Partitioning via Non-Linear Polynomial Functions: More Compact IBEs from Ideal Lattices and Bilinear Maps

Shuichi Katsumata[1,2] and Shota Yamada[2]

[1] The University of Tokyo,
shuichi_katsumata@it.k.u-tokyo.ac.jp,
[2] National Institute of Advanced Industrial Science and Technology (AIST).
yamada-shota@aist.go.jp.

Abstract. In this paper, we present new adaptively secure identity-based encryption (IBE) schemes. One of the distinguishing properties of the schemes is that it achieves shorter public parameters than previous schemes. Both of our schemes follow the general framework presented in the recent IBE scheme of Yamada (Eurocrypt 2016), employed with novel techniques tailored to meet the underlying algebraic structure to overcome the difficulties arising in our specific setting. Specifically, we obtain the following:

- Our first scheme is proven secure under the ring learning with errors (RLWE) assumption and achieves the best asymptotic space efficiency among existing schemes from the same assumption. The main technical contribution is in our new security proof that exploits the ring structure in a crucial way. Our technique allows us to greatly weaken the underlying hardness assumption (e.g., we assume the hardness of RLWE with a fixed polynomial approximation factor whereas Yamada's scheme requires a super-polynomial approximation factor) while improving the overall efficiency.
- Our second IBE scheme is constructed on bilinear maps and is secure under the 3-computational bilinear Diffie-Hellman exponent assumption. This is the first IBE scheme based on the hardness of a computational/search problem, rather than a decisional problem such as DDH and DLIN on bilinear maps with sub-linear public parameter size.

1 Introduction

Background. Identity-based encryption (IBE) is a generalization of public key encryption (PKE) where the public key of a user can be any arbitrary string such as an e-mail address. The concept of IBE was first proposed by Shamir [Sha85] in 1984, but it took nearly two decades for the first realizations of IBE [SOK00,BF01,Coc01] to appear. Since then, the construction of IBE has been one of the central topics in cryptography. Nowadays, we have constructions of IBEs from assumptions on bilinear maps [BF01,BB04a,BB04b,Wat05,Gen06,Wat09],

the quadratic residue assumption [Coc01,BGH07], and from the learning with error (LWE) assumption [GPV08,CHKP10,ABB10] whose hardness is implied by the worst case reductions to certain lattice problems [Reg05].

One of the most standard security definitions for IBE is the adaptive security, or often called full security. While it is not quite hard to obtain the adaptive security for an IBE in the random oracle model [BF01,Coc01,GPV08], the realization in the standard model is much harder. Roughly speaking, currently there are two general techniques in achieving adaptive security in the standard model: the partitioning technique [BB04b,Wat05] and the dual system encryption methodology [Wat09,LW10]. The latter is very attractive, because it allows us to construct very efficient IBE schemes [CW13,JR13] and even more advanced cryptosystems such as attribute-based encryptions [LOS+10] with adaptive security. However, it inherently relies on *decisional assumptions* on bilinear maps (e.g., SXDH and DLIN) and cannot be extended to the proofs based on *computational assumptions* on bilinear maps (e.g., computational bilinear Diffie-Hellman (CBDH) assumption) or assumptions on lattices. On the other hand, the application of the former technique is wider. We can construct adaptively secure IBE from the CBDH assumption (by the straightforward combination of the Goldreich-Levin bit [GL89] and Waters IBE [Wat05]) and from the LWE assumption [CHKP10,ABB10,Boy10]. However, IBE schemes constructed from the former approach typically requires larger parameters due to the use of the Waters' hash [Wat05] or the admissible hash [BB04b,CHKP10].

Very recently, Yamada [Yam16] constructed IBE schemes from lattices based on the partitioning technique with novel ideas that are different from the Waters' hash or the admissible hash. His schemes achieve asymptotically shorter public parameters than previous works. One of the drawbacks of the schemes is that they require super-polynomial size modulus for LWE. As a result, their ciphertexts are longer than those of previous works by a rather large super-constant factor. In addition, they have to assume the hardness of the LWE problem for *all polynomial* (i.e., $O(n^c)$ for *all* $c \in \mathbb{N}$) or the more aggressive *super-polynomial* approximation factor. Though their assumption is plausible, it is much stronger than those used in the previous works where the hardness of the LWE problem for some *fixed polynomial* approximation factor (i.e., $O(n^c)$ for *some* $c \in \mathbb{N}$) is assumed. Furthermore, since he used fully homomorphic computations of trapdoors [BGG+14], a technique unique to the lattice setting, it is a highly non-trivial task to construct analogous schemes in other settings such as bilinear maps.

Our Contribution. In this paper, we focus on the constructions of adaptively secure IBE in these settings where dual system encryption methodology is unavailable. In particular, we propose IBE schemes with shorter public parameters from ring/ideal lattices and from a certain computational assumption (rather than a decisional assumption) on bilinear groups, by extending and adding twists to the techniques of [Yam16]. Specifically, we obtain the following results. See Table 1 and 2 for the overview.

– We propose an anonymous and adaptively secure IBE scheme from the ring LWE (RLWE) assumption with *fixed polynomial* approximation factors, which is further reduced to certain worst case problems on ideal lattices. Note that simply instantiating Yamada's scheme using ideal lattices[3] will still require the RLWE assumption for *all polynomial* approximation factors, which is a much stronger assumption than what we use. As for the efficiency, the size of the public parameters, private keys, and ciphertexts in our scheme are $O(n\kappa^{1/d}\log n)$, $O(n\log n)$, and $O(n\log n)$, respectively. Here, n is the dimension of the ring elements, κ is the length of the identities, and d is a flexible constant that can be set arbitrary, but will affect the reduction cost exponentially. We note that all of them achieve the best efficiency among the other adaptively secure IBE from the RLWE assumption in an asymptotic sense. Compared to the ring version of Yamada's scheme, we managed to reduce the poly-logarithmic factors contained in the public parameters, private keys, and ciphertexts.
– We propose a (non anonymous and) adaptively secure IBE scheme from the 3-computational bilinear Diffie-Hellman exponent (3-CBDHE) assumption. The 3-CBDHE assumption is a weaker variant of the n-decisional bilinear Diffie-Hellman exponent (n-DBDHE) assumption [BBG05,BGW05,BH08]. The former seems to be much a weaker assumption than the latter in two aspects. First, the former is a computational assumption whereas the latter is a decisional assumption. Second, the former is not a parameterized assumption, in the sense that the size of the problem instance only depends on the security parameter. As for the efficiency, the public parameters, private keys, and ciphertexts in our scheme require $O(\sqrt{\kappa})$ group elements. Here, κ is the length of the identities. This is the first adaptively secure IBE scheme from a computational assumption on bilinear groups with public parameters consisting of sub-linear number of group elements in the length of the identities. However, we note that the sizes of the ciphertexts and private keys of our scheme are larger than the previous schemes.

We emphasize that our result for the lattice based construction cannot be obtained through the simple switch to the ring setting in Yamada's scheme. Their proof will still require a super-polynomial-size modulus to work, whereas our new technique allows for a polynomial-size modulus. In addition, the security proof of our scheme requires new ideas that did not appear in [Yam16]. It exploits the commutative properties of the underlying ring elements in an essential way, involves a more generalized partitioning argument, and a careful analysis of the Gaussian error. Refer Sec. 2 for the technical overview. We note that the public parameter of our second scheme could be further reduced to $O(\kappa^{1/d})$ assuming the $d+1$-CBDHE assumption. However, it would come at the cost of even longer ciphertexts and complicated description of the scheme. This is beyond the scope of our work. We finally remark that the reduction costs for both of our schemes

[3] Note that he does not describe nor mention the ring variant of the scheme. However, we can convert his scheme into a ring variant in a straightforward manner as is the case in most previous works [CHKP10,ABB10,Boy10].

are inadmissible as was in the case of [Yam16]. In fact, the reduction loss for the first scheme is worse than [Yam16]. Improving them is left as an open problem.

Related Works. One way to reduce the size of the public parameters in Waters' hash and its analogue is to use Naccache's approach [Nac07,SRB12]. However, with this approach, we are only allowed to reduce the size of public parameters up to logarithmic factor. Ducas et al. [DLP14] constructed efficient IBE over NTRU lattices in the random oracle model. Gentry [Gen06] proposed adaptively secure IBE with compact parameters from a parameterized (or q-type) assumption on bilinear maps. Galindo [Gal10] and Chen et al. [CCZ11] proposed selectively secure CCA-secure IBE schemes from the CBDH assumption.

Note on Recent Works. Here, we mention two important recent related works.

Apon et al. [AFL16] proposed an adaptively secure IBE scheme from lattices whose parameters are very compact, using collision resistant hash function with output-length $\kappa = \omega(\log \lambda)$. Here, λ is the security parameter. While their scheme is more efficient than our scheme, we clarify that they implicitly assume exponential security on the collision resistant hash function, which is a stronger assumption than what we use. To demonstrate this, let us set $\kappa = \log^2 \lambda$. If there is no better attack than the birthday attack against the hash function, no PPT adversary can find a collision with more than negligible probability. On the other hand, the existence of even a sub-exponential time attack would compromise the security of the IBE. For example, assume that there exists an attack that finds a collision in time $2^{\sqrt{\kappa}}$. Then, the collision for the hash can be found in linear time in λ, since $2^{\sqrt{\kappa}} = 2^{\log \lambda} = \lambda$.

In their very recent work, Zhang et al. [ZCZ16] constructed an IBE scheme with poly-logarithmic public parameters. While their scheme achieves better asymptotic space efficiency than our scheme, their scheme is Q-bounded, in the sense that the security of the scheme is not guaranteed any more if the adversary obtains more than Q private keys. This restriction cannot be removed by just making Q super-polynomial, because the running time of the encryption algorithm in their scheme is at least linear in Q. We note that our scheme is secure against an unbounded collusion.

2 Overview of Our Techniques

2.1 Construction from Ring and Ideal Lattices

The Yamada IBE. We briefly review the Yamada IBE [Yam16], for our proposed IBE scheme follows the framework of theirs and overcomes some of the major problems posed by their construction. Their construction follows the general framework of constructing lattice-based IBE schemes that associates to each identity ID the matrix $[\mathbf{A}|\mathsf{H}(\mathsf{ID})] \in \mathbb{Z}_q^{n \times 2m}$. In previous IBE constructions [ABB10,CHKP10], the function $\mathsf{H}(\mathsf{ID})$ was computed by using the rather long κ public matrices $\{\mathbf{B}_i\}_{i \in [\kappa]}$, where $\kappa = O(n)$ is the length of the identities. The main technical contribution of the Yamada IBE was in reducing the size of the public matrices to $\kappa^{1/d}$ for any constant d and hence reducing the size of the

public parameters by incorporating a primitive called fully homomorphic trapdoor functions. Hereafter, we consider the case $d = 2$ for simplicity. In detail, they used an injective map $S : \{0,1\}^\kappa \to 2^{[\ell]\times[\ell]}$ that maps an identity to a subset of the set $[\ell] \times [\ell]$ where $\ell = \lceil \kappa^{1/2} \rceil$, and computed the function $\mathsf{H}(\mathsf{ID})$ as

$$\mathsf{H}(\mathsf{ID}) = \mathbf{B}_0 + \sum_{(i,j)\in S(\mathsf{ID})} \mathbf{B}_{1,i} \cdot \mathbf{G}^{-1}(\mathbf{B}_{2,j}) \tag{1}$$

where the number of public matrices $\mathbf{B}_0, \{\mathbf{B}_{i,j}\}_{(i,j)\in[2]\times[\ell]}$ are now reduced to $O(\kappa^{1/2})$. Here, $\mathbf{G}$ is a special gadget matrix whose trapdoor is publicly known [MP12] and $\mathbf{G}^{-1}$ is viewed as a deterministic function rather than a matrix, that maps a matrix $\mathbf{V} \in \mathbb{Z}_q^{n\times m}$ to a matrix $\mathbf{U} \in \{0,1\}^{m\times m}$ such that $\mathbf{G} \cdot \mathbf{U} = \mathbf{V} \mod q$.

During the security proof, the reduction algorithm first prepares random integers $y_0, \{y_{i,j}\}_{(i,j)\in[2]\times[\ell]} \in \mathbb{Z}_q$ from certain domains whose size grows linear in the number of key extraction query Q of the adversary. Then after sampling $\mathbf{R}_0, \{\mathbf{R}_{i,j}\}_{i\in[2],j\in[\ell]} \in \mathbb{Z}^{m\times m}$ with small spectral norm, the reduction algorithm prepares the public parameters as

$$\mathbf{B}_0 = \mathbf{A}\mathbf{R}_0 + y_0\mathbf{G}, \quad \mathbf{B}_{i,j} = \mathbf{A}\mathbf{R}_{i,j} + y_{i,j}\mathbf{G}$$

for $(i,j) \in [2]\times[\ell]$. Then during the security reduction the hash value for identity ID Eq.(1) is computed as

$$\begin{aligned}
\mathsf{H}(\mathsf{ID}) &= (\mathbf{A}\mathbf{R}_0 + y_0\mathbf{G}) + \sum_{(i,j)\in S(\mathsf{ID})} (\mathbf{A}\mathbf{R}_{1,i} + y_{1,i}\mathbf{G}) \cdot \mathbf{G}^{-1}(\mathbf{B}_{2,j}) \\
&= (\mathbf{A}\mathbf{R}_0 + y_0\mathbf{G}) + \sum_{(i,j)\in S(\mathsf{ID})} (\mathbf{A}\mathbf{R}_{1,i}\mathbf{G}^{-1}(\mathbf{B}_{2,j}) + y_{1,i}\mathbf{B}_{2,j}) \\
&= (\mathbf{A}\mathbf{R}_0 + y_0\mathbf{G}) + \sum_{(i,j)\in S(\mathsf{ID})} \big(\mathbf{A}\mathbf{R}_{1,i}\mathbf{G}^{-1}(\mathbf{B}_{2,j}) + y_{1,i}(\mathbf{A}\mathbf{R}_{2,j} + y_{2,j}\mathbf{G})\big) \\
&= (\mathbf{A}\mathbf{R}_0 + y_0\mathbf{G}) + \sum_{(i,j)\in S(\mathsf{ID})} \big(\mathbf{A}\mathbf{R}_{1,i}\mathbf{G}^{-1}(\mathbf{B}_{2,j}) + \mathbf{A}(y_{1,i}\mathbf{R}_{2,j}) + y_{1,i}y_{2,j}\mathbf{G}\big) \\
&= \mathbf{A}\underbrace{\left(\mathbf{R}_0 + \sum_{(i,j)\in S(\mathsf{ID})} \big(\mathbf{R}_{1,i}\mathbf{G}^{-1}(\mathbf{B}_{2,j}) + y_{1,i}\mathbf{R}_{2,j}\big)\right)}_{:=\mathbf{R}_{\mathsf{ID}},\text{ which is ``small''}} + \underbrace{\left(y_0 + \sum_{(i,j)\in S(\mathsf{ID})} y_{1,i}y_{2,j}\right)}_{:=\mathsf{F}_{\mathbf{y}}(\mathsf{ID})} \cdot \mathbf{G} \\
&= \mathbf{A}\mathbf{R}_{\mathsf{ID}} + \mathsf{F}_{\mathbf{y}}(\mathsf{ID})\mathbf{G}.
\end{aligned} \tag{2}$$

Observe that we implicitly relied on the fact that $\mathbf{A}$ and $y_{1,i}$ commutes. Therefore, the reduction algorithm is able to sample a secret key for ID using the trapdoor of $\mathbf{G}$ if and only if $\mathsf{F}_{\mathbf{y}}(\mathsf{ID}) \neq 0 \mod q$. Hence, the simulation succeeds when the adversary queries on secret keys for ID satisfying $\mathsf{F}_{\mathbf{y}}(\mathsf{ID}) \neq 0 \mod q$, and queries for a challenge ciphertext for $\mathsf{ID}^\star$ satisfying $\mathsf{F}_{\mathbf{y}}(\mathsf{ID}^\star) = 0 \mod q$ in which case the reduction algorithm can embed its LWE challenge.

