Overview of Post-Quantum Attribute-Based Credential Schemes

Adéla Felcmanová[1], Calvin Pärn[2], Pavel Loutocký[3], and Jan Hajný[4]

[1] Brno University of Technology, Czech Republic
216941@vutbr.cz
[2] Cybernetica, Estonia
calvin.parn@cyber.ee
[3] Masaryk University, Czech Republic
loutocky@muni.cz
[4] Brno University of Technology, Czech Republic
hajny@vut.cz

Abstract. The imminent transition to post-quantum cryptography poses particular challenges to complex privacy-preserving systems whose security relies on more than standard cryptographic primitives. Attribute-Based Credential (ABC) systems, which enable users to prove possession of attributes without revealing their identity, fall into this category as they employ more advanced cryptographic tools such as zero-knowledge proofs and non-standard signatures.
This paper presents a systematic comparison of post-quantum attribute-based credential schemes. We analyze eight prominent proposals based on lattice cryptography, examining their underlying hardness assumptions, cryptographic building blocks, design choices, and claimed properties, as well as practical aspects including proof sizes and the availability of public implementation. A central contribution of this work is a comprehensive comparison table that brings these aspects together in a single structured view, which enables direct comparison across schemes. By providing a structured comparative overview, this work serves as a practical guide for researchers and practitioners to select a post-quantum ABC system for their specific needs and purposes and to identify weak spots that need further attention.

Keywords: Post-Quantum · Cryptography · Security · Anonymity · Privacy.

1 Introduction

As the transition to post-quantum cryptography is now starting to gain momentum, and the first standards have been released, it is also necessary to find alternatives for more complex systems where quantum resilience cannot be achieved by simply replacing the underlying primitives. Identity management systems are a prominent example of this challenge. The increase in reliance on identity

management has led to users disclosing more personal information than necessary, often revealing their identity even when only specific attributes are needed, which raises significant privacy and security concerns.

This is also important from a legal standpoint, as legislation in general (and particularly GDPR[5]) establishes principles related to the minimization and processing of personal data. Crucially, the eIDAS Regulation[6] enshrines this approach to authentication based on attributes (resp. electronic attestation of attributes), which will be discussed in more detail below.

Attribute-Based Credentials (ABCs) address this issue by enabling users to prove specific attributes without revealing their full identity. Related approaches, such as Attribute-Based Signatures, which require the user's attributes to fulfill some relation in order to form a valid signature, pursue similar goals. This paper focuses exclusively on ABCs and their post-quantum variants.

We give an overview of the currently available post-quantum ABC schemes. At present, the number of available constructions remains limited. Only a handful of schemes have been proposed, and even fewer have been implemented. Despite this, the existing works already exhibit notable differences in design choices, focusing on different practical uses. The presented schemes are invariably based on lattice assumptions, as many of the lattice-based primitives have reached a state of maturity in the literature.

Before presenting the overview, we provide a brief background on lattices and the relevant hardness assumptions. We then discuss the schemes one by one, highlighting the key differences in their design. The results are summarized in a comparison table, which provides a structured and concise reference for practitioners and researchers. By bringing together and structuring the currently limited body of work, this overview enables clearer comparisons between schemes and provides a concise view of the current state of post-quantum ABC research. Based on this structured analysis, we also recommend what we consider to be the most practical scheme out of the candidates.

2 Theoretical background

We provide a brief overview of the necessary background on lattices and the underlying hardness assumptions. This section is not intended to be detailed. For a more comprehensive treatment, we refer the reader to standard references in lattice-based cryptography (e.g., [17], [19]).

[5] 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)

[6] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

2.1 Notation

In the following we denote matrices over fields with uppercase bold letters e.g. $\mathbf{A}$ and vectors with lowercase bold letters e.g. $\mathbf{b}$, which will be column vectors by default. $\mathbf{0}$ denotes the zero vector of a vector space and the notation $\mathbf{e} \leftarrow \chi^n$ represents sampling a column vector of length n, where every coordinate is sampled independently from a distribution χ.

