Lower Bounds for Lattice-based Compact Functional Encryption

Erkan Tairi[1]* and Akin Ünal[2]**

[1] DIENS, École normale supérieure, CNRS, Inria, PSL University, Paris, France
[2] ISTA, Klosterneuburg, Austria

Abstract. Functional encryption (FE) is a primitive where the holder of a master secret key can control which functions a user can evaluate on encrypted data. It is a powerful primitive that even implies indistinguishability obfuscation (iO), given sufficiently compact ciphertexts (Ananth-Jain, CRYPTO'15 and Bitansky-Vaikuntanathan, FOCS'15). However, despite being extensively studied, there are FE schemes, such as function-hiding inner-product FE (Bishop-Jain-Kowalczyk, AC'15, Abdalla-Catalano-Fiore-Gay-Ursu, CRYPTO'18) and compact quadratic FE (Baltico-Catalano-Fiore-Gay, Lin, CRYPTO'17), that can be only realized using pairings. This raises the question if there are some mathematical barriers that hinder us from realizing these FE schemes from other assumptions.
In this paper, we study the difficulty of constructing lattice-based compact FE. We generalize the impossibility results of Ünal (EC'20) for lattice-based function-hiding FE, and extend it to the case of compact FE. Concretely, we prove lower bounds for lattice-based compact FE schemes which meet some (natural) algebraic restrictions at encryption and decryption, and have ciphertexts of linear size and secret keys of minimal degree. We see our results as important indications of why it is hard to construct lattice-based FE schemes for new functionalities, and which mathematical barriers have to be overcome.

1 Introduction

Functional encryption (FE) [BSW11; ONe10] is an advanced encryption primitive that allows fine-grained access control over the encrypted data. In contrast to conventional encryption schemes, which are all-or-nothing, in FE there is a master secret key msk that allows to generate constrained functional secret keys. More precisely, every secret key sk_f is associated with a function f and, given an encryption of some message x, the decryption with sk_f only reveals $f(x)$, and nothing more about x.

Since its introduction, FE has been subject to intense study, which resulted in both FE schemes for general functionalities [Gar+13; AR17; Che+18; AV19], thereby entailing feasibility results, and FE schemes for limited classes of functions that are of particular interest for practical applications, e.g., (function-hiding) inner-product FE (IPFE) [Abd+15; BJK15; ALS16; Lin17; Tom19; Agr+20] and compact FE for quadratic functions [Bal+17; Lin17; AS17; Gay20; Tom23]. Furthermore, IPFE and quadratic FE have been extended to multi-input [Abd+17; Abd+18; AGT21a; AGT22], (decentralized) multi-client [Cho+18; Abd+19; LT19; ABG19; AGT21b], and identity/attribute-based [Abd+20; Cin+23] settings.

We also know that FE is a powerful primitive that even implies indistinguishability obfuscation (iO). In fact, it has been shown that a succinct subexponentially secure single-key FE implies iO [AJ15; BV15; LT17; KNT18; Agr19; AP20; JLS21; JLS22].

Moreover, we know that FE for general functionalities with a *bounded* number of secret keys (that an adversary can learn), can be achieved from minimal assumptions [AV19], such as public-key encryption (PKE) and one-way functions (OWFs). However, if we want to achieve security for an *unbounded* number of secret keys, we either need to rely on heavy-machinery, such as iO [Gar+13], or restrict ourselves to (function-hiding) IPFE, linearly compact quadratic FE or FE for constant-degree polynomials which are obtained by relinearization. Even so, for linearly compact quadratic FE and function-hiding FE the only known constructions are pairing-based [BJK15; Bal+17; Lin17; Gay20].

* Work done while the author was at TU Wien.
** Work done while the author was at ETH Zurich.

In a recent work, Ünal [Ünal20] showed implausibility of constructing lattice-based function-hiding IPFE. More precisely, he extracted the common properties (of decryption and encryption algorithms) of known lattice-based FE schemes, and showed that under these properties an FE scheme cannot be function-hiding. Given this result and the usefulness of compact FE for constructing advanced primitives, such as iO, we ask the following question in this work:

What hinders us from constructing ***compact*** *lattice-based FE?*

1.1 Lattice-Based Functional Encryption Framework

To investigate the above question, we need to capture *lattice-based FE* schemes in a non-black box way. Towards this end, we reintroduce here the framework of Ünal [Ünal20]:

Definition 1 (Lattice-Based FE Scheme). *Let* $\mathsf{FE} = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *be an FE scheme. Let* q *be a prime and* $p < q$ *be the modulus of the message space. We call* FE ***lattice-based*** *if the following conditions are met:*

1. Enc *computes ciphertexts as follows: On input a master secret key* msk *and a message* $x \in \mathbb{Z}_p^n$, Enc *first samples (potentially correlated) polynomials* $r_1, \ldots, r_m \in \mathbb{Z}_q[X_1, \ldots, X_n]$ *of constant degree without looking at* x*. It then evaluates* $r_1, \ldots, r_m$ *at* x *and outputs the ciphertext*

$$\mathsf{ct}_x := (r_1(x), \ldots, r_m(x)) \in \mathbb{Z}_q^m \,.$$

2. *Each secret key output by* KeyGen *is a polynomial in* $\mathbb{Z}_q[Z_1, \ldots, Z_m]$ *of constant degree.*
3. *On input a secret key* $\mathsf{sk} \in \mathbb{Z}_q[Z_1, \ldots, Z_m]$ *and a ciphertext* $\mathsf{ct} \in \mathbb{Z}_q^m$*, the decryption algorithm* Dec *evaluates the polynomial* sk *at* ct_x *and rounds the result to the nearest integer modulo* p*, i.e.,*

$$\mathsf{Dec}(\mathsf{sk}, \mathsf{ct}) = \lceil \mathsf{sk}(\mathsf{ct}) \cdot p/q \rfloor \in \mathbb{Z}_p \,.$$

The lattice-based FE framework makes strong restrictions on the encryption and decryption algorithms of FE schemes. However, since compact and function-hiding FE schemes do exist assuming the security of pairing groups [BJK15; Gay20], it is necessary to restrict the computational model of an FE scheme at some points. We argue that the restrictions made by the framework of [Ünal20] are the right ones, in the sense that they are loose enough to capture all relevant FE schemes whose security relies on the Learning With Errors (LWE) assumption. Moreover, these restrictions are decisive enough to make impossibility results for schemes captured by this framework provable. Let us discuss this in more detail. A closer look at the existing lattice-based IBE/ABE/PE/FE schemes [ABB10; GVW13; Bon+14; ALS16; AR17; AP20] reveals that the restrictions imposed in Definition 1 are quite natural and fulfilled by most[3] of these schemes. As a prime example, we can present here the encryption algorithm of the IPFE scheme due to Agrwal, Libert and Stehlé [ALS16]: The public key consists of two matrices $A \in \mathbb{Z}_q^{m \times n}, B \in \mathbb{Z}_q^{\ell \times n}$. To encrypt input vectors $x \in \mathbb{Z}_p^\ell$, ciphertexts are generated by sampling a uniformly random vector $s \leftarrow \mathbb{Z}_q^n$, two Gaussian noise vectors $e_0 \leftarrow \mathcal{D}_{\mathbb{Z}^m,\sigma}, e_1 \leftarrow \mathcal{D}_{\mathbb{Z}^\ell,\sigma}$ and computing

$$\mathsf{ct} = (As + e_0, Bs + e_1 + f \cdot x),$$

where f is the scaling factor (commonly $\lfloor q/K \rfloor$, for some integer K). Now observe that we can rewrite this in two parts:

- a complex *offline* part, where $m + \ell$ multivariate degree-1 polynomials

$$g_1(X), \ldots, g_m(X), h_1(X), \ldots, h_\ell(X) \in \mathbb{Z}_q[X_1, \ldots, X_\ell]$$

[3] An exception is the decryption algorithms of some ABE schemes [GVW13; Bon+14], that need to evaluate a predicate of high depth at decryption. If those ABE schemes are only instantiated with constant depth predicates, then their decryption algorithm also fits our framework. For more exceptions, see Section 6.

are sampled using only the public values (p, q, f, A, B) (and without looking at the input x),

$$g_i(X_1, \ldots, X_\ell) := \langle a_i \mid s \rangle + e_{0,i}, \qquad i \in [m],$$
$$h_j(X_1, \ldots, X_\ell) := \langle b_j \mid s \rangle + e_{1,j} + f \cdot X_j, \qquad j \in [\ell],$$

- and a simple *online* part, where the previously sampled polynomials are evaluated on input x in order to compute the ciphertext,

$$\mathsf{ct} = (g_1(x), \ldots, g_m(x), h_1(x), \ldots, h_\ell(x)).$$

This shows that the encryption algorithm of [ALS16] fits into our framework (their decryption algorithm falls into our framework too, which is easy to verify).

For our restrictions at decryption, we point out that it was already noted by Brakerski et al. [Bra+19] that even all lattice-based fully homomorphic encryption (FHE) schemes[4] decrypt by evaluating a low-degree polynomial at the ciphertext and then rounding to the nearest result.

Moreover, we note that since the publication of [Ünal20] there has been no construction of function-hiding FE from LWE (or any other lattice-based assumption). While the results of [Ünal20] only hold in the aforementioned lattice-based FE framework, they (up to now) correctly predicted that constructing function-hiding FE from LWE requires breakthrough methods. This justifies to see the framework of [Ünal20] as a gauge for measuring the hardness of lattice-based FE schemes and understanding the mathematical barriers that are needed to be overcome.

1.2 Contribution

We generalize the results of Ünal [Ünal20] for lattice-based function-hiding FE, and extend them to the setting of lattice-based compact FE. Our main contribution is captured with the following informal theorem.

Theorem 1 (Informal Main Theorem 5). *Let $q > p$ be s.t. q is prime, $q/p \in \mathsf{poly}(\lambda)$ and p is greater than some constant.*

Let FE *be a* lattice-based *functional encryption scheme for polynomials of degree $d > 1$ with input space $\mathbb{Z}_p^n$, where each ciphertext is contained in $\mathbb{Z}_q^m$.*

Assume that FE *is* linearly compact*, i.e., $m \in O(n)$, and that each secret key output by* KeyGen *is a degree-d polynomial over the ciphertexts.*

If FE *is correct, then it cannot be selectively IND-CPA secure.*

At a high level, our proof idea consists of deriving a (special) SKE scheme from a lattice-based compact FE scheme. By using the existence of low-degree algebraic relationships, which has been shown in [Ünal23], we can use the compactness of the FE scheme to prove correctness of the aforementioned SKE scheme. This in turn leads to a contradiction to Corollary 3 of [Ünal20] (cf. Theorem 2) and gives us implicitly an attack on lattice-based compact FE scheme. As a small side result, we can apply the same techniques to (loosely) compact FE schemes, where ciphertexts only have a constant vector dimension. We outline this result and its proof in Appendix A.

1.3 Interpretation, Limitations and Open Problems

Parameter Restrictions. We have analogous parameter restrictions as in [Ünal20]. More precisely, in order to prove Theorem 1, we require that the exterior modulus q of the FE scheme is prime. Furthermore, the fraction q/p needs to be bounded by a polynomial[5] in the security parameter λ, where p is the interior

[4] However, it should be noted that most FHE schemes use an inverse gadget matrix at homomorphic evaluations, which circumvents our restrictions at encryption.

[5] The runtime of the attack that is implicitly used by Theorem 2 lies in $\mathsf{poly}(q/p)$. If q/p is superpolynomial, then our result still yields an adversary with equally superpolynomial time complexity.

modulus, and p needs to be greater than some constant that depends on the depth of the FE scheme. These parameter restrictions are usual for schemes whose security is implied by standard LWE, i.e., LWE with polynomial modulus q, which admits a reduction to worst-case lattice problems [Reg05].

Additionally, we require a strict notion of compactness where we demand the dimensional length of ciphertexts to be linear in the length of messages. Furthermore, we assume decryption to be as simple as possible, i.e., the algebraic degree of secret keys must equal the algebraic degree of the functionality supported by the FE scheme.

To relax both requirements it would be necessary to prove some technical theorem about homogeneity of ciphertexts (Theorem 6) for more general FE schemes. Concretely, we suspect the following:

Conjecture 1. Let FE be a lattice-based FE scheme for degree-d polynomials over n variables. Furthermore, let FE be *relaxed compact*, i.e., we have $m \in O(n^{d-e})$ where m is the dimension of ciphertexts of FE and $e > 0$ is some fixed constant. Denote by d_2 the decryption depth of FE.

If FE is IND-CPA secure against adversaries of complexity $n^{O(n^{d-e\cdot d_2/(d_2-1)})}$, then Theorem 6 does hold for FE. This implies that FE cannot be IND-CPA secure against adversaries of size $n^{O(n^{d-e\cdot d_2/(d_2-1)})}$ if FE is correct.

Interpretation and Open Problems. We view the results in this paper as a useful argument in understanding the difficulties of constructing lattice-based compact FE schemes. We leave it as an interesting open problem to derive similar lower bounds for other types of FE schemes, such as noisy linear FE [AP20] or FE for attribute-weighted sums [AGW20].

A potential approach to circumvent the lower bounds introduced here is to consider gadget matrices (as in FHE schemes and as in the predicate encryption scheme of [GVW15]). More precisely, if during encryption we compute a bit-decomposition, $G^{-1}(x)$, of an input vector x, then our techniques are not applicable anymore, and one would need to develop more advanced techniques. However, it is still unclear if inverse gadget sampling is helpful for constructing lattice-based FE schemes. We discuss more open questions and ways to circumvent our results in Section 6.

Note on Algebraic LWE. A natural question to ask is whether more algebraically structured variants of LWE, such as Ring-LWE [LPR10] or Module-LWE [LS15], can be used to overcome the lower bounds introduced in this work. Analogous to the results of [Ünal20], the additional algebraic structure does not help, as long as the requirements of Theorem 1 are met. The reason for this is that the rings and modules considered in algebraic LWE variants are vector spaces over $\mathbb{Z}_q$ with the natural addition whose multiplication operation can be modeled by quadratic polynomials.

1.4 Related Work

Ananth and Vaikuntanathan [AV19] showed that FE for $\mathsf{P/poly}$ with a bounded number of secret keys can be achieved from minimal assumptions, i.e., PKE in the public-key setting and OWFs in the secret-key setting. But, the ciphertexts in their schemes are growing linearly with the number of secret keys handed out to the adversary. This is not surprising given that a bounded public-key FE scheme with relaxed compact ciphertext size, i.e., sublinear in the number of secret keys, implies[6] iO [AJ15; BV15]. Similarly, Kitagawa, Nishimaki and Tanaka [KNT18] showed that a bounded and compact secret-key FE scheme implies iO. Moreover, Ananth, Jain and Sahai [AJS15] showed how to transform any collusion-resistant FE into a single-key FE scheme with compact encryption circuit. De Caro, Iovino, Jain, O'Neill, Paneth and Persiano [De +13] showed that compact FE with simulation-based security is impossible for general functions [Agr+13; De +13], however, for constructing iO from compact FE selective indistinguishability security suffices.

As explained in Section 1.5, we consider encryption algorithms that can be decomposed into simple online and complex offline parts. Such a decomposition has been previously used both for constructing

[6] Technically, [AJ15; BV15] define compactness with respect to the running time of the encryption algorithm. More precisely, the running time of the encryption algorithm must only be a polynomial in the security parameter and input message length, and has only sublinear dependency on the function size, i.e., $\mathsf{poly}(\lambda, |x|) \cdot |f|^{1-e}$ for some constant $e \in (0, 1]$.

new FE schemes [HW14; AR17] and showing impossibility results [Ünal20]. However, none of these works considered the compact FE case.

Other Models of Computation. Computational models are a popular approach in cryptography to prove lower bounds for solving certain problems. Nonetheless, the most well-known models, such as the generic group model [Mau05; Sho97], the algebraic group model [FKL18] and the random oracle model [BR93] only deal with group-based resp. hash-based problems and primitives.

We are not aware of many other models besides [Ünal20] for lattice-based settings. Guo, Kamath, Rosen and Sotiraki [Guo+22] studied the lattice-based non-interactive key exchange (NIKE) problem and introduced a (comparatively more rigid) model where Alice and Bob always send LWE samples $A \cdot x_1 + e_1$ and $A^T \cdot x_2 + e_2$ as their key parts, respectively. Afterwards, they may apply any key reconciliation function to extract a common secret key. The authors could show lower bounds for the complexity and amount of information the reconciliation function needs.

There are some similarities between the lower bounds obtained in our model and the lower bounds obtained by Applebaum, Avron and Brzuska [AAB15] for *arithmetic circuits*. In our setting, the encryption and decryption functionalities come close to arithmetizing circuits, i.e., their algebraic descriptions are (almost) independent of the underlying field $\mathbb{Z}_q$. The lower bound for lattice-based function-hiding FE, for example, could almost be reduced to a lower bound in [AAB15] for three-party protocols where a semi-arithmetic Alice and a non-arithmetic Bob want to make a fully arithmetic Carol learn a function of both parties' data without learning any non-trivial information. However, the crux is that we allow the decryption algorithm to perform a rounding operation from $\mathbb{Z}_q$ to $\mathbb{Z}_p$ at the end. Since rounding is a non-arithmetic of forbiddingly high degree, the decryption algorithm of lattice-based FE schemes is non-arithmetic and, hence, not fully captured by the lower bounds in [AAB15].

1.5 Technical Overview

In this subsection, we will sketch a proof for Theorem 1. Towards this end, we will first introduce the framework of Ünal [Ünal20] for modeling lattice-based FE schemes, which we use in this work. Next, we will revisit a strategy for proving lower bounds for lattice-based *function-hiding* FE schemes and generalize it. Finally, we will attempt to adapt the generalized strategy on *relaxed compact* lattice-based FE schemes. Unfortunately, our first attempt will fail, however, we will be able to fix the strategy for linearly compact lattice-based FE schemes with secret keys of minimal degree.

Our Framework. A (secret-key) *functional encryption* (FE) scheme consists of four algorithms: Setup, KeyGen, Enc and Dec. On input the security parameter 1^λ, Setup computes a master secret key msk. On input msk and a suitable function $f\colon \mathbb{Z}_p^n \to \mathbb{Z}_p$, KeyGen generates a secret key sk_f for f. On input msk and a message $x \in \mathbb{Z}_p^n$, Enc outputs a ciphertext ct_x. Finally, on input sk_f and ct_x, Dec outputs $f(x)$.

In this work, we want to prove lower bounds for *lattice-based* FE schemes. In order to do so,we focus on FE schemes $\mathsf{FE} = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ that are subject to the following two restrictions:

- Enc is of constant *depth*, i.e., the output of $\mathsf{Enc}(\mathsf{msk}, x)$ is computed in two phases: in the complex *offline* phase, Enc only knows msk and computes arbitrarily complicated randomness $(r_1, \ldots, r_m)$. In the simple *online* phase, Enc sees the message $x \in \mathbb{Z}_p^n$ and the randomness $(r_1, \ldots, r_m)$ from the previous phase. However, in this phase Enc must compute the ciphertext by an arithmetic circuit of constant depth.
  Formally, we require that there exists an offline algorithm $\mathsf{Enc}_{\mathsf{off}}$ that on input msk outputs random polynomials $r_1, \ldots, r_m \in \mathbb{Z}_q[X_1, \ldots, X_n]$ of *constant* degree. $\mathsf{Enc}(\mathsf{msk}, x)$ is then expected to work by first sampling $(r_1, \ldots, r_m) \leftarrow \mathsf{Enc}_{\mathsf{off}}(\mathsf{msk})$, and then outputting the ciphertext $\mathsf{ct}_x = (r_1(x), \ldots, r_m(x)) \in \mathbb{Z}_q^m$. We call the maximum degree of $r_1, \ldots, r_m$ the *depth* of Enc.
- Each secret key sk_f is a polynomial in $\mathbb{Z}_q[Y_1, \ldots, Y_m]$ of constant degree and Dec works in a typical lattice-based manner: it evaluates sk_f on the ciphertext ct_x and rounds the result to the next number modulo p. Formally, we require

$$\mathsf{Dec}(\mathsf{sk}_f, \mathsf{ct}_x) = \left\lceil \frac{p}{q} \cdot \mathsf{sk}_f(\mathsf{ct}_x) \right\rfloor .$$

For simplicity, we call FE schemes that adhere to these restrictions *lattice-based*.

Lower Bounds for Function-Hiding FE. We explain here the strategy of [Üna20] for showing implausibility of lattice-based *function-hiding* FE schemes, before we generalize and adapt it to the case of *compact* FE.

First, remember that in a function-hiding FE scheme the secret key sk_f hides the function f it evaluates at decryption, i.e., given sk_f and ct_x an adversary learns nothing about x *and* f besides $f(x)$. If we are given a function-hiding FE scheme $\mathsf{FE} = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ for computing linear functions over $\mathbb{Z}_p^n$, we can construct a secret-key encryption scheme $\mathsf{SKE}' = (\mathsf{Setup}', \mathsf{Enc}', \mathsf{Dec}')$ for messages in $\mathbb{Z}_p$ from FE s.t. its encryption algorithm Enc' is of *constant depth* and produces *short* ciphertexts. In fact, consider the following setup and encryption algorithms:

Setup': On input 1^λ, Setup' samples $\mathsf{msk} \leftarrow \mathsf{Setup}(1^\lambda)$. Then, it derives secret keys $\mathsf{sk}_1, \ldots, \mathsf{sk}_{Q-1} \leftarrow \mathsf{KeyGen}(\mathsf{msk}, 0)$ for the zero function and one secret key $\mathsf{sk}_Q \leftarrow \mathsf{KeyGen}(\mathsf{msk}, f)$ for the function f that maps a vector $x \in \mathbb{Z}_p^n$ to its first coordinate x_1. It returns $\mathsf{msk}' := (\mathsf{msk}, \mathsf{sk}_1, \ldots, \mathsf{sk}_Q)$.

Enc': On input $\mathsf{msk}' = (\mathsf{msk}, \mathsf{sk}_1, \ldots, \mathsf{sk}_Q)$ and a message $x_1 \in \mathbb{Z}_p$, Enc' computes the ciphertext $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{msk}, (x_1, 0, \ldots, 0))$ and then applies the polynomials $\mathsf{sk}_1, \ldots, \mathsf{sk}_{Q-1}$ on it and outputs

$$\mathsf{ct}' = (\mathsf{sk}_1(\mathsf{ct}), \ldots, \mathsf{sk}_{Q-1}(\mathsf{ct})) \in \mathbb{Z}_q^{Q-1}\,.$$

Since FE is a lattice-based FE scheme in the sense of our framework, its encryption algorithm Enc is offline/online of constant depth. It follows that Enc' is of constant depth as well, since Enc' first runs Enc and then again evaluates $Q-1$ fixed polynomials $\mathsf{sk}_1, \ldots, \mathsf{sk}_{Q-1} \in \mathbb{Z}_q[Y_1, \ldots, Y_m]$ of constant degree on the output of Enc. Therefore, the depth of the online phase of Enc' is bounded by the depth of Enc times the maximum degree of $\mathsf{sk}_1, \ldots, \mathsf{sk}_Q$.

Additionally, each ciphertext output by Enc' is short, i.e.,

$$||\mathsf{ct}'||_\infty \leq \frac{q}{p}.$$

To see this, note that the decryption algorithm of FE is given by $\mathsf{Dec}(\mathsf{sk}, \mathsf{ct}) = \lceil \mathsf{sk}(\mathsf{ct}) \cdot p/q \rfloor$. Now for $i \in [Q-1]$, we know that $\mathsf{Dec}(\mathsf{sk}_i, \mathsf{ct})$ must be zero, because sk_i is a secret key for the zero function. It follows that $\mathsf{sk}_i(\mathsf{ct}) \cdot p/q$ must be rounded to zero in $\mathbb{Z}_p$, which implies that the absolute value of $\mathsf{sk}_i(\mathsf{ct})$ cannot be larger than q/p.

