Exploring Digital Signature Methods: A Comprehensive Review

Asst.Prof. Dalal N. Hammod [1] **Mustafa Amer Mohammed Ali** [2]
Dalal.naeem@nahrainuniv.edu.iq mustafa.a.mohammedali.sci24@ced.nahrainuniv.edu.iq

Abstract: Because of the digit development height since (2019) and the result market demand for data security investigate, it grows speedy and more than adequately with an obligation to form a huge scope of electronic mark examine. These range from classical embedded designs, through revocable and certificate-linked signatures to aggregate signatures, multi-party signatures for the wide system setting and finally privacy preserving blind signatures. It also includes post-quantum methods and proposals for blockchain environments and embedded systems, traffic, and vehicle areas. The selected and compared research works are presented in this manuscript for the years 2023 to 2025 by jointly collecting them on different features including key generation or setup cost, signature size, signature time, cycles of computation, verification time and communication cost as well as system-level load reduction. The equivalency illuminates that no one approach performs best on all measures. For aggregate and hierarchical schemes, more signature scalability is yielded at the cost of larger signatures compared to classical embedded signature schemes. We further remark that post-quantum designs are becoming more suitable and suitability-oriented through providing tech-practical trade-outs for blockchain, IoT, to a lesser extent also hardware delegates. (EdDSA) and (ECC) will still be good preferred choices for applications which require high efficiency with reasonable to strong security, while (RSA) will still stay a suitable candidate & preferred choice for legacy systems or situations were compatibility and compliance are critical driver as always.
Keywords: Digital signature; direct signature; arbitration signature; integrated signature.

1. Introduction

Digital signatures are a very powerful and common system and tool for security, used to secure valuables in digital form. They associate the signer with data in

[0] Assist. Prof., Computer Science Department, College of Science, Al-Nahrain University, Baghdad, Iraq
[2] M.Sc. Student, Computer Science Department, College of Science, Al-Nahrain University, Baghdad, Iraq

A way that strengthens integrity, authenticity and verifiable consent as a part thereof the electronic workflows. Recent applied studies reveal their significance and importance beyond the traditional cotizacion simple file exchange function to cover also role functionality in processing official documents, protection for low-resource

Internet of Things (IoT) (configurations, + hybrid secure communication architectures). This change implies that “signature schemes” are no longer just judged by the level of theoretical security they provide, but also along other important metrics, including (implementation cost, interoperability response time and application environment) [1], [3], [7].

The scientific literature defines digital signatures in a number of similar ways. A digital signature is simply a value produced from an input (“the private key”) that can be verified via the public key to determine if the source of the message matches and has not been tampered with or altered without authorization, as viewed through the lens of cryptography. Even more broadly, from a systems perspective, digital signatures are viewed as an axiom of trust for enabling platforms to authenticate content attribution (i.e. who created the content), ensure non-repudiation in auditable workflows and most importantly, ensuring integrity, and security of data. Especially in modern applications where it is crucial that signed data remains authentic after being stored or transmitted, digital signatures are tied to traceability and reliable verification [1, 4].

Digital signatures provide lots of advantages and benefits; they can help Prevent “unauthorized alteration”, enable “source authentication” and “increase accountability”, while diminishing manual trust processes in automated systems. These traits bolster trust in transmitted content and improved service continuity in applications like secure data exchange, document processing, and IoT communications. Yet, limitations and some practical considerations still exist such as complex structuring & managing of certificates and keys, implementation sensitivity, revocation cost, high storage or computing overhead in advanced or post quantum environments [2] [7]. Lastly, the objective of this research is to review the digital signature techniques discussing their pros and cons in order to find out which method is more suited depending on user requirements. This research is organized as follows: In Section 2, we explain types of digital signatures; in Section 3, we present some related works; inSection4, we present and discuss the results obtained;in Section5, we introduce the conclusions issued from this study;(the references are presented in Section 6.

2. Types of Digital Signatures

The digital signature workflow typically revolves around four interconnected stages: key generation/setup, message fingerprinting, signature generation and verification. While this generic architecture is regarded stable, a recent paper defines signature schemes in terms of their cryptographic basis as well as application. Others rely on the design to add some privacy, different authorization, clustering or quantum resistance so they can be used in specific deployments or others opt for a more explicit signer-verifier interaction. Consequently, digital signature classes could be examined both as operational kinds and algorithm families [1, 3].

2.1Workflow and General Algorithmic Workflow of Digital Signature Systems

To generally represent the field, we can abstract the independent of RSA, ECC, EdDSA, post-quantum, blind loop or clustering digital signature process. This general context of the model shows on one hand visible algorithmic difference (note that they are mainly focused on the functions with respect to producing and generating the signature, keys and verification), while in another hand operational logical approach stays similar (in terms of step counts: prepare/message, produce signature, send, verify, decision making [1], [3], [7]).

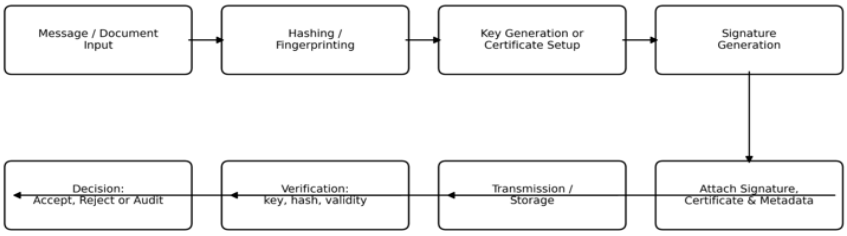

Figure 1. General workflow steps for a digital signature system

Step	General operation
1	Define the security context: user identity, application domain, trust model, certificate policy, and required security level.
2	Generate or obtain cryptographic keys and public verification credentials according to the selected signature family.
3	Prepare the message or document and compute a unique digest or fingerprint using a secure hash function.
4	Use the private signing credential to generate a signature over the digest, together with any required metadata such as timestamp or certificate status.
5	Attach or transmit the signature, public certificate information, and signed data to the verifier or storage system.
6	At verification time, validate the public key or certificate chain, revocation state, timestamp, and policy constraints.
7	Recompute the message digest and apply the verification function using the public verification credential.
8	Accept the signature if verification succeeds and policy conditions are met; otherwise reject it or forward it to audit/dispute handling.

Algorithm 1. General algorithm for creating a digital signature.

This also explains why comparisons should not be made based on a single variable. When all parameters such as signature time, signature size, verification time, cancellation processing communication costs, deployment compatibility and memory resource consumption then will to get the final selection of digital signature approach.

