International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Methodology for Elliptic Curve Cryptography-Based Digital Signature Scheme: A System with Enhanced Security

[1]S. Senthil Kumar, [2]Dr. K. Poongothai, [3]M. K. Nivodhini, [4]Dr. S. Nithyakalyani

Submitted: 07/02/2024 **Revised**: 15/03/2024 **Accepted**: 21/03/2024

Abstract: To increment rural efficiency, accuracy horticulture incorporates robotization and the utilization of an assortment of IT devices. Here, shrewd contraptions accumulate an immense measure of information and speak with servers and different gadgets over open channels. Subsequently, a few attacks against shrewd cultivating are conceivable. These assaults can have unfavorable impacts since detected information is commonly handled to help assess the condition of horticultural fields and to support navigation. Regardless of the way that few security procedures have been proposed in the writing to resolve these issues, they are either ineffectual or powerless against interruptions. Understanding Diffie-Hellman key trade and utilizing elliptic bend highlights are the most important phases in the task. It finishes up with significant data about Elliptic Bend Cryptography, remembering its viability and productivity for little gadgets, more limited key length, transfer speed reserve funds, simplicity of key age during information encryption and decoding, and surefire quicker encryption and unscrambling.

Keyword: *Elliptic Curve Cryptography, Digital Signature Scheme, Encryption, Hypertext Transfer Protocol, Secured Socket Layer.*

1. Introduction

The study of sending private data is called cryptography. Cryptography is urgent in the present society for some things, such building the web and facing conflicts. It is a fundamental instrument for the headway of human culture. This book sums up the prologue to cryptography, the prologue to elliptic bends, the standards behind ECC, thinks about ECC to different codes, features ECC developments, and applies ECC utilizing the interaction writing audit.

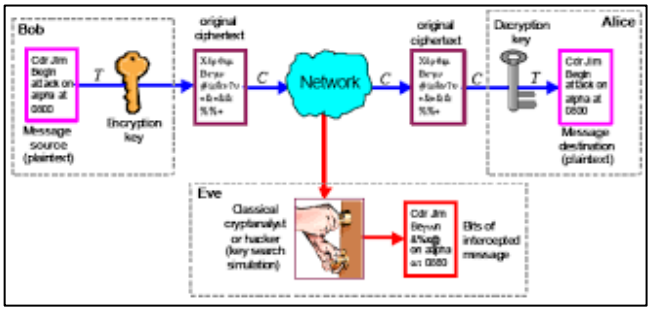

Figure 1: Application of Cryptography using Elliptic Curves

A framework of ECC's development is given. The correlation explains the advantages and disadvantages of ECC. A prologue to cryptography can raise public attention to cryptography, a prologue to elliptic bends and the standards of ECC can teach general society about ECC, and a utilization of ECC can show how it genuinely helps individuals in their everyday lives. These means can assist with working with direct upgrades. In light of everything, this post assists more individuals with finding out about cryptography, particularly ECC, and how we can all cooperate to improve it later on. This page sums up earlier endeavours to further develop ECC and gives a few valuable systems and suggestions for further developing it further.

2. Literature Review

Madaliev et al.'s (2023) the fields of construction and engineering technology are explored in a study published in the Journal of Construction and Engineering Technology. It is probable that the writers investigate several facets of building techniques, supplies, or innovations to improve productivity, durability, or security in the building sector. Unfortunately, it is difficult to offer a thorough critique without access to the particular publication. Nonetheless, it may be assumed from the journal's focus that the research adds to the continuing conversation on improving building techniques.

N. I. Koblitz's (2002) study explores the topic of mathematics, specifically the subfield of cryptography, and was published in the Moscow Mathematical Journal. Koblitz is well known for his contributions to the field of elliptic curve cryptography (ECC), which uses elliptic curve mathematics to offer security. Koblitz may cover the fundamental ideas of ECC, its uses, or developments

[1]*Assistant Professor Department of Electrical and Electronics Engineering K.S.R. College of Engineering, Tiruchengode, TamilNadu-637215*
[2]*Associate professor, Department of information technology, M.kumarasamy college of engineering, Karur. Tamilnadu*
[3]*Assistant Professor, Department of Computer Science and Engineering, K.S.R. College of Engineering Tiruchengode, TamilNadu-637215*
[4]*Professor/CSE KGiSL Institute of Technology Saravampatti, Coimbatore*

in the area during that time in the aforementioned article. Due to its effectiveness and security features, ECC has become increasingly popular and is now an essential part of contemporary cryptographic systems.

