Research Article

Javad Sharafi and Hassan Daghigh*

A Ring-LWE-based digital signature inspired by Lindner–Peikert scheme

https://doi.org/10.1515/jmc-2021-0013
received April 19, 2021; accepted April 24, 2022

Abstract: In this article, we give a digital signature by using Lindner–Peikert cryptosystem. The security of this digital signature is based on the assumptions about hardness of Ring-LWE and Ring-SIS problems, along with providing public key and signature of compact (1–1.5 kilobytes) size. We prove the security of our signature scheme in the Quantum Random Oracle Model. Our cryptanalysis has been done based on methods of Aggarwal et al. and Chen et al.

Keywords: lattice-based cryptography, Ring-LWE problem, Ring-SIS problem, Lindner–Peikert cryptosystem, digital signature

MSC 2020: 81P94

1 Introduction

The advent of Quantum computing threatens to break a lot of classical cryptographic schemes. This leads to innovations in public key cryptography that focus on post-quantum cryptography primitives and protocols resistant to quantum computing threats. Lattice-based cryptography is a promising post-quantum cryptography family, both in terms of foundational properties and its application to both traditional and emerging security problems such as encryption, digital signature, key exchange, homomorphic encryption, etc.

The breakthrough work of Ajtai [1] provides confidence for adopting lattice-based schemes in cryptography. Ajtai proved that solving NP-hard lattice problems, e.g., *Shortest Vector Problem* (**SVP**), in the average case is as hard as solving the worst-case assumption. It is conjectured that there is no probabilistic polynomial-time algorithm that can approximate certain computational problems on lattices within polynomial factors [2]. This is the basis for the security of lattice-based schemes. Based on the Ajtai's works in the past two decades, great progress has been made in the lattice-based cryptography on various hard lattice computational problems such as *closest vector problem* (**CVP**), *Shortest Independent Vectors Problem* (**SIVP**), *bounded distance decoding* (**BDD**), *Shortest Integer Solution* (**SIS**), etc. [2–5].

Definition 1.1. Given n linearly independent vectors $b_1, b_2, \ldots, b_n \in \mathbb{R}^d$, the *lattice* $\mathcal{L}$ is defined as

$$\mathcal{L} = \{a_1 b_1 + \cdots + a_n b_n \mid a_i \in \mathbb{Z}\}, \tag{1.1}$$

where the set of $B = \{b_1, \ldots, b_n\}$ is called a *basis* for the lattice. The integers n, d are called *rank* and *dimension* of $\mathcal{L}$, respectively. If $n = d$, then $\mathcal{L}$ is called a *full rank* (or *full dimension*) in $\mathbb{R}^d$, which is very common to use in lattice-based cryptography.

* **Corresponding author: Hassan Daghigh,** Department of Mathematics, University of Kashan, Kashan, Iran, e-mail: Hassan@Kashanu.ac.ir
Javad Sharafi: Department of Mathematics, University of Kashan, Kashan, Iran, e-mail: Javadsharafi@grad.kashanu.ac.ir

Remark 1.2. A lattice basis B is not unique. For a lattice $\mathcal{L}$ with basis B, and for every unimodular matrix $U \in \mathbb{Z}^{n\times n}$ (i.e., one having determinant ± 1), $B.\ U$ is also a basis of $\mathcal{L}(B)$.

Due to Regev [6] a large number of cryptographic constructions based on the lattices are built over the average-case *Learning With Errors* (**LWE**) problem.

Definition 1.3. (**LWE distribution**). Let $\mathbf{s}$ be a vector in $\mathbb{Z}_q^n$ (which is called *secret*). The LWE distribution $A_{\mathbf{s},\chi}$ over $\mathbb{Z}_q^n \times \mathbb{Z}_q$ is defined by sampling $\mathbf{a} \in \mathbb{Z}_q^n$ uniformly at random and choosing $e \leftarrow \chi$, then outputting $(\mathbf{a}, b = \langle \mathbf{s}, \mathbf{a} \rangle + e \bmod q)$ where $\langle \mathbf{s}, \mathbf{a} \rangle$ denotes the inner product of vectors $\mathbf{s}$ and $\mathbf{a}$.

There are two main versions of the LWE problem: the *search version* which is finding the secret according to the given LWE samples, and the *decision version* which is distinguishing between LWE samples and uniformly random samples:

Definition 1.4. (**Search**-LWE$_{n,q,\chi,m}$). It is to find $\mathbf{s}$ uniformly randomly, from $\mathbb{Z}_q^n$, so that m independent samples $(\mathbf{a}_i, b_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ are drawn from $A_{\mathbf{s},\chi}$ ($\mathbf{s}$ is fixed for all samples).

Definition 1.5. (**Decision**-LWE$_{n,q,\chi,m}$). It is to distinguish which of the followings is the case (with non-negligible advantage). m independent samples $(\mathbf{a}_i, b_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ are either distributed according to $A_{\mathbf{s},\chi}$ where $\mathbf{s} \in \mathbb{Z}_q^n$ uniformly random (fixed for all samples), or they are distributed uniformly.