Direct Digital Signature : The Message is signed directly by the "signing party" using (his/her) corresponding private key and the recipient verifies it using their associated public key. This model is also typical for the cases where we would like to provide authenticity and integrity directly, without any relying on a separate entity [1].

Verified digital Signature: In this type, a trusted third party, or verification authority is involved in identity confirmation, certificate issuance and dispute resolution. This is valid when verification needs more "robust administrative controls", policy enforcement or established trust relationships. Digital signature types classification according to their application is illustrated in table 2 [2].

Table 2: Comparison of different types of digital signatures based on method of usage

Feature	Direct Signature	Arbitrated Signature
Third Party	no	Yes
Speed	Faster	slower
Security Level	Medium	higher
Dispute Resolution	Difficult	Easier
Scalability	High	Limited
Complexity	low	Higher

RSA Signature : It is one of the "oldest and most widely used", based on the(RSA algorithm). It utilizes a pair of keys: one public and another private. It is used in secure(e-mail, digital certificates and SSL/TLS environment).

DSA Signature: It was based on the digital signature algorithm (1991), it is also only for signing, not encryption, and is considered to be a member of the classic public-key signature family.

ECDSA (Elliptic Curve Digital Signature Algorithm): This signature is based on (elliptic curve encryption), uses smaller keys with a similar level of security in comparison to many other algorithms, and it is used in the (blockchain, IoT and low-resource security systems).

EdDSA: This signature is built on new "Edwards curves", used in modern systems and high-speed applications. Its appeal is established through its own signature

efficiency, robust security features and ability to support advanced blockchain oriented signature architectures (2).

The advantages and disadvantages of each type of digital signature is shown in Table (1).

Digital Signature type	advantages	disadvantages
RSA Signature	High security, and widely supported in most systems.	Relatively slower and requires large keys.
DSA Signature:	It is faster than RSA in some operations, and is an official standard in many systems.	Less flexible compared to RSA.
ECDSA Signature (Elliptic Curve Cryptography)	High speed, low power consumption, and suitable for devices with limited resources.	High mathematical complexity, sensitivity to execution errors, and the possibility of being exposed to side channel attacks.
EdDSA signatures	Very strong security, resistance to some side attacks, and fast execution.	Limited compatibility with legacy systems, and limited support in some PKI architectures and hardware systems.

Various other signature types for random signatures and complex signatures: The most up-to-date studies have extended the trademark paradigm and arise basic structure printing to support secrecy, trademark compression, collective authorization and potent attacks on quantum computing. As a result, the recent literature often considers ring, blind, collective, aggregate, post-quantum and multi-signature signatures as dedicated classes achieved and engineered for specific environments including reputation systems [5]So called “Electronic evidence” (evidence produced with methods of electronic services [6])Blockchain flows[7]Composite networks: VANETs[8];IoT Systems 9.

1.Blind signature: In this case, the signatory signs on a message (without knowing what it contains) that preserves one party's privacy from another party. For example, they include systems providing anonymity for cryptocurrency [5], securely conducting electronic voting [4], and - more importantly - large-scale workflows to provide privacy guarantees for digital evidence[6].

2.Ring signature — allows any one of a group to (sign a message on behalf of the entire group whilst hiding the actual identity behind the signature). This can involve privacy-preserving transaction protocols, data reporting systems and anonymous payments [10].

3.Group signature: Combine “many signatures into a single one” and can prove the correctness of each individual member's signature. This includes “blockchain systems”, VANETs, and multi-device IoT systems [8].

4.Group signature: Allows a selected group member to sign on a message, while allowing a trusted party to unveil the identity of the signer when needed. Use cases

such as enterprise approval workflows [38, 44], reputation systems [7], and authentication and verification in multi-domain industrial IoT architecture [5].

5.Multi-signature : One is a type of signature that needs (multiple parties needed in order to sign a message) or a transaction for it to be valid. Such accounts involve scenarios like cryptocurrency wallets, a collaborative approval process and so on [9].

6.Post-quantum digital signatures: it is a quantum resistance digital signature and relies on algorithms ("novel like network-based algorithms, hash function or quantum-assisted architectures"). Some examples are secure communication systems, blockchains, and security systems for the resource-constrained devices [4, 7].

Even accounts filled through signature batching are a huge benefit to the pools who fill live space in other blocks, as these bloated signatures must be stored somewhere ("account state"), they take up disk and network bandwidth! Key generation (or setup) costs are also non-negligible if credentials are renewed frequently or generated at scale. The time of "verification" and "signing" influencing the system responsiveness next to a computing power and memory which may be important for embedded devices as well. This can be especially true for collaborative, networked environments where the communication overhead and aggregate verification cost may potentially matter more than the time required by a single signing operation [3, 8].

3. Related Works

Modern Digital Security: The Role of Digital Signatures This is fundamental to validating data from being altered, verification of identities and enabling secure electronic transactions and interactions in an interconnected world. So, below are the list of many researches which in here study about digital signatures principle and concept on these types [21]

Although it only provides minimal security, Advanced Asymmetric Digital Signature : Lalem et al. In [11] proposed, a Hybrid digital signature scheme which integrates advantage of symmetric and asymmetric; it is intended to be computationally inexpensive while still being appropriate for cryptography environments. This signature was only "320 bits long", and the signing and verification in total took "48.4 milliseconds". They found that their proposed method yielded a right balance between small size and total execution time compared with several reference schemes.

ISBN: 978-3-030-58150-9IE-RCBS-kCAA Revocable Signature Pejaś et al. Example: [12] has solved the issue of certificate revocation by creating associative revocable signature with inner and outer certificates The study found signature times of "20 to 138 ms", verification times from "12 to 175 ms" and sequential

signature sizes varying between “387 and 1250 bytes” for different tested field sizes. Because of how the researchers integrate cancellation with real-world practicality, their method is appropriate for situations where long-term guarantee against non-cancellation is needed.

Algazy et al. — Syrga-1 Post-Quantum Hash-Based Signature The Syrga-1 algorithm introduced by [13] is a new post-quantum digital signature algorithm based on hash-based design rules. The research confirms private key of 8K bytes, public key of “8k bytes” and signature size of “1.033’s a bit” which supports around 1024 messages per private keys. It ca be observed that the time taken to generate keys was “4982 milliseconds”, the signature generation time was “632 milliseconds”, and the verification took “1296 milliseconds” in average respectively. It is less speedy than conventional lightweight schemes but provides a clear quantitative signature.

