wjert, 2024, Vol. 10, Issue 8, 15-25. Review Article ISSN 2454-695X

World Journal of Engineering Research and Technology
WJERT
www.wjert.org
SJIF Impact Factor: 7.029

SURVEY OF ELLIPTIC CURVE CRYPTOGRAPHY AND ITS SECURITY APPLICATIONS

Bamarouf Mohamed*, Ahmed Asimi and Mbarek Lahdoud

Department of Mathematics, Faculty of Sciences, Ibnou Zohr University B.P 8106, City Dakhla, Agadir, Morocco.

Article Received on 11/06/2024 **Article Revised on 01/07/2024** **Article Accepted on 22/07/2024**

***Corresponding Author**
Bamarouf Mohamed
Department of Mathematics, Faculty of Sciences, Ibnou Zohr University B.P 8106, City Dakhla, Agadir, Morocco.

ABSTRACT

Elliptic curve cryptography (ECC) over the finite fields, whose Elliptic curve cryp- tosystems are based on ECDLP (Elliptic Curve Discrete Logarithm Problem which is the problem of finding the positive number n given a point nP, where P is a point on the curve) for their security, is a powerful branch of cryptography (public key and secret key). The discrete logarithm (DL), in a finite field, is one of the NP −complete problems in number theory and it applies in several fields such as elliptic curves and cryptography. This problem has been raised by several authors such as Martin Hell- man, Tonelli Shanks, John M. Pollard, Adleman. Moreover, numerous methods have been proposed to solve it like Pohlig-Hellman algorithm, Baby-Step, Giant-Step algo- rithm, Rho-Pollard algorithm and Index computation algorithms. The ECC widely used in various security applications due to its efficiency, strong security properties and shorter keys (less-memory requirements and faster field arith- metic operations) such as authentification protocol design, key generation protocol, key exchange protoco, digital signatures, hash functions, security proofs in topical areas like cloud computing, blockchains, Internet of Things and Artificial Intelligence. Our aim in this paper is to present an extensive and careful study of elliptic curve cryptography (ECC) over finite fields and its security applications and also to discuss the arithmetic involved in elliptic curve and how these curve operations are crucial in determining the performance of cryptographic systems.

KEYWORDS: Elliptic curve cryptography, Finite fields, Security applications, Cloud computing, Blockchains, Internet of Things.

1 Introduction, Notations and Background on finit fields and Elliptic Curves

1.1 INTRODUCTION

In cryptography, the computer security of IoT and cloud computing based on public key cryptosystems characterized by the possibility of sharing encryption keys, while keeping the keys secret of decryption, is based on calculations of discrete logarithms in finite fields, more precisely, on the difficulty of Computation Diffe−Hellman problem (CDH) and Decision Diffe-Hellman problem (DDH).

1.2 Notations

In this section we introduce the notation and terminology that will be used throughout this paper.

N	:	The set of natural numbers.
= =	:	Boolean equality
:=	:	Affectation equality
=	:	Equation equality
! =	:	Boolean negation
Fp	:	Finite field of order a prime number p.
F^*_p	:	Cyclic multiplicative group of all non zero elements in Fp of order p − 1.
θ(G)	:	The order of group G.
[n, m] with n < m	:	range of integers between n and m
ϕ()	:	Euler Indicator.
θ(a)	:	The order of a.
mod	:	Modulo.
r = n%m	:	r is the remainder of the Euclidean division of n by m.
E(x)	:	Integer part.
DLAP	:	Discret Logarithm Arithmetic Peoblem.
DLP	:	Discret Logarithm Problem.
DHP	:	Diffie-Hellman Problem.
NFS	:	Number Field Sieve.
CDH	:	Computation Diffe −Hellman
DDH	:	Decision Diffe −Hellman

ECDLP : Elliptic Curve Discrete Logarithm Problem

1.3 Background on Discrete Logarithm Problem and Elliptic Curves over finite fields

We refer to[19], [2], [4], [20], [17],[18], [9] and we deduce the following results. Theorem 1.1. Every finite field is commutative and admits a primitive element. Theorem 1.2. Let (K, +,.) be a finite field, the multiplicative group K∗ is cyclic.

