Lower Bounds for Lattice-based Compact Functional Encryption

Erkan Tairi[1] and Akın Ünal[2]

[1] TU Wien, Vienna, Austria
erkan.tairi@tuwien.ac.at
[2] Department of Computer Science, ETH Zurich, Zürich, Switzerland
akin.uenal@inf.ethz.ch

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 whether there are some mathematical barriers which 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 messages and ciphertexts of constant dimensions. 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, O'N10] 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 (secret-key) 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 $\mathsf{Enc}(\mathsf{msk}, x)$ of some message x (under the master secret key msk), 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 [GGH$^+$13, AR17, CVW$^+$18, AV19], thereby entailing feasibility results, and FE schemes for limited classes of functions that are of particular interest for practical applications, e.g., (function-hiding) inner-product FE (IPFE) [ABDP15, BJK15, ALS16, Lin17, Tom19, ALMT20] and compact FE for quadratic functions [BCFG17, Lin17, AS17, Gay20, Tom23]. Furthermore, IPFE and quadratic FE have been extended to multi-input [AGRW17, ACF$^+$18, AGT21a, AGT22], (decentralized) multi-client [CDG$^+$18, ABKW19, LT19, ABG19, AGT21b], and identity/attribute-based [ACGU20, CRS$^+$22] settings.

We also know that FE is a powerful primitive that even implies indistinguishability obfuscation (iO). More precisely, we know that a compact (i.e., sublinear ciphertext size) single-key FE together with plausible assumptions imply iO [AJ15, BV15, LT17, KNT18, Agr19, AP20, JLS21, JLS22].

Moreover, we know that FE for general functionalities with *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, then we either need to rely on heavy-machinery, such as iO [GGH$^+$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, BCFG17, Lin17, Gay20].

In a recent work, Ünal [Üna20] showed implausibility of constructing lattice-based function-hiding IPFE. More precisely, Ünal [Üna20] 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, in this work we ask the following question:

What hinders us from constructing lattice-based compact 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. For this end, we reintroduce here the framework of Ünal [Üna20]:

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 generates random 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* sk *on* 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 algorithm 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 [Üna20] are the right ones, in the sense that they are loose enough to capture all relevant FE schemes (including identity-based (IBE), attributed-based (ABE) and predicate encryption (PE) schemes), whose security rely on the Learning With Errors-assumption (LWE). Moreover, these restrictions are decisive enough to make impossibility results for schemes captured by this framework provable. Let us discuss this in more detail:

First, a closer look at existing lattice-based FE/IBE/ABE/PE schemes [ABB10, GVW13, BGG+14, GVW15, ALS16, AR17, AP20] reveals that the restrictions imposed in Definition 1 are quite natural and fulfilled by almost[3] all of those schemes. As a prime example, we can present here the encryption algorithm of the FE 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

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

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

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

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

$$g_i(X_1, \ldots, X_\ell) := \langle a_i \mid s \rangle + e_{0,i},$$
$$h_i(X_1, \ldots, X_\ell) := \langle b_i \mid s \rangle + e_{1,i} + f \cdot X_i$$

[3] An exception is the decryption algorithms of some ABE schemes [GVW13, BGG+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.

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

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

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

For our restrictions at decryption, we point out that it was already noted by Brakerski et al. [BDGM19] 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.

Second, we note that since the publication of [Üna20] there has been no construction of function-hiding FE from LWE (or any other lattice-based assumption). While the results of [Üna20] only hold in the aforementioned lattice-based FE framework, they (up to now) correctly predicted that constructing function-hiding FE from LWE is almost impossible. This justifies to see the framework of [Üna20] as gauge for measuring the hardness of lattice-based FE schemes and understanding the mathematical barriers that are needed to be overcome.

Third, we believe that one advantage of the lattice-based FE framework is that it allows stripping down unnecessary details of concrete lattice-based FE schemes, and reduce them to only a few relevant details. Take for example the noisy linear FE scheme of Agrawal and Pellet-Mary [AP20]. Their construction is highly convoluted and lacks a security proof, however it is easy to check that it fits into our framework[5]. Therefore, instead of analysing this noisy linear FE scheme, one can rather investigate if the notion of noisy correctness and noisy security is impossible in the lattice-based FE framework, which allows one to focus solely on the relevant details. However, we do not study the scheme of [AP20] here and instead leave it as an interesting open problem.

1.2 Contribution

We generalize the results of Ünal [Üna20] 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 $n, m \in O(1)$ and let FE *be a* lattice-based *functional encryption scheme for quadratic polynomials with input space $\mathbb{Z}_p^n$ where each ciphertext is contained in $\mathbb{Z}_q^m$.*

We assume that FE *is compact i.e., the inequality*

$$m < \binom{n}{2} = \frac{n^2 - n}{2}.$$

for the dimension n of the message space and the dimension m of the ciphertext space of FE *does hold.*

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 FE scheme and using the compactness of the FE scheme to prove correctness of the aforementioned SKE scheme. This in turn leads to a contradiction of a theorem specified in [Üna20] and gives us implicitly an attack on lattice-based compact FE scheme.

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

[5] The decryption algorithm of [AP20] applies the modulo operation twice, which is equivalent to rounding twice. This is one more rounding than the lattice-based FE framework allows. However, this is not an issue, since in both cases decryptions to zero must imply that the scalar product of secret key and ciphertext is small.

In fact, for our result and the result of [Üna20] the decryption restriction of the framework can be relaxed to the requirement that the evaluation of the polynomial sk_f on the ciphertext ct_x must be small if $f(x) = 0$.

1.3 Interpretation, Limitations and Open Problems

Parameter Restrictions. We have analogous parameter restrictions as in [Üna20]. 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 is bounded by a polynomial in the security parameter λ, where p is the interior modulus, such that p is for almost all λ 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 LWE.

Additionally, we require that the input space dimension n and ciphertext space dimension m are both constants, i.e., we restrict ourselves to constant-dimension messages and ciphertexts in this work. While this is a non-standard restriction of parameters (most lattice-based schemes have ciphertexts of non-constant dimensions), generalizing our results here for ciphertexts of non-constant dimension is highly non-trivial, which will become apparent in Section 1.5.

Interpretation and Open Problems. We view the results in this paper as a useful argument in understanding the difficulties in 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 the aforementioned 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 the FHE schemes). 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 in constructing lattice-based FE schemes.

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 [Üna20], in our case also 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 modelled 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 public-key setting and OWFs in secret-key setting. Though, 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 compact ciphertexts, i.e., sublinear[6] ciphertext size, implies iO [AJ15, BV15] [7] . 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 [DIJ⁺13] showed that that compact FE with simulation-based security is impossible for general functions [AGVW13, DIJ⁺13], however for constructing iO from compact FE using the aforementioned works selective indistinguishability security suffices.

As explained in Section 1.5, in this work we consider that the encryption algorithm can be decomposed into simple online and complex offline parts. Such a decomposition has been previously used both for constructing new FE schemes [HW14, AR17] and showing impossibility results [Üna20]. However, none of these works considered the compact FE case.

[6] By "sublinear" we mean that the ciphertext size is sublinear in the number of function secret keys requested by the FE adversary.

[7] Technically, [AJ15] and [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 dependence on the function size, i.e., $\mathsf{poly}(\lambda, |x|) \cdot |f|^{1-e}$ for some constant $e \in (0, 1]$.

Other Models of Computation. Computational models are a popular approach in cryptography to prove lower bounds for solving certain problems. However, 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. In fact, we are not aware of any other model than [Üna20] for capturing lattice-based problems and primitives.

One model that potentially comes close is the model of *arithmetic circuits* of Applebaum, Avron and Brzuska [AAB17]. They consider primitives and protocols where each party resp. primitive is computed by an algebraic circuit that can be evaluated over any finite field. In their work, they prove several lower bounds for protocols and primitives that *arithmetizes*. However, the model of arithmetic circuits falls short to capture the lattice-based setting we consider here. In comparison with the lattice-based FE framework, we note three differences:

1. In lattice-based FE schemes, encryption algorithms come in fact close to arithmetic circuits: they sample some randomness and then apply an algebraic low-degree circuit on it. However, in the model of [AAB17], the arithmetic circuit can only sample random bits and random field elements, while our framework allows the circuit to sample any randomness that may depend on the field $\mathbb{Z}_q$ (for example, arithmetic circuits are unable to sample a uniformly random integer from $\{0, \dots, \lceil q/2 \rfloor\} \subset \mathbb{Z}_q$).
2. We do not make any restrictions on the Setup and KeyGen algorithms of the FE schemes, while the model of [AAB17] requires these algorithms to be arithmetic circuits.
3. The most crucial differences are our restrictions at decryption: at decryption our FE schemes apply an arithmetic low-depth circuit at secret key and ciphertext and then round the result from $\mathbb{Z}_q$ to $\mathbb{Z}_p$. However, rounding is a prime example of a function that does not arithmetize, at all. In fact, the algebraic degree of the rounding function grows with the size of the field.

Taking all these three points together, we see that the model of arithmetic circuits [AAB17] is not able to capture typical characteristics of lattice-based primitives.

1.5 Technical Overview

In this subsection, we will sketch a proof for Theorem 1. To this end, we will first introduce the framework of Ünal [Üna20] for modelling lattice-based FE schemes, which we use in this work. Next, we will revisit the strategy of [Üna20] for proving lower bounds for lattice-based *function-hiding* FE schemes and generalize it. Finally, we will attempt to adapt the generalized strategy on *compact* lattice-based FE schemes. Unfortunately, our first attempt will fail, however we will be able to fix the strategy for compact lattice-based FE schemes with ciphertexts and messages of *constant dimensions*.

Our Framework. A (secret-key) *functional encryption* (FE) scheme consists of four algorithms: Setup, KeyGen, Enc and Dec. On input the security parameter 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 that we adapt the framework from [Üna20], i.e., 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 $(r_1, \dots, r_m)$. In the simple *online* phase, Enc sees the message $x \in \mathbb{Z}_p^n$ and the randomness $(r_1, \dots, r_m)$ 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 $r_1, \dots, r_m \in \mathbb{Z}_q[X_1, \dots, X_n]$ of *constant* degree. $\mathsf{Enc}(\mathsf{msk}, x)$ is then expected to work by first sampling $(r_1, \dots, r_m) \leftarrow \mathsf{Enc}_{\mathsf{off}}(\mathsf{msk})$, and then outputting the ciphertext $\mathsf{ct}_x = (r_1(x), \dots, r_m(x)) \in \mathbb{Z}_q^m$. We call the maximum degree of $r_1, \dots, r_m$ 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. Implausibility of lattice-based *function-hiding* FE schemes has already been shown in [Üna20]. We explain here the strategy used in [Üna20], before we generalize it and adapt it to the *compact* FE case.

