



EÖTVÖS LORÁND UNIVERSITY

FACULTY OF INFORMATICS

DEPT. OF SOFTWARE TECHNOLOGY AND METHODOLOGY

P2P Cooperative System to combat double spending with Lattice-based blind signatures

Supervisor:

Dr. Péter Kutas

Associate Professor

Author:

Bhardwaj Aditya

Computer Science MSc Cybersecurity

Budapest, 2024

Abstract

Blind signatures were first introduced by David Chaum. They allow a user to have a message signed by a signer without revealing the message itself. This property is particularly useful in applications such as electronic voting and digital cash, where user anonymity is important. In a blind signature scheme, the user blinds their message before sending it to the signer, who signs the blinded message. The user then unblinds the signed message to obtain a valid signature that can be verified publicly, ensuring that the signer cannot trace the signed message back to the original unblinded version. A good analogy is placing the message inside an envelope and having the envelope signed. Once the envelope is opened, the signature remains valid for the enclosed message, ensuring that the content remains confidential.

Such constructions provide anonymity and privacy to the user but given a practical quantum computer, the security of traditional cryptosystems providing such features will be broken. To address this, the development of quantum-resistant cryptographic protocols is essential for maintaining the security of digital transactions and data. Aligning with the same goal, this thesis aims to thoroughly review the background of lattice-based blind signatures and then look at a scheme for *ecash* or digital cash, which we can adopt for providing post-quantum security.

Contents

Acknowledgements	3
1 Introduction	4
1.1 Objective of the thesis	5
1.2 Outline of the thesis	7
2 Digital Signatures	8
2.1 Applications	9
2.2 Digital signature scheme	9
2.3 Security of Digital Signatures	10
2.4 Hashing	10
2.5 Computational Hard Problems	11
2.6 Digital Signature schemes	12
2.6.1 RSA Digital Signature scheme	12
2.6.2 DSA Digital Signature scheme	13
2.6.3 ECDSA	14
2.7 Security	16
3 Blind Signatures	19
3.1 Blind signature scheme	20
3.2 Security	21
3.3 Evolution of blind signature schemes	22
3.4 Blind signature schemes	23
3.4.1 RSA-FDH Blind signature	23
3.4.2 DLP based blind Schnorr signatures	24
3.5 Other types of blind signatures	26
3.6 Security models and Attacks	27
3.6.1 Random Oracle Model (ROM)	27

3.6.2	Standard Model	28
3.6.3	Common Reference String model	29
3.6.4	ROS Attack	30
4	Lattice-based Signatures	32
4.1	Basics	32
4.2	Hard problems in Lattices	34
4.3	Lattice-based cryptography	35
4.4	Lattice trapdoors	39
4.5	Signatures	40
4.5.1	Hash-and-Sign	40
4.5.2	Fiat-Shamir	41
5	Lattice-based blind signatures	43
5.1	State of the art	43
5.2	Round optimal lattice-based signature	45
5.2.1	Intuition	45
5.2.2	Building blocks	46
5.2.3	Construction	49
5.2.4	Extension to partially blind signature	50
5.3	Comparison to pre-quantum blind signatures	51
5.4	Application - electronic cash (eCash)	52
5.4.1	P2P system for tackling double spending	52
5.4.2	Lattice-based eCash	54
5.4.3	Peer-to-peer system based eCash	56
6	Conclusion	58
	Bibliography	60

Acknowledgements

I learnt a lot of things while I was writing the thesis. I would like to thank my supervisor Dr. Péter Kutas who guided me along the way and cleared all my doubts. My parents were very supportive of me and made sure I could focus solely on my studies. Lastly I would like to thank ELTE for giving me the opportunity to study and my friends, who stayed by my side all the time.

Chapter 1

Introduction

Public-key cryptography which is another name for asymmetric cryptography, is at the heart of current communication systems. In symmetric cryptography, both sides - sender and receiver, share the same secret key. In public-key cryptography, on the other hand, there are two keys, one public and one private. This allows anyone to encrypt messages with the public key, but only the holder of matching private key can decrypt them. Many security protocols are based on this method, which makes sure that communication over unprotected channels like the Internet is safe, confidential and authenticated. Transport Layer Security (TLS), Secure Shell protocol (SSH), IPSec, Pretty Good Privacy (PGP) are some of the well-known protocols that employ public-key encryption in their schemes.

In the year 1983, public-key cryptography was still in its early days when David Chaum devised eCash [1] in his paper titled *Blind Signatures for Untraceable Payments*. The goal was to create an electronic form of cash that would have the same privacy and secrecy as real cash. This notion was revolutionary, particularly during this time of the internet when public-key cryptography was being developed. To realize this idea, he introduced *blind* signatures, a form of digital signature in which the content of a message is blinded or hidden from the signer before it is signed. Hence, in the context of eCash, a masked digital cash token is made during token generation and is then signed by a bank. While the blind signature confirms that the token is authentic and is indeed signed by the bank, the signer doesn't see the message content. The person then *unblinds* or unmask the token, which shows the original digital token that was signed. This process protects privacy and security by enabling transactions without being able to link the person to the original

token. In e-voting systems [2], blind signatures are used to maintain voter privacy by allowing ballots to be signed without revealing the voter's choices. In credential systems [3], it helps users prove credentials without revealing themselves, addressing privacy concerns in access control systems.

The basis of security in public key cryptography today largely relies on the computational difficulty of certain mathematical problems like the *Integer Factorization Problem* or *Discrete Logarithm Problem*. These problems are already broken theoretically by Shor algorithm [4] but it assumes a quantum computer free of noise and error, which is still largely not practical. Given the current computing technology that includes both classical and current quantum computing capabilities, it still remains infeasible to solve these problems (for the relevant parameters) within a reasonable frame of time. One can still not downplay the threat which is posed by the continuous advancements in quantum computing. It is necessary to create new cryptographic algorithms and modify existing ones to maintain continuous security. Post-quantum cryptography is a field that deals with cryptographic problems that are considered to be resistant to attacks from quantum computers.

In 2016, NIST [5] started a process to assess, and standardize a few public-key cryptography algorithms that are based on such problems. The objective was to standardise algorithms that are resistant to attacks from both classical and quantum computers. In 2022, four algorithms were selected for the standardization - CRYSTALS-Kyber [6], CRYSTALS-Dilithium [7], SPHINCS+ [8] and FALCON [9]. While CRYSTALS-Kyber is a key encapsulation mechanism, the others are digital signature schemes. Out of these four algorithms, three are based on lattice-based cryptography which is the focus of this thesis. Lattice structure are discrete sets of points in multidimensional space formed by linear combinations of vectors called a *basis*. For the majority of real-world applications, lattice-based cryptography's overall performance is adequate and can develop powerful tools for key exchange, homomorphic encryption, attribute-based encryption, signatures and hash functions.

1.1 Objective of the thesis

There are different approaches to post-quantum cryptography and these are Lattice-based, code-based, multivariate-based, hash-based, isogeny-based, and hash-based schemes. Their security is based on different mathematical problems that are

believed to be resistant to quantum attacks. This thesis focuses on lattice-based cryptography which is one of the most potential PQC candidates due to its advantages [10]:

- Strong security: Ajtai [11] gave the worst-case to average-case reduction for lattice problems. It states that a ‘randomly chosen instance of a certain lattice problem is at least as hard as the worst-case instance of a related lattice problem’. The two hard problems in lattice, Shortest Vector Problem SVP and CVP are shown to be NP-hard and moreover, the underlying structure of lattice-cryptography work in high dimensions, which can be several hundreds or thousands.
- Performance: Lattice-based schemes are on par with the current public key algorithms. Even though lattice-based cryptography creates larger keys than of RSA and ECC schemes, it has a balanced performance and efficiency compared to other post-quantum cryptosystems. And works [12], [13] by researchers like Gentry, Vaikuntanathan, Lyubashevsky, Chris Peikert have provided us efficient lattice-based constructions for a wide variety of applications.

Since Ruckert et al. [14] gave the first lattice-based blind signature in 2010, constructions have also been given for specific scenarios including group, ring, blind, and proxy signatures. The main topic of this thesis is lattice-based blind signatures and the objectives are as follows:

- Give an overview of lattice-based cryptography and the main construction tools available.
- Review the recent lattice-based blind signature schemes and the new security assumptions they are based on.
- Study some recent attacks and list the schemes affected by these attacks
- Describe the construction of the first blind signature scheme to have a formal security proof in the quantum random oracle model
- Review the approaches that tackle the problem of double-spending in electronic cash and briefly evaluate their feasibility if lattice-based blind signatures are used.

1.2 Outline of the thesis

We briefly discussed about public-key cryptography and then blind signatures, where the signer signs on a message without seeing the message itself. The underlying security of today's digital infrastructure relies on the fact that some mathematical problems are hard to solve (in a feasible amount of time). A practical and strong enough quantum computer could pose a threat to the same and hence development of post-quantum cryptography is evident.

The goal of the thesis is to familiarize the reader with blind signatures and then discuss the construction of a lattice-based blind signature scheme finally. We talk briefly about digital signatures in Chapter 2. In Chapter 3, we discuss blind signatures in a little detail along with *ROS* problem. Lattice-based cryptography is one of the techniques that use the mathematical structure of lattices. Some problems in lattices are proven to be resistant against quantum attacks. We discuss these and the construction of lattice-based signatures in Chapter 4. Finally we discuss the state of the art in lattice-based blind signatures in Chapter 5 and understand the construction of the scheme given by del Pino and Katsumata et al. [15].

Chapter 2

Digital Signatures

Until the mid-1970s, all cipher systems used symmetric cryptography. In this system, a single key is used to encrypt and decrypt the data. The private or secret key must be known to both sender and receiver. While this is fast and efficient, for n parties, this involves $n(n - 1)$ keys to be distributed. If an eavesdropper intercepts the key using transmission, they can decrypt and see the messages which brings us to the issue of authentication and trust between the communicating parties. In 1976, Whitfield Diffie and Martin Hellman introduced the concept of public key cryptography in their landmark paper “New Directions in Cryptography,” [16]. (they were influenced by Merkle’s work [17] who discussed about secure transmission of keys in insecure channel but was not practical). They proposed the idea of a private key and a corresponding public key which allows the parties to establish a shared secret-key over insecure channel; this is known as the Diffie-Hellman key exchange. Along with asymmetric key cryptography, Diffie and Hellman were also the first one to give the notion of digital signature scheme.

Like paper-based signatures, digital signatures could provide two guarantees: *Authentication*, that a message came from the right person and *Non – repudiation*, that a signer of a message cannot deny and claim they did not sign it. Diffie and Hellman had conjectured that such schemes use one-way functions but it was still unknown whether such functions exist. It was in 1978 when Rivest, Shamir and Adleman gave the construction of first digital signature scheme which was based on the RSA public-key cryptosystem [18]. It’s security lies in the extreme difficulty of factoring large integers and the modular exponentiation function works as the one-way function.

2.1 Applications

A digital signature algorithm enables an entity to verify both the integrity of signed data and the identity of the signer. When receiving a signed message, the recipient can present the digital signature as proof to a third party that it indeed originated from the intended signer. This concept, known as non-repudiation, prevents the signer from easily disowning the signature afterward. Digital signature algorithms find application in various domains, including electronic mail, electronic funds transfer, electronic data interchange, software distribution, data storage, and other contexts where ensuring data integrity and authenticating data origin are essential. In a practical setting, digital certificates are used in Public Key Infrastructure (PKI) which helps establish trustworthiness among the entities (users, devices and networks). Digital certificates act as a proof of ownership of a public key which also contains other information about the entity along with digital signature. PKI sets policies, roles and creates, distributes and can revoke (if needed) these digital certificates. It is the underlying infrastructure which allows safe communication (TLS protocol), secure e-mail (PGP) or digital signing of applications or software.

NIST publishes Federal Information Processing Standard (FIPS) in which they also share the schemes that can be used for generation and verification of digital signature so as to promote secure, interoperable, and standardized technologies. The three algorithms are Rivest-Shamir-Adleman (RSA) Algorithm, Elliptic Curve Digital Signature Algorithm (ECDSA) and Edwards Curve Digital Signature Algorithm (EdDSA) [19].

2.2 Digital signature scheme

A digital signature scheme typically consists of three algorithms (*KeyGen*, *Sign*, *Verify*), they are as follows:

***KeyGen*(k)** With an input parameter k , this algorithm generates a private key which is selected from a set of possible private keys. We get the pair of cryptographic keys (sk, pk) where sk is the private key and pk is the corresponding public key pk . We can denote it as $\text{KeyGen}(k) \rightarrow (sk, pk)$

***Sign*(m, sk)** Given the message m and private key sk as the input, signing algorithm generates the signature π . This is denoted as $\text{Sign}(m, sk) \rightarrow \pi$

Verify(m, π, pk) Finally, this deterministic algorithm takes as input a message m , the signature π to verify and the public key pk . It returns true or bit 1 if (m, π) is a valid message-signature pair. Otherwise, the signature is rejected and algorithm returns false or 0 bit. We can denote it as $\text{Verify}(m, \pi, pk) \rightarrow (true/false)$.

2.3 Security of Digital Signatures

Unforgeability is a fundamental security property of digital signature schemes, ensuring that for a public key pk , only the legitimate signer S can create valid signatures σ for a given message m . It guarantees that no adversary can forge a signature on a new message even with knowledge of other signed messages (given by the signer S). For the formal definition of security, we refer to [20]. Let the signature scheme be $\Pi = (\text{Gen}, \text{Sign}, \text{Vrfy})$. For an adversary \mathcal{A} and given parameter n , the signature experiment $\text{Sig-forge}_{\mathcal{A}, \Pi}(n)$ is as follows:

1. $\text{Gen}(1^n) \rightarrow \text{key pair } (pk, sk)$.
2. Given pk and access to an oracle $\text{Sign}_{sk}(\cdot)$, the goal of the adversary \mathcal{A} is to generate the message-signature pair (m, σ) for the message m which he has not queried to the signing oracle $\text{Sign}_{sk}(\cdot)$ before. Let \mathcal{Q} represent all queries that \mathcal{A} sent to the oracle.
3. \mathcal{A} wins this experiment if $m \notin \mathcal{Q}$ and $\text{Vrfy}_{pk}(m, \sigma) = 1$ i.e. (m, σ) is a valid pair. In this case the output of the experiment is defined to be 1 and otherwise 0.

We summarize this discussion in the following definition ([20, Definition 12.2]):

Definition 1. A signature scheme $\Pi = (\text{Gen}, \text{Sign}, \text{Vrfy})$ is existentially unforgeable under an adaptive chosen-message attack, or just secure, if for all probabilistic polynomial-time adversaries \mathcal{A} , there is a negligible function negl such that:

$$\Pr \left[\text{Sig-forge}_{\mathcal{A}, \Pi}(n) = 1 \right] \leq \text{negl}(n).$$

2.4 Hashing

In digital signatures, hashing is used to convert long-arbitrary message input into a fixed length value called hash. In digital signature schemes, we sign the hash value rather than the message itself. The entity that receives the message and the

corresponding signature, first derives the message's hash and then confirms if the provided signature is valid for the hash value.

Definition 2. For an arbitrary input, a hash function is a function H that gives us a fixed-length output. This is simply called the *hash* or the message *digest*. We can denote the hash function H as:

$$y = H : \{0, 1\}^* \rightarrow \{0, 1\}^k$$

where k denotes the length of the output.

Along with the above property of input-compression, it is desirable to have the following properties:

1. Fast and Ease of computation: It should be easy to compute the hash $H(x)$ for an input x .
2. Preimage resistance: Given a hash value h , it should be computationally infeasible to find any input x such that $H(x) = h$.
3. Second Pre-image resistance: For any given input x_1 , it should be computationally infeasible to find another input x_2 such that $H(x_1) = H(x_2)$.
4. Collision Resistance: It should be computationally infeasible to find two inputs x_1, x_2 where $x_1 \neq x_2$ and $H(x_1) = H(x_2)$.

2.5 Computational Hard Problems

There are computational tasks for which we (yet) do not have efficient algorithms to solve them in polynomial time. Number theory presents us these problems [21] where the amount of computational resources (such as time and memory) required to solve them grows exponentially with the size of the input. The most widely used problems which are used in the construction of public-key cryptosystems and hence signature schemes are as follows:

1. Integer Factorization Problem (IFP): This problem is the basis of the popular algorithms like RSA [18] and Rabin [22]. It is as following: given a positive integer n , find the prime factorization with the components e_i and p_i such as

$$N = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$$

where p_i are the prime numbers and $e_i \geq 1$. This problem is computationally difficult for large numbers with hundreds or thousands of digits.

2. The Discrete Logarithm Problem (DLP): It involves finding an integer x such that $g^x = h$, where g is a generator of a finite cyclic group G of order p , and h is an element in G . The security of several cryptographic protocols, such as the Diffie-Hellman (DH) key exchange, Digital Signature Algorithm (DSA), and ElGamal encryption relies on the assumption that the DLP is computationally difficult to solve.
3. Elliptic Curve Discrete Logarithmic Problem (ECDLP): Given an elliptic curve point P , a generator point G , and a prime p , find k such that $P = k \cdot G$ in the elliptic curve group over \mathbb{F}_p . The integer k , denoted as $k = \log_P Q$, is called the discrete logarithm of P and is hard to find. The elliptic curve variant schemes, Elliptic Curve Diffie-Hellman (ECDH) and Elliptic Curve Digital Signature Algorithm (ECDSA) are some schemes whose security rely on this problem.

2.6 Digital Signature schemes

Now we describe some of the most notable digital signature schemes namely RSA (named after the authors Rivest–Shamir–Adleman) and Digital Signature Algorithm (DSA). While RSA is based on the integer factorization problem, DSA relies on the discrete logarithm problem.

2.6.1 RSA Digital Signature scheme

Key generation

To set up the RSA signature scheme and create signatures, Alice (the signer) needs to generate her pair of public and private key. She chooses two large prime numbers, p and q , and computes the product $n = pq$, the *modulus*. Alice also calculates the Euler's totient $\phi(n) = (p - 1)(q - 1)$.