2.2 Lattices

Let $B = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\} \subseteq \mathbb{R}^n$ be a set of linearly independent vectors forming a basis. The n-dimensional full-rank lattice generated by B is defined as

$$\mathcal{L}(B) := \left\{ \sum_{i=1}^{n} a_i \boldsymbol{b}_i \;\middle|\; a_i \in \mathbb{Z} \right\}. \tag{1}$$

Different bases can represent the same lattice, but some bases are considered "good" (for example, those having short and close to orthogonal vectors) and others "bad". We can define the closest vector problem (CVP) and the shortest vector problem (SVP). Given a lattice in $\mathbb{R}^n$ and its "bad" basis, CVP states that it is hard to find the closest lattice point to a given point in $\mathbb{R}^n$, while SVP states that it is hard to find a non-zero vector with the smallest norm in the lattice. If certain variants of these problems are hard in the worst case, then it follows that certain computational problems are hard in the average case. This reduction is one of the main reasons why lattice cryptography has become so popular as a quantum-safe alternative to traditional number-theoretical cryptography.

2.3 Hardness assumptions

Lattice-based cryptography relies on the average-case hardness of the Shortest Integer Solution (SIS) and Learning With Errors (LWE) problems, which reduce to the previously mentioned worst-case problems. The SIS problem is: given a uniformly random matrix $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$, find a nonzero vector $\boldsymbol{s} \in \mathbb{Z}_q^n$ such that $\mathbf{A}\boldsymbol{s} = \mathbf{0}$ and $\boldsymbol{s}$ is short w.r.t. an appropriate norm. The search LWE problem asks one to find a solution to a noisy linear equation system and the distinguish version of it asks one to distinguish an LWE instance from an uniformly random vector. Equivalently, given a matrix $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$ and a vector $\boldsymbol{t} = \mathbf{A}\boldsymbol{s} + \boldsymbol{e}$, where $\boldsymbol{s} \in \mathbb{Z}_q^n$ and $\boldsymbol{e} \leftarrow \chi^n$, it is hard to find $\boldsymbol{s}$ in the search version and hard to distinguish $\boldsymbol{t}$ from an uniformly random vector in $\mathbb{Z}_q^n$ in the distinguish version of LWE.

Module SIS (M-SIS) and Module LWE (M-LWE) can be understood as module analogues of SIS and LWE. Instead of working over $\mathbb{Z}_q$, they work over modules over polynomial rings $\mathcal{R}_q = \mathbb{Z}_q[X]/(X^n + 1)$, where n is a power of two and $(X^n + 1)$ is an ideal generated by a cyclotomic polynomial.

2.4 Security models

Security proofs may be established either in the standard model or in the random oracle model (ROM). In the ROM, hash functions are modeled as ideal random functions, which often enables more efficient constructions and simpler proofs, whereas standard-model proofs avoid idealized assumptions [12].

3 Attribute-Based Credentials

In an ABC scheme, users receive credentials from an issuer on their attributes (e.g., identity, age, name) and later prove possession of these credentials to a verifier, without revealing their identity. Beyond their cryptographic design, such systems may also need to operate within legal frameworks governing the use, disclosure, and verification of identity-related data. In connection with identity management, the legislation establishes electronic attestation of attributes, which means an attestation in electronic form that allows attributes to be authenticated.[7] This approach will be particularly important, among other things, in connection with the use of the European Digital Identity Wallet to provide the necessary data or attributes.[8]

The first model of ABCs was presented by Fuchsbauer et al. in [9]. The authors call a system *multi-show* if the showings of a credential performed by the same user cannot be linked. A credential for a user is issued by an organization for a set of attributes, and the user can then show a subset of their attributes while hiding the rest. An ABC system consists of several Probabilistic Polynomial-Time (PPT) algorithms divided into four phases:

- Key generation for the issuer and user.
- Issuance of a credential for a set of attributes.
- Showing of a credential and a subset of attributes.
- Verification by a verifier.

Usually, a user obtains a signature on (commitments to) attributes, randomizes the signature (to obtain unlinkability to the issued signature), and proves in zero-knowledge that the signature corresponds to the shown attributes as well as to the undisclosed attributes. In the security model for multi-show ABCs [9], the required security properties are:

Correctness A showing of a credential with respect to a non-empty subset of attributes always verifies if the credential was issued honestly for the full attribute set.

Unforgeability A user cannot perform a valid showing of attributes for which they do not possess a credential.

[7] Article 3(44) eIDAS Regulation.

[8] See more e.g.: `https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/881984674/Wallet+for+service+providers`

Anonymity During a showing, no verifier and no (malicious) organization (even if they collude) are able to identify the user or learn anything other than that they own a valid credential for the shown attributes. Furthermore, different showings of the same credential are unlinkable.

