Journal of Computing and Electronic Information Management
ISSN: 2413-1660 | Vol. 16, No. 3, 2025

Research and Development of Digital Signatures

Hui Meng, Zixin Sang

College of Software, Henan Polytechnic University, Jiaozuo 454000, China.

Abstract: Since Diffie and Hellman's pioneering work on asymmetric cryptography in 1976, digital signature technology has evolved through three phases—theoretical foundation, standardization, and diversified innovation—emerging as a cornerstone of trust in digital societies. Theoretically, foundational frameworks were established by RSA, DSA, and Schnorr algorithms. Standardization efforts, including NIST DSS, ISO/IEC series, and national systems (e.g., China's SM2/SM9, Russia's GOST), fostered a multipolar ecosystem. Extended-attribution technologies (blind, group, and ring signatures) addressed privacy and scenario-specific demands. Current challenges, such as quantum computing threats and privacy-regulation trade-offs, drive advancements in post-quantum cryptography (lattice-based signatures, hash-based XMSS) and privacy-enhancing mechanisms (verifiably encrypted signatures, homomorphic signatures), guided by ISO/IEC redactable standards and NIST's post-quantum initiative. Moving forward, digital signatures will deepen capabilities in provable security, quantum resistance, and adaptive policy control, underpinning trust architectures for emerging ecosystems like Web3 and the metaverse.

Keywords: Digital Signature Technology; Privacy-Enhancing Mechanisms; Standardization Process.

1. Introduction

Traditional authentication methods such as handwritten signatures, seals, and biometric features (e.g., fingerprints) have historically served as fundamental mechanisms for identity verification and document authentication in human societal development. These physical validation techniques operate by establishing traceable individual identifiers, thereby enabling three critical security properties: authenticity (confirming the identity of the document signer), integrity (ensuring the unaltered state of document content), and non-repudiation (preventing the signer from denying their participation in the signing act). With the advancement of digital transformation, digital signature technology has emerged as a seminal achievement in cryptography. Leveraging asymmetric cryptographic mechanisms, it not only inherits the core functionalities of physical signatures but also achieves substantial security augmentation. This innovation addresses inherent vulnerabilities in traditional methods, such as susceptibility to forgery and limited traceability, while maintaining compliance with the tripartite security requirements of authenticity, integrity, and non-repudiation in electronic environments.

The core architecture of digital signature technology is based on the Public Key Infrastructure (PKI), with its technical characteristics manifested in three dimensions: firstly, ensuring the authenticity of the signer's identity through the unique binding mechanism between digital certificates and private keys; secondly, guaranteeing data integrity by generating message digests using cryptographic hash functions combined with digital signature algorithms; thirdly, achieving non-repudiation of signing acts through mathematically irreversible cryptographic principles. Compared to traditional signature methods, digital signatures demonstrate significant technical advantages in implementation: the signature generation phase requires encryption operations using the signer's exclusive private key, while the verification process depends solely on publicly distributed public keys. This asymmetric mechanism effectively addresses technical flaws such as susceptibility to forgery and difficulty in traceability inherent in traditional signatures.

From a technical implementation perspective, a standard digital signature system comprises the following core components: (1) a key generation algorithm that produces mathematically linked public-private key pairs; (2) a signing algorithm that cryptographically binds the private key to a message digest; (3) a verification algorithm that decrypts and validates the signature using the public key. For large-scale data scenarios, the system adopts a preprocessing mechanism—generating fixed-length message digests via collision-resistant hash functions before performing signature operations on the digests—thereby ensuring both computational efficiency and cryptographic security requirements are met while maintaining compliance with the fundamental principles of digital signature protocols.

The security of digital signature mechanisms must satisfy the following fundamental requirements: first, the computational infeasibility of deriving the private key from the public key within polynomial time (i.e., the one-way property of the trapdoor function); second, the inability of unauthorized entities to construct valid message-signature pairs. According to modern cryptographic security models, the mechanism must achieve Existential Unforgeability under Adaptive Chosen-Message Attacks (EUF-CMA) [1], meaning that even after obtaining polynomially bounded message-signature pairs, an adversary cannot forge a valid signature for a new message. The more stringent Strong Existential Unforgeability (SUF-CMA) [2] further requires that an adversary cannot generate a new valid signature for an already signed message, a property critical for defending against replay attacks and signature splitting attacks.

2. Evolution of Digital Signatures

Since Whitfield Diffie and Martin Hellman introduced the concept of digital signatures in their seminal 1976 paper New Directions in Cryptography [3], this technology has undergone over four decades of theoretical breakthroughs and practical evolution. From early feasibility explorations rooted in computational complexity theory, to the formalization of security models and the realization of provably secure constructions, and further to the development of feature-specific technological advancements for diverse application scenarios, digital signature technology has matured from an academic concept into a core security infrastructure underpinning modern digital societies.

