Online at: https://researchtrendsjournal.com ISSN No: 2584-282X

INTERNATIONAL JOURNAL OF TRENDS IN EMERGING RESEARCH AND DEVELOPMENT

Volume 1; Issue 1; 2023; Page No. 281-285

Received: 20-11-2023
Accepted: 24-12-2023

Role of data security in elliptic curve cryptography

[1]Ranjita and [2]Dr. Gautam Kumar Rajput

[1]Research Scholar, Sunrise University Alwar Rajasthan, Rajasthan, India
[2]Associate Professor, Sunrise University Alwar Rajasthan, Rajasthan, India

DOI: https://doi.org/10.5281/zenodo.13643253

Corresponding Author: Ranjita

Abstract

Elliptic Curve Cryptography (ECC) has emerged as a powerful tool in modern cryptographic systems, offering high security with relatively small key sizes. As data security becomes increasingly critical in the digital age, ECC's role in safeguarding information is more prominent than ever. This paper explores the significance of data security within the framework of ECC, emphasizing its efficiency, scalability, and robustness against attacks. By leveraging the mathematical properties of elliptic curves, ECC provides strong encryption while minimizing computational overhead, making it ideal for resource-constrained environments such as mobile devices and IoT networks. The paper also discusses the challenges and advancements in implementing ECC, particularly in protecting sensitive data from emerging threats like quantum computing. Overall, ECC's integration into various security protocols highlights its essential role in ensuring data integrity, confidentiality, and authenticity in an increasingly connected world.

Keywords: Elliptic curve cryptography, robustness, security, data, efficiency, integrity, confidentiality, and authenticity

Introduction

The term "data security" refers to the practice of keeping sensitive information safe from prying eyes. Protecting information against loss in the event of a disaster. Natural catastrophes, server or computer failure, theft, or any other event that might cause data loss are all examples of such problems. A big obstacle for them is ensuring the security of the information that is kept on computers and sent over public networks. A number of writers have offered definitions of information security that boil down to:

"Preservation of confidentiality, integrity and availability of information. Note: In authenticity, accountability, non-repudiation and reliability can also be involved" according to the standards set forth by ISO/IEC 27000:2009... [Kahate 2008, Stallings 2011].

"The protection of information systems as well as information against unauthorized access, disclosure, use, modification or destruction in order to provide confidentiality, integrity, and availability." (CNSS, 2010) [Kahate 2008, Stallings 2011]

Determination/sharing of shared secret key using ECC

Using definition 1.2.4 Aman and Bobby generates their Pair of private and public keys as (n_A, P_A) and (n_B, P_B) respectively.

Aman send P_A to Bobby and Bobby send P_B to Aman.

Aman calculates $K_A = n_A . P_B$ and Bobby calculates $K_B = n_B . P_A$ Shared secret key of Aman and Bobby is given by $K_A = K_B = K$. It is noticeable that $K \in E$.

Anformation/data sharing between Aman and bobby using symmetric encryption with ECC: Suppose Aman want to communicate with Bobby using the point M (as on E). Aman uses shared secret key M in plain text, using K to encrypt it as

$C = M + K$

After receiving C from Aman, Bobby uses shared secret key K in order to crack the encrypted text message C.

$M = C + K^{-1}$

Information/data sharing between Aman and bobby using asymmetric encryption with ECC

Aman uses Bobby encrypts the plain text using its own private key and its public key. text message *M* as

$C = \{n_A . P, M + n_A . P_B\}$

After receiving cipher text message C from Aman, Bobby uses Aman's public key and its own private key are needed to decode the encrypted message C as

$M = (M + n_A . P_B) - n_B(n_A P)$

Example 1.1 Compute and exchange Secret shared key between two users on the elliptic curve $E_{211}(0, -4)$ to the base point (2, 2).

Solution: Suppose Aman and Bobby want to swap an elliptic curve secret key $E_{211}(0, -4)$ to the base point (2, 2)
Here P = (2, 2)

$$E_{211}(0,-4) = \{(x,y): y^2 mod\ 211 = (x^3 - 4) mod\ 211\}$$

Using equation 1.2, 1.3 and 1.4, it can be easily checked that 240(2, 2) = 0,

Which imply that order (P) = 240 i.e. n = 240
Aman and Bobby respectively select integers n_A = 121 and n_B = 203 as their private keys and calculate their public keys P_A and p_B as
$P_A = n_A . P = 121(2, 2) = (115, 48)$
$P_B = n_B . P = 203(2, 2) = (130, 203)$
Again, Aman and Bobby respectively compute
$K_A = n_A . P_B = 121(130, 203) = (161, 69)$
$K_B = n_B . P_A = 203(115, 48) = (161, 69)$
Now exchanged shared secret key of Aman and Bobby is given by $K_A = K_B = K$

