International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Design and Analysis of various computations using Elliptic Curve Cryptography (ECC) and Rivest Shamir Adleman (RSA)

Raman Kumar[1]*, Sandeep Thakur[2], Harpreet Kaur Bajaj[3]

Submitted:13/03/2024 **Revised**: 28/04/2024 **Accepted**: 05/05/2024

Abstract: Elliptic Curve Cryptography provides high level of security using the concept of number theory. It is specialized field of engineering which deals with the design and development of detailed engineering plan and design which is similar to the other engineering activities but the added advantage is to protect it from misuse. It is more secure as compared to RSA. Such new techniques avoid the various operations related to the sender and receiver. We have discussed Point Addition, Finite Field, Smooth Elliptic Curves are Groups and Trapdoor Function etc. The various notorious attacks are impractical for proposed hypothesis.

Keywords: *Information Security, ECC (Elliptic Curve Cryptography), Authentication and Authorization*.

1. Introduction

In a network security area, whenever end user request to access server's service, end user must have to pass network authentication. In this altered security schemes are used to check if the user has exact access rights to use authentication and authorization services. When user try to access services on the server, message transmission between server and user must kept safe and secure. To secure the communications between user and server they use a session key agreement.

To secure the network communication remote user authentication scheme proposed and also other schemes proposed to increase network security, functionality and network capacity. Fig. 1 illustrates Elliptic Curve Cryptography. Fig. 2 depict point addition using Elliptic Curve Cryptography. Fig. 3 exemplifies various operations using Elliptic Curve Cryptography.

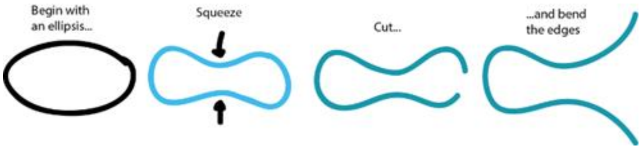

Fig. 1 ECC

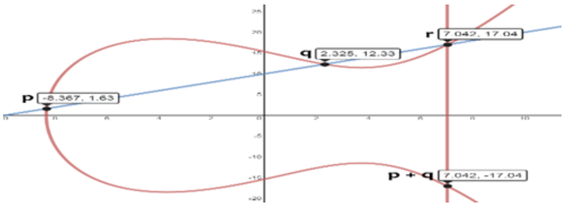

Fig. 2 Point Addition using Elliptic Curve Cryptography

A. Point Addition

B. Finite Field

C. Smooth Elliptic Curves are Groups

D. Trapdoor Function

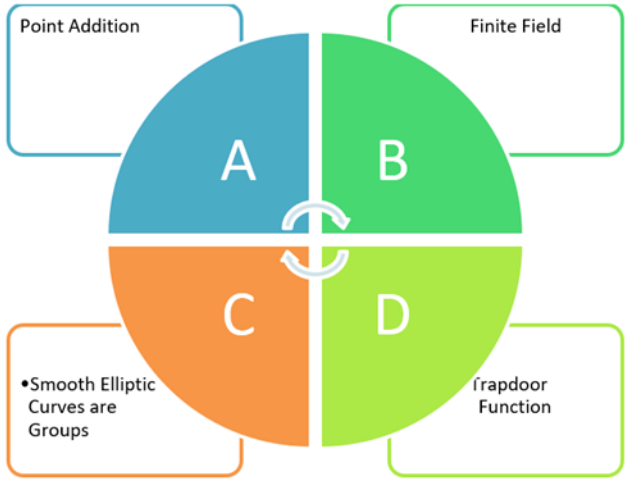

Fig. 3 Operations using Elliptic Curve Cryptography

2. Literature Survey

Kumari, S., Karuppiah, M., Das, A.K. et al. have investigated various authentication schemes. But this paper, is only susceptible to various attacks and said scheme unable to provide security against various attacks [1].

Alavalapati Goutham Reddy, Ashok Kumar Das, Vanga Odelu, Kee-Young Yoo. In this paper they enhanced security features by implementing the smart card based on elliptic curve cryptography, that handled various attacks and provided clock synchronism [2].