In this paper: Deniable periodic digital signature based on ISRSAC: Zhang et al. On the other hand, Wang et al. [14] introduced a high-throughput deniable periodic signature scheme for anonymous reporting and blockchain-like environments. Signature size for “100 ring members” was “1.2 KB”, while the signature generation time was “48 ms” with only a \approx “57\%” reduction in signature length and \approx 81\% generation speed improvement relative to structured or RSA-based schemes (improvements of storage space from deniable proof area were up to about 0.8KB/cycle).

ECC & CUK : Certificateless Group Signature ECAE: Wang et al. The ECAE scheme [15] proposed a certificateless group signature scheme without binary coupling related to NDN-IoT environments. Unlike the basic binary couplings, this method use elliptic curve operations which are cheaper. The total run time of ECAE is “81.9544 ms”, and when compared with some Reference schemes in the paper it is smaller. They also indicated how many hashes, multiplications, and additions were performed by both the user and server.

Hyper-Multi-Party Digital Signature (HMPS) [Guediri et al] The HMPS scheme was presented in [16] for such environments where multiple signers work collaboratively while the system is also monitored. Among three signers – total execution time was “2.2 ms”, (addition of generation and verification time). The researchers compared this to slower methods, including one that took 343 milliseconds, and reached the conclusion that a hierarchical structure facilitates reliable coordination of signatures with low-latency.

SPDM-AggSig Group Signature Kwon [17] added group signature mode into a scalable device authorization protocol. This approach not only makes individual signing faster, but also lightens the entire protocol load when many devices authenticate at once. The performance results demonstrated a ≈84.18% reduction in computation load and “≈96.22%” reduction in communication load over the

(SPDM-Origin) reference design, while still maintaining non-sequential certificates at approximately “300 bytes” or less [82].
FPGA Implementation of Falcon: Nguyen et al. [18] designed a hardware/software digital signature device based on the Falcon-1024 algorithm on an Arty-7 XC7A35T board. Key generation, signing and on-device verification times were “1516.2 ms”, “5.0 ms” and “2.238 ms” respectively. The importance of this work is that it shows how to successfully implement post-quantum signatures as opposed to just describing them algorithmically. To ensure embedded IoT devices network-based signatures,Iavich et al. [19] targeted embedded devices and introduced a post-quantum design along with explicit cycle counts and stack/heap measurements. Key generation consumed “102,400 cycles” and signing and verification took “496 k cycles” and “298.7 k cycles” respectively. It had a signature size of “2.8kb” and peak RAM usage just lower than “10kb”.
Blind Signature The last utility we discuss in our survey of the state-of-the-art are blind signatures, endorsed by (TBS21) Ticleanu et al. Privacy focused environments — A blind signature scheme [20] has been proposed. Their analysis showed a cryptanalysis time of “1.7ms”, signature time of “5.2ms” and verification time of “4.6ms” with signature “size =256” bits at “n=2048”. This work showed that adding more privacy to blind signatures does not depend on larger signature or longer times unlike other more expensive families of blind signatures.
Asymmetrical Quantum Signature with Multi-Branch Verkle Trees (k-cat Verkle trees): Iavich and Kapalov [21] put forward a signature architecture based on Virkle trees at “128 bits” of security. - The search returned a proof/signature size of “1.2 KB”, a verification time of “0.2 ms”, public key size as “1 KB “and private key as 1.5 KB. It claimed to reduce the signature size by two-thirds and increase verification speed by nearly a factor of four in comparison to “ML-DSA” from the same paper.
Better Verkle Signature Based on PRNG and QRNG Seeds: Iavich and Kapalov [22] then introduced an enhanced quantum signature architecture based on Verkle, using a pseudo-random generator seeded with a random number from the quantum seed to compress memory. The signature size was 5KB, the public key and private key were “1 KB” and “2 KB” respectively, while the signature time was approximately “15 ms” and verification time around “8 ms” (the latter being reduced to around 5 ms in NEON). It also indicated that it required “12 MB” of memory to store the private information for 10,000 keys and could verify “10,000” transactions in a batch within “2.1 seconds”.
Optimized Batch Verification on ECDSA of Blockchain: Wu et al. It was inspired by [23] which studied batch verification of blockchain transaction signatures. Both KTP-ECDSA and EC-GAMR-A signature scheme offer a batch signing ability, allowing the same signatories to perform 16th batches in parallel.

method achieved a single verification time of “58 ms”, whereas batch verification incurred times of “4.8 ms”. With a batch size of “1400”, the single signature verification time that was “177 ms” (per signatory), and the batch only took “5.2 ms” to be verified by all four signatories (one at a time). These values still prove that the verification process is mostly sped by the data provider. Linkable Ring Signature for Blockchain-Enabled Industrial IoT: Guo et al Weiyang et al. [24] proposed a new linkable ring signature scheme to protect users' privacy for industrial IoTs in blockchain networks. The sizes (in bytes) of public key, signature and private key for “80 bit” security was “362.42 KB”, “14.11 KB”, and “0.09 KB” respectively and these increase to be 【38†source】1444.87 KB, 28.22 KB, and “0.19 KB” respectively for “192” bits [2]. Their research suggested that these sizes were more efficient than various network ring options in comparison to them.

Blockchain-Based Post-Quantum Forensics For Internet of Vehicles: Zhang et al. Wang et al. When increasing the number of ring members to “1024”, the signature time reached as low as “232 ms” and verification was around “78 ms”; It also finds that when there are up to “32 vehicles participate”- ng, vehicle signature until RSU verification takes at most only 19 milliseconds in required IoV environment [17].

SMAD-LDS: An Efficient and Lightweight Digital Signature for IoV Devices: Ahmed et al. The SMAD-LDS scheme for secure authentication and message dissemination in unregulated Internet of Vehicles was proposed by [26]. The proposed methods lowered the computational cost in registration phase (“at least 46.8%”) and in transmission/receipt phases (“at least 94%”) compared to existent schemes. The communication costs are “234 bytes” for group message exchange and “320 bytes” for bilateral exchange, which represent considerable reductions compared with reference methods.

A Note on the Trying of Non-Tru-Based Certificate-Free Ring Signature with Logarithmic Growth: Gao etal. An NTRU based certificate free ring signature scheme and its electronic voting application were proposed in [27]. Although the ring size is supposed to be one of a few factors on the logarithmic growth in signature size, from “61.08 KB” at “N = 8” to “65.02 KB” at “N =512” (“signature key size was constant at 1.43 KB”) It also found signature times of “3.39”, “45.23”, “180.71” and “722.61 ms” over basic ring sizes, with realization times of duration “minutes 6.96” (“±0.334”),49.six All calculations were performed on durations in milliseconds [45].

