

On Advances of Anonymous Credentials—From Traditional to Post-Quantum

Author

Chathurangi, Madusha, Li, Qinyi, Foo, Ernest

Published

2025

Journal Title

Cryptography

Version

Version of Record (VoR)

DOI

[10.3390/cryptography9010008](https://doi.org/10.3390/cryptography9010008)

Rights statement

© 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Downloaded from

<https://hdl.handle.net/10072/435105>

Griffith Research Online

<https://research-repository.griffith.edu.au>



Review

On Advances of Anonymous Credentials—From Traditional to Post-Quantum

Madusha Chathurangi , Qinyi Li * and Ernest Foo

School of Information and Communication Technology, Griffith University, Brisbane 4111, Australia; madusha.chathurangi@griffithuni.edu.au (M.C.); e.foo@griffith.edu.au (E.F.)

* Correspondence: qinyi.li@griffith.edu.au

Abstract: Anonymous credential (AC) systems are privacy-preserving authentication mechanisms that allow users to prove that they have valid credentials anonymously. These systems provide a powerful tool for several practical applications, such as anonymous payment systems in e-commerce, preserving robust privacy protection for users. Most existing AC systems are constructed using traditional number-theoretic approaches, making them insecure under quantum attacks. With four decades of research in anonymous credential systems, there is a need for a comprehensive review that identifies the design structures of AC systems, organizes the research trends, and highlights unaddressed gaps for the future development of AC, especially bringing AC to post-quantum cryptography. This work is a complete study describing AC systems, as well as their architecture, components, security, and performance. Additionally, real-world implementations of various applications are identified, analyzed, and compared according to the design structure. Lastly, the challenges hindering the shift toward the quantumly secure lattice-based AC designs are discussed.

Keywords: anonymous credential; authentication; quantumly secure anonymous credentials

1. Introduction

In 1976, Wilfred Diffie and Martin Hellman introduced digital signatures [1], which are widely used in authentication systems for e-signatures, e-passports, e-ticketing, and several other applications. However, verifying digital signatures necessitates disclosing users' attributes, including their name, age, and address. Hence, digital signatures are not enough to address specific scenarios, and there is a growing demand for systems that allow customers to request services from providers without revealing their private information. For example, consider an online forum that requires users to verify their adult status before participating. In such a scenario, the verifier only needs to check that the user is over 18 years old without requiring knowledge of the user's age, name, or other personal details. With digital signatures, the service needs to verify the user's identity and check their date of birth to ensure the user is an adult. This raises privacy concerns, allowing the service to track users' future activities or phishing. To overcome these kinds of concerns, by bridging authenticity and privacy, the two seemingly orthogonal security concepts for practical applications, anonymous credential (AC) systems have been introduced.

AC systems enable users to prove their possessions of valid credentials while keeping the privacy of their other undisclosed attributes. As an example, AC systems can be used to address the aforementioned issue; the forum can confirm the user's status as an adult without knowing other personal information unnecessary to the service, thus protecting users' privacy. For another example, ACs can be applied to electronic voting systems to



Received: 30 November 2024

Revised: 16 January 2025

Accepted: 23 January 2025

Published: 26 January 2025

Citation: Chathurangi, M.; Li, Q.; Foo, E. On Advances of Anonymous Credentials—From Traditional to Post-Quantum. *Cryptography* **2025**, *9*, 8. <https://doi.org/10.3390/cryptography9010008>

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

enable voters to prove their eligibility for voting without disclosing their identities, ensuring privacy and maintaining the integrity and confidentiality of the election process. Research has indicated that AC systems play a crucial role in various real-world applications such as decentralized identity authentication [2], healthcare systems [3], payment systems [4,5], and so on and so forth.

AC systems were first proposed by Chaum [6], initially referred to as pseudonym systems. Later, AC systems were developed into well-defined attribute-based credential systems. In an attribute-based AC system, as depicted in Figure 1, three primary entities are involved: users, organizations (signers), and service providers (verifiers). The user holds anonymous credentials signed and issued by the service organization, and the service provider verifies the validity of the credentials. The core concept revolves around users having a set of attributes, and then organizations are responsible for issuing credentials to users for their attributes. Once receiving the credential, users can prove their possession of the credential to the verifier and gain service access. Unlike digital signatures, which directly link the signature to the signer's (user) identity, AC systems allow users to prove their knowledge of the message–signature pair without revealing their identity. Hence, digital signatures are not generally anonymous; AC systems provide users with anonymity. In contrast to blind signatures, where the user unblinds the message during verification, AC systems allow users to selectively disclose only the necessary attributes without revealing the entire message. Although group signatures provide anonymity for group members, the group manager can revoke this anonymity if needed. However, anonymous credentials require full anonymity for users. These examples ensure AC systems differ fundamentally from other commonly used privacy-preserving cryptographic primitives.

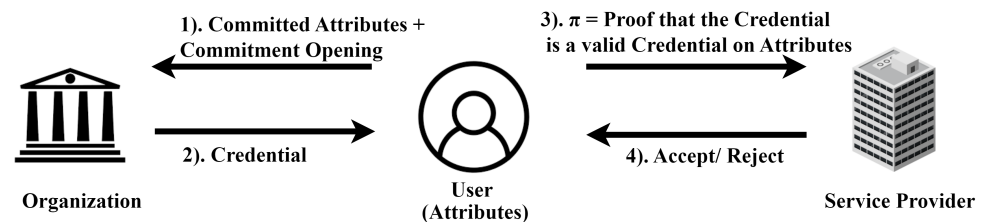


Figure 1. Basic structure of the attribute-based AC scheme: **(Step 1)** The user shares committed attributes with the organization. **(Step 2)** The organization issues a credential on committed attributes. **(Step 3)** The user proves the knowledge of the credential. **(Step 4)** The service provider verifies the credentials.

1.1. Our Contribution

With four decades of research in anonymous credential systems, there is a need for a comprehensive review of the development, design principles, security properties, and relevant applications of AC. The contribution of this paper is fourfold. First, we provide a comprehensive review of the evolution of AC schemes from its start to the most recent development, identifying the necessary cryptographic primitives, key features, security notions, and efficiency for AC schemes. Second, we propose a construction-based approach to AC design principles. Our framework separately identifies AC design principles in the primary model and practical applications. Third, we investigate the most recent development in post-quantum AC schemes from lattices. Finally, we identify gaps in AC designs, particularly concerning the latest trends in post-quantum AC schemes that have not yet been addressed—a key area for future research.

Comparison with Kakvi et al.'s Recent Work

To the best of our knowledge, the only survey on AC is by Kakvi et al. [7]. Our work substantially differs from Kakvi et al.'s and brings new insights. We summarize the distinctive aspects of our work below.

- **Design Principles:** We propose a construction-based approach to AC design principles, focusing on the structure of AC schemes. We classify AC schemes in two dimensions, the design structure and application, which helps to unify and guide the design of the AC scheme.
 1. **Design Structures of Basic AC Schemes:** We identify four design structures of the basic AC model: single-attribute AC, multi-attribute AC, multi-authority AC, and credential-modifiable AC. For each category, we identify the cryptographic primitives needed for the constructions. In addition, we highlight the associated advantages and disadvantages.
 2. **Application-Oriented Design Principles for Practical Use:** We identify four major application-oriented types of AC: traceable AC, revocable AC, delegatable AC, and decentralized AC. We outline each type's cryptographic principles used in the key designs.
- **Post-Quantum AC Schemes:** Recently, with the advancement of quantum computing, cryptography research has significantly focused on post-quantum solutions. Among post-quantum cryptographic approaches, lattice-based cryptography has gained prominence, especially due to NIST standardization [8] of lattice-based key encapsulation mechanisms (KEMs) and digital signatures. As a result, the design and analysis of post-quantum AC schemes from lattices have become increasingly important. Here, we provide a qualitative and quantitative analysis of the most recent proposed lattice-based AC schemes.
- **Real-World Applications:** We identify the real-world applications of AC systems and provide a comparative analysis of the security notions achieved by the applications.
- **Open directions including Quantum-Resistant AC Schemes:** Most AC systems are based on discrete-log-related problems and will become insecure with large-scale quantum computers. We identify research gaps based on the most recent development of post-quantum AC schemes, which is not covered in Kakvi et al. [7].

To conclude, Kakvi et al.'s work [7] provides an analysis of attribute-based AC systems and their features; our survey, being different from Kakvi et al. [7], takes a constructive approach by focusing on the design principles of AC that enable security and different application features for practical AC systems. First, we elaborate on how these design principles work, which allows readers to understand the fundamental mechanisms involved in constructing AC systems. Moreover, our review is more beneficial as it addresses the emerging domain of post-quantum AC systems, a topic that is becoming increasingly important with the advancements in quantum computing. Kakvi et al.'s work only covers the AC systems that are based on the traditional number-theoretic problems, e.g., integer factoring and discrete logarithm problems, and is hence insecure with the advent of quantum computers [9]. To make AC resistant to quantum attacks, it is necessary to design and implement AC systems (including their components) using new post-quantum objects, e.g., lattice-based ZKPs that prove the knowledge of digital signatures. In this work, we analyze existing post-quantum lattice-based AC systems systematically, identify their limitations, and explore open research directions in post-quantum AC.

1.2. Road Map

The subsequent sections of this paper are organized as follows. Moving on to Section 2, we identify three different trends in designing AC systems from 1985 onwards. Section 3 provides an analysis of the design of AC schemes with a complete categorization highlighting fundamental cryptographic primitives needed for each structure. Section 4 provides a security analysis of existing AC systems, and Section 5 provides a quantitative analysis of performance. Finally, we discuss the real-world applications of AC schemes and identify open directions in Section 6.

2. Evolution of Anonymous Credential Schemes

In this section, we will discuss the evolution of AC systems, which can be divided into three main parts: classical pseudonym systems before the booming of pairing-based cryptography, advances in pairing-based AC schemes, and new developments of AC focusing on post-quantum security. We will cover the design structure of each type, along with respective benefits and drawbacks and areas that need improvement.

2.1. Early Development

The concept of AC stems from the work of Chaum [6], which was initially termed as pseudonym systems. While Chaum's seminal paper introduced the concept, it did not provide formal definitions, constructions, or security requirements; however, Chaum's pioneering work laid out the fundamental idea of utilizing digital signature schemes for signing. Chaum and Evertse [10] constructed a pseudonym system based on RSA, which bears full trust to a trust center that transfers all credentials. Damgård addressed the trust issue using multi-party computations, limiting the trusted center's job to pseudonym validation, i.e., ensuring each pseudonym links to some legitimate user but with an inefficient zero-knowledge system.

Chen [11] proposed another pseudonym system based on the discrete-log problem (DLog) in which the trust center participants in credential transfer must be, again, trusted to behave honestly. Lysyanskaya et al. [12] formalized a pseudonym system that minimizes the trust to the trust center and gives a construction from the DLog problem. This work marked a significant step forward in the evolution of AC schemes as it sets out the basic structure and security requirements for the subsequent pseudonym and AC systems.

Design of Pseudonym Systems: A pseudonym system allows users to maintain privacy while interacting with multiple organizations. In this system, the user possesses a single master secret key (msk) from which the user can generate multiple public keys, known as pseudonyms. As shown in Figure 2, an issuer (organization) issues a credential to a pseudonym (nym_1) attached to the user. The user can then prove possession of this credential to a verifier under a different pseudonym (nym_2) without revealing user identity [12–15]. It is important to note that the nym s should be unlinkable to one another.

