An Empirical Study to Demonstrate that EdDSA can be used as a Performance Improvement Alternative to ECDSA in Blockchain and IoT

Guruprakash J and Srinivas Koppu
E-mail: guruprakash.j2019@vitstudent.ac.in, srinukoppu@vit.ac.in and www.vit.ac.in
School of Information Technology and Engineering, Vellore Institute of Technology, India

Student paper

Keywords: digital signature, ECDSA, EdDSA, blockchain, IoT

Received: November 1, 2021

Digital signatures are a vital part of the digital world. The trust factor in the digital world is ensured with a digital signature. Over the evolution, the purpose remained constant, but the applicability and frontier continued to evolve, thus raising the demand for continuous performance, security level and computational improvement. Especially with emerging IoT, blockchain and cryptocurrency, the digital signature security level and performance improvement demand continue to rise. A digital signature scheme (DSS) is used to generate signatures. This paper investigates the widely used elliptic curve digital signature algorithm (ECDSA) and its application to blockchain and IoT. Then, we performed an empirical comparison of ECDSA with the Edwards curve digital signature algorithm (EdDSA). The study concludes by showing that EdDSA is superior to ECDSA and can be applied in blockchain and IoT domains to reap immediate benefits.

Povzetek: Avtorja primerjata dve metodi generiranja varnih digitalnih podpisov in pokažeta, da je EdDSA boljša kot ECDSA.

1 Introduction

Since the evolution of digital technology, digital signatures have played a vital role in providing integrity and security to the system. The rapid advancement and technological requirements did not leave the digital signature dormant, and they kindled the advancement needed for its coexistence. The transition could be observed in the rapid transformation from RSA to elliptic curve cryptography (ECC) and toward the advanced elliptic curve digital signature algorithm (ECDSA). These evolutions captured the researcher's attention, and ECDSA was mainly adopted due to its superiority in providing enhanced security with smaller keys and less operational space. This study aims to find a better performing alternative to ECDSA that can cater to IoT and blockchain based applications. The remaining part of this section introduces the digital signature, digital signature algorithm, and elliptic curve cryptography.

1.1 Digital signature

The digital signature (DS) is generated from a standard algorithm called the digital signature algorithm (DSA), which has to follow a specified standard scheme as put forth in the digital signature scheme (DSS). National Institute of Standards and Technology (NIST) and security council groups reviewed, tested, and described these standards. A digital signature authenticates identity, detects unauthorised data manipulation, guarantees against data tamper and is the only way for nonrepudiation in the digital world. Nonrepudiation assures evidence to the third party by the signatory. Later, the signatory cannot deny the activity with the third party or repudiate the sign [1].

The Figure 1 on page 277 shows that digital signatures provide authenticity, integrity and nonrepudiation.

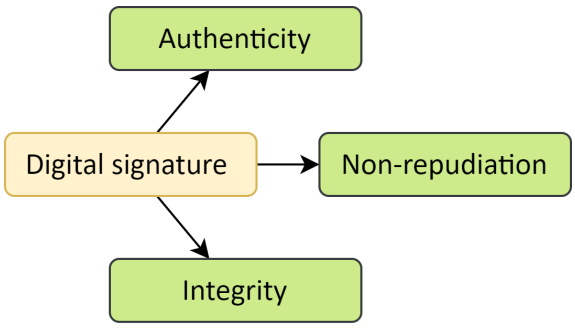

Figure 1: Application of Digital signature.

1.2 Digital signature algorithm

To achieve digital signatures, several forms of secure cryptographic standards of the digital signature algorithm (DSA) can be deployed. Figure 2 on page 278 shows digitally signed node interactions in an IoT domain. These

standards vary on the basic arithmetic operation involved, modular exponentiation and discrete logarithmic problem. DSA has a generic systematic flow for key generation, message signing, and verification; the standard provides deterministic and nondeterministic output. Generally, deterministic factors are considered to be safer and more secure.Evolution and demand brought in the need for modern cryptography, ECC. ECC was considered a successor to conventional DSA because it provided a shorter key, shorter signature, higher security and better performance. DSA, based on ECC, worked on cyclic groups of an elliptic curve over a finite field and difficult was based on the elliptic curve discrete logarithmic problem (ECDLP). The widely used variants are the ECDSA and Edwards curve digital signature algorithm (EdDSA).

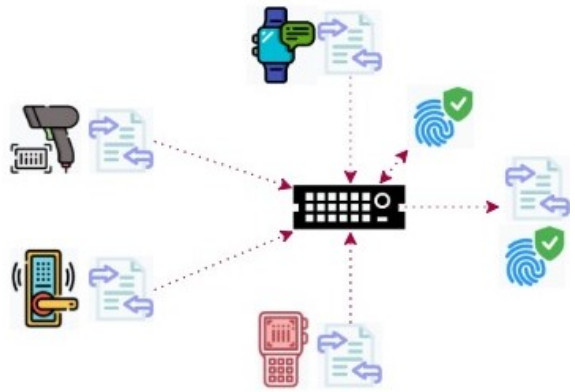

Figure 2: Digitally signed IoT node interaction in a connected domain.

1.3 Elliptic curve cryptography

ECDSA and EdDSA are among the variants of ECC with different curves as shown in Figure 3 on page 279. ECDSA, is based on the ElGamal signature and works on the group elements. The ECDSA computes a hash based on random keys, these random keys open a potential vulnerability, and the attacker can use it to gain an advantage. To overcome this, a non-deterministic variant based on HMAC (Hash message authentication code)became an alternative. EdDSA is the successor to ECDSA with fast DSA using Edwards curves Ed25519 and Ed448. EdDSA a variant of deterministic Schnorr's signature; solves the inherent problem of ECDSA. EdDSA is simple, secure and fast; unlike ECDSA, it relies on discrete logarithmic problems. Table 1 on page 279 shows various curve forms, their representation, plot and summary.

The article is structured as follows; Section 2 presents the objective and contribution. Section 3 illustrates the existing literature and application of digital signatures. Section 4 compares the elliptic and Edwards curve basic operations and metric of functional operations. Section 5 presents discussion and Section 6 concludes this article.

2 Objective & contributions

This work aims to perform an empirical study on ECDSA vs EdDSA and provide evidence-based results to prove that EdDSA has performance advantages. We collected evidence-based on the existing state-of-the-art current research in the fields of 1) the application of digital signatures, 2) the application of elliptic curve in blockchain, 3) the application of elliptic and Edwards curve in the IoT, 4) Schnorr's signature application, and 5) The application of Schnorr's-based aggregate signature in blockchain.In addition 6) Attribute to attribute comparison studies on Edwards curve DSA vs ECDSA help us demonstrate our stands on the superiority of the Edwards curve.