Verkle-based HORST: Iavich et al. [28] introduced a new signature scheme that swaps out Merkle proof in favor of Verkle-based commitments. Spotting methods best suited for blockchain, IoT and any cyclic or recursive verification could also be highly relevant so the paper showed an implementation reducing signature size from “12.8 KB” to “3.2 KB” (“75%”) with a constant verification time rather than logn complexity!

Two-round multi-signatures using Okamoto signatures: Lee and Kim [29] introduced a two-round multi-signature structure based on Okamoto signatures In their analysis, the estimated times for key generation and verification was “3.032” ms &”4.548 ms” respectively, which were both independent of the number of signatories. While increasing the number of signatories does increase the time to generate the pooled key using our scheme, even large pools take at most “1.525 milliseconds”, so collaborative signing is feasible in blockchain-type environments. HinTS Silent-Configuration Marginal Signatures: Garg et al hinTS

Table 3: Summary of related work based on the review

Refere nce	Year	The method	The problem	the goal	Result	size the signature	generation / Key Settings	Signature / Total	/ Verification Load
[11]	2023	Advanced asymmetri c digital signature	to be The need signature It is asymmetrical It is integrated . time All less	design signature My work low Time . It is also short . Outputs	size It is smaller And so too time The whole It is less Compared to . several Plans	bits 320	N/R	ms (total) 48.4	Included in total
[12]	2023	IE-RCBS-kCAA revocable signature	He should that remains cancellation Certificates Acceptable And it is possible to expand And it will be benefit . Legal	Presentation and presentation signature It is acceptable Cancel With certificates implicit And . frank	cancellation practical with Cost Signature Verification / specific It is quantitative Through or via sizes Fields	B 1250-387	bit-638-160 fields	ms 138-20	ms 175-12

Refere nce	Year	The method	The problem	the goal	Result	size the signature	generation / Key Settings	Signature / Total	/ Verification Load
[13]	2024	Syrga-1	The need or the purpose to signature What will be after quantitative It will be with data size and . time Clear	Update and development algorithm signature New It is approved . on Hash	Presentation and provision file complete For size And time , with Use messages 1024 . be per key	KB 1.033	ms 4982	ms 632	ms 1296
[14]	2025	Periodic deniable signature (ISRSAC)	Signatures Ring The midwife To deny, you face or Suffering mostly from weakness Expansion in :Two things storage And . time	Planning or design signature He is periodic Meet To deny For the episodes . The big one	with regards For 100 members in : Episode Smallest By and faster %57 It is 81% of line The foundation Which is standing on RSA .	KB 1.2	KB 0.8 evidence/cy cle	ms 48	%81/%57 reduction
[15]	2025	ECAE	NDN-IoT authentication is required that Beware or avoid weight or load Conjunctions Which is dual The high . ground	Create or build signature My collection Incomplete Certificates and empty Also from Conjunctions .On ECC	Time Executive The whole It is less from several plans Compilation . Previous	Aggregate form	1H+3Mul+1 Add (user)	ms 81.9544	Pairing-free aggregate verify
[16]	2025	HMPS	Systems Distributed It requires or needs Signature It is multiple Levels In time It is low or . small very	Building or construction signature pyramidal It is multiple Parties For systems The cooperative .	ms includes 2.2 or includes all For three Signatories; Be faster By far from lines basis The aforementioned .	Compact aggregate	signers 3	ms (total) 2.2	Included in total

[17]	2025	SPDM-AggSig	He faces or suffers Verification from Devices from to rise Cost Computing And communication . s	Include or merge Signatures assembly In SPDM for authentication be midwife For . expansion	to provide It is large on level Regarding the protocol comparison b SPDM-Origin . .	Chainless cert B 300=>	Group attestation setup	.lower comp %84.18	lower %96.22 .comm
[18]	2025	Falcon FPGA device	Signatures Which is what after Quantity You need Published It is practical And enhanced or supported . Hardware-wise	Falcon-1024 implementation on Arty-7 FPGA board with control It's . software-based	Falcon device is practical with Times amount For the purpose of childbirth and the signature And . verification	Falcon compact PQ	ms 1516.2	ms 5.0	ms 2.238
[19]	2025	Lattice DS for embedded IoT	Devices Included or listed You need to Our safety What will be after quantitatively with border For courses And . memory	Enhance or improve the signature Network For devices Specific or . restricted	file balanced from party or from where Courses and size And . memory	KB 2.8	102,400 cycles	cycles 496,000	cycles 298,700
[20]	2025	Temperat e blind signature	Signatures , Which is blind what Still It requires or needs Insertion or merger in environments The restricted . one	Building or construction design light governor on . Privacy	time Competitive response with Signatures that . are short very	bits 256	Blinding 1.7 ms	ms 5.2	ms 4.6

Refere nce	Year	The method	The problem	the goal	Result	size the signature	generation / Key Settings	Signature / Total	/ Verification Load
[21]	2025	k-ary Verkle-tree PQ signature	Many and numerous from Signatures what after Quantity Remain or what Still large or slow in Verification . process	reduction Proofs And also speeding up Verification process through or via . Verkle trees	smallest And hurry from lines basis Which are mentioned when 128- bit . security	KB 1.2	/ Pub 1.0 KB Priv 1.5 KB	N/R	ms 0.2
[22]	2025	Optimized Verkle PQ signature	the signature Which is what after Quantitative He should that Reduces memory And also maintains . on Speed	Inserting or merging Verkle with seeded PRNG quantitatively To sign . Effective	balance Be strong between Size and consumption memory And . also speed	KB 5	/ Pub 1 KB Priv 2 KB	ms 15	ms (5 ms 8 (NEON
[23]	2025	Blockchai n-based KTP-ECDSA batch verificatio n	Payments Which is large in Blockchain make Verification process . Expensive	acceleration Verification process Payment For ECDSA signatories They are identical And they are . different	reduce or decrease sharp in time Verification process Likewise with more size The . payment	Batch mode	Batch size 16	/ ms individual 58 ms batch 4.8	ms 177 / individual ms batch 5.2
[24]	2025	Linkable ring signature for IIoT	IIoT privacy needs and requires Concealment process Identity And also the possibility Link Also, balance . Sizes	Update and development signature annular It is acceptable For linking For supported IIoT environments With . blockchain	Reduction and reduction sizes Keys and the signature In comparison several plans network Ring- . shaped	KB 14.11 ;(bit-80) KB 28.22 (bit-192)	/ Priv 0.09 KB 0.19	Lower than compared schemes	Lower transaction-signing cost