ECC as a lightweight cryptography

WSN, RFID, Smart Grid, e-Health, and other developing technologies in IoT paradigms benefit from lightweight cryptography. This distinguishes itself from the ECC in that it has to demonstrate that it understands the limitations of lightweight cryptography implementation applications and adjusts demands appropriately. These boundaries include those related to energy, size, performance, and safety. The same security features that should be preserved in both ECC and lightweight cryptography are comparable. It may thus be used to provide comparable security characteristics. The strength of the ECC-based lightweight cryptography relies on how stiff the discrete logarithmic issue is. This concept may be used to provide service signature, encryption, authentication, and key installation in conjunction with a security protocol. Following that, these technologies may be used in the constrained environment for the previously mentioned applications in the fields of security, defense, and health care.
Lightweight ECC systems that are suitable for resource-constrained applications were the focus of research. Mathematical models may be one factor contributing to ECC's low weight; design and implementation choices may be the other. Cryptographers look at which ECC implementations are most popular and thought to be lightweight. Figure 1. depicts a set of keywords related with lightweight cryptography, while Figure 2. illustrate ones that are based on ECC.

Fig 1: A set of keywords belong to lightweight cryptography

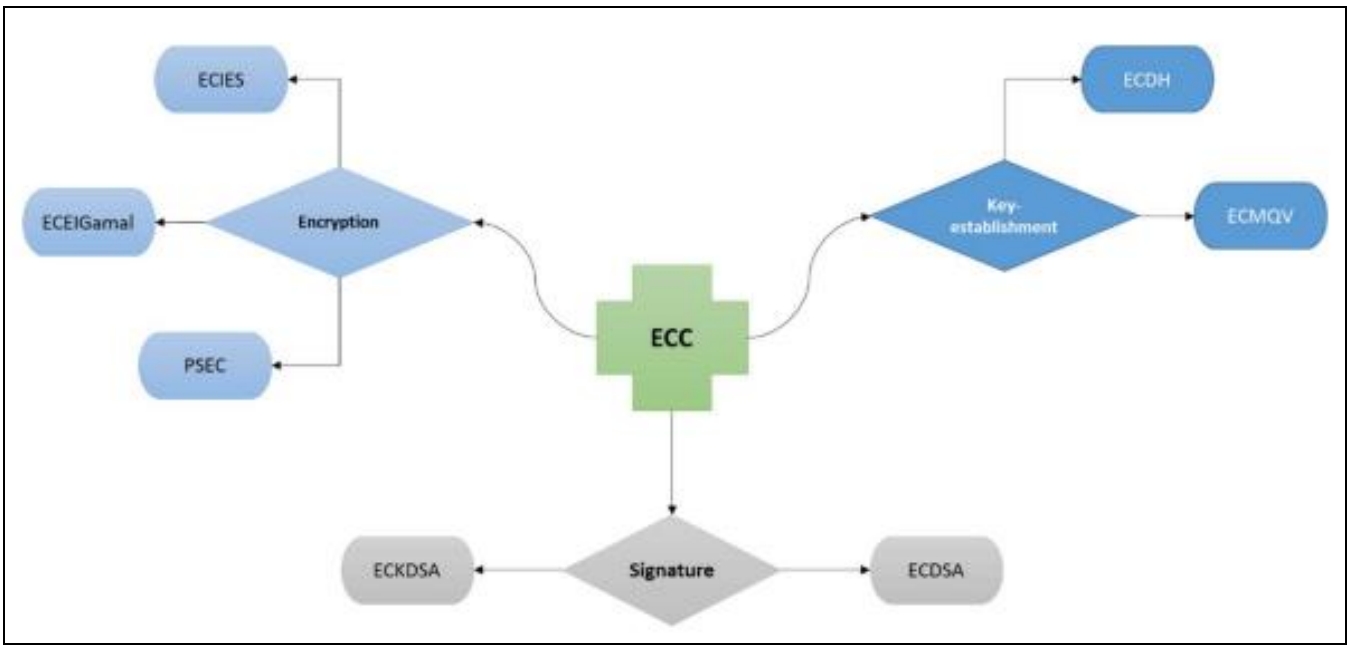

Fig 2: Different Elliptic curve-based schemes

Lightweight protocols are designed to supply security service for applications with limited resources. Authentication, signature, and key establishment are the most popular security services; however, data encryption is also considered. These schemes are very efficient and their efficiencies can be calculated using the communicated quantity of bits and estimated step matrix for necessary number of operations, as the work involving protocol design do not carry out execution of their solution.