Overview of the Construction and Security Proof. The major drawback of the Yamada IBE is that they require the modulus size q to be super-polynomial.

This stems from the fact that the size of $y_0, y_{i,j} \in \mathbb{Z}_q$ must grow linearly in the number of adversarial key extraction query Q for the security proof to be meaningful, i.e., $\Pr_{\mathbf{y}}[\mathsf{F}_{\mathbf{y}}(\mathsf{ID}^\star) = 0 \wedge \mathsf{F}_{\mathbf{y}}(\mathsf{ID}_1) \neq 0 \wedge \cdots \wedge \mathsf{F}_{\mathbf{y}}(\mathsf{ID}_Q) \neq 0]$ is noticeable in n. However, since the size of the $\mathbf{G}$-trapdoor $\mathbf{R}_{\mathsf{ID}}$ used during simulation grows proportionally to the size of $y_{1,i}$ (check above Eq.(2) to see how $\mathbf{R}_{\mathsf{ID}}$ was created), thereby growing proportional to $Q = \mathsf{poly}(n)$, we need to set the modulus size q to be at least super-polynomial in n for the trapdoor to operate properly. Therefore, if we try to restrict ourselves to a polynomial sized modulus q, it seems the best we can achieve is a scheme where we have to set a bound on the number of adversarial key extraction queries before instantiation, i.e., a Q-bounded scheme.

In our work, we combine several ideas in a novel way to circumvent the above seemingly inevitable problem. The first idea is to extend the elements $y_0, y_{i,j} \in \mathbb{Z}_q$ to matrices $\mathbf{Y}_0, \mathbf{Y}_{i,j} \in \mathbb{Z}_q^{n \times n}$ so that instead of increasing the size of the element $y \in \mathbb{Z}_q$, we can "pack" small elements in the entries of the matrix $\mathbf{Y} \in \mathbb{Z}_q^{n \times n}$. Namely, since the matrix has n^2 entries, if the number of key extraction query is $Q = n^c$ for some constant c, we can always set up the matrix so that c of the entries are packed by elements of size $O(n)$. Since there are n^2 entries in total, this allows us to pack the matrix with small entries (e.g., $O(n)$) for arbitrary $Q = \mathsf{poly}(n)$ without the need of increasing the modulus size q. However, this simple idea alone does not work, since during the security proof to obtain Eq.(2), we crucially relied on the fact that $\mathbf{A}$ and $y_{1,i}$ commutes. For our idea to work we need the two matrices $\mathbf{A}$ and $\mathbf{Y}_{1,i}$ to commute, however, in general this does not hold.

To overcome this problem, we introduce our second idea of using the ring structure of ideal lattices. Concretely, we use the special polynomial ring $R = \mathbb{Z}[X]/(X^n + 1)$ to construct our scheme for n a power of 2. The construction itself is exactly the same as the ring analogue of the Yamada IBE, however, our new security proof relies crucially on the underlying ring structure. In detail, the reduction algorithm prepares the public parameters as

$$\boldsymbol{b}_0 = \boldsymbol{a}\boldsymbol{R}_0 + y_0\boldsymbol{g}, \quad \boldsymbol{b}_{i,j} = \boldsymbol{a}\boldsymbol{R}_{i,j} + y_{i,j}\boldsymbol{g}$$

for $(i,j) \in [2] \times [\ell]$, where $\boldsymbol{a}, \boldsymbol{b}_0, \boldsymbol{b}_{i,j} \in R_q^k$, $\boldsymbol{R} \in R_q^{k \times k}$, $y_0, y_{i,j} \in R_q$ and $\boldsymbol{g} \in R_q^k$ is the ring analogue of the $\mathbf{G}$-trapdoor. Observe that $y_0, y_{i,j}$ are now elements in R_q instead of $\mathbb{Z}_q$. Although this y is not quite a matrix, this is actually more than enough for us to use the packing technique described above. This can be seen by first noticing the natural isomorphism between $R_q \cong \mathbb{Z}_q^n$ induced by the coefficient embedding and viewing $y \in R_q$ as a vector in $\mathbb{Z}_q^n$. Since y has n entries when viewed as vectors, it can support up to n^n queries by packing each entry with small elements of size $O(n)$. Furthermore, the second part of the problem addressed above is naturally resolved, since now that we are working in a ring we get the commutativity of $\boldsymbol{a}$ and $y_{1,j}$ for free. This key role in the commutativity for rings is somewhat reminiscent to the signature scheme of [DM14]. We note that the technique used by [Alp15] (which has also been used in [Xag13]) to extend the results of [DM14] to matrices seems to be inapplicable

in our setting. This is because in our setting we need to commute the LWE challenge matrix $\mathbf{A}$ instead of the gadget matrix $\mathbf{G}$ whose associating trapdoor is known. To summarize, by incorporating our second idea, we obtain the ring variant of Eq.(2) and the trapdoor operates as specified. We note that one might be tempted to pack the entries of y with constant size elements, since 2^n is still exponential in n and hence $Q(n) < 2^n$. However, the security proof relies heavily on the fact that the density (i.e., the number of entries that are packed) of y is bounded by some constant. Therefore, we must choose the size of the packed elements with care to make the overall scheme secure.

The final idea is carefully crafting a properly distributed challenge ciphertext. To be precise, the main issue is in the difficulty of creating a ciphertext that has errors that are properly distributed. This problem of generating a properly distributed challenge ciphertext was addressed in [Yam16] as well, however, they used the standard technique called the "smudging" or "noise flooding" technique which came at the cost of making the modulus size q super-polynomial in n. This was not a problem for them, since as we pointed out earlier, their scheme inherently needed a super-polynomial sized modulus to work. However, this tactic is inapplicable to our setting since we want to restrict ourselves to the polynomial sized modulus. To overcome this we devise a way to carefully craft the error term; a technique reminiscent of [GPV08,ACPS09]. First, assume we have $\mathsf{F}(\mathsf{ID}^\star) = 0$ for the challenge identity $\mathsf{ID}^\star$ and thus $\mathsf{H}(\mathsf{ID}) = \mathbf{A}\mathbf{R}_{\mathsf{ID}^*}$. Note that for ease of understanding we explain the technique in the matrix form instead of the ring form. To prove security, we have to embed the LWE challenge $\mathbf{A}$ and $\mathbf{v}$ into the challenge ciphertext, where $\mathbf{v} = \mathbf{s}\mathbf{A} + \mathbf{x}$ or $\mathbf{v}$ a random vector. One natural way is to set

$$\mathbf{x}_1 = \mathbf{x}, \quad \mathbf{x}_2 = \mathbf{x}\mathbf{R}_{\mathsf{ID}^\star} \tag{3}$$

and compute the challenge ciphertext as

$$\mathbf{s}[\mathbf{A}|\mathsf{H}(\mathsf{ID}^\star)] + [\mathbf{x}_1|\mathbf{x}_2] = [\mathbf{v}|\mathbf{v}\mathbf{R}_{\mathsf{ID}^\star}].$$

However, one can not simply use the standard generalized leftover hash lemma for lattices presented in [ABB10]; a technique often used in proving such forms. This is because $\mathbf{R}_{\mathsf{ID}^\star}$ is not uniformly sampled as in the case of [ABB10], but instead highly correlated to the values of $y, \{y_{i,j}\}$ used during the simulation. Alternatively, we present a noise rerandomization technique and add a small extra noise to Eq.(3) and statistically hide $\mathbf{R}_{\mathsf{ID}}$. Namely, we sample noises $\mathbf{e}_1$ and $\mathbf{e}_2$ from a particular Gaussian distribution with variance computed from $\mathbf{R}_{\mathsf{ID}^\star}$ and set

$$\mathbf{x}_1 = \mathbf{x} + \mathbf{e}_1, \quad \mathbf{x}_2 = \mathbf{x}\mathbf{R}_{\mathsf{ID}^\star} + \mathbf{e}_2.$$

Thus the challenge ciphertext is created as above by further adding the new noise terms. Although the general idea of this technique has been around since [Reg05,GPV08] and has been used in contexts elsewhere, as far as we know, we believe this is a nice application for rerandomizing the noise without the need of adding a huge (super-polynomial sized) noise.

An Additional Idea. Working in the ring setting introduces some subtle yet crucial obstacles, which we did not have to address before. Namely, for q a prime and n a power of 2, the domain $R_q = \mathbb{Z}[X]/(q, X^n + 1)$ we work in is no longer a field as in the case of $\mathbb{Z}_q$. Additionally, if we use a modulus q such that $q \equiv 1 \mod 2n$ as in [LPR10,LPR13], the ring R_q completely splits into n fields. In such a ring, each field only contains $q = \mathsf{poly}(n)$ elements so the Schwartz-Zippel lemma during our security proof can not be applied. We get around this by using a modulus q such that $q \equiv 3 \mod 8$ where it is known to split into only two fields. Then, since each field now contains $q^{n/2}$ elements and R_q acts roughly as a field, we are able to apply our proof techniques. As for the purpose of completeness, we prove the hardness of LWE over such rings by the straightforward combination of previous results. We finally note that we also obtain a nice regularity lemma over such rings which helps us attain better parameters for the scheme.

We also employ some ideas to further optimize the sizes of the public parameters, secret keys and ciphertexts. Namely, we use the (ring version of the) $\mathbf{G}$-trapdoor where the base is set as n^η for some positive constant η. We use $\eta = \frac{1}{4}$ for our concrete parameter selection. By incorporating this idea, we can further reduce the size of the parameters by a factor of $\log n$. However, this comes at the cost of making the scheme less efficient, since the function $\mathbf{G}^{-1}(\cdot)$ has a slower running time for a larger base.

2.2 Construction from Bilinear Maps

Here, we explain our IBE scheme from bilinear maps. We start with a slightly modified version of Waters IBE [Wat05] and gradually modify it to obtain our scheme. Let us consider a group $\mathbb{G}$ with prime order p whose generator is g. The group is equipped with a efficiently computable bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$. The public parameters of the scheme contains rather long $\kappa + 3$ group elements $\{g^{w_i}\}_{i\in[0,\kappa]}$, g^α, g^β, and a randomness $\mathsf{rand} \in \{0,1\}^{|\mathbb{G}_T|}$ that is used to derive the Goldreich-Levin hardcore bit function $\mathsf{GL} : \{0,1\}^{|\mathbb{G}_T|} \times \{0,1\}^{|\mathbb{G}_T|} \to \{0,1\}$. The form of the ciphertexts and private keys in the scheme are as follows:

$$C = \left(g^s,\ g^{s\mathsf{H}(\mathsf{ID})},\ \mathsf{GL}\left(e(g^\alpha, g^\beta)^s, \mathsf{rand}\right) \oplus \mathsf{M} \right), \quad \mathsf{sk}_{\mathsf{ID}} = \left(g^{\alpha\beta} \cdot g^{r\mathsf{H}(\mathsf{ID})},\ g^{-r} \right)$$

where $\mathsf{M} \in \{0,1\}$ is the message to be encrypted, and s and r are random elements in $\mathbb{Z}_p$ that are picked during the encryption and key generation algorithms, respectively.

Here, $\mathsf{H} : \{0,1\}^\kappa \to \mathbb{Z}_p$ is defined as $\mathsf{H}(\mathsf{ID}) = w_0 + \sum_{\mathsf{ID}_i=1} w_i$ where ID_i is the i-th bit of ID. The reason why we use the hardcore bit function is to base the security of the scheme on the *computational* bilinear Diffie-Hellman (CBDH) assumption, rather than the stronger *decisional* bilinear Diffie-Hellman (DBDH) assumption which was used to prove the security of the original Waters IBE.

Next, we try to reduce the size of the public parameters using the idea of the Yamada IBE. A natural way to do this would be to introduce the injective

map $S : \{0,1\}^\kappa \to 2^{[\ell]\times[\ell]}$ with $\ell = \lceil \kappa^{1/2} \rceil$, change the public parameters to be $g^{w_0}, \{g^{w_{i,j}}\}_{(i,j)\in[2]\times[\ell]}$, and modify the function H as

$$\mathsf{H}(\mathsf{ID}) = w_0 + \sum_{(i,j)\in S(\mathsf{ID})} w_{1,i} w_{2,j}.$$

Through this change, we can reduce the size of the public parameters from $O(\kappa)$ group elements to $O(\sqrt{\kappa})$, just in as [Yam16]. However, we come across an immediate problem: We cannot efficiently compute $g^{s\mathsf{H}(\mathsf{ID})}$ from the public parameters! A straightforward solution to this problem is to put "helper" terms $\{g^{w_{1,i}w_{2,j}}\}$ into the public parameters. However, this makes the size of the public parameters large again.

Our solution to this problem is to rely on the Boneh-Boyen technique [BB04a] to compute something similar to the problematic term. Namely, we compute

$$g^{s\mathsf{H}(\mathsf{ID})+\sum_{j\in S(\mathsf{ID})}\tilde{t}_j w_{2,j}}, \qquad \{\ g^{\tilde{t}_j}\ \}_{j\in[\ell]} \tag{4}$$

instead of computing only $g^{s\mathsf{H}(\mathsf{ID})}$. Here, $\{\tilde{t}_j\}$ are additional randomness introduced by the encryption algorithm. Accordingly, we change the form of the ciphertexts and private keys of our scheme as follows:

$$\begin{aligned} C &= \left(g^s,\ g^{s\mathsf{H}(\mathsf{ID})+\sum_{j\in[\ell]}\tilde{t}_j w_{2,j}},\ \{g^{\tilde{t}_j}\}_{j\in[\ell]},\ \mathsf{GL}\left(e(g^\alpha, g^\beta)^s, \mathsf{rand}\right) \oplus \mathsf{M} \right), \\ \mathsf{sk}_{\mathsf{ID}} &= \left(g^{\alpha\beta}\cdot g^{r\mathsf{H}(\mathsf{ID})},\ g^{-r},\ \{g^{r w_{2,j}}\}_{j\in[\ell]} \right). \end{aligned} \tag{5}$$

Note that although the size of the public parameters is smaller than the original scheme, the sizes of the ciphertexts and private keys are larger due to the additional terms. We now show that one can efficiently compute the ciphertext. In particular, we show that it is possible to generate the terms in Eq.(4). To see this, let us introduce the variables $\{t_j\}$ such that

$$\tilde{t}_j := t_j - s\left(\sum_{i\in\{i\in[1,\ell]|(i,j)\in S(\mathsf{ID})\}} w_{1,i} \right). \tag{6}$$

Then, we have

$$\begin{aligned} & s\mathsf{H}(\mathsf{ID}) + \sum_{j\in[\ell]} \tilde{t}_j w_{2,j} \\ &= s\mathsf{H}(\mathsf{ID}) + \sum_{j\in[\ell]} w_{2,j}\left(t_j - s\left(\sum_{i\in\{i\in[1,\ell]|(i,j)\in S(\mathsf{ID})\}} w_{1,i} \right)\right) \\ &= s\mathsf{H}(\mathsf{ID}) + \sum_{j\in[\ell]} w_{2,j} t_j - s\sum_{j\in[\ell]}\left(\sum_{i\in\{i\in[1,\ell]|(i,j)\in S(\mathsf{ID})\}} w_{1,i}w_{2,j} \right) \\ &= sw_0 + \cancel{s\sum_{(i,j)\in S(\mathsf{ID})} w_{1,i}w_{2,j}} + \sum_{j\in[\ell]} w_{2,j}t_j - \cancel{s\sum_{(i,j)\in S(\mathsf{ID})} w_{1,i}w_{2,j}} \end{aligned}$$

$$= sw_0 + \sum_{j\in[\ell]} w_{2,j}t_j. \tag{7}$$

Since Eq.(6) and (7) are linear in w_0, $w_{i,j}$, it can be seen that the terms in Eq.(4) can be computed efficiently, as desired.