[25]	2025	IoV forensics with PQ blockchain	Mechanism or systems Evidence criminal In IoV you need Monitoring or tracking with protection It is what after . amount	Insert or merge Signatures Which is what after Quantity with storage Blockchain For .IoV	Show or display Times amount be on level Episode And also on - level Vehicle .to -RSU	Dual-ring style	vehicles 32	ms (1024 232 (members	ms; <=19 78 ms V-to-RSU
[26]	2025	SMAD-LDS	IoV messages require or need pregnancy Communication And mathematically . They are less	Usage and application signature digital It is light For the purpose of publishing Messages and . authentication	Decreases and drops large in Cost , Calculation with also loads Messages Small .	B 234 / group B one- 320 to-one	Registration phase	lower %46.8 regular cost	lower %94 ;.comp %70/%28 .comm
[27]	2025	Logarithm ic NTRU-based CLS ring signature	Signatures Episodes Special voting electronic It must or should that It increases or grows slowly with size The . episode	Construction and building signature annular The one who is indefinite Certificates growth or logarithmic increase On .NTRU	It grows or increases size the signature In a small way only From N=8 .to N=512	65.02-61.08 KB	Signing key KB 1.43	ms 722.61-3.39	ms 623.44-6.96
[28]	2025	Verkle-based HORST	Signatures Which is what after Quantity Which are approved on Hash Remain or what Still She faces and suffers from . Proofs Large	Replacement or substitution Merkle's proofs of obligations Which are approved On Verkle in .HORST	discount %75 and reduction in size the signature with Verification process time . Fixed	KB 3.2	N/R	N/R	Const.-time verify

Reference	Year	The method	The problem	the goal	Result	size the signature	generation / Key Settings	Signature / Total	/ Verification Load
[29]	2023	Two-round MS from Okamoto signatures	Signatures Which are multiple from Two rounds It requires and needs In short And our security . Officially	Construction and building first a plan Be safe from Two rounds , and that Based on .On Okamoto	Times practical For production and generation key and verification with key My compilation It is acceptable And it's possible to . return Usage	Succinct multi-signature	ms 3.032 GenKey	AggKey <=1.525 s	ms 4.548 Verify
[30]	2024	hinTS threshold signatures	the signature The limit He should that Enhances or supports Policies Balanced from Don or other numbers It is . expensive	Planning or design signature My limit , with Creating or preparing silent existing On .BLS	It grows or expands well Up to 1000 signatories with cost verification It . is constant	Constant-size threshold .sig	signers 1000	ms; agg. <0.5 s 1	ms 17.5

N/R = Non Mentioned Honestly in Table Quantitative or Text Available from The source . And when Requirement Used lineage reduction on level * . Protocol or Values Storage Instead from time verification Solo

3.1 Open Questions and Challenges from Previous Research

The studies and the literature reviewed indicate definite progress , but also highlight a series of remaining or only partially resolved barriers and challenges. These obstacles do not occur in isolation, but also arise regularly with classical digital signature studies and some other recent topics such as collusion, privacy, IoT

settings/post-quantum technologies/blockchain. These open issues are summarized in **Table 3a, along with linking the evidence from the reviewed studies.**

Problem category	Evidence from reviewed studies	Remaining gap	Practical effect	Possible research direction
Compact post-quantum signatures	Hash-, lattice-, Falcon-, and Verkle-based schemes improve quantum resistance [13], [18], [19], [21], [22], [28].	Many post-quantum schemes still require larger signatures, keys, memory, or setup time than classical signatures.	Higher storage and transmission overhead, especially in IoT, blockchain, and embedded systems.	Develop compression-aware parameters, hardware acceleration, and hybrid classical/post-quantum deployment profiles.
Certificate revocation and lifecycle management	Revocable signature designs address implicit and explicit certificates [12].	Revocation remains costly when credentials are frequently renewed or checked at scale.	Verification delays and administrative complexity increase in long-term document and legal workflows.	Use short-lived credentials, lightweight revocation proofs, and policy-based status checking.
Scalable verification for high-volume systems	Aggregate, collective, threshold, and batch verification schemes reduce protocol load [15], [17], [23], [26], [30].	A scheme that is fast for one signature may still be inefficient at the network or protocol level.	Blockchain, VANET, IIoT, and device attestation systems may experience bottlenecks during mass verification.	Move verification to aggregate/batch/gateway levels and evaluate protocol load, not only single-operation time.
Resource-constrained implementation	Embedded IoT and FPGA studies report cycles, RAM, signing time, and verification time [18], [19], [26].	Security improvements can conflict with battery life, RAM limits, hardware area, and real-time constraints.	Low-power devices may fail to support strong schemes without optimization.	Design implementation-aware schemes and publish benchmarks on comparable constrained hardware.
Privacy versus accountability	Blind, ring, linkable ring, deniable, and group-oriented methods provide privacy-related features [14], [20], [24], [25], [27].	Strong anonymity can conflict with auditability, dispute resolution, and legal accountability.	E-voting, electronic forensics, and IoV systems require both privacy and controlled traceability.	Adopt traceable privacy, accountable anonymity, and auditable policy layers.
Interoperability and legacy migration	RSA remains widely used, while ECC, EdDSA, and Schnorr-based schemes are more efficient in modern settings [1], [2], [9].	Newer efficient schemes are not always compatible with existing PKI, hardware tokens, and regulatory workflows.	Organizations may delay adoption despite better efficiency.	Use hybrid support, phased migration, and compatibility testing across PKI and application layers.
Unified benchmarking methodology	The reviewed papers report heterogeneous metrics, including bits, bytes, cycles, milliseconds, communication load, and percentage reductions [11]-[30].	Direct comparison is difficult when studies use different hardware, security levels, workloads, and measurement assumptions.	Readers may overestimate a scheme by focusing on one favorable metric.	Create standardized comparison profiles by application domain, security level, platform, and workload size.

Open problems still needing further solutions — as evidenced by the analysis of reviewed digital signature literature in table 3a.

So this survey is not primarily on the lack of new digital signature algorithms: it misses a balanced solution which considers (simultaneously size, scalability, revocation efficiency, post-quantum resistance, privacy and an acceptable implement ability with respect to current infrastructure). This gap makes comparative review studies and application-oriented selection guidelines necessary.

4. Results and Discussion

A. Small signature size: This group has small signatures, which are found in classical or lightweight privacy-oriented schemes. The classical one in [11] costs “320 bits” and the blind signature scheme in [20] takes 256 bits. On the post-quantum front, the smallest valid sizes seem to be “1.2 KB “[21], “1.033 KB (7†)” in [13] and up to” 3.2 KB” for Verkle-based commitments after replacing homogeneous Merkle proofs with those from [28]. This pattern reinforces that small size still is a serious barrier when quantum computing is a structural and design goal.

