

Review

A Review of Attribute-Based Credentials for Secure and Privacy-Preserving Identity Management

Jingdu Lei ¹, Lina Wang ², Yanyu Zhang ³, Gen Sun ¹, Yuzhou Liu ⁴ and Chen Du ^{5,*}

¹ School of Cyber Science and Engineering, Engineering Research Center of Digital Forensics, Ministry of Education, Nanjing University of Information Science and Technology, Nanjing 210044, China; 202412492360@nuist.edu.cn (J.L.); 202483290135@nuist.edu.cn (G.S.)

² School of Artificial Intelligence (School of Future Technology), Nanjing University of Information Science and Technology, Nanjing 210044, China; wangln@nuist.edu.cn

³ Shandong Sacred Sun Power Sources Co., Ltd., Qufu 273100, China; zhangyanyu@sacredsunsun.cn

⁴ Portland Institute, Nanjing University of Posts and Telecommunications, Nanjing 210003, China; p23000112@njupt.edu.cn

⁵ Jinan Huanghe Road and Bridge Construction Group Co., Ltd., Jinan 250001, China

* Correspondence: 15588888913@163.com

Abstract

Attribute-Based Credentials (ABCs) are cryptographic credential systems that enable holders to selectively disclose certified attributes or prove predicates over them, thereby supporting privacy-preserving identity verification while limiting unnecessary information exposure. This paper presents a review of the system model, core security and privacy properties, classification, comparative analysis, and practical deployment challenges of ABCs. It develops a two-dimensional taxonomy consisting of a construction dimension and an extension dimension. The construction dimension covers publicly verifiable signature-based, keyed-verification and MAC-based, and general-purpose ZKP-based ABC constructions, while the extension dimension covers issuer-hiding, threshold and multi-authority, and dynamic-lifecycle ABCs. The resulting comparison shows that these categories exhibit different trade-offs in verifier openness, proof flexibility, privacy guarantees, trust requirements, lifecycle support, and practical deployment requirements. The review further examines key challenges related to the efficiency and scalability of multi-attribute management, privacy-preserving credential lifecycle management, inference risks in selective disclosure, interoperability, post-quantum security, and holder binding. Finally, it synthesizes recent trends and identifies research directions toward efficient, interoperable, privacy-preserving, and practically deployable ABC systems that strengthen digital trust and support trustworthy digital identity infrastructures.

Keywords: attribute-based credentials; selective disclosure; privacy-preserving identity management; digital trust; credential lifecycle management



Academic Editor: Hung-Yu Chien

Received: 24 July 2026

Revised: 20 August 2026

Accepted: 24 August 2026

Published: 28 August 2026

Copyright: © 2026 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 \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

1. Introduction

The continued growth of online services, decentralized applications, and digital platforms has increased the demand for secure and privacy-preserving identity management. Conventional identity and credential systems often rely on persistent identifiers or credentials containing fixed collections of subject information. Consequently, users may be required to disclose more information than is necessary for a particular transaction, increasing the exposure of personally identifiable information and the risks of cross-service linkage, profiling, and re-identification [1].

Legal and technical initiatives have attempted to mitigate these risks from different perspectives. The General Data Protection Regulation (GDPR), for example, establishes principles and legal obligations for the processing and protection of personal data, including data minimization [2]. The W3C Verifiable Credentials Data Model, meanwhile, defines an interoperable representation for issuing, holding, and presenting digital credentials [3]. However, neither legal requirements nor credential data models alone guarantee selective disclosure or unlinkability. These properties depend on the cryptographic mechanisms and presentation protocols adopted by a credential system [4]. A privacy-preserving identity system should therefore allow users to disclose only the information required for a specific purpose or to prove that a verification condition is satisfied without revealing the underlying attribute values.

More broadly, security and trust requirements are also critical in dynamic and heterogeneous communication environments, where authentication, secure data exchange, and key management must accommodate changing network topologies and participants. For example, Tan et al. proposed a cross-domain heterogeneous data aggregation scheme integrating dynamic group key agreement for hybrid satellite networks, together with re-authentication and secure cross-domain transmission mechanisms to cope with highly dynamic network conditions [5]. In another highly dynamic setting, Sen et al. developed a PUF-based authentication framework for UAV flying ad hoc networks (FANETs), incorporating UAV registration and mutual authentication to establish secure and robust communications [6].

Attribute-Based Credentials (ABCs) provide cryptographic mechanisms for fine-grained and privacy-preserving authentication. In an ABC system, a credential holder can prove possession of a valid credential certifying particular attributes or demonstrate that predicates over those attributes are satisfied while limiting the information disclosed to the verifier. For example, a user may prove that their age satisfies a required threshold or that they belong to an authorized organization without revealing their exact age, complete identity, or unrelated attributes. These capabilities distinguish privacy-enhancing ABCs from conventional public-key certificates, which typically bind a public key to a fixed set of certified subject information that may be exposed during certificate presentation [7]. By enabling verifiers to establish trust in certified attributes without requiring the disclosure of complete identities or unrelated personal information, ABCs provide a cryptographic foundation for privacy-preserving digital trust.

The conceptual roots of ABCs can be traced to Chaum's anonymous transaction and credential systems [8]. Subsequent constructions, including the Camenisch–Lysyanskaya credential framework [7], established practical mechanisms for credential randomization, selective disclosure, and unlinkable presentation. Related technologies, such as Direct Anonymous Attestation, adapted anonymous authentication techniques to attestation in trusted-computing environments [9]. Representative systems such as Idemix and U-Prove further demonstrated the feasibility of privacy-enhancing credential mechanisms in concrete system designs, although their privacy properties, verification models, and deployment characteristics differ [10–12].

Since these foundational developments, the cryptographic design space of ABCs has expanded substantially. Existing constructions employ publicly verifiable credential signatures, keyed-verification or message-authentication-code-based mechanisms, and general-purpose zero-knowledge proof systems. These mechanisms differ in their verification models, trust assumptions, proof-generation costs, and compatibility with existing credential infrastructures. Research has also explored post-quantum constructions, assisted credential systems, and structure-preserving and randomizable signatures [13–15].

In parallel, ABC research has introduced cross-cutting extensions addressing issuer privacy, distributed trust, accountability, and credential lifecycle management. Issuer-hiding constructions conceal the exact issuer of a credential, while threshold and multi-authority mechanisms distribute issuance, revocation, verification, or tracing operations among several authorities. Dynamic lifecycle management supports controlled post-issuance changes to credential contents, validity, status, scope, or derivation relationships. Representative capabilities include attribute updates, revocation, redaction, delegation, and derived credentials [16–18]. Taken together, these developments reflect a broader shift from a primary focus on individual credential primitives and presentation protocols toward diversified verification models and lifecycle-aware, trust-distributed credential systems.

1.1. Motivation

Existing surveys have examined Self-Sovereign Identity (SSI) and decentralized identity primarily at the architectural, ecosystem, standardization, and application levels. Mühle et al. [19] identified the essential components of SSI, while Schardong and Custódio [20] provided a systematic review, mapping, and taxonomy of SSI research. Soltani et al. [21] surveyed the broader SSI ecosystem, including its stakeholders, technologies, platforms, and trust relationships. More recent studies have reviewed Decentralized Identifier (DID) and Verifiable Credential (VC) standards, technical mechanisms, and related frameworks [3,22,23], as well as SSI applications and deployment challenges across different domains [24]. However, these reviews primarily focus on high-level architectures, ecosystems, standardization processes, application scenarios, and socio-technical trust models. They commonly treat credentials primarily as architectural or system-level components and provide limited scheme-level analysis of the cryptographic and protocol mechanisms through which credentials support attribute certification, selective disclosure, predicate proofs, unlinkable presentation, and lifecycle management.

Dedicated studies have systematized anonymous credentials from complementary perspectives, including terminology, security definitions, cryptographic constructions, advanced credential properties, design principles, performance, applications, and post-quantum development [4,25]. Although ABCs and anonymous credentials overlap, the two concepts are not coextensive, and their organizing emphases are not identical. In particular, the present review adopts a different organizing principle by structuring ABCs along two complementary dimensions: the principal cryptographic construction and verification mechanism, and cross-cutting extension capabilities related to privacy, trust distribution, and credential lifecycle. Table 1 summarizes these differences.

More specifically, existing literature exhibits the following gaps:

- Lack of a unified taxonomy: Existing literature lacks a unified taxonomy for organizing ABC schemes according to their construction and extension dimensions.
- Lack of a unified comparative framework: Existing studies have not provided a unified framework for comparing different types of ABC schemes across their construction, verification, privacy, trust, lifecycle, efficiency, and deployment characteristics.
- Insufficient analysis of practical deployment challenges: Existing studies provide insufficient analysis of the key challenges involved in deploying ABCs in practical settings.

Table 1. Comparison of Existing Reviews and Our Review.

Review	Scope	Primary Classification Logic	Limitations
Mühle et al. [19]	Blockchain-based SSI	SSI components and Identifier/Claim Registry models.	Limited scheme-level analysis of credential mechanisms.
Soltani et al. [21]	SSI ecosystem	Building blocks, privacy techniques, platforms, regulations, and challenges.	Limited scheme-level analysis of credential mechanisms.
Schardong and Custódio [20]	SSI literature	Conceptual and practical taxonomy.	Limited scheme-level analysis of credential mechanisms.
Mazzocca et al. [22]	DIDs and VCs	Threats, implementations, applications, regulations, and challenges.	Limited scheme-level analysis of credential mechanisms.
Fathalla et al. [24]	SSI-based identity management	Multi-dimensional SSI framework covering system, security, deployment, and application aspects.	Limited scheme-level analysis of credential mechanisms.
Kakvi et al. [4]	Anonymous credentials	Core-property realization approaches and advanced credential properties.	Advanced properties are not consolidated into higher-level capability families.
Chathurangi et al. [25]	Anonymous credentials	Two dimensions: credential design structure and application.	Additional credential properties are discussed separately rather than integrated into the two-dimensional classification.
Our review	Attribute-Based Credentials	ABC-oriented two-dimensional taxonomy: (i) principal cryptographic construction and verification mechanism; (ii) a unified cross-cutting extension framework integrating privacy, trust distribution, and credential lifecycle capabilities.	–

1.2. Contributions

To address the research gaps identified above, this paper presents a review of ABCs and develops a two-dimensional taxonomy of ABC schemes. The main contributions of this review are as follows:

- **A two-dimensional taxonomy of ABC schemes:** This review organizes existing ABC schemes along two complementary dimensions: Cryptographic Construction and Verification Mechanisms, referred to as the construction dimension, and Privacy, Trust, and Lifecycle Extensions, referred to as the extension dimension.
- **A multidimensional comparative framework for ABC categories:** This review provides a multidimensional comparison of the construction and extension categories in terms of their principal cryptographic basis, verification and proof capabilities, privacy and trust characteristics, efficiency considerations and operational overhead, lifecycle functionality, deployment requirements, and main limitations.
- **A focused analysis of key practical deployment challenges:** This review examines the major challenges involved in transitioning ABCs from theoretical cryptographic constructions to practical identity-management applications and discusses representative technical responses to these challenges.
- **A discussion of future research directions:** Based on the review of existing studies and the analysis of key challenges, this paper identifies several directions for future ABC research.

1.3. Organization

The remainder of this paper is organized as follows. Section 2 describes the review methodology and literature selection process. Section 3 introduces the system model, core functions, and fundamental properties of ABCs. Section 4 presents the two-dimensional taxonomy organized along the construction and extension dimensions, together with a multidimensional comparative analysis of the categories. Section 5 examines major practical deployment challenges, representative technical responses, and future research directions. Section 6 concludes the paper.

2. Survey Methodology

This review adopts a targeted literature review process to identify, classify, and analyze studies on Attribute-Based Credentials (ABCs). The review combines a structured database search in IEEE Xplore, the ACM Digital Library, and the Web of Science Core Collection with supplementary literature discovery to establish the evidence base for the taxonomy, comparative analysis, and discussion of related technical challenges. The objective of the review is to cover the dominant and recurrent research directions in the ABC literature rather than to provide an exhaustive enumeration of all credential constructions.

2.1. Search Strategy

The structured database search combined credential-related terms with representative terms describing cryptographic constructions, privacy and trust extensions, and credential lifecycle functions. The following Boolean query was used as the common search expression:

("attribute-based credential*" OR "anonymous credential*" OR "privacy-preserving credential*" OR "selective-disclosure credential*") AND ("zero-knowledge proof" OR "zk-SNARK" OR "randomizable signature*" OR "structure-preserving signature*" OR "keyed-verification credential*" OR "algebraic MAC*" OR "issuer hiding" OR "threshold" OR "multi-authority" OR "revocation" OR "delegation" OR "redactable credential*" OR "updatable credential*")

The same Boolean query was applied using the database-specific search fields: All Metadata in IEEE Xplore, AllField in the ACM Digital Library, and Topic in the Web of Science Core Collection. The searches covered records available up to 30 June 2026. Database-specific field definitions and filtering functions were accommodated while preserving the same search scope.