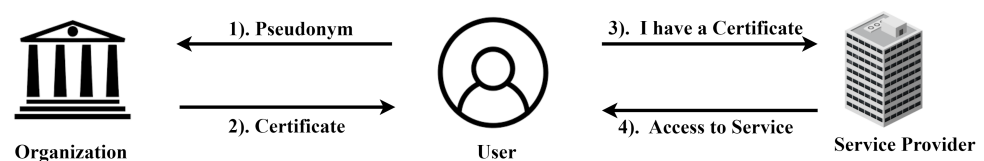


Figure 2. Basic structure of the pseudonym system: (Step 1) The user shares the pseudonym with the organization. (Step 2) The organization issues a certificate. (Step 3) The user proves the knowledge of the certificate. (Step 4) The service provider verifies the certificate and gives access to the service.

Subsequent advancements [16,17] in AC systems introduced several notable features. Firstly, the limitation of one-show credentials in pseudonym systems was addressed by Brands [16] with the first multi-show pseudonym system. Secondly, the evolution from a pseudonym system to an attribute-based AC system [16] enabled users to possess multiple attributes, enhancing anonymity. Thirdly, AC systems with selective attribute disclosure [17] emerged as a crucial enhancement, allowing users to retain privacy by revealing only a subset of their attributes to verifiers while keeping the rest concealed. These advancements have greatly improved the flexibility, security, and confidentiality of AC systems, meeting diverse application requirements.

2.1.1. Formalizing Attribute-Based Anonymous Credential Systems

The early research of pseudonym systems [12] led to the basic structure, as shown in Figure 2. It also forms today’s widely accepted definition of modern AC systems, Definition 1, due to Fuchsbaauer et al. [18]. In an AC system, the user and the organization generate their keys; the user who holds a set of attributes runs the protocols (Obtain, Issue) with the organization to receive a credential to these attributes from the organization; then, the user runs the protocols (Show, Verify) with the verifier (also known as the service provider) to show its credential for verification. This structure and system definition are adapted by the most recent AC system constructions [18–23].

Definition 1 ([18]). Let λ be the security parameter and $A = [A_i]_{i \in [\ell]}$ be a set of attributes with $\ell > 0$ as the size of the array of attributes the organization will certify. An anonymous credential system is defined as follows:

- $(\text{opk}, \text{osk}) \leftarrow \text{OrgKeyGen}(1^\lambda)$: A probabilistic algorithm that outputs the organization’s public key opk and private key osk .
- $(\text{upk}, \text{usk}) \leftarrow \text{UserKeyGen}(1^\lambda)$: A probabilistic algorithm that outputs the user’s public key upk and private key usk .
- $(\text{cred} / \perp) \leftarrow (\text{Obtain}(\text{opk}, \text{usk}, A), \text{Issue}(\text{osk}, \text{upk}, A))$: An interactive protocol that outputs the credential (cred) over attribute set A or an error symbol \perp .
- $(1/0, \perp) \leftarrow (\text{Show}(\text{usk}, A, D, \text{cred}), \text{Verify}(\text{opk}, D))$: An interactive protocol that verifies the credential over that subset (D) of attributes (A). The protocol outputs 1 if the cred is a valid credential over $D \subset A$ and returns 0 otherwise.

An anonymous credential scheme is correct if for any ϵ negligible in λ , it holds that

$$\Pr \left[\begin{array}{l} (\text{opk}, \text{osk}) \leftarrow \text{OrgKeyGen}(1^\lambda), \\ (\text{upk}, \text{usk}) \leftarrow \text{UserKeyGen}(1^\lambda), \\ \text{cred} \leftarrow (\text{Obtain}(\text{opk}, \text{usk}, A), \text{Issue}(\text{osk}, \text{upk}, A)), \\ 1 \leftarrow (\text{Show}(\text{usk}, A, D, \text{cred}), \text{Verify}(\text{opk}, D)) \end{array} \right] \geq 1 - \epsilon$$

where the probability is taken over the random coins of the algorithms.

2.1.2. Cryptographic Components for Anonymous Credential Systems.

The early research of pseudonym systems and attribute-based AC systems also contributes to the formal security definitions of modern AC systems. They especially enlighten the fundamental cryptographic primitives [13] that are needed to build AC systems to meet the requirements of real-world applications.

There are three fundamental cryptographic primitives identified for a basic AC system—cryptographic commitment, digital signatures, and zero-knowledge proofs—usually compatible with a cryptographic commitment scheme and a digital signature system.

A commitment scheme allows one to commit a message, which can be opened later by the message holder. It requires that (1) the commitment hides the message, known as hiding property, and (2) any commitment cannot be opened into another message different from the committed one, known as the binding property. As shown in Figure 3, when it comes to an AC, the user usually uses a commitment scheme to commit attributes without revealing them directly to the signer. The commitment scheme serves two key purposes: ensuring the attributes cannot be changed once committed (binding property) and keeping them concealed from the signer (hiding property). Famous commitment schemes, such as Pedersen [24], Fujisaki and Okamoto [25], and Moni Naor’s bit commitment [26], were used in the early pseudonym systems.

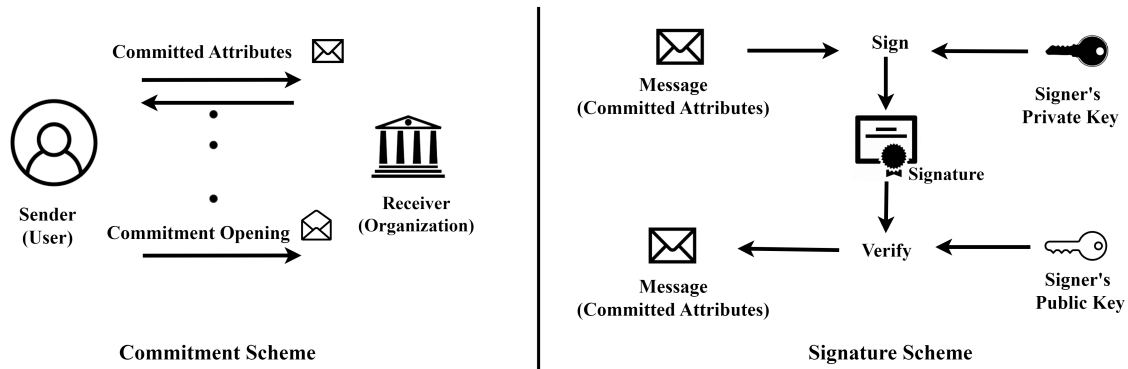


Figure 3. Illustration of a commitment scheme (left) and signature scheme (right) in an AC system.

A (digital) signature system is a public-key cryptosystem in which the private key holder can digitally sign messages to obtain signatures that are verifiable using the user’s public key. A digital signature cannot be produced without the private key, known as the unforgeability property. In an AC system, the organization utilizes a signature scheme to endorse the (committed) attributes by signing the attribute commitments. The unforgeability ensures that no one can forge the endorsements. Classical pseudonym systems used signature schemes such as RSA signature [27], Fiat–Shamir signature [28], Schnorr’s signature [29], Brand’s signature [16], and Bellare and Micali’s BM signature [30,31].

A zero-knowledge proof (ZKP) system is a cryptographic protocol that enables one party (the prover) to demonstrate possession of certain information to another party (the verifier) without disclosing the actual information itself. As depicted by Figure 4, a ZKP system in an AC scheme is used by the user for dual purposes: (1) to prove the knowledge of committed attributes to the signer and (2) to demonstrate the knowledge of the message–signature pair to the verifier. It typically requires three security notions: completeness, soundness, and zero knowledge. It should be noted that there exists an interactive version and a non-interactive version of ZKPs. The former requires interactions [32] between the prover and the verifier, while the latter does not. When applying to AC, they correspond to interactive or non-interactive verification of commitment/credential. The choice shall depend on the application’s needs.

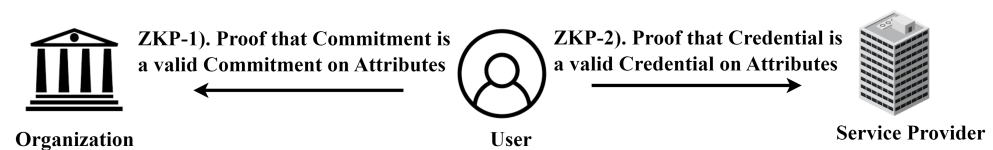


Figure 4. Illustration of two zero-knowledge proofs in an AC system. (ZKP-1) Zero-knowledge proof used in (Obtain, Issue) protocol. (ZKP-2) Zero-knowledge proof used in (Show, Verify) protocol.

2.1.3. Summary

The early stage of development of AC systems determined a high-level design blueprint for constructing AC systems satisfying intuitive security requirements. However, these early systems contain drawbacks from both security and construction perspectives.

Security-wise, the early systems do not have clear and clean security definitions (especially formal adversarial models) for what is known now as the fundamental security properties of AC systems: credential unforgeability, credential unlinkability, and anonymity. In the early systems, the security requirements were argued to be met by the security of the individual underlying cryptographic primitives in ad hoc ways. In addition, the early developments of AC systems did not extend to achieve many useful features for practical applications, such as traceability, signer hiding, and credential revocation.

Construction-wise, the early systems fall short in scalability. For example, in scenarios where credentials are obtained from multiple organizations or credentials for multiple attributes, the size of credentials grows linearly with the number of organizations and the number of attributes. This limits the efficiency of the AC systems. Meanwhile, the early systems seemed to have difficulty enabling the aforementioned useful security properties. The fundamental obstacle to these is that the underlying building blocks lack flexible algebraic properties, which are offered by pairing-based cryptography.

2.2. Enhancement from Pairing-Based Cryptography

Pairing-based cryptography significantly advances the research of AC systems in nearly all the dimensions that the early systems fell short of: security, efficiency, and functionality.

The design of AC schemes has significantly improved through pairing-based digital signatures and zero-knowledge proof systems. Pairing-based signatures use pairings (also known as bilinear maps) from elliptic curves over finite fields. Their security is based on the elliptic curve Dlog problem, which has a much shorter parameter size than that of the Dlog problem over finite fields on integers for the same security level. The key sizes and signature sizes of pairing-based signature systems can be as short as 320 bits [33,34], which helps make anonymous credentials short and reduce the computational overhead. Another important feature of pairing-based signatures is that they work well with the versatile pairing-based ZKPs [35,36]. The combination of pairing-based signatures (examples: aggregate signatures [23,37], CL signatures [14,38], redactable/sanitizable signatures [22,39,40], and structure-preserving signatures [18,41]) and their compatible ZKPs shows great power in the design of AC systems.

Pairing-based AC systems have a distinct advantage when it comes to credential aggregation. Traditional AC schemes struggle to deal with situations where users hold credentials from multiple issuers and prove their knowledge of each signature to a verifier. This results in larger proof sizes due to separate proofs for each credential. As illustrated in Figure 5, with pairing-based aggregate signatures for AC schemes [23,37], a user can combine multiple signatures from different issuers into a single signature. The critical advantage of these schemes is that even when aggregating several signatures, they still end up with a constant-sized credential, keeping the prover cost independent of the number of attributes and issuers.