Depending on the intended use in practice, the schemes can provide additional properties, such as:

Non-transferability Only the original issuee can provide proofs using the credential.

Updatability After being issued, the attributes in the credentials can be modified.

Revocability The credentials can be revoked if they expire or the user misbehaves.

Untraceability The credentials are randomized; therefore, the issuer will not be able to link them to a user after the issuing phase.

In real-world implementations, these technical applications are linked to legal requirements concerning, in particular, data minimization, accountability, and the conditions under which authorization can be revoked. Particularly in the context of the GDPR, systems are expected to apply principles such as data minimization and purpose limitation, which naturally correspond to mechanisms for selective access. At the same time, features such as traceability or revocation must be carefully designed to ensure compliance with requirements for lawful processing, transparency, and a clear division of responsibility among the parties involved. For this reason, it is prohibited to link or combine personal data in connection with the use of (qualified) attestation of attributes services.[9] Otherwise, the significance and purpose of such a privacy-by-design/default approach would be undermined.

4 Overview of the schemes

In this section, we provide an overview of each of the currently available post-quantum ABC schemes. We first point out their unique contributions and then follow with a comparison based on criteria such as underlying security assumptions, additional properties, implementation, and performance.

4.1 Analysis

Jeudy et al. [11] For the purpose of ABCs, Jeudy et al. [11] aim to optimize the commitement scheme, the signature and the zero-knowledge proof system together. These types of signatures, designed to interact well with other parts of the scheme, are known as *signatures with efficient protocols* (SEPs). For this purpose, the authors propose a new signature scheme as an alternative to the one described in [14] and optimize the zero-knowledge proof system of Yang et al. YAZ+ [20].

[9] Article 45h eIDAS Regulation.

Argo et al. [2] Argo et al. [2] take the same approach as [11] but improve performance by addressing the inefficiency caused by the need to use a large matrix to satisfy the security proof, which almost doubles the signature's dimension. The authors design a new SEP intended to interact smoothly with the zero-knowledge proof of [16]. The authors also implemented their proposal, and their benchmark results report the average time for credential issuance to be under 400 ms and the credential showing time to be around 500 ms.

Chathurangi et al. [8] Chathurangi et al. [8] also build on the work of Jeudy et al. [11] extending the model of [9] by enabling the conditional de-anonymization of users via tracing in case of misbehavior. For this purpose, the authors design a new trapdoor for lattice-based commitments, which allows partial recovery of the commitment randomness.

New entities are introduced: a tracer who extracts identifying information and a judge, a semi-trusted authority that verifies the tracer's computation and authorizes the disclosure of the user's identity. A tracer provided with the private tracing key generates deanonymization data when credential misuse is suspected. This data is then forwarded to the judge, who uses their private key to recover the identity linked to the suspicious credential. This raises the need for another security notion. *Exculpability* ensures that a malicious tracer cannot manipulate the tracing process to allow the judge to attribute a credential to a user who is not the owner of the credential. *Tracing key confidentiality* then ensures that repeated tracings do not leak information about the private tracing key. The added tracing does not affect the functionality of [11] and allows preserving privacy while enabling accountability.

This functionality has an important legal aspect, as any mechanisms that enable the tracking or retroactive identification of users would have to be subject to clearly defined terms of use, appropriate authorization, and effective oversight. Such an approach is fundamentally at odds with the principle of attribute-based credentials, whose primary goal is to minimize the processing of personal data and protect user privacy. The entire concept is based on proving only the necessary attributes without revealing a person's identity. If data were subsequently linked and used in a way that allows for the identification of a specific individual, this would constitute an approach that is largely incompatible with these principles.[10]

Lai et al. [13] Lai et al. [13] combine a commitment scheme and a signature scheme to introduce a new primitive called a commit-transferable signature (CTS). Using CTS, it is possible to compute a signature directly on a committed value so that the user only needs to perform a zero-knowledge proof of knowledge

[10] For further reference see also: Bauer, Gerd and Alamillo, Ignacio, Attestation of Attributes Issued by Public Bodies: A Citizen-Centric Trust Model for the EUDI Wallet (May 30, 2025). Available at SSRN: https://ssrn.com/abstract=5398805 or http://dx.doi.org/10.2139/ssrn.5398805

of the opening. In this way, to prove possession of a signature on the opening, it is sufficient to reveal the signature and the proof of knowledge of the opening rather than the committed value. For this purpose, the authors use the BDLOP [4] commitment scheme.