The structured database search was complemented by targeted supplementary literature discovery. Targeted searches in Google Scholar and backward or forward citation tracing from relevant publications were used to identify additional ABC studies that were not captured by the three structured database searches, particularly foundational work, recent preprints, and technically relevant studies cited by key publications. Supplementary discovery was also used to identify closely related literature needed to provide standards and interoperability context or to support the discussion of technical challenges and potential solutions.

2.2. Eligibility and Screening Procedure

The inclusion criteria were original research articles, conference papers, and technically substantive reports that proposed, implemented, extended, or formally analyzed credential systems in which one or more attributes were certified and could be selectively disclosed or used in privacy-preserving statements or predicates. Accordingly, this review adopts a functionality-based rather than terminology-based scope. Anonymous credential systems satisfying these criteria were considered relevant even when the original authors did not explicitly use the term “attribute-based credential”.

Anonymous credential schemes focusing solely on anonymous authentication, membership, or token redemption without meaningful attribute certification or privacy-preserving attribute presentation were excluded from the primary ABC analysis. Studies addressing issuer hiding, threshold or multi-authority operations, credential update, revocation, redaction, delegation, or other lifecycle functions were retained when these mechanisms were integrated into or directly extended an ABC or a functionally equivalent credential system.

Peer-reviewed journal articles and conference papers were treated as the principal research sources. Standards and authoritative technical specifications were considered when the specification itself constituted the principal source for a protocol, data model, or implementation. Studies focusing exclusively on Attribute-Based Encryption, Attribute-Based Access Control, signcryption, general blockchain identity architectures, or anonymous membership and authentication were not treated as primary ABC studies unless they directly supported attribute certification, selective disclosure, privacy-preserving attribute proofs, or closely integrated credential lifecycle functions.

The records identified through the structured database search were first merged and deduplicated. The resulting unique records were then screened by title and abstract against the functionality-based scope and eligibility criteria described above, followed by full-text assessment of potentially relevant publications. Publications identified through supplementary discovery were assessed using the same functionality-based eligibility criteria and, where appropriate, the same full-text relevance assessment. The initial title/abstract screening and full-text relevance assessment were conducted by one author using the eligibility criteria described above. A second author reviewed potentially relevant, borderline, and uncertain cases to verify the consistency of the screening decisions. Any disagreements were resolved through discussion with reference to the same eligibility criteria.

2.3. Search and Selection Results

The quantitative search and screening flow reported in this subsection refers specifically to the records identified through the structured searches of IEEE Xplore, the ACM Digital Library, and the Web of Science Core Collection. The database searches identified 173 records from IEEE Xplore, 182 records from the ACM Digital Library, and 102 records from the Web of Science Core Collection, resulting in a total of 457 records before deduplication.

After the retrieved records were merged, 47 duplicate entries were removed, leaving 410 unique records for title and abstract screening. Based on the functionality-based scope and eligibility criteria described above, 251 records were not carried forward to full-text assessment because they lacked sufficiently direct relevance to ABC mechanisms or primarily addressed topics outside the main scope of the review. The remaining 159 publications proceeded to full-text relevance assessment.

From these 159 publications, 32 representative studies were selected as the structured-search core set for detailed analysis. The selection considered technical relevance, coverage of the construction and extension dimensions of the proposed taxonomy, and the avoidance of substantial redundancy among studies addressing closely similar mechanisms. Publications not selected for this representative core set were not necessarily considered ineligible. Rather, the core set was intended to provide a technically representative basis for detailed analysis without attempting to enumerate every publication covering closely related constructions.

As summarized in Table 2, 49 ABC-related studies constituted the analytical study set used to inform the taxonomy and comparative analysis in Section 4. This set combined the representative structured-search core with additional ABC studies identified through supplementary discovery. Other supplementary publications were used only as supporting sources for foundational concepts, standards and interoperability, related cryptographic mechanisms, deployment challenges, and future research directions, and are therefore not included in this ABC-study count.

Table 2. Structured Database Search, Screening, and Analytical Study Set.

Selection Stage	Number of Records/Studies
Structured database search and screening pathway	
Records identified from IEEE Xplore	173
Records identified from ACM Digital Library	182
Records identified from Web of Science Core Collection	102
Total records identified	457
Duplicate records removed	47
Unique records screened by title and abstract	410
Records not carried forward to full-text assessment	251
Full-text publications assessed for relevance	159
Representative studies selected as the structured-search core set for detailed analysis	32
Supplementary discovery and final analytical study set	
Additional ABC-related studies incorporated through supplementary discovery	17
ABC studies informing the taxonomy and comparative analysis	49

3. System Model and Properties

Despite differences in their cryptographic constructions, trust assumptions, verification models, and supported functionalities, most ABC systems can be described using a common set of roles and core issuance and presentation stages [26].

3.1. Core Entities

A generic ABC system involves three core roles: a holder, an issuer, and a verifier. During credential presentation, the holder acts as the prover. Figure 1 illustrates the principal interactions among these roles during credential issuance and presentation. The verification material shown in Figure 1 may be provisioned in advance and does not imply that the verifier must contact the issuer during each credential presentation.

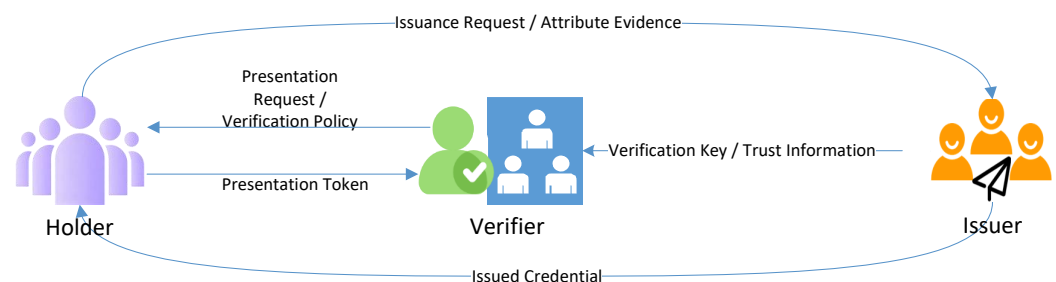


Figure 1. Generic Issuance and Presentation Flow in an Attribute-Based Credential System.

The roles of the three entities are described as follows:

- **Holder:** The holder requests, obtains, and stores a credential certifying a set of attributes. During issuance, the holder submits an issuance request and either provides the required attribute evidence or proves possession of it. Depending on the construction, the holder may also contribute a secret, commitment, pseudonym, device-bound value, or other holder-side input to the issuance protocol. During presentation, the holder generates a presentation token in response to the verifier's presentation request or verification policy. The token may disclose selected attributes or prove predicates over hidden attributes.
- **Issuer:** The issuer validates the holder's attribute evidence or otherwise establishes sufficient assurance regarding its authenticity and issues a credential certifying the corresponding attributes. Depending on the construction, issuance may rely on public-key signatures, keyed-verification mechanisms, blind or interactive protocols, or distributed cooperation among multiple authorities. The issuer establishes or controls the verification material required to validate credentials issued under its authority. Depending on the verification model, this material may be published, retained by the issuer, securely provisioned to authorized verifiers, or made available through an external trust infrastructure.
- **Verifier:** The verifier specifies a presentation request or verification policy and evaluates the presentation token generated by the holder. It determines whether the token was generated from a valid credential, whether the credential satisfies the applicable validity or status requirements, and whether the required disclosure or predicate conditions are met. Under the privacy guarantees provided by the specific scheme, the verifier should learn no more than the attributes intentionally disclosed and the information logically implied by the verified predicates.

3.2. Core and Lifecycle Functions of ABCs

The following abstract interfaces capture the core setup, key generation, issuance, presentation, and verification functions of ABC systems. Since lifecycle functionality is

scheme-dependent, we distinguish these core operations from optional lifecycle operations that may be supported by dynamic-lifecycle ABC constructions.

- $\text{Setup}(1^\lambda) \rightarrow pp$: Given a security parameter λ , the setup algorithm generates the public system parameters pp .
- $\text{KeyGen}(pp) \rightarrow (isk, ivk)$: The issuer generates an issuer secret key isk and corresponding verification material ivk . Depending on the construction, ivk may be a public verification key or secret verification material available only to the issuer or authorized verifiers.
- $\text{Issue}(isk, \mathcal{A}, ev; hin) \rightarrow cred$: The issuer and holder execute an issuance protocol for an attribute set $\mathcal{A}$ and supporting attribute evidence ev . The value hin abstracts holder-side inputs, such as a holder secret, commitment, pseudonym, device-bound value, or protocol randomness. Upon successful completion, the holder obtains a credential $cred$, which may be bound to holder-specific information or another possession factor.
- $\text{Present}(cred, pol, ctx) \rightarrow \tau$: In response to a verification policy pol , the holder generates a presentation token τ . The policy may specify attributes to be disclosed and predicates to be proved over hidden attributes. The value ctx denotes optional contextual information, such as a verifier challenge, domain identifier, nonce, or session information.
- $\text{Verify}(ivk, \tau, pol, ctx, st) \rightarrow \{0, 1\}$: The verifier checks the presentation token using the relevant verification material and, where applicable, the current credential state st . This state may represent expiration, revocation, epoch, update, or other credential-status information. The algorithm outputs 1 if the token is valid and satisfies the required policy and outputs 0 otherwise.

Beyond these core operations, dynamic-lifecycle ABC constructions may provide additional interfaces for controlled post-issuance changes to credential contents, validity, status, or authorization relationships. These interfaces are deliberately abstract, since not all ABC constructions support all lifecycle operations and the authorization model varies across schemes. The value $auth$ abstracts the scheme-specific authorization material required to invoke the corresponding lifecycle operation, while ref denotes a scheme-specific credential or status reference used for lifecycle management. Representative abstract lifecycle operations are as follows.

- $\text{Update}(cred, \Delta; auth) \rightarrow cred'$: An authorized update changes permitted credential attributes, metadata, validity information, or related information according to an authorized change Δ . Depending on the construction, the holder may participate in the update protocol and obtain an updated credential $cred'$. *Authorized invoker*: the issuer, a designated update authority, or an appropriately authorized holder, depending on the construction.
- $\text{Revoke}(ref, st; auth) \rightarrow st'$: The operation permanently invalidates a credential, credential version, or associated status reference so that subsequent presentations relying on the revoked credential or status are rejected. *Authorized invoker*: the issuer or a designated revocation authority; in delegatable constructions, an authorized delegator may also revoke credentials delegated under its authority.
- $\text{Suspend}(ref, st; auth) \rightarrow st'$: The operation temporarily disables a credential or associated authorization state without permanently revoking it, allowing validity to be restored according to the scheme-specific status-management mechanism. *Authorized invoker*: the issuer or a designated status authority.
- $\text{Delegate}(cred, pol_d, rec; auth) \rightarrow cred_d$: A delegated credential is created from an existing credential for a delegatee represented by rec according to a delegation policy pol_d . The value rec abstracts scheme-specific information identifying or binding the delegatee, while the policy may restrict the delegated attributes, authorization scope, validity

period, or delegation depth. *Authorized invoker*: a holder or delegator possessing the delegation authority required by the construction.

- **Derive**(cred, pol_r; auth) → cred': A new credential or credential representation is derived from an existing valid credential according to a derivation policy pol_r, while preserving the validity and derivation relationships required by the construction. *Authorized invoker*: a holder possessing the source credential and any derivation authorization required by the construction.

3.3. Core Security and Privacy Properties

This subsection summarizes the core properties commonly considered when analyzing ABC schemes.

- **Correctness**: A presentation token honestly generated from a valid credential should be accepted by an honest verifier when the credential satisfies the applicable validity requirements and the required disclosure or predicate conditions are met.
- **Unforgeability**: An adversary that has not obtained an appropriate valid credential should not be able to generate a credential or presentation token that is accepted by an honest verifier as satisfying the required verification policy.
- **Collusion Resistance**: Multiple malicious holders should not be able to combine their credentials, certified attributes, or secret information to produce a valid presentation satisfying a policy that none of them can satisfy individually.
- **Selective Disclosure and Attribute Privacy**: A holder should be able to disclose only the certified attributes required for a particular transaction while keeping unrelated attributes hidden. Hidden attribute values should remain confidential except for information intentionally disclosed or logically implied by the predicates proved during presentation.

Additional privacy properties, such as presentation unlinkability, anonymity, and issuer hiding, are scheme-dependent.