3 Literature review

In this section, we review the literature based on five broad questions. 1.How researchers have used digital signatures for blockchain and IoT based applications? 2.How does ECC find its application in blockchain, and what benefits they provide? 3.How elliptic and Edwards curves keep IoT devices secure and resources optimal? 4.How does Schnorr's signature help generate multiple signs and its advantage in blockchain-based applications? 5.How aggregate signatures have added value in blockchain applications? The review of the existing research proved the cumulative advantage and provided guidance for better alternative choices when designing future systems.

3.1 Digital signature

In this sub-section research works on various applications of Digital signatures are reviewed and presented.

[6] conducted a review of the existing DSA, RSA, ECDSA, and EdDSA and highlighted that DSA operations based on algebraic properties forming public-key cryptosystems can mutually authenticate. [7] implemented a self-sufficient library X64ECC for ECC that supported basic cryptographic functions such as key exchange, Zero Knowledge Proofs, and digital signature. The library was able to accelerates mission-critical arithmetic operations by leveraging the compiler intrinsic. [8] proposed a new public key scheme by implementing a twisted Edwards curve model. The secure message transmission in this scheme was ensured by using the property of one way, indistinguishability (IND) under chosen-plaintext attack (CPA), chosen-ciphertext attack (CCA) and the variant of other digital signature algorithms. [9] developed an ECC processor based on the Edwards25519 curve implemented using FPGA for increased speed, reduced area, and simple arithmetic with efficient hardware using projective coordinates. [10] proposed using EdDSA with SHA-512 for Bitcoin as it would help in better security and efficiency compared with existing secp256k1 with hash SHA-265.[11] proposed a new method for counting the order of Edwards Curve (Ed) and elliptic curves over a finite field that can be used

Curve form	Representation	Plot	Summary
Edwards	$ax^2 + y^2 = 1 + dx^2y^2$	a)x^2 + y^2 = 1-299 x^2 y^2	fast and complete
Weierstrass	$y^2 = x^3 + ax + b$	b) y^2 = x^3 - 0.5 x + 0.8	form is slow,trusted and incomplete
Jacobi-quartic	$y^2 = x^4 + 2ax^2 + 1$	c) x^2 = y^4 - 1.9 y^2 + 1	has the capacity for extensions
Hessian	$ax^3 + y^3 + 1 = dxy$	d) x^3 - y^3 + 1 = 0.3 x y	has a uniform and week representation

Table 1: Curves and represents [2] [3] [4] [5].

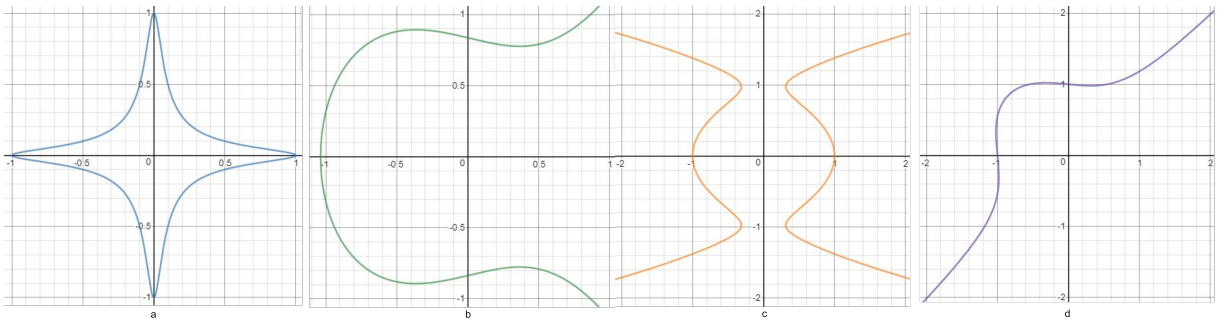

Figure 3: Plot of Curves a) Edwards, b) Weierstrass, c) Jacobi-quartic and d) Hessian.

for fast group operations with less complexity. The proposed method determines whether the curve is supersingular over a finite field. [12] cryptographically implement a simple Maps connecting Kummer, Montgomery curves and twisted Edwards lines. It was also evident that we can propose a low-power, low-area FPGA implementation of the Edwards curve and Montgomery curve [13]. In the method, the EdDSA provides faster digital signatures than existing schemes. [14] suggested secure and efficient software implementation of EdCDH, and EdDSA using SIMD parallel processing and obtained high performance.[15] focused on the Edwards curve to increase the performance and security over binary fields to overcome side-channel attacks. [16] implemented ECC on an FPGA with more speed, less area, and side-channel attack resistance. The processor supports point multiplication on different derivatives and achieves accelerated point multiplication with minimal hardware utilisation.[17] evaluated Montgomery-Twisted-Edwards and ECC implementations on IoT devices based on three different factors - ROM, RAM, and execution time. Their study provides reference results for the transition from legacy ECC to MoTE-ECC. [18] proposed a flexible Pedersen commitment implementation based on elliptic curves in twisted Edwards form, which helped to improve security, adaptive data size, and data point flexibility.[19] investigated optimal prime fields for lightweight ECC implementation, focusing on performance and security.[20] performed a comparative study of algorithms for batch verification of Edwards curve digital signatures and showed that small batch size algorithms S2' and SP yield better speedup results than the default algorithm N'.

Table 2 on page 280 shows various applications of Digital signature.

3.2 Application of elliptic curve cryptography in blockchain

In this sub-section research works on various applications of Elliptic curve cryptography in blockchain are reviewed and presented.