Ideally, it should be infeasible to extract the message x_1 out of ct'. However, since FE is function-hiding and lattice-based, decryption with non-trivial success probability is possible. In fact, the distributions $\mathsf{KeyGen}(\mathsf{msk}, 0)$ and $\mathsf{KeyGen}(\mathsf{msk}, f)$ must look indistinguishable for a PPT adversary. If Q is large enough, one can show that the polynomial sk_Q must lie in the span of the polynomials $\mathsf{sk}_1, \ldots, \mathsf{sk}_{Q-1}$ with probability $1 - o(1)$, i.e., for $Q \in \mathsf{poly}(\lambda)$ large enough, we have that

$$\Pr_{\substack{\mathsf{sk}_1, \ldots, \mathsf{sk}_{Q-1} \leftarrow \mathsf{KeyGen}(\mathsf{msk}, 0) \\ \mathsf{sk}_Q \leftarrow \mathsf{KeyGen}(\mathsf{msk}, f)}} \left[\mathsf{sk}_Q \in \mathrm{span}_{\mathbb{Z}_q} \{\mathsf{sk}_1, \ldots, \mathsf{sk}_{Q-1}\}\right] \geq 1 - o(1).$$

This phenomenon gives rise to the following decryption algorithm Dec' for SKE':

Dec': On input $\mathsf{msk}' = (\mathsf{msk}, \mathsf{sk}_1, \ldots, \mathsf{sk}_Q)$ and a ciphertext $\mathsf{ct}' = (c_1, \ldots, c_{Q-1}) \in \mathbb{Z}_q^{Q-1}$, Dec' checks if $\mathsf{sk}_Q \in \mathrm{span}_{\mathbb{Z}_q} \{\mathsf{sk}_1, \ldots, \mathsf{sk}_{Q-1}\}$. If so, Dec' computes scalars $\alpha_1, \ldots, \alpha_{Q-1}$ s.t. $\mathsf{sk}_Q = \alpha_1 \cdot \mathsf{sk}_1 + \ldots + \alpha_{Q-1} \cdot \mathsf{sk}_{Q-1}$, otherwise Dec' aborts. Dec' can now reconstruct $\mathsf{sk}_Q(\mathsf{ct})$ by computing

$$\begin{aligned} \mathsf{sk}_Q(\mathsf{ct}) &= (\alpha_1 \cdot \mathsf{sk}_1 + \ldots + \alpha_{Q-1} \cdot \mathsf{sk}_{Q-1})(\mathsf{ct}) \\ &= \alpha_1 \cdot \mathsf{sk}_1(\mathsf{ct}) + \ldots + \alpha_{Q-1} \cdot \mathsf{sk}_{Q-1}(\mathsf{ct}) \\ &= \alpha_1 \cdot c_1 + \ldots + \alpha_{Q-1} \cdot c_{Q-1}. \end{aligned}$$

Given $\mathsf{sk}_Q(\mathsf{ct})$, Dec' can now output

$$\mathsf{Dec}(\mathsf{sk}_Q, \mathsf{ct}) = \lceil \mathsf{sk}_Q(\mathsf{ct}) \cdot p/q \rfloor \in \mathbb{Z}_p\,.$$

Assuming that FE is correct, the probability of Dec' to return the correct message is at least $1 - o(1)$.

In summary, by assuming a lattice-based correct function-hiding FE scheme FE, we can construct an SKE scheme $\mathsf{SKE}' = (\mathsf{Setup}', \mathsf{Enc}', \mathsf{Dec}')$ with the following properties:

- Enc' encrypts messages in $\mathbb{Z}_p$ and is of constant depth.
- Each ciphertext output by Enc' is short, i.e., lies in $[-q/p, q/p]^{Q-1}$.
- The probability of Dec' decrypting correctly is at least $1 - o(1)$.
- Additionally, if FE is selectively IND-CPA secure, it can be shown—by a direct reduction—that SKE' is selectively IND-CPA secure, too.

The key observation of [Ünа20] is that such a secret-key encryption scheme cannot exist, if $q/p \in \mathsf{poly}(\lambda)$. In fact, the following result has been proven:

Theorem 2 ([Ünа20] (Informal Corollary 3)). *Let SKE be a secret-key encryption scheme of depth $d \in O(1)$ (with prime modulus q). Let $B \in \mathsf{poly}(\lambda)$ s.t. q/B is larger than some constant and assume that each ciphertext of SKE lies in $[-B, B]^{Q-1}$. Let $\{0, \ldots, 2d\}$ be the message space of SKE.*

SKE is selectively IND-CPA secure iff the statistical distance of the distributions $(\mathsf{msk}, \mathsf{Enc}(\mathsf{msk}, x))$ and $(\mathsf{msk}, \mathsf{Enc}(\mathsf{msk}, y))$ is negligible for each pair of messages $x, y \in \{0, \ldots, 2d\}$.

This yields a contradiction to the scheme SKE' we constructed, because Dec' cannot have a high decryption advantage when ciphertexts $\mathsf{ct}'_x \leftarrow \mathsf{Enc}'(\mathsf{msk}, x)$ and $\mathsf{ct}'_y \leftarrow \mathsf{Enc}'(\mathsf{msk}, y)$ are statistically close to each other.

It follows that one of the premises must have been wrong. Hence, if FE is lattice-based, correct and function-hiding, it cannot be selectively IND-CPA secure.

Generalization. In the following, we generalize the previous strategy to show lower bounds for arbitrary lattice-based FE schemes. We follow the idea to construct a special secret-key encryption scheme $\mathsf{SKE}'' = (\mathsf{Setup}'', \mathsf{Enc}'', \mathsf{Dec}'')$ from a given lattice-based FE scheme $\mathsf{FE} = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$. Since FE is lattice-based and correct, SKE'' will have an encryption algorithm of constant depth and short ciphertexts. Furthermore, if FE is selectively IND-CPA secure, then SKE'' is as well (by a direct reduction). By Theorem 2, it follows that Dec'' can have no meaningful success at decrypting ciphertexts of SKE''. A contradiction to the security of FE now follows if we can show that Dec'' must have a non-trivial success probability at decryption.

Concretely, SKE'' is given by the following algorithms:

Setup'': Let $\mathcal{F}$ denote the space of functions supported by FE. On input 1^λ, Setup'' chooses Q functions $f_1, \ldots, f_Q$ from $\mathcal{F}$. Additionally, it chooses an index $i_* \in [Q]$ and a degree-1 function $\nu_{i_*} \colon \mathbb{Z}_p \to \mathbb{Z}_p^n$ s.t. we have for each $x_1 \in \mathbb{Z}_p$

$$f_i(\nu_{i_*}(x_1)) = 0 \quad \text{for all } i \neq i_*, \qquad \text{but} \quad f_{i_*}(\nu_{i_*}(x_1)) = x_1.$$

Then, Setup'' samples $\mathsf{msk} \leftarrow \mathsf{Setup}(1^\lambda)$ and $\mathsf{sk}_i \leftarrow \mathsf{KeyGen}(\mathsf{msk}, f_i)$ for $i \in [Q]$, and outputs

$$\mathsf{msk}'' := (\mathsf{msk}, \mathsf{sk}_1, \ldots, \mathsf{sk}_Q, \nu_{i_*}, i_*).$$

Enc'': Given msk'' and $x_1 \in \mathbb{Z}_p$, Enc'' computes $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{msk}, \nu_{i_*}(x_1))$. It applies the polynomials $\mathsf{sk}_1, \ldots, \mathsf{sk}_{i_*-1}$, $0, \mathsf{sk}_{i_*+1}, \ldots, \mathsf{sk}_Q$ at ct and returns

$$\mathsf{ct}'' := (\mathsf{sk}_1(\mathsf{ct}), \ldots, \mathsf{sk}_{i_*-1}(\mathsf{ct}), 0, \mathsf{sk}_{i_*+1}(\mathsf{ct}), \ldots, \mathsf{sk}_Q(\mathsf{ct})) \in \mathbb{Z}_q^Q\,.$$

Dec'': On input msk'' and $\mathsf{ct}'' = (c_1, \ldots, c_Q)$, Dec'' computes the set

$$S := \left\{\mathsf{sk}_{i_*}(w) \mid w \in \mathbb{Z}_q^m, \forall i \neq i_* \colon \mathsf{sk}_i(w) = c_i\right\}. \tag{1}$$

It chooses a uniformly random element $\mathsf{sk}_{i_*}(w) \leftarrow S$ and outputs

$$\lceil \mathsf{sk}_{i_*}(w) \cdot p/q \rfloor = \mathsf{Dec}(\mathsf{sk}_{i_*}, w) \in \mathbb{Z}_p\,.$$

Note that SKE'' generalizes the ideas of SKE' and does not fully specify Setup''. In fact, the choice of the functions $f_1, \ldots, f_Q$ in Setup'' will depend on the concrete FE scheme. Similarly to SKE', SKE'' is of constant depth if FE is lattice-based. Moreover, it has short ciphertexts if FE is lattice-based and correct, and SKE'' is selectively IND-CPA secure if FE is so. We show these properties in detail in the proof of Lemma 2.

Because of Theorem 2, we know that SKE'' cannot be correct if FE is lattice-based, correct and selectively IND-CPA secure. However, in the case of a *function-hiding* FE scheme, it can be shown that Dec'' has a high probability to correctly decrypt ciphertexts. The idea in this text is to prove that Dec'' also has a high success probability at decryption in the case of *compact* FE schemes. However, as it turns out, grasping and using the compactness property of a lattice-based FE scheme is more complex than using the function-hiding property and requires a more algebraic approach.

Compact Case. In the following, we outline our strategy for the case of (relaxed) compact FE and sketch a proof attempt to show why Dec''—intuitively—has a non-trivial advantage at decrypting compact ciphertexts. However, as we explain later, this proof attempt has some gaps. In this work, we fill these gaps in the case of linear compactness and minimal decryption depth.

First, we give an informal definition of compactness (resp. succinctness):

Definition 2. *Let* $\mathsf{FE} = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *be an FE scheme with ciphertexts in* $\mathbb{Z}_q^m$ *and message space* $\mathbb{Z}_p^n$ *for polynomials of degree* d*. We call* FE ***relaxed compact*** *if there is a constant* $e > 0$ *s.t.*

$$m \in O(n^{d-e}).$$

In other words, we demand that ciphertexts are by a polynomial amount smaller than encrypting the relinearization $x^{\otimes d}$ of a message $x \in \mathbb{Z}_p^n$ and using an IPFE scheme. In the literature, there are different definitions of compactness and succinctness (cf. [BV15; AJ15; KNT18; AV19]). We note that Definition 2 is comparatively weaker and is implicitly fulfilled by the notions of the aforementioned works.

Now, let $\mathsf{FE} = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ be a compact lattice-based FE scheme that supports the evaluation of quadratic polynomials, i.e., the function space of FE is given by

$$\mathcal{F} = \{f \in \mathbb{Z}_p[X_1, \ldots, X_n] \mid \deg f \leq 2\},$$

while its message space is $\mathbb{Z}_p^n$. Compactness now states that we have $m \in O(n^{2-e})$ for a constant $e > 0$. This implies that the number of coordinates of a ciphertext of FE is significantly smaller than the number of secret keys for linearly independent functions of $\mathcal{F}$. Our idea is to combine this together with a result of [Ünal23] to achieve a non-trivial success probability at decryption.

First, we will specify how Setup'' chooses the functions $f_1, \ldots, f_Q \in \mathcal{F}$, the index $i_* \in [Q]$ and the function $\nu_{i_*} \colon \mathbb{Z}_p \to \mathbb{Z}_p^n$. Setup'' enumerates all pairs (a, b) with $1 \leq a < b \leq n$ and indexes them by

$$(a_{i_1}, b_{i_1}), \ldots, (a_{i_Q}, b_{i_Q}),$$

for $Q := \binom{n}{2} = \frac{n^2-n}{2}$. For $i \in [Q]$, it sets f_i to be the monomial of the a_i-th and b_i-th variable, i.e.,

$$f_i(X_1, \ldots, X_n) := X_{a_i} \cdot X_{b_i} \in \mathcal{F}.$$

It draws $i_* \leftarrow [Q]$ uniformly at random and sets ν_{i_*} to be the affine linear map

$$\begin{aligned} \nu_{i_*} \colon \mathbb{Z}_p &\longrightarrow \mathbb{Z}_p^n \\ x &\longmapsto x \cdot e_{a_{i_*}} + e_{b_{i_*}}, \end{aligned}$$

where $e_{a_{i_*}}$ and $e_{b_{i_*}}$ denote the a_{i_*}-th and b_{i_*}-th unit vectors. More precisely, the vector $\nu_{i_*}(x)$ has the value x at position a_{i_*}, 1 at position b_{i_*} and 0 at every other position. It now follows for all $i \in [Q]$ and $x \in \mathbb{Z}_p$,

$$f_i(\nu_{i_*}(x)) = \begin{cases} x, & \text{if } i = i_*, \\ 0, & \text{if } i \neq i_*. \end{cases}$$

To prove that Dec'' has non-trivial advantage at decryption when receiving msk'' and a ciphertext ct'', we need to show that the set S computed by Dec'' in Equation (1) is small. Let $\mathsf{ct}'' := (\mathsf{sk}_1(\mathsf{ct}), \dots, \mathsf{sk}_{i_*-1}(\mathsf{ct}), 0, \mathsf{sk}_{i_*+1}(\mathsf{ct}), \dots, \mathsf{sk}_Q(\mathsf{ct}))$ for some $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{msk}'', \nu_{i_*}(x))$. Then, S must contain the correct value $\mathsf{sk}_{i_*}(\mathsf{ct})$ besides other values $\mathsf{sk}_{i_*}(w)$. Algebraically, showing that S is small boils down to the problem of *polynomial prediction*: we do not know ct, but we know its evaluations $\mathsf{sk}_i(\mathsf{ct})$ for many polynomials $\mathsf{sk}_1, \dots, \mathsf{sk}_{i_*-1}, \mathsf{sk}_{i_*+1}, \dots, \mathsf{sk}_Q \in \mathbb{Z}_q[Y_1, \dots, Y_m]$ of constant degree. Therefore, we can substantially bound the number of possible values of $\mathsf{sk}_{i_*}(\mathsf{ct})$. We illustrate this idea with a toy example:

Example 1. In our toy example, we assume that ciphertexts of FE have two coordinates $\mathsf{ct} = (c_1, c_2)$. Furthermore, assume that $i_* = 3$ and that the first three secret keys are given by

$$\mathsf{sk}_1(Y_1, Y_2) = Y_1 + Y_2, \quad \mathsf{sk}_2(Y_1, Y_2) = Y_2^2, \quad \mathsf{sk}_3(Y_1, Y_2) = Y_1 \in \mathbb{Z}_q[Y_1, Y_2].$$

Now, when we are given a ciphertext ct'' of SKE'', the values $a := \mathsf{sk}_1(\mathsf{ct}) = c_1 + c_2$ and $b := \mathsf{sk}_2(\mathsf{ct}) = c_2^2$ are fixed. In this situation, can we limit the number of possible values of $\mathsf{sk}_3(\mathsf{ct})$?

The answer turns out to be yes. Indeed, set $h(T_1, T_2, T_3) := (T_1 - T_3)^2 - T_2 = T_1^2 - 2T_1T_3 - T_2 + T_3^2$ and note that we have

$$h(\mathsf{sk}_1(Y_1, Y_2), \mathsf{sk}_2(Y_1, Y_2), \mathsf{sk}_3(Y_1, Y_2)) = 0. \tag{2}$$

Now, if we plug in the values $a, b \in \mathbb{Z}_p$, we get the univariate degree-2 polynomial

$$h(\mathsf{sk}_1(\mathsf{ct}), \mathsf{sk}_2(\mathsf{ct}), T_3) = h(a, b, T_3) = T_3^2 - 2a \cdot T_3 + a^2 - b.$$

Because of Equation (2), we know that $h(\mathsf{sk}_1(\mathsf{ct}), \mathsf{sk}_2(\mathsf{ct}), T_3)$ must vanish at $\mathsf{sk}_3(\mathsf{ct})$. In fact, $\mathsf{sk}_3(\mathsf{ct})$ is a root of $h(a, b, T_3)$ and S is contained in the set of points where $h(a, b, T_3)$ vanishes. Since $h(a, b, T_3)$ is of degree 2, there are at most 2 possible values for $\mathsf{sk}_3(\mathsf{ct})$. Hence, the probability of Dec'' to draw the correct value $\mathsf{sk}_3(\mathsf{ct})$ from S and decrypting correctly is at least $1/2$, which is noticeably larger than $1/p$.

In general, the polynomials $\mathsf{sk}_1, \dots, \mathsf{sk}_Q$ are of some constant degree, let's say $d \in O(1)$, and their number $Q = \binom{n}{2} \in \Omega(n^2)$ is substantially larger than the number of coordinates $m \in O(n^{2-e})$ of a ciphertext ct of FE. It has been shown in [Üna23] that in such cases there exists a polynomial h of sublinear degree that algebraically relates the polynomials $\mathsf{sk}_1, \dots, \mathsf{sk}_Q$:

Theorem 3 (Adapted from [Üna23]). *Let $Q \in \Omega(n^{d_0})$ and $m \in O(n^{d_0-e})$ for a constant $e > 0$. Let $g_1, \dots, g_Q \in \mathbb{Z}_q[Y_1, \dots, Y_m]$ be of degree $d \in O(1)$.*

Then, there exists a polynomial $h \in \mathbb{Z}_q[T_1, \dots, T_Q]$ with the following properties:

$$\begin{aligned} &h(T_1, \dots, T_Q) \neq 0, \\ &h(g_1(Y_1, \dots, Y_m), \dots, g_Q(Y_1, \dots, Y_m)) = 0, \\ &\deg h \in O(m^{1-\frac{e}{(d_0-e)(d-1)}}) = O(n^{d_0-e-\frac{e}{d-1}}). \end{aligned}$$

Given this polynomial h, we can show that each element of the set S computed by Dec'' in Equation (1) must be a root of the polynomial

$$h(\mathsf{sk}_1(\mathsf{ct}), \dots, \mathsf{sk}_{i_*-1}(\mathsf{ct}), T_{i_*}\, \mathsf{sk}_{i_*+1}(\mathsf{ct}), \dots, \mathsf{sk}_Q(\mathsf{ct})) \in \mathbb{Z}_q[T_{i_*}]. \tag{3}$$

Hence, the size of S is bounded by $\deg h \in O(n^{2-e-e/(d-1)})$. Therefore, the success probability of Dec'' to decrypt correctly is at least $n^{e+e/(d-1)-2}$, which is significantly larger than the trivial success probability $1/p$, if $p \in \omega(n^{2-e-e/(d-1)})$.

The above reasoning illustrates how we can use the compactness of FE to construct a correct and secure SKE scheme SKE'' with special properties to ultimately derive a contradiction to Theorem 2 and an attack on the security of FE. However, there is one gap that needs to be adressed: what happens if the univariate polynomial in Equation (3) is zero? In this case, the size of S does not need to be bounded by $\deg h$ and S

could contain each element of $\mathbb{Z}_q$. Now, what happens if the polynomial in Equation (3) is zero for almost all ciphertexts generated by $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{msk}, \nu_{i_*}(x))$? In this case, we cannot guarantee a non-trivial success probability for Dec''. Subsequently, SKE'' is not sufficiently correct, and we fail to reach a contradiction with Theorem 2.

In an attempt to fix this problem, one can consider the coefficients of the polynomial in Equation (3). Each coefficient is computed by a polynomial in the variables $T_1, \ldots, T_{i_*-1}$, $T_{i_*+1}, \ldots, T_m$ of lower degree. Concretely, we have

$$h(T_1, \ldots, T_m) = \sum_{j=0}^{\deg h} h_j(T_1, \ldots, T_{i_*-1}, T_{i_*+1}, \ldots, T_m) \cdot T_{i_*}^j,$$

for fitting polynomials $h_0, \ldots, h_{\deg h} \in \mathbb{Z}_q[T_1, \ldots, T_{i_*-1}, T_{i_*+1}, \ldots, T_m]$ of sublinear degree. We can assume that the highest degree coefficient $h_{\deg h}$ is non-zero. If the polynomial in Equation (3) is almost always zero for $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{msk}, \nu_{i_*}(x))$, it follows that $h_{\deg h}$ will almost always vanish on ct, and we could replace h with its coefficient $h_{\deg h}$. If $h_{\deg h}$ does always vanish on $\mathsf{sk}_1(\mathsf{ct}), \ldots, \mathsf{sk}_{i_*-1}(\mathsf{ct})$, $\mathsf{sk}_{i_*+1}(\mathsf{ct}), \ldots, \mathsf{sk}_Q(\mathsf{ct})$, but does not become zero when we plug in $\mathsf{sk}_1(\mathsf{ct}), \ldots, \mathsf{sk}_{i_*-1}(\mathsf{ct}), \mathsf{sk}_{i_*+1}(\mathsf{ct}), \ldots, \mathsf{sk}_{Q-1}(\mathsf{ct})$, we could use it to bound the number of possible values of $\mathsf{sk}_Q(\mathsf{ct})$ while fixing the values of $\mathsf{sk}_1(\mathsf{ct}), \ldots, \mathsf{sk}_{Q-1}(\mathsf{ct})$. However, $\mathsf{sk}_Q(\mathsf{ct})$ will not be of great help to us if ct encrypts $\nu_{i_*}(x)$, since we have $\mathsf{Dec}(\mathsf{sk}_Q, \mathsf{ct}) = f_Q(\nu_{i_*}(x)) = 0$. In fact, we need that $h_{\deg h}$ *behaves well* for the different distribution $\mathsf{Enc}(\mathsf{msk}, \nu_Q(x))$ of ciphertexts. This yields a problem: it may happen that $h_{\deg h}(\mathsf{sk}_1(\mathsf{ct}), \ldots, \mathsf{sk}_{i_*-1}(\mathsf{ct}), \mathsf{sk}_{i_*+1}(\mathsf{ct}), \ldots, \mathsf{sk}_{Q-1}(\mathsf{ct}))$ is always zero when we sample $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{msk}, \nu_{i_*}(x))$, but does not become zero when ct encrypts a *useful* message and is sampled from $\mathsf{Enc}(\mathsf{msk}, \nu_Q(x))$.

Linear Compactness and Secret Keys of Minimal Degree. To solve the above problem, we need that some kind of homogeneity among the ciphertexts of FE for different messages does hold. In particular, we need that whenever a polynomial g vanishes with overwhelming probability on the distribution $\mathsf{Enc}(\mathsf{msk}, x)$, for some $x \in \mathbb{Z}_p^n$, then for each $y \in \mathbb{Z}_p^n$, g vanishes with overwhelming probability on the distribution $\mathsf{Enc}(\mathsf{msk}, y)$. However, we can show this kind of homogeneity only in cases where g has a constant degree.

Now, the algebraic relationship h is of degree $O(n^{2-e-e/(d-1)})$ according to Theorem 3, where $e > 0$ describes the compactness of ciphertexts and d the degree of secret keys. If our ciphertexts are linearly compact, i.e., $m \in O(n)$, then e equals 1. Furthermore, if our secret keys are of minimal degree $d = 2$, then h is of constant degree $O(n^{2-e-e/(d-1)}) = O(n^0) = O(1)$, and we can guarantee some kind of homogeneity among the ciphertexts for h. Now, the insecurity of FE follows. In Section 4, we will generalize this result for FE schemes for polynomials of degree $d > 1$ with linear compactness $m \in O(n)$ and secret keys of degree d.

