REVIEW ARTICLE

Security Vulnerabilities in Proxy Signature Schemes: Cryptanalysis, Design Weaknesses, and Open Challenges

Saddam Hussain[1,*] **and Nayab**[2]

[1] Faculty of Computing, Riphah International University, Islamabad 44000, Pakistan
[2] Department of Information Technology, The University of Haripur, Haripur 22620, Pakistan

Abstract

Proxy signature schemes allow an original signer to delegate signing authority to a proxy signer, supporting flexible authentication in distributed and resource-constrained environments such as cloud computing, blockchain, and Internet of Things (IoT) networks. Although many constructions have been proposed, a large number have later been broken due to flawed design assumptions, weak delegation binding, or the absence of rigorous provable security. This paper surveys proxy signature schemes with a focus on their security weaknesses. It presents a taxonomy of existing constructions by cryptographic primitive, delegation mechanism, and proof framework, and then consolidates known cryptanalytic results, identifying recurring weaknesses such as forgery, proxy misuse, warrant manipulation, insider threats, and ineffective revocation. The paper also identifies schemes that rely on informal or incomplete security arguments rather than formal proofs. Through comparative analysis across the identity-based, certificateless, and certificate-based paradigms, the survey presents recurring design flaws and outlines open challenges and directions toward secure and efficient proxy signatures.

Keywords: proxy signature, cryptanalysis, delegation, provable security, forgery attack, post-quantum cryptography.

1 Introduction

The concept of proxy signature was first introduced by Mambo et al. [1], allowing an original signer to delegate signing authority to a designated proxy signer. In this approach, the proxy signer possesses the appropriate credentials to generate signatures on behalf of the original signer, while the verifier relies on the authorization procedure established during delegation. Proxy signature schemes are generally classified into three types based on the degree of delegation: full delegation, partial delegation, and delegation by warrant [1, 2].

While these schemes provide flexible delegation mechanisms, ensuring their security against various adversarial models remains a critical challenge. Over the years, proxy signature schemes have been constructed under Identity-Based Proxy Signature (IBPS) [3–5], Certificateless Proxy Signature (CLPS) [6, 7], and Certificate-Based Proxy Signature (CBPS) [8, 9]. Despite numerous constructions,

Submitted: 14 June 2026
Revised: 19 August 2026
Accepted: 23 August 2026
Published: 20 September 2026

Vol. 2, **No.** 3, 2026.
10.62762/TISC.2026.211619

***Corresponding author:**
✉Saddam Hussain
saddam.hussain@riphah.edu.pk

Citation
Hussain, S., & Nayab (2026). Security Vulnerabilities in Proxy Signature Schemes: Cryptanalysis, Design Weaknesses, and Open Challenges. *ICCK Transactions on Information Security and Cryptography*, 2(3), 136–158.

cryptanalysis has revealed significant vulnerabilities, including forgery attacks, impersonation attacks, and weaknesses in delegation verification [2, 10].

In IBPS schemes, the public key of each party is derived from its public identity, eliminating the need for certification of public keys [11]. However, IBPS schemes suffer from the key escrow problem, since the Key Generation Center (KGC) generates users' private keys [11]. In addition, many IBPS constructions rely on bilinear pairing operations, which introduce significant computational overhead. To minimize the computational overhead, several pairing-free constructions based on Elliptic Curve Cryptography (ECC) have been proposed; nevertheless, a considerable number of these schemes lack formal security proofs and remain susceptible to forgery attacks. Subsequent cryptanalytic studies further reveal that even improved IBPS schemes frequently fail to resolve these underlying vulnerabilities, as later work demonstrates that such constructions remain insecure or fail to achieve their claimed security properties [2].

CLPS schemes were proposed to eliminate the key escrow problem inherent in identity-based cryptography while avoiding the certificate management overhead associated with traditional public-key infrastructure [12–15]. In this model, the KGC issues only a partial private key, which the user combines with a self-generated secret value to form the complete private key, thereby ensuring that no single party has full knowledge of it.

CBPS schemes combine the advantages of public key infrastructure and identity-based cryptography through the use of implicit certificates, wherein the certifying authority contributes to private key generation without granting it full knowledge of the resulting key, thereby avoiding key escrow while reducing certificate management complexity relative to traditional PKI [10, 16].

Proxy signature schemes have further been extended to a range of application domains, including role delegation systems [17], IoT and healthcare environments [18], and UAV networks [19, 20], underscoring both the practical significance of these schemes and the growing complexity of preserving security, efficiency, and privacy across increasingly diverse deployment environments. This paper, however, focuses specifically on the security vulnerabilities inherent in the classical IBPS, CLPS, and CBPS paradigms.

1.1 Comparison with Existing Surveys

A few surveys and evaluation studies on proxy signatures already exist, making it necessary to clarify how the present review differs from and builds upon them. Das et al. [21] presented an early survey that categorized first-generation proxy signature schemes into constructions based on the Discrete Logarithm Problem (DLP), the Rivest–Shamir–Adleman (RSA) cryptosystem, the Elliptic Curve Digital Signature Algorithm (ECDSA), and bilinear pairings, and reviewed a number of representative constructions under each category. Agarwal et al. [22] later provided a brief tutorial-style survey of DLP-, RSA-, and pairing-based proxy signature models for data sharing.

More recent studies each confine their scope to a single paradigm. Hussain et al. [2] evaluated the computational efficiency of IBPS, ranking schemes by computation time and communication overhead using the EDAS multi-criteria decision-making model. The companion study [23] examined only the security dimensions of IBPS, while [10] evaluated the computational and communication complexity of CBPS exclusively. Existing reviews are therefore either efficiency-oriented or confined to a single paradigm, and none offers a cross-paradigm, cryptanalysis-centric account of why proxy signature schemes continue to fail. The present survey addresses this gap along four dimensions. First, to the best of our knowledge, it is the first survey to examine the three classical paradigms, namely IBPS, CLPS, and CBPS, under a unified security-failure lens. Second, each surveyed scheme is organized around the specific attack that compromised it, including the attacker model, and structural cause. Third, it traces recurring root causes, including weak delegation binding, certificate-confidentiality misuse, inadequate adversarial modeling, and loose security reductions, across all three paradigms. Fourth, it consolidates this evidence in structured summary tables of broken and unproven schemes (Sections 6.5 and 6.4). Table 1 presents a feature-by-feature comparison between this survey and the existing related work.

1.2 Methodology and Literature Selection

To ensure that this review is systematic and reproducible, the surveyed literature was collected according to the following protocol.

Search strategy: We queried IEEE Xplore, ScienceDirect, SpringerLink, the ACM Digital Library, the IACR Cryptology ePrint Archive, and Google Scholar using

Table 1. Comparison of this survey with existing related surveys on proxy signatures.

Survey	Year	IBPS	CLPS	CBPS	Cryptanalysis	Root-cause analysis	Quantitative synthesis	Efficiency analysis
Das et al. [21]	2006	◗	✗	✗	◗	✗	◗	◗
Agarwal et al. [22]	2016	✗	✗	✗	✗	✗	✗	✗
Hussain et al. [2]	2025	✓	✗	✗	✗	✗	✗	✓
Hussain et al. [10]	2025	✗	✗	✓	◗	✗	◗	✓
Hussain et al. [23]	2026	✓	✗	✗	✓	◗	✓	✓
This survey	–	✓	✓	✓	✓	✓	✓	✗

Note: ✓ : covered, ◗ : partially covered, ✗ : not covered.

combinations of the keywords "proxy signature," "identity-based proxy signature," "certificateless proxy signature," "certificate-based proxy signature," "cryptanalysis," "forgery attack," "key replacement attack," and "designated verifier proxy signature," covering the period from 2004 to 2026.

Inclusion criteria: A scheme was included if it belongs to the IBPS, CLPS, or CBPS paradigm and satisfies at least one of the following conditions: (i) a concrete cryptanalytic attack against it has been published, henceforth referred to as *broken*, or (ii) it was published without a formal security proof in either the Random Oracle Model (ROM) or the Standard Model (SM), relying instead on informal arguments or automated verification tools such as AVISPA and BAN logic, henceforth referred to as *unproven*. The latter criterion reflects the fact that the absence of a verifiable security reduction is itself a documented precursor of cryptanalytic failure. Works that mount an attack are reviewed jointly with their corresponding targets.

Exclusion criteria: Schemes that are both formally proven in the ROM or SM and free of any reported attack fall outside the vulnerability focus of this survey and are therefore excluded, except where they arise as repaired constructions accompanying an attack. Variants outside the three classical paradigms, such as threshold, blind, and multi-proxy signatures, were likewise excluded unless required as attack context.

Counting convention: Papers presenting multiple constructions are counted per distinct construction when the constructions differ in security status; for instance, the second scheme of Li et al. [24] and the third scheme of Qiao et al. [25] fall within the scope of this survey, whereas their formally proven counterparts do not. Conversely, families of constructions within a single paper that share both the same status and the same cryptanalysis result are counted once, as in the nine schemes of Lal and Verma [26].

Backward and forward snowballing was applied to the reference lists and citation records of the included papers to minimize the risk of omissions, and to the best of our knowledge, the resulting coverage is exhaustive within the stated criteria. In total, the survey covers 44 schemes with documented security concerns, comprising 22 IBPS, 11 CLPS, and 11 CBPS schemes, of which 24 are broken and 20 are unproven.

1.3 Contributions

Based on the above discussion, the main contributions of this paper are summarized as follows:

- This paper examines proxy signature constructions across three major paradigms, namely IBPS, CLPS, and CBPS, highlighting their design principles and structural differences.
- This work collects and analyzes existing cryptanalysis on IBPS, CLPS, and CBPS.
- The study investigates the root causes of vulnerabilities, such as weak underlying signature primitives, improper delegation verification, and lack of formal security proofs, which lead to repeated failures in proxy signature constructions.
- This survey provides comprehensive coverage of the insecure and unproven proxy signature literature, consolidating 44 schemes in total (22 IBPS, 11 CLPS, and 11 CBPS), each reviewed concisely and classified as either broken or unproven, together with a systematic comparison against existing surveys in the field.
- Based on the analyzed vulnerabilities, this paper outlines the need for robust design methodologies that ensure secure delegation, strong verification mechanisms, and resistance to known attacks in future proxy signature schemes.

The remainder of this paper is organized as follows.

Section 2 presents the necessary preliminaries and background concepts. Section 3 introduces the taxonomy of proxy signature schemes, accompanied by a hierarchical classification diagram. Section 4 provides a concise review of the insecure and unproven literature across the three paradigms. Section 5 provides a comprehensive analysis of security vulnerabilities. Section 6 presents a detailed cryptanalytic survey, including summary tables that compile the known cryptanalytic results. Section 7 discusses comparative observations and recurring design flaws, and Section 8 outlines open research challenges. Finally, Section 9 concludes the paper.

2 Preliminaries and Background

This section presents the fundamental concepts required to understand proxy signature schemes and their associated security vulnerabilities. We first define proxy signatures, then discuss their delegation models, essential security requirements, and underlying mathematical assumptions.

2.1 Definition of Proxy Signature

A proxy signature scheme is a digital signature mechanism that allows an original signer to delegate its signing rights to a designated entity, called a proxy signer, who can generate signatures on behalf of the original signer [1, 27].

Formally, a proxy signature scheme consists of the following processes:

- **Key Generation:** Generates the public and private keys for the original signer and the proxy signer.
- **Delegation:** The original signer produces delegation information to authorize the proxy signer to sign messages on its behalf, often associated with a warrant that specifies the scope of delegation.
- **Proxy Signing:** The proxy signer generates a proxy signature on a message using the delegated authority.
- **Verification:** A verifier checks the validity of the proxy signature to ensure that it was generated under the authorization of the original signer.