By substituting $\tilde{t}_j$ in Eq.(5) with the right-hand side of Eq.(4), we obtain our final scheme. As for the security, we can prove the adaptive security of the scheme from the 3-computational bilinear Diffie-Hellman exponent (3-CBDHE) assumption. We need to rely on this stronger assumption than the standard CBDH assumption, because of the different algebraic structure incorporated by the modified Waters IBE.

3 Preliminaries

Due to the space limitation, most of the proofs for the lemmas presented in this paper are omitted. For the full proof refer to our full version.

Notations. We use non-italic bold lowercase letters (e.g., $\mathbf{v}$) for vectors with entries in $\mathbb{R}$ and italic bold lowercase letters (e.g., $\boldsymbol{v}$) for vectors with entries in rings or number fields. We view vectors in the row form stated otherwise. Matrices are denoted by uppercase bold letters analogously. For a vector $\mathbf{v} \in \mathbb{R}^n$, denote $\|\mathbf{v}\|_p$ as the L_p-norm, where $p = 2$ is the standard Euclidean norm. For a matrix $\mathbf{R} \in \mathbb{R}^{n\times n}$, denote $\|\mathbf{R}\|_{\mathsf{GS}}$ as the longest column of the Gram-Schmidt orthogonalization of $\mathbf{R}$ and denote $s_1(\mathbf{R})$ as the largest singular value (spectral norm). We denote $[\cdot|\cdot]$ (resp. $[\cdot;\cdot]$) as the horizontal (resp. vertical) concatenation of vectors and matrices. We denote $[a, b]$ as the set $\{a, a+1, \ldots, b-1, b\}$ for any integers $a, b \in \mathbb{N}$ satisfying $a \le b$, and for simplicity write $[b]$ for the special case $a = 1$. For a (quotient) polynomial ring R over $\mathbb{Z}$, we denote $[-b, b]_R \subseteq R$ as the set of elements in R with all coefficients in the interval $[-b, b]$. Statistical distance between two random variables X and Y with support Ω is defined as $\Delta(X;Y) = \frac{1}{2}\sum_{s\in\Omega} |\Pr[X = s] - \Pr[Y = s]|$. A function $f : \mathbb{N} \to \mathbb{R}_{\ge 0}$ is said to be negligible, if for all c, there exists λ_0 such that $f(\lambda) < 1/\lambda^c$ for all $\lambda > \lambda_0$. We denote by $\mathsf{negl}(\lambda)$ a negligible function in λ.

3.1 Identity-Based Encryption

We use the standard syntax of IBE [BF01]. We briefly recall the security notion of IBEs and refer the exact definition to the full version. In our paper, we define two security notions: *adaptive security* and *adaptively-anonymous security*. The former adaptive security is the standard notion for IBEs as in [Wat05]. The latter adaptively-anonymous security is a notion that additionally requires the ciphertext to be indistinguishable from random. The term anonymous captures the fact the the ciphertext does not reveal the identity for which it was sent to. Furthermore, we use two random variables coin and $\widehat{\mathsf{coin}}$ in $\{0, 1\}$ for defining the security for IBEs. coin refers to the random value chosen by the challenger at the beginning of the security game and $\widehat{\mathsf{coin}}$ refers to the random value outputted by

the adversary at the end of the game. We provide a general statement concerning coin and $\widehat{\mathsf{coin}}$ in Sec. 3.4.

3.2 Lattices and Gaussian Distributions

An n-dimensional (full rank) lattice $\Lambda \subseteq \mathbb{R}^n$ is the set of all integer linear combinations of some set of n linearly independent basis vectors $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\} \subseteq \mathbb{R}^n$, $\Lambda = \{\sum_{i\in[n]} z_i \mathbf{b}_i | \mathbf{z} \in \mathbb{Z}^n\}$. For positive integers q, n, m, a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and a vector $\mathbf{u} \in \mathbb{Z}_q^n$, the m-dimensional "shifted" integer lattice is defined as $\Lambda_{\mathbf{u}}^{\perp}(\mathbf{A}) = \{\mathbf{z} \in \mathbb{Z}^m | \mathbf{A}\mathbf{z}^T = \mathbf{u}^T \mod q\}$. We simply write $\Lambda^{\perp}(\mathbf{A})$ in case $\mathbf{u} = \mathbf{0}$.

For $s > 0$, the n-dimensional Gaussian function $\rho_s : \mathbb{R}^n \to (0, 1]$ is defined as $\rho_s(\mathbf{x}) = \exp(-\pi\|\mathbf{x}\|_2^2/s^2)$. The (spherical) continuous Gaussian distribution D_s over $\mathbb{R}^n$ is the distribution with density function proportional to ρ_s. When the dimension n is not clear from context, we explicitly write it as D_s^n. More generally, for any matrix $\mathbf{B} \in \mathbb{R}^{n\times m}$, denote $D_{\mathbf{B}}$ as the distribution of $\mathbf{x}\mathbf{B}^T$ where $\mathbf{x}$ is distributed as D_1^m. A well known fact is that for any two matrices $\mathbf{B}_1, \mathbf{B}_2$, the sum of an independent sample from $D_{\mathbf{B}_1}$ and $D_{\mathbf{B}_2}$ is distributed as $D_{\mathbf{C}}$ where $\mathbf{C} = (\mathbf{B}_1\mathbf{B}_1^T + \mathbf{B}_2\mathbf{B}_2^T)^{1/2}$.

For a n-dimensional lattice Λ and a vector in $\mathbf{u} \in \mathbb{R}^n$, the discrete Gaussian distribution $D_{\Lambda+\mathbf{u},s}$ over the coset $\Lambda+\mathbf{u}$ is defined as $D_{\Lambda+\mathbf{u},s}(\mathbf{x}) = \rho_s(\mathbf{x})/\rho_s(\Lambda+\mathbf{u})$ for all $\mathbf{x} \in \Lambda+\mathbf{u}$. We also define the discrete Gaussian distribution $D^{\mathsf{coeff}}_{\Lambda+\mathbf{u},r}$ over a (quotient) polynomial ring R in X over $\mathbb{R}$. The discrete Gaussian distribution $D^{\mathsf{coeff}}_{\Lambda+\mathbf{u},r}$ is the distribution of $a = \sum_{i=0}^{n-1} \alpha_i X^i \in R$ where the coefficient vector $[\alpha_0, \ldots, \alpha_{n-1}] \in \mathbb{R}^n$ is sampled from the discrete Gaussian distribution $D_{\Lambda+\mathbf{u},r}$. This definition naturally extends to vectors $\boldsymbol{a} \in R^k$ in case of nk-dimensional lattices.

The following lemma on noise rerandomization plays an important role in the security proof of our scheme when creating a properly distributed challenge ciphertext. This allows us to simulate the challenge ciphertext without resorting to the noise flooding technique as in [Yam16]. Namely, during simulation we set $\ell = 2m$, $\mathbf{V} = [\mathbf{I}_m | \mathbf{R}_{\mathsf{ID}}]$ and $\mathbf{b} + \mathbf{x}$ as the LWE challenge (note that we view the LWE challenge in a slightly different way than usual).

Lemma 1 (Noise Rerandomization). *Let q, ℓ, m be positive integers and r a positive real satisfying $r > \max\{\omega(\sqrt{\log m}), \omega(\sqrt{\log \ell})\}$. Let $\mathbf{b} \in \mathbb{Z}_q^m$ be arbitrary and $\mathbf{x}$ chosen from $D_{\mathbb{Z}^m,r}$. Then for any $\mathbf{V} \in \mathbb{Z}^{m\times\ell}$ and positive real $\sigma > s_1(\mathbf{V})$, there exists a PPT algorithm $\mathsf{ReRand}(\mathbf{V}, \mathbf{b}+\mathbf{x}, r, \sigma)$ that outputs $\mathbf{b}' = \mathbf{b}\mathbf{V}+\mathbf{x}' \in \mathbb{Z}_q^\ell$ where $\mathbf{x}'$ is distributed statistically close to $D_{\mathbb{Z}^\ell, 2r\sigma}$.*

3.3 Rings and Ideal Lattices

We try to provide a minimum exposition of rings and ideal lattices to keep it self-contained. For further detail see the full version or refer to other works [LPR10,LPR13].

Preparation. Let n be a power of 2 and set $m = 2n$. Define the ring $R = \mathbb{Z}[X]/(\Phi_m(X))$, where $\Phi_m(X) = X^n + 1$ is the mth cyclotomic polynomial. For

an integer q, denote R_q as $R/qR = \mathbb{Z}[X]/(q, \Phi_m(X))$. By viewing the elements in R as $n-1$ degree polynomials in $\mathbb{Z}[X]$, we can consider a natural coefficient embedding of R onto the integer lattice $\mathbb{Z}^n$. Namely, we define the coefficient embedding $\phi : R \to \mathbb{Z}^n$ that maps $a = \sum_{i=0}^{n-1} \alpha_i X^i \in R$ to $[\alpha_0, \alpha_1, \ldots, \alpha_{n-1}] \in \mathbb{Z}^n$. We extend the coefficient embedding naturally to vectors and matrices. On the other hand, we can also identify R as the subring of anti-circulant matrices in $\mathbb{Z}^{n\times n}$ by viewing each ring element $a \in R$ as a linear transformation $r \to a{\cdot}r$ of R. Concretely, we define the ring homomorphism $\mathrm{rot} : R \to \mathbb{Z}^{n\times n}$ that sends $a \in R$ to a matrix in $\mathbb{Z}^{n\times n}$ such that the i-th row is $\phi(a \cdot X^{i-1} \mod \Phi_m(X)) \in \mathbb{Z}^n$. Note that the first row of $\mathrm{rot}(a)$ is $\phi(a)$. Similarly to above, the definition of the map rot naturally extends to vectors and matrices.

Norms in R. We define the Euclidean length for an element $a \in R$ and a vector $\boldsymbol{v} \in R^k$ by identifying R with $\mathbb{Z}^n$ through the coefficient embedding.[4] Therefore, when we say a vector $\boldsymbol{v}$ in R^k is "short", we mean that $\|\phi(\boldsymbol{v})\|_2$ is small. We also define the largest singular value of a matrix $\boldsymbol{R} \in R^{s\times t}$ by identifying the ring R with $\mathbb{Z}^{n\times n}$ through the map rot.[5] Namely, $s_1(\boldsymbol{R}) := \max_{\|\mathbf{z}\|_2=1} \|\mathbf{z} \cdot \mathrm{rot}(\boldsymbol{R})\|_2$. Note that this definition allows us to consider singular values of an element in R as well.

Properties for Elements in R. As with matrices with entries in $\mathbb{R}$, we have similar singular value bounds for matrices with elements in R. Namely, we can bound the singular value of a random matrix chosen from $[-b, b]_R^{s\times t}$. Recall that an element of $[-b, b]_R$ is an element in R with all of its coefficients in the interval $[-b, b]$.

Lemma 2 ([DM15], Special case of Fact 1). *Let b be a positive integer and $\boldsymbol{R}$ be a $s \times t$ matrix chosen uniformly at random from $[-b, b]_R^{s\times t}$. Then, there exists a universal constant $C(\approx 1/\sqrt{2\pi})$ such that*

$$\Pr[s_1(\boldsymbol{R}) \geq C \cdot b\sqrt{n} \cdot (\sqrt{s} + \sqrt{t} + \omega(\sqrt{\log n}))] = \mathsf{negl}(n)$$

We note that similarly to matrices with entries in $\mathbb{R}$, we have $s_1(\boldsymbol{R}_1\boldsymbol{R}_2) \leq s_1(\boldsymbol{R}_1)s_1(\boldsymbol{R}_2)$ for all $\boldsymbol{R}_1, \boldsymbol{R}_2 \in R^{k\times k}$, which follows from the fact that rot is a ring homomorphism. Furthermore, it also holds when $\boldsymbol{R}_1$ is replaced by an element a in R.

Regularity Lemma. The former Lemma shows that there exists a quotient ring $R_q = R/(q, \Phi_m(X))$ that acts roughly as a field, or in other words, R_q has exponentially many invertible elements. The latter Lemma is a ring analogue of the standard lattice regularity lemma.

Lemma 3. *Let q be a prime such that $q \equiv 3 \mod 8$ and n be a power of 2. Then, $\Phi_{2n}(X) = X^n + 1$ splits as $X^n + 1 \equiv t_1 t_2 \mod q$ for two irreducible*

[4] We could have identified the Euclidean length by the *canonical* embedding as done in other works. However, for our special case where n is power of 2, the lengths are equivalent up to a factor of $\sqrt{n}$.

[5] For the special case where n is a power of 2, $s_1(\boldsymbol{R})$ defined by the coefficient and canonical embeddings are both equivalent to the one defined by the map rot.

polynomials $t_1 = X^{n/2} + uX^{n/4} - 1$ *and* $t_2 = X^{n/2} - uX^{n/4} - 1$ *in* $\mathbb{Z}_q[X]$ *where* $u^2 \equiv -2 \mod q$. *Furthermore, all* $x \in R_q$ *satisfying* $\|\phi(x)\|_2 < \sqrt{q}$ *are invertible, i.e.,* $x \in R_q^*$.

Lemma 4 (Regularity Lemma). *Let* n *be a power of 2,* q *be a prime larger than* $4n$ *such that* $q \equiv 3 \mod 8$, *and* ℓ, k', k, ρ *be positive integers satisfying* $\ell, k' \geq 1$, $k \geq 2$, $\rho < \frac{1}{2}\sqrt{q/n}$. *Define the family of hash functions* $\mathcal{H} = \{h_{\boldsymbol{A}}(\boldsymbol{x}) : [-\rho, \rho]_R^k \to R_q^{k'}\}$, *where* $h_{\boldsymbol{A}}(\boldsymbol{x}) = \boldsymbol{A}\boldsymbol{x}$ *for* $\boldsymbol{A} \in R_q^{k' \times k}$, $\boldsymbol{x} \in R_q^{k \times 1}$. *Then,* $\mathcal{H}$ *is a universal hash family. Furthermore, for* $\boldsymbol{A} \xleftarrow{\$} R_q^{k' \times k}$ *and* $\boldsymbol{X} \xleftarrow{\$} [-\rho, \rho]_R^{k \times \ell}$, *we have*

$$\Delta((\boldsymbol{A}, \boldsymbol{A}\boldsymbol{X}) \ ; \ (\boldsymbol{A}, U(R_q^{k' \times \ell}))) \leq \frac{\ell}{2} \cdot \sqrt{\left(\frac{q^{k'}}{(2\rho+1)^k}\right)^n}.$$

Ring Learning with Errors. The ring LWE problem was introduced by Lyubashevsky et al. [LPR10]. They showed that solving it on the average is as hard as (quantumly) solving several standard problems on ideal lattices in the worst case.

Definition 1 (RLWE). *For positive integers* $n = n(\lambda)$, $k = k(n)$, *a prime integer* $q = q(n) > 2$, *an error distribution* $\chi = \chi(n)$ *over* R_q, *and an PPT algorithm* $\mathcal{A}$, *an advantage for the RLWE problem* $\mathsf{RLWE}_{n,k,q,\chi}$ *of* $\mathcal{A}$ *is defined as follows:*

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{RLWE}_{n,k,q,\chi}} = |\Pr[\mathcal{A}(\{(a_i, v_i)\}_{i=1}^k) \to 1] - \Pr[\mathcal{A}(\{(a_i, a_i s + e_i)\}_{i=1}^k) \to 1]|$$

where $a_1, \ldots, a_k, v_1, \ldots, v_k, s \xleftarrow{\$} R_q$ *and* $e_1, \ldots, e_k \xleftarrow{\$} \chi$. *We say that* $\mathsf{RLWE}_{n,k,q,\chi}$ *assumption holds if* $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{RLWE}_{n,k,q,\chi}}$ *is negligible for all PPT* $\mathcal{A}$.