Reza Azarderakhsh and Arash Reyhani-Masoleh In this paper they have analysed the data flow and designed architectures that implement point multiplication on binary

[1] *Department of Computer Science and Engineering, I K Gujral Punjab Technical University Kapurthala, 144603, Punjab, India.*
Email Id: er.ramankumar@aol.in
https://orcid.org/0000-0003-4661-4764
[2] *M Tech Student*
[3] *DAV Institute of Engineering and Technology, Jalandhar, Punjab, India.*
** Corresponding Author Email: er.ramankumar@aol.in*

Edward and generalized Hessian curves. They have investigated various techniques to remove data dependency and reduce latency of point multiplication [3].

Shehzad Ashraf Chaudhry, Khalid Mahmood,Husnain Naqvi,Muhammad Khurram Khan. In this paper they provide various schemes to handle numerous attacks related to the patient data only [4].

Shehzad Ashraf Chaudhry, Khalid Mahmood,Husnain Naqvi,Muhammad. In this paper they are work on less number security attacks and unable to handle attacks to system [5].

Alowolodu O.D, Alese B.K,Adetunmbi A.O., Adewale O.S. In the present paper they proposed elliptic curve cryptography techniques to secure the cloud network with various attacks schemes [6].

Lara-Nino, Carlos & Díaz-Pérez, Arturo & Morales-Sandoval, Miguel. They proposed new schemes for network security using elliptic curve cryptography and minimize the network security key size for better system performance [7].

Jagadish Thiruvayipati. The proposed method in this paper they provide security schemes to handle various attacks and implemented security key using cryptography techniques with smaller size encryption key pair in the cloud network environment [8].

Dindayal Mahto and Dilip Kumar Yadav.In this paper they provide performance dissimilarity with key security techniques and analyzed it with various network security key size and performance evaluation in different network [9].

Xueqin Zhang, Baoping Wang, Wenpeng Zhang. In the proposed paper they handle remote authentication schemes for multiple server systems and handle various security attack in multiple server environment with cryptography techniques [10]

Saru Kumari, Marimuthu Karuppiah, Ashok Kumar Das, Xiong Li, Fan Wu & Neeraj Kumar. They provide various security techniques to handle network security attacks. But the proposed schemes are not able to handle different types of network attacks [11].

Jiaqing, Zhongwang Hu, Yuhua Lin. Have investigated security methods mobile networks and handle various mobile network attack using security algorithms [12].

The authors only analysed that Small size, high security and other features characterize ECC [16]. They only discussed a few advantages. In [17], they only proposed a fast and configurable hardware accelerator for NIST P-256/-521 ECC. In [18,19] they only analysed ECC is better than RSA. In this [18], they only targeting ECC multiplication only and they only analysed that RSA and ECC in WSNs. In [20], they only analysed that RSA and ECC in comparative manner. In [21], they only analysed that RSA and ECC compared the efficacy in terms of security among the well-known public key cryptography algorithms. In [22, 23], they Simulate results and visualized in a way that clearly depicts which algorithm is most suitable and in [23] they worked only in ASCII values. In [24], they only analysed that ECC and HECC. In [25, 26 and 27], they only present a point multiplication processor over the binary field GF (2233).

Table 1 Record of Elliptic Curve Cryptography

Sr. No	References	Availability	Confidentiality	Data Integrity	Identity and Access Management (IAM)	Control	Audit
1.	[27]	×	×	×	×	×	×
2.	[26]	×	×	×	×	×	×
3.	[25]	×	×	×	×	×	×
4.	[24]	×	×	×	×	×	×
5.	[23]	×	×	×	×	×	×
6.	[22]	×	×	×	×	×	×
7.	[21]	×	×	×	×	×	×
8.	[20]	×	×	×	×	×	×
9.	[19]	×	×	×	×	×	×
10.	[18]	×	×	×	×	×	×
11.	[17]	×	×	×	×	×	×
12.	[16]	×	×	×	×	×	×
13.	[15]	×	×	×	×	×	×
14.	[14]	×	×	×	×	×	×
15.	[13]	×	×	×	×	×	×
16.	[12]	×	×	×	×	×	×
17.	[11]	×	×	×	×	×	×
18.	[10]	×	×	×	×	×	×
19.	[9]	×	×	×	×	×	×
20.	[8]	×	×	×	×	×	×
21.	[7]	×	×	×	×	×	×

