Towards Tightly Secure Lattice Short Signature and Id-Based Encryption

Xavier Boyen and Qinyi Li(✉)

Queensland University of Technology, Brisbane, Australia
qinyi.li@hdr.qut.edu.au

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

Xavier Boyen—Research conducted with generous support from the Australian Research Council under Discovery Project grant ARC DP-140103885.

J.H. Cheon and T. Takagi (Eds.): ASIACRYPT 2016, Part II, LNCS 10032, pp. 404–434, 2016.
DOI: 10.1007/978-3-662-53890-6_14

a challenging task. Some of the existing short signature schemes use random oracles, e.g., [10,19,36,48,50], or rely on non-standard computational assumptions (strong, interactive assumptions, and/or q-type parametric assumptions), e.g., [16,26,30,33,34], 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 [20,51]. 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 [4,32] 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., [1,11,43], or merely have heuristic security arguments based on random oracles, e.g., [39,48]. 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 is a 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 [17]. 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 [14,27] and the adaptive model [12,15,29,35,56,57], and from lattices in the adaptive model [2,5,28]. 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., [6,12,29,44]). 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. [2,5,28], 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: $\mathsf{PRF} : \mathcal{K} \times \mathcal{D} \rightarrow \mathcal{R}$ with the following security property. For random secret key K from $\mathcal{K}$, $\mathsf{PRF}(K, \cdot)$ is computationally indistinguishable from a random function $\Omega : \mathcal{D} \rightarrow \mathcal{R}$, 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 [40]), number-theoretic assumptions (e.g., the DDH/k-LIN assumption [31,47,53]), and lattice assumption LWE [8,9].

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. Depending on the underlying hardness assumption and the reduction of PRF, underlying assumptions and tightness of our signature/IBE scheme vary.

Our work indicates that tightly secure PRFs, which are based on standard assumptions and computable by polynomial size Boolean circuits, are sufficient for us to build tightly, adaptively secure lattice signature/IBE schemes. Ideally, it is better if the PRF instantiations assume weak assumptions and have shallow Boolean circuits implementations. In particular, by instantiating the 'almost" tightly secure PRFs from [8,9], (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.[1] 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, and allows us to answer the Open Problem #3.

While constructing low-depth (e.g. circuits in NC^1), tightly secure PRFs from standard assumptions with constant security loss in the black-box sense[2] remains an open problem, any progress made in such direction will improve our work toward solving Open Problem #1 and #2 (under SIS/LWE assumption). For instance, if the DDH/k-LIN-based PRFs from [47] achieve security loss $O(\log^2 \lambda)$ for security parameter λ, we obtain signature/IBE schemes enjoy the same security loss under the combined assumptions.

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] and the representative signature schemes from traditional number-theoretic assumptions, including (strong) RSA, Dlog and linear assumptions over pairings. Our signature scheme loses a factor of $O(\log^2 \lambda)$ in security proof if the DDH-based PRF instantiation achieves the same security loss. 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 [20] 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 [2,20,28]. So our constructions have larger concrete size of verification key than the signature scheme in [20] 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

[1] The (direct) lattice-based PRFs from [8,9] assume LWE assumption with super-polynomial modulus, which makes our schemes rely on LWE assumption for super-polynomial modulus.

[2] The security reduction does not require a priori information about a given adversary.

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 [20]	$O(1) \times \mathbb{Z}^m$	$O(\lambda q_s)$	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.

secure lattice-based signature/IBE scheme such as [2]. Although complexity leveraging 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 leveraged from selective DBDH-based IBE scheme 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 and sometimes require even stronger assumptions (in the lattice setting). Therefore, our current results are of more theoretical 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.

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 [19]	$O(1) \times \mathbb{G}$	$O(\lambda q_s)$	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 $c > 1$.

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, $5+k$ random matrices are chosen from $\mathbb{Z}_q^{n \times m}$, comprising: a "left" matrix $\mathbf{A}$, 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 consists of a "short" basis $\mathbf{T}_\mathbf{A}$ of $\mathbf{A}$ and a PRF key $K \in \{0,1\}^k$ for PRF.

