Journal of Universal Computer Science, vol. 30, no. 12 (2024), 1662-1690
submitted: 24/11/2023, accepted: 12/5/2024, appeared: 28/11/2024 CC BY-ND 4.0

Certificateless Aggregate Signatures: A Comprehensive Survey and Comparative Analysis

Rupesh Kumar Verma
(Department of Mathematics, MATS University,
Raipur 492004, Chhattisgarh, India
rupkv1993@gmail.com)

A. J. Khan
(Department of Mathematics, MATS University,
Raipur 492004, Chhattisgarh, India
https://orcid.org/0000-0001-9108-6687, khanaj@matsuniversity.ac.in)

Sunil Kashyap
(School of Sciences, MATS University, Raipur 492004, Chhattisgarh, India
https://orcid.org/0000-0003-4948-3712, 7sunilkumarkashyap@gmail.com)

* **Manoj Kumar Chande**
(Shri Shankaracharya Institute of Professional Management and Technology
Raipur, 492015, Chhattisgarh, India
https://orcid.org/0000-0001-5471-4496
* Corresponding Author: manojkumarchande@gmail.com)

Abstract: This paper presents a comprehensive survey of the certificateless aggregate signature scheme in terms of their computational performance and security. This signature scheme is of significant interest because of its relevance in various domains such as Internet of Things (IoT), Vehicular Ad-hoc Networks (VANETs), E-Healthcare Medical Systems, and Mobile Healthcare Systems. Further, we point towards potential future directions for research and development in this field and conclude our study. This survey serves as a valuable resource for expanding the horizons of this scheme by envisioning new applications.

Keywords: Certificateless Aggregate Signature (CLAS), Computational Diffie-Hellman (CDH) Problem, Elliptic Curve Discrete Logarithm Problem (ECDLP).
Categories: J.2, J.6, L.4
DOI: 10.3897/jucs.116249

1 Introduction

The introduction of Public-Key Cryptography (PKC) by Diffie and Hellman [Diffie and Hellman 1976] marked a pivotal moment in the field of computer-supported communication security. In this system handling of Public Key Identities (PKI) cost was very high and this was the challenge of the widespread adoption of PKC. One of the initial solutions proposed to address this issue was Identity-Based (ID-Based) Cryptography. In 1984, Shamir [Shamir 1984], attempted to provide a method for this issue known as ID-Based Cryptography, in which no such public keys are required. In

ID-Based Cryptography, having knowledge of specific identities, such as information like email addresses, is adequate for encrypting messages and verifying signatures. The Trusted Authority (TA) only distribute secret keys after identifying the user properly. The security concern with ID-Based Cryptography lies in the fact that the TA possesses the private keys of all users within the system. Consequently, the TA must be trustworthy and refrain from any misuse of users' private keys.

In 2003, Riyami and Paterson [Al-Riyami and Paterson 2003], adopted a novel approach referred to as Certificateless (CL) cryptography to resolve the underlying issue with ID-Based cryptography. In the CL approach, a user's secret key consists of two components: the initial part is provided by a Key Generation Center (KGC) and linked to the user's identity, while the second part is contributed by the user individually and remains undisclosed to any third parties. This approach effectively circumvents the key escrow problem, as the KGC does not possess the complete secret key. In the same year Boneh et al. [Boneh et al. 2003], defined as aggregation of signatures, is simply a generalization of scheme of Itakura and Nakamura [Itakura and Nakamura 1983], which allows multiple signatures on a message, which can be combined into a single signature.

Aggregation of Signatures

A bit string σ on a message m_i which proves that the signers $U_1, U_2, \cdots, U_n$ of a set $\mathbb{U}$ signed the message m_i. The goal is to achieve a fixed-size signature and decrease the time needed for signature verification.

In Aggregate Signatures (AS), it is no longer required that the message must be unique. Consequently, an Aggregate Signature comprises a roster of signers $\mathbb{U} = (U_1, U_2, \cdots, U_n)$ along with a list of messages $\mathbb{M} = (m_1, m_2, \cdots, m_n)$, along with a bit string confirming that user U_i has signed the corresponding message m_i. Three distinct types of aggregation are defined:

Type 1 Signatures by different signers on a single message.

Type 2 Signatures by a specific signer on different messages.

Type 3 Signatures by multiple signers on multiple messages.

We have organized our survey article as follows - In Section 2, we have described the preliminary study which helps to understand the structure of Certificateless Aggregate Signature (CLAS) schemes. Section 3 discusses about the security assumptions and intractable mathematical problems involved in CLAS schemes. In Section 4, we have discussed about CLAS and security models. Section 5 provided a rigourous survey of CLAS scheme. Section 6 is about the comparison of computational complexity and comprehensive security analysis of the CLAS schemes in existence. In Section 7, we delve into the prospective avenues for research and development within the realm of CLAS schemes. Ultimately, our study culminates with a conclusion in the final section.

2 Preliminaries

This section summarizes the fundamental concepts that provide the foundation for the CLAS scheme.

2.1 Bilinear Mapping

Let us consider $\mathbb{G}_1$ and $\mathbb{G}_2$ be finite groups with $|\mathbb{G}_1| = |\mathbb{G}_2| = |\mathbb{G}_T|$. A bilinear mapping is a function $e : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T$, which holds the properties:

- Bilinearity - For all $P \in \mathbb{G}_1$ and $Q \in \mathbb{G}_2$, $a, b \in \mathbb{Z}$, then the equation holds: $e(aP, bQ) = e(P, Q)^{ab}$.
- Non Degeneracy - Suppose Q serves as a generator of $\mathbb{G}_2$, and $\psi(\cdot)$ represents a homomorphism from $\mathbb{G}_2$ to $\mathbb{G}_1$. In this context, it holds that $e(\psi(Q), Q) \neq 1$.
- Symmetry - $\forall P, Q \in \mathbb{G}_1, e(P, Q) = e(Q, P)$.
- Admissible - Efficient computation of $e(.,.)$ is feasible.

2.2 Elliptic Curve

Consider F_q as a finite field with a modulus of q, where q represents a substantial prime number. An elliptic curve over this finite field F_q is defined as follows:

$$E : y^2 = x^3 + ax + b \bmod p,$$

where $a, b, x, y \in F_q$ and $\nabla = 4a_3 + 27b_2 \neq 0 \bmod p$.

Let's consider a point $P = (x_1, y_1)$ on the elliptic curve E, where P is a point belonging to E, and its negative point is denoted as $-P = (x_1, -y_1) \bmod p$. Now, let's assume another point $Q = (x_2, y_2)$ on the same curve, with the condition that Q is not equal to $-P$. We can define a line l that passes through points P and Q and intersects the elliptic curve at a new point $R = (x_3, y_3)$. The symmetrical point of R about the x-axis is represented as $R' = (x_3, -y_3)$.

With these definitions, we can establish $R = P + Q$. The operation of scalar multiplication on the elliptic curve can be elucidated as follows: $k \cdot P = P + P + P + \cdots + P$, where k belongs to the set of non-zero integers modulo q ($k \in Z_q^*$).

2.3 One-Way Hash Function

A One-Way Hash Function (OWHF) is a function denoted as h that meets the following criteria:

- The input argument m can vary in length, while the output result $h(m)$ always possesses a constant length of n bits.
- The hash function must exhibit one-way properties, meaning that under certain conditions:

  - Given a value Y in the range of h, it should be computationally challenging to discover a message m such that $h(m) = Y$ (pre-image resistance).

  - Given both a message m and its hash $h(m)$, it should also be computationally challenging to find a distinct message $m" \neq X$ such that $h(m") = h(m)$.

  These properties ensure the security and reliability of the hash function.

3 Security Assumptions and Intractable Mathematical Problems

The mathematical assumptions and intractable mathematical problems that provide cryptographic security to CLAS schemes are described here.

- Computational Diffie-Hellman (CDH) Problem: In the context of a multiplicative group denoted as $(\mathbb{G}, .)$, and with elements α, α^a, and α^b belonging to $\mathbb{G}$, the computation involves finding α^{ab}.
- Decisional Diffie-Hellman (DDH) Problem: Let's contemplate a group denoted as G_1 with a prime order of q. The DDH problem involves the determination of whether T equals abP, where P is a generator of G_1, and we have random numbers a and b taken from G_1, with T provided as part of the problem statement.
- Discrete Logarithm Problem (DLP): Consider a cyclic group denoted as G with an order of n, and let g serve as a generator for this group. When presented with an element y belonging to G, the discrete logarithm problem involves the task of discovering an integer x such that $g^x = y$.
- RSA Problem: Suppose we have an RSA public key represented as (n, e), and a given ciphertext denoted as C. In the RSA problem, the objective is to determine a message m that satisfies the equation $C \equiv m \cdot e \pmod{n}$.
- Elliptic Curve Discrete Logarithm Problem (ECDLP): Consider an elliptic curve denoted as E defined over a finite field F_q, and let P be a point belonging to $E(F_q)$ with an order of n. Given another point Q belonging to the subgroup generated by P, the ECDLP entails the task of finding an integer l, where $0 \leq l \leq n-1$, such that $Q = lP$. ECDLP is a specific instance of the DLP where the cyclic group G is represented by the subgroup generated by the point P on an elliptic curve.

4 Certificateless Aggregate Signature Scheme

The Certificateless Signature (CLS) scheme serves as the foundation for CLAS schemes. To understand CLAS, we first need to delve into CLS. The CLS involves a signature process where Certificateless Public Key Cryptography (CL-PKC) is applied. In this process, a signature for a message is generated using the signer's secret key, employing CL-PKC. The verifier then verifies this signature using the public key and identifier of the signer, along with the public key of the KGC.

CLS is designed for signing individual messages, whereas CLAS is tailored for generating aggregate signatures for multiple messages. In scenarios with multiple senders, each sender produces signatures for their respective messages. This implies that there will be n signatures for n messages, each generated by a different sender. Consequently, during verification, the verifier needs to individually verify n messages, utilizing the public keys of all n senders.

To streamline this verification process, CLAS aggregates these n signatures into a single signature. While the verification process still employs n public keys, it offers the advantage of verifying all n signatures for n messages in a single step. This efficiency helps reduce the computational load involved in verification.

Typically, the CLAS scheme encompasses the following procedures:

- Setup: Performed by KGC to generate required parameters.
- Partial Private Key Extract: Carried out by the KGC to generate partial secret keys.
- SetSecret Value: Performed by signer to produce secret key.

- SetPublic Key: Performed by signer to generate public key.
- CLSign: The signer sign the desired message.
- CLVerify: Individual signature verification is done in this step.
- CLAggregate: Aggregation of the individual signatures is done by aggregator.
- CLAggregate Verify: Finally the verification of the aggregated signature is done by verifier.

4.1 Security Models for Certificateless Aggregate Signature Scheme

In the literature, based on the ability to undermine the security of CLAS schemes, Gong et al. [Gong et al. 2007], put the adversaries into two categories and a third type of adversary is presented by Viet et al. [Viet and Ogata 2015]. Under these adversaries, CLAS schemes should remain invulnerable.

- A_1 Type Or Type I: An adversary cannot acquire the master key of the system, but they have the capability to substitute the public keys of the legitimate signer. Typically, the KGC functions as an adversary of Type A_1.
- A_2 Type Or Type II : An adversary can obtain the master key of the system, but they are unable to alter the public keys of a legitimate signer. Typically, an adversary of Type A_2 is a malicious insider.
- A_3 Type Or Type III: The highly malicious KGC has the capability to collaborate with signers, excluding a specific target signer, and it can also substitute the public keys of signers.

The initial security model was introduced by Zhang et al. [Zhang et al. 2010], along with CLAS scheme. Actually the security model is defined in form of a game with two players a challenger C and an adversary A defined by a probabilistic polynomial-time Turing machine, $A \in \{A_1, A_2\}$. So, A has complete command of the communication channel of all parties. Parties can only respond to queries raised by A and A_1 & A_2 cannot directly interact with each other. In literature several authors, depending on the security requirements, presented different security models [Zhao et al. 2020, Zhan et al. 2020, Shu et al. 2020, Ye et al. 2021].

5 Literature Review

In 2007, Castro et al. [Castro and Dahab 2007] introduced a CLAS Scheme and asserted that, to their knowledge, no signature aggregation scheme had been proposed by any researcher in the field of CL cryptography. The authors extended the standard model of aggregate signature to accommodate certificateless signatures. The first CLAS scheme based on bilinear pairings was introduced by Gong et al. [Gong et al. 2007]. They proposed two schemes (a & b), where the first reduces the computations for the signer and communication cost, but consumes more storage space. On the other hand, their second scheme required less storage but communication cost is greater than first scheme. The security of their schemes was proven under weaker model and rely on intractable mathematical problem CDHP.

In 2008, Zhang et al. [Zhang and Zhang 2008], analyzed security model of Gong et al. [Gong et al. 2007], and point out the shortcomings. Furthermore, Zhang et al. [Zhang and Zhang 2008] introduced a stronger security model and a CLAS scheme, asserting

that the scheme is secure against both Type I and Type II adversaries. In 2009, Zhang and Zhang [Zhang and Zhang 2009] introduced an innovative CLAS scheme based on the CDHP and asserted that their scheme was Existentially Unforgeable Against Adaptive Chosen-Message Attack (EU-ACMA). Zhang and Zhang [Zhang and Zhang 2009] constructed their scheme by building upon the works of Gentry et al. [Gentry and Ramazan 2006] and Zhang et al. [Zhang et al. 2006]. Later, Shim [Shim 2011], launched a coalition attack against Zhang and Zhang [Zhang and Zhang 2009], and developed a defense plan with enhanced security features that included coalition resistance. Shim [Shim 2011], showed that KGC in conjunction with a malicious user is capable of forging schemes given by Zhang and Zhang [Zhang and Zhang 2009]. Viet et al. [Viet and Ogata 2015], also analyzed and broke Zhang et al. [Zhang and Zhang 2009], by introducing a category of adversary named Type III. In this they showed that an attack can be framed as a coalition of malicious KGCs and Signers forging signatures. Further Viet et al. [Viet and Ogata 2015], presented two CLAS schemes and also proved their security against all three types of adversary. Further Kang and Xu [Kang and Xu 2016] conducted a security analysis of Zhang et al. [Zhang and Zhang 2009] and subsequently, they introduced their own CLAS scheme, demonstrating its EU-ACMA security under the CDH assumption. A partial secret key of the signer is combined with the signed message in order to prevent inside forgery attacks.

In 2010, Gong et al. [Gong et al. 2010], proposed two practical CLAS schemes namely CAS-1 and CAS-2. In CAS-1 scheme signature generation process required less computation, so it can be applied in situations a signer has limited computational capability. Scheme CAS-2 could be a suitable choice in situations where storage space is limited, as the length of the aggregate signature remains constant regardless of the number of signers. The security of both the schemes is based on the CDHP and has been shown to be secure under Random Oracle Model (ROM), a security model that was given by Bellare and Rogaway [Bellare and Rogaway]. The CLAS scheme presented by Zhang et al. [Zhang et al. 2010] and security is proven in ROM. As part of their security analysis, the authors claim that their scheme was protected when using CDH assumption and it is EU-ACMA. Following that, Hu et al. [Hu et al. 2010] introduced a secure construction for a CLAS scheme based on pairings, and the security of their scheme was demonstrated, relying on the CDHP. Next, Xiong et al. [Xiong et al. 2011] introduced an efficient CLAS scheme that did not require signers to synchronize their actions, unlike the schemes proposed in [Zhang et al. 2010] and [Zhang and Zhang 2009], which imposed certain synchronization requirements on signers. The weakness of Xiong et al. [Xiong et al. 2011], pointed out by Shen and Sun [Shen et al. 2012]. They demonstrated that in Xiong et al.'s CLAS scheme an adversary of Type I will be able to replace the public key of a signer for an aggregating set $\mathbb{U}$. This will enable him to forge a legitimate signature for a recipient. The Type II adversary knows the master key and can impersonate any identity of an aggregating set $\mathbb{U}$ to produce a genuine aggregate signature.