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, too, 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.,

$$\mathsf{ct}' \in [-q/p, q/p]^{Q-1}.$$

This is because the decryption algorithm of FE works as $\mathsf{Dec}(\mathsf{sk}, \mathsf{ct}) = \lceil \mathsf{sk}(\mathsf{ct}) \cdot p/q \rfloor$. 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.

Normally, extracting the message x_1 out of ct' would be impossible. 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

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

This property 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

$$\mathsf{sk}_Q \in \operatorname{span}_{\mathbb{Z}_q} \{\mathsf{sk}_1, \ldots, \mathsf{sk}_{Q-1}\} .$$

If that is the case, 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 $1 - o(1)$.

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 [Üna20] 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 ([Üna20] (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 for each pair of messages* $x, y \in \{0, \ldots, 2d\}$ *the statistical distance of the distributions* $(\mathsf{msk}, \mathsf{Enc}(\mathsf{msk}, x))$ *and* $(\mathsf{msk}, \mathsf{Enc}(\mathsf{msk}, y))$ *is negligible.*

This yields a contradiction to the scheme SKE' we constructed, because Dec' cannot have a successful decryption probability of $1-o(1)$ when ciphertexts $\mathsf{ct}'_x \leftarrow \mathsf{Enc}'(\mathsf{msk}, x)$ and $\mathsf{ct}'_y \leftarrow \mathsf{Enc}'(\mathsf{msk}, y)$ are statistically very 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 adapt 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'' will be too (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'' will have indeed a non-trivial success probability at decryption.

Concretely, SKE'' contains 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 an affine linear function $\nu_{i_*} \colon \mathbb{Z}_p \to \mathbb{Z}_p^n$ s.t. we have for each $x_1 \in \mathbb{Z}_p$

$$\begin{aligned}\forall i \neq i_* \colon f_i(\nu_{i_*}(x_1)) &= 0 \\ f_{i_*}(\nu_{i_*}(x_1)) &= x_1.\end{aligned}$$

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 $\mathsf{sk}_1, \dots, \mathsf{sk}_{i_*-1}$, $0, \mathsf{sk}_{i_*+1}, \dots, \mathsf{sk}_Q$ at ct and returns

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

Dec'': On input msk'' and $\mathsf{ct}'' = (c_1, \dots, c_Q)$, 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 $f_1, \dots, f_Q$ 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 prove these properties in detail in Section 3.

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 in correctly decrypting a ciphertext. 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 way more complicated 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 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 messages and ciphertexts of constant dimensions.

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 function space* $\mathcal{F}$*. We call* FE ***compact*** *(resp.* ***succinct****) if there is a constant* $e > 0$ *s.t.*

$$\log(q) \cdot m \in O(\log(\# \mathcal{F})^{1-e}).$$

In other words, we demand that the binary representation of a ciphertext grows polynomially smaller than the average binary representation of a function $f \in \mathcal{F}$. In the literature, there are different definitions of compactness and succinctness (c.f. [BV15, AJ15, AV19, KNT18]). 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

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

while its message space is $\mathbb{Z}_p^n$. Compactness now states that we have

$$\log(q) m \in O(\log(\# \mathcal{F})^{1-e}) = O((\log(p) \cdot n^2)^{1-e}) = O(\log(p)^{1-e} \cdot n^{2-2e}) \tag{2}$$

for a constant $e > 0$. In particular, since $p < q$, we have $m \in O(n^{2-2e})$, which means 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 [Üna23] to achieve a non-trivial success probability at decryption.

First, we will specify how Setup'' chooses the functions $f_1, \dots, f_Q \in \mathcal{F}$, 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

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

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 defines 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 $i \in [Q]$,

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

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 $\mathsf{ct}'' := (\mathsf{sk}_1(\mathsf{ct}), \ldots, \mathsf{sk}_{i_*-1}(\mathsf{ct}), 0, \mathsf{sk}_{i_*+1}(\mathsf{ct}), \ldots, \mathsf{sk}_Q(\mathsf{ct}))$ 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 $\mathsf{sk}_1, \ldots, \mathsf{sk}_{i_*-1}, \mathsf{sk}_{i_*+1}, \ldots, \mathsf{sk}_Q \in \mathbb{Z}_q[Y_1, \ldots, Y_m]$ of constant degree. Therefore, we can substantially bound the number of possible values of $\mathsf{sk}_{i_*}(\mathsf{ct})$. We illustrate this with the following simple 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 $h(T_1, T_2, T_3) := T_1^4 + T_2^2 + T_3^4 - 2T_1^2T_2 - 2T_1^2T_2^2 - 2T_2^2T_3^2$ and note that we have

$$h(\mathsf{sk}_1(Y_1, Y_2), \mathsf{sk}_2(Y_1, Y_2), \mathsf{sk}_3(Y_1, Y_2)) = 0. \tag{3}$$

Now, if we plug in the values $a, b \in \mathbb{Z}_p$, we get the univariate degree-4 polynomial

$$h(\mathsf{sk}_1(\mathsf{ct}), \mathsf{sk}_2(\mathsf{ct}), T_3) = h(a, b, T_3) = T_3^4 - 2(a^2 + b)T_3^2 + (a^4 + b^2 - 2a^2b).$$

Because of Equation (3), 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 zero locus of $h(a, b, T_3)$. Since $h(a, b, T_3)$ is of degree 4, there are at most 4 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 $1/4$, which is noticeably larger than $1/p$.

In general, the polynomials $\mathsf{sk}_1, \ldots, \mathsf{sk}_Q$ are of some constant degree, let's say $d \in O(1)$, and their number $Q = \binom{n}{2}$ is substantially larger than the number of coordinates $m \in O(n^{2-2e})$ 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 $\mathsf{sk}_1, \ldots, \mathsf{sk}_Q$:

Theorem 3 (Adapted from [Üna23]). *Let $Q \in \Omega(n^2)$ and $m \in O(n^{2-2e})$ for a constant $e > 0$. Let $g_1, \ldots, g_Q \in \mathbb{Z}_q[Y_1, \ldots, Y_m]$ be of degree $d \in O(1)$.*

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

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

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

$$h(\mathsf{sk}_1(\mathsf{ct}), \dots, \mathsf{sk}_{i_*-1}(\mathsf{ct}), T_{i_*}\, \mathsf{sk}_{i_*+1}(\mathsf{ct}), \dots, \mathsf{sk}_Q(\mathsf{ct})) \in \mathbb{Z}_q[T_{i_*}]. \tag{4}$$

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

The above reasoning shows how we can use the compactness of FE, which is considerably harder to grasp than other properties like function-hiding, 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 a gap in the above reasoning. What happens if the univariate polynomial in Equation (4) 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 (4) 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 relevant success probability anymore for Dec''. Subsequently, SKE'' is not sufficiently correct anymore, 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 (4). Each coefficient is computed by a polynomial in the variables $T_1, \dots, T_{i_*-1}$, $T_{i_*+1}, \dots, T_m$ of lower degree. Concretely, we have

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

for fitting polynomials $h_0, \dots, h_{\deg h} \in \mathbb{Z}_q[T_1, \dots, T_{i_*-1}, T_{i_*+1}, \dots, T_m]$ of sublinear degree. We can assume that the highest degree coefficient $h_{\deg h}$ is non-zero. If the polynomial in Equation (4) 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 $\mathsf{sk}_1(\mathsf{ct}), \dots, \mathsf{sk}_{i_*-1}(\mathsf{ct})$, $\mathsf{sk}_{i_*+1}(\mathsf{ct}), \dots, \mathsf{sk}_Q(\mathsf{ct})$, but does not become zero when we plug in $\mathsf{sk}_1(\mathsf{ct}), \dots, \mathsf{sk}_{i_*-1}(\mathsf{ct}), \mathsf{sk}_{i_*+1}(\mathsf{ct}), \dots, \mathsf{sk}_{Q-1}(\mathsf{ct})$, we could use it to bound the number of possible values of $\mathsf{sk}_Q(\mathsf{ct})$ while fixing the values of $\mathsf{sk}_1(\mathsf{ct}), \dots, \mathsf{sk}_{i_*-1}(\mathsf{ct}), \mathsf{sk}_{i_*+1}(\mathsf{ct}), \dots, \mathsf{sk}_{Q-1}(\mathsf{ct})$. 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 a different distribution of ciphertexts, namely $\mathsf{Enc}(\mathsf{msk}, \nu_Q(x))$. This yields the following problem: it may happen that $h_{\deg h}(\mathsf{sk}_1(\mathsf{ct}), \dots, \mathsf{sk}_{i_*-1}(\mathsf{ct}), \mathsf{sk}_{i_*+1}(\mathsf{ct}), \dots, \mathsf{sk}_{Q-1}(\mathsf{ct}))$ 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 comes from $\mathsf{Enc}(\mathsf{msk}, \nu_Q(x))$.

To solve this problem, we need that some kind of homogeneity among ciphertexts of FE for different messages does hold. In particular, we need that if some 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, this kind of homogeneity can only be proven in cases where g has a constant degree and each ciphertext only has a constant number of entries. This leads to the result of our paper, which shows lower bounds for lattice-based compact FE schemes where the dimensions of messages and ciphertexts are constant.

Messages and Ciphertexts of Constant Dimension. Let FE be lattice-based with support for quadratic polynomials and messages and ciphertexts of constant size, by which we mean that their lengths n, m as vectors are constant (p and q do not need to be constant). Note that in this case Definition 2 does not make any sense, since Equation (2) cannot be fulfilled when n, m are constant, since $q > p$. Instead, we demand – in the spirit of Definition 2 – that we have the sharp inequality

$$m < \binom{n}{2} = \frac{n^2 - n}{2}. \tag{5}$$

Note that, if n and m would not be constant, Definition 2 would imply that $m \in O(n^{2e-2})$ and Equation (5) would be fulfilled in the non-constant case for λ large enough. This justifies the plausibility of Equation (5) for an FE scheme with ciphertexts of constant dimension.