[22] proposed a four-layer framework for decentralised privacy-preserving management for electronic medical records using blockchain with Elliptic curve based digital signatures and content extraction signature(CES) and achieved access control and data privacy.[23] deployed an EMR on a blockchain-based infrastructure and mitigated a single point of failure on electronic medical records. ECC and ECDSA provide the security backbone for all operations. The major problems in the Bitcoin system were solved by employing ECDSA to circumvent security traps and generate new keys for each transaction, thereby improving security against attacks [24]. Increasing the number of electric vehicles and the internet of electric vehicles bring trust issues into the environment [25] exploited the use of blockchain and smart contracts to bring trust and tackle disputes in energy trading. [26] used blockchain-based mobile crowd sensing application for collective intelligence, and blockchain aided in keeping the process decentralised, secure, fast, optimised storage and privacy preserved. [27] proposed a modified ECC based on identity and derived an Elliptic curve access control mechanism and a lightweight digital signature algorithm to ensure data privacy and security. [28] employed ECC and a certificateless aggregate system(CAS) to achieve traceability, integrity and secure storage of electronic health records. The use of ECC and CAS helped to safeguard from unauthorised access when utilising the cloud storage. [29] build a

EC / DSS / DSA	Domain	Solution	#
		Security enhancement	
	Cryptocurrency	Efficiency improvement	[10]
		Security enhancement	[8]
		Security enhancement	[11]
		Security enhancement	
		Cost reduction	[12]
Edwards		Optimal arithmetic	
Curve		Performance improvement	
		Optimal arithmetic	[14]
		Reduced execution time	
		Performance improvement	
	General	Security improvement	[15]
		Speed improvement	
		Reduced space	
		Enhanced security	[16]
		Optimal arithmetic	
		Security enhancement	
		Runtime optimisation	[18]
		Enhance computation speed	[20]
Generic		Review	[6]

Table 2: Digital Signature applications in various domain.

designated verifier proof of assert (DV-POA) for currency exchange entirely based on ECC making it provable, secure and efficient. Voting requires great privacy, and the real identity of the voter should not be exposed. Nevertheless, the voter should be a verifiable identity. [30] built an E2E verifiable voting system based on blockchain. The cryptography and signatures are supported by BLS over a well-known elliptic curve providing a short signature and voter anonymity. User privacy is the most difficult challenge to overcome in regard to data mining and sociological mining. [31] created a blockchain-based privacy protection scheme with a ring signature and an elliptic curve that adds privacy to data storage and performs anonymous mining in a secure manner. Edge computing is always resource-starved, and enhancement needs to be in place for continuous improvement. [32] used an elliptic curve cryptosystem to preserve privacy and eliminated attacks. Their scheme was resilient with a computing environment based on the random public key. Medical data integrity is vital, while utilising cloud-based storage sufficient mechanism to protect the data needs to be employed. [33] employed ECDSA and build a lightweight auditing scheme for medical data privacy. [34] built a security and privacy scheme for coin mixing using an elliptic curve digital signature scheme with standard ring signature. They were able to achieve unforgeability with appreciable transaction efficiency. Unmanned aerial vehicles(UAVs) have captured substantial market share, and privacy-preserving and authentication have become growing issues in UAVs. [35] proposed a solution based on ECC and DS to achieve all the cryptography services required for UAV certification. [36] presents signcryption using the advanced Elliptic curve to protect the stringent legal and privacy required for the E-prescription system. The use of ECC helped them achieve the required protection in a low resource and computing constraint environment. [37] used elliptic curve cryptography to sign and encrypt data uploaded through patient authorisation via third party proxies. The use of ECC made their scheme light and suitable for authentication on cloud-based medical systems that provide computing and storage service to the healthcare domain. [38] survey demonstrated that most blockchain and cryptocurrency used structured based on the elliptic curve digital signature algorithm. Bitcoin mainly uses secp256k1 and assumed to be a platform with high encryption and security.In [37] they built a system based on an elliptic curve digital signature and practical Byzantine fault-tolerance, to achieve security demanded by China's electricity market.[39] used signatures based on bilinear pairing and elliptic curves to ensure transmission integrity and reliability for data security of shared storage system based on a smart contract. Compared with the traditional method, the application of the elliptic curve reduced block confirmation and improved transmission.[40] provided privacy enhancement to a Bitcoin transaction by mixing an elliptic curve digital signature and ring signature scheme. The outcome resulted in the users being able to identify the customer associated with the address.[41] employed elliptic curve discrete logarithm and bilinear for aggregate signature to shorten and compress a single signature. Their work demonstrated that the signature size remained constant irrespective of multiple inputs and outputs in the transaction. [75] the authors applied and enhanced ECC based encryption and decryption of IoT data transmission to its core ecosystem. They showed that application of ECC significantly help to improve the overall performance.

Table 3 on page 281 shows various applications of ECC in blockchain

EC / DSS / DSA	Domain	Solution	#
ECC	Computation	Key generation, Privacy-preserving, Security enhancement	[32]
	Egovernance	Enhance security, Digital signature, Identity management	[30]
	Healthcare	Storage optimisation, Efficiency improvement, Access control, Authentication, Security enhancement, Privacy, Identity management	[22],[23], [28],[36], [37]
	IoT Mobile	Privacy, Authentication, Key generation, Privacy-preserving, Security enhancement	[35],[26]
	Security Enhancement	Enhance security, Runtime optimisation	[42],[72]
ECDSA	Cloud Cloud storage	Performance improvement, Security enhancement, Storage, Signature , Privacy, Data management	[27],[33], [41],[31]
	Cryptocurrency	Signature generation verification, Provability, Privacy, Enhanced security, Identity Key management	[29],[34], [38],[40], [24]
	Electric vehicle	Storage, Security enhancement, Privacy, protection	[37],[25], [39]

Table 3: Application of ECC in blockchain.

3.3 Edwards curve application in IoT

In this sub-section research works on various Edwards curve applications in IoT are reviewed and presented.

[9] designed a public key generation with unified point addition on twisted Edwards curve for IoT security. The choice of Edwards curve for the digital signature was its fast grouping operation and resistance to side-channel attack, which was the drawback of elliptic curves. [43] presented the need for public-key cryptography for IoT based applications to provide exceptional efficiency, reduce resources and increase security levels in a small setup. Using Edwards curve cryptography for resource and power constrained IoT applications was an optimal choice. [13] presented EdDSA implementation using ED25519 and achieved reduced hardware implementation complexity for IoT applications. The application of ECC is catching up recently for IoT and allied application. [44] proposed the Edwards curve to optimise the power and memory consumption in a physical device. [45] presented a fast, low power and highly secure cryptography for IoT by using a binary Edwards curve. They were able to achieve optimised curve arithmetic and provide the performance benefit of intrinsic security for IoT devices against physical attacks. ECC is widely used for keys, encryption, decryption and digital signatures. [21] used a twisted Edwards curve variant and demonstrated performance improvement on target platform. Verification of digital signature from ECDSA requires double scalar multiplication. These issues result in speed and size issues in IoT applications. [76] enhanced Edwards curve to achieve nonrepudiation in IoT blockchain ecosystem. [19] Their work demonstrates the use of the Edwards curve and showcases how they can reduce implementation space, and operational cost and perform fast verification.

Table 4 on page 282 summarises on how the Edwards curve is used in IoT for security enhancement.

3.4 Schnorr's signature for multi-signature

In this sub-section research works on various applications of Schnorr's signature for Multi-signature are reviewed and presented.