The signer takes three steps to generate the signature of message $\mathsf{M} = x_1 x_2 \ldots x_t \in \{0,1\}^t$. Firstly, it uses the key-homomorphic evaluation algorithm developed from [18,24,38] to compute the unique matrix $\mathbf{A}_{\mathsf{PRF},\mathsf{M}}$ from the circuit

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

Scheme	Security loss	Assumption	Standard model?	Quantum-safe?
BF'01 [17]	$O(q_{\mathsf{id}})$	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 $O(\log^2(\lambda))$.

of PRF and the $k+t$ matrices $\{\mathbf{B}_i\}_{i\in[k]}$, $\mathbf{C}_{x_1}$, $\mathbf{C}_{x_2}, \ldots, \mathbf{C}_{x_t}$.[3] 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 $K \in \{0,1\}^k$ 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

[3] 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 Sect. 3.3 for details.

$\{\mathbf{B}_i\}_{i\in[k]}, \mathbf{C}_{x_1}, \mathbf{C}_{x_2}, \ldots, \mathbf{C}_{x_t}$. 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 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 $\mathbf{R}_{\mathbf{A}_0}, \mathbf{R}_{\mathbf{A}_1}, \{\mathbf{R}_{\mathbf{B}_i}\}_{i\in[k]}, \mathbf{R}_{\mathbf{C}_0}, \mathbf{R}_{\mathbf{C}_1}$ from $\{1,-1\}^{m\times m}$, a PRF secret key $K = s_1 s_2 \ldots s_k \in \{0,1\}^k$ 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 $\mathbf{A}_{\mathsf{PRF},\mathsf{M}} = \mathbf{AR} + \mathsf{PRF}(K,\mathsf{M})\mathbf{G}$ 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 $\mathbf{F}_{\mathsf{M},1-b} = [\mathbf{A} \mid \mathbf{A}_{1-b} - \mathbf{A}_{\mathsf{PRF},\mathsf{M}}] = [\mathbf{A} \mid \mathbf{AR} + (1-2b)\mathbf{G}]$ 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 $\mathbf{F}_{\mathsf{id}^*,b} = [\mathbf{A} \mid \mathbf{AR}]$ for which the simulator cannot produce private key. Another ciphertext based on $\mathbf{F}_{\mathsf{id}^*,1-b} = [\mathbf{A} \mid \mathbf{AR} + (1-2b)\mathbf{G}]$ 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.

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 left-over hash lemma.

Lemma 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 $(\mathbf{A}, \mathbf{AR}, \mathbf{R}^\top \mathbf{w})$ 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], 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

Lattice Definitions

Definition 1. *Let a basis* $\mathbf{B} = [\mathbf{b}_1 | \ldots | \mathbf{b}_m] \in (\mathbb{R}^m)^m$ *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. *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* $\Lambda_q^{\mathbf{u}}(\mathbf{A}) = \{\mathbf{e} \in \mathbb{Z}^m : \mathbf{Ae} = \mathbf{u} \pmod q\}$.

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 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 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 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 $\rho_{1/s}(\Lambda^* \backslash \{\mathbf{0}\}) < \epsilon$.

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

Lemma 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 $D_{\mathbb{Z},\sqrt{(r\|\mathbf{r}\|)^2+\alpha^2}}$.

Lattice Sampling Algorithms. Our constructions make use of the "two-sided trapdoor" framework from [2,20] 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 $\mathbf{F} = [\mathbf{A} \mid \mathbf{B}]$. The algorithm outputs a vector $\mathbf{d} \in \mathbb{Z}^{m+m_1}$ in the set $\Lambda_q^{\mathbf{u}}(\mathbf{F})$.

Theorem 1 ([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 $\mathbf{F} = [\mathbf{A} \mid \mathbf{AR} + \mathbf{B}]$; the algorithm outputs a vector $\mathbf{d} \in \mathbb{Z}^{m+m_1}$ in the set $\Lambda_q^{\mathbf{u}}(\mathbf{F})$

Theorem 2 ([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 $D_{\Lambda_q^{\mathbf{u}}(\mathbf{F}),s}$.

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

Lemma 6 ([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 7 ([18], 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 $\|\mathbf{G}^{-1}(\mathbf{A})\| \le m$.

