Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 1, 403-412
2025
Publisher: Learning Gate
DOI: 10.55214/25768484.v9i1.4154

Digital signatures and their legal significance

Josip Stanešić[1], Zlatan Morić[2*], Damir Regvart[3], Ivan Bencarić[4]
[1,2,3,4]Department of System Engineering and Cybersecurity Algebra University Zagreb, Croatia; josip.stanesic@algebra.hr (J.S.) zlatan.moric@algebra.hr (Z.M.) damir.regvart@algebra.hr (D.R.) ibencar@algebra.hr (I.B.)

Abstract: This paper examines the crucial function of digital signatures in guaranteeing electronic communications' validity, integrity, and non-repudiation. It investigates digital signatures' technological advancement and practical uses in diverse sectors by thoroughly analyzing foundational technologies, including Public Key Infrastructure (PKI) and cryptographic hash functions. It also considers emerging innovations such as blockchain-based trust models and quantum-resistant algorithms. Significant difficulties, such as cryptographic flaws and regulatory harmonization, are also addressed. The results indicate the imperative for ongoing improvements in cryptographic techniques and incorporating decentralized trust mechanisms to bolster system resilience, as digital signatures are indispensable for safe digital transactions. The results underscore the necessity of implementing innovative cryptographic solutions and aligning international rules to address the requirements of advancing digital ecosystems.

Keywords: *Blockchain, Cryptographic algorithms, Cybersecurity, Digital signatures, Electronic transactions, PKI, Quantum-resistant cryptography, Regulatory frameworks.*

1. Introduction

In the current digital era, ensuring secure communication and document authenticity has become crucial for trust in online interactions. Digital signatures serve as a critical mechanism, providing integrity, authenticity, and non-repudiation for digital transactions across diverse applications such as e-commerce, healthcare, and governmental systems. The legal recognition of digital signatures has further cemented their importance, facilitating seamless and trustworthy digital operations.

This paper explores the technological underpinnings, evolving applications, and legal significance of digital signatures. It delves into the intricacies of digital signature algorithms, Public Key Infrastructure (PKI), hash functions, and blockchain's emerging role in decentralizing trust. Moreover, the paper investigates security concerns like algorithm vulnerabilities and quantum computing threats. It addresses how regulatory frameworks like the E-Sign Act and eIDAS ensure legal compliance and global interoperability.

This paper's contributions are threefold: First, it comprehensively reviews advancements in digital signature technologies, including post-quantum cryptography and blockchain-integrated systems. Second, it highlights digital signatures' practical applications and challenges across sectors, offering insights into their transformative impact. Third, it proposes directions for future research, emphasizing the need for hybrid cryptographic solutions, optimized algorithms for resource-constrained environments, and enhanced global regulatory alignment.

The rest of this paper is organized as follows. The next section reviews foundational security principles and examines the role of PKI, hash functions, and signature algorithms in establishing robust digital signature systems. The subsequent section discusses the evolving applications of digital signatures across industries and their legal frameworks. An analysis of technological advancements and associated security challenges follows this. Finally, the paper concludes with a discussion of future research opportunities and a summary of findings.

History: Received: 27 November 2024; Revised: 24 December 2024; Accepted: 3 January 2025; Published: 9 January 2025
* Correspondence: zlatan.moric@algebra.hr

2. Related Work

Digital signatures have been increasingly integrated into various domains as a cornerstone technology for secure communications, ensuring authenticity, integrity, and non-repudiation. Over the last few years, research has explored algorithm advancements, applications in emerging technologies, and responses to evolving security challenges. The proliferation of digital signatures in e-commerce, healthcare, government, and blockchain sectors demonstrates their critical role in maintaining trust in digital transactions. Several studies have analyzed the performance of widely used algorithms such as RSA, ECDSA, and EdDSA, emphasizing their adaptability to various use cases and evolving threat landscapes [1, 2]. A notable shift has been the exploration of post-quantum cryptography, with algorithms such as CRYSTALS-Dilithium and Falcon emerging as viable quantum-resistant alternatives [3, 4].

Integrating digital signatures with blockchain technology has also gained momentum, enabling decentralized trust mechanisms and enhancing transparency in certificate issuance and revocation processes. Studies highlight blockchain's resilience to centralized points of failure, a notable limitation in traditional hierarchical CA models [5]. Quantum-assisted digital signatures (QADS) have been proposed to bridge classical and quantum cryptographic methods, promising increased security in the quantum era [6]. Research further underscores the importance of hardware optimizations for digital signature systems, as seen in developing efficient GPU and FPGA architectures to improve the throughput and latency of post-quantum algorithms [7, 8].