While the modulus n is published as a part of the public key, $\phi(n)$ is kept secret. Alice selects an integer e which is co-prime to $\phi(n)$, it means $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$. This integer e is also part of the public key. Alice finally computes

the private exponent d such that $d \equiv e^{-1} \pmod{\phi(n)}$ or $de \equiv 1 \pmod{\phi(n)}$. This means d is the modular inverse of e modulo $\phi(n)$.

The public key is (e, n) and the private key is (d, n) .

Signing

Given a message m and her private key (d, n) , Alice first calculates the hash or the message digest $h \leftarrow H(m)$ where $H(m)$ is a hash function. With the private exponent d , she generates the signature $s : s \leftarrow h^d \pmod{n}$.

Alice can now send the message m along with the signature s to Bob (the verifier).

Verification

Bob has Alice's public key (e, n) . Given the message-signature pair (m, s) , he computes the hash value h of the message m . He computes $s^e \pmod{n}$ to get h' i.e. $h' \leftarrow s^e \pmod{n}$ and can check if $h = h'$. If they match, Bob concludes that the signature s is valid and the message m was indeed signed by Alice.

This is because:

$$h' = s^e \pmod{n} = (h^d)^e \pmod{n} = h$$

2.6.2 DSA Digital Signature scheme

Key generation

The key generation phase has two parts. First the parameters are selected and then the key pair is generated. Digital Signature Standard (DSS) [23] specifies the parameter choices. A prime number p is chosen such that $p - 1$ is a multiple of a large prime q . DSS has specified the length of p and q as well. For example if prime q is of 256-bit length, then p can be a 2048-bit or a 3072-bit prime. Also, a generator g of the subgroup of order q in \mathbb{Z}_p^* is taken.

To generate the private and public keys, Alice generates a random integer x from $\{1, q - 1\}$. This is her private key. She computes the public key as $y = g^x \pmod{p}$.

Signing

The signature of a message m consists of the pair of numbers r and s .

Alice chooses a random integer k from $\{1, q-1\}$ and then computes $r = (g^k \bmod p) \bmod q$. If $r = 0$, she chooses a different k . Alice calculates the hash value $h \leftarrow H(m)$ and then $s = k^{-1}(h + xr) \bmod q$. She finally publishes the message m and signature (r, s) .

Verification

Bob obtains (p, q, g, y) which contains Alice's public key and public parameters. Given the message m and signature (r, s) , he computes the hash value $h \leftarrow H(m)$ and $w = s^{-1} \bmod q$.

Bob calculates $u_1 = h \cdot w \bmod q$ and $u_2 = r \cdot w \bmod q$. He computes $v = ((g^{u_1} \cdot y^{u_2}) \bmod p) \bmod q$. If $v = r$, the signature is valid; otherwise, it's invalid.

This is because

$$\begin{aligned} (g^{u_1} \cdot y^{u_2}) \bmod p &= (g^{hw} \cdot y^{rw}) \bmod p \\ (g^{u_1} \cdot y^{u_2}) \bmod p &= (g^{hw} \cdot (g^x)^{rw}) \bmod p \\ (g^{u_1} \cdot y^{u_2}) \bmod p &= (g^{hw+xrw}) \bmod p \end{aligned}$$

Just taking the exponent, the value is

$$hw + xrw = w(h + xr)$$

Earlier we saw that $w = s^{-1} \bmod q$. Then

$$\begin{aligned} w(h + xr) &= s^{-1}(h + xr) \bmod q \\ w(h + xr) &= k \cdot (h + xr)^{-1}(h + xr) \bmod q \\ &= k \bmod q \end{aligned}$$

Hence $(g^{hw+xrw}) \bmod p = (g^k \bmod p) \bmod q = r$

2.6.3 ECDSA

Elliptic Curve Digital Signature Algorithm (ECDSA) is the elliptic curve variant of DSA. Both signer and verifier, agree on some parameters that define the elliptic curve. NIST publishes their recommendation for such curves and parameters [24].

Key generation

To generate the key pair and send signed messages, Alice and Bob first decide on the domain parameters, these are as follows:

- p , a large prime number
- coefficients a and b defining the elliptic curve E
- $G = (x_G, y_G)$ a base point on the curve E that generates the subgroup
- n , the order of this subgroup

Alice selects a random integer d from $\{1, n - 1\}$. This will be her private key. She computes the public key $Q = d \cdot G$.

Signing

Alice first generates a random integer k from $\{1, n - 1\}$ and calculates the curve point $P = k \cdot G = (x_P, y_P)$. She calculates $r = x_P \bmod n$ and $s = k^{-1}(h + dr) \bmod n$, where $h \leftarrow H(m)$ is the hash of the message m and d is her private key. Alice publishes the signature pair (r, s) .

Verification

Given Alice's public key Q , the base point G , the message m and the signature pair (r, s) , Bob first computes $w = s^{-1} \bmod n$ and hash value $h \leftarrow H(m)$.

Bob calculates $u_1 = hw \bmod n$ and $u_2 = rw \bmod n$ and computes the elliptic curve point in the following way:

$$(x_2, y_2) = u_1 G + u_2 Q$$

The signature is valid if $r \equiv x_2 \bmod n$, otherwise it's invalid.

Correctness

We recall that $w = s^{-1} \bmod n$ and Bob computed $u_1 = hw \bmod n$ and $u_2 = rw \bmod n$. Substituting w in the equations of u_1, u_2 :

$$u_1 = hs^{-1} \bmod n \quad \text{and} \quad u_2 = rs^{-1} \bmod n$$

$$(x_2, y_2) = (hs^{-1})G + (rs^{-1})Q$$

Since $Q = d \cdot G$, this becomes:

$$(x_2, y_2) = (hs^{-1})G + (rs^{-1})dG = (hs^{-1} + rds^{-1})G$$

Take the expression inside the parenthesis:

$$x_2 \equiv (hs^{-1} + rds^{-1}) \pmod{n} \equiv ((h + rd)s^{-1}) \pmod{n}$$

During signing step, computed :

$$s = k^{-1}(h + dr) \pmod{n} \Rightarrow k \equiv (h + rd)s^{-1} \pmod{n}$$

Therefore:

$$x_2 \equiv k \cdot G \pmod{n}$$

$$x_2 \equiv r \pmod{n}$$

2.7 Security

Security level (bits)	RSA	Elliptic Curve - ECDSA, EdDSA
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

Table 2.1: Key-size (bits) for same level of security. Selections in bold are recommended by NIST

Table 2.1 shows the security provided by the schemes RSA and elliptic curve based ECDSA and EdDSA. When we say that a scheme provides security level of 128 bits, it refers to the brute-force attack where the adversary would need 2^{128} operations to succeed. NIST guidance says that “*the use of keys that provide less than 112 bits of security strength for key agreement is now disallowed*” [25].

The security of RSA relies on the hardness of factoring integers. If the attacker can successfully factor the public modulus $N = pq$ available in the public key, they can compute the private key as well. Finding the prime factors p and q appears to be

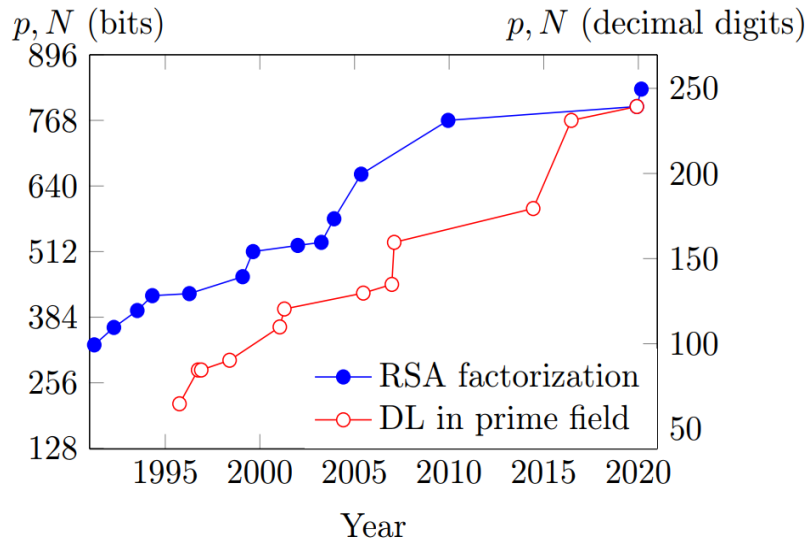


Figure 2.1: Current RSA and DL breaking records [26]

the logical approach in breaking RSA but there might be ways of decrypting RSA ciphertexts or forging RSA signatures without factorization. Hence we know that this RSA problem is as easy as factoring and not vice-versa.

In practice, cryptographic algorithms use *semiprime* (product of two prime numbers), whose factors are similar in size. These are the most difficult to factor. Figure 2.1 shows the current factoring and discrete logarithm records. In 2020, [27] showed the factoring of RSA-250, a 829-bit number and before this, [28] completed factorization of RSA-240, a 795-bit number, and a discrete logarithm computation over a 795-bit prime field. The authors used the *Number Field Sieve* algorithm to achieve the same in both the cases.

There are classical algorithms to factor numbers if their prime factors have *certain* forms. For example Pollard $p - 1$ algorithm can find a factor p of an integer if the $p - 1$ value has small prime factors. Some other algorithms are Pollard's *rho* and Fermat's factorization [26]. These types of algorithms are applied before general purpose algorithms because cryptographic constructions avoid usage of such numbers of *certain* forms or characteristics .

Number Field Sieve (NFS) algorithm is an example of general purpose algorithms where the running time depends solely on the size of integer to be factored. Continued fraction factorization and Quadratic sieve are some of other examples of general purpose factoring algorithms.

The current fastest algorithm is the *General Number Field Sieve* (GNFS), and

it runs in approximately

$$O\left(\exp\left(\frac{64}{9}n^{1/3}(\log n)^{2/3}\right)\right)$$

time, where n refers to bits used to represent the number. Shor's algorithm [4] runs in

$$O\left((\log n)^2 \cdot \log \log n\right)$$

time [29]. Even though Shor's algorithm presents an attack in polynomial time, it assumes a quantum computer free of noise and errors which is still a practical challenge.

In elliptic-curve based cryptography, Pollard *rho* or baby-step giant-step method are some of the most efficient algorithms for solving ECDLP problem and needs $O(\sqrt{n})$ steps to solve, where n is the order of the group. The size of the underlying field should be roughly twice the security parameter. For example, for 128-bit security one needs a 256-bit elliptic curve. In contrast, the size of key in RSA would be 3072 bits for the same level of security. Elliptic-curve based schemes offer shorter keys and hence, are widely used for protocols and cryptographic constructions. Choice of *weaker* implementations of curve can affect the security and hence NIST Digital Signature Standards [23] contains recommendations for curves that are chosen for efficiency and optimal security.

Chapter 3

Blind Signatures

Blind signatures are an extension of digital signatures, which allows a user to obtain a signature on a message without revealing the contents of the message to the signer. A good analogy to blind signatures is electronic voting. Though there are other security factors in implementations of e-voting in the real world [30], the one logically desired property in such scheme is anonymity i.e. the election authority should not be able to view any information about the votes.

To have a better idea, we describe the simple RSA blind signature scheme, a user who wants a message signed first blinds the message by multiplying it with a random blinding factor, r , raised to the public exponent, e , modulo the RSA modulus, n . This blinded message, $m' = m \cdot r^e \pmod n$, is sent to the signer. The signer, unaware of the original message, signs the blinded message using their private key, d , resulting in $s' = (m')^d \pmod n$. The user then receives the blinded signature, s' , and removes the blinding factor by computing $s = s' \cdot r^{-1} \pmod n$, where r^{-1} is the modular inverse of r . The result, s , is a valid RSA signature on the original message m , ensuring the user's message is signed without revealing the message to the signer, thus maintaining the user's privacy.

The correctness for the signature s is as follows:

$$\begin{aligned} s &= (m \cdot r^e)^d \cdot r^{-1} \pmod n \\ &= m^d \cdot (r^e)^d \cdot r^{-1} \pmod n \\ &= m^d \cdot r^{ed} \cdot r^{-1} \pmod n \\ &= m^d \cdot r^1 \cdot r^{-1} \pmod n \quad (\text{since } ed \equiv 1 \pmod{\phi(n)}) \\ &= m^d \cdot r \cdot r^{-1} \pmod n = m^d \pmod n \end{aligned}$$

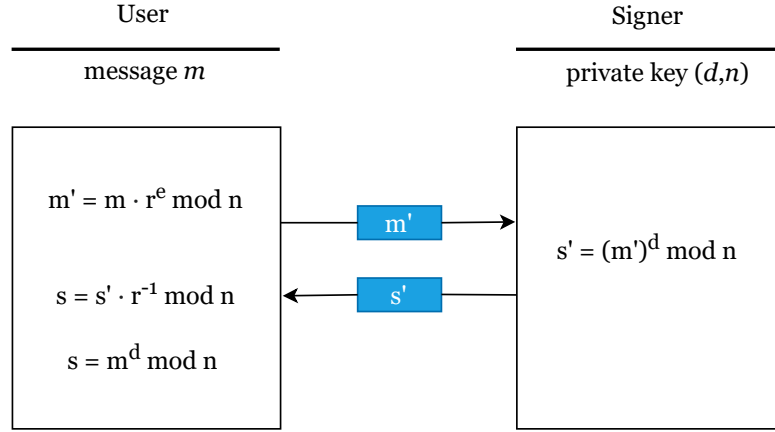


Figure 3.1: RSA blind signatures

Thus, s is indeed $m^d \bmod n$, which is the standard RSA signature of the original message m .

3.1 Blind signature scheme

According to [1], a blind signature scheme Π_{BS} consists of three algorithms ($KeyGen$, $Sign$, $Verify$) and two parties, the user U and the signer S :

$KeyGen(k)$ It takes a security parameter k as the input and generates a pair (pk, sk) as the output. sk is the private key and pk is the corresponding public key. We can denote this as $KeyGen(k) \rightarrow (sk, pk)$

$Sign(m, sk)$ This is an interactive and probabilistic polynomial time protocol between the user and signer where the user U intends to get the signature π on a message m from the signer S . The user blinds the message m to get m' and sends it to the signer. With the private key pk , signer signs on m' , obtains π' and sends it to the user. The user U now unblinds π' to get π , the blind signature on message m . This is denoted as $Sign(m, sk) \rightarrow \pi$

$Verify(m, \pi, pk)$ This deterministic algorithm takes as input a message m , the signature π to verify and the public key pk . It returns *true* or 1 if (m, π) is a valid message-signature pair. Otherwise, the signature is rejected and algorithm returns *false* or 0. We can denote it as $Verify(m, \pi, pk) \rightarrow (accept/reject)$

3.2 Security

The example of simple RSA blind signature which we saw earlier, is not secure. An adversary can use the blind signature process to trick a signer into decrypting a RSA ciphertext. An adversary, who has an encrypted message $c = m^e \bmod n$ and wants to decrypt it, can choose a random blinding factor r and compute the blinded message $c' = c \cdot r^e \bmod n$. The adversary then presents c' to the signer for a blind signature. The signer, unaware that c' is related to c , signs c' using their private key d , resulting in $s' = (c')^d \bmod n$. The adversary receives s' , and by removing the blinding factor, computes $s = s' \cdot r^{-1} \bmod n$. Since $s' = (c \cdot r^e)^d \bmod n = m \cdot r \bmod n$, removing r reveals m , effectively decrypting the original message c .

Moreover, an adversary who wants to forge signature on a message m can do so by requesting signatures for two other messages

$$\begin{aligned} m_1 &\bmod n \\ m \cdot m_1^{-1} &\bmod n \end{aligned}$$

With their respective signatures s_1 and s_2 , he can compute $s = s_1 \cdot s_2 \bmod n$ to obtain signature s for the message m .

We see the secure version of RSA blind signature scheme in the section 3.4.1 where the hash or *digest* of the message m is signed. A secure blind signature scheme must satisfy the following three requirements [31]:

Correctness: The blind signature verification algorithm $\text{Verify}(m, \pi, pk)$ will always accept the signature π if both, the signer S and the user U follow the signature generation correctly i.e. $\text{Verify}(m, \pi, pk) \rightarrow (\text{accept})$

Unforgeability: The user U should not be able to generate or forge signatures without the knowledge of signer's private key sk . More precisely, if the user is in possession of l valid pairs of messages and signatures, then the signer S ran the signature generation algorithm at least l times. This property is also called 'one-more forgery' which was first mentioned in [32]

Blindness: Let V be the view of the protocol that consists of all the parameters which are visible to the signer. While running one instance of blind signature scheme, for a valid message-signature pair of (m, π) and the corresponding view V , the signer S cannot link this view V to (m, π) at a later time. This is also

called unlinkability [1] and simply means that the signer's view V of (m, π) and V' of another pair, (m', π') are statistically independent.

3.3 Evolution of blind signature schemes

After proposing the concept of blind signatures [1] for the first time, Dr. D. Chaum also proposed the RSA-based blind signature scheme [33]. In 1994, Camenisch et al. proposed blind signature scheme based on discrete logarithm problem for the first time in [34]. The paper presented two schemes in which one was derived from a variation of Digital Signing Algorithm (DSA) [35], the second one was based on the Nyeberg-Rueppel signature scheme [36]. Pointcheval [32] [37] provided the first provably secure blind signature scheme.

In 1992, Solms et al. [38] raised concerns regarding dangers of implementing blind signatures for digital cash/currency. The authors argued that the total anonymity can be misused to commit 'perfect crime' where authority has no way of linking a transaction to criminals. They can use such payment systems to obtain ransoms or launder money. To address this issue, Stadler et al. [39] proposed the concept of *fair* blind signature scheme. With the help of a trusted third-party, the anonymity of a user can be revoked in case of a dispute between signer and user. The work proposed two schemes in which the revocation mechanism works in two separate directions: given the signer's view V of a session, the third party could enable the signer to efficiently identify the message-signature pair, or links a given message-signature pair to the corresponding view V of the protocol.