Zhdanov and Chalkin's (2013) gives a thorough introduction to the topic of elliptic curves and its applications in cryptography. Basic ideas like discrete logarithm problems, elliptic curve arithmetic, and ECC-based cryptographic protocols are probably covered by the writers. They could also explore real-world applications and enhancements of ECC for a range of cryptographic functions, such as key exchange, digital signatures, and encryption.

Afreen and Mehrotra's (2011) Review focuses on using ECC in embedded systems, which have constrained processor and memory capacities among other computing resources. It is probable that the writers will delve into methods of enhancing ECC algorithms for embedded systems, guaranteeing effective and safe cryptographic functions in settings with limited resources. They could also discuss the difficulties and compromises in putting ECC into practice on embedded systems, such side-channel attack resistance and performance concerns.

3. Methodology

The three primary classes of public-key cryptosystems are summed up in Table 1. The graph plainly exhibits that while the well known assault on ECC calls for remarkable investment, DSA, Diffie Hellman, and RSA may be in every way liable to assaults using subexponentially procedures. Keys for symmetric-key codes are normally shared or communicated by means of public-key frameworks. The symmetric key's work element ought to compare with the sum expected to penetrate the public-key framework utilized for key trade, as the framework's security is just pretty much as solid as its most fragile part.

Table 1. A comparison of cryptosystems using public keys (Vanstone, 2003)

System of public keys	As an illustration	A Mathematical Issue	Most well-known approach to arithmetic problem solving (running time)
Numerical factorization on	Rabin Williams, RSA	Determine the prime factors of a given number, n.	The sieve for number fields is exp [1.923(logn)1/3(lo glogn)2/3]. (Below exponential)
Logarithm in discrete form	ELGamal, DSA, and Diffie-Hellman (DH)	Determine x such that h=gx modn given a prime number n, g, and h.	The sieve for number fields is exp [1.923(logn)1/3(lo glogn)2/3]. (less than exponential)
Discrete logarithm of an elliptic bend	ECDSA and ECDH	Track down x given an elliptic bend E, focuses P and Q on E.	Fully exponential algorithm: Pollard-Rho

EC Diffie-Hellmann class conducts several postprocessing on the secret agreement before providing the value, instead than disclosing it immediately. The key derivation function, or post-processing approach, allows you to select the KDF to use and configure its settings using a set of attributes on the Diffie-Hellman object instance.

5.1. Suggested Method

Standard techniques incorporate the Diffie-Hellman key trade calculation, elliptic bend elements and computations, secluded number-crunching numerical ideas, the Euclidean calculation, and science of cryptography are totally remembered for the periods of the proposed system.

5.3. Supplies and Equipment

The program was developed using the Dev C++ IDE. The primary programming language utilized was C++. A network of computers with a minimum CPU type of Pentium IV or above, a minimum hard drive capacity of 10GB, and a minimum RAM of 1GB may operate the program.

4. Result and Discussion

4.1. Comparison between RSA and ECC Key Lengths

The amount of computer power required and the speed at which encryption and decryption may be completed are directly correlated with the length of the key used in encryption. Table 3 and Figure 4.9 demonstrate how much less the ECC key length is when compared to RSA for the same degree of security. This demonstrates that data encryption using ECC would be quicker than with RSA.

Table 2. Comparing the Key Lengths of ECC and RSA

Bit-wise Security Level	Pieces of the RSA key	Bit length of the ECC key	Approximately the ratio
81	1025	161-224	6-7:2
113	2049	225-256	9-10:2
129	3073	257-284	12-13:1
193	7681	385-512	16-21:2
257	15361	513-572	28-31:2