Key milestones in its developmental trajectory include: (1) Diffie and Hellman's pioneering proposal of the asymmetric cryptographic framework in 1976, establishing the theoretical foundation for digital signatures [3]; (2) Rivest, Shamir, and Adleman's introduction of the first practical RSA algorithm in 1978 [4], accompanied by Rabin's modular square-based one-time signature scheme the same year [5]; (3) Merkle's 1979 hash chain-based signature algorithm [6], whose Merkle tree structure became a foundational component for blockchain technologies; (4) Elgamal's discrete logarithm-based signature framework [9], Shamir's identity-based cryptography paradigm (IBC) [10], and Goldwasser et al.'s formalization of the EUF-CMA security model [1] in 1984; (5) The Fiat-Shamir transformation enabling systematic conversion of authentication protocols to digital signatures in 1986 [11]; (6) Schnorr's modular signature scheme [12] and the first commercial implementation in Lotus Notes 1.0 [14], both emerging in 1989.

The standardization process accelerated in the 1990s with critical advancements: (7) the 1991 NIST publication of the DSA standard [15] and Zimmermann's release of PGP 1.0 supporting RSA signatures [17]; (8) the 1993 PKCS#1 v1.5 specification standardizing RSA encoding rules [20]; (9) the 1995 integration of signature algorithms into the SSL 2.0 protocol [21]; (10) Bellare and Rogaway's 1996 provably secure RSA-PSS scheme [22], Pointcheval and Stern's formalization of the Forking Lemma for security analysis [23], and Kocher's groundbreaking revelation of side-channel attack vulnerabilities [24]; (11) Gennaro et al.'s 1999 realization of RSA security constructions in the Standard Model [25, 26], marking a paradigm shift in cryptographic proof methodologies.

Since the 21st century, digital signature technology has diversified across multiple directions: (12) The 2001 introduction of the BLS short signature algorithm [27], which significantly improved spatial efficiency through pairing-based cryptography; (13) The successive proposals of identity-based signature (IBS) schemes leveraging bilinear pairings in 2002 [28, 29]; (14) The 2003 Al-Riyami-Paterson certificateless signature framework [30], initiating research into novel paradigms beyond traditional PKI; (15) The 2008 breakthrough by Gentry et al. in achieving provably secure lattice-based signatures [34], laying groundwork for post-quantum cryptography; (16) The 2017 launch of NIST's post-quantum cryptography standardization initiative [37], accelerating the development of quantum-resistant algorithms like XMSS; (17) The 2018 unification of certificateless signature security models by Cheng and Chen [31], resolving critical inconsistencies in prior frameworks.

This evolutionary trajectory reveals two fundamental principles: cryptographic theoretical breakthroughs (e.g., bilinear pairings, lattice theory) persistently catalyze novel signature paradigms, while evolving security threats (e.g., quantum computing, side-channel attacks) continuously drive technological innovation. Currently, digital signature technology exists in a transitional phase of coexistence between classical security models and post-quantum cryptographic frameworks. As quantum-resistant algorithms mature and hybrid systems emerge, its ongoing evolution will persistently reshape the trust architecture of digital societies, balancing legacy compatibility with forward-looking cryptographic resilience.

3. Multifunctional Digital Signatures

With the maturation of generic digital signature technologies, numerous extended-attribution digital signature schemes have emerged to address privacy preservation and fairness requirements in specialized application scenarios such as electronic cash and electronic voting. The following enumerates representative technical paradigms and their core characteristics (this list serves as an illustrative subset; comprehensive analyses may be found in systematic surveys such as [38, 39]):

1) Blind Signatures: Proposed by Chaum in 1982 [40], this mechanism permits signers to generate valid signatures on blinded messages without accessing plaintext content, enabling anonymous authentication critical for electronic voting and digital currency systems.

2) Multi-Signatures & Aggregate Signatures: Introduced by Itakura-Nakamura in 1983 [41], multi-signatures allow multiple signers to collaboratively produce a compact signature, while aggregate signatures [42, 43] enable compression of multiple independent signatures into a single verifiable unit, optimizing blockchain transaction validation.

3) Threshold Signatures: Formalized by Desmedt in 1987 [44], a (k,n)-threshold scheme mandates that any subset of k signers from n participants must collaborate to generate valid signatures, enhancing robustness against insider threats.

4) Undeniable Signatures: Designed by Chaum-van Antwerpen in 1989 [45], this interactive mechanism requires signer participation during verification, preventing third-party misuse of signed data.

