From Single-Input to Multi-Input Functional Encryption in the Private-Key Setting

Zvika Brakerski* Ilan Komargodski† Gil Segev‡

Abstract

We construct a general-purpose *multi-input* functional encryption scheme in the private-key setting. Namely, we construct a scheme where a functional key corresponding to a function f enables a user holding encryptions of $x_1, \ldots, x_t$ to compute $f(x_1, \ldots, x_t)$ but nothing else. Our construction assumes any general-purpose private-key *single-input* scheme (without any additional assumptions), and is proven to be *adaptively-secure* for any constant number of inputs t. Moreover, it can be extended to a super-constant number of inputs assuming that the underlying single-input scheme is sub-exponentially secure.

Instantiating our construction with existing single-input schemes, we obtain multi-input schemes that are based on a variety of assumptions (such as indistinguishability obfuscation, multilinear maps, learning with errors, and even one-way functions), offering various trade-offs between security and efficiency.

Previous constructions of multi-input functional encryption schemes either relied on somewhat stronger assumptions and provided weaker security guarantees (Goldwasser et al., EUROCRYPT '14), or relied on multilinear maps and could be proven secure only in an idealized generic model (Boneh et al., EUROCRYPT '15).

Keywords: Private-key encryption, functional encryption, generic constructions, minimal assumptions.

*Department of Computer Science and Applied Mathematics, Weizmann Institute of Science, Rehovot 76100, Israel. Email: zvika.brakerski@weizmann.ac.il. Supported by the Israel Science Foundation (Grant No. 468/14) and by the Alon Young Faculty Fellowship.

†Department of Computer Science and Applied Mathematics, Weizmann Institute of Science, Rehovot 76100, Israel. Email: ilan.komargodski@weizmann.ac.il. Supported in part by a grant from the I-CORE Program of the Planning and Budgeting Committee, the Israel Science Foundation, BSF and the Israeli Ministry of Science and Technology.

‡School of Computer Science and Engineering, Hebrew University of Jerusalem, Jerusalem 91904, Israel. Email: segev@cs.huji.ac.il. Supported by the European Union's Seventh Framework Programme (FP7) via a Marie Curie Career Integration Grant, by the Israel Science Foundation (Grant No. 483/13), and by the Israeli Centers of Research Excellence (I-CORE) Program (Center No. 4/11).

Contents

1 Introduction

The emerging vision of functional encryption [SW08, BSW11, O'N10] extends the traditional "all-or-nothing" view of encryption schemes. Specifically, functional encryption schemes offer tremendous flexibility by supporting restricted decryption keys that allow users to learn specific functions of the encrypted data without learning any additional information. Building upon the early examples of functional encryption schemes for restricted function families (such as identity-based encryption [Sha84, BF03, Coc01]), extensive research is currently devoted to the construction of functional encryption schemes offering a variety of expressive families of functions (see, for example, [SW08, BSW11, O'N10, GVW12, AGV+13, BO13, BCP14, GGH+13, GKP+13, ABS+14, Wat14, GGH+14, BS15, KSY15]).

Until very recently, research on functional encryption has focused on the case of *single-input* functions. In a single-input functional encryption scheme, a functional key sk_f corresponding to a function f enables a user holding an encryption of a value x to compute $f(x)$, while not revealing any additional information on x. In many scenarios, however, dealing only with single-input functions is insufficient, and a more general framework allowing *multi-input* functions is required.

Motivated by a wide range of applications based on mining aggregate information from several different data sources,[1] Goldwasser et al. [GGG+14] recently introduced the notion of a *multi-input* functional encryption scheme. In such a scheme, a functional key corresponding to a t-input function f enables a user holding encryptions of $x_1, \ldots, x_t$ to compute $f(x_1, \ldots, x_t)$ without learning any additional information on the x_i's.

Goldwasser et al. presented a rigorous framework for capturing the security of multi-input schemes in the public-key setting and in the private-key one. In addition, relying on indistinguishability obfuscation and one-way functions [BGI+12, GGH+13, KMN+14], they constructed the first multi-input functional encryption schemes. In terms of functionality, their schemes are extremely expressive, supporting all multi-input functions that are computable by bounded-size circuits. In terms of security, however, their private-key scheme satisfies a weak selective notion, which does not allow the adversary to access an encryption oracle (which is quite crippling in the private-key setting).

Following the work of Goldwasser et al. [GGG+14], a private-key multi-input functional encryption scheme that satisfies a more standard notion of security (one that allows access to an encryption oracle) was constructed by Boneh et al. [BLR+15]. Their scheme is based on multilinear maps, and is proven secure in the idealized generic multilinear map model.

1.1 Our Contributions

In this paper we present a construction of private-key *multi-input* functional encryption from *any* general-purpose private-key *single-input* functional encryption scheme (without introducing any additional assumptions). The resulting scheme supports any set of efficiently-computable functions, and provides adaptive security in the standard model for any constant number of inputs. Assuming that the underlying single-input scheme is sub-exponentially secure, our scheme provides adaptive security in the standard model for a *super-constant* number of inputs (we refer the reader to Section 1.3 for more details). Following [AAB+13, BS15], our scheme provides not only message privacy, but in fact a unified notion that captures both message privacy and function privacy (this notion is known as *full security* – see Section 2.3 for more details).

[1] These include, for example, running SQL queries on encrypted databases, computing over encrypted data streams, non-interactive differentially-private data release, and order-revealing encryption – all of which are relevant in both the public-key setting and the private-key one. We refer the reader to [GGG+14] for a discussion of these applications.

Comparison with existing multi-input schemes. Compared to the private-key scheme of Goldwasser et al. [GGG+14] and to Boneh et al. [BLR+15], our work yields stronger security guarantees and at the same time relies solely on a necessary assumption. Specifically, whereas Goldwasser et al. and Boneh et al. rely on indistinguishability obfuscation and multilinear maps, respectively, we rely on the existence of any general-purpose private-key single-input scheme, which is obviously necessary. In addition, whereas the scheme of Goldwasser et al. provides a selective notion of security which also does not allow adversaries to access an encryption oracle, and the scheme of Boneh et al. is proved secure only in an idealized generic model that does not properly capture real-world adversaries, our scheme provides adaptive security in the standard model.

Instantiations. Instantiating our construction with existing private-key single-input schemes, we obtain multi-input schemes that are based on a variety of assumptions in the standard model. Specifically, we obtain schemes that are secure for an unbounded number of encryption and key-generation queries based on indistinguishability obfuscation or multilinear maps. In addition, if the number of encryption and key-generation queries is a-priori bounded, we can rely on much milder assumptions such as learning with errors [GKP+13] or even the existence of one-way functions or low-depth pseudorandom generators [GVW12]. See Section 2.2 for further discussion.

1.2 Related Work

Extensive research has been devoted to the study of functional encryption, and for concreteness we focus here only on those previous efforts that are directly relevant to the techniques used in this paper.

Function-private functional encryption. The security guarantees of functional encryption typically focus on *message privacy*. Intuitively, message privacy asks that a functional key sk_f does not help in distinguishing encryptions of two messages, m_0 and m_1, as long as $f(m_0) = f(m_1)$. In various cases, however, it is also useful to consider *function privacy* [SSW09, BRS13, AAB+13, BS15], asking that a functional key sk_f does not reveal any unnecessary information on the function f. Specifically, in the private-key setting, function privacy asks that an encryption of a message m does not help in distinguishing two functional keys, sk_{f_0} and sk_{f_1}, as long as $f_0(m) = f_1(m)$. Brakerski and Segev [BS15] recently showed that any private-key functional encryption scheme can be generically transformed into one that satisfies a unified notion of security, referred to as *full security*, which considers both message privacy and function privacy.

Other than being a useful notion for various applications, function privacy was found useful as a building block in the construction of several functional encryption schemes [ABS+14, KSY15]. One of the key insights that we utilize in this work is that function-private functional encryption allows to successfully apply proof techniques "borrowed" from the indistinguishability obfuscation literature (including, for example, a variant of the punctured programming approach of Sahai and Waters [SW14]).

Key-encapsulation techniques in functional encryption. Key encapsulation (also known as "hybrid encryption") is an extremely useful approach in the design of encryption schemes, both for improved efficiency and for improved security. Specifically, key encapsulation typically means that instead of encrypting a message m under a fixed key sk, one can instead sample a random key k, encrypt m under k and then encrypt k under sk. Recently, Ananth et al. [ABS+14] showed that key encapsulation is useful also in the setting of functional encryption. They showed that it can be used to transform any selectively-secure functional encryption scheme into an adaptively-secure one (in both the public-key setting and the private-key one). Their construction and proof technique hint that key encapsulation techniques may in fact be a general tool that is useful in the design of functional encryption schemes. Our constructions incorporate key encapsulation techniques, demonstrating once again their applicability to functional encryption schemes. Specifically, as discussed in Section 1.3, key encapsulation techniques enable us to create "sufficient independence" between combinations of different ciphertexts, a crucial ingredient in our constructions.

1.3 Overview of Our Constructions and Techniques

In this section we provide a high-level overview of our constructions. For concreteness, we focus here mainly on two-input schemes, and then briefly discuss the generalization of our approach to more than two inputs (we refer the reader to Appendix A for the generalization to t-input schemes for $t \geq 2$). In what follows, we start by briefly describing the functionality and security of two-input schemes in the private-key setting. Then, we explain the main ideas underlying our constructions. We emphasize that the forthcoming overview is very high-level and ignores many technical details. For the full details we refer to Sections 3 and 4.

Functionality and security. In a private-key two-input functional encryption scheme, the master secret key msk of the scheme is used for encrypting any messages x and y to the first and second coordinates, respectively, and for generating functional keys for two-input functions. A functional key sk_f corresponding to a function f enables to compute $f(x, y)$ given encryptions of x and y. Building upon the previous notions of security for private-key multi-input functional encryption schemes [GGG+14, BLR+15], we consider a strengthened notion of security that combines both message privacy and function privacy (as in [AAB+13, BS15] for single-input schemes), to which we refer as *full security.*[2] Specifically, we consider *adaptive* adversaries that are given access to "left-or-right" key-generation and encryption oracles. These oracles operate in one out of two modes corresponding to a randomly-chosen bit b. The key-generation oracle receives as input pairs of the form (f_0, f_1) and outputs a functional key for f_b. The encryption oracle receives as input pairs of the form (x_0, x_1) for the first coordinate, or (y_0, y_1) for the second coordinate, and outputs an encryption of x_b or y_b. We require that no efficient adversary can guess the bit b with probability noticeably higher than $1/2$, as long as for each such three queries (f_0, f_1), (x_0, x_1) and (y_0, y_1) it holds that $f_0(x_0, y_0) = f_1(x_1, y_1)$.

Intuition: Input aggregation. Given a two-input function $f(\cdot, \cdot)$, one can view f as a single-input function, f^*, that takes a tuple (x, y), which we denote by $x\|y$ to avoid confusion, and computes $f^*(x\|y) = f(x, y)$. Using a single-input scheme, we can generate a functional key for the function f^*. We thus remain with the problem of *aggregating the input.* That is, we need to be able to encrypt inputs x and y, such that given $\mathsf{Enc}(x)$ and $\mathsf{Enc}(y)$ it is possible to compute $\mathsf{Enc}(x\|y)$. At a very high-level, this is achieved by having the encryption of x be an "aggregator": To encrypt x, we will generate a functional key for the function $\mathsf{AGG}_x(\cdot)$, that on input y outputs an encryption of $x\|y$. There are many technical difficulties in realizing this intuition, as we explain in the remainder of this section.

Step 1: Functional keys as ciphertexts. Given any private-key single-input functional encryption scheme, $\mathsf{1FE}$, the first step in our transformation is to use both its ciphertexts and its functional keys as ciphertexts for a two-input scheme $\mathsf{2FE}$: An encryption of a message x to the first coordinate is a functional key sk_x corresponding to a certain functionality that depends on x, and an encryption of a message y to the second coordinate is simply an encryption of y. Intuitively, the hope is that

[2] We consider a unified notion capturing both message privacy and function privacy not only as a useful feature for various applications. In fact, the function privacy of the resulting two-input scheme plays a crucial role when extending our results to more than two inputs.

the function privacy of $\mathsf{1FE}$ will hide x, and that the message privacy of $\mathsf{1FE}$ will hide y. More specifically, a first attempt towards realizing this intuition is as follows:

1. The master secret key consists of two keys, $\mathsf{msk_{in}}$ and $\mathsf{msk_{out}}$, for the single-input scheme $\mathsf{1FE}$. The key $\mathsf{msk_{in}}$ is used for encryption, and the key $\mathsf{msk_{out}}$ is used to decryption.
2. An encryption of a message x to the first coordinate is a functional key $\mathsf{sk}_{x,\mathsf{msk_{out}}}$ that is generated using $\mathsf{msk_{in}}$ and corresponds to the following functionality: Given an input y, it outputs an encryption $\mathsf{Enc}_{\mathsf{msk_{out}}}(x||y)$ of x concatenated with y under $\mathsf{msk_{out}}$. An encryption of a message y to the second coordinate is simply an encryption $\mathsf{Enc}_{\mathsf{msk_{in}}}(y)$ of y under $\mathsf{msk_{in}}$.
3. A functional key for a two-input function f is a functional key that is generated using $\mathsf{msk_{out}}$ for the function f when viewed as a single-input function.
4. Given a functional key for a function f, and two encryptions $\mathsf{sk}_{x,\mathsf{msk_{out}}}$ and $\mathsf{Enc}_{\mathsf{msk_{in}}}(y)$, we first apply $\mathsf{sk}_{x,\mathsf{msk_{out}}}$ on $\mathsf{Enc}_{\mathsf{msk_{in}}}(y)$ for obtaining $\mathsf{Enc}_{\mathsf{msk_{out}}}(x||y)$, and then apply the functional key for f on $\mathsf{Enc}_{\mathsf{msk_{out}}}(x||y)$.

It is straightforward to verify that the above scheme indeed provides the required functionality of a two-input scheme. Proving its security, however, does not seem to go through: When "attacking" the key $\mathsf{msk_{out}}$, we clearly cannot embed it in the encryptions $\mathsf{sk}_{x,\mathsf{msk_{out}}}$ generated to the first coordinate. A typical approach for dealing with such a difficulty (e.g., [ABS+14, BS15, KSY15]) is to embed all possibly-needed encryptions under $\mathsf{msk_{out}}$ inside the ciphertexts of the two-input scheme (so that the key $\mathsf{msk_{out}}$ will not be explicitly needed). Note, however, that when an adversary makes T encryption queries there may be roughly T^2 different pairs of the form (x, y), and these T^2 pairs cannot be embedded into T ciphertexts (we note that $T = T(\lambda)$ may be any polynomial and it is not known in advance).[3]

Step 2: Selective security via "one-sided" key encapsulation. Our approach for resolving the difficulty described above is inspired by the recent work of Ananth et al. [ABS+14] that uses key encapsulation techniques in functional encryption. Our main idea here is that when encrypting a message x, we sample a fresh key $\mathsf{msk}^\star$ for the single-input scheme, and output two components: $\mathsf{Enc}_{\mathsf{msk_{out}}}(\mathsf{msk}^\star)$ and $\mathsf{sk}_{x,\mathsf{msk}^\star}$. Given an encryption $\mathsf{Enc}_{\mathsf{msk_{in}}}(y)$ of a message y, the component $\mathsf{sk}_{x,\mathsf{msk}^\star}$ enables to compute $\mathsf{Enc}_{\mathsf{msk}^\star}(x||y)$. In addition, a functional key for a function f is now generated using $\mathsf{msk_{out}}$ for the following functionality: Given an input $\mathsf{msk}^\star$, it outputs a functional key for f (viewed as a single-input function) using $\mathsf{msk}^\star$. This enables to compute $f(x, y)$ given $\mathsf{Enc}_{\mathsf{msk}^\star}(x||y)$ and provides the required functionality.

This "one-sided" key encapsulation enables us to prove a selectively-secure variant of our notion of security.[4] In this variant we require adversaries to specify their encryption queries in advance, and they are then given adaptive access to the left-or-right key-generation oracle. The main idea underlying the proof of security is that our one-sided key encapsulation approach yields sufficient independence and allows attacking the x's one by one, by attacking their corresponding encapsulated keys. Focusing on one message x and its encapsulated key msk^*, an adversary that make T encryption queries $y_1, \ldots, y_T$ to the second coordinate induces only T pairs $\{(x, y_i)\}_{i\in[T]}$ (instead of T^2 pairs as above). Moreover, given that the encryption queries are chosen in advance, we can embed an encryption of $x||y_i$ under $\mathsf{msk}^\star$ inside the encryption of each y_i. This way the key $\mathsf{msk}^\star$ is not explicitly needed, and thus can be attacked (while not affecting any of the other x's).

[3] An additional approach is to use a *public-key* functional encryption scheme for the role played by $\mathsf{msk_{out}}$ (i.e., replacing $\mathsf{sk}_{x,\mathsf{msk_{out}}}$ with $\mathsf{sk}_{x,\mathsf{pk_{out}}}$). Although this solution allows to prove security in the two-input setting, it cannot be extended to a larger number of inputs (essentially because public-key schemes cannot be function private). Furthermore, we would like to avoid relying on a stronger primitive than necessary.

[4] "One-sided" here refers to the fact that the encapsulated key $\mathsf{msk}^\star$ is generated only from the side of the x's.

This enables us to construct a selectively-secure two-input scheme from any selectively-secure single-input one (we refer the reader to Section 3 for the scheme and its proof of security). Note, however, that this approach is limited to selective adversaries: embedding an encryption of $x||y_i$ inside the encryption of y_i requires knowing x before the adversary queries for the encryption of y_i.

Step 3: Adaptive security via "two-sided" key encapsulation. Next, we present a generic transformation from selective security to adaptive security (in fact, to our stronger notion of full security). This transformation is based on "two-sided" key encapsulation, where each pair of messages x and y has its own encapsulated key $\mathsf{msk}^\star$. This, more subtle approach, enables us to "attack" a specific pair of messages each time, since each such pair uses a different encapsulated key: If x is known before y then we embed $x||y$ inside the encryption of y, and if x is known after y then we embed $x||y$ inside the encryption of x. This leaves the problem of how to realize this idea of two-sided key encapsulation. Our two-sided key encapsulation works as follows.

1. An encryption of a message y consists of two components: $\mathsf{Enc}_{\mathsf{msk}_{\mathsf{out}}}(t)$ and $\mathsf{Enc}_{\mathsf{msk}_{\mathsf{in}}}(y,t)$, where t is a fresh random tag.
2. An encryption of a message x consists of two components: $\mathsf{Enc}_{\mathsf{msk}_{\mathsf{out}}}(s)$ and $\mathsf{sk}_{x,s}$, where s is a fresh random tag. The functional key $\mathsf{sk}_{x,s}$ is generated using $\mathsf{msk}_{\mathsf{in}}$ and corresponds to the following functionality: Given an input (y,t), derive $\mathsf{msk}^\star = \mathsf{PRF}(s,t)$,[5] and output $\mathsf{Enc}_{\mathsf{msk}^\star}(x||y)$.
3. A functional key for a function f is generated using $\mathsf{msk}_{\mathsf{out}}$ for the following functionality: Given *two inputs*, s and t, derive $\mathsf{msk}^\star = \mathsf{PRF}(s,t)$, and output a functional key for f (viewed as a single-input function) using $\mathsf{msk}^\star$.

The crucial observation is that although now $\mathsf{msk}_{\mathsf{out}}$ is a master secret key for a *two-input* scheme, it is only applied on random tags, and thus only needs to be selectively secure (this is inspired by the recent selective-to-adaptive transformation of Ananth et al. [ABS$^+$14] for single-input schemes – see Section 1.2). Our two-sided key encapsulation approach enables us to construct a fully-secure two-input scheme from any selectively-secure one (we refer the reader to Section 4 for the scheme and its proof of security).

Generalization to t-input schemes. The generalization of our result to t-input schemes, for $t \geq 2$, consists of two components. The first component is a construction that uses any $(t-1)$-input scheme for building a selectively-secure t-input scheme, for any $t \geq 2$. The second component is a construction that uses any selectively-secure t-input scheme for building a fully-secure t-input scheme. Thus, for obtaining a fully-secure t-input scheme from any single-input scheme, one can iteratively apply our first component $t-1$ times, and then apply our second component on the resulting t-input scheme.

This iterative application of our first component places a restriction on the number of supported inputs. In general, each such application may result in a polynomial blow-up in the parameters of the scheme. Therefore, $t-1$ applications may result in a blow-up of $\lambda^{2^{O(t)}}$ which must be kept polynomial. Without any additional assumptions, this implies that t can be any fixed constant. Assuming, in addition, that the underlying single-input scheme is sub-exponentially secure, the number of inputs can be made super-constant. Specifically, for any constant $0 < \epsilon < 1$, when instantiating the underlying single-input scheme with security parameter $\tilde{\lambda} = 2^{(\log \lambda)^\epsilon}$, the first component can be iteratively applied to reach $t = \Theta(\log \log \lambda)$ inputs. Obtaining a generic transformation that supports a super-constant number of inputs without assuming sub-exponential security is left as an open problem.

[5] More accurately, the key $\mathsf{msk}^\star$ is computed by applying the setup algorithm of $\mathsf{1FE}$ with randomness $\mathsf{PRF}(s,t)$.

1.4 Paper Organization

The remainder of this paper is organized as follows. In Section 2 we provide an overview of the notation, definitions, and tools underlying our constructions. In Section 3 we present a construction of a selectively-secure two-input functional encryption scheme from any single-input scheme. In Section 4 we present a construction of a fully-secure two-input functional encryption scheme from any selectively-secure one. In Appendix A we generalize approach to t-input schemes for $t \geq 2$, and in Appendix B we provide the formal proofs of our claims from Sections 3 and 4.

2 Preliminaries

In this section we present the notation and basic definitions that are used in this work. For a distribution X we denote by $x \leftarrow X$ the process of sampling a value x from the distribution X. Similarly, for a set $\mathcal{X}$ we denote by $x \leftarrow \mathcal{X}$ the process of sampling a value x from the uniform distribution over $\mathcal{X}$. For a randomized function f and an input $x \in \mathcal{X}$, we denote by $y \leftarrow f(x)$ the process of sampling a value y from the distribution $f(x)$. For an integer $n \in \mathbb{N}$ we denote by $[n]$ the set $\{1, \ldots, n\}$. A function $\mathsf{neg} : \mathbb{N} \to \mathbb{R}$ is *negligible* if for every constant $c > 0$ there exists an integer N_c such that $\mathsf{neg}(\lambda) < \lambda^{-c}$ for all $\lambda > N_c$.

Two sequences of random variables $X = \{X_\lambda\}_{\lambda \in \mathbb{N}}$ and $Y = \{Y_\lambda\}_{\lambda \in \mathbb{N}}$ are *computationally indistinguishable* if for any probabilistic polynomial-time algorithm $\mathcal{A}$ there exists a negligible function $\mathsf{neg}(\cdot)$ such that $\left|\Pr[\mathcal{A}(1^\lambda, X_\lambda) = 1] - \Pr[\mathcal{A}(1^\lambda, Y_\lambda) = 1]\right| \leq \mathsf{neg}(\lambda)$ for all sufficiently large $\lambda \in \mathbb{N}$. Throughout the paper, we denote by λ the security parameter.

2.1 Pseudorandom Functions

Let $\{\mathcal{K}_\lambda, \mathcal{X}_\lambda, \mathcal{Y}_\lambda\}_{\lambda \in \mathbb{N}}$ be a sequence of sets and let $\mathsf{PRF} = (\mathsf{PRF.Gen}, \mathsf{PRF.Eval})$ be a function family with the following syntax:

- $\mathsf{PRF.Gen}$ is a probabilistic polynomial-time algorithm that takes as input the unary representation of the security parameter λ, and outputs a key $K \in \mathcal{K}_\lambda$.
- $\mathsf{PRF.Eval}$ is a deterministic polynomial-time algorithm that takes as input a key $K \in \mathcal{K}_\lambda$ and a value $x \in \mathcal{X}_\lambda$, and outputs a value $y \in \mathcal{Y}_\lambda$.

The sets $\mathcal{K}_\lambda$, $\mathcal{X}_\lambda$, and $\mathcal{Y}_\lambda$ are referred to as the *key space*, *domain*, and *range* of the function family, respectively. For easy of notation we may denote by $\mathsf{PRF.Eval}_K(\cdot)$ or $\mathsf{PRF}_K(\cdot)$ the function $\mathsf{PRF.Eval}(K, \cdot)$ for $K \in \mathcal{K}_\lambda$. The following is the standard definition of a pseudorandom function family.

Definition 2.1 (Pseudorandomness)**.** A function family $\mathsf{PRF} = (\mathsf{PRF.Gen}, \mathsf{PRF.Eval})$ is *pseudorandom* if for every probabilistic polynomial-time algorithm $\mathcal{A}$ there exits a negligible function $\mathsf{neg}(\cdot)$ such that

$$\mathsf{Adv}_{\mathsf{PRF},\mathcal{A}}(\lambda) \stackrel{\mathsf{def}}{=} \left| \Pr_{K \leftarrow \mathsf{PRF.Gen}(1^\lambda)}\left[\mathcal{A}^{\mathsf{PRF.Eval}_K(\cdot)}(1^\lambda) = 1\right] - \Pr_{f \leftarrow F_\lambda}\left[\mathcal{A}^{f(\cdot)}(1^\lambda) = 1\right] \right| \leq \mathsf{neg}(\lambda),$$

for all sufficiently large $\lambda \in \mathbb{N}$, where F_λ is the set of all functions that map $\mathcal{X}_\lambda$ into $\mathcal{Y}_\lambda$.

In addition to the standard notion of a pseudorandom function family, we rely on the seemingly stronger (yet existentially equivalent) notion of a *puncturable* pseudorandom function family [KPT+13, BW13, SW14, BGI14]. In terms of syntax, this notion asks for an additional probabilistic polynomial-time algorithm, $\mathsf{PRF.Punc}$, that takes as input a key $K \in \mathcal{K}_\lambda$ and a set $S \subseteq \mathcal{X}_\lambda$ and outputs a "punctured" key K_S. The properties required by such a puncturing algorithm are captured by the following definition.

Definition 2.2 (Puncturable PRF)**.** A pseudorandom function family $\mathsf{PRF} = (\mathsf{PRF.Gen}, \mathsf{PRF.Eval}, \mathsf{PRF.Punc})$ is *puncturable* if the following properties are satisfied:

1. **Functionality:** For all sufficiently large $\lambda \in \mathbb{N}$, for every set $S \subseteq \mathcal{X}_\lambda$, and for every $x \in \mathcal{X}_\lambda \setminus S$ it holds that

$$\Pr_{\substack{K \leftarrow \mathsf{PRF.Gen}(1^\lambda); \\ K_S \leftarrow \mathsf{PRF.Punc}(K,S)}} [\mathsf{PRF.Eval}_K(x) = \mathsf{PRF.Eval}_{K_S}(x)] = 1.$$

2. **Pseudorandomness at punctured points:** Let $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ be any probabilistic polynomial-time algorithm such that $\mathcal{A}_1(1^\lambda)$ outputs a set $S \subseteq \mathcal{X}_\lambda$, a value $x \in S$, and state information state. Then, for any such $\mathcal{A}$ there exists a negligible function $\mathsf{neg}(\cdot)$ such that

$$\mathsf{Adv}_{\mathsf{PRF},\mathcal{A}}(\lambda) \stackrel{\mathsf{def}}{=} |\Pr[\mathcal{A}_2(K_S, \mathsf{PRF.Eval}_K(x), \mathsf{state}) = 1] - \Pr[\mathcal{A}_2(K_S, y, \mathsf{state}) = 1]| \leq \mathsf{neg}(\lambda)$$

for all sufficiently large $\lambda \in \mathbb{N}$, where $(S, x, \mathsf{state}) \leftarrow \mathcal{A}_1(1^\lambda)$, $K \leftarrow \mathsf{PRF.Gen}(1^\lambda)$, $K_S = \mathsf{PRF.Punc}(K, S)$, and $y \leftarrow \mathcal{Y}_\lambda$.

For our constructions we rely on pseudorandom functions that need to be punctured only at one point (i.e., in both parts of Definition 2.2 it holds that $S = \{x\}$ for some $x \in \mathcal{X}_\lambda$). As observed by [KPT+13, BW13, SW14, BGI14] the GGM construction [GGM86] of PRFs from any one-way function can be easily altered to yield such a puncturable pseudorandom function family.

2.2 Private-Key Single-Input Functional Encryption

A private-key single-input functional encryption scheme over a message space $\mathcal{X} = \{\mathcal{X}_\lambda\}_{\lambda \in \mathbb{N}}$ and a function space $\mathcal{F} = \{\mathcal{F}_\lambda\}_{\lambda \in \mathbb{N}}$ is a quadruple $(\mathsf{FE.S}, \mathsf{FE.KG}, \mathsf{FE.E}, \mathsf{FE.D})$ of probabilistic polynomial-time algorithms. The setup algorithm $\mathsf{FE.S}$ takes as input the unary representation 1^λ of the security parameter $\lambda \in \mathbb{N}$ and outputs a master-secret key msk. The key-generation algorithm $\mathsf{FE.KG}$ takes as input a master-secret key msk and a single-input function $f \in \mathcal{F}_\lambda$, and outputs a functional key sk_f. The encryption algorithm $\mathsf{FE.E}$ takes as input a master-secret key msk and a message $x \in \mathcal{X}_\lambda$, and outputs a ciphertext ct. In terms of correctness we require that for all sufficiently large $\lambda \in \mathbb{N}$, for every function $f \in \mathcal{F}_\lambda$ and message $x \in \mathcal{X}_\lambda$ it holds that $\mathsf{FE.D}(\mathsf{FE.KG}(\mathsf{msk}, f), \mathsf{FE.E}(\mathsf{msk}, x)) = f(x)$ with all but a negligible probability over the internal randomness of the algorithms $\mathsf{FE.S}$, $\mathsf{FE.KG}$, and $\mathsf{FE.E}$.

In terms of security, we rely on the private-key variant of the existing indistinguishability-based notions for message privacy and function privacy. In fact, following [AAB+13, BS15], our notion of security combines both message privacy and function privacy. When formalizing this notion it would be convenient to use the following standard notion of a *left-or-right oracle*.

Definition 2.3 (Left-or-right oracle)**.** Let $\mathcal{O}(\cdot,\cdot)$ be a probabilistic two-input functionality. For each $b \in \{0, 1\}$ we denote by $\mathcal{O}_b$ the probabilistic three-input functionality $\mathcal{O}_b(k, z_0, z_1) \stackrel{\mathsf{def}}{=} \mathcal{O}(k, z_b)$.

Intuitively, a private-key functional-encryption scheme is secure if encryptions of messages x_1, $\ldots, x_T$ together with functional keys corresponding to functions $f_1, \ldots, f_T$ reveal essentially no information other than the values $\{f_i(x_j)\}_{i,j \in [T]}$. We consider an adaptive notion of security, to which we refer to as *full security*, in which adversaries are given adaptive access to left-or-right encryption and key-generation oracles.

Definition 2.4 (Full security [AAB+13, BS15]). A private-key single-input functional encryption scheme $\mathsf{FE} = (\mathsf{FE.S}, \mathsf{FE.KG}, \mathsf{FE.E}, \mathsf{FE.D})$ over a message space $\mathcal{X} = \{\mathcal{X}_\lambda\}_{\lambda \in \mathbb{N}}$ and a function space $\mathcal{F} = \{\mathcal{F}_\lambda\}_{\lambda \in \mathbb{N}}$ is *fully secure* if for any probabilistic polynomial-time adversary $\mathcal{A}$ there exists a negligible function $\mathsf{neg}(\cdot)$ such that

$$\begin{aligned}\mathsf{Adv}^{\mathsf{full1FE}}_{\mathsf{FE},\mathcal{A},\mathcal{F}}(\lambda) &\stackrel{\mathsf{def}}{=} \left|\Pr\left[\mathcal{A}^{\mathsf{KG}_0(\mathsf{msk},\cdot,\cdot),\mathsf{Enc}_0(\mathsf{msk},\cdot,\cdot)}(1^\lambda) = 1\right] - \Pr\left[\mathcal{A}^{\mathsf{KG}_1(\mathsf{msk},\cdot,\cdot),\mathsf{Enc}_1(\mathsf{msk},\cdot,\cdot)}(1^\lambda) = 1\right]\right| \\ &\leq \mathsf{neg}(\lambda)\end{aligned}$$

for all sufficiently large $\lambda \in \mathbb{N}$, where for every $(f_0, f_1) \in \mathcal{F}_\lambda \times \mathcal{F}_\lambda$ and $(x_0, x_1) \in \mathcal{X}_\lambda \times \mathcal{X}_\lambda$ with which $\mathcal{A}$ queries the left-or-right key-generation and encryption oracles, respectively, it holds that $f_0(x_0) = f_1(x_1)$. Moreover, the probability is taken over the choice of $\mathsf{msk} \leftarrow \mathsf{FE.S}(1^\lambda)$ and the internal randomness of $\mathcal{A}$.

