International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 /doi:10.14445/22315381/IJETT-V69I7P211
Volume 69 Issue 7, 76-79, July, 2021
©2021 Seventh Sense Research Group®

SIFK based Isobeta Cryptosystem

Ajay B. Thatere[1], Akshaykumar Meshram[*2], Chandrashekhar Meshram[3] and N. M. Wazalwar[4]

[1]*Department of Electronics Engineering, YeshwantraoChavan College of Engineering, Nagpur-441110, M.S., India.*

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

[3]*Department of Post Graduate Studies and Research in Mathematics, JayawantiHaksar Government Post-Graduation College, College of Chhindwara University, Betul, M.P, 460001, India.*

[4]*Department of Statistics, RashtrasantTukadojiMaharaj Nagpur University, Nagpur-440033, M.S., India.*

[1]ajay.thatere@yahoo.co.in, [*2]akshaykjmeshram@gmail.com, [3]cs_meshram@rediffmail.com

Abstract — *The current effort takes the unique technique to construct is beta cryptosystem, whose security is established on santilli'sisofields first-kind ($\mathcal{SIFK}$), generalized discrete logarithm problem ($\mathcal{GDLP}$) and integer factorization problem ($\mathcal{IFP}$) in the isomultiplicative isogroup of finite $\mathcal{SIFK}$. The attacker have to find isoelement from $\mathcal{SIFK}$ and simplify both distinct $\mathcal{GDLP}$ and $\mathcal{IFP}$ together in the isomultiplicativeisogroup of finite $\mathcal{SIFK}$ in order to get back comparable massage from the secured cipertext and so this technique is probable to achieve a higher level of security.*

Keywords — *Public Key Cryptosystem ($\boldsymbol{\mathcal{PKC}}$), $\boldsymbol{\mathcal{SIFK}}$, $\boldsymbol{\mathcal{GDLP}}$ and $\boldsymbol{\mathcal{IFP}}$.*

I. INTRODUCTION

The technique of $\mathcal{PKC}$ suggested in article "New Directions in Cryptography" by Diffie-Hellman [1]. After that several $\mathcal{PKC}$ were suggested. Among these $\mathcal{PKC}$ techniques based on hard mathematical problems, which security be dependent on the impracticable of factoring a large integer. Among these $\mathcal{PKC}$ techniques based on hard mathematical problems, which security be dependent on the impracticable of factoring a large integer [2] and the complexity of derive the square root modulo a massive composite integer [3]. ElGamal offered an efficient $\mathcal{PKC}$ based on $\mathcal{DLP}$, which is too hard to simplify as deal with prime field or elliptic curve defined over a finite field [4]. All $\mathcal{PKC}$ based on $\mathcal{DLP}$ and $\mathcal{IFP}$ are not reliable if mathematical structure for $\mathcal{DLP}$ and $\mathcal{IFP}$ are solved. The techniques build on a single mathematical structure have security issues, so researchers proposed $\mathcal{PKC}$ based on multiple hard mathematical structure. Various $\mathcal{PKC}$ have been built on together $\mathcal{DLP}$ and $\mathcal{IFP}$ [5-22]. Some $\mathcal{PKC}$ have been built on dihedral group and suzuki-2 group [23-25]. At the latest, Meshram A. suggested key exchange protocol based on ring isopolynomials with isointeger coefficient [26]. Dani M. offered santilli'sisofields second-kind based key exchange protocol for secure communication[27]and key exchange protocol based on $\mathcal{SIFK}$[28].

Regrettably, we observed that $\mathcal{DLP}$ and $\mathcal{IFP}$ based unified presented $\mathcal{PKC}$ cannot be considered as secure. Hence, we construct a unique beta cryptosystem based on $\mathcal{SIFK}$, $\mathcal{GDLP}$ and $\mathcal{IFP}$ along its assured security, we additionally demonstrated that it is extremely capable to be enforce in the physical world applications.