5) Fail-Stop Signatures: Conceptualized by Pfitzmann in 1991 [46], this paradigm provides cryptographic evidence to expose forgery attempts, offering enhanced protection against quantum adversaries.

6) Group Signatures: Proposed by Chaum-van Heyst in 1991 [47], this framework enables group members to sign anonymously while permitting authorized tracing via a group manager, balancing privacy and accountability in consortium blockchains.

7) Designated Confirmer Signatures: Introduced by Chaum in 1994 [50], this semi-trusted third-party mechanism delegates signature verification authority to a designated confirmer via verifiable encryption. The scheme preserves signer control while resolving verification deadlocks caused by signer non-cooperation in undeniable signature protocols.

8) Proxy Signatures: Proposed by Mambo et al. in 1996 [51], this delegation model enables secure transfer of signing rights through digital authorization credentials. Proxy signers gain limited signing privileges without accessing the original private key, making it suitable for permission management in distributed systems.

9) Designated Verifier Signatures: Developed by Jakobsson et al. in 1996 [52], this framework binds verification capability to a specific recipient using cryptographic key pairing, ensuring only designated parties can validate signatures. By eliminating third-party verification, it enhances privacy in scenarios like confidential business contracts.

10) Signcryption: Pioneered by Yuliang Zheng in 1997 [53], this cryptographic hybrid integrates encryption and signing

into a single operation, reducing computational overhead by 50-70% compared to traditional "sign-then-encrypt" approaches. Its variants now include identity-based [80] and post-quantum secure [81] implementations, particularly advantageous for IoT and 5G networks.

11) Ring Signatures & Derivatives: Rivest et al.'s 2001 framework [54] enables ad-hoc anonymous signing from arbitrary public key sets (rings) without group administrators. Key variants include: Threshold ring signatures [55] enforcing (k,n) collaborative signing policies; Linkable ring signatures [56] detecting duplicate signer activity while preserving anonymity; Traceable ring signatures [57] balancing auditability through controlled identity revelation; Mesh signatures [58] enabling non-PKI-based group expansion, widely adopted in privacy coins like Monero.

12) Signatures with Efficient Protocols: Camenisch and Lysyanskaya's 2001 paradigm [59] combines secure multi-party computation with zero-knowledge proofs to enable: Blind signature generation with content privacy preservation; Efficient proof-of-signature-possession mechanisms; This breakthrough underpins critical applications like Direct Anonymous Attestation (DAA) [60] in trusted platform modules.

13) Homomorphic Signatures: Johnson et al.'s 2002 innovation [61] allows computations (linear combinations [63], polynomial transforms [64]) on signed data while preserving verifiability. Extended implementations include: Sanitizable signatures [67] for authorized partial modifications; Append-only signatures [68] supporting dynamic data expansion; Blank signatures [69] enabling template-based signing workflows; Protean signatures [70] integrating multi-dimensional revisions; Standardization efforts under ISO/IEC 29167-20 [71] aim to unstrate these for industrial adoption.

14) Verifiably Encrypted Signatures: Boneh et al.'s 2003 construction [72] employs arbitrator-controlled encryption to ensure fair contract execution. Its evolution, commuting signatures, enables encrypted-domain verification, overcoming limitations of separate encryption-signature architectures.

15) Concurrent Signatures: Chen et al.'s 2004 protocol [73] introduces keystone-controlled atomic exchange, ensuring mutual signature binding in e-commerce transactions while preventing post-signing repudiation.

16) Anonymous Signatures: Yang et al.'s 2006 design [74] decouples signer identity from message context, achieving metadata-free verification for anonymous credential systems.

17) Signatures of Knowledge: Chase and Lysyanskaya's 2006 framework [75] embeds zero-knowledge proofs into signatures, enabling implicit assertions (e.g., group membership) without revealing evidence.

18) Structure-Preserving Signatures: Abe et al.'s 2010 scheme [76] constrains cryptographic elements to bilinear groups, enabling modular composition with privacy-preserving protocols like anonymous credentials.

19) Attribute-Based Signatures: Maji et al.'s 2011 model [77] binds signing rights to attribute sets, with policy-based extensions [78] enabling complex logical expressions for cloud access control.

20) Functional Signatures: Boyle et al.'s 2014 framework [79] restricts signing to function outputs f(m), establishing foundational cryptography for verifiable cloud computing and federated learning.

These extended signature technologies share a common characteristic: the innovative integration of cryptographic primitives. This integration enables functional extensions tailored to specific requirements—such as privacy enhancement, access control, and efficiency optimization—while preserving core authentication capabilities. This evolutionary trajectory exemplifies the "demand-driven innovation" principle in cryptography, demonstrating how theoretical advancements respond to real-world challenges. By systematically addressing diverse needs across digital ecosystems, these technologies collectively furnish a versatile toolkit for constructing sophisticated digital trust architectures, balancing foundational security guarantees with adaptive functionality for emerging use cases.