A digital signature is the building block of a transaction in the blockchain. [46] addressed the problem of time consumption in multiple signature endorsement transactions. Their new schemes helped to achieve secure, transaction efficiency and low storage utilisation.Partial random signature generation attacks are the most common type of attack in a multi-signature environment. [47] proposed a Schnorr based multi-signature with a verifiable and deterministic nonce that can work non-interactively with a zero-knowledge proof. [48] proposed a multi-party computation protocol that is computationally cheap than the similar multi-signature model. They achieved a considerable contribution to privacy protection in blockchain. Their main idea was to merge and sign transactions under anonymous conditions using Pedersen commit with the Schnorr signature.[49] used a combination of identity and Schnorr to authenticate the mobile system. Their method was proposed as an alternative to certificate-based proxy methods and are secure against possible attacks. The multi-party ElGamal and Schnorr based signature for authentication proposed by [50] achieved multi-party computation across the unauthentic channel.[51] proposed a new Secret Handshake scheme with a Multi-Symptom Intersection derived from a Schnorr signature. They authorised Private Set Intersection only if their target authentication policies are satisfied to execute. [52] proposed a new single and multi blind signature scheme that combines the Schnorr signature schemes and RSA based. MuSig is a new Schnorr-based multi-signature scheme proposed by [53].The use of Schnorr signatures makes it simple, efficient and support key aggregation. In [54] the authors introduced a security model for general aggregate signature schemes based on multi-user and thereby achieved a significant reduction

EC/DSS/DSA	Domain	Solution	#
Edwards Curve ECC	IoT	Security enhancement	[9], [13], [44], [45], [17] , [76] [19], [43]

Table 4: Elliptic and Edwards curve application in IoT.

in key size. [55] proposed a novel trust management system based on ECC for the MANET and classified different trust levels and types of attackers. [56] focused their work on developing path-checking protocols to ensure that supply chains have valid paths. Their method achieved multi-signatures and verification based on a modified Schnorr signature scheme. [57] the authors used developers self-signature and centre's signature on Schnorr's based signature scheme and created an Android self-signature policy. [58] created a scheme for signatures with multivariate linear polynomials using Schnorr's signature scheme and ElGamal public key cryptography for verification based on a threshold. [59] presented a comprehensive resilient security framework for multipath routing wireless ad hoc networks. They were using a self-certified public key and an integrated multi-signature scheme to ensure secure data transfer. Table 5 on page 283 summarize multi-signature implementation using Schnorr signature.

3.5 Aggregate signature using Schnorr's signature

In this sub-section research works on various application of Aggregate signature using Schnorr's signature are reviewed and presented.

[60] proposed Key Aggregable Interactive Aggregate Signatures (KAIAS), which has a verification function that uses only a single aggregated public key, dynamic signature aggregation, and only allows messages to be signed only by the message initiator. These benefits benefited in reducing the size of signatures for Bitcoin implementation. [61] proposed an alternative to the current Bitcoin signature scheme with the Schnorr signature scheme, based aggregation scheme.Their protocol allowed participants to run a decentralised mixer on the Bitcoin blockchain to exchange coins. [62] demonstrated that the aggregate signature from groups actually works against the ordinary implementation of DSA based aggregate signatures with Schnorr's variants. Their proposed scheme had maximum performance and compatibility. [63] compared a non-interactive aggregate signature cryptographic scheme to the ECDSA cryptographic schemes with Schnorr. Their work showcased the need for enhancement with a non-interactive model. [64] analysed Mimblewimble's provable security and formally demonstrated that under standard assumptions, the inflation and coin theft can be provably secured using Pedersen commitments with Schnorr or Pedersen commitments with BLS signatures. [54] introduced a multi-user secure model for conventional aggregate signature schemes, in disparity to BGLS's original. They achieved a reduction of key-prefixed BLS security in a multi-user model. They also used Katz and Wang technique to demonstrate a reduction from a variant of multi-user key-prefixed [65] used lightweight identity-based Schnorr signature scheme and proposed an identity-based aggregate signature scheme variant where signer need not agree on common randomness. The scheme reduced time-consuming bilinear pairing operation, making it computationally effective. [76] proposed an aggregate signature scheme, which can be used in [77] to enhance the data privacy and has the potential to be applied in [78] an pipelined cryptography verification to provide a novel hybrid method.

Table 6 on page 283 shows the application of Schnorr's signature for Aggregate signature

4 Elliptic curve cryptography

The last decade showed a slow transition of the Digital signature from the RSA signature to DS, and towards ECC with modern inventions, the shift focused on optimised performance. Modern cryptography based on the ECDSA is the adoption trend due to its key length, signature length, security level and performance [66]. The Elliptic curve has taken a broad, proven space in cryptography, replacing its ancestor DSA. The elliptic curve has a successor called the edwards curve, and they are taking up the elliptic curve in cryptography space. edwards curve have a superior advantage and doubling and tripling than the Weierstrass form of the elliptic curve. Edwards addition laws do not have exceptions as in the Weierstrass curve. Elliptic curves concepts are widely used for ECC. Harold Edwards, in 2007 explores and studied the Elliptic curve family and presented a new addition named Edwards curves. The Edwards curve became the core of the Edwards curve digital signature algorithm (EdDSA). EdDSA offers standard performance and overcomes most of the security problems faced by conventional digital signature schemes (DSSs).

4.1 Elliptic Curve DSA (ECDSA) and Edwards Curve DSA (EdDSA)

Figure 4 represents the flow of EdDSA and ECDSA.

4.2 Basic operations

4.2.1 Addition

The Edwards curve handles addition and doubling using the same formula compared with another version of the curve that uses different operation formulas. Addition law is a century-old but captured cryptography attention in the recent decade. Unlike other elliptic curves that use chords

EC / DSS / DSA	Domain	Solution	#
Schnorr's signature	Blockchain		[46], [48]
	General	Security enhancement	[58]
	Healthcare		[51]
	Network		[59]
	Mobile	Security enhancement, Authentication	[49], [57]
	Supply chain		[56]
	Cryptocurrency	Security enhancement, Performance optimisation	[47]
ECC	Mobile	Security enhancement, Trust Management	[55]
Boneh-Gentry-Lynn	Security	Security enhancement	[54]

Table 5: Schnorr's signature for Multi-signature.