Applications in resource-constrained environments such as IoT, V2V communication, and mobile devices underscore the need for lightweight algorithms. ECC-based schemes like ECDSA are particularly well-suited for such scenarios due to their lower computational overhead [9]. Digital signatures have also been pivotal in securing sensitive data in healthcare and e-commerce, where integrity and confidentiality are paramount [10, 11]. Advances in hybrid signature schemes combining algorithms like ElGamal and IDEA provide enhanced robustness against tampering and unauthorized modifications [12].

The ongoing threat posed by vulnerabilities in cryptographic primitives such as SHA-1 has led to a transition towards more secure hash functions like SHA-256 and SHA-3, addressing the risks of hash collisions [13]. Research emphasizes rigorous implementation practices to prevent side-channel attacks and other exploitations from improper cryptographic operations [14]. With quantum computing on the horizon, hybrid solutions combining traditional cryptographic algorithms with quantum-resistant technologies are gaining traction as interim measures [15]. Moreover, advancements in regulatory frameworks such as the eIDAS Regulation and the E-Sign Act have harmonized the legal acceptance of digital signatures across borders, facilitating global commerce [16].

3. Public Key Infrastructure

Public Key Infrastructure is a sophisticated framework for managing digital keys and certificates, enabling secure electronic communications and transactions. At its core, PKI is built on asymmetric cryptography, which utilizes private and public keys. Its owner keeps The private key confidential, while the public key is publicly available. This dual-key mechanism ensures that data encrypted with the public key can only be decrypted using the corresponding private key and vice versa, forming the foundation of secure digital signatures [12]. The process begins with generating a cryptographic key pair, consisting of a private key, which the signer keeps secure, and a public key, which is shared with others for verification purposes. The strength of PKI lies in the secure creation, storage, and usage of these keys [14]. When signing a document, the signer uses a cryptographic hash function to produce a unique hash value for the document. This hash is then encrypted with the signer's private key, resulting in a digital signature. Alongside the document, the signature and the public key allow recipients to verify the document's authenticity and the signer's identity [15].

To verify the signature, the recipient uses the signer's public key to decrypt the digital signature, extracting the original hash value. The recipient then generates a new hash from the received document and compares it to the decrypted hash. A match confirms that the document remains unaltered and verifies the identity of the signer [13]. A trusted authority issues a digital certificate to associate a public

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 1: 403-412, 2025
DOI: 10.55214/25768484.v9i1.4154

key with its owner. This certificate is essentially a data file that includes the public key and information about the owner, such as their name and the key's validity period. The trusted entity responsible for issuing these certificates is known as a Certificate Authority (CA). CAs play a vital role in PKI by managing certificate issuance, renewal, and revocation. Before issuing a certificate, the CA validates the requester's identity through a stringent verification [15].

A digital certificate typically contains key elements such as the public key of the certified entity, information about the entity (e.g., organization or domain name), details about the issuing CA, the validity period, and the CA's digital signature, which ensures the certificate's authenticity. The standard format for these certificates is X.509, widely used in protocols such as TLS/SSL for securing web communications, S/MIME for secure emails, and IPsec for internet communications. X.509 specifies the certificate format, certification path validation algorithms, certificate revocation lists (CRLs), and attribute certificates [12]. An X.509 certificate includes significant fields such as the version number (currently version 3), a serial number uniquely assigned by the CA, the signature algorithm, issuer name (identifying the issuing CA), the validity period with start and end dates, and the subject name (identifying the entity receiving the certificate). It also specifies the subject's public key information, including the public key algorithm (e.g., RSA, ECDSA) and the key itself. Additionally, it contains details about the algorithm used by the CA to sign the certificate and the signature itself.

PKI relies on different trust models, with the most prevalent hierarchical model. In this model, root CAs certify intermediate CAs, which then certify end entities. Other models, such as the web of trust and hybrid models, also exist but are less commonly implemented. Registration Authorities (RAs) assist CAs by performing administrative tasks, such as verifying users' identities before issuing certificates. Certificate repositories are another essential component of PKI. These repositories store certificates and certificate revocation lists, which are records of certificates revoked before expiration due to compromise or other issues. CRLs ensure that revoked certificates are no longer trusted within the system.

By securely managing keys and certificates, PKI provides a reliable framework for digital signatures. The interactions among key pairs, CAs, RAs, and CRLs create a robust infrastructure that supports secure communications and transactions. As per Chauhan et al.'s work, PKI continues to be a cornerstone for ensuring the trust and security of digital signatures [16].

4. Hash Functions

A hash function is a mathematical algorithm designed to take an input, often called a "message," and produce a fixed-size string of bytes known as a hash value or hash code. This output appears random and is unique to each distinct input. A critical property of hash functions is the avalanche effect, where even a minor change in the input results in a drastically different output [17]. Hash functions are deterministic, meaning the same input will always yield the same output [18].