2.2 Delegation Types in Proxy Signatures

Proxy signature schemes are distinguished by how much signing power the original signer hands over to the proxy signer. The taxonomy traces back to Mambo et al. [1] and was refined in later constructions [27–29]; it comprises three base mechanisms together with a widely used hybrid.

- **Full Delegation:** the original signer simply hands its own private key to the proxy. The proxy can then emit signatures that are computationally identical to the original signer's, which makes the variant trivial to realize but unsafe in practice, since the original key is exposed and the two parties' signatures can no longer be told apart.
- **Partial Delegation:** instead of sharing its key, the original signer derives a separate proxy signing key from it and passes only that key to the proxy. The original private key therefore stays secret and proxy signatures remain distinguishable, but on its own this mode places no upper bound on how many messages the proxy may sign.
- **Delegation by Warrant:** a signed warrant is attached to the delegation, fixing parameters such as the parties' identities, the validity window, and the admissible set of messages. This yields fine-grained control over what the proxy is permitted to do, at the price of extra verification work to check the warrant.
- **Partial Delegation with Warrant:** the hybrid folds the warrant directly into the derivation of the proxy signing key, so that controlled, scope-limited delegation is obtained without having to verify the original signer's and proxy signer's signatures separately, combining restriction with efficiency.

2.3 Security Requirements of Proxy Signatures

The properties a proxy signature scheme should guarantee were first set out by Mambo et al. and sharpened by subsequent work [1, 30, 31, 33]. A scheme is normally required to meet the following:

- **Unforgeability:** a valid proxy signature can be produced only by the designated proxy signer; no outside party, and not even the original signer, should be able to fabricate one, which is what guarantees the authenticity of delegated signing.
- **Verifiability:** from the proxy signature alone, a verifier should be convinced that the original signer agreed to the message being signed, so that the delegation is publicly and correctly enforced.
- **Identifiability:** the proxy signature must reveal which proxy signer generated it, binding

each signature to a specific party and thereby supporting accountability.

- **Undeniability:** having produced a proxy signature, the proxy signer must not be able to later disown it, ensuring it remains answerable for anything signed under the delegated authority.
- **Distinguishability:** a delegated signature must be separable from a signature the original signer would issue directly, preventing the two from being confused.
- **Prevention of Misuse:** the proxy signing key must be usable only within the delegated scope, and any attempt to exceed that scope should be detectable and attributable to the responsible proxy.

Particular variants impose further requirements on top of these. Proxy blind signatures additionally demand unlinkability, so that a finished signature cannot be tied back to the interaction or message that produced it [31], while anonymous proxy signatures require that the proxy signer's identity stay hidden from ordinary verifiers without breaking the correctness of verification [32].

2.4 Mathematical Background

The construction of proxy signature schemes relies on fundamental cryptographic primitives, including ECC and bilinear pairings [34, 35].

2.4.1 Elliptic Curve Cryptosystem

ECC is defined over a finite field F_p, where an elliptic curve E is given by

$$y^2 \equiv x^3 + ax + b \mod p, \tag{1}$$

where $a, b \in F_p$ and $4a^3 + 27b^2 \neq 0$ ensures that the curve is non-singular [34]. The set of points on E, together with the point at infinity O, forms a cyclic additive group of prime order with a generator. The fundamental operations include point addition, point doubling, and scalar multiplication. The security of ECC-based constructions relies on the hardness of the Elliptic Curve Discrete Logarithm Problem (ECDLP).

2.4.2 Bilinear Pairing

In some proxy signature constructions, bilinear pairings are defined over cyclic groups to enable advanced cryptographic functionalities. A bilinear map is defined as

$$\hat{e} : G_1 \times G_1 \to G_2, \tag{2}$$

where G_1 is an additive cyclic group and G_2 is a multiplicative cyclic group of the same prime order [35]. This mapping satisfies bilinearity, non-degeneracy, and efficient computability. These properties are utilized in pairing-based proxy signature schemes, particularly in identity-based and certificateless settings.

2.4.3 Complexity Assumptions and Proof Models

For completeness, we formally define the computational assumptions and proof models referred to throughout this survey.

- **Discrete Logarithm Problem (DLP):** given a cyclic group G of prime order q with generator g and an element $y = g^x \in G$, compute $x \in \mathbb{Z}_q^*$ [36].
- **Elliptic Curve Discrete Logarithm Problem (ECDLP):** given points $P, Q \in E(F_p)$ with $Q = xP$, compute the integer x. ECDLP is the elliptic-curve analogue of the DLP and underpins all pairing-free ECC-based constructions surveyed here [34, 37].
- **Computational Diffie-Hellman Problem (CDHP):** given (P, aP, bP) for unknown $a, b \in \mathbb{Z}_q^*$, compute abP [36].
- **Bilinear Diffie-Hellman Problem (BDHP):** given (P, aP, bP, cP) for unknown $a, b, c \in \mathbb{Z}_q^*$ and a bilinear map $\hat{e}$, compute $\hat{e}(P, P)^{abc}$ [38].
- **Random Oracle Model (ROM):** an idealized proof model in which every hash function is replaced by a truly random function accessible only through oracle queries; security reductions bound the adversary's advantage in terms of its oracle queries [39].
- **Standard Model (SM):** the proof model that makes no idealized assumptions about hash functions; security is reduced directly to a well-defined computational hardness assumption such as CDHP. SM proofs are regarded as stronger evidence of security, but are typically harder to obtain and often costlier to instantiate [40].

3 Taxonomy of Proxy Signature Schemes

To facilitate a systematic understanding of the proxy signature landscape, this section presents a hierarchical taxonomy of existing constructions. The taxonomy classifies schemes along three principal dimensions: (i) the underlying public key infrastructure paradigm, (ii) the cryptographic

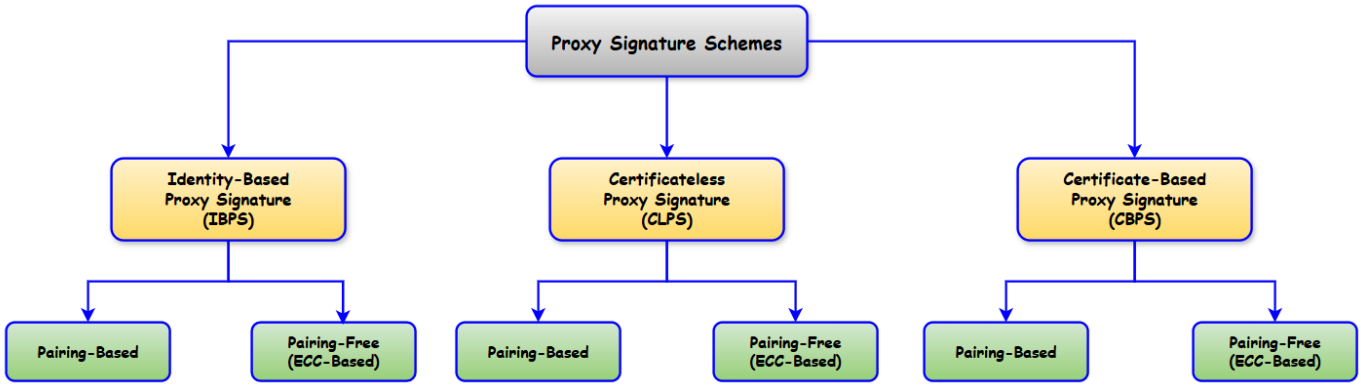

Figure 1. Hierarchical taxonomy of proxy signature schemes across the three major paradigms.

primitive used in the construction, and (iii) the specialized functional variant offered by the scheme. Figure 1 provides a visual representation of this classification. Consistent with the methodology of Section 1.2, this survey covers two categories of schemes: those broken by a published cryptanalytic attack, and those published without a formal proof in the ROM/SM; the former are presented in the attack tables of Section 6.5 and the latter are listed in Table 2 (Section 6.4). Formally proven, unbroken schemes fall outside the scope of this vulnerability survey.

3.1 Classification by Public Key Infrastructure Paradigm

At the highest level, proxy signature schemes are classified into three principal paradigms based on the public key infrastructure they rely upon:

- **IBPS:** In IBPS schemes, the public key of each user is derived directly from a unique identifier such as an email address or a user ID. The corresponding private key is generated by a trusted KGC. This approach eliminates the need for certificate management but introduces the key escrow problem, since the KGC has access to all user private keys.
- **CLPS:** CLPS schemes aim to resolve the key escrow problem of IBPS while avoiding the certificate management overhead of traditional PKI. In these constructions, the KGC provides only a partial private key, while the user generates the remaining secret value. Consequently, no single entity holds the complete private key of the user.
- **CBPS:** CBPS schemes integrate the benefits of identity-based and traditional public key cryptography through the use of implicit certificates. The CA issues a certificate that simultaneously serves as part of the user's private key, thereby eliminating the certificate revocation problem and the key escrow issue.

3.2 Classification by Cryptographic Primitive

Within each paradigm, proxy signature schemes can be further classified according to the underlying cryptographic primitive used for their construction:

- **Pairing-Based Constructions:** A large body of proxy signature schemes rely on bilinear pairings defined over elliptic curve groups. While bilinear pairings enable elegant constructions and facilitate identity-based functionality, they incur significant computational overhead.
- **Pairing-Free Constructions:** To address the inefficiency of pairing operations, several schemes have been proposed using ECC without bilinear pairings. These constructions typically rely on the hardness of the ECDLP and are more suitable for resource-constrained environments.

Beyond the primitive used, schemes are also distinguished by the functional variant they realize (e.g., standard, message-recovery, designated-verifier, blind, and anonymous proxy signatures); Figure 2 summarizes these variants together with their defining characteristics.

3.3 Classification by Security Proof Framework

Finally, proxy signature schemes can be classified based on the formal model used for their security proofs, as illustrated in Figure 3:

- **ROM:** Most existing schemes provide security proofs under the ROM, where hash functions are modeled as ideal random oracles. While convenient, ROM-based proofs may not translate directly to concrete instantiations.

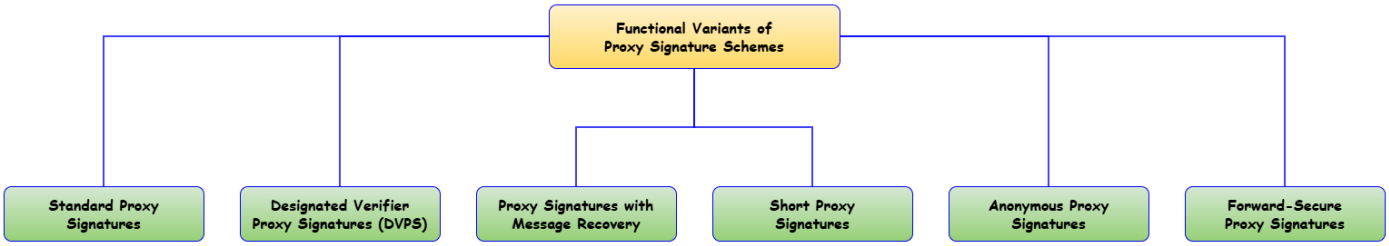

Figure 2. Classification of proxy signature schemes by functional variants, with the defining characteristic of each variant.

- **SM:** A smaller subset of schemes provide security proofs in the SM, relying solely on standard cryptographic assumptions without idealized oracles.
- **Informal Security Arguments:** A significant portion of proposed schemes provide only informal security arguments, which has historically led to many of the cryptanalytic failures reviewed in this paper.

The taxonomy presented in this section serves as a roadmap for the detailed vulnerability analysis that follows. The classification by paradigm directly structures the cryptanalytic survey, while the classification by primitive, functional variant, and proof framework provides the analytical lens through which recurring design weaknesses are identified.

