Towards Tightly Secure Short Signature and IBE

Xavier Boyen, Qinyi Li

Queensland University of Technology, Brisbane, Australia

Abstract

Constructing short signatures with tight security from standard assumptions is a long-standing open problem. We present an adaptively secure, short (and stateless) signature scheme, featuring a constant security loss relative to a conservative hardness assumption, Short Integer Solution (SIS), and the security of a concretely instantiated pseudorandom function (PRF). This gives a class of tightly secure short lattice signature schemes whose security is based on SIS and the underlying assumption of the instantiated PRF.

Our signature construction further extends to give a class of tightly and adaptively secure "compact" Identity-Based Encryption (IBE) schemes, reducible with constant security loss from Regev's vanilla Learning With Errors (LWE) hardness assumption and the security of a concretely instantiated PRF. Our approach is a novel combination of a number of techniques, including Katz and Wang signature, Agrawal et al. lattice-based secure IBE, and Boneh et al. key-homomorphic encryption.

Our results, at the first time, eliminate the dependency between the number of adversary's queries and the security of short signature/IBE schemes in the context of lattice-based cryptography. They also indicate that tightly secure PRFs (with constant security loss) would imply tightly, adaptively secure short signature and IBE schemes (with constant security loss).

1 Introduction

Short signatures are useful and desirable for providing data authenticity in low-bandwidth and/or high-throughput applications where many signatures have to be processed very quickly. Most digital signature schemes are based on computationally hard problems on specific algebraic groups, e.g., finite fields, curves, and lattices. A signature is "short" if the signature consists in a (small) constant number of group elements (e.g., field elements or lattice points).

Although bare-bones signatures can be obtained from very weak assumptions (e.g., collision-resistant hash functions), constructing efficient short signatures satisfying standard security requirements (e.g., existential unforgeability under adaptively chosen-message attacks), from reasonable assumptions, appears to be a challenging task. Some of the existing short signature schemes use random oracles, e.g., [20, 10, 48, 36, 50], or rely on non-standard computational assumptions (strong, interactive assumptions, and/or q-type parametric assumptions), e.g., [34, 30, 33, 16, 26], or require signers to maintain state across signatures, e.g., [45].

The first short signature scheme from a reasonable and non-parametric assumption without random oracles was proposed by Waters [56]. Hohenberger and Waters later proposed a short signature scheme from standard RSA [46]. Lattice-based short signatures from the very mild SIS assumption in the standard model were proposed in [21, 51]. Recently, the "confined guessing" technique developed by Böhl et al. [13] has produced short signatures from standard RSA and bilinear-group CDH assumptions, and also from the ring-SIS/SIS assumption in combination with lattice techniques [32, 4] with very loose reductions.

Despite these elegant constructions, signature schemes that are *short* and enjoy *tight security* reductions to *standard assumptions* in the *standard model* (without random oracle), remain

unknown. Existing tightly secure signature schemes either have large signature size, e.g., [43, 1, 11], or merely have heuristic security arguments based on random oracles, e.g., [48, 38]. We have not been able to ascertain the earliest occurrence of this long-standing folklore problem in cryptography, but here [11] is one recent formulation:

> *Open Problem #1*—**Tightly Secure Short Signatures**
> "Construct a tightly secure and short (in the sense that the signature contains constant number of group elements or vectors and the security loss is a constant) signature scheme from standard assumptions." —Blazy, Kakvi, Kiltz, Pan (2015)

1.1 Tight Security

The reductionist approach to cryptographic security algorithms seeks to prove theorems along the lines of: "If a t-time adversary attacks the scheme with successful probability ϵ, then a t'-time algorithm can be constructed to break some computational problem with success probability $\epsilon' = \epsilon/\theta$ and $t' = k \cdot t + o(t)$.". The parameters $\theta \geq 1$ and $k \geq 1$, or more simply the product $k \cdot \theta$, measures how tightly the security of the cryptographic scheme is related to the hardness of the underlying computational problem. Alternatively, when $k \approx 1$ as is the case in many reductions, θ measures the security loss of the security reduction of our cryptographic scheme from the underlying assumption. A cryptographic scheme is *tightly secure* if θ is a small constant that in particular does not depend on parameters under the adversary's control, such as the adversary's own success probability ϵ, the number of queries it chooses to make, and even the scheme's security parameter. The reduction phrases "almost tight security" from the literature refers to the case where θ only depends on a small polynomial of the security parameter.

Tight reduction is an elegant notion from a theoretical point of view. A tight reductionist proof (with respect to a well-defined security model) indicates that the security of a cryptographic scheme is (extremely) closely related to the hardness of the underlying hard problem, which is the optimal case we expect from provable security theory. On the other hand, it is also a determinant factor to the practicality of real-world security. Its opposite, loose security, means that in order to realise a desired "real" target security level, one has to increase the "apparent" security level inside the construction to compensate for the loose reduction. This inflates the size of data atoms by some polynomial, with in turn increases the running time of cryptographic operations by another polynomial, combining multiplicatively.

1.2 Identity-Based Encryption with Tight Security

Digital signatures and identity-based encryption (IBE) are closely connected, which suggests that techniques that improve upon the security of signatures might also improve upon the security of IBE. In this work, we also investigate the problem of constructing tightly secure IBE from standard assumptions (without random oracles).

In an IBE system, any random string that uniquely represents a user's identity, such as email address or driver license number, can act as a public key (within a certain domain or realm). Encryption uses this identity, together with some common domain-specific public parameters, to encrypt messages. Users are issued private decryption keys corresponding to their public identities, by a trusted authority (or distributed authorities) called Private Key Generator (PKG) which hold(s) (shares of) the master secret key for a domain. Decryption succeeds if the identity associated with the ciphertext matches the identity associated with the private key, in the same domain.

The strongest, most natural and most widely accepted notion of security for IBE is the *adaptive* security model or *full* security model, formally defined in [18]. In this model, the adversary is able to announce its target (the challenge identity it wants to attack) at any time during the course of its adaptive interaction with the system. Without the luxury of random

oracles, an easier security model to achieve was the *selective* security model, where the adversary must announce its target identity at the onset of its interaction with the system.

In the last fifteen years, a great many IBE schemes have been proposed, with varying efficiency, security models, hardness assumptions, and other features. In the standard model (i.e., without random oracles or other idealised oracles), we mention several notable IBE schemes which have been constructed from bilinear maps in the selective model [27, 14] and the adaptive model [15, 56, 35, 57, 29, 12], and from lattices in the adaptive model [2, 28, 5]. It is fair to say that, by now, the art of selectively secure IBE has been well honed. However, adaptively secure IBE schemes from standard assumptions with tight security (in the sense that the security loss is a small constant) remain unknown. The best known adaptively secure IBE schemes in terms of tight reduction are based on linear assumptions over pairings and achieve almost tight security (e.g., [29, 12, 6, 44]). Waters [56] states this open problem as follows:

> *Open Problem #2*—**Tight Adaptively Secure IBE**
> "Construct a tightly, adaptively secure IBE scheme from standard computational hardness assumptions without random oracles." —Waters (2005)

Furthermore, for all known directly constructed adaptively secure IBE scheme from standard post-quantum assumption (specifically the LWE assumption), i.e. [2, 28, 5], their security loss during reduction depends on the number adversary's of queries. That is there is current no even "almost tightly" secure adaptive IBE scheme based on standard computational problems which are conjectured to be hard under quantum attacks. The following problem is still open.

> *Open Problem #3*—**"Almost" Tight Adaptively Secure, Post-Quantum IBE**
> "Construct an "almost" tightly, adaptively secure IBE scheme from standard post-quantum assumptions without random oracles."

1.3 Our Results

Our work uses pseudorandom functions (PRFs). Recall a PRF is a (deterministic) function: $\mathsf{PRF} : \mathcal{K} \times \mathcal{D} \to \mathcal{R}$ with the following security property. For random secret key $K \xleftarrow{\$} \mathcal{K}$, $\mathsf{PRF}(K, \cdot)$ is computationally indistinguishable from a random function $\Omega : \mathcal{D} \to \mathcal{R}$, given oracle access to either $\mathsf{PRF}(K, \cdot)$ or $\Omega(\cdot)$. PRFs can be constructed from general assumptions (e.g., the existence of pseudo-random number generators [39]), number-theoretic assumptions (e.g., the DDH/k-LIN assumption [53, 31, 47]), and lattice assumption LWE [9, 8].

Our contribution is a construction of a class of adaptively secure short signature schemes/IBE schemes in the standard model. The schemes' security is tightly related to SIS/LWE and the security of an instantiated PRF PRF in the sense that the security loss is a nearly optimal constant factor. More precisely, let ϵ and ϵ' be the advantage of an adversary in attacking our signature and IBE schemes respectively, ϵ_{SIS} and ϵ_{LWE} be the security level of the SIS and LWE assumptions on which our schemes are based, and ϵ_{PRF} is the security level of the PRF instantiation PRF. Our constructions provide the following: $\epsilon \approx 2(\epsilon_{\mathsf{SIS}} + \epsilon_{\mathsf{PRF}})$, $\epsilon' \approx 2(\epsilon_{\mathsf{LWE}} + \epsilon_{\mathsf{PRF}})$, and the (polynomial) runtime of reduction is approximately the same as attacker's runtime.

Note that, depending on the underlying hardness assumption and the reduction of PRF, underlying assumptions and tightness of our signature/IBE scheme vary. By instantiating existing lattice-based/number theoretic-based PRFs, we obtain the following improvements upon known results:

- By instantiating the "almost" tightly secure PRFs from [9, 8] which are based on LWE assumption with super-polynomial modulus, we obtain the first "almost" tightly secure short signature/IBE schemes from LWE with super-polynomial modulus whose security does not depend on the number of adversarial queries. Previously, the known lattice signature schemes either enjoy short signatures but loose reduction (such as [21, 51, 32])

or have tight reduction but signatures consisting of a rather large number of lattice points ([11]), and the known adaptively secure lattice-based IBE schemes ([2, 5]) have loose reductions. This, at the first time, eliminates the dependency between the number of adversary's queries and the security of lattice-based short signature scheme/IBE scheme.

- If we relex the requirement of quantum resistance, by instantiating the (black-box) tightly secure PRFs based on DDH or k-LIN, whose security loss is only $O(\log^2 \lambda)$ for security parameter λ, due to Jager [47], we obtain the IBE scheme with tightest security reduction so far: a factor of $O(\log^2 \lambda)$. Previous IBE schemes with almost tight security [29, 12] have a factor of $O(\lambda)$ of security loss. This improvement brings us closer again to answering the Open Problem #1 and #2.

Meanwhile, an interesting and independent contribution of our work is that it indicates that tightly secure PRFs, which are efficiently computable by Boolean circuits, from standard computational assumptions are sufficient for us to build tightly, adaptively secure lattice signature/IBE from SIS/LWE assumption.

Finally, we note that many existing provably secure PRF constructions, for instance the DDH-based constructions from [53, 31, 47] and lattice-based constructions from [9, 8], are efficient and can be computed by Boolean circuits in NC^1 class. Instantiating a PRF circuits from these candidates in our construction results in polynomial SIS/LWE modulus in our construction (not the modulus for LWE-based PRFs). On the other hand, however, the (direct) lattice-based PRFs from [9, 8] assume LWE assumption with super-polynomial modulus, which makes our schemes rely on LWE assumption for super-polynomial modulus. How to construct efficient and low-depth PRFs from LWE with polynomial modulus remains an interesting open question.

Table 1 provides a comparison between our signature scheme with a LWE-based PRF instantiation (from [9]) and a representative sample of the prominent lattice-based (quantum-safe) signature schemes from the literature. Note, Katz and Wang did not propose a SIS-based signature scheme in [48]. The scheme we refer to is a straightforward application of Katz-Wang's proof technique to GPV'08 signature scheme. Table 2 provides a comparison between our signature scheme with DDH-based PRF instantiation from [47], which only looses a factor $O(\log^2 \lambda)$ in security proof, and the representative signature schemes from traditional number-theoretic assumptions, including (strong) RSA, Dlog and linear assumptions over pairings. All of those assumptions are not conjectured to be quantum-safe. In each case, the two tables refer to conjectured quantum safe and quantum-unsafe constructions respectively. Table 3 gives a comparison between our IBE scheme (with both direct LWE-based PRF instantiation from [9] and DDH-based instantiation from [47]) and a representative selection of existing IBE schemes from the literature.

It needs to mention that the bit length of PRF secret key determines the number of public matrices in our constructions. In the SIS-based signature scheme from [21] and LWE-based IBE schemes from [2, 28], the number of public matrices are determined by the bit length of messages and identities respectively. For the provably secure PRFs, the bit length of secret key is usually significantly larger than the bit length of messages and identities needed in [21, 2, 28]. So our constructions have larger concrete size of verification key than the signature scheme in [21] and larger concrete size of public parameters than the IBE schemes in [2, 28].

Efficiency Consideration. Though we focus on tightness of reduction in the context of short signature and IBE, we do not hide the inefficiency of our schemes, particularly with comparison to the adptively secure lattice-based signature/IBE scheme obained from the "complexity leveraging" [14] of efficient selectively secure lattice-based signature/IBE scheme such as [2]. Although complexity leveraing is not very satisfactory from a theoretical perspective, it indeed often leads to the most practical secure cryptographic schemes. In the context of IBE, we have seen that the adaptively secure IBE scheme levearaged from selective DBDH-based IBE scheme

Table 1: Comparison between signature schemes from quantum-safe (Ring-)SIS assumption

Scheme	Signature size	Security loss	Assumption(s)	Standard model?
KW'03 [48]	$O(1) \times \mathbb{Z}^m$	$O(1)$	SIS, $\beta = \tilde{\Omega}(n^{3/2})$	ROM
GPV'08 [36]	$O(1) \times \mathbb{Z}^m$	$O(q_{\text{hash}})$	SIS, $\beta = \tilde{\Omega}(n^{3/2})$	ROM
Boyen'10 [21]	$O(1) \times \mathbb{Z}^m$	$O(\lambda q_s)$	SIS, $\beta = \tilde{\Omega}(n^{7/2})$	✔
Lyu'12 [50]	$O(1) \times \mathbb{Z}^m$	$O(\lambda q_s)$	SIS, $\tilde{\Omega}(n^{3/2})$	ROM
MP'12 [51]	$O(1) \times \mathbb{Z}^m$	$O(\lambda q_s)$	SIS, $\beta = \tilde{\Omega}(n^{5/2})$	✔
BHJKSS'13 [13]	$O(\log \lambda) \times \mathbb{Z}^m$	$O(\lambda q_s)$	SIS, $\beta = \tilde{\Omega}(n^{5/2})$	✔
DM'14 [32]	$O(1) \times \mathcal{R}_q^{O(\log q)}$	$O(\lambda q_s)$	Ring-SIS, $\beta = \tilde{\Omega}(n^{7/2})$	✔
BKKP'15 [11]	$O(\lambda) \times \mathbb{Z}^m$	$O(1)$	SIS, $\beta = \tilde{\Omega}(n^{3/2})$	✔
Alperin'15 [4]	$O(1) \times \mathbb{Z}^m$	$O(\lambda q_s)$	SIS, $\beta = \tilde{\Omega}(\delta^{2\delta} \cdot n^{11/2})$	✔
Ours	$O(1) \times \mathbb{Z}^m$	$O(\lambda)$	SIS+LWE*, $\beta = \tilde{\Omega}(\ell^{4c} \cdot n^{7/2})$	✔

λ is the security parameter, n is the lattice hardness parameter, m is the lattice dimension, and β is the SIS parameter. q_{hash} is the number of random-oracle queries (if applicable). q_s is the number of signing queries. For DM'14, the ring $\mathcal{R} = \mathbb{Z}_q[X]/(f(X))$ for some cyclotomic polynomial f of degree n and $q \geq \beta\sqrt{n}\omega(\sqrt{\log n})$. For Alperin'15, δ satisfies $2q_s^2/\epsilon < 2^{\lfloor c'^\delta \rfloor}$ for attacker's success probability ϵ and arbitrary constant $c' > 1$. Our construction here consider instantiation of the direct LWE-based PRF from [9] which has security loss $O(\lambda)$ and can be computed by a NC^1 circuit with input length ℓ and depth $c \log \ell$ for some constant $c > 1$.
* The security of direct LWE-based PRF construction from [9] relies on LWE assumption with super-polynomial modulus. So LWE here refers to LWE assumption with super-polynomial modulus.

in [14] has higher real-world efficiency than the adaptively secure Waters IBE scheme [56] (as well as the subsequent adaptive IBE schemes from similar standard pairing assumptions without random oracles) for the same security level. This may seem counter-intuitive, but to design adaptively secure IBE schemes one needs to carefully embed some specially crafted complex structures into the scheme, to provide enough freedom for the security reduction. This makes directly constructed adaptive IBE schemes rather bulky. Therefore, our current results are of more theoretic value. One the other hand, directly constructing adaptively secure schemes from standard assumptions usually requires new proof ideas and techniques which advance the state-of art and lead to further applications. Trying to get tighter reduction for the directly constructed adaptively secure schemes should be always welcome as it remains a very promising way of bridging the efficiency gap.

1.4 Overview of Our Approach

Construction Outline. Our constructions use a PRF $\mathsf{PRF} : \{0,1\}^k \times \{0,1\}^t \to \{0,1\}$ which takes as input a truly random secret key from $\{0,1\}^k$ and a string from $\{0,1\}^t$, and deterministically outputs a bit which is computationally indistinguishable from a random bit. In our signature scheme, apart from the "left" matrix $\mathbf{A}$ typical of all SIS/LWE based constructions, we set another $4 + k$ random matrices from $\mathbb{Z}_q^{n \times m}$, comprising: two "signature subspace selection" matrices $\mathbf{A}_0, \mathbf{A}_1$, k "PRF secret key" matrices $\{\mathbf{B}_i\}_{i \in [k]}$, and two "message representation" matrices $\mathbf{C}_0, \mathbf{C}_1$. The key generation algorithm further expresses PRF as a NAND Boolean circuit, which serves as a part of the public parameters or perhaps a common reference string. The signing key is a "short" basis $\mathbf{T}_{\mathbf{A}}$ of $\mathbf{A}$ and a PRF key $K \xleftarrow{\$} \{0,1\}^k$ for PRF.

The signer takes three steps to generate the signature of message $\mathsf{M} = x_1 x_2 \ldots x_t \in \{0,1\}^t$.

Table 2: Comparison between signature schemes from various quantum-unsafe assumptions

Scheme	Sig. size	Sec. loss	Assumption(s)	Standard model?
GHR'99 [34]	$O(1) \times \mathbb{Z}_N$	$O(1)$	Strong-RSA + D-I Hash	✔
BLS'01 [20]	$O(1) \times \mathbb{G}$	$O(\lambda q_s)$	CDH	ROM
KW'03 [48]	$O(1) \times \lvert\mathcal{D}\rvert$	$O(1)$	CFP	ROM
BB'04 [16]	$O(1) \times \mathbb{G}$	$O(1)$	q_s-SDH	✔
Waters'05 [56]	$O(1) \times \mathbb{G}$	$O(\lambda q_s)$	CDH	✔
HW'09 [46]	$O(1) \times \mathbb{Z}_N$	$O(\lambda q_s)$	RSA	✔
BHJKSS'13 [13]	$O(1) \times \mathbb{G}$	$O(\lambda q_s)$	DLog	✔
BHJKSS'13 [13]	$O(1) \times \mathbb{Z}_N$	$O(\lambda q_s)$	RSA	✔
ADKMO'13 [1]	$O(\lambda) \times \mathbb{G}$	$O(1)$	DLIN	✔
CW'13 [29]	$O(k) \times \mathbb{G}$	$O(\lambda)$	k-LIN	✔
BKP'14 [12]	$O(k) \times \mathbb{G}$	$O(\lambda)$	k-LIN	✔
BKKP'15 [11]	$O(\lambda) \times \mathbb{G}$	$O(1)$	DLog	✔
BKKP'15 [11]	$O(\lambda) \times \mathbb{Z}_N$	$O(1)$	RSA,FAC	✔
Ours	$O(1) \times \mathbb{Z}^m$	$O(\log^2 \lambda)$	SIS+DDH, $\beta = \tilde{\Omega}(\ell^{4c} \cdot n^{7/2})$	✔

λ is the security parameter, n is the lattice hardness parameter, m is the lattice dimension, q_s the number of signing queries, N is the RSA modulus, m is the lattice dimension, β is the SIS parameter, and k is a non-adversary-query-dependent parameter of the LIN assumption. For GHR'99, D-I hash stands for division-intractable hash. For KW'03, $|\mathcal{D}|$ the domain size of the instantiated claw-free permutation, which is abbreviated as CFP. Our construction here consider instantiating the DDH-based PRF from [47] which has security loss $O(\log^2 \lambda)$ and can be computed by a NC^1 circuit with input length ℓ and depth $c \log \ell$ for some constant $c > 1$.