2 Preliminaries

Notation.. In this text, we always denote the security parameter by $\lambda \in \mathbb{N} = \{1, 2, \ldots\}$, by which each scheme and adversary is parametrized. For $n \in \mathbb{N}$, set $[n] = \{1, 2, \ldots, n\}$. Define

$$\mathsf{poly}(\lambda) := \left\{ f \colon \mathbb{N} \to \mathbb{N} \mid \exists d \in \mathbb{N} \colon f(\lambda) \in O(\lambda^d) \right\},$$
$$\mathsf{negl}(\lambda) := \left\{ \varepsilon \colon \mathbb{N} \to \mathbb{R} \mid \forall d \in \mathbb{N} \colon \limsup_{\lambda \to \infty} \varepsilon(\lambda) \cdot \lambda^d = 0. \right\}.$$

In this text, we will work with two moduli $p, q > 2$ s.t. q is always prime and we always have $2p < q$. We will identify the finite field with the corresponding sets of integers centered around zero, $\mathbb{Z}_q = \left\{ \frac{-q+1}{2}, \ldots, \frac{q-1}{2} \right\}$, and embed $\mathbb{Z}_p$ into $\mathbb{Z}_q$ as the non-negative numbers $\mathbb{Z}_p = \{0, \ldots, p-1\} \subset \mathbb{Z}_q$.

For two distributions A, B with the same support S, we define their **statistical distance** by

$$\Delta(A, B) := \frac{1}{2} \sum_{s \in S} \left| \Pr_{a \leftarrow A}[a = s] - \Pr_{b \leftarrow B}[b = s] \right|.$$

We will denote by $\forall_\infty$, resp. $\exists_\infty$, the quantifiers *for almost all* and *for infinitely many*.

Lemma 1 (Simplified from [Ünа23]). *Let k be a field. Let $d > 1$ be a constant and let $Q \in \Omega(m^d)$. There is a constant degree bound $D \in O(1)$ s.t. for each list of polynomials $f_1, \ldots, f_Q \in k[Y_1, \ldots, Y_m]$ of degree d there is one polynomial $h \in k[T_1, \ldots, T_Q]$ s.t.*

$$h \neq 0, \qquad \deg h \leq D, \qquad \text{and} \qquad h(f_1(Y), \ldots, f_Q(Y)) = 0.$$

2.1 Functional Encryption

Definition 3. *Let $\mathcal{X} = (\mathcal{X}_\lambda)_\lambda$ be a family of sets. We call $\mathcal{X}$ a **message space** or **value space** if there is an $s \in \mathsf{poly}(\lambda)$ s.t. each $x_\lambda \in \mathcal{X}_\lambda$ has a binary representation of size $\#x_\lambda \leq s(\lambda)$. A **subspace** $\widetilde{\mathcal{X}} \subset \mathcal{X}$ is a family of sets $\widetilde{\mathcal{X}} = (\widetilde{\mathcal{X}}_\lambda)_\lambda$ s.t. $\widetilde{\mathcal{X}}_\lambda \subseteq \mathcal{X}_\lambda$ for all λ. $\mathcal{X}$ is called **poly-size** if we have $\#\mathcal{X}_\lambda \in \mathsf{poly}(\lambda)$ and there is a poly-time algorithm that on input 1^λ can enumerate $\mathcal{X}_\lambda$.*

*If $\mathcal{X} = (\mathcal{X}_\lambda)_\lambda$ is a message space and $\mathcal{Y} = (\mathcal{Y}_\lambda)_\lambda$ is a value space, we call $\mathcal{F} = (\mathcal{F}_\lambda)_\lambda$ a **function space** if each $f_\lambda \in \mathcal{F}_\lambda$ is a function of type $f_\lambda \colon \mathcal{X}_\lambda \to \mathcal{Y}_\lambda$ and if there is an $s \in \mathsf{poly}(\lambda)$ s.t. each $f_\lambda \in \mathcal{F}_\lambda$ has a binary representation of size $\#f_\lambda \leq s(\lambda)$. In this case, we will write $\mathcal{F} \colon \mathcal{X} \to \mathcal{Y}$.*

Definition 4 (Functional Encryption). *A (secret-key) **functional encryption** (FE) scheme for the function space $\mathcal{F} \colon \mathcal{X} \to \mathcal{Y}$ is a tuple of four algorithms $\mathsf{FE} = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ that are described as follows:*

Setup**:** *On input a (unary encoded) security parameter 1^λ, it outputs a master secret key msk.*
KeyGen**:** *On input a master secret key msk and a description of a function f in the function space $\mathcal{F}$ of FE, it outputs a secret key sk_f for $f \in \mathcal{F}_\lambda$.*
Enc**:** *On input a master secret key msk and a message $x \in \mathcal{X}_\lambda$, it outputs a ciphertext ct_x of x.*
Dec**:** *On input a secret key sk_f and a ciphertext ct_x, it outputs a value $y \in \mathcal{Y}_\lambda$.*

*We call FE **correct**, if there is an $\varepsilon \in \mathsf{negl}(\lambda)$ s.t. we have for all $(f_\lambda)_\lambda \in \mathcal{F}$ and $(x_\lambda)_\lambda \in \mathcal{X}$ that $\Pr[\mathsf{Dec}(\mathsf{sk}_f, \mathsf{ct}_x) \neq f_\lambda(x_\lambda)] \leq \varepsilon(\lambda)$, where we sample $\mathsf{msk} \leftarrow \mathsf{Setup}(1^\lambda)$, $\mathsf{sk}_f \leftarrow \mathsf{KeyGen}(\mathsf{msk}, f_\lambda)$ and $\mathsf{ct}_x \leftarrow \mathsf{Enc}(\mathsf{msk}, x_\lambda)$.*

Definition 5 (Selective IND-CPA Security). *Let $\mathsf{FE} = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ be an FE scheme for a functionality $\mathcal{F} \colon \mathcal{X} \to \mathcal{Y}$. We define the **selective IND-CPA** security game of FE as an experiment $\mathsf{Exp}^{\mathsf{ind\text{-}cpa}}_{\mathsf{FE},\mathcal{A}}(\lambda, \mathcal{F})$ between an adversary $\mathcal{A}$ and a challenger $\mathcal{C}$ that proceeds in the following steps:*

Experiment $\mathsf{Exp}^{\mathsf{ind\text{-}cpa}}_{\mathsf{FE},\mathcal{A}}(\lambda, \mathcal{F})$

1. *$\mathcal{A}$ computes two lists of candidate messages $(x_1^0, \ldots, x_N^0), (x_1^1, \ldots, x_N^1) \in \mathcal{X}_\lambda^N$ and a list of functions $(f_1, \ldots, f_Q) \in \mathcal{F}_\lambda^Q$, and submits all three lists to the challenger $\mathcal{C}$.*
2. *$\mathcal{C}$ draws a random bit $b \leftarrow \{0, 1\}$, computes $\mathsf{msk} \leftarrow \mathsf{Setup}(1^\lambda)$ and*

$$\mathsf{ct}_i \leftarrow \mathsf{Enc}(\mathsf{msk}, x_i^b) \quad \text{for } i = 1, \ldots, N,$$
$$\mathsf{sk}_j \leftarrow \mathsf{KeyGen}(\mathsf{msk}, f_j) \quad \text{for } j = 1, \ldots, Q.$$

   $\mathcal{C}$ sends the lists $(\mathsf{ct}_1, \ldots, \mathsf{ct}_N)$ and $(\mathsf{sk}_1, \ldots, \mathsf{sk}_Q)$ to $\mathcal{A}$.
3. *$\mathcal{A}$ outputs a guess bit b'.*
4. *If $b = b'$ and for each $i \in [N]$ and $j \in [Q]$*

$$f_j(x_i^0) = f_j(x_i^1),$$

   then the experiment outputs 1, else 0.

*For a fixed algorithm $\mathcal{A}$ and an FE scheme FE, the **advantage** of $\mathcal{A}$ is defined[7] by*

$$\mathsf{Adv}^{\mathsf{ind\text{-}cpa}}_{\mathsf{FE},\mathcal{A}}(\lambda, \mathcal{F}) := 2 \cdot \Pr\left[\mathsf{Exp}^{\mathsf{ind\text{-}cpa}}_{\mathsf{FE},\mathcal{A}}(\lambda, \mathcal{F}) = 1\right] - 1.$$

[7] Note that we allow the advantage of $\mathcal{A}$ to be negative. This may seem strange, however, this notion of advantage is linear, i.e., we may condition and partition $\mathcal{A}$'s advantage on different events.

We call FE ***selectively IND-CPA secure*** *if any* PPT *adversary* $\mathcal{A}$ *has negligible advantage in the above game.*

2.2 Lattice-Based Encryption Algorithms

In the following, we will recapitulate the definition of *offline/online encryption* of constant depth that has been introduced in [Ünal20]. This notion allows the master secret key to have a computationally unbounded influence on the computed ciphertext as long as the message only influences the ciphertext polynomially:

Definition 6. *Let* $\mathsf{FE} = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *be an FE scheme with message space* $\mathcal{X} = \mathbb{Z}_p^n$*. Furthermore, let* $q = q(\lambda)$ *be a prime s.t. each ciphertext output by* Enc *is a vector in* $\mathbb{Z}_q^m$*.*

Let $d \in \mathbb{N}$ *be a constant. We say that* Enc *is of* ***depth*** d *if there is an* off-line *algorithm* $\mathsf{Enc}_{\mathsf{off}}$ *that on input* msk *outputs* m *polynomials* $r_1, \ldots, r_m \in \mathbb{Z}_q[X_1, \ldots, X_n]$ *of degree* $\leq d$ *s.t. the following distributions are identical for each* $\mathsf{msk} \leftarrow \mathsf{Setup}(1^\lambda)$ *and* $x \in \mathbb{Z}_p^n$*:*

$$\{(r_1(x), \ldots, r_m(x)) \mid (r_1, \ldots, r_m) \leftarrow \mathsf{Enc}_{\mathsf{off}}(\mathsf{msk})\} \text{ and } \{\mathsf{ct} \mid \mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{msk}, x)\}.$$

Note that we do not impose any bounds on the computational complexity of $\mathsf{Enc}_{\mathsf{off}}$*.*

In other words, an encryption algorithm of constant depth works in two phases. In an *offline* phase, it first sees the secret key, but does not get to know the message that is to be encrypted. It can then use any amount of time to compute polynomially bounded randomness for the second step. In the *online* phase, the algorithm gets the randomness from the first phase and sees the message. It must now compute each entry of the ciphertext vector in an arithmetically very simple way, i.e., by applying constant degree polynomials over the randomness from the offline phase and the coordinates of the message vector.

Since we want to build upon the results of [Ünal20], we also need to introduce the notion of *encryption of polynomial width.*

Definition 7. *Let* Enc *be an encryption algorithm that outputs vectors in* $\mathbb{Z}_q^m$*. We say that* Enc *is of* ***width*** $B = B(\lambda) < q/2$ *if there is an* $\varepsilon \in \mathsf{negl}(\lambda)$ *s.t. we have for each* $(x_\lambda)_\lambda \in \mathcal{X}$

$$\Pr_{\substack{\mathsf{msk} \leftarrow \mathsf{Setup}(1^\lambda) \\ \mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{msk}, x_\lambda)}} [||\mathsf{ct}||_\infty > B] \leq \varepsilon(\lambda),$$

where $||\mathsf{ct}||_\infty$ *is defined as the largest absolute value among entries of* $\mathsf{ct} \in \left\{-\frac{q-1}{2}, \ldots, \frac{q-1}{2}\right\}^m = \mathbb{Z}_q^m$*.*

When we speak of *lattice-based* FE schemes, we will make the same restrictions on FE schemes that have been made in [Ünal20]:

Definition 8 (Lattice-Based FE Scheme). *Let* $\mathsf{FE} = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *be an FE scheme. Let* q *be a prime and* $n, m \in \mathsf{poly}(\lambda)$*. Let* $d_1, d_2 \in \mathbb{N}$ *be constants. We call* FE ***lattice-based*** *if the following conditions are met:*

1. *The message space of* FE *is* $\mathcal{X} = \mathbb{Z}_p^n$*.*
2. *Each ciphertext of* FE *is an element of* $\mathbb{Z}_q^m$ *for prime* q*.*
3. Enc *is of depth* d_1*.*
4. *Each secret key output by* KeyGen *is a polynomial in* $\mathbb{Z}_q[Z_1, \ldots, Z_m]$ *of total degree* $\leq d_2$*, i.e., each secret key can be written as a linear combination of monomials containing at most* d_2 *(not necessarily different)* Z*-variables.*
5. *We have* $p < q$ *and the decryption algorithm* Dec *works as follows:*

$$\mathsf{Dec}(\mathsf{sk}, \mathsf{ct}) = \lceil \mathsf{sk}(\mathsf{ct}) \cdot p/q \rfloor \in \mathbb{Z}_p.$$

We call d_1 *the* ***encryption depth*** *and* d_2 *the* ***decryption depth*** *of* FE*.*

Definition 9. *We call* $\mathsf{FE} = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ ***(linearly) compact*** *if the dimension of ciphertexts is linear in the message length, i.e.,* $m \in O(n)$*.*

2.3 Secret-Key Encryption

We will define here secret-key encryption schemes as a special case of functional encryption schemes where the function spaces only contain the identity function.

Definition 10 (Secret-Key Encryption). *A **secret-key encryption** (SKE) scheme is an FE scheme* $\mathsf{SKE} = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *for a function space* $\mathcal{F}$*, where each* $\mathcal{F}_\lambda$ *only contains the identity function* $\mathsf{id}\colon \mathcal{X}_\lambda \to \mathcal{X}_\lambda$*.*

For an SKE scheme $\mathsf{SKE} = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$*, we will always assume that the master secret key* msk *and the derived key* $\mathsf{sk}_{\mathsf{id}}$ *of the identity are identical and that* $\mathsf{KeyGen}(\mathsf{msk}, \mathsf{id})$ *will always output* msk*. Subsequently, we will omit the algorithm* KeyGen *from the list of algorithms, i.e.,* $\mathsf{SKE} = (\mathsf{Setup}, \mathsf{Enc}, \mathsf{Dec})$*.*

For convenience, we also introduce the notion of *partial* secret-key encryption schemes. A partial SKE is essentially a normal SKE without a decryption algorithm.

Definition 11 (Partial Secret-Key Encryption). *A **partial secret-key encryption** scheme* $\mathsf{SKE} = (\mathsf{Setup}, \mathsf{Enc}, \_)$ *is a pair of algorithms* Setup *and* Enc *with a fitting message space* $\mathcal{X}$ *that adheres to the syntax in Definition 4.*

A fitting decryption algorithm *for* $(\mathsf{Setup}, \mathsf{Enc}, \_)$ *is an algorithm* Dec *s.t. the tuple* $(\mathsf{Setup}, \mathsf{Enc}, \mathsf{Dec})$ *is an SKE in the sense of Definition 10.*

Note that the notion of selective IND-CPA security in the sense of Definition 5 is well-defined for partial SKEs. Additionally, the notions of bounded encryption depth and width in the sense of Definitions 6 and 7 are well-defined for partial SKEs.

3 General Approach

We present here a general approach for showing lower bounds of lattice-based FE schemes in the sense of Definition 8. This approach generalizes the strategy of Ünal [Üna20] for function-hiding FE schemes and will be applied by us again on compact FE schemes. The key element for showing IND-CPA insecurity in [Üna20] was the following theorem.

Theorem 4 ([Üna20]). *Let* q *be a prime,* d *be a constant and* $B \in \mathsf{poly}(\lambda)$*. Let* $M = M(\lambda) \in \mathbb{N}$ *be such that* $M \geq 2d$ *and* $c \cdot M^d \cdot B < q$ *for some constant*[8] $c \in \mathbb{N}$ *that depends on* d*.*

Let $\mathsf{SKE} = (\mathsf{Setup}, \mathsf{Enc}, \_)$ *be a partial SKE scheme with message space* $\mathcal{X} := \{0, \dots, M\}$ *s.t.* Enc *is of depth* d *and width* B*. Then, the following are equivalent:*

1. SKE *is selectively IND-CPA secure against* PPT *adversaries.*
2. SKE *is selectively IND-CPA secure against unbounded adversaries (that get to know the secret key of* SKE*).*
3. *For each polynomial* $r \in \mathsf{poly}(\lambda)$ *there is an* $\varepsilon \in \mathsf{negl}(\lambda)$ *s.t. for* $\mathsf{msk} \leftarrow \mathsf{Setup}(1^\lambda)$*, it holds that*
$$\Pr\left[\forall x, y \in \mathcal{X}_\lambda\colon \Delta(\mathsf{Enc}(\mathsf{msk}, x), \mathsf{Enc}(\mathsf{msk}, y)) < \frac{1}{r(\lambda)}\right] \geq 1 - \varepsilon(\lambda).$$
4. *There is an* $\varepsilon \in \mathsf{negl}(\lambda)$ *s.t. we have* $\Delta(C_x, C_y) \leq \varepsilon(\lambda)$ *for all* $x, y \in \mathcal{X}$*, where* C_x *is the distribution that computes* $\mathsf{msk} \leftarrow \mathsf{Setup}(1^\lambda), \mathsf{ct}_x \leftarrow \mathsf{Enc}(\mathsf{msk}, x_\lambda)$ *and outputs* $(\mathsf{msk}, \mathsf{ct}_x)$*.*

In [Üna20], only the equivalence of the first and third statement has been shown. However, it is easy to see that the second and fourth statement are equivalent to the third statement.

Given a lattice-based FE scheme FE of encryption depth $d_1 \in O(1)$ and decryption depth $d_2 \in O(1)$, we want to use Theorem 4 to deduce lower bounds for FE. Towards this end, we construct a partial SKE for integer messages from FE as follows:

[8] More precisely, we have that $c = 2(d+1)^2(d!)^3 d^d$ as shown in [Üna20].

Definition 12. *Let* $\mathsf{FE} = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *be an FE scheme with functionality* $\mathcal{F}\colon \mathbb{Z}_p^n \to \mathbb{Z}_p$*. Let* $M \leq p$*. We construct a partial SKE scheme* $\mathsf{SKE}' = (\mathsf{Setup}', \mathsf{Enc}', \_)$ *with message space* $\mathcal{X}' := \{0, \dots, M\}$ *with the following algorithms:*

$\mathsf{Setup}'_{\mathsf{Pre}}$*:* *There is a preceding setup algorithm that on input* 1^λ *chooses functions* $f_1, \dots, f_Q \in \mathcal{F}$*. Then, it chooses an index* $i_* \in [Q]$ *and a degree-1 map*

$$\nu\colon \mathbb{Z}_p \longrightarrow \mathbb{Z}_p^n,$$

s.t. we have for all $x \in \mathbb{Z}_p$*,*

$$\begin{aligned} \forall i \neq i_*\colon f_i(\nu(x)) &= 0, \\ f_{i_*}(\nu(x)) &= x. \end{aligned}$$

It outputs $(f_1, \dots, f_Q, \nu, i_*)$*.*

Setup'*:* *On input* 1^λ*,* Setup' *runs* $(f_1, \dots, f_Q, \nu, i_*) \leftarrow \mathsf{Setup}'_{\mathsf{Pre}}(1^\lambda)$*. Then,* Setup' *computes* $\mathsf{msk} \leftarrow \mathsf{Setup}(1^\lambda)$ *and* $\mathsf{sk}_i \leftarrow \mathsf{KeyGen}(\mathsf{msk}, f_i)$ *for* $i \in [Q]$*, and outputs the new master secret key*

$$\mathsf{msk}' := (\mathsf{msk}, \mathsf{sk}_1, \dots, \mathsf{sk}_Q, \nu, i_*).$$

Enc'*:* *On input* $\mathsf{msk}' := (\mathsf{msk}, \mathsf{sk}_1, \dots, \mathsf{sk}_Q, \nu, i_*)$ *and a message* $x \in \{0, \dots, M\}$*,* Enc' *runs* $\mathsf{ct}_x \leftarrow \mathsf{Enc}(\mathsf{msk}, \nu(x))$ *and outputs the new ciphertext*

$$\mathsf{ct}'_x := (\mathsf{sk}_1(\mathsf{ct}_x), \dots, \mathsf{sk}_{i_*-1}(\mathsf{ct}_x), 0, \mathsf{sk}_{i_*+1}(\mathsf{ct}_x), \dots, \mathsf{sk}_Q(\mathsf{ct}_x)).$$

We demand that $\mathsf{Setup}'_{\mathsf{Pre}}$ *can be computed by a* PPT *algorithm.*

We now have the following result:

Lemma 2. *In the scheme* $\mathsf{SKE}' = (\mathsf{Setup}', \mathsf{Enc}', \_)$ *from Definition 12,* Enc' *is of depth* $d_1 \cdot d_2$*, if* FE *is lattice-based with encryption depth* d_1 *and decryption depth* d_2*.*

If FE *is correct and lattice-based, then* Enc' *is of width* $\lceil q/p \rfloor$*, and if* FE *is selectively IND-CPA secure, then* SKE' *is selectively IND-CPA secure.*

Proof. 1. Let FE be lattice-based with encryption depth d_1 and decryption depth d_2. Then, there is an algorithm $\mathsf{Enc}_{\mathsf{off}}$ that on input msk outputs m polynomials $r_1, \dots, r_m \in \mathbb{Z}_q[X_1, \dots, X_n]$ of degree $\leq d_1$ s.t. $\mathsf{Enc}(\mathsf{msk}, x)$ is equally distributed as $(r_1(x), \dots, r_m(x))$ for each $x \in \mathbb{Z}_p^n$.
We now define $\mathsf{Enc}_{\mathsf{off}}{}'$ as follows. On input $\mathsf{msk}' := (\mathsf{msk}, \mathsf{sk}_1, \dots, \mathsf{sk}_Q, \nu, i_*)$, $\mathsf{Enc}_{\mathsf{off}}{}'$ first computes $(r_1, \dots, r_m) \leftarrow \mathsf{Enc}_{\mathsf{off}}(\mathsf{msk})$ and then returns the polynomials

$$\begin{aligned} \forall i \neq i_*\colon r'_i(X) &:= \mathsf{sk}_i(r_1(\nu(X)), \dots, r_m(\nu(X))) \in \mathbb{Z}_q[X], \\ r'_{i_*}(X) &:= 0. \end{aligned}$$

The degree of each $\mathsf{sk}_i(r_1(\nu(X)), \dots, r_m(\nu(X)))$ is bounded by $d_1 \cdot d_2 \cdot 1$, since each sk_i is a polynomial in $\mathbb{Z}_q[Z_1, \dots, Z_m]$ of degree $\leq d_2$ and ν is an affine linear function, i.e., a degree-1 polynomial.
Moreover, for each $x \in \{0, \dots, M\}$ and msk', the output of $\mathsf{Enc}'(\mathsf{msk}', x)$ is identically distributed as $(r'_1(x), \dots, r'_Q(x))$ for $(r'_1, \dots, r'_Q) \leftarrow \mathsf{Enc}_{\mathsf{off}}{}'(\mathsf{msk}')$.

2. Let FE be correct, i.e., there is an $\varepsilon \in \mathsf{negl}(\lambda)$ s.t. for each $(g_\lambda)_\lambda \in \mathcal{F}$ and $(x_\lambda)_\lambda \in \mathcal{X}$ we have

$$\Pr_{\substack{\mathsf{msk} \leftarrow \mathsf{Setup}(1^\lambda) \\ \mathsf{sk} \leftarrow \mathsf{KeyGen}(\mathsf{msk}, g_\lambda) \\ \mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{msk}, x_\lambda)}} [\mathsf{Dec}(\mathsf{sk}, \mathsf{ct}) = g_\lambda(x_\lambda)] \geq 1 - \varepsilon(\lambda).$$

Since FE is lattice-based, Dec works as $\mathsf{Dec}(\mathsf{sk}, \mathsf{ct}) = \lceil \mathsf{sk}(\mathsf{ct}) \cdot p/q \rfloor$.

