ADV MATH SCI JOURNAL
Advances in Mathematics: Scientific Journal **9** (2020), no.12, 11169–11177
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.9.12.97

RIPIC BASED KEY EXCHANGE PROTOCOL

AKSHAYKUMAR J. MESHRAM[1], CHANDRASHEKHAR MESHRAM, SUNIL D. BAGDE, AND RUPALI R. MESHRAM

ABSTRACT. In this article, we intend to bring out a unique system of designing key exchange protocol (KEP) based on isomathematics. The significant concept of our proposal is to use ring isopolynomials with the usage of general isointegral coefficient. This class of KEP is an interesting asset for further study because of isomathematical structure permutable permutation of ring isopolynomials with isointeger coefficient (RIPIC).

1. INTRODUCTION

A KEP is a key formation technique where a common secret key is determined by more than two users as a component of data deliberated by, or connected with each of these users, in an ideal situation in such a way that no user can foreordain the subsequent value [1, 2]. In a symmetric key cryptography based protocols, two conveying users use a commonly identified algorithm and a secret key that is shared by the users. Secret key exchange can be made possible by employing few ways like- utilizing out-of-band correspondence, (for example, by telephone, via mail, manual entry etc.), utilizing a trusted third party key distribution center, and so forth. The greater parts of these techniques require approximately from the earlier secret key creation between the protocol and single users. Secret key

[1]*corresponding author*

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

Key words and phrases. Iso-mathematics, iso-zero, iso-unit, RIPIC and Diffie-Hellman Problem.

exchange without the utilization of an out-of-band channel still remains an exceptionally difficult issue [3].

Diffie-Hellman [4], KEP is the first applied asymmetric cryptographic scheme that allows more than two users who have not seen each of them ahead of time to set up a typical secret key over an apprehensive network. These days, the most ordinarily utilized public KEP's are number theory based. The theoretical quality depends upon the structure of abelian groups. Their robustness depends on the difficulty of solving certain issue over finite commutative algebraic structures. The discrete logarithm problem [5, 6] is, as one with the integer factorization problem [7,8] and the elliptic curve discrete logarithm problem [9] which is one of the primary issues where public key cryptosystems are constructed. In this way, for the competently computable groups, the discrete logarithm problem is difficult to break are vital in cryptography [10,11]. Different executions of the Diffie-Hellman protocol in matrix rings, for different kind of matrices, are offered in [12, 13]. Meshram C. [14] presented some new cryptographic protocol based on double discrete logarithm problem and some other implication on cryptography protocols in [15, 17]. This work focuses basically on the design of public KEP's over ring polynomial with integral coefficient. Meshram A. [18, 20] offered certain new cryptographic protocol based on suzuki 2-group and dihedral group which are secure in CPA, IND-CPA, IND-CCA2. Recently, Meshram C. [21] suggested QERPKC based on Partial Discrete Logarithm Problem (PDLP). Security of the presented scheme is based on the hardness of PDLP.

2. Preliminaries

In this article, we offer a novel technique for designing KEP based on RIPIC. We can represent isopolynomials and take them as the underlying work structure. By doing so, it is much secure and easy to execute the KEP. The rest of the article is organized different sections. In section 3, we have discussed the related required background for article. Section 4, explains the proposed RIPIC based KEP. Finally, in section 5, we have given the conclusions.

Herein, we have explained the definition such as RIPIC, Symmetrical Decomposition Problem (SDP) over ring $\Re$ with isopolynomial, Diffie-Hellman Problem (DHP) over ring $\Re$ with isopolynomial and some implications on ring isopolynomial.

Isomathematics:
The framework of isomathematics was first proposed by Santilli [22], which is generalization of multiplication, division and multiplicative unity "1" in modern mathematics. By using isomathematics, we show that "Four multiplied by three is equal to sixty" (for inverse of isounit $\widehat{T} = 5$).

Arithmetic Operations in Modern Mathematics:
We all familiar with arithmetic operations, are addition, subtraction, multiplication, and division. In modern mathematics, "0" and "1" are additive unity and multiplicative unity respectively such that:

$$m + 0 = m,\ m - 0 = m,\ m^0 = 1,\ m \times 1 = 1 \times m = m,\ m \div 1 = m,$$
$$1 \div m = \tfrac{1}{m},\ m \times n = mn, \text{ and } m \div n = \tfrac{m}{n}, \text{ etc.}$$

Arithmetic Operations in Santilli's Iso-mathematics:
Santilli [22], define isoaddition $\widehat{+}$, isosubtraction $\widehat{-}$, isomultiplication $\widehat{\times}$ and isodivision $\widehat{\div}$ as follows:

$$m\widehat{+}n = m + \widehat{\kappa} + n,\ m\widehat{-}n = m - \widehat{\kappa} - n,\ m\widehat{\times}n = m\widehat{T}n, \text{ and } m\widehat{\div}n = \left(\tfrac{m}{n}\right)\widehat{I},$$

where, i) $\widehat{T}\widehat{I} = 1$, $\widehat{T}$ is called inverse of isounit $\widehat{I} \neq 1$; ii) $\widehat{\kappa}$ is called isozero.