If n and m are constant, then the degree of the algebraic relation $h \in \mathbb{Z}_q[T_1, \dots, T_Q]$ among the polynomials $\mathsf{sk}_1, \dots, \mathsf{sk}_Q$ is constant too. If $x, y \in \mathbb{Z}_p^n$ are two different messages, we can sufficiently relate the probability of any constant-degree polynomial $g \in \mathbb{Z}_q[Y_1, \dots, Y_m]$ vanishing on ciphertexts of x with the probability of g vanishing on ciphertexts of y. In fact, let $\mathsf{ct}_x \leftarrow \mathsf{Enc}(\mathsf{msk}, x)$ and $\mathsf{ct}_y \leftarrow \mathsf{Enc}(\mathsf{msk}, y)$, then for each $\ell \in \mathsf{poly}(\lambda)$ there is an $\varepsilon_\ell \in \mathsf{negl}(\lambda)$ s.t.

$$\Pr\left[g(\mathsf{ct}_x) = 0\right] \geq \ell \cdot \Pr\left[g(\mathsf{ct}_y) = 0\right] - (\ell - 1) - O(1/(\ell + 1)) - \varepsilon_\ell. \tag{6}$$

In particular, $\Pr\left[g(\mathsf{ct}_x) = 0\right]$ must be overwhelming iff $\Pr\left[g(\mathsf{ct}_y) = 0\right]$ is overwhelming. This homogeneity among ciphertexts of FE allows us to fix the flaws of our previous attempt and reach a contradiction, which results in an attack for lattice-based FE schemes for quadratic polynomials with messages and ciphertexts of constant size that adhere to Equation (5). We detail this in Section 4.

On Difficulty of Overcoming Constant Dimensions. To extend the proof strategy here to FE schemes with ciphertexts of non-constant dimensions m, one would need to extend the statements of Lemmas 6 and 7.

For Lemma 7, a non-constant dimension m would mean, the inequality (6) becomes

$$\Pr\left[g(\mathsf{ct}_x) = 0\right] \geq \ell \cdot \Pr\left[g(\mathsf{ct}_y) = 0\right] - (\ell - 1) - O(m^{\deg g}/(\ell + 1)) - \varepsilon_\ell, \tag{7}$$

where the degree $\deg g$ is sublinear in m. However, since the term ℓ, which stems from the runtime of a potential IND-CPA adversary, must always be polynomial, and $O(m^{\deg g})$ grows significantly larger than each polynomial, inequality (7) does not give us a meaningful connection between the behaviour of g on ciphertexts of different messages anymore.

Furthermore, an extension of Lemma 6 to the non-constant case would imply that each chain $0 = p_0(\lambda) \leq \ldots \leq p_Q(\lambda) = 1$ of probabilities has, for non-constant Q, a function $I \colon \mathbb{N} \to \mathbb{N}$ s.t. we have for infinitely many λ

$$I(\lambda) \leq Q(\lambda),\ p_{I(\lambda)}(\lambda) \geq 1 - \mathsf{negl}(\lambda) \text{ and } p_{I(\lambda)}(\lambda) - p_{I(\lambda)-1}(\lambda) \notin \mathsf{negl}(\lambda).$$

However, for non-constant Q this is impossible. In fact, a counter-example is given by

$$p_i(\lambda) := \begin{cases} 0, & \text{if } i \notin [Q], \\ 1 - 2^{i-Q}, & \text{if } i \in [Q]. \end{cases}$$

2 Preliminaries

Notation. In this text, we will 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

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

In this text, we will work with two moduli $p, q > 2$ s.t. q is always prime and we always have $p < 2q$. 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'.

2.1 Mathematical Preliminaries

Lemma 1 ([Üna20]). *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*

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

Lemma 2. *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 $h \in \mathbb{Z}_q[Y_1,\ldots,Y_m,T_1,\ldots,T_m]$ of degree $\leq d$ the implication

$$\begin{aligned}&\psi_d(y_{\ell+1}) \in \operatorname{span}_{\mathbb{Z}_q}\{\psi_d(y_1),\ldots,\psi_d(y_\ell)\}, \forall i \in [\ell] : h(y_i,T_1,\ldots,T_Q) = 0\\ &\implies h(y_{\ell+1},T_1,\ldots,T_Q) = 0.\end{aligned}$$

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 $\psi_d(y_{\ell+1}) \in \operatorname{span}_{\mathbb{Z}_q}\{\psi_d(y_1),\ldots,\psi_d(y_\ell)\}$ 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

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

□

Lemma 3. *Let $m, d \in \mathbb{N}$. For $D = (m+1)d^m$, we have $\binom{m+1+D}{m+1} > \binom{m+dD}{m}$.*

Proof. We have the following equivalent inequalities:

$$\binom{m+1+D}{m+1} > \binom{m+dD}{m}$$

$$\begin{aligned}
&\iff (m+1+(m+1)d^m)\cdot(m+(m+1)d^m)\cdots(1+(m+1)d^m)\\
&\qquad > (m+1)\cdot(m+(m+1)d^{m+1})\cdots(1+(m+1)d^{m+1})\\
&\iff (1+d^m)\cdot(m+(m+1)d^m)\cdots(1+(m+1)d^m)\\
&\qquad > (m+(m+1)d^{m+1})\cdots(1+(m+1)d^{m+1})\\
&\iff 1+d^m > \frac{m+(m+1)d^{m+1}}{m+(m+1)d^m}\cdots\frac{1+(m+1)d^{m+1}}{1+(m+1)d^m}. \qquad (8)
\end{aligned}$$

Equation (8) does hold since we have $\frac{i+(m+1)d^{m+1}}{i+(m+1)d^m} \leq d$ for $i \geq 0$. □

2.2 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 **constant** if we have $\mathcal{X}_\lambda = \mathcal{X}_{\lambda+1}$ for all $\lambda \in \mathbb{N}$.*

*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 $f_\lambda : X_\lambda \to Y_\lambda$ 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 $\mathcal{F} : \mathcal{X} \to \mathcal{Y}$.*

Definition 4 (Functional Encryption). *A (secret-key) **functional encryption** (FE) scheme for the function space $(\mathcal{F}_\lambda)_\lambda$ 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 of the message space $\mathcal{X}$ of* FE*, it outputs a ciphertext ct_x of $x \in \mathcal{X}_\lambda$.*

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 $\Pr[\mathsf{Dec}(\mathsf{sk}_f, \mathsf{ct}_x) \neq f_\lambda(x_\lambda)] \leq \varepsilon(\lambda)$ for all $(f_\lambda)_\lambda \in \mathcal{F}$ and $(x_\lambda)_\lambda \in \mathcal{X}$ where $\mathsf{msk} \leftarrow \mathsf{Setup}(1^\lambda)$, $\mathsf{sk}_f \leftarrow \mathsf{KeyGen}(\mathsf{msk}, f_\lambda)$, $\mathsf{ct}_x \leftarrow \mathsf{Enc}(\mathsf{msk}, x_\lambda)$.*

Definition 5 (Selective IND-CPA Security). *Let $\mathsf{FE} = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ be an FE scheme for the function space $(\mathcal{F}_\lambda)_\lambda$. We define the **selective IND-CPA** security game of* FE *as an experiment $\mathsf{Exp}^{\mathsf{ind\text{-}cpa}}_{\mathsf{FE}}(\mathcal{A}, 1^\lambda)$ between an adversary $\mathcal{A}$ and a challenger $\mathcal{C}$ that proceeds in the following steps:*

Experiment $\mathsf{Exp}^{\mathsf{ind\text{-}cpa}}_{\mathsf{FE}}(\mathcal{A}, 1^\lambda)$

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*

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

   $\mathcal{C}$ 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 if for each $i \in [N]$ and $j \in [Q]$*

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

   the experiment outputs 1, else 0.

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

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

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

2.3 Lattice-Based Encryption Algorithms

In the following, we will recapitulate the definition of *offline-/online-encryption* of constant depth that has been used in [Üna20].

Definition 6. *Let* $\mathsf{FE} = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *be a functional encryption scheme with messages space* $\mathcal{X} = \mathbb{Z}_p^n$*.*

Let further $q = q(\lambda)$ be a primes.t. each ciphertext output by Enc *is a vector in* $\mathbb{Z}_q^m$*.*

Let $d \in \mathbb{N}$ be constant. We say that Enc *is of* ***depth*** *d if there is an offline 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 $\leq d$ s.t. the following distributions are identical for each* $\mathsf{msk} \leftarrow \mathsf{Setup}(1^\lambda)$ *and $x \in \mathbb{Z}_p^n$:*

$$\{(r_1(x), \dots, r_m(x)) \mid (r_1, \dots, r_m) \leftarrow \mathsf{Enc}_{\mathsf{off}}(\mathsf{msk})\}$$

and

$$\{\mathsf{ct} \mid \mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{msk}, x)\}.$$

Note, that we don't 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 doesn't 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 gets to see 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 [Üna20], 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 all $(x_\lambda)_\lambda \in \mathcal{X}$*

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

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

When we speak of *lattice-based* FE schemes, we will make the same restrictions on FE schemes that have been made in [Üna20].

Definition 8 (Lattice-Based FE Scheme). *Let* $\mathsf{FE} = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *be an FE scheme. Let q be 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 $\mathbb{Z}_q[Z_1, \dots, Z_m]$ of total degree $\leq d_2$*
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*.*

2.4 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 9 (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* $\mathsf{id} : \mathcal{X}_\lambda \to \mathcal{X}_\lambda$.

For an SKE $\mathsf{SKE} = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$*, 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* $(\mathsf{Setup}, \mathsf{Enc}, \mathsf{Dec})$ *of* SKE.

