TTM4502 – 2026

Student: Aleksander Thornes Vestlund
Main supervisor: Associate Professor Tjerand Aga Silde
Co-supervisor: Professor Srinivas Devadas

Lattice-Based Privacy-Preserving Credentials in the European Digital Identity Wallet

Summary. In this master's thesis, we will explore the transition to lattice-based cryptographic primitives within the European Digital Identity (EUDI) Wallet ecosystem. As current identity standards rely on schemes vulnerable to quantum adversaries, developing and testing post-quantum alternatives is critical for long-term international security. We will investigate how privacy-preserving properties can be efficiently realized using such primitives. Unlike classical cryptography, where these features are well established via, for instance, Boneh–Boyen–Shacham (BBS) signatures, post-quantum constructions face significant trade-offs regarding signature size, computational overhead, and proof complexity. To assess the practical viability of these protocols, we will test the implementations against the EUDI Wallet's high-level requirements and utilize the Norwegian Digitalization Agency's sandbox environment for real-world validation.

1 Introduction

This document is mainly a background study for the thesis, and the background is split into two parts. Section 2 covers the European Digital Identity (EUDI) Wallet and the zero-knowledge proofs (ZKPs) and anonymous credentials (ACs) that can make it more private, while Section 3 covers lattice-based cryptography, the post-quantum (PQ) family we build on.

1.1 Motivation

In late 2025, the Australian government began enforcing a ban on social media for users under the age of 16, causing children to lose access to millions of accounts [AW26]. Less than a year later, the European Union (EU) proposed a similar ban [EC26a]. For the platforms in question, this has posed the non-trivial question of how to verify the age of their users. Some companies have resorted to questionable methods, including those described below.

Facial age estimation. The user's age is estimated from a selfie or a short video of their face. Roblox requires this through Persona before users can chat [KB25], and Meta [META26] and TikTok [TikTok25] offer it through Yoti.

Identity documents. The user uploads a photo of a government ID or scans the chip of their passport. Reddit lets users verify their age this way through Persona [For25], and LinkedIn uses passport chips to verify identities for its verification badge [LinkedIn26].

These methods have their fair share of downsides. From a privacy perspective, the methods listed above give the services more personal information than they require.

Another method is to use digital identity wallets. We focus on the EUDI Wallet, a project started by the EU allowing users to securely disclose personal documents to services that require them. Member States will make it available to every citizen, resident, and business by the end of 2026, and age verification is only one of its many applications [EC26c]. Users will also be able to open bank accounts, make online payments, show a mobile driving license, present diplomas and travel documents, claim prescriptions, and sign contracts with it [EC26b].

Even so, neither the wallet nor ZKPs, which let a user prove a statement without revealing anything else, make age verification unproblematic. In a joint statement, 437 security and privacy researchers warn that age checks are easily bypassed, for instance with bought or borrowed credentials, and that they exclude people without a certified credential, a compatible device, or the digital skills to use them, such as the elderly and, if the checks build on the EUDI Wallet, non-EU citizens [ABH+26, p. 2]. Similarly, Celi, Den Hartog, and Haddadi [CDH25] argue that ZKPs alone cannot solve the broader problems of age verification, as repeated proofs can narrow down the user's date of birth, revocation checks can let issuers track where a credential is used, and a handful of issuers gain the power to decide who gets access. Finally, the statement warns that if unlinkability is interpreted loosely, so that only verifiers cannot link presentations, a central authority may retain a complete view of user activity [ABH+26, pp. 6–7].

Furthermore, the current implementation of the EUDI Wallet uses schemes, such as the Elliptic Curve Digital Signature Algorithm (ECDSA), that are not PQ-secure. In response to the quantum threat, the EU [NISCG25, pp. 3, 7] and the United States government [EOP26, p. 38484] have set goals for the PQ transition, with deadlines between 2030 and 2035. More recently, Google [AS26] and Cloudflare [Wes26] have both moved their targets to 2029 and prioritized authentication. Cloudflare attributes the earlier timelines to recent advances, including a resource estimate for breaking P-256, the curve that verifiers of the wallet must support for device signatures, with only 10,000 qubits [Wes26].

1.2 Research Questions

In this project, we investigate how to make the EUDI Wallet quantum-safe using lattice-based primitives, starting from the current ECDSA-based framework. We also examine to what extent we can achieve stronger privacy properties without general-purpose succinct non-interactive arguments of knowledge (SNARKs). Two such properties are issuer unlinkability, where the issuer cannot recognize the credentials

it issued when they are presented, and issuer hiding, where the verifier only learns that a credential comes from one of several accepted issuers, but not which one.

RQ1. What is the cost, in terms of performance and privacy properties, of directly replacing the Elliptic Curve Digital Signature Algorithm (ECDSA) in the current European Digital Identity Wallet, for both issuer and device signatures, with standardized lattice-based signatures?

RQ2. How can issuer unlinkability and issuer hiding be achieved with quantum-safe primitives within the current framework of salted hashes and batch issuance, without relying on anonymous credentials?

RQ3. How practical are lattice-based blind signatures for issuing one-show credentials in the European Digital Identity Wallet, compared with multi-show anonymous credentials, and how can such credentials be revoked?

RQ4. How well do the proposed lattice-based solutions meet the Architecture and Reference Framework high-level requirements in practice, and how do they compare with the current wallet and classical baselines?

By "without general-purpose SNARKs," we mean that proof systems which prove arbitrary rank-1 constraint system (R1CS) statements, such as lattice-based recursively amortized demonstration of R1CS (LaBRADOR) [BS23], are out of scope.

1.3 Related Work

The related work within this domain is quite limited, but there have been some recent developments, all of them preprints, which are described below. In the thesis, we will also discuss the following work in detail: The lattice-based ACs by Bootle et al. [BLNS23b] and Jeudy, Roux-Langlois, and Sanders [JRS23], the lattice-based blind signatures by Agrawal et al. [AKSY22], del Pino and Katsumata [dPK22], and Beullens et al. [BLNS23a], and the lattice-based ZKPs by Lyubashevsky, Nguyen, and Plançon [LNP22] and Beullens and Seiler [BS23].

Lattice-Based Blind Signatures. In a blind signature scheme, the signer signs a message without seeing it, so an issuer can sign credentials that they cannot recognize later. Blazy, Mallordy, and Wen [BMW26] build such a scheme on a lattice problem believed to be hard even for quantum computers without including a ZKP in the signature. This reduces the signature size from 22 KiB in the smallest-sized previous work to 4.7 KiB through Gentry–Peikert–Vaikuntanathan (GPV) [GPV08] preimages.

Post-Quantum Private Groups. Connell et al. [CFG+26] built a modular scheme with strong privacy guarantees from lattice-based signatures with re-randomizable keys, meaning that a key can be turned into a fresh-looking one that cannot be linked to the original. That is, "simply 'swapping in' quantum-safe primitives is unlikely to yield an optimal protocol," and hence, they created a group system "from the ground-up" whose core operations are even more efficient than those of Signal's current, classical deployment.

Issuer Hiding. Flamini et al. [FFK+26] achieve issuer hiding with key-randomizable signatures, without the policy keys that earlier schemes used to define the set of

accepted issuers. Their scheme is also compatible with Boneh–Boyen–Shacham (BBS)-based schemes, the leading classical approach to ACs.

2 Credentials and Digital Identity Wallets

2.1 The European Digital Identity Wallet

In 2024, electronic Identification, Authentication, and Trust Services (eIDAS) 2.0 amended the original eIDAS Regulation from 2014 and made it mandatory for every EU Member State to provide at least one digital identity wallet [EU24, Article 5a(1)]. How to implement such a wallet is specified in the *European Digital Identity Wallet Architecture and Reference Framework (ARF)*, which is developed by the European Commission together with the Member States through the European Digital Identity Cooperation Group [EDICG26, Section 1.2].

The organization that creates a credential is called the *issuer*, the entity that receives and controls it is the *holder*, and the entity that requests and checks it is the *verifier* [RFC9901, Section 1.2]. In the Architecture and Reference Framework (ARF), issuers of person identification data (PID) are called PID Providers, and issuers of electronic attestations of attributes are called Attestation Providers [EDICG26, Sections 3.4, 3.6–3.8, Annex 1].

Every wallet supports two credential formats [EDICG26, Section 5.4.1]: The mobile document (mdoc) format of ISO/IEC 18013-5 [ISO/IEC18013-5] and Selectively Disclosable JavaScript Object Notation Web Token-based Verifiable Digital Credentials (SD-JWT VCs) [TFC26]. Both formats achieve selective disclosure (SD) through salted hashes [EDICG26, Section 5.4.1]. Issuers typically sign the credentials with ECDSA [FS26, pp. 1, 3; FIPS186, Section 6]. Since the hashes, salts, and signature are identical in every presentation of a credential, verifiers can link presentations through them [EDICG26, Section 7.4.3.5.1]. To limit such linking, every wallet must support both credentials that are issued in batches and presented only once each, and single credentials that are presented repeatedly until they expire [EDICG26, Annex 2, ISSU_37]. Only the former fully prevents verifiers from linking presentations [EDICG26, Section 7.4.3.5.2].

