1^{\hat{u}}\hat{\mathcal{H}}_2^{\hat{v}}$,

$\hat{\chi} = \begin{bmatrix} \hat{\alpha}_{\hat{a}\hat{b}} & \hat{\psi}_{\hat{a}\hat{v}} \\ \hat{0} & \hat{\beta}_{\hat{a}\hat{b}} \end{bmatrix} = \hat{\mathcal{H}}_1^{\hat{a}}\hat{\mathcal{H}}_2^{\hat{b}}$

$\hat{\mathcal{H}}_1^{\hat{u}} = \begin{bmatrix} \hat{\alpha}_1^{\hat{u}} & \hat{\gamma}_1^{(\hat{u})} \\ \hat{0} & \hat{\beta}_1^{\hat{u}} \end{bmatrix}$ ,

$\hat{\mathcal{H}}_1^{\hat{a}} = \begin{bmatrix} \hat{\alpha}_1^{\hat{a}} & \hat{\gamma}_1^{(\hat{a})} \\ \hat{0} & \hat{\beta}_1^{\hat{a}} \end{bmatrix}$

$\hat{\mathcal{H}}_2^{\hat{v}} = \begin{bmatrix} \hat{\alpha}_2^{\hat{v}} & \hat{\gamma}_2^{(\hat{v})} \\ \hat{0} & \hat{\beta}_2^{\hat{v}} \end{bmatrix}$ and

$\hat{\mathcal{H}}_2^{\hat{b}} = \begin{bmatrix} \hat{\alpha}_2^{\hat{b}} & \hat{\gamma}_2^{(\hat{b})} \\ \hat{0} & \hat{\beta}_2^{\hat{b}} \end{bmatrix}$

Suppose that, $\hat{\mathcal{H}}_{\text{Taylor}} = \hat{\mathcal{H}}_1^{\hat{u}}\hat{\chi}\hat{\mathcal{H}}_2^{\hat{v}} = \begin{bmatrix} \hat{\alpha}_{\hat{a}} & \hat{K}_{\text{Taylor}} \\ \hat{0} & \hat{\beta}_{\hat{a}} \end{bmatrix}$ and $\hat{\mathcal{H}}_{\text{Eileen}} = \hat{\mathcal{H}}_1^{\hat{a}}\hat{\psi}\hat{\mathcal{H}}_2^{\hat{b}} = \begin{bmatrix} \hat{\alpha}_{\hat{a}} & \hat{K}_{\text{Eileen}} \\ \hat{0} & \hat{\beta}_{\hat{a}} \end{bmatrix}$

Then, $\hat{\mathcal{H}}_{\text{Taylor}} = \hat{\mathcal{H}}_1^{\hat{u}}\hat{\chi}\hat{\mathcal{H}}_2^{\hat{v}} = \hat{\mathcal{H}}_1^{\hat{u}}\hat{\mathcal{H}}_1^{\hat{a}}\hat{\mathcal{H}}_2^{\hat{b}}\hat{\mathcal{H}}_2^{\hat{v}} = \hat{\mathcal{H}}_1^{\hat{a}}\hat{\mathcal{H}}_1^{\hat{u}}\hat{\mathcal{H}}_2^{\hat{v}}\hat{\mathcal{H}}_2^{\hat{b}} = \hat{\mathcal{H}}_1^{\hat{a}}\hat{\psi}\hat{\mathcal{H}}_2^{\hat{b}} = \hat{\mathcal{H}}_{\text{Eileen}}$

Hence, $\hat{K}_{\text{Taylor}} = \hat{K}_{\text{Eileen}}$ hold i.e., the isokey interchange protocol is successful achieved.

## 5. Suggested Isonumber based Isokey Interchange Protocol

If foe incapable to find isounit then suggested isokey interchange protocol secure and if foe capable to find isounit then following attack is secure.

***Brute force attacks:*** For large order for $\hat{\mathcal{H}}_1$ and $\hat{\mathcal{H}}_2$ as 1024 bits then Brute force attacks not applicable.

***Menezes and Wu algorithm [31]:*** Since no isomatrix powers are published over network. Thus Menezes and Wu algorithm is not feasible for the suggested protocol.