4. Standardization Journey

The standardization process of digital signature technologies has evolved into a multipolar landscape with diversified developments. In the United States, NIST published the Digital Signature Algorithm (DSA) in 1991 and formally established it as the Digital Signature Standard (DSS) through FIPS 186 in 1994 [15]. The elliptic curve variant ECDSA achieved standardization via FIPS 186-2 in 2000, forming a dual-track technical framework combining discrete logarithm and elliptic curve cryptography. The standardization of RSA reflects an evolutionary security philosophy: PKCS#1 v1.5 (1993) adopted the EMSA-PKCS1-v1_5 padding scheme [20], while v2.2 introduced the provably secure RSA-PSS scheme in 2002, later solidified at the protocol layer through RFC 8017 in 2016 [81]. In 2017, the EdDSA algorithm, leveraging Edwards-curve advantages and formal security proofs, was standardized in RFC 8032 [82], ultimately contributing to TLS 1.3 protocol [83] establishing its quadruple algorithm system: RSASSA-PKCS1-v1_5, RSA-PSS, ECDSA, and EDDSA.

The international standardization landscape exhibits a diversified competitive pattern: Russia established an independent cryptographic system through the GOST R 34.10 series standards (1994-2012) [84-86]; regional standards such as South Korea's KCDSA/ECKCDA (1998) [87-89], Germany's EC-GDSA (2005) [90], and China's SM2/SM9 (2012-2016) [91-92] were subsequently formalized. ISO/IEC has constructed a multidimensional standardization framework encompassing five technical dimensions: Message Recovery Mechanisms: ISO/IEC 9796 series standards [93-94] governing digital signatures with message recovery capabilities. Appendix-Type Signatures: ISO/IEC 14888 series standards [95-96], where Part 2 specifies seven integer factorization-based algorithms and Part 3 integrates fourteen discrete logarithm-based schemes. Anonymous Signatures: ISO/IEC 20008 series standards [97] defining group public key-based anonymous signing mechanisms. Blind Signatures: ISO/IEC 18370 series standards [98] standardizing discrete logarithm-based blind signature implementations. Redactable Signatures: ISO/IEC 23264 series standards [71] regulating asymmetric redaction mechanisms for authenticated data.

The ISO/IEC 13888 non-repudiation technical standard system [99-100] establishes a comprehensive assurance framework encompassing source authentication, delivery confirmation, and timestamp validation through dual-track symmetric and asymmetric cryptographic mechanisms. Its technical implementation pathways include a composite verification mechanism based on symmetric cryptography (ISO/IEC 13888-2) and multi-modal non-repudiation protocols leveraging digital signatures (ISO/IEC 13888-3), providing systematic protection against repudiation risks across transactional lifecycle phases.

5. Summary

Digital signature technology has evolved over four decades into a mature ecosystem that integrates theoretical innovation, standardization, and industrial application. This article systematically reviews key technological breakthroughs, characteristic evolutionary trajectories, and standardization processes, revealing its transformation from cryptographic theoretical achievements to a trust cornerstone of digital society. With emerging threats such as quantum computing, digital signature technology will continue advancing while preserving foundational security attributes, deepening developments in provable security, quantum resistance, privacy enhancement, and related directions.

References

[1] Goldwasser S., Micali S., Rivest R. L. “A Paradoxical Solution to the Signature Problem.” In Proc. CRYPTO’84, Berlin, Heidelberg, 1985, pp. 467–477.

[2] An J.H., Dodis Y., Rabin T. On the Security of Joint Signature and Encryption. Advances in Cryptology — EUROCRYPT 2002. Amsterdam, 2002-04-28, p. 83-107.

[3] Diffie W., Hellman M. “New Directions in Cryptography.” IEEE Trans. Inf. Theory, vol. 22, no. 6, pp. 644–654, 1976.

[4] Rivest R., Shamir A., Adleman L. “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.” Commun. ACM, vol. 21, no. 2, pp. 120–126, 1978.

[5] Rabin M. “Digitalized Signatures and Public Key Functions as Intractable as Factorization.” MIT Lab. Comput. Sci. Tech. Rep, 1979, pp. 1–22.

[6] Merkle R. Secrecy, Authentication and Public Key Systems / A Certified Digital Signature (Ph.D. dissertation, Stanford University, America 1979). p. 1-150.

[7] Lamport L. “Constructing Digital Signatures from a One-Way Function.” Tech. Rep. CSL-98, SRI International, Palo Alto, CA, USA, 1979.