In the year 2012, Chen et al. [Chen et al. 2012], presented a novel CLAS scheme and they compared computational performance with the schemes given in Gong et al. [Gong et al. 2007] and Zhang and Zhang [Zhang and Zhang 2009]. In the performance analysis of their scheme [Chen et al. 2012], authors claimed that their scheme is more efficient then scheme (b) given in Gong et al. [Gong et al. 2007]. The signature verification can be done efficiently in comparison to Zhang and Zhang [Zhang and Zhang 2009] and scheme (b) of Gong et al. [Gong et al. 2007]. In addition the public keys are smaller than scheme (a) and (b) of [Gong et al. 2007] and the length of signature is equal to the length of signature developed in Zhang and Zhang [Zhang and Zhang 2009]. Lu et al. [Lu et al.

2012] introduced a formal model and presented a corresponding CLAS scheme. Their scheme's security has been established in the ROM, and it offers the advantage of having an aggregate signature length that remains constant regardless of the number of signers involved.

In 2013, Xiong et al. [Xiong et al. 2013] introduced an efficient CLAS scheme characterized by constant pairing computations. The scheme relies on a CDHP in a ROM with a tight reduction and reduces computational complexity for aggregate verification. He et al. [He et al. 2014] also examined the work of Xiong et al. [Xiong et al. 2013] and, through practical attacks, illustrated that an adversary has the ability to create a valid signature for any arbitrary message of their choosing. To attack [Xiong et al. 2013], no secret key of user is required but only knowledge of partial secret key and a genuine signature is sufficient. Further He et al. [He et al. 2014], proposed an improved scheme which resists the attack, by restricting A_2 to get T_i, by making improvements in the signing phase and verification. Yang et al. [Yang et al. 2013], observed that the forged signatures of He et al. [He et al. 2014], are not random and the security advantage of [Xiong et al. 2013], remains valid for Type II adversaries, further Yang et al. [Yang et al. 2013], demonstrated that Xiong et al. [Xiong et al. 2013] is vulnerable to two passive malicious KGC attack methods. Yang et al. [Yang et al. 2013], also claimed that their attack is applicable to He et al. [He et al. 2014], as well and finally proposed an enhanced CLAS scheme. In his paper Aboud [Aboud 2013], also demonstrated that Xiong et al. [Xiong et al. 2013], is vulnerable to an honest-but-curious attack. Next, Tu et al. [Tu et al. 2014] introduced a novel Type II attack on Xiong et al. [Xiong et al. 2013]. This attack allowed an adversary to forge a valid signature for any arbitrary message of their choosing. Zhang et al. [Zhang et al. 2014], find that the conclusion of Xiong et al. [Xiong et al. 2013], was wrong and their scheme was vulnerable to four specific attacks. In the first two attacks, Zhang et al. [Zhang et al. 2014] demonstrated that Xiong et al. [Xiong et al. 2013] is susceptible to universal forgery, both in the case of an honest-but-curious KGC and a malicious-but-passive KGC. In [Zhang et al. 2014], authors showed that in the scheme Xiong et al. [Xiong et al. 2013], it is feasible for the signers to collide and forge signatures, otherwise the signers can collide with a malicious-but-passive KGC and forge signatures. In the analysis part they mentioned that such attacks are practically feasible, so the CLAS scheme should be designed to avoid such attacks. Further Zhang et al. [Zhang et al. 2014], proposed an improved CLAS scheme which results in a short aggregate signature. Next, Chen et al. [Chen et al. 2014], point out that there is equivalence in the flaws of Xiong et al. [Xiong et al. 2013], and standard security definitions associated with CLS and CLAS schemes. Yang et al. [Yang et al. 2015] demonstrated that Xiong et al. [Xiong et al. 2013] is susceptible to attacks by malicious-but-passive KGCs. According to Yang et al. [Yang et al. 2015], a malicious-but-passive KGC can not only impersonate a single entity to create a signature for a message but can also assume any identity to generate a signature for a random message. In addition Yang et al. [Yang et al. 2015], mentioned that their approach of attack is also applicable to the scheme of He et al. [He et al. 2014]. In Chen et al. [Chen et al. 2014], they formalize the flaws as an attack which an adversary of Type II can mount in order to forge the signature. This is done by breaking the scheme of Liu et al. [Liu et al. 2014(a)]. Zhang [Zhang et al. 2016(b)] assessed the security of Chen et al. [Chen et al. 2014] by launching two specific attacks and determined that it was unsuitable for real-time applications, because a legitimate signature can be forged by an adversary for any random message of his choice. Next, Yang et al. [Yang et al. 2018], analyzed Chen et al. [Chen et al. 2014] and showed that these schemes were susceptible to coalition attacks. They pointed out that an adversary is capable of forging a genuine aggregate

signature with the help of individual illegal signatures. Yang et al. [Yang et al. 2018], enhanced a CLAS scheme based on the foundation provided by Chen et al. [Chen et al. 2014]. In their work, Cheng et al. [Cheng et al. 2015], showed that Xiong et al. [Xiong et al. 2013], was vulnerable to even "honest but-curious" KGC attacks. However, they introduced an enhanced scheme that offers protection against "malicious but-passive" KGC attacks in the ROM. The scheme proposed by Xiong et al. [Xiong et al. 2013] was further scrutinized by Chen et al. [Chen et al. 2015(a)], who concluded that the scheme does not hold up to its security claims against Normal Type II adversaries [Shen et al. 2012, He et al. 2014]. Subsequently, Yang et al. [Yang et al. 2018(a)], discovered that the CLAS scheme presented by Cheng et al. [Cheng et al. 2015], was susceptible to coalition attacks from internal signers. Furthermore, Yang et al. [Yang et al. 2018(a)], introduced an enhanced CLAS scheme and demonstrated its existential unforgeability under the CDHP.

Ming et al. [Ming et al. 2014], also proposed a novel design of CLAS scheme with constant length aggregate signature. Zhang et al. [Zhang et al. 2015(a)], analyzed He et al. [He et al. 2014], they also reviewed Ming et al. [Ming et al. 2014], and pointed out that the KGC could mount a passive attack on Ming's CLAS scheme. Building upon the work presented in [Ming et al. 2014], Zhang et al. [Zhang et al. 2015(a)] put forward two enhanced designs for CLAS schemes. Du et al. [Hongzhen and Qiaoyan 2017] identified that Ming et al. [Ming et al. 2014] CLAS scheme was considered insecure due to its vulnerability to malicious KGC attacks, and they presented an alternative CLAS scheme. Further Yang et al. [Yang et al. 2018], analyzed Du et al. [Hongzhen and Qiaoyan 2017] and showed that these schemes were susceptible to coalition attacks. In the work by Luo et al. [Luo et al. 2016], demonstrated that the initial scheme proposed by Zhang et al. [Zhang et al. 2015(a)] was secure against Type I and Type II adversaries. However, the second scheme introduced by Zhang et al. [Zhang et al. 2015(a)] was found to be vulnerable to these types of adversaries. Further modification of the second scheme was proposed.

Liu et al. [Liu et al. 2014(a)], introduced a novel CLAS scheme, which needs short group elements to produce aggregate signature and it also requires constant pairing calculations for aggregate verification, this results increase in efficiency because, it does not relate to the associated number of signers. In their research, Liu et al. [Liu et al. 2014(a)], mentioned that in [Gong et al. 2007, Zhang and Zhang 2009, Chen et al. 2012] and Liu et al. [Liu et al. 2014(b)], the computational cost of pairing is directly proportional to the number of signers, which does not address the entire purpose of aggregate signatures. In order for this scheme Liu et al. [Liu et al. 2014(a)], to be secure, it relies on CDHP, and it involves two constant group elements in creating aggregate signatures. Wang et al. [Wang and Yuan 2015], shown by mounting two concrete attack that CLAS scheme given in Liu et al. [Liu et al. 2014(a)], cannot resist adaptive chosen message attack and hence it cannot attain the security level as per their claim. Next, in their work Deng et al. [Deng et al. 2014], by mounting a concrete attack, demonstrated that Hou et al. [Hou et al. 2013], is insecure. Later, Kumar et al. [Kumar et al. 2016(b)] Observed that the claim of Deng et al. [Deng et al. 2014], was found to be false. Kumar et al. [Kumar et al. 2016(b)] noted that the security of [Deng et al. 2014] is dependent on both the user's private key and a random number selected by the user. However, malicious KGC computed a fixed value and was able to forge the signature without knowing the private key and random number. Another pairing based CLAS scheme was presented by Xiu et al. [Xiu and Da-Ke 2014], the security of their scheme was proven under ROM. In the same year Hou et al. [Hou et al. 2013] and Du et al. [Du et al. 2013] also presented their design of CLAS scheme. In their study, Liu et al. [Liu et al.

2016(a)] conducted a security analysis of by Du et al. [Du et al. 2013] and identified a security flaw in their scheme, specifically that it does not possess the property of unforgeability. Liu et al. [Liu et al. 2016(a)], showed that a malicious KGC is capable of forging a genuine CLAS scheme without knowledge of the secret key of the signer. To resist this kind of forgery attack, Liu et al. [Liu et al. 2016(a)], included an OWHF and this inclusion does not increase the computational cost. Xu et al. [XU et al. 2016], also conducted an analysis of Du et al. [Du et al. 2013] and proposed an improved scheme in their paper. Following that, Zhou et al. [Zhou et al. 2014] introduced an innovative CLAS scheme that incorporates compact full aggregation, which maintains the same size as an individual signature. Additionally, two security models are analyzed in the ROM to protect against malicious KGC and malicious users. According to the authors, the scheme is a combination of EU-ACMA and chosen-identity attacks due to CDHP. Next, Chen et al. [Chen et al. 2016], provided cryptanalysis of [Zhou et al. 2014], and showed that it is vulnerable to a Type-I attack.

Horng et al. [Horng et al. 2015] introduced a CLAS scheme tailored for vehicular sensor networks. The authors additionally asserted that their scheme achieves conditional secrecy preservation by associating each traffic message from a vehicle with a distinct pseudo-identity. In their security analysis, Horng et al. [Horng et al. 2015] demonstrated that their scheme can withstand existential forgery under adaptively chosen message attacks. The security of their scheme is grounded in the CDHP and has been proven in the ROM. Subsequently, Li et al. [Li et al. 2016] demonstrated that Horng et al. [Horng et al. 2015] is susceptible to malicious-but-passive KGC attacks and introduced an improved CLAS scheme to address this vulnerability. Furthermore, Batra et al. [Batra and Malhi 2015], Chen et al. [Chen et al. 2015(b)] and Li et al. [Li et al. 2015], also separately presented their CLAS schemes with pairing computations. The security of their scheme relies on the CDHP problem and has been proven in the ROM. Zhang et al. [Zhang et al. 2015(b)], mount concrete and simple attacks, and demonstrate that in Liu et al. [Liu et al. 2014(b)], a Type II and KGC adversary could create a CLAS scheme through passive attack and malicious attack .

Furthermore, Zhang et al. [Zhang et al. 2016(a)] conducted an analysis of Chen et al. [Chen et al. 2016] and demonstrated that their scheme lacked security as it was vulnerable to both Type I and Type II adversaries. Zhang et al. [Zhang et al. 2016(a)], in addition, pointed out that in [Chen et al. 2016], it is possible to forged a CLS for a random message; they explained the reason for this and offered suggestions to prevent such attacks. Further, Wang et al. [Wang et al. 2016] identified the security vulnerabilities of Chen et al.'s scheme [Chen et al. 2016] against both Type I and Type II adversaries. Additionally, it was demonstrated that due to weaknesses in the underlying basic CLS scheme, the CLAS scheme was unable to attain the necessary level of security. Shen et al. [Shen et al. 2016] demonstrated that Liu et al. [Liu et al. 2014(a)] does not fulfill the unforgeability property, because their scheme it is possible for an adversary to forge a legitimate signature without possessing knowledge of the signer's secret value or partial secret key. Subsequently, Nie et al. [Nie et al. 2016] introduced a novel and efficient CLAS scheme. They provided proof that the scheme satisfied the EU-ACMA property and was resistant to chosen-identity attacks in the ROM, based on the intractability of the CDHP. Next, Pakniat et al. [Pakniat and Noroozi 2016], citing Nie et al. [Nie et al. 2016], scheme was not secure against an adversary of type I. In continuation, Kar [Kar 2016], proposed an efficient and provably secure CLAS of short length and Liu et al. [Liu et al. 2016(b)], presented a novel roaming authentication scheme with anonymity. Tian [Tian 2016] also introduced the design of a CLAS scheme that doesn't rely on bilinear pairing. Furthermore, Deng et al. [Deng et al. 2016] was found to be

insecure by Kumar et al. [Kumar et al. 2017(a)], due to its susceptibility to a collision resistance attack. Additionally, the flaws in Deng et al. [Deng et al. 2016] CLAS scheme are shown by Kumar et al. [Kumar and Sharma 2017]. Kumar et al. [Kumar et al. 2016(a)] conducted a comprehensive review of CLAS schemes.

In 2017, Kang et al. [Kang et al. 2017] introduced a CLAS scheme and demonstrated that their scheme achieved EU-ACMA security. In their paper, Xu et al. [Xu et al. 2018], analyzed Kang et al. [Kang et al. 2017], and found that it was vulnerable to a malicious KGC attack. Next, Zhou et al. [Zhou et al. 2020], analyzed Kang et al. [Kang et al. 2017] and found that it was insecure against the forged signature attack of the adversary of Type II. Subsequently, they introduced a revocable CLAS scheme and asserted that their scheme was the pioneering solution of this nature.

In 2018, Cui et al. [Cui et al. 2018] developed a CLAS scheme using ECC and asserted that their scheme provided conditional privacy preservation. Essentially, Cui et al. [Cui et al. 2018] showcased an application of the CLAS scheme, illustrating secure communication between vehicles and infrastructure in VANETs. Du et al. [Du et al. 2019] highlighted that the CLAS schemes of Cui et al. [Cui et al. 2018] were insecure against Type II adversaries, and the CLAS scheme of Qu et al. [Qu and Mu 2018] was susceptible to forgery by Type I adversaries under the attack of public key replacement. Furthermore, they proposed a CLAS scheme and claimed that their scheme was the first to achieve secure communication in Healthcare Wireless Sensor Networks (HWSN) without using pairings. Kumar et al. [Kumar et al. 2018] devised a CLAS scheme for green HWSNs and established its security in ROM. Following to Kumar et al. [Kumar et al. 2018], Wu et al. [Wu et al. 2018] identified a security vulnerability in their CLAS scheme, where signature forgery was demonstrated as a potential threat. Further they rectified the security flaws and proposed a CLAS scheme, in which security was strengthened with less computation cost. Kamil et al. [Kamil and Ogundoyin 2019(b)], analyzed and demonstrated by mounting concrete attacks that Wu et al. [Wu et al. 2018], were insecure against forgery attack by the Type II adversary. Another study by Kumar et al. [Kumar et al. 2018], demonstrated that the Scheme Malhi and Batra [Batra and Malhi 2015], were insecure against concrete attack “honest but curious”. In their research, Qu et al. [Qu and Mu 2018], introduced the first CLAS scheme that is resistant to bilinear pairings and possesses the characteristics of both aggregate signatures and certificateless cryptography. They also demonstrated that their CLAS scheme was secure against both Type I and Type II adversaries under the DLA in the ROM. The security of their proposed scheme was confirmed by EU-ACMA, based on the intractability of the ECDLP. Du et al. [Du et al. 2019] pointed out that Qu et al. [Qu and Mu 2018] was susceptible to forgery by Type I adversaries under the attack of public key replacement. In 2018, Liu et al. [Liu et al. 2018], introduced an enhanced CLAS scheme designed to handle large-scale concurrent data in the context of Mobile Healthcare Crowd Sensing (MHCS). As part of the scheme, batch verification is applied, which helps with batch health data authentication and privacy protection at the same time. Kamil et al. [Kamil and Ogundoyin 2019(b)], analyzed and demonstrated by mounting concrete attacks that Liu et al. [Liu et al. 2018] were insecure against forgery attack by the Type II adversary.