Definition 1.1. Let (K, +,.) be a finite field. A generator of the multiplicative group K∗ is called a primitive element of K.

Definition 1.2. For a nonnegative integer k, the kth Fermat number Fk is defined by Fk = 22k + 1.

Definition 1.3.: A primitive element of Fp is a generator of a cyclic units group $F*_p$.

1.4 Elliptic curves over finite fields

In 1985, Miller[12], Koblitz[7] independently proposed a cryptosystem based on elliptic curves in a finite field.

Definition 1.4. An elliptic curve in a finite field Fp is the set of points (x, y) ∈ Fp ×Fp such that y2 = x3 + ax + b mod p with a, b ∈ Fp and 4a3 + 27b2 /= 0 to which we add a point at infinity O, denoted by E(Fp) = {(x, y) ∈ Fp × Fp; y2 = x3 + ax + b mod p and 4a3 + 27b2 /= 0} ∪ {O}.

Propriety 1.1. Let Fp be a finite field with p > 3. The set E(Fp) endowed with the law + defined by:

1. For all P ∈ E(Fp) : P + O = O + P = P.
2. LEt P (x, y) ∈ E(Fp) : −P = (x, −y).
3. Let P1(x1, y1), P2(x2, y2), P3(x3, y3) ∈ E(Fp) with P1 /= −P2. If P1 + P2 = P3(x3, y3) then we get.

$$\begin{cases} x_3 &= \lambda^2 - x_1 - x_2 \\ y_3 &= \lambda(x_1 - x_3) - y_1 \end{cases} \quad where \begin{cases} \lambda &= \frac{y_2 - y_1}{x_2 - x_1} \quad where\ P_1 \neq P_2 \\ \lambda &= \frac{3x_1^2 + a}{2y_1} \quad ELSE \end{cases}$$

Lemma 1.1. We can define the multiplication by a scalar of a point on elliptic curves.

$$For\ all\ k \in \mathbb{N}^*\ k \cdot P = \underbrace{P + P + \ldots + P}_{k\ times}$$

The main operation performed in a protocol based on elliptic curves is the multiplication of a point by a scalar. The most common algorithm for performing this operation is the Doubling and Addition algorithm.[3]

Definition 1.5.: A primitive element of Fp is a generator of a cyclic units group $F*_p$.

Definition 1.6. Let g ∈ Fp. g is a primitive element of Fp if the order de g in the units group $F*_p$ is p − 1.

Lemma 1.2. The number of primitive elements of Fp is ϕ(p − 1).

The references used in the following are:[10][6][1][8][14]

1.5 Elliptic Curve Discrete Logarithm Problem

The Elliptic Curve Discrete Logarithm Problem (ECDLP) stands as a cornerstone in modern cryptography, particularly in elliptic curve-based systems.

In essence, ECDLP involves determining the exponent d in the equation Q=d.P, where P is a point on a specific elliptic curve and Q is another point on the same curve. This task proves exceptionally challenging, even with knowledge of the points' coordinates.

Security in elliptic curve cryptography hinges on the formidable complexity of solving the ECDLP. Traditional algorithms like Baby-step Giant-step and Pollard's rho struggle to efficiently crack this problem when elliptic curve parameters are carefully chosen to ensure ample size.

Put simply, while the ECDLP theoretically permits resolution, real-world elliptic curves are engineered to render solving this problem exceedingly difficult, even with state-of-the-art algorithms and resources.

Cryptographic systems leveraging ECDLP are prevalent across various modern security protocols, including Elliptic Curve Cryptography (ECC) for encryption and digital signatures. Yet, it's vital to emphasize that the efficacy of these systems heavily relies on meticulously selecting elliptic curve parameters and accurately implementing associated cryptographic algorithms.

2 Cloud computing security based on elliptic curves

In addition, utilizing ECC in cloud computing enables.