Device binding is mandatory for PIDs and for credentials in the mdoc format and recommended for SD-JWT VCs [EDICG26, Section 6.6.3.8, Annex 2, ISSU_17]. For remote presentations, the ARF requires verifiers to at least support ECDSA with P-256 to verify the signature of the device [EDICG26, Annex 2, OIA_03b, OIA_03c; YLBH25, Section 7]. A PQ-secure wallet must therefore replace the signature of the device in addition to that of the issuer.

Batch issuance does not prevent linking by the issuer, and according to the ARF, the only viable mitigation is to replace salted hashes with ZKPs [EDICG26, Section 7.4.3.5.3]. The discussion paper on ZKPs divides ZKP schemes into multi-message signature schemes, such as BBS+, and proofs for arithmetic circuits, such as SNARKs [EC25, Section 3]. The former require issuers to adopt new signature

schemes, while the latter work on credentials in the existing formats, at the cost of computational overhead and larger proofs [EC25, Sections 3.1.3, 3.2, 4.3]. Neither the discussion paper nor the technical specifications that build on it consider PQ security.

2.2 Zero-Knowledge Proofs

ZKPs were first introduced in Goldwasser, Micali, and Rackoff [GMR85]. Intuitively, a ZKP is a protocol between a *prover*, $\mathcal{P}$, and a verifier, $\mathcal{V}$, where the prover convinces the verifier that a statement is true, for instance that she knows a secret value, without revealing anything beyond this fact [FFS88, pp. 77, 79]. In contrast with other proofs, these are often *interactive*, meaning that the prover and verifier exchange messages back and forth.

Two auxiliary algorithms are used to formalize the properties of a ZKP. A *simulator*, Sim, is an algorithm that can simulate the view of the verifier in the protocol without knowing the secret value. An *extractor*, Ext, is an algorithm that can extract the secret value from the prover if she can convince the verifier of her knowledge of the secret value.

For a protocol to be a ZKP, it must satisfy three properties, which are defined as follows:

Completeness. If the prover knows the secret value, then she can convince the verifier of this fact.

Soundness. If the statement is false, then the prover cannot convince the verifier of it, except with small probability. This is not sufficient when the prover claims to know a secret value, since such a value may exist without the prover knowing it. In that case, the stronger property of *knowledge soundness* is required, where if the prover can convince the verifier, then an extractor can obtain the secret value from the prover.

Zero-knowledge. The verifier learns nothing about the secret value from the protocol, in the sense that a simulator can produce the verifier's view without it.

The most common interactive ZKP system is the Σ-*protocol*. The name partly comes from the shape that the sequence of three messages follows [Cra97, p. 19]. First, the prover commits to the verifier using privately generated randomness $r \xleftarrow{R} \mathcal{R}$. The verifier responds with a privately sampled challenge $c \xleftarrow{R} \mathcal{C}$. Finally, the prover responds with a value based on both r and c. Σ-protocols satisfy *special soundness*, meaning the secret value can be computed from two accepting transcripts with the same first message and different challenges, which implies knowledge soundness.

For the Σ-protocol to become a non-interactive zero-knowledge (NIZK) proof, the challenge can be generated by the prover herself, instead of the verifier. This is done by using a hash function, on both the statement and the prover's first message, to generate the challenge c, which is then sent to the verifier along with the proof [BPW12, pp. 626–627]. This is known as the *Fiat–Shamir transformation* [FS87]. The security

of this transformation is proven by modeling the hash function as a *random oracle*, meaning that it behaves like a random function [BR93].

2.3 Anonymous Credentials

A credential system is "a system in which [holders] can obtain credentials from organizations and demonstrate possession of these credentials," and such a system is anonymous "when transactions carried out by the same [holder] cannot be linked" [CL01, p. 93].

Camenisch and Lysyanskaya [CL04, p. 62] note that "in order to construct an [AC] system, it is sufficient to exhibit a commitment scheme, a signature scheme, and efficient protocols for (1) proving equality of two committed values; (2) getting a signature on a committed value (without revealing this value to the signer); and (3) proving knowledge of a signature on a committed value." We now describe the properties an AC system should provide, some of which the current implementation of the EUDI Wallet lacks.

Selective disclosure. With SD, the holder reveals only a chosen subset of the attributes in a credential to the verifier [RFC9901, Section 1.2]. The verifier then learns nothing about the remaining attributes, except what follows from the disclosed attributes or from sources other than the credential [RFC9901, Section 9]. The formats used by the current implementation of the EUDI Wallet achieve this with *salted hashes*. Instead of signing each attribute directly, the issuer signs a hash of the attribute together with a random salt. To disclose an attribute, the holder sends its value and salt, and the verifier hashes them and checks that the result is among the signed hashes. The salt prevents the verifier from finding undisclosed values by hashing guesses [RFC9901, Section 1].

Unlinkability. As described by Fett, Yasuda, and Campbell [RFC9901, Section 10.1], "[u]nlinkability is a property whereby adversaries are prevented from correlating credential presentations of the same [holder] beyond the [holder]'s consent." In the simplest variant, *presentation unlinkability*, a verifier cannot link two presentations of the same credential. In *verifier/verifier unlinkability*, presentations made to different verifiers do not reveal that the same credential was presented, even if the verifiers collude [RFC9901, Section 10.1]. There are two ways to achieve this. The first is a *multi-show* credential, which can be presented an arbitrary number of times without the presentations being linkable to each other [CL01, p. 94]. The second, which the current implementation of the EUDI Wallet uses, is *batch issuance*, where the holder receives several *one-show* credentials with the same attributes and presents each of them only once. Since each credential in the batch uses fresh salts and device keys, verifiers cannot link the credentials through these values [RFC9901, Section 10.1].

Issuer unlinkability. Batch issuance only protects against verifiers, since the issuer has signed every credential in the batch. Protecting against the issuer as well requires issuer unlinkability, meaning that the issuer cannot tell that a

holder presented a credential to a certain verifier, even if the verifier shares the presentation with the issuer [RFC9901, Section 10.1]. This "cannot be achieved in salted hash-based selective disclosure approaches [...] as the issued credential with the [i]ssuer's signature is directly presented to the [v]erifier, who can forward it to the [i]ssuer" [RFC9901, Section 10.1]. Since the current implementation of the EUDI Wallet uses such approaches, it does not provide issuer unlinkability.

Blind issuance. In a *blind signature scheme*, the signer signs a message without learning it. Such a scheme must satisfy two properties, which were formalized by Juels, Luby, and Ostrovsky [JLO97]. *Blindness* means that "the malicious signer learns nothing about the [holder's] input and output after the protocol execution," and *one-more unforgeability* means that after n interactions with the signer, the holder cannot output $n + 1$ valid signatures on distinct messages [RFC9474, Section 7]. For credentials, the issuer is usually not fully blind, since it has to know the attributes it vouches for. Instead, it signs some values without seeing them, such as a secret key of the holder, which is the second protocol in the quote at the start of this subsection. Combined with batch issuance, blindness also provides issuer unlinkability, as the issuer cannot recognize the one-show credentials it has signed when they are presented. The lattice-based blind signature from Section 1.3 could therefore give a PQ wallet issuer unlinkability.

Issuer hiding. Even if all the properties above are satisfied, a presentation still reveals which issuer signed the credential, since standard AC schemes assume that the verifier knows the public key of the issuer that generated the credential [ST24, p. 646]. The current implementation of the EUDI Wallet reveals the issuer in the same way, as the verifier checks the signature using a trust anchor of the issuer [EDICG26, Section 6.6.3.6]. Bobolz et al. [BEK+21, p. 158] introduced issuer hiding, where "the verifier can define a set of acceptable issuers in an ad-hoc manner, and the [holder] can then prove that her credential was issued by one of the accepted issuers — without revealing which one." In the definition by Sanders and Traoré [ST24, p. 649], this must also hold under collusion, as "the verifier, even colluding with all issuers, is unable to identify under which public key the presented signature has been signed." Achieving this with PQ primitives, for instance through key-randomizable signatures as in Section 1.3, is one of the aims of this project.

Device binding. To prevent a credential from being copied to another device, for instance from a parent's phone to a child's, it can be *device-bound*. The credential is then tied to a key protected by the device's secure element, and "any presentation of the credential requires a fresh contribution of the [secure element]" [FHLL26, p. 345]. Deployed secure elements typically support Rivest–Shamir–Adleman (RSA) [RSA78] and ECDSA, but not pairings or lattices, and

replacing them takes about a decade [FS26, p. 3]. Neither RSA nor ECDSA is PQ-secure [Sho94]. Apple's Secure Enclave has, however, supported the Module-Lattice-Based Digital Signature Algorithm (ML-DSA) since iOS 26 [AAPL26a]. Device binding also conflicts with unlinkability, as a revealed device public key lets verifiers link the presentations of a holder [FS26, p. 38]. Batch issuance therefore uses a fresh device key for every credential, as described above, while ZKP-based presentations must keep the device public key hidden [FS26, p. 36].