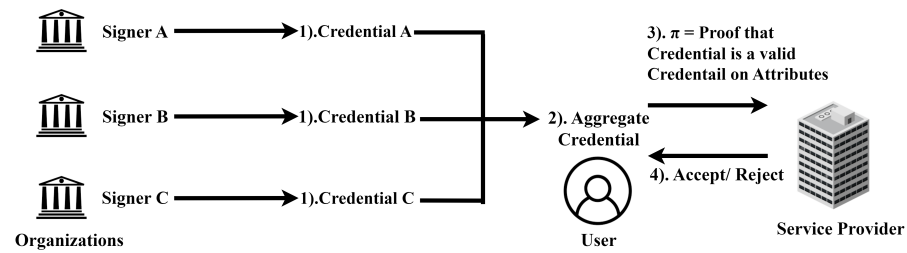


Figure 5. AC system based on aggregate signature: **(Step 1)** User obtains credentials A, B, and C from three different organizations. **(Step 2)** User aggregates the credentials into one. **(Step 3)** User proves the knowledge of the aggregate credential. **(Step 4)** The service provider verifies the credentials.

Initially, the early progress in AC systems encountered challenges in modifying or hiding certain parts of the issued credentials, necessitating users to present all information to the verifier. Pairing-based signatures addressed this issue with redactable signatures and sanitizable signatures. As depicted in Figure 6, redactable-signature-based AC systems [22,39] have the ability to selectively conceal or remove specific parts of the credential while proving the validity of the remaining information. Similarly, sanitizable signatures [40] allow, once a credential for ℓ attributes is received, the user (known as a sanitizer) to modify the signature for k out of ℓ attributes. However, the most efficient approach lies in constant-size redactable/sanitizable AC systems [22] instead of linearly growing ones, which are particularly beneficial for applications such as membership or age verification, which usually do not want to reveal personal information to the verifier.

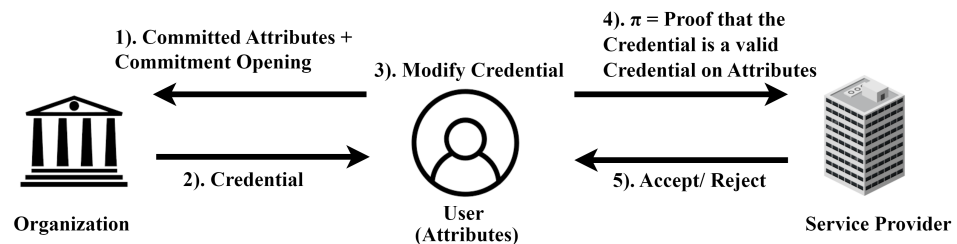


Figure 6. AC system based on redactable/sanitizable signature. **(Step 1)** User shares committed attributes with the organization. **(Step 2)** Organization issues a credential. **(Step 3)** User modifies the credential. **(Step 4)** User proves the knowledge of the credential. **(Step 5)** The service provider verifies the credentials.

Thus far, AC systems have proved secure using the security of individual cryptographic primitives, signature, commitment, and zero-knowledge proof, which is unsuitable as it does not define attackers and corresponding security goals for the whole system. However, pairing-based AC systems identified two fundamental security notions, unforgeability and anonymity, and these notions are analyzed in Section 4. Another feature added in pairing-based signatures to AC systems is randomization, which allows the user to randomize the credential once received, so different showings of the same credential cannot be linkable.

When deploying AC systems, several practical issues need to be considered. We discuss some examples of AC systems that have been successfully constructed using pairings to address these issues. Revocable AC systems are designed for situations where attributes in credentials may become outdated, or users may no longer be authorized to hold a specific credential. Partial revocation may also be necessary, such as when certificates are valid only for a particular period and must be revoked accordingly, such as electronic ID [42]. As digital cash [4], traceable AC systems have been proposed for applications where a tracing authority must track or link a user's activities while maintaining the user's anonymity. Additionally, delegatable AC systems enable users to delegate credentials,

such as in access control [43,44]. Furthermore, signer-hiding AC systems [45,46] were designed for specific applications, such as national eIDs and remote attestations. Section 3.2 summarizes how these features were added, and the corresponding applications are listed in Section 6.1.

In conclusion, the rich structure of pairing-based signatures has added several properties that the classical AC systems have not achieved. However, the AC systems discussed thus far rely on computational problems whose hardness is ultimately based on the difficulties of solving the LRSW assumption (named after its authors [12]) and the bilinear Diffie–Hellman assumptions, such as BDH, DBDH, and DHBDH problems. These problems are known to be vulnerable to quantum attacks [9] and will be broken if large-scale quantum computers become available. Following the effort of transitioning classically secure public-key encryption and digital signature systems to quantum-resistant ones, exploring quantum-resistant AC systems is well motivated.

2.3. Next-Generation Post-Quantum

As mentioned, the development of quantum computing presents a vital threat to most of the existing AC systems due to them being based on quantumly tractable problems. This motivates the study of designing AC systems from computational problems that are not efficiently solvable by quantum computers, which are hard computational problems on high-dimensional lattices. To the best of our knowledge, four lattice-based AC schemes have been introduced recently ([19–21,47]), and a comparison of the designs of these schemes is provided in Section 5.

These recent constructions of lattice-based AC systems also follow the structural design of combining the three main cryptographic primitives: commitment, signature, and their compatible zero-knowledge proofs. Jeudy et al. [21] introduced a lattice-based AC system under the short integer solution problem and learning with errors problem over module lattices (respectively known as the MSIS problem and MLWE problem) (module lattices are a family of lattices that generalize the integer lattices and ring lattices). The construction modifies Libert et al.'s [48] zero-knowledge proof system for Boyen's signature scheme [49] with more efficient proving systems, leading to a noticeable reduction in credential size, equivalent to 30 times less than using the original protocol by Libert et al. [48].

Another lattice-based AC scheme by Bootle et al. [19] introduces a new hard problem called Inhomogeneous Shortest Integer Solution (ISIS_f), unlike previously discussed schemes based on MSIS and Ring LWE. The ISIS problem asks to find a short non-zero vector over a system of linear equations modulo some vector. In contrast, the new problem ISIS_f asks to find a short non-zero vector over a system of linear equations modulo a target function f . The entire scheme [19] is based on the ISIS_f assumption, making the security of the scheme more challenging to analyze. In fact, the hardness of the ISIS_f problem depends on the choice of the function f , where f is modeled as a random oracle, or else, f is a cryptographic hash function. However, the scheme [19] uses NTRU lattices, which makes it more efficient compared to the previous two schemes [20,21] that used standard and structured lattices.

Lai et al. [20] introduced a commit transferable signature scheme (CTS) for AC based on MSIS and RLWE. The main advantage of this scheme is that it supports pseudonyms and obtains smaller credential sizes compared to the scheme of Jeudy et al. [21]. The scheme [20] (and also the scheme of Bootle et al. [19]) requires multi-theorem straight-line extractability, which allows the prover to extract witnesses directly from multiple pairs of statements of non-interactive zk proofs. In addition, the multi-theorem straight-line extractability makes the system have less soundness error compared to the single-proof extractability proof system with exact soundness error [50].

The aforementioned lattice-based AC systems follow the formal security model of AC established from the pairing-based AC systems. We discuss this matter for lattice-based AC schemes in Section 4. Moreover, we provide a detailed performance analysis of current lattice-based AC schemes in Section 5. In conclusion, lattice-based constructions have yet to be improved to obtain greater efficiency and functionality compared to pairing-based AC schemes, which leaves substantial room for further research, as we will discuss in Section 6.2.

2.4. Summary

In this section, we summarize the development of the AC systems discussed.

Figure 7 highlights the key papers outlining the evolution of AC systems. It is clear that AC schemes introduced before 2023 were primarily based on pre-quantum assumptions, the discrete logarithm problem, and the RSA problem, which are insecure according to Shor's algorithm [9]. In contrast, recent developments focus on post-quantum security, addressing the need for AC schemes resistant to quantum attacks. Despite these advancements, significant challenges and problems remain in designing robust and efficient post-quantum AC systems, as discussed in Section 6.2.

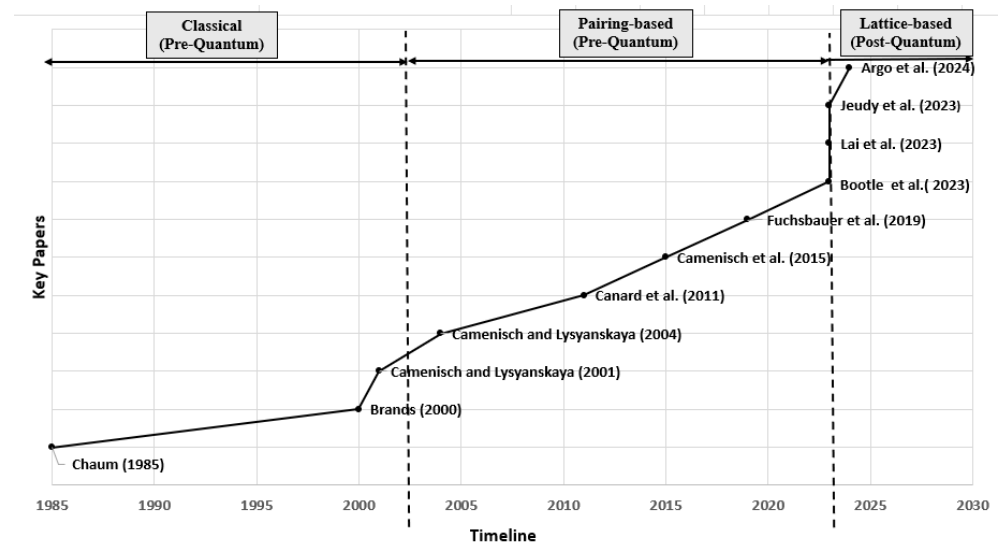


Figure 7. Timeline of key papers on the evolution of anonymous credential systems (1985–present), highlighting key contributions: [6,14,16,18–21,37,39,47,51].

3. Design and Structure of AC Schemes

In this section, we discuss the design of AC systems from the perspectives of system structures of AC and the security properties of AC. This allows us to further categorize AC systems into structural categories and application-oriented categories.

3.1. AC Categorization Based on Design Structure

We categorize existing AC schemes (under the unified notion of attribute-based AC) into four categories depending on their design structures.

1. **Single-Attribute Anonymous Credentials:** As shown in Figure 2, single-attribute AC systems were introduced in the early stages of AC development. In this type of system, users receive one credential for each attribute. While having a simple structure, this type of AC falls short in terms of efficiency; the public/private key sizes, the credential size, and/or the computational overhead of credential verification all increase linearly with the number of attributes if multiple attributes are needed, i.e., users must demonstrate knowledge of each credential for every attribute [52].

2. **Multi-Attribute Anonymous Credentials:** This category, as depicted by Figure 1, refers to the AC systems in which users have multiple attributes, such as name, age, university, and more, being able to obtain a single credential for all of these attributes [16]. Two main types within this category exist: (1) selective disclosure (s) of attributes and (2) proving relations (r) of attributes during the verification process. Selective disclosure allows users to share a subset of their attributes with verifiers while keeping the remaining attributes concealed [18,23,46]. In contrast, proving relationships enables users to demonstrate the connection between their attributes to the verifier [13,22,38].
3. **Multi-Authority Anonymous Credentials:** Both above AC schemes struggle to deal with situations where users hold credentials from multiple issuers and prove their knowledge of each signature to a verifier. This potentially results in larger credential sizes, e.g., linear with the number of issuers, due to separate credentials to be received from different issuers. To address this challenge, aggregate signatures are adopted in the AC system design. AC incorporated with aggregate signatures is depicted in Figure 5. It allows users to combine credentials from multiple organizations into a single credential. The crucial advantage of these schemes is that even when aggregating several signatures, they still end up with a constant-sized credential that is the same length as a single credential, keeping the prover cost independent of the number of issuers while still allowing verification of validities of the credentials [23].
4. **Credential-Modifiable Anonymous Credentials:** This category, as depicted in Figure 6, represents a type of AC system that allows users to modify or hide certain parts of the issued credentials. It is used to overcome challenges encountered when requiring users to present the entire credential or the originally received credential to the verifier. Firstly, self-blinding or re-randomizable signature schemes [46,53] are the primary cryptographic primitives used for this type of AC. Once a user obtains a credential from an issuer, the user can randomize the credential into a new credential under the same attributes. Hence, they often make the AC system multi-show-unlinkable. Secondly, redactable [22,39] or sanitizable [40] signatures are the main cryptographic primitives that enable credentials to be modifiable. They introduce the ability to conceal or remove specific parts of the credential selectively while proving the validity of the remaining information. Similarly, sanitizable signatures allow, once a credential for ℓ number of attributes is received, the user (known as a sanitizer) to modify the signature for k out of ℓ attributes. The most efficient approach lies in constant-size redactable/sanitizable AC systems instead of linearly growing ones, which are particularly beneficial for applications such as membership or age verification.