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

Definition 10 (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 fitting message space* $\mathcal{X}$ *that adhere 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 9.*

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 *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* $\mathcal{X} = \{0, \ldots, M\}$ *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* $\mathsf{msk} \leftarrow \mathsf{Setup}(1^\lambda)$
$$\Pr\left[\forall x, y \in \mathcal{X}_\lambda : \mathit{\Delta}(\mathsf{Enc}(\mathsf{msk}, x), \mathsf{Enc}(\mathsf{msk}, y)) < \frac{1}{r(\lambda)}\right] \geq 1 - \varepsilon(\lambda).$$
4. *There is an* $\varepsilon \in \mathsf{negl}(\lambda)$ *s.t. we have* $\mathit{\Delta}(C_x, C_y) \leq \varepsilon(\lambda)$ *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 as follows to deduce lower bounds for FE. To 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 11. *Let* $\mathsf{FE} = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *be a functional encryption scheme with message space* $\mathcal{X} = \mathbb{Z}_p^n$. *Let* $M \in \mathsf{poly}(\lambda)$. *We construct a partial SKE* $\mathsf{SKE}' = (\mathsf{Setup}', \mathsf{Enc}', \_)$ *with message space* $\mathcal{X}' := \{0, \ldots, M\}$ *with the following algorithms:*

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

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

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

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

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

Setup' : *On input* 1^λ, Setup' *runs* $(f_1, \ldots, f_Q, \nu, i_*) \leftarrow \mathsf{Setup_{Pre}}'(1^\lambda)$.
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*

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

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

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

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

We now have the following result:

Lemma 4. *In the scheme* $\mathsf{SKE}' = (\mathsf{Setup}', \mathsf{Enc}', \_)$ *from Definition 11,* 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 $\mathsf{Enc_{off}}$ that on input msk outputs m polynomials $r_1, \ldots, r_m \in \mathbb{Z}_q[X_1, \ldots, X_n]$ of degree $\leq d_1$ s.t. $\mathsf{Enc}(\mathsf{msk}, x)$ is equally distributed as $(r_1(x), \ldots, r_m(x))$ for each $x \in \mathbb{Z}_p^n$.
We now define $\mathsf{Enc_{off}}'$ as follows. On input $\mathsf{msk}' := (\mathsf{msk}, \mathsf{sk}_1, \ldots, \mathsf{sk}_Q, \nu, i_*)$, $\mathsf{Enc_{off}}'$ first computes $(r_1, \ldots, r_m) \leftarrow \mathsf{Enc_{off}}(\mathsf{msk})$ and then returns the polynomials

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

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

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

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

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

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.

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

In particular, for this $\lambda \in \mathbb{N}$, there exists an $f \in \mathcal{F}_\lambda$ and an $x \in \mathcal{X}_\lambda$ s.t.

$$\Pr_{\substack{\mathsf{msk} \leftarrow \mathsf{Setup}(1^\lambda) \\ \mathsf{sk} \leftarrow \mathsf{KeyGen}(\mathsf{msk}, f) \\ \mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{msk}, x)}} [\mathsf{Dec}(\mathsf{sk}, \mathsf{ct}) \neq f(x)] > \varepsilon(\lambda).$$

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 one 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 security of FE.
If $\mathcal{A}'$ is a selective IND-CPA adversary against 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 $i \in [N], \beta \in \{0, 1\}$, $\mathcal{A}$ computes
$$x_i^\beta := \nu({x'_i}^\beta) \in \mathbb{Z}_p^n\,.$$
(d) $\mathcal{A}$ submits the lists $(x_1^0, \ldots, x_N^0)$, $(x_1^1, \ldots, x_N^1)$, $(f_1, \ldots, f_{i_*-1}, f_{i_*+1}, \ldots, f_Q)$ to $\mathcal{C}'$ and 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 the messages $x_1^b, \ldots, x_N^b$ with 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 $i \in [N]$ and $j \neq i_*$
$$f_j(x_i^0) = f_j(\nu({x'_i}^0)) = 0 = f_j(\nu({x'_i}^1)) = f_j(x_i^1).$$
In other words, $\mathcal{A}$ is a valid adversary, and hence, does not submit to $\mathcal{C}'$ any combination of function and message pairs that would help him to win trivially. 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'.

□

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 11 that is constructed from* FE *with message space* $\{0, \dots, M\}$*.*

Then, there is no 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*

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

Proof. Set $\mathcal{X}' := \{0, \dots, M\}$. Because of Lemma 4, 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.

$$\varDelta(\mathsf{Dec}(\mathsf{msk}'_1, \mathsf{ct}'_x), \mathsf{Dec}(\mathsf{msk}'_2, \mathsf{ct}'_y)) \leq \varepsilon' \tag{9}$$

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

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

$$\Pr_{\substack{x \leftarrow \{0,\dots,M\}\\ \mathsf{msk}' \leftarrow \mathsf{Setup}'(1^\lambda)\\ \mathsf{ct}' \leftarrow \mathsf{Enc}'(\mathsf{msk}', x)}} \left[\mathsf{Dec}'(\mathsf{msk}', \mathsf{ct}') = x\right] \geq \frac{1}{\#\mathcal{X}'_\lambda} + \frac{1}{r(\lambda)}. \tag{10}$$

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

$$\begin{aligned}
&\Pr\left[\mathsf{Dec}'(\mathsf{msk}', \mathsf{ct}'_x) \in \mathcal{X}\right] \\
=\ & \sum_{y \in \mathcal{X}'_\lambda} \Pr\left[\mathsf{Dec}'(\mathsf{msk}', \mathsf{ct}'_x) = y\right] \\
\overset{Eq.~(9)}{\geq}\ & \sum_{y \in \mathcal{X}_\lambda} \left(\Pr\left[\mathsf{Dec}'(\mathsf{msk}', \mathsf{ct}'_x) = x\right] - \varepsilon'(\lambda)\right) \\
=\ & (M+1) \Pr\left[\mathsf{Dec}'(\mathsf{msk}', \mathsf{ct}'_x) = x\right] - (M+1)\varepsilon'(\lambda) \\
\overset{Eq.~(10)}{\geq}\ & 1 + \frac{M+1}{r(\lambda)} - (M+1)\varepsilon'(\lambda).
\end{aligned}$$

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, which is captured with the following theorem:

Theorem 5. *Let $q > p > 2$ with q prime and $n, m \in O(1)$ with $n < m < Q := \binom{n}{2}$.*

Let $\mathsf{FE} = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ be a lattice-based functional encryption scheme with message space $\mathcal{X} = \mathbb{Z}_p^n$ and function space

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

Let each ciphertext of FE be contained in $\mathbb{Z}_q^m$, and let $d_1 \in O(1)$ be the encryption depth and $d_2 \in O(1)$ be the decryption depth of FE. Set $M := 2(m+1) \cdot d_2^m$ and assume that the following inequalities hold:

$$q/p \in \mathsf{poly}(\lambda), \qquad c \cdot M^{d_1 \cdot d_2} < p \qquad \text{and} \qquad M \geq 2d_1d_2$$

for some constant c that depends on d_1d_2.

If FE is correct and if there exist pseudorandom functions (which are pseudorandom against PPT adversaries), then FE is not selectively IND-CPA secure.

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

1. Although requiring the existence of pseudorandom functions may seem odd, we note that we need this solely because we want to assume – without loss of generality – that the key generation algorithm KeyGen of FE is deterministic (which eases some technicalities of our proof). In fact, if KeyGen is probabilistic we can use a pseudorandom function PRF to derandomize it: we replace the algorithms Setup and KeyGen of FE by new algorithms $\mathsf{Setup}_{\mathrm{det}}$ and $\mathsf{KeyGen}_{\mathrm{det}}$. $\mathsf{Setup}_{\mathrm{det}}$ runs Setup to get the master secret key msk, and additionally, samples a random key k for PRF and outputs (msk, k) as the new master secret key. $\mathsf{KeyGen}_{\mathrm{det}}$ receives (msk, k) and the description of a function $f \in \mathcal{F}$. It evaluates PRF with key k on a binary description of f to generate pseudorandom coins r for KeyGen. With these pseudorandom bits, $\mathsf{KeyGen}_{\mathrm{det}}$ can simulate the probabilistic algorithm KeyGen in a deterministic way.
   The IND-CPA security of the scheme $(\mathsf{Setup}_{\mathrm{det}}, \mathsf{KeyGen}_{\mathrm{det}}, \mathsf{Enc}, \mathsf{Dec})$ follows via a hybrid argument. Assuming the existence of pseudorandom functions is not a restriction for our theorem, since their existence is implied by standard assumptions, such as LWE with super-polynomial noise ratio [BPR12].
2. In Theorem 5, we do not specify if there is an arithmetic reduction modulo p when evaluating the polynomials in $\mathcal{F} \subset \mathbb{Z}_p[X_1, \dots, X_n]$ on messages in $\mathcal{X} = \mathbb{Z}_p^n$. The reason is it is irrelevant for our proof. In fact, our proof only considers quadratic monomials $X_i \cdot X_j \in \mathcal{F}$ 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. We only need that for constants m, Q there are functions $f_1, \dots, f_Q \in \mathcal{F}$ and 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 5 is to assume that FE is secure and then to use Corollary 1 to deduce a contradiction. To this end, we define the following $\mathsf{Setup_{Pre}}'$ algorithm for the FE scheme in Theorem 5:

$\mathsf{Setup_{Pre}}'$: On input 1^λ, $\mathsf{Setup_{Pre}}'$ computes the set of all pairs of numbers in $[n]$

$$I := \{\{a, b\} \mid a, b \in [n], a < b\}\,.$$

Let $\{a_1, b_1\}, \dots, \{a_Q, b_Q\}$ be an enumeration of all elements of I where $Q = \binom{n}{2} = \frac{n^2 - n}{2}$. For each $i \in [Q]$, $\mathsf{Setup_{Pre}}'$ outputs the polynomial

$$f_i(X_1, \dots, X_n) := X_{a_i} \cdot X_{b_i} \in \mathbb{Z}_p[X_1, \dots, X_n].$$

Then, $\mathsf{Setup_{Pre}}'$ 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 $\mathsf{Setup_{Pre}}'$, we can now define the partial SKE $\mathsf{SKE}' = (\mathsf{Setup}', \mathsf{Enc}', \_)$ as in Definition 11. To prove Theorem 5, 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 prove necessary algebraic properties of FE in Lemmas 5 to 7:

Lemma 5. *Let* $\mathsf{msk}' = (\mathsf{msk}, \mathsf{sk}_1, \ldots, \mathsf{sk}_Q, \nu, i_*)$ *be a master secret key outputted by* Setup'. *Then, there exists a polynomial* $h_{\mathsf{msk}} \in \mathbb{Z}_q[T_1, \ldots, T_Q]$ *with the following properties:*

$$\begin{aligned} &h_{\mathsf{msk}} \neq 0 \in \mathbb{Z}_q[T_1, \ldots, T_Q], \\ &h_{\mathsf{msk}}(\mathsf{sk}_1, \ldots, \mathsf{sk}_Q) = 0 \in \mathbb{Z}_q[Y_1, \ldots, Y_m], \\ &\deg h_{\mathsf{msk}} \leq (m+1) \cdot d_2^m = M/2. \end{aligned}$$

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 $B := \{g \in \mathbb{Z}_q[Y_1, \ldots, Y_m] \mid \deg g \leq (m+1) \cdot d_2^{m+1}\}$ 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 existence of an algebraic dependence h_{msk} of $\mathsf{sk}_1, \ldots, \mathsf{sk}_Q$, we will follow the idea of [Üna23] and use Lemma 3. 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

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

We have that the last term is at least 1 according to Lemma 3. □

As explained in Remark 1, we assume – without loss of generality – that KeyGen is deterministic. Hence, h_{msk} only depends on msk outputted by Setup. In particular, there is a deterministic mapping that assigns to each master secret key msk of FE a polynomial h_{msk} with the properties in Lemma 5.