Furthermore, the user will be able to randomize the commitment and transform the initial signature into a signature with respect to the randomized commitment. This way, the new commitment and the signature will be unlinkable to the original one.

Bootle et al. [6] Bootle et al. [6] introduce a new family of lattice assumptions called ISIS_f (Inhomogeneous SIS with parameter f), which states that given a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, a function $f : \{1, \ldots, N\} \to \mathbb{Z}_q^n$, a random input $x \in \{1, \ldots, N\}$, and a short vector $\boldsymbol{s}$ such that $\mathbf{A}\boldsymbol{s} = f(x)$, it is computationally hard to find a new x' and a corresponding short vector $\boldsymbol{s}'$ satisfying $\mathbf{A}\boldsymbol{s}' = f(x')$. This assumption facilitates more efficient zero-knowledge proofs. An additional advantage is the use of NTRU lattices, which come equipped with a trapdoor. The trapdoor can be used to sample short vectors satisfying $\mathbf{A}\boldsymbol{s} = \boldsymbol{t}$ for any $\boldsymbol{t}$, enabling shorter signatures. The authors then use the ABDLOP [16] commitment scheme, which extends the BDLOP [4] and Ajtai [1] commitment schemes.

Zhaolu et al. [21] Zhaolu et al. [21] address the issue of reliance on a trusted issuer by adding threshold credential issuance. A valid credential proof can be generated only if the user obtains partial credentials from at least t out of N authorities. They also add linkability to tackle the issue of unconditional anonymity and mitigate the risk of credential abuse resulting in potentional financial losses for service providers in the role of credential verifiers. All the credential proofs generated by the same user for the same event are linked and their anonymity can be forcibly revoked to trace the user's identity.

From a broader perspective, this reflects the legal and regulatory tension between personal data protection, the prevention of misuse of data, and enforcement requirements. In particular, selective disclosure is generally consistent with the GDPR principles of data minimization and purpose limitation (if the purpose is set)[11] , whereas further linkability, traceability, or de-anonymization may require a clear legal basis and a transparent definition of purpose and responsibility.[12]

The scheme builds upon the LNP [16] framework for zero-knowledge arguments and uses a variant of the Ajtai [1] commitment scheme.

Camenish et al. [7] Camenish et al. [7] use a group signature scheme (building upon a GPV signature [10]) to form a simplification of an anonymous credential scheme called *anonymous attribute tokens*. Here, the issuer assigns a list of attributes to a user's signing key, and during the verification process, the user

[11] See respectively Article 5 GDPR.
[12] Further assess Articles 6 or 13 GDPR.

selectively reveals some of their attributes in a token to convince the verifier of their valid credential. They provide two schemes; one with revocation (AAT+R) and one without revocation (AAT-R).

In AAT-R, a user is issued a credential containing the attributes chosen by the issuer and can later authenticate anonymously to a verifier using an authentication token. The authentication token is anonymous and reveals only a subset of the attributes from the user's credential.

The AAT+R additionally gives the issuer the ability to reveal the identity of the user who generated a given token. The authors also show how both schemes can be combined to offer revocation while also protecting honest users from being framed by the issuer. That is, no one other than the user themselves can create a token that would be attributed to them when opened.

Blazy et al. [5] Blazy et al. [5] also construct an attribute based credential scheme from a group signature and additionally use a verifiable encryption scheme that allows one to prove certain relations. An issuer first issues a credential for a set of attributes associated with a certain identity. The user can then create a *presentation token*, which is a presentation of a subset of the user's attributes. The authors use a modified version of the verifiable encryption scheme LN presented in [15], the BDLOP commitment scheme from [4], the PLS signature scheme presented in [18] and the ALS zero-knowledge arguments from [3]. The scheme supports traceability, which ensures that all presentation tokens should trace to an issuer or a member of the forging collusion. The scheme also allows a trusted authority (an opener) to reveal the identity associated with a certain presentation token.

