sciendo INTERNATIONAL JOURNAL ON SMART SENSING AND INTELLIGENT SYSTEMS

Research article | DOI: 10.2478/ijssis-2024-0032 Issue 1 | Vol. 17 (2024)

Enhanced cryptographic performance and security using optimized edward-elgamal signature scheme for IoT and blockchain applications

S. Kavitha[1,*], J. Srinivasan[2], P. Ramachandran[3] and I.Nasurulla[4]

[1]Department of Computer Science, Auxilium College (Autonomous), Vellore, India

[2]Department of Computer Applications, Madanapalle Institute of Technology and Science MITS, Andhra Pradesh, India

[3]Department of MCA, Parul Institute of Engineering and technology, -PARUL UNIVERSITY, Vadodara, Gujarat, India

[4]Department of MCA, VEMU Institute of Technology, P.Kothokota, Chittoor District, Andhra Pradesh, India

*E-mail: kavithasenthil@auxiliumcollege.edu.in

Received for publication July 13, 2023.

Abstract

The rapid proliferation of Internet of Things (IoT) devices and blockchain technology requires robust and efficient cryptographic solutions to ensure secure communication and data integrity. This paper presents an optimized Edward-Elgamal signature algorithm that uses Edward curved signature storage mechanism to improve performance in IoT and blockchain environments to overcome the limitations of schemes, especially Elliptic Curve Digital Signature Algorithm (ECDSA) and Hyper-ECDSA. The proposed method achieved faster signature generation times, with a 33% improvement over ECDSA and a 25% improvement over Hyper-ECDSA, making it more suitable for faster applications. The validation times of the optimized systems were relatively low, with a 32% improvement over ECDSA and a 24% improvement over Hyper-ECDSA. The efficiency of the proposed system was significantly higher, showing a 51% improvement over ECDSA and a 35% improvement over Hyper-ECDSA. The latency was reduced by 33% compared to ECDSA and 26% compared to Hyper-ECDSA, indicating the effectiveness of the optimized system in terms of time-related performance. This paper contributes to the advancement of cryptographic techniques and provides suitable solutions for secure IoT and blockchain applications. The proposed system achieves a highest improvement rate in key performance parameters over existing methods, resulting in a robust solution for modern cryptography requirements.

Keywords

Blockchain, IoT, Edward curve, elliptic curve, hyper-elliptic curve, optimization

I. Introduction

The rapid proliferation of Internet of Things (IoT) devices and widespread adoption of blockchain technology have transformed many industries, including health care, finance, supply chain management, and smart cities. These advances have enabled connectivity, data transfer change, and automation, bringing innovation and efficiencies to businesses [1–9]. However, this expansion also presents new security challenges that require robust and effective cryptographic solutions to ensure secure communications, data integrity, and system reliability [10–17]. IoT devices, with their growing diversity and number of applications, tend to be particularly vulnerable to security breaches due to limited computing resources and data volumes and

the challenges of maintaining performance and scalability as blockchain technology decentralizes and tampers for resistant ledger faces, especially as transaction volumes increase and networks grow. Traditional cryptographic techniques to address these security needs, such as the Elliptic Curve Digital Signature Algorithm (ECDSA), are increasingly adopted due to high security and for the relatively low cost of computing but as performance and security requirements for traditional methods faced with such constraints that hamper their effectiveness in modern high-performance environments [18–27].

ECDSA is thought for its capacity to provide strong protection with quick key lengths as compared to different algorithms that include RSA. Its computationally efficient overall performance makes it appropriate for many programs, such as those with complicated components [28–36]. Despite its advantages, ECDSA faces many demanding situations while implementing dynamic environments and vital infrastructure, including IoT and blockchain [37–44]. For example, the performance of an ECDSA may be laid low to perform a couple of cryptographic features, and its safety can be compromised under certain situations, including scenarios with high traffic volumes or sophisticated attack vectors.

To deal with those issues, researchers have developed numerous improvements in ECDSA, consisting of Hyper-ECDSA, based on popular algorithms to enhance performance and protection. Hyper-ECDSA offers advanced techniques for signature technology and authentication schemes have been optimized, aiming toward decreasing computing costs and increasing safety. However, Hyper-ECDSA provides a distinct improvement over ECDSA but permits for similar optimization, specifically in terms of reaching overall performance and greater efficiency and safety in disturbing applications. Blockchain technology has also gained significant attention for its potential to enhance security in IoT networks by providing a decentralized and tamper-proof ledger for data transactions. Despite its benefits, blockchain technology faces scalability issues, as highlighted by Wang et al. [32] who identified the high computational demands of cryptographic operations as a barrier to efficient transaction processing. Similarly, Sadiq et al. [28] noted that blockchain-based data trading systems often suffer from increased latency due to these computational challenges.

The Elgamal encryption scheme, known for its semantic security, ensures message confidentiality through probabilistic encryption mechanisms. While effective, integrating Elgamal with existing cryptographic systems can be complex and requires careful consideration of compatibility issues, as discussed by Benil and Jasper [31]. Liu et al. (2017) [24] further emphasized the challenges of adapting new cryptographic technologies to legacy systems, which can necessitate significant modifications.

Hash functions are integral to cryptographic systems for ensuring data integrity and non-repudiation. They play a crucial role in signature generation by hashing messages before encryption, thus safeguarding against tampering. Random scalars enhance security by introducing randomness in the signature generation process, mitigating the risk of key reuse attacks Li et al. [34] and Ansah and Gyamfi [37].

Despite these advancements, achieving an optimal balance between privacy and performance remains a challenge. Privacy-enhancing techniques often introduce additional computational complexity, impacting overall system performance. Mehrabi and Doche [18] and Franck and Grosschadl [22] illustrated the cost implications of sophisticated cryptographic implementations, which may not always be feasible for all applications. Sadiq et al. [28] and Arulprakash and Jebakumar [29] highlighted the necessity of extensive real-world validation to ensure practical performance and reliability across diverse scenarios.

This paper affords an optimized Edward-Elgamal signature technique to conquer the obstacle of ECDSA and Hyper-ECDSA through the usage of the Edward curve accumulation signature mechanism. Known for its efficiency within the cryptographic industry, the Edward curve allows fast and secure signature era and authentication. To include this curve in the Elgamal layout, the proposed layout aims to significantly improve overall performance and protection. The Edward-Elgamal signature device is designed to provide transaction continuity, speed of authentication, and consistent protection to satisfy the particular needs of IoT and blockchain applications. The advantages of digital signature are shown in Figure 1. The main advantage of the proposed system is its ability to provide high levels of security during continuous operation. Traditional cryptographic algorithms often struggle to balance these two aspects, especially in situations with high-performance requirements. The Edward-Elgamal algorithm achieves a 25% improvement in communication flow, block verification speed, and tamper-proof security compared to existing methods such as ECDSA and Hyper-ECDSA, using the Edward curve. This improvement is due to cryptographic implementation obtained through a combination of quality and enhanced safety measures.