3.2. AC Categorization Based on Additional Properties

When it comes to practice, AC schemes usually need extra properties other than the basic security properties discussed before depending on the requirements of real-world applications. We identified that traceability, revocation, delegation, and decentralization are the widely used practical AC properties, and we give design guidelines for each mechanism.

3.2.1. Traceable Anonymous Credentials (TACs)

In real-world settings, users in AC systems may misbehave while remaining anonymous. Hence, there should be a mechanism in place to trace misbehaviors. Traceable anonymous credentials (TACs) are an extension of the AC framework designed to enable the tracing and de-anonymization or blacklisting of malicious users who violate the system's rules. The purpose is to achieve two simultaneous notions of security: anonymity and accountability (also known as traceability).

The concept of TAC was proposed in 2001 by Camenisch and Lysyanskaya [51]. As depicted in Figure 8, a TAC system relies on a trusted third party (TTP), also known as tracing authority (TA), which is only involved when there is a request to reveal the user's identity. However, the existing TACs do not allow the tracing authority to make decisions about tracing results; instead, another algorithm Judge is used to reveal the identities of the users who have been traced once the tracing process is completed. The security aspect of this concept is referred to as *non-frameability* in the context of TACs, which ensures that no party, including the credential issuer, can unjustly accuse or incriminate an honest user. This guarantees that no one can falsely generate a valid trace or proof of a user's credential usage without the user's participation. While TACs have been based on prior efforts in non-quantum settings [23,40,51,54], the challenge of building quantumly secure TAC schemes remains relatively new.

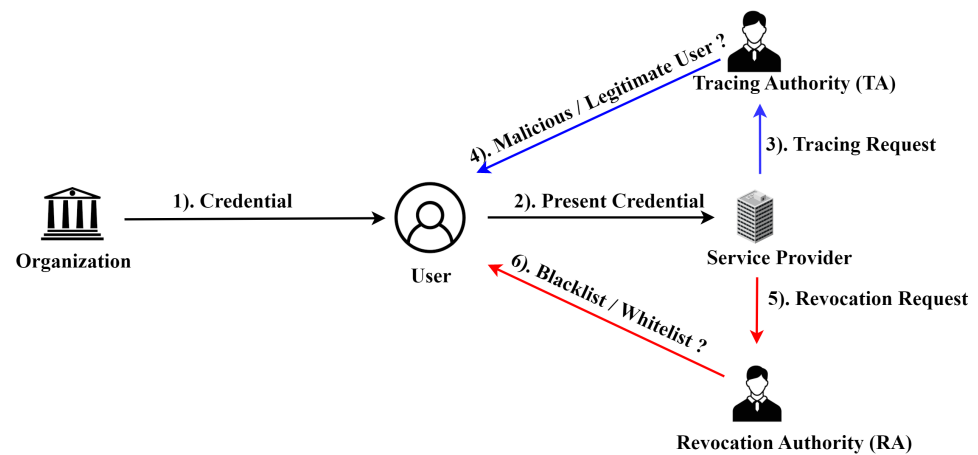


Figure 8. Basic structure of traceable/revocable AC scheme: (**Tracing Process**) (1) A user obtains a credential from the organization. (2) The user undergoes verification with the service provider. (3) The service provider requests tracing. (4) The TA determines whether the user is malicious or legitimate. (**Revocation Process**) (1) A user obtains a credential from the organization. (2) The user undergoes verification with the service provider. (5) The service provider requests revocation. (6) The RA determines whether the credential is valid or invalid.

3.2.2. Revocable Anonymous Credentials (RACs)

RACs are important when the attributes of the credentials may change or expire or users may hold invalid credentials. Therefore, a mechanism should be in place to remove malicious or outdated credentials. RAC systems address this requirement by performing membership revocation for users who hold invalid credentials. The purpose of RACs is to determine whether a user's credential is valid and, if not, revoke the credential to make it non-verifiable. We identify five types of revocation mechanisms:

1. **Setting Expiry Dates:** This is the type of RAC where the credential issuer sets expiration dates for each credential, which becomes outdated after a specific period. Therefore, the user has to request a new credential from the issuer once it expires, which is inefficient because the user has to request new credentials every time they expire. However, if the issuer introduces a mechanism to update all the credentials without user interaction, the user will be able to download the updated version before the authentication. The protocol proposed by Camenisch et al. [42] introduces a method to update the credential once issued without requiring interaction between the user and the issuer.
2. **Blacklist/Whitelist:** An additional entity, referred to as the revocation authority (RA), is introduced for the purpose of revocation. This entity may be a trusted third party

- (TTP), issuer, or verifier. Each credential is associated with a unique identifier, which can be categorized under a whitelist or a blacklist. The RA is responsible for maintaining a list of valid identifiers, known as a whitelist, or a list of invalid identifiers, known as a blacklist. Following the completion of the verification process by the user, the verifier will proceed to confirm whether the user's credentials are present in the whitelist or absent from the blacklist. However, the revocation mechanism can also be implemented without relying on a trusted third party (TTP), as introduced by [55,56].
3. **Cryptographic Accumulator-Based:** The construction of an RAC requires the RA to maintain a large list of identifiers (serial numbers) and continuously update the list, which is sometimes inefficient. To overcome this challenge, dynamic accumulators are introduced [57] to help the RA distribute a short accumulated value instead of a large set of identifiers. The term dynamic refers to an RA being able to add or delete identifiers to the accumulator, and it outputs a short value independent of the number of identifiers. Moreover, the term universal accumulator refers to accumulators which support membership proofs. The accumulator-based RAC systems operate as follows: Each credential is associated with a serial number, and the RA outputs the accumulated value of valid or invalid serial numbers, which it then publishes. When a user goes through the credential verification process, additionally, the user must prove that their credential has not been revoked. Hence, the user must prove that the serial number associated with their credential is included in the accumulated value of valid serial numbers. Alternatively, if the RA publishes the accumulated value of invalid serial numbers, the user must show that their serial number is not included in that accumulated value. Hence, the user has to prove the membership or non-membership of the accumulated value using a zero-knowledge proof [58–60] during the credential Show protocol.
 4. **Verifier-Local Revocation (VLR):** Verifier-local revocation (VLR) is commonly used for group signatures [34,61,62] and was later introduced for anonymous credentials [63]. Here, a trusted third party (TTP) or RA maintains and publishes a list of tokens associated with each credential. Users reveal the proof of knowledge of their tokens to the verifier during authentication. Then, the service provider (verifier) downloads the list of tokens associated with revoked credentials and checks whether the presented token has been revoked.
 5. **Verifiable Encryption (VE):** Verifiable encryption is a public key encryption scheme in which a prover can encrypt a piece of information using the public key of the receiver, and then the prover can convince a third party that the encrypted data satisfy certain properties. The VE-based RAC systems work as follows. In this type, a trusted revocation authority (RA) is involved, and the RA has a public–secret key pair. Let each credential be associated with a unique identifier; the user encrypts the credential identifier using the public key of the RA. After that, the user shares the encrypted version of the credential identifier with the verifier during the credential (Show, Verify) protocol. The verifier does not have direct access to the identifier but knows the encrypted version, so it cannot be decrypted. However, the verifier needs to confirm that the identifier has not been associated with a revoked credential. To achieve this, the verifier sends a request to the RA to check the validity of the identifier. The RA then decrypts the identifier using their secret key, checks whether it is on the revocation list, and informs the verifier about its revocation status. This method ensures that verifiers can verify the validity of credentials [64,65]; however, in VE-based RAC systems, the user put full trust in the RA.

Remark: Alongside the techniques discussed, additional revocation mechanisms such as hash chains [66] and combined methods [67,68] are found in the literature. In particular,

the scheme by Lueks et al. [67] combines verifier-local revocation with setting expiration dates to blacklist misbehaviors. In contrast, the RAC system known as Nymble [66] is designed to blacklist misbehaviors in anonymizing networks, such as Tor. This system utilizes a hash chain; however, it is inefficient because it continuously stores pseudonyms, a collection of nymbles to track the future activities of the same user. In conclusion, various revocation mechanisms exist for AC systems, each suited to different application requirements, with no single approach being better than the others.

3.2.3. Delegatable Anonymous Credentials (DACs)

In the basic AC model, the issuer should always provide the credential directly to the user. However, in practical scenarios, the issuer may delegate their responsibility to authorized delegators, who can then issue credentials to other users. In such cases, users utilize the credentials delegated via a series (chain) of users from the original credential holder. DACs were introduced by Chase et al. [69], which hide the whole delegation chain, that is, the identities of the delegators and the delegates during the credential verification. In this system, the primary issuer is denoted as level 0, with a series of intermediate issuers known as delegators responsible for issuing or delegating credentials from one level to the next. It is crucial to note that despite the credential passing through multiple delegators, the final credential should not expose any information about the intermediate delegators during verification, preserving anonymity. Moreover, it is required that the number of delegations performed does not increase the credential size. Various methods for DACs have been proposed in the literature. The first proposed the DAC system [69], which was later developed by [43] using randomizable proofs. Subsequently, several DAC systems were introduced based on malleable signatures [70] and structure-preserving signatures [44,44].

3.2.4. Decentralized Anonymous Credentials

Traditional AC schemes follow a centralized model; that is, the credential issuer is trusted by the users (credential holders) and service providers. Blockchain technologies have been introduced to AC schemes [2] to overcome this issue, creating a public ledger that decentralizes the issuance process. Users register by submitting their personal information and a self-generated credential to the ledger. Then, servers collect these registration data to identify eligible users. This concept has been further developed into various applications, including blacklisting [71], smart grids [72], and more.

3.2.5. Summary of AC Additional Properties

However, in addition to the above-discussed mechanisms, there are a few extra mechanisms in the literature. Additional parties and cryptographic primitives can be added to enhance the schemes with extra features in practical applications, as outlined in Table 1. Apart from the properties discussed above, we also added AC systems with other properties from the literature.

Table 1. Practical properties achieved in AC schemes.

Property	Description	Mechanism
Non-transferability [51]	Credentials should not be transferable between users.	Certification authority (CA) is introduced.
Traceability [23,40,54].	Ability to trace credentials to prevent misuse.	Tracing authority (TA) is introduced.
Revocability [42,58]	Revoke outdated credentials.	Revocation mechanism is introduced
Delegation [43,44,69,70]	Users can delegate credentials to other users.	A delegation chain/list is introduced.
Issuer Hiding [45,46]	The identity of the credential issuer is hidden.	A set of acceptable issuers/the signing key space is introduced by the verifier (verification policy).
Updatable [73]	After the credential was issued, its attributes were modified.	A protocol (update function) is introduced between the issuer and the user.
Self-Blinding [18]	The credential is randomized by the user before showing.	A randomizable signature scheme is utilized.
Keyed Verification [74]	The issuer of credentials is also the verifier.	A shared key/algebraic MAC is used between the issuer and verifier.