1. Lower Resource Usage: ECC requires smaller key sizes compared to other asymmetric encryption algorithms like RSA. This means less computational power and memory are needed for key generation, encryption, and decryption operations, making it ideal for resource-constrained cloud environments.
2. Faster Performance: The smaller key sizes and efficient algorithms of ECC result in faster cryptographic operations. This can improve overall system performance and responsiveness in cloud applications, especially when handling a large number of si- multaneous cryptographic operations.
3. Improved Scalability: ECC's efficiency extends to its scalability. As cloud comput- ing environments often need to scale dynamically to accommodate varying workloads, ECC's ability to handle cryptographic operations efficiently can contribute to smoother scalability without sacrificing security.
4. Reduced Bandwidth Usage: Smaller key sizes in ECC result in shorter ciphertexts, which can reduce the amount of data transmitted over the network. This is advan- tageous in cloud computing scenarios where bandwidth usage is a concern, such as in mobile cloud computing or data-intensive applications.
5. Resistance to Quantum Attacks: ECC is believed to be more resistant to quantum computing attacks compared to traditional cryptographic algorithms like RSA. This future-proofs data encrypted with ECC against potential advances in quantum com- puting technology.

Overall, ECC offers a compelling combination of security, efficiency, and scalability that makes it well-suited for securing data and communications in cloud computing environments. The integration of Elliptic Curve Cryptography (ECC) into cloud computing provides several significant advantages. Firstly, it ensures compliance with modern security standards such as Transport Layer Security(TLS), thereby ensuring the security of communications over the Internet. Moreover, its flexibility and compatibility with a variety of hardware and software platforms allow for deployment in different cloud environments, providing developers and administrators with freedom of choice. By simplifying key management through the use of smaller key sizes, it addresses major security concerns in the cloud. Additionally, encrypting data with ECC enhances the confidentiality of stored and transmitted data, meeting requirements for privacy protection and regulatory compliance. Lastly, with its ability to adapt to future advances in cryptography, ECC ensures scalable security in an ever- evolving cloud environment. In summary, ECC in cloud computing offers a comprehensive solution

for securing data and communications in a distributed and shared environment.

3 Blockchain security based on elliptic curves

Blockchain is a revolutionary technology in decentralized systems that enables secure decentralized transaction processing while ensuring data privacy and authenticity. It is now playing a significant role in several areas such the Internet of Things, supply-chain management, manufacturing, cyber-physical systems, healthcare systems, and much more. Unlike centralized transaction processing solutions, blockchain uses a distributed ledger mechanism to record data transactions on multiple devices, this will prevent data breach, identity theft, and a plethora of cyber-related attacks, in essence, leading to a sustainability in data privacy and security.

The blockchain is a database in the form of a chain of signed blocks. Each block contains transactions. Blockchain technology (or network) is the database replicated on all nodes and under a set of protocols establishing algorithms. In order to recap, we give the blockchain properties below, for all the details see.[16][13][15]

1. Each block is made up of two parts: a header which records metadata and a body which groups transactions;
2. The blocks are connected by a Merkle tree; where the fingerprints are written in the header;
3. Each participant can have a copy of the database;
4. A consensus algorithm ensures that a decision is obtained by all the nodes instead of a central entity.

4 Security in Internet of Things based on elliptic curves

ECC (Elliptic Curve Cryptography) serves as a cryptographic technique employed to safeguard communications across networks, notably within the realm of the Internet of Things (IoT). The following encapsulates key insights into ECC's role within IoT.

1. ECC Overview: Unlike conventional methods like RSA, ECC leverages elliptic curves for key generation, renowned for its comparable security to RSA but with a notable advantage in smaller key sizes. This aspect makes ECC a pragmatic choice for environments with constrained resources, such as IoT devices.
2. Security Features: ECC's robust security stems from its inherent difficulty in solving the discrete logarithm problem on elliptic curves, a foundation of its operations. Consequently, ECC ensures formidable resistance against attacks, with the extraction of

private keys from public keys posing a significant challenge for potential adversaries.

3. IoT Integration: Given the prevalent limitations in processing power, storage capacity, and communication capabilities within IoT ecosystems, ECC emerges as a favored cryptographic solution. Its ability to reduce key sizes translates into substantial savings in device resources, thereby aligning seamlessly with the exigencies of IoT deployments.
4. Energy Efficiency: Particularly noteworthy within the IoT landscape is ECC's contribution to energy conservation. By necessitating less computational power for cryptographic operations owing to smaller key sizes, ECC facilitates extended battery life for IoT devices, a critical consideration in IoT applications.
5. Implementation Considerations: Effective integration of ECC within IoT environments mandates adequate hardware and software support. Developers must prioritize the incorporation of ECC cryptography libraries and meticulously select elliptic curves tailored to the specific requirements of their IoT applications.