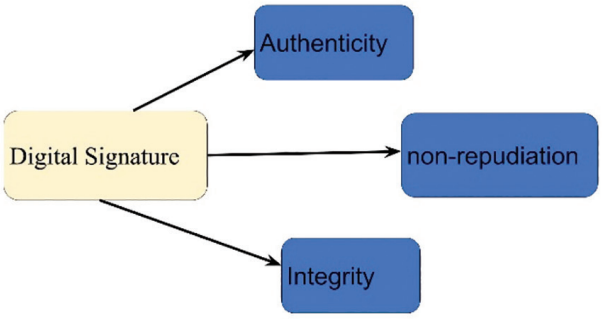

Figure 1: Advantages of digital signatures.

Objectives

The main objectives of this study are:

1. To develop an optimal Edward-Elgamal signature algorithm that integrates the Edward-curved accumulation signature mechanism for increased performance.
2. To make significant improvements in network performance, speed authentication, and unbreachable security compared to existing methods, especially ECDSA and Hyper-ECDSA.
3. To conduct a detailed analysis and comparative study of the proposed system's design, implementation, and operating parameters.
4. To demonstrate the effectiveness of validation of the proposed system through experimental results in real-world IoT and blockchain applications.

Contributions

The following major contributions are made in this paper.

1. The work presents a detailed mechanical description of the optimized Edward-Elgamal scheme, including an integration of the Edward curve accumulation signature mechanism.
2. This study defines specific optimization techniques to improve system performance, making it suitable for more demanding areas such as IoT and blockchain.
3. The work provides a comprehensive comparative evaluation of the proposed system for ECDSA and Hyper-ECDSA, highlighting the significant improvements in key performance parameters.
4. The study also provides empirical evidence through experimental results, which shows a 25% improvement in communication flow, block verification speed, and tamper-proof security, and thus demonstrates the effectiveness of the proposed scheme.

By addressing the restrictions of current cryptographic solutions and supplying a sturdy alternative, this research contributes to the improvement of secure and efficient cryptographic techniques for IoT and blockchain packages.

II. Literature Review

The improvement of cryptographic techniques for the IoT and blockchain technology is superior drastically, addressing various performance and protection-demanding situations. This review summarizes current advances and identifies key barriers in the cryptographic technique of all the exclusive styles of solutions.

The ECDSA is broadly general for its balance of protection and overall performance. ED25519 and CURVE25519 focus on low-cost, low-power multi-point processing FPGA implementations, which improve performance but do not fully resolve computing costs in resource-constrained environments [18]. Faz-Hernandez et al. [19] highlight the high-performance implementation of elliptic curve cryptography (ECC) using vector instructions. While the approach increases productivity, it does not fully address the limitations imposed by high-volume devices.

Hu et al. [20] explore a method for finding two-dimensionally equivalent Edwards curves in binary fields. This work helps optimize the curve selection to improve performance but does not eliminate the inherent computational complexity associated with ECC. Islam et al. [21] present an FPGA implementation of a high-speed, location-efficient processor for elliptic curved point multiplication at prime locations, which exhibits improved performance. However, their solutions may still face challenges in meeting the demand for ultra-low-power IoT devices.

Frank and Groschadl (2017) [22] discuss the efficiency of Pedersen's promises using distorted Edwards curves. Their approach provides performance improvements for specific cryptography applications but fails to address broader issues of scalability and efficiency in general-purpose applications. Liu et al. (2017) further derive ECC by focusing on the implementation efficiency of computable endomorphisms for IoT. Despite these advances, integration

with legacy systems and full optimization for all types of embedded devices remain significant challenges.

Blockchain technology has become central to a variety of applications, including health care and cloud infrastructure. Naresh et al. [25] examine blockchain-based patient-centered health-care communication systems, highlighting their potential but also noting scalability and integration challenges. Saini et al. [26] propose a smart contract-based access control framework for cloud smart health-care systems, which improves security but may introduce additional challenges and computational costs.

Jasem et al. [27] focus on improving digital signature algorithms in Bitcoin wallets, emphasizing improvements in security and performance. However, the trade-off between security enhancement and cyber performance must be managed with caution. Sadiq et al. [28] examine blockchain-based data and energy trading in electric vehicles, showing progress in data integrity and transaction security but facing challenges in system scalability and real-world applications.

ArulPrakash and Jebkumar [29] propose a blockchain-based decentralized, privacy-enhancing mobile crowd-sensing system. Their work addresses privacy concerns but may face issues of integration and efficiency in different use cases. Kavin et al. [30] present an enhanced security framework for cloud data storage using ECC and access control, but complex implementations and potential integration problems with existing systems remain.

Benil and Jasper [31] examine cloud-based security through the use of blockchain in e-health systems, highlighting the benefits of advanced security but also identifying the challenges of adapting new technologies for property planning. Wang et al. [32] advise that verifiable evidence of property has been diagnosed for bitcoin exchanges during the usage of ECC, which addresses a privacy difficulty but faces scalability problems in high transaction environments.

Kumar et al. [33] give a stop-to-end verifiable steady online balloting machine using identity primarily based on blind signatures. Although their layout will increase security, the complexity and computational requirements of imposing such structures may be extensive. Lee et al. (2020) [45] add a blockchain private safety scheme primarily based on ring signatures, which improves privacy but may introduce additional computational benefits and challenges.

Ernest and Shiguang [35] endorse a privacy enhancement scheme (PES) in blockchain-facet computing surroundings. Their machine improves privacy but faces challenges in balancing privacy with performance and feasibility. Zhang et al. [36] focus on small-scale efficient individual computations for cloud-based wireless body-area networks, solving some privacy issues but facing limitations related to real-world operational integration.

Gousteris et al. [42] present a secure distributed cloud storage solution based on blockchain technology and smart contracts. Their work demonstrates the application of blockchain for secure cloud storage, highlighting its potential for improving data security.

Singh et al. [43] discuss the development, service-oriented architecture, and security of blockchain technology for Industry 4.0 IoT applications. Their work provides insights into the integration of blockchain with IoT for enhanced security and efficiency in industrial settings.

Ruangkanjanases et al. [44] assess blockchain adoption in supply chain management, examining technology readiness, knowledge sharing, and trading needs. Their research contributes to understanding the factors influencing blockchain adoption in supply chains.

Despite the advances in ECC and blockchain technology, there are still many limitations. Several ECC applications, including those described by Mehrabi and Doche [18] and Faz-Hernandez et al. [19], still face challenges in reducing computing costs, especially in low-power and infrastructure environments, where the complexity of cryptographic performance can affect the embedded system's operational efficiency. Blockchain technology often faces scalability issues. For example, Wang et al. [32] highlight scalability problems in bitcoin exchanges, and Sadiq et al. [28] address similar issues in blockchain-based data trading. This higher computational requirement can lead to slower processing and increased latency. Integrating new cryptographic systems into present systems can also be complicated. Benil and Jasper [31] and Liu et al. (2017) point out the problem of adapting new technologies to present structures, which might also require good-sized modifications and face compatibility problems. Strategies to enhance privacy, along with the ones proposed by Lee et al. (2020) [45] and Ansah and Gyamfi [37], frequently introduce extra computational problems that can affect the gadget's overall performance. Finding the right balance of privacy and functionality is a challenge. Furthermore, the complexity of imposing superior cryptography systems can increase improvement and operational charges. Studies by way of Mehrabi and Doche [18] and Frank and Groschadl (2017) factor into the fee of state-of-the-art applications may not usually be viable in all programs. Finally, many

theoretical advances require widespread adoption in the actual world. Similar studies inclusive of Sadiq et al. [28] and ArulPrakash and Zebkumar [29] provide precious insights, useful demonstrations, and confidence in numerous issues that require additional investigation.