B. Signature and Verification Time: HMPS [16] is a single end-to-end proposal in the shortest multi-platform workflow, where both signing and verification for three signatures only consume “2.2 ms”. Similar good operational performance can also be seen with the Falcon FPGA-based device in [18] which reports “5.0 ms” for signing and “2.238 ms” for verification, but key generation takes significantly

slower. Embedded, integrated or collaborative architectures can still support the application in which moderate signing cost and fast verification are prioritized [20] and [29].

C. Embedded and Post-Quantum Environments: Our works [18], [19], [21] and [28], demonstrate that post-quantum digital signatures are bridging its gap from the theoretical level (i.e., design, architecture) to practical engineering levels. One reason is that working on embedded devices in [19] provides a major benefit since the number of cycles, memory consumption and signature size are all in one place. We note that the "FPGA" implementation in [18] demonstrates real implement ability, and that Verkle-based methods in [21] and [28] demonstrate concrete improvements to signature integrity and ZK verification efficiency using the proof architecture.

D. System-level scalability: Several of the most substantial contributions to the reviewed literature are those that eliminate a significant amount of overall system cost, rather than achieving the shortest time for an individual single signature.[19] We found that non-system-specific research can yield increased throughput through CT optimization and chain design/optimization results as well, and describe here key areas of system design for efficient signatures in unique execution processes; such as cross-chain relay positioning[20]. SPDM-AggSig lowered the communication and computation costs in [17] by "84.18%" and "96.22%", respectively. In [23], for example, batch verification was sped up as the batch size increased. In [26], SMAD-LDS significantly reduced the communication and computing costs in a vehicle environment. These results show that the state of the art in digital signature research now defines success at the level of protocols, not cryptography.

E. Reading between the lines: The most tempered way to finish is not that any scheme is superior or inferior all the way across the board, but that whether each approach ought be judged considering the operational envelope it was built for like table shown by

Table 4 : priorities of modern application in digital signature schemes

Application Type	Priority Criteria	Reason
Document-Signing System	A deterministic verification and a signature size that is integrated	To reduce and minimize the size of the signature and also to ensure rapid and predictable verification in formal workflows.
Block chain System	Aggregate/Batch Verification	Blockchain environments require and need effective verification of a large number of signatures within blocks.
IOT Environments	Low number of cycles, small number of bytes, and minimal RAM usage	IoT devices that are resource-limited require and need lightweight encryption schemes.
Post-Quantum Security System	Accepting larger signature sizes in exchange for stronger security	The post-quantity schemes give importance and priority to security that is long-term, even if the size of the signature increases.

Table 5 : comparative between types of digital signature based on level of security and efficiency

Types Of Digital Signature	Security Level	Key Length	Sig. Speed	Verification Speed	efficiency
RSA	High	2048-4096 Bit	Medium To Lower	Medium To Lower	less
ECC	High	256-521 Bit	Fast	Fast	improvement

Types Of Digital Signature	Security Level	Key Length	Sig. Speed	Verification Speed	efficiency
EdDSA	Very High	256 Bit	Very Fast	Very Fast	Very high (balance with security)
Direct Signature	Depend On Algorithm	Depend On Algorithm	Fast	Fast	Depend on application
Arbitrary Signature	Depend On Algorithm	Depend On Algorithm	Medium	Medium	Depend on application

Thus, (EdDSA) and (ECC) preferred for the "applications and uses with high efficiency needs and security" where "RSA" also remains fit to support legacy systems as well in virtual environments or timeliness is very crucial.

In addition, the comparative discussion made in this review shows that a digital signature scheme is value limited to its deployment rather than absolute. Conducting Signature based on Binary Matrix: In classic, light-weight schemes [11; 20], signature size is very small, which has a huge benefit through the workflow and behavior of documents and communications with low-bandwidth. But these schemes may not solve the long-term quantum resistant or large-scale verification problems. On the contrary, post-quantum and Verkle-tailored solutions [13], [18], [19], [21], [22], or under such a need in business Encryption guarantees or long-term compatibility are less well suited, but with high storage, setup, and implementation costs.

However, from the point of view of scalability, we can conclude that aggregational [16]; boundary [30]; hierarchical [15], group; and batch signatures [[17], [23]] show that the most significant performance gains are possible at the level of systems. Any scheme with a price per signature that is moderately lower than the previous list makes sense to use if it lowers communication overhead, aggregates many signatures, or allows for time-resolved verification between large groups of participants. This is the reason that blockchain, IoV, VANET and IIoT environments are focusing more on the total cost of the protocol rather than just time to sign (individual signatures).

Schemes that offer privacy-preservation [14], [20], 24, [27] further complicate the comparison. They may not be favored or selected purely for their lower latency,

compactness but because they protect the privacy of the signatory (in some cases), provide deniability or hide group membership. Nevertheless, a careful consideration about accountability (requirements), particularly in electronic evidence, electronic voting, institutional approvals and vehicle evidence applications and systems must take place over the privacy mechanisms. Thus, academic as well as scientific analysis of the comparison suggests that it is a multi-criteria decision problem in terms of mandate and choice of digital signature, involving security level, context of application, cost, trust model and sustainability.
Z. Practical proposals and suggestions for addressing identified problems—Drawing upon the gaps summarized in Table 3a (above) and following from the comparison discussion, we make a number of suggestions that may help practitioners strengthen practical adoption of digital signature schemes.

Table 6. Realistic suggestions for enhancing the rate of digital signature implementation and comparison studies

Identified problem	Practical proposal	Expected contribution
Large post-quantum signatures and setup cost	Use hybrid classical/post-quantum signatures during migration; apply parameter tuning, Verkle-based proof reduction, and hardware acceleration where possible.	Improves long-term security while limiting storage and latency growth.
Expensive certificate revocation	Integrate short-lived certificates, cached revocation proofs, timestamping, and periodic status validation.	Reduces verification delays and improves trust in long-term signed documents.
High load in blockchain, IoV, and IoT networks	Use aggregate, batch, threshold, or gateway-assisted verification at network checkpoints.	Reduces communication overhead and avoids repeated individual verification.
Limited RAM, energy, and processing power	Select schemes according to measured cycles, memory, and message size; offload heavy verification to edge gateways when appropriate.	Improves suitability for embedded and low-power devices.
Conflict between privacy and accountability	Use linkable, traceable, or policy-controlled privacy mechanisms instead of absolute anonymity when legal audit is required.	Maintains user privacy while supporting dispute resolution and forensic investigation.
Lack of comparable benchmarks	Report all experiments using common metrics: security level, signature size, key sizes, signing time, verification time, hardware platform, memory, and communication load.	Enables fair scientific comparison and clearer selection guidelines.
Legacy compatibility barriers	Adopt phased migration from RSA-heavy systems to ECC/EdDSA and post-quantum-ready schemes with compatibility testing.	Supports modernization without disrupting existing PKI and document systems.