Kamil and Ogundoyin [Kamil and Ogundoyin 2019(a)], studied Cui et al. [Cui et al. 2018], and demonstrated that it was insecure, further they proposed a new CLAS scheme based on ECC for VANETs. They applied a batch verification process to boost verification and optimize efficiency, and proved the security of the implemented scheme in ROM. Ye et al. [Ye et al. 2021], proved that Kamil and Ogundoyin [Kamil and Ogundoyin 2019(a)] scheme was insecure as two malicious users could collude and forge an aggregate signature. The security of Kamil and Ogundoyin [Kamil and

Ogundoyin 2019(a)], was examined by Xiong et al. [Xiong et al. 2022]. The findings demonstrate that their plan was vulnerable to collusion attacks because it was possible to undermine the comparable validity and further proposed an enhanced CLAS method against collusion attacks for VANETs. It has been demonstrated that the suggested CA-CLAS scheme satisfies the equivalency validity condition of the aggregate signature scheme by enjoying unforgeability in the ROM under ECDLP assumption. Furthermore, Wang et al. [Wang and Teng 2018], developed a CLAS scheme to ensure the security and authentication of information transmission between vehicle nodes in VANETs. The authors also established security in ROM and demonstrated that their CLAS scheme was resilient against adaptive chosen-message attacks. Xiongdong et al. [Xiongdong et al. 2019] revealed vulnerabilities in Wang et al. [Wang and Teng 2018], including susceptibility to three types of forgery attacks: honest-but-curious KGC attacks, malicious KGC and Road Side Unit (RSU) coalition attacks, and internal signers' coalition attacks. In their analysis of CLAS schemes, according to Hu et al. [Hu et al. 2020(d)], the schemes in Xiaodong et al. [Xiongdong et al. 2019], do not possess unforgeability, so it was insecure against forgery by malicious users. Furthermore, the authors introduced an enhanced CLAS scheme designed to withstand all three types of attacks. Hu et al. [Hu et al. 2020(a)], furthered their research on the CLAS scheme based on Wang and Teng [Wang and Teng 2018] and proposed an enhanced CLAS scheme tailored for VANETs. In order to enhance the security level while minimizing computational and communication overhead, Gayathri et al. [Gayathri and Reddy 2018], proposed a CLAS scheme featuring full aggregation. Next, Yang et al. [Yang et al. 2018(b)], identified the security loop holes of Kumar and Sharma [Kumar and Sharma 2018], and they showed that their scheme was vulnerable to coalition attacks and subsequently introduced an improved CLAS scheme designed to withstand such attacks. Liu et al. [Liu et al. 2020], designed and applied an improved CLAS scheme to propose a Monitoring Data Batch Verification (MDBV) scheme for internet vehicles. Deng et al. [Deng et al. 2018], presented the first CLAS scheme that incorporated RSA and DLP, and their scheme had provable security in ROM, so it was less computationally costly than bilinear pairing schemes.

According to Xie et al. [Xie et al. 2019], the CLAS scheme Kumar et al. [Kumar et al. 2018], was easily forgeable and did not even provide the necessary privacy protections. Further, Zhan et al. [Zhan and Wang 2019], dismissed the claim of Kumar et al. [Kumar et al. 2018]. Kamil et al. [Kamil and Ogundoyin 2019(b)], analyzed Xie et al. [Xie et al. 2019], and demonstrated by mounting concrete attacks that the said scheme was insecure against forgery attack by the Type II adversary. Next, Gayathri et al. [Gayathri et al. 2019], to ensure secrecy and safety of medical data proposed a CLAS scheme without pairing. Shim [Shim 2020(a)], demonstrated that Gayathri et al. [Gayathri et al. 2019], cannot resist universal forgery attack hence it was insecure. However, Yang et al. [Yang et al. 2020], demonstrated that Gayathri et al. [Gayathri et al. 2019], scheme was vulnerable to insider attacks, allowing for universal forgery. In their work, Liu et al. [Liu et al. 2020], conducted a comprehensive review of Gayathri et al. [Gayathri et al. 2019] identified vulnerabilities of type I and type II adversaries in the scheme and proposed an enhanced scheme that provides provable security under the ROM. Zhan et al. [Zhan et al. 2020], analyzed Liu et al. [Liu et al. 2020], and demonstrated its vulnerability to attack. Zhan et al. [Zhan et al. 2020], asserted that their enhanced scheme effectively thwarted attacks from both Type I and Type II adversaries. Yang et al. [Yang et al. 2020], further showed, via concrete attacks, that Liu et al. [Liu et al. 2020] scheme was insecure and proposed an enhanced version to address the identified vulnerabilities. Zhou and Yin et al. [Zhou & Yin 2022], discovered that the proposed by Zhan et al. [Zhan

et al. 2020] is not resistant to malicious MSN_i attacks. Meanwhile, [Zhou & Yin 2022] demonstrated the reason that malicious MSN_i assaults may be launched against this method. It is clear that Zhan et al.'s plan is unable to ensure patient confidentiality and the safe transfer of medical information. Further, Zhou and Yin et al. [Zhou & Yin 2022], provided fixes for the problem and built a better PF-CLAS scheme that could provide provable security. Next Yang et al. [Yang et al. 2023], offered a cryptographic study of the ZH-CLAS scheme [Zhan et al. 2020], in their article using two different kinds of practical attack techniques. The findings showed that the scheme designed in Zhan et al. [Zhan et al. 2020], was vulnerable to coalition assaults from malevolent sensor nodes as well as public key replacement attacks and further, Yang et al. [Yang et al. 2023], proposed a security-enhanced CLAS scheme to address security flaws of [Zhan et al. 2020]. Next, Qiao et al. [Qiao et al. 2023], review the security of Gayathri et al. [Gayathri et al. 2019] scheme and demonstrate that the scheme was unsecure. Furthermore, Qiao et al. demonstrated that the attack strategies put forth by Liu et al. [Liu et al. 2020] are false, and the enhanced CLAS schemes created by Liu et al. [Liu et al. 2020] and Zhan et al. [Zhan et al. 2020], are unable to maintain the security they purport to. Lastly, a new, more secure CLAS strategy is introduced, and the security rely on the intractability of DLP. Deng et al. [Deng et al. 2019], also developed a CLAS scheme that required less computation than the existing CLAS schemes and was suitable for mobile devices. Kamil et al. [Kamil and Ogundoyin 2019(b)], analyzed and demonstrated by mounting concrete attacks that Xie et al. [Xie et al. 2019] were insecure against forgery attack by the Type II adversary. A CLAS scheme developed by Kumar et al. [Kumar et al. 2019], for VANET's which was resistant to adaptive chosen-message attacks. Next, Hashimoto and Ogata [Hashimoto and Ogata 2019] introduced the first design of an unrestricted and compact CLAS scheme with a constant-size aggregate signature. In Shim [Shim 2020(b)], it was revealed that Hashimoto and Ogata [Hashimoto and Ogata 2019], was insecure against super-type I attacks. In this case, the adversary has knowledge of the user's private key. By replacing the public key with the private key, he can generate a legitimate CLS for a random message of his choosing. However, the attacker must possess knowledge of the partial private key corresponding to the master secret. Zhong et al. [Zhong et al. 2019], observed that the most difficult challenge in VANETs was assuming an ideal Tamper-Proof Device (TPD) and optimizing computational and communication costs. In an effort to address these challenges, Zhong et al. [Zhong et al. 2019] introduced a privacy-preserving authentication scheme with full aggregation for VANETs. Cui et al. [Cui et al. 2020], analyzed Zhong et al. [Zhong et al. 2019] and found that their scheme was not secure against attacks by adversaries of type II. Furthermore, in response to the security vulnerabilities identified in the scheme by Zhong et al. [Zhong et al. 2019], Cui et al. [Cui et al. 2020], introduced a CLAS scheme that maintains a constant length and does not rely on bilinear pairings. They also claimed that the proposed scheme was secured against adversaries of Type I and Type II. Further, Kamil et al. [Kamil and Ogundoyin 2020], first pointed out the flaws of Zhong et al. [Zhong et al. 2019], then proposed an improved approach with full aggregation for VANET. The authors also provided a proof of security for their scheme in the ROM against both Type I and Type II adversaries. Trinh [Trinh 2019] introduced the initial multisignature variant of the CLAS scheme, featuring a constant size, and demonstrated its security in the standard model under an extended Diffie-Hellman exponent assumption. Their scheme was only compromised by the fact that the signature was produced with the help of the authority. Li et al. [Li et al. 2019] harnessed online/offline CLAS schemes without the need for pairings and employed a map-to-hash function to construct an efficient conditional privacy-preserving authentication scheme, effectively mitigating the security

and privacy concerns in VANETs. Liu and You [Liu and You 2019], put forward a CLAS scheme with high efficiency and proven security in ROM. The past security models did not explicitly address coalition attacks, to address this issue the study of Shen et al. [Shen et al. 2019] provide a new certificateless scheme with a designated verifier together with a redesigned security model.

To address the issues of secure routing and authentication in resource-constrained VANETs, Xu et al. [Xu et al. 2020(a)], devised a CLAS scheme. They contended that their scheme was provably secure, capable of withstanding various types of attacks, and boasted computational efficiency superior to existing schemes. Benil et al. [Benil and Jasper 2020], using blockchain technology ECC, developed a CLAS scheme to ensure the security of medical data. Nex, Zhao et al. [Zhao et al. 2020] introduced an advanced and efficient CLAS scheme based on ECC with security prove under ROM. Specially, Wu et al. [Wu et al. 2020], presented a fully chosen-key attack and argued that in traditional models for providing CLAS security, such an attack wasn't considered. Next, Lee et al. [Lee et al. 2020], designed a CL Aggregate Arbitrated Signature (CLAAS) scheme based on ECC for IoT. The proposed design is resilient against threats like public key replacement attacks and malicious KGC attacks. Xu et al. [Xu and Zeng 2021], demonstrated that Lee et al. [Lee et al. 2020], was not secure against a Type I adversary, contrary to its claimed security, as a Type I adversary could replace the user's public key and engage in forgery. Ma et al. [Ma et al. 2020], introduced a variant of the CLAS scheme with the designated verifier property, building upon the work of Chen et al. [Chen et al. 2015(b)]. However, Hu et al. [Hu et al. 2020(b)], conducted an analysis of Ma et al. [Ma et al. 2020] and identified that their scheme lacks the unforgeability property. Hu et al. [Hu et al. 2020(c)], in their other work pointed out that the CLAS schemes given in [Liu and You 2019] and [Zhao et al. 2020(a)], were insecure against an attack mounted by a malicious user. Further, Hu et al. [Hu et al. 2020(c)], proposed an improved secure scheme against such attacks. According to Hu et al. [Hu et al. 2020(d)], the scheme Hua [Hua 2020], do not possess unforgeability, as it was insecure against forgery by malicious users. Further Hu et al. [Hu et al. 2020(d)], constructed a CLAS with improvements which was secure against said attacks. Hu et al. [Hu et al. 2020(e)], conducted an analysis of Cao et al. [Cao et al. 2019] and provided evidence that their scheme was vulnerable to two distinct types of attacks. In a related development, Shu et al. [Shu et al. 2020], introduced a CLAS scheme tailored for a blockchain-based Medical Cyber-Physical System (MCPS) without relying on bilinear pairings. The authors claimed that their scheme preserved identity privacy while ensuring proper message authentication. The scheme was based on ECC and therefore it was efficient than existing schemes. Thumbur et al. [Thumbur et al. 2020], introduced a pairing-free CLAS scheme tailored for VANETs, emphasizing its enhanced security and efficiency compared to existing schemes. Yang et al. [Yang et al. 2022], examine the scheme given in [Thumbur et al. 2020] and discover that it is vulnerable to coalition and public key replacement attacks. Further, improved scheme given in [Yang et al. 2022] and additionally, the analysis's findings show that the enhanced plan satisfies a number of security standards. Xu et al. [Xu et al. 2020(b)], suggested a more effective and secure certificateless aggregate signature authentication mechanism that is ideal for V2I communication in In VANETs, which can prevent the information injection attack in the signature aggregation phase. In their article Deng et al. [Deng et al. 2020] constructed a new CLS scheme and derived a new CLAS scheme using the newly developed CLS scheme. The schemes are secured due to CDHP and unforgeable against Type I/II adversaries in an Standard model. Next, Mei et al. [Mei et al. 2021], described an effective CLAS scheme with conditional privacy preservation that can withstand both

the malicious-but-passive KGC and external attacker attacks and proved security in the ROM, further the security justification is provided under the CDH assumption. Liang and Liu [Liang & Liu 2023], examine the security of Mei et al. [Mei et al. 2021] and draw attention to the fact that Mei et al. [Mei et al. 2021], was vulnerable to forgeries and suggest an enhanced plan to resolve the security flaw. According to the security analysis, Liang and Liu [Liang & Liu 2023] satisfies certain security requirements in VANETs and is secure against Type I and Type II adversaries in the ROM.

In 2021, Deng et al. [Deng 2021], introduced a system model and security properties for the CL designated verifiable anonymous aggregate signature scheme. They also presented a specific construction of this scheme and provided security proofs to support its effectiveness. Furthermore, Xu et al. [Xu and Zeng 2021], also noted that the scheme proposed by Addobea et al. [Addobea et al. 2020], did not uphold its security properties. Vallent et al. [Vallent et al. 2021], introduced an efficient CLAS scheme for VANET based on elliptic curves, which incorporates conditional privacy preservation. They established the security of their proposed scheme in the ROM. In a separate development, Tiwari and Gangadharan [Tiwari and Gangadharan 2021], proposed a novel hierarchical CLAS scheme to establish a scalable authentication model for Software as a Service (SaaS) in cloud computing. Their scheme's security was validated under ROM and relied on the CDHP and DDHP. Next, Kar et al. [Kar et al. 2021], introduced a CLAS scheme(CL-ASS) tailored for WSNs. Further authors analyzed security of their scheme under ROM, assuming the computational hardness of CDHP.

In 2022, Khan and colleagues [Khan et al. 2022], proposed a version of CLAS based on Hyper Elliptic Curve Cryptography (HECC). In a security analysis of their scheme, the authors show that it protects against malicious entities attempting to forge authentication requests and responses. Wang et al. [Wangw et al. 2022(b)], proposed a lightweight CLAS architecture with revocation mechanism for 5G-enabled vehicle networks. The suggested scheme for internet of vehicle by Zhu et al. [Zhu et al. 2022], concealed the names of the vehicles by using pseudonymous identities, and a reliable authority could track down the malevolent vehicles after the incident. Security proof demonstrates that the suggested approach meets authentication and integrity under the ROM, assuming the ECDLP. Han et al. [Han et al. 2022], suggested a eCLAS scheme based on the ECDLP hardness assumption and secure against both type I and type II attackers. Zheng et al. [Zheng et al. 2023], examined and assessed Han et al. [Han et al. 2022], and found that that a malevolent network participant can still exploit their technique by offering a specific example of an attack. Further authors addressed the security vulnerabilities by proposing updated security technique, EUF-CMA in the ROM. In order to enhance security and privacy in VANET, Cahyadi et al. [Cahyadi et al. 2022], put out a CLAS scheme, with efficiency taking center stage. Chen and Chen [Chen & Chen 2022] developed a fully aggregated, effective CLAS strategy for VANETs, their CPP-CLAS scheme achieves vehicle anonymity, traceability, and unlinkability in addition to message authenticity, integrity, and nonrepudiation through the use of ECC. Additionally, authors demonstrated that, under the ROM, the CPP-CLAS scheme is existentially unforgeable against adversaries of Types I and II.