Theorem 1. *Let* α *be a positive real,* m *be a power of* 2, ℓ *be an integer,* $\Phi_m(X) = X^n + 1$ *be the* m*th cyclotomic polynomial where* $m = 2n$, *and* $R = \mathbb{Z}[X]/(\Phi_m(X))$. *Let* $q \equiv 3 \mod 8$ *be a (polynomial size) prime such that there is another prime* $p \equiv 1 \mod m$ *satisfying* $p \leq q \leq 2p$ *and* $\alpha q \geq n^{3/2} k^{1/4} \omega(\log^{9/4} n)$. *Then, there is a probabilistic polynomial-time quantum reduction from* $\tilde{O}(\sqrt{n}/\alpha)$*-approximate SIVP (or SVP) to* $\mathsf{RLWE}_{n,k,q,\chi}$ *with* $\chi = D_{\mathbb{Z}^n, \alpha q}^{\mathsf{coeff}}$.

The proof is obtained by a straightforward combination of previous results [LPR10,LS15]. Due to the Linnik's theorem and Dirichlet's theorem on arithmetic progressions, we have that there are sufficiently many primes p and q satisfying the assumption of the theorem.

Trapdoors for Rings. Define the gadget matrix $\boldsymbol{g}_b = [1|b|\cdots|b^{k'-1}|\boldsymbol{0}] \in R_q^k$, where b is a positive integer and $k \geq k' = \lceil \log_b q \rceil$. When $k = k'$ and $b = 2$, this corresponds to the matrix representation of the gadget matrix $\mathbf{G} \in \mathbb{Z}_q^{n \times nk}$ often used in the literatures by properly rearranging the rows and columns of $\mathrm{rot}(\boldsymbol{g}_2)$. The following algorithms are simple modification of traditional lattice based algorithms.

Lemma 5. *Let n be a power of 2, q be a prime larger than $4n$ such that $q \equiv 3 \mod 8$, and b, ρ be a positive integer satisfying $\rho < \frac{1}{2}\sqrt{q/n}$. Furthermore, define $\log_1(\cdot) := \log_2(\cdot)$. Then, there exist polynomial time algorithms with the properties below:*

- $\mathsf{TrapGen}(1^n, 1^k, q, \rho) \to (\boldsymbol{a}, \boldsymbol{T_a})$ ([MP12], Lemma 5.3): *a randomized algorithm that, when $k \geq 2\log_\rho q$, outputs a vector $\boldsymbol{a} \in R_q^k$ and a matrix $\boldsymbol{T_a} \in R^{k\times k}$, where $\mathrm{rot}(\boldsymbol{a}^T)^T \in \mathbb{Z}_q^{n\times nk}$ is a full-rank matrix and $\mathrm{rot}(\boldsymbol{T_a}) \in \mathbb{Z}^{nk\times nk}$ is a basis for $\Lambda^\perp(\mathrm{rot}(\boldsymbol{a}^T)^T)$ such that $\boldsymbol{a}$ is $\mathsf{negl}(n)$-close to uniform and $\|\mathrm{rot}(\boldsymbol{T_a})\|_{\mathsf{GS}} = O(b\rho \cdot \sqrt{n\log_\rho q})$.*[6]
- $\mathsf{SampleLeft}(\boldsymbol{a}, \boldsymbol{b}, u, \boldsymbol{T_a}, \sigma) \to \boldsymbol{e}$ ([CHKP10]): *a randomized algorithm that, given vectors $\boldsymbol{a}, \boldsymbol{b} \in R_q^k$ where $\mathrm{rot}(\boldsymbol{a}^T)^T, \mathrm{rot}(\boldsymbol{b}^T)^T \in \mathbb{Z}_q^{n\times nk}$ are full-rank, an element $u \in R_q$, a matrix $\boldsymbol{T_a} \in R^{k\times k}$ such that $\mathrm{rot}(\boldsymbol{T_a}) \in \mathbb{Z}^{nk\times nk}$ is a basis for $\Lambda^\perp(\mathrm{rot}(\boldsymbol{a}^T)^T)$, and a Gaussian parameter $\sigma > \|\mathrm{rot}(\boldsymbol{T_a})\|_{\mathsf{GS}} \cdot \omega(\sqrt{\log nk})$, outputs a vector $\boldsymbol{e} \in R^{2k}$ sampled from a distribution which is $\mathsf{negl}(n)$-close to $D^{\mathsf{coeff}}_{\Lambda^\perp_{\phi(u)}([\mathrm{rot}(\boldsymbol{a}^T)^T|\mathrm{rot}(\boldsymbol{b}^T)^T]),\sigma}$, i.e., $[\boldsymbol{a}|\boldsymbol{b}]\boldsymbol{e}^T = u$ and $\phi(\boldsymbol{e}) \in \mathbb{Z}^{2nk}$ is distributed according to $D_{\Lambda^\perp_{\phi(u)}([\mathrm{rot}(\boldsymbol{a}^T)^T|\mathrm{rot}(\boldsymbol{b}^T)^T]),\sigma}$.*
- $\mathsf{SampleRight}(\boldsymbol{a}, \boldsymbol{g}_b, \boldsymbol{R}, y, u, \boldsymbol{T}_{\boldsymbol{g}_b}, \sigma) \to \boldsymbol{e}$ *where* $\boldsymbol{b} = \boldsymbol{a}\boldsymbol{R} + y\boldsymbol{g}_b$ ([ABB10]): *a randomized algorithm that, given vectors $\boldsymbol{a}, \boldsymbol{g}_b \in R_q^k$ such that $\mathrm{rot}(\boldsymbol{a}^T)^T, \mathrm{rot}(\boldsymbol{g}_b)$*[7] *$\in \mathbb{Z}_q^{n\times nk}$ are full-rank matrices, elements $y \in R_q^*, u \in R_q$, a matrix $\boldsymbol{R} \in R^{k\times k}$, a matrix $\boldsymbol{T}_{\boldsymbol{g}_b} \in R^{k\times k}$ such that $\mathrm{rot}(\boldsymbol{T}_{\boldsymbol{g}_b}) \in \mathbb{Z}^{nk\times nk}$ is a basis for $\Lambda^\perp(\mathrm{rot}(\boldsymbol{g}_b))$, and a Gaussian parameter $\sigma > s_1(\boldsymbol{R}) \cdot \|\mathrm{rot}(\boldsymbol{T}_{\boldsymbol{g}_b})\|_{\mathsf{GS}} \cdot \omega(\sqrt{\log nk})$, outputs a vector $\boldsymbol{e} \in R^{2k}$ sampled from a distribution which is $\mathsf{negl}(n)$-close to $D^{\mathsf{coeff}}_{\Lambda^\perp_{\phi(u)}([\mathrm{rot}(\boldsymbol{a}^T)^T|\mathrm{rot}(\boldsymbol{b}^T)^T]),\sigma}$, i.e., $[\boldsymbol{a}|\boldsymbol{b}]\boldsymbol{e}^T = u$ and $\phi(\boldsymbol{e}) \in \mathbb{Z}^{2nk}$ is distributed according to $D_{\Lambda^\perp_{\phi(u)}([\mathrm{rot}(\boldsymbol{a}^T)^T|\mathrm{rot}(\boldsymbol{b}^T)^T]),\sigma}$.*
- ([MP12]:) *Let $k \geq \lceil \log_b q \rceil$. There exists a publicly known matrix $\boldsymbol{T}_{\boldsymbol{g}_b}$ such that $\mathrm{rot}(\boldsymbol{T}_{\boldsymbol{g}_b}) \in \mathbb{Z}^{nk\times nk}$ is a basis for the lattice $\Lambda^\perp(\mathrm{rot}(\boldsymbol{g}_b))$ and $\|\mathrm{rot}(\boldsymbol{T}_{\boldsymbol{g}_b})\|_{\mathsf{GS}} \leq \sqrt{b^2+1}$. Furthermore, there exists a deterministic polynomial time algorithm $\boldsymbol{g}_b^{-1}$ which takes input $\boldsymbol{u} \in R_q^k$ and outputs $\boldsymbol{R} = \boldsymbol{g}_b^{-1}(\boldsymbol{u})$ such that $\boldsymbol{R} \in [-b, b]_R^{k\times k}$ and $\boldsymbol{g}_b\boldsymbol{R} = \boldsymbol{u}$.*

Note that we abuse the notation $\boldsymbol{g}_b^{-1}$ by viewing it as a function rather than a vector. Namely, for any $\boldsymbol{u} \in R_q^k$ there are many choices for $\boldsymbol{R} \in R^{k\times k}$ such that $\boldsymbol{g}_b\boldsymbol{R} = \boldsymbol{u}$, and $\boldsymbol{g}_b^{-1}(\boldsymbol{u})$ is a function that deterministically outputs a particular short matrix from the possible candidates. Since we have $s_1(\boldsymbol{R}) \leq b \cdot nk$ for any $\boldsymbol{R} \in [-b, b]_R^{k\times k}$, $s_1(\boldsymbol{g}_b^{-1}(\boldsymbol{u})) \leq bnk$ holds for arbitrary $\boldsymbol{u} \in R_q^k$.

Homomorphic Computation. Let d be a natural number. We introduce the function $\mathsf{PubEval}_d : (R_q^k)^d \to R_q^k$ as in [Yam16], which takes a set of vectors $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_d \in R_q^k$ as inputs and outputs a vector in R_q^k. This function will be

[6] We combine several lemmas from [MP12] and the regularity lemma (Lemma 4) to show correctness of $\mathsf{TrapGen}$. See the full version for further detail. Further, the unusual lattice $\Lambda^\perp(\mathrm{rot}(\boldsymbol{a}^T)^T)$ is used only to be consistent with the other algorithms. Namely, we could have instead defined the trapdoor for the lattice $\Lambda^\perp(\mathrm{rot}(\boldsymbol{a}))$.

[7] We have $\mathrm{rot}(\boldsymbol{g}_b^T)^T = \mathrm{rot}(\boldsymbol{g}_b)$ since all the entries of $\boldsymbol{g}_b$ are integers.

used to hash identities to R_q^k in our lattice-based IBE construction. The function is defined recursively as follows:

$$\mathsf{PubEval}_d(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_d) = \begin{cases} \boldsymbol{b}_1 & \text{if } d = 1 \\ \boldsymbol{b}_1 \cdot \boldsymbol{g}_b^{-1}\big(\mathsf{PubEval}_{d-1}(\boldsymbol{b}_2, \ldots, \boldsymbol{b}_d)\big) & \text{if } d \geq 2. \end{cases}$$

Lemma 6. *Let $y_1, \ldots, y_d$ be elements in R, $\boldsymbol{a}, \boldsymbol{b}_1, \ldots, \boldsymbol{b}_d$ be vectors in R_q^k and $\boldsymbol{R}_1, \ldots, \boldsymbol{R}_d$ be matrices in $R^{k\times k}$ such that $\boldsymbol{b}_i = \boldsymbol{a}\boldsymbol{R}_i + y_i\boldsymbol{g}_b$ for $i \in [d]$. Furthermore, we assume that $s_1(\boldsymbol{R}_i) \leq B, \|\phi(y_i)\|_1 \leq \delta$ for $i \in [d]$. Then, there exists an efficient algorithm $\mathsf{TrapEval}_d$ that takes $\boldsymbol{R}_1, \ldots, \boldsymbol{R}_d$, $y_1, \ldots, y_d$ as inputs and outputs $\boldsymbol{R}' \in R^{k\times k}$ such that*

$$\mathsf{PubEval}_d(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_d) = \boldsymbol{a}\boldsymbol{R}' + y_1 \cdots y_d \boldsymbol{g}_b \in R_q^k$$

and $s_1(\boldsymbol{R}') \leq B\delta^{d-1} + Bbnk\big(\frac{\delta^{d-1}-1}{\delta-1}\big)$.

3.4 Other Facts

Lemma 7 (Expansion of Coefficients). *Let $c_1, c_2, B_1, B_2 \in \mathbb{N}$. Let also $u = u_0 + u_1 X + \cdots u_{c_1-1}X^{c_1-1} \in R$ and $v = v_0 + v_1 X + \cdots v_{c_2-1}X^{c_2-1} \in R$ be ring elements. We further assume that $c_1 + c_2 < n$ and $\|\phi(u)\|_\infty < B_1$ and $\|\phi(v)\|_\infty < B_2$. Then we have $\|\phi(uv)\|_\infty \leq \min\{c_1, c_2\} \cdot B_1 B_2$.*

The following Lemma addresses a general statement for bounding the success probability of an adversary engaging with the security game of IBE. In more detail, when the partitioning technique is used to prove security, the guess returned by the adversary is correlated with the key extraction queries it has made. Therefore, we need to argue with care to obtain a meaningful bound on the success probability that holds for arbitrary key extraction queries.

Lemma 8 (Implicit in [BR09,Yam16]). *Let us consider an IBE scheme and an adversary $\mathcal{A}$ that breaks adaptive security (adaptively-anonymous security) with advantage ϵ. Let us also consider a map γ that maps a sequence of identities to a value in $[0, 1]$. We consider the following experiment. We first execute the security game for $\mathcal{A}$. Let $\mathsf{ID}^\star$ be the challenge identity and $\mathsf{ID}_1, \ldots, \mathsf{ID}_Q$ be the identities for which key extraction queries were made. We denote $\mathbb{ID} = (\mathsf{ID}^\star, \mathsf{ID}_1, \ldots, \mathsf{ID}_Q)$. At the end of the game, we set $\mathsf{coin}' \in \{0, 1\}$ as $\mathsf{coin}' = \widehat{\mathsf{coin}}$ with probability $\gamma(\mathbb{ID})$ and $\mathsf{coin}' \xleftarrow{\$} \{0, 1\}$ with probability $1 - \gamma(\mathbb{ID})$. Then, the following holds.*

$$\left|\Pr[\mathsf{coin}' = \mathsf{coin}] - \frac{1}{2}\right| \geq \gamma_{\min} \cdot \epsilon - \frac{\gamma_{\max} - \gamma_{\min}}{2}$$

where $\gamma_{\min}$ (resp. $\gamma_{\max}$) is the maximum (resp. minimum) of $\gamma(\mathbb{ID})$ taken over all possible $\mathbb{ID}$.

Injective map. Let d and κ be some integers. Furthermore, let ℓ be $\ell = \lceil \kappa^{1/d} \rceil$. Then, an element of $[1, \kappa]$ can be written as an element of $[1, \ell]^d$ using some canonical map. Furthermore, it is also possible to write a subset of $[1, \kappa]$ as a subset of $[1, \ell]^d$ by naturally extending the canonical map. By identifying a bit string in $\{0,1\}^\kappa$ with a subset of $[1, \kappa]$ (for example, by regarding the former as the indicator vector of a subset of $[1, \kappa]$), we can define an efficiently computable injective map S that maps a bit string $\mathsf{ID} \in \{0,1\}^\kappa$ to a subset $S(\mathsf{ID})$ of $[1, \ell]^d$.

3.5 Core Lemma for Our Partitioning

We make a general statement concerning the partitioning technique for IBEs, which we use during the security analysis for both our lattice and bilinear map based constructions. Namely, we use the following Lemma in order to argue that the probability of the hash value for identities corresponding to the key extraction queries being invertible and the hash value for the challenge identity being zero is non-negligible.