So ECC emerges as a proficient and secure cryptographic paradigm ideally suited for fortifying communications amidst IoT devices. Its adeptness in delivering robust security while accommodating resource constraints underscores ECC's pivotal role in advancing the security landscape of IoT deployments.

5 Security in Artificial Intelligence based on elliptic curves

Elliptic curves are utilized in artificial intelligence (AI) for various applications, notably in cryptography and security. They offer intriguing mathematical properties for creating secure encryption systems, as seen in public key encryption algorithms such as the Elliptic Curve Digital Signature Algorithm (ECDSA) or Elliptic Curve Diffie-Hellman (ECDH). Beyond security, elliptic curves are also employed in certain machine learning algorithms, particularly for classification and prediction. Their utilization primarily resides in the realm of deep learning and reinforcement learning, where they can model complex relationships among data. In these domains, elliptic curves can be utilized in several ways: Modeling Complex Relationships: Elliptic curves can model nonlinear relationships among data. Unlike linear models, elliptic curves can capture more complex and nonlinear relationships between variables, which can be crucial for complex machine learning tasks. Feature Extraction: Elliptic curves can also extract relevant features from data. By representing data as points on an elliptic curve, machine learning techniques can extract discriminative features that can be used for classification, prediction, or other tasks. Learning Representations: In the context of

deep learning, elliptic curves can be integrated into the architecture of neural networks to learn data representations. For example, they could be used as nonlinear transformation layers in a neural network to learn more abstract and discriminative representations of input data. In summary, the use of elliptic curves in machine learning offers intriguing possibilities for modeling complex relationships, extracting relevant features, and learning data represen- tations in advanced machine learning tasks. A concrete example of using elliptic curves in machine learning could be in the field of image recognition. Suppose we have a dataset of human face images and we want to develop a facial recognition system. We could use elliptic curves to extract features from faces in the images. For instance, we could represent each face as a set of points on an elliptic curve, where the coordinates of the points are deter- mined by features such as the shape of the face, contours of the eyes, nose, and mouth. By employing machine learning techniques such as convolutional neural networks (CNNs), we could train a model to recognize faces based on features extracted from elliptic curves. The model could learn to distinguish between different individuals by analyzing the spatial and structural relationships among points on elliptic curves. Thus, elliptic curves would serve as the basis for representing faces in feature space, and machine learning would be used to learn to recognize faces based on these representations. This example illustrates how elliptic curves can be integrated into a machine learning system to solve complex pattern recognition tasks.

Elliptic curve-based encryption enhances security in machine learning by encrypting both data and models. For example, in medical applications, patient data, including diagnoses and medical histories, is encrypted before sharing. A third-party researcher receives en- crypted data for model training without accessing decrypted data. The trained model can diagnose new patients without revealing personal data. This approach ensures data security, preserving patient privacy while enabling AI model utilization in medical settings.

Elliptic curves offer a robust means to bolster the security of machine learning endeav- ors, allowing for the encryption of both data and models. By employing elliptic curve-based techniques, sensitive data can be encrypted prior to its utilization in training AI models. This strategy guarantees that in the event of data compromise, it remains indecipherable without the requisite decryption key. Furthermore, elliptic curve-based encryption meth- ods can safeguard communications among different components of an AI system, effectively mitigating threats related to data interception or tampering.

6 Comparison study

In the four aforementioned domains, a comparison of the performance of the two asymmetric cryptography systems (ECC vs RSA) will yield the following two tables.[5] and [11], through the following tables, demonstrate that key sizes and allocated re- source capacities are superior in ECC compared to RSA.

Key Size.

Table 1: Security levels recommended by NIST.

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

Encryption/Decryption Delays

Table 2: Time in seconds for 256 bits.