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 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 $LWE_{n,q,\chi}$ 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 $LWE_{n,q,\chi}$ problem as*

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

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).[4] 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 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*

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

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

We say the (t, ϵ_{SIS})-$SIS_{n,q,\beta,m}$ *assumption holds if no* t*-time algorithm* $\mathcal{A}$ *that has advantage at least* ϵ_{SIS} *in solving the* $SIS_{n,q,\beta,m}$ *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 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* $PRF : \{0,1\}^k \times \{0,1\}^t \to \{0,1\}^l$ *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*

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

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* $(t_{PRF}, \epsilon_{PRF})$*-secure if for all* t_{PRF}*-time adversaries* $\mathcal{A}$, $Adv_{PRF,\mathcal{A}}(\lambda) \le \epsilon_{PRF}$.

2.3 Key-Homomorphic Evaluation Algorithm

Recall the matrix key-homomorphic evaluation algorithm, which is developed by Gentry et al. [38], Boneh et al. [18] 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 deterministically computes $\mathbf{A}_C = \mathbf{AR}_C + C(x_1, \ldots, x_\ell)\mathbf{G} \in \mathbb{Z}_q^{n\times m}$ 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 $\mathbf{A}_u = \mathbf{AR}_u + x_u\mathbf{G}$ and $\mathbf{A}_v = \mathbf{AR}_v + x_v\mathbf{G}$ where x_u and x_v are input bits of u and v respectively, the evaluation algorithm computes

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

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. [47,53]) and lattice assumptions (e.g. [8,9]) 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 3 (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 8. *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 Eval_{BV} that takes as input C and $\{\mathbf{A}_i\}_{i \in [\ell]}$ and outputs a matrix $\mathbf{A}_C = \mathbf{A}\mathbf{R}_C + C(x_1, \ldots, x_\ell)\mathbf{G} = \mathsf{Eval}_{BV}(C, \mathbf{A}_1, \ldots, \mathbf{A}_\ell)$ 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 $x_1, \ldots, x_\ell$. Eval_{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* Eval_{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.*

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* $\|\mathbf{R}_C\|_2 \leq O(\ell^{2c} \cdot m^{3/2})$.

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 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, $\mathsf{Encrypt}$, and $\mathsf{Decrypt}$. 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 adaptive (full) security under chosen-plaintext attack ($\mathsf{IND\text{-}ID\text{-}CPA}$) of IBE system. The $\mathsf{IND\text{-}ID\text{-}CPA}$ 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 requests keys for any identity id of its choice. $\mathcal{B}$ responds with the corresponding private key $\mathsf{Sk}_{\mathsf{id}}$ by running algorithm KeyGen.

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. $\mathcal{A}$ continues to make key quires for any identity $\mathsf{id} \neq \mathsf{id}^*$.

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

We refer to such an adversary $\mathcal{A}$ as an $\mathsf{IND\text{-}ID\text{-}CPA}$ 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 8. *For a security parameter λ, let $t = t(\lambda)$, $q_{id} = q_{id}(\lambda)$, and $\epsilon = \epsilon(\lambda)$. We say that an IBE system $\mathcal{E}$ is (t, q_{id}, ϵ)-IND-ID-CPA secure if for any t-time IND-ID-CPA adversary $\mathcal{A}$ that makes at most q_{id} private key queries, we have $\mathsf{Adv}_{\mathcal{E},\mathcal{A}}(\lambda) \leq \epsilon$.*

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 $\mathbf{A}_{C_{\mathsf{PRF}},\mathsf{M}} = \mathsf{Eval}_{\mathsf{BV}}(C_{\mathsf{PRF}}, \{\mathbf{B}_i\}_{i\in[k]}, \mathbf{C}_{m_1}, \mathbf{C}_{m_2}, \ldots, \mathbf{C}_{m_t}) \in \mathbb{Z}_q^{n\times m}$.[5]
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 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, 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 8 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 $q = O(16^d \cdot m^4) \cdot (\omega(\sqrt{\log m}))^2$.

Particularly, if we choose PRF from the well-known efficient and provably secure candidates of PRFs like the ones from [8,9,31,47,53] 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.

[5] 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 Sect. 3.3.