Mathematical concepts for security

The cryptographic algorithm used for providing information security contains the essence of modern algebra in its every step. That is the concepts of modern algebra including set theories, relationships, algebraic functions, group theories, rings, fields, integral domain, and number theories are contributed in Cryptographic Algorithms. All of the above-mentioned algebraic concepts contribute significantly to the creation of algorithms that provide information exchange and web security.

Groups, rings and fields

Natural numbers are the most popular type of numbers in number theory. The notation of the natural numbers is N. Sometimes, natural numbers are called Whole numbers or counting numbers and 0,1,2,3... is the format of the Natural numbers. The numbers consisting of positive and negative numbers are said to be Integers. The notations followed for the representation of the natural numbers is Z. The number 0 is common to both positive and negative numbers and the set {... -2, -1, 0, 1, 2.} is the format of the Natural numbers. A rational number is an integer divided by a positive integer. That means, any integer can be placed in the numerator and only a positive integer can be placed in the denominator. The notation of the rational number is Q={x/ y | x ϵ Z, y ϵ N} and this is the format of the Rational numbers. The format of the complex numbers is "a+bi" where "a" and "b" in this are real numbers and hence it is divided into real and imaginary parts in which "i" is called the imaginary unit.

Groups

The concept of groups was developed by a team of three mathematicians and the most prominent member among them is Joesph Louis Lagrange. He proposed the idea of permutation groups, sub-groups, order of groups and his theorem on sub groups says that the order of a subgroup divides the order of a group.It was later on used for the development of cyclic groups and also the Galois Theory. The mathematician Galois in 1832 defined the concepts of normal subgroups, solvable groups and he asserted the existence of Sylow subgroups.

A group is represented by {G, *}, consisting of elements from the non-empty set G with the binary operation '*', such that for the following mathematical properties namely,

1 Closure property, ie, ∀ a, b, if a, b ϵ G, the n a*b ϵ G.
2 Associative Rule: ∀ a, b, c ϵ G, a*(b*c)=(a*b)*c.
3 The reality of identity: ∃eϵG: if a ϵ G, then a*e=a=e*a.
4 Inverse Existence: For every a ϵ G, there is a member

a^{-1}ϵGsuchthatthepropertya*a^{-1}=e=a^{-1}*a are satisfied.

Rings

A ring is a non-empty set G together with two binary operators, namely + and * (addition and multiplication, respectively) satisfying the properties namely closure, associativity, commutativity, existence of identity and inverse rules for addition, multiplicative associativity as well as left and right distributivity rules.

Field

A field is a commutative ring with unity in whose multiplicative identity is assigned to each non-zero element. Finite Fields A finite field is consisting of a finite number of elements, namely n and it is also, also called as Galois field. A Galois field has pm elements where p isa prime number m is a positive integer. For any prime p and positive integer m, there is always a Galois field of order pm which is existing. Two finite fields are said to be isomorphic if they have the same order. This is called as the Galois field of the order p^m, which is denoted by either GF (p^m) or F_p^m. Here, p is called the characteristic of the known finite field GF(p^m). In general, the properties of the field Fareed noted as char(F) = p. Moreover, the arithmetic operations over the finite field can be reduced simply to multiplication modulo p and addition modulo p. The study of Groups, Rings and Fields are the basis for the development of many cryptographic algorithms.

Elliptic curve cryptography

Elliptic-Curve Cryptography (ECC) is an approach proposed in the public key cryptography that occurs in finite fields based on the algebraic structure of elliptical curves. When Elliptic curve cryptography is compared with other public key cryptography algorithms, the ECC allows smaller keys for encryption and decryption based on the Galois fields and also provides equivalent protection to other cryptography. Public-key cryptography is based on the inherent nature of the mathematical functions. Initially, some assumptions were there about the public-key system, which means that it is very difficult to factorize the multiplier value of a large number among two prime numbers with two or more factors. Later, the basic assumption is made such that it will be difficult and not possible to find the discrete logarithm of the random point on the elliptic curve. This is called the "Elliptical Curve Discrete Logarithm Problem".

In the generic RSA approach, encryption is performed using the public key. Additionally, the private key linked to the encryption is used to decode the encrypted communication. These asymmetric algorithms' characteristics vary depending on the connection between the keys used in them. That is, it is depending on the difficulty in locating another key associated with it using one key. If we list the contributions of Public Key cryptography, that are many including Fermat's theorem, Euler's theorem, Group Theory, El-gamal cryptography, the RSA algorithm, and the Diffie-Hellman key exchange algorithm.