EC/DSS/DSA	Domain	Solution	#
Aggregate and Schnorr Signature	Blockchain	Verification speed	
		Security enhancement	[62]
		Storage optimisation	
	Cryptocurrency	Security enhancement	
		Computation improvement	
		Signature size	[60]
		Security enhancement	[61]
		Speed improvement	[63]
		Signature size-reduction	[64]
	Security Enhancement	Security enhancement	
		Security enhancement	
		Security enhancement	[54],[75]
		Identity authentication	[65],[73]

Table 6: Aggregate signature using Schnorr's signature.

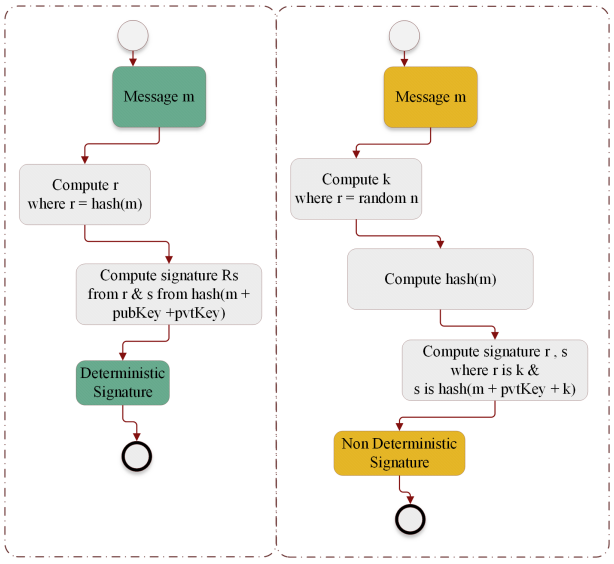

Figure 4: Flowchart of EdDSA and ECDSA.

and tangent to construct a point, the Edwards curve uses its method as a form of unit circle addition law. This says that if there are (x1,y1) and (x2,y2) in the Edwards curve the following (x3,y3) are known to be derived from the same curve such that x3 = (x1.y2 + x2.y1)/(a.(1+x1.y1x.2.y2)) and y3 = (y1.y2 — x1.x2)/(a.(1 — x1.y1x2.y2))

4.2.2 Doubling

Similarly, the doubling property can be applied by replacing (x2, y2) with (x1, y1) in the addition formula to obtain the doubling formula (x1, y1) + (x1, y1) = (x3, y3) such that x3 = (x1.y1 + x1.y1)/(a.(1+x1.y1.x1.y1)) and y3 = (y1.y1 — x1.x1)/(a.(1 — x1.y1.x1.y1)) This makes Edwards curves calculate a target point quickly [2].

4.2.3 Domain parameter and Key generation

Key generation starts with a self-generated private key and initializes the domain parameters. The generated private key is not accessible from outside by any third party. The public key is generated using the private key and the initialised parameter. This public key is accessed and readable from the outside. The private and public key pair ensure transmission protection.

4.2.4 Signature computation

The Edwards curve uses a hash of message instead of a random number, making this system collision-free and a different key for every message. Signature computation is based on the SHA algorithm are fixed length. The signature and the private key are used to generate a signature and sign the message. This digital signature allows the receiver to determine authenticity and offer non-repudiation.

4.2.5 Signature verification

Signature verification is a process by which the system can determine the authenticity of the message using the public key. The operation required the public key, digital signature and message.

Table 7 on page 285 represents the arithmetic operation cost comparison of the Edwards curve with other curves used in ECC.

4.3 Elliptic vs Edwards curve

EdDSA is a deterministic elliptic curve signature scheme with two curves Ed25519 and Ed448 [68]. ECDSA relies on cyclic groups over the finite field of the curve and is of discrete logarithm problem and a variant of the ElGamal signature scheme. The more improved version EdDSA is a variant based on Schnorr's signature scheme. EdDSA is simple, secure and fast compare with ECDSA.

4.3.1 Comparison of EdDSA vs ECDSA

The comparison of basic arithmetic, group law, and prime order are optimal for EdDSA. Curve safety is high in EdDSA. The performance of EdDSA is high in the segment and prevents security flaws. In the case of key loss or stolen its impossible to recovery in EdDSA. All of this is presented in 8 on page 285. Table 8 on page 285 tabulates the Comparison of EdDSA vs ECDSA as derived from [68] and [69]. Table 9 on page 285 presents the parameter comparison as presented in [70].

4.3.2 Security comparison

As presented in Figure 5 on page 284, the Edwards curve security level is far stronger at all security levels of 128,192 and 256 compared with the Weierstrass curve. Security level comparison of rho complexity is derived from [71] and [72].

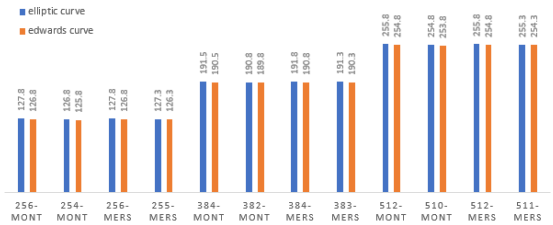

Figure 5: Security level[71] and complexity comparison[72].

4.3.3 Cost comparison

Figure 6 on page 284 shows the comparison of the total cost of TLS handshake both in compressed (C) and uncompressed (U) formats, illustrating that the Edwards curve has

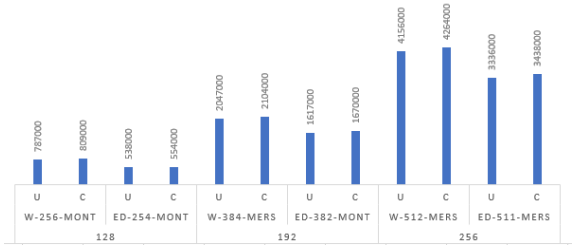

Figure 6: Cost estimate comparison[72].

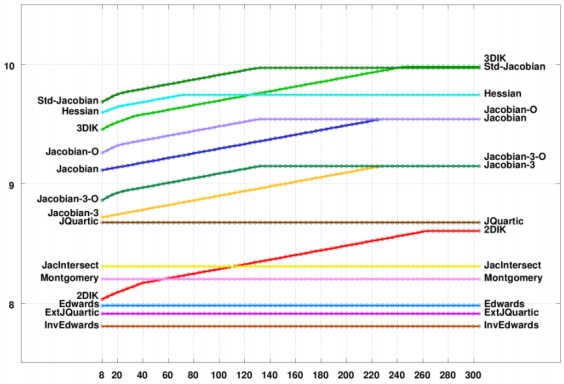

Figure 7: Speed comparison of curves [73].

the best values compared to the elliptic curve. Total cost estimate derived from [72]

4.3.4 Computation comparison

Figure 7 on page 284 shows the computation comparison on various curves. The Edwards curve has the least requirement, benefiting its implementation across various domains where the computation resource limits and requires speedy computation.