MAC denotes message authentication code.

4. Security of Anonymous Credentials

Attribute-based AC systems generally possess two fundamental security properties: unforgeability and anonymity. Unforgeability ensures that anyone cannot forge a valid credential, emphasizing that only credentials issued by the authorized entity are valid. Anonymity refers to there being no verifier or malicious organization that can identify or learn any information about the user except when possessing a valid credential for disclosed attributes. Beyond these core properties, various additional features are associated with practical applications. For example, property revocation is needed for e-passports, valid only for a specific period; then, the user needs to renew after the expiration date. In contrast, property accountability is required for e-cash systems to trace back an over-spender [4].

In the early stage of AC research, it was emphasized that the overall security of an AC scheme is based on the security of the individual cryptographic primitives used to build the whole AC system [13]. However, this approach was limited as the security model for the AC system may not necessarily reflect all attacking strategies that the adversary may use. Later, Camenisch et al. [39] proposed security notions for AC systems in the Universal Composability (UC) framework proposed by Ran Canetti [75]. Subsequently, in 2019, Fuchsbauer et al. give a formal security model for AC via the widely used game-based definitions, as detailed in [18], which is now one of the most widely adopted security models for AC.

Though it is certainly preferable to formalize the security of AC by treating AC as one primitive (rather than attributing its security simply to the security of its components), it is still very useful to examine how the individual components contribute to the security of AC, especially from a constructive perspective; this guides and motivates the development of cryptographic primitives for AC.

Table 2 summarizes the contribution of each cryptographic primitive in constructing an AC scheme.

Table 2. The basic security notions of anonymous credentials.

Property	Requirement	Cryptographic Primitives
Unforgeability	It should be infeasible to forge credentials. Malicious provers must be prevented.	Signature Scheme: EUF-CMA security ZK Proof System: Soundness
Anonymity	Attributes must not be leaked to the issuer. The secret key must not be leaked.	Commitment Scheme: Hiding Zero-Knowledge Proof System
Unlinkability	Different showings of the credentials cannot be linked.	Zero-Knowledge Proof System/Self Blindable

EUF-CMA denotes the existential unforgeable under chosen message attack.

Hence, it is clear that the construction of an AC scheme necessitates the incorporation of a commitment scheme, a signature scheme, and a zero-knowledge proof system. In conclusion, the reader must select three cryptographic primitives to construct an AC scheme that preserves the following security notions:

1. Commitment Scheme: hiding, binding;
2. Signature Scheme: EUF-CMA security;
3. Zero-Knowledge Proof System: completeness, soundness, zero Knowledge.

Here, the term self-blindable [46,53] refers to the fact that once the user receives the credential for their attributes from the issuer, the user modifies the credential into a new one under the same attributes. This randomization property of signature schemes makes the different showings of the same credential unlinkable. However, many AC schemes generate new zero-knowledge proofs for each showing to obtain a multi-show unlinkability property.

The security of TAC and RAC schemes must meet several security requirements to ensure robust functionality, in addition to the security notions outlined in Table 2. TAC schemes must satisfy two key principles: traceability and exculpability. Traceability ensures that each valid credential can be traced back to a specific (unique) user. Exculpability, also known as non-frameability, guarantees that the TA cannot falsely accuse an honest user of wrongdoing. Similarly, RAC systems have additional security requirements based on their revocation mechanisms. The revocation completeness ensures that an honest user with valid credentials will always pass verification successfully. Moreover, revocation soundness prevents a revoked credential from being incorrectly identified as unrevoked by an adversary, ensuring that the RA can declare valid revocations only. Furthermore, revocation privacy protects the identities of honest users by ensuring that adversaries cannot determine which unrevealed tokens the RA manages.

In the analysis of security models for AC schemes, researchers have used three security models to prove security: the standard model (known as the plain model), the random oracle model (ROM) [76], and the generic group model (GGM) [77]. The choice of a particular security model often depends upon how the security of the underlying signature scheme and zero-knowledge proof system are proved. For example, some AC schemes, such as the one presented in [51], demonstrate security under the standard model, specifically under strong RSA and additional Diffie–Hellman assumptions. However, certain schemes [37,40] utilize the random oracle model (ROM) [76], as security under the standard model is deemed inadequate for signature schemes such as RSA, Diffie–Hellman, Fiat–Shamir, and Schnorr. Conversely, many AC schemes based on pairing-based cryptography have used the generic group model to prove security.

5. Performance Analysis

The efficiency of AC systems has improved significantly from 1985 to the present. In this analysis, we aim to evaluate the performance of three types of AC schemes: classical, pairing-based, and lattice-based. Since classical, pairing-based, and post-quantum AC

systems exist in different dimensions, the analysis varies significantly from one system to another. Several comparisons can be found in the literature for those interested [18,46].

Table 3 presents a comparative analysis of non-quantum AC schemes, underlying assumptions, credential sizes, and security models.

Table 3. Efficiency comparison of anonymous credentials.

Scheme	Main Assumptions	Setting	$ cred $	$ cred $ (KB)	Model
[51]	sRSA, DDH	\mathbb{Z}_N	$3\mathbb{Z}_N$	06.00	SM
[13]	sRSA	\mathbb{Z}_N	$3\mathbb{Z}_N$	06.00	SM
[14]	LRSW, DDH	BG	$(2\ell + 2)\mathbb{G}_1$	21.00	SM
[37]	q -ADHSDH, DDH	BG	$\ell\mathbb{G}_1 + \mathbb{G}_2$	10.50	ROM
[40]	DL, DDH, SDH	BG	$(2\ell + 2)(\mathbb{G}_1 + \mathbb{Z}_p)$	42.00	ROM
[39]	CDH, q -SDH, SXDH	BG	$6\mathbb{G}_1 + 2\mathbb{G}_2 + \mathbb{Z}_p$	04.50	CRS
[53]	LRSW	BG	$(2\ell + 4)(\mathbb{G}_1 + \mathbb{Z}_p)$	44.00	SM
[18]	DDH, q -co-DL	BG	$3\mathbb{G}_1 + \mathbb{G}_2 + 2\mathbb{Z}_p$	03.00	GGM
[22]	DDH, DL	BG	$2\mathbb{G}_1 + 2\mathbb{G}_2$	02.00	GGM
[78]	DL, DDH	BG	$4\mathbb{G}_1$	02.00	GGM
[38]	q -(co-)SDH, SDH	BG	$\mathbb{G}_1 + 6\mathbb{Z}_p$	03.50	SM
[46]	DDH, q -co-DL	BG	$18\mathbb{G}_1 + 3\mathbb{G}_2 + 6\mathbb{Z}_p$	13.50	SM

The terms sRSA, Dlog, DDH, and CDH stand for strong RSA, the discrete logarithm problem, the decisional Diffie–Hellman problem, and the computational Diffie–Hellman problem, respectively. In addition, assumptions LRSW [12], q -SDH [33], and q -ADHSDH [79] were defined in the relevant literature. \mathbb{Z}_N indicates the integer ring for RSA, and BG refers to the asymmetric bilinear maps $\mathbb{G}_1, \mathbb{G}_2$ with a bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ with cyclic groups $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ of order p ; \mathbb{Z}_p denotes the set of integers under modulo p . Here, π denotes the proof of knowledge of the message–signature pair while ℓ denotes the number of attributes. Finally, SM stands for the standard model, CRS stands for the common reference string model, GGM stands for the generic group model, and ROM stands for the random oracle model. Note: For credential size estimations, we assume \mathbb{Z}_N has a 2048-bit size, \mathbb{Z}_p has a 512-bit size, groups \mathbb{G}_1 and \mathbb{G}_2 have 512-bit sizes, and the number of attributes ℓ is 20.

Table 3 clearly shows that the credential sizes of the schemes [14,37,40,53] increase linearly with the number of attributes. As a result, these schemes [14,37,40,53] have larger credential sizes compared to others [22,38,78]. However, when compared with the credential sizes of lattice-based AC schemes, pairing-based AC schemes are more efficient because lattice ACs have large credential sizes. Moreover, pairing-based ACs, such as in [22,78], achieve credential sizes less than half of classical AC schemes [13,51] due to the compactness of pairing-based techniques.

Classical AC systems rely on the RSA signature scheme, which necessitates large modulus sizes, typically approaching a modulus size of $2k$ where $k = 2048$. This results in large proof-of-knowledge sizes, reducing the schemes’ efficiency. However, pairing-based schemes are more efficient in performance than classical AC systems, as they achieve the same security level as classical systems but with shorter key sizes. Additionally, nowadays, many schemes support the selective attribute disclosure [18,46,78] of property rather than proving relations [22,38]. However, a comprehensive comparison of recent pairing-based AC systems goes beyond credential sizes and assumptions. The efficiency of issuing and showing protocols is important but not analyzed here. Interested readers can calculate the number of pairings further.

Another factor in analyzing the efficiency is the size of the zero-knowledge proof used by the user to prove the knowledge of the message–signature pair. In this regard, the most efficient schemes minimize interactions between the user and verifier. Therefore, it is recommended to use non-interactive zero-knowledge proof systems instead of interactive proof of knowledge used in classical AC systems. However, researchers have proposed another method that involves using self-blindable schemes [53], which have been identified to be more efficient than zero-knowledge proofs.

Although lattice-based cryptography is widely researched for many other privacy-preserving cryptographic primitives, such as group signatures and blind signatures, there are only a few post-quantum anonymous credential schemes available in the literature. Table 4 summarizes the cryptographic components utilized in current lattice-based AC schemes. However, some schemes have slightly modified the mentioned components for greater efficiency.

Table 4. The design of lattice-based anonymous credentials.

Scheme	Assumption	Commitment	Signature	ZKPs
[21]	MSIS/MLWE	Ajtai [80]	[48] *	[81,82]
[20]	MSIS/RLWE	BDLOP [83], ABDLOP [82]	CTS [20]	[84]
[19]	NTRU-ISIS _f	ABDLOP [82]	[85]	[50]
[47]	MSIS/MLWE	ABDLOP	[21] *	[82]

* Scheme uses a modified version of the signature scheme. The term ZKP refers to zero-knowledge proof, a cryptographic protocol that allows proving a statement’s truth without revealing anything other than the fact that the statement being proven is true.

A comparison of quantum-resistant lattice-based AC systems is provided in Table 5, including public key size $|pk|$, credential (signature) size $|cred|$, the size of the zero-knowledge proof of possession of a message–signature pair $|\pi|$, and the security model.

According to Table 5, the schemes [20,21,47] were constructed based on trapdoor sampling of standard lattices and their ring setting. However, the structure of the paper [19] was different as it used NTRU trapdoors. Hence, it is clear that the use of NRTU lattices improved the efficiency of the scheme as it reduced the credential size noticeably. In addition, the zero-knowledge proof of that scheme [19] has fewer and simpler relations, so its proof size is low compared to the scheme in [21] (less than 750 KB). Furthermore, scheme [19] succeeded in ensuring that the prover and verifier’s running times are independent of the number of users but linear in terms of the number of attributes. Although these quantum-secure lattice-based AC schemes achieved the expected security goals, their larger key sizes can affect performance. Therefore, further research should be conducted to increase efficiency. In addition, although several practical AC systems have been implemented for classical and pairing-based structures, quantum-secure research must also be undertaken for practical applications as the power of quantum computers continues to grow, and cryptography research is actively working towards transitioning to post-quantum cryptographic algorithms.