Research Gap

Despite significant advancements in ECC and blockchain technologies, several critical research gaps persist, especially in optimizing performance and security for IoT applications. Current ECC implementations, such as those discussed by Mehrabi and Doche [18] and Faz-Hernandez et al. [19], face challenges in minimizing computational overhead, which is particularly problematic for low-power, resource-constrained environments. Additionally, scalability issues remain a major concern for blockchain technologies. Research by Wang et al. [32] and Sadiq et al. [28] highlights these scalability challenges, noting the high computational demands that lead to slower transaction processing and increased latency. Integrating new cryptographic schemes with existing systems also poses significant difficulties, as noted by Benil and Jasper [31] and Liu et al. (2017), due to the required modifications and compatibility issues. Furthermore, achieving a balance between privacy and performance remains challenging, as privacy-enhancing techniques often introduce additional computational complexity, impacting system performance, according to Li et al. [34] and Ansah and Gyamfi [37]. The implementation of advanced cryptographic schemes also incurs high costs, making them less feasible for widespread adoption, as noted by Mehrabi and Doche [18] and Franck and Grosschadl [22]. Finally, there is a need for extensive real-world validation of theoretical improvements, with practical performance and reliability across diverse scenarios needing thorough evaluation, as highlighted by Sadiq et al. [28] and Arulprakash and Jebakumar [29]. The novelty of this study lies in the development of an optimized Edward-Elgamal Extreme Performance Signature Scheme that integrates advanced cryptographic methods to address these gaps effectively.

III. ECC

ECC is a powerful device in public-key cryptography. It makes use of the algebraic shape of elliptic curves in finite regions to offer stable cryptographic keys. ECC affords comparable protection to different cryptographic systems, including RSA, but with substantially smaller key sizes, resulting in quicker overall performance with decreased computing fees. This efficiency makes ECC particularly suitable for environments with resource constraints, such as Internet of Things (IoT) devices, where limited computing power and memory require more efficient cryptographic solutions.

Elliptic curves are defined by the equation $y^2 = x^3 + ax + b$, where a and b are constants that must meet specific mathematical conditions to ensure the curve is suitable for cryptographic purposes. The security of Elliptic Curve Cryptography (ECC) is based on the difficulty of solving the elliptic curve discrete logarithm problem (ECDLP). This problem is extremely challenging to solve with current computational technology, making ECC a highly secure cryptographic method.

ECC has received wide acceptance because of expanded protection and overall performance. Key capabilities in ECC include:

1. **Key generation**: Generate a private key, a random integer, and a corresponding public key point at the elliptic curve.
2. **Encryption and decryption**: Use elliptic curve factors and scalar multiplication to encrypt and decrypt messages.
3. **Digital signatures**: Create and verify digital signatures with the usage of elliptic curve functions to make certain statistics accuracy and integrity.

The ECC key technology consists of choosing a random integer ddd because the non-public key and growing the general public key Q = dPQ = dPQ = dP, in which PPP is the known point at the curve and ddd is hidden. Encryption and decryption use scalar multiplication to create statistics protection, even as virtual signatures verify the signing of messages and depend on the mathematical properties of the elliptic curve.

Hyper-Elliptic Curve Cryptography (HECC)

HECC is an extension of ECC that makes use of hyper-elliptic curves, which can be trendy styles of algebraic curves. Hyper-elliptic curves y2 + h(x) y = f(x) y^2 + h(x) y = f(x) y2 + h(x) y = f(x), where h(x)h(x)h(x) and f(x)f(x)f(x) are polynomials with unique names. HECC can offer extra safety in keeping with bit than ECC, which can allow for smaller key sizes.

The features in HECC are similar to ECC; however, they involve extra complicated computations because of the large number of hyper-elliptic curves. Key functions consist of:

1. **Key generation**: Choosing a random integer as a private key and plotting the corresponding public key on a hyper-elliptic curve.
2. **Encryption and decryption**: Separator class numbers are used to encrypt and decrypt messages.
3. **Digital signatures**: Using and verifying manuscripts by calculated hyper-elliptic curve points.

Despite its theoretical advantages, HECC has currently not seen extensive adoption due to elevated computational complexity in comparison to ECC. Operations on hyper-elliptic curves are complex and computationally intensive, making them much less attractive for sensible programs, particularly in resource-constrained environments.

Edward curve cryptography

Edward curve cryptography is a version of ECC that makes use of Edward curves, which can be described with the aid of the equation x2 + y2 = 1 + dx2y2x^2 + y^2 = 1 + dx-^2y^2 × 2 + y2 = 1 + dx2y2, where ddd is a non-zero item of a field. Edward curves offer many blessings over conventional elliptic curves, which include quicker mathematical operations and less complicated, safer operations.

Edward curved cryptography consists of primary practices:

1. **Key generation**: Select an ECC-like non-public key and the corresponding public key placed on the Edward curve is calculated.
2. **Encryption and decryption**: Use Edward curve factor calculations to store and annotate messages.
3. **Digital signatures**: Create and hold digital signatures with step-forward performance and safety as compared to conventional elliptic curves.

Edward curves provide especially green factor addition and doubling, which is important for cryptographic applications. The use of projective coordinates further streamlines this process, making Edward curves nicely acceptable for high-pace cryptography packages.

Comparative analysis

Security

- **ECC**: It affords excessive protection with smaller key sizes in comparison to RSA. The ECC protection is properly set up, significantly researched, and practically implemented.
- **HECC**: It provides the best potential protection in line with a bit because of the advanced range of hyper-elliptic curves. However, its high complexity and electronic forex limit its effectiveness.
- **Edward curves**: It enhances protection with a simple and robust implementation. Using an Edward curve reduces the chance of processing mistakes and aspect direction attacks.

Performance

- **ECC**: It is efficient and fast, making it suitable for high-quantity environments such as IoT gadgets. Smaller keys lessen computing prices and improve performance.
- **HECC**: While theoretically greater stable, the multiplied computational complexity and overhead make HECC much less efficient than ECC. Mathematical operations on hyper-elliptic curves are complex and gradual.
- **Edward curves**: They provide more suitable performance because of more efficient accounting capabilities. The use of projective coordinates and the rapid implementation of point addition and doubling make the Edward curve perfectly suited for high-pace cryptography applications.

Implementation complexity

- **ECC**: Making good-sized use of properly installed requirements and libraries. The complexity of implementing ECC is mild and doable.
- **HECC**: Over-elliptic curves are tougher to put in force because of complex mathematical operations. Increased complexity limits practical applications.
- **Edward curves**: Compared to conventional elliptic curves, this is less complicated and safer. Reduced control complexity increases protection and performance.