The LWE-based schemes, however, are not particularly efficient because LWE-based schemes inherently give rise to key sizes and/or outputs which are $\tilde{O}(\lambda^2)$ in the security parameter λ. In 2010, Lyubashevsky et al. [7] introduced the *Ring-LWE Problem* that is the ring-based analogue of LWE, and proved the hardness of the related problems. Ring-LWE is parameterized by a ring R of degree n over $\mathbb{Z}$, a positive integer modulus q that defines the quotient ring $R_q = R/q$, and an error distribution χ over R. Typically, one takes R to be a *cyclotomic* ring, and χ to be some kind of discrete Gaussian in the canonical embedding of R.

Definition 1.6. (**Ring-LWE distribution**). For all $s \in R_q$ called the secret, the Ring-LWE distribution $A_{s,\chi}$ over $R_q \times R_q$ is sampled by choosing $a \in R_q$ uniformly at random, choosing $e \leftarrow \chi$, and outputting $(a, b = sa + e \bmod q)$.

Definition 1.7. (**The Ring-LWE Problem, decision version**). Let R denote the ring $\frac{\mathbb{Z}[X]}{<X^n+1>}$ for n which is a power of 2, and R_q be the residue ring R/q. Distinguish which of the following is the case (with non-negligible advantage); for a uniform random secret $s \leftarrow \mathcal{U}(R_q)$ and given m samples; each of them is of the form $(a, b = sa + e \bmod q)$ where the coefficients of e are independently sampled from distribution χ, or they are from uniform distribution $(a, b) \leftarrow \mathcal{U}(R_q \times R_q)$.

Remark 1.8. As it is stated before, due to the particularly nice algebraic structure of *cyclotomic rings* for implementation purposes, most proposals opt to work with this kind of rings such as $\frac{\mathbb{Z}[X]}{<X^n+1>}$ for n a power of 2. Cyclotomic rings also have the feature that the *decision version* of the Ring-LWE problem in these rings is hard [8], which makes them even more useful for cryptographic applications.

We conclude this section by introducing the "Short Integer Solution (SIS) Problem" whose hardness is needed as a part of security of our proposed scheme. (For the hardness of the SIS problem relative to worst-case lattice problems, see ref. [3, Section 4.1.2].) The SIS Problem is parameterized by positive integers n and q, which defines the group $\mathbb{Z}_q^n$ a positive real number β and a number m of group elements.

Definition 1.9. (**The SIS Problem**). Given m uniformly random vectors $a_i \in \mathbb{Z}_q^n$ forming the columns of a matrix $A \in \mathbb{Z}_q^{n\times m}$, find a nonzero integer vector $z \in \mathbb{Z}^m$ of norm $||z|| \le \beta$ such that $Az = \sum_i a_i z_i = 0 \in \mathbb{Z}_q^n$.

Inspired by the ideas behind the "NTRU cryptosystem" [9], Micciancio [10] introduced a compact ring-based analogue of Ajtai's SIS problem. This analogue has come to be known as the "Ring-SIS Problem" and is parameterized by a ring R which is often (but not always) taken to be a degree-n polynomial of the form $R = \frac{\mathbb{Z}[X]}{\langle f(X)\rangle}$, a positive integer modulus q, a real norm bound $\beta > 0$, and a number m of samples.

Definition 1.10. (**The Ring-SIS Problem**). Given m uniformly random elements $a_i \in R_q = R/q$, defining a vector $\overrightarrow{a} \in R_q^m$, find a nonzero vector $\overrightarrow{z} \in R^m$ of norm $||\overrightarrow{z}|| \leq \beta$ such that $\langle \overrightarrow{a}, \overrightarrow{z} \rangle = \sum_i a_i z_i = 0 \in R_q$.

Remark 1.11. Ring-SIS and its associated cryptographic functions can be proved at least as hard as certain lattice problems in the *worst case*, similar to SIS ([3], Section 4.3.4).

2 Related works and our contribution

For a long time, lattice-based signatures have been designed so that their security were obtainable only for inefficiently large parameters, i.e., they were far from practicality, e.g., ref. [11], or were, like **GGH** [12] and **NTRUSign** [13] broken due to flaws in the ad-hoc design approaches [14,15]. Though using the *ideal lattices*, introduced by Micciancio [10], and the related computationally hard problems, such as Ring-SIS and Ring-LWE, one can find many promising digital signatures in this area. In particular, the schemes that use the *Fiat–Shamir* approach [16] have led to a family of fast signature schemes with reasonable signature and key sizes [11,17–20].