Lemma 9. *Let $\nu, \mu, d, Q \geq 1$ be any integers. Let Φ be a ring and $\Omega_1, \ldots, \Omega_\nu$ be a set of fields equipped with homomorphisms $\pi_j : \Phi \to \Omega_j$ for $j \in [\nu]$. Assume that the map Π defined as $\Pi : \Phi \ni y \mapsto (\pi_1(y), \ldots, \pi_\nu(y)) \in \Omega_1 \times \cdots \times \Omega_\nu$ is an isomorphism. Let S_0 and S_1 be subsets of Φ with finite cardinality. Let us consider a set of multivariate polynomials $f_i(Y_1, \ldots, Y_\mu) \in \Phi[Y_1, \ldots, Y_\mu]$ for $i \in [0, Q]$ We further assume the following properties:*

1. *The map π_j is injective on S_1 for all $j \in [\nu]$.*
2. *We have $\pi_j(f_0) - \pi_j(f_i)$ is a non-zero polynomial with degree d for all $i \in [Q]$ and $j \in [\nu]$. Here π_j is extended to $\pi_j : \Phi[X] \to \Omega_j[X]$ in a natural way.*
3. *We have $S_0 \supseteq \cup_{i \in [0,Q]} \{-f_i(y_1, \ldots, y_\mu) | y_1, \ldots, y_\mu \in S_1\}$.*

Then, for $y_0 \xleftarrow{\$} S_0$ and $y_1, \ldots, y_\mu \xleftarrow{\$} S_1$, we have

$$\frac{1}{|S_0|}\left(1 - \frac{d\nu Q}{|S_1|}\right) \leq \gamma \leq \frac{1}{|S_0|}$$

where we denote

$$\gamma = \Pr_{y_0, \boldsymbol{y}'}[\ y_0 + f_0(\boldsymbol{y}') = 0 \ \wedge \ y_0 + f_1(\boldsymbol{y}') \in \Phi^* \ \wedge \cdots \wedge \ y_0 + f_Q(\boldsymbol{y}') \in \Phi^*],$$

$\boldsymbol{y}' = (y_1, \ldots, y_\mu)$, and $\Phi^* = \Pi^{-1}(\Omega_1^* \times \cdots \times \Omega_\nu^*)$.

4 Construction from RLWE

In this section, we show our IBE scheme from the RLWE assumption. Let d be a (flexible) constant number. In addition, let the identity space of the scheme be $\mathcal{ID} = \{0,1\}^\kappa$ for some $\kappa \in \mathbb{N}$ and the message space be $\{0,1\}^n \subset R$.[8] For our

[8] Note that we regard m as an elements in R via $\phi^{-1} : \mathbb{Z}^n \to R$ (the inversion of coefficient embedding).

construction, we consider an efficiently computable injective map S that maps an identity $\mathsf{ID} \in \{0,1\}^\kappa$ to a subset $S(\mathsf{ID})$ of $[1,\ell]^d$, where $\ell = \lceil \kappa^{1/d} \rceil$. Such a map can be constructed easily as we explained in Sec. 3.4. Let $n := n(\lambda)$, $b := b(n)$, $\rho := \rho(n)$, $m := 2n$, $k := k(n)$, $q := q(n)$, $\ell := \ell(n)$, $\alpha := \alpha(n)$, $\alpha' := \alpha'(n)$, and $\sigma := \sigma(n)$ be parameters that are specified later. Let also $\Phi_m(X) = X^n + 1$ be the mth cyclotomic polynomial and $R = \mathbb{Z}[X]/(\Phi_m(X))$.

$\mathsf{Setup}(1^\lambda)$: On input 1^λ, it first runs $(\boldsymbol{a}, \boldsymbol{T}_{\boldsymbol{a}}) \xleftarrow{\$} \mathsf{TrapGen}(1^n, 1^k, q, \rho)$ to obtain $\boldsymbol{a} \in R_q^k$ and $\boldsymbol{T}_{\boldsymbol{a}} \in R^{k \times k}$. It also picks $u \xleftarrow{\$} R_q, \boldsymbol{b}_0, \boldsymbol{b}_{i,j} \xleftarrow{\$} R_q^k$ for $(i,j) \in [d] \times [\ell]$ and outputs

$$\mathsf{mpk} = (\boldsymbol{a}, \boldsymbol{b}_0, \{\boldsymbol{b}_{i,j}\}_{(i,j)\in[d]\times[\ell]}, u) \quad \text{and} \quad \mathsf{msk} = \boldsymbol{T}_{\boldsymbol{a}}.$$

In the following, we use a deterministic function $\mathsf{H} : \mathcal{ID} \to R_q^k$ defined as

$$\mathsf{H}(\mathsf{ID}) = \boldsymbol{b}_0 + \sum_{(j_1,\ldots,j_d)\in S(\mathsf{ID})} \mathsf{PubEval}_d(\boldsymbol{b}_{1,j_1}, \boldsymbol{b}_{2,j_2}, \ldots, \boldsymbol{b}_{d,j_d}) \in R_q^k.$$

$\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{ID})$: It first computes $\mathsf{H}(\mathsf{ID})$ and picks $\boldsymbol{e} \in R^{2k}$ such that

$$[\boldsymbol{a}|\mathsf{H}(\mathsf{ID})] \cdot \boldsymbol{e}^T = u$$

using $\mathsf{SampleLeft}(\boldsymbol{a}, \mathsf{H}(\mathsf{ID}), u, \mathbf{T}_{\boldsymbol{a}}, \sigma) \to \boldsymbol{e}$. It returns $\mathsf{sk}_{\mathsf{ID}} = \boldsymbol{e}$.

$\mathsf{Encrypt}(\mathsf{mpk}, \mathsf{ID}, \mathsf{M})$: To encrypt a message $\mathsf{M} \in \{0,1\}^n \subset R$, it first picks $s \xleftarrow{\$} R_q$, $x_0 \xleftarrow{\$} D^{\mathsf{coeff}}_{\mathbb{Z}^n,\alpha q}$, $\boldsymbol{x}_1, \boldsymbol{x}_2 \xleftarrow{\$} \left(D^{\mathsf{coeff}}_{\mathbb{Z}^n,\alpha'}\right)^k$. Then it computes

$$c_0 = su + x_0 + \lfloor q/2 \rceil \cdot \mathsf{M}, \quad \boldsymbol{c}_1 = s[\boldsymbol{a}|\mathsf{H}(\mathsf{ID})] + [\boldsymbol{x}_1|\boldsymbol{x}_2].$$

Finally, it outputs the ciphertext $C = (c_0, \boldsymbol{c}_1) \in R_q \times R_q^{2k}$.

$\mathsf{Decrypt}(\mathsf{mpk}, \mathsf{sk}_{\mathsf{ID}}, C)$: To decrypt a ciphertext $C = (c_0, \boldsymbol{c}_1)$ using a private key $\mathsf{sk}_{\mathsf{ID}} = \boldsymbol{e}$, it computes $\left(\lfloor (2/q) \cdot \phi(c_0 - \boldsymbol{c}_1 \boldsymbol{e}^T) \rceil \mod 2\right) = m$. Here, the rounding function $\lfloor \cdot \rceil$ is applied componentwise.

4.1 Correctness and Parameter Selection.

The following lemma addresses the correctness of the scheme.

Lemma 10 (Correctness). *Assume* $\alpha q \omega(\sqrt{\log n}) + \sqrt{nk}\alpha'\sigma\omega(\sqrt{\log nk}) \le q/5$ *holds with over whelming probability. Then the above scheme has negligible decryption error.*

Parameter selection. We refer the precise requirements for the parameter selection to the full version. One concrete selection for the parameters is as follows:

$$k = 8d + 12, \qquad q = n^{2d+3}, \qquad b = \rho = n^{\frac{1}{4}},$$
$$\sigma = n^d \cdot \omega(\log n), \quad \alpha = n^{-2d-\frac{3}{8}} \cdot \omega(\log^2 n)^{-1}, \quad \alpha' = n^{d+\frac{5}{2}} \cdot \omega(\log^{\frac{3}{4}} n)^{-1},$$

where d is a (flexible) constant which may be set very small (e.g., $d = 2$ or 3) in a typical setting and the length κ of the identities ID is set as n. This specific instantiation is denoted as the Type 2 IBE scheme in Sec. 6. Table 1. Furthermore, the other concrete instantiation provided only in the full version, where we set $b = 2$ and $k = O(\log n)$, is denoted as the Type 1 IBE scheme.

4.2 Security Proof for the Scheme

The following theorem addresses the security of the scheme. The proof proceeds in a similar manner as in [Yam16], but we incorporate several novel ideas as we explained in Sec. 2.

Theorem 2. *The above IBE scheme is adaptively-anonymous secure assuming* $\mathsf{RLWE}_{n,k+1,q,D^{\mathsf{coeff}}_{\mathbb{Z}^n,\alpha q}}$ *is hard, where the ciphertext space is* $\mathcal{C} = R_q \times R_q^{2k}$.

Proof. Let $\mathcal{A}$ be a PPT adversary that breaks the adaptively-anonymous security of the scheme. In addition, let $\epsilon = \epsilon(n)$ and $Q = Q(n)$ be its advantage and the upper bound of the number of key extraction queries, respectively.

Since $\mathcal{A}$ is PPT and λ and n are polynomially related (namely, $n = O(\lambda^\delta)$ for some constant δ), there exists a constant number $c_1 \in \mathbb{N}$ such that $4(dQ+1) \leq n^{c_1}$ for all n that are sufficiently large. Similarly, since $\mathcal{A}$ breaks the security of the scheme, there exists $c_2 \in \mathbb{N}$ such that $2\epsilon \geq n^{-c_2}$ holds for infinitely many n. By setting $c = c_1 + c_2$, we have that

$$4dQ \leq n^c \text{ for all } n \in \mathbb{N} \quad \text{and} \quad \frac{\epsilon}{2(dQ+1)} \geq \frac{1}{n^c} \quad \text{for infinitely many } n \in \mathbb{N}. \tag{8}$$

In the proof, we will assume $d(c-1) < n$. Since both c and d are constant numbers, this holds for sufficiently large n.

We show the security of the scheme via the following games. In each game, a value $\mathsf{coin}' \in \{0,1\}$ is defined. While it is set $\mathsf{coin}' = \widehat{\mathsf{coin}}$ in the first game, these values might be different in the later games. In the following, we define X_i to be the event that $\mathsf{coin}' = \mathsf{coin}$.

Game_0 : This is the real security game. In the challenge phase, the challenge ciphertext is set as $C^\star = (c_0, \boldsymbol{c}_1) \xleftarrow{\$} R_q \times R_q^{2k}$ if $\mathsf{coin} = 1$. Otherwise, it is set as $C^\star \leftarrow \mathsf{Encrypt}(\mathsf{mpk}, \mathsf{ID}, \mathsf{M})$, where M is the message chosen by $\mathcal{A}$. At the end of the game, $\mathcal{A}$ outputs a guess $\widehat{\mathsf{coin}}$ for coin. Finally, the challenger sets $\mathsf{coin}' = \widehat{\mathsf{coin}}$. By definition, we have

$$\left|\Pr[X_0] - \frac{1}{2}\right| = \left|\Pr[\mathsf{coin}' = \mathsf{coin}] - \frac{1}{2}\right| = \left|\Pr[\widehat{\mathsf{coin}} = \mathsf{coin}] - \frac{1}{2}\right| = \epsilon.$$

Game_1 : For integers $t_0, t_1 \in \mathbb{Z}$ such that $t_0 \leq t_1$ and positive integer $c \in \mathbb{N}$, let us denote $[t_0, t_1]_{R,c}$ as

$$[t_0, t_1]_{R,c} := \left\{ \sum_{i=0}^{c-1} a_i X^i \;\middle|\; a_i \in [t_0, t_1] \text{ for all } i \in [0, c-1] \right\} \subseteq R.$$

In words, $[t_0, t_1]_{R,c}$ denotes the set of polynomials of degree less then $c-1$ with all of its coefficients in the interval $[t_0, t_1]$. Note that c is the constant defined in Eq.(8). In this game, we change Game_0 so that the challenger performs the following additional step at the end of the game. First, the challenger picks $\boldsymbol{y} = (y_0, \{y_{i,j}\}_{(i,j)\in[d,\ell]})$ as

$$y_0 \xleftarrow{\$} [-\kappa(cn)^d, -1]_{R,(c-1)d+1} \qquad \text{and} \qquad y_{i,j} \xleftarrow{\$} [1, n]_{R,c} \tag{9}$$

for $(i,j) \in [d] \times [\ell]$. Recall κ is the length of the identities. We then define a function $\mathsf{F}_{\boldsymbol{y}} : \mathcal{ID} \to R_q$ as follows:

$$\mathsf{F}_{\boldsymbol{y}}(\mathsf{ID}) = y_0 + \sum_{(j_1,\ldots,j_d)\in S(\mathsf{ID})} y_{1,j_1} \cdots y_{d,j_d}.$$

Then the challenger checks whether the following condition holds:

$$\mathsf{F}_{\boldsymbol{y}}(\mathsf{ID}^\star) = 0 \ \wedge \ \mathsf{F}_{\boldsymbol{y}}(\mathsf{ID}_1) \in R_q^* \ \wedge \ \cdots \ \wedge \ \mathsf{F}_{\boldsymbol{y}}(\mathsf{ID}_Q) \in R_q^*, \tag{10}$$

where $\mathsf{ID}^\star$ is the challenge identity, and $\mathsf{ID}_1, \ldots, \mathsf{ID}_Q$ are identities for which $\mathcal{A}$ has made key extraction queries. If it does not hold, the challenger ignores the output $\widehat{\mathsf{coin}}$ of $\mathcal{A}$, and sets $\mathsf{coin}' \xleftarrow{\$} \{0,1\}$. In this case, we say that the challenger aborts. If condition (10) holds, the challenger sets $\mathsf{coin}' = \widehat{\mathsf{coin}}$. As we will show in Lemma 11, we have

$$\left|\Pr[X_1] - \frac{1}{2}\right| \geq \frac{1}{(\kappa c^d n^d)^{(c-1)d+1}} \left(\frac{\epsilon}{2} - \frac{dQ}{n^c}\right).$$

So as not to interrupt the proof of Theorem 2, we intentionally skip the proof for the time being.

Game_2 : In this game, we change the way $\boldsymbol{b}_0$ and $\boldsymbol{b}_{i,j}$ are chosen. At the beginning of the game, the challenger picks $\boldsymbol{R}_0, \boldsymbol{R}_{i,j} \xleftarrow{\$} [-\rho,\rho]_R^{k\times k}$ for $(i,j) \in [d] \times [\ell]$. It also picks $\boldsymbol{y}$ as in Game_1. Then, $\boldsymbol{a}$, $\boldsymbol{b}_0$, and $\boldsymbol{b}_{i,j}$ are defined as

$$\boldsymbol{b}_0 = \boldsymbol{a}\boldsymbol{R}_0 + y_0\boldsymbol{g}_b, \qquad \boldsymbol{b}_{i,j} = \boldsymbol{a}\boldsymbol{R}_{i,j} + y_{i,j}\boldsymbol{g}_b, \tag{11}$$

for $(i,j) \in [d] \times [\ell]$. The rest of the game is the same as in Game_1.
Now, we bound $|\Pr[X_2] - \Pr[X_1]|$. By Lemma 4, the distributions

$$\left(\boldsymbol{a}, \boldsymbol{a}\boldsymbol{R}_0 + y_0\boldsymbol{g}_b, \{\boldsymbol{a}\boldsymbol{R}_{i,j} + y_{i,j}\boldsymbol{g}_b\}_{(i,j)\in[d]\times[\ell]}\right) \ \text{ and } \ \left(\boldsymbol{a}, \boldsymbol{b}_0, \{\boldsymbol{b}_{i,j}\}_{(i,j)\in[d]\times[\ell]}\right)$$

are $\mathsf{negl}(n)$-close, where $\boldsymbol{b}_0, \boldsymbol{b}_{i,j} \xleftarrow{\$} R_q^k$. Thus, we have $|\Pr[X_1] - \Pr[X_2]| = \mathsf{negl}(n)$.

Game_3 Recall that in the previous game, the challenger aborts at the end of the game if condition (10) is not satisfied. In this game, we change the game so that the challenger aborts as soon as the abort condition becomes true. Since this is only a conceptual change, we have $\Pr[X_2] = \Pr[X_3]$.