***Climent et al. algorithm [32]:*** For identity isomatrix $\mathcal{J}_{\hat{w}}$ of size $\hat{w}$ and null matrix $\hat{0}_{\hat{w}}$ of the same size, an equation

$$\hat{\zeta}_{\hat{\mathcal{H}}}(\hat{\mu}) = \det\left(\hat{\mu}\mathcal{J}_{\hat{w}} - \hat{\mathcal{H}}\right) = \hat{c}_0 + \hat{c}_1\hat{\mu} + \hat{c}_2\hat{\mu}^2 \ldots\ldots + \hat{c}_{\hat{w}-1}\hat{\mu}^{\hat{w}-1} + \hat{\mu}^{\hat{w}}$$

is the characteristic equation for isomatrix $\widehat{\mathcal{H}} \in \mathcal{GL}_{\widehat{\mathcal{w}}}(\mathcal{Z}_{\hat{q}})$.

Then

$$\hat{\zeta}_{\widehat{\mathcal{H}}}(\widehat{\mathcal{H}}) = \hat{c}_0 + \hat{c}_1\widehat{\mathcal{H}} + \hat{c}_2\widehat{\mathcal{H}}^2 \ldots\ldots + \hat{c}_{\widehat{\mathcal{w}}-1}\widehat{\mathcal{H}}^{\widehat{\mathcal{w}}-1} + \widehat{\mathcal{H}}^{\widehat{\mathcal{w}}} = \hat{0}_{\widehat{\mathcal{w}}},$$

Meanwhile two different characteristic equations for two different isomatrices, so the attack based on Cayley–Hamilton theorem is not feasible for the suggested protocol.

The inefficiency of this type of attack is guaranteed by Alvarez R et al [1].

## 6. Conclusion

In this article, we have suggested a new isokey interchange protocol based on isomathematics; utilizing isonumbers for corresponding isounits and for isointegers $\boldsymbol{\hat{a}}$, $\boldsymbol{\widehat{\mathcal{b}}}$; the behavior of isomatrix isoproducts of the type $\boldsymbol{\widehat{\mathcal{H}}_1^{\hat{a}}\,\widehat{\mathcal{H}}_2^{\hat{b}}}$, where $\boldsymbol{\widehat{\mathcal{H}}_1}$; $\boldsymbol{\widehat{\mathcal{H}}_2}$ over $\boldsymbol{\mathcal{BUTI}}$ with a large sufficient order as, for example, 1024 bits. Large isoprime isonumbers are absence in suggested protocol which is one of the primary asset of this protocol. Moreover, Brute force attacks, Menezes and Wu algorithm and Climent et al. algorithm are infeasible in suggested isokey interchange protocol.

## References

[1] Alvarez R., Tortosa L., Vicent J-F, Zamora A., "*Analysis and design of a secure key exchange scheme*," Information Sciences, 179 (12), pp. 2014-2021, (2009). DOI: 10.1016/j.ins.2009.02.008

[2] Alvarez R., *Aplicaciones de las matrices por bloques a los criptosistemas de cifrado en flujo*, Ph.D. Thesis Dissertation, University of Alicante, (2005). (https://rua.ua.es/dspace/bitstream/10045/13571/1/tesis_ralvarez.pdf)

[3] Diffie W., Hellman M., "*New directions in cryptography*," IEEE Transactions on Information Theory, 22, pp. 644–654, (1976). DOI: 10.1109/TIT.1976.1055638

[4] Ko S., Leem C. S., Na Y. J., Yoon C. Y., "*Distribution of digital contents based on non-secret key considering execution speed and security*," Information Sciences, 174 (3–4), pp. 237–250, (2005). DOI: 10.1016/j.ins.2004.08.011

[5] Meshram C., "*The Beta Cryptosystem*," Bulletin of Electrical Engineering and Informatics, 4 (2), pp. 155-159, (2015). (http://journal.portalgaruda.org/index.php/EEI/article/view/442)

[6] Meshram C. and Meshram S. A., "*PKC Scheme Based on DDLP*," International Journal of Information & Network Security, 2 (2), pp. 154-159, (2013). (http://ijins.iaescore.com/index.php/IJINS/article/view/17480)