3.3 Security of the Signature Scheme

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

Theorem 4. *Let λ be a security parameter. The parameters n, m, and q are chosen as the Sect. 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)-EUF-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 $\big[\mathbf{A} \mid \mathbf{A}_{1-b} - \mathbf{A}_{C_{\mathsf{PRF}},\mathsf{M}^*}\big]\,\mathbf{d}^* = \mathbf{0} \pmod q$, $\mathcal{B}$ aborts. Otherwise, we have $\big[\mathbf{A} \mid \mathbf{A}_b - \mathbf{A}_{C_{\mathsf{PRF}},\mathsf{M}^*}\big]\,\mathbf{d}^* = \mathbf{0} \pmod q$. 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 $\|\mathbf{e}\| \leq \beta$ 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 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 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 $\mathsf{M} \neq \mathsf{M}'$ such that $\mathbf{A}_{C_{\mathsf{PRF}},\mathsf{M}} = \mathbf{A}_{C_{\mathsf{PRF}},\mathsf{M}'}$. Assume an efficient adversary finds $\mathsf{M} \neq \mathsf{M}'$ 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 $\mathsf{PRF}(K,\mathsf{M}) \neq \mathsf{PRF}(K,\mathsf{M}')$, which will happen essentially 1/2 probability if PRF is secure, we have $\mathbf{R}_{C_{\mathsf{PRF}},\mathsf{M}} \neq \mathbf{R}_{C_{\mathsf{PRF}},\mathsf{M}'}$ 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 6 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 $\bar{\mathbf{d}} \neq \mathbf{0}$ and $\|\bar{\mathbf{d}}\| \leq s'\sqrt{m}$ for some Gaussian parameter $s' \geq \sqrt{5}\cdot\omega(\sqrt{\log m})$. 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, 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 $\epsilon_{\mathsf{SIS}} \geq \epsilon/2 - \epsilon_{\mathsf{PRF}} - \mathsf{negl}(\lambda)$ 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 4, $\mathbf{d}_1, \mathbf{d}_2 \leq s\sqrt{m}$. By Lemma 8, we have $\|\mathbf{e}\| \leq \|\mathbf{d}_1\| + \|\mathbf{R}\|_2 \cdot \|\mathbf{d}_2\| \leq O(4^d \cdot m^{3/2}) \cdot s\sqrt{m}$. Let $\beta \geq O(4^d \cdot m^{3/2}) \cdot s\sqrt{m}$ is sufficient.

It remains to show that $\mathbf{e} = \mathbf{d}_1 + \mathbf{R}\cdot\mathbf{d}_2 \neq \mathbf{0}$. Suppose $\mathbf{d}_2 \neq \mathbf{0}$, we have $\mathbf{e} \neq \mathbf{0}$ since $\mathbf{d} \neq \mathbf{0}$. On the other hand, we have $\mathbf{d}_2 = (d_1, \ldots, d_m)^\top \neq \mathbf{0}$ 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

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

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 [20] 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 Scheme with Tight Security

4.1 Construction with CPA Security

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

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 $\mathsf{id}{=}x_1 x_2 \ldots x_t \in \{0,1\}^t$, 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 $\mathsf{id} = x_1 x_2 \ldots x_t \in \{0,1\}^t$:

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}.[6]

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

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 $(c_{1,0}, \mathbf{c}_{1,1})$[7]. 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 4. To ensure correctness of decryption, we need

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

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

[7] 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.

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 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 real scheme and $\mathsf{SampleRight}$ in the simulation algorithm $\mathsf{Sim.KeyGen}$ (see section) 4.4 have the same output distribution per Theorem 2, 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 Lemmas 10 and 16), 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 [22,54,55] 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 make 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 [8,9]) 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. [18,25,37], and predicate encryption for circuits [41].

4.4 Proof of Security

The security of our IBE scheme with respect to the Definition 8 can be stated by the following theorem.

Theorem 5. *Let λ be a security parameter. The parameters n, q are chosen as the Sect. 4.3. Let χ be the distribution $D_{\mathbb{Z}^m,\sqrt{n}}$. If the $(t_{\mathsf{LWE}}, \epsilon_{\mathsf{LWE}})$-$\mathsf{LWE}_{n,q,\chi}$ assumption holds and the PRF used in the IBE scheme is $(t_{\mathsf{PRF}}, \epsilon_{\mathsf{PRF}})$-secure, then the IBE scheme is (t, q_{id}, ϵ)-IND-ID-CPA secure such that $\epsilon \leq 2(\epsilon_{\mathsf{PRF}} + \epsilon_{\mathsf{LWE}}) + \mathsf{negl}(\lambda)$ for some negligible function $\mathsf{negl}(\lambda)$, and $\max(t_{\mathsf{PRF}}, t_{\mathsf{LWE}}) \leq t + O(q_{id} \cdot (T_S + T_E))$ where T_S is the maximum running time of SampleRight and T_E is the maximum running time of $\mathsf{Eval}_{\mathsf{BV}}$ 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 neighbouring 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.