In the year 2023, Tomar et al.[Tomar et al. 2023], uses a certificateless methodology and suggests a blockchain-based CLAS technique that offers privacy, integrity, and authenticity in the context of the suggested smart grid. Nevertheless, many of the earlier proposed CLAS protocols for VANET do not allow for an effective means of validating the legitimacy of the public keys of the cars. Because of this, a malicious key generation center (KGC) can produce authentic signatures by disguising itself as any kind of vehicle, as a solution to this issue Li et al. [Li et al. 2023], proposes RelCLAS, a trustworthy

malicious KGC-resistant CLAS protocol. RelCLAS uses a mix of CLAS and registration-based encryption (RBE) to overcome the key escrow problem. A novel system (PCAS) for vehicle authentication on VANETs and address the shortcomings of the aggregation signature scheme developed by Gong et al. [Gong et al. 2023], which is an improvement of Liu et al [Liu et al. 2020]. According to security proof analysis, PCAS in the ROM is impervious to adaptive chosen message assaults. In their work Guo et al. [Guo et al. 2023], proposed a dynamic revocation mechanism for VANETs along with a CLAS. Shim [Shim 2023], showed that Wang et al. [Wangw et al. 2022(a)] scheme was insecure against the malicious-but-passive attacks. Further, Yuan et al. [Yuan et al. 2023], conduct a security evaluation of Wang et al. [Wangw et al. 2022(a)] scheme, emphasizing its conditional privacy-preserving in VANETs. Yuan et al. [Yuan et al. 2023], demonstrated that the technique was susceptible to both public key replacement and KGC attacks and further, offered an improved CLAS scheme that addresses the security problems. Iqbal et al. [Iqbal et al. 2023], used the HECC for their CLAS scheme. Authors also conduct a verifiable security analysis using the ROM, which was based on the DLP of the hyperelliptic curve, further they demonstrated that the suggested scheme is impervious to both Type 1 (FGR1) and Type 2 (FGR2) forgers. The security of Chen et al. [Chen & Chen 2021] proposed CLAS system for VANETs is examined Xu et al. [Xu et al. 2023]. Based on underwater sound communication, Xu and Li [Xu & Li 2023], suggested an NTRU certificateless aggregate signature approach. Consequently, signatures Replay attacks are intended to be avoided by employing time-stamps and ocean noise polynomials. The outcomes demonstrated that the scheme given by Xu and Li [Xu & Li 2023], had a reduced signature length and offers clear benefits in terms of communication and processing efficiency.

Recently in 2024, Gritti [Gritti 2024] introduced Organizational CLAS (OASIS), for IoT that mitigates the challenging PKI certification management with an organizational architecture based on two tiers. In their study, Park and Koo [Park & Koo 2024], demonstrated that Wang et al. [Wangw et al. 2022(a)] and its upgraded scheme, which applies Shim's [Shim 2023] countermeasure, are vulnerable to forgery attacks. Authors also suggests that Wang et al. [Wangw et al. 2022(a)], scheme can be improved by using other secure pairing-free CLAS schemes.

We made an attempt to include the contributions made by researchers to the development of the CLAS scheme and their applications to real-life situations. The researchers designed several schemes based on the different mathematical tools, security models also discussed security strength along with computational analysis of the proposed schemes.

6 Comparative Analysis

In this section, we conducted an analysis of the existing CLAS schemes and offer our insights regarding their computational complexity. Further, we present a comprehensive comparison that encompasses the methodologies utilized, the intractable mathematical problems involved, security models and the current security status of these CLAS schemes.

6.1 Computational Complexity Analysis

First, we go through the notations and their descriptions for the time consuming cryptographic mathematical operations that are used to create CLAS schemes which are shown in the Table (1).

Notation	Description
T_{bp}	The time taken to perform a bilinear pairing operation.
$T_{bp(m)}$	The time required to complete a scalar multiplication operation within a pairing.
$T_{bp(a)}$	The time needed to perform a point addition operation in the context of bilinear pairing.
T_{sm}	The time required to perform a scalar multiplication operation.
T_a	The time needed to perform an addition operation.
$T_{h(mtp)}$	The time required to perform a Map to Point hash operation.
T_h	The time it takes to execute a one-way hash function operation.
$T_{E(m)}$	The time needed to perform elliptic curve point scalar multiplication.
$T_{E(a)}$	The time needed to calculate the addition of elliptic curve points.
T_{exp}	Time required for exponentiation operation.
T_{pm}	The time required for one vector modulo multiplication operation
T_{pa}	The time required for one vector modulo addition operation
$T_{he(m)}$	The time needed to perform scalar multiplication of hyperelliptic curve.

Table 1: Notations Used for CLAS Scheme Mathematical Operation

This section compares the compute execution times of the CLAS and its applications for the different popular time-consuming cryptographic operations, which are compiled in Table (2). One of the obvious fact is that pairing-free CLAS schemes outperform systems that require pairing in terms of computation performance. We examine the computational cost needed to construct a single signature and verify an aggregate signature in the Table (2).

S. N.	Scheme	Individual Signature	Aggregate Signature Verification
1	Gong et al. [Gong et al. 2023]	$T_{E(m)} + 3T_{h(mtp)}$	$(2n+1)T_{E(m)} + 2nT_{E(a)} + 2nT_{h(mtp)}$
2	Guo et al. [Guo et al. 2023]	$T_{E(m)}$	$(2n-1)T_{E(m)}$
3	Iqbal et al. [Iqbal et al. 2023]	$2T_{he(m)}$	$101T_{sm} + 199T_a + 100T_h$
4	Li et al. [Li et al. 2023]	$T_{E(m)} + T_h$	$(2n+2)T_{E(m)} + 3nT_{E(a)} + 3nT_h$
5	Liang and Liu [Liang & Liu 2023]	$4T_{e(m)} + 3T_{h(mtp)}$	$4T_{bp(m)} + 2nT_{e(m)} + 2nT_{h(mtp)}$
6	Qiao et al. [Qiao et al. 2023]	$T_{sm} + T_h$	$(2n+1)T_{sm} + (3n+1)T_a + 2nT_h$
7	Tomar et al. [Tomar et al. 2023]	$T_{E(m)} + T_h$	$(n+1)T_{E(m)} + nT_h + (2n+1)T_{E(a)}$
8	Xu et al. [Xu et al. 2023]	$T_{E(m)}$	$(2n+2)T_{E(m)} + (2n+2)T_{E(a)}$
9	Xu et al [Xu & Li 2023]	$5T_{pm} + 5T_{pa} + 2T_h$	$(n+1)T_{pm} + (n+1)T_h$
10	Yang et al. [Yang et al. 2023]	$T_m + 3T_h$	$3nT_m + (3n-1)T_a + (3n+1)T_h$
11	Yuan et al. [Yuan et al. 2023]	$2T_{sm} + 2T_h$	$2T_{bp} + 3nT_{sm} + 3nT_h$
12	Zheng et al. [Zheng et al. 2023]	$T_{sm} + 2T_h$	$300T_{sm} + 301T_a + 300T_h$
13	Chayadi et al. [Cahyadi et al. 2022]	$3T_{bp(m)}$	$3T_{bp} + 2nT_{bp(m)}$
14	Han et al. [Han et al. 2022]	$T_{sm} + T_h$	$101T_{sm} + 199T_a + 100T_h$
15	Wang et al. [Wangw et al. 2022(a)]	$T_{bp(a)} + 3T_{h(mtp)}$	$2nT_{bp(m)} + 3nT_{bp(a)} + 2T_{bp}$
16	Wang et al. [Wangw et al. 2022(b)]	$T_{E(m)}$	$2T_{E(m)} + 2T_{E(a)}$
17	Xiong et al. [Xiong et al. 2022]	$2T_{E(m)} + 2T_h$	$(n+1)T_{E(m)} + (n+1)T_h$
18	Yang et al. [Yang et al. 2022]	$T_{E(m)}$	$4nT_{E(m)} + 3nT_{E(a)}$
19	Zhou et al. [Zhou & Yin 2022]	$T_{E(m)}$	$(2n+1)T_{E(m)} + +(4n-1)T_{E(a)}$
20	Zhu et al. [Zhu et al. 2022]	$T_{E(m)}$	$(2n+1)T_{E(m)} + (4n-1)T_{E(a)}$
21	Chen et al. [Chen & Chen 2021]	$T_{E(m)} + T_h$	$(2n+1)T_{E(m)} + 2nT_h + 2nT_{E(a)}$
22	Deng et al. [Deng 2021]	$T_{sm} + 2T_a + 2T_h$	$2nT_{sm} + (3n-2)T_a + (3n+1)T_h$
23	Kar et al. [Kar et al. 2021]	$T_{E(m)} + T_h$	$(2n+1)T_{E(m)} + 2nT_h + 2nT_{E(a)}$
24	Mei et al. [Mei et al. 2021]	$T_m + 2T_{h(mtp)}$	$4T_{bp} + 2nT_m$
25	Tiwari et al. [Tiwari and Gangadharan 2021]	$3T_{E(m)} + 4T_{E(a)} + T_h$	$(n+2)T_{bp} + 2T_{E(m)} + T_h$
26	Vallent et al. [Vallent et al. 2021]	$2T_{sm} + T_h$	$(2n-1)T_{sm} + 3T_a + 2nT_h$
27	Ye et al. [Ye et al. 2021]	$T_{E(m)} + T_h$	$(n+1)T_{E(m)} + 2T_{E(a)} + 2nT_h$
28	Addobea et al. [Addobea et al. 2020]	$T_{sm} + T_h$	$2T_{bp} + 2T_{bp(m)} + T_{bp(a)} + T_{exp} + T_h$
29	Benil et al. [Benil and Jasper 2020]	$3T_{E(m)} + T_{sm} + 3T_h$	$+3T_{bp}+(2n+1)T_{bp(m)}+2nT_{bp(a)}+(3n+1)T_h$
30	Hu et al. [Hu et al. 2020(a)]	$3nT_{bp(m)} + 3T_{sm} + 4T_h$	$2T_{bp(a)} + 5nT_h$
31	Hu et al. [Hu et al. 2020(b)]	$4T_{sm} + 2T_a + 2T_{h(mtp)} + 2T_h$	$4T_{bp} + 3nT_{bp(m)} + 3nT_{bp(a)} + T_{exp} + (n+2)T_{h(mtp)} + 2nT_h$
32	Hu et al. [Hu et al. 2020(c)]	$4T_{sm} + T_a + 3T_{h(mtp)}$	$2T_{bp} + 2nT_{bp(m)} + T_{bp(a)} + 3nT_{h(mtp)}$
33	Hu et al. [Hu et al. 2020(e)]	$T_{sm} + 2T_a + 2T_h$	$2nT_{sm} + (3n-2)T_a + 2nT_h$
34	Kamil et al. [Kamil and Ogundoyin 2020]	$3T_{bp(m)} + T_a + 2T_h$	$3T_{bp}+2nT_{bp(m)}+(2n-1)T_{bp(a)}+nT_{h(mtp)}+nT_h$
35	Lee et al. [Lee et al. 2020]	$2T_{sm} + 2T_a + T_h$	$(n+1)T_{sm} + (2n+3)T_a + (n+1)T_h$
36	Cui et al. [Cui et al. 2020]	$T_{sm} + 2T_a + 3T_h$	$(n+2)T_{sm} + 3nT_h$
37	Liu et al. [Liu et al. 2020]	$2T_{sm} + 3T_h$	$2nT_{sm} + 3nT_h$
38	Shu et al. [Shu et al. 2020]	$T_{E(m)} + 3T_h$	$(2n+1)T_{E(m)} + (2n+1)T_{E(a)} + 2nT_{h(mtp)}$
39	Thumbur et al. [Thumbur et al. 2020]	$2T_{sm} + 2T_h$	$(2n+1)T_{sm} + (3n-1)T_{bp(a)} + 2nT_h$
40	Wu et al. [Wu et al. 2020]	$4T_{sm} + T_h$	$(2n+3)T_{bp} + 2nT_{bp(m)} + nT_h$
41	Xu et al. [Xu et al. 2020(a)]	$2T_{bp(m)} + 3T_{bp(a)} + T_{h(mtp)} + 2T_h$	$3T_{bp} + 2nT_{bp(m)} + (3n-2)T_{bp(a)} + (n+1)T_{h(mtp)} + 2nT_h$

S. N.	Scheme	Individual Signature	Aggregate Signature Verification
42	Yang et al. [Yang et al. 2020]	$T_{sm} + 2T_h + 2Ta$	$3nT_h + 4nT_{sm} + 3Ta$
43	Zhan et al. [Zhan et al. 2020]	$T_{E(m)} + 2T_{h(mtp)}$	$(3n+1)T_{E(m)} + (4n-1)T_{E(a)} + 3nT_{h(mtp)}$
44	Zhao et al. [Zhao et al. 2020]	$T_{E(m)} + 2T_a + 2T_h$	$(n+2)T_{E(m)} + (n+3)T_{E(a)} + nT_h$
45	Zhao e al. [Zhao et al. 2020(a)]	$2T_{E(m)} + 2T_{E(a)} + 2T_h$	$(4n+2)T_{em} + (4n+3)T_{E(a)} + +2nT_{h(mtp)}$
46	Zhou et al. [Zhou et al. 2020]	$4T_{sm}+2T_a+2T_{h(mtp)}+T_h$	$4T_{bp} + nT_{bp(m)} + 2(n-1)T_{bp(a)} + 2(n+1)T_{h(mtp)} + nT_h$
47	Cao et al. [Cao et al. 2019]	$T_{sm} + 2T_a + T_h$	$T_{sm} + (3n-2)T_a + T_h$
48	Deng et al. [Deng et al. 2019]	$T_{sm} + +3T_a + T_{h(mtp)} + 2T_h$	$2T_{bp} + nT_{sm} + 5nT_a + T_{h(mtp)} + 3nT_h$
49	Du et al. [Du et al. 2019]	$3T_{sm} + 2T_a + 2T_{h(mtp)}$	$(3n+1)T_{sm} + (3n-1)T_a + 3nT_h$
50	Gayathri et al. [Gayathri et al. 2019]	$2T_{sm} + 3T_a + 3T_h$	$(2n+1)T_{sm} + (2n+1)T_a + 2nT_h$
51	Hashimoto et al. [Hashimoto and Ogata 2019]	$3T_{sm} + 2T_a + 2T_{h(mtp)}$	$(n+3)T_{bp} + (n-1)T_{bp(a)} + (2n+1)T_{h(mtp)}$
52	Kamil et al [Kamil and Ogundoyin 2019(a)]	$3T_{E(m)} + 2T_{E(a)} + 3T_h$	$2nT_{E(m)} + nT_{E(a)} + nT_h$
53	Kamil et al. [Kamil and Ogundoyin 2019(b)]	$T_{sm} + T_a + T_h$	$2T_{sm} + 2T_a + 2nT_h$
54	Kumar et al. [Kumar et al. 2019]	$4T_{sm}+2T_a+T_{h(mtp)}+2T_h$	$4T_{bp} + 3nT_{bp(m)} + 2nT_{h(mtp)} + nT_{h(mtp)} + 3nT_h$
55	Li et al. [Li et al. 2019]	$T_{E(m)} + T_h$	$(n+2)T_{E(m)} + 3nT_{E(a)} + 2nT_h$
56	Shen et al. [Shen et al. 2019]	$3T_{sm}$	$(2n+1)T_{bp} + 2nT_{bp(m)}+T_{exp}$
57	Trinh [Trinh 2019]	$(2n+9)T_{exp} + (2n+1)T_h$	$(n+1)T_{exp} + 3T_{bp} + (2n+1)T_h$
58	Xie et al. [Xie et al. 2019]	$T_{sm} + 2T_a + 2T_h$	$(2n+5)T_{bp(m)} + 3nT_{bp(a)} + (3n+1)T_h$
59	Zhong et al. [Zhong et al. 2019]	$3T_{sm} + T_a + T_h$	$3T_{bp}+2nT_{bp(m)}+(2n-1)T_{bp(a)}+nT_{h(mtp)}+nT_h$
60	Cui et al. [Cui et al. 2018]	$T_{sm} + T_a + T_h$	$(n+2)T_{bp} + nT_{bp(m)} + nT_{bp(a)} + 2nT_{h(mtp)}$
61	Deng et al. [Deng et al. 2018]	$3T_{sm} + T_a + +2T_{exp} + T_{h(mtp)}$	$(2n+1)T_{sm} + 2nT_a + nT_{exp} + nT_{h(mtp)}$
62	Gayathri et al. [Gayathri and Reddy 2018]	$4T_{sm} + 2T_a + 2T_{h(mtp)} + 2T_h$	$4T_{bp} + 3nT_{bp(m)} + (4n-3)T_{bp(a)} + (2n+1)T_{h(mtp)} + 2nT_h$
63	Li et al. [Li et al. 2018]	$4T_{bp(m)} + 3T_{bp(a)} + 3T_{h(mtp)} + 2T_h$	$3T_{bp} + 2nT_{bp(m)} + (4n-2)T_{bp(a)} + (n+1)T_{h(mtp)} + 2nT_h$
64	Liu et al. [Liu et al. 2018]	$2T_{sm} + T_a + T_h$	$2T_{bp} + T_{bp(a)} + nT_{h(mtp)} + nT_h$
65	Liu et al. [Liu et al. 2020]	$3T_{sm}+2T_a+T_{h(mtp)}+2T_h$	$3T_{bp} + 2nT_{bp(m)} + (2n-1)T_{bp(a)} + (n+1)T_{h(mtp)} + 2nT_h$
66	Kumar et al. [Kumar et al. 2018]	$3T_{bp(m)} + 2T_{bp(a)} + T_{h(mtp)} + T_h$	$3T_{bp} + nT_{bp(m)} + (3n-1)T_{bp(a)} + (n+1)T_{h(mtp)} + nT_h$
67	Pankaj et al. [Kumar and Sharma 2018]	$4T_{sm} + 2T_h$	$3nT_{bp} + 3nT_h$
68	Qu et al. [Qu and Mu 2018]	$3T_{E(a)} + 2T_{E(m)} + T_h$	$(4n+1)T_{E(a)} + (2n+1)T_{E(m)} + nT_h$
69	Wang et al. [Wang and Teng 2018]	$4T_{sm} + 2T_a + T_h$	$3T_{bp} + nT_{bp(a)} + 3nT_{bp(m)} + 2nT_h$
70	Wu et al. [Wu et al. 2018]	$4T_{sm} + T_{h(mtp)} + 3T_h$	$3T_{bp}+2nT_{bp(m)}+2nT_{bp(a)}+(n+1)T_{h(mtp)}+2nT_h$
71	Xu et al. [Xu et al. 2018]	$4T_{sm}+2T_a+T_{h(mtp)}+2T_h$	$3T_{bp} + (n+1)T_{bp(m)} + (n-1)T_{bp(a)} + (n+1)T_{h(mtp)} + 2nT_h$
72	Yang et al. [Yang et al. 2018]	$4T_{exp} + 2T_h + 2T_{h(mtp)}$	$3nT_{bp} + 2nT_{h(mtp)} + 2nT_h$
73	Yang et al. [Yang et al. 2018(a)]	$T_{exp} + 2T_{(mtp)}$	$2nT_{bp} + (2n+1)T_h$
74	Du et al. [Hongzhen and Qiaoyan 2017]	$4T_{sm}$	$(n+3)T_{bp} + nT_{sm}$
75(i)	Fan et al. [Fan and Wang 2017]	$2T_{sm} + 2T_a + T_{h(mtp)}$	$3T_{bp} + 2nT_{bp(m)} + (2n-1)T_{bp(a)} + nT_{h(mtp)}$
75(ii)	Fan et al. [Fan and Wang 2017]	$2T_{sm} + 2T_a + T_{h(mtp)}$	$4T_{bp} + 2nT_{bp(m)} + 3(n-1)T_{bp(a)} + nT_{h(mtp)}$
76	Kang et al. [Kang et al. 2017]	$4T_{sm}+2T_a+2T_{h(mtp)}+T_h$	$4T_{bp} + nT_{bp(m)} + 3(n-1)T_{bp(a)} + (n+2)T_{h(mtp)} + nT_h$
77	Chen et al. [Chen et al. 2016]	$3T_{sm}+2T_a+T_{h(mtp)}+2T_h$	$(n+3)T_{bp} + 2nT_{bp(a)} + (n-1)T_{bp(m)} + nT_{h(mtp)} + (n+1)T_h$