Known constructions. Private-key single-input functional encryption schemes that satisfy the above notion of full security and support circuits of any a-priori bounded polynomial size are known to exist based on a variety of assumptions.

Ananth et al. [ABS+14] gave a generic transformation from selective-message (or selective-function) security to full security. Moreover, Brakerski and Segev [BS15] showed how to transform any message-private functional encryption scheme into a functional encryption scheme which is fully secure, and the resulting scheme inherits the security guarantees of the original one. Therefore, based on [ABS+14, BS15], given any selective-message (or selective-function) message-private functional encryption scheme we can generically obtain a fully-secure scheme. This implies that schemes that are fully secure for any number of encryption and key-generation queries can be based on indistinguishability obfuscation [GGH+13, Wat14], differing-input obfuscation [BCP14, ABG+13], and multilinear maps [GGH+14]. In addition, schemes that are fully secure for a bounded number $T = T(\lambda)$ of encryption and key-generation queries can be based on the Learning with Errors (LWE) assumption (where the length of ciphertexts grows with T and with a bound on the depth of allowed functions) [GKP+13], based on pseudorandom generators computable by small-depth circuits (where the length of ciphertexts grows with T and with an upper bound on the circuit size of the functions) [GVW12], and even based on one-way functions (for $T = 1$) [GVW12].

2.3 Private-Key Two-Input Functional Encryption

In this section we define the functionality and security of private-key *two-input* functional encryption scheme (we refer the reader to Appendix A.1 for the generalization to t-input schemes for any $t \geq 2$). Let $\mathcal{X} = \{\mathcal{X}_\lambda\}_{\lambda \in \mathbb{N}}$, $\mathcal{Y} = \{\mathcal{Y}_\lambda\}_{\lambda \in \mathbb{N}}$, and $\mathcal{Z} = \{\mathcal{Z}_\lambda\}_{\lambda \in \mathbb{N}}$ be ensembles of finite sets, and let $\mathcal{F} = \{\mathcal{F}_\lambda\}_{\lambda \in \mathbb{N}}$ be an ensemble of finite two-ary function families. For each $\lambda \in \mathbb{N}$, each function $f \in \mathcal{F}_\lambda$ takes as input two strings, $x \in \mathcal{X}_\lambda$ and $y \in \mathcal{Y}_\lambda$, and outputs a value $f(x, y) \in \mathcal{Z}_\lambda$. A private-key two-input functional encryption scheme Π for $\mathcal{F}$ consists of four probabilistic polynomial time algorithm Setup, Enc, KG and Dec, described as follows.

- $\mathsf{Setup}(1^\lambda)$ – The setup algorithm takes as input the security parameter λ, and outputs a master secret key msk.
- $\mathsf{Enc}(\mathsf{msk}, m, \mathsf{i})$ – The encryption algorithm takes as input a master secret key msk, message input m, and an index $\mathsf{i} \in [2]$, where $m \in \mathcal{X}_\lambda$ if $\mathsf{i} = 1$ and $m \in \mathcal{Y}_\lambda$ if $\mathsf{i} = 2$. It outputs a ciphertext ct_i.
- $\mathsf{KG}(\mathsf{msk}, f)$ – The key-generation algorithm takes as input a master secret key msk and a function $f \in \mathcal{F}_\lambda$, and outputs a functional key sk_f.

- $\mathsf{Dec}(\mathsf{sk}_f, \mathsf{ct}_1, \mathsf{ct}_2)$ – The (deterministic) decryption algorithm takes as input a functional key sk_f and two ciphertexts ct_1 and ct_2, and outputs a string $z \in \mathcal{Z}_\lambda \cup \{\perp\}$.

Definition 2.5 (Correctness)**.** A private-key two-input functional encryption scheme $\Pi = (\mathsf{Setup}, \mathsf{Enc}, \mathsf{KG}, \mathsf{Dec})$ for $\mathcal{F}$ is *correct* if there exists a negligible function $\mathsf{neg}(\cdot)$ such that for every $\lambda \in \mathbb{N}$, for every $f \in \mathcal{F}_\lambda$, and for every $(x, y) \in \mathcal{X}_\lambda \times \mathcal{Y}_\lambda$, it holds that

$$\Pr\left[\mathsf{Dec}(\mathsf{sk}_f, \mathsf{Enc}(\mathsf{msk}, x, 1), \mathsf{Enc}(\mathsf{msk}, y, 2)) = f(x, y)\right] \geq 1 - \mathsf{neg}(\lambda),$$

where $\mathsf{msk} \leftarrow \mathsf{Setup}(1^\lambda)$, $\mathsf{sk}_f \leftarrow \mathsf{KG}(\mathsf{msk}, f)$, and the probability is taken over the internal randomness of $\mathsf{Setup}, \mathsf{Enc}$ and KG.

Intuitively, we say that a two-input scheme is secure if for any two pairs of messages (x_0, x_1) and (y_0, y_1) that are encrypted with respect to indices $\mathsf{i} = 1$ and $\mathsf{i} = 2$, respectively, and for every pair of functions (f_0, f_1), the triplets $(\mathsf{sk}_{f_0}, \mathsf{Enc}(\mathsf{msk}, x_0, 1), \mathsf{Enc}(\mathsf{msk}, y_0, 2))$ and $(\mathsf{sk}_{f_1}, \mathsf{Enc}(\mathsf{msk}, x_1, 1), \mathsf{Enc}(\mathsf{msk}, y_1, 2))$ are computationally indistinguishable as long as $f_0(x_0, y_0) = f_1(x_1, y_1)$ (note that this considers both message privacy and function privacy). The formal notions of security build upon this intuition and capture the fact that an adversary may in fact hold many functional keys and ciphertexts, and may combine them in an arbitrary manner. As in the case of single-input schemes, we formalize our notions of security using left-or-right key-generation and encryption oracles. Specifically, for each $b \in \{0, 1\}$ and $\mathsf{i} \in \{1, 2\}$ we let $\mathsf{KG}_b(\mathsf{msk}, f_0, f_1) \stackrel{\mathsf{def}}{=} \mathsf{KG}(\mathsf{msk}, f_b)$ and $\mathsf{Enc}_b(\mathsf{msk}, (m_0, m_1), \mathsf{i}) \stackrel{\mathsf{def}}{=} \mathsf{Enc}(\mathsf{msk}, m_b, \mathsf{i})$. Before formalizing our notions of security we define the notion of a *valid two-input adversary*.

Definition 2.6 (Valid two-input adversary)**.** A probabilistic polynomial-time algorithm $\mathcal{A}$ is a *valid two-input adversary* if for all private-key two-input functional encryption schemes $\Pi = (\mathsf{Setup}, \mathsf{KG}, \mathsf{Enc}, \mathsf{Dec})$ over a message space $\mathcal{X} \times \mathcal{Y} = \{\mathcal{X}_\lambda\}_{\lambda \in \mathbb{N}} \times \{\mathcal{Y}_\lambda\}_{\lambda \in \mathbb{N}}$ and a function space $\mathcal{F} = \{\mathcal{F}_\lambda\}_{\lambda \in \mathbb{N}}$, for all $\lambda \in \mathbb{N}$ and $b \in \{0, 1\}$, and for all $(f_0, f_1) \in \mathcal{F}_\lambda$, $((x_0, x_1), 1) \in \mathcal{X}_\lambda \times \mathcal{X}_\lambda \times \{1\}$ and $((y_0, y_1), 1) \in \mathcal{Y}_\lambda \times \mathcal{Y}_\lambda \times \{2\}$ with which $\mathcal{A}$ queries the left-or-right key-generation and encryption oracles, respectively, it holds that $f_0(x_0, y_0) = f_1(x_1, y_1)$.

We consider two notions of security for two-input functional encryption schemes, both of which combine message privacy and function privacy. The first notion, *full security*, considers adversaries that have adaptive access to both the encryption oracle and the key-generation oracle. The second notion, *selective-message security*, considers adversaries that must specify all of their encryption queries in advance, but can then have adaptive access to the key-generation oracle. Full security clearly implies selective-message security, and our work shows that the two notions are in fact equivalent for multi-input schemes.

Definition 2.7 (Full security)**.** A private-key two-input functional encryption scheme $\Pi = (\mathsf{Setup}, \mathsf{KG}, \mathsf{Enc}, \mathsf{Dec})$ over a message space $\mathcal{X} \times \mathcal{Y} = \{\mathcal{X}_\lambda\}_{\lambda \in \mathbb{N}} \times \{\mathcal{Y}_\lambda\}_{\lambda \in \mathbb{N}}$ and a function space $\mathcal{F} = \{\mathcal{F}_\lambda\}_{\lambda \in \mathbb{N}}$ is *fully secure* if for any valid two-input adversary $\mathcal{A}$ there exists a negligible function $\mathsf{neg}(\cdot)$ such that

$$\mathsf{Adv}^{\mathsf{full2FE}}_{\Pi, \mathcal{F}, \mathcal{A}} \stackrel{\mathsf{def}}{=} \left| \Pr\left[\mathsf{Exp}^{\mathsf{full2FE}}_{\Pi, \mathcal{F}, \mathcal{A}}(\lambda) = 1\right] - \frac{1}{2} \right| \leq \mathsf{neg}(\lambda),$$

for all sufficiently large $\lambda \in \mathbb{N}$, where the random variable $\mathsf{Exp}^{\mathsf{full2FE}}_{\Pi, \mathcal{F}, \mathcal{A}}(\lambda)$ is defined via the following experiment:

1. $\mathsf{msk} \leftarrow \mathsf{Setup}(1^\lambda)$, $b \leftarrow \{0, 1\}$.

2. $b' \leftarrow \mathcal{A}^{\mathsf{KG}_b(\mathsf{msk},\cdot,\cdot),\mathsf{Enc}_b(\mathsf{msk},(\cdot,\cdot),\cdot)}\left(1^\lambda,\right)$.
3. If $b' = b$ then output 1, and otherwise output 0.

Definition 2.8 (Selective-message security)**.** A private-key two-input functional encryption scheme $\Pi = (\mathsf{Setup}, \mathsf{KG}, \mathsf{Enc}, \mathsf{Dec})$ over a message space $\mathcal{X} \times \mathcal{Y} = \{\mathcal{X}_\lambda\}_{\lambda\in\mathbb{N}} \times \{\mathcal{Y}_\lambda\}_{\lambda\in\mathbb{N}}$ and a function space $\mathcal{F} = \{\mathcal{F}_\lambda\}_{\lambda\in\mathbb{N}}$ is *selective-message secure* if for any valid two-input adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ there exists a negligible function $\mathsf{neg}(\lambda)$ such that

$$\mathsf{Adv}^{\mathsf{sel2FE}}_{\Pi,\mathcal{F},\mathcal{A}} \stackrel{\mathsf{def}}{=} \left| \Pr\left[\mathsf{Exp}^{\mathsf{sel2FE}}_{\Pi,\mathcal{F},\mathcal{A}}(\lambda) = 1\right] - \frac{1}{2} \right| \leq \mathsf{neg}(\lambda),$$

for all sufficiently large $\lambda \in \mathbb{N}$, where the random variable $\mathsf{Exp}^{\mathsf{sel2FE}}_{\Pi,\mathcal{F},\mathcal{A}}(\lambda)$ is defined via the following experiment:

1. $(\vec{x}, \vec{y}, \mathsf{state}) \leftarrow \mathcal{A}_1\left(1^\lambda\right)$, where $\vec{x} = ((x_1^0, x_1^1), \ldots, (x_T^0, x_T^1))$ and $\vec{y} = ((y_1^0, y_1^1), \ldots, (y_T^0, y_T^1))$.
2. $\mathsf{msk} \leftarrow \mathsf{Setup}(1^\lambda)$, $b \leftarrow \{0, 1\}$.
3. $\mathsf{ct}_{1,i} \leftarrow \mathsf{Enc}(\mathsf{msk}, x_i^b, 1)$ and $\mathsf{ct}_{2,i} \leftarrow \mathsf{Enc}(\mathsf{msk}, y_i^b, 2)$ for $i \in [T]$.
4. $b' \leftarrow \mathcal{A}_2^{\mathsf{KG}_b(\mathsf{msk},\cdot,\cdot)}\left(1^\lambda, \mathsf{ct}_{1,1}, \ldots, \mathsf{ct}_{1,T}, \mathsf{ct}_{2,1} \ldots, \mathsf{ct}_{2,T}, \mathsf{state}\right)$.
5. If $b' = b$ then output 1, and otherwise output 0.

3 A Selectively-Secure Two-Input Scheme from any Single-Input Scheme

In this section we construct a private-key two-input functional encryption scheme that is selectively secure. Let $\mathcal{F} = \{\mathcal{F}_\lambda\}_{\lambda\in\mathbb{N}}$ be a family of two-ary functionalities, where for every $\lambda \in \mathbb{N}$ the set $\mathcal{F}_\lambda$ consists of functions of the form $f : \mathcal{X}_\lambda \times \mathcal{Y}_\lambda \to \mathcal{Z}_\lambda$. Our construction relies on the following building blocks:

1. A private-key single-input functional encryption scheme $\mathsf{1FE} = (\mathsf{1FE.S}, \mathsf{1FE.KG}, \mathsf{1FE.E}, \mathsf{1FE.D})$.
2. A pseudorandom function family $\mathsf{PRF} = (\mathsf{PRF.Gen}, \mathsf{PRF.Eval})$.

As discussed in Section 1.1, we assume that the scheme 1FE is sufficiently expressive in the sense that 1FE supports the function family $\mathcal{F}$ (when viewed as a family of single-input functions), the evaluation procedure of the pseudorandom function family PRF, the encryption and key-generation procedures of the private-key functional encryption scheme 1FE, and a few additional basic operations. Our scheme $\mathsf{2FE^{sel}} = (\mathsf{2FE^{sel}.S}, \mathsf{2FE^{sel}.KG}, \mathsf{2FE^{sel}.E}, \mathsf{2FE^{sel}.D})$ is defined as follows.

- **The setup algorithm.** On input the security parameter 1^λ the setup algorithm $\mathsf{2FE^{sel}.S}$ samples $\mathsf{msk_{out}}, \mathsf{msk_{in}} \leftarrow \mathsf{1FE.S}(1^\lambda)$ and outputs $\mathsf{msk} = (\mathsf{msk_{out}}, \mathsf{msk_{in}})$.
- **The key-generation algorithm.** On input the master secret key msk and a function $f \in \mathcal{F}_\lambda$, the key-generation algorithm $\mathsf{2FE^{sel}.KG}$ samples a random string $z \leftarrow \{0, 1\}^\lambda$ and outputs $\mathsf{sk}_f \leftarrow \mathsf{1FE.KG}(\mathsf{msk_{out}}, D_{f,\perp,z,\perp})$, where $D_{f,\perp,z,\perp}$ is a single-input function that is defined in Figure 1.

$\boldsymbol{D_{f_0,f_1,z,u}((\mathsf{msk}^\star, K, w))}$:	$\boldsymbol{C_f((x, y))}$:
1. If $\mathsf{msk}^\star = \perp$, output u and HALT. 2. Compute $r = \mathsf{PRF.Eval}(K, z)$. 3. Output $\mathsf{1FE.KG}(\mathsf{msk}^\star, C_{f_w}; r)$.	1. Output $f(x, y)$.

Figure 1: The single-input functions $D_{f_0,f_1,z,u}$ and C_f.

- **The encryption algorithm.** On input the master secret key msk, a message m and an index $\mathsf{i} \in [2]$, the encryption algorithm $\mathsf{2FE^{sel}.E}$ has two cases:
  - If $(m, \mathsf{i}) = (x, 1)$, it samples a master secret key $\mathsf{msk}^\star \leftarrow \mathsf{1FE.S}(1^\lambda)$, a PRF key $K \leftarrow \mathsf{PRF.Gen}(1^\lambda)$, and a random string $s \in \{0,1\}^\lambda$, and then outputs a pair $(\mathsf{ct}_1, \mathsf{sk}_1)$ defined as follows:

$$\mathsf{ct}_1 \leftarrow \mathsf{1FE.E}(\mathsf{msk_{out}}, (\mathsf{msk}^\star, K, 0))$$
$$\mathsf{sk}_1 \leftarrow \mathsf{1FE.KG}(\mathsf{msk_{in}}, \mathsf{AGG}_{x,\perp,0,s,\mathsf{msk}^\star,K}),$$

    where $\mathsf{AGG}_{x,\perp,0,s,\mathsf{msk}^\star,K}$ is a single-input function that is defined in Figure 2.
  - If $(m, \mathsf{i}) = (y, 2)$, it samples a random string $t \in \{0,1\}^\lambda$, and outputs

$$\mathsf{ct}_2 \leftarrow \mathsf{1FE.E}(\mathsf{msk_{in}}, (y, \perp, t, \perp, \perp)).$$

$\mathsf{AGG}_{x_0,x_1,a,s,\mathsf{msk}^\star,K}((y_0, y_1, t, s', v))$:

1. If $s' = s$ output v and HALT.
2. Compute $r = \mathsf{PRF.Eval}(K, t)$.
3. Output $\mathsf{1FE.E}(\mathsf{msk}^\star, (x_a, y_a); r)$.

Figure 2: The single-input function $\mathsf{AGG}_{x_0,x_1,a,s,\mathsf{msk}^\star,K}$.

- **The decryption algorithm.** On input a functional key sk_f and two ciphertexts, $(\mathsf{ct}_1, \mathsf{sk}_1)$ and ct_2, the decryption algorithm $\mathsf{2FE^{sel}.D}$ computes $\mathsf{ct}' = \mathsf{1FE.D}(\mathsf{sk}_1, \mathsf{ct}_2)$, $\mathsf{sk}' = \mathsf{1FE.D}(\mathsf{sk}_f, \mathsf{ct}_1)$ and outputs $\mathsf{1FE.D}(\mathsf{sk}', \mathsf{ct}')$.

The correctness of the above scheme with respect to any family of two-ary functionalities follows in a straightforward manner from the correctness of the underlying functional encryption scheme $\mathsf{1FE}$. Specifically, consider any pair of messages x and y and any function f. The encryption of x with respect to the index i =1 and the encryption of y with respect to the index $\mathsf{i} = 2$ result in ciphertexts $(\mathsf{ct}_1, \mathsf{sk}_1)$ and ct_2, respectively. Using the correctness of the scheme $\mathsf{1FE}$, by executing $\mathsf{1FE.D}(\mathsf{sk}_1, \mathsf{ct}_2)$ we obtain an encryption ct' of the message (x, y) under the key $\mathsf{msk}^\star$. In addition, by executing $\mathsf{1FE.D}(\mathsf{sk}_f, \mathsf{ct}_1)$ we obtain a functional key sk' for C_f under the key $\mathsf{msk}^\star$. Therefore, executing $\mathsf{1FE.D}(\mathsf{sk}', \mathsf{ct}')$ outputs the value $C_f((x, y)) = f(x, y)$ as required.

The following theorem captures the security of the scheme, stating that under suitable assumptions on the underlying building blocks, the two-input scheme $\mathsf{2FE^{sel}}$ is selective-message secure (see Definition 2.8).

Theorem 3.1. *Assuming that (1)* $\mathsf{1FE}$ *is fully secure, and (2)* PRF *is a pseudorandom function family, then* $\mathsf{2FE^{sel}}$ *is selective-message secure.*

We note that for proving that $\mathsf{2FE^{sel}}$ is selective-message secure it suffices to require selective-message security from $\mathsf{1FE}$. However, given the generic transformations of Ananth et al. [ABS+14] (from selective security to adaptive security) and of Brakerski and Segev [BS15] (from message security to full security), for simplifying the proof of Theorem 3.1 we assume that $\mathsf{1FE}$ is fully secure. In addition, when assuming that $\mathsf{1FE}$ is fully secure, the scheme $\mathsf{2FE^{sel}}$ can be shown to satisfy a notion of security that seems in between selective-message security and full security. Specifically, this notion considers adversaries that first have adaptive access to encryptions only for the first coordinate, and then have adaptive access to encryptions only for the second coordinate (while having adaptive access to the key-generation oracle throughout the experiment). However, given our generic transformation from selective-message security to full security for multi-input schemes (see Section 4), for simplifying the proof of Theorem 3.1 we focus on proving selective-message security.

In addition, for concreteness we focus on the unbounded case where the underlying scheme supports an unbounded (i.e., not fixed in advance) number of key-generation queries and encryption queries. More generally, the proof of Theorem 3.1 shows that if the scheme corresponding to $\mathsf{msk_{out}}$ supports T_1 encryption queries and T_2 key-generation queries, the scheme corresponding to $\mathsf{msk_{in}}$ supports T_3 encryption queries and T_4 key-generation queries, and the scheme corresponding to each $\mathsf{msk}^\star$ supports T_5 encryption queries and T_6 key-generation queries, then the resulting scheme $\mathsf{2FE^{sel}}$ supports $\min\{T_1, T_4, T_5\}$ encryption queries with respect to index $\mathsf{i} = 1$, $\min\{T_3, T_5\}$ encryption queries with respect to index $\mathsf{i} = 2$ and $\min\{T_2, T_6\}$ key-generation queries. When the polynomials $T_1, \ldots, T_6$ are known in advance (i.e., do not depend on the adversary), such schemes are known to exist based on the LWE assumption or even only one-way functions (see Section 2.2 for a more elaborated discussion of the existing schemes).

Proof of Theorem 3.1. Let $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ be a valid adversary that issues at most $T_1 = T_1(\lambda)$ encryption queries with respect to index $\mathsf{i} = 1$, at most $T_2 = T_2(\lambda)$ encryption queries with respect to index $\mathsf{i} = 2$, and at most $T_3 = T_3(\lambda)$ key-generation queries (note that T_1, T_2, and T_3 may be any polynomials and are not fixed in advance). We assume for simplicity and without loss of generality that $T_1 = T_2 = T_3 \stackrel{\mathsf{def}}{=} T$.

We present a sequence of experiments and upper bound $\mathcal{A}$'s advantage in distinguishing each two consecutive experiments. The first experiment is the experiment $\mathsf{Exp}^{\mathsf{sel2FE}}_{\mathsf{2FE^{sel}},\mathcal{F},\mathcal{A}}(\lambda)$ (see Definition 2.8), and the last experiment is completely independent of the bit b. This enables us to prove that there exists a negligible function $\mathsf{neg}(\cdot)$ such that

$$\mathsf{Adv}^{\mathsf{sel2FE}}_{\mathsf{2FE^{sel}},\mathcal{F},\mathcal{A}}(\lambda) \stackrel{\mathsf{def}}{=} \left| \Pr\left[\mathsf{Exp}^{\mathsf{sel2FE}}_{\mathsf{2FE^{sel}},\mathcal{F},\mathcal{A}}(\lambda) = 1\right] - \frac{1}{2} \right| \le \mathsf{neg}(\lambda)$$

for all sufficiently large $\lambda \in \mathbb{N}$. In what follows we first describe the notation used throughout the proof, and then describe the experiments.

Notation. We denote the i^{th} ciphertext with respect to $\mathsf{i} = 1$ by $(\mathsf{sk}_{1,i}, \mathsf{ct}_{1,i})$ and the i^{th} ciphertext with respect to $\mathsf{i} = 2$ by $\mathsf{ct}_{2,i}$. We denote the i^{th} input pair corresponding to the index $\mathsf{i} = 1$ by (x_i^0, x_i^1), the random strings used for generating the resulting $\mathsf{sk}_{1,i}$ by s_i, the master secret key and the PRF key used for generating the resulting $\mathsf{ct}_{1,i}$ and $\mathsf{sk}_{1,i}$ by $\mathsf{msk}_i^\star$ and K_i, respectively. We denote the i^{th} input pair corresponding to the index $\mathsf{i} = 2$ by (y_i^0, y_i^1), and the randomness used for generating the resulting $\mathsf{ct}_{2,i}$ by t_i. Finally, we denote by $(f_1^0, f_1^1), \ldots, (f_T^0, f_T^1)$ the function pairs with which the adversary queries the key-generation oracle and by $z_1, \ldots, z_T$ the corresponding random strings used for generating $\mathsf{sk}_{f_1}, \ldots, \mathsf{sk}_{f_T}$.

Experiment $\boldsymbol{\mathcal{H}^{(0)}(\lambda)}$. This is the original experiment corresponding to $b \leftarrow \{0, 1\}$ chosen uniformly at random, namely, $\mathsf{Exp}^{\mathsf{sel2FE}}_{\mathsf{2FE^{sel}},\mathcal{F},\mathcal{A}}(\lambda)$. In this experiment the encryptions are generated as follows.

- Ciphertexts $(i = 1, \ldots, T)$:

$$\begin{aligned}
\mathsf{ct}_{1,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk_{out}}, (\mathsf{msk}_i^\star, K_i, 0)) \\
\mathsf{sk}_{1,i} &\leftarrow \mathsf{1FE.KG}(\mathsf{msk_{in}}, \mathsf{AGG}_{x_i^b,\perp,0,s_i,\mathsf{msk}_i^\star,K_i}) \\
\mathsf{ct}_{2,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk_{in}}, (y_i^b, \perp, t_i, \perp, \perp))
\end{aligned}$$

- Functional keys ($i = 1, \ldots, T$):

$$\mathsf{sk}_{f_i} \leftarrow \mathsf{1FE.KG}(\mathsf{msk_{out}}, D_{f_i^b,\perp,z_i,\perp})$$

Experiment $\mathcal{H}^{(1)}(\lambda)$. This experiment is obtained from the experiment $\mathcal{H}^{(0)}(\lambda)$ by modifying the encryptions as follows. Given inputs (x_i^0, x_i^1) and (y_i^0, y_i^1), instead of setting the field x_1 and y_1 to be $\perp$ we set it to be x_i^1 and y_i^1, respectively. The scheme has the following form:

- Ciphertexts ($i = 1, \ldots, T$):

$$\begin{aligned}
\mathsf{ct}_{1,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk_{out}}, (\mathsf{msk}_i^\star, K_i, 0)) \\
\mathsf{sk}_{1,i} &\leftarrow \mathsf{1FE.KG}(\mathsf{msk_{in}}, \mathsf{AGG}_{x_i^b, \boxed{x_i^1}, 0, s_i, \mathsf{msk}_i^\star, K_i}) \\
\mathsf{ct}_{2,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk_{in}}, (y_i^b, \boxed{y_i^1}, t_i, \perp, \perp))
\end{aligned}$$

- Functional keys ($i = 1, \ldots, T$):

$$\mathsf{sk}_{f_i} \leftarrow \mathsf{1FE.KG}(\mathsf{msk_{out}}, D_{f_i^b,\perp,z_i,\perp})$$

Note that all the tokens that are issued as part of the encryption according to $\mathsf{i} = 1$ are generated with $a = 0$ (where a is the third hardwired item). Thus, the circuit $\mathsf{AGG}_{x_0,x_1,a,s,\mathsf{msk}^\star,K}$ always sets $x = x_i^b$ and $y = y_i^b$ and ignores x_i^1 and y_i^1 (see Figure 2). Thus, the security the underlying scheme $\mathsf{1FE}$ guarantees that the adversary $\mathcal{A}$ has only a negligible advantage in distinguishing experiments $\mathcal{H}^{(0)}$ and $\mathcal{H}^{(1)}$. Specifically, let $\mathcal{F}'$ denote the family of functions $\mathsf{AGG}_{x_0,x_1,a,s,\mathsf{msk}^\star,K}$ (as defined in Figure 2). In Appendix B.1 we prove the following claim:

Claim 3.2. *There exists a probabilistic polynomial-time adversary $\mathcal{B}^{(0)\to(1)}$ such that*

$$\left|\Pr\left[\mathcal{H}^{(0)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(1)}(\lambda) = 1\right]\right| \leq \mathsf{Adv}^{\mathsf{full1FE}}_{\mathsf{1FE},\mathcal{F}',\mathcal{B}^{(0)\to(1)}}(\lambda).$$

Experiment $\mathcal{H}^{(2)}(\lambda)$. This experiment is obtained from the experiment $\mathcal{H}^{(1)}(\lambda)$ by modifying the functional keys as follows. Given inputs (f^0, f^1), instead of setting the fields f_1, f_2 to be $f^b, \perp$ we set it to be f^b, f^1. The scheme has the following form:

- Ciphertexts ($i = 1, \ldots, T$):

$$\begin{aligned}
\mathsf{ct}_{1,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk_{out}}, (\mathsf{msk}_i^\star, K_i, 0)) \\
\mathsf{sk}_{1,i} &\leftarrow \mathsf{1FE.KG}(\mathsf{msk_{in}}, \mathsf{AGG}_{x_i^b, x_i^1, 0, s_i, \mathsf{msk}_i^\star, K_i}) \\
\mathsf{ct}_{2,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk_{in}}, (y_i^b, y_i^1, t_i, \perp, \perp))
\end{aligned}$$

- Functional keys ($i = 1, \ldots, T$):

$$\mathsf{sk}_{f_i} \leftarrow \mathsf{1FE.KG}(\mathsf{msk_{out}}, D_{f_i^b, \boxed{f_i^1}, z_i, \perp})$$

Note that all the ciphertexts that are issued as part of the encryption according to $\mathsf{i} = 1$ are generated with $w = 0$ (where w is the third hardwired item in ct_1). Thus, the circuit $D_{f_0,f_1,z_i,u}$ always sets $f = f_i^b$ and ignores f_i^1 (see Figure 1). Thus, the security the underlying scheme $\mathsf{1FE}$ (with respect to $\mathsf{msk_{out}}$) guarantees that the adversary $\mathcal{A}$ has only a negligible advantage in distinguishing experiments $\mathcal{H}^{(1)}$ and $\mathcal{H}^{(2)}$. Specifically, let $\mathcal{F}''$ denote the family of functions $D_{f_0,f_1,z_i,u}$ (as defined in Figure 1). In Appendix B.1 we prove the following claim:

Claim 3.3. *There exists a probabilistic polynomial-time adversary $\mathcal{B}^{(1)\to(2)}$ such that*

$$\left|\Pr\left[\mathcal{H}^{(1)}(\lambda)=1\right]-\Pr\left[\mathcal{H}^{(2)}(\lambda)=1\right]\right|\leq \mathsf{Adv}^{\mathsf{full1FE}}_{\mathsf{1FE},\mathcal{F}'',\mathcal{B}^{(1)\to(2)}}(\lambda).$$

Experiment $\mathcal{H}^{(3,j)}(\lambda)$. This experiment is obtained from the experiment $\mathcal{H}^{(2)}(\lambda)$ by modifying the encryptions as follows. The first $j-1$ ciphertexts are generated such that $a=1$ and $w=1$ while the rest of the encryptions are generated as before.

- Ciphertexts $(i=1,\dots,j-1)$:

$$\begin{aligned}
\mathsf{ct}_{1,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk}_{\mathsf{out}},(\mathsf{msk}^\star_i,K_i,\boxed{1}))\\
\mathsf{sk}_{1,i} &\leftarrow \mathsf{1FE.KG}(\mathsf{msk}_{\mathsf{in}},\mathsf{AGG}_{x_i^b,x_i^1,\boxed{1},s_i,\mathsf{msk}^\star_i,K_i})\\
\mathsf{ct}_{2,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk}_{\mathsf{in}},(y_i^b,y_i^1,t_i,\perp,\perp))
\end{aligned}$$

- Ciphertexts $(i=j,\dots,T)$:

$$\begin{aligned}
\mathsf{ct}_{1,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk}_{\mathsf{out}},(\mathsf{msk}^\star_i,K_i,0))\\
\mathsf{sk}_{1,i} &\leftarrow \mathsf{1FE.KG}(\mathsf{msk}_{\mathsf{in}},\mathsf{AGG}_{x_i^b,x_i^1,0,s_i,\mathsf{msk}^\star_i,K_i})\\
\mathsf{ct}_{2,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk}_{\mathsf{in}},(y_i^b,y_i^1,t_i,\perp,\perp))
\end{aligned}$$

- Functional keys $(i=1,\dots,T)$:

$$\mathsf{sk}_{f_i}\leftarrow \mathsf{1FE.KG}(\mathsf{msk}_{\mathsf{out}},D_{f_i^b,f_i^1,z_i,\perp})$$

Notice that $\mathcal{H}^{(3,1)}=\mathcal{H}^{(2)}$.