[7] Meshram C. and Meshram S. A., "*A Non-secret key Cryptosystem based on IFP and DLP*," International Journal of Advanced Research in Computer Science, 2 (5), pp. 616-619, (2011). DOI: 10.26483/ijarcs.v2i5.823

[8] Meshram C., "*A Cryptosystem based on Double Generalized Discrete Logarithm Problem*," International Journal of Contemporary Mathematical Sciences, 6 (6), pp. 285 – 297, (2011). (http://www.m-hikari.com/ijcms-2011/5-8-2011/meshramIJCMS5-8-2011.pdf)

[9] Meshram C. and Meshram S. A., "*An identity based cryptographic model for discrete logarithm and integer factoring based cryptosystem*" Information Processing Letters, 113 (10), pp. 375-380, (2013). DOI: 10.1016/j.ipl.2013.02.009

[10] Meshram C., "*An Efficient ID-based Cryptographic Encryption based on Discrete Logarithm Problem and Integer Factorization Problem*," Information Processing Letters, 115 (2), pp. 351-358, (2015). DOI: 10.1016/j.ipl.2014.10.007

[11] Meshram C. and Obaidat M. S., "*An ID-based Quadratic-Exponentiation Randomized Cryptographic Scheme*," IEEE International Conference on Computer, Information and Telecommunication Systems, pp.1-5, (2015). DOI: 10.1109/CITS.2015.7297722

[12] Meshram C., "*An efficient ID-based Beta Cryptosystem*," International Journal of Security and Its Applications, 9 (2), pp. 189-202, (2015). (http://article.nadiapub.com/IJSIA/vol9_no2/18.pdf)

[13] Meshram C., Powar P. L., Obaidat M. S. and Lee C. C., "*An IBE Technique using Partial Discrete Logarithm*," Procedia Computer Science, 93, pp. 735-741, (2016). DOI: 10.1016/j.procs.2016.07.282

[14] Meshram C., Meshram S. A. and Zhang M., "*An ID-based cryptographic mechanisms based on GDLP and IFP*," Information Processing Letters, 112 (19), pp.753-758, (2012). DOI: 10.1016/j.ipl.2012.06.018

[15] Meshram C. and Powar P. L., "*An Efficient Identity-based QER Cryptographic Scheme*," Complex & Intelligent Systems, 2 (4), pp. 285-291, (2016). DOI: 10.1007/s40747-016-0030-8

[16] Blake, Seroussi G., Smart N., "*Elliptic Curves in Cryptography*," London Mathematical Society, Lecture Notes. Series, vol. 265, Cambridge University Press, pp. 001-204, (1999). DOI: 10.1017/CBO9781107360211

[17] Climent J. J., Ferrandiz F., Vicent J. F., Zamora A., "*A non linear elliptic curve cryptosystem based on matrices*," Applied Mathematics and Computation, 174, pp. 150–164, (2006). DOI: 10.1016/j.amc.2005.03.032

[18] Meshram A., Meshram C. and Khobragade N. W., "*An IND-CPA secure PKC technique based on dihedral group*," Indian Journal of Computer Science and Engineering, 8 (2), pp.88-94, (2017). (http://www.ijcse.com/docs/INDJCSE17-08-02-024.pdf)

[19] A. Meshram, C. Meshram and N. W. Khobragade, "*An IND-CCA2 secure non-secret key cryptographic protocol using suzuki 2-group*," Indian Journal of Science and Technology, 10 (12), pp.01-08, (2017). DOI: 10.17485/ijst/2017/v10i12/111588

[20] Meshram A., Meshram C. and Khobragade N. W., "*Non-secret key cryptographic technique based on suzuki 2-group*," International Journal of Advanced Research in

Computer Science, 8 (03), pp.300-305, (2017). DOI: 10.26483/ijarcs.v8i3.3000

[21] Meshram C., Obaidat M. S. and Meshram A., "*New efficient QERPKC based on partial discrete logarithm problem*," 2020 International Conference on Computer, Information and Telecommunication Systems (CITS), Hangzhou, China, pp. 1-5, (2020), DOI: 10.1109/CITS49457.2020.9232533.