The authors provide an implementation of the presentation token generation and verification in C. Following this implementation, they claim the proposed scheme is approximately ten times slower than the previous non post-quantum schemes. For their concrete instantiation, the time averages 1.84 s for generation and 0.17 s for verification,

4.2 Comparison

In Table 1, we summarize the considered schemes with respect to their properties, security, underlying assumptions, building blocks, and reported communication overhead. At present, only a small number of post-quantum ABC schemes have been proposed, and to the best of our knowledge, eight constructions are currently available in the literature. A direct comparison of efficiency across schemes is non-trivial due to differences in terminology and evaluation metrics. In particular, some works report credential size, while others report the size of the showing protocol, i.e., the zero-knowledge proof transmitted to the verifier.

While the essential security property is anonymity against the verifier, most of the schemes achieve full anonymity, which also includes anonymity against the issuer. Similarly, it may be important to consider whether the issuer can see the attributes they are signing, or whether some or all of them are hidden. This property, blind issuance, varies across schemes and is noted in the table.

Table 1. Comparison of Quantum-Safe ABC Schemes (targeting ≈128-bit security).

Name	Jeudy et al.	Argo et al.	Chathurangi et al.	Lai et al.	Bootle et al.	Zhaolu et al.	Blazy et al.	Camenisch et al.
Reference	[11]	[2]	[8]	[13]	[6]	[21]	[5]	[7]
Proved properties	anonymity, unforgeability, correctness	anonymity, unforgeability, correctness	anonymity, unforgeability, exculpability, tracing key confidentiality	anonymity, unforgeability, correctness (sketch)	anonymity, unforgeability, correctness	anonymity, unforgeability, linkability	—	anonymity
Claimed properties	—	—	traceability	unlinkability	unlinkability, selective disclosure	threshold credential issuance	anonymity, unforgeability, traceability	revocation, traceability, unforgeability
Buildable properties	unlinkability, selective disclosure	selective disclosure	unlinkability, revocation	selective disclosure	transferability, revocation	—	—	—
Anonymity	fully anonymous	fully anonymous	fully anonymous (also towards tracer, not judge)	fully anonymous	fully anonymous	fully anonymous	verifier-only	AAT-R fully, AAT+R verifier-only
Blind Issuance	No	No (partial in extended variant)	Yes	Yes	Partial (user choses which are hidden)	No	No	No
Assumptions	M-LWE, M-SIS	M-LWE, M-SIS	M-LWE, M-SIS	M-LWE, M-SIS	ISIS_f, M-LWE, M-SIS, NTRU	M-LWE, M-SIS	M-LWE, M-SIS, Ring-LWE	LWE, SIS
Building blocks	YAZ+ [20]	LNP [16]	YAZ+ [20]	BDLOP [4]	ABDLOP [16]	LNP [16], Ajtai [1]	BDLOP [4]	GPV [10]
Public key size (KB)	724 (10 attributes)	80 (10 attributes)	724 (10 attributes)	440	243 (8 attributes)	9142 (treshold 5, 1 attribute polynomial)	1923	—
Issued object size (KB)	317 (10 attributes)	6.81 (10 attributes)	317 (10 attributes)	236.56	122 (8 attributes)	922.7 (treshold 5, 1 attribute polynomial)	—	—
Proof size (KB)	724 (10 attributes)	80 (10 attributes)	724 (10 attributes)	372.56	243 (8 attributes)	9142 (treshold 5, 1 attribute polynomial)	1923	—
Implementation	No	Yes	No	No	No	No	Yes	No

Almost all of the schemes rely on the M-LWE and M-SIS hardness assumptions. The exception is the work of Bootle et al. [6], which introduces a new assumption that aims to reduce the size of the signatures. Additionally, seven of the eight surveyed schemes use the Fiat-Shamir transform to achieve non-interactivity and are consequently proven in the Random Oracle Model. The exception is the work of Chathurangi et al. [8], whose protocols remain interactive and all their security properties are proven in the standard model.

Notable is the lack of available implementations, which makes it difficult to compare the efficiency of the proposed schemes. Given the lack of metrics, we focus primarily on the proof sizes as the most relevant metric for comparison.

The work of Jeudy et al. [11] establishes the foundation for subsequent constructions such as [2] and [8]. Argo et al. [2] optimized their solution to achieve the smallest proof sizes while relying on standard lattice assumptions. In contrast, Chathurangi et al. [8] extended the work to support traceability.

Lai et al. [13] also achieve competitive proof sizes, while Zhaolu et al. [21] focus on decentralization through threshold issuance and introduce linkability, which enhances practical applicability but results in significantly higher communication overhead.