Firstly, it uses the key-homomorphic evaluation algorithm developed from [37, 19, 24] [1] to compute the unique matrix $\mathbf{A}_{\mathsf{PRF},\mathsf{M}}$ from the circuit of PRF and the $k+t$ matrices $\{\mathbf{B}_i\}_{i\in[k]}, \mathbf{C}_{x_1}, \mathbf{C}_{x_2}, \ldots, \mathbf{C}_{x_t}$. [2] Then it computes $b = \mathsf{PRF}(K, \mathsf{M})$ and sets the matrix $\mathbf{F}_{\mathsf{M},1-b} = [\mathbf{A} \mid \mathbf{A}_{1-b} - \mathbf{A}_{\mathsf{PRF},\mathsf{M}}] \in \mathbb{Z}_q^{n\times 2m}$. Finally, it applies the trapdoor $\mathbf{T}_\mathbf{A}$ to generate the signature: a low-norm non-zero vector $\mathbf{d}_\mathsf{M} \in \mathbb{Z}^{2m}$ such that $\mathbf{F}_{\mathsf{M},1-b} \cdot \mathbf{d}_\mathsf{M} = \mathbf{0} \pmod q$. The verification algorithm checks whether the signature is a non-zero vector in $\mathbb{Z}^{2m}$ and has low-norm, and whether $\mathbf{F}_{\mathsf{M},b} \cdot \mathbf{d}_\mathsf{M} = \mathbf{0} \pmod q$ or $\mathbf{F}_{\mathsf{M},1-b} \cdot \mathbf{d}_\mathsf{M} = \mathbf{0} \pmod q$. If all these conditions are satisfied, the signature is accepted.

Our IBE scheme works as follows. The public parameters contain matrices $\mathbf{A}$, $\mathbf{A}_0$, $\mathbf{A}_1$, $\{\mathbf{B}_i\}_{i\in[k]}$, $\mathbf{C}_0, \mathbf{C}_1$, a secure PRF PRF represented as a NAND Boolean circuit, and a random vector $\mathbf{u} \in \mathbb{Z}_q^n$ which is used to hide messages. The trapdoor basis $\mathbf{T}_\mathbf{A}$ and a secret PRF key $K \xleftarrow{\$} \{0,1\}^k$ serve as master secret key. In private key generation for identity $\mathsf{id} = x_1 x_2 \ldots x_t \in \{0,1\}^t$, the key-homomorphic evaluation algorithm is invoked to compute the unique matrix $\mathbf{A}_{\mathsf{PRF},\mathsf{id}}$ from the circuit of PRF and the $k+t$ matrices $\{\mathbf{B}_i\}_{i\in[k]}, \mathbf{C}_{x_1}, \mathbf{C}_{x_2}, \ldots, \mathbf{C}_{x_t}$. It then sets the "function" matrix to $\mathbf{F}_{\mathsf{id},1-b} = [\mathbf{A} \mid \mathbf{A}_{1-b} - \mathbf{A}_{\mathsf{PRF},\mathsf{id}}] \in \mathbb{Z}_q^{n\times 2m}$ for $b = \mathsf{PRF}(K, \mathsf{M})$, and uses $\mathbf{T}_\mathbf{A}$ to sample a Gaussian vector $\mathbf{d}_\mathsf{id} \in \mathbb{Z}^{2m}$ as private identity key where $\mathbf{F}_{\mathsf{id},1-b} \cdot \mathbf{d}_\mathsf{id} = \mathbf{u} \pmod q$.

To encrypt a message $\mathsf{Msg} \in \{0,1\}$ with an identity id, the encryptor computes $\mathbf{A}_{\mathsf{PRF},\mathsf{id}}$ and sets two "function" matrices $\mathbf{F}_{\mathsf{id},b} = [\mathbf{A} \mid \mathbf{A}_b - \mathbf{A}_{\mathsf{PRF},\mathsf{id}}]$ and $\mathbf{F}_{\mathsf{id},1-b} = [\mathbf{A} \mid \mathbf{A}_{1-b} - \mathbf{A}_{\mathsf{PRF},\mathsf{id}}]$. It

[1] We will particularly use the evaluation algorithm due to Brakerski and Vaikuntanathan [24] for optimizing the SIS/LWE modulus.

[2] It can be shown that for different massages $\mathsf{M}_0 \neq \mathsf{M}_2$ $\mathbf{A}_{\mathsf{PRF},\mathsf{M}_0} \neq \mathbf{A}_{\mathsf{PRF},\mathsf{M}_1}$ with all but negligible probability. See section 3.3 for details.

Table 3: Comparison between adaptively secure IBE schemes from various assumptions

Scheme	Security loss	Assumption	Standard model?	Quantum-safe
BF'01 [18]	$O(q_{\mathsf{id}})$	BDH	ROM	✗
KW'03 [48]	$O(1)$	BDH	ROM	✗
BB'04a [14]	$O(2^{\lambda})$	DBDH, q_{id}-BDHI	✔	✗
BB'04b [15]	$O(\lambda q_{\mathsf{id}})$	DBDH	✔	✗
Waters'05 [56]	$O(\lambda q_{\mathsf{id}})$	DBDH	✔	✗
Gentry'06 [35]	$O(1)$	q_{id}-ABDHE	✔	✗
GPV'08 [36]	$O(q_{\mathrm{hash}})$	LWE	ROM	✔
Waters'09 [57]	$O(q_{\mathsf{id}})$	DBDH	✔	✗
ABB'10 [2]	$O(\lambda q_{\mathsf{id}})$	LWE	✔	✔
CHKP'12[28]	$O(\lambda q_{\mathsf{id}})$	LWE	✔	✔
LW'12 [49]	$O(q)$	DLIN	✔	✗
CW'13 [29]	$O(\lambda)$	k-LIN	✔	✗
BKP'14 [12]	$O(\lambda)$	k-LIN	✔	✗
Ours	$O(\lambda)$	LWE *	✔	✔
	$O(\log^2(\lambda))$	DDH†+LWE	✔	✗

λ is the security level, q_{id} the number of private key queries and q_{hash} the number of random-oracle queries (if applicable). * Here we instantiate the PRF by direct LWE-based PRF construction from [9] which has $O(\lambda)$ security loss and relies on LWE assumption with super-polynomial modulus. So the LWE here refers to LWE assumption with super-polynomial modulus. The schemes ABB'10 and CHKP'12 assume LWE assumption polynomial modulus. † Here we instantiate the PRF by DDH-based PRF construction from [47] which has (black-box) security loss $O(\log^2(\lambda))$.

generates two independent GPV-style ciphertexts [36]. The first one uses $\mathbf{F}_{\mathsf{id},b}$:

$$\begin{cases} c_{b,0} &= \mathbf{s}_b^{\top}\mathbf{u} + \nu_{b,0} + \mathsf{Msg}\cdot\lfloor q/2\rfloor \\ \mathbf{c}_{b,1}^{\top} &= \mathbf{s}_b^{\top}\mathbf{F}_{\mathsf{id},b} + \boldsymbol{\nu}_{b,1}^{\top} \end{cases}$$

and the second is based on $\mathbf{F}_{\mathsf{id},1-b}$:

$$\begin{cases} c_{1-b,0} &= \mathbf{s}_{1-b}^{\top}\mathbf{u} + \nu_{1-b,0} + \mathsf{Msg}\cdot\lfloor q/2\rfloor \\ \mathbf{c}_{1-b,1}^{\top} &= \mathbf{s}_{1-b}^{\top}\mathbf{F}_{\mathsf{id},1-b} + \boldsymbol{\nu}_{1-b,1}^{\top} \end{cases}$$

for random vectors $\mathbf{s}_b, \mathbf{s}_{1-b} \xleftarrow{\$} \mathbb{Z}_q^n$, two small noise scalars $\nu_{b,0}, \nu_{1-b,0}$, and two low-norm noise vectors $\boldsymbol{\nu}_{b,1}, \boldsymbol{\nu}_{1-b,1}$.

The decryption algorithm uses $\mathbf{d}_{\mathsf{id}}$ to try both ciphertexts; one of them should work. Here as a technical caveat, we need some redundant information in the messages in order to check whether a recovered message is well-formed. To this end, one option is to apply the standard way of encrypting multiple bits in GPV-style ciphertexts without affecting the security analysis. That is, instead of using just a vector $\mathbf{u} \in \mathbb{Z}_q^n$ in the public key, we use a matrix $\mathbf{U} \in \mathbb{Z}_q^{n\times z}$ allowing us to encrypt z bits. A second option, which costs nothing if hybrid encryption is being used, is to use multi-bit GPV-style encryption to encrypt a symmetric session key without redundancy, again using a matrix $\mathbb{Z}_q^{n\times z}$ and rely on downstream symmetric integrity checks or MACs to weed out the incorrect ciphertexts.

Proof Outline. The security reduction of our signature scheme uses an efficient adversary to solve a of SIS problem instance $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$: a short non-zero vector $\mathbf{e} \in \mathbb{Z}^m$ such that

$\mathbf{Ae} = \mathbf{0} \pmod q$. The reduction embeds a randomly picked secret key K for PRF in verification key. More specifically, the reduction selects low-norm matrices $\mathbf{R}_{\mathbf{A}_0}$, $\mathbf{R}_{\mathbf{A}_1}$, $\{\mathbf{R}_{\mathbf{B}_i}\}_{i\in[k]}$, $\mathbf{R}_{\mathbf{C}_0}$, $\mathbf{R}_{\mathbf{C}_1} \xleftarrow{\$} \{1,-1\}^{m\times m}$, a PRF secret key $K = s_1 s_2 \dots s_k \xleftarrow{\$} \{0,1\}^k$ and sets $\mathbf{A}_0 = \mathbf{A}\mathbf{R}_{\mathbf{A}_0}$, $\mathbf{A}_1 = \mathbf{A}\mathbf{R}_{\mathbf{A}_1} + \mathbf{G}$, $\{\mathbf{B}_i = \mathbf{A}\mathbf{R}_{\mathbf{B}_i} + s_i\mathbf{G}\}_{i\in[k]}$, $\mathbf{C}_0 = \mathbf{A}\mathbf{R}_{\mathbf{C}_0}$ and $\mathbf{C}_1 = \mathbf{A}\mathbf{R}_{\mathbf{C}_1} + \mathbf{G}$. Here, K is completely hidden from adversary's view. For answering a signing query on message M, the reduction computes $\mathbf{A}_{\mathsf{PRF},\mathsf{M}} = \mathbf{A}\mathbf{R} + \mathsf{PRF}(K,\mathsf{M})\mathbf{G}$ for some known low-norm $m \times m$ matrix $\mathbf{R}$ that depends on $\mathbf{R}_{\mathbf{A}_0}, \mathbf{R}_{\mathbf{A}_1}, \{\mathbf{R}_{\mathbf{B}_i}\}_{i\in[k]}, \mathbf{R}_{\mathbf{C}_0}, \mathbf{R}_{\mathbf{C}_1}$, K and M. Let $\mathsf{PRF}(K,\mathsf{M}) = b$, the reduction sets $\mathbf{F}_{\mathsf{M},1-b} = [\mathbf{A} \mid \mathbf{A}_{1-b} - \mathbf{A}_{\mathsf{PRF},\mathsf{M}}] = [\mathbf{A} \mid \mathbf{A}\mathbf{R} + (1-2b)\mathbf{G}]$ and uses the trapdoor from $\mathbf{G}$ to compute the decryption key. Note, we use PRF to select the matrix $\mathbf{A}_b$ which is the same as the real scheme. For a valid forgery $(\mathsf{M}^*, \mathbf{d}_{\mathsf{M}^*})$, since $b = \mathsf{PRF}(K,\mathsf{M}^*)$ is unpredictable to the adversary, $\mathbf{F}_{\mathsf{M}^*,b} \cdot \mathbf{d}_{\mathsf{M}^*} = \mathbf{0} \pmod q$ happens with essentially probability $1/2$ leading to a valid SIS solution.

The security reduction for our IBE scheme is similar to the reduction of the signature scheme. Basically, the reduction answers key generation queries in the same way as answering signing queries in the signature scheme reduction. To construct the challenge ciphertext for a challenge identity id^*, the LWE challenge is embedded in the function matrix $\mathbf{F}_{\mathsf{id}^*,b} = [\mathbf{A} \mid \mathbf{A}\mathbf{R}]$ for which the simulator cannot produce private key. Another ciphertext based on $\mathbf{F}_{\mathsf{id}^*,1-b} = [\mathbf{A} \mid \mathbf{A}\mathbf{R} + (1-2b)\mathbf{G}]$ is generated as in the real scheme. With essentially half probability, the adversary will choose the ciphertext under $\mathbf{F}_{\mathsf{id}^*,b}$ to attack giving out useful information for solving the LWE challenge. We refer to the full details in the rest of the paper.

Related Works. In the related and concurrent work by Brakerski and Vaikuntanathan [25], a similar idea of embedding PRFs into encryption schemes has been used to construct the first semi-adaptively secure attribute-based encryption scheme from lattices supporting an a priori unbounded number of attributes. The recent work by Bai et al. [7] addresses the problem of improving efficiency of lattice-based cryptographic schemes via a different but novel way. Their proposal is about using Rényi divergence instead of statistical distance in the context of lattice-based cryptography which leads to (sometimes simpler) security proofs for more efficient lattice-based schemes.

2 Preliminaries

Notation. 'PPT' abbreviates "probabilistic polynomial-time". If S is a set, we denote by $a \xleftarrow{\$} S$ the uniform sampling of a random element of S. For a positive integer n, we denote by $[n]$ the set of positive integers no greater than n. We use bold lowercase letters (e.g. $\mathbf{a}$) to denote vectors and bold capital letters (e.g. $\mathbf{A}$) to denote matrices. For a positive integer $q \geq 2$, let $\mathbb{Z}_q$ be the ring of integers modulo q. We denote the group of $n \times m$ matrices in $\mathbb{Z}_q$ by $\mathbb{Z}_q^{n\times m}$. Vectors are treated as column vectors. The transpose of a vector $\mathbf{a}$ (resp. a matrix $\mathbf{A}$) is denoted by $\mathbf{a}^\top$ (resp. $\mathbf{A}^\top$). For $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and $\mathbf{B} \in \mathbb{Z}_q^{n\times m'}$, let $[\mathbf{A}|\mathbf{B}] \in \mathbb{Z}_q^{n\times(m+m')}$ be the concatenation of $\mathbf{A}$ and $\mathbf{B}$. We denote the Gram-Schmidt ordered orthogonalization of a matrix $\mathbf{A} \in \mathbb{Z}^{m\times m}$ by $\tilde{\mathbf{A}}$. The inner product of two vectors $\mathbf{x}$ and $\mathbf{y}$ is written $\langle \mathbf{x}, \mathbf{y} \rangle$. For a security parameter λ, a function $\mathsf{negl}(\lambda)$ is negligible in λ if it is smaller than all polynomial fractions for a sufficiently large λ.

We recall the following generalisation of the left-over hash lemma.

Lemma 2.1 ([2], Lemma 4)**.** *Suppose that $m > (n+1)\log q + \omega(\log n)$ and that $q > 2$ is prime. Let $\mathbf{R}$ be an $m \times k$ matrix chosen uniformly in $\{1,-1\}^{m\times k} \mod q$ where $k = k(n)$ is polynomial in n. Let $\mathbf{A}$ and $\mathbf{B}$ be matrices chosen uniformly in $\mathbb{Z}_q^{n\times m}$ and $\mathbb{Z}_q^{n\times k}$ respectively. Then, for all vectors $\mathbf{w} \in \mathbb{Z}_q^m$, the distribution $(\mathbf{A}, \mathbf{A}\mathbf{R}, \mathbf{R}^\top\mathbf{w})$ is statistically close to the distribution $(\mathbf{A}, \mathbf{B}, \mathbf{R}^\top\mathbf{w})$.*

For a vector $\mathbf{u}$, we let $\|\mathbf{u}\|$ and $\|\mathbf{u}\|_\infty$ denote its ℓ_2 norm and ℓ_∞ norm, respectively. For a matrix $\mathbf{R} \in \mathbb{Z}^{k\times m}$, we define two matrix norms:

– $\|\mathbf{R}\|$ denotes the ℓ_2 length of the longest column of $\mathbf{R}$.

– $\|\mathbf{R}\|_2$ is the operator norm of $\mathbf{R}$ defined as $\|\mathbf{R}\|_2 = \sup_{\mathbf{x}\in\mathbb{R}^{m+1}} \|\mathbf{R}\cdot\mathbf{x}\|$.

Lemma 2.2 ([2], Lemma 5)**.** *Let $\mathbf{R}$ be a random chosen matrix from $\{1,-1\}^{m\times m}$, then $\Pr[\|\mathbf{R}\|_2 > 12\sqrt{2m}] < e^{-m}$.*

2.1 Lattice Background

2.1.1 Lattice Definitions

Definition 2.1. Let a basis $\mathbf{B} = [\mathbf{b}_1 \mid \ldots \mid \mathbf{b}_m] \in (\mathbb{R}^m)^m$ of linearly independent vectors. The lattice generated by $\mathbf{B}$ is defined as $\Lambda = \{\mathbf{y} \in \mathbb{R}^m \ : \exists s_i \in \mathbb{Z},\ \mathbf{y} = \sum_{i=1}^m s_i\mathbf{b}_i\}$. The dual lattice Λ^* of Λ is defined as $\Lambda^* = \{\mathbf{z} \in \mathbb{R}^m \ : \forall \mathbf{y} \in \Lambda,\ \langle \mathbf{z}, \mathbf{y}\rangle \in \mathbb{Z}\}$.

Definition 2.2. For q prime, $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and $\mathbf{u} \in \mathbb{Z}_q^n$, we define the m-dimensional (full-rank) random integer lattice $\Lambda_q^\perp(\mathbf{A}) = \{\mathbf{e} \in \mathbb{Z}^m \ : \mathbf{Ae} = \mathbf{0} \pmod q\}$, and the "shifted lattice" as the coset $\Lambda_q^{\mathbf{u}}(\mathbf{A}) = \{\mathbf{e} \in \mathbb{Z}^m \ : \mathbf{Ae} = \mathbf{u} \pmod q\}$.

2.1.2 Trapdoors of Lattices and Discrete Gaussians

It is shown in [3, 51] how to sample a "nearly" uniform random matrix $\mathbf{A} \in \mathbb{Z}^{n\times m}$ along with a trapdoor matrix $\mathbf{T_A} \in \mathbb{Z}^{m\times m}$ which is a short or low-norm basis of the induced lattice $\Lambda_q^\perp(\mathbf{A})$. We refer to this procedure as $\mathsf{TrapGen}$.