22.	[6]	×	×	×	×	×	×
23.	[5]	×	×	×	×	×	×
24.	[4]	×	×	×	×	×	×
25.	[3]	×	×	×	×	×	×
26.	[2]	×	×	×	×	×	×
27.	[1]	×	×	×	×	×	×
*	[Kumar et al.]	✓	✓	✓	✓	✓	✓

3. Proposed Work

In compliance to the proposed work, we have analyzed that no such scheme is secure. In essence, no secure scheme is impractical against various attacks.

Table 2 Record of Elliptic Curve Cryptography

Sr. No	Scheme	Available
1.	[27]	×
2.	[26]	×
3.	[25]	×
4.	[24]	×
5.	[23]	×
6.	[22]	×
7.	[21]	×
8.	[20]	×
9.	[19]	×
10.	[18]	×
11.	[17]	×
12.	[16]	×
13.	[15]	×
14.	[14]	×
15.	[13]	×
16.	[12]	×
17.	[11]	×
18.	[10]	×
19.	[9]	×
20.	[8]	×
21.	[7]	×
22.	[6]	×
23.	[5]	×
24.	[4]	×
25.	[3]	×
26.	[2]	×
27.	[1]	×
*	[Kumar et al.]	✓

In this research paper we may use ECC. As ECC provides more security as compared to earlier authentication algorithms. ECC provides more security for all kind of prime numbers. We may apply multiserver authentication scheme using ECC. We have tested and analyze the performance for the following guessing attack, reply attack, insider attack, DoS attack and dictionary attack. The proposed scheme is impractical against various attacks.