The rest of this article summarize as below; in section-II, we explained $\mathcal{SIFK}$, offered beta cryptosystem based on $\mathcal{SIFK}$ in section-III, supporting example for confirmation of suggested cryptosystem in section-IV, security investigation and efficiency performance examine in section-V and in final section-VI we conclude the article.

II. $\mathcal{SIFK}$

Santilli [29] offered the generalization of arithmetic operations $\langle +,-,\times,\div \rangle$ termed as isomathematics. $\mathcal{SIFK}$ is the ring $\hat{\mathfrak{F}} = \hat{\mathfrak{F}}(\hat{y}, \hat{+}, \hat{\times})$ along with isonumbers $\hat{y} = y\hat{I}$, $y \in \mathfrak{F}, \hat{I} = \frac{1}{\hat{T}} \notin \mathfrak{F}$ along with arithmetic operations $\langle \hat{+}, \hat{-}, \hat{\times}, \hat{\div} \rangle$, $\hat{y} \hat{+} \hat{x} = (y + x)\hat{I}$an isosum, with additive unit $0 = 0\hat{I} = 0$, $\hat{y} + 0 = 0 + \hat{y} = \hat{y}$ and isoproduct $\hat{y} \hat{\times} \hat{x} = \hat{y}\hat{T}\hat{x} = y\hat{I}\hat{T}x\hat{I} = (yx)\hat{I}$, where, the left and right new unit $\hat{I}$, $\hat{I} \hat{\times} \hat{y} = \hat{y} \hat{\times} \hat{I} = \hat{y}$ is called isounit and $\hat{T}\hat{I} = 1, \hat{T}$ is called inverse of isounit $\hat{I} \neq 1$.

III. ISOBETA CRYPTOSYSTEM BASED ON$\mathcal{SIFK}$

The mechanism for isobeta cryptosystem involves three steps;

Step-A: Key Formation Algorithm

Client-1 runs following algorithm for key formation;

i. Select two large isoprimeisonumbers$\hat{\mathcal{A}}$ and $\hat{\mathcal{B}}$ of the same size.
ii. Numerate the IsoEulerphi function $\varphi(\hat{\mathcal{N}}) = (\hat{\mathcal{A}} - 1)(\hat{\mathcal{B}} - 1)$ for isointeger $\hat{\mathcal{N}} = \hat{\mathcal{A}} * \hat{\mathcal{B}}$.
iii. Pick an arbitrary isointeger $\hat{q}$, $1 \leq \hat{q} \leq \varphi(\hat{\mathcal{N}})$ such that, $\gcd\left(\hat{q}, \varphi(\hat{\mathcal{N}})\right) = 1$.
iv. Pick an arbitrary isointeger $\hat{w}$ such that $2 \leq \hat{w} \leq \varphi(\hat{\mathcal{N}}) - 1$.

This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

v. Numerate $\hat{z}_1 = \hat{\beta}^{\hat{w}}(mod\hat{\mathcal{N}})$ for any arbitrary isoelement $\hat{\beta}$ of the isomultiplicative isogroup $\hat{\mathcal{Z}}^*_{\hat{\mathcal{N}}}$.

vi. Numerate unique isointeger $\hat{p}, 1 \le \hat{p} \le \varphi(\hat{\mathcal{N}})$ such that $\hat{q}\hat{p} \equiv 1(mod\hat{\mathcal{N}})$ by using extended Euclidean algorithm.

Thus $(\hat{p}, \hat{w}, \hat{\beta})$ is a isosecretisokey for comparable isopublicisokey$(\hat{\mathcal{N}}, \hat{q}, \hat{\beta}^{\hat{w}})$.