This raises the point that in *fully* blind signatures, the signers are oblivious to the message being signed. For example, in a simple e-cash system, the signer would like to control certain attributes like 'date of issue' or 'validity' rather than the user. *Partially* blind signatures compensates for these features. Abe and Fujisaki [40] introduced the concept of partially blind signatures in which signer can include some information which is agreed upon earlier. In the example of e-cash, the signer can add details about the validity of a token in the signing message to prevent abuse. Abe and Okamoto [41] then gave a formal definition of such scheme and gave proof of completeness, partial blindness and unforgeability in the *Random Oracle Model* (ROM).

3.4 Blind signature schemes

In this section, we go over the construction of blind RSA *Full-Domain Hashing* scheme which is based on the computational difficulty of the RSA problem (and the related integer factorization problem) and *Schnorr* blind signatures, whose securities relies on the discrete logarithm problem.

3.4.1 RSA-FDH Blind signature

This is the modified version of the RSA-FDH [42] signature scheme which follows the *hash-and-sign* paradigm. It hashes the message onto the full domain of the RSA cryptosystem i.e. image(output) size of the hash function equals the size of the RSA modulus N .

Key generation

In the RSA-FDH scheme, key generation follows the standard RSA key generation process. The signer selects two large prime numbers, p and q , and computes their product $n = pq$, which is used as the modulus. The public exponent e is chosen such that it is relatively prime to $\phi(n) = (p - 1)(q - 1)$, and the private exponent d is computed as the modular inverse of $e \bmod \phi(n)$. The public key consists of (e, n) and the private key is (d, n) .

Signing

The signing process involves three steps: blinding, signing, and unblinding. First, the user chooses a random blinding factor r such that $\gcd(r, n) = 1$ and computes the blinded message $m' = H(m) \cdot r^e \bmod n$, where $H(m)$ is the digest of message m from the hash function. $H : \{0, 1\}^* \rightarrow \mathbb{Z}_n$. The user then sends m' to the signer. The signer, using their private key d , computes the blind signature $s' = (m')^d \bmod n$ and sends s' back to the user. The user then unblinds the signature by computing $s = s' \cdot r^{-1} \bmod n$, resulting in a valid signature s on the original hashed message $H(m)$.

Verification

The verification process is straightforward and follows the standard RSA signature verification. The verifier, who knows the signer's public key pk consisting (e, n) , verifies the signature by checking that $s^e \bmod n = H(m)$. If this equation holds true, the signature is considered valid. This verification confirms that the signature was indeed produced by the signer's private key and that the message has not been altered, thus ensuring the integrity and authenticity of the signed message.

Completeness: If the user and signer follow the protocol honestly, then if

$$\begin{aligned} s' &= (m')^d \bmod n \\ s &= (s' \times r^{-1}) \bmod n \rightarrow \text{then } s \text{ is a valid signature for } m \text{ as} \\ s^e &\bmod n = H(m) \end{aligned}$$

Unforgeability: [43] showed that one-more forgery is possible if the hash function H is poorly implemented. However [44] introduced '*one-more-RSA-inversion*' problem and gave proof that the scheme is unforgeable if hash function H is considered a random oracle.

3.4.2 DLP based blind Schnorr signatures

One of the recommended digital signatures schemes by NIST [23] is the Edwards-curve Digital Signature Algorithm (EdDSA). This scheme uses a variant of a Schnorr signature [45] based on elliptic curves called *twisted Edwards* curves. Before we look at the scheme of blind Schnorr signatures, we have a brief description [46] of the Schnorr [45] signature scheme.

Schnorr signatures

With group \mathbb{G} of order p and a generator G , the private key is a randomly generated integer $x \xleftarrow{\$} \mathbb{Z}_p$. The public key is then $X \leftarrow xG$.

To sign a message m , signer chooses $r \xleftarrow{\$} \mathbb{Z}_p$ and sends the value $R := rG$ to the user. The user calculates $c := H(R, m)$ with hash function $H : \{0, 1\}^* \rightarrow \mathbb{Z}_p$ and sends the value of c back. With c , signer finally calculates $s := r + cx \bmod p$ and publishes the signature on message m as $\sigma := (R, s)$.

The user can evaluate the condition $sG = R + cX$ to check if σ is a valid signature. The correctness holds because $sG = R + cX$ is $(r + cx)G = rG + cxG$.

Blind Schnorr signatures

Key generation

With group \mathbb{G} of order p , generator G a hash function $H : \{0, 1\}^* \rightarrow \mathbb{Z}_p$, public parameters (p, \mathbb{G}, G, H) are setup. Then key generation follows where the private key is a randomly generated integer $x \xleftarrow{\$} \mathbb{Z}_p$ and public key is then $X \leftarrow xG$.

Signing: An interactive protocol

The goal is to get the signature $\sigma := (R', s')$ for a message m . As before, signer chooses $r \xleftarrow{\$} \mathbb{Z}_p$ and sends the value $R := rG$ to the user. This time, the user generates two random blinding factors $\alpha, \beta \xleftarrow{\$} \mathbb{Z}_p$ and calculates $R' := R + \alpha G + \beta X$. User also computes $c' := H(R', m)$ and then uses β to blind c as $c := c' + \beta \bmod p$. The challenge c is then blindly signed by the signer by doing $s := r + cx \bmod p$. To get the unblinded signature, the user has to unblind s as $s' := s + \alpha \bmod p$. And the signature is $\sigma := (R', s')$.

Verification

For the signature $\sigma := (R', s')$ where X is the public key and m is message. A user who wants to verify the signature can do so by checking if the following equation holds:

$$\begin{aligned} s'G &= R' + c'X \\ &= R' + H(R', m)X \end{aligned}$$

Correctness

For the verification, the following equation is checked

$$s'G = R' + c'X \tag{3.1}$$

which is the same form as in original Schnorr signature, $sG = R + cX$

In eq. 3.1 we replace s, R, c , with the values used in the blind signature scheme.

$$\begin{aligned}s &= s' - \alpha \\ R &= R' - \alpha G - \beta X \\ c &= c' + \beta\end{aligned}$$

and then the correctness holds for eq. 3.1 as:

$$\begin{aligned}sG &= R + cX \\ (s' - \alpha)G &= R' - \alpha G - \beta X + (c' + \beta)X \\ s'G - \alpha G &= R' - \alpha G + c'X \\ s'G &= R' + c'X\end{aligned}$$

3.5 Other types of blind signatures

In section 3.3, we mentioned three types of blind signature - total, fair and partially blind signatures. There are other variants that have studied and proposed by researchers over time. We go over them briefly:

Restrictive blind signatures In a total blind signature scheme, the signer is totally unaware of the message content. Restrictive blind signature provides the desirable ability for the signer to impose certain restrictions or conditions on the blinded message before signing. For example, in e-cash system, the signer (bank) may require customers to include their identity in the blinded message.

Proxy blind signatures Proxy blind signatures allow a designated proxy entity to obtain a blind signature on behalf of another user. The motivation is to [47] implement secure delegation of signature authority, that is, by introducing a proxy signer that can sign on behalf of the original signer, and the proxy cannot forge the signature of the original signer.

Group blind signatures Group blind signatures allow a group of users to collectively obtain a signature on a message in such a way that the signer cannot determine which user requested the signature. This ensures anonymity within the group while still providing a valid signature.

Threshold blind signatures In threshold blind signature schemes, multiple signers collectively generate a blind signature for a message. A certain threshold of signers must collaborate to produce the signature, ensuring that no single signer can produce the signature alone. This enhances security and prevents any one entity from abusing the signing power.

Blind multi-signatures Blind multi-signatures extend the concept of blind signatures to support multiple signers. Multiple parties can jointly sign a message without revealing individual signing keys or requiring each signer to see the entire message. This allows for distributed signing while maintaining privacy and unlinkability.

3.6 Security models and Attacks

3.6.1 Random Oracle Model (ROM)

The Random Oracle Model, introduced by Bellare and Rogaway in [42], is a theoretical framework allowing to prove the security of hash-and-sign signature schemes. In this model, the hash function is seen as an oracle that outputs a random value for each new query. However, security proofs in the random oracle are not real proofs, since the random oracle is replaced by a well defined hash function in practice. Canetti et al. [48] showed that a security proof in the random oracle model does not necessarily imply that a scheme is secure in the real world.

In ROM, all the algorithms of the blind-signature scheme $KG, \mathcal{S}, \mathcal{U}, Vf$ gets a black-box access to an oracle $O : \{0, 1\}^n \rightarrow \{0, 1\}^n$, and can query the oracle on any input x . Initial constructions of blind signature schemes were in the random oracle model.

Pointcheval et al. [32] were the first to give a secure blind signature schemes. They first proposed various definitions of unforgeability:

- (The $(l, l + 1)$ -Forgery). For any integer l , an $(l, l + 1)$ -Forgery comes from an attacker that provides $l + 1$ signatures after l interactions with the signer \mathcal{S} .
- (The "One-More" Forgery). A "One-More" Forgery is an $(l, l + 1)$ Forgery for some integer l , polynomially bounded in the security parameter k .
- (The Strong "One-More" Forgery). A Strong "One-More" Forgery is an $(l, l + 1)$ -Forgery for some integer l , poly-logarithmically bounded in the security parameter k i.e. $l \leq (\log k)^\alpha$ for some constant α .

They also focus on two kinds of attacks -

- The sequential attack : the attacker interacts sequentially with the signer. For example, in a e-cash system, this attack can be performed by a user who withdraws coins, one after the other.
- The parallel attack : the attacker interacts l times in parallel with the signer. This attack is stronger. The attacker can initiate new interactions with the signer before previous ones have ended. In the same example of e-cash, this attack can be performed by a group of users who withdraw many coins at the same time.

Till 2000, known practical blind signature schemes whose security against adaptive and parallel attacks can be proven in the random oracle model either needed five data exchanges between the signer and the user or are limited to issue only logarithmically many signatures in terms of a security parameter. Abe [49] presented an efficient blind signature scheme that allows a polynomial number of signatures to be securely issued while only three data exchanges are needed.

The scheme given by Abe provides polynomial security, i.e., one-more unforgeable even if polynomially many signatures are issued in an adaptive and concurrent manner. Another advantage of the scheme is its potential support of protocols that need additional functionality. One can easily extend the scheme to be partially blind schemes. The security is proven in the random oracle model. The scheme remains practical as it requires only three to four times more computation than the original Schnorr signatures.

3.6.2 Standard Model

In cryptography the standard model is the model of computation in which the adversary is only limited by the amount of time and computational power available. Cryptographic schemes are usually based on complexity assumptions, which state that some problem, for example integer factorization, cannot be solved in polynomial time. Schemes which can be proven secure using only complexity assumptions are said to be secure in the standard model. Security proofs are notoriously difficult to achieve in the standard model, so in many proofs, cryptographic primitives are replaced by idealized versions.

Juels et al. [50] gave a blind signature scheme and this was the first scheme whose proof of security was proven only using complexity assumptions. All previ-

ous proofs were in random oracle model, based on number-theory assumptions only and were not fully polynomial. They showed how to achieve their protocol based on any one-way trapdoor permutations. Lindell also showed the impossibility of concurrently-secure blind signatures if simulation-based definitions of security are used [51]. However, Hazay et al. [52] presented a concurrently-secure blind signature scheme which relies on standard cryptographic assumptions (e.g., trapdoor permutations and the decisional Diffie-Hellman assumption), and they prove security with respect to game-based definitions that are stronger, also bypassing the impossibility result of Lindell [51].

3.6.3 Common Reference String model

The common reference string (CRS) is a model where there is a public string that was generated in a trusted manner, and all parties have access to the string. Schemes proven secure in the CRS model are secure given that the setup was performed correctly. Datta [53] states the definition ([53, Definition 3]):

Definition 3. *A blind signature scheme, in Common Reference String (CRS) model, consists of a tuple of efficient algorithms $BS = (C, KG, \langle \mathcal{S}, \mathcal{U} \rangle, Vf)$ where*

CRS Generation. $C(1^n)$ generates a common reference string crs .

Key Generation $KG(crs)$ generates a key pair (sk, pk) .

Signature Issuing The joint execution of algorithm $\mathcal{S}(crs, sk)$ and algorithm $\mathcal{U}(crs, pk, m)$ for message $m \in \{0, 1\}^n$ generates an output σ of the user,

$(\perp, \sigma) \leftarrow \langle \mathcal{S}(crs, sk), \mathcal{U}(crs, m, pk) \rangle$

Verification $Vf(crs, pk, m, \sigma)$ outputs a bit.

We conclude that a scheme is complete if, for a valid signature σ , generated after the joint execution of $\mathcal{S}(crs, sk)$ and $\mathcal{U}(crs, pk, m)$, the verification algorithm $Vf(crs, pk, m, \sigma)$ outputs the bit 1.

The main advantage of the CRS model over the random oracle model is that security is standard, and doesn't rely on a heuristic belief system that the real protocol that uses a standard hash function is secure. In [54] Fischlin presented a scheme in the CRS model which has a two-move signature protocol. The scheme is a generic construction from basic primitives, namely schemes for commitment, encryption and signatures as well as generic non-interactive zero knowledge (NIZK) proofs for NP-languages. The signature request protocol consists of the user sending

a commitment to the message to the signer, who responds with a signature on the commitment. The user then uses this signature on the commitment to construct the blind signature, by first encrypting the commitment and the signature, and then adding a NIZK proof that the encrypted signature is a valid signature on the encrypted commitment. Such two-move signature scheme is round-optimal (single message by user and single response from signer). It doesn't deal with the issue of security in concurrent setting and with the desire to avoid the use of the random oracle, much recent work has focused on developing round-optimal blind signatures in the CRS model.

3.6.4 ROS Attack

The *ROS*-problem was originally studied by Schnorr [55] in the context of blind signature schemes. They presented a novel parallel one-more signature forgery against blind Okamoto-Schnorr and blind Schnorr signatures in which an attacker interacts some l times with a legitimate signer and produces from these interactions $l + 1$ signatures. The attack uses a solution of the following ROS-problem which Schnorr [55] states as follows:

ROS-problem: Find an overdetermined, solvable system of linear equations modulo q with random inhomogenities. Specifically, given an oracle random function $F : \mathbf{Z}_q^l \rightarrow \mathbf{Z}_q$, find coefficients $a_{k,\ell} \in \mathbf{Z}_q$ and a solvable system of $l + 1$ distinct equations in the unknowns c_1, \dots, c_l over \mathbf{Z}_q :

$$a_{k,1}c_1 + \dots + a_{k,l}c_l = F(a_{k,1}, \dots, a_{k,l}) \text{ for } k = 1, \dots, t.$$

They presented an attack against Schnorr signatures which does not depend on the generator g or the public key h .

The signer sends commitments $g_1 = g^{r_1}, \dots, g_l = g^{r_l}$. The attacker \mathcal{A} selects $a_{k,1}, \dots, a_{k,l} \in \mathbf{Z}_q$ and messages m_1, \dots, m_t , and computes $f_k = g_1^{a_{k,1}} \cdot \dots \cdot g_l^{a_{k,l}}$ and $H(f_k, m_k)$ for $k = 1, \dots, t$. The coefficients $a_{k,\ell}$ selected by the attacker are arbitrary values.

Then \mathcal{A} solves $l + 1$ of the t equations in the unknowns c_1, \dots, c_l over \mathbf{Z}_q :

$$H(f_k, m_k) = \sum_{\ell=1}^l a_{k,\ell}c_\ell \text{ for } k = 1, \dots, t. \quad (3.2)$$

\mathcal{A} sends the solutions c_1, \dots, c_l as challenges to the signer. The signer sends back $z_\ell := r_\ell + c_\ell x \in \mathbf{Z}_q$ for $\ell = 1, \dots, l$. For each solved equation 3.2, the attacker gets a valid signature (m_k, c'_k, z'_k) by setting

$$c'_k := \sum_{\ell=1}^l a_{k,\ell} c_\ell = H(f_k, m_k) \text{ and } z'_k := \sum_{\ell=1}^l a_{k,\ell} z_\ell.$$

Correctness holds as the equations 3.2 imply that

$$g^{z'_k} h^{-c'_k} = g_1^{a_{k,1}} \cdot \dots \cdot g_l^{a_{k,l}} = f_k \text{ and } H(g^{z'_k} h^{-c'_k}, m_k) = c'_k.$$

Using a solver for the ROS problem, Wagner [56] showed that the unforgeability of the Schnorr and Okamoto-Schnorr blind signature schemes can be attacked in subexponential time whenever more than $\text{polylog}(\lambda)$ signatures are issued concurrently with λ the security parameter. It was only recently that Benhamouda et al. [57] proposed an elegant polynomial time attack against ROS_ℓ for $\ell = \text{poly}(\lambda)$ concurrent sessions. A number of schemes are affected, it includes threshold signature scheme [58], multi-signature scheme like [59], partially blind signature [41] and conditionally blind signature [60]. Benhamouda et al. have shared such schemes in their work [57]. Their attack is very practical, for instance when $\ell = 128$, it only takes time roughly 2^{32} hash computations to break unforgeability.

In [61], authors presented a problem called Parallel Random inhomogeneities in an Overdetermined Solvable system of linear equations (pROS) problem and show that an attack against pROS implies an attack to more blind signatures. The attack breaks 4-concurrent unforgeability of isogeny-based (partially) blind signature scheme, *CSI – Otter* [62] in time roughly 2^{34} hash computations. Furthermore, it can achieve the same result for *Blaze+* [63] and *BlindOR* [64] with approximately 2^{43} hash computations.