Camenish et al. [7] and Blazy et al. [5] build ABCs from group signatures rather than blind signatures and show the ownership of certain attributes via a presentation token.

The works of Argo et al. [2] and Blazy et al. [5] are the only constructions that provide efficiency measurements. Argo et al. [2] report credential issuance and showing times of 400 ms and 1840 ms, respectively, whereas Blazy et al. [5] report token generation and verification times of 500 ms and 170 ms, respectively.

Based on the comparative analysis presented above, we consider the scheme by Argo et al. [2] to be the most suitable for practical deployment, as it offers a public implementation and achieves the lowest credential sizes among the surveyed constructions. The main drawback of [2] is its limited set of properties, whose extension could be a focus of future work. In contrast, [6] offers more functionality with comparable credential sizes, but relies on new security assumptions and does not provide a public implementation.

However, other works offer important additional features that may be required in specific applications. In particular, Chathurangi et al. [8] introduce traceability, and Zhaolu et al. [21] provide threshold issuance and linkability, addressing challenges related to decentralization and credential abuse.

4.3 Conclusion

This paper provides an overview and comparison of current post-quantum attribute-based credential schemes, focusing on their security properties, underlying assumptions, and practical efficiency.

Overall, the current state of post-quantum ABCs reflects a trade-off between efficiency, functionality, and reliance on well-established assumptions.

Due to the availability of implementation, smallest proof sizes, and proven security relying on well-established security assumptions, we consider the work by Argo et al. [2] to be the most practically promising.

An important direction for future work is the implementation of the proposed schemes, which would allow for a more reliable comparison of their practical performance. For practical implementation and further development of the approaches discussed from a technical perspective, it is necessary to evaluate them in terms of compliance with efficiency and safety requirements, taking into account the legal and regulatory constraints of the specific use case as indicated above.

Acknowledgments. This work is supported by the European Union under Grant Agreement No. 101087529 CHESS. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

References

1. Ajtai, M.: Generating hard instances of lattice problems (extended abstract). In: Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing. p. 99–108. STOC '96, Association for Computing Machinery, New York, NY, USA (1996). https://doi.org/10.1145/237814.237838, https://doi.org/10.1145/237814.237838
2. Argo, S., Güneysu, T., Jeudy, C., Land, G., Roux-Langlois, A., Sanders, O.: Practical post-quantum signatures for privacy. In: Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security. p. 1523–1537. CCS '24, Association for Computing Machinery, New York, NY, USA (2024). https://doi.org/10.1145/3658644.3670297, https://doi.org/10.1145/3658644.3670297
3. Attema, T., Lyubashevsky, V., Seiler, G.: Practical product proofs for lattice commitments. In: Micciancio, D., Ristenpart, T. (eds.) Advances in Cryptology – CRYPTO 2020. pp. 470–499. Springer International Publishing, Cham (2020), https://doi.org/10.1007/978-3-030-56880-1_17
4. Baum, C., Damgård, I., Lyubashevsky, V., Oechsner, S., Peikert, C.: More efficient commitments from structured lattice assumptions. In: Catalano, D., De Prisco, R. (eds.) Security and Cryptography for Networks. pp. 368–385. Springer International Publishing, Cham (2018), https://doi.org/10.1007/978-3-319-98113-0_20
5. Blazy, O., Chevalier, C., Renaut, G., Ricosset, T., Sageloli, E., Senet, H.: Efficient implementation of a post-quantum anonymous credential protocol. In: Proceedings of the 18th International Conference on Availability, Reliability and Security. ARES '23, Association for Computing Machinery, New York, NY, USA (2023). https://doi.org/10.1145/3600160.3600188, https://doi.org/10.1145/3600160.3600188
6. Bootle, J., Lyubashevsky, V., Nguyen, N.K., Sorniotti, A.: A Framework for Practical Anonymous Credentials from Lattices, pp. 384–417 (08 2023). https://doi.org/10.1007/978-3-031-38545-2_13
7. Camenisch, J., Neven, G., Rückert, M.: Fully anonymous attribute tokens from lattices. In: Visconti, I., De Prisco, R. (eds.) Security and Cryptography for Networks. pp. 57–75. Springer Berlin Heidelberg, Berlin, Heidelberg (2012), https://doi.org/10.1007/978-3-642-32928-9_4
8. Chathurangi, M., Li, Q., Foo, E., Zhang, L.: Post-quantum traceable anonymous credentials from lattices. IACR Communications in Cryptology **2** (01 2026). https://doi.org/10.62056/ak5wl8n4e
9. Fuchsbauer, G., Hanser, C., Slamanig, D.: Structure-preserving signatures on equivalence classes and constant-size anonymous credentials. J. Cryptol. **32**(2), 498–546 (Apr 2019). https://doi.org/10.1007/s00145-018-9281-4, https://doi.org/10.1007/s00145-018-9281-4

10. Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing. p. 197–206. STOC '08, Association for Computing Machinery, New York, NY, USA (2008). https://doi.org/10.1145/1374376.1374407, https://doi.org/10.1145/1374376.1374407
11. Jeudy, C., Roux-Langlois, A., Sanders, O.: Lattice signature with efficient protocols, application to anonymous credentials. In: Advances in Cryptology – CRYPTO 2023: 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20–24, 2023, Proceedings, Part II. p. 351–383. Springer-Verlag, Berlin, Heidelberg (2023). https://doi.org/10.1007/978-3-031-38545-2_12, https://doi.org/10.1007/978-3-031-38545-2_12
12. Katz, J., Lindell, Y.: Introduction to Modern Cryptography, Second Edition. Chapman & Hall/CRC, 2nd edn. (2014)
13. Lai, Q., Chen, C., Liu, F.H., Lysyanskaya, A., Wang, Z.: Lattice-based commit-transferrable signatures and applications to anonymous credentials. Cryptology ePrint Archive, Paper 2023/766 (2023), https://eprint.iacr.org/2023/766
14. Libert, B., Ling, S., Mouhartem, F., Nguyen, K., Wang, H.: Signature schemes with efficient protocols and dynamic group signatures from lattice assumptions. In: Proceedings, Part II, of the 22nd International Conference on Advances in Cryptology — ASIACRYPT 2016 - Volume 10032. p. 373–403. Springer-Verlag, Berlin, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53890-6_13, https://doi.org/10.1007/978-3-662-53890-6_13
15. Lyubashevsky, V., Neven, G.: One-shot verifiable encryption from lattices. In: Coron, J.S., Nielsen, J.B. (eds.) Advances in Cryptology – EUROCRYPT 2017. pp. 293–323. Springer International Publishing, Cham (2017), https://doi.org/10.1007/978-3-319-56620-7_11
16. Lyubashevsky, V., Nguyen, N.K., Plançon, M.: Lattice-based zero-knowledge proofs and applications: Shorter, simpler, and more general. In: Advances in Cryptology – CRYPTO 2022: 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15–18, 2022, Proceedings, Part II. p. 71–101. Springer-Verlag, Berlin, Heidelberg (2022). https://doi.org/10.1007/978-3-031-15979-4_3, https://doi.org/10.1007/978-3-031-15979-4_3
17. Peikert, C.: A decade of lattice cryptography. Found. Trends Theor. Comput. Sci. **10**(4), 283–424 (Mar 2016). https://doi.org/10.1561/0400000074, https://doi.org/10.1561/0400000074
18. del Pino, R., Lyubashevsky, V., Seiler, G.: Lattice-based group signatures and zero-knowledge proofs of automorphism stability. In: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. p. 574–591. CCS '18, Association for Computing Machinery, New York, NY, USA (2018). https://doi.org/10.1145/3243734.3243852, https://doi.org/10.1145/3243734.3243852
19. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. J. ACM **56**(6) (Sep 2009). https://doi.org/10.1145/1568318.1568324, https://doi.org/10.1145/1568318.1568324
20. Yang, R., Au, M.H., Zhang, Z., Xu, Q., Yu, Z., Whyte, W.: Efficient lattice-based zero-knowledge arguments with standard soundness: Construction and applications. In: Advances in Cryptology – CRYPTO 2019: 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18–22, 2019, Proceedings, Part I. p. 147–175. Springer-Verlag, Berlin, Heidelberg

(2019). https://doi.org/10.1007/978-3-030-26948-7_6, https://doi.org/10.1007/978-3-030-26948-7_6

21. Zhaolu, T., Wang, H.: Post-quantum anonymous authentication for web3: a lattice-based decentralized linkable anonymous credential scheme. The Journal of Supercomputing **81** (09 2025). https://doi.org/10.1007/s11227-025-07872-w