Assume, for the sake of contradiction, that Enc' is not of width q/p. This implies that there is one $\lambda \in \mathbb{N}$ and an $x' \in \{0, \ldots, M(\lambda)\}$ s.t.

$$\begin{aligned} Q(\lambda) \cdot \varepsilon(\lambda) &< \Pr_{\substack{\mathsf{msk}' \leftarrow \mathsf{Setup}'(1^\lambda) \\ \mathsf{ct}' \leftarrow \mathsf{Enc}'(\mathsf{msk}', x')}} \left[||\mathsf{ct}'||_\infty > \frac{q}{p} \right] \\ &= \Pr_{\substack{(f_1, \ldots, f_Q, \nu, i_*) \leftarrow \mathsf{Setup}'_{\mathsf{Pre}}(1^\lambda) \\ \mathsf{msk} \leftarrow \mathsf{Setup}(1^\lambda) \\ \forall i\colon\ \mathsf{sk}_i \leftarrow \mathsf{KeyGen}(\mathsf{msk}, f_i) \\ \mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{msk}, \nu(x'))}} \left[\exists i \neq i_*\colon\ |\mathsf{sk}_i(\mathsf{ct})| > \frac{q}{p} \right] \\ &= \Pr_{\substack{(f_1, \ldots, f_Q, \nu, i_*) \leftarrow \mathsf{Setup}'_{\mathsf{Pre}}(1^\lambda) \\ \mathsf{msk} \leftarrow \mathsf{Setup}(1^\lambda) \\ \forall i\colon\ \mathsf{sk}_i \leftarrow \mathsf{KeyGen}(\mathsf{msk}, f_i) \\ \mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{msk}, \nu(x'))}} \left[\exists i \neq i_*\colon\ \mathsf{Dec}(\mathsf{sk}_i, \mathsf{ct}) \neq 0 = f_i(\nu(x')) \right]. \end{aligned}$$

In particular, for this $\lambda \in \mathbb{N}$, there exists a tuple $(f_1, \ldots, f_Q, \nu, i_*)$ s.t.

$$\begin{aligned} Q(\lambda) \cdot \varepsilon(\lambda) &< \Pr_{\substack{\mathsf{msk} \leftarrow \mathsf{Setup}(1^\lambda) \\ \forall i\colon\ \mathsf{sk}_i \leftarrow \mathsf{KeyGen}(\mathsf{msk}, f_i) \\ \mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{msk}, \nu(x'))}} \left[\exists i \neq i_*\colon\ \mathsf{Dec}(\mathsf{sk}_i, \mathsf{ct}) \neq f_i(\nu(x')) \right] \\ &\leq \sum_{i \neq i_*} \Pr_{\substack{\mathsf{msk} \leftarrow \mathsf{Setup}(1^\lambda) \\ \mathsf{sk}_i \leftarrow \mathsf{KeyGen}(\mathsf{msk}, f_i) \\ \mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{msk}, \nu(x'))}} \left[\mathsf{Dec}(\mathsf{sk}_i, \mathsf{ct}) \neq f_i(\nu(x')) \right]. \end{aligned}$$

Hence, there is one $i \in [Q]$ s.t. $\Pr[\mathsf{Dec}(\mathsf{sk}_i, \mathsf{ct}) \neq f_i(\nu(x'))] > \varepsilon$. This contradicts the correctness of FE. Hence, our assumption must be wrong and Enc' must be of width q/p.

3. Let FE be selectively IND-CPA secure. We reduce the selective IND-CPA security of SKE' to the selective IND-CPA security of FE by constructing a reduction that transforms a PPT adversary $\mathcal{A}'$ against the selective IND-CPA security of SKE' to a PPT adversary $\mathcal{A}$ against the selective IND-CPA security of FE. If $\mathcal{A}'$ is an adversary against the selective IND-CPA security of SKE' and $\mathcal{C}'$ is a challenger for the selective IND-CPA security of FE, then $\mathcal{A}$ proceeds as follows:
   (a) On input 1^λ, $\mathcal{A}$ computes $(f_1, \ldots, f_Q, \nu, i_*) \leftarrow \mathsf{Setup}_{\mathsf{Pre}}(1^\lambda)$.
   (b) $\mathcal{A}$ runs $\mathcal{A}'(1^\lambda)$ to receive two lists $({x'_1}^0, \ldots, {x'_N}^0)$, $({x'_1}^1, \ldots, {x'_N}^1) \in \{0, \ldots, M\}^N$ of candidate messages.
   (c) For each $i \in [N], \beta \in \{0,1\}$, $\mathcal{A}$ sets $x_i^\beta := \nu({x'_i}^\beta) \in \mathbb{Z}_p^{n_1}$.
   (d) $\mathcal{A}$ submits the message lists $(x_1^0, \ldots, x_N^0)$, $(x_1^1, \ldots, x_N^1)$ and the function list $(f_1, \ldots, f_{i_*-1}, f_{i_*+1}, \ldots, f_Q)$ to $\mathcal{C}'$. It receives secret keys $\mathsf{sk}_1, \ldots, \mathsf{sk}_{i_*-1}, \mathsf{sk}_{i_*+1}, \ldots, \mathsf{sk}_Q$ for the functions $f_1, \ldots, f_{i_*-1}, f_{i_*+1}, \ldots, f_Q$ and ciphertexts $\mathsf{ct}_1, \ldots, \mathsf{ct}_N$ for $x_1^b, \ldots, x_N^b$ with an unknown b.
   (e) For each $i \in [N]$, $\mathcal{A}$ computes

$$\mathsf{ct}'_i := (\mathsf{sk}_1(\mathsf{ct}_i), \ldots, \mathsf{sk}_{i_*-1}(\mathsf{ct}_i), 0, \mathsf{sk}_{i_*+1}(\mathsf{ct}_i) \ldots, \mathsf{sk}_Q(\mathsf{ct}_i)),$$

   and sends the list $(\mathsf{ct}'_1, \ldots, \mathsf{ct}'_N)$ to $\mathcal{A}'$.
   (f) $\mathcal{A}'$ responds with a guess $b' \in \{0,1\}$. $\mathcal{A}$ forwards b' to $\mathcal{C}'$.

   The view of $\mathcal{A}'$ in the interaction with $\mathcal{A}$ is identical to its view in $\mathsf{Exp}^{\mathsf{ind\text{-}cpa}}_{\mathsf{SKE}'}$. Furthermore, $\mathcal{A}$ wins exactly iff $\mathcal{A}'$ wins. This is, because we have for all $j \in [N]$ and $i \neq i_*$,

$$f_i(x_j^0) = f_i(\nu({x'_j}^0)) = 0 = f_i(\nu({x'_j}^1)) = f_i(x_j^1).$$

   In other words, $\mathcal{A}$ does not submit any combination of function and message pairs that would help it to win trivially. Hence, $\mathcal{A}$ is a valid adversary in the selective IND-CPA security game of FE. In conclusion, the advantage of $\mathcal{A}$ in the selective IND-CPA security game of FE is equal to the advantage of $\mathcal{A}'$ in the selective IND-CPA security game of SKE'.

Hence, the claims of the lemma are proven. □

Corollary 1. *Let* FE *be a lattice-based, correct and selectively IND-CPA secure FE scheme of constant encryption depth* $d_1 \in O(1)$ *and decryption depth* $d_2 \in O(1)$ *s.t. the message space of* FE *is* $\mathbb{Z}_p^n$ *and each ciphertext of* FE *is a vector in* $\mathbb{Z}_q^m$ *for* $q > p > 2$*, where* q *is prime.*

Let $M \in \mathsf{poly}(\lambda)$ *and assume that we have* $q/p \in \mathsf{poly}(\lambda)$*,* $M \geq 2d_1 \cdot d_2$ *and* $c \cdot M^{d_1 \cdot d_2} < p$ *for some constant* c *that depends on* $d_1 \cdot d_2$*.*

Let $\mathsf{SKE}' = (\mathsf{Setup}', \mathsf{Enc}', \_)$ *be the partial SKE scheme from Definition 12 that is constructed from* FE *with message space* $\{0, \ldots, M\}$*.*

Then, there is no (computationally unbounded) algorithm Dec' *s.t. the scheme* $(\mathsf{Setup}', \mathsf{Enc}', \mathsf{Dec}')$ *has a non-negligible advantage at correctly decrypting ciphertexts, i.e., there is an* $\varepsilon \in \mathsf{negl}(\lambda)$ *s.t. we have for each* Dec'*,*

$$\Pr_{\substack{x \leftarrow \{0,\ldots,M\},\\ \mathsf{msk}' \leftarrow \mathsf{Setup}'(1^\lambda),\\ \mathsf{ct}' \leftarrow \mathsf{Enc}'(\mathsf{msk}', x),\\ y \leftarrow \mathsf{Dec}'(\mathsf{msk}', \mathsf{ct}')}} [x = y] \leq \frac{1}{M+1} + \varepsilon(\lambda).$$

Proof. Set $\mathcal{X}' := \{0, \ldots, M\}$. Because of Lemma 2, we can apply Theorem 4 on SKE'. Therefore, there is an $\varepsilon \in \mathsf{negl}(\lambda)$ s.t. the distributions

$$(\mathsf{msk}', \mathsf{ct}'_x) \quad \text{with} \quad \mathsf{msk}' \leftarrow \mathsf{Setup}'(1^\lambda),\ \mathsf{ct}'_x \leftarrow \mathsf{Enc}'(\mathsf{msk}', x),$$

for all $x \in \mathcal{X}'_\lambda$, have negligible distance $\varepsilon(\lambda)$ to each other. It follows that the distributions $\mathsf{Dec}'(\mathsf{msk}', \mathsf{ct}'_x)$, for all $x \in \mathcal{X}'_\lambda$, are in statistically negligible distance to each other. In particular, there is a negligible $\varepsilon' \in \mathsf{negl}(\lambda)$ s.t.

$$\Delta(\mathsf{Dec}(\mathsf{msk}'_1, \mathsf{ct}'_x), \mathsf{Dec}(\mathsf{msk}'_2, \mathsf{ct}'_y)) \leq \varepsilon', \tag{4}$$

for all $x, y \in \mathcal{X}'_\lambda$, where we sample $\mathsf{msk}'_1, \mathsf{msk}'_2 \leftarrow \mathsf{Setup}'(1^\lambda), \mathsf{ct}'_x \leftarrow \mathsf{Enc}'(\mathsf{msk}'_1, x), \mathsf{ct}'_y \leftarrow \mathsf{Enc}'(\mathsf{msk}'_2, y)$.

Assume for the sake of contradiction, that there would be an $r \in \mathsf{poly}(\lambda)$ s.t.

$$\Pr_{\substack{x \leftarrow \{0,\ldots,M\} = \mathcal{X}'_\lambda\\ \mathsf{msk}' \leftarrow \mathsf{Setup}'(1^\lambda)\\ \mathsf{ct}' \leftarrow \mathsf{Enc}'(\mathsf{msk}', x)}} \left[\mathsf{Dec}'(\mathsf{msk}', \mathsf{ct}') = x\right] \geq \frac{1}{\#\,\mathcal{X}'_\lambda} + \frac{1}{r(\lambda)}, \tag{5}$$

for infinitely many $\lambda \in \mathbb{N}$. For those λ, we have, when we sample $x \leftarrow \mathcal{X}'_\lambda, \mathsf{msk}' \leftarrow \mathsf{Setup}'(1^\lambda), \mathsf{ct}' \leftarrow \mathsf{Enc}(\mathsf{msk}', x)$,

$$\begin{aligned}
& \Pr\left[\mathsf{Dec}'(\mathsf{msk}', \mathsf{ct}'_x) \in \mathcal{X}\right] \\
= \quad & \sum_{y \in \mathcal{X}'_\lambda} \Pr\left[\mathsf{Dec}'(\mathsf{msk}', \mathsf{ct}'_x) = y\right] \\
\overset{Equation\ (4)}{\geq} \quad & \sum_{y \in \mathcal{X}'_\lambda} \left(\Pr\left[\mathsf{Dec}'(\mathsf{msk}', \mathsf{ct}'_y) = y\right] - \varepsilon'(\lambda)\right) \\
= \quad & -\#\,\mathcal{X}'_\lambda \cdot \varepsilon'(\lambda) + \sum_{y \in \mathcal{X}'_\lambda} \Pr_{z \leftarrow \mathcal{X}'_\lambda}\left[\mathsf{Dec}'(\mathsf{msk}', \mathsf{ct}'_z) = z | z = y\right] \\
= \quad & -(M+1) \cdot \varepsilon'(\lambda) + \#\,\mathcal{X}'_\lambda \cdot \sum_{y \in \mathcal{X}'_\lambda} \Pr_{z \leftarrow \mathcal{X}'_\lambda}\left[\mathsf{Dec}'(\mathsf{msk}', \mathsf{ct}'_z) = z | z = y\right] \cdot \Pr_{z \leftarrow \mathcal{X}'_\lambda}[z = y] \\
= \quad & -(M+1) \cdot \varepsilon'(\lambda) + (M+1) \cdot \Pr_{z \leftarrow \mathcal{X}'_\lambda}\left[\mathsf{Dec}'(\mathsf{msk}', \mathsf{ct}'_z) = z\right] \\
\overset{Equation\ (5)}{\geq} \quad & 1 + \frac{M+1}{r(\lambda)} - (M+1) \cdot \varepsilon'(\lambda).
\end{aligned}$$

However, $1 + \frac{M+1}{r(\lambda)} - (M+1)\varepsilon'(\lambda)$ becomes larger than 1 for $\varepsilon'(\lambda)$ small enough. Hence, we reach a contradiction. □

4 Lower Bounds for Compact Functional Encryption

In this section we prove the main result of this paper. Towards this end, we introduce the space of d-linear functions over $\mathbb{Z}_p$. A function $f\colon (\mathbb{Z}_p^n)^d \to \mathbb{Z}_p$ is called **d-linear** iff, for vectors of variables $X^{(1)} = (X_1^{(1)}, \ldots, X_n^{(1)})$, $\ldots$, $X^{(d)} = (X_1^{(d)}, \ldots, X_n^{(d)})$, the expression $f(X^{(1)}, \ldots, X^{(d)})$ is linear in $X^{(i)}$ for each $i \in [d]$. Equivalently, one can require that $f(X^{(1)}, \ldots, X^{(d)})$ is given by $\phi(X^{(1)} \otimes \cdots \otimes X^{(d)})$, for a linear function ϕ, where $\otimes$ denotes the Kronecker product.

In the following, we consider the functionality $\mathcal{F}\colon \mathcal{X} \to \mathcal{Y}$ of d-linear functions, where the message space is $\mathcal{X} = \mathbb{Z}_p^{d \times n}$ and the value space is $\mathcal{Y} = \mathbb{Z}_p$.

Theorem 5. *Let $d > 1$ be a constant and $q > p > 2$ with q prime. Let $Q = n^d$, $m \in O(n)$ and let $D \in O(1)$ be the constant from Lemma 1.*

Let $\mathsf{FE} = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ be a lattice-based FE for the functionality $\mathcal{F}$ s.t. we have:

1. *FE is compact, i.e., the dimension $m \in O(n)$ of ciphertexts is linear.*
2. *The decryption depth of FE is d.*
3. *We have*

$$q/p \in \mathsf{poly}(\lambda) \qquad \text{and} \qquad c \cdot (\max\{2d_1 \cdot d + 1, 2D + 1\})^{d_1 \cdot d} < p,$$

where d_1 denotes the encryption depth of FE and c is the constant from Theorem 4.

If FE is correct, then FE is not selectively IND-CPA secure.

Remark 1. We remark two things about the requirements of Theorem 5:

1. We do not specify if there is an arithmetic reduction modulo p when evaluating the polynomials in $\mathcal{F} \subset \mathbb{Z}_p[X^{(1)}, \ldots, X^{(d)}]$ on messages. In fact, this is irrelevant for our proof, since it will only consider monomial functions $X_{i_1}^{(1)} \cdots X_{i_d}^{(d)} \in \mathcal{F}$. Furthermore, at most one entry of each message vector that our adversary considers will not lie in $\{0, 1\}$. Hence, evaluations $f(x)$ will never exceed p.
2. The space of d-linear functions is contained in the space of degree-d polynomials. Hence, any compact FE scheme with decryption depth d for degree-d polynomials implies a compact FE scheme for d-linear functions with the same decryption depth d.

Our proof idea for Theorem 5 is to assume that FE is secure, and then, to use Corollary 1 to deduce a contradiction. Set $M = \max\{2D + 1, 2d_1 \cdot d + 1\}$ and let $\mathcal{X}' := \{0, \ldots, M\}$ be the message space of a new SKE scheme SKE' that we will construct in the following according to Definition 12. Towards this end, we define the following $\mathsf{Setup}'_{\mathsf{Pre}}$ algorithm for the FE scheme in Theorem 5:

$\mathsf{Setup}'_{\mathsf{Pre}}$: On input 1^λ, $\mathsf{Setup}'_{\mathsf{Pre}}$ sets $Q = n^d$ and fixes deterministically an enumeration $\alpha_1, \ldots, \alpha_Q$ of $[n]^d$. For each tuple of indices $\alpha_i = (\alpha_{i,1}, \ldots, \alpha_{i,d}) \in [n]^d$, it sets

$$f_i(X^{(1)}, \ldots, X^{(d)}) := X_{\alpha_{i,1}}^{(1)} \cdots X_{\alpha_{i,d}}^{(d)}.$$

Additionally, it draws $i_* \leftarrow [Q]$ uniformly at random and sets $(\alpha_{*,1}, \ldots, \alpha_{*,d}) := \alpha_* := \alpha_{i_*} \in [n]^d$. Furthermore, it sets

$$\begin{aligned} \nu\colon \mathbb{Z}_p &\longrightarrow \mathbb{Z}_p^{d \times n} \\ x &\longmapsto (x \cdot e_{\alpha_{*,1}}, e_{\alpha_{*,2}}, \ldots, e_{\alpha_{*,d}}), \end{aligned}$$

where e_j denotes the j-th unit vector in $\mathbb{Z}_p^n$ for $j \in [n]$. It outputs $f_1, \ldots, f_Q$, ν and i_*. Note that we have for all $x \in \mathbb{Z}_p$,

$$\begin{aligned} \forall i \neq i_*\colon f_i(\nu(x)) &= 0, \\ f_{i_*}(\nu(x)) &= x. \end{aligned}$$

Given $\mathsf{Setup}'_{\mathsf{Pre}}$, we can define the partial SKE scheme $\mathsf{SKE}' = (\mathsf{Setup}', \mathsf{Enc}', \_)$ as in Definition 12. To prove Theorem 5, we assume that FE is selectively IND-CPA secure. Subsequently, we construct a fitting decryption algorithm Dec' that has a non-negligible advantage at decrypting ciphertexts of SKE'. This in turn yields a contradiction to Corollary 1, thereby, proving that FE cannot be secure. To construct Dec', we first derandomize the key generation algorithm KeyGen of FE, i.e., we can assume—without loss of generality—that KeyGen is a deterministic algorithm. In fact, if KeyGen is probabilistic, we can distinguish two cases: first, if one-way functions (OWFs) do not exist, then in particular IND-CPA secure SKEs cannot exist, and hence, FE cannot be IND-CPA secure. Second, if OWFs do exist, we can construct secure pseudorandom functions (PRFs) out of them. Using a PRF PRF, we can derandomize KeyGen as follows: we change Setup s.t. it additionally samples a random key k for PRF and adds it to the output master secret key msk. Then, KeyGen on input msk and $f \in \mathcal{F}$, does not generate new random coins, instead it evaluates PRF on k and a description of f and uses the output of $\mathsf{PRF}(k, f)$ as bits for its random tape.

To continue the proof, we will now show some necessary properties of FE:

Lemma 3. *There is a constant $D \in O(1)$ s.t. for each master secret key $\mathsf{msk}' = (\mathsf{msk}, \mathsf{sk}_1, \dots, \mathsf{sk}_Q, \nu, i_*)$ output by Setup', there exists a polynomial $h_{\mathsf{msk}} \in \mathbb{Z}_q[T_1, \dots, T_Q]$ with the following properties:*

$$h_{\mathsf{msk}} \neq 0 \in \mathbb{Z}_q[T_1, \dots, T_Q], \tag{6}$$
$$h_{\mathsf{msk}}(\mathsf{sk}_1, \dots, \mathsf{sk}_Q) = 0 \in \mathbb{Z}_q[Y_1, \dots, Y_m], \tag{7}$$
$$\deg h_{\mathsf{msk}} \leq D. \tag{8}$$

Furthermore, h_{msk} only depends on msk.

Proof. Since $Q = n^d$ and $m = O(n)$, we have $Q \in \Omega(m^d)$. Moreover, Theorem 5 requires each secret key sk_i to be a polynomial over $\mathbb{Z}_q$ of degree d. Lemma 1 now implies that there is a constant D such that for each collection of degree-d polynomials $\mathsf{sk}_1, \dots, \mathsf{sk}_Q \in \mathbb{Z}_q[Y_1, \dots, Y_m]$ there exists an algebraic relationship h that fulfills the requirements in Equations (6) to (8).

Now, fix some msk. Since $\mathsf{Setup}'_{\mathsf{Pre}}$ chooses the functions $f_1, \dots, f_Q$ deterministically and since we can assume that KeyGen is derandomized, the secret keys $\mathsf{sk}_1 \leftarrow \mathsf{KeyGen}(\mathsf{msk}, f_1)$,..., $\mathsf{sk}_Q \leftarrow \mathsf{KeyGen}(\mathsf{msk}, f_Q)$ only depend on msk. Since the algebraic relationship h only depends on q and $\mathsf{sk}_1, \dots, \mathsf{sk}_Q$, it follows that each choice of msk determines a relationship h_{msk} of degree $\leq D$. □

Note that $h_{\mathsf{msk}}(\mathsf{sk}_1(Y), \dots, \mathsf{sk}_m(Y))$ is the zero polynomial of $\mathbb{Z}_q[Y_1, \dots, Y_m]$, which vanishes on each ciphertext of FE. If we choose h_{msk} of minimal degree, we know that $h_{\mathsf{msk}}(T_1, \mathsf{sk}_2(Y), \dots, \mathsf{sk}_m(Y)) \in \mathbb{Z}_q[T_1, Y_2, \dots, Y_m]$ cannot be zero. However, it may happen that $h_{\mathsf{msk}}(T_1, \mathsf{sk}_2(Y), \dots, \mathsf{sk}_m(Y))$ vanishes on almost all ciphertexts of FE. For our decryption algorithm Dec', it will be important that we have for $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{msk}, x)$,

$$\Pr\left[h_{\mathsf{msk}}(T_1, \dots, T_{i_*-1}, \mathsf{sk}_{i_*}(\mathsf{ct}), \mathsf{sk}_{i_*+1}(\mathsf{ct}), \dots, \mathsf{sk}_m(\mathsf{ct})) = 0\right] \in 1 - \mathsf{negl}(\lambda),$$
$$\Pr\left[h_{\mathsf{msk}}(T_1, \dots, T_{i_*-1}, \quad T_{i_*} \quad, \mathsf{sk}_{i_*+1}(\mathsf{ct}), \dots, \mathsf{sk}_m(\mathsf{ct})) \neq 0\right] \notin \mathsf{negl}(\lambda).$$

Because, if there is a ciphertext $\mathsf{ct} \in \mathbb{Z}_q^m$ s.t. $h_{\mathsf{msk}}(T_1, \dots, T_{i_*-1}, \mathsf{sk}_{i_*}(\mathsf{ct}), \dots, \mathsf{sk}_m(\mathsf{ct})) = 0$, but $h_{\mathsf{msk}}(T_1, \dots, T_{i_*}, \mathsf{sk}_{i_*+1}(\mathsf{ct}), \dots, \mathsf{sk}_m(\mathsf{ct})) \neq 0$, then $\mathsf{sk}_{i_*}(\mathsf{ct})$ is a root of the polynomial $h_{\mathsf{msk}}(T_1, \dots, T_{i_*}, \mathsf{sk}_{i_*+1}(\mathsf{ct}), \dots, \mathsf{sk}_m(\mathsf{ct}))$, which we consider as a univariate polynomial with coefficients in $\mathbb{Z}_q[T_1, \dots, T_{i_*-1}]$ and unknown T_{i_*}. Since this polynomial is non-zero, it has at most $\deg h_{\mathsf{msk}} \leq D$ different roots. In such cases, Dec' can limit the number of potential values for $f_{i_*}(x)$ to D, which gives Dec' a non-negligible advantage at decryption. To make these ideas concrete, let us introduce some technicalities.