Security Level (bits)	Encryption ECC	Encryption RSA	Decryption ECC	Decryption RSA	Total Time ECC	Total RS
80	7.9240	0.5596	22.8851	19.3177	30.8091	19.87
112	39.7008	0.5815	26.3331	102.0337	66.0339	102.6
128	58.4386	0.5611	27.4060	209.6086	85.8446	210.1
144	77.5034	0.5718	32.1522	311.0649	109.6556	311.6

What makes ECC also suitable for smartphones, tablets, and 'small' connected devices is its lower computational requirements, reduced memory usage, and lower energy consumption compared to RSA. Additionally, the total encryption/decryption time is better in ECC than in RSA starting from a security level of 112 bits.

REFERENCES

1. KM Abirami, R Srikanth, and R Kavitha. Comparative analysis of elliptic curve cryptography methods and survey of its applications. International Journal of Intelligent Systems and Applications in Engineering, 2023; 11(11s): 430–434.
2. M Welleda Baldoni, Ciro Ciliberto, and Giulia Maria Piacentini Cattaneo. Elementary number theory, cryptography and codes. Springer, 2009.
3. Daniel J Bernstein and Tanja Lange. Faster addition and doubling on elliptic curves. In international conference on the theory and application of cryptology and information security, 2007; pages 29–50. Springer.

4. John William Scott Cassels and Albrecht Fr¨ohlich. Algebraic number theory: proceedings of an instructional conference. Academic press, 1967.
5. Levent Ertaul and Nitu J Chavan. Rsa and elliptic curve-elgamal threshold cryptography (ecceg-tc) implementations for secure data forwarding in manets. Threshold, 2007; 7(8): 9.
6. Mohammad Rafeek Khan, Kamal Upreti, Mohammad Imran Alam, Haneef Khan, Shams Tabrez Siddiqui, Mustafizul Haque, and Jyoti Parashar. Analysis of elliptic curve cryptography & rsa. Journal of ICT Standardization, 2023; 11(4): 355–378.
7. Neal Koblitz. Elliptic curve cryptosystems. Mathematics of computation, 1987; 48(177): 203– 209.
8. Carlos Andres Lara-Nino, Arturo Diaz-Perez, and Miguel Morales-Sandoval. Elliptic curve lightweight cryptography: A survey. IEEE Access, 2018; 6: 72514–72550.
9. Jiyou Li and Daqing Wan. On the subset sum problem over finite fields. Finite Fields and Their Applications, 2008; 14(4): 911–929.
10. Meilin Liu, Kirill Kultinov, and Chongjun Wang. The implementations and applications of elliptic curve cryptography. Proceedings of 39th International Confer, 2024; 98: 89–102.
11. Dindayal Mahto and Dilip Kumar Yadav. Rsa and ecc: a comparative analysis. International journal of applied engineering research, 2017; 12(19): 9053–9061.
12. Victor S Miller. Use of elliptic curves in cryptography. In Conference on the theory and application of cryptographic techniques, pages 417–426. Springer, 1985.
13. Satoshi Nakamoto and A Bitcoin. A peer-to-peer electronic cash system. Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf, 2008; 4(2): 15.
14. Sonali U Nimbhorkar and LG Malik. A survey on elliptic curve cryptography (ecc). International Journal of Advanced Studies in Computers, Science and Engineering, 2012; 1(1): 1– 5.
15. Francesco Restuccia, Salvatore D Kanhere, Tommaso Melodia, and Sajal K Das. Blockchain for the internet of things: Present and future. arXiv preprint arXiv. 2019; 1903. 07448.
16. Tara Salman, Maede Zolanvari, Aiman Erbad, Raj Jain, and Mohammed Samaka. Security services using blockchains: A state of the art survey. IEEE communications surveys & tutorials, 2018; 21(1): 858–880, 2018.
17. Pierre Samuel. Th´eorie alg´ebrique des nombres, 1967.
18. William Stein. Elementary number theory: primes, congruences, and secrets: a compu-

tational approach. Springer Science & Business Media, 2008.

19. Oleg Nikolaevich Vasilenko. Number-theoretic algorithms in cryptography, volume 232. American Mathematical Soc, 2007.
20. Lawrence C Washington. Introduction to cyclotomic fields, volume 83. Springer Science & Business Media, 1997.