In general, for building lattice-based signatures, there are two (seemingly distinct) frameworks: one using lattice trapdoors [21–23] and the other, as mentioned above, through the Fiat–Shamir heuristic, whereas, a strong connection between these two approaches has been recently found, see ref. ([24], Theorem 1.4). In this article, inspiring from the protocol introduced by Lindner–Peikert [25] and using the Fiat–Shamir paradigm, we present a lattice-based digital signature scheme whose structure is designed for a fixed length message, i.e., we will use the *hash and sign* approach. Our contribution is a *straight applying* the Lindner–Peikert scheme [25], which can be seen, to the best of our knowledge, as a novel idea for constructing digital signature through this primitive. In addition, as we will see in Section 6, we get an appropriate trade off between the security levels and the key sizes, where the security of the proposed scheme has been estimated by a very pessimistic approach (from the viewpoint of the defender against a quantum adversary), namely the core SVP hardness, see Section 5.1. Although we cannot claim that the proposed signature is the best one (for a summarized comparison between some similar lattice-based digital signatures, see Section 6), but one may hope for future improvements on this "naive" framework.

Remark 2.1. From sight of the practicality, the only complexity would be related to implementing performance of the *decode–encode function*, see Definition 3.1, and to the *symmetric primitives*, i.e., the hash functions, and based on this, we expect the proposed scheme has a reasonable implementation speed, whereas we have not yet implemented that and will be done in the future works. Also, one can consider the "*Module-LWE*"-based version of the proposed signature, to achieve a more (expected) secure one, see Remark 6.2.

3 The proposed digital signature

In 2011, as a generalization of the previous LWE-based cryptosystems such as [6,21] and as an instance of Micciancio's proposed system in ref. [26], Lindner–Peikert [25] gave a cryptosystem based on LWE and Ring-LWE problems. The Lindner–Peikert cryptosystem provided smaller keys and ciphertexts by a factor of about $\log q$ and a concrete security stronger than the previous works (by the convention, the base-2 logarithm is denoted by log).

In this article, using the Lindner–Peikert cryptosystem [25], we give a Ring-LWE-based digital signature whose public key/signature sizes lie in the range 1–1.5 kilobytes, along with an easier implementation and a slightly weaker security than the proposed scheme in ref. [25].

Let $R = \frac{\mathbb{Z}[X]}{\langle f(X)\rangle}$ be the *cyclotomic* polynomial ring where $f(X) = X^n + 1$ with n a power of 2. Other properties of this ring such as its security and cyclotomic polynomials, including degrees $n \neq 2$ of the mentioned ring, are discussed in detail in ref. [7]. Suppose that the following considerations hold: $q \in \mathbb{Z}$ is a sufficiently large integer modulus for which $f(x)$ splits into linear (or very low-degree) factors modulo q; $R_q = \frac{Z_q[X]}{f(X)}$; χ_k and χ_e are error distributions over R which are concentrated on "small" elements of R. Hence, the error distributions enable rigorous security proofs (see refs [7] and [25]).

Let Σ be a message alphabet, e.g., $\Sigma = \{0, 1\}$. The message encoder and decoder are functions $encode : \Sigma^n \to R_q$ and $decode : R_q \to \Sigma^n$, such that

$$\text{decode}(\text{encode}(m) + e \bmod q) = m, \quad \text{for any small enough } e \in R. \tag{3.1}$$

As an example consider an e such that for some integer threshold $t \geq 1$, its coefficients as a polynomial in R are all in $[-t, t)$.

Definition 3.1. [25] For $m \in \{0, 1\}$ and a module q, define the functions *encode* and *decode* as follows:

$$\text{encode}: \{0,1\} \to \mathbb{Z}_q, \qquad \text{decode}: \mathbb{Z}_q \to \{0,1\}$$

$$m \mapsto \hat{m} = m \cdot \left\lfloor \frac{q}{2} \right\rfloor, \qquad \hat{m} \mapsto m = \begin{cases} 0, & \text{if } \hat{m} \in \left[-\left\lfloor \frac{q}{4} \right\rfloor, \left\lfloor \frac{q}{4} \right\rfloor \right) \\ 1, & \text{otherwise}. \end{cases}$$

We extend these functions component-wise to vectors.

Remark 3.2. Note that in the above method the error tolerance is $t = \lfloor \frac{q}{4} \rfloor$.

In this protocol, we use a uniformly random $a \in R_q$ that can be generated by a trusted source or it is chosen by the user. Suppose that the signer (from now on will be called *Alice*) wants to sign the message m and send it to the verifier (from now on will be called *Bob*).

- First Alice computes the values $r_1, r_2 \leftarrow \chi_k$ and $\bar{m} = \text{encode}(H(m))$ where H is a **collision-resistant hash function**. The public key consists of the pair $(p = r_1 - ar_2, a) \in R_q^2$ and the secret key is r_2.
- For per-signing, Alice generates $e_i \leftarrow \chi_e$, $i = 1, \ldots, 4$, and Computes the values C_is as follows:

$$C_1 \coloneqq pe_1 + e_2,$$
$$C_2 \coloneqq pae_1 + e_3 + \bar{m},$$
$$C_3 \coloneqq ae_2 + e_4.$$

  Note that following Section 3.1 in ref. [25], we take $a, p, m \in \Sigma^n$.
- The assigned signature to m is the quadruple (C_1, C_2, C_3, h), where

$$h = H(m || H(\text{decode}(ar_2e_1))),$$

  with a *collision-resistant hash function* H. (Note that computing the value of $\text{decode}(ar_2e_1)$ is meaningful, since $ar_2e_1 \in R_q$, see Definition 3.1.)