4 Literature Review of Proxy Signature Schemes

This section reviews the 44 schemes covered by this survey, presented concisely and in chronological order within each functional group, in accordance with the methodology described in Section 1.2. These comprise proxy signature constructions that were either broken by a published cryptanalytic attack or published without a formal security proof in the ROM/SM. Each entry specifies the construction's underlying primitive, its claimed security basis, and its resulting status, while detailed analyses of the corresponding attacks are deferred to Section 6. The broken schemes are presented in Tables 3–5, and the unproven schemes are listed in Table 2. Formally proven constructions that remain unbroken fall outside the scope of this survey and are discussed only where they arise as repaired schemes accompanying a reported attack.

4.1 Identity-Based Proxy Signature Literature

Zhang and Kim [41] proposed an early pairing-based IBPS scheme, which presupposes a secure key-distribution channel, offers no revocation, and collapses once a private key is exposed [42]. Cao and Cao [43] proposed the first direct SM construction under CDHP, subsequently broken by a delegator forgery [44]. Similarly, Gu et al. [45] strengthened the SM security model with self-proxy signing and proxy-key oracle access under CDHP, but the scheme fell to a delegator key-extraction forgery [46], whose authors supplied a repaired SM construction. James and Thumbur [47] proposed a pairing-free ECC construction supported only by informal arguments. Hu et al. [48] constructed an SM scheme under CDHP whose reduction was later shown to be loose and which does not withstand the delegator attack [49]. Sarde and Banerjee [50] proposed a pairing-based scheme under CDHP with informal analysis. Mukherjee et al. [42] added knapsack-based key distribution and private-key revocation to Zhang and Kim's design, again without a formal proof. Hu et al. [51] described a generic transformation from identity-based signatures to IBPS but supplied no reductionist proof. Recently, Bannore et al. [17] combined role-based access control with a forward-secure ECC proxy signature, validated only via BAN logic and AVISPA.

Okamoto et al. [52] initiated short IBPS from pairings on the Extended K-Plus problem. However, the secret key is recoverable from any two signatures [53]. Zhang and Yu [54] proposed a short SM scheme under CDHP, later shown to admit insider and outsider forgeries and proxy-key recovery from three signatures [55].

Lal and Verma [26] proposed nine Identity-Based Strong Designated-Verifier Proxy Signature (IBSDVPS) schemes with informal analysis using bilinear pairing. However, all of the proposed schemes fail the strong designated-verifier property [56]. Later, Zhang and Mao [57] proved an SDVPS under the BDHP in the ROM. However, the scheme still fails the same property [56]. Yang [58] removed the trusted-PKG requirement, but their design lets the agent derive the original signer's private key, prompting the revision of Wang [59], which in turn permits a colluding PKG and original signer to tamper with the warrant

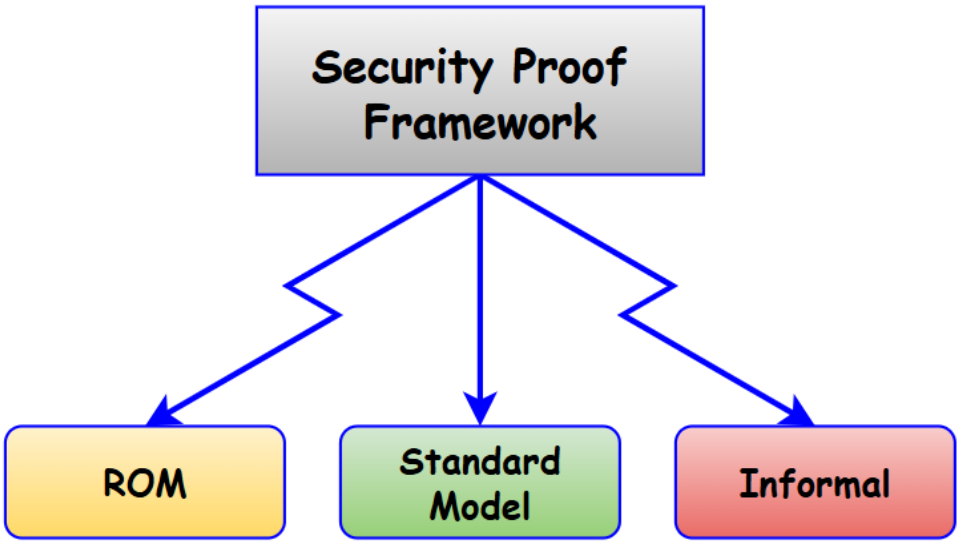

Figure 3. Classification by security proof framework.

[60]. Kang et al. [56] offered two improved DVS/proxy constructions without formal or informal proof. Lee et al. [61] removed trust in the PKG, and Wei [62] proposed a pairing-free DLP-based variant; neither substantiates its claims with a ROM/SM proof. Likewise, Sarde and Banerjee [63] proposed a pairing-based SDVPS under CDHP with informal analysis. Sha [60] improved Wang's design against the PKG-signer collusion, again without a formal proof.

Singh and Verma [64] reduced bandwidth by embedding the message in the signature, with a ROM proof under CDHP. However, the proposed scheme was broken twice by [65, 66], and Zhou [66] accompanied the second attack with a repaired construction. Yoon et al.[67] attempted a lower-bandwidth repair without a formal proof, but the claimed recovery property does not hold [68]. Later, Asaar et al.[68] supplied a corrected, proven scheme alongside their refutation.

4.2 Certificateless Proxy Signature Literature

Li et al. [69] initiated the CLPS primitive from pairings with an informal argument. However, a concrete forgery was found by Lu et al. [70]. However, Lu et al. [70] did not provide a formal security proof for their proposed countermeasure. Eslami and Pakniat [71] presented the first SM construction, which fell to key-replacement and malicious-KGC attacks [15]. Unfortunately, the Square-CDH replacement of Lu and Li [15] was itself broken by a public-key-replacement attack [72]. Recently, Ullah et al. [73] and Ullah et al. [74] proposed hyperelliptic-curve constructions for the Industrial IoT, the latter with a zero-knowledge identity-privacy layer. However, both schemes are validated only with AVISPA and informal analysis.

Yu et al. [75] proposed an anonymous proxy signature proven in the ROM under the DLP and CDHP. However, the scheme was later shown not to offer the claimed anonymity property [76]. Chou's improved construction [76] restores anonymity with revocation but still provides no formal proof.

Padhye and Tiwari [77] proved a pairing-free message-recovery scheme in the ROM under the ECDLP, which was subsequently broken by a Type-I adversary [78].

He et al. [20] introduced the first certificateless designated-verifier proxy signature for UAV networks with a ROM proof. Unfortunately, the proposed scheme was later shown vulnerable to user impersonation by Xu et al. [79], who accompanied their attack with a secured replacement for UAV delivery in smart cities.

Yang et al. [80] targeted the malicious-but-passive KGC threat with an SM proof under the DLP, CDHP, and the collision-resistant hash problem (CRHP), but the scheme was broken and fails to resist precisely that attack [81].

4.3 Certificate-Based Proxy Signature Literature

Kang et al. [82] proposed the certificate-based signature from which the paradigm grew. However, the proposed scheme was found vulnerable to key-replacement attacks [24]. Later, Li et al. [24] presented the first formal CBPS treatment with two

constructions: the first carries a ROM proof under the CDHP and falls outside the scope of this survey, while the second is presented without any proof. Chen and Huang [83] proposed a pairing-based scheme supported only by an informal argument. Liang et al. [84] introduced a certificate-based strong designated-verifier proxy signature from pairings with a claimed ROM/CDHP analysis, though no verifiable formal proof accompanies the construction. Huang et al. [85] studied the relationship between warrant-based proxy signatures and certificate-based signatures and described a generic transformation, again without a formal proof. Mahmoodi et al. [86] proposed the first CBPS with message recovery over the ECDLP with a ROM proof, but the construction is incorrect because its delegation depends on the confidential original-signer certificate [25]. Verma and Thakur [87] proposed a pairing-based CBPS whose algorithm is incompletely specified and unproven. Verma and Singh [88] presented a short pairing-based scheme proven in the ROM under CDH and BDH, and Verma et al. [19] the first certificate-based designated-verifier short proxy signature for UAV networks under the BDHP and CDHP; both are invalidated by the same certificate-confidentiality flaw [25]. Verma et al. [16] proposed a pairing-free IIoT scheme with a ROM proof that was broken three times [25, 89, 90]. Qiao et al. [25] repaired the IIoT line with three constructions: the first two are formally proven and fall outside the scope of this survey, whereas the third, publicly verifiable variant is given without a formal proof or performance analysis.

5 Vulnerability Analysis of Proxy Signature Schemes

Although proxy signature design has advanced considerably, a substantial number of proposed constructions have subsequently been found insecure. This survey documents 44 such schemes: 24 broken by concrete published attacks and 20 published without any formal security proof. The recurring causes are structural in nature: delegation parameters that are not firmly bound to the proxy key, security reductions that are loose or entirely absent, threat models that omit realistic adversarial capabilities, and warrant data left unprotected. This section organizes the reported and analytically identified weaknesses by attack class, and links each class to representative broken schemes that are analyzed in detail in Section 6.

5.1 Forgery Attacks

Forgery is the most damaging failure for a proxy signature scheme, since it lets an adversary issue valid signatures without holding genuine delegated authority. It typically becomes possible through key-substitution or public-key-replacement weaknesses, or through delegation data that is not properly authenticated. Constructions that do not firmly tie the proxy signer's identity to the delegation parameters are especially exposed to rogue-proxy forgeries. Representative instances include the total break of the short IBPS of Okamoto et al. [52], whose secret key is recoverable from any two message-signature pairs [53]; the single-observation forgery against the message-recovery scheme of Singh and Verma [64] demonstrated by Zhou [66]; and the malicious-proxy forgery against the IIoT-oriented CBPS of Verma et al. [16] shown by Zhu et al. [89] (Section 6).

5.2 Warrant Manipulation Attacks

Warrant-based delegation depends on the integrity of the warrant to bound the proxy's authority. When the warrant is not cryptographically protected or is not bound into signature generation, an adversary can alter its contents, for example widening the validity period or the set of permitted messages, and thereby extend the delegated rights beyond what was intended. A concrete example is the trusted-PKG-free SDVPS of Wang [59], in which a colluding PKG and original signer can tamper with the warrant, as demonstrated by Sha [60] (Section 6).

5.3 Proxy Misuse Attacks

Proxy misuse arises when an otherwise legitimate proxy signs outside the scope it was granted. The root cause is usually a verification procedure that never explicitly checks the delegation conditions, which lets the proxy exploit loosely specified warrants or verification steps to sign messages it was never authorized to sign. The delegation-reuse attack of Qiao et al. [25] against the CBPS of Verma et al. [16], in which a Type-II adversary derives a valid delegation for an arbitrary new warrant from a single known delegation and reuses delegations undetectably, is a paradigmatic example.

5.4 Revocation Weaknesses

The capacity to withdraw delegated authority is essential in dynamic deployments, yet many schemes either omit revocation entirely or implement it through costly system-wide key updates. Either way, a proxy

may continue to produce accepted signatures after its authority was meant to lapse. Mukherjee et al. [42] showed, for instance, that the early ID-based scheme of Zhang and Kim [41] offers no revocation and collapses entirely once a participant's private key is exposed.

5.5 Insider Attacks

Insider threats occur when the original signer or the proxy signer departs from the protocol, for instance an original signer trying to forge proxy signatures after delegating, or a proxy signer trying to recover the original signer's private key from the delegation data. Schemes that do not enforce a clean separation between the two signing roles are the most susceptible. The delegator forgeries against Cao and Cao [43] by Sun et al. [44] and against Gu et al. [45] by Hu et al. [46], as well as the insider forgery and proxy-key recovery against Zhang and Yu [54] by Yuan [55], exemplify this class.