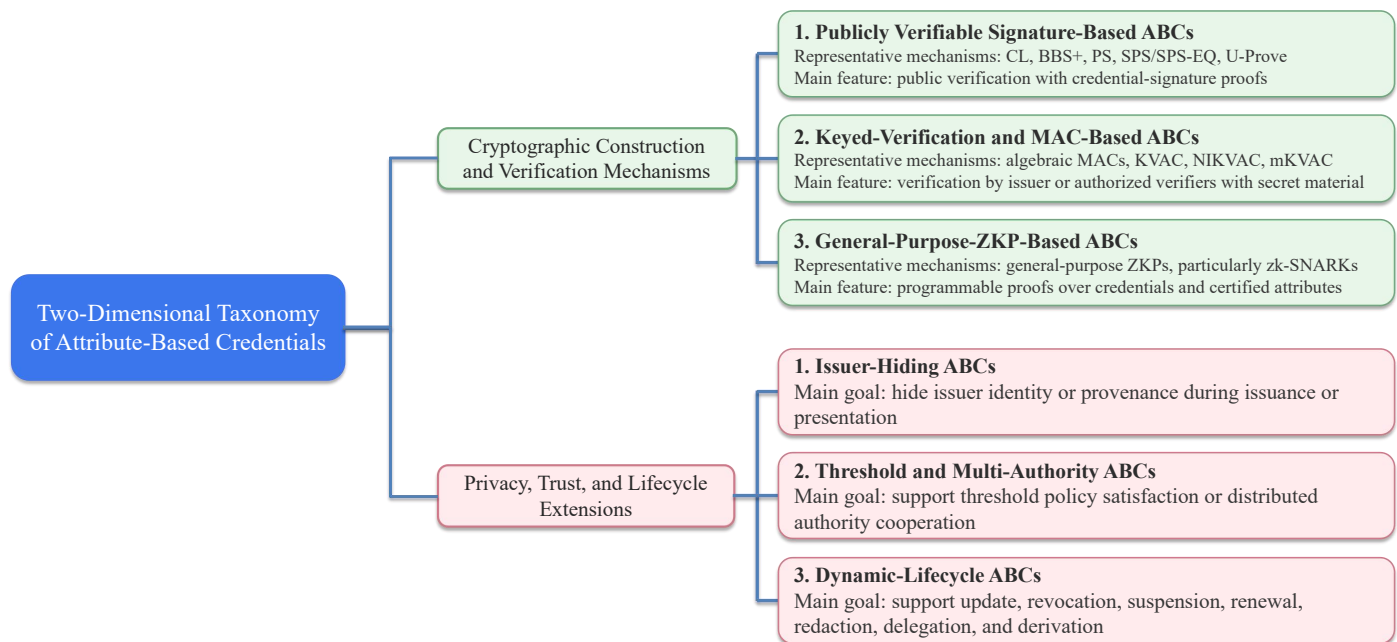
4. Classification of Attribute-Based Credentials

Existing ABC schemes differ in their cryptographic constructions, verification models, privacy objectives, trust structures, and lifecycle capabilities. Accordingly, this review organizes them along the construction and extension dimensions, as illustrated in Figure 2. The taxonomy focuses on the dominant and recurrent categories identified in the existing ABC literature rather than attempting to enumerate every specialized construction. The two dimensions are cross-cutting. Practical ABC schemes may incorporate multiple auxiliary cryptographic mechanisms. For classification along the construction dimension, however, each scheme is assigned according to its principal cryptographic construction and privacy-preserving presentation mechanism. Highly specialized schemes are therefore discussed within the most closely related category rather than introduced as additional standalone categories.

Table 3 maps representative ABC schemes to the corresponding construction categories. The extension tags in the table correspond to the extension capabilities considered in this review and indicate additional capabilities supported by the schemes rather than features inherent to or required by the corresponding construction category; different schemes within the same construction category may support different combinations of extensions. It should be noted that the general-purpose-ZKP-based category defined in this review refers to constructions in which a general-purpose zero-knowledge proof system serves as the principal privacy-preserving presentation layer, rather than constructions relying on proof mechanisms specifically designed for possession, selective disclosure, or attribute predicates over a particular credential or cryptographic primitive.

Table 3. Mapping of Representative ABC Schemes to the Construction Categories.

Category	Representative Scheme	Credential Primitive	Presentation Proof Layer	Verifier Model	Extension Tags
Publicly Verifiable Signature-Based ABCs	Idemix [10]	CL signature	CL-signature-specific interactive ZK proof	Public verifier	–
	Coconut [27]	Threshold re-randomizable signature	Sigma-protocol proofs of knowledge of discrete-log representations	Public verifier	Threshold issuance
	Graebnitz et al. [28]	BBS+ signature	BBS+-specific signature proofs of knowledge (SPKs)	Public verifier	Revocation
Keyed-Verification and MAC-Based ABCs	KVAC [29]	Algebraic MAC	Algebraic-MAC-specific interactive ZK proof	Issuer or verifier sharing the secret verification key	–
	NIKVAC [30]	Algebraic MAC	Oblivious designated-verifier NIZK	Designated verifier holding secret verification material	–
General-Purpose ZKP-Based ABCs	ZKclaims [31]	Traditional public-key signature	General-purpose zk-SNARK	Public verifier	–
	zk-creds [32]	Credential commitment with issuance-list membership; standard-signature issuance also supported	General-purpose zk-SNARKs (Groth16 implementation)	Public verifier	Issuer hiding; Threshold issuance; Revocation, Delegation



Note: The two dimensions are cross-cutting, and the categories are not mutually exclusive. A practical ABC scheme may combine mechanisms from multiple construction categories and incorporate one or more privacy, trust, or lifecycle extensions.

Figure 2. Two-Dimensional Taxonomy of Attribute-Based Credentials.

4.1. Cryptographic Construction and Verification Mechanisms

In this dimension, ABC schemes are classified into three categories according to their principal cryptographic architecture: publicly verifiable signature-based ABC constructions, keyed-verification and MAC-based ABC constructions, and general-purpose ZKP-based ABC constructions. For each category, the following discussion highlights several representative and recurrent construction approaches to help readers understand its principal mechanisms and distinguishing characteristics.

4.1.1. Publicly Verifiable Signature-Based ABC Constructions

Publicly verifiable signature-based credential constructions use publicly verifiable signature primitives, including conventional public-key signatures and dedicated credential-signature schemes, to authenticate certified attributes. Through the issuance protocol, the issuer authenticates a set of attributes, committed attributes, or another structured credential representation using its issuing key. During presentation, the holder may selectively disclose certified attributes and, where supported, randomize the credential or generate a proof of knowledge demonstrating possession of a valid signature and satisfaction of the required presentation conditions. Any verifier possessing authentic public verification material can validate the resulting presentation without access to secret issuer-side verification material.

CL-Signature-Based Credentials: Camenisch–Lysyanskaya (CL) signatures and their variants are foundational multi-message signature constructions for privacy-preserving ABC systems, particularly anonymous-credential systems [7,33]. Their associated issuance and proof protocols allow attributes to remain committed or hidden while enabling the holder to prove knowledge of a valid signature, selectively disclose certified attributes, or prove supported relations over undisclosed attributes. Idemix is a prominent CL-based credential system that supports privacy-preserving credential issuance, selective disclosure, predicate proofs, and unlinkable credential presentations [10].

BBS+ Signature-Based Credentials: The BBS+ signature scheme used in privacy-preserving credential constructions was detailed and analyzed by Au et al. [34] as a modifi-

cation of the Boneh–Boyen–Shacham (BBS) short group signature construction [35]. BBS+ is a pairing-based multi-message signature construction that supports efficient proofs of knowledge of a valid signature, through which a holder can selectively disclose signed messages while keeping the remaining messages hidden. Doerner et al. proposed a threshold BBS+ protocol for distributed anonymous-credential issuance, while Graebnitz et al. specified a BBS+-based anonymous credential system supporting privacy-preserving attribute presentation, device binding, non-duplication, and privacy-preserving revocation [28,36].

Pointcheval Sanders (PS) Signature-Based Credentials: PS signatures are short, randomizable, pairing-based multi-message signatures that support efficient proofs of knowledge of a valid signature on committed or hidden messages [37]. During presentation, a holder can randomize the signature, selectively disclose certified attributes, and prove knowledge of the remaining signed values without revealing the complete credential. Their algebraic structure facilitates composition with pairing-based proof protocols and distributed issuance mechanisms. Coconut combines PS-based techniques with additional signature mechanisms to support threshold issuance, credential re-randomization, and unlinkable selective-disclosure presentations, while Sanders and Traoré adapted PS signatures to construct issuer-hiding anonymous credentials [27,38].

Structure-Preserving Signature and SPS-EQ-Based Credentials: Structure-Preserving Signatures (SPSs) represent messages, signatures, and public verification material as group elements and express verification through pairing-product equations, thereby facilitating composition with pairing-based proof systems [39]. Structure-Preserving Signatures on Equivalence Classes (SPS-EQ) further allow signed message representatives and their corresponding signatures to be consistently randomized within an equivalence class while preserving verifiability, supporting unlinkable presentations and proofs over certified group elements [40]. Fuchsbauer et al. used SPS-EQ to construct a constant-size, multi-show attribute-based anonymous credential system, while Connolly et al. subsequently improved related credential constructions and extended their proof capabilities [40,41].

U-Prove-Based Credentials: U-Prove is a publicly verifiable, pairing-free ABC technology derived from Brands-style discrete-logarithm-based credential constructions. An issuer creates a token encoding certified attributes, and the holder can prove possession of the token while selectively disclosing attributes; accompanying extensions can additionally support predicates over committed attributes [11]. U-Prove offers relatively compact tokens and efficient verification, but its privacy model differs from that of multi-show unlinkable credential systems because repeated use of the same token may permit linkage; unlinkable use therefore generally requires distinct tokens. Mostowski and Vullers implemented U-Prove anonymous credentials on smart cards, demonstrating their feasibility on resource-constrained devices, while de Fuentes et al. adapted and evaluated U-Prove for privacy-preserving attribute presentation in vehicular services [42,43].

Specialized Signature-Based Credentials: Beyond the major constructions above, some ABC schemes employ specialized signature primitives that support randomization, aggregation, redaction, delegation, or transformations among equivalent message representations. When integrated with appropriate issuance and presentation protocols, these properties can enable unlinkable credential transformations, compact presentation of credentials from multiple issuers, controlled removal or derivation of certified attributes, and delegatable credentials. The signature properties alone do not constitute a complete ABC system and must be combined with mechanisms for attribute certification, privacy-preserving presentation, and policy verification. Mir et al. constructed issuer-hiding multi-authority anonymous credentials using aggregate signatures with randomizable tags and public keys and aggregate mercurial signatures [44]. Shi et al. proposed threshold

attribute-based credentials based on redactable signatures, while Mir et al. developed practical delegatable anonymous credentials from equivalence-class signatures [45,46].

4.1.2. Keyed-Verification and MAC-Based ABC Constructions

Keyed-verification and MAC-based ABC constructions use secret verification material rather than a publicly verifiable signature to authenticate certified attributes. The issuer typically generates a credential using an algebraic Message Authentication Code (MAC) or another keyed credential primitive. During presentation, the holder proves possession of a valid credential and, where supported, discloses selected attributes or proves relations over hidden attributes without revealing the credential itself or the secret verification material. The resulting presentation can be validated only by the issuer or by authorized verifiers that have been securely provisioned with the required verification material.

Algebraic-MAC-Based Credentials: Algebraic-MAC-based credentials authenticate certified attributes using MACs whose algebraic structure supports privacy-preserving proofs of credential possession. Chase et al. introduced algebraic MACs and constructed Keyed-Verification Anonymous Credential (KVAC) schemes in which a holder proves possession of a valid MAC over certified attributes without revealing the MAC or the undisclosed attribute values [29]. Barki et al. subsequently proposed improved algebraic MAC constructions and practical KVAC protocols for efficient credential issuance and presentation, supporting selective disclosure, multi-show unlinkability, and constant-size presentations [47]. More recently, Mirzamohammadi et al. proposed two keyed-verification credential constructions with efficient partial disclosure and constant-size presentations, including a pairing-based construction using structure-preserving MACs on equivalence classes and a pairing-free construction based on homomorphic MACs [48]. Chase, Perrin, and Zaverucha further integrated an algebraic-MAC-based keyed-verification credential scheme with verifiable encryption in the Signal private-group system, enabling users to prove possession of credentials over encrypted identifiers and profile-related attributes while allowing the server to enforce group-membership and administrative policies without learning the underlying identities [49].

Non-Interactive Keyed-Verification Credentials: Non-interactive keyed-verification credentials allow a holder to generate a presentation that can be verified using secret verification material without an additional online challenge–response exchange. Couteau and Reichle constructed the first Non-Interactive Keyed-Verification Anonymous Credential (NIKVAC) system in the standard model without bilinear pairings [30]. Their attribute-based construction combines an algebraic MAC with a designated-verifier non-interactive zero-knowledge proof, allowing holders to prove possession of credentials over certified attributes while supporting multi-show unlinkability and conditional anonymity revocation. This presentation model is particularly relevant to one-pass, asynchronous, or offline communication settings in which interactive verification is impractical.

Multi-Verifier Keyed-Verification Credentials: Conventional keyed-verification credentials generally assume that the issuer also performs verification or shares secret verification material with a restricted verifier. Multi-verifier keyed-verification credentials extend this model by supporting multiple authorized verifiers without enabling unrestricted public verification. Bobolz et al. formalized Multi-Verifier Keyed-Verification Anonymous Credentials (mKVACs), in which each verifier shares an individual secret key with the issuer and holders obtain verifier-specific credentials. Their pairing-free construction preserves multi-show unlinkability and prevents the compromise of one verifier from undermining the unforgeability guarantees associated with other verifiers [50].