Lemma 2.3. *There is a PPT algorithm $\mathsf{TrapGen}$ that takes as input integers $n \geq 1$, $q \geq 2$ and a sufficiently large $m = O(n\log q)$, outputs a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and a trapdoor matrix $\mathbf{T_A} \in \mathbb{Z}^{m\times m}$, such that $\mathbf{A}\cdot\mathbf{T_A} = 0$, the distribution of $\mathbf{A}$ is statistically close to the uniform distribution over $\mathbb{Z}_q^{n\times m}$ and $\|\tilde{\mathbf{T}}_\mathbf{A}\| = O(\sqrt{n\log q})$.*

Discrete Gaussians. Let $m \in \mathbb{Z}_{>0}$ be a positive integer and $\Lambda \subset \mathbb{Z}^m$. For any real vector $\mathbf{c} \in \mathbb{R}^m$ and positive parameter $\sigma \in \mathbb{R}_{>0}$, let the Gaussian function $\rho_{\sigma,\mathbf{c}}(\mathbf{x}) = \exp\left(-\pi\|\mathbf{x}-\mathbf{c}\|^2/\sigma^2\right)$ on $\mathbb{R}^m$ with center $\mathbf{c}$ and parameter σ. Define the discrete Gaussian distribution over Λ with center $\mathbf{c}$ and parameter σ as $D_{\Lambda,\sigma} = \rho_{\sigma,\mathbf{c}}(\mathbf{y})/\rho_\sigma(\Lambda)$ for $\forall \mathbf{y} \in \Lambda$, where $\rho_\sigma(\Lambda) = \sum_{\mathbf{x}\in\Lambda}\rho_{\sigma,\mathbf{c}}(\mathbf{x})$. For notational convenience, $\rho_{\sigma,\mathbf{0}}$ and $D_{\Lambda,\sigma,\mathbf{0}}$ are abbreviated as ρ_σ and $D_{\Lambda,\sigma}$.

The following lemma bounds the length of a discrete Gaussian vector with sufficiently large Gaussian parameter.

Lemma 2.4 ([52])**.** *For any lattice Λ of integer dimension m with basis $\mathbf{T}$, $\mathbf{c} \in \mathbb{R}^m$ and Gaussian parameter $\sigma \geq \|\tilde{\mathbf{T}}\|\cdot\omega(\sqrt{\log m})$, we have $\Pr[\|\mathbf{x}-\mathbf{c}\| > \sigma\sqrt{m} : \mathbf{x} \leftarrow D_{\Lambda,\sigma,\mathbf{c}}] \leq \mathsf{negl}(n)$.*

Smoothing Parameter. We recall the very important notion of smoothing parameter of a lattice Λ. It is the smallest value of s such that the discrete Gaussian $D_{\Lambda,s}$ "behaves" like a continuous Gaussian.

Definition 2.3 ([52])**.** For any lattice Λ and positive real tolerance $\epsilon > 0$, the smoothing parameter $\eta_\epsilon(\Lambda)$ is the smallest real $s > 0$ such that $\rho_{1/s}(\Lambda^* \setminus \{\mathbf{0}\}) < \epsilon$.

We will make use of the following lemma, which is a special case of Corollary 3.10 from [55].

Lemma 2.5 (special case of Corollary 3.10 of [55])**.** *Let $\mathbf{r} \in \mathbb{Z}^m$ be a vector and $r, \alpha > 0$ be reals. Assume that $1/\sqrt{1/r^2 + (\|\mathbf{r}\|/\alpha)^2} \geq \eta_\epsilon(\mathbb{Z}^m)$ for some $\epsilon < 1/2$. Let $\mathbf{y}$ be a vector with distribution $D_{\mathbb{Z}^m,r}$ and e be a scalar with distribution $D_{\mathbb{Z},\alpha}$. The distribution of $\langle \mathbf{r}, \mathbf{y}\rangle + e$ is statistically close to $D_{\mathbb{Z},\sqrt{(r\|\mathbf{r}\|)^2+\alpha^2}}$.*

2.1.3 Lattice Sampling Algorithms

Our constructions make use of the "two-sided trapdoor" framework from [2, 21] which consists of two sampling algorithms SampleLeft and SampleRight.

$$\textit{Algorithm } \mathsf{SampleLeft}(\mathbf{A}, \mathbf{B}, \mathbf{T_A}, \mathbf{u}, s) \tag{1}$$

Inputs: a full-rank matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and a short basis $\mathbf{T_A}$ of $\Lambda_q^{\perp}(\mathbf{A})$, a matrix $\mathbf{B} \in \mathbb{Z}_q^{n \times m_1}$, a vector $\mathbf{u} \in \mathbb{Z}_q^n$, and a Gaussian parameter s.

Output: Let $\mathbf{F} = \big[\mathbf{A} \mid \mathbf{B}\big]$. The algorithm outputs a vector $\mathbf{d} \in \mathbb{Z}^{m+m_1}$ in the set $\Lambda_q^{\mathbf{u}}(\mathbf{F})$.

Theorem 2.6 ([2, 28])**.** *Let $q > 2$, $m > n$ and $s > \|\tilde{\mathbf{T}}_{\mathbf{A}}\| \cdot \omega(\sqrt{\log(m + m_1)})$. Then the algorithm $\mathsf{SampleLeft}(\mathbf{A}, \mathbf{B}, \mathbf{T_A}, \mathbf{u}, s)$ taking inputs as in (1), outputs a vector $\mathbf{d} \in \mathbb{Z}^{m+m_1}$ distributed statistically close to $D_{\Lambda_q^{\mathbf{u}}(\mathbf{F}),s}$.*

$$\textit{Algorithm } \mathsf{SampleRight}(\mathbf{A}, \mathbf{B}, \mathbf{R}, \mathbf{T_B}, \mathbf{u}, s) \tag{2}$$

Inputs: matrices $\mathbf{A} \in \mathbb{Z}_q^{n \times k}$ and $\mathbf{R} \in \mathbb{Z}^{k \times m}$, a full-rank matrix $\mathbf{B} \in \mathbb{Z}_q^{n \times m}$, a short basis $\mathbf{T_B}$ of $\Lambda_q^{\perp}(\mathbf{B})$, a vector $\mathbf{u} \in \mathbb{Z}_q^n$, and a Gaussian parameter s.

Output: Let $\mathbf{F} = \big[\mathbf{A} \mid \mathbf{AR} + \mathbf{B}\big]$; the algorithm outputs a vector $\mathbf{d} \in \mathbb{Z}^{m+m_1}$ in the set $\Lambda_q^{\mathbf{u}}(\mathbf{F})$

Theorem 2.7 ([2], Theorem 19)**.** *Let $q > 2$, $m > n$. Let $s > \|\tilde{\mathbf{T}}_{\mathbf{B}}\| \cdot \|\mathbf{R}\|_2 \cdot \omega(\sqrt{\log m})$. Then $\mathsf{SampleRight}(\mathbf{A}, \mathbf{B}, \mathbf{R}, \mathbf{T_B}, \mathbf{u}, s)$ taking inputs as in (2), outputs a vector $\mathbf{d} \in \mathbb{Z}^{m+k}$ distributed statistically close to $D_{\Lambda_q^{\mathbf{u}}(\mathbf{F}),s}$.*

2.1.4 Gadget Matrix

The "gadget matrix" $\mathbf{G}$ defined in [51]. We recall the following two facts.

Lemma 2.8 ([51], Theorem 1)**.** *Let q be a prime, and n, m be integers with $m = n \log q$. There is a fixed full-rank matrix $\mathbf{G} \in \mathbb{Z}_q^{n \times m}$ such that the lattice $\Lambda_q^{\perp}(\mathbf{G})$ has a publicly known trapdoor matrix $\mathbf{T_G} \in \mathbb{Z}^{n \times m}$ with $\|\tilde{\mathbf{T}}_{\mathbf{G}}\| \leq \sqrt{5}$.*

Lemma 2.9 ([19], Lemma 2.1)**.** *There is a deterministic algorithm, denoted $\mathbf{G}^{-1}(\cdot) : \mathbb{Z}_q^{n \times m} \to \mathbb{Z}^{m \times m}$, that takes any matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ as input, and outputs the preimage $\mathbf{G}^{-1}(\mathbf{A})$ of $\mathbf{A}$ such that $\mathbf{G} \cdot \mathbf{G^{-1}}(\mathbf{A}) = \mathbf{A} \pmod q$ and $\|\mathbf{G}^{-1}(\mathbf{A})\| \leq m$.*

2.1.5 Computational Assumptions

We recall the two most mainstream and conservative average-case computational assumptions for lattice problems.

The learning with errors problem was first proposed by Regev [55]. For a vector $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^n$ and a noise distribution χ over $\mathbb{Z}_q$, let $A_{\mathbf{s},\chi}$ be the distribution over $\mathbb{Z}_q^n \times \mathbb{Z}_q$ by taking $\mathbf{a} \xleftarrow{\$} \mathbb{Z}_q^n$ and $x \leftarrow \chi$, and outputting $(\mathbf{a}, \mathbf{s}^{\top}\mathbf{a} + x) \pmod q$. Usually, χ is a discrete Gaussian $D_{\mathbb{Z},\alpha q}$ for some $\alpha < 1$, reduced modulo q. We refer to [55] for further details.

Definition 2.4. For a security parameter Λ, let a positive integer $n = n(\lambda)$, a prime $q = q(\lambda)$, and a distribution χ over $\mathbb{Z}_q$. The learning with errors problem $\mathrm{LWE}_{n,q,\chi}$ is to distinguish the oracle $\mathcal{O}_{\mathbf{s}}$, which outputs samples from the distribution $A_{\mathbf{s},\chi}$, from the oracle $\mathcal{O}_{\$}$, which outputs samples from the uniform distribution over $\mathbb{Z}_q^n \times \mathbb{Z}_q$, for an unspecified polynomial number of queries. We define the advantage (in the security parameter λ) of an algorithm $\mathcal{A}$ in solving the $\mathrm{LWE}_{n,q,\chi}$ problem as

$$\mathsf{Adv}_{\mathcal{A}}^{\mathrm{LWE}_{n,q,\chi}}(\lambda) = \Big|\Pr[\mathcal{A}^{\mathcal{O}_{\mathbf{s}}}(1^{\lambda}) = 1] - \Pr[\mathcal{A}^{\mathcal{O}_{\$}}(1^{\lambda}) = 1]\Big|$$

We say that the $(t, \epsilon_{\mathsf{LWE}})$-$\mathsf{LWE}_{n,q,\chi}$ assumption holds if no t-time algorithm $\mathcal{A}$ that has advantage at least ϵ_{LWE} in solving the $\mathsf{LWE}_{n,q,\chi}$ problem.

For polynomial size q in λ, there are known quantum [55] and classical [22] reductions from the average-case $\mathrm{LWE}_{n,q,\chi}$ assumption to many standard worst-case lattice problems (e.g., GapSVP). [3] Peikert [54] also gave a classic reduction that applies (only) for exponential moduli q in λ. These reductions further strengthen the appeal of the LWE assumption.

The security of our adaptively secure signature scheme is based on the SIS problem, which can be seen as an average-case approximate shortest vector problem on random integer lattices. In a sense, SIS is the computational counterpart to the decisional LWE.

Definition 2.5. For a security parameter λ, let $n = n(\lambda)$, $m = m(\lambda)$, and $\beta = \beta(\lambda)$. Let q be a prime integer. The short integer solution problem $\mathsf{SIS}_{n,q,\beta,m}$ is as follows. Given a uniform random matrix $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n\times m}$, find a non-zero vector $\mathbf{e} \in \mathbb{Z}^m$ such that $\mathbf{Ae} = \mathbf{0} \pmod q$ and $\|\mathbf{e}\| \le \beta$. We define the advantage (function of the security parameter λ) of an algorithm $\mathcal{A}$ in solving the $\mathsf{SIS}_{n,q,\beta,m}$ problem as

$$\mathsf{Adv}^{\mathsf{SIS}_{n,q,\beta,m}}_{\mathcal{A}}(\lambda) = \left[\begin{array}{c|c} \mathbf{Ae} = \mathbf{0} \pmod q \\ \text{and } \|\mathbf{e}\| \le \beta, \\ \text{and } \mathbf{e} \neq \mathbf{0}. \end{array} : \begin{array}{c} \mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n\times m} \\ \mathbf{e} \leftarrow \mathcal{A}(1^\lambda, \mathbf{A}) \end{array}\right]$$

We say the $(t, \epsilon_{\mathsf{SIS}})$-$\mathsf{SIS}_{n,q,\beta,m}$ assumption holds if no t-time algorithm $\mathcal{A}$ that has advantage at least ϵ_{SIS} in solving the $\mathsf{SIS}_{n,q,\beta,m}$ problem.

It has been shown in [52] that solving the average-case instances of the $\mathsf{SIS}_{n,q,\beta,m}$ problem for certain parameters is as hard as solving worst-case instances of the approximate Shortest Independent Vector Problem (SIVP).

2.2 Pseudorandom Functions

Definition 2.6 (Pseudorandom Functions)**.** Let $\lambda > 0$ be the security parameter, and let $k = k(\lambda)$, $t = t(\lambda)$ and $l = l(\lambda)$. A pseudorandom function $\mathsf{PRF} : \{0,1\}^k \times \{0,1\}^t \to \{0,1\}^l$ is an efficiently computable, deterministic two-input function where the first input, denoted by K, is the key. Let Ω be the set of all functions that map t bits strings to l bits strings. We define the advantage (in the security parameter λ) of an adversary $\mathcal{A}$ in attacking the PRF as

$$\mathsf{Adv}_{\mathsf{PRF},\mathcal{A}}(\lambda) = \left|\Pr[\mathcal{A}^{\mathsf{PRF}(K,\cdot)}(1^\lambda) = 1] - \Pr[\mathcal{A}^{F(\cdot)}(1^\lambda) = 1]\right|$$

where the probability is taken over a uniform choice of key $K \xleftarrow{\$} \{0,1\}^k$ and $F \xleftarrow{\$} \Omega$, and the randomness of $\mathcal{A}$. We say that PRF is $(t_{\mathsf{PRF}}, \epsilon_{\mathsf{PRF}})$-secure if for all t_{PRF}-time adversaries $\mathcal{A}$, $\mathsf{Adv}_{\mathsf{PRF},\mathcal{A}}(\lambda) \le \epsilon_{\mathsf{PRF}}$.

2.3 Key-Homomorphic Evaluation Algorithm

Recall the matrix key-homomorphic evaluation algorithm, which is developed by Gentry et al. [37], Boneh et al. [19] and Brakerski and Vaikuntanathan [24] in the context of fully homomorphic encryption and attribute-based encryption, works generally in the following. Given a fan-in-2 Boolean NAND circuits $C : \{0,1\}^\ell \to \{0,1\}$, ℓ different matrices $\{\mathbf{A}_i = \mathbf{AR}_i + x_i\mathbf{G} \in \mathbb{Z}_q^{n\times m}\}_{i\in[\ell]}$ which correspond to each input wire of C where $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n\times m}$, $\mathbf{R}_i \xleftarrow{\$} \{1,-1\}^{m\times m}$, $x_i \in \{0,1\}$ and $\mathbf{G} \in \mathbb{Z}_q^{n\times m}$ is the gadget matrix, the key-homomorphic evaluation algorithm

[3] Equivalently, this is to say that many classic worst-case lattice *problems* reduce *to* the average-case LWE *problem*, for suitable parameters.

deterministically computes $\mathbf{A}_C = \mathbf{A}\mathbf{R}_C + C(x_1, \ldots, x_\ell)\mathbf{G} \in \mathbb{Z}_q^{n\times m}$ where $\mathbf{R}_C \in \mathbb{Z}^{m\times m}$ has low norm and $C(x_1, \ldots, x_\ell) \in \{0, 1\}$ is the output bit of C on the arguments $x_1, \ldots, x_\ell$. This is done, in general, by inductively evaluating each NAND gate. For a NAND gate $g(u, v; w)$ with input wires u, v and output wire w, matrices $\mathbf{A}_u = \mathbf{A}\mathbf{R}_u + x_u\mathbf{G}$ and $\mathbf{A}_v = \mathbf{A}\mathbf{R}_v + x_v\mathbf{G}$ where x_u and x_v are input bits of u and v respectively, the evaluation algorithm computes

$$\begin{aligned}\mathbf{A}_w &= \mathbf{G} - \mathbf{A}_u \cdot \mathbf{G}^{-1}(\mathbf{A}_v) \\ &= \mathbf{G} - (\mathbf{A}\mathbf{R}_u + x_u\mathbf{G}) \cdot \mathbf{G}^{-1}(\mathbf{A}\mathbf{R}_v + x_v\mathbf{G}) \\ &= \mathbf{A}\mathbf{R}_g + (1 - x_u x_v)\mathbf{G}\end{aligned}$$

where $1 - x_u x_v \stackrel{\mathsf{def}}{=} \mathsf{NAND}(x_u, x_v)$, and $\mathbf{R}_g = -\mathbf{R}_u \cdot \mathbf{G}^{-1}(\mathbf{A}_v) - x_u\mathbf{R}_v$ has low-norm if $\mathbf{R}_u, \mathbf{R}_v$ have low-norm.

In this paper, we consider evaluating circuits of PRFs. Most of the well-known PRFs from number-theoretic assumptions (e.g. [53, 47]) and lattice assumptions (e.g. [9, 8]) can be computed by circuits in class NC^1 (i.e. with polynomial size, logarithmic depth $O(\log \ell)$ in input length ℓ and fan-in 2). For circuits in NC^1, by applying above procedure in a general tree-fashion, the norm of $\mathbf{R}_C$ in the matrix $\mathbf{A}_C$ is roughly bounded by $m^{O(\log \ell)}$, which in turn usually results in superpolynomial or sub-exponential LWE/SIS modulus q (in the security parameter) in certain applications.

In [24], Brakerski and Vaikuntanathan observed that the norm of $\mathbf{R}_C$ matrix in above homomorphic evaluation is accumulated in an asymmetric way. They exploited this feature to design a special evaluation algorithm that evaluates NC^1 circuits with moderately increasing the norm of $\mathbf{R}_C$. Specifically, the observation is that any circuit with depth d can be simulated by a length-4^d and width-5 branching program, through the Barrington's theorem. Such a branching program can be computed by multiplying 4^d 5-by-5 permutation matrices. It is showed in [24] that homomorphically evaluating the multiplication of permutation matrices using above homomorphic evaluation procedure and the asymmetrical noise-growth feature only increases the noise by a polynomial factor and, therefore, allows us to use polynomial size LWE/SIS modulus q in the security parameter. Such result has been used to construct efficient ABE scheme for branching programs (with bounded length) from LWE with polynomial modulus [42]. In our constructions, we particularly use the Brakerski and Vaikuntanathan's evaluation algorithm [24] and denote it by $\mathsf{Eval}_{\mathsf{BV}}$.

We recall the Barrington's Theorem.

Theorem 2.10 (Barrington's Theorem)**.** *Every Boolean NAND circuit C that acts on ℓ inputs and has depth d can be computed by a width-5 permutation branching program Π of length 4^d. Given the description of the circuit Ψ, the description of the branching program C can be computed in poly$(\ell, 4^d)$ time.*

The following theorem follows from the Claim 3.4.2 and Lemma 3.6 of [24] and the Barrington's Theorem.

Lemma 2.11. *Let $C : \{0, 1\}^\ell \to \{0, 1\}$ be a NAND Boolean circuit. Let $\{\mathbf{A}_i = \mathbf{A}\mathbf{R}_i + x_i\mathbf{G} \in \mathbb{Z}_q^{n\times m}\}_{i\in[\ell]}$ be ℓ different matrices correspond to each input wire of C where $\mathbf{A} \stackrel{\$}{\leftarrow} \mathbb{Z}_q^{n\times m}$, $\mathbf{R}_i \stackrel{\$}{\leftarrow} \{1, -1\}^{m\times m}$, $x_i \in \{0, 1\}$ and $\mathbf{G} \in \mathbb{Z}_q^{n\times m}$ is the gadget matrix. There is an efficient deterministic algorithm $\mathsf{Eval}_{\mathsf{BV}}$ that takes as input C and $\{\mathbf{A}_i\}_{i\in[\ell]}$ and outputs a matrix $\mathbf{A}_C = \mathbf{A}\mathbf{R}_C + C(x_1, \ldots, x_\ell)\mathbf{G} = \mathsf{Eval}_{\mathsf{BV}}(C, \mathbf{A}_1, \ldots, \mathbf{A}_\ell)$ where $\mathbf{R}_C \in \mathbb{Z}^{m\times m}$ and $C(x_1, \ldots, x_\ell)$ is the output of C on the arguments $x_1, \ldots, x_\ell$. $\mathsf{Eval}_{\mathsf{BV}}$ runs in time poly$(4^d, \ell, n, \log q)$.*

Let $\|\mathbf{R}_{max}\|_2 = max\{\|\mathbf{R}_i\|_2\}_{i\in[\ell]}$, the norm of $\mathbf{R}_C$ in $\mathbf{A}_C$ output by $\mathsf{Eval}_{\mathsf{BV}}$ can be bounded,with

overwhelming probability, by

$$\begin{aligned}\|\mathbf{R}_C\|_2 &\leq O(L \cdot \|\mathbf{R}_{max}\|_2 \cdot m) \\ &\leq O(L \cdot 12\sqrt{2} \cdot \sqrt{m} \cdot m) \\ &\leq O(4^d \cdot m^{3/2})\end{aligned}$$

where L is the length of the width-5 branching program which simulates C and $\|\mathbf{R}_i\|_2 \leq 12\sqrt{2m}$ for $i \in [\ell]$ with overwhelming probability, by Lemma 2.2.

