International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Elliptic Curve Cryptography with the Introduction of Montgomery Ladder Algorithm (Physics)

Mrs. B. Divya Rekha[1], S. Deepika[2], Avneet Kaur[3]

[1]Asst. Professor, Department of Computer Science, Hyderabad, India
[2]Student (BCA), Bhavan's Vivekananda College, Hyderabad, India
[3]Student (Bsc Mecs), Bhavan's Vivekananda College, Hyderabad, India
[1]b.d.rekha0310@gmail.com, [2]dy25218@gmail.com, avi170105@gmail.com

ABSTRACT—

Most of the risks of attacking the cloud server come from the inside, many organizations have insisted on protecting the cloud server from the outside. Cryptography refers to the process of hiding or coding information so that only the person a message was intended for can read it. For decades, cryptography has been employed for coding messages and is continued in bank cards, computer passwords, confidential government data, and e-commerce. This cybersecurity practice is more famously referred to as cryptology, wherein a set of different domains or fields-such as computer science, physics, and mathematics-are combined to establish complex codes in encrypting messages and keeping them secure.

It keeps the communication and information encrypted and unreadable by any unauthorized parties. Various algorithms or mathematical concepts turn messages into unreadable codes using cryptographic keys, techniques of digital signing to protect data privacy, credit card transactions, emails, and browsing.

Keywords—Cryptography, Elliptic Curve Cryptography, Encryption, Decryption, Montgomery Ladder Algorithm, Scalar Product

Literature review

The traditional algorithms in asymmetric cryptography are RSA, Elliptic Curve Diffie-Hellman, which have been the basis for safe communications between systems till date.

While the day-to-day demand for greater security and more proficient cryptographic techniques has increased, researchers looked toward alternatives that would provide better performance without sacrificing security in the process. Of the recent lots of development, elliptic curve cryptography has gained considerable attention because of strong security with smaller key size and hence emerged as an effective tool in modern cryptographic application.

ECC is a form of public-key encryption technology based on principles inherent in elliptic curve theory that can be used to generate smaller, yet more proficient cryptographic keys. The most frequently found uses of ECC nowadays are in digital signatures with cryptocurrencies, such as Bitcoin and Ethereum, and one-way encryption of emails, data, and software.

An elliptic curve isn't actually an ellipse-or oval shape-but graphically it is represented by a looping line that intersects through two axes, which are lines on a graph used to show the position of a point. The resulting curve is symmetric, or reflected, along the x-axis of the graph.

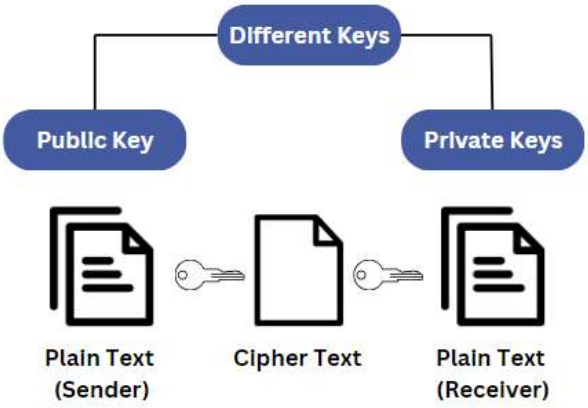

Figure 1: Cryptography mechanism

For ECC key generation, it is based more on the properties and relationship of an elliptic curve equation rather than a traditional method of generation - being the product of large prime numbers. From a cryptographic point of view, the points along the graph in Figure 2-6 can be derived using the following equation:

$y^2=x^3 + ax + b$

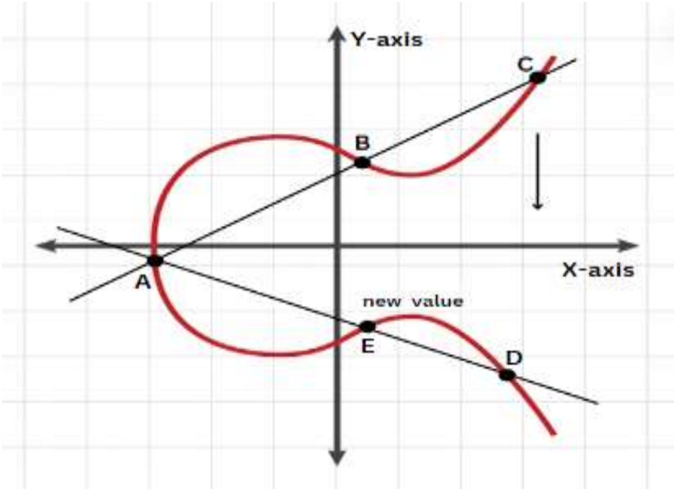

Figure 2: Elliptic curve cryptography graph

Given below are a few advantages of the elliptic curve cryptography:

Higher Security per Bit

Due to the mathematical properties of elliptic curves, ECC offers a higher security level per bit of key length. This means that for the same key length, ECC provides stronger security than RSA or DSA.

Efficiency

Smaller key sizes in ECC result in faster computation, which leads to quicker encryption and decryption processes. This efficiency makes ECC particularly suitable for environments where processing power, memory, or bandwidth is limited, such as mobile devices and embedded systems.

Lower Resource Consumption

Because ECC requires less computational power and memory, it is ideal for devices with constrained resources. This makes it a preferred choice for applications like IoT (Internet of Things), where power and computational efficiency are crucial.

Scalability

ECC scales well with increasing security requirements. As computing power grows and security needs increase, ECC can be scaled to higher security levels without a substantial increase in computational overhead, unlike RSA, which requires exponentially larger key sizes for small increases in security.

Preliminary Data

ECC is a variant of public key cryptography, with various advantageous factors over other public key cryptosystems. However, there are also disadvantages of using it. A few of them are listed below:

Key Exchange Complexities

Key exchange in ECC uses asymmetric keys. For an instance, Elliptic Curve Diffie-Hellman is more difficult to implement than their classic key exchange siblings. Because the core of an ECC key exchange involves heavier mathematical operations like point multiplication and modular arithmetic, it becomes really very difficult to overcome the implementation challenges. Also, in ECC key exchange, parameters need to be selected with great care and should be validated.

Side Channel Attacks

Such an approach is vulnerable to a variety of attacks, including timing and power analysis attacks, which could reveal the secret of a system. In one such attack, information from the implementation-such as execution time for some operations or characteristics in power consumption-may be used to recover the private key, or possibly the electromagnetic radiation emitted by the device.

For example, if any time attack is present, then the attacker can measure the time that is being executed for a scalar multiplication operation. On the basis of this, he may recover the key.

Limitations on Key Size

While ECC grants strong security with smaller key sizes, the key size itself becomes a limitation. The larger the key size gets, the more secure it becomes but computational overhead increases too. For example, a 256-bit ECC key has equivalent security to a 3072-bit RSA key. Applications requiring security levels even higher than these may also require larger key sizes.

Implementation challenges

While it can be secure and efficient, ECC is actually quite sensitive in its implementation and may be extremely challenging for the average developer in cryptography to implement. In the implementation of ECC, one needs to make sure the elliptic curve is implemented well, that key generation and exchange are securely executed, and the implementation is resistant to side-channel attack.

Quantum Computer Vulnerability

It should be mentioned that a quantum computer could make some sort of attack for which ECC would be vulnerable, probably breaking the encryption. Quantum computers make some kinds of calculations way faster than a classical computer could; this might be used in order to attack systems based on ECC.

Proposed Algorithm

The Montgomery ladder is an algorithm to perform scalar multiplication that is a method used in elliptic curve cryptography. This will be an idea for one to effectively compute the scalar multiplication of a point on an elliptic curve, i.e., one of the main operations in ECC.