4.1.3. General-Purpose ZKP-Based ABC Constructions

General-purpose ZKP-based ABC Constructions use a programmable zero-knowledge proof system as the principal presentation and verification layer. Rather than relying exclusively on a signature or MAC specifically designed for privacy-preserving credentials, these constructions encode the validity of one or more underlying credentials and statements or predicates over their certified attributes as a general proof relation. During presentation, the holder proves that the underlying credentials were issued by accepted authorities and that their certified attributes satisfy the required conditions without revealing the complete credentials or the private witnesses used to generate the proof. The programmability of the proof relation enables range, set-membership, equality, consistency, and application-specific predicates over hidden certified attributes, as well as proofs combining information from multiple credentials or issuers. It can also accommodate heterogeneous credential representations, although more complex proof relations generally increase circuit size, prover cost, memory consumption, and implementation complexity.

The category does not include every ABC construction that employs a zero-knowledge proof as an auxiliary presentation mechanism. Instead, it covers constructions in which a general-purpose zero-knowledge proof system serves as the principal mechanism for privacy-preserving credential presentation and verification. Representative constructions are predominantly based on SNARKs, particularly zk-SNARKs. ZKclaims applies SNARKs to enable privacy-preserving and non-interactive proofs of statements over credentials issued by trusted authorities [31]. More recently, Rosenberg et al. proposed zk-creds, which uses general-purpose zk-SNARKs to derive flexible privacy-preserving credentials from existing identity documents and infrastructures and supports composable statements over multiple credentials [32].

4.2. Privacy, Trust, and Lifecycle Extensions

The extension dimension classifies ABC schemes according to the additional privacy, trust-distribution, and lifecycle capabilities incorporated into their credential systems. These categories are cross-cutting and may overlap, as the same ABC scheme may combine several extension capabilities depending on its privacy objectives, trust model, and deployment requirements.

4.2.1. Issuer-Hiding ABCs

Issuer-hiding ABCs conceal issuer-related information that might otherwise be exposed through public keys, identifiers, credential formats, verification parameters, or presentation metadata. Such information may reveal sensitive contextual details about the holder, including institutional affiliation, organizational membership, service usage, or interaction with a particular authority. Issuer hiding is therefore a cross-cutting privacy extension rather than an independent credential-authentication mechanism: it may be incorporated into different ABC constructions while preserving credential authenticity and issuer authorization [51,52]. Different constructions vary according to the parties from whom the issuer is hidden, the issuer-related information that remains visible, and whether the issuer can be identified under exceptional conditions.

Verifier-Side Issuer-Hiding: Verifier-side issuer-hiding credentials allow a holder to prove that a credential was issued by an authorized issuer, or by a member of an accepted issuer set, without revealing the exact issuer to the verifier. Bobolz et al. proposed an issuer-hiding credential scheme in which a holder can demonstrate credential validity while concealing the issuer's public key from the verifier [53]. Hecate further combines issuer hiding with threshold credential issuance and private-verifier authorization, allowing

credential validity and access policies to be verified without revealing the specific issuing authority [54].

Double-Issuer-Hiding: Double-issuer-hiding credentials conceal the identity of the credential issuer from both the holder during issuance and the verifier during presentation. Shi et al. introduced Double Issuer-Hiding Attribute-Based Credentials (DIHAC), in which a central authority authorizes a group of issuers, a holder obtains an attribute-based credential from one authorized issuer without learning its specific identity, and the holder subsequently proves to a verifier that the credential originated from an authorized issuer without revealing which one [55].

4.2.2. Threshold and Multi-Authority ABCs

Threshold and multi-authority operations distribute credential-related conditions, responsibilities, or decision-making across multiple attributes or authorities. They may allow a holder to satisfy a threshold policy, require several issuers to cooperate in credential issuance, enable attributes certified by different authorities to be combined within one presentation, or distribute revocation, verification, and accountability functions among several entities.

Threshold functionality appears at both the policy level and the authority level. Policy-level threshold satisfaction concerns how many attribute conditions must be proved by a holder, whereas authority-level threshold operations concern how many authorities must cooperate in a credential-related process. Authority-level constructions can reduce dependence on a single entity and support more flexible trust models, but they also introduce additional coordination, availability, and key-management requirements.

Policy-Level Thresholds: Policy-level threshold mechanisms allow a holder to prove that at least t out of n designated certified attributes or policy conditions are satisfied without disclosing all of the underlying attributes. Shahandashti and Safavi-Naini introduced threshold attribute-based signatures and applied them to construct a threshold attribute-based anonymous credential system, enabling threshold verification over certified attributes while preserving attribute privacy [56].

Threshold Credential Issuance: Threshold credential issuance distributes issuance authority among multiple issuers so that a valid credential can be generated only after a prescribed threshold of issuance shares has been collected. In a conventional t -out-of- n setting, each issuer contributes a partial issuance result, and at least t valid contributions are required. Doerner et al. constructed a threshold BBS+ protocol for distributed anonymous-credential issuance [36]. Hecate further combines threshold credential issuance with private-verifier functionality and issuer hiding [54]. Weighted threshold issuance generalizes equal issuer participation by assigning different weights to the participating issuers and authorizing issuance once their combined weight reaches a predefined threshold. Zhang et al. proposed Weighted Threshold Anonymous Credentials (WTAC), combining weighted threshold issuance with redactable fine-grained blind signatures and issuer hiding from both holders and verifiers [57].

Multi-Authority Attribute Certification: Multi-authority attribute certification allows independent authorities to certify attributes or credential components within their respective domains, after which the holder combines the resulting credentials or presentation proofs to satisfy a verification policy. Unlike threshold issuance, the authorities need not jointly participate in generating a single credential or meet a prescribed issuance threshold. Hébant and Pointcheval proposed traceable constant-size multi-authority credentials that support the combination of credentials issued by multiple authorities while retaining accountability [15]. Mir et al. further constructed issuer-hiding multi-authority anonymous

credentials using aggregate signatures, allowing credential information from multiple issuers to be combined while concealing the participating issuers during presentation [44].

Threshold Revocation and Credential Management: Threshold revocation and credential management distribute post-issuance authority so that credential revocation or another lifecycle action requires cooperation from a prescribed subset of authorities. Jia et al. proposed a generic threshold credential-management system supporting threshold issuance and revocation together with user-autonomy credential aggregation, in which multiple credential managers jointly approve issuance and revocation operations [58]. Bisht et al. further proposed Revocable TACO, which integrates a dynamic-threshold-accumulator-based revocation mechanism into threshold anonymous credentials deployed over blockchains [59].

Threshold Accountability: Threshold accountability distributes conditional identity recovery among multiple authorized authorities so that no single entity can independently identify the holder associated with an anonymous credential. Naaz et al. proposed DTRAC, which integrates threshold opening with threshold credential issuance over blockchains and requires cooperation among distributed openers to reveal a holder's identity under authorized conditions [60]. More recently, Xie et al. proposed AccCred, an accountable anonymous credential system in which users and issuers select a hidden committee from a set of authenticated candidates to perform conditional identity recovery, while the identities of the selected committee members remain concealed from nonmembers [61]. Jia et al. proposed a multi-authority anonymous credential system with efficient and decentralized supervision. A threshold of supervisors can jointly trace credential proofs to recover the identities of misbehaving users and generate linking keys that enable verifiers to efficiently link their credential proofs [62].

4.2.3. Dynamic-Lifecycle ABCs

Dynamic-Lifecycle ABCs support controlled post-issuance changes to credential contents, validity, status, or authorization scope. Representative capabilities include credential and attribute updates, revocation and suspension, expiration and renewal, epoch transitions, credential redaction, delegation, and credential derivation [17,63,64]. These capabilities are important in environments where certified attributes, organizational roles, validity conditions, holder status, or authorization relationships may change over time. They allow a credential system to respond to such changes without necessarily requiring complete credential reissuance for every lifecycle event.

Credential and Attribute Updates: Credential and attribute update mechanisms allow authorized changes to certified attributes after issuance while preserving the authenticity of the unchanged credential information. Blömer et al. introduced updatable anonymous credentials in which a holder interacts with the issuer to update certified attributes without revealing their previous values to the issuer [17]. Yang et al. applied updatable attribute-based anonymous credentials in AnoPay, where credential attributes are updated to support privacy-preserving vehicle-parking payments with constant payment overhead [65]. More recently, Sawai et al. proposed Attribute-Based Anonymous Credentials with Update Broadcast (ABC-UB), enabling an issuer to broadcast a common update token that holders use to update their credentials locally, thereby reducing the issuer's computation and communication costs for large-scale updates [66].

Credential Revocation and Suspension: Credential revocation permanently invalidates a credential or a defined scope of its use, whereas suspension temporarily disables credential use and may permit later reinstatement. Derler et al. constructed a revocable attribute-based anonymous credential system that supports privacy-preserving verification of credential status [63]. More recently, Xie et al. proposed FDAAC-CR, a delegatable

attribute-based anonymous credential system with fine-grained delegation management and chainable revocation, in which revoking a credential within a delegation chain also invalidates the credentials subsequently derived from it [67].

Expiration, Renewal, and Epoch Transitions: Expiration limits credential validity to a predefined period, while renewal extends or refreshes that validity for an eligible holder. Epoch-based mechanisms divide credential operation into discrete periods and require credentials, status information, or presentation components to be updated for the current epoch. Lueks et al. proposed an epoch-based revocation mechanism for attribute-based credentials in which epoch- and verifier-specific revocation tokens enable efficient credential-status verification while limiting linkage across different epochs [68]. More recently, Li et al. proposed MA-ACEW, which combines long-term credentials with fresh epoch-specific credential components to support efficient updates across epoch transitions and ensure that only credentials valid for the current epoch are accepted [69].

Credential Redaction: Credential redaction allows an authorized party to remove selected attributes or components from a credential, or to derive a reduced credential containing only an authorized subset of certified attributes, while preserving the authenticity and verifiability of the retained information. Unlike selective disclosure, which hides attributes only within a particular presentation while leaving the underlying credential unchanged, redaction produces a transformed or derived credential representation. Liu et al. proposed PERCE, which supports permissioned credential redaction together with period- and epoch-dependent controls over credential use [64]. More recently, Hatsugai et al. introduced Attribute-Based Credentials with Credential Redaction (ABC-CR), enabling a holder to extract selected attributes and create credentials that can be delegated and presented by another party, using an unlinkable twice-redactable signature construction [70].

Credential Delegation and Derivation: Credential delegation enables an authorized holder or intermediate issuer to derive a restricted credential for another holder while preserving a verifiable chain to an authorized root issuer. The derived credential may contain a subset of certified attributes or impose narrower authorization scopes and delegation constraints. Blömer and Bobolz proposed delegatable attribute-based anonymous credentials based on dynamically malleable signatures [71]. Mir et al. later combined threshold issuance with controlled and fine-grained credential delegation in a decentralized anonymous-credential system [72]. Griffy et al. further constructed mercurial-signature-based delegatable anonymous credentials with stronger privacy against tracing by intermediate issuers and support for revocation tokens [73].

4.3. Comparative Analysis of ABC Categories

Table 4 compares publicly verifiable signature-based, keyed-verification and MAC-based, and general-purpose ZKP-based ABC constructions, whereas Table 5 compares issuer-hiding, threshold and multi-authority, and dynamic-lifecycle ABC extensions. The comparison distinguishes structural and protocol-level characteristics from qualitative implementation tendencies. The entries concerning cryptographic basis, verification, proof capability, privacy and trust, and deployment requirements summarize structural or protocol-level characteristics supported by the designs and properties reported for representative schemes. The entries concerning typical efficiency considerations and extension-related overhead and availability instead summarize qualitative tendencies and dominant cost factors rather than a quantitative ranking of the categories. These entries should therefore not be interpreted as category-level performance rankings or as results obtained from a common experimental benchmark. As also observed in prior systematizations of anonymous credentials, comprehensive efficiency comparison is difficult because com-

parable reference implementations are limited and the relevant metrics, scaling factors, evaluation settings, and reporting formats differ across schemes [4].

Publicly verifiable signature-based ABCs enable verification using public trust material without provisioning individual verifiers with secret credential-verification keys. Keyed-verification and MAC-based ABCs instead restrict verification to parties holding authorized secret verification material, thereby introducing verifier authorization, provisioning, and key-management requirements. General-purpose ZKP-based ABCs provide programmable proof relations for complex predicates and heterogeneous credential formats. Their concrete prover cost and implementation effort depend strongly on the selected proof system, credential encoding, and statement complexity. Accordingly, the efficiency entries in Table 4 identify typical cost factors and implementation tendencies rather than providing a quantitative ranking of the construction categories.

Table 4. Comparison of ABC Construction Categories.