Particularly, if C has depth $d = c \log \ell$ for some constant c, i.e. C is in NC^1, we have $L = 4^d = \ell^{2c}$ and $\|\mathbf{R}_C\|_2 \leq O(\ell^{2c} \cdot m^{3/2})$.

Remark. In our constructions, the circuit of an instantiated PRF serves as a part of verification key (in the signature case) or public parameters (in the IBE case). This is in contrast to the FHE and ABE cases addressed by [37, 19, 24] in which circuits can be dynamically chosen by participants of protocols. Therefore further optimization on such a specific PRF circuit (e.g. depth, number of gates) could be possible. Here we consider circuit class NC^1 as a more general case to include almost all efficient and provably secure PRF candidates.

2.4 Digital Signatures

A digital signature scheme consists of three PPT algorithms: KeyGen, Sign, and Ver. The algorithm KeyGen takes as input a security parameter and generates a public verification key Vk and a private signing key Sk. The signing algorithm Sign takes as input the signing key Sk and a massage M, and outputs the signature Sig of M. The verification algorithm Ver takes as input a signature-message pair $(\mathsf{Sig}, \mathsf{M})$ as well as the verification key Vk. It outputs 1 if Sig is valid, or 0 if Sig is invalid.

We review the standard security notion of digital signature schemes. The existential unforgeability under chosen-message attack (EUF-CMA) of a digital signature scheme Π is defined through the following security game between an adversary $\mathcal{A}$ and a challenger $\mathcal{B}$.

Setup. $\mathcal{B}$ runs $\mathsf{Setup}(1^\lambda) \to (\mathsf{Sk}, \mathsf{Vk})$, and passes Vk to $\mathcal{A}$.

Query. $\mathcal{A}$ adaptively selects messages $\mathsf{M}_1, \ldots, \mathsf{M}_{q_s}$ to ask for the corresponding signatures under Vk from $\mathcal{B}$. For the query M_i, $\mathcal{B}$ responds with a signature $\mathsf{Sig}_i \leftarrow \mathsf{Sign}(\mathsf{Sk}, \mathsf{M}_i)$.

Forge. $\mathcal{A}$ outputs a pair $(\mathsf{Sig}^*, \mathsf{M}^*)$ and wins if

1. $\mathsf{M}^* \notin \{\mathsf{M}_1, \ldots, \mathsf{M}_{q_s}\}$, and
2. $\mathsf{Ver}(\mathsf{Vk}, \mathsf{Sig}^*, \mathsf{M}^*) \to 1$.

We refer to such an adversary $\mathcal{A}$ as EUF-CMA adversary. We define the advantage (in the security parameter λ) $\mathsf{Adv}_{\Pi,\mathcal{A}}(\lambda)$ of $\mathcal{A}$ in attacking a digital signature scheme Π to be the probability that $\mathcal{A}$ wins above game.

Definition 2.7. For a security parameter λ, let $t = t(\lambda)$, $q_s = q_s(\lambda)$ and $\epsilon = \epsilon(\lambda)$. We say that a digital signature scheme Π is (t, q_s, ϵ)-EUF-CMA secure if for any t time EUF-CMA adversary $\mathcal{A}$ that makes at most q_s signing queries and has $\mathsf{Adv}_{\Pi,\mathcal{A}}(\lambda) \leq \epsilon$.

2.5 Identity-Based Encryption

An Identity-Based Encryption system (IBE) consists of four PPT algorithms: Setup, KeyGen, Encrypt, and Decrypt. The algorithm Setup takes as input a security parameter and generates public parameters Pub and a master secret key Msk. The algorithm KeyGen uses the master

secret key Msk to produce an identity private key $\mathsf{Sk}_{\mathsf{id}}$ corresponding to an identity id. The algorithm $\mathsf{Encrypt}$ takes the public parameters Pub to encrypt messages for any given identity id. The algorithm $\mathsf{Decrypt}$ decrypts ciphertexts using the identity private key if the identity of the ciphertext matches the identity of the private key.

We review the security model of IBE proposed in [18]. It defines the indistinguishability of ciphertexts under an adaptive chosen-ciphertext and adaptive chosen-identity attack ($\mathsf{IND\text{-}ID\text{-}CCA2}$). The $\mathsf{IND\text{-}ID\text{-}CCA2}$ security of IBE is defined through the following game between an adversary $\mathcal{A}$ and a challenger $\mathcal{B}$. For a security parameter λ, let $\mathcal{M}_\lambda$ be the message space and $\mathcal{C}_\lambda$ be the ciphertext space.

Setup. $\mathcal{B}$ runs $\mathsf{Setup}(1^\lambda) \to (\mathsf{Pub}, \mathsf{Msk})$, passes the public parameters Pub to $\mathcal{A}$, and keeps the master secret Msk.

Phase 1. $\mathcal{A}$ adaptively issues queries $q_1, \ldots, q_m$ where each query q_i is one of:

- Private key query for identity id_i. $\mathcal{B}$ runs KeyGen to generate $\mathsf{Sk}_{\mathsf{id}_i}$ and sends it to $\mathcal{A}$.
- Decryption query for a ciphertext $\mathsf{Ctx}_{\mathsf{id}_i}$ under identity id_i. $\mathcal{B}$ runs KeyGen to generate $\mathsf{Sk}_{\mathsf{id}_i}$. Then, $\mathcal{B}$ runs the decryption algorithm to decrypt $\mathsf{Ctx}_{\mathsf{id}_i}$ and returns the message to $\mathcal{A}$.

Challenge. When $\mathcal{A}$ decides the Phase 1 is over, it outputs a challenge identity id^*, which is not been queried during Phase 1, and two equal length messages $\mathsf{Msg}_0, \mathsf{Msg}_1 \in \mathcal{M}_\lambda$. $\mathcal{B}$ flips a fair coin $\gamma \xleftarrow{\$} \{0,1\}$ and sets $\mathsf{Ctx}_{\mathsf{id}^*} \leftarrow \mathsf{Encrypt}(\mathsf{Pub}, \mathsf{Msg}_\gamma, \mathsf{id}^*)$. Finally $\mathcal{A}$ passes $\mathsf{Ctx}_{\mathsf{id}^*}$ to $\mathcal{A}$.

Phase 2. $\mathcal{A}$ adaptively issues more queries $q_{m+1}, \ldots, q_n$ where q_i is one of

- Private key query for identity $\mathsf{id}_i \neq \mathsf{id}^*$.
- Decryption query for a ciphertext $\mathsf{Ctx}_{\mathsf{id}_i} \neq \mathsf{Ctx}_{\mathsf{id}^*}$.

In both cases, $\mathcal{B}$ responds as in Phase 1.

Guess. $\mathcal{A}$ outputs $\gamma' \in \{0,1\}$ and it wins if $\gamma' = \gamma$.

We refer to such an adversary $\mathcal{A}$ as an $\mathsf{IND\text{-}ID\text{-}CCA2}$ adversary. We define the advantage (in the security parameter λ) of $\mathcal{A}$ in attacking an IBE scheme $\mathcal{E}$ as $\mathsf{Adv}_{\mathcal{E},\mathcal{A}}(\lambda) = |\Pr[\gamma' = \gamma] - 1/2|$.

Definition 2.8. For a security parameter λ, let $t = t(\lambda)$, $q_{\mathsf{id}} = q_{\mathsf{id}}(\lambda)$, $q_{\mathsf{Ctx}} = q_{\mathsf{Ctx}}(\lambda)$, and $\epsilon = \epsilon(\lambda)$. We say that an IBE system $\mathcal{E}$ is $(t, q_{\mathsf{id}}, q_{\mathsf{Ctx}}, \epsilon)$-$\mathsf{IND\text{-}ID\text{-}CCA2}$ secure if for any t-time $\mathsf{IND\text{-}ID\text{-}CCA2}$ adversary $\mathcal{A}$ that makes at most q_{id} private key queries and at most q_{Ctx} decryption queries, we have $\mathsf{Adv}_{\mathcal{E},\mathcal{A}}(\lambda) \leq \epsilon$.

Chosen-Plaintext Security. We define the chosen-plaintext security ($\mathsf{IND\text{-}ID\text{-}CPA}$) for IBE systems as in above security game, except the adversary is not allowed to issue decryption queries. The adversary is still able to adaptively make private key queries.

Definition 2.9. We say that an IBE system $\mathcal{E}$ is $(t, q_{\mathsf{id}}, \epsilon)$-$\mathsf{IND\text{-}ID\text{-}CPA}$ secure if $\mathcal{E}$ is $(t, q_{\mathsf{id}}, 0, \epsilon)$-$\mathsf{IND\text{-}ID\text{-}CCA2}$ secure.

Selective Security. A weaker and less realistic security model of IBE system, introduced in [27], is the selective security model in which adversary is required to commit to the challenge identity even before seeing the public parameters. We note that under computational assumptions with sub-exponential hardness, a selectively secure IBE is also adaptively secure through a standard "complexity leveraging" argument from [14]; however, complexity leveraging incurs a rather severe loss of tightness in the security reduction, causing the resulting scheme to suffer from a possibly large loss of efficiency per a similar argument as discussed in the introduction.

3 Signature Scheme with Tight Security

3.1 Constructions

$\mathsf{KeyGen}(1^\lambda)$ The key generation algorithm does the following.

1. Sample a matrix $\mathbf{A}$ along with a trapdoor basis of lattice $\Lambda_q^\perp(\mathbf{A})$ by $\mathsf{TrapGen}$.
2. Select matrices $\mathbf{A}_0$, $\mathbf{A}_1$, "PRF key" matrices $\mathbf{B}_1, \ldots, \mathbf{B}_k$, and "PRF input" matrices $\mathbf{C}_0$, $\mathbf{C}_1$ from $\mathbb{Z}_q^{n\times m}$ uniformly at random.
3. Select a secure pseudorandom function $\mathsf{PRF} : \{0,1\}^k \times \{0,1\}^t \to \{0,1\}$, express it as a NAND Boolean circuit C_{PRF} with depth $d = d(\lambda)$, and select a PRF key $K = s_1 s_2 \ldots s_k \xleftarrow{\$} \{0,1\}^k$.
4. Select a Gaussian parameter $s > 0$.
5. Output the verification key and signing key as:

$$\mathsf{Vk} = \left(\mathbf{A}, \{\mathbf{A}_0, \mathbf{A}_1\}, \{\mathbf{B}_i\}_{i\in[k]}, \{\mathbf{C}_0, \mathbf{C}_1\}, s, \mathsf{PRF}, C_{\mathsf{PRF}}\right), \quad \mathsf{Sk} = (\mathbf{T}_{\mathbf{A}}, K)$$

$\mathsf{Sign}(\mathsf{Vk}, \mathsf{Sk}, \mathsf{M})$ The signing algorithm takes as input the public verification key Vk, the signing key Sk and a message $\mathsf{M} = m_1 m_2 \ldots m_t \in \{0,1\}^t$. It does:

1. Compute $\mathbf{A}_{C_{\mathsf{PRF}},\mathsf{M}} = \mathsf{Eval}_{\mathsf{BV}}(C_{\mathsf{PRF}}, \{\mathbf{B}_i\}_{i\in[k]}, \mathbf{C}_{m_1}, \mathbf{C}_{m_2}, \ldots, \mathbf{C}_{m_t}) \in \mathbb{Z}_q^{n\times m}$. [4]
2. Compute bit value $b = \mathsf{PRF}(K, \mathsf{M})$ and set $\mathbf{F}_{\mathsf{M},1-b} = \left[\mathbf{A} \mid \mathbf{A}_{1-b} - \mathbf{A}_{C_{\mathsf{PRF}},\mathsf{M}}\right]$.
3. Run $\mathsf{SampleLeft}$ to sample $\mathbf{d}_{\mathsf{M}} \in \mathbb{Z}^{2m}$ with distribution $D_{\Lambda_q^\perp(\mathbf{F}_{\mathsf{M},1-b}),s}$.
4. Output the signature $\mathsf{Sig} = \mathbf{d}_{\mathsf{M}}$.

$\mathsf{Ver}(\mathsf{Vk}, \mathsf{M}, \mathsf{Sig})$ The verification algorithm takes as input the verification key Vk, message M and the signature of M, verifies as follows:

1. Assume $\mathsf{Sig} = \mathbf{d}$. It checks if $\mathbf{d} \in \mathbb{Z}^{2m}$, $\mathbf{d} \neq \mathbf{0}$, and $\|\mathbf{d}\| \leq s\sqrt{2m}$.
2. Compute $\mathbf{A}_{C_{\mathsf{PRF}},\mathsf{M}} = \mathsf{Eval}_{\mathsf{BV}}(C_{\mathsf{PRF}}, \{\mathbf{B}_i\}_{i\in[k]}, \mathbf{C}_{m_1}, \mathbf{C}_{m_2}, \ldots, \mathbf{C}_{m_t}) \in \mathbb{Z}_q^{n\times m}$.
   Check if $\mathbf{F}_{\mathsf{M},b}\mathbf{d} = \left[\mathbf{A} \mid \mathbf{A}_b - \mathbf{A}_{C_{\mathsf{PRF}},\mathsf{M}}\right]\mathbf{d} = \mathbf{0} \pmod q$ for $b = 0$ or 1.
3. If all above verifications pass, accept the signature; otherwise, reject.

3.2 Parameters Selection and Discussion

Let λ be the security parameter, we set $n = n(\lambda)$, let the message length be $t = t(\lambda)$ and the secret key length of PRF be $k = k(\lambda)$. For the most general case, let the circuit depth of C_{PRF} be $d = d(\lambda)$. To ensure we can run $\mathsf{TrapGen}$ in the Lemma 2.3, we set $m = n^{1+\eta}$ for some η (we assume $n^\eta > O(\log q)$). To run $\mathsf{SampleLeft}$ and $\mathsf{SampleRight}$ in the real scheme and simulation per Theorem 2.7, we set s sufficiently large such that $s > \|\tilde{\mathbf{T}}_{\mathbf{G}}\| \cdot \|\mathbf{R}\|_2 \cdot \omega(\sqrt{\log m})$ for $\mathbf{R} = \mathbf{R}_{\mathbf{A}_b} - \mathbf{R}_{C_{\mathsf{PRF}},\mathsf{M}}$ (see the security proof below). By Lemma 2.11 we set $s = O(4^d \cdot m^{3/2}) \cdot \omega(\sqrt{\log m})$. For the SIS parameter β, we need $\beta \geq O(4^d \cdot m^{3/2} \cdot s\sqrt{2m})$. So we set $\beta = O(16^d \cdot m^{7/2}) \cdot \omega(\sqrt{\log m})$. To ensure the applicability of the average-case to worst-case reduction for SIS, we need $q \geq \beta \cdot \omega(\sqrt{n \log n})$. So we set $q = O(16^d \cdot m^4) \cdot (\omega(\sqrt{\log m}))^2$.

[4] It turns out that if PRF is secure, an efficient SIS algorithm can be tightly reduced to an efficient algorithm that finds $\mathsf{M} \neq \mathsf{M}'$ such that $\mathbf{A}_{C_{\mathsf{PRF}},\mathsf{M}} = \mathbf{A}_{C_{\mathsf{PRF}},\mathsf{M}'}$. We prove this in the section 3.3.

Particularly, if we choose PRF from the well-known efficient and provably secure candidates of PRFs like the ones from [53, 31, 47, 9, 8] can be computed by NC^1 circuits, let $\ell = t + k$ be the input length of PRF (which is a polynomial in the security parameter), the circuit depth of C_{PRF} will be $d = c \log \ell$ for some constant c. In this case we can set $\beta = O(\ell^{4c} \cdot m^{7/2}) \cdot \omega(\sqrt{\log m})$ and $q = O(\ell^{4c} \cdot m^4) \cdot (\omega(\sqrt{\log m}))^2$ which are polynomial in the security parameter.

It needs to mention that if we instantiate PRF by the (direct) LWE-based PRF from [9] or by the LWE-based PRF from [8] whose security relies on LWE assumption with super-polynomial modulus, the security of our signature scheme has to rely on LWE assumption with super-polynomial modulus. Such LWE assumption is stronger than the SIS assumption with polynomial modulus (as we set above) from which we make the proof for the following theorem.

3.3 Security of the Signature Scheme

The security of our signature scheme is stated by the following theorem.

Theorem 3.1. *Let λ be a security parameter. The parameters n, m, and q are chosen as the section 3.2. If the $(t_{\mathsf{SIS}}, \epsilon_{\mathsf{SIS}})$-$\mathsf{SIS}_{n,q,\beta,m}$ assumption holds and the PRF used in the signature scheme is $(t_{\mathsf{PRF}}, \epsilon_{\mathsf{PRF}})$-secure, the signature scheme is (t, q_s, ϵ)-$\mathsf{EUF\text{-}CMA}$ secure where $\epsilon_{\mathsf{SIS}} \geq \epsilon/2 - \epsilon_{\mathsf{PRF}} - \mathsf{negl}(\lambda)$, for some negligible statistical error $\mathsf{negl}(\lambda)$, and $\max(t_{\mathsf{PRF}}, t_{\mathsf{SIS}}) \leq t + O(q_s \cdot (T_S + T_E))$ where q_s is the number of signing query, T_S is the maximum running time of $\mathsf{SampleRight}$, and T_E is the maximum running time of $\mathsf{Eval}_{\mathsf{BV}}$ for one input message.*

Proof. Consider the following security game between an adversary $\mathcal{A}$ and a simulator $\mathcal{B}$. Upon receiving a $\mathsf{SIS}_{n,q,\beta,m}$ challenge $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, the challenger $\mathcal{B}$ prepares Vk as follows:

1. Select $k + 4$ matrices $\mathbf{R}_{\mathbf{A}_0}$, $\mathbf{R}_{\mathbf{A}_1}$, $\{\mathbf{R}_{\mathbf{B}_i}\}_{i \in [k]}$, $\mathbf{R}_{\mathbf{C}_0}$, $\mathbf{R}_{\mathbf{C}_1} \xleftarrow{\$} \{1, -1\}^{m \times m}$.
2. Select a secure pseudorandom function $\mathsf{PRF} : \{0,1\}^k \times \{0,1\}^t \to \{0,1\}$ and express it as a NAND Boolean circuit C_{PRF} with depth d.
3. Select a PRF key $K = s_1 s_2 \dots s_k \xleftarrow{\$} \{0,1\}^k$.
4. Set $\mathbf{A}_b = \mathbf{A}\mathbf{R}_{\mathbf{A}_b} + b\mathbf{G}$ and $\mathbf{C}_b = \mathbf{A}\mathbf{R}_{\mathbf{C}_b} + b\mathbf{G}$ for $b = 0, 1$.
5. Set $\mathbf{B}_i = \mathbf{A}\mathbf{R}_{\mathbf{B}_i} + s_i\mathbf{G}$ for $i \in [k]$.
6. Select a Gaussian parameter $s > 0$.
7. Publish $\mathsf{Vk} = \big(\mathbf{A}, \{\mathbf{A}_0, \mathbf{A}_1\}, \{\mathbf{B}_i\}_{i \in [k]}, \{\mathbf{C}_0, \mathbf{C}_1\}, \mathsf{PRF}, C_{\mathsf{PRF}}\big)$.