The operation of a hash function begins by dividing the input data into several fixed-sized blocks. Padding is applied to ensure the input's length matches the hash algorithm's block size requirements. Padding typically involves appending a single '1' bit, followed by a series of '0' bits, and finally adding the length of the original message. The algorithm initializes with fixed values specific to the hash function being used. The core process involves a compression function that processes each data block in a series of rounds, combining the block with the current hash value to produce a new one. This process is repeated for all blocks, and the final hash value, a fixed-size hash code, is generated [18]. In digital signatures, hash functions ensure message integrity and authenticity. When creating a digital signature, the message or document is first processed through a hash function to produce a compact hash value representing the original content. This hash value is then encrypted using the sender's private key, forming the digital signature. Since only the sender can access their private key, the signature confirms their identity [19].

When the recipient receives the message with the digital signature, they use the sender's public key to decrypt the signature, recovering the original hash value. The recipient independently computes the hash of the received message using the same hash function and compares it with the decrypted hash. If the two match, the message is verified as authentic and unaltered. Any mismatch indicates either tampering or an invalid signature. The design of hash functions ensures that even the slightest change in the original message produces an entirely different hash, making tampering immediately noticeable [17].

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 1: 403-412, 2025
DOI: 10.55214/25768484.v9i1.4154

Hashing is computationally efficient, enabling the rapid processing of large datasets, and the fixed-size hash value simplifies both storage and transmission compared to handling the original message or document.

Although strong hash functions aim to minimize collisions, where two different inputs produce the same hash, no hash function is entirely immune to collisions. Over time, advances in cryptanalysis may expose vulnerabilities in specific hash functions. The overall security of a digital signature system heavily relies on the robustness of the chosen hash function, as weaknesses in the function could compromise the integrity of the entire system.

5. Digital Signature Algorithms

Digital signature algorithms guarantee digital documents' authenticity, integrity, and non-repudiation. By employing cryptographic methods to create and verify signatures, these algorithms facilitate secure digital document exchange and signage across various platforms [9]. Several widely used algorithms offer distinct features and advantages, ensuring secure and efficient digital communication.

5.1. Rivest-Shamir-Adleman

RSA is one of the earliest and most popular digital signature algorithms (Rivest-Shamir-Adleman). RSA relies on the mathematical challenge of factoring large prime numbers, which underpins its security. The algorithm uses two keys: a private key for signing and a public key for verification. To create a signature, RSA generates a document hash and encrypts it with the signer's private key. Verification involves decrypting the signature using the public key and comparing the result to a hash of the received document. RSA is renowned for its compatibility and widespread acceptance across numerous platforms. However, ensuring robust security requires relatively large key sizes (2048 bits or more), which can lead to slower performance when compared to newer algorithms [2].

5.2. Digital Signature Algorithm

The Digital Signature Algorithm (DSA), developed by the National Institute of Standards and Technology (NIST), offers another practical approach. DSA is based on modular exponentiation and discrete logarithms, distinct from RSA's mathematical foundations. Like other algorithms, DSA uses a private key for signing and a public key for verification, creating and verifying signatures through hashing. DSA is particularly efficient in signature generation and often produces smaller signature sizes. Nonetheless, it is generally slower at signature verification than RSA and less adaptable to some cryptographic scenarios [20].

5.3. Elliptic Curve Digital Signature Algorithm

The Elliptic Curve Digital Signature Algorithm (ECDSA) represents a modern evolution in digital signature technology, leveraging the properties of elliptic curves over finite fields. ECDSA achieves the same security level as RSA but with significantly smaller key sizes. For instance, a 256-bit ECDSA key offers comparable security to a 3072-bit RSA key. This compactness enables faster computations and reduces storage requirements, making ECDSA ideal for environments with constrained resources, such as mobile devices and IoT systems [21]. The algorithm generates a document hash signed using a private elliptic curve key. The signature can be verified using the associated public key. While ECDSA is highly secure and efficient, proper implementation is essential to avoid vulnerabilities, particularly those arising from weak random number generation [9].

5.4. Edwards-curve Digital Signature Algorithm

Edwards-curve Digital Signature Algorithm (EdDSA) is a recent addition to digital signature schemes, optimized for high security and performance. Utilizing twisted Edwards curves enhances the efficiency and security of cryptographic operations. EdDSA, mainly its variant Ed25519, is known for speed, robustness, and resistance to common cryptographic implementation errors [3]. It employs a process similar to other algorithms: hashing the document and signing it with a private key, while

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 1: 403-412, 2025
DOI: 10.55214/25768484.v9i1.4154

verification is achieved through the public key. EdDSA stands out for its fast key generation, signing, and verification, making it a compelling choice for modern cryptographic applications due to its strong security and performance [1].