Chapter 4

Lattice-based Signatures

4.1 Basics

A lattice is a set of points in n -dimensional space with a regular structure. Consider the following matrix \mathcal{A} with dimension $m \times n$. It is denoted as:

$$\mathcal{A} = \begin{bmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & a_{m3} & \dots & a_{mn} \end{bmatrix}$$

Given n linear independent vectors $\vec{b}_1, \dots, \vec{b}_n \in \mathbb{R}^m$ with $m \geq n$, the generated lattice is formally defined to be the set of vectors:

$$\mathcal{L}(\vec{b}_1, \dots, \vec{b}_n) = \left\{ \sum_{i=1}^n a^i \vec{b}^i \mid a^i \in \mathbb{Z} \right\}$$

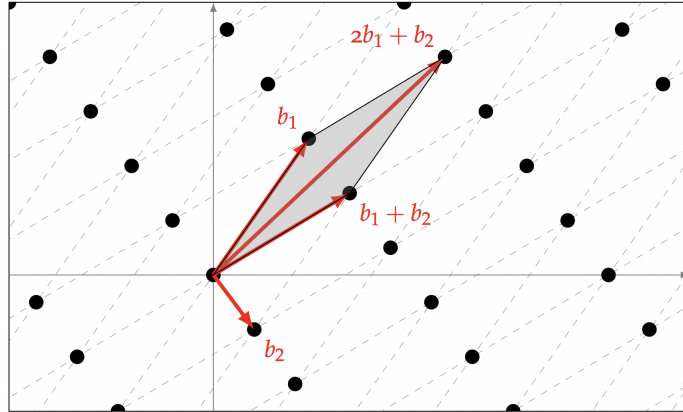


Figure 4.1: Lattice from the linear combinations of points \vec{b}_1 and \vec{b}_2
[65]

where vectors $\vec{b}_1 \dots, \vec{b}_n$ are called the basis of the generated lattice. The integers n and m are called rank and dimension respectively. In this thesis, we will only consider lattices where the rank and dimension are equal ($m = n$).

All integer linear combinations of the vectors $\vec{b}_1, \dots, \vec{b}_n$ generate a lattice. Note that the same lattice can be generated in several different ways. That is, the same lattice can be generated by different bases. Figure 4.1 gives an example of a 2-dimensional lattice with basis $\{\vec{b}_1, \vec{b}_2\}$. Combinations of linear vectors $\vec{b}_1 + \vec{b}_2$ and $2\vec{b}_1 + \vec{b}_2$ generate the same lattice points.

Now we will define fundamental domain of a lattice and later see how can we measure how orthogonality of a lattice basis. This will be later important to understand good and bad basis. We refer to the work [66] to see the definition of fundamental domain.

Definition 4. Fundamental domain of \mathcal{L} : Suppose $\mathcal{L} \subset \mathbb{R}^n$ is an n -dimensional lattice with basis $\mathcal{B} = \{\vec{v}_1, \dots, \vec{v}_n\}$. Then the fundamental domain \mathcal{F} of \mathcal{L} corresponding to \mathcal{B} is:

$$\mathcal{F}(\vec{v}_1, \dots, \vec{v}_n) = \{t_1\vec{v}_1 + \dots + t_n\vec{v}_n \mid 0 \leq t_i < 1\}$$

An important result regarding fundamental domains is the Hadamard's inequality [66] which states for fundamental domain \mathcal{F} of lattice \mathcal{L} .

$$\det(\mathcal{L}) = \text{Vol}(\mathcal{F}) \leq \|\vec{v}_1\| \dots \|\vec{v}_n\|$$

If \mathcal{L} 's basis is orthogonal then the above is an equality. Thus the above can be seen as a measure of how orthogonal a basis of a lattice \mathcal{L} is.

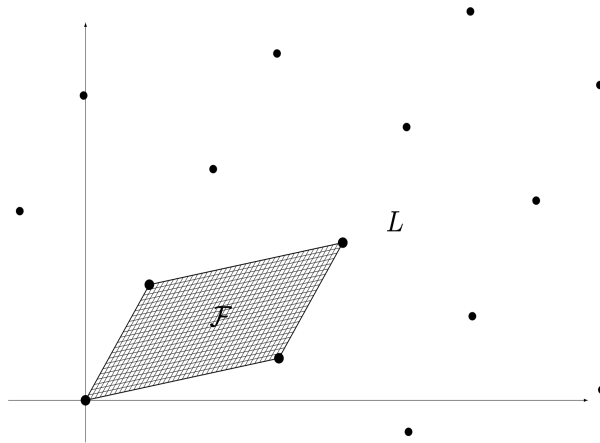


Figure 4.2: A 2-Dimensional lattice with fundamental domain \mathcal{F} [66]

4.2 Hard problems in Lattices

Although lattice structures are simple to define, there are some mathematical hard problems that form the basis of lattice-based cryptography. Finding the shortest non-zero vector in a lattice is the most prominent one. The problem is to find a vector achieving the first lattice minimum $\lambda_1(\mathcal{L}) := \min_{\mathbf{v} \in \mathcal{L} \setminus \{\mathbf{0}\}} \|\mathbf{v}\|$. This is the minimum distance of a lattice \mathcal{L} which is the length of a shortest nonzero vector in the lattice. We refer to the work by Peikert [67, Definitions 2.2.1, 2.2.2, 2.2.4] which gives us following definitions.

Definition 5. Shortest Vector Problem SVP: Given an arbitrary basis \mathcal{B} for lattice \mathcal{L} , find a shortest non-zero lattice vector (i.e. $v \in \mathcal{L}$ for which $\|v\| = \lambda_1(\mathcal{L})$).

Definition 6. Approximate Shortest Vector Problem SVP_γ : Given a basis \mathcal{B} for a lattice \mathcal{L} , find a non-zero vector $v \in \mathcal{L}$ such that $\|v\| \leq \gamma(n) \cdot \lambda_1(\mathcal{L})$ (where $\gamma(n) \geq 1$ is an approximation factor taken to be a function of the lattice dimension n).

As the name suggests, SVP_γ asks us to find a lattice vector that’s “approximately” the shortest (lattice) vector. A variant of SVP_γ is SIVP_γ .

Definition 7. Approximate Shortest Independent Vector Problem SIVP_γ : Given a basis \mathcal{B} of n -dimensional lattice \mathcal{L} , output a set $\mathcal{S} \subset \mathcal{L}$ of n linearly independent lattice vectors such that $\|s_i\| \leq \gamma(n) \cdot \lambda_n(\mathcal{L})$ for all $s_i \in \mathcal{S}$.

In high dimensional lattices, these problems becomes harder to solve. In 1996 Ajtai proved that the SVP is NP-hard for randomized reductions [11]. The Closest Vector Problem (CVP) is a computational problem on lattices closely related to SVP. Given a lattice \mathcal{L} and a target point t , CVP asks to find the lattice point closest to the target. We define dist which takes as input a n -dimensional lattice \mathcal{L} and a target vector $t \in \mathbb{R}^n$ and returns $\text{dist}(t, \mathcal{L}) := \min_{\mathbf{v} \in \mathcal{L}} \|\mathbf{v}\|$. Then CVP can be described as follows [10, Definition 2.2]:

Definition 8. Closest Vector Problem (CVP): Given a lattice basis \mathcal{L} and a target point $t \in \mathbb{R}^n$, find $v \in \mathcal{L}$ such that

$$\|v - t\| = \text{dist}(t, \mathcal{L})$$

In lattice-based cryptography, the exact SVP and CVP are rarely used as the security foundation directly. Most of lattice-based schemes actually correspond to some variants of SVP and CVP.

4.3 Lattice-based cryptography

The SVP and CVP problems are not convenient for straightforward constructions of lattice-based schemes. Some design-friendly hard problems, including SIS, LWE and NTRU, were later introduced for lattice-based cryptography. These problems and their variants have been the foundation of modern lattice-based cryptography. Next we give some preliminary descriptions to these problems.

SIS (Short Integer Solution) problem: The SIS problem was introduced and studied in Ajtai's breakthrough work [11]. Ajtai showed that the average-case SIS problem is at least as hard as the worst-case approximate SVP problem. SIS is the first hard problem for lattice-based cryptography of the worst-case/average-case reduction, which provides a strong security guarantee for lattice-based schemes. Since its introduction, SIS has been used as the foundations of many lattice-based primitives, e.g. hash functions and digital signatures.

SIS Problem: For integers $n, m, q > 0$ and a real number $B > 0$, the $\text{SIS}_{n,m,q,B}$ problem is as follows [10, Definition 2.7]:

Given uniformly random $A \in \mathbb{Z}_q^{n \times m}$, find some non-zero $x \in \mathbb{Z}^m$ such that $\|x\| \leq B$ and $Ax = 0 \pmod q$.

LWE (Learning With Errors) problem: Another cornerstone of lattice-based cryptography is the introduction of the LWE problem by Oded Regev [68]. The average-case LWE can also be shown to be at least as hard as some worst-case lattice problems. Different from the SIS problem, LWE is able to be used to construct lattice-based public key encryption and cryptosystems. The LWE problem has a decision and search variant which [10, Definition 2.8] states as follows :

LWE Problem: For integers $n, m, q > 0$ and a distribution χ over \mathbb{Z} , let $A_{\mathbf{s},\chi}$ for given $\mathbf{s} \in \mathbb{Z}^n$ be the distribution of $(a, b = \langle a, \mathbf{s} \rangle + e \pmod q)$ where $a \leftarrow U(\mathbb{Z}_q^n)$ and $e \leftarrow \chi$.

- The decision $\text{LWE}_{n,m,q,\chi}$ problem is as follows: Given m samples drawn from $A_{\mathbf{s},\chi}$ where $\mathbf{s} \leftarrow U(\mathbb{Z}_q^n)$ and m samples from $U(\mathbb{Z}_q^n \times \mathbb{Z}_q)$, distinguish them.

- The search $\text{LWE}_{n,m,q,\chi}$ problem is as follows: Given m samples drawn from $A_{\mathbf{s},\chi}$ where $\mathbf{s} \leftarrow U(\mathbb{Z}_q^n)$, find \mathbf{s} .

Lattice reduction

Cryptanalysis allows us to perform analysis of the security of cryptosystems. It avoids weak design and helps fix concrete security estimates and parameter selections. The security of a scheme relies on solving the underlying hard problems of the cryptosystem. Figure 4.3 shows steps of cryptanalysis of a lattice-based cryptosystem.

There are two kinds of SVP algorithms [69], depending on whether they give an exact solution or an approximate one:

- Exact SVP algorithms: They find the non-zero shortest lattice vector by searching through all the short vectors. Examples include enumeration and sieving.
- Approximate SVP algorithms: They output short lattice vectors, not always the shortest ones. These are faster than exact SVP algorithms. Examples include LLL and BKZ.

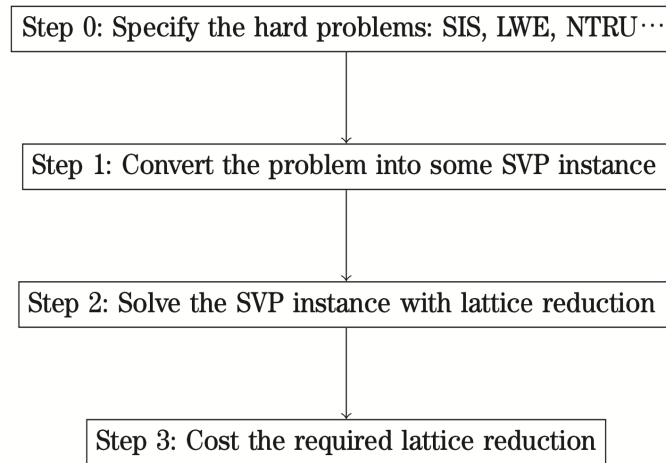


Figure 4.3: Cryptanalysis of lattice-based scheme [10]

Now we refer to [70, Definition 2.1] for the definition of lattice reduction and also see an example of good and bad basis.

Definition 9. Lattice reduction is a process of reducing the basis \mathbf{B} of a lattice \mathcal{L} to a shorter basis \mathbf{B}' while keeping \mathcal{L} the same. Figure 4.4 shows a lattice with two different basis. A basis $(\mathbf{b}_1, \mathbf{b}_2)$ is said to be reduced if it satisfies following condition:

$$\|\mathbf{b}_1\| \leq \|\mathbf{b}_2\|$$

$$u = \frac{\mathbf{b}_1 \cdot \mathbf{b}_2}{\|\mathbf{b}_1\|^2} \leq \frac{1}{2}$$

u is called the orthogonal projection coefficient

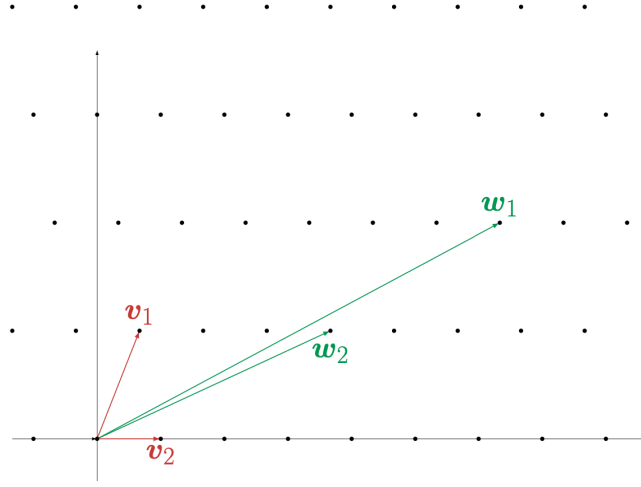


Figure 4.4: A ‘good’ basis $\{v_1, v_2\}$ and a ‘bad’ basis $\{w_1, w_2\}$
[71]

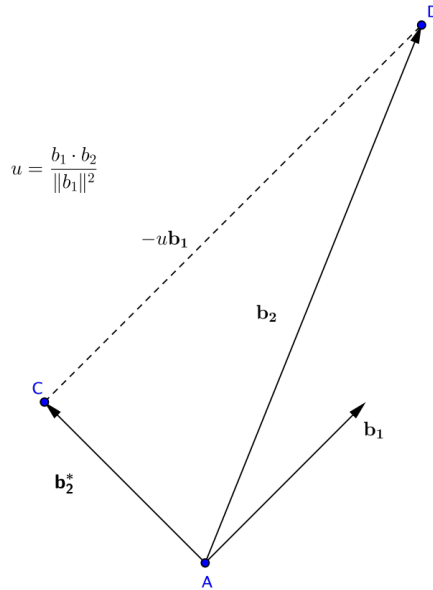


Figure 4.5: The set $\{b_1, b_2^*\}$ is the orthogonal basis for the lattice generated by basis $\{b_1, b_2\}$
[70]

Gram-Schmidt Orthogonalization

The idea of basis reduction in two dimensional lattice is to find the orthogonal basis based on the given basis [70]. Gauss lattice reduction [72] is one method of finding optimal basis but only in two-dimensional lattice. We need to generalize the algorithm to n -dimensions. Gram-Schmidt Orthogonalization is also one process

that generates orthogonal basis vectors and we refer to [70, Theorem 3.1] for the theorem.

Theorem 1. *Gram-Schmidt Orthogonalization: Given a basis $\{\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_m\}$ of a subspace H_m of \mathbb{R}^n , we define*

$$\begin{aligned} \mathbf{b}_1^* &= \mathbf{b}_1, \\ \mathbf{b}_2^* &= \mathbf{b}_2 - u_{1,2}\mathbf{b}_1, & \text{where } u_{1,2} &= \frac{\mathbf{b}_2 \cdot \mathbf{b}_1^*}{\mathbf{b}_1^* \cdot \mathbf{b}_1^*} \\ &\vdots \\ \mathbf{b}_m^* &= \mathbf{b}_m - \sum_{i < m} u_{i,m}\mathbf{b}_i, & \text{where } u_{i,m} &= \frac{\mathbf{b}_m \cdot \mathbf{b}_i^*}{\mathbf{b}_i^* \cdot \mathbf{b}_i^*} \end{aligned}$$

Then, $\{\mathbf{b}_1^, \mathbf{b}_2^*, \dots, \mathbf{b}_m^*\}$ is an orthogonal basis of H_m .*

LLL Reduction

Lenstra, Lenstra, and Lovász (and hence the name LLL algorithm) proposed an approximation algorithm [73] using the Gram-Schmidt orthogonalization for lattice basis reduction in higher dimensions. Given a basis $\{\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n\}$ where n is the dimension, the LLL algorithm can be depicted as follows. We refer to [70] for the algorithm steps.

Algorithm 1 LLL Algorithm

```

Input :  $\{\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n\}$ 
Repeat two steps until find the LLL reduced basis
Step 1: Gram-Schmidt orthogonalization
for  $i = 1$  to  $n$  do
    for  $k = i - 1$  to  $1$  do
         $m \leftarrow$  nearest integer of  $u_{k,i}$ 
         $\mathbf{b}_i \leftarrow \mathbf{b}_i - m\mathbf{b}_k$ 
    end for
end for
Step 2: Check Condition 2, and swap
for  $i = 1$  to  $n - 1$  do
    if  $\|\mathbf{b}_{i+1}^* + u_{i,i+1}\mathbf{b}_i^*\|^2 < \frac{3}{4} \|\mathbf{b}_i^*\|^2$  then
        swap  $\mathbf{b}_{i+1}$  and  $\mathbf{b}_i$ 
        go to step 1
    end if
end for

```

They gave the definition of LLL reduced basis and we refer to [70, Definition 4.1] for the same:

Definition 10. LLL reduced basis: Let $\{\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n\}$ be a basis for a n -dimensional Lattice \mathcal{L} , and $\{\mathbf{b}_1^*, \mathbf{b}_2^*, \dots, \mathbf{b}_n^*\}$ be the orthogonal basis generated due to Gram-Schmidt Orthogonalization, and we have $u_{i,k} = \frac{\mathbf{b}_k \cdot \mathbf{b}_i^*}{\mathbf{b}_i \cdot \mathbf{b}_i^*}$. We say $\{\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n\}$ is a LLL reduced basis if it satisfies two conditions:

- (1) $\forall i \neq k, u_{i,k} \leq \frac{1}{2}$
- (2) For each $i, \|\mathbf{b}_{i+1}^* + u_{i,i+1} \mathbf{b}_i^*\|^2 \geq \frac{3}{4} \|\mathbf{b}_i^*\|^2$.

The authors, Lenstra, Lenstra, and Lovász showed the result that LLL algorithm is a polynomial-time running algorithm and a LLL reduced basis is a good basis. [72].