3.1 Verification

Bob accept a quadruple (C_1, C_2, C_3, h) as a valid signature for the message m (with $\bar{m} = \text{encode}(H(m))$) if the following conditions hold:

(i) $\text{decode}(C_2 - aC_1 + C_3) = H(m)$; note that

$$C_2 - aC_1 + C_3 = pae_1 + e_3 + \bar{m} - ape_1 - ae_2 + ae_2 + e_4 = \text{encode}(H(m)) + \underbrace{e_3 + e_4}_{\text{small}}, \tag{3.2}$$

see the relation (3.1).

(ii) $h = H(m||H(\omega))$, where $\omega = \text{decode}(-C_1)$; note that

$$-C_1 = -pe_1 - e_2 = (ar_2 - r_1)e_1 - e_2 = ar_2e_1 + (\underbrace{-r_1e_1 - e_2}_{\text{small}}) \in R_q, \tag{3.3}$$

which implies that $\text{decode}(-C_1)$ is meaningful as an element of $\{0, 1\}^n$.

Therefore, the signature will be verified as long as the "error terms" $e_3 + e_4$ and $-r_1e_1 - e_2$ are within the error threshold of the function *decode* (see Definition 3.1); these hold with high probability when χ_e and χ_k are sufficiently concentrated.

Remark 3.3. As stated before, the function H in the above scheme is a collision-resistant hash function. For implementation, one may use **SHAKE-128** [27].

3.2 Correctness (decoding)

Based on the error terms which are $e_3 + e_4$ and $-r_1e_1 - e_2$, respectively, in equations (3.2) and (3.3), one can say that the upper bound on the Gaussian parameters of s_k, s_e (respectively, corresponding to χ_k and χ_e) in terms of the desired per-symbol error probability δ in [25, Section 3.2] works here:

Lemma 3.4. [25, Lemma 3.1] *In the above signature scheme, the error probability per-symbol* (*over the choice of secret key*) *is bounded from above by any desired* $\delta > 0$, *as long as*

$$s_k \cdot s_e \leq \frac{\sqrt{2}\pi t}{c \cdot \sqrt{2n \log \frac{2}{\delta}}}, \tag{3.4}$$

where c *is the value that depends only on* n (*greater than* 1), s_k, s_e: *are the Gaussian parameters*, n: *is the dimension of the cyclotomic ring* $R = \frac{\mathbb{Z}[X]}{X^n+1}$, t *is the error tolerance* (*which is* $\left\lfloor \frac{q}{4} \right\rfloor$ *in the encode–decode algorithms in* Definition 3.1), and log *denotes the base-2 logarithm*.

In ref. ([25], Section 3.2) using a per-symbol error probability of $\delta = 0.01$, the parameters in the above lemma (with the decoding failure rate 2^{-40}) are bounded as in Table 1 below.

We will choose parameters for our proposed digital signature in Section 5.

4 Security

The standard security notion for digital signatures is **UF-CMA** security, which is unforgeability under Chosen Message Attacks. In this security model, the adversary gets the public key and has access to a signing oracle to sign messages of his choice. The adversary's goal is to come up with a valid signature of a new message. A slightly stronger security requirement which can be useful sometimes is **SUF-CMA** (Strong Unforgeability under Chosen Message Attacks), which also allows the adversary to win by producing a different signature of a message that he has already seen.

We also take quantum attackers into account. We need to consider the security of the scheme when the adversary can query the hash function on a superposition of inputs (i.e., security in the quantum random oracle model **QROM**). The **UF-CMA** security of our signature scheme is based on two hard assumptions:

- The Decision Ring-LWE assumption which is needed to protect against key-recovery.
- An "intermediate problem" that is the assumption upon which the new message forgery is based. It is based on the combined hardness of the Ring-SIS problem and the cryptography hash function H.

By the decision Ring-LWE assumption, the public key $(p = r_1 - ar_2, a)$ is indistinguishable from (t, a) where t is chosen uniformly at random. Hence, to prove **UF-CMA** security, we only need to analyze the hardness of the experiment where the adversary receives a random (t, a) and then needs to output a valid message/signature pair m, (C_1', C_2', C_3', h') such that

(i) $\text{decode}(C_2' - aC_1' + C_3') = H(m)$;

(ii) $h' = H(m||H(\text{decode}(-C_1')))$.