2.4 Classical Baselines

There exist schemes that satisfy the properties of an AC system. We base our account of BBS on the retelling by Tessaro and Zhu [TZ23, pp. 691–692].

Camenisch–Lysyanskaya Signatures. The Camenisch–Lysyanskaya (CL) signature scheme generalized the AC framework of Camenisch and Lysyanskaya [CL01], operating in the group of quadratic residues modulo a special RSA modulus N, which has hidden order, under the strong RSA (SRSA) assumption [CL03]. In this scheme, the issuer can sign a message vector or issue signatures directly over an integer commitment $C = g^r \prod_{i=1}^{L} h_i^{m_i} \pmod{N}$ [DF02; FO97], where $g, h_1, \ldots, h_L$ are public generators of the group, the ℓ_m-bit integers $m_1, \ldots, m_L$ represent the L secret attributes, and r is a randomizing exponent. However, working in RSA groups requires large moduli and heavy multi-exponentiations, leading to high computational and transmission costs.

To reduce these overheads, Camenisch and Lysyanskaya [CL04] introduced pairing-based CL signatures, moving the construction to symmetric bilinear pairings $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$, where $\mathbb{G}$ is an elliptic curve group with generator P and $\mathbb{G}_T$ is the target group, under the Lysyanskaya–Rivest–Sahai–Wolf (LRSW) assumption.

Boneh–Boyen–Shacham Signatures. In parallel, Boneh, Boyen, and Shacham [BBS04] proposed BBS to construct efficient group signatures using a bilinear pairing $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$, where the elliptic curve groups $\mathbb{G}_1$ and $\mathbb{G}_2$ of prime order p are written additively with generators P_1 and P_2, and $\mathbb{G}_T$ is the target group. When abstracted as a standalone multi-attribute signature scheme, the issuer has a secret key $x \in \mathbb{Z}_p^*$ and a public key $W = xP_2 \in \mathbb{G}_2$. To sign L message attributes $m_1, \ldots, m_L \in \mathbb{Z}_p$ with public generators $H_1, \ldots, H_L \in \mathbb{G}_1$, the issuer selects a random scalar $r \in \mathbb{Z}_p^*$ and computes $A \in \mathbb{G}_1$ such that $(x + r)A = P_1 + \sum_{i=1}^{L} m_i H_i$. This yields a compact signature tuple (A, r), which is verified via $e(A, W + rP_2) = e\Big(P_1 + \sum_{i=1}^{L} m_i H_i, P_2\Big)$ [CL04, pp. 69–70; TZ23, p. 699]. Although this base signature yields a small footprint, BBS was originally designed for group signatures and lacked a full security proof for multi-attribute AC applications.

To resolve this limitation, Au, Susilo, and Mu [ASM06] presented the BBS+ scheme, adding a second randomizing scalar $s \in \mathbb{Z}_p^*$ to form the signature tuple (A, r, s) satisfying $(x + r)A = P_1 + sH_0 + \sum_{i=1}^{L} m_i H_i$, where $H_0 \in \mathbb{G}_1$ is another public generator. The holder can randomize A and construct ZKPs over any subset

Table 1: Properties provided by salted hashes with ECDSA as in the current EUDI Wallet and by BBS.

Property	**EUDI Wallet**	BBS
SD	Yes	Yes
Unlinkability	Yes*	Yes
Issuer unlinkability	No	Yes
Blind issuance	No	Yes†
Issuer hiding	No	Yes†
Device binding	Yes	Yes†
PQ unforgeability	No	No

* One-show credentials only.
† With extensions.

of signed attributes for unlinkable multi-show presentations. Camenisch, Drijvers, and Lehmann [CDL16] proved the scheme secure for type-3 pairings and gave a proof of knowledge (PoK) of a signature before Tessaro and Zhu [TZ23] provided an updated security proof for the base BBS scheme under q-strong Diffie–Hellman, together with a tight proof in the algebraic group model, proving that s is redundant and re-allowing signatures to consist solely of the short tuple (A, r).

The standardization of BBS is, however, not yet final [LKW+26]. Moreover, because BBS relies on the mathematical hardness of pairing-based elliptic curve problems, its unforgeability is vulnerable to a cryptographically relevant quantum computer, whereas the privacy of its proofs holds even against computationally unbounded adversaries [LKW+26, Section 6.10]. A competitor of BBS is Longfellow, the proof system of Frigo and shelat [FS26, p. 1], which instead proves statements about existing ECDSA-signed credentials in zero-knowledge (ZK), so that neither the issuers nor the devices have to change.

Table 1 summarizes which of the AC properties are provided by the current implementation of the EUDI Wallet and by BBS with extensions [DDKT25; FFK+26; FHLL26; KB26]. Neither of them is PQ-secure, which motivates the research questions in Section 1.2.

3 Lattice-Based Cryptography

Our presentation builds on the work of Lyubashevsky [Lyu24], one of the creators of both the Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) [FIPS203] and ML-DSA [FIPS204].

3.1 Why Lattices?

There are numerous primitives believed to be PQ-secure. However, we focus on lattices as a building block for digital signatures. Why focus on lattices and not on other primitives, such as codes, hash functions, multivariate polynomials, isogenies, or multiparty computation-in-the-head (MPCitH)?

In short, ML-DSA is one of the few PQ algorithms standardized by the National Institute of Standards and Technology (NIST) [FIPS204], meaning that it is among the most likely to be implemented in practice, for instance in the secure elements used for device binding [AAPL26a]. Furthermore, AC systems, and digital signature algorithms in general, benefit from being relatively structured, as this allows for succinct and efficient proofs.

Code-based, hash-based, and multivariate signatures are less suited for AC systems. Code-based schemes rely on problems such as the syndrome decoding problem [BMvT78] or learning parity with noise [BFKL94], which may remain hard even if lattice problems are broken. However, they require large parameters, and their Hamming-weight noise over small fields is costly to handle in efficient ZKPs.

Hash-based signatures are standardized alongside ML-DSA in the form of the Stateless Hash-Based Digital Signature Algorithm (SLH-DSA), which builds on a hypertree of Merkle trees [FIPS205, p. 7]. Unlike lattices, standard hash functions have no algebraic structure. Proving knowledge of a hash preimage, or of a valid signature, therefore requires arithmetizing many hash evaluations, which is expensive [GKR+21, p. 519; ZSE+24, p. 5].

In multivariate trapdoor schemes such as unbalanced oil and vinegar (UOV) [KPG99] and MAYO [Beu22], a signature is a solution to a public system of quadratic equations whose right-hand side is a hash of the message. This makes efficient ZKPs of signature possession hard for two reasons. The public keys are large, leading to large proofs, and hashing the message breaks the algebraic link between the message and the signature, so a proof about hidden attributes must also show that the hash was evaluated correctly, which is expensive.

This leaves isogeny-based signatures and the MPCitH paradigm [IKOS07]. However, neither short quaternion and isogeny signature (SQIsign) [DKL+20] nor any MPCitH scheme (e.g., syndrome decoding-in-the-head (SDitH) [FJR22], multivariate quadratic on my mind (MQOM) [BFR24], and FAEST [BBD+23]) is standardized yet, as they are still, at the time of this writing, candidates in the third round of the process for additional signatures by NIST [NIST26, p. 8]. Lattices are therefore the only family that offers both standardized signature schemes and the algebraic structure that AC systems need. Isogenies do, however, look promising due to their algebraic structure.

Lattices do not avoid the hashing problem, however. ML-DSA also hashes the message, and its verification uses Secure Hash Algorithm Keccak (SHAKE) [FIPS204, pp. 10, 13–14, 27], so proving the verification of an ML-DSA signature in ZK also requires arithmetizing hash evaluations. The team behind Longfellow has nevertheless used it to prove possession of an ML-DSA signature [FSGC26]. This is out of scope for the thesis, as the techniques and goals differ, but it may still offer useful lessons. The real advantage of lattices is instead that they allow designing signatures with efficient protocols that integrate well with lattice-based ZKPs. Many lattice-based credentials

and blind signatures, such as those by del Pino and Katsumata [dPK22] and Blazy, Mallordy, and Wen [BMW26], build on the same trapdoor sampling as the FFT over NTRU-Lattice-Based Digital Signature Algorithm (FN-DSA) [FHK+20], whose signer uses a trapdoor to sample a short preimage of the hashed message [GPV08].

3.2 Hardness Assumptions

The building blocks of public-key cryptography are the hardness assumptions on which the security of the cryptographic primitives is based. For lattice-based cryptography, there are similar problems, but we only describe two of them in detail, namely the short integer solution (SIS) and learning with errors (LWE) problems.