5.6 Lack of Rigorous Security Proofs

Many schemes are published with only informal security arguments, or with reductions that fail to capture realistic adversarial power. Heuristic reasoning readily overlooks subtle attack paths, and even a formal proof offers no protection if it rests on an incorrect assumption or a flawed reduction, which is why so many such constructions are broken after the fact. Sections 4 and 6 identify twenty such schemes across the three paradigms, including the CBPS of Verma and Thakur [87] and several identity-based designated-verifier constructions [61–63], whose claimed guarantees rest entirely on informal or tool-based reasoning.

Taken together, these weaknesses point to a common conclusion: robust, provable security frameworks, rather than ad hoc arguments, are needed for future proxy signature design.

6 Cryptanalytic Survey

This section surveys, paradigm by paradigm, the proxy signature constructions for which a concrete attack has been reported in the literature. Unlike efficiency-oriented reviews, each entry is presented from the perspective of its security failure. The scheme and its claimed guarantee are stated briefly, followed by the work that broke it, the class of attack used, and where possible the structural cause of the failure and whether a repaired construction was offered. Constructions published without any formal proof in the ROM or SM are also included. The absence of a verifiable security argument is itself a recognized weakness that has often preceded cryptanalytic failure, so such schemes belong in a survey of security shortcomings. Schemes that are both formally proven and free of any reported attack fall outside the scope of this survey and are mentioned only when they appear as repaired constructions accompanying an attack. The unproven schemes among the 44 covered by this survey are also listed in Section 6.4.

6.1 Identity-Based Proxy Signature

Cao and Cao [43] gave, in 2010, the first direct identity-based proxy signature (IDBPS) proven existentially unforgeable in the SM under the CDH assumption against adaptive chosen-message and chosen-identity attacks. Three years later, Sun et al. [44] showed the guarantee to be unattainable: a malicious delegator can exploit a gap in the security model to forge, and the construction is moreover computationally heavy.

The framework of Gu et al. [45] strengthened the IDBPS model by admitting self-proxy signing and granting the adversary access to arbitrary proxy-signing keys, with an SM proof under CDHP. Hu et al. [46] subsequently demonstrated that a malicious delegator who obtains a single proxy-signing key for one warrant can produce a valid signature on an arbitrary message-warrant pair, without ever holding the proxy signer's key; this directly violates unforgeability. The authors supplied a repaired CDH-based SM construction.

Hu et al. [48] later proposed an SM scheme built on the short-signature technique of Kang et al. [91]. Its weakness is twofold and was noted by Hu et al. [49]: the reduction is loose, so the adversary's advantage is not tightly bound to the underlying hard problem, and the scheme remains exposed to the delegator attack, in addition to relying on a large parameter set and costly pairings.

An early pairing-based ID-based proxy scheme of Zhang and Kim [41] was revisited by Mukherjee et al. [42], who observed that it presupposes a secure channel for key distribution, offers no revocation, and collapses once a participant's private key is exposed, while permitting universal verification. Their improved pairing-based scheme adds knapsack-based key distribution and private-key revocation.

In the short-signature setting, Okamoto et al. [52] proposed the first short IDBPS from pairings, founded on the Extended K-Plus problem. Zhang and

Chen [53] broke it completely by recovering the signer's secret key from any two message-signature pairs, which enables forgery on arbitrary messages.

Zhang and Yu [54] presented a short proxy signature in the SM under CDHP, claimed secure against Type-I to Type-III adversaries. Yuan [55] refuted strong unforgeability with both insider and outsider forgeries, and further showed that the proxy signer's signing key can be reconstructed from three observed signatures.

For message recovery, Singh and Verma [64] proposed a low-bandwidth IDBPS proven unforgeable under CDH. The scheme was broken twice: Tian et al. [65] exhibited two forgery attacks, and Zhou [66] showed that observing a single valid signature suffices to forge on any message, while also identifying a flaw in the proof. Yoon et al. [67] attempted to repair Singh-Verma with a lower-bandwidth message-recovery variant, but Asaar et al. [68] proved that the promised message-recovery property does not actually hold, so the construction is not short as claimed; they in turn gave a corrected short scheme.

Among identity-based designated-verifier proxy signatures, both the SDVPS of Zhang and Mao [57], proven under BDHP in the ROM, and the nine schemes of Lal and Verma [26] were shown by Kang et al. [56] to fail the strong designated-verifier requirement: any party that intercepts a single signature can thereafter verify subsequent ones, defeating the intended non-transferability. The chain of trusted-PKG-free SDVPS constructions collapsed twice in succession: the original design of Yang [58] was undermined by Wang [59], who showed that an authorized agent can derive the original signer's private key and thereby forge on its behalf, and the revised scheme of Wang was in turn found by Sha [60] to permit a colluding PKG and original signer to tamper with the warrant; Sha provided a construction resilient to this collusion, which is, however, itself supported only by informal analysis without a proof in the ROM or SM.

A further group of IDBPS schemes is of concern not because an attack has been published, but because their security was never formally established. In the foundational flavor, James and Thumbur [47] constructed a pairing-free IDBPS over ECC offering the customary set of security properties, Hu et al. [51] gave a generic standard-model transformation that turns a secure identity-based signature into an IDBPS, and Bannore et al. [17] proposed a forward-secure, role-based proxy signature over ECC validated with BAN logic and AVISPA. To these must be added the pairing-based construction of Sarde and Banerjee [50], which claims the full set of proxy security properties under the CDHP, and the improved scheme that Mukherjee et al. [42] attached to their attack on [41], featuring knapsack-based key distribution and private-key revocation. In each case the claimed guarantees rest on informal or tool-based reasoning, with no reductionist proof in the ROM or SM.

The same gap recurs among identity-based designated-verifier proxy signatures. Lee et al. [61] proposed a trusted-party-free IDB-DVS, Wei [62] a pairing-free variant founded on the discrete logarithm problem, and Sarde and Banerjee [63] a bilinear-pairing IDB-SDVPS, each claiming the full set of designated-verifier properties. Likewise, the two improved designated-verifier constructions that Kang et al. [56] offered alongside their attacks are presented without any formal or even informal proof. None of these works supplies a formal proof in the ROM or SM to substantiate their claims, so their security remains unverified.

6.2 Certificateless Proxy Signature

The first CLPS, proposed by Li et al. [69] from bilinear pairings with a pairing-free signing step, was claimed unforgeable under the pairing-inversion and CDH problems. Lu et al. [70] broke it with a forgery that transforms one valid proxy signature into another that appears to have been authorized for the adversary; they proposed a countermeasure, though neither work provided a formal proof.

Eslami and Pakniat [71] introduced the first SM CLPS. Lu and Li [15] refuted its unforgeability with two concrete attacks, one based on public-key replacement and one on a malicious KGC, and replaced it with a Square-CDH construction in the SM. That replacement was itself later cryptanalyzed: Zhou et al. [72] showed it succumbs to a public-key-replacement attack in which a malicious original or proxy signer forges a valid signature, and they offered no repair.

Yang et al. [80] targeted the stronger malicious-but-passive KGC (MbpKGC) threat, presenting an SM CLPS reduced to the DLP, CDHP, and CRHP and claimed secure against both public-key-replacement and MbpKGC attacks. Lin et al. [81] demonstrated that an adversary can nonetheless forge signatures, so the scheme does not in fact resist the MbpKGC attack; no corrected scheme was given.

The message-recovery CLPS of Padhye and Tiwari [77], built over ECDLP and proven in the ROM against Type-I and Type-II adversaries, was shown by Shi et al. [78] to be insecure against a concrete Type-I attack, rendering it unsuitable for deployment. In the designated-verifier setting, the UAV-oriented CLDVS of He et al. [20] was found by Xu et al. [79] to be unable to withstand a user-impersonation attack, prompting a secured replacement for smart-city UAV delivery. Finally, the anonymous CLPS of Yu et al. [75] was shown by Chou [76] to fall short of the anonymity it claimed, and Chou supplied an improved anonymous construction. Chou's replacement, however, is itself accompanied only by an informal security argument, with no formal proof in the ROM or SM, so its claimed properties likewise remain unverified. The same verification gap affects the recent hyperelliptic-curve constructions of Ullah et al. for the Industrial IoT, namely the single-layer scheme of [73] and its multilayer successor with an identity-privacy sub-protocol [74], both of which are validated only with the AVISPA tool and informal reasoning rather than a reductionist proof in the ROM or SM.

6.3 Certificate-Based Proxy Signature

The certificate-based signature of Kang et al. [82] was shown by Li et al. [24] to be vulnerable to key-replacement attacks; the same work then gave the first formal CBPS construction, although the second of its two schemes was presented without a proof.

The pairing-free IIoT-oriented CBPS of Verma et al. [16] attracted three independent cryptanalyses. Zhu et al. [89] showed that it fails unforgeability under a weak Type-II adversary acting as a malicious proxy signer; Qiao et al. [25] showed that a Type-II adversary can derive a valid delegation for any new warrant from a single known delegation and can reuse delegations undetectably; and Park and Kim [90] traced the underlying cause to a weak ordinary signature primitive, demonstrating that the same forgery carries over even to the improved scheme.

Mahmoodi et al. [86] proposed the first CBPS providing message recovery, built over the ECDLP and proven in the ROM against existential forgery under chosen-message and identity attacks. Qiao et al. [25] subsequently identified a design flaw: the delegation is bound to a hash value derived together with the original signer's certificate, yet the proxy signer never holds that certificate and therefore cannot recompute the hash required to validate the delegation. Because verification cannot be completed, Qiao et al. conclude that the construction is incorrect.

Verma and Singh [88] presented a short CBPS from pairings that removes the key-escrow problem of identity-based cryptography, resists key-replacement attacks, dispenses with a secure channel, and is proven in the ROM under the CDH and BDH assumptions. Qiao et al. [25] showed that it suffers from the same structural defect, since its delegation likewise relies on a certificate-derived hash that the proxy signer is unable to compute without the confidential original-signer certificate, which again renders the scheme incorrect.

Verma et al. [19] introduced the first certificate-based designated-verifier short proxy signature, targeted at UAV networks and proven in the ROM under the BDHP and CDHP, while claiming source authentication, message integrity, misuse prevention, and resistance to modification, replay, impersonation, and man-in-the-middle attacks. Qiao et al. [25] once more demonstrated that the delegation depends on a hash computed from the secret original-signer certificate, which the proxy signer cannot access; the resulting inability to verify the delegation makes this construction incorrect as well. The recurrence of the identical root cause across [19, 86, 88] indicates a systematic design flaw in certificate-based delegation rather than three isolated errors.

A separate certificate-based construction whose security is unverified is that of Verma and Thakur [87], a CBPS from bilinear pairings claiming strong unforgeability, identifiability, repudiability, verifiability, and prevention of misuse. The scheme provides neither a formal analysis in the ROM or SM nor a complete description of its algorithm, leaving its asserted guarantees without any verifiable basis. The same shortcoming affects several further certificate-based works: the pairing-based scheme of Chen and Huang [83] and the generic transformation from certificate-based signatures to proxy signatures of Huang et al. [85] are supported only by informal arguments; the certificate-based strong designated-verifier construction of Liang et al. [84] claims a ROM analysis under the CDHP but supplies no verifiable formal proof; and the third, publicly verifiable construction of Qiao et al. [25] is presented without either a formal proof or a performance analysis, in contrast to that paper's first two schemes.

6.4 Overview of Schemes Lacking Formal Security Proofs

While the preceding subsections analyzed the schemes that were explicitly broken, the second category of surveyed schemes consists of constructions whose security was never formally established. Table 2 lists the 20 such schemes: 10 IBPS, 4 CLPS, and 6 CBPS constructions. For each entry, the table gives the functional variant, the underlying primitive, and the kind of security analysis actually provided by the authors: informal reasoning, automated tools such as AVISPA or BAN logic, or, in some cases, no analysis at all. The historical record consolidated in this survey shows why this category matters: several of the broken schemes of Tables 3–5 were likewise published with only heuristic arguments before their weaknesses were exposed, so the entries below should be regarded as unverified rather than secure.