In particular, a (quantum) adversary who is successful at creating a forgery of a new message is able to find C_1' such that $H(\text{decode}(-C_1')) = H(\text{decode}(ar_2e_1))$ (corresponding to the fixed message m). But (t, a) is completely random, so this is the aforementioned intermediate problem. Note that a standard forking lemma [28] shows that an adversary solving the above problem in the (standard) random oracle model, can be used to solve the Ring-SIS problem.

5 Choosing parameters

Recall that our proposed digital signature has been inspired by the Lindner–Peikert cryptosystem [25]. Hence, we can estimate the concrete security and also compute the space requirements for the Ring-LWE-based digital signature, completely similar to ref. [25]. Note that for any message m with $\text{length}(H(m)) = 128 \leq n$, the public key and signature sizes, respectively, are $2n\log q$ and $3n\log q + 128$ bits.

Remark 5.1. By the convention, the base-2 logarithm is denoted by log.

In the first step we set $s_k = s_e = s > 0$, whereas we can use slightly smaller s_k and correspondingly larger s_e parameters to get a slightly stronger overall security versus a more complicated implementation, see [25, Section 6]. Indeed distinguishing the public key and the components of C_is of a signature (C_1, C_2, C_3, h), from the uniform ones, is not equally hard. It is because compared to the signature, the public key exposes fewer LWE samples (the random polynomials r_1, r_2 are fixed, but the error terms e_i change for per-signing).

The modulus q should be chosen large enough (according to the bounds in Table 1) such that for a Gaussian parameter $s \geq 8$, one has the discrete Gaussian $D_{\mathbb{Z}_q^m,s}$ that approximates the continuous Gaussian D_s as well. On the other hand, as in most lattice-based schemes that are based on operations over polynomial rings, we have to choose our ring so that the multiplication operation has a very efficient implementation via the **Number Theoretic Transform** (**NTT**), see e.g., [29,30], which is just a version of **FFT** that works over the finite field $\mathbb{Z}_q$ rather than over the complex numbers. To enable the NTT, we need to choose a prime number q so that the group $\mathbb{Z}_q^*$ has an element of order $2n$ or equivalently $q \equiv 1(\text{mod } 2n)$. Thereby we

Table 1: Boundaries on parameters taken from [25, Figure 1]

$2n$	$c \geq$	$(s_k.\ s_e)/t \leq$
256	1.35	0.08936
384	1.28	0.07695
512	1.25	0.06824
640	1.22	0.06253

Table 2: The proposed parameter sets inspired from security analysis in ref. [25]

Parameters				Distinguish		Decode		Key sizes (in Bytes)		
n	q	s	ε	δ	log(s)	δ	log(s)	Public key	Secret key	Signature
256	7,681	11.44	2^{-32}	1.0064	84	1.0067	76	826	416	1,255
	(low_security)		2^{-64}	1.0070	67	1.0072	63			
320	7,681	10.95	2^{-32}	1.0052	130	1.0055	117	1,032	520	1564.8
	(recommended)		2^{-64}	1.0056	109	1.0057	108			

"Distinguish" columns show the root-Hermite factors δ needed to obtain respective distinguishing advantages (over the random LWE error vector) and the corresponding logarithmic runtime (in seconds) (according to ref. ([25], Section 5)). The "Decode" columns show the decoding attack introduced in ref. [25], the corresponding root-Hermite factors, and the estimating runtime of the attack (these are by using "LWE-estimator" [33]).

have set $q = 7{,}681$, which slightly reduces the security level compared to the ones proposed in ([25], Section 6), (Tables 2 and 3).

5.1 Estimating the security

In cryptanalysis of the lattice-based cryptography, the hardness of Ring-LWE has been analyzed as a LWE problem. It is because so far the best known attacks do not make use of the ring structure. Indeed, while some new quantum algorithms against Ideal-SVP recently appeared, they do not seem to affect Ring-LWE, see ([31], Section 6.1).

In general, there are two different categories for algorithms solving the LWE problem, namely algorithms solving the LWE problem directly (without targeting the underlying lattice) and solving the LWE problem via lattices ([32], Section III). From the first approach, following ref. [25], we will analyze the security of our scheme against two well-known attacks usually referred to as the *distinguishing attack* and the *decoding attack*. In addition, following ref. [31], we also estimate the security of the proposed algorithm against the *lattice-based attacks*, the second category, which divide into the *primal attack* and the *dual attack*.

In distinguishing attacks, the adversary will be successful if they could distinguish (with some noticeable advantage) an LWE instance $(A, B = A^t s + e)$ from a uniformly random instance. Typically, this distinguishing is enough to break the semantic security of an LWE-based cryptosystem with the same advantage. The decoding attack, introduced by Lindner–Peikert [25], is stronger than the distinguishing attack. In this attack, the secret error vector in the LWE instance can actually be recovered (hence the ciphertext is decrypted) with the same or better advantage. For all the investigated parameter settings in ref. [25] the decoding attack yields a better total effort as a ratio of time/advantage, and it is significantly more efficient in the high-advantage regime (see [25, Section 6] for a complete description of these attacks).