Scalar multiplication in ECC has been performed by repeated doubling and adding points on the curve, referred as the double-and-add algorithm. However, this may leak information under some side-channel attacks hence compromise the security of the system.

The Montgomery ladder algorithm does its scalar multiplication in a very different way, evaluating the scalar product via a sort of ladder of steps, where each ladder step involves some lightweight addition or multiplication that is done in some side-channel-attack-resistant manner. Another considerable advantage of the Montgomery ladder algorithm is its efficiency and that it inherently prepares for implementation in a form resistant to side-channel attack. It will likely prove an attractive solution to implement in ECC systems, at least for applications where security is overriding.

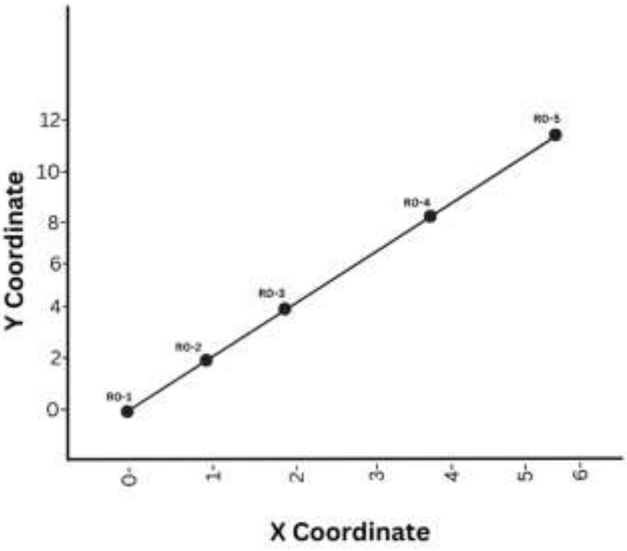

Figure 3: Montgomery Ladder Algorithm Graph

Testing

The Montgomery ladder algorithm computes the scalar product in elliptic curve cryptography using a "ladder step" approach. Each ladder step contains some basic arithmetic operations, such as addition and doubling of a point; this is made in such a way that it provides resistance to side-channel attacks. It gives uniformity in computation processes from which an attacker cannot get information. If something is represented mathematically, it would depict a sequence of the kind of operations applied to the points of an elliptic curve, ensuring efficiency and safety with respect to scalar multiplication. Given below is the mathematical description of the algorithm.

Elliptic Curve Cryptography makes great use of scalar multiplication wherein a point P on an elliptic curve is multiplied by an integer k to get another point, Q=kP. Montgomery ladder provides this multiplication in a secure and rather efficient way.

Input

A Point P on an elliptic curve.

A scalar k (normally large integer).

Output

Q = kP, which is the product of the point P and the scalar k.

Algorithm Initialization

Set R0=P (at the initial point)

Set R1=2P (point addition)

Ladder Step (for each bit ki, from the most significant to the least significant):

To process each bit ki of the binary representation of k:

If ki=0:

R0=R0+R1;

R1=2R1

If ki=1:

R1=R0+R1;

R0=2R0

Final Result:

At the end of the loop, the point kP is in R0.

Binary Representation:

K = (kn−1 kn−2…k1 k0) in binary representation where ki's are the bits of k and kn-1 is the most significant bit.

Initialization:

R0 🡐 P

R1 🡐 2P

Ladder Step (for every bit ki from the most significant to the least significant):

For every bit ki in binary representation of k:

If ki=0:

R1 🡐 R0+R1;

R0 🡐 2R1

If ki=1:

R0🡐R0+R1;

R1 🡐 2R0

Output:

Returns R0 which is kP.

Comparative Analysis

The Montgomery ladder algorithm is among the most efficient and secure methods of performing scalar multiplication in an ECC that boasts very high resistance against side-channel attacks, thus granting very high security for cryptographic applications. It is superior compared to a double and add algorithm because it resists side-channel attacks and is highly efficient and secure. Though it has a higher degree of complexity, its advantages make it highly applicable in settings of secure web browsing, digital signatures, and key exchange.