[8] Buchmann J., Dahmen E., Hülsing A. XMSS - A Practical Forward Secure Signature Scheme Based on Minimal Security Assumptions. Post Quantum Cryptography. Darmstadt, 2011-11-29, p. 117-129.

[9] ElGamal T. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. Advances in Cryptology. CRYPTO 1984. Berlin, Heidelberg, 1985, p. 10-18.

[10] Shamir A. Identity-Based Cryptosystems and Signature Schemes. Advances in Cryptology. CRYPTO 1984. Berlin, Heidelberg, 1985, p. 47-53.

[11] Fiat A., Shamir A. How To Prove Yourself: Practical Solutions to Identification and Signature Problems. Advances in Cryptology — CRYPTO’ 86. Santa Barbara, 1986-08-11, p. 186-194.

[12] Schnorr C.P. Efficient Identification and Signatures for Smart Cards. Advances in Cryptology — EUROCRYPT ’89. Houthalen, 1989-04-10, p. 239-252.

[13] Bernstein D.J., Duif N., Lange T., Schwabe P., Yang B.-Y. High-Speed High-Security Signatures. Journal of Cryptographic Engineering. 2012, Vol. 2 (No. 2), p. 77-89.

[14] Lotus Domino Wiki. “Supported Key Sizes in Notes/Domino.” [Online]. Available: https://www-10.lotus.com/ldd/dominowiki.nsf/dx/supported-key-sizes-in-notesdomino [Accessed: Sep. 15, 2023].

[15] FIPS PUB 186: Digital Signature Standard (DSS). NIST, America 1994.

[16] Brown D.R.L. The Exact Security of ECDSA. Technical Report CORR 2000-54. University of Waterloo, 2000.

[17] Stallings W., Zimmermann P. PGP Message Exchange Formats. RFC 1991. Internet Engineering Task Force, 1996-08-01.

[18] Girault M. Self-Certified Public Keys. Advances in Cryptology — EUROCRYPT ’91. Brighton, 1991-04-08, p. 490-497.

[19] Poupard G., Stern J. Security Analysis of A Practical "On The Fly" Authentication and Signature Generation. Advances in Cryptology — EUROCRYPT'98. Helsinki, 1998-05-31, p. 422-436.

[20] Kaliski B. PKCS #1: RSA Encryption 1.5. RFC 2313. Internet Engineering Task Force, 1998-03-01.

[21] Information on: https://tools.ietf.org/html/draft-hickman-netscape-ssl-00

[22] Bellare M., Rogaway P. The Exact Security of Digital Signatures-How to Sign with RSA and Rabin. Advances in Cryptology — EUROCRYPT ’96. Zaragoza, 1996-05-12, p. 399-416.

[23] Pointcheval D., Stern J. Security Proofs for Signature Schemes. Advances in Cryptology — EUROCRYPT ’96. Zaragoza, 1996-05-12, p. 387-398.

[24] Kocher P.C. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. Advances in Cryptology — CRYPTO ’96. Santa Barbara, 1996-08-18, p. 104-113.

[25] Gennaro R., Halevi S., Rabin T. Secure Hash and-Sign Signatures Without the Random Oracle. Advances in Cryptology — EUROCRYPT ’99. Prague, 1999-05-02, p. 123-139.

[26] Cramer S., Shoup V. Signature Schemes Based on the Strong RSA Assumption. ACM Transactions on Information and System Security. 2000, Vol. 3 (No. 3), p. 161-185.

[27] Boneh D., Lynn B., Shacham H. Short Signatures from the Weil Pairing. Advances in Cryptology — ASIACRYPT 2001. Gold Coast, 2001-12-09, p. 514-532.

[28] Choon J.C., Hee Cheon J. An Identity-Based Signature from Gap Diffie-Hellman Groups. Public Key Cryptography — PKC 2003. Miami, 2003-01-06, p. 18-30.

[29] Hess F. Efficient Identity Based Signature Schemes Based on Pairings. Selected Areas in Cryptography. St. John's, 2002-08-15, p. 310-324.

[30] Al-Riyami S.S., Paterson K.G. Certificateless Public Key Cryptography. Advances in Cryptology - ASIACRYPT 2003. Taipei, 2003-11-30, p. 452-473.

[31] Cheng Z., Chen L. Certificateless Public Key Signature Schemes from Standard Algorithms. Information Security Practice and Experience. Tokyo, 2018-09-25, p. 45-62.

[32] Goldreich O., Goldwasser S., Halevi S. Public-key cryptosystems from lattice reduction problems. Advances in Cryptology — CRYPTO '97. Santa Barbara, 1997-08-17, p. 112-131.