Before describing the next game, we define $\boldsymbol{R}_{\mathsf{ID}} \in R^{k\times k}$ for an identity $\mathsf{ID} \in \mathcal{ID}$ as

$$\boldsymbol{R}_{\mathsf{ID}} = \boldsymbol{R}_0 + \sum_{(j_1,\ldots,j_d)\in S(\mathsf{ID})} \mathsf{TrapEval}_d(\boldsymbol{R}_{1,j_1}, \ldots, \boldsymbol{R}_{d,j_d}, y_{1,j_1}, \ldots, y_{d,j_d}). \tag{12}$$

Note that by the definition of $\boldsymbol{R}_{\mathsf{ID}}$, $\mathsf{H}(\mathsf{ID})$, $\mathsf{PubEval}$ and $\mathsf{TrapEval}$ (Lemma 6) we have

$$\mathsf{H}(\mathsf{ID}) = \boldsymbol{b}_0 + \sum_{(j_1,\ldots,j_d)\in S(\mathsf{ID})} \mathsf{PubEval}_d(\boldsymbol{b}_{1,j_1}\boldsymbol{b}_{2,j_2}, \ldots, \boldsymbol{b}_{d,j_d})$$

$$= \boldsymbol{a}\boldsymbol{R}_{\mathsf{ID}} + \mathsf{F}_{\boldsymbol{y}}(\mathsf{ID})\boldsymbol{g}_b. \tag{13}$$

Since $\boldsymbol{R}_0, \boldsymbol{R}_{i,j} \xleftarrow{\$} [-\rho, \rho]_R^{k\times k}$, from Lemma 2 we have $s_1(\boldsymbol{R}_0), s_1(\boldsymbol{R}_{i,j}) \le B$ with all but negligible probability where $B = C' \cdot \rho\sqrt{n}(\sqrt{k} + \omega(\sqrt{\log n}))$ for some positive absolute constant C'. Furthermore, we have $\|y_{i,j}\|_1 \le cn$ from Eq. (9). Therefore by Lemma 6, we have

$$\begin{aligned} s_1(\boldsymbol{R}_{\mathsf{ID}}) &\le s_1(\boldsymbol{R}_0) + \sum_{(j_1,\ldots,j_d)\in S(\mathsf{ID})} s_1(\mathsf{TrapEval}_d(\boldsymbol{R}_{1,j_1},\ldots,\boldsymbol{R}_{d,j_d}, y_{1,j_1},\ldots,y_{d,j_d})) \\ &\le B\left(1 + \kappa(cn)^{d-1} + \kappa bnk\frac{(cn)^{d-1}-1}{cn-1}\right), \end{aligned} \tag{14}$$

for any $\mathsf{ID} \in \mathcal{ID}$ with all but negligible probability.

Game_4 In this game, we change the way the vector $\boldsymbol{a}$ is sampled. Namely, Game_4 challenger picks $\boldsymbol{a} \xleftarrow{\$} R_q^k$ instead of generating it with a trapdoor. By Lemma 5, this makes only negligible difference. Furthermore, we also change the way the key extraction queries are answered. When $\mathcal{A}$ makes a key extraction query for an identity ID, the challenger first computes $\boldsymbol{R}_{\mathsf{ID}}$ as in Eq.(12). It aborts if $\mathsf{F}_{\boldsymbol{y}}(\mathsf{ID}) \notin R_q^*$ as in the previous game and runs

$$\mathsf{SampleRight}(\boldsymbol{a}, \boldsymbol{g}_b, \boldsymbol{R}_{\mathsf{ID}}, \mathsf{F}_{\mathbf{y}}(\mathsf{ID}), u, \mathbf{T}_{\boldsymbol{g}_b}, \sigma) \to \boldsymbol{e},$$

otherwise. Note that in the previous game the private key was sampled as

$$\mathsf{SampleLeft}(\boldsymbol{a}, \mathsf{H}(\mathsf{ID}), u, \mathbf{T}_{\boldsymbol{a}}, \sigma) \to \boldsymbol{e}.$$

By Eq.(14) and for our choice of σ, the output distribution of $\mathsf{SampleRight}$ is $\mathsf{negl}(n)$-close to $D^{\mathsf{coeff}}_{\Lambda^{\perp}_{\phi(u)}([\mathrm{rot}(\boldsymbol{a}^T)^T | \mathrm{rot}(\mathsf{H}(\mathsf{ID})^T)^T]),\sigma}$. Furthermore, by the choice of σ, this distribution is $\mathsf{negl}(n)$-close to the output distribution of $\mathsf{SampleLeft}$. Therefore, the above change alters the view of $\mathcal{A}$ only negligibly. Thus, we have $|\Pr[X_3] - \Pr[X_4]| = \mathsf{negl}(n)$.

Game_5 : In this game, we change the way the challenge ciphertext is created when $\mathsf{coin} = 0$. Recall in the previous games when $\mathsf{coin} = 0$, we created a valid challenge ciphertext as in the real scheme. If $\mathsf{coin} = 0$ and $\mathsf{F}_{\boldsymbol{y}}(\mathsf{ID}^\star) = 0$ (i.e., if it does not abort), to create the challenge ciphertext Game_5 challenger first picks $s \xleftarrow{\$} R_q$ and $\boldsymbol{x} \xleftarrow{\$} (D^{\mathsf{coeff}}_{\mathbb{Z}^n,\alpha q})^k$ and computes $\boldsymbol{v} = s\boldsymbol{a} + \boldsymbol{x} \in R^k$. It then runs the algorithm

$$\mathsf{ReRand}\left(\mathrm{rot}([\boldsymbol{I}_k | \boldsymbol{R}_{\mathsf{ID}^\star}]), \phi(\boldsymbol{v}), \alpha q, \frac{\alpha'}{2\alpha q}\right) \to \mathbf{c} \in \mathbb{Z}_q^{2nk}$$

from Lemma 1, where $\boldsymbol{I}_k \in R^{k\times k}$ is the identity matrix of size $k \times k$. Finally, it picks $x_0 \xleftarrow{\$} D^{\mathsf{coeff}}_{\mathbb{Z}^n,\alpha q}$ and sets the challenge ciphertext as

$$C^\star = \left(c_0 = v_0 + \lfloor q/2 \rceil \cdot \mathsf{M},\ \boldsymbol{c}_1 = \phi^{-1}(\mathbf{c}) \right) \in R_q \times R_q^{2k}, \tag{15}$$

where $v_0 = su + x_0$ and M is the message chosen by $\mathcal{A}$. We claim that this change alters the view of $\mathcal{A}$ only negligibly. To show this, observe that the input to ReRand is $\mathrm{rot}\big([\boldsymbol{I}_k|\boldsymbol{R}_{\mathsf{ID}^\star}]\big) \in \mathbb{Z}_q^{nk\times 2nk}$ and

$$\phi(\boldsymbol{v}) = \phi(s\boldsymbol{a}+\boldsymbol{x}) = \phi(s)\mathrm{rot}(\boldsymbol{a}) + \phi(\boldsymbol{x}) \in \mathbb{Z}_q^{nk},$$

where $\phi(\boldsymbol{x})$ is distributed as $\phi(\boldsymbol{x}) \xleftarrow{\$} D_{\mathbb{Z}^{nk},\alpha q}$. Therefore, by the property of ReRand and our choice of α and α', the output $\mathbf{c} \in \mathbb{Z}_q^{2nk}$ is

$$\begin{aligned}\mathbf{c} &= \Big(\phi(s)\mathrm{rot}(\boldsymbol{a})\Big)\cdot \mathrm{rot}\big([\boldsymbol{I}_k|\boldsymbol{R}_{\mathsf{ID}^\star}]\big) + \mathbf{x}' \\ &= \phi(s)\cdot \mathrm{rot}\big([\boldsymbol{a}|\mathsf{H}(\mathsf{ID}^\star)]\big) + \mathbf{x}' \\ &= \phi\big(s\big[\boldsymbol{a}|\mathsf{H}(\mathsf{ID}^\star)\big]\big) + \mathbf{x}',\end{aligned}$$

where the distribution of $\mathbf{x}'$ is within negligible distance from $\mathbf{x}' \xleftarrow{\$} D_{\mathbb{Z}^{2nk},\alpha'}$ due to Lemma 1. Here, we use the fact that $\mathsf{H}(\mathsf{ID}^\star) = \boldsymbol{a}\boldsymbol{R}_{\mathsf{ID}^\star}$ holds since $\mathsf{F}_{\boldsymbol{y}}(\mathsf{ID}^\star) = 0$. It can be readily seen that the distribution of $\boldsymbol{c}_1 = \phi^{-1}(\mathbf{c})$ in Game_5 is statistically close to that in Game_4. Therefore, we conclude that $|\Pr[X_4] - \Pr[X_5]| = \mathsf{negl}(n)$.

Game_6 In this game, we change the way the challenge ciphertext is created when $\mathsf{coin} = 0$. If $\mathsf{coin} = 0$ and the abort condition is not satisfied, to create the challenge ciphertext for identity $\mathsf{ID}^\star$ and message M, Game_6 challenger first picks $v_0 \xleftarrow{\$} R_q$, $\boldsymbol{v}' \xleftarrow{\$} R_q^k$ and $\boldsymbol{x} \xleftarrow{\$} (D^{\mathsf{coeff}}_{\mathbb{Z}^n,\alpha q})^k$, and runs

$$\mathsf{ReRand}\left(\mathrm{rot}\big([\boldsymbol{I}_k|\boldsymbol{R}_{\mathsf{ID}^\star}]\big), \phi(\boldsymbol{v}), \alpha q, \frac{\alpha'}{2\alpha q}\right) \to \mathbf{c} \in \mathbb{Z}_q^{2nk}, \tag{16}$$

where $\boldsymbol{v} = \boldsymbol{v}' + \boldsymbol{x}$. Then, the challenge ciphertext is set as in Eq.(15). As we will show in Lemma 12, assuming $\mathsf{RLWE}_{n,k+1,q,D^{\mathsf{coeff}}_{\mathbb{Z}^n,\alpha q}}$ is hard, we have $|\Pr[X_5] - \Pr[X_6]| = \mathsf{negl}(n)$.

Game_7 In this game, we further change the way the challenge ciphertext is created. When $\mathsf{coin} = 0$ and the abort condition is not satisfied, the challenge ciphertext for $\mathsf{ID}^\star$ is created as

$$C^\star = (\ c_0 = v_0 + \lfloor q/2\rceil \cdot \mathsf{M},\ \boldsymbol{c}_1 = [\boldsymbol{v}'|\boldsymbol{v}'\boldsymbol{R}_{\mathsf{ID}^\star}] + [\boldsymbol{x}_1|\boldsymbol{x}_2]\ ) \in R_q \times R^{2k},$$

where $v_0 \xleftarrow{\$} R_q$, $\boldsymbol{v}' \xleftarrow{\$} R_q^k$ and $\boldsymbol{x}_1, \boldsymbol{x}_2 \xleftarrow{\$} (D^{\mathsf{coeff}}_{\mathbb{Z}^n,\alpha'})^k$.
We claim that this change alters the view of $\mathcal{A}$ only negligibly. This can be seen by a similar argument to that we made in the step from Game_3 to Game_4. We first observe that in Game_6 the input to ReRand is $\mathrm{rot}\big([\boldsymbol{I}_k|\boldsymbol{R}_{\mathsf{ID}^\star}]\big) \in \mathbb{Z}_q^{nk\times 2nk}$ and

$$\phi(\boldsymbol{v}) = \phi(\boldsymbol{v}' + \boldsymbol{x}) = \phi(\boldsymbol{v}') + \phi(\boldsymbol{x}) \in \mathbb{Z}_q^{nk}, \tag{17}$$

where $\phi(\boldsymbol{x})$ is distributed as $D_{\mathbb{Z}^{nk},\alpha q}$. Therefore, the output $\mathbf{c} \in \mathbb{Z}_q^{2nk}$ of ReRand is

$$\mathbf{c} = \phi(\boldsymbol{v}')\cdot \mathrm{rot}\big([\boldsymbol{I}_k|\boldsymbol{R}_{\mathsf{ID}^\star}]\big) + \mathbf{x}' = \phi\big([\boldsymbol{v}'|\boldsymbol{v}'\boldsymbol{R}_{\mathsf{ID}^\star}]\big) + \mathbf{x}',$$

where the distribution of $\mathbf{x}'$ is within negligible distance from $\mathbf{x}' \xleftarrow{\$} D_{\mathbb{Z}^{2nk},\alpha'}$ due to Lemma 1. Hence, the distribution of $\boldsymbol{c}_1 = \phi^{-1}(\mathbf{c})$ in Game_6 is statistically close to that in Game_7. Therefore, we have $|\Pr[X_6] - \Pr[X_7]| = \mathsf{negl}(n)$.

Game_8 In this game, we change the way the key extraction queries are answered. Instead of running $\mathsf{SampleLeft}$ or $\mathsf{SampleRight}$, the (possibly inefficient) challenger directly picks a secret key $\mathsf{sk}_{\mathsf{ID}}$ for identity ID as $\mathsf{sk}_{\mathsf{ID}} \xleftarrow{\$} D^{\mathsf{coeff}}_{\Lambda^{\perp}_{\phi(u)}([\mathrm{rot}(\boldsymbol{a}^T)^T|\mathrm{rot}(\mathsf{H}(\mathsf{ID})^T)^T]),\sigma}$ without using $\boldsymbol{R}_{\mathsf{ID}}$. Similarly to the change from Game_3 to Game_4, by the choice of σ and Eq.(14), this alters the view of $\mathcal{A}$ only negligibly. Therefore, we have $|\Pr[X_7] - \Pr[X_8]| = \mathsf{negl}(n)$. Note that this is only a conceptual game in order to get rid of any (negligible) correlation between the secret key and $\boldsymbol{R}_{\mathsf{ID}}$ so as not to interfere with the statistical argument using $\boldsymbol{R}_{\mathsf{ID}^\star}$ in the following game.