Experiment $\mathcal{H}^{(4,j)}(\lambda)$. This experiment is obtained from the experiment $\mathcal{H}^{(3,j)}(\lambda)$ by modifying the j^{th} ciphertext to *not* include the master secret key $\mathsf{msk}^\star_j$ and the PRF key K_j (that is, we replace them with $\perp$'s). Moreover, for every $i\in[T]$ in the i^{th} ciphertext corresponding to $\mathsf{i}=2$ we hardwire the pair (s_j,γ_i), where $\gamma_i=\mathsf{1FE.E}(\mathsf{msk}^\star_j,(x_j^b,y_i^b);\mathsf{PRF.Eval}(K_j,t_i))$.

- Ciphertexts $(i=1,\dots,j-1)$:

$$\begin{aligned}
\mathsf{ct}_{1,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk}_{\mathsf{out}},(\mathsf{msk}^\star_i,K_i,1))\\
\mathsf{sk}_{1,i} &\leftarrow \mathsf{1FE.KG}(\mathsf{msk}_{\mathsf{in}},\mathsf{AGG}_{x_i^b,x_i^1,1,s_i,\mathsf{msk}^\star_i,K_i})\\
\mathsf{ct}_{2,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk}_{\mathsf{in}},(y_i^b,x_i^1,t_i,\boxed{s_j,\gamma_i}))\\
\gamma_i &= \mathsf{1FE.E}(\mathsf{msk}^\star_j,(x_j^b,y_i^b);\mathsf{PRF.Eval}(K_j,t_i))
\end{aligned}$$

- Ciphertext $(i=j)$:

$$\begin{aligned}
\mathsf{ct}_{1,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk}_{\mathsf{out}},(\mathsf{msk}^\star_i,K_i,0))\\
\mathsf{sk}_{1,i} &\leftarrow \mathsf{1FE.KG}(\mathsf{msk}_{\mathsf{in}},\mathsf{AGG}_{x_i^b,x_i^1,0,s_i,\boxed{\perp},\boxed{\perp}})\\
\mathsf{ct}_{2,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk}_{\mathsf{in}},(y_i^b,y_i^1,t_i,\boxed{s_j,\gamma_i}))\\
\gamma_i &= \mathsf{1FE.E}(\mathsf{msk}^\star_j,(x_j^b,y_i^b);\mathsf{PRF.Eval}(K_j,t_i))
\end{aligned}$$

- Ciphertexts ($i = j+1, \dots, T$):

$$\begin{aligned}\mathsf{ct}_{1,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk}_{\mathsf{out}}, (\mathsf{msk}_i^\star, K_i, 0))\\ \mathsf{sk}_{1,i} &\leftarrow \mathsf{1FE.KG}(\mathsf{msk}_{\mathsf{in}}, \mathsf{AGG}_{x_i^b, x_i^1, 0, s_i, \mathsf{msk}_i^\star, K_i})\\ \mathsf{ct}_{2,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk}_{\mathsf{in}}, (y_i^b, y_i^1, t_i, \boxed{s_j, \gamma_i}))\\ &\gamma_i = \mathsf{1FE.E}(\mathsf{msk}_j^\star, (x_j^b, y_i^b); \mathsf{PRF.Eval}(K_j, t_i))\end{aligned}$$

- Functional keys ($i = 1, \dots, T$):

$$\mathsf{sk}_{f_i} \leftarrow \mathsf{1FE.KG}(\mathsf{msk}_{\mathsf{out}}, D_{f_i^b, f_i^1, z_i, \perp})$$

We observe that the only combinations that are affected by this change are combinations that include the j^{th} ciphertext corresponding to $\mathsf{i} = 1$. However, using the hardwired values γ_i for $i \in [T]$ the functionalities stay the same. Thus, the security of the underlying $\mathsf{1FE}$ scheme guarantees that the adversary $\mathcal{A}$ has only a negligible advantage in distinguishing experiments $\mathcal{H}^{(3,j)}$ and $\mathcal{H}^{(4,j)}$. In Appendix B.1 we prove the following claim:

Claim 3.4. *There exists a probabilistic polynomial-time adversary $\mathcal{B}^{(3,j)\to(4,j)}$ such that*

$$\left|\Pr\left[\mathcal{H}^{(3,j)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(4,j)}(\lambda) = 1\right]\right| \le \mathsf{Adv}^{\mathsf{full1FE}}_{\mathsf{1FE}, \mathcal{F}', \mathcal{B}^{(3,j)\to(4,j)}}(\lambda).$$

Experiment $\mathcal{H}^{(5,j)}(\lambda)$. This experiment is obtained from the experiment $\mathcal{H}^{(4,j)}(\lambda)$ by modifying the j^{th} ciphertext as follows. We replace $(\mathsf{msk}_j^\star, K_j, 0)$ with $(\perp, \perp, 0)$. Moreover, in the i^{th} functional key corresponding to the functions (f_i^0, f_i^1) we hardwire the value $\delta_i = \mathsf{1FE.KG}(\mathsf{msk}_j^\star, C_{f_i^b};$ $\mathsf{PRF.Eval}(K_j, z_i))$.

- Ciphertexts ($i = 1, \dots, j-1$):

$$\begin{aligned}\mathsf{ct}_{1,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk}_{\mathsf{out}}, (\mathsf{msk}_i^\star, K_i, 1))\\ \mathsf{sk}_{1,i} &\leftarrow \mathsf{1FE.KG}(\mathsf{msk}_{\mathsf{in}}, \mathsf{AGG}_{x_i^b, x_i^1, 1, s_i, \mathsf{msk}_i^\star, K_i})\\ \mathsf{ct}_{2,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk}_{\mathsf{in}}, (y_i^b, y_i^1, t_i, s_j, \gamma_i))\\ &\gamma_i = \mathsf{1FE.E}(\mathsf{msk}_j^\star, (x_j^b, y_i^b); \mathsf{PRF.Eval}(K_j, t_i))\end{aligned}$$

- Ciphertext ($i = j$):

$$\begin{aligned}\mathsf{ct}_{1,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk}_{\mathsf{out}}, (\boxed{\perp, \perp}, 0))\\ \mathsf{sk}_{1,i} &\leftarrow \mathsf{1FE.KG}(\mathsf{msk}_{\mathsf{in}}, \mathsf{AGG}_{x_i^b, x_i^1, 0, s_i, \perp, \perp})\\ \mathsf{ct}_{2,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk}_{\mathsf{in}}, (y_i^b, y_i^1, t_i, s_j, \gamma_i))\\ &\gamma_i = \mathsf{1FE.E}(\mathsf{msk}_j^\star, (x_j^b, y_i^b); \mathsf{PRF.Eval}(K_j, t_i))\end{aligned}$$

- Ciphertexts ($i = j+1, \dots, T$):

$$\begin{aligned}\mathsf{ct}_{1,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk}_{\mathsf{out}}, (\mathsf{msk}_i^\star, K_i, 0))\\ \mathsf{sk}_{1,i} &\leftarrow \mathsf{1FE.KG}(\mathsf{msk}_{\mathsf{in}}, \mathsf{AGG}_{x_i^b, x_i^1, 0, s_i, \mathsf{msk}_i^\star, K_i})\\ \mathsf{ct}_{2,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk}_{\mathsf{in}}, (y_i^b, y_i^1, t_i, s_j, \gamma_i))\\ &\gamma_i = \mathsf{1FE.E}(\mathsf{msk}_j^\star, (x_j^b, y_i^b); \mathsf{PRF.Eval}(K_j, t_i))\end{aligned}$$

- Functional keys ($i = 1, \ldots, T$):

$$\mathsf{sk}_{f_i} \leftarrow \mathsf{1FE.KG}(\mathsf{msk}_{\mathsf{out}}, D_{f_i^b, f_i^1, z_i, \boxed{\delta_i}})$$
$$\delta_i = \mathsf{1FE.KG}(\mathsf{msk}_j^\star, C_{f_i^b}; \mathsf{PRF.Eval}(K_j, z_i))$$

We observe that the only combinations that are affected by this change are combinations that include the j^{th} ciphertext corresponding to $\mathsf{i} = 1$. However, using the hardwired value δ the functionality stays the same. Thus, the security of the underlying scheme 1FE guarantees that the adversary $\mathcal{A}$ has only a negligible advantage in distinguishing experiments $\mathcal{H}^{(4,j)}$ and $\mathcal{H}^{(5,j)}$. In Appendix B.1 we prove the following claim:

Claim 3.5. *There exists a probabilistic polynomial-time adversary $\mathcal{B}^{(4,j)\to(5,j)}$ such that*

$$\left|\Pr\left[\mathcal{H}^{(4,j)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(5,j)}(\lambda) = 1\right]\right| \leq \mathsf{Adv}^{\mathsf{full1FE}}_{\mathsf{1FE},\mathcal{F}',\mathcal{B}^{(4,j)\to(5,j)}}(\lambda).$$

Experiment $\mathcal{H}^{(6,j)}(\lambda)$. This experiment is obtained from the experiment $\mathcal{H}^{(5,j)}(\lambda)$ by modifying the hardwired value $\gamma_1, \ldots, \gamma_T$ and $\delta_1, \ldots, \delta_T$ to use randomness sampled uniformly at random rather than randomness generated using a PRF.

- Ciphertexts ($i = 1, \ldots, j-1$):

$$\mathsf{ct}_{1,i} \leftarrow \mathsf{1FE.E}(\mathsf{msk}_{\mathsf{out}}, (\mathsf{msk}_i^\star, K_i, 1))$$
$$\mathsf{sk}_{1,i} \leftarrow \mathsf{1FE.KG}(\mathsf{msk}_{\mathsf{in}}, \mathsf{AGG}_{x_i^b, x_i^1, 1, s_i, \mathsf{msk}_i^\star, K_i})$$
$$\mathsf{ct}_{2,i} \leftarrow \mathsf{1FE.E}(\mathsf{msk}_{\mathsf{in}}, (y_i^b, y_i^1, t_i, s_j, \gamma_i))$$
$$\boxed{\gamma_i} = \mathsf{1FE.E}(\mathsf{msk}_j^\star, (x_j^b, y_i^b))$$

- Ciphertext ($i = j$):

$$\mathsf{ct}_{1,i} \leftarrow \mathsf{1FE.E}(\mathsf{msk}_{\mathsf{out}}, (\perp, \perp, 0))$$
$$\mathsf{sk}_{1,i} \leftarrow \mathsf{1FE.KG}(\mathsf{msk}_{\mathsf{in}}, \mathsf{AGG}_{x_i^b, x_i^1, 0, s_i, \perp, \perp})$$
$$\mathsf{ct}_{2,i} \leftarrow \mathsf{1FE.E}(\mathsf{msk}_{\mathsf{in}}, (y_i^b, y_i^1, t_i, s_j, \gamma_i))$$
$$\boxed{\gamma_i} = \mathsf{1FE.E}(\mathsf{msk}_j^\star, (x_j^b, y_i^b))$$

- Ciphertexts ($i = j+1, \ldots, T$):

$$\mathsf{ct}_{1,i} \leftarrow \mathsf{1FE.E}(\mathsf{msk}_{\mathsf{out}}, (\mathsf{msk}_i^\star, K_i, 0))$$
$$\mathsf{sk}_{1,i} \leftarrow \mathsf{1FE.KG}(\mathsf{msk}_{\mathsf{in}}, \mathsf{AGG}_{x_i^b, x_i^1, 0, s_i, \mathsf{msk}_i^\star, K_i})$$
$$\mathsf{ct}_{2,i} \leftarrow \mathsf{1FE.E}(\mathsf{msk}_{\mathsf{in}}, (y_i^b, y_i^1, t_i, s_j, \gamma_i))$$
$$\boxed{\gamma_i} = \mathsf{1FE.E}(\mathsf{msk}_j^\star, (x_j^b, y_i^b))$$

- Functional keys ($i = 1, \ldots, T$):

$$\mathsf{sk}_{f_i} \leftarrow \mathsf{1FE.KG}(\mathsf{msk}_{\mathsf{out}}, D_{f_i^b, f_i^1, z_i, \delta_i})$$
$$\boxed{\delta_i} = \mathsf{1FE.KG}(\mathsf{msk}_j^\star, C_{f_i^b})$$

The pseudorandomness of $\mathsf{PRF.Eval}(K_j, \cdot)$ guarantees that the adversary $\mathcal{A}$ has only a negligible advantage in distinguishing experiments $\mathcal{H}^{(5,j)}$ and $\mathcal{H}^{(6,j)}$. In Appendix B.1 we prove the following claim:

Claim 3.6. *For every $j \in [T]$ there exists a probabilistic polynomial-time adversary $\mathcal{B}^{(5,j)\to(6,j)}$ such that*

$$\left|\Pr\left[\mathcal{H}^{(5,j)}(\lambda)=1\right]-\Pr\left[\mathcal{H}^{(6,j)}(\lambda)=1\right]\right| \leq \mathsf{Adv}_{\mathsf{PRF},\mathcal{B}^{(5,j)\to(6,j)}}(\lambda).$$

Experiment $\mathcal{H}^{(7,j)}(\lambda)$. This experiment is obtained from the experiment $\mathcal{H}^{(6,j)}(\lambda)$ by modifying the ciphertext as follows. In the i^{th} ciphertext corresponding to $\mathsf{i}=2$ we embed in γ_i the encryption of (x_j^1, y^1) rather than (x_j^b, y^b). Moreover, we replace the circuit embedded in δ_i in the i^{th} functional key to be $C_{f_i^1}$ rather than $C_{f_i^b}$.

- Ciphertexts $(i=1,\ldots,j-1)$:

$$\begin{aligned}
\mathsf{ct}_{1,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk}_{\mathsf{out}}, (\mathsf{msk}_i^\star, K_i, 1))\\
\mathsf{sk}_{1,i} &\leftarrow \mathsf{1FE.KG}(\mathsf{msk}_{\mathsf{in}}, \mathsf{AGG}_{x_i^b, x_i^1, 1, s_i, \mathsf{msk}_i^\star, K_i})\\
\mathsf{ct}_{2,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk}_{\mathsf{in}}, (y_i^b, y_i^1, t_i, s_j, \gamma_i))\\
\gamma_i &= \mathsf{1FE.E}(\mathsf{msk}_j^\star, \boxed{(x_j^1, y_i^1)})
\end{aligned}$$

- Ciphertext $(i=j)$:

$$\begin{aligned}
\mathsf{ct}_{1,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk}_{\mathsf{out}}, (\perp, \perp, 0))\\
\mathsf{sk}_{1,i} &\leftarrow \mathsf{1FE.KG}(\mathsf{msk}_{\mathsf{in}}, \mathsf{AGG}_{x_i^b, x_i^1, 0, s_i, \perp, \perp})\\
\mathsf{ct}_{2,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk}_{\mathsf{in}}, (y_i^b, y_i^1, t_i, s_j, \gamma_i))\\
\gamma_i &= \mathsf{1FE.E}(\mathsf{msk}_j^\star, \boxed{(x_j^1, y_i^1)})
\end{aligned}$$

- Ciphertexts $(i=j+1,\ldots,T)$:

$$\begin{aligned}
\mathsf{ct}_{1,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk}_{\mathsf{out}}, (\mathsf{msk}_i^\star, K_i, 0))\\
\mathsf{sk}_{1,i} &\leftarrow \mathsf{1FE.KG}(\mathsf{msk}_{\mathsf{in}}, \mathsf{AGG}_{x_i^b, x_i^1, 0, s_i, \mathsf{msk}_i^\star, K_i})\\
\mathsf{ct}_{2,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk}_{\mathsf{in}}, (y_i^b, y_i^1, t_i, s_j, \gamma_i))\\
\gamma_i &= \mathsf{1FE.E}(\mathsf{msk}_j^\star, \boxed{(x_j^1, y_i^1)})
\end{aligned}$$

- Functional keys $(i=1,\ldots,T)$:

$$\begin{aligned}
\mathsf{sk}_{f_i} &\leftarrow \mathsf{1FE.KG}(\mathsf{msk}_{\mathsf{out}}, D_{f_i^b, f_i^1, z_i, \delta_i})\\
\delta_i &= \mathsf{1FE.KG}(\mathsf{msk}_j^\star, \boxed{C_{f_i^1}})
\end{aligned}$$

The above change only affects evaluations that correspond to the combination of any ciphertext corresponding to $\mathsf{i}=2$ with the j^{th} ciphertext corresponding to $\mathsf{i}=1$. Using the fact that the adversary is *valid* (see Definition 2.6), the functionality stays exactly the same. Thus, the security of the underlying scheme $\mathsf{1FE}$ guarantees that the adversary $\mathcal{A}$ has only a negligible advantage in distinguishing experiments $\mathcal{H}^{(6,j)}$ and $\mathcal{H}^{(7,j)}$. In Appendix B.1 we prove the following claim:

Claim 3.7. *There exists a probabilistic polynomial-time adversary $\mathcal{B}^{(6,j)\to(7,j)}$ such that*

$$\left|\Pr\left[\mathcal{H}^{(6,j)}(\lambda)=1\right]-\Pr\left[\mathcal{H}^{(7,j)}(\lambda)=1\right]\right| \leq \mathsf{Adv}^{\mathsf{full1FE}}_{\mathsf{1FE},\mathcal{F}',\mathcal{B}^{(6,j)\to(7,j)}}(\lambda).$$

Experiment $\mathcal{H}^{(8,j)}(\lambda)$. This experiment is obtained from the experiment $\mathcal{H}^{(7,j)}(\lambda)$ by modifying the hardwired values $\gamma_1, \ldots, \gamma_T$ and $\delta_1, \ldots, \delta_T$ to use randomness generated using a PRF rather than randomness sampled uniformly at random.

- Ciphertexts ($i = 1, \ldots, j-1$):

$$\begin{aligned}
\mathsf{ct}_{1,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk_{out}}, (\mathsf{msk}_i^\star, K_i, 1)) \\
\mathsf{sk}_{1,i} &\leftarrow \mathsf{1FE.KG}(\mathsf{msk_{in}}, \mathsf{AGG}_{x_i^b, x_i^1, 1, s_i, \mathsf{msk}_i^\star, K_i}) \\
\mathsf{ct}_{2,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk_{in}}, (y_i^b, y_i^1, t_i, s_j, \gamma_i)) \\
\boxed{\gamma_i} &= \mathsf{1FE.E}(\mathsf{msk}_j^\star, (x_j^1, y_i^1); \mathsf{PRF.Eval}(K_j, t_i))
\end{aligned}$$

- Ciphertext ($i = j$):

$$\begin{aligned}
\mathsf{ct}_{1,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk_{out}}, (\perp, \perp, 0)) \\
\mathsf{sk}_{1,i} &\leftarrow \mathsf{1FE.KG}(\mathsf{msk_{in}}, \mathsf{AGG}_{x_i^b, x_i^1, 0, s_i, \perp, \perp}) \\
\mathsf{ct}_{2,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk_{in}}, (y_i^b, y_i^1, t_i, s_j, \gamma_i)) \\
\boxed{\gamma_i} &= \mathsf{1FE.E}(\mathsf{msk}_j^\star, (x_j^1, y_i^1); \mathsf{PRF.Eval}(K_j, t_i))
\end{aligned}$$

- Ciphertexts ($i = j+1, \ldots, T$):

$$\begin{aligned}
\mathsf{ct}_{1,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk_{out}}, (\mathsf{msk}_i^\star, K_i, 0)) \\
\mathsf{sk}_{1,i} &\leftarrow \mathsf{1FE.KG}(\mathsf{msk_{in}}, \mathsf{AGG}_{x_i^b, x_i^1, 0, s_i, \mathsf{msk}_i^\star, K_i}) \\
\mathsf{ct}_{2,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk_{in}}, (y_i^b, y_i^1, t_i, s_j, \gamma_i)) \\
\boxed{\gamma_i} &= \mathsf{1FE.E}(\mathsf{msk}_j^\star, (x_j^1, y_i^1); \mathsf{PRF.Eval}(K_j, t_i))
\end{aligned}$$

- Functional keys ($i = 1, \ldots, T$):

$$\begin{aligned}
\mathsf{sk}_{f_i} &\leftarrow \mathsf{1FE.KG}(\mathsf{msk_{out}}, D_{f_i^b, f_i^1, z_i, \delta_i}) \\
\boxed{\delta_i} &= \mathsf{1FE.KG}(\mathsf{msk}_j^\star, C_{f_i^1}; \mathsf{PRF.Eval}(K_j, z_i))
\end{aligned}$$

The pseudorandomness of $\mathsf{PRF.Eval}(K_j, \cdot)$ guarantees that the adversary $\mathcal{A}$ has only a negligible advantage in distinguishing experiments $\mathcal{H}^{(7,j)}$ and $\mathcal{H}^{(8,j)}$. The proof of the following claim is analogous to the proof of Claim 3.5.

Claim 3.8. *There exists a probabilistic polynomial-time adversary $\mathcal{B}^{(7,j)\to(8,j)}$ such that*

$$\left| \Pr\left[\mathcal{H}^{(7,j)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(8,j)}(\lambda) = 1\right] \right| \leq \mathsf{Adv}_{\mathsf{PRF}, \mathcal{B}^{(7,j)\to(8,j)}}(\lambda).$$

Experiment $\mathcal{H}^{(9,j)}(\lambda)$. This experiment is obtained from the experiment $\mathcal{H}^{(8,j)}(\lambda)$ by modifying the j^{th} ciphertext to contain the pair $(\mathsf{msk}_j^\star, K_j)$. Moreover, in the functional key corresponding to the function f_i for $i \in [T]$ we remove the hardwired value δ_i.

- Ciphertexts ($i = 1, \ldots, j-1$):

$$\begin{aligned}
\mathsf{ct}_{1,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk_{out}}, (\mathsf{msk}_i^\star, K_i)) \\
\mathsf{sk}_{1,i} &\leftarrow \mathsf{1FE.KG}(\mathsf{msk_{in}}, \mathsf{AGG}_{x_i^b, x_i^1, 1, s_i, \mathsf{msk}_i^\star, K_i}) \\
\mathsf{ct}_{2,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk_{in}}, (y_i^b, y_i^1, t_i, s_j, \gamma_i)) \\
\gamma_i &= \mathsf{1FE.E}(\mathsf{msk}_j^\star, (x_j^1, y_i^1); \mathsf{PRF.Eval}(K_j, t_i))
\end{aligned}$$

- Ciphertext $(i = j)$:

$$\begin{aligned}
\mathsf{ct}_{1,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk}_{\mathsf{out}}, (\boxed{\mathsf{msk}_i^\star, K_i, 1})) \\
\mathsf{sk}_{1,i} &\leftarrow \mathsf{1FE.KG}(\mathsf{msk}_{\mathsf{in}}, \mathsf{AGG}_{x_i^b, x_i^1, 0, s_i, \perp, \perp}) \\
\mathsf{ct}_{2,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk}_{\mathsf{in}}, (y_i^b, y_i^1, t_i, s_j, \gamma_i)) \\
&\quad \gamma_i = \mathsf{1FE.E}(\mathsf{msk}_j^\star, (x_j^1, y_i^1); \mathsf{PRF.Eval}(K_j, t_i))
\end{aligned}$$

- Ciphertexts $(i = j+1, \ldots, T)$:

$$\begin{aligned}
\mathsf{ct}_{1,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk}_{\mathsf{out}}, (\mathsf{msk}_i^\star, K_i)) \\
\mathsf{sk}_{1,i} &\leftarrow \mathsf{1FE.KG}(\mathsf{msk}_{\mathsf{in}}, \mathsf{AGG}_{x_i^b, x_i^1, 0, s_i, \mathsf{msk}_i^\star, K_i}) \\
\mathsf{ct}_{2,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk}_{\mathsf{in}}, (y_i^b, y_i^1, t_i, s_j, \gamma_i)) \\
&\quad \gamma_i = \mathsf{1FE.E}(\mathsf{msk}_j^\star, (x_j^1, y_i^1); \mathsf{PRF.Eval}(K_j, t_i))
\end{aligned}$$

- Functional keys $(i = 1, \ldots, T)$:

$$\mathsf{sk}_{f_i} \leftarrow \mathsf{1FE.KG}(\mathsf{msk}_{\mathsf{out}}, D_{f_i^b, f_i^1, z_i, \boxed{\perp}})$$

We observe that the only combinations that are affected by this change are combinations that include the j^{th} ciphertext corresponding to $\mathsf{i} = 1$. However, using the fact that we replace $(\perp, \perp)$ in $\mathsf{ct}_{1,j}$ with $(\mathsf{msk}_j^\star, K_j)$ and remove the hardwired values δ_i the functionality stays the same. Thus, the security of the underlying scheme $\mathsf{1FE}$ guarantees that the adversary $\mathcal{A}$ has only a negligible advantage in distinguishing experiments $\mathcal{H}^{(8,j)}$ and $\mathcal{H}^{(9,j)}$. The proof of the following claim is analogous to the proof of Claim 3.4.

Claim 3.9. *There exists a probabilistic polynomial-time adversary $\mathcal{B}^{(8,j)\to(9,j)}$ such that*

$$\left|\Pr\left[\mathcal{H}^{(8,j)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(9,j)}(\lambda) = 1\right]\right| \leq \mathsf{Adv}^{\mathsf{full1FE}}_{\mathsf{1FE},\mathcal{F}',\mathcal{B}^{(8,j)\to(9,j)}}(\lambda).$$

Experiment $\mathcal{H}^{(10,j)}(\lambda)$. This experiment is obtained from the experiment $\mathcal{H}^{(9,j)}(\lambda)$ by modifying the ciphertexts as follows. For the i^{th} ciphertext corresponding to $\mathsf{i} = 2$ we remove the hardwired pair (s_j, γ_i). Moreover, we encrypt the j^{th} ciphertext corresponding to $\mathsf{i} = 1$ with $2 = 1$. Notice that $\mathcal{H}^{(10,j)} = \mathcal{H}^{(3,j+1)}$.

- Ciphertexts $(i = 1, \ldots, \boxed{j})$:

$$\begin{aligned}
\mathsf{ct}_{1,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk}_{\mathsf{out}}, (\mathsf{msk}_i^\star, K_i, 1)) \\
\mathsf{sk}_{1,i} &\leftarrow \mathsf{1FE.KG}(\mathsf{msk}_{\mathsf{in}}, \mathsf{AGG}_{x_i^b, x_i^1, 1, s_i, \mathsf{msk}_i^\star, K_i}) \\
\mathsf{ct}_{2,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk}_{\mathsf{in}}, (y_i^b, y_i^1, t_i, \boxed{\perp, \perp}))
\end{aligned}$$

- Ciphertexts $(i = j+1, \ldots, T)$:

$$\begin{aligned}
\mathsf{ct}_{1,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk}_{\mathsf{out}}, (\mathsf{msk}_i^\star, K_i, 0)) \\
\mathsf{sk}_{1,i} &\leftarrow \mathsf{1FE.KG}(\mathsf{msk}_{\mathsf{in}}, \mathsf{AGG}_{x_i^b, x_i^1, 0, s_i, \mathsf{msk}_i^\star, K_i}) \\
\mathsf{ct}_{2,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk}_{\mathsf{in}}, (y_i^b, y_i^1, t_i, \boxed{\perp, \perp}))
\end{aligned}$$

- Functional keys ($i = 1, \ldots, T$):

$$\mathsf{sk}_{f_i} \leftarrow \mathsf{1FE.KG}(\mathsf{msk_{out}}, D_{f_i^b, f_i^1, z_i, \perp})$$

We observe that the only combinations that are affected by this change are combinations that include the j^{th} ciphertext corresponding to $\mathsf{i} = 1$. However, since the hardwired values γ_i for $i \in [T] \cup \{0\}$ preserved the functionalities when $a = 1$ for the j^{th} ciphertext, when we remove them and add back $\mathsf{msk}_j^\star$ and K_j the functionalities stay the same. Thus, the security of the underlying scheme $\mathsf{1FE}$ guarantees that the adversary $\mathcal{A}$ has only a negligible advantage in distinguishing experiments $\mathcal{H}^{(9,j)}$ and $\mathcal{H}^{(10,j)}$. The proof of the following claim is analogous to the proof of Claim 3.4.

Claim 3.10. *There exists a probabilistic polynomial-time adversary $\mathcal{B}^{(9,j)\to(10,j)}$ such that*

$$\left|\Pr\left[\mathcal{H}^{(9,j)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(10,j)}(\lambda) = 1\right]\right| \leq \mathsf{Adv}^{\mathsf{full1FE}}_{\mathsf{1FE},\mathcal{F}',\mathcal{B}^{(9,j)\to(10,j)}}(\lambda).$$

Experiment $\mathcal{H}^{(11)}(\lambda)$. This experiment is obtained from the experiment $\mathcal{H}^{(3,T+1)}(\lambda)$ by modifying the ciphertexts *not* to include f_i^b at all.

- Ciphertexts ($i = 1, \ldots, T$):

$$\begin{aligned}
\mathsf{ct}_{1,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk_{out}}, (\mathsf{msk}_i^\star, K_i, 1)) \\
\mathsf{sk}_{1,i} &\leftarrow \mathsf{1FE.KG}(\mathsf{msk_{in}}, \mathsf{AGG}_{x_i^b, x_i^1, 1, s_i, \mathsf{msk}_i^\star, K_i}) \\
\mathsf{ct}_{2,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk_{in}}, (y_i^b, y_i^1, t_i, \perp, \perp))
\end{aligned}$$

- Functional keys ($i = 1, \ldots, T$):

$$\mathsf{sk}_{f_i} \leftarrow \mathsf{1FE.KG}(\mathsf{msk_{out}}, D_{\boxed{\perp}, f_i^1, z_i, \perp})$$

We observe that at this point all ciphertext have $w = 1$. Therefore, the first parameter f_i^b is always ignored and the functionalities stay the same. Thus, the security of the underlying $\mathsf{1FE}$ scheme guarantees that the adversary $\mathcal{A}$ has only a negligible advantage in distinguishing experiments $\mathcal{H}^{(3,T+1)}$ and $\mathcal{H}^{(11)}$. The proof of the following claim is analogous to the proof of Claim 3.3.

Claim 3.11. *There exists a probabilistic polynomial-time adversary $\mathcal{B}^{(3,T+1)\to(11)}$ such that*

$$\left|\Pr\left[\mathcal{H}^{(3,T+1)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(11)}(\lambda) = 1\right]\right| \leq \mathsf{Adv}^{\mathsf{full1FE}}_{\mathsf{1FE},\mathcal{F}',\mathcal{B}^{(3,T+1)\to(11)}}(\lambda).$$

Experiment $\mathcal{H}^{(12)}(\lambda)$. This experiment is obtained from the experiment $\mathcal{H}^{(11)}(\lambda)$ by modifying the ciphertexts *not* to include x_i^b and y_i^b at all. Notice that this experiment is completely independent of the bit b, and therefore $\Pr[\mathcal{H}^{(12)}(\lambda) = 1] = 1/2$.

- Ciphertexts ($i = 1, \ldots, T$):

$$\begin{aligned}
\mathsf{ct}_{1,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk_{out}}, (\mathsf{msk}_i^\star, K_i, 1)) \\
\mathsf{sk}_{1,i} &\leftarrow \mathsf{1FE.KG}(\mathsf{msk_{in}}, \mathsf{AGG}_{\boxed{\perp}, x_i^1, 1, s_i, \mathsf{msk}_i^\star, K_i}) \\
\mathsf{ct}_{2,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk_{in}}, (\boxed{\perp}, y_i^1, t_i, \perp, \perp))
\end{aligned}$$

- Functional keys ($i = 1, \ldots, T$):

$$\mathsf{sk}_{f_i} \leftarrow \mathsf{1FE.KG}(\mathsf{msk}_{\mathsf{out}}, D_{\perp, f_i^1, z_i, \perp})$$

We observe that at this point all ciphertext have $w = 1$. Therefore, the first parameters f_i^b are always ignored and the functionalities stay the same. Thus, the security of the underlying 1FE scheme guarantees that the adversary $\mathcal{A}$ has only a negligible advantage in distinguishing experiments $\mathcal{H}^{(11)}$ and $\mathcal{H}^{(12)}$. The proof of the following claim is analogous to the proof of Claim 3.2.