4.4 Lattice trapdoors

Let's consider the RSA function $f(x) = x^e \bmod N$ where $N = pq$ with the primes p, q and $\gcd(e, \varphi(N)) = 1$. Then $d = e^{-1} \bmod \varphi(N)$ is the *trapdoor* because $(x^e)^d = x \bmod N$. So if one can factorize N into p and q , then they can also calculate the trapdoor d . Thus, the function $f(x)$ is a trapdoor function because, given $f(x)$ and the secret trapdoor d , we can compute x .

Piekert [67] states “A *trapdoor function* is a function that is easy to evaluate and hard to invert on its own, but which can be generated together with some extra trapdoor information that makes inversion easy”.

Gentry et al. [13] showed that we can use lattice problems to construct certain types of trapdoor functions. We now share two notions of lattice trapdoor as discussed by Vaikuntanathan in [74, Definition 1.2, 1.4]:

Definition 11. (‘Type 1’ Trapdoor). For matrices $A \in \mathbb{Z}_q^n \times m$ and $T \in \mathbb{Z}_q^{m \times m}$, T is a trapdoor for A if:

1. $AT \equiv 0^{n \times m} \bmod q$
2. T is full rank over \mathbb{Z} i.e. rank is equal to the matrix dimension size
3. Each column t_i of $T = [t_1 t_2 \dots t_m]$ is short.

The first type of trapdoor is a *short* basis which is a lattice basis consisting of short-orthogonal vectors. This short basis can be used for efficient signing operations, where a hash of the message is mapped to a close lattice vector which is preimage-resistant without the trapdoor. The work in [13] also shared an approach to signing that provably leaks no information about the secret basis.

Definition 12. (*‘Type 2’ Trapdoor*). For matrices $A \in \mathbb{Z}_q^n \times m$ and $R \in \mathbb{Z}_q^{m \times n \log q}$, R is a trapdoor for A if:

1. $AR = G$
2. Each column r_i of $R = [r_1 r_2 \cdots r_m]$ is ‘short’.

Here G is a gadget matrix. It is a special matrix whose structure allows for efficient solution of LWE problem. Given an LWE sample $s^T A + e^T$ and a type 2 trapdoor R for A :

$$(s^T A + e^T) R = s^T G + (e^T R)$$

This is an LWE sample for G with error $e' = e^T R$. This means we can use the same secret for constructing LWE samples for G from the samples for A . Peikert [67, Section 5.4.1] states that “*gadget trapdoors are technically simpler to work with in SIS/LWE-based applications, computationally more efficient, and at least as powerful*” as short basis trapdoors that we defined in the previous definition of ‘Type 1’ trapdoors.

4.5 Signatures

In the construction of lattice-based cryptographic signatures, there are two prominent families [10] of signature schemes: the *Hash-and-Sign* family and the *Fiat-Shamir* family. They have distinct methodologies and offer different advantages in terms of security, efficiency, and implementation.

4.5.1 Hash-and-Sign

The hash-and-sign lattice-based signatures use a lattice trapdoor as the secret key. Goldreich Goldwasser and Halevi gave what is known as the GGH signature scheme [75]. This is one of the earliest lattice-based signature proposals which uses hash-and-sign paradigm. With a good basis as the secret key, it computes the corresponding public key which is a bad basis. We refer to [10, Section 4.2] which describes the hash-and-sign scheme at a very high level to give the intuition:

- **Key Generation:** Generate a lattice $\mathcal{A} \subseteq \mathbb{Z}^n$ with a trapdoor T and a public representation P of \mathcal{A} . Return the public key P and the secret key T .

- **Signing:** Given message m , compute $c = \text{hash}(m) \in \mathbb{Z}^n$. Compute $v \in \mathcal{A}$ close to c using T . Return the signature $\mathbf{s} = \mathbf{v} - \mathbf{c}$.

- **Verification:** Given message m and its signature s , compute $c = \text{hash}(m)$. Accept if \mathbf{s} is short and $\mathbf{s} + \mathbf{c} \in \mathcal{A}$, otherwise reject.

The modern designs follow the provably secure framework by Gentry, Peikert and Vaikuntanathan [13] called GPV, in which the signature distribution is some discrete Gaussian, independent of the trapdoor i.e. the distribution of the signatures does not reveal any information about the trapdoor function which was used to create them. This provides a formal proof of unforgeability in the ROM [67]. One of the signature schemes Falcon [9], which is to be standardized by NIST, is based on the GPV framework and works over NTRU [76] lattices. It is fast and has the smallest signature size among other signature schemes. However it comes at the cost of complex construction where it is also non-trivial to understand and implement this scheme [77].

4.5.2 Fiat-Shamir

The Fiat-Shamir signature paradigm in lattices was given by Lyubashevsky in [78]. . At a high-level, the Fiat-Shamir approach transforms an interactive identification scheme into a non-interactive signature scheme. In lattices, it consists generating a non-interactive zero-knowledge (NIZK) proof that the signer knows the secret short vector. To ensure that the signature distribution leaks information with negligible probability, Fiat-Shamir signatures uses rejection sampling. A very high-level description of Fiat-Shamir signatures is stated in [10, Section 4.2] as follows. Let χ be some distribution of small elements, and the algorithms:

- **Key Generation:** Generate $A \leftarrow U(\mathbb{Z}_q^{n \times m})$ and $S \in \mathbb{Z}^{m \times k}$ of small coefficients. Return the public key $(A, T = AS)$ and the secret key S .

- **Signing:** Given message m , sample $y \leftarrow \chi^m$, compute $d = (Ay \bmod q)$ and $c = \text{hash}(d, m)$ where the hash domain is a set of short vectors. Return $(z = Sc + y, c)$ with certain probability, otherwise restart.

- **Verification:** Given message m and its signature (z, c) , compute $d = (Az - Tc \bmod q)$. Accept if $c = \text{hash}(d, m)$ and z is short, otherwise reject.

Dilithium [7] is based on Module-LWE and uses the Fiat-Shamir approach for its design. Compared to Falcon, it has larger key and signature sizes but much simpler

implementation [79]. Dilithium is selected as the primary signature algorithm for NIST PQC standardization. We now refer to [79, Section 3.2] who gave a simplified description of the scheme.

Key Generation: A matrix A and two short vectors s_1 and s_2 are obtained via random sampling. A , s_1 , and s_2 are used to calculate $t = As_1 + s_2$. The public key pk comprises of (A, t) and the secret key sk is (A, t, s_1, s_2) .

$$\begin{aligned} A &\leftarrow R^{m \times n} \\ s_1 &\leftarrow S_m^n, s_2 \leftarrow S_m^m \\ t &= As_1 + s_2 \\ pk &= (A, t), sk = (A, t, s_1, s_2) \end{aligned}$$

Signing: The signing phase starts with choosing a short vector y , then computing $w = Ay$. It uses the Fiat-Shamir transform to create the challenge polynomial c . The high bits of w are taken with a message M , then challenge c is $H(\text{High}(w), M)$ where H is a hash function. For z calculated as the sum $y + cs_1$, the scheme checks to see if z or $w - cs_2$ reveals any secret information. This is the rejection sampling step and if there is any leakage, the signing process starts again. If not, we get the signature as z and c .

$$\begin{aligned} y &\leftarrow S_\gamma^n \\ w &= Ay \\ c &= H(\text{High}(w), M) \in B_{60} \\ z &= y + cs_1 \\ \|z\|_\infty &> \gamma - \beta \vee \|\text{Low}(w - cs_2)\|_\infty > \gamma - \beta \implies \text{restart} \\ \text{sig} &= (z, c) \end{aligned}$$

Verification: Given public key $pk = (A, t)$ and the signature $\text{sig} = (z, c)$, a verifier takes the high bits of $Az - ct$ and computes a new challenge polynomial c' . Here the rejection sampling step is done again to check c' against c included in the received signature, to see if they match.

$$\begin{aligned} c' &= H(\text{High}(\underbrace{Az - ct}_{w - cs_2}), M) \\ \|z\|_\infty &\leq \gamma - \beta \wedge c' = c \implies \text{accept} \end{aligned}$$

If it matches then (z, c) is indeed a signature on message M .

Chapter 5

Lattice-based blind signatures

5.1 State of the art

The first lattice based blind signature was given by Ruckert [14]. He followed the structure of three-move paradigm as seen in Schnorr or Okamoto-Schnorr blind signatures. This approach was extended and many publications followed but Hauck et al [80] showed that these had an error in their security proof. And these were not as safe as it was claimed earlier. He also gave the construction of the first provably secure lattice-based blind signature with the signature size of approximately 7.9 MB and communication cost of 34 MB. It only supported 7 signatures per verification key before it needed to be regenerated. The more recent works have tried to construct more efficient and provably secure blind signatures based on lattices where the number of signatures are not bounded.

Lyubashevsky et al. proposed a scheme which had signatures size of 150KB and communication cost of around 16 MB. [81], thus making a huge improvement over previous works. Its security is based on the standard hardness of MSIS and MLWE assumptions but the signing cost increases with the number of signatures. This makes the scheme unusable in cases where we don't know the amount of signatures to be generated in advance. Agrawal et al. [82] gave a very practical scheme which relies on the Gentry, Peikert and Vaikuntanathan (GPV) signature [13]. They build upon the Fischlin protocol [54] which allows them to construct round-optimal signatures instead of three-moves. Round-optimal means that the signature will be created after two moves. This skips the possibility of concurrent executions in signing protocol and hence the resulting security issues. The signature size is around 45 KB and the

scheme supports unbounded number of signatures. This efficient scheme was the result of using NIZKs by Lyubashevsky et al. [83] but its security is based on a new non-standard hardness assumption they introduced, which they call *one-more-inhomogeneous* SIS assumption.

A new construction was proposed by del Pino and Katsumata [15]. By using the Fischlin construction [54], they were able to provide round-optimal signatures with size of 100 KB and communication cost of around 850 KB. The security of the scheme relies on the standard hardness of MSIS and MLWE assumptions while supporting unbounded number of signatures. The scheme can also be transformed into a partially-blind signature scheme, which allows the user and signer to append a common, agreed-upon message. This is useful for applications in e-cash and e-voting. The authors also gave a security proof in the Quantum-ROM (QROM) against quantum adversaries and they believe that by using the efficient techniques by Lyubashevsky et al. [81], they can bring down the communication cost from 850 KB to around 100 KB. A shorter and efficient round-optimal blind signature scheme was proposed by Beullens et al. [84] with the signature size of just 22 KB. While following the Fischlin [54] general idea, they modified the construction by Agrawal et al. [82] to remove the new one-more ISIS assumption. It is also worth noting that they also use the techniques by Lyubashevsky et al. [81] to achieve this efficiency.

Blind signature schemes can also be used to construct anonymous credentials. This mechanism allows users to prove the possession of necessary credentials required to use or access a service. Once these credentials are issued to the user, the user can choose to present them to the issuer for verification (by using zero-knowledge proof) instead of revealing all information. This allows for anonymity and selective-disclosure. Bootle et al. [85] gave the construction of a blind signature scheme based on a newly proposed ISIS_f assumption and showed how to turn the same protocol to an anonymous credential scheme. The credential size was roughly 120 KB. The authors compare it to the recent works of [86] and [87] where the credential size was around 640KB and 500KB respectively.

A new notion called non-interactive blind signature (NIBS) was recently put forward by Hanzlik [88] who made the observation that in many cases, the signed message was selected randomly. He explained that signer can create partial signatures called pre-signatures from the requester's public key. Later, the requester could extract a pair of blinded signature and the message from the pre-signature by

using their private key. He also extended this idea to *tagged* non-interactive blind signatures (T-NIBS) where a tag or unblinded metadata could be included with the signature. This functionality of T-NIBS resembles a partially-blind signature.

Taking the idea from the above, Baldimtsi et al. [89] proposed the first practical construction of non-interactive blind signatures (NIBS) from lattices. Thus signer can issue pre-signatures without interacting with the requester, who later can extract valid blind signatures. They prove their security under a new variant of the one-more ISIS assumption [82] called *randomized* one-more ISIS (rOM-ISIS) with signature size of 68KB and communication cost of just 0.96 KB.

5.2 Round optimal lattice-based signature

The aim is to choose an appropriate scheme for the use case of e-cash. In a simple electronic cash or any other system using just blind signature, the signer has no control over the attributes except the ones already defined in the public key. It is ideal to use partially-blind signatures where the requester and signer can both agree on some common information to be added to blind signature. In the previous section, where the start-of-art was presented, one of the schemes made most sense to study. The construction by del Pino and Katsumata [15] meets the criteria. It supports unbounded polynomially many signatures and is provably secure. The scheme is based on standard assumptions as opposed to similar other works who either introduced new assumptions or doesn't include construction that provides partial blindness. Moreover, the authors established the security both in ROM and QROM, and even against malicious signer. Now we talk about the intuition, building blocks and construction of their scheme below:

5.2.1 Intuition

We saw that the Fischlin protocol [54] is a nice starting point for many blind signature schemes and it provides round-optimal signature. This scheme by del Pino and Katsumata [15] also builds on same generic construction and supports unbounded many signatures.

In the presented blind signature construction, the signer or signing authority has a signing key sk , (which is kept secret) and a verification key vk (which can be

published).

To get a blind signature on a message M , the user or the requester submits a commitment $\text{com} \leftarrow \text{Com}(M; \text{rand})$ to the signer who gives the signature $\sigma \xleftarrow{\$} \text{Sig}(\text{sk}, \text{com})$.

The user also constructs a ciphertext $\text{ct} \leftarrow \text{Enc}(\text{ek}, \text{com} \parallel \text{rand} \parallel \sigma; \text{rand}')$ using a PKE scheme and a NIZK proof π that proves equations 5.1 and 5.2 are equal. Here the statement is $(\text{vk}, \text{ek}, \text{ct}, M)$ and the witness is $(\text{com}, \text{rand}, \sigma, \text{rand}')$.

The user can now give $\Sigma = (\pi, \text{ct})$ as the blind signature.

$$\text{com} = \text{Com}(M; \text{rand}) \wedge \text{Verify}(\text{vk}, \sigma, \text{com}) \quad (5.1)$$

$$\top \wedge \text{ct} = \text{Enc}(\text{ek}, \text{com} \parallel \text{rand} \parallel \sigma; \text{rand}') \quad (5.2)$$

The main restriction is giving an efficient lattice-based NIZK π that proves equations 5.1 and 5.2 are equal. It proves the possession of a valid signature on the hidden message (com in this case).

The present lattice-based signatures doesn't have signing algorithm which are compatible with efficient and lattice-based NIZKs. To solve this limitation, the authors have pointed towards the technique by Pino et al. [90] in which they gave construction of efficient group signatures.

5.2.2 Building blocks

A group signature allows a user to sign anonymously on a message, whose identity can be revealed later by the group manager in case of dispute. For the group user with identity $I \in [N]$, the group manager generates a signature $\sigma \xleftarrow{\$} \text{Sig}(\text{sk}, I)$ which functions as the certificate for user I . When this user wants to sign on the behalf of the group, the user I generates $\text{ct} \leftarrow \text{Enc}(\text{ek}, I; \text{rand}')$ using a PKE scheme and constructs an NIZK proof π that proves

$$\text{Verify}(\text{vk}, \sigma, I) = \top \wedge \text{ct} = \text{Enc}(\text{ek}, I; \text{rand}') \quad (5.3)$$

The statement is X_{gs} is $(\text{vk}, \text{ek}, \text{ct})$ and the witness W_{gs} is $(\sigma, I, \text{rand}')$. We can notice that though Eq. 5.3 is simpler than Eq. 5.1 and 5.2, it still provides a valid signature on a hidden message, which in this case is the identity I of the user.

In del Pino et al. [90], the authors have used Boyen lattice signature [91] as the building block for their group signature scheme. In order to generate a credential for user I , the group owner or manager takes I as the message and samples a short vector \mathbf{e} satisfying

$$[\mathbf{a}_1 \mid \mathbf{a}_2 + I \cdot \mathbf{g}] \mathbf{e}^\top = u \quad (5.4)$$

where \mathbf{g} is the gadget matrix. The verification key consists of a random element $u \in R_q$ and vectors $(\mathbf{a}_1, \mathbf{a}_2) \in R_q^k \times R_q^k$, where R_q is the polynomial ring $\mathbb{Z}_q[X]/(X^d + 1)$. The signing key sk is a short basis $\mathbf{T}_{\mathbf{a}_1} \in R^{k \times k}$ that satisfies the relation $\mathbf{a}_1 \mathbf{T}_{\mathbf{a}_1} = \mathbf{0} \bmod q$.

In the case when the identity I is public, the user can use lattice-based NIZKs based on standard assumptions of Module-SIS or Module-LWE to prove possession of \mathbf{e} , which is the certificate for that user. The proof is of the form $\bar{\mathbf{a}}\bar{\mathbf{e}}^\top = \bar{u}$, where the statement is $(\bar{\mathbf{a}}, \bar{u})$ and $\bar{\mathbf{e}}$ is the witness.

But in a group signature, the identity of the user I is required to be hidden. Generating a lattice-based NIZK becomes hard as compared to the previous case (when I is made public) because eq. (5.4) becomes a quadratic relation.

To tackle this limitation authors have used BDLOP commitment by Baum et al. [92]. It is of the form $\text{com} = \begin{bmatrix} \mathbf{t}_0 \\ \mathbf{t}_1 \end{bmatrix} = \begin{bmatrix} \mathbf{b}_0 \\ \mathbf{b}_1 \end{bmatrix} \mathbf{R} + \begin{bmatrix} 0 \\ I \cdot \mathbf{g} \end{bmatrix}$, where $\mathbf{b}_0, \mathbf{b}_1$ is the commitment key, \mathbf{R} is the commitment randomness, and $I \cdot \mathbf{g}$ is the message.