Lemma 4. *There exists a map $\mathcal{I}\colon \mathbb{N} \to P(\mathbb{N})$ s.t.*

$$\forall \lambda \in \mathbb{N}\colon \mathcal{I}(\lambda) \subseteq [Q(\lambda)] \quad \textit{and} \quad \#\mathcal{I}(\lambda) = D.$$

Additionally, the probability when we sample $\mathsf{msk} \leftarrow \mathsf{Setup}(1^\lambda)$ that h_{msk} contains non-trivially a monomial $T_{i_1} \cdots T_{i_{D'}}$ for some $D' \leq D$ with $i_1, \dots, i_{D'} \in \mathcal{I}(\lambda)$ is larger than $Q(\lambda)^{-D}$.

Proof. For each msk, h_{msk} must be a non-zero polynomial in $\mathbb{Z}_q[T_1, \ldots, T_Q]$ of degree $\leq D$. Since $\mathbb{Z}_q[T_1, \ldots, T_Q]$ contains $\binom{Q+D}{D} \leq Q^D$ monomials of degree $\leq D$, there must exist one monomial $T_{i_1} \cdots T_{i_{D'}}$ for each $\lambda \in \mathbb{N}$ s.t.

$$\Pr_{\mathsf{msk} \leftarrow \mathsf{Setup}(1^\lambda)} \left[h \text{ contains } T_{i_1} \cdots T_{i_{D'}} \right] \geq Q^{-D}.$$

Hence, we can choose $\mathcal{I}(\lambda)$ s.t. it contains $i_1, \ldots, i_{D'}$. □

By permuting the indices $1, \ldots, Q(\lambda)$ for each $\lambda \in \mathbb{N}$, we can enforce that the set $\mathcal{I}(\lambda)$ will be $\{1, \ldots, D\}$ for each λ. This is simply a relabelling of indices that does not change the algorithms Setup and Setup', but reduces some notations in the following.

We will call a master secret key msk **good**, if h_{msk} contains non-trivially a monomial $T_{i_1} \cdots T_{i_{D'}}$ with $i_1, \ldots, i_{D'} \in \mathcal{I}(\lambda) = \{1, \ldots, D\}$, and we will call msk **bad**, otherwise. Denote by $\mathsf{Setup}_{\mathsf{good}}(1^\lambda)$ the distribution of $\mathsf{Setup}(1^\lambda)$ conditioned on the output msk being good. For $\mathsf{Setup}_{\mathsf{good}}$, we have the following:

Theorem 6. *For $u, n \in \mathbb{N}$, set $E_u := \{e_i \cdot v \mid i \in [n], v \in \{0, \ldots, u\}\} \subset \mathbb{Z}_p^n$ where e_i denotes the i-th unit vector. Consider the poly-size subspace*

$$\widetilde{\mathcal{X}} := E_M \times E_1 \times \ldots \times E_1 \subset (\mathbb{Z}_p^n)^d.$$

For $\lambda \in \mathbb{N}$, $x \in \widetilde{\mathcal{X}}_\lambda$ and $i \in \{1, \ldots, D+1\}$, set

$$p_\lambda(i, x) := \Pr_{\substack{\mathsf{msk} \leftarrow \mathsf{Setup}_{\mathsf{good}}(1^\lambda) \\ \mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{msk}, x)}} \left[h_{\mathsf{msk}}(T_1, \ldots, T_{i-1}, \mathsf{sk}_i(\mathsf{ct}), \ldots, \mathsf{sk}_Q(\mathsf{ct})) = 0 \right].$$

There is an index $i_\dagger \in [D]$ and functions $\varepsilon \in \mathsf{negl}(\lambda)$, $\rho \notin \mathsf{negl}(\lambda), \rho \geq 0$ s.t. we have for all $\lambda \in \mathbb{N}$ and $x \in \widetilde{\mathcal{X}}_\lambda$,

$$p_\lambda(i_\dagger, x) \geq 1 - \varepsilon(\lambda),$$
$$p_\lambda(i_\dagger, x) - p_\lambda(i_\dagger + 1, x) \geq \rho(\lambda).$$

Since the proof of Theorem 6 is very technical and requires a lot of lemmata, we defer it to Section 5. Theorem 6 guarantees some homogeneity among ciphertexts of different messages. In particular, it states that the polynomial $h_{\mathsf{msk}}(T_1, \ldots, T_{i_\dagger - 1}, \mathsf{sk}_{i_\dagger}(\mathsf{ct}), \ldots, \mathsf{sk}_Q(\mathsf{ct}))$ will almost always vanish on a ciphertext $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{msk}, x)$, for any message $x \in \widetilde{\mathcal{X}}$, while the polynomial $h_{\mathsf{msk}}(T_1, \ldots, T_{i_\dagger}, \mathsf{sk}_{i_\dagger + 1}(\mathsf{ct}), \ldots, \mathsf{sk}_Q(\mathsf{ct}))$ (in which the variable $T_{i_\dagger}$ remains unsubstituted) will with non-negligible probability not vanish.

Proof (Theorem 5). Assume, for the sake of contradiction, that FE is selectively IND-CPA secure. If that was the case, then SKE' would be selectively IND-CPA secure as well. We lead this assumption to a contradiction by constructing a (computationally unbounded) decryption algorithm Dec' for SKE' that has a non-negligible advantage at decrypting correctly, i.e., there is a $\rho'(\lambda) \notin \mathsf{negl}(\lambda)$ s.t.

$$\Pr_{\substack{x' \leftarrow \{0, \ldots, M\}, \\ \mathsf{msk}' \leftarrow \mathsf{Setup}'(1^\lambda), \\ \mathsf{ct}' \leftarrow \mathsf{Enc}'(\mathsf{msk}', x'), \\ y' \leftarrow \mathsf{Dec}'(\mathsf{msk}', \mathsf{ct}')}} [x' = y'] \geq \frac{1}{M+1} + \rho'(\lambda).$$

This directly contradicts Corollary 1 and proves that the assumption is wrong. Hence, FE must be insecure.

First, we sketch the strategy of Dec'. Towards this end, let $\mathsf{msk}' = (\mathsf{msk}, \mathsf{sk}_1, \ldots, \mathsf{sk}_Q, \nu, i_*) \leftarrow \mathsf{Setup}'(1^\lambda)$, $x' \in \mathcal{X}'$ and $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{msk}, \nu(x'))$. Then, a ciphertext $\mathsf{ct}' := (c_1, \ldots, c_Q) \leftarrow \mathsf{Enc}'(\mathsf{msk}', x')$ is given by

$$c_i = \begin{cases} \mathsf{sk}_i(\mathsf{ct}), & \text{if } i \neq i_*, \\ 0, & \text{if } i = i_*. \end{cases}$$

On input $(\mathsf{msk}', \mathsf{ct}')$, Dec' proceeds as follows:

1. Dec' checks if msk is good. If msk is bad, Dec' terminates by outputting a uniformly random element of $\mathcal{X}' := \{0, \ldots, M\}$.
2. Dec' computes $i_\dagger \in [D]$ from Theorem 6. If $i_\dagger \neq i_*$, Dec' terminates by outputting a uniformly random element of $\mathcal{X}' := \{0, \ldots, M\}$.
3. Dec' computes the set

$$A(\mathsf{msk}) := \left\{ w \in \mathbb{Z}_q^m \mid h_{\mathsf{msk}}(T_1, \ldots, T_{i_*-1}, \mathsf{sk}_{i_*}(w), \ldots, \mathsf{sk}_Q(w)) = 0 \right\}.$$

   According to Theorem 6, the original ciphertext ct of $\mathsf{Enc}(\mathsf{msk}, \nu(x'))$ lies in $A(\mathsf{msk})$ with overwhelming probability $p_\lambda(i_\dagger, x') \geq 1 - \varepsilon(\lambda)$. However, since Dec' does not know ct, it cannot check if ct lies in $A(\mathsf{msk})$. Hence, Dec assumes from here on that ct lies in $A(\mathsf{msk})$.
4. Dec' computes the subset

$$B(\mathsf{msk}) := \{ w \in A(\mathsf{msk}) \mid h_{\mathsf{msk}}(T_1, \ldots, T_{i_*}, \mathsf{sk}_{i_*+1}(w), \ldots, \mathsf{sk}_Q(w)) \neq 0 \}.$$

   Again, according to Theorem 6, ct lies with non-negligible probability $1 - p_\lambda(i_\dagger + 1, x') \geq \rho(\lambda)$ in $B(\mathsf{msk})$. Under the assumption that ct lies in $A(\mathsf{msk})$, Dec' can now check if ct lies in $B(\mathsf{msk})$. If ct does not lie in $B(\mathsf{msk})$, Dec' outputs a uniformly random element of $\mathcal{X}'$ and stops.
5. At this point, Dec' knows that ct lies in $B(\mathsf{msk})$ and can compute the set

$$S(\mathsf{msk}, \mathsf{ct}') := \{ \mathsf{sk}_{i_*}(w) \mid w \in B(\mathsf{msk}), \forall i \neq i_* \colon \mathsf{sk}_i(w) = \mathsf{sk}_i(\mathsf{ct}) \}.$$

   It is clear that $S(\mathsf{msk}, \mathsf{ct}')$ must contain $\mathsf{sk}_{i_*}(\mathsf{ct})$. We will show that $S(\mathsf{msk}, \mathsf{ct}')$ contains at most $\deg h_{\mathsf{msk}} \leq D \leq M/2$ different values. Dec' chooses a uniformly random value $\mathsf{sk}_{i_*}(w)$ from $S(\mathsf{msk}, \mathsf{ct}')$ and outputs

$$\left\lceil \mathsf{sk}_{i_*}(w) \cdot \frac{p}{q} \right\rfloor = \mathsf{Dec}(\mathsf{sk}_{i_*}, w) \in \mathbb{Z}_p.$$

Let y' be the value output by $\mathsf{Dec}'(\mathsf{msk}', \mathsf{ct}')$. Since Dec' outputs a uniformly random element of $\{0, \ldots, M\}$ whenever msk is bad or $i_* \neq i_\dagger$, it suffices to lower-bound the probability of Dec' to return the correct message x' in the case where msk is good and $i_* = i_\dagger$ (both events will happen with non-negligible probability $\geq Q^{-D-1}$). In this case, we have

$$\begin{aligned}
\Pr[y' = x'] \geq{}& \Pr[y' = x' \mid \mathsf{ct} \in A(\mathsf{msk})] \cdot \Pr[\mathsf{ct} \in A(\mathsf{msk})] \\
&+ \Pr[y' = x' \mid \mathsf{ct} \notin A(\mathsf{msk})] \cdot \Pr[\mathsf{ct} \notin A(\mathsf{msk})] \\
\geq{}& \Pr[y' = x' \mid \mathsf{ct} \in A(\mathsf{msk})] \cdot (1 - \varepsilon(\lambda)) \\
\geq{}& \Pr[y' = x' \mid \mathsf{ct} \in A(\mathsf{msk})] - \varepsilon(\lambda) \\
\geq{}& \Pr[y' = x' \mid \mathsf{ct} \in B(\mathsf{msk})] \cdot \rho(\lambda) \\
&+ \Pr[y' = x' \mid \mathsf{ct} \in A(\mathsf{msk}) \setminus B(\mathsf{msk})] \cdot (1 - \rho(\lambda)) - \varepsilon(\lambda) \\
\geq{}& \Pr[y' = x' \mid \mathsf{ct} \in B(\mathsf{msk})] \cdot \rho(\lambda) + \frac{1}{M+1} \cdot (1 - \rho(\lambda)) - \varepsilon(\lambda) \\
\geq{}& \frac{2}{M} \cdot \rho(\lambda) + \frac{1}{M+1} \cdot (1 - \rho(\lambda)) - \varepsilon(\lambda) \geq \frac{\rho(\lambda)}{M} + \frac{1}{M+1}.
\end{aligned}$$

This yields a contradiction with the statement of Corollary 1.

What remains is to show that the set $S(\mathsf{msk}, \mathsf{ct}')$ contains at most $D < M/2$ elements for $\mathsf{ct} \in B(\mathsf{msk})$. To this end, set

$$g(T_{i_*}) = h_{\mathsf{msk}}(T_1, \ldots, T_{i_*}, \mathsf{sk}_{i_*+1}(\mathsf{ct}), \ldots, \mathsf{sk}_Q(\mathsf{ct})).$$

We consider g as a univariate polynomial with coefficients in $\mathbb{Z}_q[T_1, \ldots, T_{i_*-1}]$ and of degree $\leq D$. Since $\mathsf{ct} \in B(\mathsf{msk})$, we know that g is not the zero polynomial. On the other hand, we know that $g(\mathsf{sk}_*(\mathsf{ct})) = 0$, since we assume $\mathsf{ct} \in A(\mathsf{msk})$. In fact, each element of $S(\mathsf{msk}, \mathsf{ct}')$ is a root of g. It follows that $S(\mathsf{msk}, \mathsf{ct}')$ has at most $\deg g \leq \deg h_{\mathsf{msk}} \leq D < M/2$ elements. Since $x' \in \mathcal{X}'$ was chosen arbitrarily, the non-negligible advantage of Dec' at decryption follows. □

5 Proof of Theorem 6

We first introduce the following notion:

Definition 13. *For a fixed master secret key* msk *and a subset* $A \subset [Q]$*, denote by* $\tau_{\mathsf{msk},A}\colon \mathbb{Z}_q[T] \to \mathbb{Z}_q[T,Y]$ *the ring morphism that substitutes* T_i *by* $s_i(Y)$ *iff* $i \in A$*, i.e.,*

$$\tau_{\mathsf{msk},A}\colon \mathbb{Z}_q[T_1,\dots,T_Q] \longrightarrow \mathbb{Z}_q[T_1,\dots,T_Q,Y_1,\dots,Y_m]$$
$$T_i \longmapsto \begin{cases} \mathsf{sk}_i(Y), & i \in A, \\ T_i, & i \notin A. \end{cases}$$

Lemma 5. *Let* $D \in O(1)$*. For each* $\lambda \in \mathbb{N}$*, let* p'_λ *be a monotonically decreasing function*

$$p'_\lambda\colon \{1,\dots,D+1\} \longrightarrow [0,1]$$

s.t. $p'_\lambda(1) = 1$ *and* $p'_\lambda(D+1) = 0$*.*

Then, there is an $i_\dagger \in [D]$*, an* $\varepsilon' \in \mathsf{negl}(\lambda)$ *and an* $r' \in \mathsf{poly}(\lambda)$ *s.t.*

$$\forall \lambda \in \mathbb{N}\colon p'_\lambda(i_\dagger) \geq 1 - \varepsilon'(\lambda),$$
$$\exists_\infty \lambda \in \mathbb{N}\colon p'_\lambda(i_\dagger) - p'_\lambda(i_\dagger + 1) \geq \frac{1}{r'(\lambda)}.$$

Proof. Let $i_\dagger \in [D]$ be minimal s.t. there is an $r' \in \mathsf{poly}(\lambda), r' > 0$, with

$$\exists_\infty \lambda \in \mathbb{N}\colon p'_\lambda(i_\dagger) - p'_\lambda(i_\dagger + 1) \geq \frac{1}{r'(\lambda)}.$$

Since D is constant, such an $i_\dagger$ must exist. Since $i_\dagger$ is minimal, there are negligible functions $\varepsilon_1,\dots,\varepsilon_{i_\dagger - 1} \in \mathsf{negl}(\lambda)$ s.t. for $i < i_\dagger$,

$$p_\lambda(i)' - p'_\lambda(i+1) \leq \varepsilon_i(\lambda).$$

In particular, we can conclude that

$$\begin{aligned} 1 - p'_\lambda(i_\dagger) &= p'_\lambda(1) - p'_\lambda(2) + p'_\lambda(2) - p'_\lambda(3) + \ldots + p'_\lambda(i_\dagger - 1) - p'_\lambda(i_\dagger) \\ &\leq \varepsilon_1(\lambda) + \ldots + \varepsilon_{i_\dagger - 1}(\lambda) \in \mathsf{negl}(\lambda). \end{aligned}$$

Note that $\varepsilon_1(\lambda) + \ldots + \varepsilon_{i_\dagger - 1}(\lambda)$ lies in $\mathsf{negl}(\lambda)$, since $i_\dagger - 1$ is constant. □

Lemma 6. *For* $i \in \{1,\dots,D+1\}$*, set* $A_i(\lambda) := \{i,\dots,Q(\lambda)\}$ *and*

$$p_\lambda(i) := \Pr_{\substack{\mathsf{msk} \leftarrow \mathsf{Setup}_{\mathsf{good}}(1^\lambda) \\ y \leftarrow \mathsf{Enc}(\mathsf{msk},0)}} \left[\tau_{\mathsf{msk},A_i(\lambda)}(h_{\mathsf{msk}})(T,y) = 0\right].$$

There is an index $i_\dagger \in [D]$ *together with functions* $\varepsilon' \in \mathsf{negl}(\lambda)$*,* $r' \in \mathsf{poly}(\lambda)$*,* $r' > 0$ *s.t. we have*

$$\forall \lambda \in \mathbb{N}\colon p_\lambda(i_\dagger) \geq 1 - \varepsilon'(\lambda),$$
$$\exists_\infty \lambda \in \mathbb{N}\colon p_\lambda(i_\dagger) - p_\lambda(i_\dagger + 1) \geq 1/r'(\lambda).$$

Proof. Note that $p_\lambda(i)$ is monotonically decreasing. Furthermore, we have $p_\lambda(0) = 1$, since $\tau_{\mathsf{msk},A_0}(h_{\mathsf{msk}}) = \tau_{\mathsf{msk},[Q]}(h_{\mathsf{msk}}) = h_{\mathsf{msk}}(\mathsf{sk}_1(Y),\dots,\mathsf{sk}_Q(Y))$ is the zero polynomial in $\mathbb{Z}_q[T,Y]$.

On the other side, $p_\lambda(D)$ must be zero, since there must be a monomial $T_{i_1} \cdots T_{i_{D'}}$ with $i_1,\dots,i_{D'} \in [D]$ that occurs in h_{msk}, as msk is good. The monomial $T_{i_1} \cdots T_{i_{D'}}$ also appears in $\tau_{\mathsf{msk},A_D}(h_{\mathsf{msk}})$, since the variables $T_1,\dots,T_D$ will not be substituted by τ_{msk,A_D}. Hence, $\tau_{\mathsf{msk},A_D}(h_{\mathsf{msk}})(y)$ cannot be zero for any $y \in \mathbb{Z}_q^m$.

By Lemma 5, it now follows that there must exist an index $i_\dagger \in [D]$ together with $\varepsilon' \in \mathsf{negl}(\lambda)$ and $r' \in \mathsf{poly}(\lambda)$ s.t. we have

$$\forall \lambda \in \mathbb{N}\colon p_\lambda(i_\dagger) \geq 1 - \varepsilon'(\lambda),$$
$$\exists_\infty \lambda \in \mathbb{N}\colon p_\lambda(i_\dagger) - p_\lambda(i_\dagger + 1) \geq \frac{1}{r'(\lambda)}$$

as we claimed. □

We make use of the following lemma about learning linear spaces from [Üna20]:

Lemma 7. *Let k be a field and let $s \in \mathbb{N}$. Let $C \subset k^s$ be a memoryless distribution. For each $m \in \mathbb{N}$, we have*

$$\Pr_{v_1,\ldots,v_m \leftarrow C}\left[v_m \in \mathrm{span}_k\left\{v_1,\ldots,v_{m-1}\right\}\right] \geq 1 - \frac{s}{m}.$$

Lemma 8. *Let $d, m, Q \in \mathbb{N}$ and let q be a prime. Let $Y_1,\ldots,Y_m$ be m variables and let $T_1,\ldots,T_Q$ be Q additional fresh variables. Set $t := \binom{m+d}{d}$ and let $Y^{I_1},\ldots,Y^{I_t}$ be an enumeration of all monomials of $\mathbb{Z}_q[Y_1,\ldots,Y_m]$ of degree $\leq d$. Let*

$$\begin{aligned}\psi_d : \mathbb{Z}_q^m &\longrightarrow \mathbb{Z}_q^t \\ y &\longmapsto (y^{I_1},\ldots,y^{I_t})\end{aligned}$$

be the map that assigns to each point y a vector of all products of its entries of degree $\leq d$.

We have for all $\ell \in \mathbb{N}, y_1,\ldots,y_{\ell+1} \in \mathbb{Z}_q^m$ and $h \in \mathbb{Z}_q[Y_1,\ldots,Y_m,T_1,\ldots,T_Q]$ of degree $\leq d$ the follow implication,

$$\left.\begin{array}{l}\psi_d(y_{\ell+1}) \in \mathrm{span}_{\mathbb{Z}_q}\left\{\psi_d(y_1),\ldots,\psi_d(y_\ell)\right\} \\ \text{and}\ \ \forall i \in [\ell]\colon h(y_i, T_1,\ldots,T_Q) = 0\end{array}\right\} \implies h(y_{\ell+1}, T_1,\ldots,T_Q) = 0.$$

Proof. Since $h \in \mathbb{Z}_q[Y_1,\ldots,Y_m,T_1,\ldots,T_Q]$ is of degree $\leq d$, there are polynomials $c_1,\ldots,c_t \in \mathbb{Z}_q[T_1,\ldots,T_Q]$ s.t. it can be written as

$$h(Y_1,\ldots,Y_m,T_1,\ldots,T_Q) = \sum_{i=1}^{T} c_i(T_1,\ldots,T_Q)\cdot Y^{I_i}.$$

Assume that we have $\psi_d(y_{\ell+1}) \in \mathrm{span}_{\mathbb{Z}_q}\left\{\psi_d(y_1),\ldots,\psi_d(y_\ell)\right\}$ and $h(y_i,T_1,\ldots,T_Q) = 0$ for each $i \in [\ell]$. Then, there are scalars $\gamma_1,\ldots,\gamma_\ell \in \mathbb{Z}_q$ s.t.

$$\psi_d(y_{\ell+1}) = \gamma_1\cdot\psi_d(y_1) + \ldots + \gamma_\ell\cdot\psi_d(y_\ell).$$

In particular, we have for each multi-index I_i

$$y_{\ell+1}^{I_i} = \gamma_1\cdot y_1^{I_i} + \ldots + \gamma_\ell\cdot y_\ell^{I_i}.$$

We now have

$$\begin{aligned}h(y_{\ell+1},T_1,\ldots,T_Q) &= \sum_{i=1}^{T} c_i(T_1,\ldots,T_Q)\cdot y_{\ell+1}^{I_i} \\ = \sum_{i=1}^{T} c_i(T_1,\ldots,T_Q)\cdot\left(\sum_{j=1}^{\ell}\gamma_j y_j^{I_i}\right) &= \sum_{j=1}^{\ell}\gamma_j\cdot\left(\sum_{i=1}^{T} c_i(T_1,\ldots,T_Q)\cdot y_j^{I_i}\right) \\ = \sum_{j=1}^{\ell}\gamma_j\cdot h(y_j,T_1,\ldots,T_Q) &= \sum_{j=1}^{\ell}\gamma_j\cdot 0 = 0\end{aligned}$$

as we claimed. □

To prove Theorem 6, we will introduce a PPT adversary $\mathcal{A}$ for the IND-CPA security game of FE. $\mathcal{A}$ will query multiple challenge ciphertexts, but will not ask for any secret keys.