RIPIC:
We define, additive abelian group $(\Re, +, \widehat{\kappa})$ and $(\Re, *, \widehat{I})$ for ring $\Re$. Let us consider RIPIC with ring application. Firstly, the concept of scale multiplication over $\Re$ is already a known fact.

As $\widehat{n} \in \mathbb{Z} > 0$ and $\widehat{x} \in \Re, (\widehat{n})\widehat{x} \triangleq \underbrace{\{\widehat{x} + \widehat{x} + \widehat{x} + ... + \widehat{x}\}}_{n\text{-times}}$. When $\widehat{n} \in \mathbb{Z} < 0$, we can define $(\widehat{n})\widehat{x} \triangleq (-\widehat{n})(-\widehat{x}) = \underbrace{(-\widehat{x}) + ... - \widehat{x}}_{-n\text{-times}}$. If $\widehat{n} = 0$, then it can be defined that $(\widehat{n})\widehat{x} = \widehat{\kappa}$.

Property 1. *For every $\widehat{x} \in \Re$, we get $(\widehat{c})\widehat{x}^{\widehat{m}} * (\widehat{d})\widehat{x}^{\widehat{k}} = (\widehat{c}\widehat{d})\widehat{x}^{\widehat{m}+\widehat{k}} = (\widehat{d})\widehat{x}^{\widehat{k}} * (\widehat{c})\widehat{x}^{\widehat{m}}, \forall \widehat{c}, \widehat{d}, \widehat{m}, \widehat{k} \in \mathbb{Z}$.*

Proof. As per the defined scale multiplication we can conclude that the distributivity of multiplication with respect to addition, and commutativity of addition.

As per observations, for distinct isonumbers $\widehat{x}$ and $\widehat{w}$, we get $(\widehat{c})\widehat{x} * (\widehat{d})\widehat{w} \neq (\widehat{d})\widehat{w} * (\widehat{c})\widehat{x}$.

Assume that $\widehat{f}(\widehat{y}) = \widehat{c_0} + \widehat{c_1}\widehat{y} + ... + \widehat{c_k}\widehat{y_k} \in \mathbb{Z}^+[\widehat{y}]$. is a given RIPIC. By allocating this isopolynomial and using an element $\widehat{x}$ in $\Re$, an outcome we get $\widehat{f}(\widehat{x}) = \sum_{i=0}^{k}(\widehat{c_i})\widehat{x^i} = (\widehat{c_0}) + (\widehat{c_1})\widehat{x} + \cdots + (\widehat{c_k})\widehat{x^k} \in \Re$. Further, when we consider $\widehat{x}$ as a variable in $\Re$, then $\widehat{f}(\widehat{x})$ can be viewed as a isopolynomial about variable $\widehat{x}$. All these isopolynomials, taking over all $\widehat{f}(\widehat{x}) \in \mathbb{Z}^+[\widehat{x}]$, can be considered the extension of $\mathbb{Z}^+$ with $\widehat{x}$ denoted by $\mathbb{Z}^+[\widehat{x}]$. Suitably, it can be called as the set of $\Re-$isopolynomials with 1-ary positive IC.

Let us consider that if $\widehat{f}(\widehat{x}) = \sum_{i=0}^{\widehat{k}}(\widehat{c_i})\widehat{x^i} \in \mathbb{Z}^+[\widehat{x}], \widehat{h}(\widehat{x}) = \sum_{j=0}^{\widehat{m}}(\widehat{d_i})\widehat{x^i} \in \mathbb{Z}^+[\widehat{x}]$ and $\widehat{k} \geq \widehat{m}$, then $(\sum_{i=0}^{\widehat{k}}(\widehat{c_i})\widehat{x^i}) + (\sum_{j=0}^{\widehat{m}}(\widehat{d_j})\widehat{x^j}) = (\sum_{i=0}^{\widehat{m}}(\widehat{c_i} + \widehat{d_i})\widehat{x^i}) + (\sum_{i=\widehat{m}+1}^{\widehat{k}}(\widehat{c_i})\widehat{x^i})$, and as per property and distributivity, it results into $(\sum_{i=0}^{\widehat{m}+1}(q_i)\widehat{x^i}) = (\sum_{i=0}^{\widehat{k}}(\widehat{c_i})\widehat{x^i}) * (\sum_{j=0}^{\widehat{m}}(\widehat{d_j})\widehat{x^j})$, where $q_i = \sum_{j=0}^{i}(\widehat{c_i})\widehat{d}_{i-j} = \sum_{j+n=i}\widehat{c_i}\widehat{d_n}$ Henceforth, coming to a conclusion following is the theorem according to property. □