[33] Hoffstein J., Howgrave-Graham N., Pipher J., Silverman J.H., Whyte W. NTRUSign: Digital Signatures Using the NTRU Lattice. Topics in Cryptology — CT RSA 2003. San Francisco, 2003-04-13, p. 122-140.

[34] Gentry C., Peikert C., Vaikuntanathan V. Trapdoors for Hard Lattices and New Cryptographic Constructions. Proceedings of

the 40th ACM Symposium on Theory of Computing. Victoria, 2008-05-17, p. 197-206.

[35] Ducas L., Durmus A., Lepoint T., Lyubashevsky V. Lattice Signatures and Bimodal Gaussians. Advances in Cryptology – CRYPTO 2013. Santa Barbara, 2013-08-18, p. 117-131.

[36] Ducas L., Kiltz E., Lepoint T., Lyubashevsky V., Schwabe P., Seiler G., Stehlé D. CRYSTALS Dilithium: A Lattice-Based Digital Signature Scheme. IACR Transactions on Cryptographic Hardware and Embedded Systems. 2018, Vol. 2018 (No. 1), p. 238-268.

[37] Information on: https://csrc.nist.gov/projects/post-quantum-cryptography

[38] Menezes A. J., van Oorschot P. C., Vanstone S. A. *Handbook of Applied Cryptography*. Boca Raton, FL, USA: CRC Press, 1996.

[39] D. Demirel, D. Derler, C. Hanser, H. C. Pöhls, D. Slamanig, G. Traverso, “PRISMACLOUD D4.4: Overview of Functional and Malleable Signature Schemes,” PRISMACLOUD Project Deliverable D4.4, H2020 Project 644962, Vienna, Austria: PRISMACLOUD Consortium, 2015. [Online]. Available: https://www.prismacloud.eu/deliverables/ [Accessed: Sep. 15, 2023].

[40] Chaum D. Blind Signatures for Untraceable Payments. Advances in Cryptology. Santa Barbara, 1983-08-22, p. 199-203.

[41] Itakura K., Nakamura K. A Public-Key Cryptosystem Suitable for Digital Multisignatures. NEC Research and Development. 1983, Vol. 71, p. 1-8.

[42] Boneh D., Gentry C., Lynn B., Shacham H. Aggregate and Verifiably Encrypted Signatures from Bilinear Maps. Advances in Cryptology — EUROCRYPT 2003. Warsaw, 2003-05-04, p. 51-65.

[43] Lysyanskaya A., Micali S., Reyzin L., Shacham H. Sequential Aggregate Signatures from Trapdoor Permutations. Advances in Cryptology — EUROCRYPT 2004. Interlaken, 2004-05-02, p. 89-104.

[44] Desmedt Y. Society and Group Oriented Cryptography: A New Concept. Advances in Cryptology— CRYPTO ’87. Santa Barbara, 1987-08-16, p. 120-135.

[45] Chaum D., van Antwerpen H. Undeniable Signatures. Advances in Cryptology — CRYPTO’ 89 Proceedings. Santa Barbara, 1989-08-20, p. 212-227.

[46] Pfitzmann B. Fail-Stop Signatures; Principles and Applications. Proc. COMPSEC'91, 8th World Conference on Computer Security, Audit and Control. London, 1991-09-15, p. 125-134.

[47] Chaum D., van Heyst E. Group Signatures. Advances in Cryptology — EUROCRYPT ’91. Brighton, 1991-04-08, p. 257-265.

[48] Kiayias A., Tsiounis Y., Yung M. Traceable Signatures. Advances in Cryptology - EUROCRYPT 2004. Interlaken, 2004-05-02, p. 189-204.

[49] Kohlweiss M., Miers I. Accountable Metadata Hiding Escrow: A Group Signature Case Study. Proceedings on Privacy Enhancing Technologies. 2015, Vol. 2015 (No. 2), p. 206-221.

[50] Chaum D. Designated confirmer signatures. In: De Santis A. (eds) Advances in Cryptology — EUROCRYPT'94. Perugia, 1994-05-09, p. 86-91.

[51] Mambo M., Usuda K., Okamoto E. Proxy Signatures: Delegation of The Power to Sign Messages. IEICE Transactions on Fundamentals. 1996, Vol. E79-A (No. 9), p. 1338-1354.

[52] Jakobsson M., Sako K., Impagliazzo R. Designated Verifier Proofs and Their Applications. Advances in Cryptology — EUROCRYPT ’96. Zaragoza, 1996-05-12, p. 143-154.

[53] Zheng Y. Digital Signcryption or How to Achieve Cost(Signature & Encryption) << Cost(Signature) +Cost(Encryption). Advances in Cryptology — CRYPTO '97. Santa Barbara, 1997-08-17, p. 165-179.