Table 5. Efficiency comparison of lattice-based AC Schemes with 128-bit security.

Scheme	Assumption	Setting	$ pk $ (KB)	$ cred $ (KB)	$ \pi $ (KB)	Security Model
[21]	MSIS/MLWE	standard	117.10 ³	261	306.10 ³	ROM
[21]	MSIS/MLWE	module	276.48	317	724	ROM
[20]	MSIS/RLWE	structured	440	236.56	372.56	ROM *
[20]	MSIS/RLWE	structured	276.5	16,711.68	25,364.48	ROM
[19]	ISIS _f	NTRU	17	243	473	ROM
[19]	ISIS _f	Int-NTRU	3.5	62	107	ROM
[47]	MSIS/MLWE	module	49.91	6.81	80	ROM

Int-NTRU denotes the interactive NTRU assumption. ROM denotes random oracle model. * Adaptive security proof involves an exponential loss.

6. Discussion

This discussion summarizes the researched real-world applications and the security properties needed by these applications. Furthermore, we identify research gaps and future directions.

6.1. Real-World Applications

To maintain privacy, AC schemes are utilized in various real-world applications. Microsoft's U-Prove [86], which uses Brand's signature in AC, and IBM's Identity Mixer [87], which uses CL signatures in AC, are among these solutions that industry leaders have deployed since 2010. AC systems were frequently utilized in online transactions, allowing users to conduct transactions without exposing their identities. Smart cards [88], e-voting [89], e-cash transactions [4,5], and e-tokens [90] are popular examples. Furthermore, AC systems are used for authentication in applications such as electronic ID [17], membership revocation [57], access control [91], age verification [92], decentralized systems [2], and direct anonymous attestation (DAA) [93]. Moreover, research papers also explained how to employ AC systems for traffic communication [94] and the health industry [3]. In summary, the real-world uses of AC systems include digital authentication, healthcare privacy, and secure online transactions, making them a diverse solution for protecting personal information while allowing smooth access to services. Table 6 summarizes various real-world applications and the additional security properties that these applications achieve, in addition to the previously discussed unforgeability and anonymity.

Table 6. Real-world applications of anonymous credentials.

AC Security Properties	Real-World Applications
Non-Transferability	E-Voting
Revocation	KYC Verification, Membership Revocation
Traceability	Smart Cards, Digital Cash
Selective attribute disclosure	Digital ID, Healthcare Systems
Delegation	Access Control, Transactions in Blockchain
Authenticity	Anonymous Survey
Verifiability	E-Voting
Transparency	E-Voting
Exculpability	Cryptocurrencies, Digital Cash

In our analysis of the practical anonymous credentials, we have identified four basic properties that are widely utilized in real-world settings: traceability, revocability, delegation, and decentralization. TAC systems have found application in various domains, including anonymous certifications [95], smart cards [96], KAVC systems [54], digital cash and cryptocurrencies, and online transactions (e.g., e-Cash [4]). RAC systems have found applications in various domains, including direct anonymous attestation (DAA) [97], Identity Escrow schemes [57], Java cards [98], and e-tokens [90]. There are plenty of applications of DAC systems, including access control systems [99] and blockchain transaction authentication [100].

In real-world applications, it is essential to achieve the mentioned security notions to address the unique requirements inherent to each application. The property revocation allows the system to remove credentials that are no longer valid due to expiration, misuse, or violations. Without this feature, malicious users could still gain access to services. Revocation is primarily used in Know Your Customer (KYC) applications [24] to prevent customers from participating in fraudulent activities when accessing financial services. Similarly, revocation in membership systems [57] ensures that customers who violate system policies cannot continue using services. In contrast, particular applications require property

traceability to link back to the origin user for different purposes. For instance, traceability in digital cash [4] can help prevent money laundering and double-spending, while smart cards [54] utilize traceability to manage access logs and detect misuse. Furthermore, the property-selective attribute disclosure allows users to reveal only the attributes required for a transaction or service while hiding some information, which prevents unnecessary exposure of sensitive data. For instance, in healthcare systems [3], patients can reveal their blood type to a clinic while keeping other medical history private. In conclusion, practical applications require additional security notions, which can vary depending on specific requirements.

Delegation and exculpability are important security notions often used in real-world AC (anonymous credential) applications. The property delegation allows the original credential owner to authorize another party to act on their behalf while restricting the scope of what the delegate can do. For instance, in access control [43,44], a manager can grant temporary access to a contractor to use the system, thereby minimizing the risk of system misuse. Moreover, the exculpability property protects users from being falsely accused of actions they did not take. For example, in e-cash [4], exculpability ensures users cannot be wrongly linked to a fraudulent transaction they did not initiate. Hence, exculpability in digital cash protects users from false accusations of double-spending or illegal activities.

E-voting systems in ACs [89,101] allow participants to vote remotely without moving to the polling station. However, when designing remote voting systems, several security notions must be achieved in addition to basic security notions of unforgeability and anonymity. Among these requirements, verifiability lets participants confirm that their votes are correctly recorded without revealing individual ballots, while transparency ensures the election process is transparent and open. However, security requirements can vary based on the application, and different notions may be achieved, so there is no guarantee that only these properties will be achieved.

6.2. Open Directions

In our analysis, we have identified several research gaps in the field of ACs. Researchers need to design AC systems that are secure against quantum computers, as early AC systems in classical cryptography and pairing-based designs were found to be vulnerable to quantum attacks. Interested researchers can focus on lattice-based designs, addressing the gaps mentioned below. Additionally, code-based, hash-based, and isogeny-based designs can be implemented, which were not analyzed in this study.

- The current literature indicates that the credential sizes of these lattice-based schemes are comparatively large compared to existing schemes. Interested readers can focus on minimizing the credential sizes of quantumly secure AC schemes.
- Although several AC systems have been proposed for specific properties in pairing-based cryptography, only a few designs have been proposed for lattice-based cryptography. Interested readers may explore constructions for properties such as revocability, traceability, signer hiding, and delegation in lattice-based AC systems.
- Although aggregate, redactable, and sanitizable signatures have been used in pairing-based designs, it is worth investigating their suitability for quantum-secure AC systems.
- To the best of our knowledge, the existing AC systems based on lattices remain less efficient than the classical and pairing-based AC systems and are not practical enough. Researchers are encouraged to address this gap and explore innovative solutions in developing quantum-resistant AC schemes for practical, real-world applications.

In addition, the construction lattice-based multi-authority AC systems face challenges due to the requirement of aggregate signatures, which allow multiple credentials from different issuers to be combined into a single credential. General aggregate signatures

(ASs) enable offline aggregation of credentials without requiring the users' private keys. In contrast, sequential aggregate signatures (SASs) require users to be online as signing and aggregation happen simultaneously. While lattice-based SAS schemes have been proposed [102,103], fully lattice-based aggregate signature schemes have recently been introduced [104], with high computational costs. Another challenge is compatibility with lattice-based ZK proofs. Further research is required to improve post-quantum lattice-based aggregation for shorter credential sizes and better verification efficiency to construct post-quantum multi-authority AC systems.

7. Conclusions

This paper comprehensively analyzed anonymous credentials from 1985 to the present. This research provides a systematic review, defining AC systems, discussing standard designs, and outlining crucial security definitions for practical applications. Moreover, the study provides a comprehensive review of the generation of AC systems in construction, covering classical, pairing-based, and post-quantum designs. Our aim of this thorough review of evolution is to identify the current trends in constructing AC systems and to determine what still needs to be achieved in the post-quantum lattice setting compared to pre-quantum constructions. Furthermore, this paper provides insights into real-world applications of current AC schemes in the application section. In conclusion, this paper serves as a road map for future post-quantum AC designers.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AC	Anonymous Credential
TAC	Traceable Anonymous Credential
RAC	Revocable Anonymous Credential
DAC	Delegatable Anonymous Credential
TA	Tracing Authority
RA	Revocation Authority
ZKPs	Zero-Knowledge Proofs

References

1. Diffie, W.; Hellman, M.E. New directions in cryptography. In *Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman*; Association for Computing Machinery: New York, USA, 2022; pp. 365–390.
2. Garman, C.; Green, M.; Miers, I. Decentralized anonymous credentials. In *Network and Distributed System Security (NDSS) Symposium*; The Internet Society: San Diego, USA, 2013.
3. Pussewalage, H.S.G.; Oleshchuk, V.A. An anonymous delegatable attribute-based credential scheme for a collaborative e-health environment. *ACM Trans. Internet Technol. (TOIT)* **2019**, *19*, 1–22.
4. Bourse, F.; Pointcheval, D.; Sanders, O. Divisible e-cash from constrained pseudo-random functions. In Proceedings of the Advances in Cryptology—ASIACRYPT 2019: 25th International Conference on the Theory and Application of Cryptology and Information Security, Kobe, Japan, 8–12 December 2019; Proceedings, Part I 25; Springer: Berlin/Heidelberg, Germany, 2019; pp. 679–708.
5. Canard, S.; Gouget, A. Divisible e-cash systems can be truly anonymous. In Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques, Barcelona, Spain, 20–24 May 2007; Springer: Berlin/Heidelberg, Germany, 2007; pp. 482–497.
6. Chaum, D. Security without identification: Transaction systems to make big brother obsolete. *Commun. ACM* **1985**, *28*, 1030–1044.