Claim 3.12. *There exists a probabilistic polynomial-time adversary $\mathcal{B}^{(11)\to(12)}$ such that*

$$\left|\Pr\left[\mathcal{H}^{(11)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(12)}(\lambda) = 1\right]\right| \leq \mathsf{Adv}^{\mathsf{full1FE}}_{\mathsf{1FE}, \mathcal{F}', \mathcal{B}^{(11)\to(12)}}(\lambda).$$

Finally, putting together Claims 3.2–3.12 with the facts that $\mathcal{H}^{(0)}(\lambda) = \mathsf{Exp}^{\mathsf{sel2FE}}_{\mathsf{2FE}^{\mathsf{sel}}, \mathcal{F}, \mathcal{A}}(\lambda)$, $\mathcal{H}^{(2)}(\lambda) = \mathcal{H}^{(3,1)}(\lambda)$ and $\Pr\left[\mathcal{H}^{(12)}(\lambda) = 1\right] = 1/2$, we observe that

$$\begin{aligned}
\mathsf{Adv}^{\mathsf{sel2FE}}_{\mathsf{2FE}^{\mathsf{sel}}, \mathcal{F}, \mathcal{A}} &\stackrel{\mathsf{def}}{=} \left|\Pr\left[\mathsf{Exp}^{\mathsf{sel2FE}}_{\mathsf{2FE}^{\mathsf{sel}}, \mathcal{F}, \mathcal{A}}(\lambda) = 1\right] - \frac{1}{2}\right| \\
&= \left|\Pr\left[\mathcal{H}^{(0)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(12)}(\lambda) = 1\right]\right| \\
&\leq \sum_{i=0}^{1} \left|\Pr\left[\mathcal{H}^{(i)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(i+1)}(\lambda) = 1\right]\right| \\
&\quad + \sum_{i=1}^{T} \sum_{j=3}^{10} \left|\Pr\left[\mathcal{H}^{(j,i)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(j+1,i)}(\lambda) = 1\right]\right| \\
&\quad + \left|\Pr\left[\mathcal{H}^{(3,T+1)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(11)}(\lambda) = 1\right]\right| \\
&\quad + \left|\Pr\left[\mathcal{H}^{(11)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(12)}(\lambda) = 1\right]\right| \\
&\leq \mathsf{neg}(\lambda).
\end{aligned}$$

■

4 From Selective to Adaptive Security for Two-Input Schemes

In this section we show how to transform any private-key selective-message secure two-input functional encryption scheme (see Definition 2.8) into a fully secure one (see Definition 2.7). Our construction relies on the following building blocks:

1. A private-key single-input functional encryption scheme $\mathsf{1FE} = (\mathsf{1FE.S}, \mathsf{1FE.KG}, \mathsf{1FE.E}, \mathsf{1FE.D})$.
2. A private-key two-input functional encryption scheme $\mathsf{2FE}^{\mathsf{sel}} = (\mathsf{2FE}^{\mathsf{sel}}.\mathsf{S}, \mathsf{2FE}^{\mathsf{sel}}.\mathsf{KG}, \mathsf{2FE}^{\mathsf{sel}}.\mathsf{E}, \mathsf{2FE}^{\mathsf{sel}}.\mathsf{D})$.
3. A puncturable pseudorandom function family $\mathsf{PRF} = (\mathsf{PRF.Gen}, \mathsf{PRF.Eval}, \mathsf{PRF.Punc})$.

We assume that the schemes 1FE and $\mathsf{2FE}^{\mathsf{sel}}$ are sufficiently expressive in the sense that they support the function family $\mathcal{F}$ (when viewed as a family of single-input functions), the evaluation procedure of the pseudorandom function family PRF, the setup, encryption and key-generation procedures of the scheme 1FE, and a few additional basic operations. The scheme $\mathsf{2FE} = (\mathsf{2FE.S}, \mathsf{2FE.KG}, \mathsf{2FE.E}, \mathsf{2FE.D})$ is defined as follows.

- **The setup algorithm.** On input the security parameter 1^λ the setup algorithm $\mathsf{2FE.S}$ samples $\mathsf{msk}_1 \leftarrow \mathsf{1FE.S}(1^\lambda)$ and $\mathsf{msk}_2 \leftarrow \mathsf{2FE}^{\mathsf{sel}}.\mathsf{S}(1^\lambda)$ and then outputs $\mathsf{msk} = (\mathsf{msk}_1, \mathsf{msk}_2)$.
- **The key-generation algorithm.** On input the master secret key msk and a function $f \in \mathcal{F}_\lambda$, the key-generation algorithm $\mathsf{2FE.KG}$ outputs $\mathsf{sk}_f \leftarrow \mathsf{2FE}^{\mathsf{sel}}.\mathsf{KG}(\mathsf{msk}_2, D_{f,\perp,1,\perp,\perp,\perp})$, where $D_{f,\perp,1,\perp,\perp,\perp}$ is a two-input function that is defined in Figure 3.

$\boldsymbol{D_{f_0,f_1,\mathsf{c},s',t',u}((K^{\mathsf{msk}}, K^{\mathsf{key}}, s, \mathsf{thr}), (\mathsf{c}', t))}$:	$\boldsymbol{C_f((x,y))}$:
1. If $s' = s$ and $t' = t$, output u and HALT.	1. Output $f(x,y)$.
2. Compute $r = \mathsf{PRF.Eval}(K^{\mathsf{msk}}, t)$.	
3. Compute $r' = \mathsf{PRF.Eval}(K^{\mathsf{key}}, t)$.	
4. Compute $\mathsf{msk}_{s,t} = \mathsf{1FE.S}(1^\lambda; r)$.	
5. If $\mathsf{c} \leq \mathsf{thr}$ and $\mathsf{c}' \leq \mathsf{thr}$ set $f = f_1$.	
6. Else (if $\mathsf{c} > \mathsf{thr}$ or $\mathsf{c}' > \mathsf{thr}$) set $f = f_0$.	
7. Output $\mathsf{1FE.KG}(\mathsf{msk}_{s,t}, C_f; r')$.	

Figure 3: The two-input function $D_{f_0,f_1,\mathsf{c},s',t',u}$ and the single-input function C_f.

- **The encryption algorithm.** On input the master secret key msk, a message m and an index $\mathsf{i} \in [2]$, the encryption algorithm $\mathsf{2FE.E}$ has two cases:
  - If $(m, \mathsf{i}) = (x, 1)$, it samples $s \leftarrow \{0,1\}^\lambda$ uniformly at random, three PRF keys K^{enc}, $K^{\mathsf{key}}, K^{\mathsf{msk}} \leftarrow \mathsf{PRF.Gen}(1^\lambda)$ and outputs a pair $(\mathsf{ct}_1, \mathsf{sk}_1)$ defined as follows:

$$\mathsf{ct}_1 \leftarrow \mathsf{2FE}^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_2, (K^{\mathsf{msk}}, K^{\mathsf{key}}, s, 0), 1)$$
$$\mathsf{sk}_1 \leftarrow \mathsf{1FE.KG}(\mathsf{msk}_1, \mathsf{AGG}_{x,\perp,0,s,K^{\mathsf{msk}},K^{\mathsf{enc}},\perp,\perp})$$

    where the single-input function $\mathsf{AGG}_{x,\perp,0,s,K^{\mathsf{msk}},K^{\mathsf{enc}},\perp,\perp}$ is defined in Figure 4.
  - If $(m, \mathsf{i}) = (y, 2)$, it samples $t \leftarrow \{0,1\}^\lambda$ uniformly at random and outputs a pair $(\mathsf{ct}_2, \mathsf{ct}_3)$ defined as follows:

$$\mathsf{ct}_2 \leftarrow \mathsf{2FE}^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_2, (1, t), 2)$$
$$\mathsf{ct}_3 \leftarrow \mathsf{1FE.E}(\mathsf{msk}_1, (y, \perp, 1, t, \perp, \perp)).$$

$\boldsymbol{\mathsf{AGG}_{x_0,x_1,\mathsf{thr},s,K^{\mathsf{msk}},K^{\mathsf{enc}},t',v'}((y_0, y_1, \mathsf{c}, t, s', u'))}$:

1. If $t' = t$ output v' and HALT.
2. If $s' = s$ output u' and HALT.
3. Compute $r = \mathsf{PRF.Eval}(K^{\mathsf{msk}}, t)$.
4. Compute $r' = \mathsf{PRF.Eval}(K^{\mathsf{enc}}, t)$.
5. Compute $\mathsf{msk}_{s,t} = \mathsf{1FE.S}(1^\lambda; r)$.
6. If $\mathsf{c} \leq \mathsf{thr}$ set $x = x_1$ and $y = y_1$.
7. Else (if $\mathsf{c} > \mathsf{thr}$) set $x = x_0$ and $y = y_0$.
8. Output $\mathsf{1FE.E}(\mathsf{msk}_{s,t}, (x, y); r')$.

Figure 4: The single-input function $\mathsf{AGG}_{x_0,x_1,\mathsf{thr},s,K^{\mathsf{msk}},K^{\mathsf{enc}},t',v'}$.

- **The decryption algorithm.** On input a functional key sk_f and two ciphertexts $(\mathsf{ct}_1, \mathsf{sk}_1)$ and $(\mathsf{ct}_2, \mathsf{ct}_3)$, the decryption algorithm $\mathsf{2FE.D}$ first computes the value $\mathsf{sk}' = \mathsf{2FE}^{\mathsf{sel}}.\mathsf{D}(\mathsf{sk}_f, \mathsf{ct}_1, \mathsf{ct}_2)$, then it computes the value $\mathsf{ct}' = \mathsf{1FE.D}(\mathsf{sk}_1, \mathsf{ct}_3)$, and finally it outputs $\mathsf{1FE.D}(\mathsf{sk}', \mathsf{ct}')$.

The correctness of the above scheme with respect to any family of two-ary functionalities follows in a straightforward manner from the correctness of the underlying functional encryption schemes $\mathsf{1FE}$ and $\mathsf{2FE}^{\mathsf{sel}}$. Specifically, consider any pair of messages x and y and any function f. The encryption of x with respect to the index $\mathsf{i} = 1$ and the encryption of y with respect to the index $\mathsf{i} = 2$ result in ciphertexts $(\mathsf{ct}_1, \mathsf{sk}_1)$ and $(\mathsf{ct}_2, \mathsf{ct}_3)$, respectively. Using the correctness of the scheme $\mathsf{2FE}^{\mathsf{sel}}$, by executing $\mathsf{2FE}^{\mathsf{sel}}.\mathsf{D}(\mathsf{sk}_f, \mathsf{ct}_1, \mathsf{ct}_2)$ we obtain a functional key sk' for C_f under the key $\mathsf{msk}_{s,t}$. In addition, by executing $\mathsf{1FE.D}(\mathsf{sk}_1, \mathsf{ct}_3)$ we obtain a an encryption ct' of (x, y) under the key $\mathsf{msk}_{s,t}$. Therefore, executing $\mathsf{1FE.D}(\mathsf{sk}', \mathsf{ct}')$ outputs the value $C_f((x, y)) = f(x, y)$ as required.

The following theorem captures the security of the scheme. This theorem states that under suitable assumptions on the underlying building blocks, the two-input scheme $\mathsf{2FE}$ is fully secure (see Definition 2.7).

Theorem 4.1. *Assuming that (1)* $\mathsf{1FE}$ *is fully secure, (2)* $\mathsf{2FE}^{\mathsf{sel}}$ *is selective-message secure, and (3)* PRF *is a puncturable pseudorandom function family, then* $\mathsf{2FE}$ *is fully secure.*

As in Section 3, for concreteness we focus on the unbounded case where the underlying schemes, $\mathsf{1FE}$ and $\mathsf{2FE}^{\mathsf{sel}}$, support an unbounded (i.e., not fixed in advance) number of key-generation queries and encryption queries. More generally, the proof of Theorem 4.1 shows that if the scheme corresponding to msk_1 supports T_1 encryption queries and T_2 key-generation queries, the scheme corresponding to msk_2 supports $T_3^{(1)}$ encryption queries with respect to index $\mathsf{i} = 1$ and $T_3^{(2)}$ encryption queries with respect to index $\mathsf{i} = 2$, and T_4 key-generation queries, and the scheme corresponding to each $\mathsf{msk}_{s,t}$ supports a *single* encryption query and T_5 key-generation queries, then the resulting scheme $\mathsf{2FE}$ supports $\min\{T_2, T_3^{(1)}\}$ encryption queries with respect to index $\mathsf{i} = 1$, $\min\{T_1, T_3^{(2)}\}$ encryption queries with respect to index $\mathsf{i} = 2$ and $\min\{T_4, T_5\}$ key-generation queries. When the polynomials $T_1, T_2, T_3^{(1)}, T_3^{(2)}, T_4$ and T_5 are known in advance (i.e., do not depend on the adversary), such schemes are known to exist based on the LWE assumption or even only one-way functions (see Section 2.2 for a more elaborated discussion of the existing schemes).

Proof of Theorem 4.1. Let $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ be a probabilistic polynomial-time adversary that issues at most $T_1 = T_1(\lambda)$ encryption queries with respect to index $\mathsf{i} = 1$, at most $T_2 = T_2(\lambda)$ encryption queries with respect to index $\mathsf{i} = 2$, and at most $T_3 = T_3(\lambda)$ key-generation queries (note that T_1, T_2 and T_3 may be any polynomials and are not fixed in advance), and let $\mathcal{F}$ be a family of two-ary functionalities. We assume for simplicity and without loss of generality that $T_1 = T_2 = T_3 \stackrel{\mathsf{def}}{=} T$.

We present a sequence of experiments and upper bound $\mathcal{A}$'s advantage in distinguishing each two consecutive experiments. The first experiment is the experiment in which $\mathcal{A}$ gets oracle access to a left-or-right key generation oracle $\mathsf{KG}_b(\mathsf{msk}, \cdot, \cdot)$ and to a left-or-right encryption oracle $\mathsf{Enc}_b(\mathsf{msk}, (\cdot, \cdot), \cdot)$ for $b \leftarrow \{0, 1\}$ chosen uniformly at random (see Definition 2.7), and the last experiment is completely independent of the bit b. This enables us to prove that there exists a negligible function $\mathsf{neg}(\cdot)$ such that

$$\mathsf{Adv}^{\mathsf{full2FE}}_{\mathsf{2FE},\mathcal{F},\mathcal{A}}(\lambda) \stackrel{\mathsf{def}}{=} \left| \Pr\left[\mathsf{Exp}^{\mathsf{full2FE}}_{\mathsf{2FE},\mathcal{F},\mathcal{A}}(\lambda) = 1\right] - \frac{1}{2} \right| \leq \mathsf{neg}(\lambda)$$

for all sufficiently large $\lambda \in \mathbb{N}$. In what follows we first describe the notation used throughout the proof, and then describe the experiments.

Notation. We denote the i^{th} ciphertext with respect to $\mathsf{i} = 1$ by $(\mathsf{sk}_{1,i}, \mathsf{ct}_{1,i})$ and the i^{th} ciphertext with respect to $\mathsf{i} = 2$ by $(\mathsf{ct}_{2,i}, \mathsf{ct}_{3,i})$. Recall that the adversary $\mathcal{A}$ has unrestricted access to an encryption oracle with respect to index $\mathsf{i} = 1$ and $\mathsf{i} = 2$. We denote the i^{th} input the adversary queries the encryption oracle with $\mathsf{i} = 1$ by (x_i^0, x_i^1), the random string used by s_i and the three PRF keys used for $\mathsf{sk}_{1,i}$ and $\mathsf{ct}_{1,i}$ by $K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}$ and K_i^{enc}. Similarly, we denote the i^{th} input the adversary queries the encryption oracle with $\mathsf{i} = 2$ by (y_i^0, y_i^1) and the random string used by t_i. Finally we denote by $(f_1^0, f_1^1), \ldots, (f_T^0, f_T^1)$ the function-pairs with which the adversary queries the key-generation oracle.

Experiment $\mathcal{H}^{(0)}(\lambda)$. This is the original experiment corresponding to $b \leftarrow \{0,1\}$ chosen uniformly at random. That is, $\mathcal{A}$ gets oracle access to the key-generation oracle $\mathsf{KG}_b(\mathsf{msk}, \cdot)$ and oracle access to a left-or-right encryption oracle $\mathsf{Enc}_b(\mathsf{msk}, (\cdot,\cdot), \cdot)$ where $b \leftarrow \{0,1\}$ is chosen uniformly at random.

- Ciphertexts ($i = 1, \ldots, T$):

$$\begin{aligned}
\mathsf{ct}_{1,i} &\leftarrow \mathsf{2FE}^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_2, (K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}, s_i, 0), 1)\\
\mathsf{sk}_{1,i} &\leftarrow \mathsf{1FE.KG}(\mathsf{msk}_1, \mathsf{AGG}_{x_i^b,\perp,0,s_i,K_i^{\mathsf{msk}},K_i^{\mathsf{enc}},\perp,\perp})\\
\mathsf{ct}_{2,i} &\leftarrow \mathsf{2FE}^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_2, (1,t), 2)\\
\mathsf{ct}_{3,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk}_1, (y_i^b, \perp, 1, t_i, \perp, \perp))
\end{aligned}$$

- Functional keys ($i = 1, \ldots, T$):

$$\mathsf{sk}_{f_i} \leftarrow \mathsf{2FE}^{\mathsf{sel}}.\mathsf{KG}(\mathsf{msk}_2, D_{f_i^b,\perp,1,\perp,\perp,\perp})$$

Experiment $\mathcal{H}^{(1)}(\lambda)$. This experiment is obtained from the experiment $\mathcal{H}^{(0)}(\lambda)$ by modifying the encryptions as follows. Given inputs (x_i^0, x_i^1) and (y_i^0, y_i^1), instead of setting the field x_1 and y_1 to be $\perp$ we set it to be x_i^1 and y_i^1, respectively. In addition, in the encryptions $\mathsf{ct}_{3,i}$ corresponding to $\mathsf{i} = 2$ we embed a counter.

- Ciphertexts ($i = 1, \ldots, T$):

$$\begin{aligned}
\mathsf{ct}_{1,i} &\leftarrow \mathsf{2FE}^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_2, (K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}, s_i, 0), 1)\\
\mathsf{sk}_{1,i} &\leftarrow \mathsf{1FE.KG}(\mathsf{msk}_1, \mathsf{AGG}_{x_i^b,\boxed{x_i^1},0,s_i,K_i^{\mathsf{msk}},K_i^{\mathsf{enc}},\perp,\perp})\\
\mathsf{ct}_{2,i} &\leftarrow \mathsf{2FE}^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_2, (1,t), 2)\\
\mathsf{ct}_{3,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk}_1, (y_i^b, \boxed{y_i^1}, \boxed{i}, t_i, \perp, \perp))
\end{aligned}$$

- Functional keys ($i = 1, \ldots, T$):

$$\mathsf{sk}_{f_i} \leftarrow \mathsf{2FE}^{\mathsf{sel}}.\mathsf{KG}(\mathsf{msk}_2, D_{f_i^b,\perp,1,\perp,\perp,\perp})$$

Note that all the functional keys that are issued as part of the encryption according to $\mathsf{i} = 1$ are generated with $a = 0$ (where a is the third hardwired item). Moreover, since $\mathsf{thr} = 0$ it always holds that $\mathsf{thr} < \mathsf{c}$ which ensures that the functionality does not change. Thus, the circuit $\mathsf{AGG}_{x_0,x_1,a,s,K^{\mathsf{msk}},K^{\mathsf{key}}}$ always sets $x = x_i^b$ and $y = y_i^b$ and ignores x_i^1 and y_i^1 (see Figure 4). Thus, the security of the underlying scheme $\mathsf{1FE}$ guarantees that the adversary $\mathcal{A}$ has only a negligible advantage in distinguishing experiments $\mathcal{H}^{(0)}$ and $\mathcal{H}^{(1)}$. Specifically, let $\mathcal{F}'$ denote the family of functions $\mathsf{AGG}_{x_0,x_1,a,s,K^{\mathsf{msk}},K^{\mathsf{key}}}$ (as defined in Figure 4). In Appendix B.2 we prove the following claim:

Claim 4.2. *There exists a probabilistic polynomial-time adversary* $\mathcal{B}^{(0)\to(1)}$ *such that*

$$\left|\Pr\left[\mathcal{H}^{(0)}(\lambda)=1\right]-\Pr\left[\mathcal{H}^{(1)}(\lambda)=1\right]\right| \le \mathsf{Adv}^{\mathsf{full1FE}}_{\mathsf{1FE},\mathcal{F}',\mathcal{B}^{(0)\to(1)}}(\lambda).$$

Experiment $\mathcal{H}^{(2)}(\lambda)$. This experiment is obtained from the experiment $\mathcal{H}^{(1)}(\lambda)$ by modifying the functional keys as follows. Given inputs (f_i^0, f_i^1), instead of setting the field f_1 to be $\perp$ we set it to be f_i^1. In addition, in the ciphertexts $\mathsf{ct}_{2,i}$ corresponding to $\mathsf{i}=2$ and in the functional keys we embed a counter.

- Ciphertexts ($i = 1, \dots, T$):

$$\begin{aligned}
\mathsf{ct}_{1,i} &\leftarrow \mathsf{2FE}^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_2, (K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}, s_i, 0), 1)\\
\mathsf{sk}_{1,i} &\leftarrow \mathsf{1FE.KG}(\mathsf{msk}_1, \mathsf{AGG}_{x_i^b, x_i^1, 0, s_i, K_i^{\mathsf{msk}}, K_i^{\mathsf{enc}}, \perp, \perp})\\
\mathsf{ct}_{2,i} &\leftarrow \mathsf{2FE}^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_2, (\boxed{i}, t), 2)\\
\mathsf{ct}_{3,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk}_1, (y_i^b, y_i^1, i, t_i, \perp, \perp))
\end{aligned}$$

- Functional keys ($i = 1, \dots, T$):

$$\mathsf{sk}_{f_i} \leftarrow \mathsf{2FE}^{\mathsf{sel}}.\mathsf{KG}(\mathsf{msk}_2, D_{f_i^b, \boxed{f_i^1}, \boxed{i}, \perp, \perp, \perp})$$

Note that all the functional keys that are issued as part of the encryption according to $\mathsf{i}=1$ are generated with $w=0$ which ensures that the functionality does not change (Thus, the circuit $D_{f_0,f_1,s',t',u}$ always sets $f_w = f_i^b$ and ignores f_i^1. Thus, the security of the underlying scheme $\mathsf{2FE}^{\mathsf{sel}}$ guarantees that the adversary $\mathcal{A}$ has only a negligible advantage in distinguishing experiments $\mathcal{H}^{(1)}$ and $\mathcal{H}^{(2)}$. Specifically, let $\mathcal{F}'$ denote the family of functions $D_{f_0,f_1,s',t',u}$ (as defined in Figure 3). In Appendix B.2 we prove the following claim:

Claim 4.3. *There exists a probabilistic polynomial-time adversary* $\mathcal{B}^{(1)\to(2)}$ *such that*

$$\left|\Pr\left[\mathcal{H}^{(1)}(\lambda)=1\right]-\Pr\left[\mathcal{H}^{(2)}(\lambda)=1\right]\right| \le \mathsf{Adv}^{\mathsf{sel2FE}}_{\mathsf{2FE}^{\mathsf{sel}},\mathcal{F}',\mathcal{B}^{(1)\to(2)}}(\lambda).$$

Experiment $\mathcal{H}^{(3,j,k)}(\lambda)$. This experiment is obtained from the experiment $\mathcal{H}^{(2)}(\lambda)$ by modifying the encryptions as follows. The first $j-1$ ciphertexts are generated such that $\mathsf{thr} = T$, the j^{th} ciphertext is generated such that $\mathsf{thr} = k$ and the rest of the ciphertexts are generated as before.

- Ciphertexts ($\mathsf{i}=1$ and $i = 1, \dots, j-1$):

$$\begin{aligned}
\mathsf{ct}_{1,i} &\leftarrow \mathsf{2FE}^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_2, (K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}, s_i, \boxed{T}), 1)\\
\mathsf{sk}_{1,i} &\leftarrow \mathsf{1FE.KG}(\mathsf{msk}_1, \mathsf{AGG}_{x_i^b, x_i^1, \boxed{T}, s_i, K_i^{\mathsf{msk}}, K_i^{\mathsf{enc}}, \perp, \perp})
\end{aligned}$$

- Ciphertexts ($\mathsf{i}=1$ and $i = j$):

$$\begin{aligned}
\mathsf{ct}_{1,i} &\leftarrow \mathsf{2FE}^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_2, (K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}, s_i, \boxed{k}), 1)\\
\mathsf{sk}_{1,i} &\leftarrow \mathsf{1FE.KG}(\mathsf{msk}_1, \mathsf{AGG}_{x_i^b, x_i^1, \boxed{k}, s_i, K_i^{\mathsf{msk}}, K_i^{\mathsf{enc}}, \perp, \perp})
\end{aligned}$$

- Ciphertexts ($\mathsf{i}=1$ and $i = j+1, \dots, T$):

$$\begin{aligned}
\mathsf{ct}_{1,i} &\leftarrow \mathsf{2FE}^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_2, (K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}, s_i, 0), 1)\\
\mathsf{sk}_{1,i} &\leftarrow \mathsf{1FE.KG}(\mathsf{msk}_1, \mathsf{AGG}_{x_i^b, x_i^1, 0, s_i, K_i^{\mathsf{msk}}, K_i^{\mathsf{enc}}, \perp, \perp})
\end{aligned}$$

- Ciphertexts ($\mathsf{i} = 2$ and $i = 1, \ldots, T$):

$$\mathsf{ct}_{2,i} \leftarrow \mathsf{2FE}^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_2, (i, t), 2)$$
$$\mathsf{ct}_{3,i} \leftarrow \mathsf{1FE}.\mathsf{E}(\mathsf{msk}_1, (y_i^b, y_i^1, i, t_i, \perp, \perp))$$

- Functional keys ($i = 1, \ldots, T$):

$$\mathsf{sk}_{f_i} \leftarrow \mathsf{2FE}^{\mathsf{sel}}.\mathsf{KG}(\mathsf{msk}_2, D_{f_i^b, f_i^1, i, \perp, \perp, \perp})$$

Notice that $\mathcal{H}^{(3,1,0)} = \mathcal{H}^{(2)}$.

Experiment $\mathcal{H}^{(4,j,k)}(\lambda)$. This experiment is obtained from the experiment $\mathcal{H}^{(3,j,k)}(\lambda)$ by modifying the encryptions as follows. First, we sample in advance s_j, t_k, K_j^{msk}, K_j^{key} and K_j^{enc}, and compute $\mathsf{msk}_{s_j,t_k} = \mathsf{1FE}.\mathsf{S}(1^\lambda; \mathsf{PRF}.\mathsf{Eval}(K_j^{\mathsf{msk}}, t_k))$. Then, we act according to the following two cases: If the j^{th} encryption with respect to index $\mathsf{i} = 1$ comes *before* the k^{th} encryption with respect to index $\mathsf{i} = 2$, we embed into $\mathsf{ct}_{3,k}$ the pair of values (s_j, γ) where $\gamma = \mathsf{1FE}.\mathsf{E}(\mathsf{msk}_{s_j,t_k}, (x_j^b, y_k^b); \mathsf{PRF}.\mathsf{Eval}(K_j^{\mathsf{enc}}, t_k))$. Otherwise, if the j^{th} encryption with respect to index $\mathsf{i} = 1$ comes *after* the k^{th} encryption with respect to index $\mathsf{i} = 2$, we embed into $\mathsf{ct}_{1,j}$ the pair of values (t_k, γ).

Finally, instead of using K_j^{msk} and K_j^{key} in the j^{th} encryption with respect to msk_1, we use $K_j^{\mathsf{msk}}|_{\{t_k\}}$ and $K_j^{\mathsf{enc}}|_{\{t_k\}}$ which are the keys K_j^{msk} and K_j^{enc} punctured at the point $\{t_k\}$.

For concreteness we assume that the latter is the case, namely, that the j^{th} encryption with respect to index $\mathsf{i} = 1$ came *after* the k^{th} encryption with respect to index $\mathsf{i} = 2$ (the other case is handled similarly).

- Ciphertexts ($\mathsf{i} = 1$ and $i = 1, \ldots, j-1$):

$$\mathsf{ct}_{1,i} \leftarrow \mathsf{2FE}^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_2, (K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}, s_i, T), 1)$$
$$\mathsf{sk}_{1,i} \leftarrow \mathsf{1FE}.\mathsf{KG}(\mathsf{msk}_1, \mathsf{AGG}_{x_i^b, x_i^1, T, s_i, K_i^{\mathsf{msk}}, K_i^{\mathsf{enc}}, \perp, \perp})$$

- Ciphertexts ($\mathsf{i} = 1$ and $i = j$):

$$\mathsf{ct}_{1,i} \leftarrow \mathsf{2FE}^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_2, (K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}, s_i, k), 1)$$
$$\mathsf{sk}_{1,i} \leftarrow \mathsf{1FE}.\mathsf{KG}(\mathsf{msk}_1, \mathsf{AGG}_{x_i^b, x_i^1, k, s_i, \boxed{K_i^{\mathsf{msk}}|_{\{t_k\}}}, \boxed{K_i^{\mathsf{enc}}|_{\{t_k\}}}, \boxed{t_k, \gamma}})$$
$$\mathsf{msk}_{s_j,t_k} = \mathsf{1FE}.\mathsf{S}(1^\lambda; \mathsf{PRF}.\mathsf{Eval}(K_i^{\mathsf{msk}}, t_k))$$
$$\gamma = \mathsf{1FE}.\mathsf{E}(\mathsf{msk}_{s_j,t_k}, (x_j^b, y_k^b); \mathsf{PRF}.\mathsf{Eval}(K_i^{\mathsf{enc}}, t_k))$$

- Ciphertexts ($\mathsf{i} = 1$ and $i = j+1, \ldots, T$):

$$\mathsf{ct}_{1,i} \leftarrow \mathsf{2FE}^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_2, (K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}, s_i, 0), 1)$$
$$\mathsf{sk}_{1,i} \leftarrow \mathsf{1FE}.\mathsf{KG}(\mathsf{msk}_1, \mathsf{AGG}_{x_i^b, x_i^1, 0, s_i, K_i^{\mathsf{msk}}, K_i^{\mathsf{enc}}, \perp, \perp})$$

- Ciphertexts ($\mathsf{i} = 2$ and $i = 1, \ldots, T$):

$$\mathsf{ct}_{2,i} \leftarrow \mathsf{2FE}^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_2, (i, t), 2)$$
$$\mathsf{ct}_{3,i} \leftarrow \mathsf{1FE}.\mathsf{E}(\mathsf{msk}_1, (y_i^b, y_i^1, i, t_i, \perp, \perp))$$

- Functional keys ($i = 1, \ldots, T$):

$$\mathsf{sk}_{f_i} \leftarrow \mathsf{2FE}^{\mathsf{sel}}.\mathsf{KG}(\mathsf{msk}_2, D_{f_i^b, f_i^1, i, \perp, \perp, \perp})$$

We observe that the combination of the k^{th} ciphertext with respect to $\mathsf{i} = 2$ with the j^{th} ciphertext with respect to $\mathsf{i} = 1$ has the same functionality due to the hardwired pair (t_k, γ) (or (s_k, γ) depending on the order they were queried on). For the rest of the combinations we have that the functionality stays the same by the functionality property of the punctured PRF. Thus, the security of the underlying 1FE scheme guarantees that the adversary $\mathcal{A}$ has only a negligible advantage in distinguishing experiments $\mathcal{H}^{(3,j,k)}$ and $\mathcal{H}^{(4,j,k)}$. In Appendix B.2 we prove the following claim:

Claim 4.4. *There exists a probabilistic polynomial-time adversary $\mathcal{B}^{(3,j,k)\to(4,j,k)}$ such that*

$$\left|\Pr\left[\mathcal{H}^{(3,j,k)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(4,j,k)}(\lambda) = 1\right]\right| \leq \mathsf{Adv}^{\mathsf{full1FE}}_{\mathsf{1FE},\mathcal{F}',\mathcal{B}^{(3,j,k)\to(4,j,k)}}(\lambda).$$

Experiment $\mathcal{H}^{(5,j,k)}(\lambda)$. This experiment is obtained from the experiment $\mathcal{H}^{(4,j,k)}(\lambda)$ by modifying the encryptions as follows. First, instead of using K_j^{msk} and K_j^{key} in the j^{th} encryption with respect to msk_2, we use $K_j^{\mathsf{msk}}|_{\{t_k\}}$ and $K_j^{\mathsf{key}}|_{\{t_k\}}$ which are the keys K_j^{msk} and K_j^{key} punctured at the point $\{t_k\}$. Second, we hardwire into every functional key for a pair $(f_i^0.f_i^1)$ the triple (s_j, t_k, δ), where $\delta = \mathsf{1FE.KG}(\mathsf{msk}_{s_j,t_k}, C_{f_i^b}; \mathsf{PRF.Eval}(K_j^{\mathsf{key}}, t_k))$.