5 Discussion

Evidently, as noted by Bill gates in [74], the computing society and researcher should ensure a continuous disaster recovery plan and immediately switch to an alternative method when an existing security method proves fallible. This brings in the responsibility of the research community to explore and keep a standby successor digital signature in the event of a compromising situation or as an improvement over the existing digital signature that supports the security of digital technology. Elliptic curves and their variants have been re-purposed and used widely since 1980; Our empirical study demonstrates that the Edwards variant of the curve can be considered a performance improvement alternative for application in blockchain and IoT domains. Our review of the existing works shows the following 1).Application of ECC in Blockchain and IoT 2).Application

Curve	ADD	reADD	mADD	DBL	UNI
Edwards	10M +1S+1D	10M+1S+1D	9M+1S+1D	3M+4S	10M+1S+1D
Hessian	12M	12M	10M	7M+1S	12M
Jacobi intersection	13M+2S+1D	11M+2S+1D	11M+2S+1D	3M+4S	13M+2S+1D
Jacobi quartic	10M+3S+1D	9M+3S+1D	8M+3S+1D	2M+6S+2D	10M+3S+1D
Projective	12M+2S	12M+2S	9M+2S	5M+6S+1D	11N+6S+1D

Table 7: Comparison of arithmetic operation cost [67].

Attribute	Edwards Curve DSA	Elliptic Curve DSA
Curves	ax^2 + yx^2 = 1 + dx^2y^2	y^2=x^3+ax+b
Signature scheme	Schnorr signature scheme	ElGamal signature scheme
Performance	Faster	Slower
Order	Not prime order	Prime order possible
Key recover	Not possible	Possible
Curve safety	More	Less
Curve form	General	Subset
Curve arithmetic	Faster addition	Slower
Group law	Complete	Exception

Table 8: Comparison of EdDSA vs ECDSA [68] [69].

Parameters	ECDSA	EdDSA
Length of Key	384b	10b
Time take for -		
key generation(sec)	0.799s	0.0006s
sign generation(sec)	0.0016s	0.0002s
sign verification(sec)	0.0082s	0.0007s

Table 9: Parameter comparison [70].

of Schnorr's signature for Multi and Aggregate signature demonstrating. The application of ECC and Schnorr's signature shown in all these work supports how the digital signature is part of almost all digital applications. Our quest to find a performance improved alternative was solved with superior primary basic operation properties on the Edwards curve over the elliptic curve. 1).Addition used unit circle addition law 2).Doubling had a fast target point calculation than the elliptic curve 3).The private key and domain parameter are not accessible only the public key is exposed for external use 4).The Signature computation is based on hash, and 5).The verification is few expensive than other curve forms as tabulated in Table 7 on page 285 , Table 8 on page 285 and Table 9 on page 285. Direct secondary level comparison on the Edwards vs elliptic curve was strong, sound and clear on how Edwards outstood the predecessor. Edwards curve implementation was able to achieve 1).A higher security level as illustrated in Figure 5 on page 284 2).competitive cost values as illustrated in Figure 6 on page 284 3).speedy computation with fewer resource requirements than elliptic curve based implementation as illustrated in Figure 7 on page 284. Using Edwards curve in building Cross-domain Applications in Internet of Things such as [77] would provide performance improvement.

6 Conclusion

In this empirical study, we have provided a comparison of EdDSA vs ECDSA and concluded that EdDSA has advantages over similar DSAs. The Edwards curve performs simple and faster arithmetic and has high performance on various applications. Signature generation does not mandate the use of unique random numbers. An attack on the system built using the Edwards curve is not catastrophic. The key size and signature have small footprints; moreover, they are complete and hash collision-resistant. EdDSA is better than ECDSA and is recommended as a better replacement but depends on the use case. ECDSA is still in use on Bitcoin and Ethereum, as signature recovery is easy compared to EdDSA.

References

[1] Kerry C.F. and Gallagher P.D., "Digital signature standard (DSS)," FIPS PUB, pp. 186-4, 2013. https://doi.org/10.6028/nist.fips.186-4

[2] Edwards H.M., "A normal form for elliptic curves," Bulletin of the American Mathematical Society, vol. 44, no. 03, pp. 393- 423, 2007. https://doi.org/10.1090/s0273-0979-07-01153-6

[3] Laska M., "An algorithm for finding a minimal Weierstrass equation for an elliptic curve," Mathematics of Computation, vol. 38, no. 157, pp. 257-257, 1982. https://doi.org/10.1090/s0025-5718-1982-0637305-2

[1] Peretti C., Leoncini A., Gastaldo P., and Zunino R., "Edwards Curves and Extended Jacobi Quartic-Curves for Efficient Support of Elliptic-Curve Cryptosystems in Embedded Systems,"

International Journal for Information Security Research, vol. 4, no. 3, pp. 449-458, 2014. https://doi.org/10.20533/ijisr.2042.4639. 2014.0052

[2] Smart N.P., "The Hessian Form of an Elliptic Curve," in Cryptographic Hardware and Embedded Systems - CHES 2001, pp. 118-125, Springer, 2001. https://doi.org/10.1007/3-540-44709-1_11

[3] Aggarwal S. and Kumar N., "Digital signatures," Advances in Computers, The Blockchain Technology for Secure and Smart Applications across Industry Verticals, pp. 95-107, 2021. https://doi.org/10.1016/bs.adcom.2020.08.004

[4] DuPont B., Franck C., and Großschädl J., "Fast and Flexible Elliptic Curve Cryptography for Dining Cryptographers Networks," Mobile, Secure, and Programmable Networking, pp. 89-109, 2021. https://doi.org/10.1007/978-3-030-67550-9_7

[5] Kirlar B.B., "Efficient message transmission via twisted Edwards curves," Mathematica Slovaca, vol. 70, no. 6, pp. 1511- 1520, 2020. https://doi.org/10.1515/ms-2017-0444

[6] Islam M.M., Hossain M.S., Hasan M.K., Shahjalal M., and Jang Y.M., "Design and Implementation of High-Performance ECC Processor with Unified Point Addition on Twisted Edwards Curve," Sensors, vol. 20, no. 18, 2020. https://doi.org/10.3390/s20185148

[7] Semmouni M.C., Nitaj A., and Belkasmi M., "Bitcoin security with a twisted Edwards curve," Journal of Discrete Mathematical Sciences and Cryptography, pp. 1-19, 2020. https://doi.org/10.1080/09720529.2019. 1681673