From this com, we can use the lower part of com , i.e. \mathbf{t}_1 for eq. (5.4) and expand it as

$$[\mathbf{a}_1 \mid \mathbf{a}_2 + I \cdot \mathbf{g}] \mathbf{e}^\top = [\mathbf{a}_1 \mid \mathbf{a}_2 + \mathbf{b}_1 \mathbf{R} + I \cdot \mathbf{g}] \mathbf{e}^\top - \mathbf{b}_1 \mathbf{R} \mathbf{e}_2^\top \quad (5.5)$$

and then finally express the left-hand side of Eq. (5.4) as

$$[\mathbf{a}_1 \mid \mathbf{a}_2 + I \cdot \mathbf{g}] \mathbf{e}^\top = [\mathbf{a}_1 \mid \mathbf{a}_2 + \mathbf{t}_1 \mid \mathbf{b}_1] \begin{bmatrix} \mathbf{e}^\top \\ -\mathbf{R} \mathbf{e}_2^\top \end{bmatrix} \quad (5.6)$$

We see that the term $[\mathbf{a}_1 \mid \mathbf{a}_2 + \mathbf{t}_1 \mid \mathbf{b}_1]$ consists only of public elements. Hence, eq. (5.4) is shown as an M-SIS relation where $[\mathbf{a}_1 \mid \mathbf{a}_2 + \mathbf{t}_1 \mid \mathbf{b}_1]$ is the statement and the witness vector is $[\mathbf{e} \mid -\mathbf{e}_2 \mathbf{R}^\top]$.

Group signature by Pino et al.: The core idea is, given the message msg , the Boyen signature on msg is converted to a signature on a commitment of msg . In the group signature setting, the message $\text{msg} = \text{identity } I$ of the user is signed

by the group manager and the user later can later show possession of valid signature (while also hiding the identity) by using a commitment. More concisely, the user transforms eq. (5.4) into eq. (5.6), constructs an efficient NIZK proof π for eq. (5.6), and finally outputs the group signature $\Sigma = (\pi, \text{com})$.

Using this technique for blind signatures: The intuition behind the construction by del Pino and Katsumata [15] is that blind signature has opposite functionality as compared to the scheme in [90]. The signer will sign the message blindly by using commitment com of the message and the user unblinds it to prove that he does possess a valid signature. Precisely the user constructs the BDLOP commitment com for the message I which is sent to the signing authority. The signer pulls out \mathbf{t}_1 included in the commitment and signs it using the Boyen signature scheme.

The signer samples a short vector \mathbf{e} satisfying

$$[\mathbf{a}_1 \mid \mathbf{a}_2 + \mathbf{t}_1] \mathbf{e}^\top = u$$

The user then reverses the transformation in Eq. (5.6) to obtain

$$[\mathbf{a}_1 \mid \mathbf{a}_2 + \mathbf{t}_1] \mathbf{e}^\top = [\mathbf{a}_1 \mid \mathbf{a}_2 + \mathbf{b}_1 \mathbf{R} + I \cdot \mathbf{g}] \mathbf{e}^\top = [\mathbf{a}_1 \mid \mathbf{a}_2 + I \cdot \mathbf{g} \mid \mathbf{b}_1] \begin{bmatrix} \mathbf{e}^\top \\ \mathbf{R} \mathbf{e}_2^\top \end{bmatrix} \quad (5.7)$$

We can notice that in the above eq. (5.7), a public vector is multiplied by a short-secret vector. With the statement as $[\mathbf{a}_1 \mid \mathbf{a}_2 + I \cdot \mathbf{g} \mid \mathbf{b}_1]$ and the witness vector of $[\mathbf{e} \mid \mathbf{e}_2 \mathbf{R}^\top]$, the signature can be a NIZK proof for Module-SIS relation.

One-more unforgeability

First we have a brief overview of how Pino et al gave the proof of unforgeability of the group signature they proposed. The reduction simulates the group manager by sampling $\mathbf{a}_1 \xleftarrow{\$} R_q^k$ and taking \mathbf{a}_2 as $\mathbf{a}_2 = \mathbf{a}_1 \mathbf{R}^* - I^* \cdot \mathbf{g}$ where I^* is the guess for the user for which the adversary gives the forgery for. When the adversary queries the certificate for some user $I \neq I^*$ the reduction can use standard techniques [93] to sample a short vector for $[\mathbf{a}_1 \mid \mathbf{a}_2 + I \cdot \mathbf{g}] = [\mathbf{a}_1 \mid \mathbf{a}_1 \mathbf{R}^* + (I - I^*) \cdot \mathbf{g}]$.

If the adversary gives a forgery, consisting of proof π and commitment t_1 , the witness also satisfies $\mathbf{t}_1 = \mathbf{b}_1 \mathbf{R}' + I' \cdot \mathbf{g}$, which is a valid BDLOP commitment. This reduction can break the MSIS problem if the adversary succeeds in unforgeability.

In the group signature, the message I can be chosen by adversary. But it is not the case in the blind signature where the reduction should be able to sample from $[\mathbf{a}_1 \mid \mathbf{a}_2 + \mathbf{t}_1] = [\mathbf{a}_1 \mid \mathbf{a}_1 \mathbf{R}^* - I^* \cdot \mathbf{g} + \mathbf{t}_1]$ for an arbitrary \mathbf{t}_1 hence the reduction cannot rely on the same trapdoor sampling techniques and presents a difficulty in simulating the real-world signer.

To tackle the same, the user also adds a NIZK proof of the well-formedness of com , π_{com} along with the commitment com . It implies that $\mathbf{t}_1 = \mathbf{b}_1 \mathbf{R}' + I' \cdot \mathbf{g}$ for some short \mathbf{R}' and I' .

The blind signature scheme can be summarized as follows. The user constructs a (BDLOP) commitment com for the message M and adds a multi-proof straight-line extractable NIZK proof π_{com} of its well-formedness. The signer receives (π_{com}, com) from the user and then samples a short vector \mathbf{e} such that $[\mathbf{a}_1 \mid \mathbf{a}_2 + \mathbf{t}_1 \mid \mathbf{b}_1] \mathbf{e}^\top = u$. Given \mathbf{e} from the signer, the user transforms the signature verification equation into an MSIS relation following almost the same computation as in eq. (5.7), and outputs a standard NIZK proof π for the MSIS relation as its signature. The full signature scheme is given in the Fig 5.1

5.2.3 Construction

$\Pi_{BS} : \mathcal{S}^H(vk = (\mathbf{a}_1, u), sk = T_{\mathbf{a}_1})$	$\mathcal{U}^H(vk, M)$
$(crs_{NIZK}^m, crs_{com}, \mathbf{a}_2) := H(\text{'crs'} \parallel 0)$, where $(\mathbf{a}_1, \mathbf{a}_2, u) \in R_q^{k_1} \times R_q^{k_2} \times R_q$ $crs_{com} := (\mathbf{b}_0, \mathbf{b}_1) \in R_q^{k_3} \times R_q^{k_3}$	
<div style="display: flex; justify-content: space-between; align-items: flex-start;"> <div style="width: 45%;"> <p>If $\text{Verify}^{H_m}(crs_{NIZK}^m, (crs_{com}, com), \pi^m) = \perp$ then return \perp $\mathbf{e} \xleftarrow{\\$} \text{SampleLeft}(\mathbf{a}_1, [\mathbf{a}_2 + \mathbf{t} \mid \mathbf{b}_1], u, T_{\mathbf{a}_1}, \sigma)$</p> </div> <div style="width: 45%;"> <p>$h := H_m(M)$ $\mathbf{R} \xleftarrow{\\$} [-1, 1]_{\text{coeff}}^{k_3 \times k_2}$ $com := \begin{bmatrix} \mathbf{t}_0 \\ \mathbf{t} \end{bmatrix} := \begin{bmatrix} \mathbf{b}_0 \\ \mathbf{b}_1 \end{bmatrix} \mathbf{R} + \begin{bmatrix} \mathbf{0} \\ h \cdot \mathbf{g} \end{bmatrix}$ $\pi^m \xleftarrow{\\$} \text{Prove}^{H_m}(crs_{NIZK}^m, (crs_{com}, com), (h, \mathbf{R} + \mathbb{1}))$</p> </div> </div> <div style="display: flex; justify-content: space-between; align-items: center; margin-top: 10px;"> <div style="width: 45%;"> <p>$(com, \pi^m) \longleftarrow$</p> </div> <div style="width: 45%;"> <p>$\mathbf{e} \longrightarrow$</p> </div> </div> <div style="margin-top: 10px;"> <p>$(\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3) := \mathbf{e} \in R_q^{k_1} \times R_q^{k_2} \times R_q^{k_3}$ Check: $\forall i \in [3], \ \mathbf{e}_i\ _2 \leq B_{\Sigma, i}^S$ and $[\mathbf{a}_1 \mid \mathbf{a}_2 + \mathbf{t} \mid \mathbf{b}_1] \cdot \mathbf{e}^\top = u$ $\tilde{\mathbf{e}}^\top := \begin{bmatrix} \mathbf{e}_1^\top \\ \mathbf{e}_2^\top \\ \mathbf{R} \mathbf{e}_2^\top + \mathbf{e}_3^\top \end{bmatrix}$ $\pi^s \xleftarrow{\\$} \text{Prove}^{H_s}((\mathbf{a}_1, \mathbf{a}_2, \mathbf{b}_1, u, h), \tilde{\mathbf{e}})$ return π^s</p> </div>	

Figure 5.1: The blind signature scheme

Now we look at the different functions in the scheme:

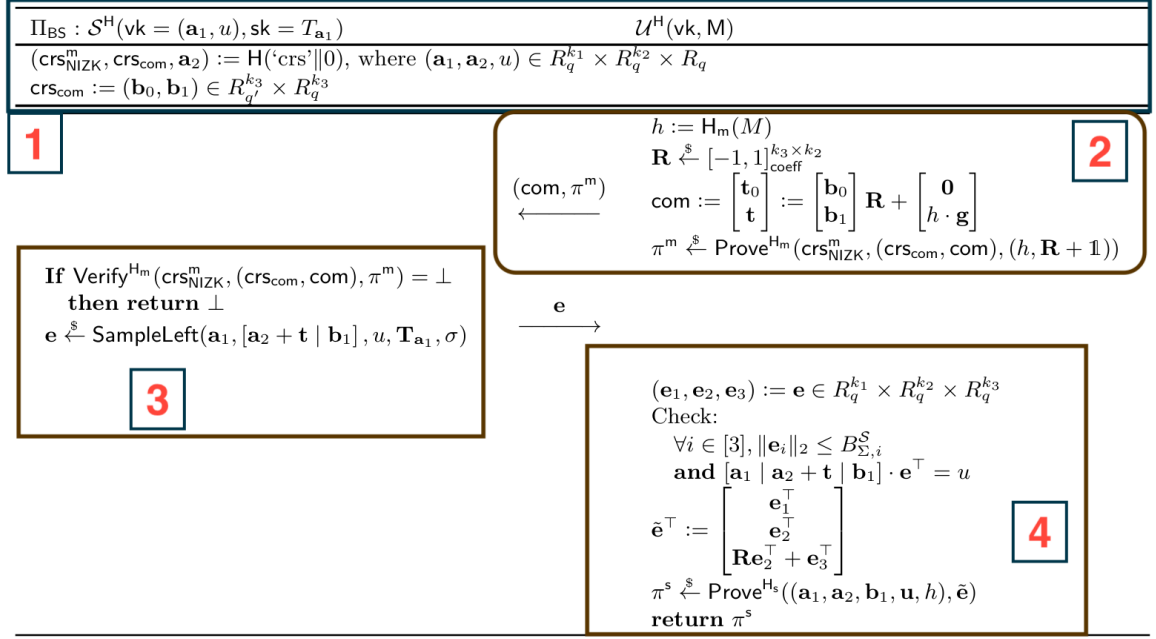


Figure 5.2: Components of the blind signature scheme

Section 1: Setup Π_{BS} is the blind signature scheme. The common random strings crs are derived correctly. With the trapdoor generation of $T_{\mathbf{a}_1}$, the pair of verification and secret key will be $\text{vk} = (\mathbf{a}_1, u), \text{sk} = T_{\mathbf{a}_1}$

Section 2: Commitment and NIZK proof For the message M and a hash function as random oracle H_m , user gets $h := H_m(M)$ for which they create a commitment com . Along with it, user constructs a NIZK proof π^m that proves the wellformedness of commitment com .

Section 3: Blind signing The verifier algorithm takes as input crs , a statement X and a proof π . It either accepts or rejects. With a valid commitment com and proof π , signer samples short vector \mathbf{e} such that $[\mathbf{a}_1 \mid \mathbf{a}_2 + \mathbf{t}_1] \mathbf{e}^\top = u$

Section 4: Signature The user creates a proof π^s that proves the knowledge of a short vector \mathbf{e} which acts as the signature.

5.2.4 Extension to partially blind signature

Partially-blind signatures are an extension of blind signature schemes in which both the parties can agree to some common message which is included in signing. The blind signature scheme of del Pino and Katsumata et al. [15] can be modified to a partially blind signature scheme.

All the building blocks are same as seen in Section 5.2.3 with minor modifications.

The hash function H_M is modified to take a message M and common message pair γ as input (M, γ) . A new hash function H_{Mc} is also introduced.

In the signing phase, the signer samples short vector e such that:

$$[\mathbf{a}_1 \mid \mathbf{a}_2 + \mathbf{t} \mid \mathbf{b}_1 \mid \cdots \mid \mathbf{b}_{k_2}] \cdot \mathbf{e}^\top = \underline{u - H_{Mc}(\gamma)} \quad (5.8)$$

instead of $[\mathbf{a}_1 \mid \mathbf{a}_2 + \mathbf{t}_1] \mathbf{e}^\top = u$ earlier.

The user can construct a proof π^s as the signature Σ which is binded to the common message γ . This partially-blind signature scheme satisfies partial blindness and one-more unforgeability [15].

5.3 Comparison to pre-quantum blind signatures

We first note the signature and key size in 3072-bit RSA [94] (which is the current recommended parameter size by NSA) and 256-bit Elliptic Curve (EC) blind signature [95] which provides the same level of security. Both signature and keys are 384 bytes in size in RSA blind signatures while EC-based blind signatures have size of 128 bytes with key size of 32 bytes.

Recently, Katsumata et al. [96] presented two round-optimal blind signature schemes in the ROM based on group-based assumptions namely symmetric external Diffie-Hellman (SXDH), decisional Diffie-Hellman (DDH) and computational Diffie-Hellman (CDH) assumptions. In their first scheme, the signature and communication size is 447 bytes and 303 bytes respectively, thus having the smallest signature size among the prior schemes they have compared with. The second scheme achieves signature size of just 96 bytes while having communication size of 2.2KB. Both of these can be extended to partially-blind signatures. The efficiency in the first scheme was made possible by modifying the blind signature construction given by Fischlin [54]. For their second scheme the authors improve upon the scheme by Blazy et al. [97] whose construction gave signatures of 96 bytes size but the communication cost increased linearly in message length.

Other comparable work includes the scheme by Hanzlik et al. [98]. The authors presented a round-optimal blind signature scheme based on the CDH assumption that gave a signature size of 5 KB and communication size of 72 KB. Prior to this, Abe et al. [99] also showed an efficient scheme based on symmetric external

Diffie-Hellman (SXDH) assumption with signature size of 5.5KB and around 1KB in communication cost.

5.4 Application - electronic cash (eCash)

The first electronic money to have properties like physical cash was proposed by David Chaum [1] whose scheme used a blind signature to achieve untraceability. In blind signature-based schemes, the customer could get the signature of the bank on the coin without disclosing any information about the coin, and spend it without revealing his identity to the merchant. But it is still desirable for the bank to include some information about the coin like validity, expiration date, identifier. Using partially blind signature schemes, we can insert public information while keeping the private contents hidden. There is also the issue of *double spending*.

Unlike paper cash, electronic cash is inherently digital so it could easily be copied and reused. So, a malicious customer could spend it twice or more. Double spending can be checked by the bank in real-time, by keeping a database of the coin spent but it assumes that every participant is online. This comes at the expense of efficiency [100] where the bank is also a single point of failure and is also challenged to maintain optimal performance. Hence, achieving double spending detection and untraceability at the same time, is an issue in an off-line e-cash system [101].

Everaere et al. [100] stated that, in a truly off-line setting, “merchants are responsible for checking the validity of the coins on their own, which quite often can be difficult and costly”. The double spending might not get detected until the merchant goes online. Hence, the following question arises naturally:

What are the practical ways of achieving protection against double-spending while not online(preferably)?

5.4.1 P2P system for tackling double spending

We discuss two studies which rely on a peer-to-peer (P2P) design to detect or avoid double spending. The first one by Osipkov et al. [102] and the other one by Everaere et al. [100]

The authors in [102] introduced a peer-to-peer system architecture to prevent double-spending. It doesn't require an on-line trusted party or tamper-resistant soft-

ware or hardware. They mention that since merchants are the beneficiaries of a fair and fraud-less payment system, they can help in avoiding double spending. The idea lies on using merchant as a *witness* to a transaction and they state that “*during creation, each coin is assigned in a random fashion to one of the merchants, which will serve as a witness for the validity of that coin*”. Expiration dates are also added in coin as public information, using a partially blind signature scheme.

In the proposed e-cash system, the merchants leave a security deposit with the broker \mathcal{B} , an entity where users can buy coin and merchants can exchange coins for bank credit/cash. When a user \mathcal{U} obtains a coin C , it is also assigned one of the merchants \mathcal{M}_C as the witness. When the user wants to spend the coin C and sends it to a merchant \mathcal{M} , this merchant has to contact the witness \mathcal{M}_C for a signature on payment transcript for the coin C . The witness merchant \mathcal{M}_C can refuse to sign if the coin was seen before. Even if the witness merchant signs a payment transcript twice, they cannot cash the coins because the broker will detect this. In this case, the witness \mathcal{M}_C is punished and their security deposit is used to pay the merchant \mathcal{M} .