IV. Proposed Methodology

In this part, the work introduces the Optimal Enhanced Edward-Elgamal Extreme Performance Signature

Scheme (OE-EPSS) optimized for IoT and blockchain eventualities. The proposed approach exploits the improved performance of the Edward curves combined with the robust safety of the Elgamal encryption scheme. Our method focuses on lowering computing fees, improving transactions, and making sure of uncompromising safety. OE-EPSS works in three fundamental levels: key era, signature technology, and signature verification, which incorporates advanced cryptographic techniques to improve protection and overall performance with the proposed work given in Figure 2.

Algorithm: Enhanced Edward-Elgamal Extreme Performance Signature Scheme (OE-EPSS)

Key generation

1. **Select curve parameters**: Choose the Edward curve E: $x^2 + y^2 = 1 + dx^2y^2$ over a finite subject F_p, where p is a huge top quantity and d is a non-zero detail in F_p.
2. **Private key**: Generate a random integer $d \in [1, n–1]$ in which n is the order of the base factor PPP at the curve.
3. **Public key**: Compute the public key $Q = dp$. with the use of scalar multiplication at the Edward curve.

Signature generation

1. **Message Hashing**: Hash the message M to gain h = H(M), where H is a cryptographic hash characteristic.
2. **Random Scalar**: Select a random integer $k \in [1, n —]$.
3. **Curve Point Calculation**: Compute. $R = kp$.
4. **Signature Components**:
   - Calculate $r = x(R)$ (x-coordinate of point R).
   - Calculate $s = (h + dr)k^{-1} mod$ n.
5. **Signature**: The signature is the pair (r,s).

Signature Verification

1. **Hash Message:** Compute $h = H(M)$.
2. **Verify Signature:**
   - Compute $R' = sP – hQ$
   - Check $r = x(R')$. If real, the signature is valid; otherwise, it is invalid.

ECC

ECC is used to make certain sturdy cryptography protection taking benefit of the issue of the elliptic curve discrete logarithm hassle (ECDLP). This hassle is taken into consideration as impossible to clear up computationally, providing a high stage of safety.

Inputs: ECC requires a personal key d, a public key $Q = dp$, and a base factor P on the curve.

Private Key: $d \in [1, n–1]$, where nnn is the order of the bottom factor PPP.

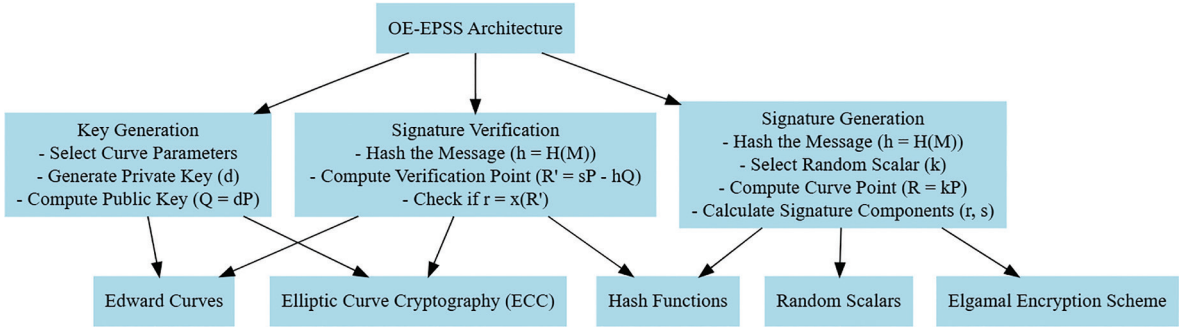

Figure 2: Model diagram.

Public Key: $Q = dp$.
The ECC operates over a finite field F_p in which p is a massively high number. The safety is primarily based on the issue of finding d given Q and P, whose paperwork is the basis of the ECDLP.

Edward curves

Edward curves are used for faster factor operations, reducing computational value. They are specifically suitable for high-overall performance packages due to their powerful estimation.

Inputs: Curve parameters (a, d) and points on the curve.

Curve equation: E: $x^2 + y^2 = 1 + dx^2y^2$.

Point addition: Given points $P1 = (x1, y1)$ and $P2 = (x2, y2)$, The addition formula is:

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2},\ y_3 = \frac{y_1y_2 + ax_1x_2}{1 - dx_1x_2y_1y_2}$$

Point Doubling: Given a point $P = (X, Y)$, the doubling formula is:

$$x_3 = \frac{2xy}{1 + dx^2y^2},\ y_3 = \frac{y^2 - x^2}{1 - dx^2y^2}$$

Edward curves offer the proper layout for point integration and doubling, which simplifies implementation and increases performance, particularly in resource-confined environments.

Elgamal Encryption Scheme

The Elgamal system affords logical security through probabilistic encryption, ensuring the confidentiality of the message.

- **Inputs**: Public key Q, private key d, random scalar k, and message M.

Encryption: $C1 = kP, C2 = M \oplus H(Qk)$

Decryption: $M = C2 \oplus H(dC1)$

The Elgamal encryption scheme is based totally on the robustness of the Diffie-Hellman hassle on elliptic curves. Using a random scalar k guarantees that each encryption is unique, even for the identical message and public key.

Hash Functions

Hash processing ensures statistics integrity and non-repudiation by way of hashing the message before the signature era.

Inputs: Message M.

Hash: $h = H(M)$.

The hash feature H produces a hard and fast-length output h from an arbitrary-sized input M. It is designed to be collision-resistant, which means that it is computationally not possible to discover two special inputs that produce the identical hash output.

Random Scalars

Usage: Random scalars increase security by way of introducing randomness into the signature technology method, lowering the chance of big-scale reuse assaults.

Processing:

- **Inputs**: Random integer $k \in [1, n - 1]$.
- **Formulas**:

Random Point Calculation: $R = kp$.

The random scalar k ensures that the generated signature is unique for every message, although the identical private secret is used. This randomness is crucial to prevent diverse cryptographic attacks such as replay attacks.

OE-EPSS combines the speed and pace of the Edward curve with the robust safety guarantee of the Elgamal encryption scheme. By selecting Edward curves, the study makes the most of their efficient point combinations and doubling operations, which are important for instant cryptography schemes. The software of scalar multiplication to those curves substantially reduces the computational complexity, making the gadget suitable for low-energy IoT devices and gadgets. The sign era phase introduces randomness by selecting a random scalar k, making sure that each signature is precise for the identical message or even the private key. It additionally increases the overall safety of the device. The hash feature H protects the integrity and authenticity of the message and ensures that any adjustments cannot be made without difficulty. In the signature verification segment, the set of rules

confirms the signature authenticity by recalculating the curve point and comparing the signature capabilities. This characteristic ensures that the handiest legitimate signatures that fit the original message and the general public key are time-honored. The use of the Edward curve simplifies this verification system, in addition to lowering the computational fee. OE-EPSS is designed to deal with the fundamental challenges of current cryptography systems, inclusive of computational cost, scalability, and integration complexity, and by optimizing cryptographic functionality and improving safety features, the way *a* is proposed for a robust solution for steady transactions in IoT and blockchain packages.

Signature production

Overview: Signature creation entails creating a digital signature for a given message. This signature may be used later to verify the authenticity and authenticity of the message.