Sim.Setup(1^λ). The algorithm does the following:

1. Select matrix $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n \times m}$.
2. Select $k + 4$ random 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 $\{1, -1\}^{m \times m}$.
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 $K = s_1 s_2 \ldots s_k \xleftarrow{\$} \{0,1\}^k$.
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 $\mathsf{Pub} = \big(\mathbf{A}, \{\mathbf{A}_0, \mathbf{A}_1\}, \{\mathbf{B}_i\}_{i\in[k]}, \{\mathbf{C}_0, \mathbf{C}_1\}, \mathbf{u}, \mathsf{PRF}, C_{\mathsf{PRF}}\big)$

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

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

3. Run $\mathsf{SampleRight}$ 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

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

and

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

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 $\mathbf{z} = (z_1, z_2, \dots, z_m) \in \mathbb{Z}^m$ with $z_i \leftarrow D_{\mathbb{Z},\sigma_{1,i}}$ for the sufficiently large Gaussian parameter $\sigma_{1,i} = \sqrt{\sigma^2 - 2(\|\mathbf{r}_i\| \cdot \sigma_{\mathsf{LWE}})^2}$.[8] 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:

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

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

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

Now we define a series of games and prove that the neighbouring 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.

Game 7. This game is the same as **Game 6** except that it runs Sim.Setup and 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 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 $|\Pr[S_i] - \frac{1}{2}|$. The following lemmas are used to prove Theorem 5. We refer to the full version of this paper ([21]) for the proofs of these lemmas.

Lemma 9. Game 1 *and* **Game 0** *are statistically indistinguishable, so* $|\Pr[S_0] - \Pr[S_1]| \leq \mathsf{negl}(\lambda)$ *for some negligible function* $\mathsf{negl}(\lambda)$.

Lemma 10. Game 2 *and* **Game 1** *are statistically indistinguishable, so* $|\Pr[S_1] - \Pr[S_2]| \leq \mathsf{negl}(\lambda)$ *for some negligible function* $\mathsf{negl}(\lambda)$.

Lemma 11. *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* $|\Pr[S_2] - \Pr[S_3]| \leq \epsilon_{LWE}$.

Lemma 12. $|\Pr[S_3] - \Pr[S_4]| = 0$.

Lemma 13. Game 5 *and* **Game 4** *are statistically indistinguishable, so* $|\Pr[S_4] - \Pr[S_5]| \leq \mathsf{negl}(\lambda)$ *for some negligible function* $\mathsf{negl}(\lambda)$.

Lemma 14. *If the PRF* PRF *is* (t, ϵ_{PRF})*-secure, then* $|\Pr[S_5] - \Pr[S_6]| \leq 2\epsilon_{PRF}$.

Lemma 15. Game 7 *and* **Game 6** *are statistically indistinguishable, so* $|\Pr[S_6] - \Pr[S_7]| \leq \mathsf{negl}(\lambda)$ *for some negligible function* $\mathsf{negl}(\lambda)$.

Lemma 16. Game 8 *and* **Game 7** *are statistically indistinguishable, so* $|\Pr[S_7] - \Pr[S_8]| \leq \mathsf{negl}(\lambda)$ *for some negligible function* $\mathsf{negl}(\lambda)$.

Lemma 17. *If* (t, ϵ_{LWE})*-*$\mathsf{LWE}_{n,q,\chi}$ *assumption holds where* χ *stands for the distribution* $D_{\mathbb{Z},\sigma_{LWE}}$ *reduced modulo* q*, then* $|\Pr[S_8] - \Pr[S_9]| \leq \epsilon_{LWE}$.

Now we prove the Theorem 5 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 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, $\max(t_{\mathsf{LWE}}, t_{\mathsf{PRF}}) \leq t + O(q_{\mathsf{id}} \cdot (T_S + T_E))$. □

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 an efficient PRF from LWE assumption with polynomial modulus.