Categories	Publicly Verifiable Signature-Based ABCs	Keyed-Verification and MAC-Based ABCs	General-Purpose ZKP-Based ABCs
Principal basis	Publicly verifiable signatures authenticate certified attributes, with presentation based on disclosure, randomization, or proofs of signature possession.	Secret-keyed relations, commonly algebraic MACs, authenticate attributes and support proofs to authorized verifiers.	Programmable zero-knowledge relations prove credential validity and statements over certified attributes.
Verification model	Any verifier with authentic public verification material can validate a presentation.	Only the issuer or authorized verifiers holding secret verification material can verify.	Verification is commonly public, while the underlying credential and trust models remain construction-dependent.
Proof capability	Commonly supports selective disclosure and credential-possession proofs; complex predicates may require additional mechanisms.	May support selective disclosure, hidden-attribute proofs, and unlinkable presentations in restricted-verifier settings.	Supports programmable predicates, cross-credential relations, and heterogeneous credential formats.
Privacy profile	Attribute privacy and unlinkability depend on credential randomization and presentation proofs.	Restricted verification limits arbitrary third-party testing, but privacy remains construction-dependent.	Proofs can hide credentials and witnesses, while unlinkability and metadata privacy require additional support.
Typical efficiency considerations	Dominant costs can include exponentiations, pairings, credential randomization, and presentation-proof generation, depending on the underlying credential and proof construction.	Representative constructions may provide compact credentials or presentations; computation depends on the underlying keyed relation, selective-disclosure mechanism, and presentation protocol.	Proofs may be succinct in some systems, whereas prover computation, memory use, and circuit or relation size depend strongly on the selected proof system and encoded statement.
Trust and deployment requirements	Requires authenticated public verification material and an appropriate public trust-distribution mechanism, but does not require per-verifier secret credential-verification keys.	Requires authorization, secure provisioning, protection, and lifecycle management of secret verification material for eligible verifiers.	Requires integration of the selected proof system with credential representations and application predicates; some systems additionally require setup material, circuit or relation engineering, and proof-system-specific infrastructure.
Main limitations	Dependence on specialized primitives, additional proof-composition costs, and limited native lifecycle support in many constructions.	Restricted verifier openness, secret-key risks, and limited cross-domain interoperability.	Potentially high prover cost, circuit or relation engineering complexity, setup requirements for some proof systems, and credential-encoding effort.

Scheme-level empirical evaluations provide additional evidence for selected implementations. For example, prior work has evaluated the memory usage and computation time of I2PA, U-Prove, and Idemix in an IoT setting, while U-Prove has also been implemented and evaluated on smart cards and adapted to privacy-preserving vehicular-service scenarios [12,42,43]. These results are useful for assessing the feasibility and performance of particular systems, but differences in supported functionality, cryptographic parameters,

implementation maturity, hardware platforms, and experimental workloads prevent them from serving as a controlled benchmark for the broader construction categories.

The extension categories address different limitations of basic credential issuance and presentation. Issuer-hiding ABCs primarily protect credential provenance. Threshold and multi-authority ABCs distribute policy satisfaction across attributes and decision-making or trust across authorities. Dynamic-lifecycle ABCs regulate how credentials evolve after issuance. These extensions are not alternatives to the construction categories and may be combined with publicly verifiable signature-based, keyed-verification and MAC-based, or general-purpose ZKP-based constructions.

Adding an extension also introduces corresponding operational obligations. Stronger issuer hiding requires appropriate issuer authorization and protection against indirect provenance leakage. Threshold and multi-authority operations require coordination, availability, and collusion resistance. Dynamic lifecycle management requires synchronized state, fresh status information, and clear propagation rules for updates, revocation, delegation, and derived credentials. The practical value of an extension therefore depends not only on whether a scheme formally supports the capability but also on whether the surrounding infrastructure can maintain its security and privacy guarantees over time.

Table 5. Comparison of ABC Extension Categories.

Categories	Issuer-Hiding ABCs	Threshold and Multi-Authority ABCs	Dynamic-Lifecycle ABCs
Extension focus	Conceal issuer identity or provenance during credential issuance or presentation.	Distribute policy satisfaction and credential operations across multiple attributes or authorities.	Control post-issuance changes to credential contents, validity, status, or authorization scope.
Core capabilities	Verifier-side issuer hiding and double issuer hiding.	Policy-level thresholds, threshold or weighted issuance, multi-authority certification, and distributed revocation or accountability.	Updates, revocation, suspension, renewal, epoch transitions, redaction, delegation, and credential derivation.
Primary benefit	Reduces issuer-based profiling, provenance leakage, and contextual inference.	Reduces reliance on a single authority and supports flexible distribution of trust and responsibility.	Adapts credentials to changing attributes, roles, validity conditions, and authorization relationships without full reissuance.
Operational requirements	Requires authorized issuer-set management, membership updates, and hidden-issuer revocation.	Requires threshold rules, authority eligibility, key or share management, coordination, and participant availability.	Requires authorization rules, version and status synchronization, and propagation across original and derived credentials.
Privacy and trust	Improves issuer privacy, but metadata and status information may reveal provenance or conflict with accountability.	Distributes trust, but sufficient collusion or shared administrative control may undermine its benefits.	Improves lifecycle responsiveness, but status checks and update interactions may introduce linkability.
Operational overhead and availability requirements	Introduces issuer-authorization proofs, trust-registry maintenance, and hidden-issuer revocation costs.	Introduces multiparty communication, distributed key management, coordination latency, and quorum-availability requirements.	Introduces status storage, update communication, renewal or epoch refresh, and delegation-chain management.
Main limitations	Indirect issuer leakage, rogue-issuer risks, and complex accountability and revocation.	Collusion, authority unavailability, communication overhead, and governance complexity.	Stale status, rollback attacks, incomplete change propagation, and increasing state-management complexity.

Table 6 provides a scheme-level comparison of representative ABC schemes across six dimensions and maps each scheme to its principal construction class and extension tags. Reported proof sizes are taken from the cited sources and should not be interpreted as directly comparable across different parameter settings, proof configurations, and implementations.

Table 6. Scheme-Level Comparison of Representative ABC Schemes.

Scheme	Class/Extensions	Assumptions	Proof Size	Verifier	Predicates	Credential Revocation	Implementation
Idemix [10,33]	PV-Sig	Strong RSA	N/R	Public	Selective disclosure; attribute predicates	Not implemented in cited prototype	Java prototype
Coconut [27]	PV-Sig/TH	LRSW, XDH, ROM	≈157 B	Public	Selective disclosure; statements over attributes	N/R	Chainspace/Ethereum smart-contract implementations
Graebnitz et al. [28]	PV-Sig/DL	q-SDH (BBS+); trusted issuer and device manufacturer	N/R	Public	Selective disclosure	Time-based Linked Validity Verifiable Credentials	Specification; no implementation
KVAC [29]	KV/MAC	GGM or DDH, depending on the MAC	256 B [30]	Secret-key verifier	Attribute relations	N/R	Operation-level benchmarks
NIKVAC [30]	KV/MAC	GGM; Paillier/DCR; short-exp DLog	756 B	Designated verifier	Attribute relations	N/R; anonymity revocation supported	No implementation reported
ZKclaims [31]	GP-ZKP	Groth zk-SNARK; trusted issuer	137 B	Public	Comparison predicates	N/R	libsark/reclaimID prototype
zk-creds [32]	GP-ZKP/IH, TH, DL	Groth16 security assumptions; ROM, DLog	192–1064 B	Public	General NP relations and composable access criteria	Issuance-list removal	Implemented and benchmarked toolkit

Abbreviations: PV-Sig: Publicly Verifiable Signature-Based; KV/MAC: Keyed-Verification and MAC-Based; GP-ZKP: General-Purpose ZKP-Based; IH: Issuer Hiding; TH: Threshold Issuance; DL: Dynamic Lifecycle; LRSW: Lysyanskaya–Rivest–Sahai–Wolf; XDH: External Diffie–Hellman; q-SDH: q-Strong Diffie–Hellman; GGM: Generic Group Model; DDH: Decisional Diffie–Hellman; DCR: Decisional Composite Residuosity; ROM: Random Oracle Model; DLog: discrete logarithm; N/R: not reported in the cited source.

4.4. Application-Oriented Use of the Taxonomy

The proposed taxonomy can also serve as a design-selection aid by mapping application requirements to construction and extension choices. Rather than identifying a universally preferable ABC category, the taxonomy helps designers first determine the required verification model and proof capability and then identify additional privacy, trust-distribution, or lifecycle functions that must be incorporated. The following scenarios illustrate this use.

Scenario 1—Cross-Domain Digital Identity and Public-Service Credentials: Consider a digital identity credential that may be presented to public agencies, universities, employers, financial institutions, or other independently administered verifiers. The holder may need to disclose only selected attributes, such as residency or professional qualification, while the set of verifiers cannot reasonably be provisioned with secret verification material. Under the construction dimension, these requirements favor a publicly verifiable signature-based ABC because presentations can be validated using authenticated public verification material across organizational boundaries. The extension dimension can then refine the design according to operational requirements. A dynamic-lifecycle extension is appropriate when attributes, authorization status, or credential validity may change after issuance and therefore require revocation, renewal, status synchronization, or update mechanisms. If revealing the issuing organization would expose sensitive affiliation or provenance information, an issuer-hiding extension may additionally be incorporated.

Scenario 2—Complex Privacy-Preserving Eligibility Verification over Heterogeneous Credentials: Consider an online service in which a user must demonstrate that several conditions are simultaneously satisfied, for example that the user exceeds an age threshold, holds a required qualification, and satisfies a residency or membership condition, while the underlying credentials and exact attribute values remain hidden. If these statements involve heterogeneous credential formats, multiple credentials, or application-specific relations, the construction dimension points toward a general-purpose ZKP-based ABC because the required conditions can be encoded as programmable proof relations. If several independent authorities must jointly certify attributes or participate in credential issuance, a threshold or multi-authority extension can be added to distribute trust and credential issuance across authorities. In contrast, if the same service is operated within a closed environment containing a limited set of authorized verifiers that can securely receive and manage secret verification material, the taxonomy indicates that a keyed-verification or MAC-based ABC may instead be appropriate, particularly when unrestricted third-party verification is unnecessary.

5. Challenges and Future Directions

5.1. Challenges and Representative Technical Responses

This section examines the major challenges identified in the reviewed literature and discusses representative technical responses. Their effectiveness depends on the credential construction, security assumptions, trust model, deployment environment, and required privacy properties. Related areas, including attribute-based encryption, access control, authentication, and statistical privacy, may also offer transferable design insights.

5.1.1. Efficiency Optimization for Multi-Attribute Management

Supporting multiple certified attributes is a central characteristic and advantage of ABCs, but it can introduce substantial computational and communication overhead during credential issuance and presentation. In some proof-based constructions, presentation cost may increase with the number of hidden or disclosed attributes, evaluated predicates, or credentials combined within a presentation.

Representative technical responses and related design approaches include the following:

- **Proof Aggregation and Batch Verification:** Proof aggregation combines multiple credential-possession statements or attribute predicates into fewer proof objects, while batch verification amortizes repeated cryptographic operations across several proofs or presentations. Aggregated and logarithmic-size proof systems can reduce proof size and verification cost in multi-attribute settings [74,75]. For example, AVCA-hDID uses randomized tag-based aggregate signatures to combine heterogeneous identity attributes into a compact verifiable object in a decentralized identity setting [76].
- **Hierarchical Structures:** Flat organization of large attribute sets, policies, or authorities may lead to inefficient verification, repeated policy processing, and increasing management overhead. Hierarchical structures introduce logical levels to improve processing efficiency and support scalable attribute and authority management. Different schemes adopt different hierarchical strategies. Ali et al. proposed a lightweight revocable hierarchical ABE scheme with a central authority and multiple domain authorities, enabling scalable key delegation and efficient user revocation [77]. He et al. integrated multiple hierarchical access policies into a unified linear secret-sharing structure, allowing users satisfying different policy levels to access the corresponding data [78]. Li et al. organized attributes into hierarchical vectors, supporting key delegation from higher-level to lower-level attributes and providing continuous leakage resilience [79].
- **Lightweight and Assisted Computation:** Lightweight and assisted-computation techniques reduce holder-side overhead through precomputation, compact cryptographic representations, or division of computation between a constrained device and a more powerful helper while retaining essential secret-dependent operations on the holder-controlled device. Hanzlik and Slamanig proposed core/helper anonymous credentials, in which a constrained core device performs a small computation independent of the credential size or the number of attributes, while a helper device completes the remaining presentation operations without being able to generate a valid presentation independently [14]. He et al. proposed a lightweight CP-ABE scheme that delegates expensive operations to a proxy server, requiring no pairing during encryption and only one pairing during decryption [80]. Gong et al. developed a multi-authority attribute-based signcryption scheme using outsourced computation and compact ciphertexts to reduce computation, communication, and storage costs for constrained users [81].