Short Integer Solution. The SIS problem is a search problem believed to be hard to solve, even for quantum computers. It was first introduced by Ajtai [Ajt96], and the version in the ∞-norm, which ML-DSA uses in module form, is shown in Figure 1: Given a random matrix $\mathbf{A}$, the adversary must find a short non-zero vector $\boldsymbol{x}$ that $\mathbf{A}$ maps to zero, where $\|\boldsymbol{x}\|_\infty$ denotes the largest absolute value of any entry of $\boldsymbol{x}$. Note that $\mathbf{A}$ must be *wide*, meaning that $\ell > k$, for a short non-zero solution to exist, and that the bound $\beta \ll q$ is what makes the problem hard, since without it one could simply use Gaussian elimination to find a valid solution.

Learning with Errors. The LWE problem, introduced by Regev [Reg05, p. 85], is believed to be hard to solve on both classical and quantum computers. In its decision version, shown in Figure 1, the adversary is given a random matrix $\mathbf{A}$ with $k \geqslant \ell$ together with either $\mathbf{A}\boldsymbol{s} + \boldsymbol{e}$, for a uniform secret $\boldsymbol{s}$ and a noise vector $\boldsymbol{e}$ with small entries sampled from an error distribution χ, or a uniformly random vector. Its advantage is the difference between the probabilities that it outputs 1 in the two cases, and the problem is hard if this advantage is negligible.

$\mathsf{SIS}_{k,\ell,q,\beta}(\mathcal{A})$	$\mathsf{LWE}_{k,\ell,q,\chi}(\mathcal{A})$
$\mathbf{A} \xleftarrow{\text{R}} \mathbb{Z}_q^{k\times\ell}$	$b \xleftarrow{\text{R}} \{0,1\}$
$\boldsymbol{x} \leftarrow \mathcal{A}(\mathbf{A})$	$\mathbf{A} \xleftarrow{\text{R}} \mathbb{Z}_q^{k\times\ell}$
if $\boldsymbol{x} = \mathbf{0}$ **then return false**	$\boldsymbol{s} \xleftarrow{\text{R}} \mathbb{Z}_q^{\ell}$
if $\|\boldsymbol{x}\|_\infty \geqslant \beta$ **then return false**	$\boldsymbol{e} \xleftarrow{\text{R}} \chi^k$
return $\mathbf{A}\boldsymbol{x} = \mathbf{0} \pmod q$	$\boldsymbol{u}_0 \leftarrow \mathbf{A}\boldsymbol{s} + \boldsymbol{e} \pmod q$
	$\boldsymbol{u}_1 \xleftarrow{\text{R}} \mathbb{Z}_q^k$
	$b' \leftarrow \mathcal{A}(\mathbf{A}, \boldsymbol{u}_b)$
	return $b = b'$

Figure 1: The SIS problem as a search game and the LWE problem as a decision game.

3.3 Polynomial Rings and Module Variants

One problem with the SIS and LWE problems is that the parameters they require, in order to be secure, are quite large. To reduce the size of the parameters, one can use polynomial rings instead of matrices and vectors. This is done by defining the problems over the ring $R_q = \mathbb{Z}_q[x]/(x^n + 1)$ instead, namely in ring-LWE (R-LWE) [LPR10] and ring-SIS (R-SIS) [LM06; PR06]. Here, n is a power of two, such as $n = 256$ in ML-KEM [FIPS203, Table 2] and ML-DSA [FIPS204, p. 5]. The reason for this is that the ring has a lot of structure: A ring element describes an $n \times n$ matrix with only n coefficients, which reduces the sizes by a factor of n and allows for more efficient computations. However, this also means that the problems might no longer be *as hard* to solve, since the structure might allow an attacker to exploit it. To this day, there are no known attacks that successfully exploit this additional structure for the parameters used in practice, and the problems are still believed to be hard to solve.

A trade-off between the plain and the ring variants can be achieved by using module variants of the problems, aptly named module LWE (MLWE) and module SIS (MSIS), which have sizes close to those of the ring variants but less algebraic structure [BGV12; LS15].

3.4 The Module-Lattice-Based Digital Signature Algorithm

We describe ML-DSA as defined in Federal Information Processing Standard (FIPS) 204 [FIPS204]. In Figure 2, the ML-DSA protocol is illustrated. Notice that here, instead of a prover $\mathcal{P}$, there is a signer $\mathcal{S}$. The protocol is an identification protocol that allows a prover to convince a verifier that she knows short secret vectors $\boldsymbol{s}_1$ and $\boldsymbol{s}_2$ such that $\mathbf{A}\boldsymbol{s}_1 + \boldsymbol{s}_2 = \boldsymbol{t}$ for a public matrix $\mathbf{A}$ and vector $\boldsymbol{t}$, without revealing any information about the secret vectors to an honest verifier, provided that the protocol does not abort. However, an extractor can only obtain a *relaxed witness*, which is longer than $\boldsymbol{s}_1$ and $\boldsymbol{s}_2$ [Lyu24, pp. 41, 45]. The protocol uses the MLWE assumption and relies on the hardness of a variant of the MSIS problem [KLS18, pp. 582–583].

Private and Public Keys. Building on MLWE, the public key is defined to be a random matrix $\mathbf{A} \in R_q^{k \times \ell}$. However, for the ML-DSA protocol to be usable in practice, this matrix is considered too large to transmit. Therefore, the matrix is instead expanded from a seed, ρ, as $\mathbf{A} \leftarrow \mathsf{ExpandA}(\rho)$. This is omitted in Figure 2 for clarity. The secret vectors $\boldsymbol{s}_1 \in R_q^\ell$ and $\boldsymbol{s}_2 \in R_q^k$ are sampled from a discrete uniform distribution such that $\|\boldsymbol{s}_i\|_\infty \leqslant \eta$ for $i = 1, 2$. To save space, the public key further consists of only the high-order part $\boldsymbol{t}_1$ of the vector $\boldsymbol{t} = \mathbf{A}\boldsymbol{s}_1 + \boldsymbol{s}_2 = 2^d\boldsymbol{t}_1 + \boldsymbol{t}_0$, where d is the number of bits dropped from each coefficient. The public key is then $(\rho, \boldsymbol{t}_1)$ and the private key is $(\boldsymbol{t}_0, \boldsymbol{s}_1, \boldsymbol{s}_2)$. In addition, both parties have the value μ, which is the hash of the encoding of the message M that is signed.

Sampling $\boldsymbol{y}$. As in a Σ-protocol, $\boldsymbol{y}$ acts as the privately sampled randomness r. As described in the standard, the prover samples a vector $\boldsymbol{y} \in R_q^\ell$ such that $\|\boldsymbol{y}\|_\infty \leqslant \gamma_1$ [FIPS204, p. 38].

$\mathcal{S}(\mathbf{A}, \boldsymbol{t}_0, \boldsymbol{t}_1, \boldsymbol{s}_1, \boldsymbol{s}_2, \mu)$	$\mathcal{V}(\mathbf{A}, \boldsymbol{t}_1, \mu, c, \boldsymbol{z}, \boldsymbol{h})$
$\boldsymbol{y} \xleftarrow{\text{R}} \left\{\boldsymbol{v} \in R_q^\ell : \left\|\boldsymbol{v}\right\|_\infty \leqslant \gamma_1\right\}$	**if** $\left\|\boldsymbol{z}\right\|_\infty \geqslant \gamma_1 - \beta$ **then return false**
$\boldsymbol{w} \leftarrow \mathbf{A}\boldsymbol{y}$	**if** $\left\|\boldsymbol{h}\right\|_1 > \omega$ **then return false**
$\boldsymbol{w}_1 \leftarrow \mathsf{HighBits}(\boldsymbol{w})$	$\boldsymbol{w}_1' \leftarrow \mathsf{UseHint}\big(\boldsymbol{h}, \mathbf{A}\boldsymbol{z} - 2^d c\boldsymbol{t}_1\big)$
$c \leftarrow \mathsf{H}(\mu \| \boldsymbol{w}_1)$	**return** $c = \mathsf{H}\big(\mu \| \boldsymbol{w}_1'\big)$
if $\left\|c\boldsymbol{t}_0\right\|_\infty \geqslant \gamma_2$ **then abort**	
$\boldsymbol{z} \leftarrow \boldsymbol{y} + c\boldsymbol{s}_1$	
if $\left\|\boldsymbol{z}\right\|_\infty \geqslant \gamma_1 - \beta$ **then abort**	
$\boldsymbol{r}_0 \leftarrow \mathsf{LowBits}(\boldsymbol{w} - c\boldsymbol{s}_2)$	
if $\left\|\boldsymbol{r}_0\right\|_\infty \geqslant \gamma_2 - \beta$ **then abort**	
$\boldsymbol{h} \leftarrow \mathsf{MakeHint}[-c\boldsymbol{t}_0, \boldsymbol{w} + c(\boldsymbol{t}_0 - \boldsymbol{s}_2)]$	
if $\left\|\boldsymbol{h}\right\|_1 > \omega$ **then abort**	
return $c, \boldsymbol{z}, \boldsymbol{h}$	

Figure 2: The Module-Lattice-Based Digital Signature Algorithm.