Acknowledgements. We would like to thank Jacob Alperin-Sheriff and Josef Pierpzyk as well as the anonymous reviewers for useful comments.

References

1. Abe, M., David, B., Kohlweiss, M., Nishimaki, R., Ohkubo, M.: Tagged one-time signatures: tight security and optimal tag size. In: Kurosawa, K., Hanaoka, G. (eds.) PKC 2013. LNCS, vol. 7778, pp. 312–331. Springer, Heidelberg (2013). doi:10.1007/978-3-642-36362-7_20
2. Agrawal, S., Boneh, D., Boyen, X.: Efficient lattice (H)IBE in the standard model. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 553–572. Springer, Heidelberg (2010). doi:10.1007/978-3-642-13190-5_28
3. Ajtai, M.: Generating hard instances of lattice problems (extended abstract). In: STOC 1996, pp. 99–108. ACM (1996)
4. Alperin-Sheriff, J.: Short signatures with short public keys from homomorphic trapdoor functions. In: Katz, J. (ed.) PKC 2015. LNCS, vol. 9020, pp. 236–255. Springer, Heidelberg (2015). doi:10.1007/978-3-662-46447-2_11
5. Apon, D., Fan, X., Liu, F.H.: Fully-secure lattice-based IBE as compact as PKE. Cryptology ePrint Archive, Report 2016/125 (2016)
6. Attrapadung, N., Hanaoka, G., Yamada, S.: A framework for identity-based encryption with almost tight security. In: Iwata, T., Cheon, J.H. (eds.) ASIACRYPT 2015. LNCS, vol. 9452, pp. 521–549. Springer, Heidelberg (2015). doi:10.1007/978-3-662-48797-6_22
7. Bai, S., Langlois, A., Lepoint, T., Stehlé, D., Steinfeld, R.: Improved security proofs in lattice-based cryptography: using the rényi divergence rather than the statistical distance. In: Iwata, T., Cheon, J.H. (eds.) ASIACRYPT 2015. LNCS, vol. 9452, pp. 3–24. Springer, Heidelberg (2015). doi:10.1007/978-3-662-48797-6_1
8. Banerjee, A., Peikert, C.: New and improved key-homomorphic pseudorandom functions. In: Garay, J.A., Gennaro, R. (eds.) CRYPTO 2014. LNCS, vol. 8616, pp. 353–370. Springer, Heidelberg (2014). doi:10.1007/978-3-662-44371-2_20
9. Banerjee, A., Peikert, C., Rosen, A.: Pseudorandom functions and lattices. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 719–737. Springer, Heidelberg (2012). doi:10.1007/978-3-642-29011-4_42
10. Bellare, M., Rogaway, P.: Random oracles are practical: A paradigm for designing efficient protocols. In: CCS 1993, pp. 62–73. ACM (1993)
11. Blazy, O., Kakvi, S.A., Kiltz, E., Pan, J.: Tightly-secure signatures from chameleon hash functions. In: Katz, J. (ed.) PKC 2015. LNCS, vol. 9020, pp. 256–279. Springer, Heidelberg (2015). doi:10.1007/978-3-662-46447-2_12
12. Blazy, O., Kiltz, E., Pan, J.: (Hierarchical) identity-based encryption from affine message authentication. In: Garay, J.A., Gennaro, R. (eds.) CRYPTO 2014. LNCS, vol. 8616, pp. 408–425. Springer, Heidelberg (2014). doi:10.1007/978-3-662-44371-2_23