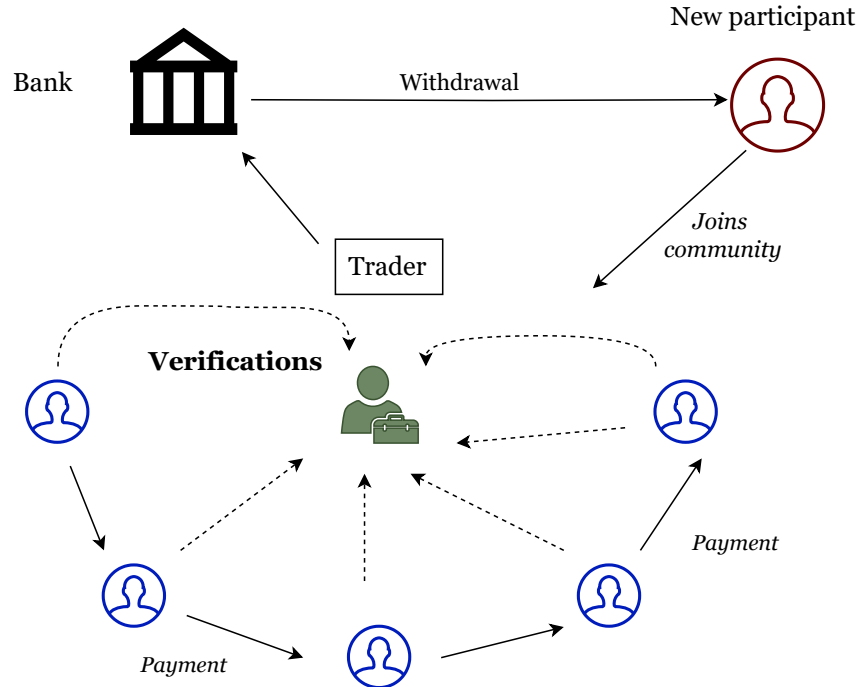


Figure 5.3: Scheme by [100]

The other study [100] describes an approach which is based on risk management for protection against double spending. The goal of the scheme is to provide coverage to user in case of loss due to invalid coin as well as to minimize the communication with bank. This involves a *trader*, an entity who will take a fee per transaction but will also cover the potential risk of double spending.

They proposed the idea of communities which are managed by a trusted third-party, trader. These communities are autonomous groups where consumer and buyers can trade between themselves using the coins issued by the trader T . When a participant \mathcal{P} (consumer or buyer) wants to join a community \mathcal{C} , they will exchange the bank certified coin $Coin_{bk}$ with trader certified coins $Coin_t$. The trader maintains a local database of the coins and these can be used for making payments within the community \mathcal{C} . A trader will also take some fee for providing coverage and insurance against double spending. When the participant \mathcal{P} wants to exit this community \mathcal{C} or enter a new community, they can redeem $Coin_t$ for bank certified $Coin_{bk}$. The novelty in their idea is that, they also address the risk taken by the trader where he may end up with double-spent coins from a malicious participant. A risk model is proposed which guarantees a minimal profit for the trader over a large number of transactions.

5.4.2 Lattice-based eCash

A good starting point for construction of lattice-based ecash system is the work by Bourse et al. [103]. The authors have proposed a generic framework for a *divisible* ecash system using primitives like psuedo-random functions (PRF), digital signatures, commitment schemes and non-interactive zero-knowledge (NIZK) proofs. A divisible ecash system addresses the problem of paying exact amount. For example, in the case when a user has to pay \$2.5 for goods and he only has a coin worth \$5 or \$10, a merchant or bank will have to pay the rest back to user. On the other hand, if the user has divisible coins, i.e. coin of smallest denomination \$0.01, they can pay the exact amount and the transaction is therefore complete.

The authors then gave construction of a divisible/compact e-cash system. It is defined by the following algorithms and has three types of entities, the bank \mathcal{B} , a user \mathcal{U} and a merchant \mathcal{M} .

The algorithms from their framework are described in a concise manner as follows:

- **Setup** ($1^\lambda, N$) : On input a security parameter λ and an integer N , this probabilistic algorithm outputs the public parameters pp for divisible coins of global value N . The public parameters pp are included in the other algorithms
- **BankKeygen**() : This probabilistic algorithm executed by the bank \mathcal{B} outputs a key pair (bsk, bpk) . It also sets L as an empty list, that will store all deposited coins.
- **Keygen**() : This probabilistic algorithm executed by a user \mathcal{U} as well as the merchant \mathcal{M} . It outputs a key pair for both user as (usk, upk) and for merchant as (msk, mpk) .
- **Withdraw** ($\mathcal{B}(bsk, upk), \mathcal{U}(usk, bpk)$) : This is an interactive protocol between the bank \mathcal{B} and a user \mathcal{U} . At the end of this protocol, the user gets a divisible coin C of value N or outputs \perp (in case of failure). The bank also stores the transcript of the protocol execution or outputs \perp .
- **Spend** ($\mathcal{U}(usk, C, bpk, V), \mathcal{M}(msk, bpk, info, V)$) : This is an interactive protocol between a user \mathcal{U} and a merchant \mathcal{M} . Here, *info* denotes a set of public information associated to the transaction, by the merchant, and V denotes the amount of this transaction. At the end of the protocol the merchant gets Z (the coins for the product) along with a proof of validity Π or outputs \perp .
- **Deposit** ($\mathcal{M}(msk, bpk, (V, info, Z, \Pi)), \mathcal{B}(bsk, L, mpk)$) : This is an interactive protocol between a merchant \mathcal{M} and the bank \mathcal{B} .

There are two other algorithms which are used in the deposit protocol. The first one, *CheckDeposit* checks if the deposit (the transcript and associated data) is valid. *Identify* checks two transcripts and outputs the public key of the user in case double spending is detected.

To make the deposit, the merchant first sends a transcript $(V, info, Z, \Pi)$ along with some additional data μ . The bank \mathcal{B} first checks the validity of all these elements with the function *CheckDeposit* and also that this merchant has not already deposited a transcript associated with *info*. This is done with the function *Identify*. If the data and transcripts are not valid, then \mathcal{B} aborts and outputs \perp . If double spending is detected, then \mathcal{B} returns another transcript $(V', info, Z', \Pi')$ along with the associated μ' . In this case, the bank can recover the serial numbers of the coin and compare it to the ones spent before. In case they were not double spent and are

valid, then \mathcal{B} adds it to the list L (the list of deposited coins) and keeps a copy of $(V, \text{info}, \text{mpk}, Z, \Pi)$.

The above feature is the novelty of the framework given by [103] in which the authors use a new family of psuedo-random functions (PRFs) called *constrained* PRFs. We refer the readers to the work [103, Section 2] for more information. Taking ideas from this framework, Deo et al. [104] then gave a construction for secure ecash system based on lattices.

5.4.3 Peer-to-peer system based eCash

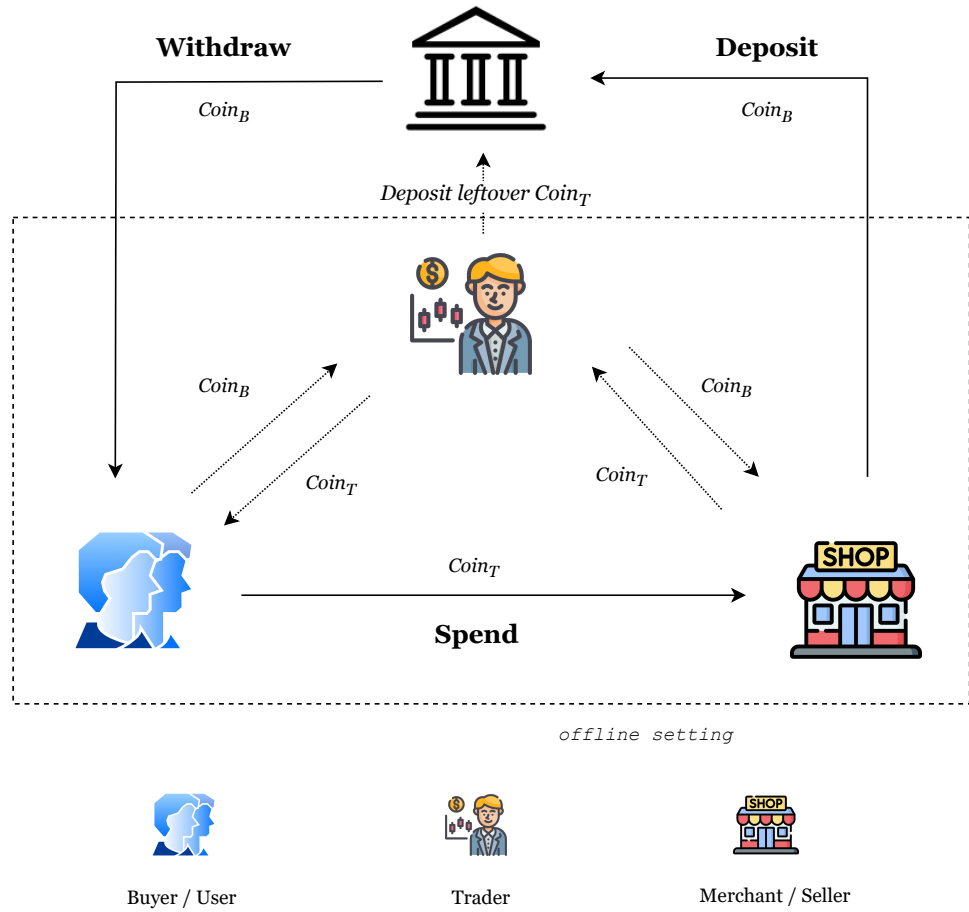


Figure 5.4: Peer-to-peer system of eCash

From the two works discussed in the section 5.4.1, the first work by Osipkov et al. [102] proposes using merchants as *witnesses* for the coins. But they don't talk about it in the context of divisible cash and the overall construction seems complicated.

Witness assignment is one of the issues. The primary issue is, for spending an amount V , the V serial numbers $SN_{i_0}, \dots, SN_{i_{V-1}}$ are derived. Then it is very much possible that different ranges in serial numbers might have different witnesses assigned to them. And each of them will be required to sign the respective transcript separately before any coins are spent. Hence, the work by [100] seems to fit the framework of ecash better. Also, the main scheme including the protocols like *Withdraw*, *Spend* and *Deposit* are already defined using lattice-based construction in the work by Deo et al. [104]. Hence the peer-to-peer scheme of [100] can be used for the already constructed lattice-based ecash system. The figure 5.4 shows our proposed peer-to-peer architecture for ecash where the entity *Trader* is shown to be integrated with the scheme by Deo et al. [104].

The user and merchants are part of a community where they can exchange the coins by bank denoted as $Coin_B$ with the coins of trader $Coin_T$. These coins will be used for making purchases. The exact steps for the spending protocol are defined in [100]. Whenever the user wants to spend coins to buy a product, the merchant generates a random value or a timestamp with the purchase order, we denote it as $Order_{Mer}$. This is sent to the user who then contacts the trader (with his coins and the $Order_{Mer}$) to get signature. The trader checks the validity of the coins, updates the local database for the coins spent and sends back the signature on the $Order_{Mer}$. This can be used by merchants to make purchases themselves or they can exchange for $Coin_B$ by interacting with the trader.

Chapter 6

Conclusion

We started with the concept of digital signatures and saw the construction of some classical signature schemes we use today. Then we moved on to blind signatures where we also described the models that are used to prove security of the schemes. Subsequently, we explained about structures called lattice and the main primitives which help us construct practical schemes that provide post-quantum security. In the last section, we show the state of art in lattice-based blind signatures and explained the construction of a round-optimal blind signature scheme in detail. Finally, we presented two peer-to-peer ecash systems that are present in the literature and saw that one of them might be a good fit to be constructed leveraging an already existing lattice-based ecash system.

The objectives of this thesis are stated in the following, along with the sections that describe or try to answer them:

Give an overview of lattice-based cryptography and the main construction tools available.

- The background of lattice-based cryptography and its primitives are described in Chapter 4.

Review the recent lattice-based blind signature schemes and the new security assumptions they are based on.

- In section 5.1, we have a detailed review of state-of-the-art in lattice-based blind signature schemes where signature sizes are shared along with the new security assumptions used.

Study some recent attacks and list the schemes affected by these attacks.

- One of the major attacks was the ROS attack. This is explained in the section 3.6.4 along with the schemes which were affected by the same.

Describe the construction of the first blind signature scheme to have a formal security proof in the quantum random oracle model.

- The scheme was proposed in the paper [15] by del Pino and Katsumata. We have attempted to explain the scheme in a detailed manner in the section 5.2.

Review the approaches that tackle the problem of double spending in electronic cash and briefly evaluate their feasibility if lattice-based blind signatures are used.

- In the section 5.4, we talk about ecash and see two models proposed to detect double spending. Finally we describe one lattice-based ecash scheme and discuss how the same scheme can be extended to include a peer-to-peer system that tackles double spending.

In this work, we proposed a design for ecash system which could benefit from the post-quantum security provided by lattice-based cryptography. The future work includes calculating the exact cost of realizing this model. This requires to calculate the cost incurred due to communication with the third party called trader. The P2P models were proposed more than a decade ago and seem practical in real-life scenario but we couldn't see any subsequent work based on them. Hence it is interesting to see if ecash systems can also make use of new and efficient lattice-based primitives [83], [105], while providing the desirable properties of real-physical cash.

Bibliography

- [1] David Chaum. “Blind Signatures for Untraceable Payments”. In: *Advances in Cryptology*. Ed. by David Chaum, Ronald L. Rivest, and Alan T. Sherman. Boston, MA: Springer US, 1983, pp. 199–203. ISBN: 978-1-4757-0602-4.
- [2] S. Ibrahim et al. “Secure E-voting with blind signature”. In: *4th National Conference of Telecommunication Technology, 2003. NCTT 2003 Proceedings*. 2003, pp. 193–197. DOI: 10.1109/NCTT.2003.1188334.
- [3] Foteini Baldimtsi and Anna Lysyanskaya. “Anonymous credentials light”. In: *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. 2013, pp. 1087–1098.
- [4] Peter W Shor. “Algorithms for quantum computation: discrete logarithms and factoring”. In: *Proceedings 35th annual symposium on foundations of computer science*. Ieee. 1994, pp. 124–134.
- [5] CFP NIST. *Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process*. 2016.
- [6] Joppe Bos et al. “CRYSTALS-Kyber: a CCA-secure module-lattice-based KEM”. In: *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE. 2018, pp. 353–367.
- [7] Léo Ducas et al. “Crystals-dilithium: A lattice-based digital signature scheme”. In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2018), pp. 238–268.
- [8] Daniel J Bernstein et al. “The SPHINCS+ signature framework”. In: *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security*. 2019, pp. 2129–2146.
- [9] Thomas Prest et al. “Falcon”. In: *Post-Quantum Cryptography Project of NIST* (2020).

- [10] Xiaoyun Wang, Guangwu Xu, and Yang Yu. “Lattice-Based Cryptography: A Survey”. In: *Chinese Annals of Mathematics, Series B* 44.6 (2023), pp. 945–960.
- [11] Miklós Ajtai. “Generating hard instances of lattice problems”. In: *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*. 1996, pp. 99–108.
- [12] Craig Gentry. “Fully homomorphic encryption using ideal lattices”. In: *Proceedings of the forty-first annual ACM symposium on Theory of computing*. 2009, pp. 169–178.
- [13] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. “Trapdoors for hard lattices and new cryptographic constructions”. In: STOC '08. Victoria, British Columbia, Canada: Association for Computing Machinery, 2008, 197–206. ISBN: 9781605580470. DOI: 10 . 1145 / 1374376 . 1374407. URL: <https://doi.org/10.1145/1374376.1374407>.
- [14] Markus Rückert. “Lattice-based blind signatures”. In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 2010, pp. 413–430.
- [15] Rafaël del Pino and Shuichi Katsumata. “A new framework for more efficient round-optimal lattice-based (partially) blind signature via trapdoor sampling”. In: *Annual International Cryptology Conference*. Springer. 2022, pp. 306–336.
- [16] W. Diffie and M. Hellman. “New directions in cryptography”. In: *IEEE Transactions on Information Theory* 22.6 (1976), pp. 644–654. DOI: 10.1109/TIT.1976.1055638.
- [17] Ralph C. Merkle. “Secure communications over insecure channels”. In: *Commun. ACM* 21.4 (1978), 294–299. ISSN: 0001-0782. DOI: 10 . 1145 / 359460.359473. URL: <https://doi.org/10.1145/359460.359473>.
- [18] R. L. Rivest, A. Shamir, and L. Adleman. “A method for obtaining digital signatures and public-key cryptosystems”. In: *Commun. ACM* 21.2 (1978), 120–126. ISSN: 0001-0782. DOI: 10 . 1145 / 359340 . 359342. URL: <https://doi.org/10.1145/359340.359342>.

- [19] NIST. “DSS”. In: *FIPS* (2023). URL: <https://doi.org/10.6028/NIST.FIPS.186-5>.
- [20] Jonathan Katz and Yehuda Lindell. *Introduction to modern cryptography: principles and protocols*. Chapman and hall/CRC, 2007.
- [21] Pierrick Gaudry. “Integer factorization and discrete logarithm problems”. In: 2014. URL: <https://api.semanticscholar.org/CorpusID:17273461>.
- [22] Rabin M.O. “Digitalized Signatures”. In: *Foundations of Secure Computation* (1978), pp. 155–168. URL: <https://cir.nii.ac.jp/crid/1573105973881933824>.
- [23] FIPS NIST. *FIPS 186-4–Digital Signature Standard (DSS)*. 2013.
- [24] Lily Chen et al. *Recommendations for discrete logarithm-based cryptography: Elliptic curve domain parameters*. Tech. rep. National Institute of Standards and Technology, 2019.
- [25] Elaine Barker. “NIST SP 800-57 Part 1 Rev. 5: Recommendation for Key Management: Part 1–General”. In: *NIST Standard* (2020).
- [26] Fabrice Boudot et al. “The state of the art in integer factoring and breaking public-key cryptography”. In: *IEEE Security & Privacy* 20.2 (2022), pp. 80–86.
- [27] Paul Zimmermann. *Factorization of RSA-250*. URL: <https://web.archive.org/web/20200228234716/https://lists.gforge.inria.fr/pipermail/cado-nfs-discuss/2020-February/001166.html>.
- [28] F. Boudot et al. *Comparing the difficulty of factorization and discrete logarithm: a 240-digit experiment*. Cryptology ePrint Archive, Paper 2020/697. <https://eprint.iacr.org/2020/697>. 2020. DOI: 10.1007/978-3-030-56880-1_3. URL: <https://eprint.iacr.org/2020/697>.
- [29] Einar Løvhøiden Antonsen. *Lattice-based cryptography - A comparative description and analysis of proposed schemes*. 2017. URL: <https://www.duo.uio.no/bitstream/handle/10852/59253/1/einarant.pdf>.
- [30] Andrew Appel. “Democracy Live internet voting: unsurprisingly insecure, and surprisingly insecure”. In: *Freedom to Tinker* 8 (2020).