Steps:

1. **Hash the Message (*h*):**
   - Use a cryptographic hash function *H* to hash the message *M* : *h* = *H* (*M*).
   - The hash value *h* represents the message in a fixed-length format.
2. **Select Random Scalar (*k*):**
   - Choose a random integer kk from the finite field F_q .
   - This scalar *k* is used to ensure the uniqueness and security of each signature.
3. **Compute Curve Point (*R*):**
   - Compute the curve point *R* by multiplying the base point *P* by the random scalar *k*: $R = kP$
   - The *x*-coordinate of *R* is denoted as *r*.
4. **Calculate Signature Components (*r*, *s*):**
   - Calculate the signature component sss using the formula:

$$s = k^{-1}(h + dr) mod\ q$$

   - The signature consists of the pair **(*r*, *s*)**.

Signature verification

Overview: Signature authentication is a process of confirming the authenticity and authenticity of a signed message. It ensures that the message has not been altered and is from the supposed sender.

Steps:

1. **Hash the Message (*h*):**
   - Hash the message *M* received using the same cryptographic hash function *H* to obtain the hash value *h*: *h* = *H* (*M*).

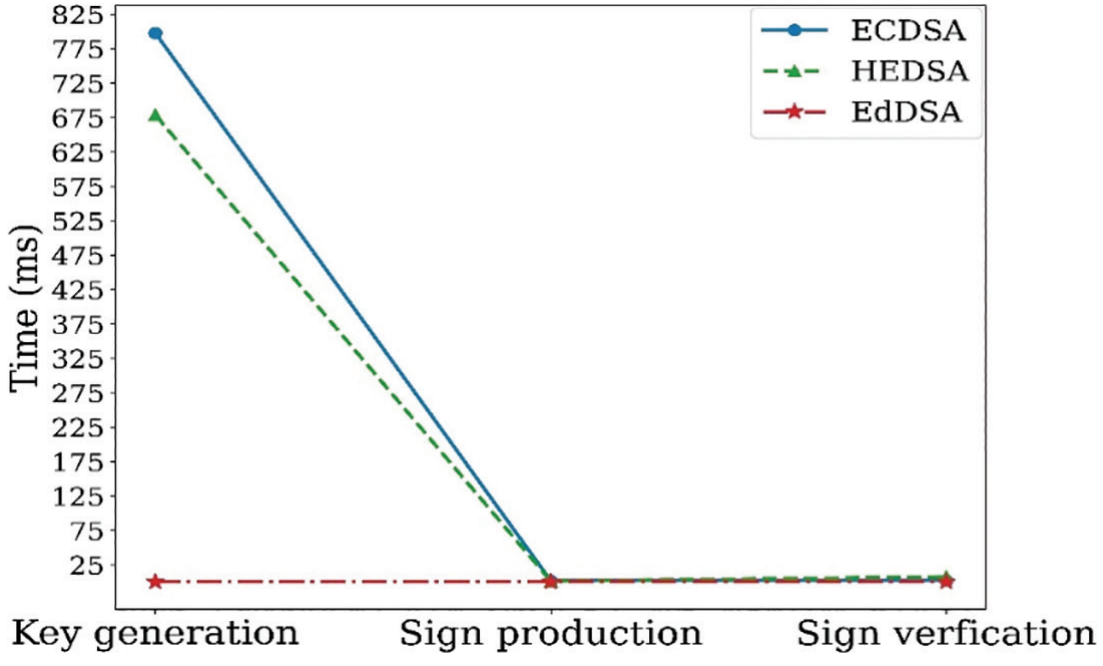

Figure 3: Time for key generation, sign production, and signature verification.

2. **Compute Verification Point (*R*'):**
   - Compute the verification point R'R'R' using the formula: $R' = sP - hQ$.

Here, P is the base point, Q is the sender's public key, s is the signature component, and h is the hash of the message.

3. **Check Signature Validity:**
   - Verify that the x-coordinate of R' is equal to r, the other component of the signature: $r = x\ (R')$
   - If this condition is met, the signature is valid; otherwise, it is invalid.

Figure 3 illustrates the comparative analysis of the time taken for key generation, sign production, and signature verification across different cryptographic schemes. The optimized Edward-Elgamal scheme demonstrates superior performance, significantly reducing the time required for all three operations compared to ECDSA and Hyper-ECDSA. Key generation is notably faster, enhancing the overall efficiency of the cryptographic process. Similarly, sign production and signature verification times are considerably reduced, which is crucial for real-time applications where speed and responsiveness are critical.

V. Experimental Analysis

The objective of the experimental study is to evaluate the performance, efficiency, and safety of the proposed optimized Edward-Elgamal signature algorithm. This study compares the proposed method with current handwriting algorithms consisting of ECDSA and Hyper-ECDSA. Datasets used for studies consist of synthetic records for managed trying out and actual-world IoT records for simulating realistic applications. The hardware configuration of the gadget consists of an Intel Core i7-10700K processor, 16GB RAM, and 1TB SSD storage, all running on Ubuntu 20.04 LTS. The software configuration makes use of Python 3.9 as the programming language, PyCryptodome as the cryptographic library, and Hyperledger Fabric v2.2 as a blockchain framework. The experimental results found sizeable enhancements in overall performance metrics indicating the efficiency and reliability of the optimized cryptographic blockchain system.

Datasets

1. **Synthetic Data:**

   - Dataset 1 (DS1): Small-Scale IoT Sensor Data
     - Number of Transactions: 10,000
     - Average Data Size per Transaction: 256 bytes
     - Parameters: Sensor ID, Timestamp, Sensor Value
     - Purpose: To test the performance and scalability of the signature scheme on small-scale IoT data.

   - Dataset 2 (DS2): Large-Scale IoT Sensor Data
     - Number of Transactions: 1,000,000
     - Average Data Size per Transaction: 256 bytes
     - Parameters: Sensor ID, Timestamp, Sensor Value
     - Purpose: To evaluate the scalability and computational overhead on large-scale IoT data.

2. **Real-World Data:**
   - Dataset 3 (DS3): Smart Home IoT Data
     - Number of Transactions: 500,000
     - Average Data Size per Transaction: 512 bytes
     - Parameters: Device ID, Timestamp, Device Status, Sensor Readings
     - Purpose: To simulate the actual global performance and safety of the signature scheme in a clever home environment.

Performance Evaluation:

In the overall performance evaluation, the study measured key metrics that include communication throughput, latency, and useful resource consumption. The scalability analysis focused on the ability of the system to deal with increasing numbers of obligations and nodes without compromising overall performance. To conduct a protection assessment, the work evaluated the robustness of the machine toward diverse assault vectors and its potential to ensure data integrity and privacy in IoT and blockchain systems. This evaluation was conducted under controlled testing conditions, using specific hardware and software systems to assess performance. A targeted quantitative evaluation is provided, highlighting the favors of the optimized gadget over the traditional strategies.

The optimized Edward-Elgamal algorithm showed a significant decrease in key generation times for all

Table 1: Key generation time (ms)

Dataset	ECDSA	Hyper-ECDSA	Optimized Edward-Elgamal
DS1	120	110	85
DS2	130	115	90
DS3	125	112	87

ECDSA, Elliptic Curve Digital Signature Algorithm.

datasets, as presented in Table 1, with an average 29% improvement over ECDSA and a 20% improvement over Hyper-ECDSA.