Each digital signature algorithm contributes unique advantages tailored to different security needs and computational contexts. RSA remains a versatile and widely used option. DSA efficiently generates compact signatures, ECDSA balances strong security with low computational cost, and EdDSA combines high performance with good security features. Selecting the most appropriate algorithm involves understanding these distinctions to meet the specific demands of digital document signage while ensuring a balance of security and efficiency.

6. Legislation and Standards

The growing reliance on digital transactions has necessitated a legal and regulatory framework to ensure electronic signatures' security, authenticity, and enforceability. Various legislative acts and standards have been established globally to define the legal validity of electronic signatures, enhance interoperability, and provide clear guidelines for their implementation. These frameworks promote trust in digital commerce, enabling secure interactions in both domestic and international contexts [22]. This section explores key legal and regulatory instruments governing digital signatures, including the E-Sign Act, the eIDAS Regulation, the Model Law on Electronic Signatures (MLES), and the NIST Digital Signature Standard (DSS).

6.1. The Electronic Signatures in Global and National Commerce Act

Enacted on June 30, 2000, the E-Sign Act is a landmark piece of U.S. legislation establishing the legal equivalence of electronic signatures and records with traditional paper-based formats in interstate and foreign commerce [23]. This act ensures that a signature, contract, or record cannot be denied legal validity solely due to its electronic nature. The E-Sign Act fosters efficiency and modernization across various industries by providing this legal recognition.

A critical element of the E-Sign Act is its emphasis on consumer protection. It mandates that consumers must be informed about their rights and explicitly consent to using electronic formats. This consent process requires demonstrating that consumers can effectively access and utilize electronic records. Furthermore, businesses must retain electronic records in a manner that preserves their integrity and ensures accessibility for the legally required retention period.

The act adopts a technology-neutral stance, refraining from mandating specific technologies for electronic signatures. This flexibility encourages innovation and ensures that the framework can accommodate future technological advancements. The E-Sign Act broadly defines an electronic signature, including any electronic sound, symbol, or process logically associated with a record and executed with the intent to sign. This inclusivity allows diverse electronic signature methods, from typed names to advanced PKI-based digital signatures.

Aligned with international standards like the EU's eIDAS regulation, the E-Sign Act supports cross-border compatibility in electronic commerce by ensuring the legal enforceability of electronic signatures regardless of the underlying technology [22].

6.2. eIDAS Regulation

The eIDAS Regulation (Regulation (EU) No 910/2014) establishes a comprehensive framework for electronic identification (eID) and trust services within the European Union. It aims to enhance trust in electronic transactions and foster a secure and unified digital market across EU member states. By replacing Directive 1999/93/EC, eIDAS addresses prior limitations and introduces a cross-sectoral approach to electronic transactions [23].

eIDAS requires mutual recognition of electronic identification schemes across member states if they meet specific regulatory standards. These schemes are categorized into three assurance levels: low, substantial, and high, with mutual recognition mandatory for substantial and high levels. This framework facilitates secure cross-border digital interactions with public authorities and businesses. Key provisions include mandatory notification of national eID schemes to the European Commission,

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 1: 403-412, 2025
DOI: 10.55214/25768484.v9i1.4154

adherence to strict liability rules for trust service providers, and immediate action in the event of security breaches, including suspending or revoking compromised eID schemes [23].

The regulation also provides a robust legal framework for various types of electronic signatures, including Qualified Electronic Signatures (QES), which have the same legal effect as handwritten signatures. QES are created using qualified electronic signature devices based on certificates issued by Qualified Trust Service Providers (QTSPs). QTSPs must adhere to stringent standards and undergo regular audits to maintain compliance, with their status recorded in the EU Trusted List.

6.3. Model Law on Electronic Signatures

Adopted by the United Nations Commission on International Trade Law (UNCITRAL) on July 5, 2001, the Model Law on Electronic Signatures (MLES) provides a uniform legal framework for recognizing and using electronic signatures in international commerce. It aims to reduce legal uncertainty and foster trust in electronic transactions, ensuring electronic signatures are as reliable as handwritten signatures.

MLES is built on three core principles: non-discrimination, which ensures that electronic signatures are not invalidated solely for being electronic; technological neutrality, which allows diverse technologies for electronic signatures; and functional equivalence, which ensures that electronic signatures fulfill the same role as traditional signatures. These principles enable flexibility and adaptability to evolving technologies.

To assist implementation, UNCITRAL provides a Guide to Enactment, which offers detailed explanations and practical guidance for legislators and stakeholders, promoting harmonization across jurisdictions.