Note that $h_{\mathsf{msk}}(\mathsf{sk}_1(Y), \ldots, \mathsf{sk}_m(Y))$ is the zero polynomial of $\mathbb{Z}_q[Y_1, \ldots, Y_m]$ and that it will vanish on each ciphertext of FE. If we choose h_{msk} of minimal degree, we know that $h_{\mathsf{msk}}(\mathsf{sk}_1(Y), \ldots, \mathsf{sk}_{m-1}(Y), T_m) \in \mathbb{Z}_q[Y_1, \ldots, Y_m, T_m]$ cannot be zero. However, it may happen that $h_{\mathsf{msk}}(\mathsf{sk}_1(Y), \ldots, \mathsf{sk}_{m-1}(Y), T_m)$ vanishes on all or almost all ciphertexts of FE. For our decryption algorithm Dec' it will be important that we have

$$\Pr_{\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{msk}, x)} [h_{\mathsf{msk}}(\mathsf{sk}_1(\mathsf{ct}), \ldots, \mathsf{sk}_{i_*}(\mathsf{ct}), T_{i_*+1}, \ldots, T_m) = 0] \in 1 - \mathsf{negl}(\lambda), \tag{11}$$

$$\Pr_{\mathsf{ct}\leftarrow\mathsf{Enc}(\mathsf{msk},x)}\left[h_{\mathsf{msk}}(\mathsf{sk}_1(\mathsf{ct}),\dots,\mathsf{sk}_{i_*-1}(\mathsf{ct}),T_{i_*},\dots,T_m)\neq 0\right]\notin\mathsf{negl}(\lambda). \tag{12}$$

Because, if there is a ciphertext $\mathsf{ct}\in\mathbb{Z}_q^m$ s.t. $h_{\mathsf{msk}}(\mathsf{sk}_1(\mathsf{ct}),\dots,\mathsf{sk}_{i_*}(\mathsf{ct}),T_{i_*+1},\dots,T_m)=0$, but $h_{\mathsf{msk}}(\mathsf{sk}_1(\mathsf{ct}),\dots,\mathsf{sk}_{i_*-1}(\mathsf{ct}),T_{i_*},\dots,T_m)\neq 0$, then $\mathsf{sk}_{i_*}(\mathsf{ct})$ is a root of the polynomial $h_{\mathsf{msk}}(\mathsf{sk}_1(\mathsf{ct}),\dots,\mathsf{sk}_{i_*-1}(\mathsf{ct}),T_{i_*},T_{i_*+1}\dots,T_m)$, which we consider as a univariate polynomial with coefficients in $\mathbb{Z}_q[T_{i_*+1},\dots,T_m]$ and unknown T_{i_*}. Since this polynomial is non-zero, it has at most $\deg h_{\mathsf{msk}}\leq M/2$ different roots. In such cases Dec' can limit the number of potential values for $f_{i_*}(x)$ to $M/2$, which gives Dec' a non-negligible advantage at decryption. In the next two lemmas, we will show that the inequalities Equation (11) and (12) will hold in a non-negligible number of cases.

Lemma 6. *For $i\in\{0,\dots,Q\}$, define*

$$p_i(0):=\Pr_{\substack{\mathsf{msk}'\leftarrow\mathsf{Setup}'(1^\lambda)\\ \mathsf{ct}\leftarrow\mathsf{Enc}(\mathsf{msk},0)}}\left[h_{\mathsf{msk}}(\mathsf{sk}_1(\mathsf{ct}),\dots,\mathsf{sk}_i(\mathsf{ct}),T_{i+1},\dots,T_Q)=0\right].$$

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

$$\begin{aligned} p_{i_\dagger}(0)&\geq 1-\varepsilon',\\ \exists_\infty\lambda\in\mathbb{N}:\ \ p_{i_\dagger}(0)-p_{i_\dagger-1}(0)&\geq\frac{1}{r'(\lambda)}.\end{aligned}$$

Proof. Note that $0=p_0(0)\leq p_1(0)\leq\ldots\leq p_Q(0)=1$. Now, let $i_\dagger\in[Q]$ be maximal s.t. there is an $r'\in\mathsf{poly}(\lambda), r'>0$, with

$$\exists_\infty\lambda\in\mathbb{N}:\ \ p_{i_\dagger}(0)-p_{i_\dagger-1}(0)\geq\frac{1}{r'(\lambda)}.$$

Since Q is constant, such an $i_\dagger$ must exist. Since $i_\dagger$ is maximal, we have for $i>i_\dagger$

$$p_i(0)-p_{i-1}(0)\in\mathsf{negl}(\lambda).$$

In particular, $1-p_{i_\dagger}(0)=p_Q(0)-p_{Q-1}(0)+p_{Q-1}(0)-p_{Q-2}(0)+\ldots+p_{i_\dagger+1}(0)-p_{i_\dagger}(0)\geq 1-\mathsf{negl}(\lambda)$. □

Lemma 7. *Let $\widetilde{\mathcal{X}}\subset\mathcal{X}$ be a constant subspace. For $y\in\widetilde{\mathcal{X}}$, $i\in\{0,\dots,Q\}$, set*

$$p_i(y):=\Pr_{\substack{\mathsf{msk}'\leftarrow\mathsf{Setup}'(1^\lambda)\\ \mathsf{ct}\leftarrow\mathsf{Enc}(\mathsf{msk},y)}}\left[h_{\mathsf{msk}}(\mathsf{sk}_1(\mathsf{ct}),\dots,\mathsf{sk}_i(\mathsf{ct}),T_{i+1},\dots,T_Q)=0\right].$$

Then, for each $\ell\in\mathsf{poly}(\lambda)$, there is a function $\varepsilon_\ell\in\mathsf{negl}(\lambda)$ s.t. we have for each $i\in\{0,\dots,Q\}$ and each pair $y,z\in\widetilde{\mathcal{X}}$

$$p_i(z)\geq\ell\cdot p_i(y)-(\ell-1)-\frac{1}{\ell+1}\binom{m+d_2D}{m}-\varepsilon_\ell.$$

In particular, if $p_i(y)\geq 1-\varepsilon'$ for some $\varepsilon'\in\mathsf{negl}(\lambda)$, then there is one $\varepsilon\in\mathsf{negl}(\lambda)$ s.t. $p_i(z)\geq 1-\varepsilon$ for all $z\in\widetilde{\mathcal{X}}$.

Proof. Let $D=(m+1)\cdot d_2^m$ be the upper bound of the degree of h_{msk} from Lemma 5. Set $t:=\binom{m+d_2D}{m}\in O(1)$ and let $y,z\in\widetilde{\mathcal{X}}$.

Let $\ell\in\mathsf{poly}(\lambda)$, we prove the statement by constructing a PPT adversary $\mathcal{A}$ against the selective IND-CPA security of FE:

1. $\mathcal{A}$ defines two lists $(x_i^0)_{i=1,\dots,\ell+1}$ and $(x_i^1)_{i=1,\dots,\ell+1}$ by

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

2. $\mathcal{A}$ submits both lists to $\mathcal{C}$ and receives a list of ciphertexts $\mathsf{ct}_1, \ldots, \mathsf{ct}_\ell$ of y and $\mathsf{ct}_{\ell+1}$ of $x^b_{\ell+1}$ for unknown $b \in \{0, 1\}$.
3. Let $\psi_D \colon \mathbb{Z}_q^m \to \mathbb{Z}_q^t$ be the map from Lemma 2. $\mathcal{A}$ computes

$$V := \operatorname{span}_{\mathbb{Z}_q} \{\psi_D(\mathsf{ct}_1), \ldots, \psi_D(\mathsf{ct}_\ell)\} \subseteq \mathbb{Z}_q^t .$$

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

Since FE is IND-CPA secure, the advantage of $\mathcal{A}$ can be bounded by

$$\begin{aligned} &\left| \Pr_{\mathsf{ct}_y \leftarrow \mathsf{Enc}(\mathsf{msk}, y)} [\psi_D(\mathsf{ct}_y) \in V] + \Pr_{\mathsf{ct}_z \leftarrow \mathsf{Enc}(\mathsf{msk}, z)} [\psi_D(\mathsf{ct}_z) \notin V] - 1 \right| \\ = &\left| \Pr_{\mathsf{ct}_y \leftarrow \mathsf{Enc}(\mathsf{msk}, y)} [\psi_D(\mathsf{ct}_y) \in V] - \Pr_{\mathsf{ct}_z \leftarrow \mathsf{Enc}(\mathsf{msk}, z)} [\psi_D(\mathsf{ct}_z) \in V] \right| \le \varepsilon_\ell(\lambda) \end{aligned}$$

for some $\varepsilon_\ell \in \mathsf{negl}(\lambda)$. Because of Lemma 1, we have

$$\Pr_{\mathsf{ct}_y \leftarrow \mathsf{Enc}(\mathsf{msk}, y)} [\psi_D(\mathsf{ct}_y) \in V] \ge 1 - \frac{t}{\ell + 1}.$$

Hence, we get

$$\Pr_{\mathsf{ct}_z \leftarrow \mathsf{Enc}(\mathsf{msk}, z)} [\psi_D(\mathsf{ct}) \in V] \ge 1 - \frac{t}{\ell + 1} - \varepsilon_\ell(\lambda). \tag{13}$$

Fix a master secret key $\mathsf{msk} \leftarrow \mathsf{Setup}(1^\lambda)$ and define for $i \in [Q]$ the polynomial

$$h_i(Y_1, \ldots, Y_m) := h_{\mathsf{msk}}(\mathsf{sk}_1(Y_1, \ldots, Y_m), \ldots, \mathsf{sk}_i(Y_1, \ldots, Y_m), T_{i+1}, \ldots, T_Q)$$

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 $\deg \mathsf{sk}_i \cdot \deg h_{\mathsf{msk}} \le d_2 \cdot D$.