[22] Meshram A., Meshram C., Bagde S. D. and Meshram R. R., "*RIPIC based key exchange protocol*," Advances in Mathematics: Scientific Journal, 9 (12), pp. 11169–11177, (2020). DOI: 10.37418/amsj.9.12.97

[23] Dani M. S., Meshram A., Meshram C., and Wazalwar N. M., "*An efficient key exchange scheme using santilli'sisofields second-kind for secure communication*," Advances in Mathematics: Scientific Journal, 10(2), pp. 1131–1139, (2021). DOI: 10.37418/amsj.10.2.39

[24] Dani M. S., Meshram A. and Meshram C., "*Santilli'sisofields firstkind based key exchange protocol,*" *Journal of Physics: Conference Series*, 1913 (1), 012095, (2021). DOI: 10.1088/1742-6596/1913/1/012095

[25] Thatere A. B., Meshram A., Meshram C., Wazalwar N. M., "*SIFK based Isobeta Cryptosystem*," International Journal of Engineering Trends and Technology, 69 (7), pp. 76-79, (2021. DOI: 10.14445/22315381/IJETT-V69I7P211

[26] Santilli R. M., "*Isonumbers and genonumbers of dimension 1, 2, 4, 8, their isoduals and pseudoduals, and "hidden numbers" of dimension 3, 5, 6, 7*," Algebras, Groups and Geometries, 10, pp. 273-322, (1993). (http://www.santilli-foundation.org/docs/Santilli-34.pdf)

[27] Climent J. J., "*Propiedades espectrales de matrices:el indice de matrices triangulares por bloques, La raiz Perron de matrices cociclicas no negativas*," Thesis for Doctoral Degree, (1993). (http://www.cervantesvirtual.com/nd/ark:/59851/bmcmk686)

[28] Hoffman K., Kunze R., "*Linear Algebra*," Prentice-Hall, New Jersey, (1971). (https://www.cin.ufpe.br/~jrsl/Books/Linear%20Algebra%20-%20Kenneth%20Hoffman%20&%20Ray%20Kunze%20.pdf)

[29] Koblitz N., "*A Course in Number Theory and Cryptography*," Springer-Verlag, (1987). (http://almuhammadi.com/sultan/crypto_books/Koblitz.2nd Ed.pdf)

[30] Odoni R. W. K., Varadharajan V., Sanders P. W., "*Public key distribution in matrix rings*," Electronic Letters, 20, pp. 386–387, (1984). DOI: 10.1049/el:19840267

[31] Menezes A., Wu Y-H., "*The discrete logarithm problem in GLðn; qÞ," Ars Combinatoria*, 47, pp. 22–32, (1997). (https://dblp.org/db/journals/arscom/arscom47.html#MenezesW97)

[32] Climent J. J., Gorla E., Rosenthal J., "*Cryptanalysis of the CFVZ cryptosystem*," Advances in Mathematics of Communications, 1, pp. 1–11, (2007). DOI: 10.3934/amc.2007.1.1

**Mamta S. Dani** is currently working as an Associate Professor with the Department of Applied Mathematics, Yeshwantrao Chavan College of Engineering Nagpur, India. She has more than 34 year teaching & research experience. Her current research interests include cryptography, network security and wireless communication.

**Akshaykumar Meshram** received the Ph.D. degree from R.T.M. Nagpur University, Nagpur, India. He is currently an Assistant Professor with the Department of Applied Mathematics, Yeshwantrao Chavan College of Engineering, Nagpur, India. His current research interests include cryptography, network security, soft computing, and wireless communications. He has published more than twelve scientific articles on the above research fields in international journals and conferences.

**Rupesh Pohane** is currently an Assistant professor with the department of Applied Mathematics, Suryodaya College of Engineering and Technology, India from last 10 years. He has done his M.Sc. Mathematics and B.ed. from Nagpur University, India. His current research interest includes cryptography, network security, black holes and relativity.

**Rupali R. Meshram** is an Assistant Professor with the Department of Mathematics, Kamla Nehru Mahavidyalaya Nagpur, India from last 03 years. She has done his M.Sc. Mathematics from Nagpur University, India. Her current research interest includes cryptography, boundry value problems and relativity.