13. Böhl, F., Hofheinz, D., Jager, T., Koch, J., Seo, J.H., Striecks, C.: Practical signatures from standard assumptions. In: Johansson, T., Nguyen, P.Q. (eds.) EUROCRYPT 2013. LNCS, vol. 7881, pp. 461–485. Springer, Heidelberg (2013). doi:10.1007/978-3-642-38348-9_28
14. Boneh, D., Boyen, X.: Efficient selective-ID secure identity-based encryption without random oracles. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 223–238. Springer, Heidelberg (2004). doi:10.1007/978-3-540-24676-3_14
15. Boneh, D., Boyen, X.: Secure identity based encryption without random oracles. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 443–459. Springer, Heidelberg (2004). doi:10.1007/978-3-540-28628-8_27
16. Boneh, D., Boyen, X.: Short signatures without random oracles. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 56–73. Springer, Heidelberg (2004). doi:10.1007/978-3-540-24676-3_4
17. Boneh, D., Franklin, M.: Identity-based encryption from the weil pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213–229. Springer, Heidelberg (2001). doi:10.1007/3-540-44647-8_13
18. Boneh, D., Gentry, C., Gorbunov, S., Halevi, S., Nikolaenko, V., Segev, G., Vaikuntanathan, V., Vinayagamurthy, D.: Fully key-homomorphic encryption, arithmetic circuit abe and compact garbled circuits. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 533–556. Springer, Heidelberg (2014). doi:10.1007/978-3-642-55220-5_30
19. Boneh, D., Lynn, B., Shacham, H.: Short signatures from the weil pairing. J. Cryptology **17**(4), 297–319 (2004)
20. Boyen, X.: Lattice mixing and vanishing trapdoors: a framework for fully secure short signatures and more. In: Nguyen, P.Q., Pointcheval, D. (eds.) PKC 2010. LNCS, vol. 6056, pp. 499–517. Springer, Heidelberg (2010). doi:10.1007/978-3-642-13013-7_29
21. Boyen, X., Li, Q.: Towards tightly secure short signature and ibe. Cryptology ePrint Archive, Report 2016/498 (2016)
22. Brakerski, Z., Langlois, A., Peikert, C., Regev, O., Stehlé, D.: Classical hardness of learning with errors. In: STOC 13, pp. 575–584. ACM (2013)
23. Brakerski, Z., Vaikuntanathan, V.: Efficient fully homomorphic encryption from (standard) LWE. In: FOCS 2011. pp. 97–106. IEEE (2011)
24. Brakerski, Z., Vaikuntanathan, V.: Lattice-based FHE as secure as PKE. In: ITCS 2014, pp. 1–12. ACM (2014)
25. Brakerski, Z., Vaikuntanathan, V.: Circuit-ABE from LWE: Unbounded attributes and semi-adaptive security. Cryptology ePrint Archive, Report 2016/118 (2016)
26. Camenisch, J., Lysyanskaya, A.: Signature schemes and anonymous credentials from bilinear maps. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 56–72. Springer, Heidelberg (2004). doi:10.1007/978-3-540-28628-8_4
27. Canetti, R., Halevi, S., Katz, J.: A forward-secure public-key encryption scheme. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 255–271. Springer, Heidelberg (2003). doi:10.1007/3-540-39200-9_16
28. Cash, D., Hofheinz, D., Kiltz, E., Peikert, C.: Bonsai trees, or how to delegate a lattice basis. J. Cryptology **25**(4), 601–639 (2012)
29. Chen, J., Wee, H.: Fully, (almost) tightly secure IBE and dual system groups. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013. LNCS, vol. 8043, pp. 435–460. Springer, Heidelberg (2013). doi:10.1007/978-3-642-40084-1_25
30. Cramer, R., Shoup, V.: Signature schemes based on the strong RSA assumption. ACM Trans. Inf. Syst. Secur. **3**(3), 161–185 (2000)