In order to estimate the security of our digital signature against distinguishing attacks, we use the calculations from [25, Section 5]. Following the computations in ref. ([25], Section 5) first a bound

Table 3: Core SVP hardness of our signature scheme

Parameters			Primal attack			Dual attack		
n	q	ξ	m	b	Security level	m	b	Security level
256	7,681	4.568	852	174	62	1,060	168	60
320	7,681	3.188	998	206	95	1,123	198	92

The parameters ξ, b, and m denote the "norm parameter" ([31], Section 6), the block size of the BKZ algorithm [34], and the number of used samples, respectively.

Table 4: Comparing some Ring-LWE-based digital signature schemes

Algorithm	Security level	Key sizes (in Bytes)		
	(bits)	Public key	Secret key	Signature
Ring-TESLA-1 [38]	79	3,100	1,700	1,400
Ring-TESLA-2 [38]	73	3,300	1,800	1,500
GLYPH [39]	137	2,000	300	1,800
BLISS-I [19]	128	875	250	700
BLISS-II [19]	128	875	250	625
BLISS-III [19]	160	875	375	750
BLISS-IV [19]	192	875	375	812.5
GLP (Set I) [18]	<80	1,500	100	900
GLP (Set II) [18]	91	3,100	300	1,900
TESLA# -I [40]	64	3,328	2,112	1,616
TESLA#-II [40]	128	7,168	4,608	3,488
	<70	826	416	1,255
Proposed signature				
	92	1,032	520	1,565

Note that for the proposed scheme, we have considered the "lowest" security level from Tables 2 and 3, namely core SVP hardness against the dual attack.

$\beta = (q/s)\sqrt{\log\left(\frac{1}{\varepsilon}\right)/\pi}$ on the length of a nonzero vector $v \in \Lambda^{\perp}(A)$ is computed. This yields the suitable distinguishing advantage over the random LWE error. After that the root-Hermite factor $\delta = 2^{\frac{(\log(\beta))^2}{4n\log(q)}}$ is found, which gives the needed vector. It should be reminded that this is done under the assumption that the attacker uses the optimal subdimension $m = \sqrt{\frac{n\log(q)}{\log(\delta)}}$ (the root-hermit factor $\delta \geq 1$ is defined exactly the same as in ref. [25]). If the optimal subdimension for this δ exceeds $2n + 128$, then δ is discarded and instead of that the one for which δ^m. $q^{\frac{n}{m}} = \beta$ is taken where $m = 2n + 128$, whereas the latter case does not occur for our parameter sets. We also calculate a lower bound on the BKZ runtime using the conservative estimator from [25, Section 5], namely $t_{\mathrm{BKZ}(\delta)} = \frac{1.8}{\log(\delta)} - 110$.

To implement the analyzing method of decoding attack in ref. [25], we used the "LWE-estimator" [33] and listed the corresponding results in Table 2.

For estimating the security against the primal and the dual attacks, we use the *Core SVP hardness* methodology described in [31, Section 6.1]. Indeed, these two attacks are a subfamily of the BKZ [34] attacks, where the algorithm BKZ proceeds by reducing a lattice basis using an *SVP oracle* in a smaller dimension b. It is known that the number of calls to the oracle remains polynomial, but its evaluating is very arduous which has led to introducing new *heuristic* ideas [31, Section 6.1]. Although, from the defender's point of view, estimating the security based on the *core SVP hardness*, the cost of *one call* to an SVP oracle in dimension b as considered in [31, Section 6.1], will be the most pessimistic method. The results for estimating security of the proposed scheme, against the primal and dual attacks, are summarized in Table 3. (For a full detailed description of the primal attack the dual attack and the core SVP hardness methodology see [31, Section 6].)

Remark 5.2. There are also purely combination attacks on LWE, namely BKW types of attacks [35,36] and linearization attacks [37] that may asymptotically perform better than lattice reduction. Since these attacks generally require more LWE samples than our signature scheme (there are only n sample available), one may rule out these attacks.

Remark 5.3. Note that the security estimation of our digital signature scheme (Table 3) includes the Ring-SIS problem, see Section 4, and the presented method work also for hardness of Ring-SIS problem, see ref. [2].

6 Comparison

In this section, we give a brief comparison between the proposed signature algorithm and a few other Ring-LWE-based algorithms [18,19,38–40]. For comparison, we chose those algorithms that to the best of our knowledge seem more related to our scheme. The results are listed in Table 4, which show that our proposed algorithm has a good trade off between the key sizes and security levels. In particular, it provides relatively shorter keys and signatures among most of the similar schemes.

Remark 6.1. In addition to the comparison in Table 4, one can consider more Ring-LWE-based digital signatures. For instance, the key sizes (public key, secret key, and signature) in refs [13, 41] have $O(n\log n)$ lengths ([41], Table I), which seem very close to the sizes of parameters in our scheme.