5.1.2. Privacy-Preserving Credential Lifecycle Management

Dynamic-lifecycle capabilities allow ABC systems to respond to changes in certified attributes, credential validity, and authorization relationships after issuance. However, introducing updates, revocation, delegation, and credential derivation also creates new challenges. Lifecycle operations may expose holder activity through repeated status interactions, impose substantial update costs on users and verifiers, or leave inconsistent authorization states across original and derived credentials. The central challenge is therefore to maintain timely and correct credential state without weakening the privacy and usability guarantees of credential presentation.

Representative technical responses and related design approaches include the following:

- **Privacy-Preserving Lifecycle Interactions:** Credential updates and non-revocation checks may require holders to interact with an issuer, revocation authority, accumulator manager, or status service. If these interactions reveal a credential identifier, accumulator position, or recurring update request, the lifecycle service may link the holder's activities even when ordinary presentations remain unlinkable. Jaques et al.

proposed ALLOSAUR, a multi-party accumulator system that supports oblivious and sublinear anonymous-credential witness updates after revocation, reducing the information exposed to credential managers during the update process [82].

- **Scalable and Timely Revocation:** Revocation mechanisms must make newly revoked credentials unusable within an acceptable period while avoiding excessive computation, communication, or state distribution. Accumulator-based approaches can provide compact non-revocation proofs, but changes to the accumulated set may require valid holders to refresh their witnesses. Epoch-based mechanisms reduce update frequency but may delay the enforcement of revocation, while large revocation lists increase storage and verification costs. Edalatnejad et al. proposed a large-scale anonymous-credential revocation approach based on Private Record Certification, enabling a holder to obtain certification of a private status record without revealing which record was queried [83].
- **Consistency Across Updated, Delegated, and Derived Credentials:** Lifecycle management becomes more complex when credentials can be partially updated, delegated, redacted, or derived from earlier credentials. An update or revocation affecting an upstream credential may also need to invalidate or restrict downstream credentials; otherwise, an obsolete authorization state may remain usable. Li et al. integrated partial attribute updates, delegation, traceability, and revocation within an attribute-based anonymous credential construction, demonstrating that these lifecycle functions can be integrated within a single credential system [84]. Sun et al. further proposed a delegatable and revocable ABC based on purgeable signatures, allowing holders to delegate credentials over selected attributes and revoke their own or previously delegated credentials [85].

5.1.3. Privacy–Utility Trade-Off in Selective Disclosure

Selective disclosure enables holders to reveal only the attributes or predicates required for verification. However, disclosing fewer attributes does not always minimize privacy risk, because combinations of attributes, repeated presentations, and contextual information may still enable inference or linkage. The central challenge is therefore to provide sufficient evidence for the verifier while minimizing unnecessary disclosure and cross-context correlation.

Representative technical responses and related design approaches include the following:

- **Association-Risk-Aware Disclosure:** Attributes that appear non-sensitive in isolation may become identifying when combined with other disclosed attributes or external background knowledge. Association-aware mechanisms evaluate the sensitivity of individual attributes and their combinations and select less revealing credentials, attributes, or predicate proofs that still satisfy the verification request. Ardagna et al. represented credential portfolios, verifier requests, and sensitive associations as graphs and developed a heuristic for identifying low-sensitivity disclosures [86]. Related statistical privacy techniques, such as attribute slicing, may also inform the analysis of correlated disclosure risks [87].
- **Automated Minimal-Disclosure Policies:** Manual attribute selection may result in excessive disclosure or failure to satisfy the verifier’s policy. Automated mechanisms use disclosure policies, sensitivity preferences, and optimization rules to select a minimally sufficient set of credentials, attributes, or predicates. Paci et al. combined trust negotiation with minimal credential disclosure to release only the attributes needed for an interaction [88]. Crowder et al. further showed that simple language and clear explanations of system operation can improve users’ willingness to adopt ABC systems, highlighting the importance of understandable disclosure guidance [89].

5.1.4. Cross-System Interoperability and Standardization

ABC systems may use incompatible credential formats, attribute vocabularies, signature suites, proof protocols, trust models, and revocation mechanisms. Consequently, credentials containing semantically equivalent attributes may still be unusable across domains, thereby limiting credential portability and increasing integration, verification, and governance costs.

Representative technical responses and related design approaches include the following:

- **Unified Architecture and Interfaces:** Common credential specifications, issuance interfaces, and presentation-policy languages can decouple application logic from the underlying cryptographic mechanisms. Different ABC implementations can therefore express comparable credential requirements, attribute disclosures, and predicates through technology-independent interfaces. The ABC4Trust project developed a common architecture and corresponding interfaces to support the integration and interchangeability of different privacy-preserving ABC technologies [90].
- **Common Data Models and Attribute Semantics:** Common data models standardize the representation of issuers, holders, claims, presentations, and credential status, while shared vocabularies, namespaces, data types, units, assurance levels, and mapping rules align attribute meanings across domains. The W3C Verifiable Credentials Data Model provides a general representation layer for exchanging digital credentials [3]. However, common representation alone does not guarantee consistent interpretation of attributes across independently developed systems. Yamamoto et al. proposed a Linked-Data-based verifiable credential construction that combines machine-readable JSON-LD semantics with BBS+-based selective disclosure, illustrating how privacy-preserving credential presentations can retain semantic links across credentials issued by different entities [91].

5.1.5. Post-Quantum Security

Many established ABC constructions rely on factoring, discrete-logarithm, or pairing-based assumptions that would be threatened by sufficiently capable quantum computers using Shor's algorithm [92]. Post-quantum migration must therefore protect not only credential signatures but also presentation proofs, commitments, revocation mechanisms, update protocols, issuer authentication, and holder binding.

Representative technical responses and related design approaches include the following:

- **Lattice-Based Anonymous Credentials:** Lattice-based cryptography provides a direct foundation for constructing post-quantum anonymous credentials. Bootle et al. developed a practical framework for building anonymous credential schemes from lattice assumptions [13]. Jeudy et al. constructed a lattice-based signature with efficient proof protocols and applied it to an anonymous credential system [93]. These constructions demonstrate that credential issuance and privacy-preserving presentation can be realized without relying on factoring, discrete logarithms, or pairings. Practical deployment must nevertheless integrate efficient attribute predicates, revocation, credential updates, and other lifecycle functions with the underlying lattice-based proofs.
- **Hash-Based Supporting Components:** Hash-based signature schemes, such as XMSS and the standardized SLH-DSA, provide post-quantum digital authentication based primarily on the security of cryptographic hash functions [94,95]. They may be used to authenticate issuers, trust-registry updates, revocation data, or other credential-management messages. However, ordinary hash-based signatures do not directly provide selective disclosure, unlinkable presentation, or zero-knowledge proofs over hidden certified attributes. They should therefore be regarded as supporting components rather than complete post-quantum ABC constructions.

5.1.6. Holder Binding and Non-Transferability

Holder binding aims to ensure that only an authorized holder can use a credential or generate a valid presentation. Purely software-based credentials cannot generally prevent collusive transfer if a holder is willing to disclose all credential-related secrets. Practical approaches therefore bind credential use to a holder secret or require the participation of a protected device, physical token, or biometric factor.

Representative technical responses and related design approaches include the following:

- **Cryptographic Secret Binding:** Cryptographic secret binding associates credential use with a holder-controlled secret and requires proof of knowledge of that secret during presentation. The binding value can remain hidden within the proof, thereby avoiding its use as a stable identifier across different presentations. Durak et al. formally studied non-transferability for anonymous tokens, which they characterize as lightweight anonymous credentials, and developed secret-binding protocols that restrict anonymous redemption to the intended holder [96].
- **Device and Token Binding:** Device binding ties credential presentation to a key held by a secure element, smart card, or other protected component, so that a valid presentation requires a fresh contribution from that component. Friedrichs et al. formalized device-bound anonymous credentials and constructed device-binding mechanisms for BBS credentials under different secure-element trust assumptions [97]. Hesse et al. combined privacy-preserving digital credentials with the mandatory participation of a physical identity card, enabling a verifier to confirm that the presenter is the rightful credential holder while preserving the privacy of unrelated attributes [98]. Liu et al. proposed an ABC construction with verifiable human binding that uses a constant-size two-party proof-of-knowledge protocol and signatures with randomizable keys to reduce presentation communication while supporting credential revocation [99].
- **Biometric Binding:** Biometric binding requires a fresh biometric measurement to participate in credential use, thereby making successful presentation dependent on a physical characteristic of the enrolled holder. Blanton and Hudelson integrated fuzzy-extractor-based biometric keys with anonymous credentials to limit both unauthorized use and voluntary credential sharing [100]. More recent biometric ABC architectures combine protected credential storage, local biometric processing, and privacy-preserving presentation mechanisms [101].

5.2. Future Research Directions

The preceding analysis suggests that several technical gaps are particularly important for the wider practical adoption of ABC systems. Four research priorities stand out: interoperability across heterogeneous credential infrastructures, privacy-preserving lifecycle management, efficient and reproducible deployment, and privacy-preserving holder binding with recovery. These gaps directly affect whether ABC systems can operate across organizational boundaries, maintain valid credential state over time, satisfy practical performance requirements, and support real users without weakening their privacy guarantees.

- **Interoperability and Standardization:** A major barrier to wider deployment is the lack of interoperable credential formats, attribute semantics, proof suites, status mechanisms, and trust-management interfaces across ABC systems. This fragmentation limits credential portability and often requires application-specific integration among issuers, holders, and verifiers. Research should therefore prioritize interoperable interfaces, common representations for credential and status information, and proof-suite negotiation mechanisms that preserve assurance information without introducing stable identifiers or cross-domain linkability.

- **Privacy-Preserving Credential Lifecycle Management:** Another critical gap is the lack of broadly deployable mechanisms for updating, revoking, renewing, delegating, and synchronizing credentials without weakening unlinkability or exposing unnecessary status information. Practical systems must maintain fresh credential state across issuers, holders, verifiers, derived credentials, and multi-authority settings while preventing rollback to obsolete states. Efficient state synchronization, privacy-preserving revocation, and secure propagation of lifecycle changes therefore remain key prerequisites for long-term ABC deployment.
- **Efficient and Reproducible Deployment:** Practical adoption is also limited by uncertain implementation costs and the lack of directly comparable evaluations across representative ABC systems. Prover computation, memory consumption, proof size, verifier cost, and operational overhead depend strongly on the credential construction, proof system, supported functionality, hardware platform, and workload. Future work should combine lightweight implementation techniques with reproducible benchmarks and realistic pilot deployments so that researchers and system designers can evaluate performance and deployment trade-offs under clearly specified and, where possible, comparable conditions.
- **Privacy-Preserving Holder Binding, Recovery, and Multi-Device Use:** Wider deployment requires mechanisms that discourage unauthorized credential sharing while also supporting device loss, recovery, migration, accessibility, and legitimate multi-device use. Existing approaches face a difficult trade-off between weak non-transferability and stronger forms of binding that may introduce stable identifiers, device-specific state, or additional interactions that undermine unlinkability. Future research should integrate privacy-preserving holder binding with recovery and device-management mechanisms while minimizing persistent identifiers and cross-context correlation.

Beyond these immediate deployment priorities, post-quantum migration remains an important longer-term research direction. Future ABC systems should support cryptographic agility and quantum-resistant constructions while preserving selective disclosure, predicate proofs, unlinkability, revocation, lifecycle functionality, and practical efficiency. Migration mechanisms are particularly important because deployed identity infrastructures may need to support classical and post-quantum credential technologies simultaneously during extended transition periods.

6. Conclusions

This paper provides a review of attribute-based credentials, covering their system model, security and privacy properties, classification, comparative analysis, and practical deployment challenges. It develops a two-dimensional taxonomy that classifies ABCs along the construction and extension dimensions, thereby providing a unified framework for organizing and comparing ABC categories.

The review shows that existing ABC approaches exhibit different trade-offs among privacy, efficiency, trust assumptions, verification models, lifecycle support, and deployment complexity. Practical adoption therefore depends not only on the security of the underlying credential primitive but also on system-level capabilities such as efficient implementation, privacy-preserving credential lifecycle management, interoperability, holder binding, and post-quantum migration.

Overall, future ABC research should move toward deployable credential ecosystems that jointly address security, privacy, interoperability, lifecycle management, usability, and post-quantum readiness. Continued progress in these areas will strengthen the role of ABCs as cryptographic foundations for secure, trustworthy, and sustainable digital identity infrastructures.

Author Contributions: Conceptualization, J.L.; methodology, J.L.; investigation, L.W. and G.S.; formal analysis, Y.Z.; writing—original draft preparation, J.L.; writing—review and editing, Y.L. and Y.Z.; visualization, G.S. and C.D.; supervision, L.W.; project administration, J.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by the National Natural Science Foundation of China under Grant L2324126 and the Undergraduate Innovation and Entrepreneurship Program (No. XJDC202610300626).