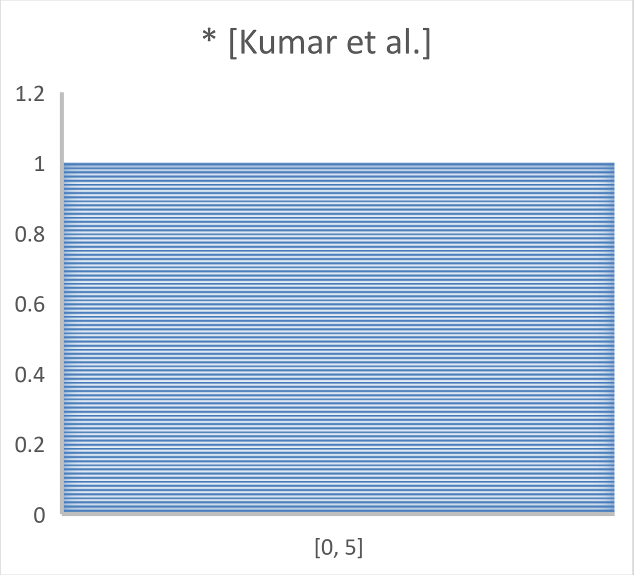

Fig. 4 Record of Elliptic Curve Cryptography

4. Simulation Analysis and Evaluation

A. Communication cost

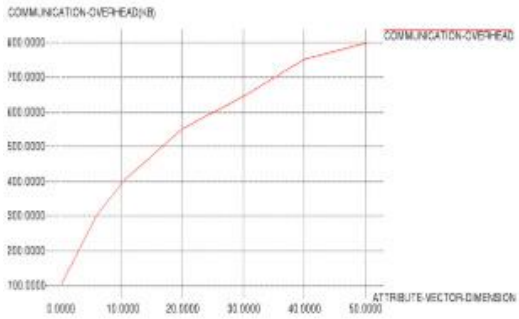

Fig. 5 Communication Cost versus Attribute Vector Dimension for proposed scheme

B. Time cost of individual client

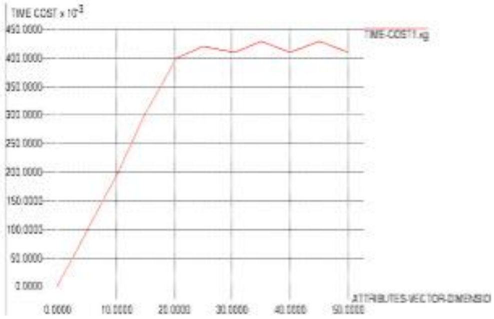

Fig. 6 Time Cost

C. Time cost Key generation for time taken for proposed scheme

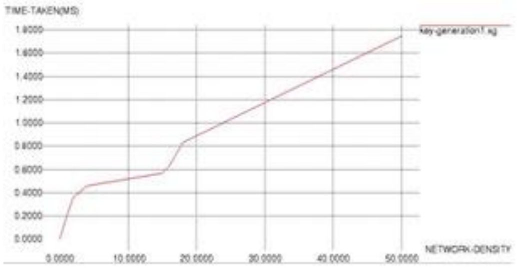

Fig. 7 Key generation for time taken for proposed scheme

D. Throughput

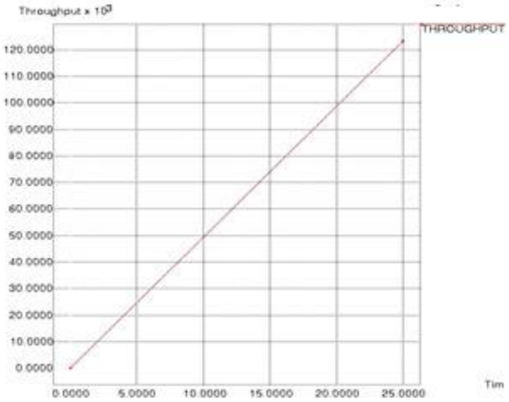

Fig. 8 Throughput for proposed scheme

Table 3 Record of Elliptic Curve Cryptography

Sr No	EC/WC	IK (bit)
1.	Curve1174	251
2.	Curve25519	255
3.	Curve383187	383
4.	Curve41417	414
5.	Curve448	448
6.	E-521	521

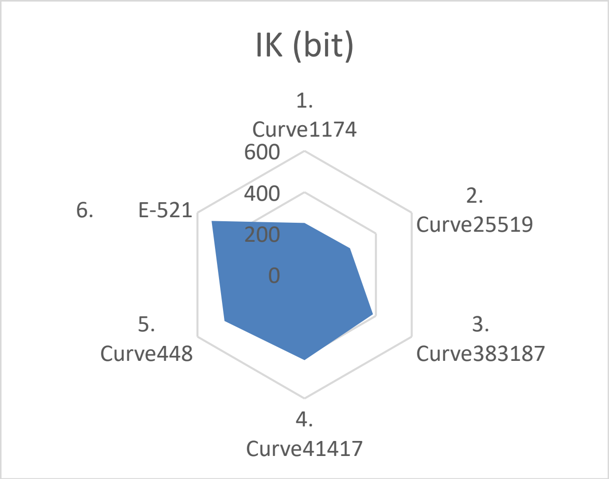

Fig. 9 Record of Elliptic Curve Cryptography over Finite Fields using EC/WC

The Fig. 8 depicts the d=300 values for EC/WC (Edwards Curve or Weierstrass form), which provide the enhanced results for the proposed hypothesis i.e. multiserver server authentication scheme. In Table 3 represents record of Elliptic Curve Cryptography over finite fields using EC/WC. The Fig. 10 depicts ECC over finite field usingEC/WC.

BRUTE FORCE ATTACK

The brute force attack is about to check all possibilities until you find the correct one

REPLY ATTACKS

The replay attack is to misdirect the recipient.

DoS ATTACK

DoS attack is to refute the authentic user access from numerous resources.

DICTIONARY ATTACK: In this attack uses a dictionary of common words to identify the user’s password and try to access to the system.

INSIDER ATTACKS

Insider attacks occur when an employee uses their authorized access to intentionally or inadvertently harm an organization by stealing, exposing or destroying its data. However, negligence is something you can actively work to avoid. This article will help you gain a better idea of how a negligent insider threat originates and what can be done to prevent an attack from costing your company millions.