Remark 6.2. As an improvement and continuation of this work, one may consider the "Module-LWE-based" version of the proposed scheme. The Module-LWE might be able to offer a better level of security than Ring-LWE and even more compact parameters. Furthermore, Module-LWE has been suggested as an interesting option to hedge against potential attacks that exploit the algebraic structure of Ring-LWE [42].

Acknowledgments: We are so grateful for the many valuable and useful suggestions of the three referees of the first draft.

Conflict of interest: Authors state no conflict of interest.

References

[1] Ajtai M. Generating hard instances of lattice problems (extended abstract). In: Proc. STOC.; 1996. p. 99–108.
[2] Micciancio D, Regev O. Lattice-based cryptography. In: Bernstein DJ, Buchmann J, Dahmen E, editors, Post-quantum Cryptography. Heidelberg, Berlin: Springer; 2009. p. 147–91.
[3] Peikert C. A decade of lattice cryptography. In: Foundations and trends in theoretical computer science. Now Publishers, Inc.; 2016. p. 283–424.
[4] Micciancio D, Goldwasser S. Complexity of Lattice Problems: a cryptographic perspective. In: The Kluwer international series in engineering and computer science. Vol. 671; Springer Science & Business Media; 2002.
[5] Aggarwal D, Dadush D, Regev O, Stephens-Davidowitz N. Solving the shortest vector problem in 2n time via discrete Gaussian sampling. Proc STOC. 2015;42:733–42.
[6] Regev O. On lattices, learning with errors, random linear codes, and cryptography. In: Gabow HN, Fagin R, editors., Proceedings of the 37th ACM Symposium on Theory of Computing (STOC); 2005. p. 84–93.
[7] Lyubashevsky V, Peikert C, Regev O. On ideal lattices and learning with errors over rings. In: Gilbert H, editor, Advances in Cryptology-EUROCRYPT. Vol. 6110, Springer; 2010. p. 1–23.
[8] Lyubashevsky V, Peikert C, Regev O. On ideal lattices and learning with errors over rings. J ACM (JACM). 2013;6:1–35.
[9] Hoffstein J, Pipher J, Silverman JH. NTRU: a ring-based public key cryptosystem. In: Buhler JP, editor. Algorithmic number theory Symposium (ANTS). Vol. 1423; 1998. p. 267–88.
[10] Micciancio D. Generalized compact knapsacks, cyclic lattices, and efficient one-way functions. Computational Complexity. 2007;16(4):365–411.
[11] Lyubashevsky V. Fiat–Shamir with aborts: Applications to lattice and factoring-based signatures. In: Matsui M, editor, Advances in Cryptology – ASIACRYPT 2009. 15th International Conference on the Theory and Application of Cryptology and Information Security. Vol. 5912. Tokyo, Japan. Heidelberg, Berlin: Springer; 2009. p. 598–616.
[12] Goldreich O, Goldwasser S, Halevi S. Public-key cryptosystems from lattice reduction problems. In: Kaliski Jr BS, editor, Advances in Cryptology - CRYPTO '97, 17th Annual International Cryptology Conference. Vol. 1294. Santa Barbara, California, USA: Springer; 1997. p. 112–31.
[13] Hoffstein J, Howgrave-Graham N, Pipher J, Silverman JH, Whyte W. NTRUSIGN: digital signatures using the NTRU lattice. In: Joye M, editor, Topics in Cryptology - CT-RSA 2003, The Cryptographers? Track at the RSA Conference 2003. Vol. 2612. San Francisco, CA, USA: Springer; 2003. p. 122–40.
[14] Nguyen PQ, Regev O. Learning a parallelepiped: cryptanalysis of GGH and NTRU signatures. J Cryptol. 2009;22:139–60.