Definition 14. *Let $\widetilde{\mathcal{X}} \subset \mathcal{X}$ be a message subspace of polynomial size. We define the following adversary $\mathcal{A}$ that plays the selective IND-CPA security game of $\mathsf{FE} = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ with a challenger $\mathcal{C}$:*

1. *$\mathcal{A}$ samples $y, z \leftarrow \widetilde{\mathcal{X}}_\lambda$ uniformly and independently at random.*
2. *$\mathcal{A}$ defines two lists $(x_i^0)_{i=1,\dots,\ell+1}$ and $(x_i^1)_{i=1,\dots,\ell'+1}$ by*

$$x_i^0 := y \text{ and } x_i^1 := \begin{cases} y, & \text{if } i \in [\ell'], \\ z, & \text{if } i = \ell' + 1. \end{cases}$$

3. *$\mathcal{A}$ submits both lists to $\mathcal{C}$ and receives a list of ciphertexts $\mathsf{ct}_1, \dots, \mathsf{ct}_{\ell'}$ of y and $\mathsf{ct}_{\ell'+1}$ of $x^b_{\ell'+1}$ for unknown $b \in \{0,1\}$.*
4. *Let $\psi_D \colon \mathbb{Z}_q^m \to \mathbb{Z}_q^t$ be the map from Lemma 8. $\mathcal{A}$ computes*

$$V := \mathrm{span}_{\mathbb{Z}_q} \{\psi_D(\mathsf{ct}_1), \dots, \psi_D(\mathsf{ct}_{\ell'})\} \subseteq \mathbb{Z}_q^t .$$

5. *If $\psi_D(\mathsf{ct}_{\ell'+1}) \in V$, then $\mathcal{A}$ outputs $b = 0$. Otherwise, $\mathcal{A}$ outputs $b = 1$.*

For a fixed $\lambda \in \mathbb{N}$, a fixed master secret key msk and fixed messages $y, z \in \widetilde{\mathcal{X}}_\lambda$, denote by

$$\mathsf{Adv}^{\mathsf{ind\text{-}cpa}}_{\mathsf{FE}} (\mathcal{A} \,|\mathsf{msk}, y, z)$$

the advantage of $\mathcal{A}$ at security level λ conditioned on the event that the challenger $\mathcal{C}$ samples msk as master secret key of FE and that $\mathcal{A}$ samples y, z as candidate message pair in step 1.

We will first show that the conditioned advantage $\mathsf{Adv}^{\mathsf{ind\text{-}cpa}}_{\mathsf{FE}} (\mathcal{A} \,|\mathsf{msk}, y, z)$ is bounded from below.

Lemma 9. *We have for all msk, y, z*

$$\mathsf{Adv}^{\mathsf{ind\text{-}cpa}}_{\mathsf{FE}} (\mathcal{A} \,|\mathsf{msk}, y, z) \geq -\frac{1}{\ell+1} \cdot \binom{m+D}{D}.$$

It may seem strange that we have to lower bound $\mathcal{A}$'s advantage by a small negative value, however, remember that we allowed $\mathcal{A}$'s advantage to be negative in Definition 5.

Proof. It suffices to show that $\mathcal{A}$ outputs 0 with probability at least $1 - \frac{\binom{m+D}{D}}{\ell+1}$ whenever $\mathcal{C}$ draws 0 as bit b. In this case, $\mathsf{ct}_1, \dots, \mathsf{ct}_{\ell+1}$ are all sampled according to the distribution $\mathsf{Enc}(\mathsf{msk}, y)$. From Lemma 7, it hence follows

$$\Pr\left[\psi_D(\mathsf{ct}_{\ell+1}) \in \mathrm{span}_{\mathbb{Z}_q} \{\psi_D(\mathsf{ct}_1), \dots, \psi_D(\mathsf{ct}_\ell)\}\right] \geq 1 - \frac{\binom{m+D}{D}}{\ell+1}.$$

Since $\mathcal{A}$ outputs 0 whenever $\psi_D(\mathsf{ct}_{\ell+1})$ lies in $V = \mathrm{span}_{\mathbb{Z}_q} \{\psi_D(\mathsf{ct}_1), \dots, \psi_D(\mathsf{ct}_\ell)\}$, the claim follows. □

According to Lemma 4, the probability of a random master secret key $\mathsf{msk} \leftarrow \mathsf{Setup}(1^\lambda)$ being good is at least Q^{-D}. We can now further condition the advantage of $\mathcal{A}$:

Lemma 10. *Fix two messages $y, z \in \widetilde{\mathcal{X}}_\lambda$ and denote by event the event that $\mathcal{C}$ samples a good master secret key and that $\mathcal{A}$ chooses y, z in step 1. We have*

$$\mathsf{Adv}^{\mathsf{ind\text{-}cpa}}_{\mathsf{FE}} (\mathcal{A}) \geq \frac{\mathsf{Adv}^{\mathsf{ind\text{-}cpa}}_{\mathsf{FE}} (\mathcal{A} \,|\, \mathsf{event})}{Q^D \cdot \# \widetilde{\mathcal{X}}_\lambda^2} - \frac{\binom{m+D}{D}}{\ell+1} \cdot \frac{Q^D \cdot \# \widetilde{\mathcal{X}}_\lambda^2 - 1}{Q^D \cdot \# \widetilde{\mathcal{X}}_\lambda^2}.$$

Proof. Note that our notion of advantage allows to partition the advantage of $\mathcal{A}$ on different events. In particular, we have

$$\begin{aligned}\mathsf{Adv}^{\mathsf{ind\text{-}cpa}}_{\mathsf{FE}}(\mathcal{A}) &= \mathsf{Adv}^{\mathsf{ind\text{-}cpa}}_{\mathsf{FE}}(\mathcal{A} \mid \mathsf{event}) \cdot \Pr[\mathsf{event}] + \mathsf{Adv}^{\mathsf{ind\text{-}cpa}}_{\mathsf{FE}}(\mathcal{A} \mid \neg\,\mathsf{event}) \cdot \Pr[\neg\,\mathsf{event}] \\ &= \mathsf{Adv}^{\mathsf{ind\text{-}cpa}}_{\mathsf{FE}}(\mathcal{A} \mid \mathsf{event}) \cdot \Pr_{\substack{\mathsf{msk}\leftarrow\mathsf{Setup}(1^\lambda)\\ y',z'\leftarrow\widetilde{\mathcal{X}}_\lambda}}[\mathsf{msk}\text{ is good}, y'=y, z'=z] \\ &\quad + \mathsf{Adv}^{\mathsf{ind\text{-}cpa}}_{\mathsf{FE}}(\mathcal{A} \mid \neg\,\mathsf{event}) \cdot \left(1 - \Pr_{\substack{\mathsf{msk}\leftarrow\mathsf{Setup}(1^\lambda)\\ y',z'\leftarrow\widetilde{\mathcal{X}}_\lambda}}[\mathsf{msk}\text{ is good}, y'=y, z'=z]\right)\end{aligned}$$

By using that

$$\Pr_{\substack{\mathsf{msk}\leftarrow\mathsf{Setup}(1^\lambda)\\ y',z'\leftarrow\widetilde{\mathcal{X}}_\lambda}}[\mathsf{msk}\text{ is good}, y'=y, z'=z] \geq \frac{1}{Q^D}\cdot\frac{1}{\#\,\widetilde{\mathcal{X}}_\lambda}\cdot\frac{1}{\#\,\widetilde{\mathcal{X}}_\lambda}$$

and that the advantage of $\mathcal{A}$ conditioned on any msk and messages y, z is always bounded by $-\frac{\binom{m+D}{D}}{\ell+1}$, we have

$$\begin{aligned}\mathsf{Adv}^{\mathsf{ind\text{-}cpa}}_{\mathsf{FE}}(\mathcal{A}) &= \mathsf{Adv}^{\mathsf{ind\text{-}cpa}}_{\mathsf{FE}}(\mathcal{A} \mid \mathsf{event}) \cdot \Pr_{\substack{\mathsf{msk}\leftarrow\mathsf{Setup}(1^\lambda)\\ y',z'\leftarrow\widetilde{\mathcal{X}}_\lambda}}[\mathsf{msk}\text{ is good}, y'=y, z'=z] \\ &\quad + \mathsf{Adv}^{\mathsf{ind\text{-}cpa}}_{\mathsf{FE}}(\mathcal{A} \mid \neg\,\mathsf{event}) \cdot \left(1 - \Pr_{\substack{\mathsf{msk}\leftarrow\mathsf{Setup}(1^\lambda)\\ y',z'\leftarrow\widetilde{\mathcal{X}}_\lambda}}[\mathsf{msk}\text{ is good}, y'=y, z'=z]\right) \\ &\geq \mathsf{Adv}^{\mathsf{ind\text{-}cpa}}_{\mathsf{FE}}(\mathcal{A} \mid \mathsf{event}) \cdot \frac{1}{Q^D\cdot\#\,\widetilde{\mathcal{X}}_\lambda^2} - \frac{\binom{m+D}{D}}{\ell+1}\cdot\frac{Q^D\cdot\#\,\widetilde{\mathcal{X}}_\lambda^2 - 1}{Q^D\cdot\#\,\widetilde{\mathcal{X}}_\lambda^2}.\end{aligned}$$

Hence, the claim of the lemma holds. □

Lemma 11. *For each $\ell \in \mathsf{poly}(\lambda)$, there is an $\varepsilon_\ell \in \mathsf{negl}(\lambda)$ s.t. we have for each pair $y, z \in \widetilde{\mathcal{X}}$*

$$\Pr\left[\phi_D(\mathsf{ct}_z) \in \mathrm{span}_{\mathbb{Z}_q}\left\{\phi_D(\mathsf{ct}_1), \ldots, \phi_D(\mathsf{ct}_{\ell'(\lambda)})\right\}\right] \geq 1 - \frac{1}{\ell} - \varepsilon_\ell$$

where $\mathsf{msk} \leftarrow \mathsf{Setup}_{\mathsf{good}}(1^\lambda)$, $\mathsf{ct}_1, \ldots, \mathsf{ct}_{\ell'(\lambda)} \leftarrow \mathsf{Enc}(\mathsf{msk}, y_\lambda)$, $\mathsf{ct}_z \leftarrow \mathsf{Enc}(\mathsf{msk}, z_\lambda)$ and

$$\ell' := \ell \cdot \binom{m+D}{D} \cdot Q^D \cdot \#\,\widetilde{\mathcal{X}}_\lambda^2 - 1.$$

Proof. Instantiate $\mathcal{A}$ with parameter ℓ' this time. Since FE is IND-CPA secure, there is some $\varepsilon_{\ell'} \in \mathsf{negl}(\lambda)$ s.t.

$$\begin{aligned}\varepsilon_{\ell'}(\lambda) \geq& \mathsf{Adv}^{\mathsf{ind\text{-}cpa}}_{\mathsf{FE}}(\mathcal{A}) \\ \overset{Lemma\ 10}{\geq}& \frac{\mathsf{Adv}^{\mathsf{ind\text{-}cpa}}_{\mathsf{FE}}(\mathcal{A} \mid \mathsf{event})}{Q^D\cdot\#\,\widetilde{\mathcal{X}}_\lambda^2} - \frac{\binom{m+D}{D}}{\ell'+1}\cdot\frac{Q^D\cdot\#\,\widetilde{\mathcal{X}}_\lambda^2 - 1}{Q^D\cdot\#\,\widetilde{\mathcal{X}}_\lambda^2}.\end{aligned}$$

By reordering the terms, we get

$$\mathsf{Adv}^{\mathsf{ind\text{-}cpa}}_{\mathsf{FE}}(\mathcal{A} \mid \mathsf{event}) \leq Q^D\cdot\#\,\widetilde{\mathcal{X}}_\lambda^2 \cdot \varepsilon_{\ell'} + \frac{(Q^D\cdot\#\,\widetilde{\mathcal{X}}_\lambda^2 - 1)\cdot\binom{m+D}{D}}{\ell'+1}. \tag{9}$$

Let

$$V = \mathrm{span}_{\mathbb{Z}_q}\left\{\phi_D(\mathsf{ct}_1), \ldots, \phi_D(\mathsf{ct}_{\ell'(\lambda)})\right\}$$

be the space computed by $\mathcal{A}$ in step 4. Note that the ciphertexts $\mathsf{ct}_1, \ldots, \mathsf{ct}_{\ell'}$ are distributed according to $\mathsf{Enc}(\mathsf{msk}, y_\lambda)$. For the advantage of $\mathcal{A}$ conditioned on event, we have

$$\mathsf{Adv}^{\mathsf{ind\text{-}cpa}}_{\mathsf{FE}}(\mathcal{A} \mid \mathsf{event}) = \Pr_{\substack{\mathsf{msk}\leftarrow\mathsf{Setup}_{\mathsf{good}}(1^\lambda)\\ \mathsf{ct}_y\leftarrow\mathsf{Enc}(\mathsf{msk},y_\lambda)}}[\psi_D(\mathsf{ct}_y) \in V] - \Pr_{\substack{\mathsf{msk}\leftarrow\mathsf{Setup}_{\mathsf{good}}(1^\lambda)\\ \mathsf{ct}_z\leftarrow\mathsf{Enc}(\mathsf{msk},z_\lambda)}}[\psi_D(\mathsf{ct}_z) \in V] \tag{10}$$

where $\mathsf{Setup}_{\mathsf{good}}(1^\lambda)$ is the distribution $\mathsf{Setup}(1^\lambda)$ conditioned on msk being good. Because of Lemma 7, we have

$$\Pr_{\substack{\mathsf{msk}\leftarrow\mathsf{Setup}_{\mathsf{good}}(1^\lambda)\\ \mathsf{ct}_y\leftarrow\mathsf{Enc}(\mathsf{msk},y_\lambda)}}[\psi_D(\mathsf{ct}_y) \in V] \geq 1 - \frac{1}{\ell'+1} \cdot \binom{m+D}{D},$$

further, we set

$$\alpha := \Pr_{\substack{\mathsf{msk}\leftarrow\mathsf{Setup}_{\mathsf{good}}(1^\lambda)\\ \mathsf{ct}_z\leftarrow\mathsf{Enc}(\mathsf{msk},z_\lambda)}}[\psi_D(\mathsf{ct}_z) \in V].$$

Combining this with Equation (10) yields

$$\mathsf{Adv}^{\mathsf{ind\text{-}cpa}}_{\mathsf{FE}}(\mathcal{A} \mid \mathsf{event}) \geq 1 - \frac{1}{\ell'+1} \cdot \binom{m+D}{D} - \alpha.$$

We can now take the upper bound Equation (9) for $\mathsf{Adv}^{\mathsf{ind\text{-}cpa}}_{\mathsf{FE}}(\mathcal{A} \mid \mathsf{event})$ into account

$$Q^D \cdot \#\widetilde{\mathcal{X}}_\lambda^2 \cdot \varepsilon_{\ell'} + \frac{(Q^D \cdot \#\widetilde{\mathcal{X}}_\lambda^2 - 1) \cdot \binom{m+D}{D}}{\ell'+1} \geq 1 - \frac{1}{\ell'+1} \cdot \binom{m+D}{D} - \alpha.$$

With regard to α, we get

$$\alpha \geq 1 - \frac{Q^D \cdot \#\widetilde{\mathcal{X}}_\lambda^2 \cdot \binom{m+D}{D}}{\ell'+1} - Q^D \cdot \#\widetilde{\mathcal{X}}_\lambda^2 \cdot \varepsilon_{\ell'}.$$

By substituting α, ℓ' and

$$\varepsilon_\ell := Q^D \cdot \#\widetilde{\mathcal{X}}_\lambda^2 \cdot \varepsilon_{\ell'}$$

the claim of the lemma follows. □

Lemma 12. *We have the following:*

1. *For each $\ell \in \mathsf{poly}(\lambda)$, there exists functions $\ell' \in \mathsf{poly}(\lambda)$, $\ell' \geq \ell$, and $\varepsilon_\ell \in \mathsf{negl}(\lambda)$ s.t. we have for each $i \in \{0, \ldots, D\}$, $\lambda \in \mathbb{N}$ and each pair $x_1, x_2 \in \widetilde{\mathcal{X}}_\lambda$,*

$$p_\lambda(i, x_1) \geq \ell'(\lambda) \cdot p_\lambda(i, x_2) - (\ell'(\lambda) - 1) - \frac{1}{\ell(\lambda)} - \varepsilon_\ell(\lambda).$$

2. *Let $\varepsilon' \in \mathsf{negl}(\lambda)$. There exists an $\varepsilon \in \mathsf{negl}(\lambda)$, s.t. we have for each $\lambda \in \mathbb{N}$: if there exists some $x_2 \in \widetilde{\mathcal{X}}_\lambda$ with $p_\lambda(i, x_2) \geq 1 - \varepsilon'(\lambda)$, then we have $p_\lambda(i, x_1) \geq 1 - \varepsilon(\lambda)$ for each $x_1 \in \widetilde{\mathcal{X}}_\lambda$.*

Proof. 1. Fix a master secret key msk and set for $i \in [Q(\lambda)]$

$$h_i(Y_1, \ldots, Y_m) := \tau_{\mathsf{msk}, A_i(\lambda)}(h_{\mathsf{msk}}) \in \mathbb{Z}_q[T][Y].$$

We consider h_i as a polynomial with coefficients in $\mathbb{Z}_q[T_1, \ldots, T_Q]$ and variables $Y_1, \ldots, Y_m$. The degree of h_i is at most $\max_{j \in A_i(\lambda)}(\deg \mathsf{sk}_j) \cdot \deg h_{\mathsf{msk}} \leq d \cdot D$. Let $\ell' \in \mathsf{poly}(\lambda)$, $\ell' \geq \ell$ and $\varepsilon_\ell \in \mathsf{negl}(\lambda)$ be the functions from the claim of Lemma 11.
For $\mathsf{ct}_{x_1} \leftarrow \mathsf{Enc}(\mathsf{msk}, x_1)$, and $\mathsf{ct}_1, \ldots, \mathsf{ct}_{\ell'} \leftarrow \mathsf{Enc}(\mathsf{msk}, x_2)$ we have according to Lemma 8 the following implication of events,

$$\begin{aligned} &\psi_D(\mathsf{ct}_{x_1}) \in \operatorname{span}_{\mathbb{Z}_q}\{\psi_D(\mathsf{ct}_1), \ldots, \psi_D(\mathsf{ct}_{\ell'})\}, h_i(\mathsf{ct}_1) = \ldots = h_i(\mathsf{ct}_{\ell'}) = 0 \\ &\implies h_i(\mathsf{ct}_{x_1}) = 0. \end{aligned}$$

For a fixed msk, we thereby have the following inequalities:

$$\begin{aligned} &\Pr_{\mathsf{ct}_{x_1} \leftarrow \mathsf{Enc}(\mathsf{msk}, x_1)}[h_i(\mathsf{ct}_{x_1}) = 0] \qquad (11) \\ \geq &\Pr_{\substack{\mathsf{ct}_{x_1} \leftarrow \mathsf{Enc}(\mathsf{msk}, x_1) \\ \mathsf{ct}_1, \ldots, \mathsf{ct}_{\ell'} \leftarrow \mathsf{Enc}(\mathsf{msk}, x_2)}} \begin{bmatrix} \psi_D(\mathsf{ct}_{x_1}) \in \operatorname{span}_{\mathbb{Z}_q}\{\psi_D(\mathsf{ct}_1), \ldots, \psi_D(\mathsf{ct}_{\ell'})\} \\ h_i(\mathsf{ct}_1) = \ldots = h_i(\mathsf{ct}_{\ell'}) = 0 \end{bmatrix} \\ \geq &\Pr_{\substack{\mathsf{ct}_{x_1} \leftarrow \mathsf{Enc}(\mathsf{msk}, x_1) \\ \mathsf{ct}_1, \ldots, \mathsf{ct}_{\ell'} \leftarrow \mathsf{Enc}(\mathsf{msk}, x_2)}} \left[\psi_D(\mathsf{ct}_{x_1}) \in \operatorname{span}_{\mathbb{Z}_q}\{\psi_D(\mathsf{ct}_1), \ldots, \psi_D(\mathsf{ct}_{\ell'})\}\right] \\ &+ \Pr_{\mathsf{ct}_1, \ldots, \mathsf{ct}_{\ell'} \leftarrow \mathsf{Enc}(\mathsf{msk}, x_2)}[h_i(\mathsf{ct}_1) = \ldots = h_i(\mathsf{ct}_{\ell'}) = 0] - 1 \\ \geq &\Pr_{\substack{\mathsf{ct}_{x_1} \leftarrow \mathsf{Enc}(\mathsf{msk}, x_1) \\ \mathsf{ct}_1, \ldots, \mathsf{ct}_{\ell'} \leftarrow \mathsf{Enc}(\mathsf{msk}, x_2)}} \left[\psi_D(\mathsf{ct}_{x_1}) \in \operatorname{span}_{\mathbb{Z}_q}\{\psi_D(\mathsf{ct}_1), \ldots, \psi_D(\mathsf{ct}_{\ell'})\}\right] \\ &+ \ell' \cdot \Pr_{\mathsf{ct}_{x_2} \leftarrow \mathsf{Enc}(\mathsf{msk}, x_2)}[h_i(\mathsf{ct}_{x_2}) = 0] - \ell'. \end{aligned}$$

We now sample msk according to $\mathsf{Setup}(1^\lambda)$, and get

$$\begin{aligned} p_\lambda(i, x_1) = &\Pr_{\substack{\mathsf{msk} \leftarrow \mathsf{Setup}(1^\lambda) \\ \mathsf{ct}_{x_1} \leftarrow \mathsf{Enc}(\mathsf{msk}, x_1)}}[h_i(\mathsf{ct}_{x_1}) = 0] \\ \overset{Eq.\ (11)}{\geq} &\Pr_{\substack{\mathsf{msk} \leftarrow \mathsf{Setup}(1^\lambda) \\ \mathsf{ct}_{x_1} \leftarrow \mathsf{Enc}(\mathsf{msk}, x_1) \\ \mathsf{ct}_1, \ldots, \mathsf{ct}_{\ell'} \leftarrow \mathsf{Enc}(\mathsf{msk}, x_2)}} \left[\psi_D(\mathsf{ct}_{x_1}) \in \operatorname{span}_{\mathbb{Z}_q}\{\psi_D(\mathsf{ct}_1), \ldots, \psi_D(\mathsf{ct}_{\ell'})\}\right] \\ &+ \ell' \cdot \Pr_{\substack{\mathsf{msk} \leftarrow \mathsf{Setup}(1^\lambda) \\ \mathsf{ct}_{x_2} \leftarrow \mathsf{Enc}(\mathsf{msk}, x_2)}}[h_i(\mathsf{ct}_{x_2}) = 0] - \ell'. \\ \overset{Lemma\ 11}{\geq} &\left(1 - \frac{1}{\ell} - \varepsilon_\ell\right) + \ell' \cdot \Pr_{\substack{\mathsf{msk} \leftarrow \mathsf{Setup}(1^\lambda) \\ \mathsf{ct}_{x_2} \leftarrow \mathsf{Enc}(\mathsf{msk}, x_2)}}[h_i(\mathsf{ct}_y) = 0] - \ell' \\ &\geq \ell' \cdot \Pr_{\substack{\mathsf{msk} \leftarrow \mathsf{Setup}(1^\lambda) \\ \mathsf{ct}_{x_2} \leftarrow \mathsf{Enc}(\mathsf{msk}, x_2)}}[h_i(\mathsf{ct}_{x_2}) = 0] - (\ell' - 1) - \frac{1}{\ell} - \varepsilon_\ell \\ &\geq \ell' \cdot p_\lambda(i, x_2) - (\ell' - 1) - \frac{1}{\ell} - \varepsilon_\ell. \end{aligned}$$

2. Assume that the claim is false. In this case, there is a negligible function $\varepsilon' \in \mathsf{negl}(\lambda)$ and a positive function $r \in \mathsf{poly}(\lambda)$ s.t. we have for infinitely many $\lambda \in \mathbb{N}$,

$$\exists x_1, x_2 \in \widetilde{\mathcal{X}}_\lambda \colon p_\lambda(i, x_1) < 1 - \frac{1}{r(\lambda)}, \quad p_\lambda(i, x_2) \geq 1 - \varepsilon'(\lambda).$$

Choose $\ell \in \mathsf{poly}(\lambda)$ s.t. we have $\ell(\lambda) > r(\lambda)$ for each $\lambda \in \mathbb{N}$. Let $\ell' \in \mathsf{poly}(\lambda), \ell' \geq \ell, \varepsilon_\ell \in \mathsf{negl}(\lambda)$ be the functions from the first claim of this lemma. We now have that for infinitely many $\lambda \in \mathbb{N}$, there exist $x_1, x_2 \in \widetilde{\mathcal{X}}_\lambda$ with

$$\begin{aligned}
1 - \frac{1}{r(\lambda)} &> p_\lambda(i, x_1) \\
&\geq \ell'(\lambda) \cdot p_\lambda(i, x_2) - (\ell'(\lambda) - 1) - \frac{1}{\ell(\lambda)} - \varepsilon_\lambda(\ell) \\
&\geq \ell'(\lambda) \cdot (1 - \varepsilon'(\lambda)) - (\ell'(\lambda) - 1) - \frac{1}{\ell(\lambda)} - \varepsilon_\lambda(\ell) \\
&\geq 1 - \ell'(\lambda)\varepsilon'(\lambda) - \frac{1}{\ell(\lambda)} - \varepsilon_\lambda(\ell).
\end{aligned}$$

This is equivalent to the following,

$$\frac{1}{r(\lambda)} < \frac{1}{\ell(\lambda)} + \varepsilon_\ell(\lambda) + \ell'(\lambda)\varepsilon'(\lambda). \tag{12}$$

However, since $\ell(\lambda) > r(\lambda)$, Equation (12) cannot hold for infinitely many $\lambda \in \mathbb{N}$. Hence, the second claim of this lemma must be true as well.