6.4. NIST Digital Signature Standard

The National Institute of Standards and Technology (NIST) defines technical guidelines for digital signatures in its Federal Information Processing Standard (FIPS) Publication 186-5. DSS approves four algorithms: DSA, RSA, ECDSA, and EdDSA. It provides detailed specifications for key generation, signature creation, and verification processes, emphasizing secure cryptographic practices [22].

Digital Signature Standard (DSS) mandates using cryptographic modules compliant with FIPS 140-2 or later for key management, ensuring secure environments for generating, storing, and using cryptographic keys. Strong key management practices are required throughout the key lifecycle, including generation, distribution, and eventual destruction.

The standard also recommends approved hash functions, such as SHA-256 or higher, to create secure message digests resistant to collisions and cryptographic attacks. These guidelines ensure that digital signature processes remain robust and reliable, forming a secure foundation for electronic communication and transactions.

7. Applications of Digital Signatures

Digital signatures are a cornerstone technology for securing digital transactions and ensuring electronic documents' authenticity, integrity, and non-repudiation. Their versatility enables their application across various industries, significantly improving efficiency, trustworthiness, and compliance with regulatory requirements. This section delves into how digital signatures are utilized in business and commerce, government and legal systems, and healthcare, showcasing their transformative impact on these critical sectors.

7.1. Business and Commerce

Digital signatures have revolutionized business and commerce by enabling secure and efficient online transactions. They allow businesses to electronically sign contracts, invoices, and other essential documents, streamlining workflows and reducing the time and costs associated with physical signatures [24]. By ensuring the authenticity of signatories and the integrity of documents, digital signatures foster trust in e-commerce and other digital interactions. Financial institutions, for instance, rely on digital signatures to authorize transactions, safeguarding access to financial records and ensuring

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 1: 403-412, 2025
DOI: 10.55214/25768484.v9i1.4154

compliance with regulatory frameworks [25]. These measures are instrumental in preventing fraud and maintaining secure operations.

Globally, platforms such as DocuSign and Adobe e-Signature have become essential tools for businesses adopting digital signatures. DocuSign facilitates secure signing and document management while offering integration with existing applications to enhance workflow automation. Adobe e-Signature integrates seamlessly with tools like Acrobat and PDF, providing robust security features and ensuring compliance with international standards. In Croatia, services like FINA's e-signature, e-invoice, and e-payment demonstrate the local application of digital signatures in streamlining financial and business processes.

7.2. Government and Legal Systems

Using digital signatures in government and legal systems enhances administrative efficiency and the security of official documents. Governments employ digital signatures for issuing licenses, permits, and tax returns, ensuring that these documents are authentic and tamper-proof. Legal systems leverage digital signatures for signing contracts, court filings, and other legal instruments, maintaining document integrity and enforceability. Digital signatures uphold the rule of law and streamline legal processes by eliminating the possibility of repudiation.

The European Union's eIDAS Regulation exemplifies a comprehensive framework that ensures the cross-border recognition of electronic signatures, fostering international trade and cooperation [24]. Initiatives like the EU Digital Identity Wallet further support secure digital identity systems, enabling citizens to access government services across member states using a single identity. In Croatia, government agencies utilize AKD PKI to issue official documents and facilitate secure electronic communication, demonstrating the integral role of digital signatures in public administration.

7.3. Healthcare

In healthcare, digital signatures are essential in securing electronic health records (EHRs) and maintaining patient information privacy. They ensure that prescriptions, medical reports, and other sensitive documents are verifiable and free from tampering, thus upholding the confidentiality and integrity of healthcare data [26]. Compliance with regulations like the Health Insurance Portability and Accountability Act (HIPAA) in the United States highlights the importance of digital signatures in protecting patient information.

Digital signatures also simplify communication between healthcare providers, enabling the secure exchange of medical information and improving coordination in patient care. Patients benefit from the ability to sign consent forms, simplifying administrative procedures electronically. In Croatia, the national healthcare IT system, "Portal Zdravlja," incorporates digital signatures for authenticating medical documents, managing e-prescriptions, and ensuring the integrity of patient records, illustrating their critical application in enhancing healthcare efficiency and security.

8. Technological Evolution and Security Concerns

As digital signatures continue to secure online interactions, technological advancements and emerging security challenges shape their development. This section addresses the critical security concerns associated with digital signature systems. It explores the evolution of underlying technologies that enhance their effectiveness and resilience in a rapidly changing digital landscape.