[15] Ducas L, Nguyen PQ. Learning a zonotope and more: Cryptanalysis of NTRUSign countermeasures. In: Wang X, Sako K, editors., Advances in Cryptology – ASIACRYPT 2012 – 18th International Conference on the Theory and Application of Cryptology and Information Security. Vol. 7658. Beijing, China: Springer; 2012. p. 433–50.
[16] Fiat A, Shamir A. How to prove yourself: Practical solutions to identification and signature problems. In: Odlyzko AM, editor, Advances in Cryptology - CRYPTO '86. Vol. 263. Santa Barbara, California, USA: Springer; 1986. p. 186–94.
[17] Lyubashevsky V. Lattice signatures without trapdoors. In: Pointcheval D, Johansson T, editors, Advances in Cryptology – EUROCRYPT 2012 – 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques. Vol. 7237. Cambridge, UK: Springer; 2012. p. 738–55.
[18] Güneysu T, Lyubashevsky V, Pöppelmann T. Practical latticebased cryptography: A signature scheme for embedded systems. In: Prouff E, Schaumont P, editors, Cryptographic Hardware and Embedded Systems - CHES 2012 – 14th International Workshop. Vol. 7428. Leuven, Belgium: Springer; 2012. p. 530–47.
[19] Ducas L, Durmus A, Lepoint T, Lyubashevsky V. Lattice signatures and bimodal Gaussians. In: Canetti R, Garay JA, editors., CRYPTO. Vol. 8042. Springer; 2013. p. 40–56. Full version available at http://eprint.iacr.org/2013/383.pdf.
[20] Bai S, Galbraith SD. An improved compression technique for signatures based on learning with errors. In: Benaloh J, editor, Topics in Cryptology - CTRSA 2014 – The Cryptographer's Track at the RSA Conference 2014. Vol. 8366. San Francisco, CA, USA: Springer; 2014. p. 28–47.
[21] Gentry C, Peikert C, Vaikuntanathan V. Trapdoors for hard lattices and new cryptographic constructions. STOC. 2008;197–206.
[22] Cash D, Hofheinz D, Kiltz E, Peikert C. Bonsai trees, or how to delegate a lattice basis. In: Gilbert H, editor, EUROCRYPT. Vol. 6110. Springer; 2010. p. 523–52.
[23] Micciancio D, Peikert C. Trapdoors for lattices: Simpler, tighter, faster, smaller. In: Pointcheval D, Johansson T, editors., EUROCRYPT. Vol. 7237. Springer; 2012. 700–18.
[24] Chen Y, Lombardi A, Ma F, Quach W. Does Fiat–Shamir require a cryptographic hash function? In: Annual International Cryptology Conference. Cham: Springer; 2021. p. 334–63.
[25] Lindner R, Peikert C. Better key sizes (and attacks) for LWE-based encryption. In: Cryptographers' Track at the RSA Conference. Berlin, Heidelberg: Springer; 2011.
[26] Micciancio D. Duality in lattice cryptography. In: Proceedings of the Public Key Cryptography; 2010.
[27] National Institute of Standards and Technology. FIPS PUB-SHA standard: Permutation-based hash and extendable-output functions; 2015. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.
[28] Pointcheval D, Stern J. Security proofs for signature schemes. In: Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques. Springer; 1996. p. 387–98.
[29] Gaborit P. Post-Quantum Cryptography. In: 5th International Workshop, PQCrypto. 2013.
[30] Aguilar-Melchor C, Barrier J, Fousse L, Killijian MO. XPIR: Private information retrieval for everyone. Proc Privacy Enhancing Technol. 2016;2:155–74.
[31] Alkim E, Ducas L, Pöppelmann T, Schwabe P. Post-quantum key exchange-a new hope. In: Proceedings of the 25th USENIX Security Symposium. USENIX Association; 2016. p. 327–43.
[32] Mariano A, Laarhoven T, Correia F, Rodrigues M, Falcao G. A practical view of the state-of-the-art of lattice-based cryptanalysis. In: IEEE Access; 2017. p. 24184–202.
[33] Albrecht MR, Curtis BR, Deo A, Davidson A, Player R, Postlethwaite EW, et al. Estimate all the LWE, NTRU schemes!. In: International Conference on Security and Cryptography for Networks. Cham: Springer; 2018. p. 351–67. https://lwe-estimator.readthedocs.io/en/latest/index.html.
[34] Chen Y, Nguyen P. BKZ 2.0: Better lattice security estimates. In: HoonLee D, Wang X, editors., Advances in Cryptology – ASIACRYPT. Vol. 7073. Heidelberg, Berlin: Springer; 2011. p. 1–20.
[35] Blum A, Kalai A, Wasserman H. Noise-tolerant learning, the parity problem, and the statistical query model. J ACM. 2003;50:506–19.
[36] Wagner D. A generalized birthday problem. In: Proceedings of the Annual International Cryptology Conference. Springer; 2002. p. 288–304.
[37] Arora S, Ge R. New algorithms for learning in presence of errors. In: International Colloquium on Automata, Languages, and Programming. Berlin, Heidelberg: Springer; 2011. p. 403–15.
[38] Chopra A. Improved Parameters for the Ring-TESLA Digital Signature Scheme. IACR Cryptol. ePrint Arch. 2016: 1099, 2016.
[39] Chopra A. GLYPH: A New Insantiation of the GLP Digital Signature Scheme. IACR Cryptol. ePrint Arch. 2017: 766, 2017.
[40] Barreto PSLM, Longa P, Naehrig M, Ricardini JE, Zanon G. Sharper Ring-LWE Signatures. IACR Cryptol. ePrint Arch. 2016: 1026 2016.
[41] Wu Y, Huang Z, Zhang J, Wen Q. A lattice-based digital signature from the Ring-LWE. In: 3rd IEEE International Conference on Network Infrastructure and Digital Content; 2012. p. 646–51.
[42] Cramer R, Ducas L, Wesolowski B. Short stickelberger class relations and application to ideal-svp. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. Cham: Springer; 2017. p. 324–48.