7. Kakvi, S.A.; Martin, K.M.; Putman, C.; Quaglia, E.A. SoK: Anonymous Credentials. In Proceedings of the International Conference on Research in Security Standardisation, Lyon, France, 22–23 April 2023; Springer: Berlin/Heidelberg, Germany, 2023; pp. 129–151.
8. Alagic, G.; Alagic, G.; Apon, D.; Cooper, D.; Dang, Q.; Dang, T.; Kelsey, J.; Lichtinger, J.; Liu, Y.K.; Miller, C.; et al. *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2022.
9. Shor, P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Rev.* **1999**, *41*, 303–332.
10. Chaum, D.; Evertse, J.H. A secure and privacy-protecting protocol for transmitting personal information between organizations. In Proceedings of the Conference on the Theory and Application of Cryptographic Techniques, Santa Barbara, CA, USA, 18–22 August 1985; Springer: Berlin/Heidelberg, Germany, 1986; pp. 118–167.
11. Chen, L. Access with pseudonyms. In Proceedings of the International Conference on Cryptography: Policy and Algorithms, Brisbane, QLD, Australia, 3–5 July 1995; Springer: Berlin/Heidelberg, Germany, 1995; pp. 232–243.
12. Lysyanskaya, A.; Rivest, R.L.; Sahai, A.; Wolf, S. Pseudonym systems. In Proceedings of the Selected Areas in Cryptography: 6th Annual International Workshop, SAC'99, Kingston, ON, Canada, 9–10 August 1999; Springer: Berlin/Heidelberg, Germany, 2000; pp. 184–199.
13. Camenisch, J.; Lysyanskaya, A. A signature scheme with efficient protocols. In Proceedings of the Security in Communication Networks: Third International Conference, SCN 2002, Amalfi, Italy, 11–13 September 2002; Revised Papers 3; Springer: Berlin/Heidelberg, Germany, 2003; pp. 268–289.
14. Camenisch, J.; Lysyanskaya, A. Signature schemes and anonymous credentials from bilinear maps. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 15–19 August 2004; Springer: Berlin/Heidelberg, Germany, 2004; pp. 56–72.
15. Lysyanskaya, A. Signature Schemes and Applications to Cryptographic Protocol Design. PhD Thesis, Massachusetts Institute of Technology, Cambridge, MA, USA, 2002.
16. Brands, S. *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy*; MIT Press: Cambridge, MA, USA, 2000.
17. Camenisch, J.; Groß, T. Efficient attributes for anonymous credentials. *ACM Trans. Inf. Syst. Secur. (TISSEC)* **2012**, *15*, 1–30.
18. Fuchsbauer, G.; Hanser, C.; Slamanig, D. Structure-preserving signatures on equivalence classes and constant-size anonymous credentials. *J. Cryptol.* **2019**, *32*, 498–546.
19. Bootle, J.; Lyubashevsky, V.; Nguyen, N.K.; Sorniotti, A. A framework for practical anonymous credentials from lattices. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 19–24 August 2023; Springer: Berlin/Heidelberg, Germany, 2023; pp. 384–417.
20. Lai, Q.; Liu, F.H.; Lysyanskaya, A.; Wang, Z. Lattice-based Commit-Transferrable Signatures and Applications to Anonymous Credentials. *Cryptol. ePrint Arch.* **2023**, *preprint*.
21. Jeudy, C.; Roux-Langlois, A.; Sanders, O. Lattice signature with efficient protocols, application to anonymous credentials. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 19–24 August 2023; Springer: Berlin/Heidelberg, Germany, 2023; pp. 351–383.
22. Sanders, O. Efficient redactable signature and application to anonymous credentials. In Proceedings of the IACR International Conference on Public-Key Cryptography, Edinburgh, UK, 4–7 May 2020; Springer: Berlin/Heidelberg, Germany, 2020; pp. 628–656.
23. Héban, C.; Pointcheval, D. Traceable constant-size multi-authority credentials. *Inf. Comput.* **2023**, *293*, 105060.
24. Chaum, D.; Pedersen, T. Wallet databases with observers. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 16–20 August 1992; pp. 89–105. 1998.
25. Fujisaki, E.; Okamoto, T. A practical and provably secure scheme for publicly verifiable secret sharing and its applications. In Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, Espoo, Finland, 31 May–4 June 1998; Springer: Berlin/Heidelberg, Germany, 1998; pp. 32–46.
26. Naor, M. Bit commitment using pseudorandomness. *J. Cryptol.* **1991**, *4*, 151–158.
27. Rivest, R.L.; Shamir, A.; Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **1978**, *21*, 120–126.
28. Fiat, A.; Shamir, A. How to prove yourself: Practical solutions to identification and signature problems. In Proceedings of the Conference on the Theory and Application of Cryptographic Techniques, Santa Barbara, CA, USA, 18–22 August 1985; Springer: Berlin/Heidelberg, Germany, 1986; pp. 186–194.
29. Schnorr, C.P. Efficient signature generation by smart cards. *J. Cryptol.* **1991**, *4*, 161–174.
30. Bellare, M.; Micali, S. How to sign given any trapdoor function. In Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing, Chicago, IL, USA, 2–4 May 1988; pp. 32–42.

31. Damgård, I.B. Payment systems and credential mechanisms with provable security against abuse by individuals. In Proceedings of the Conference on the Theory and Application of Cryptography, Davos, Switzerland, 25–27 May 1988; Springer: Berlin/Heidelberg, Germany, 1988; pp. 328–335.
32. Camenisch, J.; Stadler, M. *Proof Systems for General Statements about Discrete Logarithms*; Technical Report; Department of Computer Science, ETH Zurich: Zürich, Switzerland, 1997.
33. Boneh, D.; Boyen, X.; Shacham, H. Short group signatures. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 15–19 August 2004; Springer: Berlin/Heidelberg, Germany, 2004; pp. 41–55.
34. Boneh, D.; Shacham, H. Group signatures with verifier-local revocation. In Proceedings of the 11th ACM Conference on Computer and Communications Security, Washington, DC, USA, 25–29 October 2004; pp. 168–177.
35. Groth, J.; Sahai, A. Efficient non-interactive proof systems for bilinear groups. In Proceedings of the Advances in Cryptology—EUROCRYPT 2008: 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, 13–17 April 2008; Proceedings 27; Springer: Berlin/Heidelberg, Germany, 2008; pp. 415–432.
36. Groth, J. Efficient fully structure-preserving signatures for large messages. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, 29 November–3 December 2015; Springer: Berlin/Heidelberg, Germany, 2015; pp. 239–259.
37. Canard, S.; Lescuyer, R. Anonymous credentials from (indexed) aggregate signatures. In Proceedings of the 7th ACM workshop on Digital Identity Management, Chicago, IL, USA, 21 October 2011; pp. 53–62.
38. Tan, S.Y.; Groß, T. Monipoly—An expressive q-SDH-based anonymous attribute-based credential system. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Virtual Event, 7–11 December 2020; Springer: Berlin/Heidelberg, Germany, 2020; pp. 498–526.
39. Camenisch, J.; Dubovitskaya, M.; Haralambiev, K.; Kohlweiss, M. Composable and modular anonymous credentials: Definitions and practical constructions. In Proceedings of the Advances in Cryptology—ASIACRYPT 2015: 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, 29 November–3 December 2015; Proceedings, Part II 21; Springer: Berlin/Heidelberg, Germany, 2015; pp. 262–288.
40. Canard, S.; Lescuyer, R. Protecting privacy by sanitizing personal data: A new approach to anonymous credentials. In Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security, Hangzhou, China, 7–10 May 2013; pp. 381–392.
41. Hanser, C.; Slamanig, D. Structure-preserving signatures on equivalence classes and their application to anonymous credentials. In Proceedings of the Advances in Cryptology—ASIACRYPT 2014: 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, 7–11 December 2014; Proceedings, Part I 20; Springer: Berlin/Heidelberg, Germany, 2014; pp. 491–511.
42. Camenisch, J.; Kohlweiss, M.; Soriente, C. Solving revocation with efficient update of anonymous credentials. In Proceedings of the International Conference on Security and Cryptography for Networks, Amalfi, Italy, 13–15 September 2010; Springer: Berlin/Heidelberg, Germany, 2010; pp. 454–471.
43. Belenkiy, M.; Camenisch, J.; Chase, M.; Kohlweiss, M.; Lysyanskaya, A.; Shacham, H. Randomizable proofs and delegatable anonymous credentials. In Proceedings of the Advances in Cryptology—CRYPTO 2009: 29th Annual International Cryptology Conference, Santa Barbara, CA, USA, 16–20 August 2009; Proceedings; Springer: Berlin/Heidelberg, Germany, 2009; pp. 108–125.
44. Mir, O.; Slamanig, D.; Bauer, B.; Mayrhofer, R. Practical delegatable anonymous credentials from equivalence class signatures. *Proc. Priv. Enhancing Technol.* **2023**, *2023*, 488–513.
45. Bobolz, J.; Eidens, F.; Krenn, S.; Ramacher, S.; Samelin, K. Issuer-hiding attribute-based credentials. In Proceedings of the Cryptology and Network Security: 20th International Conference, CANS 2021, Vienna, Austria, 13–15 December 2021; Proceedings 20; Springer: Berlin/Heidelberg, Germany, 2021; pp. 158–178.
46. Connolly, A.; Lafourcade, P.; Perez Kempner, O. Improved constructions of anonymous credentials from structure-preserving signatures on equivalence classes. In Proceedings of the IACR International Conference on Public-Key Cryptography, Virtual Event, 8–11 March 2022; Springer: Berlin/Heidelberg, Germany, 2022; pp. 409–438.
47. Argo, S.; Güneysu, T.; Jeudy, C.; Land, G.; Roux-Langlois, A.; Sanders, O. Practical Post-Quantum Signatures for Privacy. In Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security, Salt Lake City, UT, USA, 14–18 October 2024.
48. Libert, B.; San Ling, F.M.; Nguyen, K.; Wang, H. Signature Schemes with Efficient Protocols and Dynamic Group Signatures from Lattice Assumptions. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, 4–8 December 2016.
49. Boyen, X. Lattice Mixing and Vanishing Trapdoors: A Framework for Fully Secure Short Signatures and More. In *Public Key Cryptography—PKC 2010*; Nguyen, P.Q., Pointcheval, D., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2010; Volume 6056, pp. 499–517.

50. del Pino, R.; Katsumata, S. A new framework for more efficient round-optimal lattice-based (partially) blind signature via trapdoor sampling. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 15–18 August 2022; Springer: Berlin/Heidelberg, Germany, 2022; pp. 306–336.
51. Camenisch, J.; Lysyanskaya, A. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In Proceedings of the Advances in Cryptology—EUROCRYPT 2001: International Conference on the Theory and Application of Cryptographic Techniques, Innsbruck, Austria, 6–10 May 2001; Proceedings 20; Springer: Berlin/Heidelberg, Germany, 2001; pp. 93–118.
52. Blazy, O.; Chevalier, C.; Renaut, G.; Ricosset, T.; Sageloli, E.; Senet, H. Efficient Implementation of a Post-Quantum Anonymous Credential Protocol. In Proceedings of the 18th International Conference on Availability, Reliability and Security, Benevento, Italy, 29 August–1 September 2023; pp. 1–11.
53. Ringers, S.; Verheul, E.; Hoepman, J.H. An efficient self-blindable attribute-based credential scheme. In Proceedings of the Financial Cryptography and Data Security: 21st International Conference, FC 2017, Sliema, Malta, 3–7 April 2017; Revised Selected Papers 21; Springer: Berlin/Heidelberg, Germany, 2017; pp. 3–20.
54. Wu, W. Efficient and Traceable Anonymous Credentials on Smart Cards. *Comput. Inf. Sci.* **2022**, *15*, 1–58.
55. Tsang, P.P.; Au, M.H.; Kapadia, A.; Smith, S.W. Blacklistable anonymous credentials: Blocking misbehaving users without TTPs. In Proceedings of the 14th ACM Conference on Computer and Communications Security, Alexandria, VA, USA, 28–31 October 2007; pp. 72–81.
56. Tsang, P.P.; Au, M.H.; Kapadia, A.; Smith, S.W. BLAC: Revoking repeatedly misbehaving anonymous users without relying on TTPs. *ACM Trans. Inf. Syst. Secur. (TISSEC)* **2010**, *13*, 1–33.
57. Camenisch, J.; Lysyanskaya, A. Dynamic accumulators and application to efficient revocation of anonymous credentials. In Proceedings of the Advances in Cryptology—CRYPTO 2002: 22nd Annual International Cryptology Conference Santa Barbara, CA, USA, 18–22 August 2002; Proceedings 22; Springer: Berlin/Heidelberg, Germany, 2002; pp. 61–76.
58. Camenisch, J.; Kohlweiss, M.; Soriente, C. An accumulator based on bilinear maps and efficient revocation for anonymous credentials. In Proceedings of the Public Key Cryptography—PKC 2009: 12th International Conference on Practice and Theory in Public Key Cryptography, Irvine, CA, USA, 18–20 March 2009; Proceedings 12; Springer: Berlin/Heidelberg, Germany, 2009; pp. 481–500.
59. Baldimtsi, F.; Camenisch, J.; Dubovitskaya, M.; Lysyanskaya, A.; Reyzin, L.; Samelin, K.; Yakoubov, S. Accumulators with applications to anonymity-preserving revocation. In Proceedings of the 2017 IEEE European Symposium on Security and Privacy (EuroS&P), Paris, France, 26–28 April 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 301–315.
60. Acar, T.; Nguyen, L. Revocation for delegatable anonymous credentials. In Proceedings of the International Workshop on Public Key Cryptography, Taormina, Italy, 6–9 March 2011; Springer: Berlin/Heidelberg, Germany, 2011; pp. 423–440.
61. Ateniese, G.; Song, D.; Tsudik, G. Quasi-efficient revocation of group signatures. In Proceedings of the Financial Cryptography: 6th International Conference, FC 2002 Southampton, Bermuda, UK, 11–14 March 2002 Revised Papers 6. Springer: Berlin/Heidelberg, Germany, 2003; pp. 183–197.
62. Zaverucha, G.M.; Stinson, D.R. Group testing and batch verification. In Proceedings of the International Conference on Information Theoretic Security, Shizuoka, Japan, 3–6 December 2009; Springer: Berlin/Heidelberg, Germany, 2009; pp. 140–157.
63. Camenisch, J.; Drijvers, M.; Hajny, J. Scalable revocation scheme for anonymous credentials based on n-times unlinkable proofs. In Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic Society, Vienna, Austria, 24–28 October 2016; pp. 123–133.
64. Camenisch, J.; Shoup, V. Practical verifiable encryption and decryption of discrete logarithms. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 17–21 August 2003; Springer: Berlin/Heidelberg, Germany, 2003; pp. 126–144.
65. Backes, M.; Camenisch, J.; Sommer, D. Anonymous yet accountable access control. In Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society, Alexandria, VA, USA, 7 November 2005; pp. 40–46.
66. Tsang, P.P.; Kapadia, A.; Cornelius, C.; Smith, S.W. Nymble: Blocking misbehaving users in anonymizing networks. *IEEE Trans. Dependable Secur. Comput.* **2009**, *8*, 256–269.
67. Lueks, W.; Alpár, G.; Hoepman, J.H.; Vullers, P. Fast revocation of attribute-based credentials for both users and verifiers. *Comput. Secur.* **2017**, *67*, 308–323.
68. Verheul, E.R. Practical backward unlinkable revocation in fido, german e-id, idemix and u-prove. *Cryptol. ePrint Arch.* **2016**, preprint.
69. Chase, M.; Lysyanskaya, A. On signatures of knowledge. In Proceedings of the Advances in Cryptology—CRYPTO 2006: 26th Annual International Cryptology Conference, Santa Barbara, CA, USA, 20–24 August 2006; Proceedings 26; Springer: Berlin/Heidelberg, Germany, 2006; pp. 78–96.
70. Chase, M.; Kohlweiss, M.; Lysyanskaya, A.; Meiklejohn, S. Malleable signatures: New definitions and delegatable anonymous credentials. In Proceedings of the 2014 IEEE 27th computer security foundations symposium, Vienna, Austria, 19–22 July 2014; IEEE: Piscataway, NJ, USA, 2014; pp. 199–213.