The level of security varies in these algorithms depending on the computations provided in these algorithms and the length of the key used in it. Table 1. provides a comparison of RSA and ECC algorithms in order to understand the key sizes of RSA and ECC algorithms and they perform the

encryption of data in a given time duration. There a son most companies choose ECC as an alternative to the RSA key algorithm is the short key of the ECC and also the ability of it to provide the same security level.

Table 1: Comparison of key sizes.

Security Level(bits)	RSA Key Size(bits)	ECC Key Size(bits)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	512

Computational Efficiencies of ECC

There are a number of articles discussing about the security of the ECC and the effectiveness of its implementation. The main strength of ECC is its ease of use and its high-speed performance. The elliptical curve process requires more mathematical operations than the others. That is, more mathematical operations than algebraic multiplication are required, for example when modules within modular functional groups can be used for multiplication and measurement point multiplication using a very small ellipse of finite fields when similar protection is required. Therefore, it is assumed that the elliptical curve cryptographic functions are more than 8 times faster than a modular algebraic multiplier, and gives the same level of protection. Furthermore, the advantages of ECC are better storage performance, lower cost of operation, better storage performance for bandwidth storage and smaller memory.

Security Issues

The basic necessity of the Discrete Logarithm for the Elliptic Curve The problem is in the Elliptic Curve Digital Signature Algorithm's and Cryptosystems' capacity to withstand security breaches. In other words, P is a point on the elliptical curve E if Zp is a group and n is the value of the number of elements or consecutive points. The point is defined as follows: Q = lp, where l is an integer that falls between 0 and n-1. Moreover, it is attacking software and hardware related industries. For most of them, software attacks are one of the most unusual. Such attacks are more likely to occur and such general attacks can be easily handled by making greater use of mathematical functions to effectively prevent this. In elliptical curve notation, the change in position of the elliptical curve is used to provide better security. The complexity of the analytical area of the elliptical curve is greatly enhanced by the fact that the matrix translation method is integrated with it, without making any changes to the optimal performance of the elliptical curve cryptography. These functions have been used with the elliptical curve of the matrix translation method. Although there is various mathematical functions are used in ECC, the matrix displacement functions multiply the security of the symbolism many times over. By emphasizing that their properties are strong. Furthermore, algorithms such as the polynomial algorithm, the Greatest Common Divisor – Least Common Multiple (GCDLCM) algorithm etc also use the Eigen values and Eigen vectors of matrices. It is emphasized that the three algorithms also combines with the algorithm proposed here to increase its security.

Matrix translation approach to security

Box brackets are a typical way to express matrices. In a matrix, the rows represent the horizontal data lines and the columns represent the vertical data lines. The quantity of rows and columns that make up a matrix is what determines its size. An m × n matrix, often known as an m-by-n matrix, is a matrix with m rows and n columns, and the numbers m and n represent its dimensions. These are the measurements of the following matrix are 2×3 up (read-two by three), because there are two rows and three columns.

Translation is a change in the structure of geometry without changing the orientation. In other words, each point of an image or place moves at a given distance and in a specific direction. That means, adding a fixed value or direction to each point and also changing its appearance is called the translation. Any translation can call isometric. This is because it protects the distance transformation between two points and also can call by the bijective. For translation functions, $R^2 \rightarrow R$, that is $f(A) = f(A + t)$.

In elliptic curve cryptography, finding the random elliptic curve element which is made by discrete logarithm is very difficult. Moreover, combination of matrices translation concept with Elliptic Curve Cryptography is a very difficult task of finding the element of the elliptic curve. In this work, A novel safe routing technique that relies on clustering and encryption has been suggested. Elliptic Curve Cryptography (ECC) is used for encryption in this algorithm since it improves the capacity to provide high-level data security with a smaller key size. In addition, this study proposes a novel matrix translation-based technique for creating keys, including private and public keys. It becomes more challenging for an opponent to predict the key using our suggested matrix translation mechanism. Current cryptographic techniques are made more secure in this manner. Even if a cluster head is hacked, attackers can still not get encryption data or knowledge of data thanks to this. In a particular sensor network, the ECC is used for the purpose of producing public and private keys for the participating sensor nodes. Here, we zero in on the cluster head election procedure and the cluster head compromised attack as potential energy hogs.