6.5 Cryptanalytic Results

To provide a comprehensive overview of the security failures discussed in the preceding subsections, Tables 3–5 summarize the proxy signature schemes that have been cryptanalyzed in the literature. For each scheme, the tables report the type of vulnerability identified, the work that uncovered the attack, and a brief description of the attack mechanism. This overview enables readers to quickly identify recurring patterns of failure across years and paradigms.

Tables 3–5 reveal several important patterns. First, cryptanalytic results span all three paradigms, indicating that no paradigm is inherently immune to design failures. Second, several schemes have been attacked multiple times by different researchers using distinct attack vectors, suggesting fundamental structural flaws rather than isolated weaknesses. Third, a significant cluster of CBPS schemes share the same root cause, namely the improper use of confidential certificate information in delegation construction, as highlighted by Qiao et al. [25]. Fourth, the consistent recurrence of forgery and key recovery attacks emphasizes the necessity of stronger formal security models in future proxy signature designs.

7 Comparative Analysis and Discussion

This section presents the findings of the vulnerability analysis presented in the previous sections and provides a comparative discussion across the three major proxy signature paradigms, IBPS, CLPS, and CBPS. The objective is to identify recurring weaknesses, structural design flaws, and the underlying causes that lead to repeated cryptanalytic failures across these constructions.

7.1 Recurring Design Flaws

A careful examination of the reviewed schemes reveals several recurring design flaws that compromise the security of proxy signature constructions. These include:

- **Weak Delegation Binding:** A significant number of schemes fail to cryptographically bind the warrant, the proxy signer's identity, and the proxy signing key. This weakness has been exploited in several IBPS schemes [44, 46], allowing a malicious delegator to forge signatures after obtaining a proxy signing key for a specific warrant.
- **Reliance on Weak Underlying Primitives:** Several CBPS schemes inherit vulnerabilities from their underlying ordinary signature primitives. For instance, Park and Kim [90] demonstrated that the root cause of the forgery attack against Verma et al. [16] lies in the weakness of the base signature scheme, which propagates to the proxy signature construction.
- **Improper Use of Certificate Information:** In CBPS constructions such as [19, 86, 88], hash values computed from the original signer's certificate are incorporated into the delegation, despite the certificate being confidential. As highlighted by Qiao et al.[25], this creates a fundamental design flaw that makes verification impossible for the proxy signer.
- **Susceptibility to Public Key Replacement Attacks:** In the certificateless setting, schemes such as those of Eslami and Pakniat [71] and Lu and Li [15] have been shown vulnerable to public key replacement attacks, where a malicious original signer or proxy signer can substitute keys to forge valid signatures.
- **Inadequate Modeling of Malicious KGC:** A few CLPS schemes underestimate the capabilities of a malicious-but-passive KGC, leading to forgery attacks as demonstrated by Lin et al. [81] against the scheme of Yang et al. [80].

7.2 Design-Principle Analysis

The record of attacks in Section 6 is not a collection of

Table 2. Overview of the proxy signature schemes published without a formal proof in the ROM or SM.

Scheme	Year	Paradigm	Variant	Primitive	Security analysis provided
Kang et al. [56] (2 schemes)	2009	IBPS	DVS / DVPS	Pairing	None (formal or informal)
Lee et al. [61]	2010	IBPS	DVPS (trusted-party-free)	Pairing	Informal analysis
Wei [62]	2013	IBPS	DVPS	Pairing-free (DLP)	Informal analysis
James and Thumbur [47]	2014	IBPS	Standard	Pairing-free (ECC)	Informal analysis
Sarde and Banerjee [63]	2014	IBPS	SDVPS	Pairing (CDHP claimed)	Informal analysis
Sarde and Banerjee [50]	2015	IBPS	Standard	Pairing (CDHP claimed)	Informal analysis
Sha [60]	2015	IBPS	SDVPS (repaired)	Pairing	Informal analysis
Mukherjee et al. [42]	2016	IBPS	Standard (with revocation)	Pairing + knapsack	Informal analysis
Hu et al. [51]	2019	IBPS	Generic construction	Pairing	No reductionist proof
Bannore et al. [17]	2024	IBPS	Forward-secure, role-based	Pairing-free (ECC)	BAN logic, AVISPA
Lu et al. [70]	2007	CLPS	Standard (repaired)	Pairing	Informal analysis
Chou [76]	2012	CLPS	Anonymous (repaired)	Pairing	Informal analysis
Ullah et al. [73]	2024	CLPS	Standard (IIoT)	Pairing-free (HECC)	AVISPA, informal analysis
Ullah et al. [74]	2025	CLPS	Multilayer (IIoT)	Pairing-free (HECC)	AVISPA, informal analysis
Li et al. [24] (Scheme 2)	2009	CBPS	Standard	Pairing	None provided
Chen and Huang [83]	2010	CBPS	Standard	Pairing	Informal analysis
Liang et al. [84]	2010	CBPS	SDVPS	Pairing	Claimed ROM/CDHP; no verifiable proof
Huang et al. [85]	2014	CBPS	Generic transformation	Pairing	Informal analysis
Verma and Thakur [87]	2019	CBPS	Standard	Pairing	None; incomplete algorithm
Qiao et al. [25] (Scheme 3)	2021	CBPS	Publicly verifiable (IIoT)	Pairing-free (ECC)	Informal analysis

"Repaired" marks constructions offered as fixes to previously broken schemes. Absence of a reported attack against these schemes should not be read as evidence of security: their claimed properties remain unverified.

unrelated accidents. Each failure class corresponds to the violation of an identifiable design principle. First, algebraic linearity of the proxy key derivation is the mechanism behind the key recovery attacks. When the proxy signing key is a linear or affine predictable combination of public randomness and secret values, a small number of observed signatures is sufficient to solve for the secret. This is exactly what happens in the two-signature key recovery against Okamoto et al. [52, 53] and in the three-signature proxy key reconstruction against Zhang and Yu [54, 55]. The design principle violated here is that the signature equations must not expose a solvable linear system in the long-term secret.

Second, incomplete hash binding explains the delegator and warrant attacks. Whenever the warrant, the identities of the two parties, or the delegation randomness are omitted from the hash inputs of the delegation and signing equations, or are only loosely coupled to them, an insider can redirect a legitimate delegation to a different warrant or message. This is the mechanism behind the delegator forgeries in [44, 46] and the delegation reuse attack in [25]. The corresponding principle is that every semantic element that bounds the authority of the proxy must be cryptographically fused into the value being signed and not merely transmitted alongside it.

Third, confusion between public and confidential system elements is the single structural cause of the entire broken CBPS cluster [19, 86, 88]. The designers treated the implicit certificate of the original signer as if it were available to the verifier of the delegation. This contradicts the certificate-based trust model, in which the certificate also serves as private key material [25]. The violated principle is that every value required by a verification algorithm must be derivable from information that the verifying party legitimately possesses.

Table 3. Cryptanalytic Results on IBPS Schemes.

Scheme	Vulnerability Found	Attacker	Attack Mechanism
Cao and Cao [43]	Delegator forgery attack	Sun et al. [44]	Malicious delegator exploits security model weakness
Gu et al. [45]	Forgery via private key extraction	Hu et al. [46]	Adversary as malicious delegator forges valid IBPS
Hu et al. [48]	Non-tight reduction, delegator attack	Hu et al. [49]	Loose security reduction; vulnerability to delegator
Zhang and Kim [41]	Insecure channel, no revocation	Mukherjee et al. [42]	Compromised private keys break the system
Okamoto et al. [52]	Secret key recovery	Zhang and Chen [53]	Any two message-signature pairs reveal secret key
Zhang and Yu [54]	Insider and outsider forgery	Yuan [55]	Proxy signing key recovery from three known signatures
Singh and Verma [64]	Forgery and proof flaw	Tian et al. [65], Zhou [66]	Forge valid signature from single observed signature
Yoon et al. [67]	False message recovery claim	Asaar et al. [68]	Scheme fails to provide claimed message recovery
Zhang and Mao [57]	Strong DV property failure	Kang et al. [56]	Any participant can verify subsequent signatures
Lal and Verma [26]	Strong DV property failure	Kang et al. [56]	Signature verification leaks to all participants
Yang [58]	OS private-key derivation	Wang [59]	Authorized agent derives OS private key, enabling forgery
Wang [59]	Warrant tampering by colluding PKG-OS	Sha [60]	Collusion enables forged warrant attacks

Fourth, under-specified adversarial models explain the remaining breaks. Many proofs consider only outside attackers and ignore the malicious delegator, the malicious-but-passive KGC, and the key-replacing Type-I adversary, even though all three are realistic in practice. The MbpKGC attack on [81] and the Type-I attack on [78] follow directly from this gap. The principle here is that the security model must cover every attacker that the scheme will face in deployment, so that a proof in the model gives real protection in practice. Viewing the findings of the survey through these four principles turns the history of attacks into clear design guidance for future constructions.

7.3 Comparative Observations Across Paradigms

Table 6 summarizes the comparative observations across the three proxy signature paradigms with respect to common attack vectors and structural weaknesses.

The comparative analysis shows that IBPS schemes are mainly affected by the key escrow problem and by delegator forgery attacks. CLPS schemes remove the key escrow problem but remain vulnerable to public key replacement attacks and to a malicious KGC. CBPS schemes are designed to combine the strengths of both paradigms, yet they often misuse certificate information and inherit weaknesses from their underlying signature primitives. These observations match the attack record in Tables 3 to 5. Forgery and key recovery attacks dominate the broken IBPS schemes, public key replacement is the most common cause of CLPS failures, and a single certificate confidentiality flaw explains three of the five broken CBPS constructions.

7.4 Root Causes of Repeated Failures

The recurrence of vulnerabilities in proxy signature schemes can be attributed to several root causes:

- **Insufficient Threat Modeling:** Many constructions consider only restricted adversarial models and overlook realistic capabilities such as insider attacks, malicious KGC, or chosen-warrant attacks.
- **Heuristic Security Arguments:** A considerable number of schemes provide only informal security arguments without formal reductions, leading to undiscovered vulnerabilities that later cryptanalysis reveals. 20 of the surveyed schemes fall into this category and are listed in Table 2.
- **Improper Reduction in Security Proofs:** Even when formal proofs are provided, flawed or loose reductions weaken the security guarantees, as observed in several IBPS schemes [49].
- **Reuse of Vulnerable Primitives:** Designers

Table 4. Cryptanalytic Results on CLPS Schemes.

Scheme	Vulnerability Found	Attacker	Attack Mechanism
Li et al. [69]	Forgery attack	Lu et al. [70]	Forge proxy signature from existing valid signature
Eslami and Pakniat [71]	Key replacement and malicious KGC attack	Lu and Li [15]	Two concrete attacks break existential unforgeability
Lu and Li [15]	Public key replacement attack	Zhou et al. [72]	Malicious OS or PS forges valid signature
Yang et al. [80]	MbpKGC attack	Lin et al. [81]	Adversary forges signatures bypassing claimed security
Padhye and Tiwari [77]	Type I adversary attack	Shi et al. [78]	Type I adversary breaks the scheme
He et al. [20]	User impersonation attack	Xu et al. [79]	Impersonation breaks UAV network delegation
Yu et al. [75]	Anonymity property failure	Chou [76]	Scheme does not provide claimed anonymity

Table 5. Cryptanalytic Results on CBPS Schemes.