□

Proof (Theorem 6). Let $i_\dagger \in [D]$ be the index from Lemma 6. Then, there exist $\varepsilon' \in \mathsf{negl}(\lambda)$ and $\rho' \notin \mathsf{negl}(\lambda), \rho' \geq 0$ s.t. we have for each $\lambda \in \mathbb{N}$,

$$\begin{aligned}
&p_\lambda(i_\dagger, 0) \geq 1 - \varepsilon'(\lambda), \\
&p_\lambda(i_\dagger, 0) - p_\lambda(i_\dagger + 1, 0) \geq \rho'(\lambda),
\end{aligned}$$

where we denote by $0 = (0, \ldots, 0)$ the zero-vector message in $\widetilde{\mathcal{X}}_\lambda$. According to Lemma 12, there is now an $\varepsilon \in \mathsf{negl}(\lambda)$ s.t. we have for each $\lambda \in \mathbb{N}$ and $x \in \widetilde{\mathcal{X}}_\lambda$,

$$p_\lambda(i_\dagger, x) \geq 1 - \varepsilon(\lambda).$$

We claim that there is some $r \in \mathsf{poly}(\lambda)$, $r > 0$, s.t. there are infinitely many $\lambda \in \mathbb{N}$ s.t. we have for each $x \in \widetilde{\mathcal{X}}_\lambda$

$$p_\lambda(i_\dagger, x) - p_\lambda(i_\dagger + 1, x) \geq \frac{1}{r(\lambda)}. \tag{13}$$

Assume, for the sake of contradiction, that the claim is false. In this case, for each $r \in \mathsf{poly}(\lambda)$, $r > 0$ and for almost all $\lambda \in \mathbb{N}$ there exists some $x \in \widetilde{\mathcal{X}}_\lambda$ s.t.

$$p_\lambda(i_\dagger, x) - p_\lambda(i_\dagger + 1, x) < \frac{1}{r(\lambda)}.$$

This implies the existence of a negligible function $\varepsilon_2' \in \mathsf{negl}(\lambda)$ s.t. we have for each $x \in \widetilde{\mathcal{X}}_\lambda$,

$$p_\lambda(i_\dagger, x) - p_\lambda(i_\dagger + 1, x) \leq \varepsilon_2'(\lambda). \tag{14}$$

Since $p_\lambda(i_\dagger, x) \geq 1 - \varepsilon(\lambda)$, Equation (14) is equivalent to

$$p_\lambda(i_\dagger + 1, x) \geq 1 - \varepsilon(\lambda) - \varepsilon_2'(\lambda).$$

However, because of Lemma 12, there must be now a negligible function $\varepsilon_2 \in \mathsf{negl}(\lambda)$ s.t. we have for each $\lambda \in \mathbb{N}$,

$$p_\lambda(i_\dagger + 1, 0) \geq 1 - \varepsilon_2(\lambda).$$

This contradicts the statement of Lemma 6. Hence, our assumption must be wrong and there must exist a polynomial $r \in \mathsf{poly}(\lambda)$, $r > 0$, s.t. Equation (13) does hold for infinitely many λ and each $x \in \widetilde{\mathcal{X}}_\lambda$. Denote the set of λ's for which Equation (13) holds by $\Lambda \subseteq \mathbb{N}$. By setting

$$\rho(\lambda) := \begin{cases} \dfrac{1}{r(\lambda)}, & \lambda \in \Lambda, \\ 0, & \lambda \notin \Lambda, \end{cases}$$

the claim of Theorem 6 follows. □

6 Limits and Open Questions

In this section we describe some methods to circumvent the lattice-based FE model that is studied in this work and pose some open questions.

Bit Decomposition. As mentioned in the introduction, if the inverse gadget matrix is used at encryption to decompose the input message, then the encryption scheme is not offline/online of constant depth any more.

If bit decomposition is used during decryption, then the decryption depth of the FE scheme is not constant any more. As an example of a scheme that uses bit decomposition at decryption, we can give the predicate encryption scheme of Gorbunov, Vaikuntanathan and Wee [GVW15]. Their scheme utilizes lattice-based FHE schemes and can issue an unbounded number of secret keys. Additionally, the size of ciphertexts grows logarithmically in the depth of predicates.

Double Arithmetic Reduction at Decryption. Another technique to circumvent the lattice-based FE framework would be to apply arithmetic reduction twice at decryption. If we take a look at the quadratic FE scheme of Agrawal and Rosen [AR17], we see that their scheme uses three prime moduli $p_1 < p_2 < q$. On input $\mathsf{ct}, \mathsf{sk} \in \mathbb{Z}_q^m$, the decryptor computes the scalar product of sk and ct modulo q and reduces it modulo p_2 and modulo p_1, i.e., it outputs

$$\Big((\mathsf{sk}^T \, \mathsf{ct} \bmod q) \bmod p_2 \Big) \bmod p_1,$$

as a value in $\mathbb{Z}_{p_1}$.

While it is known that arithmetic reduction modulo one prime $p < q$ is equivalent to scaling with p^{-1} and rounding from $\mathbb{Z}_q$ to $\mathbb{Z}_p$, it is not known if the same holds in the case of double arithmetic reduction. In particular, we don't know if there is some value $c \in \mathbb{Z}_q$ s.t. we have for each $x \in \mathbb{Z}_q$,

$$((x \bmod q) \bmod p_2) \bmod p_1 = 0 \implies |c \cdot x \bmod q| < \frac{q}{p_2}.$$

In other words, it is not clear if values that reduce to zero after two arithmetic reductions always become small when scaled with an appropriate scalar c. Hence, it may be possible to circumvent the lower bounds of this work and [Üna20] by using multiple arithmetic reductions at decryption.

Binary Messages. An important requirement for the results here and in [Üna20] is that the message modulus p of the attacked FE and SKE schemes is larger than some constant (that depends on the scheme). Indeed, taking a look at the adversary behind Theorem 4, it is necessary that the message vectors we consider allow for large enough arithmetic numbers in at least one of their entries.

If we have $p = 2$ and only consider FE schemes for binary message vectors, then the attacks here and in [Üna20] are not applicable any more. This raises the question if it is possible to circumvent the lower bounds here and in [Üna20] with simple lattice-based FE schemes that only support binary messages. Concretely, we ask if the following, simple, binary function-hiding FE scheme can be realized by LWE (or any other assumption):

Question 1. Consider the message space $\mathcal{X} = \{0,1\}$ and the function space $\mathcal{F} = \{f_0, f_1\}$ that contains the functions $f_0(x) := 0$ and $f_1(x) = x$. Note that $\mathcal{F}$ and $\mathcal{X}$ essentially compute a logical AND.

Is there a symmetric function-hiding IND-CPA secure and correct FE scheme $\mathsf{FE} = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ for $\mathcal{F}\colon\ \mathcal{X} \to \mathcal{X}$ s.t. KeyGen and Enc output vectors in $\mathbb{Z}_q^m$ (for any dimension $m \in \mathsf{poly}(\lambda)$ and modulus $q \in 2^{\mathsf{poly}(\lambda)}$) and decryption works by

$$\mathsf{Dec}(\mathsf{sk}, \mathsf{ct}) = \begin{cases} 0, & \text{if } \left|\mathsf{sk}^T \cdot \mathsf{ct}\right| \leq B, \\ 1, & \text{if } \left|\mathsf{sk}^T \cdot \mathsf{ct}\right| > B, \end{cases}$$

for some threshold $B < q/2$?

We note that since $\mathcal{X}$ and $\mathcal{F}$ only contain two elements, we basically ask here if there are keyed distributions $\mathcal{E}_{\mathsf{msk},0}$, $\mathcal{E}_{\mathsf{msk},1}$, $\mathcal{S}_{\mathsf{msk},0}$, $\mathcal{S}_{\mathsf{msk},1}$ over $\mathbb{Z}_q^m$ s.t. we have for $a, b \in \{0,1\}$ and $\mathsf{ct} \leftarrow \mathcal{E}_{\mathsf{msk},a}$, $\mathsf{sk} \leftarrow \mathcal{S}_{\mathsf{msk},b}$

$$\left|\mathsf{sk}^T \cdot \mathsf{ct}\right| \text{ is large iff } a \cdot b = 1,$$

and s.t. additionally a PPT adversary cannot distinguish between $\mathcal{E}_{\mathsf{msk},0}$ and $\mathcal{E}_{\mathsf{msk},1}$ when given access to $\mathcal{S}_{\mathsf{msk},0}$ and cannot distinguish between $\mathcal{S}_{\mathsf{msk},0}$ and $\mathcal{S}_{\mathsf{msk},1}$ when given access to $\mathcal{E}_{\mathsf{msk},0}$.

We think that any solution to Question 1 would be of large interest, even if the algorithms $\mathsf{Setup}, \mathsf{KeyGen}$ and Enc of the proposed function-hiding FE scheme would not be efficiently computable.

Weaker Notions of Security. We also want to point out that the results here take great advantage of the existence of an algebraic relationship among secret keys. In fact, this algebraic relationship allows us to substantially restrict the evaluation of a special secret key at a ciphertext, even if we only know the evaluations of different, seemingly less useful, secret keys at the ciphertext.

As long as secret keys are constant-degree polynomials, algebraic dependencies are hard to avoid in the unbounded collusion model. However, we can take algebraicity into account and prevent attacks like the ones presented in this paper, by aiming for a weaker (and more algebraic) notion of selective IND-CPA security:

Definition 15. *Let* $\mathsf{FE} = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *be an FE scheme for the function space* $\mathcal{F}$ *of degree-d polynomials in* $\mathbb{Z}_p[X_1, \ldots, X_n]$. *We define the* ***algebraically selective IND-CPA*** *security game of* FE *as an experiment* $\mathsf{Exp}^{\mathsf{alg\text{-}ind\text{-}cpa}}_{\mathsf{FE},\mathcal{A}}(\lambda, \mathcal{F})$ *between an adversary* $\mathcal{A}$ *and a challenger* $\mathcal{C}$ *that proceeds in the following steps:*

Experiment $\mathsf{Exp}^{\mathsf{alg\text{-}ind\text{-}cpa}}_{\mathsf{FE},\mathcal{A}}(\lambda, \mathcal{F})$

1. $\mathcal{A}$ *computes two lists of candidate messages* $(x_1^0, \ldots, x_N^0), (x_1^1, \ldots, x_N^1) \in \mathcal{X}_\lambda^N$ *and a list of functions* $(f_1, \ldots, f_Q) \in \mathcal{F}_\lambda^Q$, *and submits all three lists to the challenger* $\mathcal{C}$.
2. $\mathcal{C}$ *draws a random bit* $b \leftarrow \{0,1\}$, *computes* $\mathsf{msk} \leftarrow \mathsf{Setup}(1^\lambda)$ *and*

$$\mathsf{ct}_i \leftarrow \mathsf{Enc}(\mathsf{msk}, x_i^b) \quad \text{for } i = 1, \ldots, N,$$
$$\mathsf{sk}_j \leftarrow \mathsf{KeyGen}(\mathsf{msk}, f_j) \quad \text{for } j = 1, \ldots, Q.$$

   $\mathcal{C}$ *sends the lists* $(\mathsf{ct}_1, \ldots, \mathsf{ct}_N)$ *and* $(\mathsf{sk}_1, \ldots, \mathsf{sk}_Q)$ *to* $\mathcal{A}$.
3. $\mathcal{A}$ *outputs a guess bit* b'.
4. *Denote by* $R \subseteq \mathbb{Z}_p[X_1, \ldots, X_n]$ *the ring of all polynomials in* $\mathbb{Z}_p[X]$ *that are* ***algebraically dependent*** *from* $f_1, \ldots, f_Q$, *i.e.*

$$R := \{g \in \mathbb{Z}_p[X] \mid \exists h \in \mathbb{Z}_p[f_1, \ldots, f_Q][T] :\ h(T) \neq 0, h(g) = 0\}.$$

   If $b' = b$ ***and we have for each polynomial*** $g \in R$ ***and each*** $i \in [N]$

$$g(x_i^0) = g(x_i^1)$$

   the experiment outputs 1, else 0.

The requirement in the last step of the security game in Definition 15 is more strict than usual, since not only do we require that there is no queried function f_j, that can distinguish a message pair, but additionally we demand that even functions that can be algebraically derived from queried functions cannot distinguish between the two messages of a submitted challenge pair. The idea behind this requirement is that, if a function g can be symbolically derived from functions $f_1, \ldots, f_Q$, then maybe also a secret key sk_g for g can be derived from the secret keys $\mathsf{sk}_1, \ldots, \mathsf{sk}_Q$. While it is information-theoretically not possible to derive $g(x^b)$ from $f_1(x^b), \ldots, f_Q(x^b)$ as long as $f_j(x^0) = f_j(x^1)$ for $j \in [Q]$, it may be possible to derive $\mathsf{sk}_g(\mathsf{ct})$ from $\mathsf{sk}_1(\mathsf{ct}), \ldots, \mathsf{sk}_Q(\mathsf{ct})$, since the evaluations $\mathsf{sk}_j(\mathsf{ct})$ are not perfectly scaled versions of $f_j(x^b)$, but instead are perturbed by some noise that might leak sensitive information.

Acknowledgements. We want to thank the anonymous reviewers of TCC and Eurocrypt for their very helpful comments and suggestions. This work has received funding from the Austrian Science Fund (FWF) and netidee SCIENCE via grant P31621-N38 (PROFET).

References

[AAB15] Benny Applebaum, Jonathan Avron, and Christina Brzuska. "Arithmetic Cryptography: Extended Abstract". In: *ITCS 2015*. Ed. by Tim Roughgarden. ACM, Jan. 2015, pp. 143–151. DOI: 10.1145/2688073.2688114.

[ABB10] Shweta Agrawal, Dan Boneh, and Xavier Boyen. "Efficient Lattice (H)IBE in the Standard Model". In: *EUROCRYPT 2010*. Ed. by Henri Gilbert. Vol. 6110. LNCS. Springer, Heidelberg, May 2010, pp. 553–572. DOI: 10.1007/978-3-642-13190-5_28.

[Abd+15] Michel Abdalla, Florian Bourse, Angelo De Caro, and David Pointcheval. "Simple Functional Encryption Schemes for Inner Products". In: *PKC 2015*. Ed. by Jonathan Katz. Vol. 9020. LNCS. Springer, Heidelberg, Mar. 2015, pp. 733–751. DOI: 10.1007/978-3-662-46447-2_33.

[Abd+17] Michel Abdalla, Romain Gay, Mariana Raykova, and Hoeteck Wee. "Multi-input Inner-Product Functional Encryption from Pairings". In: *EUROCRYPT 2017, Part I*. Ed. by Jean-Sébastien Coron and Jesper Buus Nielsen. Vol. 10210. LNCS. Springer, Heidelberg, Apr. 2017, pp. 601–626. DOI: 10.1007/978-3-319-56620-7_21.

[Abd+18] Michel Abdalla, Dario Catalano, Dario Fiore, Romain Gay, and Bogdan Ursu. "Multi-Input Functional Encryption for Inner Products: Function-Hiding Realizations and Constructions Without Pairings". In: *CRYPTO 2018, Part I*. Ed. by Hovav Shacham and Alexandra Boldyreva. Vol. 10991. LNCS. Springer, Heidelberg, Aug. 2018, pp. 597–627. DOI: 10.1007/978-3-319-96884-1_20.

[Abd+19] Michel Abdalla, Fabrice Benhamouda, Markulf Kohlweiss, and Hendrik Waldner. "Decentralizing Inner-Product Functional Encryption". In: *PKC 2019, Part II*. Ed. by Dongdai Lin and Kazue Sako. Vol. 11443. LNCS. Springer, Heidelberg, Apr. 2019, pp. 128–157. DOI: 10.1007/978-3-030-17259-6_5.

[Abd+20] Michel Abdalla, Dario Catalano, Romain Gay, and Bogdan Ursu. "Inner-Product Functional Encryption with Fine-Grained Access Control". In: *ASIACRYPT 2020, Part III*. Ed. by Shiho Moriai and Huaxiong Wang. Vol. 12493. LNCS. Springer, Heidelberg, Dec. 2020, pp. 467–497. DOI: 10.1007/978-3-030-64840-4_16.

[ABG19] Michel Abdalla, Fabrice Benhamouda, and Romain Gay. "From Single-Input to Multi-client Inner-Product Functional Encryption". In: *ASIACRYPT 2019, Part III*. Ed. by Steven D. Galbraith and Shiho Moriai. Vol. 11923. LNCS. Springer, Heidelberg, Dec. 2019, pp. 552–582. DOI: 10.1007/978-3-030-34618-8_19.

[Agr+13] Shweta Agrawal, Sergey Gorbunov, Vinod Vaikuntanathan, and Hoeteck Wee. "Functional Encryption: New Perspectives and Lower Bounds". In: *CRYPTO 2013, Part II*. Ed. by Ran Canetti and Juan A. Garay. Vol. 8043. LNCS. Springer, Heidelberg, Aug. 2013, pp. 500–518. DOI: 10.1007/978-3-642-40084-1_28.

[Agr+20] Shweta Agrawal, Benoît Libert, Monosij Maitra, and Radu Titiu. "Adaptive Simulation Security for Inner Product Functional Encryption". In: *PKC 2020, Part I*. Ed. by Aggelos Kiayias, Markulf Kohlweiss, Petros Wallden, and Vassilis Zikas. Vol. 12110. LNCS. Springer, Heidelberg, May 2020, pp. 34–64. DOI: 10.1007/978-3-030-45374-9_2.

[Agr19] Shweta Agrawal. "Indistinguishability Obfuscation Without Multilinear Maps: New Methods for Bootstrapping and Instantiation". In: *EUROCRYPT 2019, Part I*. Ed. by Yuval Ishai and Vincent Rijmen. Vol. 11476. LNCS. Springer, Heidelberg, May 2019, pp. 191–225. DOI: 10.1007/978-3-030-17653-2_7.

[AGT21a] Shweta Agrawal, Rishab Goyal, and Junichi Tomida. "Multi-input Quadratic Functional Encryption from Pairings". In: *CRYPTO 2021, Part IV*. Ed. by Tal Malkin and Chris Peikert. Vol. 12828. LNCS. Virtual Event: Springer, Heidelberg, Aug. 2021, pp. 208–238. DOI: 10.1007/978-3-030-84259-8_8.

[AGT21b] Shweta Agrawal, Rishab Goyal, and Junichi Tomida. "Multi-Party Functional Encryption". In: *TCC 2021, Part II*. Ed. by Kobbi Nissim and Brent Waters. Vol. 13043. LNCS. Springer, Heidelberg, Nov. 2021, pp. 224–255. DOI: 10.1007/978-3-030-90453-1_8.

[AGT22] Shweta Agrawal, Rishab Goyal, and Junichi Tomida. "Multi-Input Quadratic Functional Encryption: Stronger Security, Broader Functionality". In: *TCC 2022, Part I*. Ed. by Eike Kiltz and Vinod Vaikuntanathan. Vol. 13747. LNCS. Springer, Heidelberg, Nov. 2022, pp. 711–740. DOI: 10.1007/978-3-031-22318-1_25.

[AGW20] Michel Abdalla, Junqing Gong, and Hoeteck Wee. "Functional Encryption for Attribute-Weighted Sums from k-Lin". In: *CRYPTO 2020, Part I*. Ed. by Daniele Micciancio and Thomas Ristenpart. Vol. 12170. LNCS. Springer, Heidelberg, Aug. 2020, pp. 685–716. DOI: 10.1007/978-3-030-56784-2_23.

[AJ15] Prabhanjan Ananth and Abhishek Jain. "Indistinguishability Obfuscation from Compact Functional Encryption". In: *CRYPTO 2015, Part I*. Ed. by Rosario Gennaro and Matthew J. B. Robshaw. Vol. 9215. LNCS. Springer, Heidelberg, Aug. 2015, pp. 308–326. DOI: 10.1007/978-3-662-47989-6_15.

[AJS15] Prabhanjan Ananth, Abhishek Jain, and Amit Sahai. *Indistinguishability Obfuscation from Functional Encryption for Simple Functions*. Cryptology ePrint Archive, Report 2015/730. https://eprint.iacr.org/2015/730. 2015.

[ALS16] Shweta Agrawal, Benoît Libert, and Damien Stehlé. "Fully Secure Functional Encryption for Inner Products, from Standard Assumptions". In: *CRYPTO 2016, Part III*. Ed. by Matthew Robshaw and Jonathan Katz. Vol. 9816. LNCS. Springer, Heidelberg, Aug. 2016, pp. 333–362. DOI: 10.1007/978-3-662-53015-3_12.