Challenge c. As in the Fiat–Shamir transform, the challenge c is generated by the prover herself by the use of a hash function, H. In a similar fashion to the public matrix $\mathbf{A}$, this hash is actually a seed $\tilde{c}$, from which $c \leftarrow \mathsf{SampleInBall}(\tilde{c})$ is derived. This is also omitted in Figure 2 for clarity. The goal is to maximize the number of possible values of c but still make it short so that rejection sampling succeeds after only a few attempts on average. Recall that ML-DSA is working over R_q, so a way to make the challenge short is to make the coefficients short. $\mathcal{C}$ is then $\{c \in R_q : \left\|c\right\|_\infty \leqslant 1 \wedge \left\|c\right\|_1 = \tau\}$. Since every coefficient of c is in $\{-1, 0, 1\}$, $\left\|c\right\|_1$ counts its non-zero coefficients. The size of this challenge space is $2^\tau \binom{n}{\tau}$, where n denotes the degree of the polynomial ring [FIPS204, Table 1].

Rejection Sampling. $\boldsymbol{z}$ is computed as $\boldsymbol{y} + c\boldsymbol{s}_1$ and is later transmitted to the verifier. Since $\left\|c\right\|_1 = \tau$ and $\left\|\boldsymbol{s}_1\right\|_\infty \leqslant \eta$, the shift is bounded by $\left\|c\boldsymbol{s}_1\right\|_\infty \leqslant \beta = \tau\eta$. Consider the case where elements of $\boldsymbol{z}$ fall close to or outside the edges of the *legal* values of $\boldsymbol{y}$. Then, information about the secret key $\boldsymbol{s}_1$ is leaked, as how likely such values are depends on $c\boldsymbol{s}_1$. The solution is to apply rejection sampling. This, in collaboration with the previous paragraph, is the namesake of the *Fiat–Shamir with Aborts* paradigm [Lyu09], which ML-DSA implements. This works by completing the protocol as defined up to this point, and if $\left\|\boldsymbol{z}\right\|_\infty \geqslant \gamma_1 - \beta$, it aborts and goes back to the step where it generates $\boldsymbol{y}$. Whatever $\boldsymbol{s}_1$ is, every $\boldsymbol{z}$ with $\left\|\boldsymbol{z}\right\|_\infty < \gamma_1 - \beta$ is reached by exactly one $\boldsymbol{y}$ with $\left\|\boldsymbol{y}\right\|_\infty \leqslant \gamma_1$, so all such $\boldsymbol{z}$ are equally likely. The distribution of $\boldsymbol{z}$ is thus uniform over this smaller range and independent of $\boldsymbol{s}_1$, which lets the simulator sample $\boldsymbol{z}$ without knowing the secret key.

Hinting. Upon comparing Figure 2 with what has been discussed so far, no mention of HighBits and LowBits is present. This is an implementation detail meant to reduce the size of the signature. However, to be able to drop information and for it to be possible to reconstruct, the prover issues a hint $\boldsymbol{h}$. Here, γ_2 bounds the low-order parts returned by LowBits, and ω bounds the number of ones in $\boldsymbol{h}$. The reasoning behind the correctness of the verification is provided by Ducas et al. [DKL+18, pp. 240–241].

The exact values of q, d, τ, γ_1, γ_2, k, ℓ, η, β, and ω are described by NIST [FIPS204, Table 1].

4 Methodology

In the thesis, we aim to both design a protocol and construct a prototype implementation of it.

4.1 Analysis and Prototyping of Constructions

To start off, the constructions in Section 1.3 will be explored to see whether they fulfill the high-level requirements of the EUDI Wallet, which are detailed in the ARF. Further, a naïve approach, simply replacing ECDSA in the current implementation with ML-DSA, will be examined to see how this would impact performance and privacy. Performance metrics include size (key, signature, and proof), time (issue, present, and verify), and number of interactions. We benchmark all three parameter sets of ML-DSA, which target NIST security categories 2, 3, and 5 [FIPS204, Table 1], but use ML-DSA-65 as the main point of comparison, as it is the smallest parameter set supported by Apple's Secure Enclave [AAPL26b]. Constructions from the literature are instantiated with the parameters their authors propose for 128 bits of security, so that they can be compared with ECDSA over P-256. Operations of the issuer and verifier are measured on a laptop, and operations of the holder, including device signatures, are also measured on a phone through the Norwegian Digitalization Agency (Digdir)'s demo wallet. Each operation is repeated 1,000 times after a warm-up, and we report the median, as the signing time of ML-DSA varies with the number of rejections. End-to-end flows in the sandbox are repeated 100 times. Each construction will also be assessed by which hardness assumptions it relies on and whether its security is proven. Its privacy will be evaluated against the properties in Table 1, in the same way as the current EUDI Wallet and BBS. In addition, we will examine whether lattice-based constructions can be utilized to accomplish PQ primitives that fulfill the properties that are currently not present. Promising constructions will be prototyped and integrated into Digdir's sandbox.

4.2 The Norwegian Digitalization Agency's Sandbox

All prototypes will be implemented in the prototype sandbox of Digdir. The Department of Information Security and Communication Technology at the Norwegian University of Science and Technology (NTNU) is planning to host its own instance

of the sandbox to serve as a research environment for the students who write their thesis about the EUDI Wallet. In this sandbox, we will replace parts of the current implementation with other approaches and see if they work in practice. Where possible, existing implementations of ML-DSA that conform to FIPS 204 will be used instead of a new implementation to reduce the risk of implementation errors. The prototypes will be tested end to end with Digdir's test tools for issuing [Digdir26b] and verifying [Digdir26a] credentials.

5 Project Plan

Since I will be a teaching assistant and fellow in two courses, I will work on the thesis from mid-January to mid-July. However, the plan in Figure 3 aims to submit by early June, leaving the remaining time as a buffer for delays.

First, the constructions from Section 1.3, and any published in the meantime, are evaluated against the properties in Table 1 and the high-level requirements of the ARF, and the targets are chosen in consultation with the supervisors. In parallel, ECDSA is replaced with ML-DSA in the sandbox to give a naïve baseline. The design then pursues the targets, and the resulting construction is prototyped and compared with the baseline. The rest of the thesis is mostly written afterward, and the revision incorporates feedback from the supervisors on the draft and from the presentation. The main risk is that the targets prove harder to achieve than expected, so the design starts with the most achievable ones, and negative results are documented along the way. Externally, the baseline depends on help from Digdir and on the NTNU instance of the sandbox.

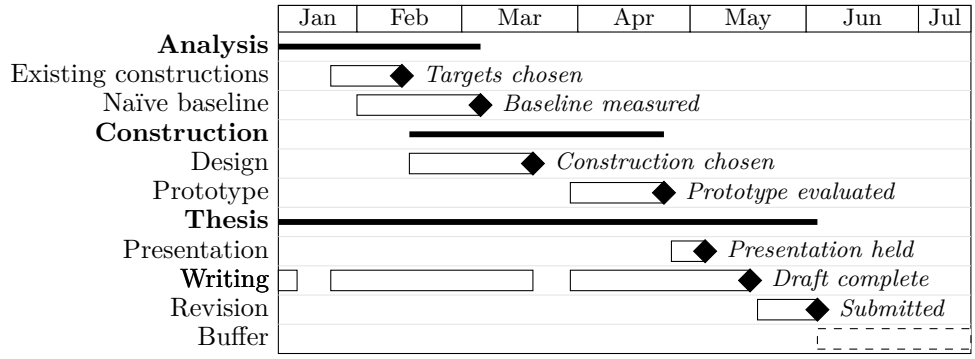


Figure 3: Gantt chart of the thesis, with the tasks grouped into analysis, construction, and the thesis itself. Each diamond marks the milestone that ends a task, gaps in the bars are breaks, and the dashed bar is the buffer between the planned submission and the deadline.

References

[AAPL26a] Apple. “Enhancing your app’s privacy and security with quantum-secure workflows,” last visited: Nov. 1, 2026. [Online]. Available: https://developer.apple.com/documentation/cryptokit/enhancing-your-app-s-privacy-and-security-with-quantum-secure-workflows

[AAPL26b] Apple. “SecureEnclave,” last visited: Nov. 11, 2026. [Online]. Available: https://developer.apple.com/documentation/cryptokit/secureenclave

[ABH+26] D. F. Aranha, O. Blazy, et al. “Joint statement of security and privacy scientists and researchers on Age Assurance,” last visited: Nov. 10, 2026. [Online]. Available: https://csa-scientist-open-letter.org/ageverif-Feb 2026

[Ajt96] M. Ajtai, “Generating hard instances of lattice problems (extended abstract),” in *28th Annual ACM Symposium on Theory of Computing*, Philadephia, PA, USA: ACM Press, May 1996, pp. 99–108.