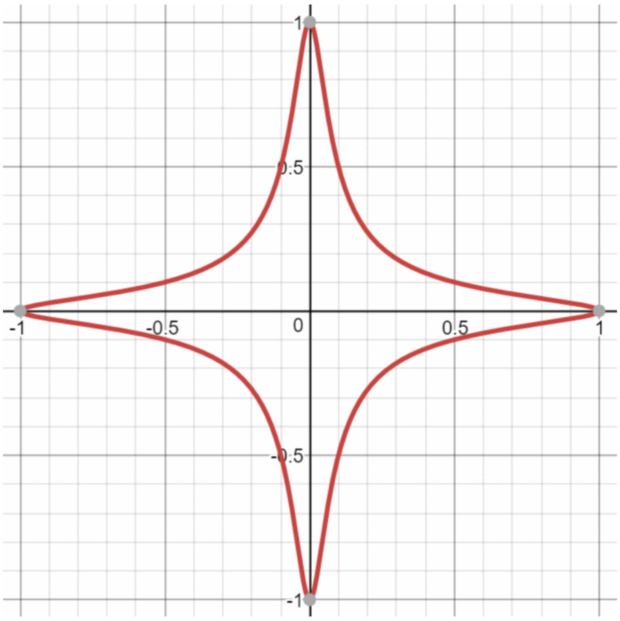

Fig. 10 Elliptic Curve Cryptography over Finite Fields using EC/WC

Elliptic Curve Cryptography over finite fields using EC/WC with no samples are provided in Table 4.

Table 4 Elliptic Curve Cryptography over finite fields using EC/WC with no samples

Name of malware	Label	Number of Samples	Description
Virtool:Win32/CeeInject	CeeInject	630	Used to inject malicious code into other applications which keep running in windows
Ransom:Win32/Grandcrab	Grand Crab	792	Seeks ransom to decrypt data which has been especially Encrypted for such purposes
PWS:Win32/Zbot	Zbot	821	Can steal important banking credentials by form grabbing and browser keystroke logging
PWS:Win32/FareIt	FareIt	836	A kind of keylogger used to steal email credentials, user names, passwords and stored account information,
PUA:Win32/DomaIQ	DomaIQ	978	It is an advertising platform that displays pop-up ads in various browsers.
Trojan:Win32/Skeeyah	Skeeyah	978	It depends on the user’s mistake as it can't spread on its own. It can have access to personal information that it provides to the hacker.
TrojanDownloader:Win32/Upatre	Upatre	990	It downloads and installs other malicious programs or components onto the device.
Virtool:Win32/Obfuscator	Obfuscator	992	It has been encrypted in order not to be detected easily which can be in the form of popups, ads, etc.
Adware:Win32/Bettersurf	Bettersurf	1205	It displays lots of advertisement, underlined words which show

			popups in various browsers.
Worm:Win32/Mira	Mira	1347	It has the potential of creating various copies of itself like a polymorphic worm
Trojan:Win32/Occamy	Occamy	1353	It targets the core system of windows
Virus:Win32/Neshta	Neshta	1369	A kind of virus which gathers information from the system by infecting .exe file
Worm:Win32/Vobfus	Vobfus	1432	Can spread by copying itself, be controlled remotely, and can change window registries
Backdoor:Win32/Berbew	Berbew	1494	Once installed, it creates so many registry entries and executables to ensure berbew's execution every time the operating system gets booted.
		Total 15217	

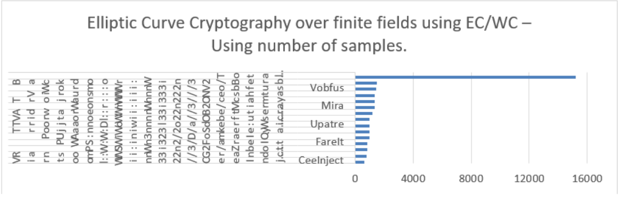

Fig. 11 Elliptic Curve Cryptography over Finite Fields using EC/WC – using Number of Samples

5. Conclusion

In this research paper we used the proposed hypothesis using ECC. ECC provides more security over RSA. We have tested and analyze the performance of secure multi-server password authenticated key agreement scheme using DLMECC for the following guessing attack, reply attack, insider attack, DoS attack and dictionary attack. The proposed scheme is impractical against various attacks.