Creating a novel cryptographic technique to enhance data security during transmission in wireless sensor networks is the primary goal of this study. The network's lifespan is extended beyond that of a regular network by implementing security measures during data transfer. In this paper, a novel cryptographic method, ECC, is suggested for use in WSN data encryption during transmission from source sensor node to destination or base station, together with a matrix translation-based encryption system. The main things this study accomplished are: Initial work on the key generation, encryption, and decryption phases involves incorporating novel approaches. The second part of our presentation is devoted to the two kinds of tables that we will be covering: space reference tables and prime number generation. First, before encrypting and decrypting the text, the values for the spaces that appear in it are assigned using the Space reference table. Afterwards, it uses the Prime number generation table and the String Position based ASCII value to transform the strings into numerical digits, allocating the closest prime number to each created numerical digit. Third, separate processes for generating public and private keys

have been established. In this work, we provide a novel encryption and decryption strategy that uses these key generation processes to secure data on WSNs. The paper concludes with the proposal of two new algorithms, namely

1. Encryption and decryption algorithm based on prime numbers and American Standard Code for Information Interchange (ASCII)
2. Method for Secure Routing using Matrix Translation and Elliptic Curve Cryptosystem (MTECSR) using a clustering approach.

Improvements in security, packet delivery ratio, and overall network performance are the key benefits of these methods. Reduced energy consumption, latency, and encryption/decryption complexity are further benefits of the suggested safe routing technique.

Conclusion

Elliptic Curve Cryptography (ECC) plays a pivotal role in modern data security, offering a robust and efficient mechanism to protect sensitive information in a wide range of applications. Its ability to provide strong encryption with smaller key sizes compared to traditional cryptographic methods makes it particularly valuable in environments where computational resources are limited. ECC's mathematical foundation ensures a high level of security, even in the face of evolving cyber threats.

As the digital landscape continues to expand, the importance of ECC in safeguarding data cannot be overstated. Its implementation in secure communications, digital signatures, and encryption protocols demonstrates its versatility and effectiveness. Moreover, with the advent of quantum computing, the need for cryptographic systems that can withstand future challenges is becoming increasingly urgent. ECC's potential to adapt and evolve in response to these challenges makes it a cornerstone of next-generation cryptography.

In conclusion, the role of data security in ECC is not only critical but also essential for maintaining trust and integrity in the digital world. As organizations and individuals continue to rely on digital platforms for communication, commerce, and data storage, ECC will remain a key player in ensuring that sensitive information remains secure, confidential, and protected from unauthorized access.

References

1. Sergienko VA. Quantum communications and cryptography. CRC Press; c2018.
2. Bouchard F, Sit A, Hufnagel F, Abbas A, Zhang Y, Heshami K, Fickler R, Marquardt C, Leuchs G, Karimi E. Quantum cryptography with twisted photons through an outdoor underwater channel. Opt Express. 2018;26:22563-22573.
3. Qi B, Li Q, Lo H-K. A brief introduction of quantum cryptography for engineers. In: Book Chapter. Publisher: arXiv; c2010.
4. Lucamarini M, Yuan ZL, Dynes JF. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. Nature. 2018;557:400-403. Available from: https://doi.org/10.1038/s41586-018-0066-6
5. Yuan Z, Plews A, Takahashi R, Doi K, Tam W, Sharpe A, Dixon A, Lavelle E, Dynes J, Murakami A, Kujiraoka M. 10-Mb/s quantum key distribution. J Lightwave Technol. 2018;36(16):3427-3433.
6. Azuma K, Tamaki K, Munro WJ. All-photonic intercity quantum key distribution. Nat Commun. 2015 Dec 16;6:10171.
7. Quantum cryptography and the future of security. Oct 8, 2018. Accessed May 13, 2019. Available from: https://www.wired.co.uk/article/quantum-cryptography-and-the-future-of-security
8. Bernard Z. A First Introduction to Quantum Computing and Information. Springer International Publishing; 2018.
9. Barcan J. Quantum code cracking creeps closer. IEEE Spectrum. 2000.
10. Gokhale P. How does Shor's algorithm work in layman's terms? Nov 16, 2015. Accessed May 13, 2019. Available from: https://www.quora.com/How-does-Shors-algorithm-work-in-laymans-terms
11. Krambeck D. Fundamentals of Quantum Computing. Aug 6, 2015. Accessed May 13, 2019. Available from: https://www.allaboutcircuits.com/technical-articles/fundamentals-of-quantum-computing/
12. Monz T, Nigg D, Martinez EA, Brandl MF, Schindler P, Rines R, Wang SX, Chuang IL, Blatt R. Realization of a scalable Shor algorithm. Science. 2016;351(6277):1068-1070.