- Ciphertexts ($\mathsf{i} = 1$ and $i = 1, \ldots, j-1$):

$$\begin{aligned}\mathsf{ct}_{1,i} &\leftarrow \mathsf{2FE}^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_2, (K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}, s_i, T), 1)\\ \mathsf{sk}_{1,i} &\leftarrow \mathsf{1FE.KG}(\mathsf{msk}_1, \mathsf{AGG}_{x_i^b, x_i^1, T, s_i, K_i^{\mathsf{msk}}, K_i^{\mathsf{enc}}, \perp, \perp})\end{aligned}$$

- Ciphertexts ($\mathsf{i} = 1$ and $i = j$):

$$\begin{aligned}\mathsf{ct}_{1,i} &\leftarrow \mathsf{2FE}^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_2, (\boxed{K_i^{\mathsf{msk}}|_{\{t_k\}}}, \boxed{K_i^{\mathsf{key}}|_{\{t_k\}}}, s_i, k), 1)\\ \mathsf{sk}_{1,i} &\leftarrow \mathsf{1FE.KG}(\mathsf{msk}_1, \mathsf{AGG}_{x_i^b, x_i^1, k, s_i K_i^{\mathsf{msk}}|_{\{t_k\}}, K_i^{\mathsf{enc}}|_{\{t_k\}}, t_k, \gamma})\\ &\mathsf{msk}_{s_j,t_k} = \mathsf{1FE.S}(1^\lambda; \mathsf{PRF.Eval}(K_i^{\mathsf{msk}}, t_k))\\ &\gamma = \mathsf{1FE.E}(\mathsf{msk}_{s_j,t_k}, (x_j^b, y_k^b); \mathsf{PRF.Eval}(K_i^{\mathsf{enc}}, t_k))\end{aligned}$$

- Ciphertexts ($\mathsf{i} = 1$ and $i = j+1, \ldots, T$):

$$\begin{aligned}\mathsf{ct}_{1,i} &\leftarrow \mathsf{2FE}^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_2, (K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}, s_i, 0), 1)\\ \mathsf{sk}_{1,i} &\leftarrow \mathsf{1FE.KG}(\mathsf{msk}_1, \mathsf{AGG}_{x_i^b, x_i^1, 0, s_i, K_i^{\mathsf{msk}}, K_i^{\mathsf{enc}}, \perp, \perp})\end{aligned}$$

- Ciphertexts ($\mathsf{i} = 2$ and $i = 1, \ldots, T$):

$$\begin{aligned}\mathsf{ct}_{2,i} &\leftarrow \mathsf{2FE}^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_2, (i, t), 2)\\ \mathsf{ct}_{3,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk}_1, (y_i^b, y_i^1, i, t_i, \perp, \perp))\end{aligned}$$

- Functional keys ($i = 1, \ldots, T$):

$$\begin{aligned}\mathsf{sk}_{f_i} &\leftarrow \mathsf{2FE}^{\mathsf{sel}}.\mathsf{KG}(\mathsf{msk}_2, D_{f_i^b, f_i^1, i, \boxed{s_j, t_k, \delta}})\\ &\mathsf{msk}_{s_j,t_k} = \mathsf{1FE.S}(1^\lambda; \mathsf{PRF.Eval}(K_j^{\mathsf{msk}}, t_k))\\ &\delta = \mathsf{1FE.KG}(\mathsf{msk}_{s_j,t_k}, C_{f_i^b}; \mathsf{PRF.Eval}(K_j^{\mathsf{key}}, t_k))\end{aligned}$$

We observe that the combination of the k^{th} ciphertext with respect to $\mathsf{i} = 2$ with the j^{th} ciphertext with respect to $\mathsf{i} = 1$ has the same functionality due to the hardwired values (s_j, t_k, δ). For the rest of the combinations we have that the functionality stays the same by the functionality property of the punctured PRF. Thus, the security of the underlying $\mathsf{2FE}^{\mathsf{sel}}$ scheme guarantees that the adversary $\mathcal{A}$ has only a negligible advantage in distinguishing experiments $\mathcal{H}^{(4,j,k)}$ and $\mathcal{H}^{(5,j,k)}$. In Appendix B.2 we prove the following claim:

Claim 4.5. *There exists a probabilistic polynomial-time adversary $\mathcal{B}^{(4,j,k)\to(5,j,k)}$ such that*

$$\left|\Pr\left[\mathcal{H}^{(4,j,k)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(5,j,k)}(\lambda) = 1\right]\right| \leq \mathsf{Adv}^{\mathsf{sel2FE}}_{\mathsf{2FE}^{\mathsf{sel}},\mathcal{F}',\mathcal{B}^{(4,j,k)\to(5,j,k)}}(\lambda).$$

Experiment $\mathcal{H}^{(6,j,k)}(\lambda)$. This experiment is obtained from the experiment $\mathcal{H}^{(5,j,k)}(\lambda)$ by modifying the encryptions as follows. Instead of using randomness generated using a PRF we use randomness sampled uniformly at random. That is, msk_{s_j,t_k}, γ and δ are generated using randomness that is sampled uniformly at random rather than generated using a PRF. We emphasize that msk_{s_j,t_k} is computed in advance once as $\mathsf{msk}_{s_j,t_k} \leftarrow \mathsf{1FE.S}(1^\lambda)$.

- Ciphertexts ($\mathsf{i} = 1$ and $i = 1, \ldots, j-1$):

$$\begin{aligned} \mathsf{ct}_{1,i} &\leftarrow \mathsf{2FE}^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_2, (K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}, s_i, T), 1) \\ \mathsf{sk}_{1,i} &\leftarrow \mathsf{1FE.KG}(\mathsf{msk}_1, \mathsf{AGG}_{x_i^b, x_i^1, T, s_i, K_i^{\mathsf{msk}}, K_i^{\mathsf{enc}}, \perp, \perp}) \end{aligned}$$

- Ciphertexts ($\mathsf{i} = 1$ and $i = j$):

$$\begin{aligned} \mathsf{ct}_{1,i} &\leftarrow \mathsf{2FE}^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_2, (K_i^{\mathsf{msk}}|_{\{t_k\}}, K_i^{\mathsf{key}}|_{\{t_k\}}, s_i, k), 1) \\ \mathsf{sk}_{1,i} &\leftarrow \mathsf{1FE.KG}(\mathsf{msk}_1, \mathsf{AGG}_{x_i^b, x_i^1, k, s_i K_i^{\mathsf{msk}}|_{\{t_k\}}, K_i^{\mathsf{enc}}|_{\{t_k\}}, t_k, \gamma}) \\ \boxed{\mathsf{msk}_{s_j,t_k}} &= \mathsf{1FE.S}(1^\lambda) \\ \boxed{\gamma} &= \mathsf{1FE.E}(\mathsf{msk}_{s_j,t_k}, (x_j^b, y_k^b)) \end{aligned}$$

- Ciphertexts ($\mathsf{i} = 1$ and $i = j+1, \ldots, T$):

$$\begin{aligned} \mathsf{ct}_{1,i} &\leftarrow \mathsf{2FE}^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_2, (K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}, s_i, 0), 1) \\ \mathsf{sk}_{1,i} &\leftarrow \mathsf{1FE.KG}(\mathsf{msk}_1, \mathsf{AGG}_{x_i^b, x_i^1, 0, s_i, K_i^{\mathsf{msk}}, K_i^{\mathsf{enc}}, \perp, \perp}) \end{aligned}$$

- Ciphertexts ($\mathsf{i} = 2$ and $i = 1, \ldots, T$):

$$\begin{aligned} \mathsf{ct}_{2,i} &\leftarrow \mathsf{2FE}^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_2, (i, t), 2) \\ \mathsf{ct}_{3,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk}_1, (y_i^b, y_i^1, i, t_i, \perp, \perp)) \end{aligned}$$

- Functional keys ($i = 1, \ldots, T$):

$$\begin{aligned} \mathsf{sk}_{f_i} &\leftarrow \mathsf{2FE}^{\mathsf{sel}}.\mathsf{KG}(\mathsf{msk}_2, D_{f_i^b, f_i^1, i, s_j, t_k, \delta}) \\ \boxed{\delta} &= \mathsf{1FE.KG}(\mathsf{msk}_{s_j,t_k}, C_{f_i^b}) \end{aligned}$$

The pseudorandomness of $\mathsf{PRF.Eval}(K_j^{\mathsf{msk}}, \cdot)$, $\mathsf{PRF.Eval}(K_j^{\mathsf{key}}, \cdot)$ and $\mathsf{PRF.Eval}(K_j^{\mathsf{enc}}, \cdot)$ guarantee that the adversary $\mathcal{A}$ has only a negligible advantage in distinguishing experiments $\mathcal{H}^{(5,j,k)}$ and $\mathcal{H}^{(6,j,k)}$. In Appendix B.2 we prove the following claim:

Claim 4.6. *There exists a probabilistic polynomial-time adversary $\mathcal{B}^{(5,j,k)\to(6,j,k)}$ such that*

$$\left|\Pr\left[\mathcal{H}^{(5,j,k)}(\lambda)=1\right]-\Pr\left[\mathcal{H}^{(6,j,k)}(\lambda)=1\right]\right|\leq 3\cdot \mathsf{Adv}_{\mathsf{PRF},\mathcal{B}^{(5,j,k)\to(6,j,k)}}(\lambda).$$

Experiment $\mathcal{H}^{(7,j,k)}(\lambda)$. This experiment is obtained from the experiment $\mathcal{H}^{(6,j,k)}(\lambda)$ by modifying the encryptions as follows. Instead of having (x_j^b, y_k^b) hardwired in γ and $D_{f_i^b}$ in δ, we hardwire the values (x_j^1, y_k^1) and $D_{f_i^1}$, respectively.

- Ciphertexts ($\mathsf{i}=1$ and $i=1,\dots,j-1$):

$$\begin{aligned}\mathsf{ct}_{1,i} &\leftarrow \mathsf{2FE^{sel}.E}(\mathsf{msk}_2,(K_i^{\mathsf{msk}},K_i^{\mathsf{key}},s_i,T),1)\\ \mathsf{sk}_{1,i} &\leftarrow \mathsf{1FE.KG}(\mathsf{msk}_1,\mathsf{AGG}_{x_i^b,x_i^1,T,s_i,K_i^{\mathsf{msk}},K_i^{\mathsf{enc}},\perp,\perp})\end{aligned}$$

- Ciphertexts ($\mathsf{i}=1$ and $i=j$):

$$\begin{aligned}\mathsf{ct}_{1,i} &\leftarrow \mathsf{2FE^{sel}.E}(\mathsf{msk}_2,(K_i^{\mathsf{msk}}|_{\{t_k\}},K_i^{\mathsf{key}}|_{\{t_k\}},s_i,k),1)\\ \mathsf{sk}_{1,i} &\leftarrow \mathsf{1FE.KG}(\mathsf{msk}_1,\mathsf{AGG}_{x_i^b,x_i^1,k,s_i K_i^{\mathsf{msk}}|_{\{t_k\}},K_i^{\mathsf{enc}}|_{\{t_k\}},t_k,\gamma})\\ \mathsf{msk}_{s_j,t_k} &= \mathsf{1FE.S}(1^\lambda)\\ \gamma &= \mathsf{1FE.E}(\mathsf{msk}_{s_j,t_k},(\boxed{x_j^1,y_k^1}))\end{aligned}$$

- Ciphertexts ($\mathsf{i}=1$ and $i=j+1,\dots,T$):

$$\begin{aligned}\mathsf{ct}_{1,i} &\leftarrow \mathsf{2FE^{sel}.E}(\mathsf{msk}_2,(K_i^{\mathsf{msk}},K_i^{\mathsf{key}},s_i,0),1)\\ \mathsf{sk}_{1,i} &\leftarrow \mathsf{1FE.KG}(\mathsf{msk}_1,\mathsf{AGG}_{x_i^b,x_i^1,0,s_i,K_i^{\mathsf{msk}},K_i^{\mathsf{enc}},\perp,\perp})\end{aligned}$$

- Ciphertexts ($\mathsf{i}=2$ and $i=1,\dots,T$):

$$\begin{aligned}\mathsf{ct}_{2,i} &\leftarrow \mathsf{2FE^{sel}.E}(\mathsf{msk}_2,(i,t),2)\\ \mathsf{ct}_{3,i} &\leftarrow \mathsf{1FE.E}(\mathsf{msk}_1,(y_i^b,y_i^1,i,t_i,\perp,\perp))\end{aligned}$$

- Functional keys ($i=1,\dots,T$):

$$\begin{aligned}\mathsf{sk}_{f_i} &\leftarrow \mathsf{2FE^{sel}.KG}(\mathsf{msk}_2,D_{f_i^b,f_i^1,i,s_j,t_k,\delta})\\ \delta &= \mathsf{1FE.KG}(\mathsf{msk}_{s_j,t_k},\boxed{C_{f_i^1}})\end{aligned}$$

We observe that the combination of the k^{th} ciphertext with respect to $\mathsf{i}=2$ with the j^{th} ciphertext with respect to $\mathsf{i}=1$ has the same functionality due to the hardwired values (s_j,t_k,δ) and the fact that the adversary is *valid* (see Definition 2.6). Thus, the security of the underlying 1FE scheme guarantees that the adversary $\mathcal{A}$ has only a negligible advantage in distinguishing experiments $\mathcal{H}^{(6,j,k)}$ and $\mathcal{H}^{(7,j,k)}$. In Appendix B.2 we prove the following claim:

Claim 4.7. *There exists a probabilistic polynomial-time adversary $\mathcal{B}^{(6,j,k)\to(7,j,k)}$ such that*

$$\left|\Pr\left[\mathcal{H}^{(6,j,k)}(\lambda)=1\right]-\Pr\left[\mathcal{H}^{(7,j,k)}(\lambda)=1\right]\right|\leq \mathsf{Adv}^{\mathsf{full1FE}}_{\mathsf{1FE},\mathcal{F}',\mathcal{B}^{(6,j,k)\to(7,j,k)}}(\lambda).$$

Experiment $\mathcal{H}^{(8,j,k)}(\lambda)$. This experiment is obtained from the experiment $\mathcal{H}^{(7,j,k)}(\lambda)$ by modifying the encryptions as follows. Instead of using randomness sampled uniformly at random we use randomness generated using a PRF. That is, msk_{s_j,t_k}, γ and δ are generated using a PRF.

- Ciphertexts ($\mathsf{i} = 1$ and $i = 1, \ldots, j-1$):

$$\mathsf{ct}_{1,i} \leftarrow \mathsf{2FE}^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_2, (K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}, s_i, T), 1)$$
$$\mathsf{sk}_{1,i} \leftarrow \mathsf{1FE.KG}(\mathsf{msk}_1, \mathsf{AGG}_{x_i^b, x_i^1, T, s_i, K_i^{\mathsf{msk}}, K_i^{\mathsf{enc}}, \perp, \perp})$$

- Ciphertexts ($\mathsf{i} = 1$ and $i = j$):

$$\mathsf{ct}_{1,i} \leftarrow \mathsf{2FE}^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_2, (K_i^{\mathsf{msk}}|_{\{t_k\}}, K_i^{\mathsf{key}}|_{\{t_k\}}, s_i, k), 1)$$
$$\mathsf{sk}_{1,i} \leftarrow \mathsf{1FE.KG}(\mathsf{msk}_1, \mathsf{AGG}_{x_i^b, x_i^1, k, s_i K_i^{\mathsf{msk}}|_{\{t_k\}}, K_i^{\mathsf{enc}}|_{\{t_k\}}, t_k, \gamma})$$
$$\boxed{\mathsf{msk}_{s_j, t_k}} \leftarrow \mathsf{1FE.S}(1^\lambda; \mathsf{PRF.Eval}(K_j^{\mathsf{msk}}, t_k))$$
$$\boxed{\gamma} \leftarrow \mathsf{1FE.E}(\mathsf{msk}_{s_j, t_k}, (x_j^1, y_k^1); \mathsf{PRF.Eval}(K_j^{\mathsf{enc}}, t_k))$$

- Ciphertexts ($\mathsf{i} = 1$ and $i = j+1, \ldots, T$):

$$\mathsf{ct}_{1,i} \leftarrow \mathsf{2FE}^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_2, (K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}, s_i, 0), 1)$$
$$\mathsf{sk}_{1,i} \leftarrow \mathsf{1FE.KG}(\mathsf{msk}_1, \mathsf{AGG}_{x_i^b, x_i^1, 0, s_i, K_i^{\mathsf{msk}}, K_i^{\mathsf{enc}}, \perp, \perp})$$

- Ciphertexts ($\mathsf{i} = 2$ and $i = 1, \ldots, T$):

$$\mathsf{ct}_{2,i} \leftarrow \mathsf{2FE}^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_2, (i, t), 2)$$
$$\mathsf{ct}_{3,i} \leftarrow \mathsf{1FE.E}(\mathsf{msk}_1, (y_i^b, y_i^1, i, t_i, \perp, \perp))$$

- Functional keys ($i = 1, \ldots, T$):

$$\mathsf{sk}_{f_i} \leftarrow \mathsf{2FE}^{\mathsf{sel}}.\mathsf{KG}(\mathsf{msk}_2, D_{f_i^b, f_i^1, i, s_j, t_k, \delta})$$
$$\boxed{\mathsf{msk}_{s_j, t_k}} \leftarrow \mathsf{1FE.S}(1^\lambda; \mathsf{PRF.Eval}(K_j^{\mathsf{msk}}, t_k))$$
$$\boxed{\delta} \leftarrow \mathsf{1FE.KG}(\mathsf{msk}_{s_j, t_k}, C_{f_i^1}; \mathsf{PRF.Eval}(K_j^{\mathsf{key}}, t_k))$$

The pseudorandomness of $\mathsf{PRF.Eval}(K_j^{\mathsf{msk}}, \cdot)$, $\mathsf{PRF.Eval}(K_j^{\mathsf{key}}, \cdot)$ and $\mathsf{PRF.Eval}(K_j^{\mathsf{enc}}, \cdot)$ guarantee that the adversary $\mathcal{A}$ has only a negligible advantage in distinguishing experiments $\mathcal{H}^{(7,j,k)}$ and $\mathcal{H}^{(8,j,k)}$. The proof of the following claim is analogous to the proof of Claim 4.6.

Claim 4.8. *There exists a probabilistic polynomial-time adversary $\mathcal{B}^{(7,j,k)\to(8,j,k)}$ such that*

$$\left|\Pr\left[\mathcal{H}^{(7,j,k)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(8,j,k)}(\lambda) = 1\right]\right| \le 3 \cdot \mathsf{Adv}_{\mathsf{PRF}, \mathcal{B}^{(7,j,k)\to(8,j,k)}}(\lambda).$$

Experiment $\mathcal{H}^{(9,j,k)}(\lambda)$. This experiment is obtained from the experiment $\mathcal{H}^{(8,j,k)}(\lambda)$ by modifying the encryptions as follows. First, instead of using a punctured keys $K_j^{\mathsf{msk}}|_{\{t_k\}}$ and $K_j^{\mathsf{key}}|_{\{t_k\}}$ in the j^{th} encryption with respect to msk_2, we use the original keys K_j^{msk} and K_j^{key}. Second, we set the threshold thr in $\mathsf{ct}_{1,j}$ to $k+1$. Lastly, we hardwire into every functional key for a pair $(f_i^0.f_i^1)$ the triple $(\perp, \perp, \perp)$ instead of (s_j, t_k, δ).

- Ciphertexts ($\mathsf{i} = 1$ and $i = 1, \ldots, j-1$):

$$\mathsf{ct}_{1,i} \leftarrow \mathsf{2FE}^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_2, (K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}, s_i, T), 1)$$
$$\mathsf{sk}_{1,i} \leftarrow \mathsf{1FE.KG}(\mathsf{msk}_1, \mathsf{AGG}_{x_i^b, x_i^1, T, s_i, K_i^{\mathsf{msk}}, K_i^{\mathsf{enc}}, \perp, \perp})$$

- Ciphertexts ($\mathsf{i} = 1$ and $i = j$):

$$\mathsf{ct}_{1,i} \leftarrow \mathsf{2FE}^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_2, (\boxed{K_i^{\mathsf{msk}}}, \boxed{K_i^{\mathsf{key}}}, s_i, \boxed{k+1}), 1)$$
$$\mathsf{sk}_{1,i} \leftarrow \mathsf{1FE.KG}(\mathsf{msk}_1, \mathsf{AGG}_{x_i^b, x_i^1, k, s_i K_i^{\mathsf{msk}}|_{\{t_k\}}, K_i^{\mathsf{enc}}|_{\{t_k\}}, t_k, \gamma})$$
$$\mathsf{msk}_{s_j,t_k} \leftarrow \mathsf{1FE.S}(1^\lambda; \mathsf{PRF.Eval}(K_j^{\mathsf{msk}}, t_k))$$
$$\gamma \leftarrow \mathsf{1FE.E}(\mathsf{msk}_{s_j,t_k}, (x_j^1, y_k^1); \mathsf{PRF.Eval}(K_j^{\mathsf{enc}}, t_k))$$

- Ciphertexts ($\mathsf{i} = 1$ and $i = j+1, \ldots, T$):

$$\mathsf{ct}_{1,i} \leftarrow \mathsf{2FE}^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_2, (K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}, s_i, 0), 1)$$
$$\mathsf{sk}_{1,i} \leftarrow \mathsf{1FE.KG}(\mathsf{msk}_1, \mathsf{AGG}_{x_i^b, x_i^1, 0, s_i, K_i^{\mathsf{msk}}, K_i^{\mathsf{enc}}, \perp, \perp})$$

- Ciphertexts ($\mathsf{i} = 2$ and $i = 1, \ldots, T$):

$$\mathsf{ct}_{2,i} \leftarrow \mathsf{2FE}^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_2, t, 2)$$
$$\mathsf{ct}_{3,i} \leftarrow \mathsf{1FE.E}(\mathsf{msk}_1, (y_i^b, y_i^1, i, t_i, \perp, \perp))$$

- Functional keys ($i = 1, \ldots, T$):

$$\mathsf{sk}_{f_i} \leftarrow \mathsf{2FE}^{\mathsf{sel}}.\mathsf{KG}(\mathsf{msk}_2, D_{f_i^b, f_i^1, i, \boxed{\perp, \perp, \perp}})$$

We observe that the combination of the k^{th} ciphertext with respect to $\mathsf{i} = 2$ with the j^{th} ciphertext with respect to $\mathsf{i} = 1$ has the same functionality due to the hardwired values (s_j, t_k, δ). For the rest of the combinations we have that the functionality stays the same by the functionality property of the punctured PRF. Thus, the security of the underlying $\mathsf{2FE}^{\mathsf{sel}}$ scheme guarantees that the adversary $\mathcal{A}$ has only a negligible advantage in distinguishing experiments $\mathcal{H}^{(8,j,k)}$ and $\mathcal{H}^{(9,j,k)}$. The proof of the following claim is analogous to the proof of Claim 4.5.

Claim 4.9. *There exists a probabilistic polynomial-time adversary $\mathcal{B}^{(8,j,k)\to(9,j,k)}$ such that*

$$\left|\Pr\left[\mathcal{H}^{(8,j,k)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(9,j,k)}(\lambda) = 1\right]\right| \leq \mathsf{Adv}^{\mathsf{sel2FE}}_{\mathsf{2FE}^{\mathsf{sel}}, \mathcal{F}', \mathcal{B}^{(8,j,k)\to(9,j,k)}}(\lambda).$$

Next, as in Claim 4.4 we observe that $\mathcal{H}^{(9,j,k)}(\lambda)$ is indistinguishable from $\mathcal{H}^{(3,j,k+1)}(\lambda)$. Moreover, we notice that $\mathcal{H}^{(3,j,T)}(\lambda) = \mathcal{H}^{(3,j+1,0)}(\lambda)$.

Claim 4.10. *There exists a probabilistic polynomial-time adversary $\mathcal{B}^{(9,j,k)\to(3,j,k+1)}$ such that*

$$\left|\Pr\left[\mathcal{H}^{(9,j,k)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(3,j,k+1)}(\lambda) = 1\right]\right| \leq \mathsf{Adv}^{\mathsf{full1FE}}_{\mathsf{1FE}, \mathcal{F}', \mathcal{B}^{(9,j,k)\to(3,j,k+1)}}(\lambda).$$

Experiment $\mathcal{H}^{(10)}(\lambda)$. This experiment is obtained from the experiment $\mathcal{H}^{(3,T+1,0)}(\lambda)$ by modifying the ciphertexts *not* to include f_i^b at all.

- Ciphertexts ($\mathsf{i} = 1$ and $i = 1, \ldots, T$):

$$\mathsf{ct}_{1,i} \leftarrow \mathsf{2FE}^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_2, (K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}, s_i, T), 1)$$
$$\mathsf{sk}_{1,i} \leftarrow \mathsf{1FE.KG}(\mathsf{msk}_1, \mathsf{AGG}_{x_i^b, x_i^1, T, s_i, K_i^{\mathsf{msk}}, K_i^{\mathsf{enc}}, \perp, \perp})$$

- Ciphertexts ($\mathsf{i} = 2$ and $i = 1, \ldots, T$):

$$\mathsf{ct}_{2,i} \leftarrow \mathsf{2FE}^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_2, (i, t), 2)$$
$$\mathsf{ct}_{3,i} \leftarrow \mathsf{1FE}.\mathsf{E}(\mathsf{msk}_1, (y_i^b, y_i^1, i, t_i, \perp, \perp))$$

- Functional keys ($i = 1, \ldots, T$):

$$\mathsf{sk}_{f_i} \leftarrow \mathsf{2FE}^{\mathsf{sel}}.\mathsf{KG}(\mathsf{msk}_2, D_{\boxed{\perp}, f_i^1, i, \perp, \perp, \perp})$$

We observe that at this point all ciphertext have $\mathsf{thr} = T$. Therefore, the first parameter f_i^b is always ignored and the functionalities stay the same. Thus, the security of the underlying $\mathsf{2FE}^{\mathsf{sel}}$ scheme guarantees that the adversary $\mathcal{A}$ has only a negligible advantage in distinguishing experiments $\mathcal{H}^{(3,T+1,0)}$ and $\mathcal{H}^{(10)}$. The proof of the following claim is analogous to the proof of Claim 4.3.

Claim 4.11. *There exists a probabilistic polynomial-time adversary* $\mathcal{B}^{(3,T+1,0)\to(10)}$ *such that*

$$\left|\Pr\left[\mathcal{H}^{(3,T+1,0)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(10)}(\lambda) = 1\right]\right| \leq \mathsf{Adv}^{\mathsf{sel2FE}}_{\mathsf{2FE}^{\mathsf{sel}}, \mathcal{F}', \mathcal{B}^{(3,T+1,0)\to(10)}}(\lambda).$$

Experiment $\mathcal{H}^{(11)}(\lambda)$. This experiment is obtained from the experiment $\mathcal{H}^{(10)}(\lambda)$ by modifying the ciphertexts *not* to include x_i^b and y_i^b at all. Notice that this experiment is completely independent of the bit b, and therefore $\Pr[\mathcal{H}^{(11)}(\lambda) = 1] = 1/2$.

- Ciphertexts ($\mathsf{i} = 1$ and $i = 1, \ldots, T$):

$$\mathsf{ct}_{1,i} \leftarrow \mathsf{2FE}^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_2, (K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}, s_i, T), 1)$$
$$\mathsf{sk}_{1,i} \leftarrow \mathsf{1FE}.\mathsf{KG}(\mathsf{msk}_1, \mathsf{AGG}_{\boxed{\perp}, x_i^1, T, s_i, K_i^{\mathsf{msk}}, K_i^{\mathsf{enc}}, \perp, \perp})$$

- Ciphertexts ($\mathsf{i} = 2$ and $i = 1, \ldots, T$):

$$\mathsf{ct}_{2,i} \leftarrow \mathsf{2FE}^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_2, (i, t), 2)$$
$$\mathsf{ct}_{3,i} \leftarrow \mathsf{1FE}.\mathsf{E}(\mathsf{msk}_1, (\boxed{\perp}, y_i^1, i, t_i, \perp, \perp))$$

- Functional keys ($i = 1, \ldots, T$):

$$\mathsf{sk}_{f_i} \leftarrow \mathsf{2FE}^{\mathsf{sel}}.\mathsf{KG}(\mathsf{msk}_2, D_{\perp, f_i^1, i, \perp, \perp, \perp})$$

We observe that at this point all ciphertext have $\mathsf{thr} = T$. Therefore, the first parameters x_i^b and y_i^b are always ignored and the functionalities stay the same. Thus, the security of the underlying $\mathsf{1FE}$ scheme guarantees that the adversary $\mathcal{A}$ has only a negligible advantage in distinguishing experiments $\mathcal{H}^{(3,T+1)}$ and $\mathcal{H}^{(10)}$. The proof of the following claim is analogous to the proof of Claim 4.2.

Claim 4.12. *There exists a probabilistic polynomial-time adversary* $\mathcal{B}^{(10)\to(11)}$ *such that*

$$\left|\Pr\left[\mathcal{H}^{(10)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(11)}(\lambda) = 1\right]\right| \leq \mathsf{Adv}^{\mathsf{full1FE}}_{\mathsf{1FE}, \mathcal{F}', \mathcal{B}^{(10)\to(11)}}(\lambda).$$

Finally, putting together Claims 4.2–4.12 with the facts that $\mathsf{Adv}^{\mathsf{full2FE}}_{\mathsf{2FE},\mathcal{F},\mathcal{A}}(\lambda) = \mathcal{H}^{(0)}(\lambda)$, $\mathcal{H}^{(2)}(\lambda) = \mathcal{H}^{(3,1,0)}(\lambda)$ and $\Pr\left[\mathcal{H}^{(11)}(\lambda) = 1\right] = 1/2$, we observe that

$$\begin{aligned}
\mathsf{Adv}^{\mathsf{full2FE}}_{\mathsf{2FE},\mathcal{F},\mathcal{A}} &\stackrel{\mathsf{def}}{=} \left|\Pr\left[\mathsf{Exp}^{\mathsf{full2FE}}_{\mathsf{2FE},\mathcal{F},\mathcal{A}}(\lambda) = 1\right] - \frac{1}{2}\right| \\
&= \left|\Pr\left[\mathcal{H}^{(0)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(11)}(\lambda) = 1\right]\right| \\
&\leq \sum_{i=0}^{1}\left|\Pr\left[\mathcal{H}^{(i)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(i+1)}(\lambda) = 1\right]\right| \\
&\quad + \sum_{j=1}^{T}\sum_{k=0}^{T}\sum_{i=3}^{8}\left|\Pr\left[\mathcal{H}^{(i,j,k)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(i+1,j,k)}(\lambda) = 1\right]\right| \\
&\quad + \left|\Pr\left[\mathcal{H}^{(3,T+1,0)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(10)}(\lambda) = 1\right]\right| \\
&\quad + \left|\Pr\left[\mathcal{H}^{(10)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(11)}(\lambda) = 1\right]\right| \\
&\leq \mathsf{neg}(\lambda).
\end{aligned}$$

■

Acknowledgments

We thank Eylon Yogev for insightful discussions and helpful remarks.

References

[AAB+13] S. Agrawal, S. Agrawal, S. Badrinarayanan, A. Kumarasubramanian, M. Prabhakaran, and A. Sahai. Function private functional encryption and property preserving encryption: New definitions and positive results. Cryptology ePrint Archive, Report 2013/744, 2013.

[ABG+13] P. Ananth, D. Boneh, S. Garg, A. Sahai, and M. Zhandry. Differing-inputs obfuscation and applications. Cryptology ePrint Archive, Report 2013/689, 2013.

[ABS+14] P. Ananth, Z. Brakerski, G. Segev, and V. Vaikuntanathan. From selective to adaptive security in functional encryption. Cryptology ePrint Archive, Report 2014/917, 2014.

[AGV+13] S. Agrawal, S. Gorbunov, V. Vaikuntanathan, and H. Wee. Functional encryption: New perspectives and lower bounds. In *Advances in Cryptology – CRYPTO '13*, pages 500–518, 2013.

[BCP14] E. Boyle, K. Chung, and R. Pass. On extractability obfuscation. In *Proceedings of the 11th Theory of Cryptography Conference*, pages 52–73, 2014.

[BF03] D. Boneh and M. K. Franklin. Identity-based encryption from the Weil pairing. *SIAM Journal on Computing*, 32(3):586–615, 2003. Preliminary version in *Advances in Cryptology – CRYPTO '01*, pages 213–229, 2001.

[BGI+12] B. Barak, O. Goldreich, R. Impagliazzo, S. Rudich, A. Sahai, S. P. Vadhan, and K. Yang. On the (im)possibility of obfuscating programs. *Journal of the ACM*, 59(2):6, 2012.

[BGI14] E. Boyle, S. Goldwasser, and I. Ivan. Functional signatures and pseudorandom functions. In *Proceedings of the 17th International Conference on Practice and Theory in Public-Key Cryptography*, pages 501–519, 2014.