8.1. Security Concerns

While digital signatures provide robust security, they are not without vulnerabilities. The foundation of their security lies in the secrecy of private keys. A compromised private key allows attackers to forge signatures, making secure storage solutions like hardware security modules (HSMs) essential. Key revocation and replacement mechanisms, such as Certificate Revocation Lists (CRLs) and the Online Certificate Status Protocol (OCSP), mitigate risks of compromised keys but introduce challenges like latency and complexity, particularly in time-sensitive applications [27].

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 1: 403-412, 2025
DOI: 10.55214/25768484.v9i1.4154

The algorithms underpinning digital signatures can become vulnerable with advancements in cryptanalysis. For example, shorter RSA keys are susceptible to factoring attacks, necessitating continuous evaluation and updates to cryptographic standards. Similarly, vulnerabilities in hash functions, such as collisions where different inputs produce the same hash, can undermine the integrity of digital signatures. The shift from SHA-1 to more secure algorithms like SHA-256 and SHA-3 reflects ongoing efforts to address these risks. Implementation errors, such as weak random number generation, can also weaken digital signature security. Proper testing, adherence to best practices, and secure hardware can mitigate such vulnerabilities. However, side-channel attacks, which exploit information leakage through timing or power consumption, remain a concern. Countermeasures like constant-time algorithms and robust hardware can provide defenses against these risks [28]. Even with secure implementations, phishing and social engineering attacks can target users, tricking them into revealing private keys or signing malicious documents. User education and robust authentication mechanisms are essential to counter these threats.

Trust models like the hierarchical Certificate Authority system, where a root CA anchors trust, introduce unique challenges. A compromise of the root CA affects all certificates issued by it and its intermediaries. Similarly, a malicious or compromised intermediate CA can issue fraudulent certificates, eroding trust across the system. Centralized control in hierarchical models concentrates power, making the system vulnerable to misuse, external pressure, or inefficiencies in certificate revocation, which can delay real-time security updates [29].

8.2. Technological Evolution

Elliptic Curve Cryptography (ECC) has emerged as a powerful alternative to traditional RSA-based systems, offering equivalent security with shorter key lengths. ECC's algorithms, such as the Elliptic Curve Digital Signature Algorithm (ECDSA), provide efficient signature generation and verification, making them suitable for resource-constrained devices like mobile phones and IoT systems. ECC's computational efficiency reduces processing time and resource consumption, replacing traditional hardware-dependent systems like smart cards with more versatile solutions [27]. Quantum computing presents a significant challenge to current cryptographic algorithms, including those used in digital signatures. Algorithms such as RSA and ECC are vulnerable to quantum attacks, prompting the development of quantum-resistant cryptography. Techniques like lattice-based, hash-based, and multivariate polynomial cryptography aim to withstand quantum computational power. Transitioning to quantum-resistant systems involves hybrid solutions that combine traditional and quantum-resistant algorithms, ensuring continuity of security during the transition.

Blockchain technology introduces a decentralized approach to trust management, addressing the limitations of hierarchical CA models. Using a distributed ledger, blockchain eliminates single points of failure, as the compromise of one node does not jeopardize the entire system. Decentralized validation processes, achieved through consensus mechanisms like Proof of Work or Proof of Stake, ensure the authenticity of transactions, including certificate issuance [28]. Blockchain's immutable nature ensures that once a certificate is recorded, it cannot be altered or deleted, providing a transparent and tamper-proof audit trail for all certificate-related transactions. Its resilience against attacks, such as Distributed Denial of Service (DDoS), makes it a robust alternative to centralized systems.

Decentralized Public Key Infrastructure (DPKI) leverages blockchain to register public keys and certificates, enabling automated certificate management through smart contracts. These self-executing contracts reduce human error and enhance transparency, ensuring that certificate issuance, renewal, and revocation adhere to predefined rules. Organizations can anchor their Certificate Authority operations on the blockchain, benefiting from its decentralized structure to bolster the security and trustworthiness of their PKI systems.

9. Future Research

The rapidly evolving landscape of digital signatures presents numerous opportunities for future research to address emerging challenges and enhance this critical technology's security. One promising area is the development and standardization of quantum-resistant cryptographic algorithms,

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 1: 403-412, 2025
DOI: 10.55214/25768484.v9i1.4154

particularly as quantum computing advances. Investigating hybrid models that integrate classical and quantum-resistant techniques will be essential for a secure transition to post-quantum cryptography. Furthermore, expanding the blockchain application in decentralized trust management systems, such as Decentralized Public Key Infrastructure, can offer innovative solutions to the vulnerabilities inherent in hierarchical Certificate Authority models.

Research into lightweight digital signature schemes optimized for resource-constrained environments, such as IoT and mobile devices, is another crucial focus area. Improved algorithmic efficiency, reduced computational requirements, and enhanced energy conservation will enable broader adoption in these domains. Additionally, exploring advanced hardware architectures, such as optimized GPU and FPGA implementations, can significantly improve the performance of quantum-resistant signature schemes.