While ECC refers to a broad category of public-key cryptography systems in general, Montgomery ladder is a specific method of scalar multiplication. The Montgomery ladder thus works inside the ECC system and provides one of the secure and efficient ways of carrying out scalar multiplication. Given below is the comparison between ECC and Montgomery ladder algorithm:

Table 1: Comparison Analysis on ECC and Montgomery Ladder Algorithm

Basis of comparison	ECC	Montgomery Ladder Algorithm
Objectives	The principle of Elliptic Curve Cryptography (ECC) is the application of the elliptical curve over the finite field which is a of public-key cryptography.	The Montgomery Ladder is a tactic made for scalar multiplication on ECC that offers higher speed and levels of security than ECC.
Functionality	Provided that ECC can generate public and private keys with shorter lengths and certificates, secure key exchange, digital signatures, and encryption are among the cryptographic methods made possible with Elliptic Curve Cryptography (ECC).	The Montgomery Ladder is the approach for scalar multiplication with some side-channel attack security, which may include timing attacks.
Security	The main stake of ECC security lies in key size where more significant the key length more is the safety therefore, it belongs to ECC.	To the contrary, the Montgomery Ladder is a specification in cryptography which does not let the attacker guess a large portion of the diagnostic query. Therefore, the cryptographic problem of generating the key and scalar multiplication is solved in a safe way.

Implementation	ECC allows for multiple implementations which depend on the curve and the switch to another algorithm.	The Montgomery Ladder is in the ECC scalar multiplication and its main role is in the secure implementation of ECC.
Approach	One of the ECC public key cryptosystems, which have lower keyed system facilities and are much more secure, is the larger one.	One of the ways in ECC is to repeatedly use Montgomery Ladder technique, which, in turn, is prime in the process of execution and therefore it provides security successfully against side-channel attacks.

Conclusion:

Elliptic Curve Cryptography (ECC) has emerged as a powerful tool in modern cryptography due to its efficiency and high-security levels, even with smaller key sizes. The introduction of the Montgomery Ladder algorithm further enhances the security and efficiency of ECC by offering a method for secure scalar multiplication that resists side-channel attacks, a common vulnerability in cryptographic implementations. This paper demonstrates that the Montgomery Ladder algorithm provides a robust solution for applications requiring high security, particularly in environments where resistance to side-channel attacks is paramount. Through comparative analysis, it is evident that the Montgomery Ladder algorithm, while more complex, offers significant advantages in secure cryptographic operations, making it a critical component in the advancement of ECC-based systems.

Acknowledgment

We are grateful for the invaluable support and guidance of Ms Divya Rekha throughout this research mission.

We also feel thankful about the resources provided by Bhavan's Vivekananda College that allowed us to go for this research.

Lastly, we praise our colleagues and peers for providing constant support.

References

[1] https://www.keyfactor.com/blog/elliptic-curve-cryptography-what-is-it-how-does-it-work/

[2] https://www.geeksforgeeks.org/blockchain-elliptic-curve-cryptography/

[3] The Montgomery Powering Ladder published by B. S. Kaliski Jr

[4] https://crypto.stackexchange.com/questions/47895/advantages-of-montgomery-ladder-based-scalar-multiplication

[5] Two Layer Symmetric Cryptography Algorithm for Protecting Data from Attacks published by Muhammad Nadeem, Ali Arshad, Saman Riaz, Syeda Wajiha Zahra, Shahab S. Band and Amir Mosavi

[6] Research on neural network chaotic encryption algorithm in wireless network security communication published by Chen Liang, Qun Zhang, Jianfeng Ma, and Kaiming Li

[7] https://www.techtarget.com/searchsecurity/definition/elliptical-curve-cryptography

[8] https://en.wikipedia.org/wiki/Elliptic_curve_point_multiplication