[AKSY22] S. Agrawal, E. Kirshanova, et al., “Practical, round-optimal lattice-based blind signatures,” in *ACM CCS 2022: 29th Conference on Computer and Communications Security*, H. Yin, A. Stavrou, et al., Eds., Los Angeles, CA, USA: ACM Press, Nov. 2022, pp. 39–53.

[AS26] H. Adkins and S. Schmieg. “Quantum frontiers may be closer than they appear,” Google, last visited: Nov. 10, 2026. [Online]. Available: https://blog.google/innovation-and-ai/technology/safety-security/cryptography-migration-timeline/

[ASM06] M. H. Au, W. Susilo, and Y. Mu, “Constant-size dynamic k-TAA,” in *SCN 06: 5th International Conference on Security in Communication Networks*, R. De Prisco and M. Yung, Eds., ser. Lecture Notes in Computer Science, vol. 4116, Maiori, Italy: Springer Berlin Heidelberg, Germany, Sep. 2006, pp. 111–125.

[AW26] A. Albanese and A. Wells. “4.7 million accounts deactivated, removed or restricted,” Prime Minister of Australia, last visited: Oct. 27, 2026. [Online]. Available: https://www.pm.gov.au/media/4-7-million-accounts-deactivated-removed-or-restricted

[BBD+23] C. Baum, L. Braun, et al., “Publicly verifiable zero-knowledge and post-quantum signatures from VOLE-in-the-head,” in *Advances in Cryptology – CRYPTO 2023, Part V*, H. Handschuh and A. Lysyanskaya, Eds., ser. Lecture Notes in Computer Science, vol. 14085, Santa Barbara, CA, USA: Springer, Cham, Switzerland, Aug. 2023, pp. 581–615.

[BBS04] D. Boneh, X. Boyen, and H. Shacham, “Short group signatures,” in *Advances in Cryptology – CRYPTO 2004*, M. Franklin, Ed., ser. Lecture Notes in Computer Science, vol. 3152, Santa Barbara, CA, USA: Springer Berlin Heidelberg, Germany, Aug. 2004, pp. 41–55.

[BEK+21] J. Bobolz, F. Eidens, et al., "Issuer-hiding attribute-based credentials," in *CANS 21: 20th International Conference on Cryptology and Network Security*, M. Conti, M. Stevens, and S. Krenn, Eds., ser. Lecture Notes in Computer Science, vol. 13099, Vienna, Austria: Springer, Cham, Switzerland, Dec. 2021, pp. 158–178.

[Beu22] W. Beullens, "MAYO: Practical post-quantum signatures from oil-and-vinegar maps," in *SAC 2021: 28th Annual International Workshop on Selected Areas in Cryptography*, R. AlTawy and A. Hülsing, Eds., ser. Lecture Notes in Computer Science, vol. 13203, Virtual Event: Springer, Cham, Switzerland, Sep. 2022, pp. 355–376.

[BFKL94] A. Blum, M. L. Furst, et al., "Cryptographic primitives based on hard learning problems," in *Advances in Cryptology – CRYPTO'93*, D. R. Stinson, Ed., ser. Lecture Notes in Computer Science, vol. 773, Santa Barbara, CA, USA: Springer Berlin Heidelberg, Germany, Aug. 1994, pp. 278–291.

[BFR24] R. Benadjila, T. Feneuil, and M. Rivain, "MQ on my mind: Post-quantum signatures from the non-structured multivariate quadratic problem," in *2024 IEEE European Symposium on Security and Privacy*, Vienna, Austria: IEEE Computer Society Press, Jul. 2024, pp. 468–485.

[BGV12] Z. Brakerski, C. Gentry, and V. Vaikuntanathan, "(Leveled) fully homomorphic encryption without bootstrapping," in *ITCS 2012: 3rd Innovations in Theoretical Computer Science*, S. Goldwasser, Ed., Cambridge, MA, USA: Association for Computing Machinery, Jan. 2012, pp. 309–325.

[BLNS23a] W. Beullens, V. Lyubashevsky, et al., "Lattice-based blind signatures: Short, efficient, and round-optimal," in *ACM CCS 2023: 30th Conference on Computer and Communications Security*, W. Meng, C. D. Jensen, et al., Eds., Copenhagen, Denmark: ACM Press, Nov. 2023, pp. 16–29.

[BLNS23b] J. Bootle, V. Lyubashevsky, et al., "A framework for practical anonymous credentials from lattices," in *Advances in Cryptology – CRYPTO 2023, Part II*, H. Handschuh and A. Lysyanskaya, Eds., ser. Lecture Notes in Computer Science, vol. 14082, Santa Barbara, CA, USA: Springer, Cham, Switzerland, Aug. 2023, pp. 384–417.

[BMvT78] E. R. Berlekamp, R. J. McEliece, and H. C. A. van Tilborg, "On the inherent intractability of certain coding problems," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 384–386, May 1978.

[BMW26] O. Blazy, L.-B. Mallordy, and W. Wen, *Concurrently secure compact blind signatures from Module-SIS*, Cryptology ePrint Archive, Paper 2026/1690, 2026. [Online]. Available: https://eprint.iacr.org/2026/1690

[BPW12] D. Bernhard, O. Pereira, and B. Warinschi, "How not to prove yourself: Pitfalls of the Fiat-Shamir heuristic and applications to Helios," in *Advances in Cryptology – ASIACRYPT 2012*, X. Wang and K. Sako, Eds., ser. Lecture Notes in Computer Science, vol. 7658, Beijing, China: Springer Berlin Heidelberg, Germany, Dec. 2012, pp. 626–643.

[BR93] M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols," in *ACM CCS 93: 1st Conference on Computer and Communications Security*, D. E. Denning, R. Pyle, et al., Eds., Fairfax, Virginia, USA: ACM Press, Nov. 1993, pp. 62–73.

[BS23] W. Beullens and G. Seiler, "LaBRADOR: Compact proofs for R1CS from module-SIS," in *Advances in Cryptology – CRYPTO 2023, Part V*, H. Handschuh and A. Lysyanskaya, Eds., ser. Lecture Notes in Computer Science, vol. 14085, Santa Barbara, CA, USA: Springer, Cham, Switzerland, Aug. 2023, pp. 518–548.

[CDH25] S. Celi, K. Den Hartog, and H. Haddadi. "The limits of zero-knowledge for age-verification," Brave, last visited: Nov. 10, 2026. [Online]. Available: https://brave.com/blog/zkp-age-verification-limits/

[CDL16] J. Camenisch, M. Drijvers, and A. Lehmann, *Anonymous attestation using the strong Diffie Hellman assumption revisited*, Cryptology ePrint Archive, Report 2016/663, 2016. [Online]. Available: https://eprint.iacr.org/2016/663

[CFG+26] G. Connell, S. Faller, et al., *A quantum-safe private group system for Signal from key re-randomizable signatures*, Cryptology ePrint Archive, Paper 2026/453, 2026. [Online]. Available: https://eprint.iacr.org/2026/453

[CL01] J. Camenisch and A. Lysyanskaya, "An efficient system for non-transferable anonymous credentials with optional anonymity revocation," in *Advances in Cryptology – EUROCRYPT 2001*, B. Pfitzmann, Ed., ser. Lecture Notes in Computer Science, vol. 2045, Innsbruck, Austria: Springer Berlin Heidelberg, Germany, May 2001, pp. 93–118.

[CL03] J. Camenisch and A. Lysyanskaya, "A signature scheme with efficient protocols," in *SCN 02: 3rd International Conference on Security in Communication Networks*, S. Cimato, C. Galdi, and G. Persiano, Eds., ser. Lecture Notes in Computer Science, vol. 2576, Amalfi, Italy: Springer Berlin Heidelberg, Germany, Sep. 2003, pp. 268–289.

[CL04] J. Camenisch and A. Lysyanskaya, "Signature schemes and anonymous credentials from bilinear maps," in *Advances in Cryptology – CRYPTO 2004*, M. Franklin, Ed., ser. Lecture Notes in Computer Science, vol. 3152, Santa Barbara, CA, USA: Springer Berlin Heidelberg, Germany, Aug. 2004, pp. 56–72.

[Cra97] R. Cramer, "Modular design of secure yet practical cryptographic protocols," Ph.D. dissertation, University of Amsterdam, Jan. 1997. [Online]. Available: https://eprints.illc.uva.nl/id/eprint/1998/

[DDKT25] N. Desmoulins, A. Dumanois, et al., *Making BBS anonymous credentials eIDAS 2.0 compliant*, Cryptology ePrint Archive, Report 2025/619, 2025. [Online]. Available: https://eprint.iacr.org/2025/619

[DF02] I. Damgård and E. Fujisaki, "A statistically-hiding integer commitment scheme based on groups with hidden order," in *Advances in Cryptology – ASIACRYPT 2002*, Y. Zheng, Ed., ser. Lecture Notes in Computer Science, vol. 2501, Queenstown, New Zealand: Springer Berlin Heidelberg, Germany, Dec. 2002, pp. 125–142.