[54] Rivest R.L., Shamir A., Tauman Y. How to Leak a Secret. Advances in Cryptology — ASIACRYPT 2001. Gold Coast, 2001-12-09, p. 552-565.

[55] Bresson E., Stern J., Szydlo M. Threshold Ring Signatures and Applications to Ad-hoc Groups. Advances in Cryptology — CRYPTO 2002. Santa Barbara, 2002-08-18, p. 465-480.

[56] Liu J.K., Wong D.S. Linkable Ring Signatures: Security Models and New Schemes. Computational Science and Its Applications – ICCSA 2005. Singapore, 2005-05-09, p. 614-623.

[57] Fujisaki E., Suzuki K. Traceable Ring Signature. Public Key Cryptography – PKC 2007. Beijing, 2007-04-16, p. 181-200.

[58] Boyen X. Mesh Signatures. Advances in Cryptology - EUROCRYPT 2007. Barcelona, 2007-05-20, p. 210-227.

[59] Camenisch J., Lysyanskaya A. A Signature Scheme with Efficient Protocols. Security in Communication Networks. Amalfi, 2002-09-11, p. 268-289.

[60] Brickell E., Camenisch J., Chen L. Direct Anonymous Attestation. Proceedings of the 11th ACM Conference on Computer and Communications Security. Washington, D.C., 2004-10-25, p. 132-145.

[61] Johnson R., Molnar D., Song D., Wagner D. Homomorphic Signature Schemes. Topics in Cryptology — CT-RSA 2002. San Francisco, 2002-02-18, p. 244-262.

[62] Steinfeld R., Bull L., Zheng Y. Content Extraction Signatures. Information Security and Cryptology — ICISC 2001. Seoul, 2001-12-06, p. 285-304.

[63] Boneh D., Freeman D., Katz J., Waters B. Signing a Linear Subspace: Signature Schemes for Network Coding. Public Key Cryptography – PKC 2009. Irvine, 2009-03-18, p. 68-87.

[64] Boneh D., Freeman D.M. Homomorphic Signatures for Polynomial Functions. Advances in Cryptology – EUROCRYPT 2011. Tallinn, 2011-05-15, p. 149-168.

[65] Bellare M., Goldreich O., Goldwasser S. Incremental Cryptography: The Case of Hashing and Signing. Advances in Cryptology — CRYPTO ’94. Santa Barbara, 1994-08-21, p. 216-233.

[66] Micali S., Rivest R.L. Transitive Signature Schemes. Topics in Cryptology — CT-RSA 2002. San Francisco, 2002-02-18, p. 236-243.

[67] Ateniese G., Chou D.H., de Medeiros B., Tsudik G. Sanitizable Signatures. Computer Security – ESORICS 2005. Milan, 2005-09-12, p. 159-177.

[68] Kiltz E., Mityagin A., Panjwani S., Raghavan B. Append-Only Signatures. Automata, Languages and Programming. Lisbon, 2005-07-11, p. 506-518.

[69] Derler D., Hanser C., Slamanig D. Blank Digital Signatures: Optimization and Practical Experiences. Privacy and Identity Management for the Future Internet. Vienna, 2014-09-17, p. 45-63.

[70] Krenn S., Pöhls H.C., Samelin K., Slamanig D. Protean Signature Schemes. In: Camenisch J., Papadimitratos P. (eds) Cryptology and Network Security. CANS 2018. Naples, 2018-09-30, p. 189-209.

[71] ISO/IEC 23264-2:2018 IT Security Techniques — Redaction of Authentic Data – Part 2: Redactable Signature Schemes Based on Asymmetric Mechanisms. Working Draft. ISO, Switzerland 2018.

[72] Fuchsbauer G. Commuting Signatures and Verifiable Encryption. Advances in Cryptology – EUROCRYPT 2011. Tallinn, 2011-05-15, p. 234-251.

[73] Chen L., Kudla C., Paterson K.G. Concurrent Signatures. Advances in Cryptology - EUROCRYPT 2004. Interlaken, 2004-05-02, p. 287-305.

[74] Yang G., Wong D.S., Deng X., Wang H. Anonymous Signature Schemes. Public Key Cryptography - PKC 2006. New York, 2006-04-24, p. 347-363.

[75] Chase M., Lysyanskaya A. On Signatures of Knowledge. Advances in Cryptology - CRYPTO 2006. Santa Barbara, 2006-08-20, p. 78-96.

[76] Abe M., Fuchsbauer G., Groth J., Haralambiev K., Ohkubo M. Structure-Preserving Signatures and Commitments to Group Elements. Advances in Cryptology – CRYPTO 2010. Santa Barbara, 2010-08-15, p. 209-236.