In the query phase, the adversary $\mathcal{A}$ adaptively issues messages for inquiring the corresponding signatures. Consider a message $\mathsf{M} = m_1 m_2 \dots m_t \in \{0,1\}^t$. $\mathcal{B}$ does the following to prepare the signature:

1. Compute $\mathbf{A}_{C_{\mathsf{PRF}}} = \mathbf{A}\mathbf{R}_{C_{\mathsf{PRF}},\mathsf{M}} + \mathsf{PRF}(K, \mathsf{M})\mathbf{G} \in \mathbb{Z}_q^{n \times m}$ by $\mathsf{Eval}_{\mathsf{BV}}(C_{\mathsf{PRF}}, \{\mathbf{B}_i\}_{i \in [k]}, \mathbf{C}_{m_1}, \mathbf{C}_{m_2}, \dots, \mathbf{C}_{m_t})$.
2. Let $b = \mathsf{PRF}(K, \mathsf{M})$, it sets

$$\begin{aligned} \mathbf{F}_{\mathsf{M},1-b} &= \big[\mathbf{A} \mid \mathbf{A}_{1-b} - \mathbf{A}_{C_{\mathsf{PRF}},\mathsf{M}}\big] \\ &= \big[\mathbf{A} \mid \mathbf{A}(\mathbf{R}_{\mathbf{A}_{1-b}} - \mathbf{R}_{C_{\mathsf{PRF}},\mathsf{M}}) + (1-2b)\mathbf{G}\big] \end{aligned}$$

and runs $\mathsf{SampleRight}$ to generate the signature $\mathsf{Sig} = \mathbf{d}_{\mathsf{M}} \sim D_{\Lambda_q^{\perp}(\mathbf{F}_{\mathsf{M},1-b}),s}$.

Finally, $\mathcal{A}$ output a forgery $(\mathbf{d}^*, \mathsf{M}^*)$. Let $\mathsf{PRF}(K, \mathsf{M}^*) = b$. If $\|\mathbf{d}\| > s\sqrt{2m}$ or $\left[\mathbf{A} \mid \mathbf{A}_{1-b} - \mathbf{A}_{C_{\mathsf{PRF}},\mathsf{M}^*}\right]\mathbf{d}^* = 0 \pmod q$, $\mathcal{B}$ aborts. Otherwise, we have $\left[\mathbf{A} \mid \mathbf{A}_b - \mathbf{A}_{C_{\mathsf{PRF}},\mathsf{M}^*}\right]\mathbf{d}^* = 0 \pmod q$. Let $\mathbf{d}^* = [\mathbf{d}_1^\top \mid \mathbf{d}_2^\top]^\top \in \mathbb{Z}^{2m}$. $\mathcal{B}$ outputs $\mathbf{e} = \mathbf{d}_1 + (\mathbf{R}_{\mathbf{A}_b} - \mathbf{R}_{C_{\mathsf{PRF}},\mathsf{M}^*})\mathbf{d}_2$ where $\|\mathbf{e}\| \le \beta$ as a solution for the $\mathsf{SIS}_{n,q,\beta,m}$ problem instance.

We show that Vk output by $\mathcal{B}$ has the correct distribution. In the real scheme, the matrix $\mathbf{A}$ is generated by $\mathsf{TrapGen}$. In the simulation, $\mathbf{A}$ has uniform distribution in $\mathbb{Z}_q^{n\times m}$ as it comes from the SIS challenge. By the Lemma 2.3, $\mathbf{A}$ generated in the simulation has right distribution except a negligibly small statistical error. Secondly, the matrices $\mathbf{A}$, $\{\mathbf{A}_0, \mathbf{A}_1\}$, $\{\mathbf{B}_i\}_{i\in[k]}$, and $\{\mathbf{C}_0, \mathbf{C}_1\}$ computed in the simulation have distribution that is statistically close to uniform distribution in $\mathbb{Z}_q^{n\times m}$ by the Lemma 2.1. In particular, the PRF secret key $\{s_i\}_{i\in[k]}$ is information-theoretically concealed by $\{\mathbf{B}_i\}_{i\in[k]}$.

Now we show that given $\{\mathbf{A}_0, \mathbf{A}_1\}$, $\{\mathbf{B}_i\}_{i\in[k]}$, and $\{\mathbf{C}_0, \mathbf{C}_1\}$, it is hard to find two messages $\mathsf{M} \ne \mathsf{M}'$ such that $\mathbf{A}_{C_{\mathsf{PRF}},\mathsf{M}} = \mathbf{A}_{C_{\mathsf{PRF}},\mathsf{M}'}$. Assume an efficient adversary finds $\mathsf{M} \ne \mathsf{M}'$ such that $\mathbf{A}_{C_{\mathsf{PRF}},\mathsf{M}} = \mathbf{A}_{C_{\mathsf{PRF}},\mathsf{M}'}$. With the public parameters set up above, we have

$$\mathbf{A}\mathbf{R}_{C_{\mathsf{PRF}},\mathsf{M}} + \mathsf{PRF}(K, \mathsf{M})\mathbf{G} = \mathbf{A}\mathbf{R}_{C_{\mathsf{PRF}},\mathsf{M}'} + \mathsf{PRF}(K, \mathsf{M}')\mathbf{G}$$

If $\mathsf{PRF}(K, \mathsf{M}) \ne \mathsf{PRF}(K, \mathsf{M}')$, which will happen essentially $1/2$ probability if PRF is secure, we have $\mathbf{R}_{C_{\mathsf{PRF}},\mathsf{M}} \ne \mathbf{R}_{C_{\mathsf{PRF}},\mathsf{M}'}$ and $\mathbf{A}(\mathbf{R}_{C_{\mathsf{PRF}},\mathsf{M}} - \mathbf{R}_{C_{\mathsf{PRF}},\mathsf{M}'}) \pm \mathbf{G} = 0 \pmod q$. By Lemma 2.8 and Algorithm 1, a low-norm vector $\bar{\mathbf{d}} \in \mathbb{Z}^{m\times m}$ can be efficiently found such that $\mathbf{G}\bar{\mathbf{d}} = \mathbf{0} \pmod q$ where $\bar{\mathbf{d}} \ne \mathbf{0}$ and $\left\|\bar{\mathbf{d}}\right\| \le s'\sqrt{m}$ for some Gaussian parameter $s' \ge \sqrt{5}\cdot\omega(\sqrt{\log m})$. Then $(\mathbf{R}_{C_{\mathsf{PRF}},\mathsf{M}} - \mathbf{R}_{C_{\mathsf{PRF}},\mathsf{M}'})\cdot\bar{\mathbf{d}}$ will be a non-zero vector with all but negligible probability and, therefore, a valid the SIS solution for $\mathbf{A}$.

In the query phase, the signatures replied to $\mathcal{A}$ have the correct distribution under the predefined conditions. Indeed, by the Theorem 2.7, for sufficient large Gaussian parameter s, the the distribution of signatures generated in the simulation by $\mathsf{SampleRight}$ is statistically close to $D_{\Lambda_q^\perp(\mathbf{F}_{\mathsf{M},1-b}),s}$ where the distribution of signatures generated in the real scheme by $\mathsf{SampleLeft}$ is also statistically close to $D_{\Lambda_q^\perp(\mathbf{F}_{\mathsf{M},1-b}),s}$.

In the forge phase, $\mathcal{A}$ will have at most advantage ϵ_{PRF} in predicting the bit value b with respect to the message it wants to forge. Therefore, if $\mathcal{A}$ can not distinguish PRF from random functions, it will randomly pick either of the matrices $\mathbf{A}_0$ or $\mathbf{A}_1$ to make a forgery. With $\frac{1}{2}$ chance it will pick the one that $\mathcal{B}$ will be able to use to solve the SIS problem. So we have $\epsilon_{\mathsf{SIS}} \ge \epsilon/2 - \epsilon_{\mathsf{PRF}} - \mathsf{negl}(\lambda)$ where $\mathsf{negl}(\lambda)$ stands for negligible statistical error in the simulation.

To argue that $\mathbf{e} = \mathbf{d}_1 + (\mathbf{R}_{\mathbf{A}_1} - \mathbf{R}_{C_{\mathsf{PRF}},\mathsf{M}^*})\mathbf{d}_2$ is a valid solution of the $\mathsf{SIS}_{n,q,\beta,m}$ problem instance, we need to show $\mathbf{e}$ is sufficiently short, and non-zero except with negligible probability. First of all, we have

$$\begin{aligned}\left[\mathbf{A} \mid \mathbf{A}_b - \mathbf{A}_{C_{\mathsf{PRF}},\mathsf{M}^*}\right]\mathbf{d}^* &= \left[\mathbf{A} \mid \mathbf{A}(\mathbf{R}_{\mathbf{A}_b} - \mathbf{R}_{C_{\mathsf{PRF}},\mathsf{M}^*})\right]\mathbf{d}^* \\ &= \mathbf{A}\mathbf{d}_1 + \mathbf{A}(\mathbf{R}_{\mathbf{A}_b} - \mathbf{R}_{C_{\mathsf{PRF}},\mathsf{M}^*})\mathbf{d}_2 \\ &= \mathbf{A}\left(\mathbf{d}_1 + \mathbf{R}\cdot\mathbf{d}_2\right) \\ &= \mathbf{0} \pmod q\end{aligned}$$

where $\mathbf{R} = \mathbf{R}_{\mathbf{A}_b} - \mathbf{R}_{C_{\mathsf{PRF}},\mathsf{M}^*}$. Since $\mathbf{d}_1, \mathbf{d}_2$ have distribution $D_{\mathbb{Z}^m,s}$ with condition $\mathbf{d} \in \Lambda_q^\perp(\mathbf{F}_{\mathsf{M},b})$, by the Lemma 2.4, $\mathbf{d}_1, \mathbf{d}_2 \le s\sqrt{m}$. By Lemma 2.11, we have $\|\mathbf{e}\| \le \|\mathbf{d}_1\| + \|\mathbf{R}\|_2 \cdot \|\mathbf{d}_2\| \le O(4^d \cdot m^{3/2}) \cdot s\sqrt{m}$. Let $\beta \ge O(4^d \cdot m^{3/2}) \cdot s\sqrt{m}$ is sufficient.

It remains to show that $\mathbf{e} = \mathbf{d}_1 + \mathbf{R}\cdot\mathbf{d}_2 \ne \mathbf{0}$. Suppose $\mathbf{d}_2 \ne \mathbf{0}$, we have $\mathbf{e} \ne \mathbf{0}$ since $\mathbf{d} \ne \mathbf{0}$. On the other hand, we have $\mathbf{d}_2 = (d_1, \ldots, d_m)^\top \ne \mathbf{0}$ and, thus, at least one coordinate of $\mathbf{d}_2$, say d_j, is not 0. We write $\mathbf{R} = (\mathbf{r}_1, \ldots, \mathbf{r}_m)$ and so

$$\mathbf{R}\cdot\mathbf{d}_2 = \mathbf{r}_j \cdot d_j + \sum_{i=1, i\ne j}^{m} \mathbf{r}_i \cdot d_i$$

Observe that for the fixed message M^* on which $\mathcal{A}$ made the forgery, $\mathbf{R}$ (therefore $\mathbf{r}_j$) depends on the low-norm matrices $\mathbf{R}_{\mathbf{A}_0}, \mathbf{R}_{\mathbf{A}_1}, \{\mathbf{R}_{\mathbf{B}_i}\}_{i\in[k]}, \mathbf{R}_{\mathbf{C}_0}, \mathbf{R}_{\mathbf{C}_1}$ and the secret key of PRF. The only information about $\mathbf{r}_j$ for $\mathcal{A}$ is from the public matrices in Vk, i.e. $\{\mathbf{A}_0, \mathbf{A}_1\}, \{\mathbf{B}_i\}_{i\in[k]}, \{\mathbf{C}_0, \mathbf{C}_1\}$. So by the pigeonhole principle there is a (exponentially) large freedom to pick a value to $\mathbf{r}_j$ which is compatible with $\mathcal{A}$'s view, i.e. $\mathbf{A}\mathbf{r}'_j = \mathbf{A}\mathbf{r}''_j \pmod q$ for admissible (low-norm) $\mathbf{r}'_j, \mathbf{r}''_j$ where $\mathbf{r}'_j \neq \mathbf{r}''_j$. (In fact, here we have more freedom than the case in [21] where $\mathbf{R}$ is picked from $\{1, -1\}^{m\times m}$).

Finally, to answer one signing query, $\mathcal{B}$'s running time is bounded by $O(T_S + T_E)$. So the total running time of $\mathcal{B}$ in the simulation is bounded by $O(q_s(T_S + T_E))$ This concludes the proof. □

4 IBE with Tight Security

4.1 Construction with CPA Security

Setup(1^λ) The setup algorithm takes as input a security parameter λ. It does the following:

1. Sample a random matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ along with a trapdoor basis $\mathbf{T}_\mathbf{A} \in \mathbb{Z}^{m\times m}$ of lattice $\Lambda_q^\perp(\mathbf{A})$ by running $\mathsf{TrapGen}$.
2. Select random matrices $\mathbf{A}_0$, $\mathbf{A}_1$, random "PRF key" matrices $\mathbf{B}_1, \ldots, \mathbf{B}_k$, and random "PRF input" matrices $\mathbf{C}_0$, $\mathbf{C}_1$ from $\mathbb{Z}_q^{n\times m}$ uniformly at random.
3. Select a random vector $\mathbf{u} \xleftarrow{\$} \mathbb{Z}_q^n$.
4. Select a secure pseudorandom function $\mathsf{PRF} : \{0,1\}^k \times \{0,1\}^t \to \{0,1\}$, express it as a NAND Boolean circuit C_PRF with depth $d = d(\lambda)$, and select a PRF key $K = s_1 s_2 \ldots s_k \xleftarrow{\$} \{0,1\}^k$.
5. Output the public parameters

$$\mathsf{Pub} = \big(\mathbf{A}, \{\mathbf{A}_0, \mathbf{A}_1\}, \{\mathbf{B}_i\}_{i\in[k]}, \{\mathbf{C}_0, \mathbf{C}_1\}, \mathbf{u}, \mathsf{PRF}, C_\mathsf{PRF}\big)$$

and the master secret key $\mathsf{Msk} = (\mathbf{T}_\mathbf{A}, K)$.

KeyGen$(\mathsf{Pub}, \mathsf{Msk}, \mathsf{id})$ Upon an input identity $\mathsf{id}{=}x_1x_2\ldots x_t \in \{0,1\}^t$, the key generation algorithm does the following:

1. Compute $b = \mathsf{PRF}(K, \mathsf{id})$.
2. Compute $\mathbf{A}_{C_\mathsf{PRF},\mathsf{id}} = \mathsf{Eval}_\mathsf{BV}(C_\mathsf{PRF}, \{\mathbf{B}\}_{i\in[k]}, \mathbf{C}_{x_1}, \mathbf{C}_{x_2}, \ldots, \mathbf{C}_{x_t}) \in \mathbb{Z}_q^{n\times m}$.
3. Set $\mathbf{F}_{\mathsf{id},1-b} = \big[\mathbf{A} \mid \mathbf{A}_{1-b} - \mathbf{A}_{C_\mathsf{PRF},\mathsf{id}}\big] \in \mathbb{Z}_q^{n\times 2m}$.
4. Run $\mathsf{SampleLeft}$ to sample $\mathbf{d}_\mathsf{id}$ from the discrete Gaussian distribution $D_{\Lambda_q^\mathbf{u}(\mathbf{F}_{\mathsf{id},1-b}),s}$ hence $\mathbf{F}_{\mathsf{id},1-b}\mathbf{d}_\mathsf{id} = \mathbf{u} \pmod q$. Output $\mathsf{Sk}_\mathsf{id} = \mathbf{d}_\mathsf{id}$.

Encrypt$(\mathsf{Pub}, \mathsf{id}, \mathsf{Msg})$ To encrypt a message $\mathsf{Msg} \in \{0,1\}$ with respect to an identity $\mathsf{id} = x_1x_2\ldots x_t \in \{0,1\}^t$:

1. Compute $\mathbf{A}_{C_\mathsf{PRF},\mathsf{id}} = \mathsf{Eval}_\mathsf{BV}(C_\mathsf{PRF}, \{\mathbf{B}_i\}_{i\in[k]}, \mathbf{C}_{x_1}, \mathbf{C}_{x_2}, \ldots, \mathbf{C}_{x_t})$.
2. Set $\mathbf{F}_{\mathsf{id},b} = \big[\mathbf{A} \mid \mathbf{A}_b - \mathbf{A}_{C_\mathsf{PRF},\mathsf{id}}\big] \in \mathbb{Z}_q^{n\times 2m}$ for $b = 0, 1$.
3. Select two random vectors $\mathbf{s}_0, \mathbf{s}_1 \xleftarrow{\$} \mathbb{Z}_q^n$.

4. Select two noise scalars $\nu_{0,0}, \nu_{1,0} \leftarrow D_{\mathbb{Z},\sigma_{\mathsf{LWE}}}$ and four noise vectors $\hat{\boldsymbol{\nu}}_{0,1}, \hat{\boldsymbol{\nu}}_{1,1} \leftarrow D_{\mathbb{Z}^m,\sqrt{2}\sigma_{\mathsf{LWE}}}$, $\check{\boldsymbol{\nu}}_{0,1}, \check{\boldsymbol{\nu}}_{1,1} \leftarrow D_{\mathbb{Z}^m,\sigma}$ where σ is sufficiently larger than σ_{LWE}. [5]

5. Compute the ciphertext $\mathsf{Ctx}_{\mathsf{id}} = (c_{0,0}, \mathbf{c}_{0,1}, c_{1,0}, \mathbf{c}_{1,1})$ as:

$$\begin{cases} c_{0,0} &= \left(\mathbf{s}_0^\top \mathbf{u} + \nu_{0,0} + \mathsf{Msg}\lfloor q/2 \rfloor\right) \bmod q \\ \mathbf{c}_{0,1}^\top &= \left(\mathbf{s}_0^\top \mathbf{F}_{\mathsf{id},0} + [\hat{\boldsymbol{\nu}}_{0,1}^\top \mid \check{\boldsymbol{\nu}}_{0,1}^\top]\right) \bmod q \end{cases}$$

$$\begin{cases} c_{1,0} &= \left(\mathbf{s}_1^\top \mathbf{u} + \nu_{1,0} + \mathsf{Msg}\lfloor q/2 \rfloor\right) \bmod q \\ \mathbf{c}_{1,1}^\top &= \left(\mathbf{s}_1^\top \mathbf{F}_{\mathsf{id},1} + [\hat{\boldsymbol{\nu}}_{1,1}^\top \mid \check{\boldsymbol{\nu}}_{1,1}^\top]\right) \bmod q \end{cases}$$

Decrypt$(\mathsf{Pub}, \mathsf{Sk}_{\mathsf{id}}, \mathsf{Ctx}_{\mathsf{id}})$ The decryption algorithm uses the key $\mathbf{d}_{\mathsf{id}}$ to try to decrypt both $(c_{0,0}, \mathbf{c}_{0,1})$ and $(c_{1,0}, \mathbf{c}_{1,1})$ [6]. W.l.o.g., assume that $(c_{b,0}, \mathbf{c}_{b,1})$ is the correct ciphertext. The decryption algorithm computes

$$\tau = \left(c_{b,0} - \mathbf{c}_{b,1}^\top \mathbf{d}_{\mathsf{id}}\right) \bmod q$$

View τ as an integer in $(-q/2, q/2]$. If τ is closer to 0 than $\pm q/2$, the output is $\mathsf{Msg} = 0$. Otherwise, it is $\mathsf{Msg} = 1$.