[AP20] Shweta Agrawal and Alice Pellet-Mary. "Indistinguishability Obfuscation Without Maps: Attacks and Fixes for Noisy Linear FE". In: *EUROCRYPT 2020, Part I*. Ed. by Anne Canteaut and Yuval Ishai. Vol. 12105. LNCS. Springer, Heidelberg, May 2020, pp. 110–140. DOI: 10.1007/978-3-030-45721-1_5.

[AR17] Shweta Agrawal and Alon Rosen. "Functional Encryption for Bounded Collusions, Revisited". In: *TCC 2017, Part I*. Ed. by Yael Kalai and Leonid Reyzin. Vol. 10677. LNCS. Springer, Heidelberg, Nov. 2017, pp. 173–205. DOI: 10.1007/978-3-319-70500-2_7.

[AS17] Prabhanjan Ananth and Amit Sahai. "Projective Arithmetic Functional Encryption and Indistinguishability Obfuscation from Degree-5 Multilinear Maps". In: *EUROCRYPT 2017, Part I*. Ed. by Jean-Sébastien Coron and Jesper Buus Nielsen. Vol. 10210. LNCS. Springer, Heidelberg, Apr. 2017, pp. 152–181. DOI: 10.1007/978-3-319-56620-7_6.

[AV19] Prabhanjan Ananth and Vinod Vaikuntanathan. "Optimal Bounded-Collusion Secure Functional Encryption". In: *TCC 2019, Part I*. Ed. by Dennis Hofheinz and Alon Rosen. Vol. 11891. LNCS. Springer, Heidelberg, Dec. 2019, pp. 174–198. DOI: 10.1007/978-3-030-36030-6_8.

[Bal+17] Carmen Elisabetta Zaira Baltico, Dario Catalano, Dario Fiore, and Romain Gay. "Practical Functional Encryption for Quadratic Functions with Applications to Predicate Encryption". In:

CRYPTO 2017, Part I. Ed. by Jonathan Katz and Hovav Shacham. Vol. 10401. LNCS. Springer, Heidelberg, Aug. 2017, pp. 67–98. DOI: 10.1007/978-3-319-63688-7_3.

[BJK15] Allison Bishop, Abhishek Jain, and Lucas Kowalczyk. "Function-Hiding Inner Product Encryption". In: *ASIACRYPT 2015, Part I*. Ed. by Tetsu Iwata and Jung Hee Cheon. Vol. 9452. LNCS. Springer, Heidelberg, Nov. 2015, pp. 470–491. DOI: 10.1007/978-3-662-48797-6_20.

[Bon+14] Dan Boneh, Craig Gentry, Sergey Gorbunov, Shai Halevi, Valeria Nikolaenko, Gil Segev, Vinod Vaikuntanathan, and Dhinakaran Vinayagamurthy. "Fully Key-Homomorphic Encryption, Arithmetic Circuit ABE and Compact Garbled Circuits". In: *EUROCRYPT 2014*. Ed. by Phong Q. Nguyen and Elisabeth Oswald. Vol. 8441. LNCS. Springer, Heidelberg, May 2014, pp. 533–556. DOI: 10.1007/978-3-642-55220-5_30.

[BR93] Mihir Bellare and Phillip Rogaway. "Random Oracles are Practical: A Paradigm for Designing Efficient Protocols". In: *ACM CCS 93*. Ed. by Dorothy E. Denning, Raymond Pyle, Ravi Ganesan, Ravi S. Sandhu, and Victoria Ashby. ACM Press, Nov. 1993, pp. 62–73. DOI: 10.1145/168588.168596.

[Bra+19] Zvika Brakerski, Nico Döttling, Sanjam Garg, and Giulio Malavolta. "Leveraging Linear Decryption: Rate-1 Fully-Homomorphic Encryption and Time-Lock Puzzles". In: *TCC 2019, Part II*. Ed. by Dennis Hofheinz and Alon Rosen. Vol. 11892. LNCS. Springer, Heidelberg, Dec. 2019, pp. 407–437. DOI: 10.1007/978-3-030-36033-7_16.

[BSW11] Dan Boneh, Amit Sahai, and Brent Waters. "Functional Encryption: Definitions and Challenges". In: *TCC 2011*. Ed. by Yuval Ishai. Vol. 6597. LNCS. Springer, Heidelberg, Mar. 2011, pp. 253–273. DOI: 10.1007/978-3-642-19571-6_16.

[BV15] Nir Bitansky and Vinod Vaikuntanathan. "Indistinguishability Obfuscation from Functional Encryption". In: *56th FOCS*. Ed. by Venkatesan Guruswami. IEEE Computer Society Press, Oct. 2015, pp. 171–190. DOI: 10.1109/FOCS.2015.20.

[Che+18] Yilei Chen, Vinod Vaikuntanathan, Brent Waters, Hoeteck Wee, and Daniel Wichs. "Traitor-Tracing from LWE Made Simple and Attribute-Based". In: *TCC 2018, Part II*. Ed. by Amos Beimel and Stefan Dziembowski. Vol. 11240. LNCS. Springer, Heidelberg, Nov. 2018, pp. 341–369. DOI: 10.1007/978-3-030-03810-6_13.

[Cho+18] Jérémy Chotard, Edouard Dufour Sans, Romain Gay, Duong Hieu Phan, and David Pointcheval. "Decentralized Multi-Client Functional Encryption for Inner Product". In: *ASIACRYPT 2018, Part II*. Ed. by Thomas Peyrin and Steven Galbraith. Vol. 11273. LNCS. Springer, Heidelberg, Dec. 2018, pp. 703–732. DOI: 10.1007/978-3-030-03329-3_24.

[Cin+23] Valerio Cini, Sebastian Ramacher, Daniel Slamanig, Christoph Striecks, and Erkan Tairi. "(Inner-Product) Functional Encryption with Updatable Ciphertexts". In: *Journal of Cryptology* 37.1 (Dec. 2023), p. 8. ISSN: 1432-1378. DOI: 10.1007/s00145-023-09486-y.

[De +13] Angelo De Caro, Vincenzo Iovino, Abhishek Jain, Adam O'Neill, Omer Paneth, and Giuseppe Persiano. "On the Achievability of Simulation-Based Security for Functional Encryption". In: *CRYPTO 2013, Part II*. Ed. by Ran Canetti and Juan A. Garay. Vol. 8043. LNCS. Springer, Heidelberg, Aug. 2013, pp. 519–535. DOI: 10.1007/978-3-642-40084-1_29.

[FKL18] Georg Fuchsbauer, Eike Kiltz, and Julian Loss. "The Algebraic Group Model and its Applications". In: *CRYPTO 2018, Part II*. Ed. by Hovav Shacham and Alexandra Boldyreva. Vol. 10992. LNCS. Springer, Heidelberg, Aug. 2018, pp. 33–62. DOI: 10.1007/978-3-319-96881-0_2.

[Gar+13] Sanjam Garg, Craig Gentry, Shai Halevi, Mariana Raykova, Amit Sahai, and Brent Waters. "Candidate Indistinguishability Obfuscation and Functional Encryption for all Circuits". In: *54th FOCS*. IEEE Computer Society Press, Oct. 2013, pp. 40–49. DOI: 10.1109/FOCS.2013.13.

[Gay20] Romain Gay. "A New Paradigm for Public-Key Functional Encryption for Degree-2 Polynomials". In: *PKC 2020, Part I*. Ed. by Aggelos Kiayias, Markulf Kohlweiss, Petros Wallden, and Vassilis Zikas. Vol. 12110. LNCS. Springer, Heidelberg, May 2020, pp. 95–120. DOI: 10.1007/978-3-030-45374-9_4.

[Guo+22] Siyao Guo, Pritish Kamath, Alon Rosen, and Katerina Sotiraki. "Limits on the Efficiency of (Ring) LWE-Based Non-interactive Key Exchange". In: *Journal of Cryptology* 35.1 (Jan. 2022), p. 1. DOI: 10.1007/s00145-021-09406-y.

[GVW13] Sergey Gorbunov, Vinod Vaikuntanathan, and Hoeteck Wee. "Attribute-based encryption for circuits". In: *45th ACM STOC*. Ed. by Dan Boneh, Tim Roughgarden, and Joan Feigenbaum. ACM Press, June 2013, pp. 545–554. DOI: 10.1145/2488608.2488677.

[GVW15] Sergey Gorbunov, Vinod Vaikuntanathan, and Hoeteck Wee. "Predicate Encryption for Circuits from LWE". In: *CRYPTO 2015, Part II*. Ed. by Rosario Gennaro and Matthew J. B. Robshaw. Vol. 9216. LNCS. Springer, Heidelberg, Aug. 2015, pp. 503–523. DOI: 10.1007/978-3-662-48000-7_25.

[HW14] Susan Hohenberger and Brent Waters. "Online/Offline Attribute-Based Encryption". In: *PKC 2014*. Ed. by Hugo Krawczyk. Vol. 8383. LNCS. Springer, Heidelberg, Mar. 2014, pp. 293–310. DOI: 10.1007/978-3-642-54631-0_17.

[JLS21] Aayush Jain, Huijia Lin, and Amit Sahai. "Indistinguishability obfuscation from well-founded assumptions". In: *53rd ACM STOC*. Ed. by Samir Khuller and Virginia Vassilevska Williams. ACM Press, June 2021, pp. 60–73. DOI: 10.1145/3406325.3451093.

[JLS22] Aayush Jain, Huijia Lin, and Amit Sahai. "Indistinguishability Obfuscation from LPN over $\mathbb{F}_p$, DLIN, and PRGs in NC^0". In: *EUROCRYPT 2022, Part I*. Ed. by Orr Dunkelman and Stefan Dziembowski. Vol. 13275. LNCS. Springer, Heidelberg, May 2022, pp. 670–699. DOI: 10.1007/978-3-031-06944-4_23.

[KNT18] Fuyuki Kitagawa, Ryo Nishimaki, and Keisuke Tanaka. "Obfustopia Built on Secret-Key Functional Encryption". In: *EUROCRYPT 2018, Part II*. Ed. by Jesper Buus Nielsen and Vincent Rijmen. Vol. 10821. LNCS. Springer, Heidelberg, Apr. 2018, pp. 603–648. DOI: 10.1007/978-3-319-78375-8_20.

[Lin17] Huijia Lin. "Indistinguishability Obfuscation from SXDH on 5-Linear Maps and Locality-5 PRGs". In: *CRYPTO 2017, Part I*. Ed. by Jonathan Katz and Hovav Shacham. Vol. 10401. LNCS. Springer, Heidelberg, Aug. 2017, pp. 599–629. DOI: 10.1007/978-3-319-63688-7_20.

[LPR10] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. "On Ideal Lattices and Learning with Errors over Rings". In: *EUROCRYPT 2010*. Ed. by Henri Gilbert. Vol. 6110. LNCS. Springer, Heidelberg, May 2010, pp. 1–23. DOI: 10.1007/978-3-642-13190-5_1.

[LS15] Adeline Langlois and Damien Stehlé. "Worst-case to average-case reductions for module lattices". In: *DCC* 75.3 (2015), pp. 565–599. DOI: 10.1007/s10623-014-9938-4.

[LT17] Huijia Lin and Stefano Tessaro. "Indistinguishability Obfuscation from Trilinear Maps and Block-Wise Local PRGs". In: *CRYPTO 2017, Part I*. Ed. by Jonathan Katz and Hovav Shacham. Vol. 10401. LNCS. Springer, Heidelberg, Aug. 2017, pp. 630–660. DOI: 10.1007/978-3-319-63688-7_21.

[LT19] Benoît Libert and Radu Titiu. "Multi-Client Functional Encryption for Linear Functions in the Standard Model from LWE". In: *ASIACRYPT 2019, Part III*. Ed. by Steven D. Galbraith and Shiho Moriai. Vol. 11923. LNCS. Springer, Heidelberg, Dec. 2019, pp. 520–551. DOI: 10.1007/978-3-030-34618-8_18.

[Mau05] Ueli M. Maurer. "Abstract Models of Computation in Cryptography (Invited Paper)". In: *10th IMA International Conference on Cryptography and Coding*. Ed. by Nigel P. Smart. Vol. 3796. LNCS. Springer, Heidelberg, Dec. 2005, pp. 1–12.

[ONe10] Adam O'Neill. *Definitional Issues in Functional Encryption*. Cryptology ePrint Archive, Report 2010/556. https://eprint.iacr.org/2010/556. 2010.

[Reg05] Oded Regev. "On lattices, learning with errors, random linear codes, and cryptography". In: *37th ACM STOC*. Ed. by Harold N. Gabow and Ronald Fagin. ACM Press, May 2005, pp. 84–93. DOI: 10.1145/1060590.1060603.

[Sho97] Victor Shoup. "Lower Bounds for Discrete Logarithms and Related Problems". In: *EUROCRYPT'97*. Ed. by Walter Fumy. Vol. 1233. LNCS. Springer, Heidelberg, May 1997, pp. 256–266. DOI: 10.1007/3-540-69053-0_18.

[Tom19] Junichi Tomida. "Tightly Secure Inner Product Functional Encryption: Multi-input and Function-Hiding Constructions". In: *ASIACRYPT 2019, Part III*. Ed. by Steven D. Galbraith and Shiho Moriai. Vol. 11923. LNCS. Springer, Heidelberg, Dec. 2019, pp. 459–488. DOI: 10.1007/978-3-030-34618-8_16.

[Tom23] Junichi Tomida. "Unbounded Quadratic Functional Encryption and More from Pairings". In: *EUROCRYPT 2023, Part III*. Ed. by Carmit Hazay and Martijn Stam. Vol. 14006. LNCS. Springer, Heidelberg, Apr. 2023, pp. 543–572. DOI: 10.1007/978-3-031-30620-4_18.

[Ünal20] Akin Ünal. "Impossibility Results for Lattice-Based Functional Encryption Schemes". In: *EUROCRYPT 2020, Part I*. Ed. by Anne Canteaut and Yuval Ishai. Vol. 12105. LNCS. Springer, Heidelberg, May 2020, pp. 169–199. DOI: 10.1007/978-3-030-45721-1_7.

[Ünal23] Akin Ünal. "Worst-Case Subexponential Attacks on PRGs of Constant Degree or Constant Locality". In: *EUROCRYPT 2023, Part I*. Ed. by Carmit Hazay and Martijn Stam. Vol. 14004. LNCS. Springer, Heidelberg, Apr. 2023, pp. 25–54. DOI: 10.1007/978-3-031-30545-0_2.

A Lower Bounds for Functional Encryption with Ciphertexts of Constant Dimensions

Using the methods of Sections 4 and 5, we show the following lower bounds for FE schemes whose ciphertexts are vectors of constant dimension.

Theorem 7. *Let $q > p > 2$ with q prime and $n, m \in O(1)$ with*

$$m < Q := n^2.$$

Let $\mathcal{F}$ be the space of bilinear functions over $\mathcal{X} = \mathbb{Z}_p^n \times \mathbb{Z}_p^n$, and let $\mathsf{FE} = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ be a lattice-based FE scheme for the functionality $\mathcal{F}$, s.t. each ciphertext of FE is contained in $\mathbb{Z}_q^m$ and d_1 and d_2 denote the encryption depth and decryption depth of FE, respectively. Set

$$M := \max(2 \cdot (m+1) \cdot d_2^m + 1, 2d_1d_2),$$

and assume that the following inequalities hold:

$$q/p \in \mathsf{poly}(\lambda) \qquad \text{and} \qquad c \cdot M^{d_1 \cdot d_2} < p$$

for some constant c that depends on d_1d_2.

If FE is correct, then FE is not selectively IND-CPA secure.

Remark 2. In Theorem 7, it does not matter if there are arithmetic reductions modulo p when evaluating bilinear functions of $\mathcal{F} \subset \mathbb{Z}_p[X_1^{(1)}, \dots, X_n^{(1)}, X_1^{(2)}, \dots, X_n^{(2)}]$ on messages in $\mathcal{X} = \mathbb{Z}_p^n \times \mathbb{Z}_p^n$. This is because we only need to consider quadratic monomials $X_i^{(1)} \cdot X_j^{(2)} \in \mathcal{F}$ as functions and simple vectors $x = (0, \dots, 0, x', 0, \dots, 0, 1, 0, \dots, 0)$ as messages, where x' is bounded by the constant M. Hence, evaluations $f(x)$ will always be bounded by a constant smaller than p.

In fact, the requirements of our theorem can be strongly relaxed. Instead of considering the space of bilinear functions, we can consider any function space $\mathcal{F}\colon \mathcal{X} \to \mathbb{Z}_p$ s.t. there is a $Q > m$ and functions $f_1, \dots, f_Q \in \mathcal{F}$ together with degree-1 polynomials $\nu_1, \dots, \nu_Q\colon \mathbb{Z}_p \to \mathcal{X}$ s.t. we have for all $i, j \in [Q]$ and $x \in \{0, \dots, M\}$,

$$f_i(\nu_j(x)) = \begin{cases} x, & \text{if } i = j, \\ 0, & \text{if } i \neq j. \end{cases}$$

Our proof idea for Theorem 7 follows the proof of Theorem 5. More precisely, we assume that FE is secure and use Corollary 1 to deduce a contradiction. We again assume that KeyGen is deterministic, otherwise we can derandomize it by using a PRF. Next, we define the following $\mathsf{Setup}'_{\mathsf{Pre}}$ algorithm for the FE scheme in Theorem 7, which will be very similar to the algorithm $\mathsf{Setup}'_{\mathsf{Pre}}$ of Section 4:

$\mathsf{Setup}'_{\mathsf{Pre}}$: On input 1^λ, $\mathsf{Setup}'_{\mathsf{Pre}}$ computes a deterministic enumeration of $(a_1, b_1), \ldots, (a_Q, b_Q)$ of $[n]^2$. For each $i \in [Q]$, $\mathsf{Setup}'_{\mathsf{Pre}}$ outputs the polynomial

$$f_i(X_1^{(1)}, \ldots, X_n^{(1)}, X_1^{(2)}, \ldots, X_n^{(2)}) := X_{a_i}^{(1)} \cdot X_{b_i}^{(2)} \in \mathbb{Z}_p[X^{(1)}, X^{(2)}].$$

Then, $\mathsf{Setup}'_{\mathsf{Pre}}$ draws $i_* \leftarrow [Q]$ and outputs i_* together with the linear function

$$\begin{aligned} \nu \colon \mathbb{Z}_p &\longrightarrow \mathbb{Z}_p^n \\ x &\longmapsto x \cdot e_{a_{i_*}} + e_{b_{i_*}}, \end{aligned}$$

where $e_{a_{i_*}}, e_{b_{i_*}}$ denote the a_{i_*}-th and b_{i_*}-th unit vectors.
Note that we have for all $x \in \mathbb{Z}_p$

$$\begin{aligned} f_{i_*}(\nu(x)) &= x, \\ \forall i \neq i_* \colon f_i(\nu(x)) &= 0. \end{aligned}$$

Given $\mathsf{Setup}'_{\mathsf{Pre}}$, we can now define the partial SKE $\mathsf{SKE}' = (\mathsf{Setup}', \mathsf{Enc}', \_)$ as in Definition 12. To prove Theorem 7, we assume that FE is IND-CPA secure and, subsequently, construct a fitting decryption algorithm Dec' that has a non-negligible advantage in decrypting ciphertexts of SKE'. This in turn yields a contradiction to Corollary 1, therefore, proving that FE cannot be secure. To construct Dec', we can follow the proof of Theorem 5, and we just need to prove the following variant of Lemma 3, which states that for each set of secret keys $\mathsf{sk}_1, \ldots, \mathsf{sk}_Q$ output by Setup', there exists some algebraic dependency h_{msk} whose degree is bounded by the constant $D := (m+1) \cdot d_2^m < M/2$.

Lemma 13. *Let $\mathsf{msk}' = (\mathsf{msk}, \mathsf{sk}_1, \ldots, \mathsf{sk}_Q, \nu, i_*)$ be a master secret key output by Setup'. Then, there exists a polynomial $h_{\mathsf{msk}} \in \mathbb{Z}_q[T_1, \ldots, T_Q]$ with the following properties:*

$$\begin{aligned} &h_{\mathsf{msk}} \neq 0 \in \mathbb{Z}_q[T_1, \ldots, T_Q], \\ &h_{\mathsf{msk}}(\mathsf{sk}_1, \ldots, \mathsf{sk}_Q) = 0 \in \mathbb{Z}_q[Y_1, \ldots, Y_m], \\ &\deg h_{\mathsf{msk}} \leq (m+1) \cdot d_2^m. \end{aligned}$$

Proof. Note that $Q > m$, hence, without loss of generality, we can assume that $Q = m + 1$. Let $A := \{h \in \mathbb{Z}_q[T_1, \ldots, T_Q] \mid \deg h \leq (m+1) \cdot d_2^m\}$ be the space of all polynomials in $T_1, \ldots, T_Q$ of degree $\leq (m+1) \cdot d_2^m$ and let $B := \left\{g \in \mathbb{Z}_q[Y_1, \ldots, Y_m] \mid \deg g \leq (m+1) \cdot d_2^{m+1}\right\}$ be space of all polynomials in $Y_1, \ldots, Y_m$ of degree $\leq d_2 \cdot (m+1) \cdot d_2^m$.

To show the existence of an algebraic dependence h_{msk} of $\mathsf{sk}_1, \ldots, \mathsf{sk}_Q$, we will follow the idea of [Üna23]. It suffices to show that the linear map

$$\begin{aligned} \Phi \colon A &\longrightarrow B \\ h(T_1, \ldots, T_Q) &\longmapsto h(\mathsf{sk}_1, \ldots, \mathsf{sk}_Q) \end{aligned}$$

that replaces each occurrence of T_i with the polynomial sk_i of degree $\leq d_2$ has a non-trivial kernel. Indeed, we can lower-bound the dimension of $\ker \Phi$ by

$$\begin{aligned} \dim \ker \Phi &= \dim A - \dim B \\ &= \binom{Q + (m+1) \cdot d_2^m}{Q} - \binom{m + (m+1) \cdot d_2^{m+1}}{m} \\ &= \binom{m + 1 + (m+1) \cdot d_2^m}{m+1} - \binom{m + (m+1) \cdot d_2^{m+1}}{m}. \end{aligned}$$

Now, the inequality $\dim \ker \phi > 0$ is equivalent to the following chain of inequalities:

$$\binom{m + 1 + (m+1) \cdot d_2^m}{m+1} > \binom{m + d_2(m+1) \cdot d_2^m}{m}$$

$$
\begin{aligned}
&\iff (m+1+(m+1)d_2^m)\cdot(m+(m+1)d_2^m)\cdots(1+(m+1)d_2^m)\\
&\qquad > (m+1)\cdot(m+(m+1)d_2^{m+1})\cdots(1+(m+1)d_2^{m+1})\\
&\iff (1+d_2^m)\cdot(m+(m+1)d_2^m)\cdots(1+(m+1)d_2^m)\\
&\qquad > (m+(m+1)d_2^{m+1})\cdots(1+(m+1)d_2^{m+1})\\
&\iff 1+d_2^m > \frac{m+(m+1)d_2^{m+1}}{m+(m+1)d_2^m}\cdots\frac{1+(m+1)d_2^{m+1}}{1+(m+1)d_2^m}. \qquad (15)
\end{aligned}
$$

Equation (15) does hold since we have $\frac{i+(m+1)d_2^{m+1}}{i+(m+1)d_2^m} \leq d_2$ for $i \geq 0$. □

We have shown that for each msk' there exists some algebraic dependency h_{msk} among the secret keys $\mathsf{sk}_1, \ldots, \mathsf{sk}_Q$, whose degree is bounded by a constant D (that only depends on FE). Since KeyGen is derandomized, h_{msk} only depends on msk. From this point on, we can directly follow the proof of Theorem 5 and show analogously that the extractor Dec' of Section 4 has a non-negligible advantage at decrypting ciphertexts of SKE'.