- [31] Song Han and Elizabeth Chang. “A pairing-based blind signature scheme with message recovery”. In: *International Journal of Information Technology* 2.4 (2005), pp. 187–192.
- [32] David Pointcheval and Jacques Stern. “Provably secure blind signature schemes”. In: *Advances in Cryptology — ASIACRYPT ’96*. Ed. by Kwangjo Kim and Tsutomu Matsumoto. Berlin, Heidelberg: Springer Berlin Heidelberg, 1996, pp. 252–265. ISBN: 978-3-540-70707-3.
- [33] David Chaum. “Blind Signature System”. In: *Advances in Cryptology: Proceedings of Crypto 83*. Ed. by David Chaum. Boston, MA: Springer US, 1984, pp. 153–153. ISBN: 978-1-4684-4730-9. DOI: 10.1007/978-1-4684-4730-9_14. URL: https://doi.org/10.1007/978-1-4684-4730-9_14.
- [34] Jan L. Camenisch, Jean-Marc Piveteau, and Markus A. Stadler. “Blind signatures based on the discrete logarithm problem”. In: *Advances in Cryptology — EUROCRYPT’94*. Ed. by Alfredo De Santis. Berlin, Heidelberg: Springer Berlin Heidelberg, 1995, pp. 428–432. ISBN: 978-3-540-44717-7.
- [35] NIST. “FIPS PUB 186”. In: *Federal Information Processing Standards Publication* (1994). URL: <https://web.archive.org/web/20131213131144/http://www.itl.nist.gov/fipspubs/fip186.htm>.
- [36] Kaisa Nyberg and Rainer A. Rueppel. “Message recovery for signature schemes based on the discrete logarithm problem”. In: *Advances in Cryptology — EUROCRYPT’94*. Ed. by Alfredo De Santis. Berlin, Heidelberg: Springer Berlin Heidelberg, 1995, pp. 182–193. ISBN: 978-3-540-44717-7.
- [37] David Pointcheval. “Strengthened security for blind signatures”. In: *Advances in Cryptology — EUROCRYPT’98*. Ed. by Kaisa Nyberg. Berlin, Heidelberg: Springer Berlin Heidelberg, 1998, pp. 391–405. ISBN: 978-3-540-69795-4.
- [38] Sebastiaan von Solms and David Naccache. “On blind signatures and perfect crimes”. In: *Computers & Security* 11.6 (1992), pp. 581–583. ISSN: 0167-4048. DOI: [https://doi.org/10.1016/0167-4048\(92\)90193-U](https://doi.org/10.1016/0167-4048(92)90193-U). URL: <https://www.sciencedirect.com/science/article/pii/016740489290193U>.
- [39] Markus Stadler, Jean-Marc Piveteau, and Jan Camenisch. “Fair Blind Signatures”. In: *Advances in Cryptology — EUROCRYPT ’95*. Ed. by Louis

- C. Guillou and Jean-Jacques Quisquater. Berlin, Heidelberg: Springer Berlin Heidelberg, 1995, pp. 209–219. ISBN: 978-3-540-49264-1.
- [40] Masayuki Abe and Eiichiro Fujisaki. “How to date blind signatures”. In: *Advances in Cryptology — ASIACRYPT ’96*. Ed. by Kwangjo Kim and Tsutomu Matsumoto. Berlin, Heidelberg: Springer Berlin Heidelberg, 1996, pp. 244–251. ISBN: 978-3-540-70707-3.
- [41] Masayuki Abe and Tatsuaki Okamoto. “Provably Secure Partially Blind Signatures”. In: *Advances in Cryptology — CRYPTO 2000*. Ed. by Mihir Bellare. Berlin, Heidelberg: Springer Berlin Heidelberg, 2000, pp. 271–286. ISBN: 978-3-540-44598-2.
- [42] Mihir Bellare and Phillip Rogaway. “Random oracles are practical: A paradigm for designing efficient protocols”. In: *Proceedings of the 1st ACM Conference on Computer and Communications Security*. 1993, pp. 62–73.
- [43] Markus Michels, Markus Stadler, and Hung Min Sun. “On the security of some variants of the RSA signature scheme”. In: *Computer Security — ESORICS 98*. Ed. by Jean-Jacques Quisquater et al. Berlin, Heidelberg: Springer Berlin Heidelberg, 1998, pp. 85–96. ISBN: 978-3-540-49784-4.
- [44] Mihir Bellare et al. “The One-More-RSA-Inversion Problems and the Security of Chaum’s Blind Signature Scheme.” In: *IACR Cryptology ePrint Archive* 2001 (Jan. 2001), p. 2.
- [45] Claus-Peter Schnorr. “Efficient identification and signatures for smart cards”. In: *Advances in Cryptology—CRYPTO’89 Proceedings 9*. Springer. 1990, pp. 239–252.
- [46] Gian Demarmels, Lucien Heuzeveldt, and Expert Elektronikingenieur HTL Daniel Voisard. *Adding Schnorr’s Blind Signature in Taler*. 2022.
- [47] Fengxia Liu et al. “A survey on lattice-based digital signature”. In: *Cybersecurity* 7.1 (2024), p. 7.
- [48] Ran Canetti, Oded Goldreich, and Shai Halevi. “The random oracle methodology, revisited”. In: *Journal of the ACM (JACM)* 51.4 (2004), pp. 557–594.
- [49] Masayuki Abe. “A secure three-move blind signature scheme for polynomially many signatures”. In: *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2001, pp. 136–151.

- [50] Ari Juels, Michael Luby, and Rafail Ostrovsky. “Security of blind digital signatures”. In: *Annual International Cryptology Conference*. Springer. 1997, pp. 150–164.
- [51] Yehuda Lindell. “Bounded-concurrent secure two-party computation without setup assumptions”. In: *Proceedings of the thirty-fifth annual ACM symposium on Theory of computing*. 2003, pp. 683–692.
- [52] Carmit Hazay et al. “Concurrently-secure blind signatures without random oracles or setup assumptions”. In: *Theory of Cryptography Conference*. Springer. 2007, pp. 323–341.
- [53] Nilanjan Datta. “Survey on security of blind signature and impossibility of blind signature from lossy-trapdoor-permutations”. PhD thesis. Indian Statistical Institute-Kolkata, 2011.
- [54] Marc Fischlin. “Round-optimal composable blind signatures in the common reference string model”. In: *Annual International Cryptology Conference*. Springer. 2006, pp. 60–77.
- [55] Claus Peter Schnorr. “Security of blind discrete log signatures against interactive attacks”. In: *International Conference on Information and Communications Security*. Springer. 2001, pp. 1–12.
- [56] David Wagner. “A generalized birthday problem”. In: *Annual International Cryptology Conference*. Springer. 2002, pp. 288–304.
- [57] Fabrice Benhamouda et al. “On the (in) security of ROS”. In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2021, pp. 33–53.
- [58] Rosario Gennaro et al. “Secure distributed key generation for discrete-log based cryptosystems”. In: *Journal of Cryptology* 20 (2007), pp. 51–83.
- [59] Ewa Syta et al. “Keeping authorities" honest or bust" with decentralized witness cosigning”. In: *2016 IEEE Symposium on Security and Privacy (SP)*. Ieee. 2016, pp. 526–545.
- [60] Panagiotis Grontas et al. “Towards everlasting privacy and efficient coercion resistance in remote electronic voting”. In: *Financial Cryptography and Data Security: FC 2018 International Workshops, BITCOIN, VOTING, and*

- WTSC, Nieuwpoort, Curaçao, March 2, 2018, Revised Selected Papers 22*. Springer. 2019, pp. 210–231.
- [61] Shuichi Katsumata, Yi-Fu Lai, and Michael Reichle. “Breaking parallel ROS: implication for isogeny and lattice-based blind signatures”. In: *IACR International Conference on Public-Key Cryptography*. Springer. 2024, pp. 319–351.
- [62] Shuichi Katsumata et al. “CSI-otter: Isogeny-based (partially) blind signatures from the class group action with a twist”. In: *Annual International Cryptology Conference*. Springer. 2023, pp. 729–761.
- [63] Nabil Alkeilani Alkadri, Rachid El Bansarkhani, and Johannes Buchmann. “On lattice-based interactive protocols: an approach with less or no aborts”. In: *Australasian Conference on Information Security and Privacy*. Springer. 2020, pp. 41–61.
- [64] Nabil Alkeilani Alkadri, Patrick Harasser, and Christian Janson. “BlindOR: an efficient lattice-based blind signature scheme from OR-proofs”. In: *International Conference on Cryptology and Network Security*. Springer. 2021, pp. 95–115.
- [65] Vinay Oedayrajsingh Varma. “A survey of classical public-key cryptography and post-quantum lattice-based cryptography”. In: ().
- [66] Joseph H Silverman, Jill Pipher, and Jeffrey Hoffstein. *An introduction to mathematical cryptography*. Vol. 1. Springer, 2008.
- [67] Chris Peikert et al. “A decade of lattice cryptography”. In: *Foundations and trends® in theoretical computer science* 10.4 (2016), pp. 283–424.
- [68] Oded Regev. “On lattices, learning with errors, random linear codes, and cryptography”. In: *Journal of the ACM (JACM)* 56.6 (2009), pp. 1–40.
- [69] Masaya Yasuda. “A survey of solving SVP algorithms and recent strategies for solving the SVP challenge”. In: *International Symposium on Mathematics, Quantum Theory, and Cryptography: Proceedings of MQC 2019*. Springer Singapore. 2021, pp. 189–207.
- [70] Xinyue Deng. “An introduction to lenstra-lenstra-lovasz lattice basis reduction algorithm”. In: *Massachusetts Institute of Technology (MIT)* (2016).

- [71] Joseph H. Silverman. *An Introduction to Lattices, Lattice Reduction, and Lattice-Based Cryptography*. 2020. URL: <https://www.ias.edu/sites/default/files/PCMISlidesX1.pdf> (visited on 05/28/2024).
- [72] 2019. URL: <https://staff.emu.edu.tr/alexanderchefranov/Documents/CMSE491/Fall2019/Hoffstein2015%20Introduction%20to%20Mathematical%20Cryptography%20436-448.pdf> (visited on 05/28/2024).
- [73] Arjen K Lenstra, Hendrik Willem Lenstra, and László Lovász. “Factoring polynomials with rational coefficients”. In: *Mathematische annalen* 261 (1982), pp. 515–534.
- [74] Vinod Vaikuntanathan. *6.876J Course: Advanced Topics in Cryptography: Lattices*. 2015. URL: <https://people.csail.mit.edu/vinodv/6876-Fall2015/L16.pdf> (visited on 05/28/2024).
- [75] Oded Goldreich, Shafi Goldwasser, and Shai Halevi. “Public-key cryptosystems from lattice reduction problems”. In: *Advances in Cryptology—CRYPTO’97: 17th Annual International Cryptology Conference Santa Barbara, California, USA August 17–21, 1997 Proceedings* 17. Springer. 1997, pp. 112–131.
- [76] Jeffrey Hoffstein et al. “NTRUSIGN: Digital signatures using the NTRU lattice”. In: *Cryptographers’ track at the RSA conference*. Springer. 2003, pp. 122–140.
- [77] *Falcon*. 2018. URL: <https://csrc.nist.gov/CSRC/media/Presentations/Falcon/images-media/Falcon-April2018.pdf>.
- [78] Vadim Lyubashevsky. “Lattice-based identification schemes secure under active attacks”. In: *International workshop on public key cryptography*. Springer. 2008, pp. 162–179.
- [79] Austin Hunt. “A Contextual Analysis of CRYSTALS-Dilithium, a Quantum-Resistant, Lattice-Based Digital Signature Scheme”. In: ().
- [80] Eduard Hauck et al. “Lattice-based blind signatures, revisited”. In: *Annual International Cryptology Conference*. Springer. 2020, pp. 500–529.

- [81] Vadim Lyubashevsky, Ngoc Khanh Nguyen, and Maxime Plancon. “Efficient lattice-based blind signatures via gaussian one-time signatures”. In: *IACR International Conference on Public-Key Cryptography*. Springer. 2022, pp. 498–527.
- [82] Shweta Agrawal et al. *Practical, Round-Optimal Lattice-Based Blind Signatures*. Cryptology ePrint Archive, Paper 2021/1565. <https://eprint.iacr.org/2021/1565>. 2021. URL: <https://eprint.iacr.org/2021/1565>.
- [83] Vadim Lyubashevsky, Ngoc Khanh Nguyen, and Maxime Plançon. “Lattice-based zero-knowledge proofs and applications: Shorter, simpler, and more general”. In: *Annual International Cryptology Conference*. Springer. 2022, pp. 71–101.
- [84] Ward Beullens et al. “Lattice-based blind signatures: Short, efficient, and round-optimal”. In: *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*. 2023, pp. 16–29.
- [85] Jonathan Bootle et al. “A framework for practical anonymous credentials from lattices”. In: *Annual International Cryptology Conference*. Springer. 2023, pp. 384–417.
- [86] Corentin Jeudy, Adeline Roux-Langlois, and Olivier Sanders. “Lattice signature with efficient protocols, application to anonymous credentials”. In: *Annual International Cryptology Conference*. Springer. 2023, pp. 351–383.
- [87] Qiqi Lai et al. “Lattice-based commit-transferrable signatures and applications to anonymous credentials”. In: *Cryptology ePrint Archive* (2023).
- [88] Lucjan Hanzlik. “Non-interactive blind signatures for random messages”. In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2023, pp. 722–752.
- [89] Foteini Baldimtsi et al. “Non-interactive Blind Signatures from Lattices”. In: *Cryptology ePrint Archive* (2024).
- [90] Rafaël Del Pino, Vadim Lyubashevsky, and Gregor Seiler. “Lattice-based group signatures and zero-knowledge proofs of automorphism stability”. In: *Proceedings of the 2018 ACM SIGSAC conference on computer and communications security*. 2018, pp. 574–591.

- [91] Xavier Boyen. “Lattice mixing and vanishing trapdoors: A framework for fully secure short signatures and more”. In: *International workshop on public key cryptography*. Springer. 2010, pp. 499–517.
- [92] Carsten Baum et al. “More efficient commitments from structured lattice assumptions”. In: *International Conference on Security and Cryptography for Networks*. Springer. 2018, pp. 368–385.
- [93] David Cash et al. “Bonsai trees, or how to delegate a lattice basis”. In: *Journal of cryptology* 25 (2012), pp. 601–639.
- [94] Frank Denis, Frederic Jacobs, and Christopher A. Wood. *RSA Blind Signatures*. RFC 9474. Oct. 2023. DOI: 10.17487/RFC9474. URL: <https://www.rfc-editor.org/info/rfc9474>.
- [95] Masayuki Abe and Tatsuaki Okamoto. “Provably secure partially blind signatures”. In: *Advances in Cryptology—CRYPTO 2000: 20th Annual International Cryptology Conference Santa Barbara, California, USA, August 20–24, 2000 Proceedings 20*. Springer. 2000, pp. 271–286.
- [96] Shuichi Katsumata, Michael Reichle, and Yusuke Sakai. “Practical Round-Optimal Blind Signatures in the ROM from Standard Assumptions”. In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 2023, pp. 383–417.
- [97] Olivier Blazy et al. “Short blind signatures”. In: *Journal of computer security* 21.5 (2013), pp. 627–661.
- [98] Lucjan Hanzlik, Julian Loss, and Benedikt Wagner. “Rai-choo! Evolving blind signatures to the next level”. In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2023, pp. 753–783.
- [99] Masayuki Abe et al. “Improved (almost) tightly-secure simulation-sound QA-NIZK with applications”. In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 2018, pp. 627–656.
- [100] Patricia Everaere, Isabelle Simplot-Ryl, and Issa Traoré. “Double spending protection for e-cash based on risk management”. In: *International Conference on Information Security*. Springer. 2010, pp. 394–408.

- [101] Yaser Baseri, Benyamin Takhtaei, and Javad Mohajeri. “Secure untraceable off-line electronic cash system”. In: *Scientia Iranica* 20.3 (2013), pp. 637–646.
- [102] Ivan Osipkov et al. “Combating double-spending using cooperative P2P systems”. In: *27th international conference on distributed computing systems (ICDCS’07)*. IEEE. 2007, pp. 41–41.
- [103] Florian Bourse, David Pointcheval, and Olivier Sanders. “Divisible e-cash from constrained pseudo-random functions”. In: *Advances in Cryptology–ASIACRYPT 2019: 25th International Conference on the Theory and Application of Cryptology and Information Security, Kobe, Japan, December 8–12, 2019, Proceedings, Part I* 25. Springer. 2019, pp. 679–708.
- [104] Amit Deo et al. “Lattice-based E-cash, revisited”. In: *Advances in Cryptology–ASIACRYPT 2020: 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7–11, 2020, Proceedings, Part II* 26. Springer. 2020, pp. 318–348.
- [105] Vadim Lyubashevsky, Ngoc Khanh Nguyen, and Gregor Seiler. “Shorter lattice-based zero-knowledge proofs via one-time commitments”. In: *IACR International Conference on Public-Key Cryptography*. Springer. 2021, pp. 215–241.