4.2 Correctness

Following the decryption algorithm, let $\mathbf{d}_{\mathsf{id}} = [\mathbf{d}_1^\top \mid \mathbf{d}_2^\top]^\top$. We have

$$\begin{aligned} \tau &= \left(c_{b,0} - \mathbf{c}_{b,1}^\top \mathbf{d}_{\mathsf{id}}\right) \bmod q \\ &= \left(\mathsf{Msg}\lfloor q/2 \rfloor + \nu_{b,0} - \hat{\boldsymbol{\nu}}_{0,1}^\top \mathbf{d}_1 - \check{\boldsymbol{\nu}}_{0,1}^\top \mathbf{d}_2\right) \bmod q \end{aligned}$$

Recall, the norm of $\mathbf{d}_1$ and $\mathbf{d}_2$ is bounded by $s\sqrt{m}$, and the norm of $\hat{\boldsymbol{\nu}}_{b,1}$ and $\check{\boldsymbol{\nu}}_{b,1}$ is bounded by $\sigma_{\mathsf{LWE}}\sqrt{m}$ and $\sigma\sqrt{m}$ respectively, by Lemma 2.4. To ensure correctness of decryption, we need

$$\begin{aligned} |\tau| &= |c_{b,0} - \hat{\boldsymbol{\nu}}_{b,1}^\top \mathbf{d}_1 - \check{\boldsymbol{\nu}}_{0,1}^\top \mathbf{d}_2| \\ &\le |c_{b,0}| + \|\hat{\boldsymbol{\nu}}_{0,1}\| \cdot \|\mathbf{d}_1\| + \|\hat{\boldsymbol{\nu}}_{0,1}\| \cdot \|\mathbf{d}_2\| \\ &\le O(s \cdot m \cdot (\sigma_{\mathsf{LWE}} + \sigma)) \\ &\le q/4 \end{aligned}$$

Accordingly, it is enough to set q such that $O(s \cdot m \cdot (\sigma_{\mathsf{LWE}} + \sigma)) \le q/4$.

4.3 Parameter Selection and Discussion

We now discuss a consistent parameter instantiation that achieves both correctness and security. Let λ be the security parameter, $t = t(\lambda)$ be the identity length, $k = k(\lambda)$ be the secret key length of PRF, and let $\ell = t + k$ be the input length of PRF. Let, for the most general case, the circuit depth of PRF be $d = d(\lambda)$. To ensure we can run $\mathsf{TrapGen}$ in the Lemma 2.3, we set $m = n^{1+\eta}$ for some $\eta > 0$ (we assume $n^\eta > O(\log q)$). To make sure $\mathsf{SampleLeft}$ in the

[5] For instance we set $\sigma = O(4^d \cdot m^{3/2}) \cdot \omega(\sqrt{\log m}) \cdot \sigma_{\mathsf{LWE}}$.

[6] To ensure correct decryption, the message should contain some redundancy to weed out the incorrect ciphertext. It is a standard technique to encrypt multiple bits in GPV-style encryption, by replacing $\mathbf{u}$ with a matrix $\mathbf{U} \in \mathbb{Z}_q^{n \times z}$ in Pub with which we can now independently encrypt $z > 1$ bits without change to the security analysis. If hybrid encryption is used, the multiple bits can be used to encrypt a symmetric key *without* redundancy, deferring the integrity check to the symmetric realm where it can be performed at minimal cost.

real scheme and SampleRight in the simulation algorithm Sim.KeyGen (see section 4.4) have the same output distribution per Theorem 2.7, we set a sufficiently large Gaussian parameter $s = \|\tilde{\mathbf{T}}_{\mathbf{G}}\| \cdot O(4^d \cdot m^{3/2}) \cdot \omega(\sqrt{\log m})$. To ensure the applicability of Regev's [55] and Peikert's [54] LWE reductions from worst-case lattice problems, we set the Gaussian parameter of LWE noise distribution to be $\sigma_{\mathsf{LWE}} = \sqrt{n}$. So the LWE noise distribution is $(D_{\mathbb{Z},\sqrt{n}}) \bmod q$. For the security proof (specifically for the proofs of Lemma 4.3 and Lemma 4.9), we set $\sigma = O(4^d \cdot m^{3/2}) \cdot \omega(\sqrt{\log m}) \cdot \sigma_{\mathsf{LWE}}$. Finally, to ensure correctness condition of decryption, we set $q = O(16^d \cdot m^{9/2}) \cdot (\omega\sqrt{\log m})^2$.

As for our signature scheme, if we the PRF can be computed by a NC^1 NAND circuit with depth $d = c \log \ell$ for some constant $c > 1$, we can set the LWE modulus $q = O(\ell^{4c} \cdot m^{9/2}) \cdot (\omega\sqrt{\log m})^2$, which is polynomial in the security parameter λ.

Tight Reduction and Hardness of LWE. It is known that larger modulus results in stronger LWE assumption, if the standard deviation of the noise distribution stays unchanged. More precisely, let B be the maximum magnitude of the LWE noise, and q be the LWE modulus. The hardness of the LWE problem depends on the ratio q/B. The LWE problem becomes easier when this ratio grows. In this regard, the appeal of our tight reduction varies: tight reduction to harder LWE problem is more preferable than tight reduction to easier LWE problem. This is true particularly when one considers the average-case hardness of LWE to worst-case hardness of classic lattice problems, e.g. GapSVP and SIVP, reductions [55, 54, 22] where ratio q/B is smaller, the solutions for classic lattice problems are better.

One feature of our IBE scheme (and the signature scheme it induces) is that depending on different circuits instantiations, the assumptions we male for our tight reduction may vary. In addition, if we use a LWE-based PRF, our IBE scheme relies on the stronger one of two LWE assumptions: one is made for the PRF and another one is made for our construction, which uses a polynomial modulus q as we chose above. Currently, basing our IBE scheme solely on LWE needs to assume the LWE assumption with super-polynomial modulus. This is because the state-of-art PRFs from LWE (from [9, 8]) in terms of efficiency and provable security require super-polynomial LWE modulus.

On the other hand, we believe that our tight reduction is still very valuable even for large ratio q/B. Firstly, it shows that, at the first time, we actually can eliminate the dependency between the number of adversary's queries and the security of lattice-based IBE scheme (as well as *short* lattice signature scheme). This is very important since the number of adversary's queries can be quite large, which will negatively impact the schemes' security seriously. Secondly, the average-case to worst-case reduction does provide some security confidence for the LWE assumption, but this is not the whole story. For certain parameters, many classic lattice problems are NP-hard. However, those parameters have no direct connection to lattice-based cryptography. (There is even evidence that the classic lattice problems with parameters relevant cryptography are not NP-hard.) On the other hand, the LWE problem (with various parameters) could be assured to be a hard problem in its own right. It has shown robustness against various attacks in a relatively long-term period. This has made LWE widely accepted as standard assumption and for use in cryptography. For instance, even for sub-exponentially large ratios $q/B = 2^{O(n^c)}$ where n is the LWE dimension and $0 < c < 1/2$, the LWE problem is still believed to be hard and leads to powerful cryptographic schemes which we were not able to obtain by other means, including fully homomorphic encryption, e.g. [23], attribute-based encryption for circuits, e.g. [40, 19, 25], and predicate encryption for circuits [41].

4.4 Proof of Security

The security of our IBE scheme with respect to the Definition 2.9 can be stated by the following theorem.

Theorem 4.1. *Let λ be a security parameter. The parameters n, q are chosen as the section 4.3. Let χ be the distribution $D_{\mathbb{Z}^m,\sqrt{n}}$. If the $(t_{LWE}, \epsilon_{LWE})$-$LWE_{n,q,\chi}$ assumption holds and the PRF used in the IBE scheme is $(t_{PRF}, \epsilon_{PRF})$-secure, then the IBE scheme is (t, q_{id}, ϵ)-IND-ID-CPA secure such that $\epsilon \leq 2(\epsilon_{PRF} + \epsilon_{LWE}) + negl(\lambda)$ for some negligible function $negl(\lambda)$, and $\max(t_{PRF}, t_{LWE}) \leq t + O\left(q_{id} \cdot (T_S + T_E)\right)$ where T_S is the maximum running time of SampleRight and T_E is the maximum running time of $Eval_{BV}$ for one input identity.*

We prove above theorem through a sequence of indistinguishable security games. The first game is identical to the IND-ID-CPA game. In the last game, the adversary has no advantage. We will show that a PPT adversary will not be able to distinguish the neighboring games which will prove that the adversary has only negligibly small advantage in wining the first (real) game.

Firstly, we define the following simulation algorithms Sim.Setup, Sim.KeyGen and Sim.Encrypt.

$\mathsf{Sim.Setup}(1^\lambda)$ The algorithm does the following:

1. Select matrix $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n \times m}$.
2. Select $k+4$ low-norm matrices $\mathbf{R}_{\mathbf{A}_0}, \mathbf{R}_{\mathbf{A}_1}, \{\mathbf{R}_{\mathbf{B}_i}\}_{i\in[k]}, \mathbf{R}_{\mathbf{C}_0}, \mathbf{R}_{\mathbf{C}_1} \xleftarrow{\$} \{1,-1\}^{m\times m}$.
3. Select a secure pseudorandom function $\mathsf{PRF} : \{0,1\}^k \times \{0,1\}^t \to \{0,1\}$ and express it as a NAND Boolean circuit C_{PRF} with depth $d = d(\lambda)$.
4. Select a uniformly random string $K = s_1 s_2 \dots s_k \xleftarrow{\$} \{0,1\}^k$.
5. Set $\mathbf{A}_b = \mathbf{A}\mathbf{R}_{\mathbf{A}_b} + b\mathbf{G}$ and $\mathbf{C}_b = \mathbf{A}\mathbf{R}_{\mathbf{C}_b} + b\mathbf{G}$ for $b = 0, 1$.
6. Set $\mathbf{B}_i = \mathbf{A}\mathbf{R}_{\mathbf{B}_i} + s_i\mathbf{G}$ for $i \in [k]$.
7. Select vector $\mathbf{u} \xleftarrow{\$} \mathbb{Z}_q^n$.
8. Publish $\mathsf{Pub} = \left(\mathbf{A}, \{\mathbf{A}_0, \mathbf{A}_1\}, \{\mathbf{B}_i\}_{i\in[k]}, \{\mathbf{C}_0, \mathbf{C}_1\}, \mathbf{u}, \mathsf{PRF}, C_{\mathsf{PRF}}\right)$

$\mathsf{Sim.KeyGen}(\mathsf{Pub}, \mathsf{Msk}, \mathsf{id})$ Upon an input identity $\mathsf{id} = x_1 x_2 \dots x_t \in \{0,1\}^t$, the algorithm uses the parameters generated from Sim.Setup to do the following:

1. Compute $\mathbf{A}_{\mathsf{PRF},\mathsf{id}} = \mathbf{A}\mathbf{R}_{C_{\mathsf{PRF}},\mathsf{id}} + \mathsf{PRF}(K, \mathsf{id})\mathbf{G} \leftarrow \mathsf{Eval}_{\mathsf{BV}}(C_{\mathsf{PRF}}, \{\mathbf{B}_i\}_{i\in[k]}, \mathbf{C}_{x_1}, \dots, \mathbf{C}_{x_t})$.
2. Let $\mathsf{PRF}(K, \mathsf{id}) = b \in \{0,1\}$. Set

$$\begin{aligned}\mathbf{F}_{\mathsf{id},1-b} &= \left[\mathbf{A} \mid \mathbf{A}_{1-b} - \mathbf{A}_{C_{\mathsf{PRF}},\mathsf{id}}\right] \\ &= \left[\mathbf{A} \mid \mathbf{A}(\mathbf{R}_{\mathbf{A}_{1-b}} - \mathbf{R}_{C_{\mathsf{PRF}},\mathsf{id}}) + (1-2b)\mathbf{G}\right].\end{aligned}$$

3. Run SampleRight to sample $\mathbf{d}_{\mathsf{id}} \in D_{\Lambda_q^{\mathbf{u}}(\mathbf{F}_{\mathsf{id},1-b}),s}$ as the private key $\mathsf{Sk}_{\mathsf{id}}$.

$\mathsf{Sim.Encrypt}(\mathsf{Pub}, \mathsf{id}^*, \mathsf{Msg})$ To encrypt a message $\mathsf{Msg}^* \in \{0,1\}$ with respect to an identity id^*:

1. Compute $b = \mathsf{PRF}(K, \mathsf{id}^*)$.
2. Set

$$\begin{aligned}\mathbf{F}_{\mathsf{id}^*,b} &= \left[\mathbf{A} \mid \mathbf{A}_b - \mathbf{A}_{C_{\mathsf{PRF}},\mathsf{id}^*}\right] \\ &= \left[\mathbf{A} \mid \mathbf{A}(\mathbf{R}_{\mathbf{A}_b} - \mathbf{R}_{C_{\mathsf{PRF}},\mathsf{id}^*})\right]\end{aligned}$$

and

$$\begin{aligned}\mathbf{F}_{\mathsf{id}^*,1-b} &= \left[\mathbf{A} \mid \mathbf{A}_{1-b} - \mathbf{A}_{C_{\mathsf{PRF}},\mathsf{id}^*}\right] \\ &= \left[\mathbf{A} \mid \mathbf{A}(\mathbf{R}_{\mathbf{A}_{1-b}} - \mathbf{R}_{C_{\mathsf{PRF}},\mathsf{id}^*}) + (1-2b)\mathbf{G}\right].\end{aligned}$$

3. Select random vectors $\mathbf{s}_b, \mathbf{s}_{1-b} \xleftarrow{\$} \mathbb{Z}_q^n$.

4. Select noise scalars $\nu_{b,0}, \nu_{1-b,0} \leftarrow D_{\mathbb{Z},\sigma_{\mathsf{LWE}}}$.

5. Sample noise vectors $\mathbf{x}, \mathbf{y} \leftarrow D_{\mathbb{Z}^m,\sigma_{\mathsf{LWE}}}$ for sufficiently large Gaussian parameter σ_{LWE} ($\sigma_{\mathsf{LWE}} \geq \eta_\varepsilon(\mathbb{Z}^m)$ for some small $\varepsilon > 0$). Set $\hat{\boldsymbol{\nu}}_{b,1} = \mathbf{x} + \mathbf{y}$.

6. Let $\mathbf{R} = \mathbf{R}_{\mathbf{A}_b} - \mathbf{R}_{\mathsf{PRF},\mathsf{id}^*}$ and $\mathbf{r}_i$ be the i-th column of $\mathbf{R}$. We sample the noise vector $\mathbf{z} = (z_1, z_2, \ldots, z_m) \in \mathbb{Z}^m$ with $z_i \leftarrow D_{\mathbb{Z},\sigma_{1,i}}$ for the sufficiently large Gaussian parameter $\sigma_{1,i} = \sqrt{\sigma^2 - 2(\|\mathbf{r}_i\| \cdot \sigma_{\mathsf{LWE}})^2}$. [7] Set $\check{\boldsymbol{\nu}}_{b,1} = \mathbf{R}^\top \cdot (\mathbf{x} - \mathbf{y}) + \mathbf{z}$.

7. Select noise vectors $\hat{\boldsymbol{\nu}}_{1-b,1} \leftarrow D_{\mathbb{Z}^m,\sqrt{2}\sigma_{\mathsf{LWE}}}$, $\check{\boldsymbol{\nu}}_{1-b,1} \leftarrow D_{\mathbb{Z}^m,\sigma}$.

8. Set the challenge ciphertext $\mathsf{Ctx}_{\mathsf{id}^*} = (c_{b,0},\ \mathbf{c}_{b,1},\ c_{1-b,0},\ \mathbf{c}_{1-b,1})$ as:

$$\begin{cases} c_{b,0} &= \left(\mathbf{s}_b^\top \mathbf{u} + \nu_{b,0} + \mathsf{Msg}\lfloor q/2 \rfloor\right) \bmod q \\ \mathbf{c}_{b,1}^\top &= \left(\mathbf{s}_b^\top \mathbf{F}_{\mathsf{id}^*,b} + [\hat{\boldsymbol{\nu}}_{b,1}^\top \mid \check{\boldsymbol{\nu}}_{b,1}^\top]\right) \bmod q \end{cases}$$

$$\begin{cases} c_{1-b,0} &= \left(\mathbf{s}_{1-b}^\top \mathbf{u} + \nu_{1-b,0} + \mathsf{Msg}\lfloor q/2 \rfloor\right) \bmod q \\ \mathbf{c}_{1-b,1}^\top &= \left(\mathbf{s}_{1-b}^\top \mathbf{F}_{\mathsf{id}^*,1-b} + [\hat{\boldsymbol{\nu}}_{1-b,1}^\top \mid \check{\boldsymbol{\nu}}_{1-b,1}^\top]\right) \bmod q \end{cases}$$

Now we define a series of games and prove that the neighboring games are either statistically indistinguishable, or computationally indistinguishable.

Game 0 This is the real IND-ID-CPA game from the definition. All the algorithms are the same as the real scheme.

Game 1 This game is the same as **Game 0** except it runs Sim.Setup and Sim.KeyGen instead of Setup and KeyGen.

Game 2 This game is the same as **Game 1** except that the challenge ciphertext is generated by Sim.Encrypt instead of Encrypt.

Game 3 This game is the same as **Game 2** except that during preparation of the challenge ciphertext for identity id^*, it samples $(c_{b,0}, \mathbf{c}_{b,1})$ uniformly random from $\mathbb{Z}_q \times \mathbb{Z}_q^{2m}$ for $b = \mathsf{PRF}(K, \mathsf{id}^*)$. Another part of the challenge ciphertext $(c_{1-b,0}, \mathbf{c}_{1-b,1})$ is computed by Sim.Encrypt as in **Game 2**.

Game 4 This game is the same as **Game 3** except for $b = \mathsf{PRF}(K, \mathsf{id}^*)$ it runs real encryption algorithm Encrypt to generate $(c_{1-b,0}, \mathbf{c}_{1-b,1})$ of the challenge ciphertext instead of using Sim.Encrypt.

Game 5 This game is the same as **Game 4** except it runs Setup and KeyGen to generate Pub and private identity keys.

Game 6 This game is the same as **Game 5** except that for $b = \mathsf{PRF}(K, \mathsf{id}^*)$, the challenge ciphertext part $(c_{b,0}, \mathbf{c}_{b,1})$ is generated by Encrypt instead of choosing it randomly, and $(c_{1-b,0}, \mathbf{c}_{1-b,1})$ is chosen randomly.

[7] In section 4.3, the σ is set large enough such that $\sigma_{1,i}$ can be larger than $\|\mathbf{R}\| \cdot \eta_\varepsilon(\mathbb{Z}^m)$.

Game 7 This game is the same as **Game 6** except that it runs $\mathsf{Sim.Setup}$ and $\mathsf{Sim.KeyGen}$ to generate Pub and private identity keys.

Game 8 This game is the same as **Game 7** except that for the bit value $b = \mathsf{PRF}(K, \mathsf{id}^*)$, it computes the challenge ciphertext $(c_{b,0}, \mathbf{c}_{b,1})$ by $\mathsf{Sim.Encrypt}$.

Game 9 This game is the same as **Game 8** except that the whole challenge ciphertext is sampled uniformly at random from the ciphertext space. Therefore, in **Game 5** the adversary has no advantage in wining the game.

In **Game** i, we let S_i be the event that $\gamma' = \gamma$ at the end of the game. The adversary's advantage in **Game** i is $|\Pr[S_i] - \frac{1}{2}|$. We prove the following lemmas to prove the Theorem 4.1.

Lemma 4.2. Game 1 *and* **Game 0** *are statistically indistinguishable, so* $|\Pr[S_0] - \Pr[S_1]| \leq \mathsf{negl}(\lambda)$ *for some negligible function* $\mathsf{negl}(\lambda)$*.*

Proof. We analyse the differences between **Game 0** and **Game 1**:

1. In **Game 0**, the matrix $\mathbf{A}$ is generated by $\mathsf{TrapGen}$, and in **Game 1**, the matrix $\mathbf{A}$ is chosen uniformly random. By the Lemma 2.3, the distributions of these two ways of constructing the matrix $\mathbf{A}$ are statistically close.