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: Yanyu Zhang is employed by Shandong Sacred Sun Power Sources Co., Ltd., and Chen Du is employed by Jinan Huanghe Road and Bridge Construction Group Co., Ltd. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

References

1. Sedlmeir, J.; Smethurst, R.; Rieger, A.; Fridgen, G. Digital identities and verifiable credentials. *Bus. Inf. Syst. Eng.* **2021**, *63*, 603–613. [CrossRef]
2. European Parliament and Council of the European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). *Off. J. Eur. Union* **2016**, *L 119*, 1–88.
3. W3C Verifiable Credentials Working Group. *Verifiable Credentials Data Model v2.0*; W3C Recommendation REC-vc-data-model-2.0-20250515; World Wide Web Consortium: Wakefield, MA, USA, 2025.
4. Kakvi, S.A.; Martin, K.M.; Putman, C.; Quaglia, E.A. SoK: Anonymous Credentials. In *Proceedings of the Security Standardisation Research; Lecture Notes in Computer Science*; Springer: Cham, Switzerland, 2023; Volume 13895, pp. 129–151. [CrossRef]
5. Tan, H.; Fang, C.; Shen, J.; Bhuiyan, Z.A.; Wu, Q.J. Cross-Domain Heterogeneous Data Aggregation with Dynamic Group Key Agreement for Hybrid Satellite Networks. *IEEE Trans. Dependable Secur. Comput.* **2025**, *23*, 4830–4844. [CrossRef]
6. Sen, M.A.; Al-Rubaye, S.; Tsourdos, A. Securing uav flying ad hoc wireless networks: Authentication development for robust communications. *Sensors* **2025**, *25*, 1194. [CrossRef] [PubMed]
7. Camenisch, J.; Lysyanskaya, A. Signature schemes and anonymous credentials from bilinear maps. In *Proceedings of the Annual International Cryptology Conference*; Springer: Berlin/Heidelberg, Germany, 2004; pp. 56–72. [CrossRef]
8. Chaum, D. Security without Identification: Transaction Systems to Make Big Brother Obsolete. *Commun. ACM* **1985**, *28*, 1030–1044. [CrossRef]
9. Brickell, E.; Camenisch, J.; Chen, L. Direct Anonymous Attestation. In *Proceedings of the 11th ACM Conference on Computer and Communications Security*; Association for Computing Machinery: New York, NY, USA, 2004; pp. 132–145. [CrossRef]
10. 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*; Association for Computing Machinery: New York, NY, USA, 2002; pp. 21–30.
11. Paquin, C.; Zaverucha, G. *U-Prove Cryptographic Specification V1.1 (Revision 5)*; Technical Report; Microsoft Corporation: Redmond, WA, USA, 2023. Available online: <https://www.microsoft.com/en-us/research/project/u-prove/> (accessed on 16 July 2026).
12. Sene, I.; Ciss, A.A.; Niang, O. I2PA, U-Prove, and Idemix: An Evaluation of Memory Usage and Computing Time Efficiency in an IoT Context. In *Proceedings of the International Conference on e-Infrastructure and e-Services for Developing Countries*; Springer: Cham, Switzerland, 2019; pp. 140–153. [CrossRef]
13. 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*; Springer: Cham, Switzerland, 2023; pp. 384–417. [CrossRef]
14. Hanzlik, L.; Slamanig, D. With a Little Help From My Friends: Constructing Practical Anonymous Credentials. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*; Association for Computing Machinery: New York, NY, USA, 2021; pp. 2004–2023. [CrossRef]
15. Héban, C.; Pointcheval, D. Traceable constant-size multi-authority credentials. *Inf. Comput.* **2023**, *293*, 105060. [CrossRef]
16. Crites, E.C.; Lysyanskaya, A. Delegatable Anonymous Credentials from Mercurial Signatures. In *Proceedings of the Cryptographers' Track at the RSA Conference*; Springer: Cham, Switzerland, 2019; pp. 535–555. [CrossRef]

17. 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*; Association for Computing Machinery: New York, NY, USA, 2019; pp. 1671–1685. [\[CrossRef\]](#)
18. Sanders, O. Efficient Redactable Signature and Application to Anonymous Credentials. In *Proceedings of the IACR International Conference on Public-Key Cryptography*; Springer: Cham, Switzerland, 2020; pp. 628–656. [\[CrossRef\]](#)
19. Mühle, A.; Grüner, A.; Gayvoronskaya, T.; Meinel, C. A survey on essential components of a self-sovereign identity. *Comput. Sci. Rev.* **2018**, *30*, 80–86. [\[CrossRef\]](#)
20. Schardong, F.; Custódio, R. Self-sovereign identity: A systematic review, mapping and taxonomy. *Sensors* **2022**, *22*, 5641. [\[CrossRef\]](#) [\[PubMed\]](#)
21. Soltani, R.; Nguyen, U.T.; An, A. A Survey of Self-Sovereign Identity Ecosystem. *Secur. Commun. Netw.* **2021**, *2021*, 8873429. [\[CrossRef\]](#)
22. Mazzocca, C.; Acar, A.; Uluagac, S.; Montanari, R.; Bellavista, P.; Conti, M. A survey on decentralized identifiers and verifiable credentials. *IEEE Commun. Surv. Tutor.* **2025**, *27*, 3641–3671. [\[CrossRef\]](#)
23. W3C Decentralized Identifier Working Group. *Decentralized Identifiers (DIDs) v1.0: Core Architecture, Data Model, and Representations*; W3c Recommendation; World Wide Web Consortium: Cambridge, MA, USA, 2022.
24. Fathalla, E.; Azab, M.; Xin, C.; Wu, H. Self-Sovereign Identity as a Secure and Trustworthy Approach to Digital Identity Management: A Comprehensive Survey. *ACM Comput. Surv.* **2025**, *58*, 190. [\[CrossRef\]](#)
25. Chaturangi, M.; Li, Q.; Foo, E. On Advances of Anonymous Credentials—From Traditional to Post-Quantum. *Cryptography* **2025**, *9*, 8. [\[CrossRef\]](#)
26. Camenisch, J.; Dubovitskaya, M.; Lehmann, A.; Neven, G.; Paquin, C.; Preiss, F.S. Concepts and languages for privacy-preserving attribute-based authentication. In *Proceedings of the IFIP Working Conference on Policies and Research in Identity Management*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 34–52.
27. Sonnino, A.; Al-Bassam, M.; Bano, S.; Meiklejohn, S.; Danezis, G. Coconut: Threshold issuance selective disclosure credentials with applications to distributed ledgers. *arXiv* **2018**, arXiv:1802.07344.
28. Graebnitz, C.; Buchmann, N.; Seiffert, M.; Margraf, M. A Specification of an Anonymous Credential System Using BBS+ Signatures with Privacy-Preserving Revocation and Device Binding. *Cryptol. ePrint Arch.* **2025**. Available online: <https://eprint.iacr.org/2025/824> (accessed on 23 August 2026).
29. 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, CCS '14*; Association for Computing Machinery: New York, NY, USA, 2014; pp. 1205–1216. [\[CrossRef\]](#)
30. Couteau, G.; Reichle, M. Non-interactive keyed-verification anonymous credentials. In *Proceedings of the IACR International Workshop on Public Key Cryptography*; Springer: Cham, Switzerland, 2019; pp. 66–96.
31. Schanzenbach, M.; Kilian, T.; Schütte, J.; Banse, C. ZKclaims: Privacy-preserving attribute-based credentials using non-interactive zero-knowledge techniques. *arXiv* **2019**, arXiv:1907.09579.
32. 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)*; IEEE: Piscataway, NJ, USA, 2023; pp. 790–808.
33. Camenisch, J.; Lysyanskaya, A. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 2001; pp. 93–118.
34. Au, M.H.; Susilo, W.; Mu, Y. Constant-size dynamic k-TAA. In *Proceedings of the International Conference on Security and Cryptography for Networks*; Springer: Berlin/Heidelberg, Germany, 2006; pp. 111–125.
35. Boneh, D.; Boyen, X.; Shacham, H. Short group signatures. In *Proceedings of the Annual International Cryptology Conference*; Springer: Berlin/Heidelberg, Germany, 2004; pp. 41–55.
36. Doerner, J.; Kondi, Y.; Lee, E.; Shelat, A.; Tyner, L. Threshold BBS+ signatures for distributed anonymous credential issuance. In *Proceedings of the 2023 IEEE Symposium on Security and Privacy (SP)*; IEEE: Piscataway, NJ, USA, 2023; pp. 773–789.
37. Pointcheval, D.; Sanders, O. Short randomizable signatures. In *Proceedings of the Cryptographers' Track at the RSA Conference*; Springer: Cham, Switzerland, 2016; pp. 111–126.
38. Sanders, O.; Traoré, J. Compact issuer-hiding authentication, application to anonymous credential. In *Proceedings on Privacy Enhancing Technologies*; PETS: Rochester, NY, USA, 2024.
39. Hanser, C.; Slamanig, D. Structure-preserving signatures on equivalence classes and their application to anonymous credentials. In *Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security*; Springer: Berlin/Heidelberg, Germany, 2014; pp. 491–511.
40. Fuchsbauer, G.; Hanser, C.; Slamanig, D. Structure-preserving signatures on equivalence classes and constant-size anonymous credentials. *J. Cryptol.* **2019**, *32*, 498–546. [\[CrossRef\]](#)

41. 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*; Springer: Cham, Switzerland, 2022; pp. 409–438. [\[CrossRef\]](#)
42. Mostowski, W.; Vullers, P. Efficient U-Prove implementation for anonymous credentials on smart cards. In *Proceedings of the International Conference on Security and Privacy in Communication Systems*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 243–260.
43. de Fuentes, J.M.; González-Manzano, L.; Serna-Olvera, J.; Veseli, F. Assessment of attribute-based credentials for privacy-preserving road traffic services in smart cities. *Pers. Ubiquitous Comput.* **2017**, *21*, 869–891. [\[CrossRef\]](#)
44. Mir, O.; Bauer, B.; Griffy, S.; Lysyanskaya, A.; Slamanig, D. Aggregate Signatures with Versatile Randomization and Issuer-Hiding Multi-Authority Anonymous Credentials. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*; Association for Computing Machinery: New York, NY, USA, 2023; pp. 30–44. [\[CrossRef\]](#)
45. Shi, R.; Feng, H.; Yang, Y.; Yuan, F.; Li, Y.; Pang, H.H.; Deng, R.H. Threshold Attribute-Based Credentials with Redactable Signature. *IEEE Trans. Serv. Comput.* **2023**, *16*, 3751–3765. [\[CrossRef\]](#)
46. Mir, O.; Slamanig, D.; Bauer, B.; Mayrhofer, R. Practical delegatable anonymous credentials from equivalence class signatures. In *Proceedings on Privacy Enhancing Technologies*; PETS: Rochester, NY, USA, 2023.
47. Barki, A.; Brunet, S.; Desmoulins, N.; Traoré, J. Improved algebraic MACs and practical keyed-verification anonymous credentials. In *Proceedings of the International Conference on Selected Areas in Cryptography*; Springer: Cham, Switzerland, 2016; pp. 360–380.
48. Mirzamohammadi, O.; Bobolz, J.; Sedaghat, M.; Heydari Beni, E.; Abidin, A.; Singelee, D.; Preneel, B. Keyed-verification anonymous credentials with highly efficient partial disclosure. *IACR Commun. Cryptol. (CiC)* **2025**, *2*, 1–50. [\[CrossRef\]](#)
49. Chase, M.; Perrin, T.; Zaverucha, G. The Signal Private Group System and Anonymous Credentials Supporting Efficient Verifiable Encryption. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*; Association for Computing Machinery: New York, NY, USA, 2020; pp. 1445–1459. [\[CrossRef\]](#)
50. Bobolz, J.; Beni, E.H.; Lehmann, A.; Mirzamohammadi, O.; Özbay, C.; Sedaghat, M. Multi-Verifier Keyed-Verification Anonymous Credentials. *Cryptol. ePrint Arch.* **2025**. Available online: <https://eprint.iacr.org/2025/2156> (accessed on 23 August 2026). [\[CrossRef\]](#)
51. Bosk, D.; Frey, D.; Gestin, M.; Piolle, G. Hidden issuer anonymous credential. *Proc. Priv. Enhancing Technol.* **2022**, *2022*, 571–607. [\[CrossRef\]](#)
52. Xie, T.; Gai, K.; Yu, J.; Zhu, L.; Xiao, B. Slvc-dida: Signature-less verifiable credential-based issuer-hiding and multi-party authentication for decentralized identity. *arXiv* **2025**, arXiv:2501.11052.
53. Bobolz, J.; Eidens, F.; Krenn, S.; Ramacher, S.; Samelin, K. Issuer-hiding attribute-based credentials. In *Proceedings of the International Conference on Cryptology and Network Security*; Springer: Cham, Switzerland, 2021; pp. 158–178. [\[CrossRef\]](#)
54. Shi, R.; Feng, H.; Yang, Y.; Li, Y.; Li, X.; Deng, R.H. Hecate: Threshold Anonymous Credentials with Private Verifiers and Issuer-Hiding. *IEEE Trans. Dependable Secur. Comput.* **2025**, *23*, 1160–1172. [\[CrossRef\]](#)
55. Shi, R.; Yang, Y.; Li, Y.; Feng, H.; Shi, G.; Pang, H.H.; Deng, R.H. Double issuer-hiding attribute-based credentials from tag-based aggregatable mercurial signatures. *IEEE Trans. Dependable Secur. Comput.* **2023**, *21*, 2585–2602. [\[CrossRef\]](#)
56. Shahandashti, S.F.; Safavi-Naini, R. Threshold attribute-based signatures and their application to anonymous credential systems. In *Proceedings of the International Conference on Cryptology in Africa*; Springer: Berlin/Heidelberg, Germany, 2009; pp. 198–216. [\[CrossRef\]](#)
57. Zhang, X.; Zhou, J.; Cao, Z.; Dong, X.; Ning, J. Weighted Threshold Anonymous Credentials with Redactable Fine-Grained Blind Signature for Auditable Lending System in Blockchains. *IEEE Trans. Dependable Secur. Comput.* **2025**, *23*, 3738–3752. [\[CrossRef\]](#)
58. Jia, M.; Chen, J.; He, K.; Shi, M.; Wang, Y.; Du, R. Generic Construction of Threshold Credential Management with User-Autonomy Aggregation. *IEEE Trans. Inf. Forensics Secur.* **2023**, *19*, 2549–2564. [\[CrossRef\]](#)
59. Bisht, K.; Kansagra, N.Y.; Ali, R.; Shaik, M.S.; Francis, M.; Kataoka, K. Revocable TACO: Revocable threshold based anonymous credentials over blockchains. In *Proceedings of the 19th ACM Asia Conference on Computer and Communications Security*; Association for Computing Machinery: New York, NY, USA, 2024; pp. 1378–1393.
60. Naaz, A.; Kumar, B.T.V.P.; Francis, M.; Kataoka, K. Integrating Threshold Opening with Threshold Issuance of Anonymous Credentials Over Blockchains for a Multi-Certifier Communication Model. *IEEE Access* **2022**, *10*, 128697–128720. [\[CrossRef\]](#)
61. Xie, S.; Shi, R.; Yang, Y.; Xie, H.; Li, Y.; Deng, R.H. AccCred: Improved accountable anonymous credentials with dynamic triple-hiding committees. *IEEE Trans. Dependable Secur. Comput.* **2024**, *22*, 1961–1975. [\[CrossRef\]](#)
62. Jia, M.; Chen, J.; Wang, Y.; He, K.; Shi, M.; Du, R. Multi-authority Anonymous Credentials with Efficient and Decentralized Supervision. *IEEE Trans. Inf. Forensics Secur.* **2025**, *20*, 8154–8166. [\[CrossRef\]](#)
63. Derler, D.; Hanser, C.; Slamanig, D. A new approach to efficient revocable attribute-based anonymous credentials. In *Proceedings of the IMA International Conference on Cryptography and Coding*; Springer: Cham, Switzerland, 2015; pp. 57–74.
64. Liu, Y.; He, D.; Feng, Q.; Luo, M.; Choo, K.K.R. PERCE: A permissioned redactable credentials scheme for a period of membership. *IEEE Trans. Inf. Forensics Secur.* **2023**, *18*, 3132–3142. [\[CrossRef\]](#)