Acknowledgements

The authors also wishes to thank many anonymous referees for their suggestions to improve this paper

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] Kumari, S., Karuppiah, M., Das, A.K. et al. A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers. J Supercomput 74, 6428–6453 (2018). https://doi.org/10.1007/s11227-017-2048-0

[2] Reddy AG, Das AK, Odelu V, Yoo KY. An Enhanced Biometric Based Authentication with Key-Agreement Protocol for Multi-Server Architecture Based on Elliptic Curve Cryptography. PLoS One. 2016 May 10;11(5):e0154308. doi: 10.1371/journal.pone.0154308. PMID: 27163786; PMCID: PMC4862638.

[3] Chaudhry, S.A., Mahmood, K., Naqvi, H. et al. An Improved and Secure Biometric Authentication Scheme for Telecare Medicine Information Systems Based on Elliptic Curve Cryptography. J Med Syst 39, 175 (2015). https://doi.org/10.1007/s10916-015-0335-y

[4] Chaudhry, S.A., Naqvi, H., Mahmood, K. et al. An Improved Remote User Authentication Scheme Using

Elliptic Curve Cryptography. Wireless Pers Commun 96, 5355–5373 (2017). https://doi.org/10.1007/s11277-016-3745-3

[5] Alowolodu O D, Alese B K, Adetunmbi A O, Adewale O S and Ogundele O S. Article: Elliptic Curve Cryptography for Securing Cloud Computing Applications. International Journal of Computer Applications 66(23):10-17, March 2013.

[6] Lara-Nino, Carlos & Díaz-Pérez, Arturo & Morales-Sandoval, Miguel. (2018). Elliptic Curve Lightweight Cryptography: A Survey. IEEE Access. PP. 1-1. 10.1109/ACCESS.2018.2881444.

[7] Dindayal Mahto and Dilip Kumar Yadav.International Journal of Network Security, Vol.20, No.4, PP.625-635, July 2018 (DOI: 10.6633/IJNS.201807 20(4).04).

[8] Xueqin Zhang, Baoping Wang, Wenpeng Zhang. International Journal of Network Security, Vol.21, No.2, PP.191-198, Mar. 2019 (DOI: 10.6633/IJNS.201903 21(2).02)

[9] Kumari, S., Karuppiah, M., Das, A.K. et al. A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers. J Supercomput 74, 6428–6453 (2018). https://doi.org/10.1007/s11227-017-2048-0.

[10] Mo, J., Hu, Z. & Lin, Y. Remote user authentication and key agreement for mobile client–server environments on elliptic curve cryptography. J Supercomput 74, 5927–5943 (2018). https://doi.org/10.1007/s11227-018-2507-2.

[11] Raman Kumar, "ANALYSIS AND DESIGN OF PROTOCOL FOR ENHANCED SELFISH ROUTING SCHEME", Indian Journal of Computer Science and Engineering (IJCSE), ISSN: 0976-5166, Vol. 8, No. 3, pp. 192-200, Jun-Jul 2017. SCOPUS INDEXED: http://www.ijcse.com/docs/INDJCSE17-08-03-018.pdf

[12] Raman Kumar, Gurpreet Singh, "Analysis and design of an optimized secure auditing protocol for storing data dynamically in cloud computing", Elsevier Materials Today: Proceedings, Volume 5, Issue 1, Part 1, August 2018, Pages 1037-1047, ISSN 2214-7853, SCOPUS and SCI INDEXED. https://doi.org/10.1016/j.matpr.2017.11.180. https://www.sciencedirect.com/science/article/pii/S2214785317324446

[13] Raman Kumar, "Cryptanalytic Performance Appraisal of Improved HLL, KUOCHEN, GENGVRF, FENGVRF Secure Signature with TKIP Digital Workspaces: For Financial Cryptography. Wireless Pers Commun 115, 1541–1563 (2020), ISSN: 0929-6212, SCI INDEXED. https://doi.org/10.1007/s11277-020-07642-2; https://link.springer.com/article/10.1007/s11277-020-07642-2