S. N.	Scheme	Individual Signature	Aggregate Signature Verification
78	Deng et al. [Deng et al. 2016]	$4T_{sm}+3T_a+T_{h(mtp)}+3T_h$	$3T_{bp}+3nT_{bp(m)}+2nT_{bp(a)}+(n+1)T_{h(mtp)}+3nT_h$
79	Kang et al. [Kang and Xu 2016]	$4T_{sm}+2T_a+2T_{h(mtp)}+T_h$	$(n+3)T_{bp}+2nT_{bp(m)}+(3n+1)T_{bp(a)}+3nT_{h(mtp)}+T_h$
80	Kar [Kar 2016]	$4T_{sm}+3T_a+T_{h(mtp)}+3T_h$	$3T_{bp}+(3n-1)T_{bp(a)}+(2n+1)T_{h(mtp)}+3nT_h$
81	Li et al. [Li et al. 2016]	$2T_{bp(m)}+T_{bp(a)}+T_{h(mtp)}+T_h$	$3T_{bp}+nT_{bp(m)}+2nT_{h(mtp)}+nT_{bp(a)}+nT_h$
82	Liu et al. [Liu et al. 2016(a)]	$3T_{sm}+2T_{bp(a)}$	$4T_{bp}+2(n-1)T_{bp(a)}+2nT_{bp(m)}$
83	Liu et al. [Liu et al. 2016(b)]	$4T_{bp(m)}+2T_a+T_{h(mtp)}+T_h$	$3T_{bp}+2nT_{sm}+(n+1)T_{h(mtp)}+nT_h$
84	Nie et al. [Nie et al. 2016]	$3T_{sm}+2T_a+2T_{h(mtp)}+nT_h$	$4T_{bp}+2nT_{sm}+(3n-2)T_{bp(a)}+2T_{h(mtp)}+nT_h$
85	Tian [Tian 2016]	$T_{exp}+2T_a+T_h$	$2nT_{exp}+(n-1)T_{sm}$
86	Xu et al [XU et al. 2016]	$3T_{sm}+2T_a+T_{h(mtp)}+T_h$	$2T_{bp}+2T_{bp(m)}+(4n-1)T_{bp(a)}+T_{h(mtp)}+nT_h$
87	Batra et al. [Batra and Malhi 2015]	$4T_{sm}+2T_a+T_h$	$3T_{bp}+3nT_{bp(m)}+nT_{bp(a)}+2nT_h$
88	Chen et al. [Chen et al. 2015(a)]	$2T_{sm}+2T_{h(mtp)}$	$3T_{bp}+T_{bp(m)}+T_{bp(a)}+2nT_{h(mtp)}$
89	Chen et al. [Chen et al. 2015(b)]	$4T_{sm}+2T_a+4T_h$	$4T_{bp}+2nT_{sm}+3nT_a+(3n+2)T_h$
90	Cheng et al. [Cheng et al. 2015]	$4T_{sm}+T_{h(mtp)}$	$3T_{bp}+2nT_{bp(m)}+2T_{bp(a)}+(2n+1)T_{h(mtp)}$
91	Horng et al. [Horng et al. 2015]	$3T_{sm}+2T_a+T_{h(mtp)}$	$3T_{bp}+nT_{sm}+nT_{bp(a)}+nT_{h(mtp)}+nT_h$
92	Li et al. [Li et al. 2015]	$4T_{bp(m)}+nT_{h(mtp)}+2T_h$	$4T_{bp}+nT_{sm}+nT_{h(mtp)}+2T_h$
93	Viet and Ogata [Viet and Ogata 2015]	$3T_{sm}+2T_a+2T_{h(mtp)}$	$4T_{bp}+(2n-1)T_{bp(m)}+(n-1)T_{bp(a)}+3nT_{h(mtp)}$
94	Chen et al. [Chen et al. 2014]	$4T_{sm}+3T_a+2T_{h(mtp)}$	$4T_{bp}+2nT_{sm}+2nT_a+2T_{h(mtp)}$
95	Deng et al. [Deng et al. 2014]	$3T_{sm}+2T_a+T_{h(mtp)}+2T_h$	$3T_{bp}+(n-1)T_{bp(m)}+nT_{bp(a)}+2nT_{h(mtp)}+2nT_h$
96	He et al. [He et al. 2014]	$3T_{sm}+2T_a+2T_{h(mtp)}$	$3T_{bp}+2nT_{bp(m)}+nT_{bp(a)}+2nT_{h(mtp)}+nT_h$
97	Liu et al. [Liu et al. 2014(a)]	$5T_{sm}+2T_{h(mtp)}$	$4T_{bp}+3nT_{bp(m)}+(2n+2)T_{h(mtp)}$
98	Liu et al. [Liu et al. 2014(b)]	$3T_{sm}+T_a$	$3T_{bp}+2nT_{sm}+2nT_a$
99	Tu et al. [Tu et al. 2014]	$3T_{sm}+2T_a+4T_{h(mtp)}$	$4T_{bp}+2nT_{sm}+5T_{h(mtp)}$
100	Zhang et al. [Zhang et al. 2014]	$2T_{sm}+T_a+2T_{h(mtp)}$	$2nT_{bp}+2nT_{sm}+nT_a+(3n+1)T_{h(mtp)}$
101	Zhou et al. [Zhou et al. 2014]	$3T_{sm}+2T_{h(mtp)}$	$(n+3)T_{bp}+(n+1)T_{h(mtp)}+nT_h$
102	Du et al. [Du et al. 2013]	$3T_{SM}+4T_h$	$4T_{bp}+(n+2)T_h$
103	Xiong et al. [Xiong et al. 2013]	$3T_{sm}+2T_a+T_h$	$3T_{bp}+nT_{bp(a)}+2nT_{bp(m)}+nT_{h(mtp)}+nT_h$
104	Chen et al. [Chen et al. 2012]	$3T_{sm}+T_a+T_{h(mtp)}$	$(n+2)T_{bp}+nT_{bp(a)}+nT_{sm}+nT_{h(mtp)}$
105	Xiong et al. [Xiong et al. 2012]	$5T_{bp(m)}+3T_{h(mtp)}$	$4T_{bp}+3nT_{bp(m)}+nT_{bp(a)}$
106	Xiong et al. [Xiong et al. 2011]	$4T_{sm}+3T_{h(mtp)}$	$3T_{bp}+3nT_{sm}+5nT_{h(mtp)}$
107(a)	Gong et al. [Gong et al. 2010]	$2T_{sm}+T_a+T_{h(mtp)}$	$(2n+1)T_{bp}+(2n-1)T_{bp(m)}+2nT_{h(mtp)}$
107(b)	Gong et al. [Gong et al. 2010]	$3T_{sm}+2T_a+2T_{h(mtp)}$	$(n+2)T_{bp}+(n-1)T_{bp(m)}+nT_{sm}+2nT_{h(mtp)}$
108	Hu et al. [Hu et al. 2010]	$4T_{sm}+2T_a+2T_{h(mtp)}$	$(n+1)T_{bp}+2nT_{bp(m)}+(n+2)T_h$
109	Zhang et al [Zhang et al. 2010]	$5T_{sm}+4T_a+3T_{h(mtp)}+T_h$	$5T_{bp}+2nT_{bp(m)}+(2n-3)T_a+2nT_{h(mtp)}+3T_h$
110	Zhang et al. [Zhang and Zhang 2009]	$3T_{bp(m)}+2T_a+2T_{h(mtp)}$	$(n+3)T_{bp}+3(n-1)T_{bp(a)}+(n+1)T_{h(mtp)}$
111(a)	Gong et al. [Gong et al. 2007]	$2T_{sm}+T_{h(mtp)}$	$(4n+1)T_{bp}+2nT_{h(mtp)}$
111(b)	Gong et al. [Gong et al. 2007]	$3T_{sm}+4T_a+2T_{h(mtp)}$	$(n+2)T_{bp}+2T_{bp(a)}+nT_{sm}+2nT_{h(mtp)}$
112	Castro et al. [Castro and Dahab 2007]	$2T_{sm}+T_a+2T_{h(mtp)}$	$(2n+1)T_{bp}+nT_{bp(m)}+nT_a+2nT_{h(mtp)}+nT_h$

Table 2: Computational Complexity of CLAS Schemes

6.2 Comprehensive Comparison of CLAS Schemes

In this subsection, we present a comprehensive comparison that encompasses the methodologies utilized, the intractable mathematical problems involved, security model and the current security status of these CLAS schemes.

S. N.	Scheme	Concept	Hard Problem	Model	Secure
1	Gritti [Gritti 2024]	Pairing	CDHP	ROM	Yes
2	Gong et al. [Gong et al. 2023]	ECC	ECDLP	ROM	Yes
3	Guo et al. [Guo et al. 2023]	ECC	ECDLP	ROM	Yes
4	Iqbal et al. [Iqbal et al. 2023]	HEC	HECDLP	ROM	Yes
5	Li et al. [Li et al. 2023]	ECC	ECDLP	ROM	Yes
6	Liang and Liu [Liang & Liu 2023]	Pairing	CDHP	ROM	Yes
7	Tomar et al. [Tomar et al. 2023]	Blockchain, ECC	ECDLP	ROM	Yes
8	Xu et al. [Xu et al. 2023]	ECC	ECDLP	ROM	Yes
9	Xu et Al. [Xu & Li 2023]	NTRU	SIS	ROM	Yes
10	Yang et al. [Yang et al. 2023]	ECC	ECDLP	ROM	Yes
11	Zheng et al. [Zheng et al. 2023]	ECC	ECDLP	ROM	Yes
12	Cahyadi et al. [Cahyadi et al. 2022]	Pairing	CDHP	ROM	Yes
13	Han et al. [Han et al. 2022]	ECC	ECDLP		No [Zheng et al. 2023]
14	Wang et al. [Wangw et al. 2022(a)]	Pairing	CDHP	Standard Model	No [Shim 2023, Yuan et al. 2023, Park & Koo 2024]
15	Wang et al. [Wangw et al. 2022(b)]	Pairing Free	ECDLP	ROM	Yes
16	Xiong et al. [Xiong et al. 2022]	Pairing Free	CDHP	ROM	Yes
17	Yang et al. [Yang et al. 2022]	Pairing Free	ECDLP	ROM	Yes
18	Zhou et al. [Zhou & Yin 2022]	Pairing Free	ECDLP	ROM	Yes
19	Zhu et al. [Zhu et al. 2022]	Pairing Free	ECDLP	ROM	Yes
20	Chen et al. [Chen & Chen 2021]	ECC	ECDLP	ROM	No [Xu et al. 2023]
21	Deng et al. [Deng 2021]	Pairing Free	CDHP	ROM	Yes
22	Kar et al. [Kar et al. 2021]	ECC	ECDLP	ROM	Yes
23	Mei et al. [Mei et al. 2021]	Pairing	CDHP	ROM	No [Liang & Liu 2023, Zhu et al. 2022]
24	Tiwari et al. [Tiwari and Gangadharan 2021]	Pairing	DDHP, CDHP	ROM	Yes
25	Vallent et al. [Vallent et al. 2021]	ECC	ECDLP	ROM	Yes
26	Ye et al. [Ye et al. 2021]	Pairing Free	ECDLP	ROM	Yes
27	Addobea et al. [Addobea et al. 2020]	Pairing	BDHP, CDHP	ROM	No [Xu and Zeng 2021]
28	Benil and Jasper [Benil and Jasper 2020]	Pairing	CDHP	ROM	Yes
29	Hu et al. [Hu et al. 2020(a)]	Pairing	CDHP	ROM	Yes
30	Hu et al. [Hu et al. 2020(c)]	Pairing	CDHP		Yes
31	Hu et al. [Hu et al. 2020(b)]	Pairing	CDHP		Yes
32	Hu et al. [Hu et al. 2020(d)]	Pairing	CDHP		Yes
33	Hu et al. [Hu et al. 2020(e)]	Pairing Free	ECDLP		Yes
34	Kamil et al. [Kamil and Ogundoyin 2020]	Pairing	CDHP	ROM	Yes
35	Lee et al. [Lee et al. 2020]	Pairing Free	ECDLP	ROM	No [Xu and Zeng 2021]
36	Li et al. [Cui et al. 2020]	Pairing Free			Yes
37	Liu et al. [Liu et al. 2020]	Pairing Free	ECDLP	ROM	No [Yang et al. 2020]
38	Shu et al. [Shu et al. 2020]	ECC	ECDLP	ROM	Yes
39	Thumbur et al. [Thumbur et al. 2020]	Pairing Free	ECDLP	ROM	No [Qiao et al. 2023, Zhu et al. 2022, Yang et al. 2022]
40	Wu et al. [Wu et al. 2020]	Pairing	CDHP	ROM	Yes
41	Xu et al. [Xu et al. 2020(a)]	Pairing	CDHP	ROM	Yes
42	Yang et al. [Yang et al. 2020]	Pairing Free	ECDLP	ROM	Yes
43	Zhao et al. [Zhao et al. 2020]	Pairing Free	ECDLP	ROM	No [Thumbur et al. 2020]
44	Zhou et al. [Zhou et al. 2020]	Pairing	CDHP	ROM	Yes
45	Cao et al. [Cao et al. 2019]	Pairing Free	ECDLP		No [Hu et al. 2020(e)]
46	Deng et al. [Deng et al. 2019]	Pairing	CDHP	ROm	Yes
47	Du et al. [Du et al. 2019]	Pairing Free	ECDLP	ROM	Yes
48	Gayathri et al. [Gayathri et al. 2019]	Pairing Free	ECDLP	ROM	No [Qiao et al. 2023, Yang et al. 2020]
49	Hashimoto and Ogata [Hashimoto and Ogata 2019]	Pairing	CDHP	ROM	No [Shim 2020(b)]
50	Kamil et al. [Kamil and Ogundoyin 2019(a)]	ECC	ECDLP	ROM	No [Xiong et al. 2022]
51	Kumar et al. [Kumar et al. 2019]	Pairing	CDHP	ROM	Yes
52	Li et al. [Li et al. 2019]	Pairing Free	ECDLP	ROM	Yes
53	Shen et al. [Shen et al. 2019]	Pairing	CDHP	ROM	Yes
54	Tinh [Trinh 2019]	Pairing Free	GDDHE	Standard Model	Yes
55	Xie et al. [Xie et al. 2019]	ECC	ECDLP	ROM	Yes
56	Xiaodong et al. [Xiongdong et al. 2019]	Pairing	CDHP	ROM	No [Hu et al. 2020(d)]
57	Zhong et al. [Zhong et al. 2019]	Pairing	CDHP	ROM	No [Thumbur et al. 2020, Cui et al. 2020],S.N.-50
58	Cui et al. [Cui et al. 2018]	ECC	ECDLP		No [Kamil and Ogundoyin 2019(a)]
59	Deng et al. [Deng et al. 2018]	Pairing Free	RSA and DLP	ROM	Yes
60	Gayathri et al. [Gayathri and Reddy 2018]	Pairing	CDHP	ROM	Yes
61	Li et al. [Li et al. 2018]	Pairing	CDHP	ROM	No [Yang et al. 2018]
62	Liu et al. [Liu et al. 2018]	Pairing	CDHP	ROM	No [Kamil and Ogundoyin 2019(b)]
63	Liu et al. [Liu et al. 2020]	Pairing	CDHP	ROM	Yes
64	Kumar et al. [Kumar et al. 2018]	Pairing Free	ECDLP	ROM	No [Xie et al. 2019, Wu et al. 2018]
65	Pankaj et al. [Kumar and Sharma 2018]	Pairing	CDHP	ROM	No [Yang et al. 2018(b)]
66	Qu and Mu [Qu and Mu 2018]	Pairing Free	ECDLP	ROM	No [Du et al. 2019]
67	Wang et al. [Wang and Teng 2018]	Pairing	CDHP	ROM	No [Xiongdong et al. 2019]
68	Wu et al. [Wu et al. 2018]	Pairing	CDHP	ROM	No [Gayathri et al. 2019, Kamil and Ogundoyin 2019(b)]
69	Xu et al. [Xu et al. 2018]	Pairing	CDHP	ROM	Yes
70	Yang et al. [Yang et al. 2018]	Pairing	CDHP	ROM	Yes
71	Yang et al. [Yang et al. 2018(a)]	Pairing	CDHP	ROM	Yes
72	Yang et al. [Yang et al. 2018(b)]	Pairing	CDHP	ROM	Yes
73	Du et al. [Hongzhen and Qiaoyan 2017]	Pairing	CDHP	ROM	No [Yang et al. 2018]
74	Fan et al. (i) and (ii) [Fan and Wang 2017]	Pairing	CDHP	ROM	Yes
75	Kang et al. [Kang et al. 2017]	Pairing	CDHP	ROM	No [Xu et al. 2018, Zhou et al. 2020]