Scheme	Vulnerability Found	Attacker	Attack Mechanism
Kang et al. [82]	Key replacement attack	Li et al. [24]	Susceptible to key replacement
Verma et al. [16]	Forgery by malicious PS (weak Type II)	Zhu et al. [89], Qiao et al. [25]	Weak underlying primitive; delegation reuse attack
Verma et al. [16]	Universal forgery	Park and Kim [90]	Weak ordinary signature propagates to proxy scheme
Mahmoodi et al. [86]	Certificate confidentiality violation	Qiao et al. [25]	PS cannot compute hash requiring secret OS certificate
Verma and Singh [88]	Certificate confidentiality violation	Qiao et al. [25]	Construction relies on confidential OS certificate
Verma et al. [19]	Certificate confidentiality violation	Qiao et al. [25]	PS unable to compute required certificate-based hash

frequently build proxy signature schemes on top of ordinary signature primitives without re-examining their security in the proxy setting, propagating existing weaknesses.

- **Lack of Application-Specific Analysis:** Several schemes are proposed without considering the deployment context, leading to designs that may be theoretically sound but practically vulnerable when applied to environments such as IoT, UAV networks, or industrial systems.

8 Open Research Challenges and Future Directions

Despite extensive research efforts, the design of secure, efficient, and practical proxy signature schemes remains an open problem. Based on the vulnerability analysis and comparative discussion presented in this paper, several open research challenges and future directions can be identified.

8.1 Provably Secure Constructions in the Standard Model

A large portion of existing proxy signature schemes rely on the ROM for their security proofs. While ROM-based proofs provide useful heuristic assurance, schemes proven secure in the ROM may fail when random oracles are instantiated with concrete hash functions. Future research should focus on constructing proxy signature schemes that are provably secure in the SM under well-established hardness assumptions, while maintaining computational efficiency. The record presented in this survey adds a cautionary counterpoint. Seven of the broken schemes carried SM proofs [15, 43, 45, 48, 54, 71, 80]. The goal is therefore not merely a proof in the SM but a proof under an adversarial model that faithfully captures malicious delegators, key-replacing adversaries, and malicious-but-passive key generation authorities, together with a tight and correct reduction.

Table 6. Comparative Analysis of Vulnerabilities Across Proxy Signature Paradigms.

Vulnerability	IBPS	CLPS	CBPS
Key Escrow Problem	●	❍	❍
Delegator Forgery Attack	●	◗	◗
Public Key Replacement	—	●	◗
Malicious KGC Attack	●	●	—
Certificate Confidentiality Violation	—	—	●
Weak Underlying Primitive	●	●	●
Lack of Formal Proof	●	◗	●
Pairing-Based Inefficiency	●	●	●

●: high prevalence (Yes/Frequent/Common), ◗: moderate (Occasional), ❍: absent but applicable (No), —: not applicable (N/A).

8.2 Resistance to Insider and Delegation-Based Attacks

The repeated success of delegator-based forgery attacks and malicious proxy signer attacks indicates that future constructions must explicitly model and resist insider threats. This requires the development of stronger delegation binding mechanisms that cryptographically link the warrant, the original signer's identity, the proxy signer's identity, and the proxy signing key in a manner that prevents key extraction and signature forgery.

8.3 Efficient and Scalable Revocation Mechanisms

The lack of efficient revocation mechanisms remains a major limitation in existing proxy signature schemes. In dynamic environments such as IoT networks, cloud platforms, and blockchain systems, the ability to revoke proxy signing authority promptly and efficiently is essential. Future research should explore lightweight revocation techniques, including time-bound delegation, accumulator-based revocation, and blockchain-assisted revocation.

8.4 Post-Quantum Proxy Signature Schemes

With the rapid advancement of quantum computing, classical hard problems such as the DLP and the ECDLP are expected to become vulnerable. As most existing proxy signature schemes rely on these assumptions, there is a pressing need for the design of post-quantum proxy signature schemes based on lattice-based [92–95], code-based, multivariate, or hash-based cryptographic primitives. Lattice-based constructions are the most developed direction so far, with identity-based, certificateless, and blind proxy signature variants already reported [95–97]. Such constructions must balance security, efficiency, and signature size to be practical for real-world deployment [3, 98]. Post-quantum designs are also not immune to the delegation flaws documented in this survey, since the first lattice-based proxy signature was broken by a forgery attack mounted by the original signer [99].

8.5 Application-Specific Proxy Signature Designs

Emerging application domains such as IoT, UAV networks, electronic healthcare systems, smart grids, and blockchain-based systems impose unique security and efficiency requirements. Future research should focus on developing proxy signature schemes tailored to these domains, taking into account constraints such as limited computational resources, energy efficiency, low communication overhead, and privacy preservation.

8.6 Integration of Physical-Layer Authentication with Cross-Layer Security

An important and largely unexplored direction is the integration of physical-layer authentication techniques with cross-layer security approaches in the environments where proxy signatures are increasingly deployed, such as vehicular networks, UAV swarms, and dense IoT deployments. Physical-layer authentication exploits inherently hard-to-forge channel characteristics, such as channel state information, received-signal-strength profiles, and radio-frequency hardware fingerprints, to provide fast, lightweight identity evidence at the lowest layer of the protocol stack. Coupling such mechanisms with cryptographic proxy delegation in a cross-layer design offers several concrete benefits: (i) *scalability*, since inexpensive physical-layer checks can filter the vast majority of illegitimate transmissions before any costly pairing or elliptic-curve verification of a proxy signature is invoked; (ii) *robustness*, because an adversary must simultaneously defeat both the cryptographic delegation binding and the physical-channel fingerprint, which substantially raises the cost of impersonation and delegation-replay

attacks; and (iii) *improved authentication performance in highly dynamic environments*, where frequent handovers and short contact times make repeated full signature verification impractical. Designing proxy signature schemes whose warrants and verification procedures are explicitly aware of physical-layer evidence, and formally modeling the combined cross-layer adversary, therefore constitutes a promising avenue for enhancing scalability, robustness, and authentication performance in future dynamic communication systems.

8.7 Formal Verification and Automated Cryptanalysis

The history of proxy signature schemes shows that informal security arguments are insufficient. Future research should integrate symbolic verification tools such as ProVerif [100, 101], Tamarin [102], and AVISPA [103], together with computer-aided proof frameworks for the computational model such as CryptoVerif [104] and EasyCrypt [105], to systematically verify the security of new constructions before deployment. Symbolic tools are well suited to checking delegation and warrant binding logic against key replacement and insider adversaries, while computational frameworks can machine-check the reduction itself and catch the incorrect proofs that affected several schemes in Table 6. This would help in identifying subtle attack vectors that may be missed by manual analysis.

8.8 Privacy-Preserving Proxy Signature Schemes

In several modern applications, the identity of the proxy signer or the contents of the warrant must remain confidential to protect user privacy. Future work should explore the integration of privacy-enhancing techniques such as zero-knowledge proofs [106], ring signatures [107], and anonymous credentials [108] within proxy signature schemes to provide stronger privacy guarantees without sacrificing accountability.

9 Conclusion

This survey examined the security of proxy signature schemes in the IBPS, CLPS, and CBPS paradigms. It presented the design principles of each paradigm and the structural differences among them. It consolidated the published cryptanalysis of these schemes and identified the structural weakness underlying each reported attack. The observed weaknesses fall into a small number of classes. These are insufficient binding of the warrant and the identities to the proxy signing key, reuse of base signature primitives whose security does not carry over to the proxy setting, incorporation of confidential certificate material into the verification equation, adversarial models that exclude the malicious delegator and the malicious KGC, and the absence of a formal security reduction. The survey covers 44 schemes in total (22 IBPS, 11 CLPS, and 11 CBPS). Published cryptanalytic results or correctness analyses have invalidated 24 of them, and the remaining 20 were proposed without a formal proof in either the random oracle model or the standard model. Each scheme is reviewed concisely and classified as broken or unproven, and the coverage is compared with existing surveys in the field.

These findings indicate that insecurity in proxy signature design is systematic rather than incidental. A new construction should therefore bind the warrant, the participant identities, and the delegation randomness into the value being signed, should re-establish the security of its base primitive within the proxy setting, and should be accompanied by a formal reduction under an adversarial model that includes malicious delegators and key generation authorities. Post-quantum constructions, efficient revocation, and privacy-preserving variants remain open problems. The taxonomy, the consolidated attack tables, and the design principles established in this survey provide a reference framework for the design and evaluation of future proxy signature schemes.

Data Availability Statement

Not applicable.

Funding

This work was supported without any funding.

Conflicts of Interest

Saddam Hussain served as an Associate Editor of the *ICCK Transactions on Information Security and Cryptography* at the time of manuscript submission. To ensure the integrity of the peer-review process, Saddam Hussain was not involved in the editorial handling, peer review, or decision-making process for this manuscript, which was handled independently by another editor. The remaining authors declare no conflicts of interest.

AI Use Statement

The authors declare that ChatGPT-5 was used for language editing of the manuscript. The authors have carefully reviewed, revised, and verified the AI-assisted output and take full responsibility for the content of the manuscript.

Ethical Approval and Consent to Participate

Not applicable.

References

[1] Mambo, M., Usuda, K., & Okamoto, E. (1996). Proxy signatures: Delegation of the power to sign messages. *IEICE transactions on fundamentals of electronics, communications and computer sciences, 79*(9), 1338-1354.

[2] Hussain, S., Tufail, A., Naim, H. A. A. G., Khan, M. A., & Barb, G. (2025). Evaluation of computationally efficient identity-based proxy signatures. *IEEE Open Journal of the Computer Society, 6*, 846-861. [CrossRef]

[3] Wu, F., Zhou, B., & Zhang, X. (2023). Identity-based proxy signature with message recovery over NTRU lattice. *Entropy, 25*(3), 454. [CrossRef]

[4] Islam, S. H., & Biswas, G. P. (2014). A provably secure identity-based strong designated verifier proxy signature scheme from bilinear pairings. *Journal of King Saud University Computer and Information Sciences, 26*(1), 55-67. [CrossRef]

[5] Verma, V., & Sharma, Y. (2023). Identity-Based Designated Verifier Proxy Signature Scheme and Its Application to Health Care. *International Conference on Recent Developments in Cyber Security*, 271-278. Springer. [CrossRef]

[6] Mehmood, A., Khan, M. A., Maple, C., & Lloret, J. (2023, October). Zero-knowledge proofs based delegation authentication for industrial Internet of Things in certificateless proxy signatures. In *2023 10th International Conference on Internet of Things: Systems, Management and Security (IOTSMS)* (pp. 8-14). IEEE. [CrossRef]

[7] Qu, Y., & Zeng, J. (2022). Certificateless proxy signcryption in the standard model for a UAV network. *IEEE Internet of Things Journal, 9*(16), 15116-15127. [CrossRef]

[8] Zhang, G., Zhou, Y., Liu, X., Yang, B., & Zhang, M. (2026). RCBPS: Revocable Certificate-based Proxy Signature Scheme in the Standard Model for Secure CloudIoT Communications. *Computer Networks*, 112181. [CrossRef]

[9] Zhang, G., Zhou, Y., Liu, X., & Yang, B. (2026). Certificate-based proxy signature scheme with revocation for Industrial Internet of Things. *Computer Standards & Interfaces, 95*, 104045. [CrossRef]

[10] Hussain, S., Tufail, A., Khan, M. A., & Ullah, F. (2025, October). Complexity Evaluation of Certificate-Based Proxy Signatures. In *2025 2nd International Symposium on AI and Cybersecurity (ISAICS)* (pp. 1-6). IEEE. [CrossRef]

[11] Wu, W., Mu, Y., Susilo, W., Seberry, J., & Huang, X. (2007, July). Identity-based proxy signature from pairings. In *International Conference on Autonomic and Trusted Computing* (pp. 22-31). Berlin, Heidelberg: Springer Berlin Heidelberg. [CrossRef]