Step-B: Encryption Algorithm

Client-2 runs following algorithm to encrypt a plaintext $\hat{h}(\hat{\mathcal{P}})$ to Client-1;

i. The genuine plaintext as $\hat{\mathcal{P}} \in [1, \hat{\mathcal{N}} - 1]$ hashed and suppose that the resultant becomes$\hat{h}(\hat{\mathcal{P}})$ by utilizing public key $(\hat{\mathcal{N}}, \hat{q}, \hat{\beta}^{\hat{w}})$.

ii. The $\hat{\mathcal{C}} = \left(\hat{h}(\hat{\mathcal{P}})\hat{\beta}^{\hat{w}}\right)^{\hat{q}}(mod\hat{\mathcal{N}})$ denotes corresponding ciphertext. (1)

Step-C: Decryption Algorithm

Client-1 runs following algorithm to retrieve the plaintext$\hat{h}(\hat{\mathcal{P}})$from the ciphertext$\hat{\mathcal{C}}$

i. Numerate $\hat{z}_2 = \hat{\beta}^{\varphi(\hat{\mathcal{N}})-\hat{w}}(mod\hat{\mathcal{N}}) = \hat{\beta}^{-\hat{w}}(mod\hat{\mathcal{N}})$.

ii. Then numerate $\hat{z}_3 = (\hat{z}_2)^{\hat{q}}(mod\hat{\mathcal{N}})$

iii. Retrieve the plaintext $\hat{h}(\hat{\mathcal{P}})$ by numerating $\left((\hat{z}_2)^{\hat{q}} * \hat{\mathcal{C}}\right)^{\hat{p}}(mod\hat{\mathcal{N}})$. (2)

IV. EXAMPLE

We demonstrate an elementary example to support too offered $\mathcal{SIFK}$ based isobeta cryptosystem.

Suppose that both client-1 & client-2 agree on inverse of isounit$\hat{\mathcal{T}} = 3$ such that $\hat{\jmath} = \left(1/\hat{\mathcal{T}}\right) < 1$. Then isointerger $\hat{\mathcal{N}} = (3741)\hat{\jmath} = 1247$ for selected two huge isoprime isonumbers $\hat{\mathcal{A}} = (87)\hat{\jmath} = 29$ and $\hat{\mathcal{B}} = (129)\hat{\jmath} = 43$ of the same size.

Key formation algorithm:

Client-1 runs following algorithm for key formation;

i. Numerate the IsoEulerphi function $\varphi(\hat{\mathcal{N}}) = (\hat{\mathcal{A}} - 1)(\hat{\mathcal{B}} - 1)$ for isointeger $\hat{\mathcal{N}}$.

ii. Pick an arbitrary isointeger $\hat{q} = 11$, such that $\gcd(11,1176) = 1$.

iii. Pick an arbitrary isointeger$\hat{w} = 19$.

iv. Numerate $\hat{z}_1 = \hat{\beta}^{\hat{w}}(mod\hat{\mathcal{N}}) = 10^{19}(mod\ 1247)$ for any arbitrary isoelement $\hat{\beta} = 10$ of the isomultiplicativeisogroup$\hat{\mathcal{Z}}^*_{\hat{\mathcal{N}}}$

v. Numerate unique isointeger= 107 ,$1 \le \hat{p} \le \varphi(\hat{\mathcal{N}})$ such that $11\hat{p} \equiv 1\ (mod\ 1247)$ by using extended Euclidean algorithm.

Thus $(\hat{p}, \hat{w}, \hat{\beta})$ is a secret key for comparable public key $(\hat{\mathcal{N}}, \hat{q}, \hat{\beta}^{\hat{w}})$.

Encryption algorithm:

Client-2 runs following algorithm to encrypt a plaintext $\hat{h}(\hat{\mathcal{P}})$ to Client-1;

i. The genuine plaintext as $\hat{\mathcal{P}} \in [1, \hat{\mathcal{N}} - 1]$ hashed and suppose that the resultant becomes$\hat{h}(\hat{\mathcal{P}}) = 1122$ by utilizing public key $(\hat{\mathcal{N}}, \hat{q}, \hat{\beta}^{\hat{w}})$.

ii. The $\hat{\mathcal{C}} = \left(\hat{h}(\hat{\mathcal{P}})\hat{\beta}^{\hat{w}}\right)^{\hat{q}}(mod\hat{\mathcal{N}}) = 791$ denotes corresponding ciphertext.