S. N.	Scheme	Concept	Hard Problem	Model	Secure
76	Deng et al. [Deng et al. 2016]	Pairing	CDHP	ROM	No [Kumar et al. 2017(a)]
77	Kang and Xu [Kang and Xu 2016]	Pairing	CDHP	ROM	Yes
78	Kar [Kar 2016]	Pairing	CDHP	ROM	Yes
79	Li et al. [Li et al. 2016]	Pairing	CDHP	ROM	Yes
80	Liu et al. [Liu et al. 2016(a)]	Pairing	CDHP	ROM	Yes
81	Liu et al. [Liu et al. 2016(b)]	Pairing	CDHP	ROM	Yes
82	Xu et al. [XU et al. 2016]	Pairing	CDHP	ROM	Yes
83	Nie et al. [Nie et al. 2016]	Pairing	CDHP	Standard Model	No [Pakniat and Noroozi 2016]
84	Tian [Tian 2016]	ID-Based, Pairing Free	DLP		Yes
85	Batra et al. [Batra and Malhi 2015]	Pairing	CDHP	ROM	No [Kumar and Sharma 2018]
86	Chen et al. [Chen et al. 2015(a)]	Pairing	CDHP	ROM	Yes
87	Chen et al. [Chen et al. 2015(b)]	Pairing	CDHP	ROM	Yes
88	Cheng et al. [Cheng et al. 2015]	Pairing	CDHP	ROM	No [Wu et al. 2020, Yang et al. 2018(a)]
89	Horng et al. [Horng et al. 2015]	Pairing	CDHP	ROM	No [Li et al. 2016]
90	Li et al. [Li et al. 2015]	Pairing	CDHP	ROM	Yes
91	Viet and Ogata (I and II) [Viet and Ogata 2015]	Pairing	CDHP	ROM	Yes
92	Chen et al. [Chen et al. 2014]	Pairing	CDHP	ROM	No [Zhang et al. 2016(b), Wang et al. 2016]
93	Deng et al. [Deng et al. 2014]	Pairing	CDHP	ROM	No [Kumar et al. 2016(b)]
94	He et al. [He et al. 2014]	Pairing	CDHP	ROM	No [Yang et al. 2015, Zhang et al. 2015(a), Yang et al. 2013], S.N-61,74
95	Liu et al. [Liu et al. 2014(a)]	Pairing	CDHP	ROM	No [Shen et al. 2016, Wang and Yuan 2015]
96	Zhang et al. [Zhang et al. 2014]	Pairing	CDHP	ROM	Yes
97	Zhou et al. [Zhou et al. 2014]	Pairing	CDHP	ROM	No [Chen et al. 2016]
98	Du et al. [Du et al. 2013]	Pairing	CDHP	ROM	No [XU et al. 2016, Liu et al. 2016(a)]
99	Hou et al. [Hou et al. 2013]	Pairing	CDHP	ROM	No [Deng et al. 2016, Deng et al. 2014]
100	Xiong et al. [Xiong et al. 2013]	Pairing	CDHP	ROM	No [Tu et al. 2014, Aboud 2013], S.N.-88,92,94,96
101	Chen et al. [Chen et al. 2012]	Pairing	eCDHP	ROM	Yes
102	Xiong et al. [Xiong et al. 2012]	Pairing	CDHP	ROM	Yes
103	Xiong et al. [Xiong et al. 2011]	Pairing	CDHP	ROM	No [Shen et al. 2012]
104	Gong et al.(I) and (II) [Gong et al. 2010]	Pairing	CDHP	ROM	Yes
105	Zhang et al. [Zhang et al. 2010]	Pairing	CDHP	ROM	Yes
106	Hu et al. [Hu et al. 2010]	Pairing	CDHP	ROM	Yes
107	Zhang and Zhang [Zhang and Zhang 2009]	Pairing	CDHP	ROM	No [Kang and Xu 2016, Shim 2011]
108	Zhang and Zhang [Zhang and Zhang 2008]	Piring	CDHP	ROM	Yes
109	Castro and Dahab [Castro and Dahab 2007]	Pairing	CDHP	ROM	Yes
110	Gong et al. (I) and (II) [Gong et al. 2007]	Pairing	CDHP	ROM	No [Zhang and Zhang 2008]

Table 3: Comprehensive Comparison of CLAS Schemes

7 Unexplored Frontiers

The initial challenge is to design a CLAS scheme that requires less storage space and computational cost is not directly proportional to the increase in messages or signers [Gong et al. 2007]. The survey briefly explains the development of CLAS schemes and their applications to the field of Vehicular Ad-hoc Networks, Internet of Things (IoT), Mobile Health System, Internet of Drones (IoD) etc. Further researchers contribute to improve CLAS schemes in all aspects like security and efficiency, but still there are few challenges which need to be addressed and we intend to accomplish:

- Our goal is to develop a more efficient CLAS scheme specifically designed for resource-constrained wireless networks.
- We intend to develop a multi-sender and multi-receiver CLAS scheme for VANETs.
- We plan to create a CLAS scheme that will be useful for vehicle-to-vehicle mutual authentication.
- Our aim is to develop a CLAS scheme that can generate aggregate signatures of a fixed size while repeatedly reusing state information.
- We intend to propose a more lightweight and secure CLAS scheme for HWMSN's.
- With the purpose of supporting the identity revocation process of the vehicle, we want to develop an authentication method based on CLAS.

- We deal with an interesting problem to build an effective CLAS scheme with full aggregation secure against insider assaults.
- In order to present a safe and effective CLAS scheme with constant size aggregate signature, we try to resolve an open problem.
- We proved that it is impossible to construct an unrestricted and compact CLAS scheme with constant pairing computation with respect to the add-pairing structure .

8 Conclusion

In this paper, we provide an overview of the evolution of certificateless aggregate signature schemes and their deployment in various real-time applications. We present the development of the CLAS scheme in chronological order together with the subsequent analysis and enhancement by other researchers. As we go through pertinent literature on CLAS schemes, we discover that it is difficult to construct an unconstrained and compact CLAS scheme with constant pairing computation in regard to the add-pairing structure. This survey will undoubtedly assist researchers in scrutinizing the weaknesses of current schemes and devising innovative applications for such schemes.

References

[Aboud 2013] Aboud, S. J.: "Cryptanalysis of Certificateless Aggregate Signature Scheme"; International Journal of Computer Networks and Security, 23, 1, 1109-1112, 2013.

[Addobea et al. 2020] Addobea, A. A., Hou, J., Li, Q.; "MHCOOS: An offline-online certificateless signature scheme for m-health devices"; Security and Communication Networks, 2020.

[Al-Riyami and Paterson 2003] Al-Riyami, S. S., Paterson, K. G.: "Certificateless public key cryptography"; In International conference on the theory and application of cryptology and information security Springer, Berlin, Heidelberg (November 2003), 452-473.

[Au et al. 2007] Au, M. H., Mu, Y., Chen, J., Wong, D. S., Liu, J. K., Yang, G.: "Malicious KGC attacks in certificateless cryptography"; In Proceedings of the 2^{nd} ACM symposium on Information, computer and communications security (March 2007), 302-311, 2007.

[Batra and Malhi 2015] Batra, S., Malhi, A. K.: "An efficient certificateless aggregate signature scheme for vehicular ad-hoc networks"; Discrete Mathematics & Theoretical Computer Science, 17, 2015.

[Bellare and Rogaway] Bellare, M., Rogaway, P.: "Random oracles are practical: A paradigm for designing efficient protocols"; In Proceedings of the 1^{st} ACM Conference on Computer and Communications Security (December 1993), 62-73.

[Benil and Jasper 2020] Benil, T., Jasper, J. J. C. N.: "Cloud based security on outsourcing using blockchain in E-health systems"; Computer Networks, 178, 107344, 2020.

[Boneh et al. 2003] Boneh, D., Gentry, C., Lynn, B., Shacham, H.: "Aggregate and verifiably encrypted signatures from bilinear maps"; In International conference on the theory and applications of cryptographic techniques, Springer, Berlin, Heidelberg (May 2003), 416-432.

[Cahyadi et al. 2022] Cahyadi, E. F., Su, T. W., Yang, C. C., & Hwang, M. S.: "A certificateless aggregate signature scheme for security and privacy protection in VANET"; International Journal of Distributed Sensor Networks, 18, 5, 15501329221080658, 2022.

[Cao et al. 2019] Cao, S., Lang, X., Liu, X.: "Probably secure and efficient certificateless aggregate signature scheme"; Netinfo Security, 19, 1, 42-50, 2019.

[Castro and Dahab 2007] Castro, R., Dahab, R.: "Efficient Certificateless Signatures Suitable for Aggregation"; IACR Cryptol. ePrint Arch., 454, 2007.

[Chen et al. 2012] Chen, Y. C., Horng, G., Liu, C. L. et al.: "Efficient certificateless aggregate signature scheme"; J. Electronic Science and Technology, 10, 209–214, 2012.

[Chen et al. 2014] Chen, Y. C., Tso, R., Mambo, M., Huang, K., Horng, G.: "Certificateless aggregate signature with efficient verification"; Security and Communication Networks, 8, 13, 2232-2243, 2014.

[Chen et al. 2015(a)] Chen, Y. C., Tso, R., Horng, G., Fan, C. I., Hsu, R. H.: "Strongly Secure Certificateless Signature: Cryptanalysis and Improvement of two Schemes"; J. Inf. Sci. Eng., 31, 1, 297-314, 2015.

[Chen et al. 2015(b)] Chen, H., Wei, S., Zhu, C.: "Secure certificateless aggregate signature scheme"; Journal of Software, 26, 5, 1173-1180, 2015.

[Chen et al. 2016] Chen, C. C., Chien, H., Horng, G.: "Cryptanalysis of a Compact Certificateless Aggregate Signature Scheme"; Int. J. Netw. Secur., 18, 4, 793-797, 2016.

[Chen & Chen 2021] Chen, Y., & Chen, J.: "CPP-CLAS: Efficient and conditional privacy-preserving certificateless aggregate signature scheme for VANETs"; IEEE Internet of Things Journal, 9, 12, 10354-10365, 2021.

[Chen & Chen 2022] Chen, Y., & Chen, J.: "CPP-CLAS: Efficient and conditional privacy-preserving certificateless aggregate signature scheme for VANETs"; IEEE Internet of Things Journal, 9, 12, 10354-10365, 2022.

[Cheng et al. 2015] Cheng, L., Wen, Q., Jin, Z., Zhang, H., Zhou, L.: "Cryptanalysis and improvement of a certificateless aggregate signature scheme"; Information Sciences, 295, 337-346, 2015.

[Cui et al. 2018] Cui, J., Zhang, J., Zhong, H., Shi, R., Xu, Y.: "An efficient certificateless aggregate signature without pairings for vehicular ad hoc networks"; Information Sciences, 451, 1-15, 2018.

[Cui et al. 2020] Cui, L., Gang, W., Xiaofeng, S., Feng, Z., Liang, Z.: "An efficient certificateless aggregate signature scheme designed for VANET"; Computers, Materials & Continua, 63, 2, 725-742, 2020.

[Deng et al. 2014] Deng, J., Xu, C., Wu, H., Yang, G.: "An improved certificateless aggregate signature"; In 2014 IEEE International Conference on Computer and Information Technology (September 2014) 919-922.

[Deng et al. 2016] Deng, J., Xu, C., Wu, H., Dong, L.: "A new certificateless signature with enhanced security and aggregation version"; Concurrency and computation: Practice and Experience, 28, 4, 1124-1133, 2016.

[Deng et al. 2018] Deng, L., Yang, Y., Chen, Y., Wang, X.: "Aggregate signature without pairing from certificateless cryptography"; Journal of Internet Technology, 19, 5, 1479-1486, 2018.

[Deng et al. 2019] Deng, L., Yang, Y., Chen, Y.: "Certificateless short aggregate signature scheme for mobile devices"; IEEE Access, 7, 87162-87168, 2019.

[Deng et al. 2020] Deng, L., Ning, B., & Jiang, Y.: "A lightweight certificateless aggregation signature scheme with provably security in the standard model"; IEEE Systems Journal, 14, 3, 4242-4251, 2020.

[Deng 2021] Deng, L., Yang, Y., Gao, R.: "Certificateless Designated Verifier Anonymous Aggregate Signature Scheme for Healthcare Wireless Sensor Networks"; IEEE Internet of Things Journal, 8, 11, 8897-8909, 2021.

[Diffie and Hellman 1976] Diffie, W., Hellman, M. E.: "New Directions in Cryptography"; IEEE Transactions on Information Theory 22, 6, 1976.