For $\mathsf{ct}_{\ell+1} \leftarrow \mathsf{Enc}(\mathsf{msk}, z)$, we have according to Lemma 2 the following implication of events in the IND-CPA game between $\mathcal{A}$ and challenger $\mathcal{C}$:

$$\begin{aligned} &\psi_D(\mathsf{ct}_{\ell+1}) \in \operatorname{span}_{\mathbb{Z}_q} \{\psi_D(\mathsf{ct}_1), \ldots, \psi_D(\mathsf{ct}_\ell)\}, h_i(\mathsf{ct}_1) = \ldots = h_i(\mathsf{ct}_\ell) = 0 \\ &\implies h_i(\mathsf{ct}_{\ell+1}) = 0. \end{aligned}$$

For a fixed msk and $i \in [Q]$, we therefore have the following inequalities:

$$\begin{aligned} &\Pr_{\mathsf{ct}_z \leftarrow \mathsf{Enc}(\mathsf{msk}, z)} [h_i(\mathsf{ct}_z) = 0] \\ \ge &\Pr_{\substack{\mathsf{ct}_z \leftarrow \mathsf{Enc}(\mathsf{msk}, z) \\ \mathsf{ct}_1, \ldots, \mathsf{ct}_\ell \leftarrow \mathsf{Enc}(\mathsf{msk}, y)}} \begin{bmatrix} \psi_D(\mathsf{ct}_z) \in \operatorname{span}_{\mathbb{Z}_q} \{\psi_D(\mathsf{ct}_1), \ldots, \psi_D(\mathsf{ct}_\ell)\} \\ h_i(\mathsf{ct}_1) = \ldots = h_i(\mathsf{ct}_\ell) = 0 \end{bmatrix} \\ \ge &\Pr_{\substack{\mathsf{ct}_z \leftarrow \mathsf{Enc}(\mathsf{msk}, z) \\ \mathsf{ct}_1, \ldots, \mathsf{ct}_\ell \leftarrow \mathsf{Enc}(\mathsf{msk}, y)}} \left[\psi_D(\mathsf{ct}_z) \in \operatorname{span}_{\mathbb{Z}_q} \{\psi_D(\mathsf{ct}_1), \ldots, \psi_D(\mathsf{ct}_\ell)\}\right] \\ &+ \Pr_{\mathsf{ct}_1, \ldots, \mathsf{ct}_\ell \leftarrow \mathsf{Enc}(\mathsf{msk}, y)} [h_i(\mathsf{ct}_1) = \ldots = h_i(\mathsf{ct}_\ell) = 0] - 1 \\ \ge &\Pr_{\substack{\mathsf{ct}_z \leftarrow \mathsf{Enc}(\mathsf{msk}, z) \\ \mathsf{ct}_1, \ldots, \mathsf{ct}_\ell \leftarrow \mathsf{Enc}(\mathsf{msk}, y)}} \left[\psi_D(\mathsf{ct}_z) \in \operatorname{span}_{\mathbb{Z}_q} \{\psi_D(\mathsf{ct}_1), \ldots, \psi_D(\mathsf{ct}_\ell)\}\right] \\ &+ \ell \cdot \Pr_{\mathsf{ct}_y \leftarrow \mathsf{Enc}(\mathsf{msk}, y)} [h_i(\mathsf{ct}_y) = 0] - \ell. \end{aligned} \tag{14}$$

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

$$
\begin{aligned}
&\Pr_{\substack{\mathsf{msk}\leftarrow\mathsf{Setup}(1^\lambda)\\ \mathsf{ct}_z\leftarrow\mathsf{Enc}(\mathsf{msk},z)}}[h_i(\mathsf{ct}_z)=0]\\
\overset{Eq.\ (14)}{\geq}\ &\Pr_{\substack{\mathsf{msk}\leftarrow\mathsf{Setup}(1^\lambda)\\ \mathsf{ct}_z\leftarrow\mathsf{Enc}(\mathsf{msk},z)\\ \mathsf{ct}_1,\ldots,\mathsf{ct}_\ell\leftarrow\mathsf{Enc}(\mathsf{msk},y)}}\left[\psi_D(\mathsf{ct}_z)\in\operatorname{span}_{\mathbb{Z}_q}\{\psi_D(\mathsf{ct}_1),\ldots,\psi_D(\mathsf{ct}_\ell)\}\right]\\
&+\ell\cdot\Pr_{\substack{\mathsf{msk}\leftarrow\mathsf{Setup}(1^\lambda)\\ \mathsf{ct}_y\leftarrow\mathsf{Enc}(\mathsf{msk},y)}}[h_i(\mathsf{ct}_y)=0]-\ell.\\
\overset{Eq.\ (13)}{\geq}\ &\left(1-\frac{t}{\ell+1}-\varepsilon_\ell\right)+\ell\cdot\Pr_{\substack{\mathsf{msk}\leftarrow\mathsf{Setup}(1^\lambda)\\ \mathsf{ct}_y\leftarrow\mathsf{Enc}(\mathsf{msk},y)}}[h_i(\mathsf{ct}_y)=0]-\ell\\
\geq\ &\ell\cdot\Pr_{\substack{\mathsf{msk}\leftarrow\mathsf{Setup}(1^\lambda)\\ \mathsf{ct}_y\leftarrow\mathsf{Enc}(\mathsf{msk},y)}}[h_i(\mathsf{ct}_y)=0]-(\ell-1)-\frac{t}{\ell+1}-\varepsilon_\ell.
\end{aligned}
$$

□

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

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

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

First, we sketch the strategy of Dec'. To 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 let $\mathsf{ct}\leftarrow\mathsf{Enc}(\mathsf{msk},\nu(x'))$. 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' computes $i_\dagger\in[Q]$ from Lemma 6. If $i_\dagger\neq i_*$, Dec' outputs a uniformly random element of $\mathcal{X}'=\{0,\ldots,M\}$ and stops.
2. Dec' computes the set
$$A(\mathsf{msk}'):=\left\{w\in\mathbb{Z}_q^m\ \mid h_{\mathsf{msk}}(\mathsf{sk}_1(w),\ldots,\mathsf{sk}_{i_*}(w),T_{i_*+1},\ldots,T_Q)=0\right\}.$$
The original ciphertext ct of $\mathsf{Enc}(\mathsf{msk},\nu(x'))$ lies in $A(\mathsf{msk}')$ with overwhelming probability $1-\varepsilon$. However, since Dec' does not know ct, it cannot check if ct lies in $A(\mathsf{msk}')$. However, Dec assumes from here on that ct lies in $A(\mathsf{msk}')$.
3. Dec' computes the subset
$$B(\mathsf{msk}'):=\left\{w\in A(\mathsf{msk}')\mid h_{\mathsf{msk}}(\mathsf{sk}_1(w),\ldots,\mathsf{sk}_{i_*-1}(w),T_{i_*},\ldots,T_Q)\neq 0\right\}.$$
ct lies with non-negligible probability ρ 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.

4. At this point, Dec' knows that ct lies in $B(\mathsf{msk}')$ and can compute the set

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

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 $\deg h_{\mathsf{msk}} \leq M/2$ different values. Dec' chooses a uniformly random value $\mathsf{sk}_{i_*}(w)$ from $S(\mathsf{msk}', \mathsf{ct}')$ and outputs

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

Let y' be the value outputted by $\mathsf{Dec}'(\mathsf{msk}', \mathsf{ct}')$. We can lower-bound the probability of Dec' to return the correct message x' as follows:

$$\begin{aligned}
&\Pr[y' = x'] \\
\geq\ & \frac{1}{Q} \cdot \Pr[y' = x' \mid i_* = i_\dagger] + \frac{Q-1}{Q} \Pr[y' = x' \mid i_* \neq i_\dagger] \\
=\ & \frac{1}{Q} \cdot \Pr[y' = x' \mid i_* = i_\dagger] + \frac{Q-1}{Q} \cdot \frac{1}{M+1} \\
\geq\ & \frac{1}{Q} \cdot (1-\varepsilon) \cdot \Pr\left[y' = x' \mid i_* = i_\dagger, \mathsf{ct} \in A(\mathsf{msk}')\right] + \frac{Q-1}{Q} \cdot \frac{1}{M+1} \\
\geq\ & \frac{1}{Q} \cdot \Pr\left[y' = x' \mid i_* = i_\dagger, \mathsf{ct} \in A(\mathsf{msk}')\right] + \frac{Q-1}{Q} \cdot \frac{1}{M+1} - \varepsilon \\
\geq\ & \frac{1}{Q} \cdot \rho \cdot \Pr\left[y' = x' \mid i_* = i_\dagger, \mathsf{ct} \in B(\mathsf{msk}')\right] \\
&+ \frac{1}{Q} \cdot (1-\rho) \cdot \Pr\left[y' = x' \mid i_* = i_\dagger, \mathsf{ct} \in A(\mathsf{msk}') \setminus B(\mathsf{msk}')\right] \\
&+ \frac{Q-1}{Q} \cdot \frac{1}{M+1} - \varepsilon \\
\geq\ & \frac{\rho}{Q} \cdot \Pr\left[y' = x' \mid i_* = i_\dagger, \mathsf{ct} \in B(\mathsf{msk}')\right] \\
&+ \frac{1-\rho}{Q(M+1)} + \frac{Q-1}{Q} \cdot \frac{1}{M+1} - \varepsilon \\
\geq\ & \frac{\rho}{Q} \cdot \frac{2}{M} + \frac{1-\rho}{Q(M+1)} + \frac{Q-1}{Q} \cdot \frac{1}{M+1} - \varepsilon \\
\geq\ & \frac{\rho}{Q \cdot M} + \frac{1}{M+1} - \varepsilon.
\end{aligned}$$

This yields a contradiction with the statement of Corollary 1.