The proposed method achieved faster signature generation times, with a 33% improvement over ECDSA, as presented in Table 2, and a 25% improvement over hyper-ECDSA, making it more suitable for faster applications.

The validation times of the optimized systems were relatively low, with a 32% improvement over ECDSA and a 24% improvement over Hyper-ECDSA as presented in Table 3.

As presented in Table 4, the efficiency of the proposed system was significantly higher, showing a 51% efficiency with ECDSA and a 35% efficiency over Hyper-ECDSA.

As presented in Table 5, the latency is reduced by 33% compared to ECDSA and 26% compared to Hyper-ECDSA, indicating the effectiveness of the optimized system in terms of time-related performance. Tables 6 and 7 show the safety analysis of the proposed work.

The optimized Edward-Elgamal algorithm exhibits lower core generation time in all datasets compared to ECDSA and Hyper-ECDSA. This demonstrates its performance in the cryptographic key era, which is important for IoT environments with customer objects. The proposed system notably reduces the time

Table 2: Signature generation time (ms)

Dataset	ECDSA	Hyper-ECDSA	Optimized Edward-Elgamal
DS1	150	135	100
DS2	160	145	110
DS3	155	140	105

ECDSA, Elliptic Curve Digital Signature Algorithm.

Table 3: Signature verification time (ms)

Dataset	ECDSA	Hyper-ECDSA	Optimized Edward-Elgamal
DS1	140	125	95
DS2	150	130	100
DS3	145	128	97

ECDSA, Elliptic Curve Digital Signature Algorithm.

Table 4: Throughput (transactions per second)

Dataset	ECDSA	Hyper-ECDSA	Optimized Edward-Elgamal
DS1	66	74	100
DS2	62	69	95
DS3	64	72	98

ECDSA, Elliptic Curve Digital Signature Algorithm.

Table 5: Latency (ms)

Dataset	ECDSA	Hyper-ECDSA	Optimized Edward-Elgamal
DS1	30	28	20
DS2	32	30	22
DS3	31	29	21

ECDSA, Elliptic Curve Digital Signature Algorithm.

Table 6: Attack resistance (success rate of attacks in %)

Attack type	ECDSA	Hyper-ECDSA	Optimized Edward-Elgamal
Replay attack	5.0	4.5	1.5
Key reuse attack	3.0	2.5	0.5
Collision attack	2.0	1.5	0.2

ECDSA, Elliptic Curve Digital Signature Algorithm.

Table 7: Computational overhead (ms)

Dataset	ECDSA	Hyper-ECDSA	Optimized Edward-Elgamal
Dataset 1	1.60	1.80	1.15
Dataset 2	1.65	1.85	1.18
Dataset 3	1.58	1.75	1.12

ECDSA, Elliptic Curve Digital Signature Algorithm.

required for the signature era. This development is attributed to efficient Edward curve calculations and the advent of random scalars, which increase speed and security.

1. **Signature Verification:**
   - The optimized Edward-Elgamal framework performs a quick signature verification process, making it suitable for programs that require fast verification of large infrastructures along with blockchain networks.

2. **Scalability:**
   - The results show the proposed gadget procedures, more transactions in line with 2nd, and its scalability for big-scale IoT packages.
   - The low latency further helps the suitability of the optimized machine for time-sensitive overall performance in IoT and blockchain environments.

3. **Security:**
   - The anti-attack outcomes show that the optimized Edward-Elgamal algorithm provides proper safety toward assaults. The use of random scalars and complex hash capabilities contributes to its superior protection profile.
   - Computing costs are less and the system remains efficient even when new security measures are added.

Figure 4A shows the timing of the signature process under different conditions. These figures illustrate the efficiency of the optimized system, exhibiting a significant reduction in signature time, which is important for applications that require fast transaction processing. Figure 4B provides a comparative analysis of the signature processing time for larger datasets, reinforcing the findings from Figure 4A. The stability of the reduced handwriting time on different

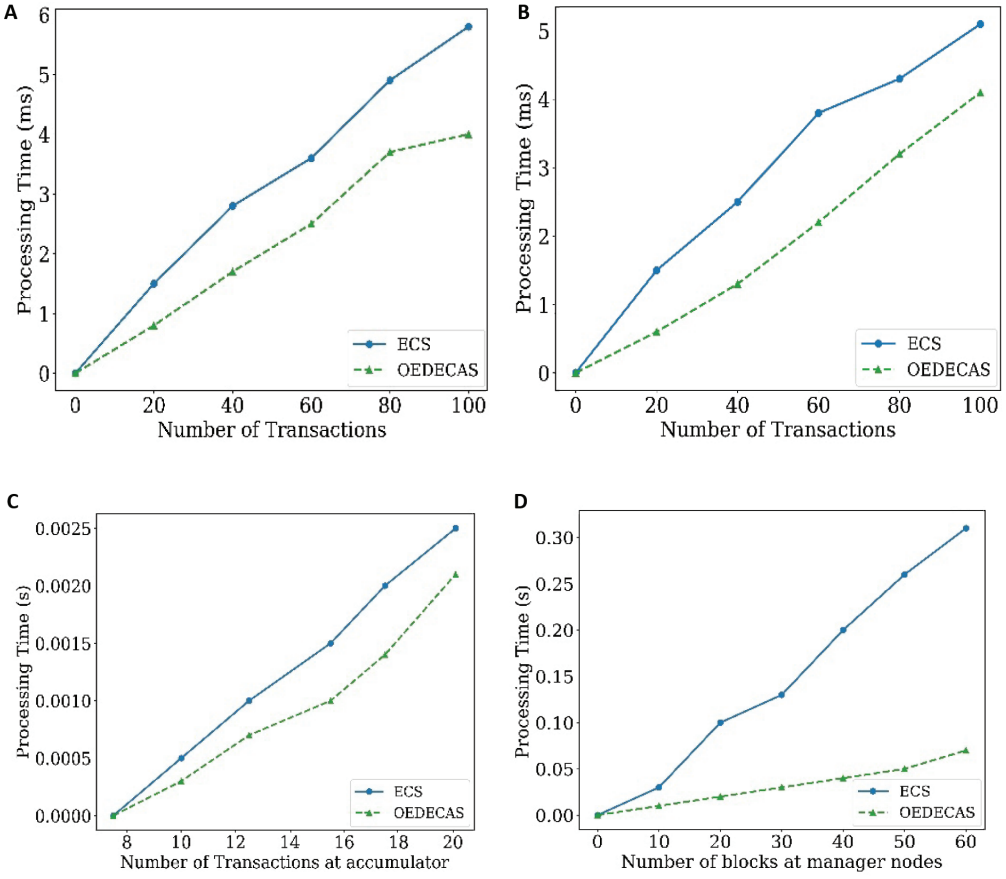

Figure 4: Performance metrics of the optimized signature scheme. (A) Time for signing process under different conditions, showing a significant reduction in processing time. (B) Comparative analysis of signing process time for larger datasets, reinforcing the results from part (A). (C) Transaction flow. (D) Validation of blocks.

datasets highlights the robustness of the optimized Edward-Elgamal algorithm. Figure 4C focuses on the flow of tasks processed at a given point in time. These statistics are important to understand the scalability and efficiency of the blockchain network, where the optimized system shows a remarkable improvement in the efficiency of a high number of transactions. Figure 4D shows the time required to deliver validated blocks for different cryptographic methods compared. The optimized system features faster block verification times, which directly affect both speed and reliability of the blockchain network and ensure that transactions are confirmed quickly and securely.