[Du et al. 2013] Du Hong-zhen, H. M. J., WEN, Q. Y.: "Efficient and provably-secure certificateless aggregate signature scheme"; ACTA ELECTONICA SINICA, 41, 1, 72, 2013.

[Du et al. 2019] Du, H., Wen, Q., Zhang, S.: "An efficient certificateless aggregate signature scheme without pairings for healthcare wireless sensor network"; IEEE Access, 7, 42683-42693, 2019.

[Fan and Wang 2017] Fan, A., Wang, Q.: "Security analysis and improvement of the certificateless aggregate signature schemes"; AMSE J-AMSE IIETA Publication, 174-188, 2017.

[Gayathri et al. 2019] Gayathri, N. B., Thumbur, G., Kumar, P. R., Rahman, M. Z. U., Reddy, P. V.: "Efficient and secure pairing-free certificateless aggregate signature scheme for healthcare wireless medical sensor networks"; IEEE Internet of Things Journal, 6, 5, 9064-9075, 2019.

[Gayathri and Reddy 2018] Gayathri, N. B., Reddy, V.: "Efficient and provably secure certificateless aggregate signature scheme from bilinear pairing"; International Journal of Pure and Applied Mathematics, 120, 5,1385-1404, 2018.

[Gentry and Ramazan 2006] Gentry, C., Ramzan, Z.: "Identity-based aggregate signatures"; In International workshop on public key cryptography, Springer, Berlin, Heidelberg (April 2006), 257-273.

[Gong et al. 2007] Gong, Z., Long, Y., Hong, X., Chen, K.: "Two certificateless aggregate signatures from bilinear maps"; In Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD 2007) (July 2007), 3, 188-193, IEEE.

[Gong et al. 2010] Gong, Z., Long, Y., Hong, X., Chen, K.: "Practical Certificateless Aggregate Signatures from Bilinear Maps"; J. Inf. Sci. Eng. 26. 6, 2093-2106, 2010.

[Gong et al. 2023] Gong, Z., Gao, T., & Guo, N.: "Pcas: An Improved Pairing-Free Certificateless Aggregate Signature with Conditional Privacy Preserving for Vanets"; Available at SSRN 4160735, 2023.

[Gritti 2024] Gritti, C.: "OASIS: An Organizational CertificateLess Aggregate Signature Scheme in Distributed Networks for IoT"; 2024.

[Guo et al. 2023] Guo, R., Dong, R., Li, X., Zhang, Y., & Zheng, D.: "Drclas: An Efficient Certificateless Aggregate Signature Scheme with Dynamic Revocation in Vehicular Ad-Hoc Networks"; Available at SSRN 4549892.

[Han et al. 2022] Han, Y., Song, W., Zhou, Z., Wang, H., & Yuan, B.: "eCLAS: An efficient pairing-free certificateless aggregate signature for secure VANET communication"; IEEE Systems Journal, 16, 1, 1637-1648, 2022.

[Hashimoto and Ogata 2019] Hashimoto, K., Ogata, W.: "Unrestricted and compact certificateless aggregate signature scheme"; Information Sciences, 487, 97-114, 2019.

[He et al. 2014] He, D., Tian, M., Chen, J.: "Insecurity of an efficient certificateless aggregate signature with constant pairing computations"; Information sciences, 268, 458-462, 2014.

[Hongzhen and Qiaoyan 2017] Hongzhen, D. U., Qiaoyan, W. E. N.: "Attack and improvement of a certificateless aggregate signature scheme"; Acta Scientiarum Naturalium Universitatis Sunyatseni, 56, 1, 77, 2017.

[Horng et al. 2015] Horng, S. J., Tzeng, S. F., Huang, P. H., Wang, X., Li, T., Khan, M. K.: "An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks"; Information Sciences, 317, 48-66, 2015.

[Hou et al. 2013] Hou, H., Zhang, X., Dong, X.: "Improved certificateless aggregate signature scheme"; Journary of Shandong University (Natural Science), 48, 9, 29-34, 2013.

[Hu et al. 2010] Hu, C., Wangan, S., Bing, Z.: "Certificateless aggregate signature scheme"; In 2010 International Conference on E-Business and E-Government (May 2010), 3790-3793, IEEE.

[Hu et al. 2020(a)] Hu, X., Tan, W., Ma, C., Xu, H.: "Certificateless Aggregate Signature Scheme with High Efficencicy in Vehicular Ad-hoc Network"; In Proceedings of the 2020 4^{th} International Conference on Electronic Information Technology and Computer Engineering, (November 2020), 1008-1012.

[Hu et al. 2020(b)] Hu, X., Ma, C., Tan, W., Jiang, W.: "Security Analysis and Improvement of Designated Verifier CLAS in Network Security Course Education"; In 2020 IEEE 3^{rd} International Conference of Safe Production and Informatization (IICSPI), (November 2020), 616-620.

[Hu et al. 2020(c)] Hu, X., Tan, W., Ma, C.: "Certificateless Aggregate Signature schemes for Privacy Protection of Security Anlysis and Improvement"; In 2020 International Conference on Computer Science and Management Technology (ICCSMT), (November 2020), 314-317.

[Hu et al. 2020(d)] Hu, X., Tan, W., Yan, J., Ma, C.: "Security and Improvement of Aggregate Signature Scheme for Underwater Wireless Sensor Networks and Certificateless Aggregate Signature Scheme for Vehicular Ad Hoc Networks"; In 2020 5^{th} International Conference on Mechanical, Control and Computer Engineering (ICMCCE), (December 2020), 574-577.

[Hu et al. 2020(e)] Hu, X., Tan, W., Ma, C., Chen, F., Yu, C.: "Study on Security Analysis and Efficient Imrovement of Certificateless Aggregate Signature Scheme"; In 2020 IEEE 11^{th} International Conference on Software Engineering and Service Science (ICSESS) (October 2020), 343-346.

[Hua 2020] Hua, G.: "An improved aggregate signature for underwater wireless network"; Journal of Unmanned Undersea Systems, 28, 4, 428-433, 2020.

[Iqbal et al. 2023] Iqbal, A., Zubair, M., Khan, M. A., Ullah, I., Ur-Rehman, G., Shvetsov, A. V., & Noor, F.: "An Efficient and Secure Certificateless Aggregate Signature Scheme for Vehicular Ad hoc Networks"; Future Internet, 15, 8, 266, 2023.

[Itakura and Nakamura 1983] Itakura, K., Nakamura, K.: "A public-key cryptosystem suitable for digital multisignatures"; NEC Research & Development, 71, 1-8, 1983.

[Kamil and Ogundoyin 2019(a)] Kamil, I. A., Ogundoyin, S. O.: "An improved certificateless aggregate signature scheme without bilinear pairings for vehicular ad hoc networks"; Journal of information security and applications, 44, 184-200, 2019.

[Kamil and Ogundoyin 2019(b)] Kamil, I. A., Ogundoyin, S. O.: "A lightweight CLAS scheme with complete aggregation for healthcare mobile crowdsensing"; Computer Communications, 147, 209-224, 2019.

[Kamil and Ogundoyin 2020] Kamil, I. A., Ogundoyin, S. O.: "On the security of privacy-preserving authentication scheme with full aggregation in vehicular ad hoc network"; Security and Privacy, 3, 3, e104, 2020.

[Kang et al. 2017] Kang, B., Wang, M., Jing, D.: "An efficient certificateless aggregate signature scheme"; Wuhan University Journal of Natural Sciences, 22, 2, 165-170, 2017.

[Kang and Xu 2016] Kang, B., Xu, D.: "A secure certificateless aggregate signature scheme"; International Journal of Security and Its Applications, 10, 3, 55-68, 2016.

[Kar 2016] Kar, J.: "Certicateless Aggregate Short Signature Scheme"; Cryptology ePrint Archive, 2016.

[Kar et al. 2021] Kar, J., Liu, X., & Li, F.: "CL-ASS: An efficient and low-cost certificateless aggregate signature scheme for wireless sensor networks"; Journal of Information Security and Applications, 61, 102905, 2021.

[Khan et al. 2022] Khan, M. A., Ullah, I., Alsharif, M. H., Alghtani, A. H., Aly, A. A., Chen, C. M.: "An Efficient Certificate-Based Aggregate Signature Scheme for Internet of Drones"; Security and Communication Networks, 2022.

[Kumar et al. 2016(a)] Kumar, P., Sharma, V., Sharma, G.: "Certificateless aggregate signature schemes: A review"; In 2016 International Conference on Computing, Communication and Automation (ICCCA) (April 2016), 531-536, IEEE.

[Kumar et al. 2016(b)] Kumar, P., Sharma, V., Sharma, G.: "Cryptanalysis of a certificateless aggregate signature scheme"; In 2016 International Conference on Computing, Communication and Automation (ICCCA)(April 2016), 1095-1098, IEEE.

[Kumar and Sharma 2017] Kumar, P., Sharma, V.: "A comment on efficient certificateless aggregate signature scheme"; In 2017 International Conference on Computing, Communication and Automation (ICCCA)(May 2017), 515-519, IEEE.

[Kumar et al. 2017(a)] KUMAR, P., SHARMA, V., KUMAR, V.: "CRYPTANALYSIS OF EFFICIENT CERTIFICATELESS AGGREGATE SIGNATURE SCHEME"; 2017.

[Kumar et al. 2018] Kumar, P., Kumari, S., Sharma, V., Sangaiah, A. K., Wei, J., Li, X.: "A certificateless aggregate signature scheme for healthcare wireless sensor network"; Sustainable Computing: Informatics and Systems, 18, 80-89, 2018.

[Kumar and Sharma 2018] Kumar, P., Sharma, V.: "On the security of certificateless aggregate signature scheme in vehicular ad hoc networks"; In Soft Computing: Theories and Applications, Springer, Singapore 715-722, 2018.

[Kumar et al. 2019] Kumar, P., Kumari, S., Sharma, V., Li, X., Sangaiah, A. K., Islam, S. H.: "Secure CLS and CL-AS schemes designed for VANETs"; The Journal of Supercomputing, 75, 6, 3076-3098, 2019.

[Lee et al. 2020] Lee, D. H., Yim, K., Lee, I. Y.: "A Certificateless Aggregate Arbitrated Signature Scheme for IoT Environments"; Sensors, 20, 14, 3983, 2020.

[Li et al. 2015] Li, Y. P., Nie, H. H., Zhou, Y. W., Yang, B.: "A novel and provably secure certificateless aggregate signature scheme"; Journal of Cryptologic Research, 2, 6, 526-535, 2015.

[Li et al. 2016] Li, J., Yuan, H., Zhang, Y.; "Cryptanalysis and improvement of certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks"; Cryptology ePrint Archive, 2016.

[Li et al. 2018] Li, J., Yuan, H., Zhang, Y.: "Cryptanalysis and improvement for certificateless aggregate signature"; Fundamenta Informaticae, 157, 1-2, 111-123, 2018.

[Li et al. 2019] Li, K., Au, M. H., Ho, W. H., Wang, Y. L.: "An efficient conditional privacy-preserving authentication scheme for vehicular ad hoc networks using online/offline certificateless aggregate signature"; In International Conference on Provable Security, Springer, Cham (October 2019), 59-76.

[Li et al. 2023] Li, X., Yin, X., & Ning, J.: "RelCLAS: A Reliable Malicious KGC-Resistant Certificateless Aggregate Signature Protocol for Vehicular Ad Hoc Networks"; IEEE Internet of Things Journal, 2023.

[Liang & Liu 2023] Liang, Y., & Liu, Y.: "Analysis and improvement of an efficient certificateless aggregate signature with conditional privacy preservation in VANETs"; IEEE Systems Journal, 17, 1, 664-672, 2023.

[Liu et al. 2014(a)] Liu, H., Liang, M., Sun, H.: "A secure and efficient certificateless aggregate signature scheme"; IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 97, 4, 991-995, 2014.

[Liu et al. 2014(b)] Liu, H., Wang, S., Liang, M., Chen, Y.: "New construction of efficient certificateless aggregate signatures"; International Journal of Security and Its Applications, 8, 1, 411-422, 2014.

[Liu et al. 2016(a)] Liu, Y., Hu, X., Tan, W.: "Study on a provably secure certificateless aggregate signature scheme"; In 2016 IEEE 13^{th} International Conference on Networking, Sensing, and Control (ICNSC)(April 2016), 1-4.

[Liu et al. 2016(b)] Dan, L. I. U., SHI, R. H., ZHANG, S., ZHONG, H.: "Efficient anonymous roaming authentication scheme using certificateless aggregate signature in wireless network"; Journal on Communications, 37, 7, 182, 2016.

[Liu et al. 2018] Liu, J., Cao, H., Li, Q., Cai, F., Du, X., Guizani, M.: "A large-scale concurrent data anonymous batch verification scheme for mobile healthcare crowd sensing"; IEEE Internet of things Journal, 6, 2, 1321-1330, 2018.

[Liu et al. 2020] Liu, J., Li, Q., Cao, H., Sun, R., Du, X., Guizani, M.: "MDBV: Monitoring data batch verification for survivability of Internet of Vehicles"; IEEE Access, 6, 50974-50983, 2018.

[Liu et al. 2020] Liu, J., Wang, L., Yu, Y.: "Improved security of a pairing-free certificateless aggregate signature in healthcare wireless medical sensor networks"; IEEE Internet of Things Journal, 7, 6, 5256-5266, 2020.

[Liu et al. 2020] Liu, J., Wang, L., & Yu, Y.: "Improved security of a pairing-free certificateless aggregate signature in healthcare wireless medical sensor networks"; IEEE Internet of Things Journal, 7, 6, 5256-5266, 2020.

[Liu and You 2019] Liu, C., You, L.: "Certificateless aggregate signature scheme"; Journal of Hangzhou Dianzi University (Natural Sciences), 39, 6, 12-17, 2019.

[Lu et al. 2012] Lu, H. J., Yu, X. Y., Xie, Q.: "Provably secure certificateless aggregate signature with constant length. Journal of Shanghai Jiaotong University"; 46, 2, 259-263, 2012.

[Luo et al. 2016] LUO, M., SUN, T., ZHANG, J., LI, L.: "Security analysis on two certificateless aggregate signature schemes"; Journal of Electronics and Information Technology, 38, 10, 2695-2700, 2016.

[Ma et al. 2020] Ma, L., Yang, Q., Lai, J.: "A certificateless-based aggregated signature scheme with designated verifier property"; Henen science and Technology, 717, 17, 10-12, 2020.

[Ma et al. 2023] Ma, K., Zhou, Y., Wang, Y., Dong, C., Xia, Z., Yang, B., & Zhang, M.: "An efficient certificateless signature scheme with provably security and its applications"; IEEE Systems Journal, 2023.

[Mei et al. 2021] Mei, Q., Xiong, H., Chen, J., Yang, M., Kumari, S., & Khan, M. K.: "Efficient certificateless aggregate signature with conditional privacy preservation in IoV"; IEEE Systems Journal, 15, 1, 245-256, 2020.

[Ming et al. 2014] Ming, Y., Zhao, X., Wang, Y.: "Certificateless aggregate signature scheme"; Journal of University of Electronic Science and Technology of China, 43, 2, 188–193, 2014.

[Nie et al. 2016] Nie, H., Li, Y., Chen, W., Ding, Y.: "NCLAS: a novel and efficient certificateless aggregate signature scheme"; Security and Communication Networks, 9, 16, 3141-3151, 2016.

[Park and Kang 2007] Park, J. H., Kang, B. G.: "Security analysis of the certificateless signature scheme proposed at SecUbiq 2006"; In International Conference on Embedded and Ubiquitous Computing, Springer, Berlin, Heidelberg (December 2007), 686-691.

[Pakniat and Noroozi 2016] Pakniat, N., Noroozi, M.: "Cryptanalysis of a certificateless aggregate signature scheme"; Cryptology ePrint Archive, 2016.

[Park & Koo 2024] J. H. Park and B. Koo: "Comments on A Conditional Privacy-Preserving Certificateless Aggregate Signature Scheme in the Standard Model for VANETs"; in IEEE Access, doi: 10.1109/ACCESS.2024.3353609, 2024.

[Qiao et al. 2023] Qiao, Z., Yang, Q., Zhou, Y., Yang, B., & Zhang, M.: "A novel construction of certificateless aggregate signature scheme for healthcare wireless medical sensor networks"; The Computer Journal, 66, 11, 2810-2824, 2023.