Remark 2.1. $\widehat{f}(\widehat{x}) * \widehat{h}(\widehat{x}) = \widehat{h}(\widehat{x}) * \widehat{f}(\widehat{x}), \forall \widehat{f}(\widehat{x}), \widehat{h}(\widehat{x}) \in \mathbb{Z}^+[\widehat{x}]$. *As per observations, for two distinct variables* $\widehat{x}$ *and* $\widehat{w}$*, we get* $\widehat{f}(\widehat{x}) * \widehat{h}(\widehat{w}) \neq \widehat{h}(\widehat{w}) * \widehat{f}(\widehat{x})$.

Some Implication on Ring Isopolynomials:
Assume if $(\Re, +, *)$ a RIPIC. At random selected element $b \in \Re$, can be define a set $Qb \subseteq \Re$ by $Qb \triangleq \{\widehat{f}(\widehat{b}) : \widehat{f}(\widehat{x}) \in \mathbb{Z}^+[\widehat{x}]\}$. Now, let us study the different forms of SDP and DHP problems over $(\Re, *)$ with its subset Qb respectively.

SDP over Ring $\Re$ *with isopolynomial:* For given $(\widehat{z}, \widehat{y}, \widehat{x}) \in \Re^3$ and $\widehat{m}, \widehat{k} \in \mathbb{Z}$, find $\widehat{z} \in Qb$ such that $\widehat{y} = \widehat{z^m}\widehat{x}\widehat{z^k}$.

DHP over Ring $\Re$ *with isopolynomial:* Compute $\widehat{x^{z_1 z_2}}$ (or $\widehat{x^{z_2 z_1}}$) for given $\widehat{x}, \widehat{x^{z_1}}$ and $\widehat{x^{z_2}}$, where $\widehat{x} \in \mathcal{G}, \widehat{z_1}, \widehat{z_2} \in Qb$.

3. RIPIC BASED KEP

Let us take RIPIC as the basic essential set - up and design an KEP, where the secret session key can be shared between the two users i.e Shekhar and Akshay through insecure channel.

The procedure is described as stated below:

(1) For launching the protocol, one of the user's i.e Shekhar refers two arbitrary small, positive integers $\widehat{m}, \widehat{k} \in \mathbb{Z}^+$ and two arbitrary elements $\widehat{c}, \widehat{d} \in \Re$ to second user i.e Akshay.
(2) Shekhar selects an arbitrary isopolynomial $\widehat{f}(\widehat{x}) \in \mathbb{Z}^+[\widehat{x}]$ such as $\widehat{f}(\widehat{c}) \neq \widehat{\kappa}$ and then takes $\widehat{f}(\widehat{c})$ as his secret key.

(3) Akshay selects an arbitrary isopolynomial $\widehat{h}(\widehat{x}) \in \mathbb{Z}^{+}[\widehat{x}]$ such as $\widehat{h}(\widehat{c}) \neq \widehat{\kappa}$ and then opts $\widehat{h}(\widehat{a})$ as his secret key.
(4) Shekhar calculates $\widehat{\alpha} = \widehat{f}(\widehat{c})^{\widehat{m}} * \widehat{d} * \widehat{f}(\widehat{c})^{\widehat{k}}$ and sends $\widehat{\alpha}$ to Akshay.
(5) Akshay calculates $\widehat{\beta} = \widehat{h}(\widehat{c})^{\widehat{m}} * \widehat{d} * \widehat{h}(\widehat{c})^{\widehat{k}}$ and sends $\widehat{\beta}$ to Shekhar.
(6) Shekhar calculates $\widehat{K}_{Shekhar} = \widehat{f}(\widehat{c})^{\widehat{m}} * \widehat{\beta} * \widehat{f}(\widehat{c})^{\widehat{k}}$ as the shared session key.
(7) Akshay calculates $\widehat{K}_{Akshay} = \widehat{h}(\widehat{c})^{\widehat{m}} * \widehat{\alpha} * \widehat{h}(\widehat{c})^{\widehat{k}}$ as the common session key.