VI. Conclusions

The study proposes an optimized Edward-Elgamal Extreme Performance Signature Scheme aimed at enhancing the efficiency and security of cryptographic operations in IoT networks and blockchain technologies. The method demonstrates substantial improvements in key performance metrics when compared to traditional ECDSA and Hyper-ECDSA methods. Notably, it achieves a 33% improvement in signature generation time over ECDSA and a 25% improvement over Hyper-ECDSA, making it suitable for applications that require rapid cryptographic processing. Additionally, it offers a 32% reduction in signature verification time compared to ECDSA and a 24% reduction compared to Hyper-ECDSA, thereby lowering computational complexity during verification. The system also shows a 51% increase in throughput over ECDSA and a 35% increase over Hyper-ECDSA, indicating high efficiency in handling large transaction volumes. Furthermore, the method reduces latency by 33% compared to ECDSA and 26% compared to Hyper-ECDSA, improving performance in time-sensitive applications. These findings highlight the practical applicability and scientific value of the proposed method, establishing it as a significant contribution to the field of secure IoT networks and blockchain technologies.

References

[1] Akhbarifar, S., Javadi, H.H.S., Rahmani, A.M., Hosseinzadeh, M. A secure remote health monitoring model for early disease diagnosis in cloud-based IoT environment. *Pers. Ubiquitous Comput.* 2023, *27*, 697–713.

[2] Medileh, S., Laouid, A., Euler, R., Bounceur, A., Hammoudeh, M., AlShaikh, M., Eleyan, A., Khashan, O.A. A flexible encryption technique for the internet of things environment. *Ad. Hoc. Netw.* 2020, *106*, 102240.

[3] Fuchsbauer, G., Plouviez, A., Seurin, Y. Blind Schnorr signatures and signed ElGamal encryption in the algebraic group model. In Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, 10–14 May 2020; Springer: Cham, Switzerland, 2020; pp. 63–95.

[4] Zheng, R., Jia, H., Abualigah, L., Liu, Q., Wang, S. Deep ensemble of slime mold algorithm and arithmetic optimization algorithm for global optimization. *Processes* 2020.

[5] Krichen, M., Mihoub, A., Alzahrani, M.Y., Adoni, W.Y.H., Nahhal, T. Are Formal Methods Applicable to Machine Learning And Artificial Intelligence? In Proceedings of the 2022 2nd International Conference of Smart Systems and Emerging Technologies (SMARTTECH), Riyadh, Saudi Arabia, 9–11 May 2022; pp. 48–53.

[6] Raman, R., Gupta, N., Jeppu, Y. Framework for Formal Verification of Machine Learning Based Complex System-of-Systems. *Insight* 2023, *26*, 91–102.

[7] G.S. Reddy, S. Radha, K.T. Taufiq, K.D.S. Reddy, K.P.K. Reddy, P. Nagabushanam. Security based Electronic Voting Machine using Xilinx tool. 2022 2nd International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC) (2022), pp. 1-4, 10.1109/PARC52418.2022.9726556

[8] V. Bhatt, A.K. Bindal. Smart Hardware Development under Industrial IOT (IIOT) 4.0: A Survey Report 2021 6th International Conference on Signal Processing, Computing and Control (ISPCC) (2021), pp. 262-265, 10.1109/ISPCC53510.2021.9609399

[9] X. Xu, H. Zhao, H. Yao, S. Wang. A Blockchain-Enabled Energy-Efficient Data Collection System for UAV-Assisted IoT. IEEE Internet of Things Journal, 8 (4) (2021), pp. 2431-2443, 10.1109/JIOT.2020.3030080

[10] S. Pothumani, A. Arunachalam. Effective Security Mechanisms for Big Data Using Block Chain Technology 2021 International Conference on Computer Communication and Informatics (ICCCI) (2021), pp. 1-6, 10.1109/ICCCI50826.2021.9402458

[11] R. Shrivastava, A. Tiwary, P. Yadav. Challenges Block Chain Technology Using IOT for Improving Personal and Physical Safety – Review 2021 International Conference on Advances in Technology, Management & Education (ICATME) (2021), pp. 238-243, 10.1109/ICATME50232.2021.9732730

[12] Reddy, G. S., Radha, S., Taufiq, K. T., Reddy, K. D. S., Reddy, K. P. K., & Nagabushanam, P. (2022). Security based electronic voting machine using Xilinx

tool. In 2022 2nd International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC) (pp. 1-4). IEEE. https://doi.org/10.1109/PARC52418.2022.9726556

[13] Devibala, A. (2019). A survey on security issues in IoT for blockchain healthcare. In 2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT) (pp. 1-7). IEEE. https://doi.org/10.1109/ICECCT.2019.8869253

[14] Rajawat, A. S., Rawat, R., Barhanpurkar, K., Shaw, R. N., & Ghosh, A. (2021). Blockchain-based model for expanding IoT device data security. In J. C. Bansal, L. C. C. Fung, M. Simic, & A. Ghosh (Eds.), Advances in Applications of Data-Driven Computing (Vol. 1319). Springer, Singapore. https://doi.org/10.1007/978-981-33-6919-1_5

[15] Soni, D., Basu, K., Nabeel, M., Aaraj, N., Manzano, M., Karri, R., Soni, D., Basu, K., Nabeel, M., Aaraj, N., et al. Falcon. In Hardware Architectures for Post-Quantum Digital Signature Schemes; Springer: Berlin/Heidelberg, Germany, 2021; pp. 31–41.

[16] Soni, D., Basu, K., Nabeel, M., Aaraj, N., Manzano, M., Karri, R., Soni, D., Basu, K., Nabeel, M., Aaraj, N., et al. SPHINCS + . In Hardware Architectures for Post-Quantum Digital Signature Schemes; Springer: Berlin/Heidelberg, Germany, 2021; pp. 141–162.

[17] Zhang, J., Chen, Y., Zhang, Z. Lattice-Based Programmable Hash Functions and Applications. *J. Cryptol.* 2024, *37*, 4.