[Qu and Mu 2018] Qu, Y., Mu, Q.: "An efficient certificateless aggregate signature without pairing"; International Journal of Electronic Security and Digital Forensics, 10, 2, 188-203, 2018.

[Shamir 1984] Shamir, A.: "Identity-based cryptosystems and signature schemes"; In Workshop on the theory and application of cryptographic techniques, Springer, Berlin, Heidelberg (August 1984), 47-53.

[Shen et al. 2012] Shen, L. and Sun, Y.: "On the security of a certificateless aggregate signature scheme"; Cryptology ePrint Archive, Report 2012/152, 2012.

[Shen et al. 2016] Shen, H., Chen, J., Hu, H., Shen, J.: "Insecurity of a certificateless aggregate signature scheme"; IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 99, 2, 660-662, 2016.

[Shen et al. 2019] Shen, L., Ma, J., Miao, Y., & Liu, H.: "Provably secure certificateless aggregate signature scheme with designated verifier in an improved security model"; IET Information Security, 13, 3, 167-173, 2019.

[Shim 2011] Shim, K. A.: "On the security of a certificateless aggregate signature scheme"; IEEE Communications Letters 15, 10, 1136-1138, 2011.

[Shim 2020(a)] Shim, K. A.: "Cryptanalysis of Two Signature Schemes for IoT-Based Mobile Payments and Healthcare Wireless Medical Sensor Networks"; IEEE Access, 8, 167203-167208, 2020.

[Shim 2020(b)] Shim, K. A.: "Forgery attacks on two provably secure certificateless signature schemes"; Information Sciences, 521, 81-87, 2020.

[Shim 2023] K.A. Shim: "Security analysis of conditional privacy-preserving authentication schemes for VANETs"; in IEEE Access, 11, 33956–33963, 2023.

[Shu et al. 2020] Shu, H., Qi, P., Huang, Y., Chen, F., Xie, D., Sun, L.: "An efficient certificateless aggregate signature scheme for blockchain-based medical cyber physical systems"; Sensors 20, 5, 1521, 2020.

[Thumbur et al. 2020] Thumbur, G., Rao, G., S., Reddy, P., V., Gayathri, N., B., Reddy, D., K., Padmavathamma, M.: "Efficient and Secure Certificateless Aggregate Signature-Based Authentication Scheme for Vehicular Ad Hoc Networks"; IEEE Internet of Things Journal, 8, 3, 1908-1920, 2020.

[Tian 2016] Tian, X.: "A novel certificateless aggregate signature scheme without bilinear pairings"; In Proc. Int. Conf. Comput. Netw. Commun. Technol.(CNCT) (December 2016), 54, 853-857.

[Tiwari and Gangadharan 2021] Tiwari, D., Gangadharan, G. R.: "SecAuth-SaaS: a hierarchical certificateless aggregate signature for secure collaborative SaaS authentication in cloud computing"; Journal of Ambient Intelligence and Humanized Computing, 12, 12, 10539-10563, 2021.

[Tomar et al. 2023] Tomar, A., Tripathi, S., & Arivarasan, K.: "A Blockchain-Based Certificateless Aggregate Signature Scheme for Fog-Enabled Smart Grid Environment"; IEEE Transactions on Green Communications and Networking, 2023.

[Trinh 2019] Trinh, V. C.: "A short server-aided certificateless aggregate multisignature scheme in the standard model"; Security and Communication Networks, 2019.

[Tu et al. 2014] Tu, H., He, D., Huang, B.: "Reattack of a certificateless aggregate signature scheme with constant pairing computations"; The Scientific World Journal, 2014.

[Vallent et al. 2021] Vallent, T. F., Hanyurwimfura, D., Mikeka, C.: "Efficient certificate-less aggregate signature scheme with conditional privacy-preservation for vehicular ad hoc networks enhanced smart grid system"; Sensors, 21, 9, 2900, 2021.

[Viet and Ogata 2015] Viet, N. Q., Ogata, W.,: "Certificateless aggregate signature schemes with improved security"; IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 98, 1, 92-99, 2015.

[Wang et al. 2016] Wang, L., Chen, K., Long, Y., Wang, H.: "Cryptanalysis of a certificateless aggregate signature scheme"; Security and communication networks, 9, 11, 1353-1358, 2016.

[Wang and Teng 2018] WANG, D., TENG, J.: "Probably secure cetificateless aggregate signature algorithm for vehicular ad hoc network"; Journal of Electronics and Information Technology, 40, 1, 11-17, 2018.

[Wangw et al. 2022(a)] H. Wang, L. Wang, K. Zhang, J. Li and Y. Luo: "A Conditional Privacy-Preserving Certificateless Aggregate Signature Scheme in the Standard Model for VANETs"; in IEEE Access, 10, 15605-15618, 2022.

[Wangw et al. 2022(b)] Wang, Z., Wang, H., Wang, Y., & Yang, X.: "CLASRM: A lightweight and secure certificateless aggregate signature scheme with revocation mechanism for 5G-enabled vehicular networks"; Wireless Communications and Mobile Computing, 1-20, 2022.

[Wang et al. 2022(c)] Wang, H., Wang, L., Zhang, K., Li, J., & Luo, Y.: "A conditional privacy-preserving certificateless aggregate signature scheme in the standard model for VANETs"; IEEE Access, 10, 15605-15618, 2022.

[Wang and Yuan 2015] Wang, C., Yuan, Y.: "Analysis of a certificateless aggregate signature scheme"; IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2015, 98, 1, 421-423.

[Wu et al. 2018] Wu, L., Xu, Z., He, D., Wang, X.: "New certificateless aggregate signature scheme for healthcare multimedia social network on cloud environment"; Security and Communication Networks, 2018.

[Wu et al. 2020] Wu, G., Zhang, F., Shen, L., Guo, F., Susilo, W.: "Certificateless aggregate signature scheme secure against fully chosen-key attacks"; Information Sciences, 514, 288-301, 2020.

[Xie et al. 2019] Xie, Y., Li, X., Zhang, S., Li, Y.: "$iCLAS$: An improved certificateless aggregate signature scheme for healthcare wireless sensor networks"; IEEE Access, 7, 15170-15182, 2019.

[Xiong et al. 2011] Xiong, H., Wu, Q., Chen, Z.: "Strong security enabled certificateless aggregate signatures applicable to mobile computation"; In 2011 Third International Conference on Intelligent Networking and Collaborative Systems (November 2011), 92-99 ,IEEE.

[Xiong et al. 2012] Xiong, H., Wu, Q., Chen, Z.: "An efficient provably secure certificateless aggregate signature applicable to mobile computation"; Control and Cybernetics, 41, 2, 373-391, 2012.

[Xiong et al. 2013] Xiong, H., Guan, Z., Chen, Z., Li, F.: "An efficient certificateless aggregate signature with constant pairing computations"; Information Sciences, 219, 225-235, 2013.

[Xiong et al. 2022] Xiong, W., Wang, R., Wang, Y., Wei, Y., Zhou, F., & Luo, X.: "Improved certificateless aggregate signature scheme against collusion attacks for vanets"; IEEE Systems Journal, 17, 1, 1098-1109, 2022.

[Xiongdong et al. 2019] Xiaodong, Y. A. N. G., Tingchun, M. A., Chunlin, C. H. E. N., Jinli, W. A. N. G., Caifen, W. A. N. G.: "Security analysis and improvement of certificateless aggregate signature scheme for vehicular ad hoc networks"; Journal of Electronics and Information Technology, 41, 5, 1265-1270, 2019.

[Xiu and Da-Ke 2014] Xiu-ying, Y., Da-ke, H.: "New certificateless aggregate signature scheme"; Application Research of Computers, 31, 8, 2485-2487, 2014.

[XU et al. 2016] XU, Y., HUANG, L. S., TIAN, M. M., ZHONG, H., CUI, J.: "A provably secure and compact certificateless aggregate signature scheme"; ACTA ELECTONICA SINICA, 44, 8, 1845, 2016.

[Xu et al. 2018] Xu, Z., Wu, L., Ren, Y., He, D.: "New Efficient Certificateless Aggregate Signature Scheme"; Journal of Internet Technology, 19, 7, 2023-2033, 2018.

[Xu et al. 2020(a)] Xu, Z., He, D., Kumar, N., Choo, K. K. R.: "Efficient certificateless aggregate signature scheme for performing secure routing in VANETs"; Security and Communication Networks, 2020.

[Xu et al. 2020(b)] Xu, G., Zhou, W., Sangaiah, A. K., Zhang, Y., Zheng, X., Tang, Q., ... & Zhou, X.: "A security-enhanced certificateless aggregate signature authentication protocol for InVANETs"; IEEE network, 34, 2, 22-29, 2020.

[Xu et al. 2023] Xu, Z., Wang, L., Luo, Y., Long, Y., Zhang, K., Yan, H., & Chen, K.: "A Security-Enhanced Conditional Privacy-Preserving Certificateless Aggregate Signature Scheme for Vehicular Ad-Hoc Networks"; IEEE Internet of Things Journal, 2023.

[Xu & Li 2023] Xu, M., & Li, C. (2023). A NTRU-Based Certificateless Aggregate Signature Scheme for Underwater Acoustic Communication. IEEE Internet of Things Journal.

[Xu and Zeng 2021] Xu, F., Zeng, H.: "Cryptanalysis of Two Signature Schemes for IoT and Mobile Health Systems"; Wireless Personal Communications, 1-9, 2021.

[Yang et al. 2013] Yang, B., Yang, Z., Xiao, Z., Li, S.: "Deep Attacks of a Certificateless Signature Scheme"; IACR Cryptol. ePrint Arch., 721, 2014.

[Yang et al. 2015] Yang, B., Yang, Z., Liu, N., Li, S.: "Further attacks and improvement of a certificateless signature scheme"; In 2015 11^th International Conference on Computational Intelligence and Security (CIS) (December 2015), 340-344, IEEE.

[Yang et al. 2018] Yang, X., Li, Y., Chen, C., Xiao, L., Wang, C.: "Cryptanalysis and improvement of three certificateless aggregate signature schemes"; Mathematical Problems in Engineering, 2018.

[Yang et al. 2018(a)] Yang, X., Wang, J., Ma, T., Li, Y., Wang, C.: "A short certificateless aggregate signature against coalition attacks"; Plos one, 13, 12, e0205453, 2018.

[Yang et al. 2018(b)] Yang, X., Chen, C., Ma, T., Li, Y., Wang, C.: "An improved certificateless aggregate signature scheme for vehicular ad-hoc networks"; In 2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC) (October 2018), 2334-2338.

[Yang et al. 2020] Yang, W., Wang, S., Mu, Y.: "An enhanced certificateless aggregate signature without pairings for E-Healthcare system"; IEEE Internet of Things Journal, 8, 6, 5000-5008, 2020.

[Yang et al. 2022] Yang, X., Chen, A., Wang, Z., Du, X., & Wang, C.: "Cryptanalysis of an efficient and secure certificateless aggregate signature-based authentication scheme for vehicular ad hoc networks"; Security and Communication Networks, 2022.

[Yang et al. 2023] Yang, X., Wen, H., Diao, R., Du, X., & Wang, C.: "Improved Security of a Pairing-Free Certificateless Aggregate Signature in Healthcare Wireless Medical Sensor Networks"; IEEE Internet of Things Journal, 2023.

[Ye et al. 2021] Ye, X., Xu, G., Cheng, X., Li, Y., Qin, Z.: "Certificateless-based anonymous authentication and aggregate signature scheme for vehicular ad hoc networks"; Wireless Communications and Mobile Computing, 2021.

[Yuan et al. 2023] Yuan, B., Huang, H., & Wu, C.: "A New Conditional Privacy-Preserving Certificateless Aggregate Signature Scheme in the Standard Model for VANETs"; Mathematics, 11, 23, 4766, 2023.

[Zhan et al. 2020] Zhan, Y., Wang, B., Lu, R.: "Cryptanalysis and Improvement of a Pairing-Free Certificateless Aggregate Signature in Healthcare Wireless Medical Sensor Networks"; IEEE Internet of Things Journal 8, 7, 5973-5984, 2020.

[Zhan and Wang 2019] Zhan, Y., Wang, B.: "Cryptanalysis of a certificateless aggregate signature scheme for healthcare wireless sensor network"; Security and Communication Networks, 2019.

[Zhang et al. 2006] Zhang, Z., Wong, D., Xu, J., Feng, D.: "Certificateless public-key signature: security model and efficient construction"; In J. Zhou, M. Yung, F. Bao (Eds.), ACNS 2006, LNCS 3989, Springer-Verlag, Singapore, 2006, 293-308.

[Zhang et al. 2010] Zhang, L., Qin, B., Wu, Q., Zhang, F.: "Efficient many-to-one authentication with certificateless aggregate signatures"; Computer Networks 54, 14, 2482-2491, 2010.

[Zhang et al. 2014] Zhang, F., Shen, L., Wu, G.: "Notes on the security of certificateless aggregate signature schemes"; Information Sciences, 287, 32-37, 2014.

[Zhang et al. 2015(a)] Yu-lei, Z., Chen-yi, L., Cai-fen, W., Yong-jie, Z.: "Security Analysis and Improvements of Certificateless Aggregate Signature Schemes"; Journal of Electronics and Information Technology, 37, 8, 1994-1999, 2015.

[Zhang et al. 2015(b)] Zhang, Y., Wang, C.: "Comment on new construction of efficient certificateless aggregate signatures"; International journal of security and its applications, 9, 1, 147-154, 2015.

[Zhang et al. 2016(a)] Zhang, J., Zhao, X., Mao, J.: "Attack on Chen et al.'s certificateless aggregate signature scheme"; Security and communication networks, 9, 1, 54-59, 2016.

[Zhang et al. 2016(b)] Zhang, H.: "Insecurity of a certificateless aggregate signature scheme"; Security and communication Networks, 9, 11, 1547-1552, 2016.

[Zhang and Zhang 2008] Zhang, L., Zhang, F.: "Security model for certificateless aggregate signature schemes"; In 2008 International Conference on Computational Intelligence and Security (December 2008) 2, 364-368, IEEE.

[Zhang and Zhang 2009] Zhang, L., Zhang, F.: "A new certificateless aggregate signature scheme"; Computer Communications 32, 6, 1079-1085, 2009.

[Zhao et al. 2020] Zhao, Y., Hou, Y., Wang, L., Kumari, S., Khan, M. K., Xiong, H.,: "An efficient certificateless aggregate signature scheme for the Internet of Vehicles"; Transactions on Emerging Telecommunications Technologies 31, 5, e3708, 2020.

[Zhao et al. 2020(a)] Zhao, N., Zhang, G., Gu, X.: "Certificateless aggregate signature scheme for privacy protection in VANET"; Computer Engineering, 46, 1, 114-128, 2020.

[Zheng et al. 2023] Zheng, H., Luo, M., Zhang, Y., Peng, C., & Feng, Q.: "A Security-Enhanced Pairing-Free Certificateless Aggregate Signature for Vehicular Ad-Hoc Networks"; in IEEE Systems Journal, 17, 3, 3822-3833, 2023.

[Zhong et al. 2019] Zhong, H., Han, S., Cui, J., Zhang, J., Xu, Y.: "Privacy-preserving authentication scheme with full aggregation in VANET"; Information Sciences, 476, 211-221, 2019.

[Zhou et al. 2014] Zhou, M., Zhang, M., Wang, C., Yang, B.: "CCLAS: A Practical and Compact Certificateless Aggregate Signature with Share Extraction"; Int. J. Netw. Secur., 16, 2, 157-164, 2014.

[Zhou et al. 2020] Zhou, F., Li, Y., Lin, C.: "A Revocable Certificateless Aggregate Signature Scheme with Enhanced Security. Int. J. Netw. Secur., 22, 4, 645-654, 2020.

[Zhou & Yin 2022] Zhou, L., & Yin, X.: "An improved pairing-free certificateless aggregate signature scheme for healthcare wireless medical sensor networks"; Plos one, 17, 7, e0268484, 2022.

[Zhu et al. 2022] ZHU, D., YIN, X., & NING, J.: "Certificateless signature scheme with strong privacy protection for internet of vehicles"; Journal of Computer Applications, 42, 10, 3091, 2022.