Next, we give the details of Dec'. To this end, set $\widetilde{\mathcal{X}} := \{0, \ldots, M\}^n \subset \mathcal{X}$. Note that $\widetilde{\mathcal{X}}$ is constant, since M and n are constant. For $x \in \widetilde{\mathcal{X}}$ and $i \in [Q]$, $p_i(x)$ is given by

$$p_i(x) = \Pr_{\substack{\mathsf{msk}' \leftarrow \mathsf{Setup}'(1^\lambda) \\ \mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{msk}, x)}} \left[h_{\mathsf{msk}}(\mathsf{sk}_1(\mathsf{ct}), \ldots, \mathsf{sk}_i(\mathsf{ct}), T_{i+1}, \ldots, T_Q) = 0 \right].$$

Let $i_\dagger \in [Q]$ be the index from Lemma 6, i.e., there is an $\varepsilon' \in \mathsf{negl}(\lambda)$, an $r' \in \mathsf{poly}(\lambda)$, $r' > 0$ and an infinite set $\Lambda \subseteq \mathbb{N}$ s.t.

$$\begin{aligned}
p_{i_\dagger}(0) &\geq 1 - \varepsilon' \\
\forall \lambda \in \Lambda \colon \ p_{i_\dagger}(0) - p_{i_\dagger - 1}(0) &\geq \frac{1}{r'(\lambda)}.
\end{aligned}$$

According to Lemma 7, there is an $\varepsilon \in \mathsf{negl}(\lambda)$ and $r \in \mathsf{poly}(\lambda), r > 0$, s.t. we have for all $x \in \widetilde{\mathcal{X}}$

$$p_{i_\dagger}(x) \geq 1 - \varepsilon \tag{15}$$

$$\forall \lambda \in \Lambda\colon \quad p_{i_\dagger}(x) - p_{i_\dagger - 1}(x) \geq \frac{1}{r(\lambda)}. \tag{16}$$

For $\lambda \in \mathbb{N}$, we define the non-negligible function

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

When we sample $\mathsf{msk}' = (\mathsf{msk}, \mathsf{sk}_1, \dots, \mathsf{sk}_Q, \nu, i_*) \leftarrow \mathsf{Setup}'(1^\lambda)$, we have $i_* = i_\dagger$ with probability $\frac{1}{Q}$. In the following, we assume that $i_* = i_\dagger$.

For a fixed message $x' \in \mathcal{X}'$, let $\mathsf{ct}' \leftarrow \mathsf{Enc}'(\mathsf{msk}', x')$. ct' is given as $(\mathsf{sk}_1(\mathsf{ct}), \dots, \mathsf{sk}_{i_*-1}(\mathsf{ct}), 0, \mathsf{sk}_{i_*+1}(\mathsf{ct}), \dots, \mathsf{sk}_Q(\mathsf{ct}))$ for some $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{msk}, \nu(x))$. Because of Equation (15), ct lies in $A(\mathsf{msk}') = \{w \mid h_{\mathsf{msk}}(\mathsf{sk}_1(w), \dots, \mathsf{sk}_{i_*}(w), T_{i_*+1}, \dots, T_Q) = 0\}$ with probability $1 - \varepsilon$. However, Dec' cannot verify this, since it does not know $\mathsf{sk}_{i_*}(\mathsf{ct})$. Under the assumption $\mathsf{ct} \in A(\mathsf{msk}')$, Dec' can check if ct is contained in $B(\mathsf{msk}') = \{w \in A(\mathsf{msk}') \mid h_{\mathsf{msk}}(\mathsf{sk}_1(w), \dots, \mathsf{sk}_{i_*-1}(w), T_{i_*}, \dots, T_Q) \neq 0\}$, since Dec' does not need to know $\mathsf{sk}_{i_*}(w)$ for this. Because of Equation (16), we know that ct must lie in $B(\mathsf{msk}')$ with probability $\geq \rho$. We claim that in the case $\mathsf{ct} \in B(\mathsf{msk}')$ the set $S(\mathsf{msk}', \mathsf{ct}') = \{\mathsf{sk}_{i_*}(w) \mid w \in B(\mathsf{msk}'), \forall i \neq i_* : \mathsf{sk}_i(w) = c_i\}$ cannot contain more than $\deg h_{\mathsf{msk}'} \leq M/2$ elements. In fact, set

$$g(T_{i_*}) = h_{\mathsf{msk}'}(\mathsf{sk}_1(\mathsf{ct}), \dots, \mathsf{sk}_{i_*-1}(\mathsf{ct}), T_{i_*}, \dots, T_m) \in \mathbb{Z}_q[T_{i_*+1}, \dots, T_m][T_{i_*}].$$

We consider g as a univariate polynomial with coefficients in $Z_q[T_{i_*+1}, \dots, T_m]$. 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 $\deg g \leq \deg h_{\mathsf{msk}'} \leq M/2$ elements. Since $x' \in \mathcal{X}'$ was chosen arbitrary, the non-negligible advantage of Dec' at decryption follows. □

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

References

AAB17. Benny Applebaum, Jonathan Avron, and Chris Brzuska. Arithmetic cryptography. *J. ACM*, 64(2), apr 2017.

ABB10. Shweta Agrawal, Dan Boneh, and Xavier Boyen. Efficient lattice (H)IBE in the standard model. In Henri Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 553–572. Springer, Heidelberg, May / June 2010.

ABDP15. Michel Abdalla, Florian Bourse, Angelo De Caro, and David Pointcheval. Simple functional encryption schemes for inner products. In Jonathan Katz, editor, *PKC 2015*, volume 9020 of *LNCS*, pages 733–751. Springer, Heidelberg, March / April 2015.

ABG19. Michel Abdalla, Fabrice Benhamouda, and Romain Gay. From single-input to multi-client inner-product functional encryption. In Steven D. Galbraith and Shiho Moriai, editors, *ASIACRYPT 2019, Part III*, volume 11923 of *LNCS*, pages 552–582. Springer, Heidelberg, December 2019.

ABKW19. Michel Abdalla, Fabrice Benhamouda, Markulf Kohlweiss, and Hendrik Waldner. Decentralizing inner-product functional encryption. In Dongdai Lin and Kazue Sako, editors, *PKC 2019, Part II*, volume 11443 of *LNCS*, pages 128–157. Springer, Heidelberg, April 2019.

ACF^{+}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 Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO 2018, Part I*, volume 10991 of *LNCS*, pages 597–627. Springer, Heidelberg, August 2018.

ACGU20. Michel Abdalla, Dario Catalano, Romain Gay, and Bogdan Ursu. Inner-product functional encryption with fine-grained access control. In Shiho Moriai and Huaxiong Wang, editors, *ASIACRYPT 2020, Part III*, volume 12493 of *LNCS*, pages 467–497. Springer, Heidelberg, December 2020.

Agr19. Shweta Agrawal. Indistinguishability obfuscation without multilinear maps: New methods for bootstrapping and instantiation. In Yuval Ishai and Vincent Rijmen, editors, *EUROCRYPT 2019, Part I*, volume 11476 of *LNCS*, pages 191–225. Springer, Heidelberg, May 2019.

AGRW17. Michel Abdalla, Romain Gay, Mariana Raykova, and Hoeteck Wee. Multi-input inner-product functional encryption from pairings. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *EUROCRYPT 2017, Part I*, volume 10210 of *LNCS*, pages 601–626. Springer, Heidelberg, April / May 2017.

AGT21a. Shweta Agrawal, Rishab Goyal, and Junichi Tomida. Multi-input quadratic functional encryption from pairings. In Tal Malkin and Chris Peikert, editors, *CRYPTO 2021, Part IV*, volume 12828 of *LNCS*, pages 208–238, Virtual Event, August 2021. Springer, Heidelberg.

AGT21b. Shweta Agrawal, Rishab Goyal, and Junichi Tomida. Multi-party functional encryption. In Kobbi Nissim and Brent Waters, editors, *TCC 2021, Part II*, volume 13043 of *LNCS*, pages 224–255. Springer, Heidelberg, November 2021.

AGT22. Shweta Agrawal, Rishab Goyal, and Junichi Tomida. Multi-input quadratic functional encryption: Stronger security, broader functionality. In Eike Kiltz and Vinod Vaikuntanathan, editors, *TCC 2022, Part I*, volume 13747 of *LNCS*, pages 711–740. Springer, Heidelberg, November 2022.

AGVW13. Shweta Agrawal, Sergey Gorbunov, Vinod Vaikuntanathan, and Hoeteck Wee. Functional encryption: New perspectives and lower bounds. In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part II*, volume 8043 of *LNCS*, pages 500–518. Springer, Heidelberg, August 2013.

AGW20. Michel Abdalla, Junqing Gong, and Hoeteck Wee. Functional encryption for attribute-weighted sums from k-Lin. In Daniele Micciancio and Thomas Ristenpart, editors, *CRYPTO 2020, Part I*, volume 12170 of *LNCS*, pages 685–716. Springer, Heidelberg, August 2020.

AJ15. Prabhanjan Ananth and Abhishek Jain. Indistinguishability obfuscation from compact functional encryption. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part I*, volume 9215 of *LNCS*, pages 308–326. Springer, Heidelberg, August 2015.

AJS15. Prabhanjan Ananth, Abhishek Jain, and Amit Sahai. Indistinguishability obfuscation from functional encryption for simple functions. Cryptology ePrint Archive, Report 2015/730, 2015. https://eprint.iacr.org/2015/730.

ALMT20. Shweta Agrawal, Benoît Libert, Monosij Maitra, and Radu Titiu. Adaptive simulation security for inner product functional encryption. In Aggelos Kiayias, Markulf Kohlweiss, Petros Wallden, and Vassilis Zikas, editors, *PKC 2020, Part I*, volume 12110 of *LNCS*, pages 34–64. Springer, Heidelberg, May 2020.