Further exploration is warranted in integrating machine learning techniques to detect and mitigate potential threats, such as side-channel attacks and phishing attempts targeting digital signature systems. Similarly, addressing the challenge of ensuring secure random number generation and preventing collisions in hash functions remains a high priority. Lastly, harmonizing global regulations and standards to facilitate seamless cross-border recognition and interoperability of digital signatures will play a pivotal role in fostering their universal adoption in commerce, governance, and beyond.

10. Conclusion

Digital signatures have become indispensable for securing digital communications and ensuring electronic documents' authenticity, integrity, and non-repudiation. Advances in cryptographic algorithms, coupled with emerging technologies such as blockchain and quantum computing, have significantly expanded the scope and applicability of digital signatures across industries. Despite these advancements, challenges such as key management, algorithmic vulnerabilities, and evolving cyber threats highlight the need for continuous innovation and research.

Future efforts must prioritize the development of quantum-resistant algorithms, the application of decentralized trust mechanisms, and the optimization of digital signature systems for diverse environments. Additionally, robust regulatory frameworks and global standardization will be critical to ensuring the widespread adoption and legal recognition of digital signatures. By addressing these challenges, digital signatures will continue to provide a secure and trustworthy foundation for digital interactions in an increasingly interconnected world.

References

[1] Y. Fang, "A research on different digital signature schemes," *Applied and Computational Engineering*, vol. 16, no. 1, pp. 27–35, 2023. https://doi.org/10.54254/2755-2721/16/20230855

[2] D. Rana, "Advancements and comparative analysis of digital signature algorithms: A review," *International Journal for Research in Applied Science and Engineering Technology*, vol. 12, no. 5, pp. 5778–5792, 2024. https://doi.org/10.22214/ijraset.2024.62955

[3] R. Khurana and E. Narwal, "Analysis of code-based digital signature schemes," *International Journal of Electrical and Computer Engineering (IJECE), Institute of Advanced Engineering and Science*, vol. 13, no. 5, p. 5534, 2023. https://doi.org/10.11591/ijece.v13i5.pp5534-5541

[4] S. Shen, H. Yang, W. Dai, H. Zhang, Z. Liu, and Y. Zhao, "High-throughput GPU implementation of dilithium post-quantum digital signature," *ArXiv*, 2022. https://doi.org/10.48550/ARXIV.2211.12265

[5] G. Paduanelli, "Quantum-assisted digital signature: A new service for future quantum-integrated optical networks," presented at the International Conference on Transparent Optical Networks (ICTON). IEEE, pp. 1–4, 2024. https://doi.org/10.1109/icton62926.2024.10647247, 2022.

[6] H. Mosanaei-Boorani and S. Bayat-Sarmadi, "A digital signature architecture suitable for V2V applications," IEEE transactions on circuits and systems I: Regular papers," *Institute of Electrical and Electronics Engineers*, vol. 71, no. 2, pp. 731–739, 2024. https://doi.org/10.1109/tcsi.2023.3337121

[7] Q. D. Truong, P. N. Duong, and H. Lee, "Efficient low-latency hardware architecture for module-lattice-based digital signature standard," *IEEE Access, vol. 12. Institute of Electrical and Electronics Engineers*, pp. 32395–32407, 2024. https://doi.org/10.1109/access.2024.3370470

[8] R. K. Lubis, A. Pardede, and H. Khair, "Digital signature security analysis by applying the Elgamal algorithm and the idea method," *Journal of Artificial Intelligence and Engineering Applications*, vol. 3, no. 1, pp. 373-382, 2023. https://doi.org/10.59934/jaiea.v3i1.336

[9] Z. Xu, "The advance of digital signature with quantum computing," *Highlights in Science, Engineering and Technology*, vol. 39, pp. 1111–1121, 2023. https://doi.org/10.54097/hset.v39i.6716

[10] N. T. Thoi, "Research and application of digital signatures in e-commerce today," *Journal of Contemporary Issues in Business and Government*, vol. 27, no. 2, pp. 2276-2282, 2021. https://doi.org/10.47750/cibg.2021.27.02.237

[11] S. B. Gawali, "A comprehensive study on digital signatures," *International Journal of Advanced Research in Science, Communication and Technology*, pp. 37–39, 2023. https://doi.org/10.48175/ijarsct-11608

[12] M. Vidaković and K. Miličević, "Performance and applicability of post-quantum digital signature algorithms in resource-constrained environments," *Algorithms*, vol. 16, no. 11, p. 518, 2023. https://doi.org/10.3390/a16110518

[13] H. Duan, "A research on quantum digital signatures," *Applied and Computational Engineering*, vol. 15, no. 1, pp. 100–109, 2023. https://doi.org/10.54254/2755-2721/15/20230814

[14] A. I. Dzhangarov and M. A. Suleymanova, "Electronic digital signature," presented at the IOP Conference Series: Materials Science and Engineering, vol. 862, no. 5. IOP Publishing, p. 052054, 2020. https://doi.org/10.1088/1757-899x/862/5/052054, 2020.