[BLR+15] D. Boneh, K. Lewi, M. Raykova, A. Sahai, M. Zhandry, and J. Zimmerman. Semantically secure order-revealing encryption: Multi-input functional encryption without obfuscation. To appear in *Proceedings of Advances in Cryptology – EUROCRYPT*, 2015. Available as Cryptology ePrint Archive, Report 2014/834.

[BO13] M. Bellare and A. O'Neill. Semantically-secure functional encryption: Possibility results, impossibility results and the quest for a general definition. In *Proceedings of the 12th International Conference on Cryptology and Network Security*, pages 218–234, 2013.

[BRS13] D. Boneh, A. Raghunathan, and G. Segev. Function-private identity-based encryption: Hiding the function in functional encryption. In *Advances in Cryptology – CRYPTO '13*, pages 461–478, 2013.

[BS15] Z. Brakerski and G. Segev. Function-private functional encryption in the private-key setting. To appear in *Proceedings of the 12th Theory of Cryptography Conference*, 2015. Available as Cryptology ePrint Archive, Report 2014/550.

[BSW11] D. Boneh, A. Sahai, and B. Waters. Functional encryption: Definitions and challenges. In *Proceedings of the 8th Theory of Cryptography Conference*, pages 253–273, 2011.

[BW13] D. Boneh and B. Waters. Constrained pseudorandom functions and their applications. In *Advances in Cryptology - ASIACRYPT '13*, pages 280–300, 2013.

[Coc01] C. Cocks. An identity based encryption scheme based on quadratic residues. In *Proceedings of the 8th IMA International Conference on Cryptography and Coding*, pages 360–363, 2001.

[GGG+14] S. Goldwasser, S. D. Gordon, V. Goyal, A. Jain, J. Katz, F.-H. Liu, A. Sahai, E. Shi, and H.-S. Zhou. Multi-input functional encryption. In *Advances in Cryptology – EUROCRYPT '14*, pages 578–602, 2014.

[GGH+13] S. Garg, C. Gentry, S. Halevi, M. Raykova, A. Sahai, and B. Waters. Candidate indistinguishability obfuscation and functional encryption for all circuits. In *Proceedings of the 54th Annual IEEE Symposium on Foundations of Computer Science*, pages 40–49, 2013.

[GGH+14] S. Garg, C. Gentry, S. Halevi, and M. Zhandry. Fully secure functional encryption without obfuscation. Cryptology ePrint Archive, Report 2014/666, 2014.

[GGM86] O. Goldreich, S. Goldwasser, and S. Micali. How to construct random functions. *Journal of the ACM*, 33(4):792–807, 1986.

[GKP+13] S. Goldwasser, Y. Kalai, R. A. Popa, V. Vaikuntanathan, and N. Zeldovich. Reusable garbled circuits and succinct functional encryption. In *Proceedings of the 45th Annual ACM Symposium on Theory of Computing*, pages 555–564, 2013.

[GVW12] S. Gorbunov, V. Vaikuntanathan, and H. Wee. Functional encryption with bounded collusions via multi-party computation. In *Advances in Cryptology – CRYPTO '12*, pages 162–179, 2012.

[KMN+14] I. Komargodski, T. Moran, M. Naor, R. Pass, A. Rosen, and E. Yogev. One-way functions and (im)perfect obfuscation. In *Proceedings of the 55th Annual IEEE Symposium on Foundations of Computer Science*, pages 374–383, 2014.

[KPT+13] A. Kiayias, S. Papadopoulos, N. Triandopoulos, and T. Zacharias. Delegatable pseudorandom functions and applications. In *Proceedings of the 20th Annual ACM Conference on Computer and Communications Security*, pages 669–684, 2013.

[KSY15] I. Komargodski, G. Segev, and E. Yogev. Functional encryption for randomized functionalities in the private-key setting from minimal assumptions. To appear in *Proceedings of the 12th Theory of Cryptography Conference*, 2015. Available as Cryptology ePrint Archive, Report 2014/868.

[O'N10] A. O'Neill. Definitional issues in functional encryption. Cryptology ePrint Archive, Report 2010/556, 2010.

[Sha84] A. Shamir. Identity-based cryptosystems and signature schemes. In *Advances in Cryptology – CRYPTO '84*, pages 47–53, 1984.

[SSW09] E. Shen, E. Shi, and B. Waters. Predicate privacy in encryption systems. In *Proceedings of the 6th Theory of Cryptography Conference*, pages 457–473, 2009.

[SW08] A. Sahai and B. Waters. Slides on functional encryption. Available at `http://www.cs.utexas.edu/~bwaters/presentations/files/functional.ppt`, 2008.

[SW14] A. Sahai and B. Waters. How to use indistinguishability obfuscation: deniable encryption, and more. In *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, pages 475–484, 2014.

[Wat14] B. Waters. A punctured programming approach to adaptively secure functional encryption. Cryptology ePrint Archive, Report 2014/588, 2014.

A Generalization to $t \geq 2$ Inputs

In this section we generalize our results to more than two inputs. In Appendix A.1 we generalize the definitions introduced in Section 2.3, and in Appendices A.2 and A.3 we generalize the constructions from Sections 3 and 4, respectively. More precisely, in Appendix A.2 we show how to obtain a *selectively-secure* t-input scheme assuming any fully secure $(t-1)$-input scheme. Then, in Appendix A.3 we show how to obtain a *fully-secure* t-input scheme assuming any fully-secure $(t-1)$-input scheme and a selectively-secure t-input scheme.

A.1 Private-Key t-Input Functional Encryption

In this section we generalize the framework introduced in Section 2.3 to the general case of t-input schemes (Section 2.3 dealt with the case $t = 2$).

For $i \in [t]$ let $\mathcal{X}_i = \{(\mathcal{X}_i)_\lambda\}_{\lambda \in \mathbb{N}}$ be an ensemble of finite sets, and let $\mathcal{F} = \{\mathcal{F}_\lambda\}_{\lambda \in \mathbb{N}}$ be an ensemble of finite t-ary function families. For each $\lambda \in \mathbb{N}$, each function $f \in \mathcal{F}_\lambda$ takes as input t strings, $x_1 \in (\mathcal{X}_1)_\lambda, \ldots, x_t \in (\mathcal{X}_t)_\lambda$, and outputs a value $f(x_1, \ldots, x_t) \in \mathcal{Z}_\lambda$. A private-key t-input functional encryption scheme Π for $\mathcal{F}$ consists of four probabilistic polynomial time algorithm Setup, Enc, KG and Dec, described as follows. The setup algorithm $\mathsf{Setup}(1^\lambda)$ takes as input the security parameter λ, and outputs a master secret key msk. The encryption algorithm $\mathsf{Enc}(\mathsf{msk}, m, \mathsf{i})$ takes as input a master secret key msk, a message m, and an index $\mathsf{i} \in [t]$, where $m \in (\mathcal{X}_\mathsf{i})_\lambda$, and outputs a ciphertext ct_i. The key-generation algorithm $\mathsf{KG}(\mathsf{msk}, f)$ takes as input a master secret key msk and a function $f \in \mathcal{F}_\lambda$, and outputs a functional key sk_f. The (deterministic) decryption algorithm Dec takes as input a functional key sk_f and t ciphertexts, $\mathsf{ct}_1, \ldots, \mathsf{ct}_t$, and outputs a string $z \in \mathcal{Z}_\lambda \cup \{\perp\}$.

Definition A.1 (Correctness)**.** A private-key t-input functional encryption scheme $\Pi = (\mathsf{Setup}, \mathsf{Enc}, \mathsf{KG}, \mathsf{Dec})$ for $\mathcal{F}$ is *correct* if there exists a negligible function $\mathsf{neg}(\cdot)$ such that for every $\lambda \in \mathbb{N}$, for every $f \in \mathcal{F}_\lambda$, and for every $(x_1, \ldots, x_t) \in (\mathcal{X}_1)_\lambda \times \cdots \times (\mathcal{X}_t)_\lambda$, it holds that

$$\Pr\left[\mathsf{Dec}(\mathsf{sk}_f, \mathsf{Enc}(\mathsf{msk}, x_1, 1), \ldots, \mathsf{Enc}(\mathsf{msk}, x_t, t)) = f(x_1, \ldots, x_t)\right] \geq 1 - \mathsf{neg}(\lambda),$$

where $\mathsf{msk} \leftarrow \mathsf{Setup}(1^\lambda)$, $\mathsf{sk}_f \leftarrow \mathsf{KG}(\mathsf{msk}, f)$, and the probability is taken over the internal randomness of $\mathsf{Setup}, \mathsf{Enc}$ and KG.

Next, we generalize the security definitions from Section 2.3 to the t-input case. As in Section 2.3, we start by defining the notion of a *valid t-input adversary.* Then, we define *full security* and *selective-message security.*

Definition A.2 (Valid t-input adversary)**.** A probabilistic polynomial-time algorithm $\mathcal{A}$ is a *valid t-input adversary* if for all private-key t-input functional encryption schemes $\Pi = (\mathsf{Setup}, \mathsf{KG}, \mathsf{Enc}, \mathsf{Dec})$ over a message space $\mathcal{X}_1 \times \cdots \times \mathcal{X}_t = \{(\mathcal{X}_1)_\lambda\}_{\lambda\in\mathbb{N}} \times \cdots \times \{(\mathcal{X}_t)_\lambda\}_{\lambda\in\mathbb{N}}$ and a function space $\mathcal{F} = \{\mathcal{F}_\lambda\}_{\lambda\in\mathbb{N}}$, for all $\lambda \in \mathbb{N}$ and $b \in \{0,1\}$, and for all $(f_0, f_1) \in \mathcal{F}_\lambda$ and $((x_i^0, x_i^1), i) \in \mathcal{X}_i \times \mathcal{X}_i \times \{i\}$ (where $i \in [t]$) with which $\mathcal{A}$ queries the left-or-right key-generation and encryption oracles, respectively, it holds that $f_0(x_1^0, \ldots, x_t^0) = f_1(x_1^1, \ldots, x_t^1)$.

Definition A.3 (Full security)**.** A private-key t-input functional encryption scheme $\Pi = (\mathsf{Setup}, \mathsf{KG}, \mathsf{Enc}, \mathsf{Dec})$ over a message space $\mathcal{X}_1 \times \cdots \times \mathcal{X}_t = \{(\mathcal{X}_1)_\lambda\}_{\lambda\in\mathbb{N}} \times \cdots \times \{(\mathcal{X}_t)_\lambda\}_{\lambda\in\mathbb{N}}$ and a function space $\mathcal{F} = \{\mathcal{F}_\lambda\}_{\lambda\in\mathbb{N}}$ is *fully secure* if for any valid t-input adversary $\mathcal{A}$ there exists a negligible function $\mathsf{neg}(\cdot)$ such that

$$\mathsf{Adv}^{\mathsf{fullFE_t}}_{\Pi,\mathcal{F},\mathcal{A}} \stackrel{\mathsf{def}}{=} \left|\Pr\left[\mathsf{Exp}^{\mathsf{fullFE_t}}_{\Pi,\mathcal{F},\mathcal{A}}(\lambda) = 1\right] - \frac{1}{2}\right| \leq \mathsf{neg}(\lambda),$$

for all sufficiently large $\lambda \in \mathbb{N}$, where the random variable $\mathsf{Exp}^{\mathsf{fullFE_t}}_{\Pi,\mathcal{F},\mathcal{A}}(\lambda)$ is defined via the following experiment:

1. $\mathsf{msk} \leftarrow \mathsf{Setup}(1^\lambda)$, $b \leftarrow \{0,1\}$.
2. $b' \leftarrow \mathcal{A}^{\mathsf{KG}_b(\mathsf{msk},\cdot,\cdot),\mathsf{Enc}_b(\mathsf{msk},(\cdot,\cdot),\cdot)}\left(1^\lambda\right)$.
3. If $b' = b$ then output 1, and otherwise output 0.

Definition A.4 (Selective-message security)**.** A private-key t-input functional encryption scheme $\Pi = (\mathsf{Setup}, \mathsf{KG}, \mathsf{Enc}, \mathsf{Dec})$ over a message space $\mathcal{X}_1 \times \cdots \times \mathcal{X}_t = \{(\mathcal{X}_1)_\lambda\}_{\lambda\in\mathbb{N}} \times \cdots \times \{(\mathcal{X}_t)_\lambda\}_{\lambda\in\mathbb{N}}$ and a function space $\mathcal{F} = \{\mathcal{F}_\lambda\}_{\lambda\in\mathbb{N}}$ is *selective-message secure* if for any valid t-input adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ there exists a negligible function $\mathsf{neg}(\lambda)$ such that

$$\mathsf{Adv}^{\mathsf{selFE_t}}_{\Pi,\mathcal{F},\mathcal{A}} \stackrel{\mathsf{def}}{=} \left|\Pr\left[\mathsf{Exp}^{\mathsf{selFE_t}}_{\Pi,\mathcal{F},\mathcal{A}}(\lambda) = 1\right] - \frac{1}{2}\right| \leq \mathsf{neg}(\lambda),$$

for all sufficiently large $\lambda \in \mathbb{N}$, where the random variable $\mathsf{Exp}^{\mathsf{selFE_t}}_{\Pi,\mathcal{F},\mathcal{A}}(\lambda)$ is defined via the following experiment:

1. $(\vec{x_1}, \ldots, \vec{x_t}, \mathsf{state}) \leftarrow \mathcal{A}_1\left(1^\lambda\right)$, where $\vec{x_i} = ((x_{i,1}^0, x_{i,1}^1), \ldots, (x_{i,T}^0, x_{i,T}^1))$ for $i \in [t]$.

2. $\mathsf{msk} \leftarrow \mathsf{Setup}(1^\lambda)$, $b \leftarrow \{0,1\}$.
3. $\mathsf{ct}_{i,j} \leftarrow \mathsf{Enc}(\mathsf{msk}, x^b_{i,j}, 1)$ for $i \in [t]$ and $j \in [T]$.
4. $b' \leftarrow \mathcal{A}_2^{\mathsf{KG}_b(\mathsf{msk},\cdot,\cdot)}\left(1^\lambda, \{\mathsf{ct}_{i,j}\}_{i\in[t],j\in[T]}, \mathsf{state}\right)$.
5. If $b' = b$ then output 1, and otherwise output 0.

A.2 A Selectively-Secure t-Input Scheme from any $(t-1)$-Input Scheme

In this section we generalize the construction from Section 3 by presenting a construction of a selectively-secure t-input scheme assuming any fully-secure $(t-1)$-input scheme. Let $\mathcal{F} = \{\mathcal{F}_\lambda\}_{\lambda\in\mathbb{N}}$ be a family of t-input functionalities, where for every $\lambda \in \mathbb{N}$ the set $\mathcal{F}_\lambda$ consists of functions of the form $f : (\mathcal{X}_1)_\lambda \times \cdots \times (\mathcal{X}_t)_\lambda \to \mathcal{Z}_\lambda$. Our construction relies on the following building blocks:

1. A private-key single-input functional encryption scheme $\mathsf{FE}_1 = (\mathsf{FE}_1.\mathsf{S}, \mathsf{FE}_1.\mathsf{KG}, \mathsf{FE}_1.\mathsf{E}, \mathsf{FE}_1.\mathsf{D})$.
2. A private-key $(t-1)$-input functional encryption scheme $\mathsf{FE}^{\mathsf{sel}}_{t-1} = (\mathsf{FE}^{\mathsf{sel}}_{t-1}.\mathsf{S}, \mathsf{FE}^{\mathsf{sel}}_{t-1}.\mathsf{KG}, \mathsf{FE}^{\mathsf{sel}}_{t-1}.\mathsf{E}, \mathsf{FE}^{\mathsf{sel}}_{t-1}.\mathsf{D})$.
3. A pseudorandom function family $\mathsf{PRF} = (\mathsf{PRF.Gen}, \mathsf{PRF.Eval})$.

Our scheme $\mathsf{FE}^{\mathsf{sel}}_t = (\mathsf{FE}^{\mathsf{sel}}_t.\mathsf{S}, \mathsf{FE}^{\mathsf{sel}}_t.\mathsf{KG}, \mathsf{FE}^{\mathsf{sel}}_t.\mathsf{E}, \mathsf{FE}^{\mathsf{sel}}_t.\mathsf{D})$ is defined as follows.

- **The setup algorithm.** On input the security parameter 1^λ the setup algorithm $\mathsf{FE}^{\mathsf{sel}}_t.\mathsf{S}$ samples $\mathsf{msk_{out}} \leftarrow \mathsf{FE}_1.\mathsf{S}(1^\lambda)$,$\mathsf{msk_{in}} \leftarrow \mathsf{FE}^{\mathsf{sel}}_{t-1}.\mathsf{S}(1^\lambda)$ and outputs $\mathsf{msk} = (\mathsf{msk_{out}}, \mathsf{msk_{in}})$.
- **The key-generation algorithm.** On input the master secret key msk and a function $f \in \mathcal{F}_\lambda$, the key-generation algorithm $\mathsf{FE}^{\mathsf{sel}}_t.\mathsf{KG}$ samples a random string $z \leftarrow \{0,1\}^\lambda$ and outputs $\mathsf{sk}_f \leftarrow \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk_{out}}, D_{f,\perp,z,\perp})$, where $D_{f,\perp,z,\perp}$ is a single-input function that is defined in Figure 5.

$D_{f_0,f_1,z,u}((\mathsf{msk}^\star, K, w))$:
1. If $\mathsf{msk}^\star = \perp$, output u and HALT.
2. Compute $r = \mathsf{PRF.Eval}(K, z)$.
3. Output $\mathsf{FE}^{\mathsf{sel}}_{t-1}.\mathsf{KG}(\mathsf{msk}^\star, C_{f_w}; r)$.

$C_f((x_1, x_2), x_3, \ldots, x_t)$:
1. Output $f(x_1, \ldots, x_t)$.

Figure 5: The single-input function $D_{f_0,f_1,z,u}$ and the $(t-1)$-input function C_f.

- **The encryption algorithm.** On input the master secret key msk, a message m and an index $\mathsf{i} \in [t]$, the encryption algorithm $\mathsf{FE}^{\mathsf{sel}}_t.\mathsf{E}$ has two cases:
  - If $(m, \mathsf{i}) = (x_1, 1)$, it samples a master secret key $\mathsf{msk}^\star \leftarrow \mathsf{FE}^{\mathsf{sel}}_{t-1}.\mathsf{S}(1^\lambda)$, a PRF key $K \leftarrow \mathsf{PRF.Gen}(1^\lambda)$, and a random string $s \in \{0,1\}^\lambda$, and then outputs a pair $(\mathsf{ct}_1, \mathsf{sk}_1)$ defined as follows:

$$\mathsf{ct}_1 \leftarrow \mathsf{FE}_1.\mathsf{E}(\mathsf{msk_{out}}, (\mathsf{msk}^\star, K, 0))$$
$$\mathsf{sk}_1 \leftarrow \mathsf{FE}^{\mathsf{sel}}_{t-1}.\mathsf{KG}(\mathsf{msk_{in}}, \mathsf{AGG}_{x_1,\perp,0,s,\mathsf{msk}^\star,K}),$$

    where $\mathsf{AGG}_{x,\perp,0,\mathsf{msk}^\star,K}$ is a $(t-1)$-input function that is defined in Figure 6.
  - If $(m, \mathsf{i}) = (x_i, i)$ where $i \in \{2, \ldots, t\}$, it samples a random string $\tau_i \in \{0,1\}^\lambda$, and outputs

$$\mathsf{ct}_i \leftarrow \mathsf{FE}^{\mathsf{sel}}_{t-1}.\mathsf{E}(\mathsf{msk_{in}}, (x_i, \perp, \tau_i, \perp, \perp), i-1).$$

$\mathsf{AGG}_{x_1^0,x_1^1,a,s,\mathsf{msk}^\star,K}((x_2^0,x_2^1,\tau_2,s_2,v_2),\ldots,(x_t^0,x_t^1,\tau_t,s_t,v_t))$:

1. If $s_2 = \cdots = s_t = s$ output $(v_2,\ldots,v_t)$ and HALT.
2. Set $y = y_a$ and $x = x_a$.
3. Compute $r_i = \mathsf{PRF.Eval}(K,\tau_i)$ for $2 \le i \le t$.
4. Output $(\mathsf{FE}^{\mathsf{sel}}_{t-1}.\mathsf{E}(\mathsf{msk}^\star,(x_1,x_2),1;r_2),\mathsf{FE}^{\mathsf{sel}}_{t-1}.\mathsf{E}(\mathsf{msk}^\star,x_3,2;r_3),\ldots,\mathsf{FE}^{\mathsf{sel}}_{t-1}.\mathsf{E}(\mathsf{msk}^\star,x_t,t-1;r_t))$.

Figure 6: The $(t-1)$-input function $\mathsf{AGG}_{x_1^0,x_1^1,a,s,\mathsf{msk}^\star,K}$.

- **The decryption algorithm.** On input a functional key sk_f and ciphertexts $(\mathsf{ct}_1,\mathsf{sk}_1),\mathsf{ct}_2,\ldots,\mathsf{ct}_t$, the decryption algorithm $\mathsf{FE}^{\mathsf{sel}}_t.\mathsf{D}$ computes $(\mathsf{ct}'_2,\ldots,\mathsf{ct}'_t) = \mathsf{FE}^{\mathsf{sel}}_{t-1}.\mathsf{D}(\mathsf{sk}_1,(\mathsf{ct}_2,\ldots,\mathsf{ct}_t))$, $\mathsf{sk}' = \mathsf{FE}_1.\mathsf{D}(\mathsf{sk}_f,\mathsf{ct}_1)$ and outputs $\mathsf{FE}^{\mathsf{sel}}_{t-1}.\mathsf{D}(\mathsf{sk}',(\mathsf{ct}'_2,\ldots,\mathsf{ct}'_t))$.

Theorem A.5. *Assuming that (1) FE_1 is fully secure, (2) $\mathsf{FE}^{\mathsf{sel}}_{t-1}$ is selective-message secure, and (3) PRF is a pseudorandom function family, then $\mathsf{FE}^{\mathsf{sel}}_t$ is selective-message secure.*

As in Theorem 3.1, we note that for proving that $\mathsf{FE}^{\mathsf{sel}}_t$ is selective-message secure it suffices to require selective-message security from FE_1. However, given the generic transformation for single-input schemes [ABS+14, BS15] (from selective security to adaptive security and from message security to full security, respectively), for simplifying the proof of Theorem A.5 we assume that FE_1 is fully secure.

Proof of Theorem A.5. Let $\mathcal{A} = (\mathcal{A}_1,\mathcal{A}_2)$ be a valid adversary that issues at most $T_{\mathsf{i}} = T_{\mathsf{i}}(\lambda)$ encryption queries with respect to index $\mathsf{i} \in [t]$ and at most $T_0 = T_0(\lambda)$ key-generation queries (note that $T_0,\ldots,T_t$ may be any polynomials and are not fixed in advance). We assume for simplicity and without loss of generality that $T_0 = \cdots = T_t \stackrel{\mathsf{def}}{=} T$.

We present a sequence of experiments and upper bound $\mathcal{A}$'s advantage in distinguishing each two consecutive experiments. The first experiment is the experiment $\mathsf{Exp}^{\mathsf{selFE_t}}_{\mathsf{FE}^{\mathsf{sel}}_t,\mathcal{F},\mathcal{A}}(\lambda)$ (see Definition A.4), and the last experiment is completely independent of the bit b. This enables us to prove that there exists a negligible function $\mathsf{neg}(\cdot)$ such that

$$\mathsf{Adv}^{\mathsf{selFE_t}}_{\mathsf{FE}^{\mathsf{sel}}_t,\mathcal{F},\mathcal{A}}(\lambda) \stackrel{\mathsf{def}}{=} \left|\Pr\left[\mathsf{Exp}^{\mathsf{selFE_t}}_{\mathsf{FE}^{\mathsf{sel}}_t,\mathcal{F},\mathcal{A}}(\lambda) = 1\right] - \frac{1}{2}\right| \le \mathsf{neg}(\lambda)$$

for all sufficiently large $\lambda \in \mathbb{N}$. In what follows we first describe the notation used throughout the proof, and then describe the experiments.

Notation. We denote the i^{th} ciphertext with respect to $\mathsf{i} = 1$ by $(\mathsf{sk}_{1,i},\mathsf{ct}_{1,i})$ and the i^{th} ciphertext with respect to $\mathsf{i} = \ell$, where $2 \le \ell \le t$, by $\mathsf{ct}_{\ell,i}$. We denote the i^{th} encryption query corresponding to the index $\mathsf{i} = 1$ by $(x^0_{1,i},x^1_{1,i})$, the random strings used for generating the resulting $\mathsf{sk}_{1,i}$ by s_i, the master secret key and the PRF key used for generating the resulting $\mathsf{ct}_{1,i}$ and $\mathsf{sk}_{1,i}$ by $\mathsf{msk}^\star_i$ and K_i, respectively. We denote the i^{th} encryption query corresponding to the index $\mathsf{i} = \ell$, where $2 \le \ell \le t$ by $(x^0_{\ell,i},x^1_{\ell,i})$, and the randomness used for generating the resulting $\mathsf{ct}_{\ell,i}$ by $\tau_{\ell,i}$. Finally, we denote by $(f^0_1,f^1_1),\ldots,(f^0_T,f^1_T)$ the function pairs with which the adversary queries the key-generation oracle and by $z_1,\ldots,z_T$ the corresponding random strings used for generating $\mathsf{sk}_{f_1},\ldots,\mathsf{sk}_{f_T}$.

Experiment $\mathcal{H}^{(0)}(\lambda)$. This is the original experiment corresponding to $b \leftarrow \{0,1\}$ chosen uniformly at random, namely, $\mathsf{Exp}^{\mathsf{selFE_t}}_{\mathsf{FE}^{\mathsf{sel}}_t,\mathcal{F},\mathcal{A}}(\lambda)$. In this experiment the encryptions are generated as follows.

- Ciphertexts ($i = 1, \dots, T$, $2 \le \ell \le t$):

$$\begin{aligned}
\mathsf{ct}_{1,i} &\leftarrow \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}_{\mathsf{out}}, (\mathsf{msk}_i^\star, K_i, 0)) \\
\mathsf{sk}_{1,i} &\leftarrow \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk}_{\mathsf{in}}, \mathsf{AGG}_{x_{1,i}^b, \perp, 0, s_i, \mathsf{msk}_i^\star, K_i}) \\
\mathsf{ct}_{\ell,i} &\leftarrow \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}_{\mathsf{in}}, (x_{\ell,i}^b, \perp, \tau_{\ell,i}, \perp, \perp), \ell - 1)
\end{aligned}$$

- Functional keys ($i = 1, \dots, T$):

$$\mathsf{sk}_{f_i} \leftarrow \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk}_{\mathsf{out}}, D_{f_i^b, \perp, z_i, \perp})$$

Experiment $\mathcal{H}^{(1)}(\lambda)$. This experiment is obtained from the experiment $\mathcal{H}^{(0)}(\lambda)$ by modifying the encryptions as follows. Given inputs $(x_{\ell,i}^0, x_{\ell,i}^1)$, instead of setting the field x_1 to be $\perp$ we set it to be $x_{\ell,i}^1$. The scheme has the following form:

- Ciphertexts ($i = 1, \dots, T$, $2 \le \ell \le t$):

$$\begin{aligned}
\mathsf{ct}_{1,i} &\leftarrow \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}_{\mathsf{out}}, (\mathsf{msk}_i^\star, K_i, 0)) \\
\mathsf{sk}_{1,i} &\leftarrow \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk}_{\mathsf{in}}, \mathsf{AGG}_{x_{1,i}^b, \boxed{x_{1,i}^1}, 0, s_i, \mathsf{msk}_i^\star, K_i}) \\
\mathsf{ct}_{\ell,i} &\leftarrow \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}_{\mathsf{in}}, (x_{\ell,i}^b, \boxed{x_{\ell,i}^1}, \tau_{\ell,i}, \perp, \perp), \ell - 1)
\end{aligned}$$

- Functional keys ($i = 1, \dots, T$):

$$\mathsf{sk}_{f_i} \leftarrow \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk}_{\mathsf{out}}, D_{f_i^b, \perp, z_i, \perp})$$

As in Claim 3.2, we have the following claim:

Claim A.6. *There exists a probabilistic polynomial-time adversary $\mathcal{B}^{(0)\to(1)}$ such that*

$$\left| \Pr\left[\mathcal{H}^{(0)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(1)}(\lambda) = 1\right] \right| \le \mathsf{Adv}^{\mathsf{selFE_{t-1}}}_{\mathsf{FE}^{\mathsf{sel}}_{t-1}, \mathcal{F}', \mathcal{B}^{(0)\to(1)}}(\lambda).$$

Experiment $\mathcal{H}^{(2)}(\lambda)$. This experiment is obtained from the experiment $\mathcal{H}^{(1)}(\lambda)$ by modifying the functional keys as follows. Given inputs (f^0, f^1), instead of setting the fields f_1, f_2 to be $f^b, \perp$ we set it to be f^b, f^1. The scheme has the following form:

- Ciphertexts ($i = 1, \dots, T$, $2 \le \ell \le t$):

$$\begin{aligned}
\mathsf{ct}_{1,i} &\leftarrow \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}_{\mathsf{out}}, (\mathsf{msk}_i^\star, K_i, 0)) \\
\mathsf{sk}_{1,i} &\leftarrow \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk}_{\mathsf{in}}, \mathsf{AGG}_{x_{1,i}^b, x_{1,i}^1, 0, s_i, \mathsf{msk}_i^\star, K_i}) \\
\mathsf{ct}_{\ell,i} &\leftarrow \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}_{\mathsf{in}}, (x_{\ell,i}^b, x_{\ell,i}^1, \tau_{\ell,i}, \perp, \perp), \ell - 1)
\end{aligned}$$

- Functional keys ($i = 1, \dots, T$):

$$\mathsf{sk}_{f_i} \leftarrow \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk}_{\mathsf{out}}, D_{f_i^b, \boxed{f_i^1}, z_i, \perp})$$

As in Claim 3.3 we have the following claim:

Claim A.7. *There exists a probabilistic polynomial-time adversary* $\mathcal{B}^{(1)\to(2)}$ *such that*

$$\left|\Pr\left[\mathcal{H}^{(1)}(\lambda)=1\right]-\Pr\left[\mathcal{H}^{(2)}(\lambda)=1\right]\right|\leq \mathsf{Adv}^{\mathsf{full1FE}}_{\mathsf{FE}_1,\mathcal{F}'',\mathcal{B}^{(1)\to(2)}}(\lambda).$$

Experiment $\mathcal{H}^{(3,j)}(\lambda)$. This experiment is obtained from the experiment $\mathcal{H}^{(2)}(\lambda)$ by modifying the encryptions as follows. The first $j-1$ ciphertexts are generated such that $a=1$ and $w=1$ while the rest of the encryptions are generated as before.

- Ciphertexts ($i=1,\ldots,j-1$):

$$\begin{aligned}\mathsf{ct}_{1,i} &\leftarrow \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}_{\mathsf{out}},(\mathsf{msk}_i^\star,K_i,\boxed{1}))\\ \mathsf{sk}_{1,i} &\leftarrow \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk}_{\mathsf{in}},\mathsf{AGG}_{x^b_{1,i},x^1_{1,i},\boxed{1},s_i,\mathsf{msk}_i^\star,K_i})\end{aligned}$$

- Ciphertexts ($i=j,\ldots,T$):

$$\begin{aligned}\mathsf{ct}_{1,i} &\leftarrow \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}_{\mathsf{out}},(\mathsf{msk}_i^\star,K_i,0))\\ \mathsf{sk}_{1,i} &\leftarrow \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk}_{\mathsf{in}},\mathsf{AGG}_{x^b_{1,i},x^1_{1,i},0,s_i,\mathsf{msk}_i^\star,K_i})\end{aligned}$$

- Ciphertexts ($i=1,\ldots,T$, $2\leq\ell\leq t$):

$$\mathsf{ct}_{\ell,i} \leftarrow \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}_{\mathsf{in}},(x^b_{\ell,i},x^1_{\ell,i},\tau_{\ell,i},\perp,\perp),\ell-1)$$

- Functional keys ($i=1,\ldots,T$):

$$\mathsf{sk}_{f_i} \leftarrow \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk}_{\mathsf{out}},D_{f_i^b,f_i^1,z_i,\perp})$$

Notice that $\mathcal{H}^{(3,1)}=\mathcal{H}^{(2)}$.