[12] He, D., Chen, Y., & Chen, J. (2013). An efficient certificateless proxy signature scheme without pairing. *Mathematical and Computer Modelling, 57*(9-10), 2510-2518. [CrossRef]

[13] Chen, Y. C., Liu, C. L., Horng, G., & Chen, K. C. (2011). A provably secure certificateless proxy signature scheme. *International Journal of Innovative Computing, Information and Control, 7*(9), 5557-5569. http://www.ijicic.org/ijicic-10-07011.pdf

[14] Deng, L., Hu, Z., Ruan, Y., & Wang, T. (2022). Provably Secure Certificateless Proxy Signature Scheme in the Standard Model. *Journal of Internet Technology, 23*(2), 279-288. [CrossRef]

[15] Lu, Y., & Li, J. (2016). Provably secure certificateless proxy signature scheme in the standard model. *Theoretical Computer Science, 639*, 42-59. [CrossRef]

[16] Verma, G. K., Singh, B. B., Kumar, N., Obaidat, M. S., He, D., & Singh, H. (2020). An efficient and provable certificate-based proxy signature scheme for IIoT environment. *Information sciences, 518*, 142-156. [CrossRef]

[17] Bannore, A., Patil, R. Y., H. Patil, Y., & Deshpande, H. (2024). Proxy signature-based role delegation scheme: formal analysis and simulation. *International Journal of Information Technology, 16*(7), 4027-4038. [CrossRef]

[18] Lin, T. W., & Hsu, C. L. (2025). ID-based proxy signature with key-insulated scheme for portable healthcare devices in 5G-IoHT. *Journal of Internet Technology, 26*(3), 283-292. https://jit.ndhu.edu.tw/article/view/3167

[19] Verma, G. K., Singh, B. B., Kumar, N., & He, D. (2019). CB-PS: An efficient short-certificate-based proxy signature scheme for UAVs. *IEEE Systems Journal, 14*(1), 621-632. [CrossRef]

[20] He, L., Ma, J., Shen, L., & Wei, D. (2021). Certificateless designated verifier proxy signature scheme for unmanned aerial vehicle networks. *Science China Information Sciences, 64*(1), 112101. [CrossRef]

[21] Das, M. L., Saxena, A., & Phatak, D. B. (2006). Algorithms and approaches of proxy signature: A survey. *arXiv preprint cs/0612098*. [CrossRef]

[22] Agarwal, N., Rana, A., & Pandey, J. P. (2016, January). Proxy signatures for secured data sharing. In *2016 6th International Conference-Cloud System and Big Data Engineering (Confluence)* (pp. 255-258). IEEE.

[CrossRef]

[23] Hussain, S., Tufail, A., Naim, H. A. A. G., Khan, M. A., & Barb, G. (2026). Exploring the Security Dimensions of Identity-Based Proxy Signature Schemes: A Comprehensive Review. *IEEE Open Journal of the Computer Society, 7*, 817-834. [CrossRef]

[24] Li, J., Xu, L., & Zhang, Y. (2009). Provably Secure Certificate-based Proxy Signature Schemes. *J. Comput.*, 4(6), 444-452. https://www.jcomputers.us/vol4/jcp0406-02.pdf

[25] Qiao, Z., Zhou, Y., Yang, B., Zhang, M., Wang, T., & Xia, Z. (2021). Secure and efficient certificate-based proxy signature schemes for industrial internet of things. *IEEE Systems Journal, 16*(3), 4719-4730. IEEE. [CrossRef]

[26] Lal, S., & Verma, V. (2006). Identity based strong designated verifier proxy signature scheme. *Cryptography eprint Archive Report 2006/394*. https://eprint.iacr.org/2006/394

[27] Zhang, L., Wu, Q., Qin, B., Domingo-Ferrer, J., Zeng, P., Liu, J., & Du, R. (2013, March). A generic construction of proxy signatures from certificateless signatures. In *2013 IEEE 27th International Conference on Advanced Information Networking and Applications (AINA)* (pp. 259-266). IEEE. [CrossRef]

[28] Zhang, J., & Ji, C. (2008). An Efficient Proxy Signature Scheme with Full-delegation. *2008 IEEE International Conference on Networking, Sensing and Control*, 513-518. IEEE. [CrossRef]

[29] Zhang, L., Zhang, F., & Wu, Q. (2012). Delegation of signing rights using certificateless proxy signatures. *Information Sciences, 184*(1), 298-309. Elsevier. [CrossRef]

[30] Wang, G., Bao, F., Zhou, J., & Deng, R. H. (2003, November). Security analysis of some proxy signatures. In *International Conference on Information Security and Cryptology* (pp. 305-319). Berlin, Heidelberg: Springer Berlin Heidelberg. [CrossRef]

[31] Lee, B., Kim, H., & Kim, K. (2001). Strong proxy signature and its applications. *Proceedings of SCIS*, 2001, 603-608. http://hdl.handle.net/10203/130232

[32] Chou, J. S., Hung, S. C., & Chen, Y. (2011). An efficient secure anonymous proxy signature scheme. *Cryptology ePrint Archive*. https://eprint.iacr.org/2011/498

[33] Boldyreva, A., Palacio, A., & Warinschi, B. (2012). Secure proxy signature schemes for delegation of signing rights. *Journal of Cryptology, 25*(1), 57-115. [CrossRef]

[34] Miller, V. S. (1985, August). Use of elliptic curves in cryptography. In *Conference on the theory and application of cryptographic techniques* (pp. 417-426). Berlin, Heidelberg: Springer Berlin Heidelberg. [CrossRef]

[35] Choon, J. C., & Hee Cheon, J. (2002, December). An identity-based signature from gap Diffie-Hellman groups. In *International workshop on public key cryptography* (pp. 18-30). Berlin, Heidelberg: Springer Berlin Heidelberg. [CrossRef]

[36] Diffie, W., & Hellman, M. E. (2022). New directions in cryptography. In *Democratizing cryptography: the work of Whitfield Diffie and Martin Hellman* (pp. 365-390). [CrossRef]

[37] Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of computation, 48*(177), 203-209. [CrossRef]

[38] Boneh, D., & Franklin, M. (2001, August). Identity-based encryption from the Weil pairing. In *Annual international cryptology conference* (pp. 213-229). Berlin, Heidelberg: Springer Berlin Heidelberg. [CrossRef]

[39] Bellare, M., & Rogaway, P. (1993, December). Random oracles are practical: A paradigm for designing efficient protocols. In *Proceedings of the 1st ACM Conference on Computer and Communications Security* (pp. 62-73). [CrossRef]

[40] Canetti, R., Goldreich, O., & Halevi, S. (2004). The random oracle methodology, revisited. *Journal of the ACM (JACM), 51*(4), 557-594. [CrossRef]

[41] Zhang, F., & Kim, K. (2003, June). Efficient ID-based blind signature and proxy signature from bilinear pairings. In *Australasian Conference on Information Security and Privacy* (pp. 312-323). Berlin, Heidelberg: Springer Berlin Heidelberg. [CrossRef]

[42] Mukherjee, D., Vyavahare, P., & Panchal, M. (2016). An improved ID based proxy signature scheme based on elliptic curve cryptography. In *Proc. 10th Int. Conf. Emerg. Secur. Inf. Syst. Technol* (pp. 235-240). https://personales.upv.es/thinkmind/dl/conferences/securware/securware_2016/securware_2016_12_30_30117.pdf

[43] Cao, F., & Cao, Z. (2010, August). An identity based proxy signature scheme secure in the standard model. In *2010 IEEE International Conference on Granular Computing* (pp. 67-72). IEEE. [CrossRef]

[44] Sun, Y., Yu, Y., Zhang, X., & Chai, J. (2013). On the security of an identity-based proxy signature scheme in the standard model. *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, 96*(3), 721-723. [CrossRef]

[45] Gu, K., Jia, W., & Jiang, C. (2015). Efficient identity-based proxy signature in the standard model. *The Computer Journal, 58*(4), 792-807. Oxford University Press. [CrossRef]

[46] Hu, X., Wang, J., Xu, H., Yang, Y., & Xu, X. (2017). An improved efficient identity-based proxy signature in the standard model. *International Journal of Computer Mathematics, 94*(1), 22-38. Taylor & Francis. [CrossRef]

[47] James, S., & Thumbur, G. (2021). Pairing-free identity-based proxy signature scheme with message recovery. *International Journal of Information Security*

and Privacy (IJISP), 15(1), 117-137. [CrossRef]

[48] Hu, X., Lu, H., Xu, H., Wang, J., & Yang, Y. (2015, May). An efficient identity-based proxy signature scheme in the standard model with tight reduction. In *Computational Intelligence in Security for Information Systems Conference* (pp. 309-319). Cham: Springer International Publishing. [CrossRef]

[49] Hu, X., Zhang, X., Wang, J., Xu, H., Tan, W., & Yang, Y. (2017). Secure and efficient identity-based proxy signature scheme in the standard model based on computational Diffie–Hellman problem. *Arabian Journal for Science and Engineering, 42*(2), 639-649. [CrossRef]

[50] Sarde, P., & Banerjee, A. (2015). A secure ID-based proxy signature scheme from bilinear pairings. *International Journal of Computer Applications, 124*(9), 1-4. [CrossRef]

[51] Hu, X., Xu, H., Wang, J., Tan, W., & Yang, Y. (2019). A generic construction of identity-based proxy signature scheme in the standard model. *International Journal of Information and Computer Security, 11*(1), 83-100. [CrossRef]

[52] Okamoto, T., Inomata, A., & Okamoto, E. (2005, April). A proposal of short proxy signature using pairing. In *International Conference on Information Technology: Coding and Computing (ITCC'05)-Volume II* (Vol. 1, pp. 631-635). IEEE. [CrossRef]

[53] Zhang, F., & Chen, X. (2005). Attack on Okamoto et al.'s New Short Signature Schemes. *Cryptology ePrint Archive*. https://eprint.iacr.org/2005/240

[54] Zhang, J., & Yu, Y. (2014). Short computational Diffie–Hellman-based proxy signature scheme in the standard model. *International Journal of Communication Systems, 27*(10), 1894-1907. [CrossRef]

[55] Yuan, Y. (2015). On the security of a proxy signature scheme in the standard model. *International Journal of Communication Systems, 28*(4), 675-681. [CrossRef]

[56] Kang, B., Boyd, C., & Dawson, E. (2009). Identity-based strong designated verifier signature schemes: attacks and new construction. *Computers & Electrical Engineering, 35*(1), 49-53. [CrossRef]

[57] Zhang, J., & Mao, J. (2008). A novel ID-based designated verifier signature scheme. *Information sciences, 178*(3), 766-773. [CrossRef]

[58] Yang, A. (2010, October). ID-based designated-verifier proxy signature scheme without a trusted party. In *2010 International Conference on Computer Application and System Modeling (ICCASM 2010)* (Vol. 7, pp. V7-191). IEEE. [CrossRef]

[59] Wang, B. (2008). A new identity based proxy signature scheme. *Cryptology ePrint Archive*. https://eprint.iacr.org/2008/323

[60] Sha, L. (2015, June). Improvement of an ID-based proxy signature scheme without trusted PKG. In *2015 IEEE/ACIS 16th International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)* (pp. 1-4). IEEE. [CrossRef]

[61] Lee, J. S., Chang, J. H., & Lee, D. H. (2010). Forgery attacks on Kang et al.'s identity-based strong designated verifier signature scheme and its improvement with security proof. *Computers & Electrical Engineering, 36*(5), 948-954. [CrossRef]

[62] Wei, B. D. (2013). A provably secure ID-based designated verifier proxy signature scheme based on DLP. *Applied Mechanics and Materials, 411*, 721-724. [CrossRef]

[63] Sarde, P. A. N. K. A. J., & Banerjee, A. M. I. T. A. B. H. (2014). An identity based strong designated verifier proxy signature scheme from bilinear pairings. *Int. J. Math. Comput. Appl. Res, 4*(6), 1-8.