[Digdir26a] Norwegian Digitalization Agency. "Demo verifisering av digitale bevis," last visited: Oct. 17, 2026. [Online]. Available: https://demo-brukersted.test.eidas2sandkasse.net

[Digdir26b] Norwegian Digitalization Agency. "Testverktøy for bevisgenerator," last visited: Oct. 17, 2026. [Online]. Available: https://bevisgenerator.test.eidas2sandkasse.net

[DKL+18] L. Ducas, E. Kiltz, et al., "CRYSTALS-Dilithium: A lattice-based digital signature scheme," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 2018, no. 1, pp. 238–268, 2018. [Online]. Available: https://tches.iacr.org/index.php/TCHES/article/view/839

[DKL+20] L. De Feo, D. Kohel, et al., "SQISign: Compact post-quantum signatures from quaternions and isogenies," in *Advances in Cryptology – ASIACRYPT 2020, Part I*, S. Moriai and H. Wang, Eds., ser. Lecture Notes in Computer Science, vol. 12491, Daejeon, South Korea: Springer, Cham, Switzerland, Dec. 2020, pp. 64–93.

[dPK22] R. del Pino and S. Katsumata, "A new framework for more efficient round-optimal lattice-based (partially) blind signature via trapdoor sampling," in *Advances in Cryptology – CRYPTO 2022, Part II*, Y. Dodis and T. Shrimpton, Eds., ser. Lecture Notes in Computer Science, vol. 13508, Santa Barbara, CA, USA: Springer, Cham, Switzerland, Aug. 2022, pp. 306–336.

[EC25] European Commission, "Discussion paper for European Digital Identity Cooperation Group regarding Topic G: Zero knowledge proof," European Commission, Discussion Paper Version 1.4, Mar. 2025. [Online]. Available: https://eudi.dev/3.0.0/discussion-topics/g-zero-knowledge-proof/

[EC26a] European Commission, *EU KIDS Act to restrict social media platforms' access to children in the EU*, Press release IP/26/1890, Sep. 2026. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/ip_26_1890

[EC26b] European Commission. “European Digital Identity,” last visited: Nov. 10, 2026. [Online]. Available: https://commission.europa.eu/topics/digital-economy-and-society/european-digital-identity_en

[EC26c] European Commission. “The EU approach to age verification,” last visited: Nov. 11, 2026. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/eu-age-verification

[EDICG26] European Digital Identity Cooperation Group, “European Digital Identity Wallet Architecture and Reference Framework (ARF),” European Commission, Tech. Rep. Version 3.0.0, Jul. 2026. [Online]. Available: https://eudi.dev/3.0.0/

[EOP26] Executive Office of the President, *Executive order 14412: Securing the nation against advanced cryptographic attacks*, Federal Register, vol. 91, no. 121, p. 38483, Jun. 2026. [Online]. Available: https://www.govinfo.gov/content/pkg/FR-2026-06-25/pdf/2026-12909.pdf

[EU24] European Parliament and the Council of the European Union, *Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework*, Official Journal of the European Union, L series, 2024/1183, Apr. 2024. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2024/1183/oj

[FFK+26] A. Flamini, K. Friedrichs, et al., *Issuer-hiding anonymous tokens and credentials from key-randomizable signatures*, Cryptology ePrint Archive, Paper 2026/870, 2026. [Online]. Available: https://eprint.iacr.org/2026/870

[FFS88] U. Feige, A. Fiat, and A. Shamir, “Zero-knowledge proofs of identity,” *Journal of Cryptology*, vol. 1, no. 2, pp. 77–94, Jun. 1988.

[FHK+20] P.-A. Fouque, J. Hoffstein, et al., “Falcon: Fast-Fourier lattice-based compact signatures over NTRU,” NIST Post-Quantum Cryptography Standardization, Specification Version 1.2, Oct. 2020. [Online]. Available: https://falcon-sign.info/falcon.pdf

[FHLL26] K. Friedrichs, F. Harding, et al., “Device-bound anonymous credentials with(out) trusted hardware,” in *Advances in Cryptology – EUROCRYPT 2026, Part II*, J. Daemen and E. Thomé, Eds., ser. Lecture Notes in Computer Science, vol. 16542, Rome, Italy: Springer, Cham, Switzerland, May 2026, pp. 345–375.

[FIPS186] National Institute of Standards and Technology, “Digital signature standard (DSS),” National Institute of Standards and Technology, Gaithersburg, MD, Federal Information Processing Standards Publication NIST FIPS 186-5, Feb. 2023. [Online]. Available: https://csrc.nist.gov/pubs/fips/186-5/final

[FIPS203] National Institute of Standards and Technology, "Module-lattice-based key-encapsulation mechanism standard," National Institute of Standards and Technology, Gaithersburg, MD, Federal Information Processing Standards Publication NIST FIPS 203, Aug. 2024. [Online]. Available: https://csrc.nist.gov/pubs/fips/203/final

[FIPS204] National Institute of Standards and Technology, "Module-lattice-based digital signature standard," National Institute of Standards and Technology, Gaithersburg, MD, Federal Information Processing Standards Publication NIST FIPS 204, Aug. 2024. [Online]. Available: https://csrc.nist.gov/pubs/fips/204/final

[FIPS205] National Institute of Standards and Technology, "Stateless hash-based digital signature standard," National Institute of Standards and Technology, Gaithersburg, MD, Federal Information Processing Standards Publication NIST FIPS 205, Aug. 2024. [Online]. Available: https://csrc.nist.gov/pubs/fips/205/final

[FJR22] T. Feneuil, A. Joux, and M. Rivain, "Syndrome decoding in the head: Shorter signatures from zero-knowledge proofs," in *Advances in Cryptology – CRYPTO 2022, Part II*, Y. Dodis and T. Shrimpton, Eds., ser. Lecture Notes in Computer Science, vol. 13508, Santa Barbara, CA, USA: Springer, Cham, Switzerland, Aug. 2022, pp. 541–572.

[FO97] E. Fujisaki and T. Okamoto, "Statistical zero knowledge protocols to prove modular polynomial relations," in *Advances in Cryptology – CRYPTO'97*, B. S. Kaliski Jr., Ed., ser. Lecture Notes in Computer Science, vol. 1294, Santa Barbara, CA, USA: Springer Berlin Heidelberg, Germany, Aug. 1997, pp. 16–30.

[For25] L. Forristal. "Reddit rolls out age verification in the UK to comply with new rules," TechCrunch, last visited: Oct. 27, 2026. [Online]. Available: https://techcrunch.com/2025/07/15/reddit-rolls-out-age-verification-in-the-uk-to-comply-with-new-rules/

[FS26] M. Frigo and a. shelat, "Anonymous credentials from ECDSA," *IACR Communications in Cryptology*, vol. 3, no. 1, May 2026. [Online]. Available: https://cic.iacr.org/p/3/1/7

[FS87] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," in *Advances in Cryptology – CRYPTO'86*, A. M. Odlyzko, Ed., ser. Lecture Notes in Computer Science, vol. 263, Santa Barbara, CA, USA: Springer Berlin Heidelberg, Germany, Aug. 1987, pp. 186–194.

[FSGC26] M. Frigo, a. shelat, et al. "libZK: PQ zero knowledge," IETF 126, CFRG, last visited: Nov. 10, 2026. [Online]. Available: https://datatracker.ietf.org/meeting/126/materials/slides-126-cfrg-longfellow-zk-00

[GKR+21] L. Grassi, D. Khovratovich, et al., "Poseidon: A new hash function for zero-knowledge proof systems," in *USENIX Security 2021: 30th USENIX Security Symposium*, M. Bailey and R. Greenstadt, Eds., USENIX Association, Aug. 2021, pp. 519–535. [Online]. Available: https://www.usenix.org/conference/usenixsecurity21/presentation/grassi

[GMR85] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof-systems (extended abstract)," in *17th Annual ACM Symposium on Theory of Computing*, Providence, RI, USA: ACM Press, May 1985, pp. 291–304.

[GPV08] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in *40th Annual ACM Symposium on Theory of Computing*, R. E. Ladner and C. Dwork, Eds., Victoria, BC, Canada: ACM Press, May 2008, pp. 197–206.

[IKOS07] Y. Ishai, E. Kushilevitz, et al., "Zero-knowledge from secure multiparty computation," in *39th Annual ACM Symposium on Theory of Computing*, D. S. Johnson and U. Feige, Eds., San Diego, CA, USA: ACM Press, Jun. 2007, pp. 21–30.

[ISO/IEC18013-5] International Organization for Standardization and International Electrotechnical Commission, "Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application," International Organization for Standardization, Geneva, Switzerland, International Standard ISO/IEC 18013-5:2021, Sep. 2021. [Online]. Available: https://www.iso.org/standard/69084.html

[JLO97] A. Juels, M. Luby, and R. Ostrovsky, "Security of blind digital signatures (extended abstract)," in *Advances in Cryptology – CRYPTO'97*, B. S. Kaliski Jr., Ed., ser. Lecture Notes in Computer Science, vol. 1294, Santa Barbara, CA, USA: Springer Berlin Heidelberg, Germany, Aug. 1997, pp. 150–164.