Decryption algorithm:

Client-1 runs following algorithm to retrieve the plaintext$\hat{h}(\hat{\mathcal{P}})$ from the ciphertext $\hat{\mathcal{C}}$

i. Numerate $\hat{z}_2 = \hat{\beta}^{\varphi(\hat{\mathcal{N}})-\hat{w}}(mod\hat{\mathcal{N}}) = \hat{\beta}^{-\hat{w}}(mod\hat{\mathcal{N}}) = 917$.

ii. Then numerate $\hat{z}_3 = (\hat{z}_2)^{\hat{q}}(mod\hat{\mathcal{N}}) = 483$.

iii. Retrieve the plaintext $\hat{h}(\hat{\mathcal{P}})$ by numerating $\left((\hat{z}_2)^{\hat{q}} * \hat{\mathcal{C}}\right)^{\hat{p}}(mod\hat{\mathcal{N}}) = 1122$

V. SECURITY INVESTIGATION

In this section, we examine presented isobeta cryptosystem in following subsections;

Consistency of the isobeta cryptosystem:

We justify our unique cryptosystem by demonstrating the following proposition.

Proposition: The decryption algorithm of encrypted plaintext in decryption procedure is accurate if key formation algorithm and encryption algorithm run smoothly.

Proof: If for every encrypted plaintext above expression-2 is accurate then ciphertext $\hat{\mathcal{C}} = \left(\hat{\hbar}(\hat{\mathcal{P}})\hat{\beta}^{\hat{\varpi}}\right)^{\hat{q}}(mod\ \hat{\mathcal{N}})$ in encryption algorithm and $\hat{z}_2 = \hat{\beta}^{\varphi(\hat{\mathcal{N}})-\hat{\varpi}}(mod\ \hat{\mathcal{N}}) = \hat{\beta}^{-\hat{\varpi}}(mod\ \hat{\mathcal{N}})$ in decryption algorithm,

And $(\hat{z}_2)^{\hat{q}}(mod\ \hat{\mathcal{N}}) = \left(\hat{\beta}^{-\hat{\varpi}}\right)^{\hat{q}}(mod\ \hat{\mathcal{N}})$, $\left((\hat{z}_2)^{\hat{q}} * \hat{\mathcal{C}}\right)^{\hat{p}}(mod\ \hat{\mathcal{N}}) = \left(\hat{\beta}^{-\hat{\varpi}\hat{q}}\left(\hat{\hbar}(\hat{\mathcal{P}})\right)^{\hat{q}}\hat{\beta}^{\hat{\varpi}\hat{q}}\right)^{\hat{p}}(mod\ \hat{\mathcal{N}}) = \left(\hat{\hbar}(\hat{\mathcal{P}})\right)^{\hat{q}\hat{p}}(mod\ \hat{\mathcal{N}}) = \hat{\hbar}(\hat{\mathcal{P}})(mod\ \hat{\mathcal{N}})$

Security Analysis:

- If foe incapable to find isounit$\hat{\mathcal{I}}$ then proposed isobeta cryptosystem secure against all general attacks.
- Somehow if foe capable to find isounit$\hat{\mathcal{I}}$ then we demonstrate that our proposed isobeta cryptosystem is heuristically secure against subsequent extreme general attacks.

- Direct attack: Foe have to simplify $\mathcal{IFP}$ and $\mathcal{GDLP}$ by utilizing the isonumberisofield sieve technique which is based on the size of isomodulus $\hat{\mathcal{N}}$ of size beyond 1024-bit. For improve the security of offered isobeta cryptosystem, we choose two huge isoprimes isonumbers$\hat{\mathcal{A}}$and$\hat{\mathcal{B}}$ (of size 512-bit each) with $\frac{\hat{\mathcal{A}}-1}{2}$ and $\frac{\hat{\mathcal{B}}-1}{2}$ such that isomodulus $\hat{\mathcal{N}} = \hat{\mathcal{A}} * \hat{\mathcal{B}}$.