These proposals build on—and further establish—the substantial practical significance of the review by converting comparative results into meaningful patterns and practices. Instead of guiding the design to one best-fit signature, the approach directs adapting the signature family to fit application needs such as: small document sizes; batch or aggregate verification for blockchain and large networks; implementation-aware, lightweight designs for IoT; privacy-prosecuting installations for secure workflows, hybrid or post-quantum constructions for long-term security.

5. Conclusions

These can be summarized in terms of our major four findings being: To begin with, the light-weighted, privacy-conscious and classical ways still provide basically the most thorough signatures. Second, at the protocol level, clustering and hierarchical/batch verification schemes can yield more significant savings. Third,

post-quantum designs are increasingly making practical waves themselves, especially those that include Verkle trees or consciously minimize memory use with FPGA support on the execution side. Fourth, practical research in blockchain, IoV and IIoT have become more concerned with specifying system-level metrics instead of mostly abstract algorithmic claims. This is why EdDSA or any Elliptic Curve approaches with security are preferred due to its high efficiency and effectiveness compared to RSA which is still one of the best candidates for legacy systems and situations where compliance, interoperability, and compatibility are top priorities.
In addition, the review outlines issues that not been fully addressed yet and should direct future work, namely: eliminating signature fees (post-quantums), improving and/or supporting cancellation management, agreeing on measurement methodologies for permissionless networks, enabling resource constrained systems to vote natively, achieving a balance between privacy and accountability. Thus, real-world deployment should follow multi-criteria selection strategies as opposed to basing choices on algorithm reputation or any single perfomance metric.

6. References

[1] K. Somsuk, "The development of signing and verification methods for high speed digital signatures on electronic official documents by using RSA cryptography," Cogent Engineering, vol. 11, no. 1, art. 2432513, 2024. doi: 10.1080/23311916.2024.2432513.

[2] K. Somsuk, "The special algorithm based on RSA cryptography for signing and verifying digital signature," Heliyon, vol. 11, no. 4, art. e42481, 2025. doi: 10.1016/j.heliyon.2025.e42481.

[3] A. A. Ahmed and O. M. Barukab, "Unforgeable Digital Signature Integrated into Lightweight Encryption Based on Effective ECDH for Cybersecurity Mechanism in Internet of Things," Processes, vol. 10, no. 12, art. 2631, 2022. doi: 10.3390/pr10122631.

[4] S. Han, K. Xu, Z. Zhu, S. Guo, H. Liu, and Z. Li, "Hash-Based Signature for Flexibility Authentication of IoT Devices," Wuhan University Journal of Natural Sciences, vol. 27, no. 1, pp. 1-10, 2022. doi: 10.1051/wujns/2022271001.

[5] H. An, D. He, Z. Bao, C. Peng, and Q. Liu, "An identity-based dynamic group signature scheme for reputation evaluation systems," Journal of Systems Architecture, vol. 139, art. 102875, 2023. doi: 10.1016/j.sysarc.2023.102875.

[6] H. Xiu, F. Ren, X. Xue, and D. Zheng, "An Efficient Code-Based One-Time Blind Signature Scheme for Electronic Forensics," IET Information Security, 2024, art. 6656367. doi: 10.1049/2024/6656367.

[7] M. I. Garcia-Cid, R. Martin, D. Domingo, V. Martin, and L. Ortiz, "Design and Implementation of a Quantum-Assisted Digital Signature," Cryptography, vol. 9, no. 1, art. 11, 2025. doi: 10.3390/cryptography9010011.
[8] H. Li, C. Shen, H. Huang, and C. Wu, "A certificateless aggregate signature scheme for VANETs with privacy protection properties," PLoS ONE, vol. 20, no. 2, art. e0317047, 2025. doi: 10.1371/journal.pone.0317047.
[9] P. Zhang, F. Ge, Z. Tang, and W. Xie, "Achieving High Efficiency in Schnorr-Based Multi-Signature Applications in Blockchain," Electronics, vol. 14, no. 9, art. 1883, 2025. doi: 10.3390/electronics14091883.
[10] L. He, X. Zhou, D. Cai, X. Hu, and S. Liu, "Post-Quantum Linkable Hash-Based Ring Signature Scheme for Off-Chain Payments in IoT," Sensors, vol. 25, no. 14, art. 4484, 2025. doi: 10.3390/s25144484.
[11] F. Lalem, A. Laouid, M. Kara, M. Al-Khalidi, and A. Eleyan, "A Novel Digital Signature Scheme for Advanced Asymmetric Encryption Techniques," Applied Sciences, vol. 13, no. 8, art. 5172, 2023. doi: 10.3390/app13085172.
[12] J. Pejaś, T. Hyla, and W. Zabierowski, "Revocable Signature Scheme with Implicit and Explicit Certificates," Entropy, vol. 25, no. 9, art. 1315, 2023. doi: 10.3390/e25091315.
[13] K. Algazy, K. Sakan, A. Khompysh, and D. Dyusenbayev, "Development of a New Post-Quantum Digital Signature Algorithm: Syrga-1," Computers, vol. 13, no. 1, art. 26, 2024. doi: 10.3390/computers13010026.
[14] Y. Zhang, Y. Yuan, Z. Yan, Y. Yang, and K. Zhang, "Practical periodic deniable signature scheme based on ISRSAC," Journal of King Saud University - Computer and Information Sciences, vol. 37, art. 210, 2025. doi: 10.1007/s44443-025-00217-w.
[15] C. Wang, H. Wu, Y. Gan, R. Zhang, and M. Ma, "ECAE: An Efficient Certificateless Aggregate Signature Scheme Based on Elliptic Curves for NDN-IoT Environments," Entropy, vol. 27, no. 5, art. 471, 2025. doi: 10.3390/e27050471.
[16] S. Guediri, M. Abbas, M. Kara, and M. AlShaikh, "Hierarchical Multiparty Digital Signature for Distributed Systems: Application in Intelligent Vehicle Surveillance," Journal of Cybersecurity and Privacy, vol. 5, no. 2, art. 22, 2025. doi: 10.3390/jcp5020022.
[17] H. Kwon, "Secure and Scalable Device Attestation Protocol with Aggregate Signature," Symmetry, vol. 17, no. 5, art. 698, 2025. doi: 10.3390/sym17050698.
[18] T.-T. Nguyen, D.-D. Nguyen, T.-T. Dao, and N.-Q. Luc, "Implementation Efficiency of Falcon Digital Signature Scheme on Arty-7 XC7A35T Board," Electronics, vol. 14, no. 22, art. 4504, 2025. doi: 10.3390/electronics14224504.