Game_9 In this game, we change the challenge ciphertext to be a random vector, regardless of whether $\mathsf{coin} = 0$ or $\mathsf{coin} = 1$. Namely, Game_9 challenger generates the challenge ciphertext $C^\star = (c_0, \boldsymbol{c}_1)$ as

$$c_0 \xleftarrow{\$} R_q, \qquad \text{and} \qquad \boldsymbol{c}_1 \xleftarrow{\$} R_q^{2k}.$$

We now proceed to bound $|\Pr[X_8] - \Pr[X_9]|$. Since Game_8 and Game_9 differ only in the creation of the challenge ciphertext when $\mathsf{coin} = 0$, we focus on this case. First, it is easy to see that c_0 is uniformly random over R_q in both of Game_8 and Game_9. Therefore, we only need to show that the distribution of $\boldsymbol{c}_1$ in Game_8 is $\mathsf{negl}(n)$-close to the uniform distribution over R_q^{2k}. To see this, it suffices to show that $[\boldsymbol{v}'|\boldsymbol{v}'\boldsymbol{R}_{\mathsf{ID}^\star}]$ is distributed statistically close to the uniform distribution over R_q^{2k}. First, observe that the following distributions are $\mathsf{negl}(n)$-close:

$$(\boldsymbol{a}, \boldsymbol{a}\boldsymbol{R}_0, \boldsymbol{v}', \boldsymbol{v}'\boldsymbol{R}_0) \approx (\boldsymbol{a}, \boldsymbol{a}', \boldsymbol{v}', \boldsymbol{v}'') \approx (\boldsymbol{a}, \boldsymbol{a}\boldsymbol{R}_0, \boldsymbol{v}', \boldsymbol{v}''), \tag{18}$$

where $\boldsymbol{a}, \boldsymbol{a}' \xleftarrow{\$} R_q^k$, $\boldsymbol{R}_0 \xleftarrow{\$} [-\rho, \rho]_R^{k\times k}$, $\boldsymbol{v}', \boldsymbol{v}'' \xleftarrow{\$} R_q^k$. It can be seen that the first and the second distributions are $\mathsf{negl}(n)$-close, by applying Lemma 4 for $[\boldsymbol{a}; \boldsymbol{v}'] \in R_q^{2\times k}$ and $\boldsymbol{R}_0$. It can also be seen that the second and the third distributions are $\mathsf{negl}(n)$-close, by applying the same lemma for $\boldsymbol{a}$ and $\boldsymbol{R}_0$. From the above, the following distributions are statistically close:

$$\begin{aligned}
&(\boldsymbol{a}, \boldsymbol{a}\boldsymbol{R}_0, \boldsymbol{v}', \boldsymbol{v}'\boldsymbol{R}_{\mathsf{ID}^\star}) \\
&= (\boldsymbol{a}, \boldsymbol{a}\boldsymbol{R}_0, \boldsymbol{v}', \boldsymbol{v}'(\boldsymbol{R}_0 + \boldsymbol{R}'_{\mathsf{ID}^\star})) \\
&\approx (\boldsymbol{a}, \boldsymbol{a}\boldsymbol{R}_0, \boldsymbol{v}', \boldsymbol{v}'' + \boldsymbol{v}'\boldsymbol{R}'_{\mathsf{ID}^\star}) \\
&\approx (\boldsymbol{a}, \boldsymbol{a}\boldsymbol{R}_0, \boldsymbol{v}', \boldsymbol{v}'')
\end{aligned}$$

where $\boldsymbol{a}, \boldsymbol{a}' \xleftarrow{\$} R_q^k$, $\boldsymbol{R}_0 \xleftarrow{\$} [-\rho, \rho]_R^{k\times k}$, $\boldsymbol{v}', \boldsymbol{v}'' \xleftarrow{\$} R_q^k$, and

$$\boldsymbol{R}'_{\mathsf{ID}^\star} := \sum_{(j_1,\ldots,j_d)\in S(\mathsf{ID})} \mathsf{TrapEval}_d(\boldsymbol{R}_{1,j_1}, \ldots, \boldsymbol{R}_{d,j_d}, y_{1,j_1}, \ldots, y_{d,j_d}).$$

The second and the third distributions above are $\mathsf{negl}(n)$-close by Eq.(18). Note that we intentionally ignored all the $\boldsymbol{a}\boldsymbol{R}_{i,j}$ terms to keep the argument

simple, since focusing on the $\boldsymbol{a}\boldsymbol{R}_0$ term is enough to prove randomness of $[\boldsymbol{v}'|\boldsymbol{v}'\boldsymbol{R}_{\mathsf{ID}^\star}]$. Therefore, we conclude that $|\Pr[X_8] - \Pr[X_9]| = \mathsf{negl}(n)$.

Analysis. From the above, we have

$$\begin{aligned}\left|\Pr[X_9] - \frac{1}{2}\right| &= \left|\Pr[X_1] - \frac{1}{2} + \sum_{i=1}^{8}(\Pr[X_{i+1}] - \Pr[X_i])\right| \\ &\geq \left|\Pr[X_1] - \frac{1}{2}\right| - \sum_{i=1}^{8}|\Pr[X_{i+1}] - \Pr[X_i]| \\ &\geq \frac{1}{(\kappa c^d n^d)^{(c-1)d+1}}\left(\frac{\epsilon}{2} - \frac{dQ}{n^c}\right) - \mathsf{negl}(n) \\ &= \frac{1}{\mathsf{poly}(n)}\left(\frac{\epsilon}{2} - \frac{dQ}{n^c}\right) - \mathsf{negl}(n) \end{aligned} \tag{19}$$

where the last equality follows from the facts that c and d are constants and $\kappa = \mathsf{poly}(n)$. Since the challenge ciphertext is independent from the value of coin in Game_9, we have $\Pr[X_9] = 1/2$ and thus $|\Pr[X_9] - 1/2| = 0$. Therefore, we have that $\epsilon/2 - dQ/n^c$ is negligible. However, by Eq.(8),

$$\frac{\epsilon}{2} - \frac{dQ}{n^c} \geq \frac{dQ+1}{n^c} - \frac{dQ}{n^c} = \frac{1}{n^c}$$

holds for infinitely many n, which is a contradiction.

To complete the proof of Theorem 2, it remains to prove Lemma 11 and 12.

Lemma 11. *For any PPT adversary $\mathcal{A}$, we have*

$$\left|\Pr[X_1] - \frac{1}{2}\right| \geq \frac{1}{(\kappa c^d n^d)^{(c-1)d+1}}\left(\frac{\epsilon}{2} - \frac{dQ}{n^c}\right).$$

Proof. For a sequence of identities $\mathbb{ID} = (\mathsf{ID}^\star, \mathsf{ID}_1, \ldots, \mathsf{ID}_Q) \in \mathcal{ID}^{Q+1}$, we define $\gamma(\mathbb{ID})$ as

$$\gamma(\mathbb{ID}) = \Pr_{\boldsymbol{y}}[\mathsf{F}_{\boldsymbol{y}}(\mathsf{ID}^\star) = 0 \wedge \mathsf{F}_{\boldsymbol{y}}(\mathsf{ID}_1) \neq 0 \wedge \mathsf{F}_{\boldsymbol{y}}(\mathsf{ID}_2) \neq 0 \wedge \cdots \wedge \mathsf{F}_{\boldsymbol{y}}(\mathsf{ID}_Q) \neq 0]$$

where the probability is taken over $\boldsymbol{y} = (y_0, \{y_{i,j}\}_{(i,j)\in[d,\ell]})$, which is chosen as specified in Game_1. Then, it suffices to show

$$\frac{1}{(\kappa c^d n^d)^{(c-1)d+1}}\left(1 - \frac{2dQ}{n^c}\right) \leq \gamma(\mathbb{ID}) \leq \frac{1}{(\kappa c^d n^d)^{(c-1)d+1}} \tag{20}$$

since by Lemma 8, this implies

$$\left|\Pr[X_1] - \frac{1}{2}\right|$$

$$
\begin{aligned}
&\geq \frac{\epsilon}{(\kappa c^d n^d)^{(c-1)d+1}}\left(1-\frac{2dQ}{n^c}\right)-\frac{1}{2(\kappa c^d n^d)^{(c-1)d+1}}\left(1-\left(1-\frac{2dQ}{n^c}\right)\right)\\
&=\frac{1}{(\kappa c^d n^d)^{(c-1)d+1}}\left(\epsilon\left(1-\frac{2dQ}{n^c}\right)-\frac{dQ}{n^c}\right)\\
&\geq \frac{1}{(\kappa c^d n^d)^{(c-1)d+1}}\left(\frac{\epsilon}{2}-\frac{dQ}{n^c}\right)
\end{aligned}
$$

where the last inequality follows from Eq.(8). In the following, we will prove Eq.(20) by applying Lemma 9. We set

$$
\begin{aligned}
&\nu=2,\ \mu=d\ell && \Phi=R_q,\\
&\Omega_j=R_q/\langle t_j\rangle, && \pi_j: R_q\to R_q/\langle t_j\rangle, \quad \text{for } j\in[2],\\
&S_0=[-\kappa(cn)^d,-1]_{R,(c-1)d+1}, && S_1=[1,n]_{R,c}
\end{aligned}
$$

where π_j is a natural homomorphism and t_1, t_2 are elements in R_q as defined in Lemma 3. Therefore, the map $\mathit{\Pi}: \Phi \ni y \mapsto (\pi_1(y), \pi_2(y)) \in \Omega_1 \times \Omega_2$ is an isomorphism. We define $f_i(\{Y_{j,j'}\}_{(j,j')\in[d]\times[\ell]})$ for $i \in [0, Q]$ as

$$
f_i\left(\{Y_{j,j'}\}_{(j,j')\in[d]\times[\ell]}\right)=\sum_{(j'_1,\ldots,j'_d)\in S(\mathsf{ID}_i)} Y_{1,j'_1}Y_{2,j'_2}\cdots Y_{d,j'_d}
$$

where we define $\mathsf{ID}_0 := \mathsf{ID}^\star$. Note that we have $\mathsf{F}_{\boldsymbol{y}}(\mathsf{ID}_i) = y_0 + f_i(\{y_{i,j}\}_{(i,j)\in[d]\times[\ell]})$. We now check that the three conditions for Lemma 9 hold.

- We prove that π_j is injective on S_1 for $j \in \{1, 2\}$. Assume for contradiction that there are $a_1, a_2 \in S_1$ with $a_1 \neq a_2$ and $\pi_j(a_1) = \pi_j(a_2) \Leftrightarrow \pi_j(a_1 - a_2) = 0$. We then have $a_1 - a_2 \notin R_q^*$. On the other hand, we have $\|\phi(a_1 - a_2)\|_2 \leq \sqrt{cn} < \sqrt{q}$. However, this contradicts Lemma 3.
- For $i \in [1, Q]$, we have

$$
\begin{aligned}
&f_0\left(\{Y_{j,j'}\}\right)-f_i\left(\{Y_{j,j'}\}\right)\\
=&\sum_{(j'_1,\ldots,j'_d)\in S(\mathsf{ID}^\star)} Y_{1,j'_1}Y_{2,j'_2}\cdots Y_{d,j'_d}-\sum_{(j'_1,\ldots,j'_d)\in S(\mathsf{ID}_i)} Y_{1,j'_1}Y_{2,j'_2}\cdots Y_{d,j'_d}.
\end{aligned}
$$

  Since $\mathsf{ID}^\star \neq \mathsf{ID}_i$ and S is an injective map, we have $S(\mathsf{ID}^\star) \neq S(\mathsf{ID}_i)$. Therefore, there exists $(j_1^\star, \ldots, j_d^\star) \in [\ell]^d$ such that $(j_1^\star, \ldots, j_d^\star) \in S(\mathsf{ID}^\star) \triangle S(\mathsf{ID}_i)$, where $S(\mathsf{ID}^\star) \triangle S(\mathsf{ID}_i)$ denotes the symmetric difference of $S(\mathsf{ID}^\star)$ and $S(\mathsf{ID}_i)$. Thus, the above polynomial is a non-zero polynomial with degree d. Since the coefficients of $f_0 - f_i$ are all in $\{-1, 0, 1\}$ and $\pi_j(\pm 1) = \pm 1$, $\pi_j(f_0 - f_i)$ is a non-zero polynomial for $j \in \{1, 2\}$ as well.
- We prove $S_0 \supseteq \{-f_i(\{y_{j,j'}\}_{(j,j')\in[d]\times[\ell]}) | y_{1,1}, \ldots, y_{d,\ell} \in S_1\}$ for all $i \in [0, Q]$. By our assumption $d(c - 1) < n$ and by regarding elements $y_{j,j'}$ as polynomials in $\mathbb{Z}[X]/(X^n + 1)$ with degree $c - 1$, we have $f_i(\{y_{j,j'}\})$ are all in $[*, *]_{R,d(c-1)+1}$ where $*$ represents some integer. It then suffices to show $\|\phi(f_i(\{y_{j,j'}\}_{(j,j')\in[d]\times[\ell]}))\|_\infty \leq \kappa(cn)^d$. For any $\{y_{j,j'}\}_{(j,j')\in[d]\times[\ell]}$, we have

$$
\|\phi(f_i(\{y_{j,j'}\}_{(j,j')\in[d]\times[\ell]}))\|_\infty
$$

$$= \left\| \phi \left(\sum_{(j'_1,\ldots,j'_d)\in S(\mathsf{ID}_i)} y_{1,j'_1} y_{2,j'_2} \cdots y_{d,j'_d} \right) \right\|_\infty \tag{21}$$

$$= \left\| \sum_{(j'_1,\ldots,j'_d)\in S(\mathsf{ID}_i)} \phi(y_{1,j'_1} y_{2,j'_2} \cdots y_{d,j'_d}) \right\|_\infty \tag{22}$$

$$\leq \sum_{(j'_1,\ldots,j'_d)\in S(\mathsf{ID}_i)} \left\| \phi(y_{1,j'_1} y_{2,j'_2} \cdots y_{d,j'_d}) \right\|_\infty \tag{23}$$

$$\leq \kappa(cn)^d \tag{24}$$

where Eq.(21) follows from the definition, Eq.(22) holds because ϕ^{-1} is a homomorphism, Eq.(23) is from the triangle inequality, and Eq.(24) is from Lemma 7 and the fact that $\|y_{j,j'}\|_\infty \leq n$.

This completes the proof of Lemma 11.

Lemma 12. *For any PPT adversary $\mathcal{A}$, there exists another PPT adversary $\mathcal{B}$ such that*

$$|\Pr[X_5] - \Pr[X_6]| \leq \mathsf{Adv}^{\mathsf{RLWE}_{n,k+1,q,D^{\mathsf{coeff}}_{\mathbb{Z}^n,\alpha q}}}_{\mathcal{B}}.$$

In particular, we have $|\Pr[X_5] - \Pr[X_6]| = \mathsf{negl}(n)$ under the $\mathsf{RLWE}_{n,k+1,q,D^{\mathsf{coeff}}_{\mathbb{Z}^n,\alpha q}}$ assumption,.

We omit the proof here. It is a standard proof where we convert the adversary distinguishing Game_5 from Game_6 into another adversary against the RLWE assumption. This is accomplished by noticing that the trapdoor information for $\boldsymbol{a}$ nor (secret) randomness used to create the ciphertext is no longer required to simulate the challengers in Game_5 and Game_6.

5 Construction from Bilinear Maps

In the following, we present our IBE scheme from bilinear maps. Here, for simplicity, we present the scheme with only single-bit message space. A variant of our scheme that can deal with longer message space will appear in the full version. Let the identity space of the scheme be $\mathcal{ID} = \{0,1\}^\kappa$ for some $\kappa \in \mathbb{N}$. For our construction, we consider an efficiently computable injective map S that maps an identity $\mathsf{ID} \in \{0,1\}^\kappa$ to a subset $S(\mathsf{ID})$ of $[1,\ell] \times [1,\ell]$, where $\ell = \lceil\sqrt{\kappa}\rceil$. We would typically set $\kappa = O(\lambda)$, and thus $\ell = O(\sqrt{\lambda})$ in such a case. We also use $\mathsf{GL}(\mathsf{K},\mathsf{rand})$ to denote the Goldreich-Levin hardcore bit [GL89] of K using randomness rand. Recall that $\mathsf{GL}(\mathsf{K},\mathsf{rand})$ is the bitwise inner product between K and rand.