- Factoring attack: Suppose foe retrieve the genuine plaintext M by eliminating $\hat{\beta}^{\hat{\varpi}}$ from ciphertex $\hat{\mathcal{C}}$ if foe have the secret isonumbers$(\hat{\beta}, \hat{\varpi})$. But at this stage $\mathcal{GDLP}$ still hard to simplify and hence foe would fail.

-Discrete logarithm attack: Foe will familiar to $\hat{z}_2$ and $(\hat{z}_2)^{\hat{q}}(mod\ \hat{\mathcal{N}}) = \left(\hat{\beta}^{-\hat{\varpi}}\right)^{\hat{q}}(mod\ \hat{\mathcal{N}})$ and retrieve the genuine plaintext M from ciphertex $\hat{\mathcal{C}}$ if foe simplify $\mathcal{GDLP}$ and find the secret isointeger $\hat{\varpi}$. Regrettably, to decipher the genuine plaintext, foe necessity have the secret isointeger $\hat{p}$ in hand but this is impractical as $\mathcal{IFP}$ is hard to simplify.

Efficiency of isobeta cryptosystem:

To examines the execution of the proposed isobeta cryptosystem in in terms of number of isokeys, communication costs and computational complexity.

Duration taken for an isomodularisomultiplication is $\hat{\tau}_{isomul}$ and for an isomodularisoexponentiationis $\hat{\tau}_{isoexp}$.

Duration taken for an isomodularisosquare-root computation is $\hat{\tau}_{isosrt}$ and for an isomodularisosquare computation is $\hat{\tau}_{isosqu}$.

Duration taken for an executing a isohash function is $\hat{\tau}_{isohash}$ and for an isomodularisoinverse computation is $\hat{\tau}_{isoinv}$. $|\hat{x}|$ stand for the bit length of $\hat{x}$ and the probability of the bit being chose as 0 or 1 is $\frac{1}{2}$.

Table: The Efficiency of isobeta cryptosystem:

$\mathcal{SIFK}$ based Isobeta Cryptosystem		
The number of keys	Computational complexity	Communication cost
isosecretisokey	Encryption: $2\hat{\tau}_{exp} + \hat{\tau}_{mul} + \hat{\tau}_{hash}$	Encryption: $2n$
isopublicisokey	Decryption: $3\hat{\tau}_{exp} + \hat{\tau}_{mul}$	Decryption: n

VI. CONCLUSION

In this article, we offered isobeta$\mathcal{PKC}$ based on $\mathcal{SIFK}$, $\mathcal{GDLP}$ and $\mathcal{IFP}$ in the isomultiplicative isogroup of finite isofields. The suggested scheme break by foe if foe be able to simplify the three above problems together and this is extremely inconceivable to occur. If foe somehow succeeds to search key to one of the primary hard problem, our isobeta$\mathcal{PKC}$ stay safe as the other problem stay hard to simplify for at best another period of time. Our presented cryptosystem is secure against the direct attack, the factoring attack and the discrete logarithm attackfor offered cryptosystem based on $\mathcal{SIFK}$, $\mathcal{GDLP}$ and $\mathcal{IFP}$.