31. Döttling, N., Schröder, D.: Efficient pseudorandom functions via on-the-fly adaptation. In: Gennaro, R., Robshaw, M. (eds.) CRYPTO 2015. LNCS, vol. 9215, pp. 329–350. Springer, Heidelberg (2015). doi:10.1007/978-3-662-47989-6_16
32. Ducas, L., Micciancio, D.: Improved short lattice signatures in the standard model. In: Garay, J.A., Gennaro, R. (eds.) CRYPTO 2014. LNCS, vol. 8616, pp. 335–352. Springer, Heidelberg (2014). doi:10.1007/978-3-662-44371-2_19
33. Fischlin, M.: The cramer-shoup strong-rsa signature scheme revisited. In: Desmedt, Y.G. (ed.) PKC 2003. LNCS, vol. 2567, pp. 116–129. Springer, Heidelberg (2003). doi:10.1007/3-540-36288-6_9
34. Gennaro, R., Halevi, S., Rabin, T.: Secure hash-and-sign signatures without the random oracle. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 123–139. Springer, Heidelberg (1999). doi:10.1007/3-540-48910-X_9
35. Gentry, C.: Practical identity-based encryption without random oracles. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 445–464. Springer, Heidelberg (2006). doi:10.1007/11761679_27
36. Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: STOC 2008, pp. 197–206. ACM (2008)
37. Gorbunov, S., Vaikuntanathan, V., Wee, H.: Attribute-based encryption for circuits. In: STOC 2013, pp. 545–554. ACM (2013)
38. Gentry, C., Sahai, A., Waters, B.: Homomorphic encryption from learning with errors: conceptually-simpler, asymptotically-faster, attribute-based. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013. LNCS, vol. 8042, pp. 75–92. Springer, Heidelberg (2013). doi:10.1007/978-3-642-40041-4_5
39. Goh, E.-J., Jarecki, S.: A signature scheme as secure as the diffie-hellman problem. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 401–415. Springer, Heidelberg (2003). doi:10.1007/3-540-39200-9_25
40. Goldreich, O., Goldwasser, S., Micali, S.: How to construct random functions. J. ACM **33**(4), 792–807 (1986)
41. Gorbunov, S., Vaikuntanathan, V., Wee, H.: Predicate encryption for circuits from LWE. In: Gennaro, R., Robshaw, M. (eds.) CRYPTO 2015. LNCS, vol. 9216, pp. 503–523. Springer, Heidelberg (2015). doi:10.1007/978-3-662-48000-7_25
42. Gorbunov, S., Vinayagamurthy, D.: Riding on asymmetry: efficient ABE for branching programs. In: Iwata, T., Cheon, J.H. (eds.) ASIACRYPT 2015. LNCS, vol. 9452, pp. 550–574. Springer, Heidelberg (2015). doi:10.1007/978-3-662-48797-6_23
43. Hofheinz, D., Jager, T.: Tightly secure signatures and public-key encryption. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 590–607. Springer, Heidelberg (2012). doi:10.1007/978-3-642-32009-5_35
44. Hofheinz, D., Koch, J., Striecks, C.: Identity-based encryption with (almost) tight security in the multi-instance, multi-ciphertext setting. In: Katz, J. (ed.) PKC 2015. LNCS, vol. 9020, pp. 799–822. Springer, Heidelberg (2015). doi:10.1007/978-3-662-46447-2_36
45. Hohenberger, S., Waters, B.: Realizing hash-and-sign signatures under standard assumptions. In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 333–350. Springer, Heidelberg (2009). doi:10.1007/978-3-642-01001-9_19
46. Hohenberger, S., Waters, B.: Short and stateless signatures from the RSA assumption. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 654–670. Springer, Heidelberg (2009). doi:10.1007/978-3-642-03356-8_38
47. Jager, T.: Tightly-secure pseudorandom functions via work factor partitioning. Cryptology ePrint Archive, Report 2016/121 (2016)

48. Katz, J., Wang, N.: Efficiency improvements for signature schemes with tight security reductions. In: CCS 2003, pp. 155–164. CCS 2003, ACM (2003)
49. Lewko, A., Waters, B.: New proof methods for attribute-based encryption: achieving full security through selective techniques. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 180–198. Springer, Heidelberg (2012). doi:10.1007/978-3-642-32009-5_12
50. Lyubashevsky, V.: Lattice signatures without trapdoors. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 738–755. Springer, Heidelberg (2012). doi:10.1007/978-3-642-29011-4_43
51. Micciancio, D., Peikert, C.: Trapdoors for lattices: simpler, tighter, faster, smaller. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 700–718. Springer, Heidelberg (2012). doi:10.1007/978-3-642-29011-4_41
52. Micciancio, D., Regev, O.: Worst-case to average-case reductions based on gaussian measures. SIAM J. Comput. **37**(1), 267–302 (2007)
53. Naor, M., Reingold, O.: Number-theoretic constructions of efficient pseudo-random functions. J. ACM **51**(2), 231–262 (2004)
54. Peikert, C.: Public-key cryptosystems from the worst-case shortest vector problem: extended abstract. In: STOC 2009, pp. 333–342. ACM (2009)
55. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. In: STOC 2005, pp. 84–93. ACM (2005)
56. Waters, B.: Efficient identity-based encryption without random oracles. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 114–127. Springer, Heidelberg (2005). doi:10.1007/11426639_7
57. Waters, B.: Dual system encryption: realizing fully secure ibe and hibe under simple assumptions. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 619–636. Springer, Heidelberg (2009). doi:10.1007/978-3-642-03356-8_36