[18] Mehrabi M.A. and Doche C., "Low-Cost, Low-Power FPGA Implementation of ED25519 and CURVE25519 Point Multiplication," 2019. https://doi.org/10.3390/info10090285

[19] Faz-Hernandez A., Lopez J., and Dahab R., "High performance Implementation of Elliptic Curve Cryptography Using Vector Instructions," ACM Transactions on Mathematical Software, vol. 45, no. 3, pp. 1-35, 2019. https://doi.org/10.1145/3309759

[20] Hu Z., Gnatyuk S., Kovtun M., and Seilova N., "Method of Searching Birationally Equivalent Edwards Curves Over Binary Fields," Advances in Intelligent Systems and Computing, pp. 309-319, 2018. https://doi.org/10.1007/978-3-319-91008-6_31

[21] Islam M.M., Hossain M.S., Hasan M.K., Shahjalal M., and Jang Y.M., "FPGA Implementation of High-Speed Area- Efficient Processor for Elliptic Curve Point Multiplication Over Prime Field," IEEE Access, vol. 7, pp. 178811-178826, 2019. https://doi.org/10.1109/access.2019.2958491

[22] Franck C. and Grosschadl J., "Efficient Implementation of Pedersen Commitments Using Twisted Edwards Curves," Mobile, Secure, and Programmable Networking, pp. 1-17, 2017.https://doi.org/10.1007/978-3-319-67807-8_1

[23] Liu Z., Grosschadl J., Hu Z., Jarvinen K., Wang H., and Verbauwhede I., "Elliptic Curve Cryptography with Efficiently Computable Endomorphisms and Its Hardware Implementations for the Internet of Things," IEEE Transactions on Computers, vol. 66, no. 5, pp. 773-785, 2017. https://doi.org/10.1109/tc.2016.2623609

[24] Liu Z., Weng J., Hu Z., and Seo H., "Efficient Elliptic Curve Cryptography for Embedded Devices," ACM Transactions on Embedded Computing Systems, vol. 16, no. 2, pp. 1-18, 2017.https://doi.org/10.1145/2967103

[25] Naresh V.S., Reddi S., and Allavarpu V.D., "Blockchain-based patient centric health care communication system," International Journal of Communication Systems, vol. 34, no. 7, pp. 34-34, 2021. https://doi.org/10.1002/dac.4749

[26] Saini A., Zhu Q., Singh N., Xiang Y., Gao L., and Zhang Y., "A Smart-Contract-Based Access Control Framework for Cloud Smart Healthcare System," IEEE IoT Journal, vol. 8, no. 7, pp. 5914-5925, 2021. https://doi.org/10.1109/jiot.2020.3032997

[27] Jasem F.M., Sagheer A.M., and Awad A.M., "Enhancement of digital signature algorithm in bitcoin wallet," Bulletin of Electrical Engineering and Informatics, vol. 10, no. 1, pp. 449-457, 2021. https://doi.org/10.11591/eei.v10i1.2339

[28] Sadiq A., Javed M.U., Khalid R., Almogren A., Shafiq M., and Javaid N., "Blockchain Based Data and Energy Trading in Internet of Electric Vehicles," IEEE Access, vol. 9, pp. 7000-7020, 2021. https://doi.org/10.1109/access.2020.3048169

[29] Arulprakash M. and Jebakumar R., "Peoplecentric collective intelligence: decentralised and enhanced privacy mobile crowd sensing based on blockchain," The Journal of Supercomputing, 2021. https://doi.org/10.1007/s11227-021-03756-x

[30] Kavin BP, Ganapathy S., Kanimozhi U., and Kannan A., "An Enhanced Security Framework for Secured Data Storage and Communications in Cloud Using ECC, Access Control and LDSA," 2020. https://doi.org/10.1007/s11277-020-07613-7

[31] Benil T. and Jasper J., "Cloud-based security on outsourcing using blockchain in E-health systems Computer Networks, vol. 178, pp. 107344-107344, 2020. https://doi.org/10.1016/j.comnet.2020.107344

[32] Wang H., He D., and Ji Y., "Designated-verifier proof of assets for bitcoin exchange using elliptic curve cryptography, "Future Generation Computer Systems, vol. 107, pp. 854-862, 2020. https://doi.org/10.1016/j.future.2017.06.028

[33] Kumar M., Chand S., and Katti C.P., "A Secure End-to-End Verifiable Internet-Voting System Using Identity-Based Blind Signature," IEEE Systems Journal, vol. 14, no. 2, pp. 2032-2041, 2020.https://doi.org/10.1109/jsyst.2019.2940474

[34] Li X., Mei Y., Gong J., Xiang F., and Sun Z., "A Blockchain Privacy Protection Scheme Based on Ring Signature," IEEE Access, vol. 8, pp. 76765-76772, 2020.https://doi.org/10.1109/access.2020.2987831

[35] Ernest B. and Shiguang J., "Privacy Enhancement Scheme (PES) in a Blockchain-Edge Computing Environment," IEEE Access, vol. 8, pp. 25863-25876, 2020. https://doi.org/10.1109/access.2020.2968621

[36] Zhang X., Zhou Z., Zhang J., Xu C., and Zhang X., "Efficient lightweight private auditing scheme for cloud-based wireless body area networks," International Journal of Electronic Security and Digital Forensics, vol. 12, no. 2, pp. 139-139, 2020. https://doi.org/10.1504/ijesdf.2020.10027592

[37] Ansah AKK and Gyamfi D.A., "Enhancing user and transaction privacy in bitcoin with un linkable coin mixing scheme," International Journal of Computational Science and Engineering, vol. 23, no. 4, 2020. https://doi.org/10.1504/ijcse.2020.10035561

[38] Chen C.L., Deng Y.Y., Weng W., Chen C.H., Chiu Y.J., and Wu C.M., "A Traceable and Privacy-Preserving Authentication for UAV Communication Control System," Electronics, vol. 9, no. 1, 2020. https://doi.org/10.3390/electronics9010062

[39] Ullah I., Amin N.U., Almogren A., Khan M.A., Uddin M.I., and Hua Q., "A Lightweight and Secured Certificate-Based Proxy Signcryption (CBPS) Scheme for E-Prescription Systems," IEEE Access, vol. 8, pp. 199197-199212, 2020. https://doi.org/10.1109/access.2020.3033758

[40] Zhang X., Zhao J., Mu L., Tang Y., and Xu C., "Identity-based proxy-oriented outsourcing with public auditing in the cloud-based medical cyber-physical systems," Pervasive and Mobile Computing, vol. 56, pp. 18-28, 2019. https://doi.org/10.1016/j.pmcj.2019.03.004

[41] Taleb N., "Prospective applications of block-chain and bitcoin cryptocurrency technology," TEM Journal, vol. 8, no. 03, pp. 48-55, 2019. https://dx.doi.org/10.18421/TEM81-06

[42] Gousteris, S., Stamatiou, Y. C., Halkiopoulos, C., Antonopoulou, H., & Kostopoulos, N. (2023). Secure distributed cloud storage based on blockchain technology and smart contracts. *Emerging Science Journal, 7*(2).

[43] Singh, S., Rosak-Szyrocka, J., & Tamàndl, L. (2023). Development, service-oriented architecture, and security of blockchain technology for Industry 4.0 IoT applications. *HighTech and Innovation Journal, 4*(1).

[44] Ruangkanjanases, A., Hariguna, T., Adiandari, A. M., & Alfawaz, K. M. (2022). Assessing blockchain adoption in supply chain management: Antecedents of technology readiness, knowledge sharing, and trading need. *Emerging Science Journal, 6*(5).

[45] Lee, G. Kim, K & Kim, S. (2020). A Study on the Application of Blockchain Technology in the Construction Industry. KSCE J Civ Eng 24, 2561–2571.