[14] Amit Verma, Siddharth Dawar, Raman Kumar, Shamkant Navathe and Vikram Goyal, "High utility and diverse itemset mining",Applied Intelligence, ISSN: 1573-7497, SCOPUS and SCI INDEXED, 10.1007/s10489-020-02063-x, Pages 1-15, 2020. doi:10.1007/s10489-020-02063-x (2021). https://link.springer.com/article/10.1007/s10489-020-02063-x

[15] Madhu and Raman Kumar, "Edge-Based Convolutional Neural Network for Improving Breast Cancer Prediction Performance", Mathematical Problems in Engineering, ISSN 1563-5147 (Online), Vol. 2021, Article ID 6613671, 15 pages, 2021. SCOPUS and SCI INDEXED https://www.hindawi.com/journals/mpe/2021/6613671/

[16] P. R. Vig and R. Tandon, "Performance Analysis of Elliptic Curve Cryptography on Reconfigurable Hardware," Lect. Notes Eng. Comput. Sci., vol. 2170, no. 1, pp. 261–264, 2008.

[17] S. Di Matteo, L. Baldanzi, L. Crocetti, P. Nannipieri, L. Fanucci, and S. Saponara, "Secure elliptic curve crypto-processor for real-time iot applications," Energies, vol. 14, no. 15, 2021, doi: 10.3390/en14154676.

[18] K. Murugan and P. Suresh, "Performance Analysis of RSA and Elliptic Curve Cryptography," Int. J. Netw. Secur., vol. 20, no. 4, p. 15, 2018, doi: 10.6633/IJNS.201807.

[19] A. V. Lucca, G. A. M. Sborz, V. R. Q. Leithardt, M. Beko, C. A. Zeferino, and W. D. Parreira, "A review of techniques for implementing elliptic curve point multiplication on hardware," J. Sens. Actuator Networks, vol. 10, no. 1, 2021, doi: 10.3390/jsan10010003.

[20] A. Kardi, R. Zagrouba, and M. Alqahtani, "Performance Evaluation of RSA and Elliptic Curve Cryptography in Wireless Sensor Networks," 21st Saudi Comput. Soc. Natl. Comput. Conf. NCC 2018, no. May 2020, 2018, doi: 10.1109/NCG.2018.8592963.

[21] M. R. Khan et al., "Analysis of Elliptic Curve Cryptography & RSA," J. ICT Stand., vol. 11, pp. 355–378, 2023, doi: 10.13052/jicts2245-800x.1142.

[22] F. Maqsood, M. Ahmed, M. Mumtaz, and M. Ali, "Cryptography: A Comparative Analysis for Modern Techniques," Int. J. Adv. Comput. Sci. Appl., vol. 8, no. 6, pp. 442–448, 2017, doi:

10.14569/ijacsa.2017.080659.

[23] L. D. Singh and K. M. Singh, “Implementation of Text Encryption using Elliptic Curve Cryptography,” Procedia Comput. Sci., vol. 54, no. 1, pp. 73–82, 2015, doi: 10.1016/j.procs.2015.06.009.

[24] A. M. Abdul-Hadi, Y. abdul-sahib Saif-aldeen, and F. G. Tawfeeq, “Performance Evaluation of Scalar Multiplication in Elliptic Curve Cryptography Implementation using Different Multipliers Over Binary Field GF (2233),” J. Eng., vol. 26, no. 9, pp. 45–64, 2020, doi: 10.31026/j.eng.2020.09.04.

[25] I. Khalid, T. Shah, S. M. Eldin, D. Shah, M. Asif, and I. Saddique, “An Integrated Image Encryption Scheme Based on Elliptic Curve,” IEEE Access, vol. 11, no. December 2022, pp. 5483–5501, 2023, doi: 10.1109/ACCESS.2022.3230096.

[26] K. M. Abirami, R. Srikanth, and R. Kavitha, “INTELLIGENT SYSTEMS AND APPLICATIONS IN Comparative Analysis of Elliptic Curve Cryptography Methods and Survey of Its Applications,” vol. 11, pp. 430–434, 2023.

[27] N. Josias Gbètoho Saho et al., “Comparative Study on the Performance of Elliptic Curve Cryptography Algorithms with Cryptography through RSA Algorithm,” 2020, [Online]. Available: https://hal.science/hal-02926106.