[JRS23] C. Jeudy, A. Roux-Langlois, and O. Sanders, "Lattice signature with efficient protocols, application to anonymous credentials," in *Advances in Cryptology – CRYPTO 2023, Part II*, H. Handschuh and A. Lysyanskaya, Eds., ser. Lecture Notes in Computer Science, vol. 14082, Santa Barbara, CA, USA: Springer, Cham, Switzerland, Aug. 2023, pp. 351–383.

[KB25] M. Kaufman and R. Bhatia. "Roblox requires age checks for communication, ushering in new safety standard," Roblox Newsroom, last visited: Oct. 27, 2026. [Online]. Available: https://about.roblox.com/newsroom/2025/11/roblox-requires-age-checks-limits-minor-and-adult-chat

[KB26] V. Kalos and G. M. Bernstein, "Blind BBS signatures," Internet Research Task Force, Internet-Draft draft-irtf-cfrg-bbs-blind-signatures-05, Oct. 2026, Work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-irtf-cfrg-bbs-blind-signatures/05/

[KLS18] E. Kiltz, V. Lyubashevsky, and C. Schaffner, "A concrete treatment of Fiat-Shamir signatures in the quantum random-oracle model," in *Advances in Cryptology – EUROCRYPT 2018, Part III*, J. B. Nielsen and V. Rijmen, Eds., ser. Lecture Notes in Computer Science, vol. 10822, Tel Aviv, Israel: Springer, Cham, Switzerland, Apr. 2018, pp. 552–586.

[KPG99] A. Kipnis, J. Patarin, and L. Goubin, "Unbalanced Oil and Vinegar signature schemes," in *Advances in Cryptology – EUROCRYPT'99*, J. Stern, Ed., ser. Lecture Notes in Computer Science, vol. 1592, Prague, Czech Republic: Springer Berlin Heidelberg, Germany, May 1999, pp. 206–222.

[LinkedIn26] LinkedIn. "Verifications on your LinkedIn profile," last visited: Oct. 27, 2026. [Online]. Available: https://www.linkedin.com/help/linkedin/answer/140551

[LKW+26] T. Looker, V. Kalos, et al., "The BBS signature scheme," Internet Research Task Force, Internet-Draft draft-irtf-cfrg-bbs-signatures-14, Oct. 2026, Work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-irtf-cfrg-bbs-signatures/14/

[LM06] V. Lyubashevsky and D. Micciancio, "Generalized compact Knapsacks are collision resistant," in *ICALP 2006: 33rd International Colloquium on Automata, Languages and Programming, Part II*, M. Bugliesi, B. Preneel, et al., Eds., ser. Lecture Notes in Computer Science, vol. 4052, Venice, Italy: Springer Berlin Heidelberg, Germany, Jul. 2006, pp. 144–155.

[LNP22] V. Lyubashevsky, N. K. Nguyen, and M. Plançon, "Lattice-based zero-knowledge proofs and applications: Shorter, simpler, and more general," in *Advances in Cryptology – CRYPTO 2022, Part II*, Y. Dodis and T. Shrimpton, Eds., ser. Lecture Notes in Computer Science, vol. 13508, Santa Barbara, CA, USA: Springer, Cham, Switzerland, Aug. 2022, pp. 71–101.

[LPR10] V. Lyubashevsky, C. Peikert, and O. Regev, "On ideal lattices and learning with errors over rings," in *Advances in Cryptology – EUROCRYPT 2010*, H. Gilbert, Ed., ser. Lecture Notes in Computer Science, vol. 6110, French Riviera: Springer Berlin Heidelberg, Germany, May 2010, pp. 1–23.

[LS15] A. Langlois and D. Stehlé, "Worst-case to average-case reductions for module lattices," *Designs, Codes and Cryptography*, vol. 75, no. 3, pp. 565–599, 2015.

[Lyu09] V. Lyubashevsky, "Fiat-Shamir with aborts: Applications to lattice and factoring-based signatures," in *Advances in Cryptology – ASIACRYPT 2009*, M. Matsui, Ed., ser. Lecture Notes in Computer Science, vol. 5912, Tokyo, Japan: Springer Berlin Heidelberg, Germany, Dec. 2009, pp. 598–616.

[Lyu24] V. Lyubashevsky, *Basic lattice cryptography: The concepts behind Kyber (ML-KEM) and Dilithium (ML-DSA)*, Cryptology ePrint Archive, Report 2024/1287, 2024. [Online]. Available: https://eprint.iacr.org/2024/1287

[META26] Meta. "New AI-powered age assurance measures to place teens in age-appropriate experiences," last visited: Oct. 27, 2026. [Online]. Available: https://about.fb.com/news/2026/05/ai-age-assurance-teens/

[NISCG25] NIS Cooperation Group, "A coordinated implementation roadmap for the transition to post-quantum cryptography," European Commission, Roadmap Part 1, Version 1.1, Jun. 2025. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

[NIST26] G. Alagic, M. Bros, et al., "Status report on the second round of the additional digital signature schemes for the NIST post-quantum cryptography standardization process," National Institute of Standards and Technology, Gaithersburg, MD, NIST Internal Report NIST IR 8610, May 2026. [Online]. Available: https://csrc.nist.gov/pubs/ir/8610/final

[PR06] C. Peikert and A. Rosen, "Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices," in *TCC 2006: 3rd Theory of Cryptography Conference*, S. Halevi and T. Rabin, Eds., ser. Lecture Notes in Computer Science, vol. 3876, New York, NY, USA: Springer Berlin Heidelberg, Germany, Mar. 2006, pp. 145–166.

[Reg05] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," in *37th Annual ACM Symposium on Theory of Computing*, H. N. Gabow and R. Fagin, Eds., Baltimore, MA, USA: ACM Press, May 2005, pp. 84–93.

[RFC9474] F. Denis, F. Jacobs, and C. A. Wood, "RSA blind signatures," RFC Editor, RFC 9474, Oct. 2023. [Online]. Available: https://www.rfc-editor.org/rfc/rfc9474.txt

[RFC9901] D. Fett, K. Yasuda, and B. Campbell, "Selective disclosure for JSON web tokens," RFC Editor, RFC 9901, Nov. 2025. [Online]. Available: https://www.rfc-editor.org/rfc/rfc9901.txt

[RSA78] R. L. Rivest, A. Shamir, and L. M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the Association for Computing Machinery*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[Sho94] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *35th Annual Symposium on Foundations of Computer Science*, Santa Fe, NM, USA: IEEE Computer Society Press, Nov. 1994, pp. 124–134.

[ST24] O. Sanders and J. Traoré, "Compact issuer-hiding authentication, application to anonymous credential," *Proceedings on Privacy Enhancing Technologies*, vol. 2024, no. 3, pp. 645–658, Jul. 2024.

[TFC26] O. Terbu, D. Fett, and B. Campbell, "SD-JWT-based verifiable digital credentials (SD-JWT VC)," Internet Engineering Task Force, Internet-Draft draft-ietf-oauth-sd-jwt-vc-26, Nov. 2026, Work in progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-oauth-sd-jwt-vc/26/

[TikTok25] TikTok. "How TikTok is complying with a new government law in Australia," last visited: Oct. 27, 2026. [Online]. Available: https://newsroom.tiktok.com/how-tiktok-is-complying-with-a-new-government-law-in-australia?lang=en-AU

[TZ23] S. Tessaro and C. Zhu, "Revisiting BBS signatures," in *Advances in Cryptology – EUROCRYPT 2023, Part V*, C. Hazay and M. Stam, Eds., ser. Lecture Notes in Computer Science, vol. 14008, Lyon, France: Springer, Cham, Switzerland, Apr. 2023, pp. 691–721.

[Wes26] B. Westerbaan. "Cloudflare targets 2029 for full post-quantum security," Cloudflare, last visited: Nov. 10, 2026. [Online]. Available: https://blog.cloudflare.com/post-quantum-roadmap/

[YLBH25] K. Yasuda, T. Lodderstedt, et al., "OpenID4VC High Assurance Interoperability Profile 1.0," OpenID Foundation, Final Specification, Dec. 2025. [Online]. Available: https://openid.net/specs/openid4vc-high-assurance-interoperability-profile-1_0.html

[ZSE+24] X. Zhang, R. Steinfeld, et al., "Loquat: A SNARK-friendly post-quantum signature based on the Legendre PRF with applications in ring and aggregate signatures," in *Advances in Cryptology – CRYPTO 2024, Part I*, L. Reyzin and D. Stebila, Eds., ser. Lecture Notes in Computer Science, vol. 14920, Santa Barbara, CA, USA: Springer, Cham, Switzerland, Aug. 2024, pp. 3–38.