In regular practice, steps (1), (2) and (4) can be completed at once and require only one time communication between Shekhar and Akshay. Further, step (3) and (5) can be completed at once and require only one time communication between Akshay and Shekhar. At the end, Shekhar and Akshay can perform step (6) and (7) individually irrespective of further communication. The illustration of the protocol is shown in the following table.

FIGURE 1. RIPIC based KEP

Pass	Shekhar	Akshay
	Slects at arbitrary $\hat{m},\ \hat{k} \in \mathbb{Z}^{+}$ Slects at arbitrary $\hat{c}, \hat{d} \in \Re$ Slects at arbitrary $\hat{f}(\hat{x}) \in \mathbb{Z}^{+}[\hat{x}]$	
1	$\hat{m}, \hat{k}, \hat{c}, \hat{d}, \hat{f}(\hat{c})^{\hat{m}} \hat{d} \hat{f}(\hat{c})^{\hat{k}}$ →	
		Slects at arbitrary $\hat{h}(\hat{x}) \in \mathbb{Z}^{+}[\hat{x}]$
2	← $\hat{h}(\hat{c})^{\hat{m}} \hat{d} \hat{h}(\hat{c})^{\hat{k}}$	
	$\widehat{K}_{\text{Shekhar}} = \hat{f}\,(\hat{c})^{\hat{m}} \hat{h}(\hat{c})^{\hat{m}} \hat{d} \hat{h}(\hat{c})^{\hat{k}} \hat{f}\,(\hat{c})^{\hat{k}} = \hat{h}(\hat{c})^{\hat{m}} \hat{f}\,(\hat{c})^{\hat{m}} \hat{d} \hat{f}\,(\hat{c})^{\hat{k}} \hat{h}(\hat{c})^{\hat{k}} = \widehat{K}_{\text{Akshay}}$	

Example 1. *RIPIC based KEP Using Matrix Rings For simplicity, let an integer* $N = 5 * 3$*, isounit* $\widehat{I} = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ *and inverse of isounit* $\widehat{T} = \begin{bmatrix} -2 & 1 \\ 1.5 & -0.5 \end{bmatrix}$.

Assume that Shekhar selects; $m = 2, k = 3, \widehat{c} = \begin{bmatrix} 22 & 30 \\ 14 & 24 \end{bmatrix}, \widehat{d} = \begin{bmatrix} 18 & 26 \\ 14 & 20 \end{bmatrix}$ *and* $\widehat{f}(\widehat{x}) = \widehat{5}\widehat{x}^{\widehat{3}} + \widehat{3}\widehat{x}^{\widehat{2}} + \widehat{x} + \widehat{2}$*. Shekhar calculate:*

$$\widehat{f}(\widehat{c}) = \widehat{5}\begin{bmatrix}22 & 30\\ 14 & 24\end{bmatrix}^{\widehat{3}} + \widehat{3}\begin{bmatrix}22 & 30\\ 14 & 24\end{bmatrix}^{\widehat{2}} + \begin{bmatrix}22 & 30\\ 14 & 24\end{bmatrix} + \widehat{2}\begin{bmatrix}1 & 2\\ 3 & 4\end{bmatrix} = \begin{bmatrix}39 & 58\\ 17 & 26\end{bmatrix} mod 15$$

$$\widehat{f}(\widehat{c}) = \begin{bmatrix}9 & 13\\ 2 & 11\end{bmatrix}$$

and

$$\widehat{\alpha} = \widehat{f}(\widehat{c})^{\widehat{m}} * \widehat{d} * \widehat{f}(\widehat{c})^{\widehat{k}}$$

$$\widehat{\alpha} = \begin{bmatrix}9 & 13\\ 2 & 11\end{bmatrix}^{\widehat{2}} * \begin{bmatrix}18 & 26\\ 14 & 20\end{bmatrix} * \begin{bmatrix}9 & 13\\ 2 & 11\end{bmatrix}^{\widehat{3}} = \begin{bmatrix}7 & 9\\ 6 & 5\end{bmatrix}$$