[8] Skuratovskii R. and Osadchyy V., "The Order of Edwards and Montgomery Curves," WSEAS TRANSACTIONS ON MATHEMATICS, vol. 19, pp. 253-264, 2020. https://doi.org/10.37394/23206.2020.19.25

[9] Hisil H. and Renes J., "On Kummer Lines with Full Rational 2-torsion and Their Usage in Cryptography," ACM Transactions on Mathematical Software, vol. 45, no. 4, pp. 1-17, 2019. https://doi.org/10.1145/3361680

[10] 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

[11] Faz-Hernández A., López 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

[12] 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

[13] 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

[14] Seo H. and Kim H., "MoTE-ECC based encryption on MSP430," Journal of Information and Communication Convergence Engineering, vol. 15, no. 10, pp. 160-164, 2017. https://doi.org/10.6109/jicce.2017.15.3.160

[15] Franck C. and Großschädl 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

[16] Liu Z., Großschädl 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

[17] Karati S. and Das A., "Batch Verification of EdDSA Signatures," Security, Privacy, and Applied Cryptography Engineering, pp. 256-271, 2014. https://doi.org/10.1007/978-3-319-12060-7_17

[18] 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

[19] 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

[20] 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 Internet of Things Journal, vol. 8, no. 7, pp. 5914-5925, 2021. https://doi.org/10.1109/jiot.2020.3032997

[21] 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

[22] 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

[23] Arulprakash M. and Jebakumar R., "People-centric 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

[24] Kavin B.P., 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

[25] 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

[26] 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

[27] 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

[28] 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

[29] 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

[30] 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

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

[32] 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

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

[34] Zhang X., Zhao J., Mu L., Tang Y., and Xu C., "Identity-based proxy-oriented outsourcing with public auditing in 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

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

[36] Chen X. and Zhang X., "Secure Electricity Trading and Incentive Contract Model for Electric Vehicle Based on Energy Blockchain," IEEE Access, vol. 7, pp. 178763-178778, 2019. https://doi.org/10.1109/access.2019.2958122

[37] Liu Y., Liu X., Tang C., Wang J., and Zhang L., "Unlinkable Coin Mixing Scheme for Transaction Privacy Enhancement of Bitcoin," IEEE Access, vol. 6, pp. 23261-23270, 2018. https://doi.org/10.1109/access.2018.2827163

[38] Yuan C., xue Xu M., and ming Si X., "Research on a new signature scheme on blockchain," Security and Communication Networks, vol. 2017, 2017. https://doi.org/10.1155/2017/4746586

[39] Sajjad A., Afzal M., Iqbal M.M.W., Abbas H., Latif R., and Raza R.A., "Kleptographic Attack on Elliptic Curve Based Cryptographic Protocols," IEEE Access, vol. 8, pp. 139903-139917, 2020. https://doi.org/10.1109/access.2020.3012823

[40] Lara-Nino C.A., Diaz-Perez A., and Morales-Sandoval M., "Lightweight elliptic curve cryptography accelerator for internet of things applications," 2020. https://doi.org/10.1016/j.adhoc.2020.102159

[41] Lara-Nino C., Diaz-Perez A., and Morales-Sandoval M., "Energy/Area-Efficient Scalar Multiplication with Binary Edwards Curves for the IoT," Sensors, vol. 19, no. 3, pp. 720-720, 2019. https://doi.org/10.3390/s19030720

[42] Loiseau A., Fournier J.A., and J, "Binary Edwards Curves for Intrinsically Secure ECC Implementations for the IoT," Proceedings of the 15th International Joint Conference on e-Business and Telecommunications. International Conference on Security and Cryptography, 2018. https://doi.org/10.5220/0006831506250631

[43] Xiao Y., Zhang P., and Liu Y., "Secure and Efficient Multi-Signature Schemes for Fabric: An Enterprise Blockchain Platform," IEEE Transactions on Information Forensics and Security, vol. 16, pp. 1782-1794, 2021. https://doi.org/10.1109/tifs.2020.3042070

[44] Nick J., Ruffing T., Seurin Y., and Wuille P., "MuSig-DN: Schnorr Multi-Signatures with Verifiably Deterministic Nonces," Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. CCS '20: 2020 ACM SIGSAC Conference on Computer and Communications Security, 2020. https://doi.org/10.1145/3372297.3417236

[45] Feng L., Jie Y., Deli K., and Jiayin Q., "A Secure Multiparty Computation Protocol Combines Pederson Commitment with Schnorr Signature for Blockchain," 2020 IEEE 20th International Conference on Communication Technology (ICCT). IEEE, 2020. https://doi.org/10.1109/icct50939.2020.9295819

[46] Sanae H., Laassiri J., and Berguig Y., "MULTI-AGENT identity combined key Signature authentication PROTOCOL based schnorr signature with provable security under AVISPA," International Journal of Advanced Trends in Computer Science and Engineering, vol. 9, no. 5, pp. 7628-7635, 2020. https://doi.org/10.30534/ijatcse/ 2020/102952020

[47] Vu D.H., Luong T.D., and Ho T.B., "An efficient approach for secure multiparty computation without authenticated channel," Information Sciences, vol. 527, pp. 356-368, 2020. https://doi.org/10.1016/j.ins.2019.07.031

[48] Wen Y., Zhang F., Wang H., Gong Z., Miao Y., and Deng Y., "A new secret handshake scheme with multisymptom intersection for mobile healthcare social networks," Information Sciences, vol. 520, pp. 142-154, 2020. https://doi.org/10.1016/j.ins.2020.02.007

[49] Tan D.N., Nam H.N., Hieu M.N., and Van H.N., "New Blind Multisignature Schemes based on ECDLP," International Journal of Electrical and Computer Engineering (IJECE), vol. 8, no. 2, pp. 1074-1074, 2018. https://doi.org/10.11591/ijece.v8i2.pp1074-1083

[50] Maxwell G., Poelstra A., Seurin Y., and Wuille P., "Simple Schnorr multisignatures with applications to Bitcoin," 2019. https://doi.org/10.1007/s10623-019-00608-x

[51] Lacharité M.S., "Security of BLS and BGLS signatures in a multiuser setting," Cryptography and Communications, vol. 10, no. 1, pp. 41-58, 2018. https://doi.org/10.1007/s12095-017-0253-6

[52] Singh O., Singh J., and Singh R., "Multilevel trust based intelligence intrusion detection system to detect the malicious nodes using elliptic curve cryptography in MANET," Cluster Computing, vol. 21, pp. 51-63, 2018. https://doi.org/10.1007/s10586-017-0927-z