71. Yang, R.; Au, M.H.; Xu, Q.; Yu, Z. Decentralized blacklistable anonymous credentials with reputation. *Comput. Secur.* **2019**, *85*, 353–371.
72. Lin, C.; He, D.; Zhang, H.; Shao, L.; Huang, X. Privacy-enhancing decentralized anonymous credential in smart grids. *Comput. Stand. Interfaces* **2021**, *75*, 103505.
73. Blömer, J.; Bobolz, J.; Diemert, D.; Eidens, F. Updatable anonymous credentials and applications to incentive systems. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, London, UK, 11–15 November 2019; pp. 1671–1685.
74. Chase, M.; Meiklejohn, S.; Zaverucha, G. Algebraic MACs and keyed-verification anonymous credentials. In Proceedings of the 2014 ACM Sigsac Conference on Computer and Communications Security, Scottsdale, AZ, USA, 3–7 November 2014; pp. 1205–1216.
75. Canetti, R. Universally composable security: A new paradigm for cryptographic protocols. In Proceedings of the 42nd IEEE Symposium on Foundations of Computer Science, Las Vegas, NV, USA, 14–17 October 2001; IEEE: Piscataway, NJ, USA, 2001; pp. 136–145.
76. Bellare, M.; Rogaway, P. Random oracles are practical: A paradigm for designing efficient protocols. In Proceedings of the 1st ACM Conference on Computer and Communications Security, Fairfax, VA, USA, 3–5 November 1993; pp. 62–73.
77. Shoup, V. Lower bounds for discrete logarithms and related problems. In Proceedings of the Advances in Cryptology—EUROCRYPT’97: International Conference on the Theory and Application of Cryptographic Techniques, Konstanz, Germany, 11–15 May 1997; Proceedings 16; Springer: Berlin/Heidelberg, Germany, 1997; pp. 256–266.
78. Héban, C.; Pointcheval, D. Traceable Constant-Size Multi-authority Credentials. In Proceedings of the Security and Cryptography for Networks, Amalfi, Italy, 12–14 September 2022; Galdi, C., Jarecki, S., Eds.; Springer: Cham, Switzerland, 2022; pp. 411–434.
79. Fuchsbauer, G. Automorphic signatures in bilinear groups and an application to round-optimal blind signatures. *Cryptol. ePrint Arch.* 2009, *preprint*.
80. Ajtai, M. Generating hard instances of lattice problems. In Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, Philadelphia, PA, USA, 22–24 May 1996; pp. 99–108.
81. Yang, R.; Au, M.H.; Zhang, Z.; Xu, Q.; Yu, Z.; Whyte, W. Efficient lattice-based zero-knowledge arguments with standard soundness: Construction and applications. In Proceedings of the Advances in Cryptology—CRYPTO 2019: 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, 18–22 August 2019; Proceedings, Part I 39; Springer: Berlin/Heidelberg, Germany, 2019; pp. 147–175.
82. Lyubashevsky, V.; Nguyen, N.K.; Plançon, M. Lattice-based zero-knowledge proofs and applications: Shorter, simpler, and more general. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 15–18 August 2022; Springer: Berlin/Heidelberg, Germany, 2022; pp. 71–101.
83. Baum, C.; Damgård, I.; Lyubashevsky, V.; Oechsner, S.; Peikert, C. More efficient commitments from structured lattice assumptions. In Proceedings of the International Conference on Security and Cryptography for Networks, Amalfi, Italy, 5–7 September 2018; Springer: Berlin/Heidelberg, Germany, 2018; pp. 368–385.
84. Peikert, C.; Shiehian, S. Noninteractive zero knowledge for NP from (plain) learning with errors. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 18–22 August 2022; Springer: Berlin/Heidelberg, Germany, 2019; pp. 89–114.
85. Agrawal, S.; Kirshanova, E.; Stehlé, D.; Yadav, A. Practical, round-optimal lattice-based blind signatures. In Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, Los Angeles, CA, USA, 7–11 November 2022; pp. 39–53.
86. Paquin, C.; Zaverucha, G. *U-Prove Cryptographic Specification v1. 1*; Technical Report; Microsoft Corporation: Redmond, WA, USA, 2011.
87. Bichsel, P.; Camenisch, J. Mixing identities with ease. In Proceedings of the Policies and Research in Identity Management: Second IFIP WG 11.6 Working Conference, IDMAN 2010, Oslo, Norway, 18–19 November 2010; Proceedings 2; Springer: Berlin/Heidelberg, Germany, 2010; pp. 1–17.
88. Hesse, J.; Singh, N.; Sorniotti, A. How to Bind Anonymous Credentials to Humans. In Proceedings of the 32nd USENIX Security Symposium (USENIX Security 23), Anaheim, CA, USA, 9–11 August 2023; pp. 3047–3064.
89. Doesburg, J.; Jacobs, B.; Ringers, S. Using IRMA for Small Scale Digital Elections. Bachelor Thesis, Radboud University, Nijmegen, The Netherlands, 2020.
90. Camenisch, J.; Van Herreweghen, E. Design and implementation of the idemix anonymous credential system. In Proceedings of the 9th ACM Conference on Computer and Communications Security, Washington, DC, USA, 18–22 November 2002; pp. 21–30.
91. Godtschalk, L. *Accountability and Access Control using Anonymous Credentials*; Eindhoven University of Technology: Eindhoven, The Netherlands, 2022.

92. Rosenberg, M.; White, J.; Garman, C.; Miers, I. zk-creds: Flexible anonymous credentials from zkSNARKs and existing identity infrastructure. In Proceedings of the 2023 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 22–24 May 2023; IEEE: Piscataway, NJ, USA, 2023, pp. 790–808.
93. Camenisch, J.; Drijvers, M.; Lehmann, A. Universally composable direct anonymous attestation. In Proceedings of the Public-Key Cryptography–PKC 2016: 19th IACR International Conference on Practice and Theory in Public-Key Cryptography, Taipei, Taiwan, 6–9 March 2016; Proceedings, Part II 19; Springer: Berlin/Heidelberg, Germany, 2016; pp. 234–264.
94. Förster, D.; Kargl, F.; Löhr, H. PUCA: A pseudonym scheme with user-controlled anonymity for vehicular ad-hoc networks (VANET). In Proceedings of the 2014 IEEE Vehicular Networking Conference (VNC), Paderborn, Germany, 3–5 December 2014; IEEE: Piscataway, NJ, USA, 2014; pp. 25–32.
95. Kaaniche, N.; Laurent, M. Attribute-based signatures for supporting anonymous certification. In Proceedings of the Computer Security–ESORICS 2016: 21st European Symposium on Research in Computer Security, Heraklion, Greece, 26–30 September 2016; Proceedings, Part I 21; Springer: Berlin/Heidelberg, Germany, 2016; pp. 279–300.
96. Hajny, J. Anonymous Authentication for Smartcards. *Radioengineering* **2010**, *19*, 363–368.
97. Brickell, E.; Camenisch, J.; Chen, L. Direct anonymous attestation. In Proceedings of the 11th ACM conference on Computer and Communications Security, Washington, DC, USA, 25–29 October 2004; pp. 132–145.
98. Bichsel, P.; Camenisch, J.; Groß, T.; Shoup, V. Anonymous credentials on a standard java card. In Proceedings of the 16th ACM conference on Computer and communications security, Chicago, IL, USA, 9–13 November 2009; pp. 600–610.
99. Matetic, S.; Schneider, M.; Miller, A.; Juels, A.; Capkun, S. {DelegaTEE}: Brokered delegation using trusted execution environments. In Proceedings of the 27th USENIX Security Symposium (USENIX Security 18), Baltimore, MD, USA, 15–17 August 2018; pp. 1387–1403.
100. Camenisch, J.; Drijvers, M.; Dubovitskaya, M. Practical UC-secure delegatable credentials with attributes and their application to blockchain. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, Dallas, TX, USA, 30 October–3 November 2017; pp. 683–699.
101. Mateu, V.; Seb e, F.; Valls, M. Constructing credential-based E-voting systems from offline E-coin protocols. *J. Netw. Comput. Appl.* **2014**, *42*, 39–44.
102. Boudgoust, K.; Takahashi, A. Sequential half-aggregation of lattice-based signatures. In Proceedings of the European Symposium on Research in Computer Security, Hague, The Netherlands, 25–29 September 2023; Springer: Berlin/Heidelberg, Germany, 2023; pp. 270–289.
103. El Bansarkhani, R.; Buchmann, J. Towards lattice based aggregate signatures. In Proceedings of the Progress in Cryptology–AFRICACRYPT 2014: 7th International Conference on Cryptology in Africa, Marrakesh, Morocco, 28–30 May 2014; Proceedings 7; Springer: Berlin/Heidelberg, Germany, 2014; pp. 336–355.
104. Lu, X.; Yin, W.; Wen, Q.; Jin, Z.; Li, W. A lattice-based unordered aggregate signature scheme based on the intersection method. *IEEE Access* **2018**, *6*, 33986–33994.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.