Then, Shekhar sends $\widehat{m}, \widehat{k}, \widehat{c}, \widehat{d}$ *and* $\widehat{\alpha}$ *to Akshay. Assume that Akshay, after receiving* $\widehat{m}, \widehat{k}, \widehat{c}, \widehat{d}$ *and* $\widehat{\alpha}$ *from Shekhar, selects a different isopolynomial* $\widehat{h}(\widehat{x}) = \widehat{2}\widehat{x}^{\widehat{5}} + \widehat{x} + \widehat{3}$ *and calculates:*

$$\widehat{h}(\widehat{c}) = \widehat{2}\begin{bmatrix}22 & 30\\ 14 & 24\end{bmatrix}^{\widehat{5}} + \begin{bmatrix}22 & 30\\ 14 & 24\end{bmatrix} + \widehat{3}\begin{bmatrix}1 & 2\\ 3 & 4\end{bmatrix} = \begin{bmatrix}14 & 9\\ 10 & 12\end{bmatrix}$$

and

$$\widehat{\beta} = \widehat{h}(\widehat{c})^{\widehat{m}} * \widehat{d} * \widehat{h}(\widehat{c})^{\widehat{k}} = \begin{bmatrix}14 & 9\\ 10 & 12\end{bmatrix}^{\widehat{2}} * \begin{bmatrix}18 & 26\\ 14 & 20\end{bmatrix} * \begin{bmatrix}14 & 9\\ 10 & 12\end{bmatrix}^{\widehat{3}} = \begin{bmatrix}9 & 12\\ 12 & 0\end{bmatrix}.$$

After that, Akshay refers $\widehat{\beta}$ *to Shekhar. Lastly, Shekhar computes the session key*

$$\widehat{K}_{Shekhar} = \widehat{f}(\widehat{c})^{\widehat{m}} * \widehat{\beta} * \widehat{f}(\widehat{c})^{\widehat{k}},$$

$$\widehat{K}_{Shekhar} = \begin{bmatrix}9 & 13\\ 2 & 11\end{bmatrix}^{\widehat{2}} * \begin{bmatrix}9 & 12\\ 12 & 0\end{bmatrix} * \begin{bmatrix}9 & 13\\ 2 & 11\end{bmatrix}^{\widehat{3}} = \begin{bmatrix}6 & 3\\ 3 & 0\end{bmatrix}$$

While Akshay computes the session key

$$\widehat{K}_{Akshay} = \widehat{h}(\widehat{c})^{\widehat{m}} * \widehat{\alpha} * \widehat{h}(\widehat{c})^{\widehat{k}},\ \widehat{K}_{Akshay} = \begin{bmatrix}14 & 9\\ 10 & 12\end{bmatrix}^{\widehat{2}} * \begin{bmatrix}7 & 9\\ 6 & 5\end{bmatrix} * \begin{bmatrix}14 & 9\\ 10 & 12\end{bmatrix}^{\widehat{3}} = \begin{bmatrix}6 & 3\\ 3 & 0\end{bmatrix}$$

Hence $\widehat{K}_{Shekhar} = \widehat{K}_{Akshay}$ *holds, i.e., the key agreement is successful achieved.*

4. Conclusion

In recent times, few of the promising non-commutative groups like as braid groups, Thompson's groups, etc. have distinctively figured out various KEP's. In this article, we have deigned a unique KEP based on the ring isopolynomials with isointeger coefficient. This set of KEP is an interesting asset that will pave the way for further study like authentication, signatures and digital identities; because of isomathematical structure permutable permutation of ring isopolynomials with isointeger coefficient.

References

[1] A. Menezes, P. van Oorschot, S. Vanstone: *Handbook of Applied Cryptography*, Boca Raton, FL: CRC, 1997.

[2] D. Xiao, X. Liao, S. Deng: *A novel key agreement protocol based on chaotic maps*, Information Sciences, **177** (2007), 136–142.

[3] P. Naik, K. Ravichandran, M. Krishna, Sivalingam: *Cryptographic key exchange based on locationing information*, Pervasive and Mobile Computing, **3** (2007), 15–35.

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

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

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

[7] I. Lin, C. Chang: *Security enhancement for digital signature scheme with fault tolerance in RSA*, Information Sciences, **177** (2007), 4031–4039.

[8] R. Rivest, A. Shamir, L. Aleman: *A method for obtaining digital signature and public-key cryptosystem*, Comm. ACM, **21**(2) (1978), 120–126.

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

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

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

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

[13] R. Alvarez, L. Tortosa, J. F. Vicent, 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.

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

[15] C. MESHRAM, 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.

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

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

[18] A. MESHRAM, C. MESHRAM, 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.

[19] A. MESHRAM, C. MESHRAM, 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.

[20] A. MESHRAM, C. MESHRAM, 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.

[21] C. MESHRAM, M. S. OBAIDAT, 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.

[22] R. M. SANTILLI: *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** (1993), 273–322.

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 Mathematics, Gondwana University
Gadchiroli MIDC Road Complex, Gadchiroli-442605
Email address: sunilkumarbagde@rediffmail.com

Department of Mathematics, Kamla Nehru Mahavidyalaya Nagpur
M.S. 440024, India
Email address: rupa.meshram15@gmail.com