2. In **Game 0**, the matrices $\{\mathbf{A}_0, \mathbf{A}_1\}$, $\{\mathbf{B}_i\}_{i\in[k]}$, $\{\mathbf{C}_0, \mathbf{C}_1\}$ are chosen uniformly at random from $\mathbb{Z}_q^{n\times m}$. In **Game 1**, They are computed as $\mathbf{A}_b = \mathbf{A}\mathbf{R}_{\mathbf{A}_b} + b\mathbf{G}$, $\mathbf{C}_b = \mathbf{A}\mathbf{R}_{\mathbf{C}_b} + b\mathbf{G}$ for $b = 0, 1$, and $\mathbf{B}_i = \mathbf{A}\mathbf{R}_{\mathbf{B}_i} + s_i\mathbf{G}$ for $i \in [k]$ for random and secret low-norm matrices $\mathbf{R}_{\mathbf{A}_0}, \mathbf{R}_{\mathbf{A}_1}, \{\mathbf{R}_{\mathbf{B}_i}\}_{i\in[k]}, \mathbf{R}_{\mathbf{C}_0}, \mathbf{R}_{\mathbf{C}_1}$ from $\{1, -1\}^{m\times m}$. By the Lemma 2.1, the distributions of these two ways of generating these public matrices are statistically close. In particular, the PRF secret key $\{s_i\}_{i\in[k]}$ is information-theoretically concealed by $\{\mathbf{B}_i\}_{i\in[k]}$.

3. We note that in both **Game 0** and **Game 1**, the use of $\mathbf{A}_0$ or $\mathbf{A}_1$ of the key generation algorithms is decided by $b = \mathsf{PRF}(K, \mathsf{id})$. For a private key query on id in **Game 1**, let

$$\begin{aligned}\mathbf{F}_{\mathsf{id},1-b} &= \left[\mathbf{A} \mid \mathbf{A}_{1-b} - \mathbf{A}_{\mathsf{PRF},\mathsf{id}}\right] \\ &= \left[\mathbf{A} \mid \mathbf{A}(\mathbf{R}_{\mathbf{A}_{1-b}} - \mathbf{R}_{\mathsf{PRF},\mathsf{id}}) + (1-2b)\mathbf{G}\right].\end{aligned}$$

   Note that the publicly known trapdoor of $\Lambda_q^{\perp}(\mathbf{G})$ is also a trapdoor of $\Lambda_q^{\perp}((1-2b)\mathbf{G})$. In **Game 1**, the identity key $\mathbf{d}_{\mathsf{id}} \in \Lambda_q^{\mathbf{u}}(\mathbf{F}_{\mathsf{id},1-b})$ is generated by $\mathsf{SampleLeft}$ with the trapdoor basis $\mathbf{T}_{\mathbf{A}}$ of $\Lambda_q^{\perp}(\mathbf{A})$. In **Game 1**, $\mathbf{d}_{\mathsf{id}}$ is generated by $\mathsf{SampleRight}$ with the trapdoor of $\Lambda_q^{\perp}((1-2b)\mathbf{G})$. By the Theorems 1 and 2, for sufficient large Gaussian parameter s, the identity key $\mathbf{d}_{\mathsf{id}}$ will have the same distribution $D_{\Lambda_q^{\mathbf{u}}(\mathbf{F}_{\mathsf{id},1-b}),s}$ up to a negligibly small statistical difference.

Summing up, the distributions of **Game 0** and **Game 1** are statistically close, and thus $|\Pr[S_0] - \Pr[S_1]| \leq \mathsf{negl}(\lambda)$ for some negligible function $\mathsf{negl}(\lambda)$. □

Lemma 4.3. Game 2 *and* **Game 1** *are statistically indistinguishable, so* $|\Pr[S_1] - \Pr[S_2]| \leq \mathsf{negl}(\lambda)$ *for some negligible function* $\mathsf{negl}(\lambda)$*.*

Proof. Let $\mathbf{R} = \mathbf{R}_{\mathbf{A}_b} - \mathbf{R}_{C_{\mathsf{PRF}},\mathsf{id}^*}$ in the $\mathsf{Sim.Encrypt}$ algorithm. The difference between **Game 1** and **Game 2** is the way of generating the challenge ciphertext. In **Game 1**, the challenge ciphertext is generated by $\mathsf{Encrypt}$, and the noise vectors are sampled from some discrete Gaussian distributions that are independent of Pub. In **Game 2** the challenge ciphertext is generated by $\mathsf{Sim.Encrypt}$, and $\mathbf{R}$, where $\mathbf{R}$ is computed from $\mathbf{R}_{\mathbf{A}_0}, \mathbf{R}_{\mathbf{A}_1}, \{\mathbf{R}_{\mathbf{B}_i}\}_{i\in[k]}, \mathbf{R}_{\mathbf{C}_0}, \mathbf{R}_{\mathbf{C}_1}$, PRF's key K, circuit C_{PRF} and id^*.

By construction, Encrypt and Sim.Encrypt generate $(c_{b,0}, c_{1-b,0}, \mathbf{c}_{1-b,1})$ in the essentially same way (besides the negligible statistical difference in their input public parameters). So $(c_{b,0}, c_{1-b,0}, \mathbf{c}_{1-b,1})$ part of the challenge ciphertexts output by Encrypt and Sim.Encrypt are statistically close.

By the construction of $\mathbf{c}_{b,1}$ in the challenge ciphertext in **Game 2**,

$$\begin{aligned}
\mathbf{c}_{b,1}^\top &= \left(\mathbf{s}_b^\top \mathbf{F}_{\mathsf{id}^*,b} + [\hat{\boldsymbol{\nu}}_{b,1}^\top \mid \check{\boldsymbol{\nu}}_{b,1}^\top]\right) \bmod q \\
&= \mathbf{s}_0^\top \left[\mathbf{A} | \mathbf{A}(\mathbf{R}_{\mathbf{A}_b} - \mathbf{R}_{C_{\mathsf{PRF}},\mathsf{id}^*})\right] + [(\mathbf{x}+\mathbf{y})^\top \mid \mathbf{R}(\mathbf{x}-\mathbf{y})^\top + \mathbf{z}^\top]\Big) \bmod q \\
&= \left(\mathbf{s}_0^\top \left[\mathbf{A} | \mathbf{A}\mathbf{R}\right] + [(\mathbf{x}+\mathbf{y})^\top | \mathbf{R}(\mathbf{x}-\mathbf{y})^\top + \mathbf{z}^\top]\right) \bmod q
\end{aligned}$$

By the Lemma 2.1 (the generalised left-over hash lemma), with $\mathbf{R}$ appearing in the challenge ciphertext, the public matrices $\mathbf{A}_0, \mathbf{A}_1, \{\mathbf{B}_i\}_{i\in[k]}, \mathbf{C}_0, \mathbf{C}_1$ still have distribution which is statistically close to the uniform distribution on $\mathbb{Z}_q^{n\times m}$.

Now we use the idea of smoothing parameter and continuous Gaussian approximation to show that the noise terms $(\mathbf{x}+\mathbf{y}, \mathbf{R}^\top(\mathbf{x}-\mathbf{y})+\mathbf{z})$ have proper distribution. [8] In particularly, we show $\mathbf{x}+\mathbf{y}$ and $\mathbf{R}^\top(\mathbf{x}-\mathbf{y})+\mathbf{z}$ have proper distributions individually and are statistically independent.

Firstly, since $\mathbf{R}$ has independent columns and $\mathbf{z}$ has independent coordinates and $\mathbf{R}, \mathbf{z}$ would not appear in other places, vector $\mathbf{R}^\top(\mathbf{x}-\mathbf{y})+\mathbf{z}$ has independent coordinates. Secondly, $\mathbf{x}-\mathbf{y}$ is discrete Gaussian with Gaussian parameter σ_{LWE} greater than the smoothing parameter $\eta_\varepsilon(\mathbb{Z}^m)$, so $\mathbf{R}^\top(\mathbf{x}-\mathbf{y})$ is a mixture of discrete Gaussians that closely approximates a (mixture of) continuous Gaussians, but only on a "large scale" greater than $\|\mathbf{R}\| \cdot \eta_\varepsilon(\mathbb{Z}^m)$. The term $\mathbf{z}$ is used to smooth out all visible discretisation introduced by $\mathbf{R}$ and make $\mathbf{R}^\top(\mathbf{x}-\mathbf{y})+\mathbf{z}$ closely approximate a continuous Gaussian that has zero-correlation and fixed standard deviation. So by the construction of Sim.Encrypt and Lemma 2.5, $\mathbf{R}^\top(\mathbf{x}-\mathbf{y})+\mathbf{z}$ has distribution which is statistically close to $D_{\mathbb{Z}^m,\sigma}$ as required. By the same reason, $\mathbf{x}+\mathbf{y}$ has discrete Gaussian distribution $D_{\mathbb{Z}^m,\sqrt{2}\sigma_{\mathsf{LWE}}}$ that closely approximates the continuous Gaussian with standard deviation $\sqrt{2}\sigma_{\mathsf{LWE}}$.

Since each of $\mathbf{x}+\mathbf{y}$ and $\mathbf{R}^\top(\mathbf{x}-\mathbf{y})+\mathbf{z}$ closely approximates a multivariate continuous Gaussian as seen above, for which the covariance $Cov(\mathbf{x}+\mathbf{y}, \mathbf{R}^\top(\mathbf{x}-\mathbf{y})+\mathbf{z}) = 0$ making (the continuous approximations of) $\mathbf{x}+\mathbf{y}$ and $\mathbf{R}^\top(\mathbf{x}-\mathbf{y})+\mathbf{z}$ statistically independent.

Summing up, $\mathbf{c}_{b,1}$ output by Encrypt has distribution that is statistically close to the distribution of $\mathbf{c}_{b,1}$ output by Sim.Encrypt. Therefore **Game 1** and **Game 2** are statistically indistinguishable and the lemma follows. □

Lemma 4.4. *If (t, ϵ_{LWE})-$LWE_{n,q,\chi}$ assumption holds where χ stands for the distribution $D_{\mathbb{Z},\sigma_{LWE}}$ reduced modulo q, then $|\Pr[S_2] - \Pr[S_3]| \leq \epsilon_{LWE}$.*

Proof. We show a simulation algorithm $\mathcal{B}$ that uses its LWE challenge to simulate either **Game 2** or **Game 3** for an adversary $\mathcal{A}$. At the beginning, $\mathcal{B}$ receives its LWE challenge $(\mathbf{W}, \mathbf{v}) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^m$ and $(\mathbf{w}, v) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ which is either from $\mathcal{O}_\$$ or $\mathcal{O}_\mathbf{s}$.

Setup. $\mathcal{B}$ prepares the public parameters for $\mathcal{A}$ as follows:

1. Set $\mathbf{A} \leftarrow \mathbf{W}$ and $\mathbf{u} \leftarrow \mathbf{v}$. We note $\mathbf{A}, \mathbf{u}$ have uniform distribution.
2. Set other public parameters as **Game 2**.

Phase 1. $\mathcal{B}$ answers private key queries like **Game 2**.

Challenge. $\mathcal{B}$ prepares the challenge ciphertext of identity id^* as follows.

[8] Notice that the simulator knows $\mathbf{R}$ and adversary does not know $\mathbf{R}$, $\mathbf{x}-\mathbf{y}$, and $\mathbf{z}$ individually.

1. Let $b = \mathsf{PRF}(K, \mathsf{id}^*)$. $\mathcal{B}$ sets

$$\begin{aligned}\mathbf{F}_{\mathsf{id}^*,1-b} &= \left[\mathbf{A} \mid \mathbf{A}_{1-b} - \mathbf{A}_{C_{\mathsf{PRF}},\mathsf{id}^*}\right] \\ &= \left[\mathbf{A} \mid \mathbf{A}(\mathbf{R}_{\mathbf{A}_{1-b}} - \mathbf{R}_{C_{\mathsf{PRF}},\mathsf{id}^*}) + (1-2b)\mathbf{G}\right]\end{aligned}$$

2. Let $\mathbf{R} = \mathbf{R}_{\mathbf{A}_0} - \mathbf{R}_{C_{\mathsf{PRF}},\mathsf{id}^*}$. $\mathcal{B}$ samples $\mathbf{y} \leftarrow D_{\mathbb{Z}^m,\sigma_{\mathsf{LWE}}}$. It also samples $\mathbf{z} \in \mathbb{Z}^m$ as in $\mathsf{Sim.Encrypt}$ by its knowledge of $\mathbf{R}$. Then to construct $(c_{b,0}, \mathbf{c}_{b,1})$, it sets

$$\begin{cases} c_{b,0} &= (v + \mathsf{Msg}^* \lfloor q/2 \rfloor) \bmod q \\ \mathbf{c}_{b,1}^\top &= \left([\mathbf{v}^\top | \mathbf{v}^\top \mathbf{R}] + [\mathbf{y}^\top | -\mathbf{y}^\top \mathbf{R} + \mathbf{z}^\top]\right) \bmod q \end{cases}$$

3. $\mathcal{B}$ sets $(c_{1-b,0}, \mathbf{c}_{1-b,1})$ the same as **Game 2**.

Phase 2. $\mathcal{B}$ replies the private key queries as in **Game 2**.

Guess. Finally, $\mathcal{A}$ outputs whether it is interacting with **Game 2** or **Game 3**. If $\mathcal{A}$ says **Game 2**, $\mathcal{B}$ decides its LWE challenge is from $\mathcal{O}_{\mathbf{s}}$. Otherwise, $\mathcal{B}$ decides the LWE challenge is from $\mathcal{O}_{\$}$.

If $\mathcal{B}$ gets the LWE challenge from the oracle $\mathcal{O}_{\mathbf{s}}$, there exists a secret vector $\mathbf{s} \in \mathbb{Z}_q^n$, a noise scalar x with distribution $D_{\mathbb{Z},\sigma_{\mathsf{LWE}}}$, a noise vector $\mathbf{x} \in \mathbb{Z}^m$ with distribution $D_{\mathbb{Z}^m,\sigma_{\mathsf{LWE}}}$ such that $\mathbf{v}^\top = \mathbf{s}^\top \mathbf{A} + \mathbf{x}^\top$ and $v = \mathbf{s}^\top \mathbf{w} + x$. Rewrite the ciphertext we have

$$\begin{aligned} c_{b,0} &= (v + \mathsf{Msg}^* \lfloor q/2 \rfloor) \bmod q \\ &= \left(\mathbf{s}^\top \mathbf{w} + x + \mathsf{Msg}^* \lfloor q/2 \rfloor\right) \bmod q \\ &= \left(\mathbf{s}_b^\top \mathbf{u} + \nu_{b,0} + \mathsf{Msg}^* \lfloor q/2 \rfloor\right) \bmod q \end{aligned}$$

and

$$\begin{aligned} \mathbf{c}_{b,1}^\top &= \left([\mathbf{v}^\top | \mathbf{v}^\top \mathbf{R}] + [\mathbf{y}^\top | -\mathbf{y}^\top \mathbf{R} + \mathbf{z}^\top]\right) \bmod q \\ &= \left([\mathbf{s}^\top \mathbf{A} + \mathbf{x}^\top | (\mathbf{s}^\top \mathbf{A} + \mathbf{x}^\top)\mathbf{R}] + [\mathbf{y}^\top | -\mathbf{y}^\top \mathbf{R} + \mathbf{z}^\top]\right) \bmod q \\ &= \left(\mathbf{s}^\top [\mathbf{A} | \mathbf{A}\mathbf{R}] + [\mathbf{x}^\top + \mathbf{y}^\top | (\mathbf{x}^\top - \mathbf{y}^\top)\mathbf{R} + \mathbf{z}^\top]\right) \bmod q \\ &= \left(\mathbf{s}_b^\top \mathbf{F}_{\mathsf{id}^*,b} + [\hat{\boldsymbol{\nu}}_{b,1}^\top | \check{\boldsymbol{\nu}}_{b,1}^\top]\right) \bmod q \end{aligned}$$

They are valid challenge ciphertext parts in **Game 2**. Therefore, in this case $\mathcal{B}$ simulates **Game 2** for $\mathcal{A}$. On the other hand, if $\mathcal{B}$ gets samples from $\mathcal{O}_{\$}$, $(c_{b,0}, \mathbf{c}_{b,1})$ constructed above will be random, which is the case of **Game 3**, and $\mathcal{B}$ simulates **Game 3**. $|\Pr[S_2] - \Pr[S_3]| \leq \epsilon_{\mathsf{LWE}}$ follows. □

Lemma 4.5. $|\Pr[S_3] - \Pr[S_4]| = 0$.

Proof. Note for generating $(c_{1-b,0}, \mathbf{c}_{1-b,1})$ of the challenge ciphertext, $\mathsf{Encrypt}$ and $\mathsf{Sim.Encrypt}$ behave the same. $(c_{b,0}, \mathbf{c}_{b,1})$ is a random string in both games. So adversary's advantages in **Game 4** and **Game 3** are the same. □

Lemma 4.6. Game 5 *and* **Game 4** *are statistically indistinguishable, so* $|\Pr[S_4] - \Pr[S_5]| \leq \mathsf{negl}(\lambda)$ *for some negligible function* $\mathsf{negl}(\lambda)$.

Proof. The proof is essentially the same as the proof for Lemma 4.2. We omit the details. □

Lemma 4.7. *If the PRF* PRF *is* $(t, \epsilon_{\mathsf{PRF}})$*-secure, then* $|\Pr[S_5] - \Pr[S_6]| \leq 2\epsilon_{\mathsf{PRF}}$.

Proof. We recall the difference between **Game 6** and **Game 5**. let $b = \mathsf{PRF}(K, \mathsf{id}^*)$ for the challenge identity id^*. In **Game 5**, the ciphertext component $(c_{b,0}, \mathbf{c}_{b,1})$ is uniformly random and $(c_{1-b,0}, \mathbf{c}_{1-b,1})$ is computed by $\mathsf{Encrypt}$. In **Game 6**, the ciphertext component $(c_{b,0}, \mathbf{c}_{b,1})$ is computed by $\mathsf{Encrypt}$ and $(c_{1-b,0}, \mathbf{c}_{1-b,1})$ is uniformly random. To prove the indistinguishably between **Game 6** and **Game 5**, three additional security games are added.

Firstly we define **Game 5.1** which is same as **Game 5** except that it samples $b \xleftarrow{\$} \{0,1\}$ to select matrix $\mathbf{A}_b$ for generating private keys and challenge ciphertext instead of using PRF to compute it. Also, if same identity is queried multiple times, the same bit b will be used (For simulation, we simply let the simulator keep a state remembering the bit for each identity.). Obviously, a distinguisher between **Game 5** and **Game 5.1** leads to a attacker for PRF. So $|\Pr[S_5] - \Pr[S_{5.1}]| \leq \epsilon_{\mathsf{PRF}}$.

Secondly, we define **Game 5.2** which is the same as **Game 5.1** except for randomly sampled bit b for id^*, it runs $\mathsf{Encrypt}$ to produce $(c_{b,0}, \mathbf{c}_{b,1})$ and samples $(c_{1-b,0}, \mathbf{c}_{1-b,1})$ uniformly random from $\mathbb{Z}_q \times \mathbb{Z}_q^{2m}$. While here b is uniformly random, we must have $|\Pr[S_{5.1}] - \Pr[S_{5.2}]| = 0$.

Finally, as **Game 6** is the same as **Game 5.2** except the bit value b is computed via PRF in key generation query phase and challenge phase, so we have $|\Pr[S_{5.2}] - \Pr[S_6]| \leq \epsilon_{\mathsf{PRF}}$.

$|\Pr[S_5] - \Pr[S_6]| \leq 2\epsilon_{\mathsf{PRF}}$ follows. □

Lemma 4.8. Game 7 *and* **Game 6** *are statistically indistinguishable, so* $|\Pr[S_6] - \Pr[S_7]| \leq \mathsf{negl}(\lambda)$ *for some negligible function* $\mathsf{negl}(\lambda)$.

Proof. The proof is essentially the same as the proof for Lemma 4.2. We omit the details. □

Lemma 4.9. Game 8 *and* **Game 7** *are statistically indistinguishable, so* $|\Pr[S_7] - \Pr[S_8]| \leq \mathsf{negl}(\lambda)$ *for some negligible function* $\mathsf{negl}(\lambda)$.