[64] Singh, H., & Verma, G. K. (2012). ID-based proxy signature scheme with message recovery. *Journal of Systems and Software, 85*(1), 209-214. [CrossRef]

[65] Tian, M., Huang, L., & Yang, W. (2012). Cryptanalysis of an ID-based proxy signature scheme with message recovery. *Applied Mathematics & Information Sciences, 6*(3), 419-422. https://www.naturalspublishing.com/files/published/97em5p1ly4a6k7.pdf

[66] Zhou, C. (2015). An improved id-based proxy signature scheme with message recovery. *International Journal of Security and Its Applications, 9*(9), 151–164. [CrossRef]

[67] Yoon, E. J., Choi, Y., & Kim, C. (2013, May). New ID-based proxy signature scheme with message recovery. In *International Conference on Grid and Pervasive Computing* (pp. 945-951). Berlin, Heidelberg: Springer Berlin Heidelberg. [CrossRef]

[68] Asaar, M. R., Salmasizadeh, M., & Susilo, W. (2016). A short ID-based proxy signature scheme. *International Journal of Communication Systems, 29*(5), 859-873. [CrossRef]

[69] Li, X. X., Chen, K. F., & Sun, L. (2005). Certificateless signature and proxy signature schemes from bilinear pairings. *Lithuanian Mathematical Journal, 45*(1), 76-83. [CrossRef]

[70] Lu, R., He, D., & Wang, C. (2007, July). Cryptanalysis and improvement of a certificateless proxy signature scheme from bilinear pairings. In *Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD 2007)* (Vol. 3, pp. 285-290). IEEE. [CrossRef]

[71] Ming, Y., & Wang, Y. (2018). Certificateless proxy signature scheme in the standard model. *Fundamenta Informaticae, 160*(4), 409-445. [CrossRef]

[72] Zhou, C., Dong, X., Wang, L., & Li, T. (2019). On the Security of a Certificateless Proxy Signature Scheme in the Standard Model. *International Journal of Network Security, 21*(4), 576-581. [CrossRef]

[73] Ullah, R., Mehmood, A., Khan, M. A., Maple, C., & Lloret, J. (2024). An optimal secure and reliable certificateless proxy signature for industrial internet of things. *Peer-to-Peer Networking and Applications, 17*(4), 2205-2220. [CrossRef]

[74] Ullah, R., Mehmood, A., Khan, M. A., & Ullah, I. (2025). Provably secure multilayers certificateless proxy signature for industrial internet of things. *Cluster Computing, 28*(5), 312. [CrossRef]

[75] Yu, Y., Xu, C., Huang, X., & Mu, Y. (2009). An efficient anonymous proxy signature scheme with provable security. *Computer Standards & Interfaces, 31*(2), 348-353. [CrossRef]

[76] Chou, J. S. (2012). A novel anonymous proxy signature scheme. *Advances in Multimedia, 2012*(1), 427961. Wiley Online Library. [CrossRef]

[77] Padhye, S., & Tiwari, N. (2015). ECDLP-based certificateless proxy signature scheme with message recovery. *Transactions on Emerging Telecommunications Technologies, 26*(3), 346-354. Wiley Online Library. [CrossRef]

[78] Shi, W., He, D., & Gong, P. (2013). On the security of a certificateless proxy signature scheme with message recovery. *Mathematical Problems in Engineering, 2013*(1), 761694. [CrossRef]

[79] Xu, Z., Luo, M., Vijayakumar, P., Peng, C., & Wang, L. (2022). Efficient certificateless designated verifier proxy signature scheme using UAV network for sustainable smart city. *Sustainable Cities and Society, 80*, 103771. [CrossRef]

[80] Yang, W., Weng, J., Huang, X., & Yang, A. (2020). A provably secure certificateless proxy signature scheme against malicious-but-passive KGC attacks. *The Computer Journal, 63*(8), 1139-1147. [CrossRef]

[81] Lin, X. J., Wang, Q., Sun, L., Yan, Z., & Liu, P. (2021). Security analysis of the first certificateless proxy signature scheme against malicious-but-passive KGC attacks. *The Computer Journal, 64*(4), 653-660. [CrossRef]

[82] Kang, B. G., Park, J. H., & Hahn, S. G. (2004, February). A certificate-based signature scheme. In *Cryptographers' Track at the RSA Conference* (pp. 99-111). Berlin, Heidelberg: Springer Berlin Heidelberg. [CrossRef]

[83] Chen, J., & Huang, Z. (2010, December). Certificate-based proxy signature. In *2010 IEEE International Conference on Progress in Informatics and Computing* (Vol. 1, pp. 465-468). IEEE. [CrossRef]

[84] Liang, X. Q., Liu, S. D., Xu, J. F., & Liu, Q. (2010, August). A certificate-based strong designated verifier proxy signature scheme. In *2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE)* (Vol. 1, pp. V1-614). IEEE. [CrossRef]

[85] Huang, R., Huang, Z., & Chen, Q. (2014). Provable secure generic construction of proxy signature from certificate-based signature. *Open Automation and Control Systems Journal, 6*, 566-574. https://www.benthamopenarchives.com/contents/pdf/TOAUTOCJ/TOAUTOCJ-6-566.pdf

[86] Mahmoodi, A., Mohajery, J., & Salmasizadeh, M. (2016). A certificate-based proxy signature with message recovery without bilinear pairing. *Security and Communication Networks, 9*(18), 4983-4991. [CrossRef]

[87] Verma, V., & Thakur, A. (2019). A Certificate-Based Proxy Signature Without Message Recovery With Bilinear Pairing. *International Journal of Scientific & Technology Research, 8*(11). https://eprint.iacr.org/2014/010

[88] Verma, G. K., & Singh, B. (2017). Short certificate-based proxy signature scheme from pairings. *Transactions on Emerging Telecommunications Technologies, 28*(12), e3214. Wiley Online Library. [CrossRef]

[89] Zhu, F., Xu, F., Yang, X., Yi, X., & Abuadbba, A. (2022). Cryptanalysis and improvements of an efficient certificate-based proxy signature scheme for IIoT environments. *Information Processing Letters, 173*, 106170. Elsevier. [CrossRef]

[90] Park, J. H., & Kim, W. H. (2024). Security weakness of a certificate-based proxy signature scheme for IIoT environments. *Information Processing Letters, 183*, 106406. [CrossRef]

[91] Kang, L., Tang, X., Lu, X., & Fan, J. (2007). A short signature scheme in the standard model. *Cryptology ePrint Archive*. Citeseer. https://eprint.iacr.org/2007/398

[92] Jiang, Y., Kong, F., & Ju, X. (2010, December). Lattice-based proxy signature. In *2010 International Conference on Computational Intelligence and Security* (pp. 382-385). IEEE. [CrossRef]

[93] Li, W. (2016, September). An identity-based proxy signature scheme from lattices in the standard model. In *2016 International conference on intelligent networking and collaborative systems (INCoS)* (pp. 167-172). IEEE. [CrossRef]

[94] Zhang, L., & Ma, Y. (2014). A Lattice-Based Identity-Based Proxy Blind Signature Scheme in the Standard Model. *Mathematical Problems in Engineering, 2014*(1), 307637. [CrossRef]

[95] Wu, F., Yao, W., Zhang, X., Wang, W., & Zheng, Z. (2019). Identity-based proxy signature over NTRU lattice. *International journal of communication systems, 32*(3), e3867. [CrossRef]

[96] Yu, H., & Wang, N. (2023). Certificateless network coding proxy signatures from lattice. *Frontiers of Computer Science, 17*(5), 175810. [CrossRef]

[97] Li, F., Yang, M., Song, Z., Wang, P., & Li, G. (2023). Post-quantum secure identity-based proxy blind signature scheme on a lattice. *Entropy, 25*(8), 1157. MDPI. [CrossRef]

[98] Wang, L., Huang, C., & Cheng, H. (2023). Novel proxy signature from lattice for the post-quantum Internet of Things. *Journal of Ambient Intelligence and Humanized Computing*, *14*(8), 9939-9946. [CrossRef]

[99] Tian, M., & Huang, L. (2011). Cryptanalysis of a lattice-based proxy signature scheme. *arXiv preprint arXiv:1110.4196*. [CrossRef]

[100] Blanchet, B. (2001). An efficient cryptographic protocol verifier based on prolog rules. *Proceedings. 14th IEEE Computer Security Foundations Workshop, 2001.*, 82-96. [CrossRef]

[101] Blanchet, B. (2016). Modeling and verifying security protocols with the applied pi calculus and ProVerif. *Foundations and Trends® in Signal Processing*, *1*(1-2), 1-135. [CrossRef]

[102] Meier, S., Schmidt, B., Cremers, C., & Basin, D. (2013, July). The TAMARIN prover for the symbolic analysis of security protocols. In *International conference on computer aided verification* (pp. 696-701). Berlin, Heidelberg: Springer Berlin Heidelberg. [CrossRef]

[103] Armando, A., Basin, D., Boichut, Y., Chevalier, Y., Compagna, L., Cuéllar, J., ... & Vigneron, L. (2005, July). The AVISPA tool for the automated validation of internet security protocols and applications. In *International conference on computer aided verification* (pp. 281-285). Berlin, Heidelberg: Springer Berlin Heidelberg. [CrossRef]

[104] Blanchet, B. (2008). A computationally sound mechanized prover for security protocols. *IEEE Transactions on Dependable and Secure Computing*, *5*(4), 193-207. [CrossRef]

[105] Barthe, G., Grégoire, B., Heraud, S., & Béguelin, S. Z. (2011, August). Computer-aided security proofs for the working cryptographer. In *Annual Cryptology Conference* (pp. 71-90). Berlin, Heidelberg: Springer Berlin Heidelberg. [CrossRef]

[106] Goldwasser, S., Micali, S., & Rackoff, C. (1989). The knowledge complexity of interactive proof systems. *SIAM Journal on Computing*, *18*(1), 186-208. [CrossRef]

[107] Bender, A., Katz, J., & Morselli, R. (2009). Ring signatures: Stronger definitions, and constructions without random oracles. *Journal of Cryptology*, *22*(1), 114-138. [CrossRef]

[108] Chathurangi, M., Li, Q., & Foo, E. (2025). On advances of anonymous credentials—from traditional to post-quantum. *Cryptography*, *9*(1), 8. MDPI. [CrossRef]

Saddam Hussain is enrolled with the School of Digital Science, Universiti Brunei Darussalam, Gadong, Brunei. He has published several papers in well-reputed journals, including IEEE, JISA, Elsevier, Cluster Computing, Computer Communication, IoTJ, and Electronics. He is serving as a reviewer in reputed journals, including IEEE Access, International Journal of Wireless Information Networks, Scientific Journal of Electrical Computer and Informatics Engineering, and CMC. His research interests include cryptography, network security, Wireless Sensor Networking (WSN), Information-Centric Networking (ICN), Named Data Networking (NDN), smart grids, Internet of Things (IoT), IIoT, quantum computing, cloud computing, and edge computing. (Email: saddam.hussain@riphah.edu.pk)

Nayab is a Computer Science researcher with over a decade of post-graduate teaching experience in Pakistan. She received her Bachelor of Computer Science (Hons) and her MS in Computer Science from Hazara University, Mansehra, Pakistan, where she also earned a Bachelor of Education as a Gold Medallist. She is currently pursuing her Ph.D. in Computer Science at the University of Haripur, Pakistan. Her research interests include probabilistic deep learning, smart grid load forecasting, IoT security, and signcryption schemes. (Email: nayabkhan.cs@gmail.com)