65. Yang, Y.; Xue, W.; Zhan, Y.; Huang, M.; Li, Y.; Deng, R.H. AnoPay: Anonymous payment for vehicle parking with updatable credential. *IEEE Trans. Dependable Secur. Comput.* **2023**, *21*, 1621–1638. [\[CrossRef\]](#)
66. Sawai, Y.; Hatsugai, K.; Asano, K.; Watanabe, Y.; Iwamoto, M. Attribute-based Anonymous Credentials with Update Broadcast. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **2026**, *E109.A*, 1272–1298. [\[CrossRef\]](#)
67. Xie, M.; Ju, P.; Zhao, Y.; Jiang, Z.L.; Au, M.H.; Fang, J.; Yu, Y.; Wang, X. FDAAC-CR: Practical delegatable attribute-based anonymous credentials with fine-grained delegation management and chainable revocation. *IEEE Trans. Inf. Forensics Secur.* **2025**, *20*, 7572–7587. [\[CrossRef\]](#)
68. 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. [\[CrossRef\]](#)
69. Li, C.; Ning, J.; Liu, X.; Liu, Y. Differential Trust: Dynamic Multi-Authority Anonymous Credentials with Epoch-Weighted Updates. In *Proceedings of the 35th USENIX Security Symposium (USENIX Security 26)*; USENIX Association: San Francisco, CA, USA, 2026.
70. Hatsugai, K.; Asano, K.; Sawai, Y.; Watanabe, Y.; Iwamoto, M. Anonymous Credentials with Credential Redaction and Its Application to SSI-Based Plug&Charge for Shared Vehicles. In *Proceedings of the Australasian Conference on Information Security and Privacy*; Springer: Singapore, 2025; pp. 42–62.
71. Blömer, J.; Bobolz, J. Delegatable attribute-based anonymous credentials from dynamically malleable signatures. In *Proceedings of the International Conference on Applied Cryptography and Network Security*; Springer: Cham, Switzerland, 2018; pp. 221–239.
72. Mir, O.; Slamanig, D.; Mayrhofer, R. Threshold delegatable anonymous credentials with controlled and fine-grained delegation. *IEEE Trans. Dependable Secur. Comput.* **2023**, *21*, 2312–2326. [\[CrossRef\]](#)
73. Griffy, S.; Lysyanskaya, A.; Mir, O.; Perez Kempner, O.; Slamanig, D. Delegatable anonymous credentials from mercurial signatures with stronger privacy. In *Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security*; Springer: Singapore, 2024; pp. 296–325.
74. Bootle, J.; Groth, J. Efficient batch zero-knowledge arguments for low degree polynomials. In *Proceedings of the IACR International Workshop on Public Key Cryptography*; Springer: Cham, Switzerland, 2018; pp. 561–588. [\[CrossRef\]](#)
75. Bünz, B.; Bootle, J.; Boneh, D.; Poelstra, A.; Wuille, P.; Maxwell, G. Bulletproofs: Short proofs for confidential transactions and more. In *Proceedings of the 2018 IEEE Symposium on Security and Privacy (SP)*; IEEE: Piscataway, NJ, USA, 2018; pp. 315–334. [\[CrossRef\]](#)
76. Ding, K.; Xie, T.; Gai, K.; Yu, J.; Guo, C.; Fang, Z.; Zhu, L.; Meng, W. Verifiable Aggregation for Heterogeneous Decentralized Identity in Internet of Things. *IEEE Internet Things J.* **2025**, *12*, 49565–49576. [\[CrossRef\]](#)
77. Ali, M.; Sadeghi, M.R.; Liu, X. Lightweight revocable hierarchical attribute-based encryption for internet of things. *IEEE Access* **2020**, *8*, 23951–23964. [\[CrossRef\]](#)
78. He, H.; Zheng, L.h.; Li, P.; Deng, L.; Huang, L.; Chen, X. An efficient attribute-based hierarchical data access control scheme in cloud computing. *Hum.-Centric Comput. Inf. Sci.* **2020**, *10*, 49. [\[CrossRef\]](#)
79. Li, J.; Yu, Q.; Zhang, Y. Hierarchical attribute based encryption with continuous leakage-resilience. *Inf. Sci.* **2019**, *484*, 113–134. [\[CrossRef\]](#)
80. He, Q.; Zhang, N.; Wei, Y.; Zhang, Y. Lightweight attribute based encryption scheme for mobile cloud assisted cyber-physical systems. *Comput. Netw.* **2018**, *140*, 163–173. [\[CrossRef\]](#)
81. Gong, B.; Guo, C.; Guo, C.; Sun, Y.; Waqas, M.; Chen, S. SLIM: A secure and lightweight multi-authority attribute-based signcryption scheme for IoT. *IEEE Trans. Inf. Forensics Secur.* **2023**, *19*, 1299–1312. [\[CrossRef\]](#)
82. Jaques, S.; Montgomery, H.; Lodder, M. ALLOSAUR: Accumulator with low-latency oblivious sublinear anonymous credential updates with revocations. In *Proceedings of the 19th ACM Asia Conference on Computer and Communications Security*; Association for Computing Machinery: New York, NY, USA, 2024; pp. 1708–1723.
83. Edalatnejad, K.; Faust, S.; Hofmann, J.; Lehwald, P.F.; Schneider, T. Do You Need a Receipt? Anonymous Credential Revocation at Continental Scale via Private Record Certification. *Cryptol. ePrint Arch.* **2026**. Available online: <https://eprint.iacr.org/2026/1189> (accessed on 23 August 2026).
84. Li, P.; Lai, J.; Yang, Y.; Sun, M.; Wu, C.; Wu, W.; Yuan, X. Attribute-based anonymous credential: Delegation, traceability, and revocation. *Comput. Netw.* **2023**, *237*, 110086. [\[CrossRef\]](#)
85. Sun, M.; Lai, J.; Wu, W.; Yang, Y.; Chu, C.K.; Deng, R.H. How to securely delegate and revoke partial authorization credentials. *IEEE Trans. Dependable Secur. Comput.* **2024**, *22*, 979–996. [\[CrossRef\]](#)
86. Ardagna, C.A.; di Vimercati, S.D.C.; Foresti, S.; Paraboschi, S.; Samarati, P. Minimizing disclosure of private information in credential-based interactions: A graph-based approach. In *Proceedings of the 2010 IEEE Second International Conference on Social Computing*; IEEE: Piscataway, NJ, USA, 2010; pp. 743–750.
87. Li, T.; Li, N.; Zhang, J.; Molloy, I. Slicing: A new approach for privacy preserving data publishing. *IEEE Trans. Knowl. Data Eng.* **2010**, *24*, 561–574. [\[CrossRef\]](#)

88. Paci, F.; Bauer, D.; Bertino, E.; Blough, D.M.; Squicciarini, A. Minimal credential disclosure in trust negotiations. In *Proceedings of the 4th ACM Workshop on Digital Identity Management*; Association for Computing Machinery: New York, NY, USA, 2008; pp. 89–96.
89. Crowder, R.; Price, G.; Groß, T. Simply tell me how—On Trustworthiness and Technology Acceptance of Attribute-Based Credentials. *arXiv* **2023** arXiv:2308.06555. [[CrossRef](#)]
90. Sabouri, A.; Krontiris, I.; Rannenber, K. Attribute-based credentials for trust (abc4trust). In *Proceedings of the International Conference on Trust, Privacy and Security in Digital Business*; Springer: Berlin/Heidelberg, Germany, 2012; pp. 218–219. [[CrossRef](#)]
91. Yamamoto, D.; Suga, Y.; Sako, K. Formalising linked-data based verifiable credentials for selective disclosure. In *Proceedings of the 2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*; IEEE: Piscataway, NJ, USA, 2022; pp. 52–65.
92. Shor, P.W. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*; IEEE: Piscataway, NJ, USA, 1994; pp. 124–134.
93. Jeudy, C.; Roux-Langlois, A.; Sanders, O. Lattice signature with efficient protocols, application to anonymous credentials. In *Proceedings of the Annual International Cryptology Conference*; Springer: Cham, Switzerland, 2023; pp. 351–383.
94. Buchmann, J.; Dahmen, E.; Hülsing, A. XMSS—a practical forward secure signature scheme based on minimal security assumptions. In *Proceedings of the International Workshop on Post-Quantum Cryptography*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 117–129.
95. National Institute of Standards and Technology. *Stateless Hash-Based Digital Signature Standard*; Technical Report NIST Federal Information Processing Standards Publications (FIPS) 205; U.S. Department of Commerce: Washington, DC, USA, 2024. [[CrossRef](#)]
96. Durak, F.B.; Marco, L.; Talayhan, A.; Vaudenay, S. Non-transferable anonymous tokens by secret binding. In *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security*; Association for Computing Machinery: New York, NY, USA, 2024; pp. 2460–2474.
97. Friedrichs, K.; Harding, F.; Lehmann, A.; Lysyanskaya, A. Device-bound anonymous credentials with (out) trusted hardware. In *Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques*; Springer: Cham, Switzerland, 2026; pp. 345–375.
98. Hesse, J.; Singh, N.; Sorniotti, A. How to bind anonymous credentials to humans. In *Proceedings of the 32nd USENIX Security Symposium (USENIX Security 23)*; USENIX Association: San Francisco, CA, USA, 2023; pp. 3047–3064.
99. Liu, Y.; He, D.; Ning, J.; Bao, Z.; Peng, C. Attribute-Based Credentials with Verifiable Human Binding: Towards Compactness and Revocability. *IEEE Trans. Dependable Secur. Comput.* **2026**, *23*, 5672–5686. [[CrossRef](#)]
100. Blanton, M.; Hudelson, W.M. Biometric-based non-transferable anonymous credentials. In *Proceedings of the International Conference on Information and Communications Security*; Springer: Berlin/Heidelberg, Germany, 2009; pp. 165–180.
101. Sarier, N.D. Best of two worlds: Efficient, usable and auditable biometric ABC on the blockchain. *Comput. Stand. Interfaces* **2025**, *92*, 103916. [[CrossRef](#)]

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.