Proof. The proof is essentially the same as the proof for Lemma 4.3. We omit the details. □

Lemma 4.10. *If* $(t, \epsilon_{\mathsf{LWE}})$-$\mathsf{LWE}_{n,q,\chi}$ *assumption holds where* χ *stands for the distribution* $D_{\mathbb{Z},\sigma_{\mathsf{LWE}}}$ *reduced modulo* q*, then* $|\Pr[S_8] - \Pr[S_9]| \leq \epsilon_{\mathsf{LWE}}$.

Proof. The proof is essentially the same as the proof for Lemma 4.4. We omit the details. □

Now we prove the Theorem 4.1 by the established lemmas.

Proof. Based on the lemmas that show the difference between the sequence of games, we have $\epsilon = |\Pr[S_0] - 1/2| \leq 2(\epsilon_{\mathsf{PRF}} + \epsilon_{\mathsf{LWE}}) + \mathsf{negl}(\lambda)$ for some negligibly small statistical error $\mathsf{negl}(\lambda)$. The running time of $\mathcal{B}$ is dominated by answering q_{id} private key generation queries from $\mathcal{A}$. For answering one such query, $\mathcal{B}$ needs to apply the key-homomorphic algorithm on the circuit of PRF. This requires time T_E. Besides that, $\mathcal{B}$ needs to run $\mathsf{SampleRight}$ to sample Gaussian vectors for constructing the private keys, which requires at most time T_S. Therefore, for one query, $\mathcal{B}$ roughly runs $O(T_S + T_E)$ time. For all q_{id} queries and constructing the challenge ciphertext, the total time is bounded by $O(q_{\mathsf{id}} \cdot (T_S + T_E))$. So if an adversary $\mathcal{A}$ has running time t, $\max(t_{\mathsf{LWE}}, t_{\mathsf{PRF}}) \leq t + O(q_{\mathsf{id}} \cdot (T_S + T_E))$. □

4.5 Adaptively CCA-Secure IBE and CCA-Secure PKE

Boneh at al. [17] showed a $\ell + 1$-depth CPA-secure Hierarchical IBE (HIBE) scheme ($\ell \geq 0$) can be tightly transferred into an ℓ-depth CCA-secure HIBE scheme with small additional overhead (known as the BCHK transformation). In particularly, a 1-depth HIBE scheme is an IBE scheme and a 0-depth HIBE scheme is a public-key encryption scheme PKE. Generally, in HIBE, identities are arranged in a directed tree. A user with identity of a father node can issue private keys for the users with identities of children nodes. This process is called delegation. Ideally, we would like to have HIBE schemes supporting identity trees with polynomial depth.

Unfortunately, directly applying our technique will result in an HIBE scheme with only log-depth identity tree. On the other hand, our technique particularly works for 2-depth HIBE scheme. So by applying the BCHK transformation, we obtain a IND-ID-CCA2 secure IBE scheme from the 2-depth IND-ID-CPA HIBE scheme and a IND-CCA2 secure PKE scheme from our IND-ID-CPA secure IBE scheme[9].

5 Conclusions

In this paper, we propose a short adaptively secure lattice signature scheme and a "compact" adaptively secure IBE scheme in the standard model. Our constructions make use of PRFs in a novel way by combining several recent techniques in the area of lattice-based cryptography. The security of our signature and IBE scheme is tightly related to the conservative lattice assumptions SIS and LWE, respectively, and the security of an instantiated PRF, with a constant loss factor. By instantiating the existing efficient PRFs from lattice and number-theoretic assumptions which can be implemented by shallow circuits, we obtain the first "almost" tightly secure lattice-based short signature/IBE scheme whose security is based on LWE assumption with super-polynomial modulus, and an adaptively secure IBE scheme with the tightest security reduction so far, i.e. with only $O(\log^2 \lambda)$ factor of security loss for the security parameter λ, based on a novel combination of lattice and number-theoretic assumptions.

The problem of constructing a tightly and adaptively secure IBE scheme from standard assumptions (in the sense that the security loss of reduction is a constant) remains open. Our work suggests that constructing tightly secure PRFs, which is another important open problem left by [31, 47], would solve it. We leave as a fascinating open problem the question of employing similar (or different) techniques to construct compact and (almost) tightly secure signature and encryption schemes with increased expressiveness, such as hierarchical and attribute-based encryption scheme, or homomorphic signatures. Another interesting open question is to construct a PRF from LWE assumption with polynomial modulus.

Acknowledgement

We would like to thank Jacob Alperin-Sheriff for useful comments.

References

[1] Masayuki Abe, Bernardo David, Markulf Kohlweiss, Ryo Nishimaki, and Miyako Ohkubo. Public-key cryptography – pkc 2013: 16th international conference on practice and theory in public-key cryptography, nara, japan, february 26 – march 1, 2013. proceedings. chapter Tagged One-Time Signatures: Tight Security and Optimal Tag Size, pages 312–331. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.

[2] Shweta Agrawal, Dan Boneh, and Xavier Boyen. Efficient lattice (h)ibe in the standard model. In Henri Gilbert, editor, *Advances in Cryptology - EUROCRYPT 2010*, volume 6110 of *Lecture Notes in Computer Science*, pages 553–572. Springer Berlin Heidelberg, 2010.

[3] Miklós Ajtai. Generating hard instances of lattice problems (extended abstract). In *Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing*, STOC '96, pages 99–108, New York, NY, USA, 1996. ACM.

[9] This transformation does not require us to add new computational assumptions. The SIS assumption, which is weaker than the LWE assumption, is enough.

[4] Jacob Alperin-Sheriff. Short signatures with short public keys from homomorphic trapdoor functions. In Jonathan Katz, editor, *Public-Key Cryptography – PKC 2015*, volume 9020 of *Lecture Notes in Computer Science*, pages 236–255. Springer Berlin Heidelberg, 2015.

[5] Daniel Apon, Xiong Fan, and Feng-Hao Liu. Fully-secure lattice-based IBE as compact as PKE. Cryptology ePrint Archive, Report 2016/125, 2016. `http://eprint.iacr.org/`.

[6] Nuttapong Attrapadung, Goichiro Hanaoka, and Shota Yamada. A framework for identity-based encryption with almost tight security. In Tetsu Iwata and JungHee Cheon, editors, *Advances in Cryptology - ASIACRYPT 2015*, volume 9452 of *Lecture Notes in Computer Science*, pages 521–549. Springer Berlin Heidelberg, 2015.

[7] Shi Bai, Adeline Langlois, Tancrède Lepoint, Damien Stehlé, and Ron Steinfeld. Improved security proofs in lattice-based cryptography: using the rényi divergence rather than the statistical distance. In *Advances in Cryptology–ASIACRYPT 2015*, pages 3–24. Springer, 2015.

[8] Abhishek Banerjee and Chris Peikert. New and improved key-homomorphic pseudorandom functions. In JuanA. Garay and Rosario Gennaro, editors, *Advances in Cryptology – CRYPTO 2014*, volume 8616 of *Lecture Notes in Computer Science*, pages 353–370. Springer Berlin Heidelberg, 2014.

[9] Abhishek Banerjee, Chris Peikert, and Alon Rosen. Pseudorandom functions and lattices. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology – EUROCRYPT 2012*, volume 7237 of *Lecture Notes in Computer Science*, pages 719–737. Springer Berlin Heidelberg, 2012.

[10] 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*, CCS '93, pages 62–73, New York, NY, USA, 1993. ACM.

[11] Olivier Blazy, SaqibA. Kakvi, Eike Kiltz, and Jiaxin Pan. Tightly-secure signatures from chameleon hash functions. In Jonathan Katz, editor, *Public-Key Cryptography – PKC 2015*, volume 9020 of *Lecture Notes in Computer Science*, pages 256–279. Springer Berlin Heidelberg, 2015.

[12] Olivier Blazy, Eike Kiltz, and Jiaxin Pan. (hierarchical) identity-based encryption from affine message authentication. In JuanA. Garay and Rosario Gennaro, editors, *Advances in Cryptology – CRYPTO 2014*, volume 8616 of *Lecture Notes in Computer Science*, pages 408–425. Springer Berlin Heidelberg, 2014.

[13] Florian Böhl, Dennis Hofheinz, Tibor Jager, Jessica Koch, Jae Hong Seo, and Christoph Striecks. *Advances in Cryptology – EUROCRYPT 2013: 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings*, chapter Practical Signatures from Standard Assumptions, pages 461–485. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.

[14] Dan Boneh and Xavier Boyen. Efficient selective-id secure identity-based encryption without random oracles. In Christian Cachin and JanL. Camenisch, editors, *Advances in Cryptology - EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 223–238. Springer Berlin Heidelberg, 2004.

[15] Dan Boneh and Xavier Boyen. Secure identity based encryption without random oracles. In Matt Franklin, editor, *Advances in Cryptology - CRYPTO 2004*, volume 3152 of *Lecture Notes in Computer Science*, pages 443–459. Springer Berlin Heidelberg, 2004.

[16] Dan Boneh and Xavier Boyen. Short signatures without random oracles. In Christian Cachin and JanL. Camenisch, editors, *Advances in Cryptology - EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 56–73. Springer Berlin Heidelberg, 2004.

[17] Dan Boneh, Ran Canetti, Shai Halevi, and Jonathan Katz. Chosen-ciphertext security from identity-based encryption. *SIAM J. Comput.*, 36(5):1301–1328, December 2006.

[18] Dan Boneh and Matt Franklin. Identity-based encryption from the weil pairing. In Joe Kilian, editor, *Advances in Cryptology CRYPTO 2001*, volume 2139 of *Lecture Notes in Computer Science*, pages 213–229. Springer Berlin Heidelberg, 2001.

[19] Dan Boneh, Craig Gentry, Sergey Gorbunov, Shai Halevi, Valeria Nikolaenko, Gil Segev, Vinod Vaikuntanathan, and Dhinakaran Vinayagamurthy. Fully key-homomorphic encryption, arithmetic circuit abe and compact garbled circuits. In PhongQ. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology - EUROCRYPT 2014*, volume 8441 of *Lecture Notes in Computer Science*, pages 533–556. Springer Berlin Heidelberg, 2014.

[20] Dan Boneh, Ben Lynn, and Hovav Shacham. Short signatures from the weil pairing. *Journal of Cryptology*, 17(4):297–319, 2004.

[21] Xavier Boyen. Lattice mixing and vanishing trapdoors: A framework for fully secure short signatures and more. In PhongQ. Nguyen and David Pointcheval, editors, *Public Key Cryptography - PKC 2010*, volume 6056 of *Lecture Notes in Computer Science*, pages 499–517. Springer Berlin Heidelberg, 2010.

[22] Zvika Brakerski, Adeline Langlois, Chris Peikert, Oded Regev, and Damien Stehlé. Classical hardness of learning with errors. In *Proceedings of the Forty-fifth Annual ACM Symposium on Theory of Computing*, STOC '13, pages 575–584, New York, NY, USA, 2013. ACM.

[23] Zvika Brakerski and Vinod Vaikuntanathan. Efficient fully homomorphic encryption from (standard) LWE. In *Proceedings of the 2011 IEEE 52nd Annual Symposium on Foundations of Computer Science*, FOCS '11, pages 97–106, Washington, DC, USA, 2011. IEEE Computer Society.

[24] Zvika Brakerski and Vinod Vaikuntanathan. Lattice-based FHE as secure as PKE. In *Proceedings of the 5th conference on Innovations in theoretical computer science*, pages 1–12. ACM, 2014.

[25] Zvika Brakerski and Vinod Vaikuntanathan. Circuit-abe from lwe: Unbounded attributes and semi-adaptive security. Cryptology ePrint Archive, Report 2016/118, 2016. `http://eprint.iacr.org/`.

[26] Jan Camenisch and Anna Lysyanskaya. *Advances in Cryptology – CRYPTO 2004: 24th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 2004. Proceedings*, chapter Signature Schemes and Anonymous Credentials from Bilinear Maps, pages 56–72. Springer Berlin Heidelberg, Berlin, Heidelberg, 2004.

[27] Ran Canetti, Shai Halevi, and Jonathan Katz. A forward-secure public-key encryption scheme. In Eli Biham, editor, *Advances in Cryptology - EUROCRYPT 2003*, volume 2656 of *Lecture Notes in Computer Science*, pages 255–271. Springer Berlin Heidelberg, 2003.

[28] David Cash, Dennis Hofheinz, Eike Kiltz, and Chris Peikert. Bonsai trees, or how to delegate a lattice basis. *Journal of Cryptology*, 25(4):601–639, 2012.

[29] Jie Chen and Hoeteck Wee. Fully, (almost) tightly secure ibe and dual system groups. In Ran Canetti and JuanA. Garay, editors, *Advances in Cryptology - CRYPTO 2013*, volume 8043 of *Lecture Notes in Computer Science*, pages 435–460. Springer Berlin Heidelberg, 2013.

[30] Ronald Cramer and Victor Shoup. Signature schemes based on the strong rsa assumption. *ACM Trans. Inf. Syst. Secur.*, 3(3):161–185, August 2000.

[31] Nico Döttling and Dominique Schröder. Efficient pseudorandom functions via on-the-fly adaptation. In *Advances in Cryptology–CRYPTO 2015*, pages 329–350. Springer, 2015.

[32] Léo Ducas and Daniele Micciancio. *Advances in Cryptology – CRYPTO 2014: 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2014, Proceedings, Part I*, chapter Improved Short Lattice Signatures in the Standard Model, pages 335–352. Springer Berlin Heidelberg, Berlin, Heidelberg, 2014.

[33] Marc Fischlin. *The Cramer-Shoup Strong-RSA Signature Scheme Revisited*, volume 2567 of *Lecture Notes in Computer Science*, pages 116–129. Springer Berlin Heidelberg, 2003.

[34] Rosario Gennaro, Shai Halevi, and Tal Rabin. *Advances in Cryptology — EUROCRYPT '99: International Conference on the Theory and Application of Cryptographic Techniques Prague, Czech Republic, May 2–6, 1999 Proceedings*, chapter Secure Hash-and-Sign Signatures Without the Random Oracle, pages 123–139. Springer Berlin Heidelberg, Berlin, Heidelberg, 1999.

[35] Craig Gentry. Practical identity-based encryption without random oracles. In Serge Vaudenay, editor, *Advances in Cryptology - EUROCRYPT 2006*, volume 4004 of *Lecture Notes in Computer Science*, pages 445–464. Springer Berlin Heidelberg, 2006.

[36] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the 40th annual ACM symposium on Theory of computing*, STOC '08, pages 197–206, New York, NY, USA, 2008. ACM.

[37] Craig Gentry, Amit Sahai, and Brent Waters. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. In Ran Canetti and JuanA. Garay, editors, *Advances in Cryptology - CRYPTO 2013*, volume 8042 of *Lecture Notes in Computer Science*, pages 75–92. Springer Berlin Heidelberg, 2013.

[38] Eu-Jin Goh and Stanisław Jarecki. *Advances in Cryptology — EUROCRYPT 2003: International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, May 4–8, 2003 Proceedings*, chapter A Signature Scheme as Secure as the Diffie-Hellman Problem, pages 401–415. Springer Berlin Heidelberg, Berlin, Heidelberg, 2003.

[39] Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to construct random functions. *J. ACM*, 33(4):792–807, August 1986.

[40] Sergey Gorbunov, Vinod Vaikuntanathan, and Hoeteck Wee. Attribute-based encryption for circuits. In *Proceedings of the 45th annual ACM symposium on Symposium on theory of computing*, STOC '13, pages 545–554, New York, NY, USA, 2013. ACM.

[41] Sergey Gorbunov, Vinod Vaikuntanathan, and Hoeteck Wee. Predicate encryption for circuits from lwe. In Rosario Gennaro and Matthew Robshaw, editors, *Advances in Cryptology – CRYPTO 2015*, volume 9216 of *Lecture Notes in Computer Science*, pages 503–523. Springer Berlin Heidelberg, 2015.

[42] Sergey Gorbunov and Dhinakaran Vinayagamurthy. Riding on asymmetry: Efficient abe for branching programs. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 550–574. Springer, 2015.

[43] Dennis Hofheinz and Tibor Jager. *Advances in Cryptology – CRYPTO 2012: 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings*, chapter Tightly Secure Signatures and Public-Key Encryption, pages 590–607. Springer Berlin Heidelberg, Berlin, Heidelberg, 2012.

[44] Dennis Hofheinz, Jessica Koch, and Christoph Striecks. Identity-based encryption with (almost) tight security in the multi-instance, multi-ciphertext setting. In Jonathan Katz, editor, *Public-Key Cryptography – PKC 2015*, volume 9020 of *Lecture Notes in Computer Science*, pages 799–822. Springer Berlin Heidelberg, 2015.

[45] Susan Hohenberger and Brent Waters. *Advances in Cryptology - EUROCRYPT 2009: 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cologne, Germany, April 26-30, 2009. Proceedings*, chapter Realizing Hash-and-Sign Signatures under Standard Assumptions, pages 333–350. Springer Berlin Heidelberg, Berlin, Heidelberg, 2009.

[46] Susan Hohenberger and Brent Waters. Short and stateless signatures from the rsa assumption. In Shai Halevi, editor, *Advances in Cryptology - CRYPTO 2009*, volume 5677 of *Lecture Notes in Computer Science*, pages 654–670. Springer Berlin Heidelberg, 2009.

[47] Tibor Jager. Tightly-secure pseudorandom functions via work factor partitioning. Cryptology ePrint Archive, Report 2016/121, 2016. `http://eprint.iacr.org/`.

[48] Jonathan Katz and Nan Wang. Efficiency improvements for signature schemes with tight security reductions. In *Proceedings of the 10th ACM Conference on Computer and Communications Security*, CCS '03, pages 155–164, New York, NY, USA, 2003. ACM.

[49] Allison Lewko and Brent Waters. New proof methods for attribute-based encryption: Achieving full security through selective techniques. In Reihaneh Safavi-Naini and Ran Canetti, editors, *Advances in Cryptology - CRYPTO 2012*, volume 7417 of *Lecture Notes in Computer Science*, pages 180–198. Springer Berlin Heidelberg, 2012.

[50] Vadim Lyubashevsky. Lattice signatures without trapdoors. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology – EUROCRYPT 2012*, volume 7237 of *Lecture Notes in Computer Science*, pages 738–755. Springer Berlin Heidelberg, 2012.

[51] Daniele Micciancio and Chris Peikert. Trapdoors for lattices: Simpler, tighter, faster, smaller. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology ? EUROCRYPT 2012*, volume 7237 of *Lecture Notes in Computer Science*, pages 700–718. Springer Berlin Heidelberg, 2012.

[52] Daniele Micciancio and Oded Regev. Worst-case to average-case reductions based on gaussian measures. *SIAM J. Comput.*, 37(1):267–302, April 2007.

[53] Moni Naor and Omer Reingold. Number-theoretic constructions of efficient pseudo-random functions. *J. ACM*, 51(2):231–262, March 2004.

[54] Chris Peikert. Public-key cryptosystems from the worst-case shortest vector problem: extended abstract. In *Proceedings of the 41st annual ACM symposium on Theory of computing*, STOC '09, pages 333–342, New York, NY, USA, 2009. ACM.

[55] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In *Proceedings of the thirty-seventh annual ACM symposium on Theory of computing*, STOC '05, pages 84–93, New York, NY, USA, 2005. ACM.

[56] Brent Waters. Efficient identity-based encryption without random oracles. In Ronald Cramer, editor, *Advances in Cryptology - EUROCRYPT 2005*, volume 3494 of *Lecture Notes in Computer Science*, pages 114–127. Springer Berlin Heidelberg, 2005.

[57] Brent Waters. Dual system encryption: Realizing fully secure ibe and hibe under simple assumptions. In Shai Halevi, editor, *Advances in Cryptology - CRYPTO 2009*, volume 5677 of *Lecture Notes in Computer Science*, pages 619–636. Springer Berlin Heidelberg, 2009.