Experiment $\mathcal{H}^{(4,j)}(\lambda)$. This experiment is obtained from the experiment $\mathcal{H}^{(3,j)}(\lambda)$ by modifying the j^{th} ciphertext to *not* include the master secret key $\mathsf{msk}_j^\star$ and the PRF key K_j (that is, we replace them with $\perp$'s). Moreover, for every $i\in[T]$ in the i^{th} ciphertext corresponding to $\mathsf{i}=2$ we hardwire the pair (s_j,γ), where $\gamma=\mathsf{FE}_1.\mathsf{E}(\mathsf{msk}_j^\star,(x^b_{1,j},x^b_{2,i});\mathsf{PRF.Eval}(K_j,\tau_{2,i}))$. Similarly, for every $i\in[T]$ in the i^{th} ciphertext corresponding to $\mathsf{i}=\ell>2$ we hardwire the pair (s_j,γ), where $\gamma=\mathsf{FE}_1.\mathsf{E}(\mathsf{msk}_j^\star,x^b_{\ell,i};\mathsf{PRF.Eval}(K_j,\tau_{\ell,i}))$

- Ciphertexts ($i=1,\ldots,j-1$):

$$\begin{aligned}\mathsf{ct}_{1,i} &\leftarrow \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}_{\mathsf{out}},(\mathsf{msk}_i^\star,K_i,1))\\ \mathsf{sk}_{1,i} &\leftarrow \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk}_{\mathsf{in}},\mathsf{AGG}_{x^b_{1,i},x^1_{1,i},1,s_i,\mathsf{msk}_i^\star,K_i})\end{aligned}$$

- Ciphertexts ($i=j$):

$$\begin{aligned}\mathsf{ct}_{1,i} &\leftarrow \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}_{\mathsf{out}},(\mathsf{msk}_i^\star,K_i,0))\\ \mathsf{sk}_{1,i} &\leftarrow \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk}_{\mathsf{in}},\mathsf{AGG}_{x^b_{1,i},x^1_{1,i},0,s_i,\boxed{\perp},\boxed{\perp}})\end{aligned}$$

- Ciphertexts ($i=j+1,\ldots,T$):

$$\begin{aligned}\mathsf{ct}_{1,i} &\leftarrow \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}_{\mathsf{out}},(\mathsf{msk}_i^\star,K_i,0))\\ \mathsf{sk}_{1,i} &\leftarrow \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk}_{\mathsf{in}},\mathsf{AGG}_{x^b_{1,i},x^1_{1,i},0,s_i,\mathsf{msk}_i^\star,K_i})\end{aligned}$$

- Ciphertexts $(i = 1, \ldots, T)$:

$$\begin{aligned} \mathsf{ct}_{2,i} &\leftarrow \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}_{\mathsf{in}}, (x^b_{2,i}, x^1_{2,i}, \tau_{2,i}, \boxed{s_j, \gamma}), 1) \\ \gamma &= \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}^\star_j, (x^b_{1,j}, x^b_{2,i}); \mathsf{PRF.Eval}(K_j, \tau_{2,i})) \end{aligned}$$

- Ciphertexts $(i = 1, \ldots, T,\ 3 \leq \ell \leq t)$:

$$\begin{aligned} \mathsf{ct}_{\ell,i} &\leftarrow \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}_{\mathsf{in}}, (x^b_{\ell,i}, x^1_{\ell,i}, \tau_{\ell,i}, \boxed{s_j, \gamma}), \ell - 1) \\ \gamma &= \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}^\star_j, x^b_{\ell,i}; \mathsf{PRF.Eval}(K_j, \tau_{\ell,i})) \end{aligned}$$

- Functional keys $(i = 1, \ldots, T)$:

$$\mathsf{sk}_{f_i} \leftarrow \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk}_{\mathsf{out}}, D_{f^b_i, f^1_i, z_i, \perp})$$

As in Claim 3.4 we have the following claim:

Claim A.8. *There exists a probabilistic polynomial-time adversary $\mathcal{B}^{(3,j)\to(4,j)}$ such that*

$$\left| \Pr\left[\mathcal{H}^{(3,j)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(4,j)}(\lambda) = 1\right] \right| \leq \mathsf{Adv}^{\mathsf{selFE_{t-1}}}_{\mathsf{FE}^{\mathsf{sel}}_{t-1}, \mathcal{F}', \mathcal{B}^{(3,j)\to(4,j)}}(\lambda).$$

Experiment $\boldsymbol{\mathcal{H}^{(5,j)}(\lambda)}$. This experiment is obtained from the experiment $\mathcal{H}^{(4,j)}(\lambda)$ by modifying the j^{th} ciphertext as follows. We replace $(\mathsf{msk}^\star_j, K_j, 0)$ with $(\perp, \perp, 0)$. Moreover, in the i^{th} functional key corresponding to the functions (f^0_i, f^1_i) we hardwire the value $\delta = \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk}^\star_j, C_{f^b_i};$ $\mathsf{PRF.Eval}(K_j, z_i))$.

- Ciphertexts $(i = 1, \ldots, j - 1)$:

$$\begin{aligned} \mathsf{ct}_{1,i} &\leftarrow \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}_{\mathsf{out}}, (\mathsf{msk}^\star_i, K_i, 1)) \\ \mathsf{sk}_{1,i} &\leftarrow \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk}_{\mathsf{in}}, \mathsf{AGG}_{x^b_{1,i}, x^1_{1,i}, 1, s_i, \mathsf{msk}^\star_i, K_i}) \end{aligned}$$

- Ciphertexts $(i = j)$:

$$\begin{aligned} \mathsf{ct}_{1,i} &\leftarrow \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}_{\mathsf{out}}, (\boxed{\perp}, \boxed{\perp}, 0)) \\ \mathsf{sk}_{1,i} &\leftarrow \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk}_{\mathsf{in}}, \mathsf{AGG}_{x^b_{1,i}, x^1_{1,i}, 0, s_i, \perp, \perp}) \end{aligned}$$

- Ciphertexts $(i = j + 1, \ldots, T)$:

$$\begin{aligned} \mathsf{ct}_{1,i} &\leftarrow \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}_{\mathsf{out}}, (\mathsf{msk}^\star_i, K_i, 0)) \\ \mathsf{sk}_{1,i} &\leftarrow \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk}_{\mathsf{in}}, \mathsf{AGG}_{x^b_{1,i}, x^1_{1,i}, 0, s_i, \mathsf{msk}^\star_i, K_i}) \end{aligned}$$

- Ciphertexts $(i = 1, \ldots, T)$:

$$\begin{aligned} \mathsf{ct}_{2,i} &\leftarrow \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}_{\mathsf{in}}, (x^b_{2,i}, x^1_{2,i}, \tau_{2,i}, s_j, \gamma), 1) \\ \gamma &= \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}^\star_j, (x^b_{1,j}, x^b_{2,i}); \mathsf{PRF.Eval}(K_j, \tau_{2,i})) \end{aligned}$$

- Ciphertexts $(i = 1, \ldots, T,\ 3 \leq \ell \leq t)$:

$$\begin{aligned} \mathsf{ct}_{\ell,i} &\leftarrow \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}_{\mathsf{in}}, (x^b_{\ell,i}, x^1_{\ell,i}, \tau_{\ell,i}, s_j, \gamma), \ell - 1) \\ \gamma &= \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}^\star_j, x^b_{\ell,i}; \mathsf{PRF.Eval}(K_j, \tau_{\ell,i})) \end{aligned}$$

- Functional keys ($i = 1, \ldots, T$):

$$\mathsf{sk}_{f_i} \leftarrow \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk_{out}}, D_{f_i^b, f_i^1, z_i, \boxed{\delta}})$$
$$\delta = \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk}_j^\star, C_{f_i^b}; \mathsf{PRF.Eval}(K_j, z_i))$$

As in Claim 3.5 we have the following claim:

Claim A.9. *There exists a probabilistic polynomial-time adversary $\mathcal{B}^{(4,j)\to(5,j)}$ such that*

$$\left|\Pr\left[\mathcal{H}^{(4,j)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(5,j)}(\lambda) = 1\right]\right| \le \mathsf{Adv}^{\mathsf{full1FE}}_{\mathsf{FE}_1, \mathcal{F}', \mathcal{B}^{(4,j)\to(5,j)}}(\lambda).$$

Experiment $\mathcal{H}^{(6,j)}(\lambda)$. This experiment is obtained from the experiment $\mathcal{H}^{(5,j)}(\lambda)$ by modifying the hardwired value of the γ's and the δ's to use randomness sampled uniformly at random rather than randomness generated using a PRF.

- Ciphertexts ($i = 1, \ldots, j-1$):

$$\mathsf{ct}_{1,i} \leftarrow \mathsf{FE}_1.\mathsf{E}(\mathsf{msk_{out}}, (\mathsf{msk}_i^\star, K_i, 1))$$
$$\mathsf{sk}_{1,i} \leftarrow \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk_{in}}, \mathsf{AGG}_{x_{1,i}^b, x_{1,i}^1, 1, s_i, \mathsf{msk}_i^\star, K_i})$$

- Ciphertexts ($i = j$):

$$\mathsf{ct}_{1,i} \leftarrow \mathsf{FE}_1.\mathsf{E}(\mathsf{msk_{out}}, (\perp, \perp, 0))$$
$$\mathsf{sk}_{1,i} \leftarrow \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk_{in}}, \mathsf{AGG}_{x_{1,i}^b, x_{1,i}^1, 0, s_i, \perp, \perp})$$

- Ciphertexts ($i = j+1, \ldots, T$):

$$\mathsf{ct}_{1,i} \leftarrow \mathsf{FE}_1.\mathsf{E}(\mathsf{msk_{out}}, (\mathsf{msk}_i^\star, K_i, 0))$$
$$\mathsf{sk}_{1,i} \leftarrow \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk_{in}}, \mathsf{AGG}_{x_{1,i}^b, x_{1,i}^1, 0, s_i, \mathsf{msk}_i^\star, K_i})$$

- Ciphertexts ($i = 1, \ldots, T$):

$$\mathsf{ct}_{2,i} \leftarrow \mathsf{FE}_1.\mathsf{E}(\mathsf{msk_{in}}, (x_{2,i}^b, x_{2,i}^1, \tau_{2,i}, s_j, \gamma), 1)$$
$$\boxed{\gamma} = \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}_j^\star, (x_{1,j}^b, x_{2,i}^b))$$

- Ciphertexts ($i = 1, \ldots, T$, $3 \le \ell \le t$):

$$\mathsf{ct}_{\ell,i} \leftarrow \mathsf{FE}_1.\mathsf{E}(\mathsf{msk_{in}}, (x_{\ell,i}^b, x_{\ell,i}^1, \tau_{\ell,i}, s_j, \gamma), \ell - 1)$$
$$\boxed{\gamma} = \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}_j^\star, x_{\ell,i}^b)$$

- Functional keys ($i = 1, \ldots, T$):

$$\mathsf{sk}_{f_i} \leftarrow \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk_{out}}, D_{f_i^b, f_i^1, z_i, \delta})$$
$$\boxed{\delta} = \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk}_j^\star, C_{f_i^b})$$

As in Claim 3.6 we have the following claim:

Claim A.10. *For every $j \in [T]$ there exists a probabilistic polynomial-time adversary $\mathcal{B}^{(5,j)\to(6,j)}$ such that*

$$\left|\Pr\left[\mathcal{H}^{(5,j)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(6,j)}(\lambda) = 1\right]\right| \le \mathsf{Adv}_{\mathsf{PRF}, \mathcal{B}^{(5,j)\to(6,j)}}(\lambda).$$

Experiment $\mathcal{H}^{(7,j)}(\lambda)$. This experiment is obtained from the experiment $\mathcal{H}^{(6,j)}(\lambda)$ by modifying the ciphertext as follows. In the i^{th} ciphertext corresponding to $\mathsf{i} = 2$ we embed in γ the encryption of $(x^1_{1,j}, x^1_{2,i})$ rather than $(x^b_{1,j}, x^b_{2,i})$. In the i^{th} ciphertext corresponding to $\mathsf{i} = \ell > 2$ we embed in γ the encryption of $x^1_{\ell,i}$ rather than $x^b_{\ell,i}$. Moreover, we replace the circuit embedded in δ in the i^{th} functional key to be $C_{f^1_i}$ rather than $C_{f^b_i}$.

- Ciphertexts ($i = 1, \ldots, j-1$):

$$\begin{aligned}\mathsf{ct}_{1,i} &\leftarrow \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}_{\mathsf{out}}, (\mathsf{msk}^\star_i, K_i, 1))\\ \mathsf{sk}_{1,i} &\leftarrow \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk}_{\mathsf{in}}, \mathsf{AGG}_{x^b_{1,i}, x^1_{1,i}, 1, s_i, \mathsf{msk}^\star_i, K_i})\end{aligned}$$

- Ciphertexts ($i = j$):

$$\begin{aligned}\mathsf{ct}_{1,i} &\leftarrow \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}_{\mathsf{out}}, (\bot, \bot, 0))\\ \mathsf{sk}_{1,i} &\leftarrow \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk}_{\mathsf{in}}, \mathsf{AGG}_{x^b_{1,i}, x^1_{1,i}, 0, s_i, \bot, \bot})\end{aligned}$$

- Ciphertexts ($i = j+1, \ldots, T$):

$$\begin{aligned}\mathsf{ct}_{1,i} &\leftarrow \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}_{\mathsf{out}}, (\mathsf{msk}^\star_i, K_i, 0))\\ \mathsf{sk}_{1,i} &\leftarrow \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk}_{\mathsf{in}}, \mathsf{AGG}_{x^b_{1,i}, x^1_{1,i}, 0, s_i, \mathsf{msk}^\star_i, K_i})\end{aligned}$$

- Ciphertexts ($i = 1, \ldots, T$):

$$\begin{aligned}\mathsf{ct}_{2,i} &\leftarrow \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}_{\mathsf{in}}, (x^b_{2,i}, x^1_{2,i}, \tau_{2,i}, s_j, \gamma), 1)\\ \gamma &= \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}^\star_j, \boxed{(x^1_{1,j}, x^1_{2,i})})\end{aligned}$$

- Ciphertexts ($i = 1, \ldots, T$, $3 \le \ell \le t$):

$$\begin{aligned}\mathsf{ct}_{\ell,i} &\leftarrow \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}_{\mathsf{in}}, (x^b_{\ell,i}, x^1_{\ell,i}, \tau_{\ell,i}, s_j, \gamma), \ell - 1)\\ \gamma &= \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}^\star_j, \boxed{x^1_{\ell,i}})\end{aligned}$$

- Functional keys ($i = 1, \ldots, T$):

$$\begin{aligned}\mathsf{sk}_{f_i} &\leftarrow \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk}_{\mathsf{out}}, D_{f^b_i, f^1_i, z_i, \delta})\\ \delta &= \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk}^\star_j, \boxed{C_{f^1_i}})\end{aligned}$$

As in Claim 3.7 we have the following claim:

Claim A.11. *There exists a probabilistic polynomial-time adversary $\mathcal{B}^{(6,j)\to(7,j)}$ such that*

$$\left|\Pr\left[\mathcal{H}^{(6,j)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(7,j)}(\lambda) = 1\right]\right| \le \mathsf{Adv}^{\mathsf{full1FE}}_{\mathsf{FE}_1, \mathcal{F}', \mathcal{B}^{(6,j)\to(7,j)}}(\lambda).$$

Experiment $\mathcal{H}^{(8,j)}(\lambda)$. This experiment is obtained from the experiment $\mathcal{H}^{(7,j)}(\lambda)$ by modifying the hardwired values in the γ's and in the δ's to use randomness generated using a PRF rather than randomness sampled uniformly at random.

- Ciphertexts ($i = 1, \ldots, j-1$):

$$\begin{aligned}\mathsf{ct}_{1,i} &\leftarrow \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}_{\mathsf{out}}, (\mathsf{msk}^\star_i, K_i, 1))\\ \mathsf{sk}_{1,i} &\leftarrow \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk}_{\mathsf{in}}, \mathsf{AGG}_{x^b_{1,i}, x^1_{1,i}, 1, s_i, \mathsf{msk}^\star_i, K_i})\end{aligned}$$

- Ciphertexts $(i = j)$:

$$\begin{aligned}\mathsf{ct}_{1,i} &\leftarrow \mathsf{FE}_1.\mathsf{E}(\mathsf{msk_{out}}, (\perp, \perp, 0))\\ \mathsf{sk}_{1,i} &\leftarrow \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk_{in}}, \mathsf{AGG}_{x^b_{1,i}, x^1_{1,i}, 0, s_i, \perp, \perp})\end{aligned}$$

- Ciphertexts $(i = j+1, \dots, T)$:

$$\begin{aligned}\mathsf{ct}_{1,i} &\leftarrow \mathsf{FE}_1.\mathsf{E}(\mathsf{msk_{out}}, (\mathsf{msk}^\star_i, K_i, 0))\\ \mathsf{sk}_{1,i} &\leftarrow \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk_{in}}, \mathsf{AGG}_{x^b_{1,i}, x^1_{1,i}, 0, s_i, \mathsf{msk}^\star_i, K_i})\end{aligned}$$

- Ciphertexts $(i = 1, \dots, T)$:

$$\begin{aligned}\mathsf{ct}_{2,i} &\leftarrow \mathsf{FE}_1.\mathsf{E}(\mathsf{msk_{in}}, (x^b_{2,i}, x^1_{2,i}, \tau_{2,i}, s_j, \gamma), 1)\\ \boxed{\gamma} &= \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}^\star_j, (x^1_{1,j}, x^1_{2,i}); \mathsf{PRF.Eval}(K_j, \tau_{2,i}))\end{aligned}$$

- Ciphertexts $(i = 1, \dots, T,\ 3 \le \ell \le t)$:

$$\begin{aligned}\mathsf{ct}_{\ell,i} &\leftarrow \mathsf{FE}_1.\mathsf{E}(\mathsf{msk_{in}}, (x^b_{\ell,i}, x^1_{\ell,i}, \tau_{\ell,i}, s_j, \gamma), \ell-1)\\ \boxed{\gamma} &= \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}^\star_j, x^1_{\ell,i}; \mathsf{PRF.Eval}(K_j, \tau_{\ell,i}))\end{aligned}$$

- Functional keys $(i = 1, \dots, T)$:

$$\begin{aligned}\mathsf{sk}_{f_i} &\leftarrow \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk_{out}}, D_{f^b_i, f^1_i, z_i, \delta})\\ \boxed{\delta} &= \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk}^\star_j, C_{f^1_i}; \mathsf{PRF.Eval}(K_j, z_i))\end{aligned}$$

As in Claim 3.8 we have the following claim:

Claim A.12. *There exists a probabilistic polynomial-time adversary $\mathcal{B}^{(7,j)\to(8,j)}$ such that*

$$\left|\Pr\left[\mathcal{H}^{(7,j)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(8,j)}(\lambda) = 1\right]\right| \le \mathsf{Adv}_{\mathsf{PRF}, \mathcal{B}^{(7,j)\to(8,j)}}(\lambda).$$

Experiment $\mathcal{H}^{(9,j)}(\lambda)$. This experiment is obtained from the experiment $\mathcal{H}^{(8,j)}(\lambda)$ by modifying the j^{th} ciphertext to contain the pair $(\mathsf{msk}^\star_j, K_j)$. Moreover, in the functional key corresponding to the function f_i for $i \in [T]$ we remove the hardwired value δ.

- Ciphertexts $(i = 1, \dots, j-1)$:

$$\begin{aligned}\mathsf{ct}_{1,i} &\leftarrow \mathsf{FE}_1.\mathsf{E}(\mathsf{msk_{out}}, (\mathsf{msk}^\star_i, K_i, 1))\\ \mathsf{sk}_{1,i} &\leftarrow \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk_{in}}, \mathsf{AGG}_{x^b_{1,i}, x^1_{1,i}, 1, s_i, \mathsf{msk}^\star_i, K_i})\end{aligned}$$

- Ciphertexts $(i = j)$:

$$\begin{aligned}\mathsf{ct}_{1,i} &\leftarrow \mathsf{FE}_1.\mathsf{E}(\mathsf{msk_{out}}, (\boxed{\mathsf{msk}^\star_i}, \boxed{K_i}, \boxed{1}))\\ \mathsf{sk}_{1,i} &\leftarrow \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk_{in}}, \mathsf{AGG}_{x^b_{1,i}, x^1_{1,i}, 0, s_i, \perp, \perp})\end{aligned}$$

- Ciphertexts $(i = j+1, \dots, T)$:

$$\begin{aligned}\mathsf{ct}_{1,i} &\leftarrow \mathsf{FE}_1.\mathsf{E}(\mathsf{msk_{out}}, (\mathsf{msk}^\star_i, K_i, 0))\\ \mathsf{sk}_{1,i} &\leftarrow \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk_{in}}, \mathsf{AGG}_{x^b_{1,i}, x^1_{1,i}, 0, s_i, \mathsf{msk}^\star_i, K_i})\end{aligned}$$

- Ciphertexts ($i = 1, \dots, T$):

$$\mathsf{ct}_{2,i} \leftarrow \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}_{\mathsf{in}}, (x^b_{2,i}, x^1_{2,i}, \tau_{2,i}, s_j, \gamma), 1)$$
$$\gamma = \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}^\star_j, (x^1_{1,j}, x^1_{2,i}); \mathsf{PRF.Eval}(K_j, \tau_{2,i}))$$

- Ciphertexts ($i = 1, \dots, T$, $3 \leq \ell \leq t$):

$$\mathsf{ct}_{\ell,i} \leftarrow \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}_{\mathsf{in}}, (x^b_{\ell,i}, x^1_{\ell,i}, \tau_{\ell,i}, s_j, \gamma), \ell - 1)$$
$$\gamma = \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}^\star_j, x^1_{\ell,i}; \mathsf{PRF.Eval}(K_j, \tau_{\ell,i}))$$

- Functional keys ($i = 1, \dots, T$):

$$\mathsf{sk}_{f_i} \leftarrow \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk}_{\mathsf{out}}, D_{f^b_i, f^1_i, z_i, \boxed{\perp}})$$

As in Claim 3.9 we have the following claim:

Claim A.13. *There exists a probabilistic polynomial-time adversary $\mathcal{B}^{(8,j)\to(9,j)}$ such that*

$$\left| \Pr\left[\mathcal{H}^{(8,j)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(9,j)}(\lambda) = 1\right] \right| \leq \mathsf{Adv}^{\mathsf{full1FE}}_{\mathsf{FE}_1, \mathcal{F}', \mathcal{B}^{(8,j)\to(9,j)}}(\lambda).$$

Experiment $\mathcal{H}^{(10,j)}(\lambda)$. This experiment is obtained from the experiment $\mathcal{H}^{(9,j)}(\lambda)$ by modifying the ciphertexts as follows. For the i^{th} ciphertext corresponding to $\mathsf{i} = \ell \geq 2$ we remove the hardwired pair (s_j, γ). Moreover, we encrypt the j^{th} ciphertext corresponding to $\mathsf{i} = 1$ with $w = 1$. Notice that $\mathcal{H}^{(10,j)} = \mathcal{H}^{(3,j+1)}$.

- Ciphertexts ($i = 1, \dots, \boxed{j}$):

$$\mathsf{ct}_{1,i} \leftarrow \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}_{\mathsf{out}}, (\mathsf{msk}^\star_i, K_i, 1))$$
$$\mathsf{sk}_{1,i} \leftarrow \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk}_{\mathsf{in}}, \mathsf{AGG}_{x^b_{1,i}, x^1_{1,i}, 1, s_i, \mathsf{msk}^\star_i, K_i})$$

- Ciphertexts ($i = j + 1, \dots, T$):

$$\mathsf{ct}_{1,i} \leftarrow \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}_{\mathsf{out}}, (\mathsf{msk}^\star_i, K_i, 0))$$
$$\mathsf{sk}_{1,i} \leftarrow \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk}_{\mathsf{in}}, \mathsf{AGG}_{x^b_{1,i}, x^1_{1,i}, 0, s_i, \mathsf{msk}^\star_i, K_i})$$

- Ciphertexts ($i = 1, \dots, T$, $2 \leq \ell \leq t$):

$$\mathsf{ct}_{\ell,i} \leftarrow \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}_{\mathsf{in}}, (x^b_{\ell,i}, x^1_{\ell,i}, \tau_{\ell,i}, \boxed{\perp, \perp}), \ell - 1)$$

- Functional keys ($i = 1, \dots, T$):

$$\mathsf{sk}_{f_i} \leftarrow \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk}_{\mathsf{out}}, D_{f^b_i, f^1_i, z_i, \perp})$$

As in Claim 3.10 we have the following claim:

Claim A.14. *There exists a probabilistic polynomial-time adversary $\mathcal{B}^{(9,j)\to(10,j)}$ such that*

$$\left| \Pr\left[\mathcal{H}^{(9,j)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(10,j)}(\lambda) = 1\right] \right| \leq \mathsf{Adv}^{\mathsf{selFE_{t-1}}}_{\mathsf{FE}^{\mathsf{sel}}_{t-1}, \mathcal{F}', \mathcal{B}^{(9,j)\to(10,j)}}(\lambda).$$

Experiment $\mathcal{H}^{(11)}(\lambda)$. This experiment is obtained from the experiment $\mathcal{H}^{(3,T+1)}(\lambda)$ by modifying the ciphertexts *not* to include f_i^b at all.

- Ciphertexts ($i = 1, \ldots, T$):

$$\mathsf{ct}_{1,i} \leftarrow \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}_{\mathsf{out}}, (\mathsf{msk}_i^\star, K_i, 1))$$
$$\mathsf{sk}_{1,i} \leftarrow \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk}_{\mathsf{in}}, \mathsf{AGG}_{x_{1,i}^b, x_{1,i}^1, 1, s_i, \mathsf{msk}_i^\star, K_i})$$

- Ciphertexts ($i = 1, \ldots, T$, $2 \leq \ell \leq t$):

$$\mathsf{ct}_{\ell,i} \leftarrow \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}_{\mathsf{in}}, (x_{\ell,i}^b, x_{\ell,i}^1, \tau_{\ell,i}, \bot, \bot), \ell - 1)$$

- Functional keys ($i = 1, \ldots, T$):

$$\mathsf{sk}_{f_i} \leftarrow \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk}_{\mathsf{out}}, D_{\boxed{\bot}, f_i^1, z_i, \bot})$$

As in Claim 3.11 we have the following claim:

Claim A.15. *There exists a probabilistic polynomial-time adversary $\mathcal{B}^{(3,T+1)\to(11)}$ such that*

$$\left|\Pr\left[\mathcal{H}^{(3,T+1)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(11)}(\lambda) = 1\right]\right| \leq \mathsf{Adv}^{\mathsf{full1FE}}_{\mathsf{FE}_1, \mathcal{F}', \mathcal{B}^{(3,T+1)\to(11)}}(\lambda).$$

Experiment $\mathcal{H}^{(12)}(\lambda)$. This experiment is obtained from the experiment $\mathcal{H}^{(11)}(\lambda)$ by modifying the ciphertexts *not* to include $x_{\mathsf{i},i}^b$ at all for $\mathsf{i} \in [t]$ and $i \in [T]$. Notice that this experiment is completely independent of the bit b, and therefore $\Pr[\mathcal{H}^{(12)}(\lambda) = 1] = 1/2$.

- Ciphertexts ($i = 1, \ldots, T$):

$$\mathsf{ct}_{1,i} \leftarrow \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}_{\mathsf{out}}, (\mathsf{msk}_i^\star, K_i, 1))$$
$$\mathsf{sk}_{1,i} \leftarrow \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk}_{\mathsf{in}}, \mathsf{AGG}_{\boxed{\bot}, x_{1,i}^1, 1, s_i, \mathsf{msk}_i^\star, K_i})$$

- Ciphertexts ($i = 1, \ldots, T$, $2 \leq \ell \leq t$):

$$\mathsf{ct}_{\ell,i} \leftarrow \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}_{\mathsf{in}}, (\boxed{\bot}, x_{\ell,i}^1, \tau_{\ell,i}, \bot, \bot), \ell - 1)$$

- Functional keys ($i = 1, \ldots, T$):

$$\mathsf{sk}_{f_i} \leftarrow \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk}_{\mathsf{out}}, D_{\bot, f_i^1, z_i, \bot})$$

As in Claim 3.12 we have the following claim:

Claim A.16. *There exists a probabilistic polynomial-time adversary $\mathcal{B}^{(11)\to(12)}$ such that*

$$\left|\Pr\left[\mathcal{H}^{(11)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(12)}(\lambda) = 1\right]\right| \leq \mathsf{Adv}^{\mathsf{selFE_{t-1}}}_{\mathsf{FE}^{\mathsf{sel}}_{t-1}, \mathcal{F}', \mathcal{B}^{(11)\to(12)}}(\lambda).$$

Finally, putting together Claims A.6–A.16 with the facts that $\mathcal{H}^{(0)}(\lambda) = \mathsf{Exp}^{\mathsf{selFE_t}}_{\mathsf{FE}^{\mathsf{sel}}_t,\mathcal{F},\mathcal{A}}(\lambda)$, $\mathcal{H}^{(2)}(\lambda) = \mathcal{H}^{(3,1)}(\lambda)$ and $\Pr\left[\mathcal{H}^{(12)}(\lambda) = 1\right] = 1/2$, we observe that

$$\begin{aligned}
\mathsf{Adv}^{\mathsf{selFE_t}}_{\mathsf{FE}^{\mathsf{sel}}_t,\mathcal{F},\mathcal{A}} &\stackrel{\mathsf{def}}{=} \left|\Pr\left[\mathsf{Exp}^{\mathsf{selFE_t}}_{\mathsf{FE}^{\mathsf{sel}}_t,\mathcal{F},\mathcal{A}}(\lambda) = 1\right] - \frac{1}{2}\right| \\
&= \left|\Pr\left[\mathcal{H}^{(0)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(12)}(\lambda) = 1\right]\right| \\
&\leq \sum_{i=0}^{1} \left|\Pr\left[\mathcal{H}^{(i)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(i+1)}(\lambda) = 1\right]\right| \\
&\quad + \sum_{i=1}^{T}\sum_{j=3}^{9} \left|\Pr\left[\mathcal{H}^{(j,i)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(j+1,i)}(\lambda) = 1\right]\right| \\
&\quad + \left|\Pr\left[\mathcal{H}^{(3,T+1)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(11)}(\lambda) = 1\right]\right| \\
&\quad + \left|\Pr\left[\mathcal{H}^{(11)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(12)}(\lambda) = 1\right]\right| \\
&\leq \mathsf{neg}(\lambda).
\end{aligned}$$

■

A.3 From Selective to Adaptive Security for *t*-Input Schemes

In this section we generalize the construction from Section 4 to get a fully-secure t-input functional encryption scheme assuming any fully-secure $(t-1)$-input functional encryption scheme and any selectively-secure t-input functional encryption scheme. Our construction relies on the following building blocks:

1. A private-key single-input functional encryption scheme $\mathsf{FE}_1 = (\mathsf{FE}_1.\mathsf{S}, \mathsf{FE}_1.\mathsf{KG}, \mathsf{FE}_1.\mathsf{E}, \mathsf{FE}_1.\mathsf{D})$.
2. A private-key $(t-1)$-input functional encryption scheme $\mathsf{FE}_{t-1} = (\mathsf{FE}_{t-1}.\mathsf{S}, \mathsf{FE}_{t-1}.\mathsf{KG}, \mathsf{FE}_{t-1}.\mathsf{E}, \mathsf{FE}_{t-1}.\mathsf{D})$.
3. A private-key t-input functional encryption scheme $\mathsf{FE}^{\mathsf{sel}}_t = (\mathsf{FE}^{\mathsf{sel}}_t.\mathsf{S}, \mathsf{FE}^{\mathsf{sel}}_t.\mathsf{KG}, \mathsf{FE}^{\mathsf{sel}}_t.\mathsf{E}, \mathsf{FE}^{\mathsf{sel}}_t.\mathsf{D})$.
4. A puncturable pseudorandom function family $\mathsf{PRF} = (\mathsf{PRF.Gen}, \mathsf{PRF.Eval}, \mathsf{PRF.Punc})$.

The scheme $\mathsf{FE}_t = (\mathsf{FE}_t.\mathsf{S}, \mathsf{FE}_t.\mathsf{KG}, \mathsf{FE}_t.\mathsf{E}, \mathsf{FE}_t.\mathsf{D})$ is defined as follows.