ALS16. Shweta Agrawal, Benoît Libert, and Damien Stehlé. Fully secure functional encryption for inner products, from standard assumptions. In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO 2016, Part III*, volume 9816 of *LNCS*, pages 333–362. Springer, Heidelberg, August 2016.

AP20. Shweta Agrawal and Alice Pellet-Mary. Indistinguishability obfuscation without maps: Attacks and fixes for noisy linear FE. In Anne Canteaut and Yuval Ishai, editors, *EUROCRYPT 2020, Part I*, volume 12105 of *LNCS*, pages 110–140. Springer, Heidelberg, May 2020.

AR17. Shweta Agrawal and Alon Rosen. Functional encryption for bounded collusions, revisited. In Yael Kalai and Leonid Reyzin, editors, *TCC 2017, Part I*, volume 10677 of *LNCS*, pages 173–205. Springer, Heidelberg, November 2017.

AS17. Prabhanjan Ananth and Amit Sahai. Projective arithmetic functional encryption and indistinguishability obfuscation from degree-5 multilinear maps. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *EUROCRYPT 2017, Part I*, volume 10210 of *LNCS*, pages 152–181. Springer, Heidelberg, April / May 2017.

AV19. Prabhanjan Ananth and Vinod Vaikuntanathan. Optimal bounded-collusion secure functional encryption. In Dennis Hofheinz and Alon Rosen, editors, *TCC 2019, Part I*, volume 11891 of *LNCS*, pages 174–198. Springer, Heidelberg, December 2019.

BCFG17. Carmen Elisabetta Zaira Baltico, Dario Catalano, Dario Fiore, and Romain Gay. Practical functional encryption for quadratic functions with applications to predicate encryption. In Jonathan Katz and Hovav Shacham, editors, *CRYPTO 2017, Part I*, volume 10401 of *LNCS*, pages 67–98. Springer, Heidelberg, August 2017.

BDGM19. Zvika Brakerski, Nico Döttling, Sanjam Garg, and Giulio Malavolta. Leveraging linear decryption: Rate-1 fully-homomorphic encryption and time-lock puzzles. In Dennis Hofheinz and Alon Rosen, editors, *TCC 2019, Part II*, volume 11892 of *LNCS*, pages 407–437. Springer, Heidelberg, December 2019.

BGG$^+$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 Phong Q. Nguyen and Elisabeth Oswald, editors, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 533–556. Springer, Heidelberg, May 2014.

BJK15. Allison Bishop, Abhishek Jain, and Lucas Kowalczyk. Function-hiding inner product encryption. In Tetsu Iwata and Jung Hee Cheon, editors, *ASIACRYPT 2015, Part I*, volume 9452 of *LNCS*, pages 470–491. Springer, Heidelberg, November / December 2015.

BPR12. Abhishek Banerjee, Chris Peikert, and Alon Rosen. Pseudorandom functions and lattices. In David Pointcheval and Thomas Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 719–737. Springer, Heidelberg, April 2012.

BR93. Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In Dorothy E. Denning, Raymond Pyle, Ravi Ganesan, Ravi S. Sandhu, and Victoria Ashby, editors, *CCS '93, Proceedings of the 1st ACM Conference on Computer and Communications Security, Fairfax, Virginia, USA, November 3-5, 1993*, pages 62–73. ACM, 1993.

BSW11. Dan Boneh, Amit Sahai, and Brent Waters. Functional encryption: Definitions and challenges. In Yuval Ishai, editor, *TCC 2011*, volume 6597 of *LNCS*, pages 253–273. Springer, Heidelberg, March 2011.

BV15. Nir Bitansky and Vinod Vaikuntanathan. Indistinguishability obfuscation from functional encryption. In Venkatesan Guruswami, editor, *56th FOCS*, pages 171–190. IEEE Computer Society Press, October 2015.

CDG$^+$18. Jérémy Chotard, Edouard Dufour Sans, Romain Gay, Duong Hieu Phan, and David Pointcheval. Decentralized multi-client functional encryption for inner product. In Thomas Peyrin and Steven Galbraith, editors, *ASIACRYPT 2018, Part II*, volume 11273 of *LNCS*, pages 703–732. Springer, Heidelberg, December 2018.

CRS$^+$22. Valerio Cini, Sebastian Ramacher, Daniel Slamanig, Christoph Striecks, and Erkan Tairi. (Inner-product) functional encryption with updatable ciphertexts. Cryptology ePrint Archive, Report 2022/1284, 2022. https://eprint.iacr.org/2022/1284.

CVW$^+$18. Yilei Chen, Vinod Vaikuntanathan, Brent Waters, Hoeteck Wee, and Daniel Wichs. Traitor-tracing from LWE made simple and attribute-based. In Amos Beimel and Stefan Dziembowski, editors, *TCC 2018, Part II*, volume 11240 of *LNCS*, pages 341–369. Springer, Heidelberg, November 2018.

DIJ$^+$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 Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part II*, volume 8043 of *LNCS*, pages 519–535. Springer, Heidelberg, August 2013.

FKL18. Georg Fuchsbauer, Eike Kiltz, and Julian Loss. The algebraic group model and its applications. In Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO 2018, Part II*, volume 10992 of *LNCS*, pages 33–62. Springer, Heidelberg, August 2018.

Gay20. Romain Gay. A new paradigm for public-key functional encryption for degree-2 polynomials. In Aggelos Kiayias, Markulf Kohlweiss, Petros Wallden, and Vassilis Zikas, editors, *PKC 2020, Part I*, volume 12110 of *LNCS*, pages 95–120. Springer, Heidelberg, May 2020.

GGH$^+$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*, pages 40–49. IEEE Computer Society Press, October 2013.

GVW13. Sergey Gorbunov, Vinod Vaikuntanathan, and Hoeteck Wee. Attribute-based encryption for circuits. In Dan Boneh, Tim Roughgarden, and Joan Feigenbaum, editors, *45th ACM STOC*, pages 545–554. ACM Press, June 2013.

GVW15. Sergey Gorbunov, Vinod Vaikuntanathan, and Hoeteck Wee. Predicate encryption for circuits from LWE. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part II*, volume 9216 of *LNCS*, pages 503–523. Springer, Heidelberg, August 2015.

HW14. Susan Hohenberger and Brent Waters. Online/offline attribute-based encryption. In Hugo Krawczyk, editor, *PKC 2014*, volume 8383 of *LNCS*, pages 293–310. Springer, Heidelberg, March 2014.

JLS21. Aayush Jain, Huijia Lin, and Amit Sahai. Indistinguishability obfuscation from well-founded assumptions. In Samir Khuller and Virginia Vassilevska Williams, editors, *53rd ACM STOC*, pages 60–73. ACM Press, June 2021.

JLS22. Aayush Jain, Huijia Lin, and Amit Sahai. Indistinguishability obfuscation from LPN over $\mathbb{F}_p$, DLIN, and PRGs in NC^0. In Orr Dunkelman and Stefan Dziembowski, editors, *EUROCRYPT 2022, Part I*, volume 13275 of *LNCS*, pages 670–699. Springer, Heidelberg, May / June 2022.

KNT18. Fuyuki Kitagawa, Ryo Nishimaki, and Keisuke Tanaka. Obfustopia built on secret-key functional encryption. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018, Part II*, volume 10821 of *LNCS*, pages 603–648. Springer, Heidelberg, April / May 2018.

Lin17. Huijia Lin. Indistinguishability obfuscation from SXDH on 5-linear maps and locality-5 PRGs. In Jonathan Katz and Hovav Shacham, editors, *CRYPTO 2017, Part I*, volume 10401 of *LNCS*, pages 599–629. Springer, Heidelberg, August 2017.

LPR10. Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. In Henri Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 1–23. Springer, Heidelberg, May / June 2010.

LS15. Adeline Langlois and Damien Stehlé. Worst-case to average-case reductions for module lattices. *Des. Codes Cryptogr.*, 75(3):565–599, 2015.

LT17. Huijia Lin and Stefano Tessaro. Indistinguishability obfuscation from trilinear maps and block-wise local PRGs. In Jonathan Katz and Hovav Shacham, editors, *CRYPTO 2017, Part I*, volume 10401 of *LNCS*, pages 630–660. Springer, Heidelberg, August 2017.

LT19. Benoît Libert and Radu Titiu. Multi-client functional encryption for linear functions in the standard model from LWE. In Steven D. Galbraith and Shiho Moriai, editors, *ASIACRYPT 2019, Part III*, volume 11923 of *LNCS*, pages 520–551. Springer, Heidelberg, December 2019.

Mau05. Ueli M. Maurer. Abstract models of computation in cryptography (invited paper). In Nigel P. Smart, editor, *10th IMA International Conference on Cryptography and Coding*, volume 3796 of *LNCS*, pages 1–12. Springer, Heidelberg, December 2005.

O'N10. Adam O'Neill. Definitional issues in functional encryption. Cryptology ePrint Archive, Report 2010/556, 2010. https://eprint.iacr.org/2010/556.

Sho97. Victor Shoup. Lower bounds for discrete logarithms and related problems. In Walter Fumy, editor, *EUROCRYPT'97*, volume 1233 of *LNCS*, pages 256–266. Springer, Heidelberg, May 1997.

Tom19. Junichi Tomida. Tightly secure inner product functional encryption: Multi-input and function-hiding constructions. In Steven D. Galbraith and Shiho Moriai, editors, *ASIACRYPT 2019, Part III*, volume 11923 of *LNCS*, pages 459–488. Springer, Heidelberg, December 2019.

Tom23. Junichi Tomida. Unbounded quadratic functional encryption and more from pairings. In Carmit Hazay and Martijn Stam, editors, *Advances in Cryptology – EUROCRYPT 2023*, pages 543–572, Cham, 2023. Springer Nature Switzerland.

Üna20. Akın Ünal. Impossibility results for lattice-based functional encryption schemes. In Anne Canteaut and Yuval Ishai, editors, *Advances in Cryptology – EUROCRYPT 2020*, pages 169–199, Cham, 2020. Springer International Publishing.

Üna23. Akın Ünal. Worst-case subexponential attacks on prgs of constant degree or constant locality. In Carmit Hazay and Martijn Stam, editors, *Advances in Cryptology – EUROCRYPT 2023*, pages 25–54, Cham, 2023. Springer Nature Switzerland.