[77] Maji H.K., Prabhakaran M., Rosulek M. Attribute-Based Signatures. Topics in Cryptology – CT-RSA 2011. San Francisco, 2011-02-14, p. 376-392.

[78] Bellare M., Fuchsbauer G. Policy-Based Signatures. Public-Key Cryptography – PKC 2014. Buenos Aires, 2014-03-26, p. 520-537.

[79] Boyle E., Goldwasser S., Ivan I. Functional Signatures and Pseudorandom Functions. Public Key Cryptography – PKC 2014. Buenos Aires, 2014-03-26, p. 501-519.

[80] FIPS PUB 186-2: Digital Signature Standard (DSS). NIST, America 2000.

[81] Moriarty K., Kaliski B., Jonsson J., Rusch A. PKCS #1: RSA Cryptography Specifications Version 2.2. RFC 8017. Internet Engineering Task Force, 2016-11-01.

[82] Josefsson S., Liusvaara I. Edwards-Curve Digital Signature Algorithm (EdDSA). RFC 8032. Internet Research Task Force, 2017-01-01.

[83] Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446. Internet Engineering Task Force, 2018-08-01.

[84] GOST R 34.10-94, Information Technology. Cryptographic Data Security. Procedures for Generation and Verification of Electronic Digital Signatures Based on Asymmetric Cryptographic Algorithm. Moscow, Russia: State Standard of the Russian Federation, 1994. (In Russian).

[85] GOST R 34.10-94, Information Technology. Cryptographic Data Security. Procedures for Generation and Verification of Electronic Digital Signatures Based on Asymmetric Cryptographic Algorithm. Moscow, Russia: State Standard of the Russian Federation, 1994. (In Russian).

[86] GOST R 34.10-2001, Information Technology. Cryptographic Data Security. Signature and Verification Processes of Electronic Digital Signatures. Moscow, Russia: State Standard of the Russian Federation, 2001. (In Russian).

[87] [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.99.8398 [Accessed: Sep. 15, 2023].

[88] TTAK.KO-12.0015/R2. Digital Signature Mechanism with Appendix - Part 3: Korean Certificate-based Digital Signature Algorithm using Elliptic Curves EC KCDSA. Korean 2014.

[89] TTAK.KO-12.0001/R3. Digital Signature Mechanism with Appendix - Part 2: Korean Certificate-based Digital Signature Algorithm KCDSA. Korean 2014.

[90] Erwin H., Pascale S. Digital Signature Scheme EC-GDSA. German Federal Office for Information Security, Germany 2005.

[91] GM/T 0003.2-2012, SM2 Elliptic Curve Public Key Cryptographic Algorithm—Part 2: Digital Signature. Beijing, China: State Cryptography Administration, 2012. (In Chinese).

[92] GM/T 0044.2-2016, SM9 Identity-Based Cryptography—Part 2: Digital Signature Algorithm. Beijing, China: State Cryptography Administration of China, 2016. (In Chinese).

[93] ISO/IEC 9796-2:2010 Information Technology — Security Techniques — Digital Signature Schemes Giving Message Recovery — Part 2: Integer Factorization Based Mechanisms. ISO, Switzerland 2010.

[94] ISO/IEC 9796-3:2006 Information Technology — Security Techniques — Digital Signature Schemes Giving Message Recovery — Part 3: Discrete Logarithm Based Mechanisms. ISO, Switzerland 2006.

[95] ISO/IEC 14888-2:2008 Information Technology — Security Techniques — Digital Signatures with Appendix — Part 2: Integer Factorization Based Mechanisms. ISO, Switzerland 2008.

[96] ISO/IEC 14888-3:2018 IT Security Techniques — Digital Signatures with Appendix — Part 3: Discrete Logarithm Based Mechanisms. ISO, Switzerland 2018.

[97] ISO/IEC 20008-2:2013 Information Technology — Security Techniques — Anonymous Digital Signatures — Part 2: Mechanisms Using A Group Public Key. ISO, Switzerland 2013.

[98] ISO/IEC 18370-2:2016 Information Technology — Security Techniques — Blind Digital Signatures — Part 2: Discrete Logarithm Based Mechanisms. ISO, Switzerland 2016.

[99] ISO/IEC 13888-2:2010 Information Technology — Security Techniques — Non-Repudiation — Part 2: Mechanisms Using Symmetric Techniques. ISO, Switzerland 2010.

[100] ISO/IEC 13888-3:2009 Information Technology — Security Techniques — Non-Repudiation — Part 3: Mechanisms Using Asymmetric Techniques. ISO, Switzerland 2009.