[19] M. Iavich, N. Kapalova, and K. Sakan, "Efficient Lattice-Based Digital Signatures for Embedded IoT Systems," Symmetry, vol. 17, no. 9, art. 1522, 2025. doi: 10.3390/sym17091522.

[20] O.-A. Ticleanu, I. D. Hunyadi, and N. Constantinescu, "Temperate Blind Signature Scheme for Particular Subspaces," Applied Sciences, vol. 15, no. 13, art. 7180, 2025. doi: 10.3390/app15137180.

[21] M. Iavich and N. Kapalova, "Asymmetric Post-Quantum Digital Signature Scheme with k-ary Verkle Trees," Symmetry, vol. 17, no. 3, art. 437, 2025. doi: 10.3390/sym17030437.

[22] M. Iavich and N. Kapalova, "Optimizing Post-Quantum Digital Signatures with Verkle Trees and Quantum Seed-Based Pseudo-Random Generators," Computers, vol. 14, no. 3, art. 103, 2025. doi: 10.3390/computers14030103.

[23] G. Wu, J. Zhou, and X. Fu, "Improved blockchain-based ECDSA batch verification scheme," Frontiers in Blockchain, vol. 8, art. 1495984, 2025. doi: 10.3389/fbloc.2025.1495984.

[24] F. Guo, Y. Gao, J. Jiang, X. Chen, X. Chen, and Z. Jiang, "Linkable Ring Signature for Privacy Protection in Blockchain-Enabled IIoT," Sensors, vol. 25, no. 12, art. 3684, 2025. doi: 10.3390/s25123684.

[25] Z. Zhang, Z. Cao, and Y. Wang, "Forensics System for Internet of Vehicles Based on Post-Quantum Blockchain," Sensors, vol. 25, no. 19, art. 6038, 2025. doi: 10.3390/s25196038.

[26] I. Z. Ahmed et al., "SMAD-LDS: Enhanced Secure Message Authentication and Dissemination with Lightweight Digital Signature in the Internet of Vehicles," 2025.

[27] W. Gao, T. Fu, S. Ren, S. Jin, X. Dong, and Z. Zhao, "Logarithmic NTRU-Based Certificateless Ring Signature in E-Voting Applications," Electronics, vol. 14, no. 7, art. 1358, 2025. doi: 10.3390/electronics14071358.

[28] M. Iavich, T. Kuchukhidze, and R. Bocu, "Post-Quantum Digital Signature: Verkle-Based HORST," Journal of Cybersecurity and Privacy, vol. 5, no. 2, art. 28, 2025. doi: 10.3390/jcp5020028.

[29] K. Lee and H. Kim, "Two-Round Multi-Signatures from Okamoto Signatures," Mathematics, vol. 11, no. 14, art. 3223, 2023. doi: 10.3390/math11143223.

[30] S. Garg, A. Jain, P. Mukherjee, R. Sinha, M. Wang, and Y. Zhang, "hinTS: Threshold Signatures with Silent Setup," Cryptology ePrint Archive, 2024.

استكشاف أساليب التوقيع الرقمي: مراجعة شاملة

مصطفى عامر محمد علي [2] أ.م.د. دلال نعيم حمود [1]

mustafa.a.mohammedali.sci24@ced.nahrainuniv.edu.iq Dalal.naeem@nahrainuniv.edu.iq

المستخلص:نظراً للتطور الهائل في مجال البيانات الرقمية منذ عام 2019، وما نتج عنه من طلب متزايد في السوق على أبحاث أمن البيانات، فقد نما هذا المجال بسرعة وبشكلٍ كبير، مما استدعى تطوير نطاق واسع من تقنيات فحص التوقيعات الإلكترونية. تتراوح هذه التقنيات من التصاميم المدمجة التقليدية، مروراً بالتوقيعات القابلة للإلغاء والمرتبطة بالشهادات، وصولاً إلى التوقيعات المجمعة، والتوقيعات متعددة الأطراف لأنظمة واسعة النطاق، وانتهاءً بالتوقيعات العمياء التي تحافظ على الخصوصية. كما تشمل هذه التقنيات أساليب ما بعد الحوسبة الكمومية، ومقترحات لبيئات سلسلة الكتل والأنظمة المدمجة، وقطاعات المرور والمركبات. يُقدم هذا البحث مجموعة مختارة من الدراسات البحثية التي تمت مقارنتها خلال الفترة من 2023 إلى 2025، وذلك من خلال تجميعها بناءً على خصائص مختلفة، تشمل تكلفة إنشاء أو إعداد المفاتيح، وحجم التوقيع، ووقت التوقيع، ودورات الحساب، ووقت التحقق، وتكلفة الاتصال، بالإضافة إلى تقليل الحمل على مستوى النظام. تُظهر المقارنة أنه لا يوجد نهج واحد يُحقق الأداء الأمثل في جميع الجوانب. ففي حالة المخططات المجمعة والهرمية، يتم الحصول على قابلية توسع أكبر للتوقيعات على حساب زيادة حجم التوقيعات مقارنةً بمخططات التوقيع المدمجة التقليدية. نلاحظ كذلك أن التصاميم ما بعد الكمومية أصبحت أكثر ملاءمةً وتوجهاً نحو التطبيق العملي من خلال توفير حلول تقنية عملية لتقنية البلوك تشين وإنترنت الأشياء، وإلى حدٍ أقل، لتفويضات الأجهزة. سيظل كل من (EdDSA) و (ECC)خيارين مفضلين للتطبيقات التي تتطلب كفاءة عالية مع مستوى أمان معقول إلى قوي، بينما سيظل (RSA) خياراً مناسباً ومفضلاً للأنظمة القديمة أو الحالات التي يكون فيها التوافق والامتثال عاملين حاسمين كما هو الحال دائماً.

الكلمات المفتاحية: التوقيع الرقمي؛ التوقيع المباشر؛ توقيع التحكيم؛ التوقيع المتكامل.

---

[0] استاذ مساعد دكتور؛ قسم علوم الحاسوب – جامعة النهرين- كلية العلوم – بغداد - العراق

[2] طالب ماجستير؛ قسم علوم الحاسوب- جامعة النهرين- كلية العلوم – بغداد – العراق