[15] S. B. Sadkhan and R. S. B. Sadkhan, "Analysis of different types of digital signature," presented at the International Engineering Conference on Sustainable Technology and Development (IEC). IEEE, pp. 241–246, 2022. https://doi.org/10.1109/iec54822.2022.9807502, 2022.

[16] Varsha Agarwal, "Impact of digital evolution on customer relationship strategies in the banking sector," *Evolutionary Studies in Imaginative Culture. Raiya Academic International LLC*, pp. 877–889, 2024. https://doi.org/10.70082/esiculture.vi.1177

[17] D. Upadhyay, N. Gaikwad, M. Zaman, and S. Sampalli, "Investigating the avalanche effect of various cryptographically secure hash functions and hash-based applications," *IEEE Access, Institute of Electrical and Electronics Engineers*, vol. 10, pp. 112472–112486, 2022. https://doi.org/10.1109/access.2022.3215778

[18] P. Gauravaram and L. R. Knudsen, "Cryptographic hash functions," encyclopedia of information assurance," CRC Press. https://doi.org/10.1081/e-eia-120047187, 2010, pp. 1–10.

[19] E. Swathi, G. Vivek, and G. S. Rani, "Role of hash function in cryptography," *NCCSIGMA-16. AI Publications*, pp. 10–13, 2016. https://doi.org/10.22161/ijaers/si.3

[20] D. T. Nguyen, "Constructing digital signature algorithms based on new key schemes," *Journal of Science and Technique*, vol. 9, no. 2, 2021. https://doi.org/10.56651/lqdtu.jst.v9.n02.207.ict

[21] J. Nalayini, C. M., P. V. Imogen, and J. M. Sahana, "A study on digital signature in Blockchain technology," presented at the Third International Conference on Artificial Intelligence and Smart Energy (ICAIS). IEEE, pp. 398–403, 2023. https://doi.org/10.1109/icais56108.2023.10073680, 2023.

[22] I. Aciobăniţei, Ş.-C. Arseni, E. Bureacă, and M. Togan, "A comprehensive and privacy-aware approach for remote qualified electronic signatures," *Electronics*, vol. 13, no. 4, p. 757, 2024.

[23] J. Velentzas, G. Kiriakoulis, G. Broni, N. Kartalis, G. Panou, and G. Fragulis, "Digital and advanced electronic signature: The security function, especially in electronic commerce," *SHS Web of Conferences*,, vol. 139, p. 03011, 2022. https://doi.org/10.1051/shsconf/202213903011

[24] A. Petcu, M. Frunzete, and D. A. Stoichescu, "A practical implementation of a digital document signature system using blockchain," presented at the International Symposium on Advanced Topics in Electrical Engineering (ATEE). IEEE, pp. 1–6, 2023. https://doi.org/10.1109/atee58038.2023.10108308, 2023.

[25] T. Wang, D. Zhao, and J. Qi, "Research on the application of digital signature in university electronic government system," presented at the International Conference on Computer Network, Electronic and Automation (ICCNEA). IEEE, pp. 125–128, 2023. https://doi.org/10.1109/iccnea60107.2023.00035, 2023.

[26] B. Ovelheiro, C. Silveira, and L. Reis, "Sustainability design applied to the digital signature of documents," advances in business strategy and competitive advantage," *IGI Global*, pp. 349–374, 2021. https://doi.org/10.4018/978-1-7998-4099-2.ch016

[27] M. A. Gani, E. Budhiarti Nababan, and A. Candra, "Enhancing digital document security with elliptic curve digital signature algorithm and watermarking techniques," presented at the International Conference on Creative Communication and Innovative Technology (ICCIT). IEEE, pp. 1–7, 2024. https://doi.org/10.1109/iccit62134.2024.10701112, 2024.

[28] R. Verma, N. Dhanda, and V. Nagar, "Analysing the security aspects of IoT using blockchain and cryptographic algorithms," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 11, no. 1s, pp. 13-22, 2023. https://doi.org/10.17762/ijritcc.v11i1s.5990

[29] S. B. Gawali, "A comprehensive study on digital signatures," *Naksh Solutions International Journal of Advanced Research in Science, Communication and Technology*, pp. 37–39, 2023. https://doi.org/10.48175/ijarsct-11608