[53] Xin W., Wang M., Shao S., Wang Z., and Zhang, "A variant of schnorr signature scheme for path-checking in RFID- based supply chains," 12th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD). IEEE, 2015. https://doi.org/10.1109/fskd.2015.7382368

[54] Lee H.C., Jung J.H., and Yi J.H., "Multi-Signature Based Tamper Detection Scheme of Android Applications," Sensor Letters, vol. 11, no. 9, pp. 1820-1827, 2013. https://doi.org/10.1166/sl.2013.3004

[55] Shen Z. and Yu X., "Threshold signature scheme with threshold verification based on multivariate linear polynomial," Journal of Shanghai Jiaotong University (Science), vol. 16, no. 5, pp. 551-556, 2011. https://doi.org/10.1007/s12204-011-1186-4

[56] Vaidya B., Makrakis D., Park J.H., and Yeo S.S., "Resilient Security Mechanism for Wireless Ad hoc Network," Wireless Personal Communications, vol. 56, no. 3, pp. 385-401, 2011. https://doi.org/10.1007/s11277-010-9978-7

[57] Kojima R., Yamamoto D., Shimoyama T., Yasaki K., and Nimura K., "A Novel Scheme of Schnorr Multisignatures for Multiple Messages with Key Aggregation," Lecture Notes in Networks and Systems,Advances on Broad-Band Wireless Computing, Communication and Applications, pp. 284-295, 2020. https://doi.org/10.1007/978-3-030-61108-8_28

[58] Barbara F. and Schifanella C., "DMix: decentralised mixer for unlinkability," 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS). IEEE, 2020. https://doi.org/10.1109/brains49436.2020. 9223282

[59] Zhao Y., "Practical Aggregate Signature from General Elliptic Curves, and Applications to Blockchain," ACM Asia Conference on Computer and Communications Security, 2019. https://doi.org/10.1145/3321705.3329826

[60] Pedrosa A.R., Potop-Butucaru M., and Tucci-Piergiovanni S., "Scalable lightning factories for Bitcoin," The 34th ACM/SIGAPP Symposium on Applied Computing. ACM, 2019. https://doi.org/10.1145/3297280.3297312

[61] Fuchsbauer G., Orrù M., and Seurin Y., "Aggregate Cash Systems: A Cryptographic Investigation of Mimblewimble," Advances in Cryptology - EUROCRYPT 2019, pp. 657-689, 2019. https://doi.org/10.1007/978-3-030-17653-2_22

[62] Selvi S.S.D., Vivek S.S., Shriram J., and Rangan C.P., "Identity based partial aggregate signature scheme without pairing," 35th IEEE Sarnoff Symposium. 2012 35th IEEE Sarnoff Symposium, 2012. https://doi.org/10.1109/sarnof.2012.6222731

[63] Sury O., "Use of the SHA-256 Algorithm with RSA, Digital Signature Algorithm (DSA), and Elliptic Curve DSA (ECDSA) in SSHFP Resource Records," Request for Comments, vol. 6594, 2012. https://doi.org/10.17487/rfc6594

[64] Bernstein D.J. and Lange T., "Faster Addition and Doubling on Elliptic Curves," in Advances in Cryptology - ASIACRYPT 2007, pp. 29-50, Springer. https://doi.org/10.1007/978-3-540-76900-2_3

[65] Josefsson S. and Liusvaara I., "Edwards-Curve Digital Signature Algorithm (EdDSA)," Internet Research Task Force, Crypto Forum Research Group, RFC, vol. 8032, pp. 257-260, 2017. https://doi.org/10.17487/rfc8032

[66] Pornin T., "Deterministic usage of the digital signature algorithm (DSA) and elliptic curve digital signature algorithm (ECDSA)," Internet Engineering Task Force RFC, vol. 6979, pp. 1-79, 2013. https://doi.org/10.17487/rfc6979

[67] Shivani Y.N., Srinivas A., Thanmayi B.K., Vignesh V., and Srividya B.V., "EdDSA Over Galois Field GF(pm̂) for Multimedia Data," Journal of Engineering Research and Reports, pp. 1-7, 2019. https://doi.org/10.9734/jerr/2019/v4i416911

[68] B. Black, J. W. Bos, C. Costello, P. Longa, and M. Naehrig, Elliptic curve cryptography (ECC) nothing up my sleeve (NUMS) curves and curve generation. 2014.

[69] Bos J.W., Costello C., Longa P., and Naehrig M., "Selecting elliptic curves for cryptography: an efficiency and security analysis," Journal of Cryptographic Engineering, vol. 6, no. 4, pp. 259-286, 2016. https://doi.org/10.1007/s13389-015-0097-y

[70] Bernstein D.J. and Lange T., "Analysis and optimisation of elliptic-curve single-scalar multiplication Data set," Finite Fields and Applications,Contemporary Mathematics, pp. 1-19, 2008. https://doi.org/10.1090/conm/461/08979

[71] Gates, B., Myhrvold, N., Rinearson, P. and Domonkos, D., The road ahead. London, England: Viking, 1995.

[72] Guruprakash J, Koppu S. EC-ElGamal and genetic algorithm-based enhancement for lightweight scalable blockchain in IoT domain. IEEE access: practical innovations, open solutions. 2020;8:141269–141281. http://dx.doi.org/10.1109/access. 2020.3013282

[73] Abouelkheir, Eman, and Jolanda G. Tromp. "A pairing free secure identity-based aggregate signature scheme under random oracle." Informatica 42.2 (2017).

[74] Gu K, Yang L, Liu Y, Yin B. Trajectory data privacy protection based on differential privacy mechanism. Informatica. An International Journal of Computing and Informatics. 2018;42(3). http://dx.doi.org/10.31449/inf.v42i3.1638

[75] Bitat A, Merniz S. Formal verification of pipelined cryptographic circuits: A functional approach. Informatica. An International Journal of Computing and Informatics. 2021;45(4). http://dx.doi.org/10.31449/inf.v45i4.3176

[76] Jayabalasamy G, Koppu S. High-performance Edwards curve aggregate signature (HECAS) for non-repudiation in IoT-based applications built on the blockchain ecosystem. Journal of King Saud University - Computer and Information Sciences. 2021. http://dx.doi.org/10.1016/j.jksuci.2021.12.001

[77] Benkhaled S, Hemam M, Djezzar M, Maimour M. An ontology – based contextual approach for cross-domain applications in internet of things. Informatica. An International Journal of Computing and Informatics. 2022;46(5). http://dx.doi.org/10.31449/inf.v46i5.3627