$\mathsf{Setup}(1^\lambda)$: On input 1^λ, it chooses an asymmetric bilinear group $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ with efficiently computable map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ of prime order $p =$

$p(\lambda)$. Let g and h be generators of $\mathbb{G}_1$ and $\mathbb{G}_2$ respectively. It then picks $w_0, w_{1,1}, \ldots, w_{1,\ell}, w_{2,1}, \ldots, w_{2,\ell}, \alpha, \beta \xleftarrow{\$} \mathbb{Z}_p$ and $\mathsf{rand} \xleftarrow{\$} \{0,1\}^{|\mathbb{G}_T|}$. It finally outputs

$$\mathsf{mpk} = (g, W_0 = g^{w_0}, \{W_{1,i} = g^{w_{1,i}}\}_{i=1}^{\ell}, \{W_{2,i} = g^{w_{2,i}}\}_{i=1}^{\ell}, g^{\alpha}, h^{\beta}, \mathsf{rand}) \quad \text{and}$$
$$\mathsf{msk} = (h, \alpha, \beta, w_0, w_{1,1}, \ldots, w_{1,\ell}, w_{2,1}, \ldots, w_{2,\ell})$$

In the following, we use a deterministic function $\mathsf{H} : \mathcal{ID} \to \mathbb{Z}_p$ that is defined as follows.

$$\mathsf{H}(\mathsf{ID}) = w_0 + \sum_{(i,j) \in S(\mathsf{ID})} w_{1,i} w_{2,j} \in \mathbb{Z}_p.$$

$\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{ID})$: It first computes $\mathsf{H}(\mathsf{ID})$ using msk and picks $r \xleftarrow{\$} \mathbb{Z}_p$. It then returns

$$\mathsf{sk}_{\mathsf{ID}} = (\ A_1 = h^{\alpha\beta + r \cdot \mathsf{H}(\mathsf{ID})},\ A_2 = h^{-r},\ \{B_j = h^{r w_{2,j}}\}_{j=1}^{\ell}\ ).$$

$\mathsf{Encrypt}(\mathsf{mpk}, \mathsf{ID}, \mathsf{M})$: To encrypt a message $\mathsf{M} \in \{0,1\}$, it picks $s, t_1, \ldots, t_\ell \xleftarrow{\$} \mathbb{Z}_p$ and computes

$$C_0 = \mathsf{M} \oplus \mathsf{GL}\big(e(g^{\alpha}, h^{\beta})^s, \mathsf{rand}\big), \quad C_1 = g^s, \quad C_2 = W_0^s \cdot \prod_{j \in [1,\ell]} W_{2,j}^{t_j},$$

$$D_j = g^{t_j} \cdot \left(\prod_{i \in \{i \in [1,\ell] \mid (i,j) \in S(\mathsf{ID})\}} W_{1,i} \right)^{-s} \qquad \text{for} \quad j \in [1,\ell]$$

Finally, it returns the ciphertext $C = (C_0, C_1, C_2, \{D_j\}_{j=1}^{\ell})$.

$\mathsf{Decrypt}(\mathsf{mpk}, \mathsf{sk}_{\mathsf{ID}}, C)$: To decrypt a ciphertext $C = (C_0, C_1, C_2, \{D_j\}_{j=1}^{\ell})$ using a private key $\mathsf{sk}_{\mathsf{ID}} = (A_1, A_2, \{B_j\}_{j=1}^{\ell})$, it first computes

$$e(C_1, A_1) \cdot e(C_2, A_2) \cdot \prod_{j \in [1,\ell]} e(D_j, B_j) = e(g,h)^{s\alpha\beta}.$$

Then it retrieves the message by $C_0 \oplus \mathsf{GL}(e(g,h)^{s\alpha\beta}, \mathsf{rand})$.

The correctness of the scheme will be shown by a simple calculation.

Definition 2 (3-Computational Bilinear Diffie-Hellman Exponent (3-CBDHE) Assumption). *We say that 3-CBDHE holds on $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T)$ if*

$$\Pr[\mathcal{A}(g, g^s, g^a, g^{a^2}, h, h^a, h^{a^2}) \to e(g,h)^{sa^3}]$$

is negligible for any PPT adversary $\mathcal{A}$ where $g \xleftarrow{\$} \mathbb{G}_1$, $h \xleftarrow{\$} \mathbb{G}_2$, $s, a \xleftarrow{\$} \mathbb{Z}_p$.

The following theorem addresses the security of the scheme.

Theorem 3. *The above IBE scheme is adaptively secure assuming the 3-CBDHE assumption.*

6 Comparisons and Discussions

In this section, we compare our IBE schemes obtained in Sec. 4 and 5 with previous schemes. Throughout this section, $|\mathsf{mpk}|$, $|C|$, and $|\mathsf{sk}_{\mathsf{ID}}|$ denote the sizes of the master public keys, ciphertexts, and private keys, respectively. We denote by κ the length of the identity, which corresponds to the output length of the collision resistant hash if we choose to hash the bit string representing an identity.

Ideal Lattice Based IBE. In Sec. 4. we proposed a new ideal lattice based IBE scheme. By changing the base b of the $\boldsymbol{g}_b$-trapdoor, we obtain two types of instantiation offering tradeoffs. Namely, by setting $b = 2$ we obtain the Type 1 IBE scheme presented in the full version and by setting $b = n^{\frac{1}{4}}$ we obtain the Type 2 IBE scheme presented in Sec. 4.1. The Type 2 IBE allows for a more compact size parameters compared to the Type 1 IBE, whereas the Type 1 IBE allows for a more efficient sampling procedure due to the smaller Gaussian width. Note that the technique of changing the base b is applicable for other existing IBE schemes as well, offering a similar tradeoff presented above. Both of our schemes achieve the best efficiency among existing adaptively secure IBE schemes assuming the fixed polynomial approximation of the RLWE problem. This is illustrated in Table 1. We point out that the largest improvement from the Yamada's IBE is that we greatly weakened the underlying hardness assumption while improving the overall efficiency of the scheme.

Table 1. Comparison of Lattice-Base IBEs in the Standard Model.

Schemes	$\lvert\mathsf{mpk}\rvert$	$\lvert C\rvert$, $\lvert\mathsf{sk}_{\mathsf{ID}}\rvert$	$1/\alpha$ for LWE Assumption	Anonymous?
[CHKP10]	$O(n\kappa \log^2 n)$	$O(n\kappa \log^2 n)$	Fixed $\mathsf{poly}(n)$	Yes
[ABB10]+[Boy10]*	$O(n\kappa \log^2 n)$	$O(n \log^2 n)$	Fixed $\mathsf{poly}(n)$	Yes
[Yam16]: Scheme 1	$O(n\kappa^{\frac{1}{d}} \log^4 n)$	$O(n \log^4 n)$	$n^{\omega(1)}$	Yes
[Yam16]: Scheme 2	$O(n\kappa^{\frac{1}{d}} \log^4 n)$	$O(n \log^4 n)$	All $\mathsf{poly}(n)$	No
Ours: Sec. 4. Type 1.	$O(n\kappa^{\frac{1}{d}} \log^2 n)$	$O(n \log^2 n)$	Fixed $\mathsf{poly}(n)$	Yes
Ours: Sec. 4. Type 2.	$O(n\kappa^{\frac{1}{d}} \log n)$	$O(n \log n)$	Fixed $\mathsf{poly}(n)$	Yes

All parameters presented in the table are obtained by instantiating the schemes in the ring setting. $d \in \mathbb{N}$ is a flexible constant, which can be set to be any value. "$1/\alpha$" for LWE assumption refers to the underlying LWE assumption used in the security reduction. "Fixed $\mathsf{poly}(n)$" means that the corresponding scheme is proven secure under the LWE assumption with $1/\alpha$ being some fixed polynomial (e.g., n^3). "All $\mathsf{poly}(n)$" mean that we have to assume the LWE assumption for all polynomial.

* In the security proof for the adaptively secure variant of IBE in [ABB10], we have a restriction that $q > Q$. Namely, only bounded form of the security is proven. This restriction is removed in the refined analysis due to Boyen [Boy10].

Bilinear Map Based IBE. Here, we compare our scheme in Sec. 5 with other adaptively secure IBE schemes based on the hardness of computational/search problems on bilinear maps in the standard model. To base the security of IBE

schemes on such problems, we have to mask the message using the Goldreich-Levin hardcore bit [GL89]. To the best of our knowledge, there are only two IBE schemes that we can apply this modification: Waters IBE [Wat05] and Naccache IBE [Nac07]. As shown in Table 2, our scheme achieves asymptotically shorter master public key size than these schemes. We note that to compare the efficiency, we count the number of group elements. However our method comes at the cost of increasing the ciphertext and private key size and we further have to rely on a stronger assumption than theirs.

Table 2. Comparison of IBE from Bilinear Maps in the Standard Model.

Schemes	$\lvert\mathsf{mpk}\rvert$	$\lvert C\rvert$, $\lvert\mathsf{sk}_{\mathsf{ID}}\rvert$	Assumption
[Wat05] + Hardcore bit	$O(\kappa)$	2	CBDH
[Nac07] + Hardcore bit	$O(\kappa/\log(\lambda)) = O(\kappa/\log(\kappa))$	2	CBDH
Ours: Sec. 5	$O(\sqrt{\kappa})$	$O(\sqrt{\kappa})$	3-CBDHE

Acknowledgement. We would like to thank anonymous reviewers of Asiacrypt 2016 for helpful comments. We also thank the members of Shin-Akarui-Angou-Benkyoukai for their helpful discussions and comments. This research was partially supported by CREST, JST. The second author is supported by JSPS KAKENHI Grant Number 16K16068.

References

ABB10. S. Agrawal, D. Boneh, and X. Boyen. Efficient lattice (H) IBE in the standard model. In *EUROCRYPT*, pp. 553–572. 2010.

ACPS09. B. Applebaum, D. Cash, C. Peikert, and A. Sahai. Fast cryptographic primitives and circular-secure encryption based on hard learning problems. In *CRYPTO*, pp. 595–618. 2009.

Alp15. J. Alperin-Sheriff. Short signatures from homomorphic trapdoor functions. In *PKC*, pp. 236–255. 2015.

AFL16. D. Apon, X. Fan, and F. Liu. Fully-secure lattice-based IBE as compact as PKE. In *IACR Cryptology ePrint Archive*. 2016:125, 2016.

BB04a. D. Boneh and X. Boyen. Efficient selective-id secure identity-based encryption without random oracles. In *EUROCRYPT*, pp. 223–238. 2004.

BB04b. D. Boneh and X. Boyen. Secure identity based encryption without random oracles. In *CRYPTO*, pp. 443–459. 2004.

BBG05. D. Boneh, X. Boyen, and E. Goh. Hierarchical identity based encryption with constant size ciphertext. In *EUROCRYPT*, pp. 440–456. 2005.

BF01. D. Boneh and M. Franklin. Identity-based encryption from the weil pairing. In *CRYPTO*, pp. 213–229. 2001.

BGG+14. D. Boneh, C. Gentry, S. Gorbunov, S. Halevi, V. Nikolaenko, G. Segev, V. Vaikuntanathan, and D. Vinayagamurthy. Fully key-homomorphic encryption, arithmetic circuit ABE and compact garbled circuits. In *EUROCRYPT*, pp. 533–556. 2014.

BGH07. D. Boneh, C. Gentry, and M. Hamburg. Space-efficient identity based encryption without pairings. In *FOCS*, pp. 647–657. 2007.

BGW05. D. Boneh, C. Gentry, and B. Waters. Collusion resistant broadcast encryption with short ciphertexts and private keys. In *CRYPTO*, pp. 258–275. 2005.

BH08. D. Boneh and M. Hamburg. Generalized identity based and broadcast encryption schemes. In *ASIACRYPT*, pp. 455–470. 2008.

BLL+15. S. Bai, A. Langlois, T. Lepoint, D. Stehlé, and R. Steinfeld. Improved security proofs in lattice-based cryptography: using the rényi divergence rather than the statistical distance. In *ASIACRYPT*, pp. 3–24. 2015.

Boy10. X. Boyen. Lattice mixing and vanishing trapdoors: A framework for fully secure short signatures and more. In *PKC*, pp. 499–517. 2010.

BR09. M. Bellare and T. Ristenpart. Simulation without the artificial abort: Simplified proof and improved concrete security for Waters IBE scheme. In *EUROCRYPT*, pp. 407–424. 2009.

CHKP10. D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert. Bonsai trees, or how to delegate a lattice basis. *EUROCRYPT*, pp. 523–552. 2010.

CCZ11. Y. Chen, L. Chen, and Z. Zhang. CCA Secure IB-KEM from computational bilinear Diffie-Hellman in the standard model. In *ICISC*, pp. 275–301. 2011.

Coc01. C. Cocks. An identity based encryption scheme based on quadratic residues. In *Cryptography and Coding*, pp. 360–363. 2001.

CW13. J. Chen and H. Wee. Fully,(almost) tightly secure IBE and dual system groups. In *CRYPTO*, pp. 435–460. 2013.

DM14. L. Ducas and D. Micciancio. Improved short lattice signatures in the standard model. In *CRYPTO*, pp. 335–352. 2014.

DLP14. L. Ducas, V. Lyubashevsky, and T. Prest. Efficient identity-based encryption over NTRU lattices. In *ASIACRYPT*, pp. 22–41. 2014.

DM15. L. Ducas and D. Micciancio. Fhew: Bootstrapping homomorphic encryption in less than a second. In *EUROCRYPT*, pp. 617–640. 2015.

Gal10. D. Galindo. Chosen-ciphertext secure identity-based encryption from computational bilinear Diffie-Hellman. In *Pairing*, pp. 445–464. 2010.

Gen06. C. Gentry. Practical identity-based encryption without random oracles. In *EUROCRYPT*, pp. 445–464. 2006.

GL89. O. Goldreich and L. Levin. A hard-core predicate for all one-way functions. In *STOC*, pp. 25–32. 1989.

GPV08. C. Gentry, C. Peikert, and V. Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *STOC*, pp. 197–206. 2008.

HJKS10. K. Haralambiev, T. Jager, E. Kiltz, and V. Shoup: Simple and efficient public-key encryption from computational Diffie-Hellman in the standard model. In *PKC*, pp. 1–18. 2010.

JR13. C. Jutla and A. Roy. Shorter quasi-adaptive NIZK proofs for linear subspaces. In *ASIACRYPT*, pp. 1–20. 2013.

LOS+10. A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. In *EUROCRYPT*, pp. 62–91. 2010.

LPR10. V. Lyubashevsky, C. Peikert, and O. Regev. On ideal lattices and learning with errors over rings. *EUROCRYPT*, pp. 1–23, 2010.

LPR13. V. Lyubashevsky, C. Peikert, and O. Regev. A toolkit for ring-lwe cryptography. In *EUROCRYPT*, pp. 35–54. 2013.

LS15. A. Langlois and D. Stehlé. Worst-case to average-case reductions for module lattices. *DES*, 75(3):565–599, 2015.

LW10. A. Lewko and B. Waters. New techniques for dual system encryption and fully secure HIBE with short ciphertexts. In *TCC*, pp. 455–479. 2010.

MP12. D. Micciancio and C. Peikert. Trapdoors for lattices: Simpler, tighter, faster, smaller. In *EUROCRYPT*, pp. 700–718. 2012.

MR04. D. Micciancio and O. Regev. Worst-case to average-case reductions based on gaussian measures. In *FOCS*, pp. 372–381, 2004.

Nac07. D. Naccache. Secure and *practical* identity-based encryption. In *IET Information Security*, volume 1(2): pp.. 59–64, 2007.

Pei10. C. Peikert. An efficient and parallel gaussian sampler for lattices. In *CRYPTO*, pp. 80–97. 2010.

Reg05. O. Regev. On lattices, learning with errors, random linear codes, and cryptography. In *STOC*, pp. 84–93. ACM Press, 2005.

Sha85. A. Shamir. Identity-based cryptosystems and signature schemes. In *CRYPTO*, pp. 47–53. 1985.

SOK00. R. Sakai, K. Ohgishi, and M. Kasahara. Cryptosystems based on pairings. In *SCIS*, 2000. (In Japanese).

SRB12. K. Singh, C. Pandu Rangan, and A. K. Banerjee. Adaptively secure efficient Lattice (H)IBE in standard model with short public parameters. In *SPACE*, pp.. 153–172, 2012.

SSTX09. D. Stehlé, R. Steinfeld, K. Tanaka, and K. Xagawa. Efficient public key encryption based on ideal lattices. In *ASIACRYPT*, pp. 617–635. 2009.

Wat05. B. Waters. Efficient identity-based encryption without random oracles. In *EUROCRYPT*, pp. 114–127. 2005.

Wat09. B. Waters. Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. In *CRYPTO*, pp. 619–636. 2009.

Xag13. K. Xagawa. Improved (hierarchical) inner-product encryption from lattices. In *PKC*, pp. 235–252. 2013.

Yam16. S. Yamada. Adaptively secure identity-based encryption from lattices with asymptotically shorter public parameters. In *EUROCRYPT*, pp. 32–62. 2016.

ZCZ16. J. Zhang, Y. Chen, and Z. Zhang. Programmable hash functions from lattices: Short signatures and IBEs with small key sizes. In *CRYPTO*. 2016. To appear.