REFERENCES

[1] W. Diffie, M. Hellman., New Directions in Cryptography, IEEE Transactions On Information Theory, 22(6) 644-654 1976.
[2] R. L. Rivest, A. Shamir, L. Adleman., A Method to Obtain Digital Signature and Public key Crytosystem Commun. ACM, 21 (1978) 121-126.
[3] M. Rabin., Digitalized Signatures and Public Key Functions as Intractable as Factorization, 1st Edition, Massachusetts Institute of Technology, Laboratory for Computer Science, Ft. Belvoir Defense Technical Information Center, (1979) 18.
[4] T. ElGamal., A public Key Cryptosystem and a Signature Scheme based on Discrete Logarithms, IEEE Transactions on Information Theory, 31 (1985) 469-472.
[5] L.Harn., Public key cryptosystem design based on factoring and discrete logarithms, IEE Proceeding of Computers Digital Techniques, (1994) 193-195.
[6] E.S. Ismail and M.S.N. Hijazi., A New Cryptosystem Based on Factoring and Discrete Logarithm Problems, Journal of Mathematics and Statistics, 7(3) (2011) 165-168.
[7] A. Kiriyama, Y. Nakagawa, T. Takaoka and Z. Tu., A New Public-Key Cryptosystem and its Applications, Proceedings of the Eighth International Conference on Enterprise Information Systems: Databases and Information Systems Integration (ICEIS 2006), Paphos, Cyprus, (2006).
[8] S. M. Kalipha, J. W. A. Sada and H. A. Hussain ., New public-key cryptosystem, International Journal of Systems Science,21(1) (1990) 205-215.
[9] N. Koblizt, A. Menezes, and S. Vanstone., The state of elliptic curve cryptography, Design, Codes Cryptography, 19 (2000) 173-193.
[10] J. Gordon, Strong RSA keys, Electron. Letter, 20, 12 (1984) 514-516.
[11] K. Lenstra and M.S. Manasse., Factoring by electronic mail Advances in CrvDtolorv - EUROCRYPT '89 Chrineer Berlin, (1990) 355-371.
[12] C. Meshram and S. Meshram., PKC Scheme Based on DDLP International Journal of Information & Network Security (IJINS), 2(2) (2013) 154-159.
[13] C. Meshram and S. Meshram ., A Public Key Cryptosystem based on IFP and DLP, International Journal of Advanced Research in Computer Science, 2(5) (2011) 616-619.
[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 and S. Agrawal., Enhancing the security of A Public key cryptosystem based on DLP γ≡ αaβb (mod p), International Journal of Research and Reviews in Computer Science, 1(4) (2010)67-70.

[16] C. Meshram and S. Agrawal., A New Design of Public Key Encryption Scheme Based on Double Discrete Logarithm Problem Proceedings of International Conference on Challenges and Application of Mathematics in Science and Technology (CAMIST), January 11-13 (2010) 495- 502.

[17] C. Meshram., New PKC Technique based on DDLP in Metacyclic Group- Proceedings of National Conference on Establishing Kinship between Mathematical Science and Society (NCKMS). October 30-31 (2009) 141-147.

[18] Z. Shi, Y. Xia and C. Yu., A Strong RFID Mutual Authentication Protocol Based on a Lightweight Public-key Cryptosystem, TELKOMNIKA Indonesian Journal of Electrical Engineering 12(3) (2014) 2320-2326.

[19] F. Amounas and E.H. El Kinani ., Construction Efficiency of the Elliptic Curve Cryptosystem using Code Computing for Amazigh Alphabet., International Journal of Information & Network Security, 2(1) (2013) 43-53.

[20] G. C. Sheng ., Multiplicative Learning with Errors and Cryptosystems" International Journal of Information & Network Security, 3(2) (2014) 92-97.

[21] J. Yao and T. Zhang ., Biometric Cryptosystem Based Energy Attack Analysis, TELKOMNIKA Indonesian Journal of Electrical Engineering, 10(5) (2012) 1130-1136.

[22] T. Mantoro and A. Zakariya., Securing E-mail Communication Using Hybrid Cryptosystem on Android-based Mobile Devices, TELKOMNIKA Indonesian Journal of Electrical Engineering, 10(4) (20152) 827-834.

[23] 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.

[24] 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.

[25] 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(3) (2017) 300-305.

[26] 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.

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

[28] M. S. Dani, A. Meshramand C. Meshram., Santilli'sisofields first-kind based key exchange protocol, Journal of Physics: Conference Series, 1913(1) (2021) 012095.

[29] C. X. Jiang., Foundations of SantillisIsonumber Theory with Applications, ISBN 1-57485-056-3, Hadronic Press, (2002).