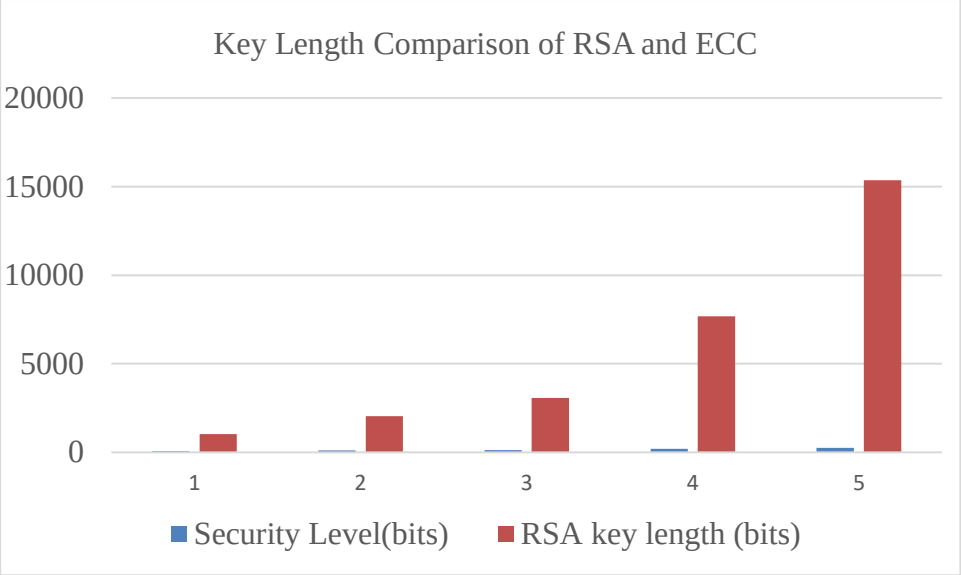

Fig 2: Comparing the Length of Keys in RSA and ECC Cryptosystems

5. Conclusion

Elliptic Curve Cryptography (ECC) is significantly more efficient than other encryption methods, according to the findings of its investigation compared to Rivest-Shamir-Adleman (RSA) and other encryption techniques. The smaller key size and length of elliptic curve cryptography is a crucial security feature. Additionally, it reduces bandwidth, which makes key generation easier for data encryption and decryption, improving performance. ECC also guarantees speedier encryption and decryption, making it effective even on tiny devices. Without a shadow of a doubt, elliptic curve cryptography is a better alternative for data security, based on all the clearly stated outcomes.

References

[1] S. Komolov, Sh. Rakhmatov Fundamentals of Artificial Intelligence. Machine learning. Izhod NAShR Publishing House. p.104. Tashkent, Uzbekistan (2022)

[2] V. Obuxov, Universum: technical sciences, (11-6 (116)), 55-56 (2023)

[3] V.S. Miller, Use of elliptic curves in cryptography. In Conference on the theory and application of cryptographic techniques (pp. 417-426). Berlin, Heidelberg: Springer Berlin Heidelberg (1985)

[4] N. I. Koblitz, Moscow Mathematical Journal, 2(4), 693-715 (2002)

[5] R. Afreen, S.C. Mehrotra, A review on elliptic curve cryptography for embedded systems. arXiv preprint arXiv:1107.3631. (2011).

[6] O.N. Zhdanov, V. A. Chalkin, Elliptic Curves: Foundations of Theory and Cryptographic Applications. Moscow: LIBROCOM Book House, (2013).

[7] T. Dostonbek, M. Jamshid, Central Asian Journal of Theoretical and Applied Science, 4(4), 93-98 (2023).
[8] Z. Abdulkhaev, et.al.,AIP Conference Proceedings 2789, 1 (2023)
[9] M. Madaliev, N. Qurbanova, X. Rustamova, Journal of Construction and Engineering Technology 1(1), 1-6 (2023)
[10] Z.E. Abdulkhaev, et.al., E3S Web of Conferences 420, 07023 (2023).
[11] Vangala, A.; Das, A.K.; Mitra, A.; Das, S.K.; Park, Y. Blockchain-Enabled Authenticated Key Agreement Scheme for Mobile Vehicles-Assisted Precision Agricultural IoT Networks. IEEE Trans. Inf. Forensics Secur. 2022, 18, 904–919.
[12] Shafi, U.; Mumtaz, R.; García-Nieto, J.; Hassan, S.A.; Zaidi, S.A.R.; Iqbal, N. Precision Agriculture Techniques and Practices: From Considerations to Applications. Sensors 2019, 19, 3796.
[13] Shi, X.; An, X.; Zhao, Q.; Liu, H.; Xia, L.; Sun, X.; Guo, Y. State-of-the-Art Internet of Things in Protected Agriculture. Sensors 2019, 19, 1833.
[14] Vangala, A.; Das, A.K.; Chamola, V.; Korotaev, V.; Rodrigues, J.J. Security in IoT-enabled smart agriculture: Architecture, security solutions and challenges. Cluster Comput. 2022, 26, 879–902.
[15] Bera, B.; Vangala, A.; Das, A.K.; Lorenz, P.; Khan, M.K. Private blockchain-envisioned drones-assisted authentication scheme in IoT-enabled agricultural environment. Comput. Stand. Interfaces 2022.