- **The setup algorithm.** On input the security parameter 1^λ the setup algorithm $\mathsf{FE}_t.\mathsf{S}$ samples $\mathsf{msk}_{t-1} \leftarrow \mathsf{FE}_{t-1}.\mathsf{S}(1^\lambda)$ and $\mathsf{msk}_t \leftarrow \mathsf{FE}^{\mathsf{sel}}_t.\mathsf{S}(1^\lambda)$ and then outputs $\mathsf{msk} = (\mathsf{msk}_{t-1}, \mathsf{msk}_t)$.
- **The key-generation algorithm.** On input the master secret key msk and a function $f \in \mathcal{F}_\lambda$, the key-generation algorithm $\mathsf{FE}_t.\mathsf{KG}$ outputs $\mathsf{sk}_f \leftarrow \mathsf{FE}^{\mathsf{sel}}_t.\mathsf{KG}(\mathsf{msk}_t, D_{f,\perp,1,\underbrace{\perp,\ldots,\perp}_{t \text{ times}},\perp})$, where $D_{f,\perp,1,\underbrace{\perp,\ldots,\perp}_{t \text{ times}},\perp}$ is a t-input function that is defined in Figure 7.

$\boldsymbol{D_{f_0,f_1,\mathsf{c},\tau'_1,\ldots,\tau'_t,u}((K^{\mathsf{msk}}, K^{\mathsf{key}}, \tau_1, \mathsf{thr}_2,\ldots,\mathsf{thr}_t),(\mathsf{c}_2,\tau_2),\ldots,(\mathsf{c}_t,\tau_t))}$:

1. If $\tau'_i = \tau_i$ for all $i \in [t]$, output u and HALT.
2. Compute $r = \mathsf{PRF.Eval}(K^{\mathsf{msk}}, \tau_2 \ldots \tau_t)$.
3. Compute $r' = \mathsf{PRF.Eval}(K^{\mathsf{key}}, \tau_2 \ldots \tau_t)$.
4. Compute $\mathsf{msk}_{\tau_1,\ldots,\tau_t} = \mathsf{FE}_1.\mathsf{S}(1^\lambda; r)$.
5. For $i = 1,\ldots,t$ do:
   (a) If $\mathsf{c}_i < \mathsf{thr}_i$ then set $f = f_1$ and exit loop.
   (b) If $\mathsf{c}_i > \mathsf{thr}_i$ then set $f = f_0$ and exit loop.
   (c) If $\mathsf{c}_i = \mathsf{thr}_i$ and $i < t$ continue to next iteration (with $i = i+1$).
   (d) If $\mathsf{c}_i = \mathsf{thr}_i$ and $i = t$ set $f = f_1$.
6. Output $\mathsf{FE}_1.\mathsf{KG}(\mathsf{msk}_{\tau_1,\ldots,\tau_t}, C_f; r')$.

$\boldsymbol{C_f((x_1,\ldots,x_t))}$:

1. Output $f(x_1,\ldots,x_t)$.

Figure 7: The t-input function $D_{f_0,f_1,\mathsf{c},\tau'_1,\ldots,\tau'_t,u}$ and the single-input function C_f.

- **The encryption algorithm.** On input the master secret key msk, a message m and an index $\mathsf{i} \in [2]$, the encryption algorithm $\mathsf{FE}_{t-1}.\mathsf{E}$ has two cases:
  – If $(m,\mathsf{i}) = (x_1, 1)$, it samples $\tau_1 \leftarrow \{0,1\}^\lambda$ uniformly at random, three PRF keys K^{enc}, $K^{\mathsf{key}}, K^{\mathsf{msk}} \leftarrow \mathsf{PRF.Gen}(1^\lambda)$ and outputs a pair $(\mathsf{ct}_1, \mathsf{sk}_1)$ defined as follows:
  $$\mathsf{ct}_1 \leftarrow \mathsf{FE}^{\mathsf{sel}}_t.\mathsf{E}(\mathsf{msk}_t, (K^{\mathsf{msk}}, K^{\mathsf{key}}, \tau_1, \underbrace{0,\ldots,0}_{t-1 \text{ times}}), 1)$$
  $$\mathsf{sk}_1 \leftarrow \mathsf{FE}_{t-1}.\mathsf{KG}(\mathsf{msk}_{t-1}, \mathsf{AGG}_{x_1,\perp,\underbrace{0,\ldots,0}_{t-1 \text{ times}},\tau_1,K^{\mathsf{msk}},K^{\mathsf{enc}},\underbrace{\perp,\ldots,\perp}_{t-1 \text{ times}},\perp})$$
  where the single-input function $\mathsf{AGG}_{x_1,\perp,\underbrace{0,\ldots,0}_{t-1 \text{ times}},\tau_1,K^{\mathsf{msk}},K^{\mathsf{enc}},\underbrace{\perp,\ldots,\perp}_{t-1 \text{ times}},\perp}$ is defined in Figure 8.
  – If $(m,\mathsf{i}) = (x_i, i)$ and $i > 1$, it samples $\tau_i \leftarrow \{0,1\}^\lambda$ uniformly at random and outputs a pair $(\mathsf{ct}_i, \mathsf{ct}'_i)$ defined as follows:
  $$\mathsf{ct}_i \leftarrow \mathsf{FE}^{\mathsf{sel}}_t.\mathsf{E}(\mathsf{msk}_t, (1, \tau_i), i)$$
  $$\mathsf{ct}'_i \leftarrow \mathsf{FE}_{t-1}.\mathsf{E}(\mathsf{msk}_{t-1}, (x_i, \perp, 1, \tau_i, \underbrace{\perp,\ldots,\perp}_{t-1 \text{ times}}, \perp), i-1).$$
- **The decryption algorithm.** On input a functional key sk_f and t ciphertexts $(\mathsf{ct}_1, \mathsf{sk}_1)$ and $(\mathsf{ct}_2, \mathsf{ct}'_2),\ldots,(\mathsf{ct}_t,\mathsf{ct}'_t)$, the decryption algorithm $\mathsf{FE}_t.\mathsf{D}$ first computes the value $\mathsf{sk}' = \mathsf{FE}_{t-1}.\mathsf{D}(\mathsf{sk}_f, \mathsf{ct}_1,\ldots,\mathsf{ct}_t)$, then it computes the value $\mathsf{ct}' = \mathsf{FE}_1.\mathsf{D}(\mathsf{sk}_1, \mathsf{ct}'_2,\ldots,\mathsf{ct}'_t)$, and finally it outputs $\mathsf{FE}_1.\mathsf{D}(\mathsf{sk}', \mathsf{ct}')$.

The following theorem captures the security of the scheme. This theorem states that under suitable assumptions on the underlying building blocks, the t-input scheme FE_t is fully private (see Definition 2.7).

Theorem A.17. *Let $t > 1$ be any fixed integer. Assuming that (1) FE_1 is fully secure, (2) FE_{t-1} is fully secure, (3) $\mathsf{FE}^{\mathsf{sel}}_t$ is selective-message secure, and (4) PRF is a puncturable pseudorandom function family, then FE_t is fully secure.*

$\mathsf{AGG}_{x_1^0, x_1^1, \mathsf{thr}_2, \ldots, \mathsf{thr}_t, \tau_1, K^{\mathsf{msk}}, K^{\mathsf{enc}}, \tau_{1,2}, \ldots, \tau_{1,t}, u_1}$
$((x_2^0, x_2^1, \mathsf{c}_2, \tau_2, \tau_{2,1}, \tau_{2,3}, \ldots, \tau_{2,t}, u_2), \ldots, (x_t^0, x_t^1, \mathsf{c}_t, \tau_t, \tau_{t,1}, \ldots, \tau_{t,t}, u_t))$ **:**

1. If $\exists i \in [t]$ such that $\forall j \in [t] \setminus \{i\}$ it holds that $\tau_{i,j} = \tau_j$, then output u_i and HALT.
2. Compute $r = \mathsf{PRF.Eval}(K^{\mathsf{msk}}, \tau_2 \ldots, \tau_t)$.
3. Compute $r' = \mathsf{PRF.Eval}(K^{\mathsf{enc}}, \tau_2 \ldots, \tau_t)$.
4. Compute $\mathsf{msk}_{\tau_1, \ldots, \tau_t} = \mathsf{FE}_1.\mathsf{S}(1^\lambda; r)$.
5. For $i = 1, \ldots, t$ do:
   (a) If $\mathsf{c}_i < \mathsf{thr}_i$ then set $x_i = x_i^1$ for all $i \in [t]$ and exit loop.
   (b) If $\mathsf{c}_i > \mathsf{thr}_i$ then set $x_i = x_i^0$ for all $i \in [t]$ and exit loop.
   (c) If $\mathsf{c}_i = \mathsf{thr}_i$ and $i < t$ continue to next iteration (with $i = i + 1$).
   (d) If $\mathsf{c}_i = \mathsf{thr}_i$ and $i = t$ set $x_i = x_i^1$ for all $i \in [t]$.
6. Output $\mathsf{FE}_1.\mathsf{E}(\mathsf{msk}_{\tau_1, \ldots, \tau_t}, (x_1 \ldots, x_t); r')$.

Figure 8: The t-input function $\mathsf{AGG}_{x_1^0, x_1^1, \mathsf{thr}_2, \ldots, \mathsf{thr}_t, \tau_1, K^{\mathsf{msk}}, K^{\mathsf{enc}}, \tau'_{1,2}, \ldots, \tau'_{1,t}, u_1}$.

We note that the proof of Theorem A.17 assumes that t is a fixed constant. The reason for this limitation is that the number of hybrids in the proof of security is $\lambda^{O(t)}$, where λ is the security parameter, which is polynomial for any constant t. If we assume that the underlying building blocks are sub-exponentially secure, then the proof of Theorem A.17 can be used for a super-constant number of inputs.

Proof of Theorem A.17. Let $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ be a valid adversary that issues at most $T_{\mathsf{i}} = T_{\mathsf{i}}(\lambda)$ encryption queries with respect to index $\mathsf{i} \in [t]$ and at most $T_0 = T_0(\lambda)$ key-generation queries (note that $T_0, \ldots, T_t$ may be any polynomials and are not fixed in advance). We assume for simplicity and without loss of generality that $T_0 = \cdots = T_t \stackrel{\mathsf{def}}{=} T$.

We present a sequence of experiments and upper bound $\mathcal{A}$'s advantage in distinguishing each two consecutive experiments. The first experiment is the experiment in which $\mathcal{A}$ gets oracle access to a left-or-right key generation oracle $\mathsf{KG}_b(\mathsf{msk}, \cdot, \cdot)$ and to a left-or-right encryption oracle $\mathsf{Enc}_b(\mathsf{msk}, (\cdot, \cdot), \cdot)$ for $b \leftarrow \{0, 1\}$ chosen uniformly at random (see Definition A.3), and the last experiment is completely independent of the bit b. This enables us to prove that there exists a negligible function $\mathsf{neg}(\cdot)$ such that

$$\mathsf{Adv}^{\mathsf{fullFE_t}}_{\mathsf{FE}_t, \mathcal{F}, \mathcal{A}} \stackrel{\mathsf{def}}{=} \left| \Pr\left[\mathsf{Exp}^{\mathsf{fullFE_t}}_{\mathsf{FE}_t, \mathcal{F}, \mathcal{A}}(\lambda) = 1 \right] - \frac{1}{2} \right| \leq \mathsf{neg}(\lambda),$$

for all sufficiently large $\lambda \in \mathbb{N}$. In what follows we first describe the notation used throughout the proof, and then describe the experiments.

Notation. We denote the i^{th} ciphertext with respect to $\mathsf{i} = 1$ by $(\mathsf{sk}_{1,i}, \mathsf{ct}_{1,i})$ and the i^{th} ciphertext with respect to $\mathsf{i} = \ell$, where $2 \leq \ell \leq t$, by $(\mathsf{ct}_{\ell,i}, \mathsf{ct}'_{\ell,i})$. We denote the i^{th} encryption query corresponding to the index $\mathsf{i} = 1$ by $(x^0_{1,i}, x^1_{1,i})$, the random strings used for generating the resulting $\mathsf{sk}_{1,i}$ by $\tau_{1,i}$, the PRF keys used for generating the resulting $\mathsf{ct}_{1,i}$ and $\mathsf{sk}_{1,i}$ by $K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}$ and K_i^{enc}. We denote the i^{th} encryption query corresponding to the index $\mathsf{i} = \ell \geq 2$ by $(x^0_{\ell,i}, x^1_{\ell,i})$, and the randomness used for generating the resulting $(\mathsf{ct}_{\ell,i}, \mathsf{ct}'_{\ell,i})$ by $\tau_{\ell,i}$. Finally, we denote by $(f_1^0, f_1^1), \ldots, (f_T^0, f_T^1)$ the function pairs with which the adversary queries the key-generation oracle to get $\mathsf{sk}_{f_1}, \ldots, \mathsf{sk}_{f_T}$.

Experiment $\mathcal{H}^{(0)}(\lambda)$. This is the original experiment corresponding to $b \leftarrow \{0,1\}$ chosen uniformly at random. That is, $\mathcal{A}$ gets oracle access to the key-generation oracle $\mathsf{KG}_b(\mathsf{msk},\cdot)$ and oracle access to a left-or-right encryption oracle $\mathsf{Enc}_b(\mathsf{msk},(\cdot,\cdot),\cdot)$ where $b \leftarrow \{0,1\}$ is chosen uniformly at random.

- Ciphertexts ($i = 1,\ldots,T$, $\ell = 2,\ldots,t$):

$$\begin{aligned}
\mathsf{ct}_{1,i} &\leftarrow \mathsf{FE}_t^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_t, (K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}, \tau_{1,i}, \underbrace{0,\ldots,0}_{t-1 \text{ times}}), 1) \\
\mathsf{sk}_{1,i} &\leftarrow \mathsf{FE}_{t-1}.\mathsf{KG}(\mathsf{msk}_{t-1}, \mathsf{AGG}_{x_{1,i}^b,\perp,\underbrace{0,\ldots,0}_{t-1 \text{ times}},\tau_{1,i},K_i^{\mathsf{msk}},K_i^{\mathsf{enc}},\underbrace{\perp,\ldots,\perp}_{t-1 \text{ times}},\perp}) \\
\mathsf{ct}_{\ell,i} &\leftarrow \mathsf{FE}_t^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_t, (1, \tau_{\ell,i}), \ell) \\
\mathsf{ct}'_{\ell,i} &\leftarrow \mathsf{FE}_{t-1}.\mathsf{E}(\mathsf{msk}_{t-1}, (x_{\ell,i}^b, \perp, 1, \tau_{\ell,i}, \underbrace{\perp,\ldots,\perp}_{t-1 \text{ times}}, \perp), \ell-1).
\end{aligned}$$

- Functional keys ($i = 1,\ldots,T$):

$$\mathsf{sk}_{f_i} \leftarrow \mathsf{FE}_t^{\mathsf{sel}}.\mathsf{KG}(\mathsf{msk}_2, D_{f_i^b,\perp,1,\underbrace{\perp,\ldots,\perp}_{t \text{ times}},\perp})$$

Experiment $\mathcal{H}^{(1)}(\lambda)$. This experiment is This experiment is obtained from the experiment $\mathcal{H}^{(0)}(\lambda)$ by modifying the encryptions as follows. Given inputs $(x_{\ell,i}^0, x_{\ell,i}^1)$, instead of setting the field x_1 to be $\perp$ we set it to be $x_{\ell,i}^1$. In addition, in the encryptions $\mathsf{ct}'_{\ell,i}$ corresponding to $\mathsf{i} = \ell \geq 2$ we embed a counter.

- Ciphertexts ($i = 1,\ldots,T$, $\ell = 2,\ldots,t$):

$$\begin{aligned}
\mathsf{ct}_{1,i} &\leftarrow \mathsf{FE}_t^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_t, (K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}, \tau_{1,i}, \underbrace{0,\ldots,0}_{t-1 \text{ times}}), 1) \\
\mathsf{sk}_{1,i} &\leftarrow \mathsf{FE}_{t-1}.\mathsf{KG}(\mathsf{msk}_{t-1}, \mathsf{AGG}_{x_{1,i}^b,\boxed{x_{1,i}^1},\underbrace{0,\ldots,0}_{t-1 \text{ times}},\tau_{1,i},K_i^{\mathsf{msk}},K_i^{\mathsf{enc}},\underbrace{\perp,\ldots,\perp}_{t-1 \text{ times}},\perp}) \\
\mathsf{ct}_{\ell,i} &\leftarrow \mathsf{FE}_t^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_t, (1, \tau_{\ell,i}), \ell) \\
\mathsf{ct}'_{\ell,i} &\leftarrow \mathsf{FE}_{t-1}.\mathsf{E}(\mathsf{msk}_{t-1}, (x_{\ell,i}^b, \boxed{x_{\ell,i}^1}, \boxed{i}, \tau_{\ell,i}, \underbrace{\perp,\ldots,\perp}_{t-1 \text{ times}}, \perp), \ell-1).
\end{aligned}$$

- Functional keys ($i = 1,\ldots,T$):

$$\mathsf{sk}_{f_i} \leftarrow \mathsf{FE}_t^{\mathsf{sel}}.\mathsf{KG}(\mathsf{msk}_2, D_{f_i^b,\perp,1,\underbrace{\perp,\ldots,\perp}_{t \text{ times}},\perp})$$

As in Claim 4.2 we have the following claim:

Claim A.18. *There exists a probabilistic polynomial-time adversary $\mathcal{B}^{(0)\to(1)}$ such that*

$$\left|\Pr\left[\mathcal{H}^{(0)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(1)}(\lambda) = 1\right]\right| \leq \mathsf{Adv}^{\mathsf{fullFE_{t-1}}}_{\mathsf{FE}_{t-1},\mathcal{F}',\mathcal{B}^{(0)\to(1)}}(\lambda).$$

Experiment $\mathcal{H}^{(2)}(\lambda)$. This experiment is obtained from the experiment $\mathcal{H}^{(1)}(\lambda)$ by modifying the functional keys follows. Given inputs (f_i^0, f_i^1), instead of setting the field f_1 to be $\perp$ we set it to be f_i^1. In addition, in the ciphertexts $\mathsf{ct}_{\ell,i}$ corresponding to $\mathsf{i} = \ell \geq 2$ and in the functional keys we embed a counter.

- Ciphertexts ($i = 1, \ldots, T$, $\ell = 2, \ldots, t$):

$$\mathsf{ct}_{1,i} \leftarrow \mathsf{FE}_t^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_t, (K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}, \tau_{1,i}, \underbrace{0, \ldots, 0}_{t-1 \text{ times}}), 1)$$

$$\mathsf{sk}_{1,i} \leftarrow \mathsf{FE}_{t-1}.\mathsf{KG}(\mathsf{msk}_{t-1}, \mathsf{AGG}_{x_{1,i}^b, x_{1,i}^1, \underbrace{0, \ldots, 0}_{t-1 \text{ times}}, \tau_{1,i}, K_i^{\mathsf{msk}}, K_i^{\mathsf{enc}}, \underbrace{\perp, \ldots, \perp}_{t-1 \text{ times}}, \perp})$$

$$\mathsf{ct}_{\ell,i} \leftarrow \mathsf{FE}_t^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_t, (\boxed{i}, \tau_{\ell,i}), \ell)$$

$$\mathsf{ct}'_{\ell,i} \leftarrow \mathsf{FE}_{t-1}.\mathsf{E}(\mathsf{msk}_{t-1}, (x_{\ell,i}^b, x_{\ell,i}^1, i, \tau_{\ell,i}, \underbrace{\perp, \ldots, \perp}_{t-1 \text{ times}}, \perp), \ell - 1).$$

- Functional keys ($i = 1, \ldots, T$):

$$\mathsf{sk}_{f_i} \leftarrow \mathsf{FE}_t^{\mathsf{sel}}.\mathsf{KG}(\mathsf{msk}_t, D_{f_i^b, \boxed{f_i^1}, \boxed{i}, \underbrace{\perp, \ldots, \perp}_{t \text{ times}}, \perp})$$

As in Claim 4.3 we have the following claim:

Claim A.19. *There exists a probabilistic polynomial-time adversary $\mathcal{B}^{(1)\to(2)}$ such that*

$$\left| \Pr\left[\mathcal{H}^{(1)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(2)}(\lambda) = 1\right] \right| \leq \mathsf{Adv}^{\mathsf{selFE_t}}_{\mathsf{FE}_t^{\mathsf{sel}}, \mathcal{F}', \mathcal{B}^{(1)\to(2)}}(\lambda).$$

Experiment $\mathcal{H}^{(3,j,k_2\ldots,k_t)}(\lambda)$. This experiment is obtained from the experiment $\mathcal{H}^{(2)}(\lambda)$ by modifying the encryptions as follows. The first $j-1$ ciphertexts with respect to index $\mathsf{i} = 1$ are generated such that $\mathsf{thr}_2, \ldots, \mathsf{thr}_t = T$ and $w = 1$, the j^{th} ciphertext with respect to index $\mathsf{i} = 1$ is generated such that $\mathsf{thr}_i = k_i$ for $i \in [T]$ and the rest of the ciphertexts are generated as before.

- Ciphertexts ($i = 1, \ldots, j-1$):

$$\mathsf{ct}_{1,i} \leftarrow \mathsf{FE}_t^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_t, (K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}, \tau_{1,i}, \underbrace{\boxed{T, \ldots, T}}_{t-1 \text{ times}}), 1)$$

$$\mathsf{sk}_{1,i} \leftarrow \mathsf{FE}_{t-1}.\mathsf{KG}(\mathsf{msk}_{t-1}, \mathsf{AGG}_{x_{1,i}^b, x_{1,i}^1, \underbrace{\boxed{T, \ldots, T}}_{t-1 \text{ times}}, \tau_{1,i}, K_i^{\mathsf{msk}}, K_i^{\mathsf{enc}}, \underbrace{\perp, \ldots, \perp}_{t-1 \text{ times}}, \perp})$$

- Ciphertexts ($i = j$)

$$\mathsf{ct}_{1,i} \leftarrow \mathsf{FE}_t^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_t, (K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}, \tau_{1,i}, \boxed{k_2, \ldots, k_t}), 1)$$

$$\mathsf{sk}_{1,i} \leftarrow \mathsf{FE}_{t-1}.\mathsf{KG}(\mathsf{msk}_{t-1}, \mathsf{AGG}_{x_{1,i}^b, x_{1,i}^1, \boxed{k_2, \ldots, k_t}, \tau_{1,i}, K_i^{\mathsf{msk}}, K_i^{\mathsf{enc}}, \underbrace{\perp, \ldots, \perp}_{t-1 \text{ times}}, \perp})$$

- Ciphertexts ($i = j+1, \ldots, T$)

$$\mathsf{ct}_{1,i} \leftarrow \mathsf{FE}_t^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_t, (K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}, \tau_{1,i}, \underbrace{0, \ldots, 0}_{t-1 \text{ times}}), 1)$$

$$\mathsf{sk}_{1,i} \leftarrow \mathsf{FE}_{t-1}.\mathsf{KG}(\mathsf{msk}_{t-1}, \mathsf{AGG}_{x_{1,i}^b, x_{1,i}^1, \underbrace{0, \ldots, 0}_{t-1 \text{ times}}, \tau_{1,i}, K_i^{\mathsf{msk}}, K_i^{\mathsf{enc}}, \underbrace{\perp, \ldots, \perp}_{t-1 \text{ times}}, \perp})$$

- Ciphertext ($i = 1, \dots, T$, $\ell = 2, \dots, t$):

$$\mathsf{ct}_{\ell,i} \leftarrow \mathsf{FE}_t^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_t, (i, \tau_{\ell,i}), \ell)$$
$$\mathsf{ct}'_{\ell,i} \leftarrow \mathsf{FE}_{t-1}.\mathsf{E}(\mathsf{msk}_{t-1}, (x^b_{\ell,i}, x^1_{\ell,i}, i, \tau_{\ell,i}, \underbrace{\bot, \dots, \bot}_{t-1 \text{ times}}, \bot), \ell - 1).$$

- Functional keys ($i = 1, \dots, T$):

$$\mathsf{sk}_{f_i} \leftarrow \mathsf{FE}_t^{\mathsf{sel}}.\mathsf{KG}(\mathsf{msk}_t, D_{f_i^b, f_i^1, i, \underbrace{\bot, \dots, \bot}_{t \text{ times}}, \bot})$$

Notice that $\mathcal{H}^{(3,1,0,\dots,0)} = \mathcal{H}^{(2)}$.

Experiment $\mathcal{H}^{(4,j,k_2\dots,k_t)}(\lambda)$. This experiment is obtained from the experiment $\mathcal{H}^{(3,j,k_2\dots,k_t)}(\lambda)$ by modifying the encryptions as follows. First, we sample in advance $\tau_{1,j}$, $\tau_{2,k_2}, \dots, \tau_{t,k_t}$, K_j^{msk}, K_j^{key} and K_j^{enc}, and compute $\mathsf{msk}_{\tau_{1,j},\tau_{2,k_2},\dots,\tau_{t,k_t}} = \mathsf{1FE.S}(1^\lambda; \mathsf{PRF.Eval}(K_j^{\mathsf{msk}}, \tau_{2,k_2} \dots \tau_{t,k_t}))$. Then, assume that the j^{th} encryption comes *after* the $k_i{}^{\text{th}}$ encryption with respect to index $\mathsf{i} = i$ for all $i > 1$. In this case, we embed into $\mathsf{sk}_{1,j}$ the values $(\tau_{2,k_2}, \dots, \tau_{t,k_t}, \gamma)$ where $\gamma = \mathsf{1FE.E}(\mathsf{msk}_{\tau_{1,j},\tau_{2,k_2},\dots,\tau_{t,k_t}}, (x^b_{1,j}, x^b_{2,k_2}, \dots, x^b_{t,k_t}); \mathsf{PRF.Eval}(K_j^{\mathsf{enc}}, \tau_{2,k_2} \dots \tau_{t,k_t}))$. (More generally, we embed into the ciphertext that comes last the corresponding values.) Finally, instead of using K_j^{msk} and K_j^{key} in the j^{th} encryption with respect to msk_1, we use $K_j^{\mathsf{msk}}|_{\{\tau_{2,k_2}\dots\tau_{t,k_t}\}}$ and $K_j^{\mathsf{enc}}|_{\{\tau_{2,k_2}\dots\tau_{t,k_t}\}}$ which are the keys K_j^{msk} and K_j^{enc} punctured at the point $\{\tau_{2,k_2} \dots \tau_{t,k_t}\}$.

For concreteness we assume that the latter is the case, namely, that the j^{th} encryption with respect to index $\mathsf{i} = 1$ came *after* the $k_i{}^{\text{th}}$ encryption with respect to index $\mathsf{i} = i$ for every $i > 1$ (the other cases are handled similarly).

- Ciphertexts ($i = 1, \dots, j - 1$):

$$\mathsf{ct}_{1,i} \leftarrow \mathsf{FE}_t^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_t, (K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}, \tau_{1,i}, \underbrace{T, \dots, T}_{t-1 \text{ times}}), 1)$$
$$\mathsf{sk}_{1,i} \leftarrow \mathsf{FE}_{t-1}.\mathsf{KG}(\mathsf{msk}_{t-1}, \mathsf{AGG}_{x^b_{1,i}, x^1_{1,i}, \underbrace{T, \dots, T}_{t-1 \text{ times}}, \tau_{1,i}, K_i^{\mathsf{msk}}, K_i^{\mathsf{enc}}, \underbrace{\bot, \dots, \bot}_{t-1 \text{ times}}, \bot})$$

- Ciphertexts ($i = j$)

$$\mathsf{ct}_{1,i} \leftarrow \mathsf{FE}_t^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_t, (K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}, \tau_{1,i}, k_2, \dots, k_t), 1)$$
$$\mathsf{sk}_{1,i} \leftarrow \mathsf{FE}_{t-1}.\mathsf{KG}\left(\mathsf{msk}_{t-1}, \mathsf{AGG}_{x^b_{1,i}, x^1_{1,i}, k_2, \dots, k_t, \tau_{1,i}, \boxed{K_i^{\mathsf{msk}}|_{\{\tau_{2,k_2}\dots\tau_{t,k_t}\}}}, \boxed{K_i^{\mathsf{enc}}|_{\{\tau_{2,k_2}\dots\tau_{t,k_t}\}}}, \boxed{\tau_{2,k_2}, \dots, \tau_{t,k_t}, \gamma}}\right)$$
$$\mathsf{msk}_{\tau_{1,j},\tau_{2,k_2}\dots\tau_{t,k_t}} = \mathsf{FE}_1.\mathsf{S}(1^\lambda; \mathsf{PRF.Eval}(K_i^{\mathsf{msk}}, \tau_{k_2} \dots \tau_{k_t}))$$
$$\gamma = \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}_{\tau_{1,j},\tau_{2,k_2}\dots\tau_{t,k_t}}, (x^b_{1,j}, x^b_{2,k_2}, \dots, x^b_{t,k_t}); \mathsf{PRF.Eval}(K_i^{\mathsf{enc}}, \tau_{2,k_2} \dots \tau_{t,k_t}))$$

- Ciphertexts $(i = j+1, \dots, T)$

$$\mathsf{ct}_{1,i} \leftarrow \mathsf{FE}_t^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_t, (K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}, \tau_{1,i}, \underbrace{0, \dots, 0}_{t-1 \text{ times}}), 1)$$

$$\mathsf{sk}_{1,i} \leftarrow \mathsf{FE}_{t-1}.\mathsf{KG}(\mathsf{msk}_{t-1}, \mathsf{AGG}_{x_{1,i}^b, x_{1,i}^1, \underbrace{0, \dots, 0}_{t-1 \text{ times}}, \tau_{1,i}, K_i^{\mathsf{msk}}, K_i^{\mathsf{enc}}, \underbrace{\perp, \dots, \perp}_{t-1 \text{ times}}, \perp})$$

- Ciphertext $(i = 1, \dots, T,\ \ell = 2, \dots, t)$:

$$\mathsf{ct}_{\ell,i} \leftarrow \mathsf{FE}_t^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_t, (i, \tau_{\ell,i}), \ell)$$
$$\mathsf{ct}'_{\ell,i} \leftarrow \mathsf{FE}_{t-1}.\mathsf{E}(\mathsf{msk}_{t-1}, (x_{\ell,i}^b, x_{\ell,i}^1, i, \tau_{\ell,i}, \underbrace{\perp, \dots, \perp}_{t-1 \text{ times}}, \perp), \ell - 1).$$

- Functional keys $(i = 1, \dots, T)$:

$$\mathsf{sk}_{f_i} \leftarrow \mathsf{FE}_t^{\mathsf{sel}}.\mathsf{KG}(\mathsf{msk}_t, D_{f_i^b, f_i^1, i, \underbrace{\perp, \dots, \perp}_{t \text{ times}}, \perp})$$

As in Claim 4.4 we have the following claim:

Claim A.20. *There exists a probabilistic polynomial-time adversary* $\mathcal{B}^{(3,j,k_2\dots,k_t)\to(4,j,k_2\dots,k_t)}$ *such that*

$$\left|\Pr\left[\mathcal{H}^{(3,j,k_2\dots,k_t)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(4,j,k_2\dots,k_t)}(\lambda) = 1\right]\right| \leq \mathsf{Adv}^{\mathsf{fullFE_{t-1}}}_{\mathsf{FE}_{t-1},\mathcal{F}',\mathcal{B}^{(3,j,k_2\dots,k_t)\to(4,j,k_2\dots,k_t)}}(\lambda).$$

Experiment $\mathcal{H}^{(5,j,k_2\dots,k_t)}(\lambda)$. This experiment is obtained from the experiment $\mathcal{H}^{(4,j,k_2\dots,k_t)}(\lambda)$ by modifying the encryptions as follows. First, instead of using K_j^{msk} and K_j^{key} in the j^{th} encryption with respect to msk_t, we use $K_j^{\mathsf{msk}}|_{\{\tau_{2,k_2}\dots\tau_{t,k_t}\}}$ and $K_j^{\mathsf{key}}|_{\{\tau_{2,k_2}\dots\tau_{t,k_t}\}}$ which are the keys K_j^{msk} and K_j^{key} punctured at the point $\{\tau_{2,k_2}\dots\tau_{t,k_t}\}$. Second, we hardwire into every functional key for a pair $(f_i^0.f_i^1)$ the list $(\tau_{1,j}, \tau_{2,k_2}, \dots, \tau_{t,k_t}, \delta)$, where $\delta = \mathsf{1FE.KG}(\mathsf{msk}_{\tau_{1,j},\tau_{2,k_2},\dots,\tau_{t,k_t}}, C_{f_i^b}; \mathsf{PRF.Eval}(K_j^{\mathsf{key}}, \tau_{2,k_2}\dots\tau_{t,k_t}))$.

- Ciphertexts $(i = 1, \dots, j-1)$:

$$\mathsf{ct}_{1,i} \leftarrow \mathsf{FE}_t^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_t, (K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}, \tau_{1,i}, \underbrace{T, \dots, T}_{t-1 \text{ times}}), 1)$$

$$\mathsf{sk}_{1,i} \leftarrow \mathsf{FE}_{t-1}.\mathsf{KG}(\mathsf{msk}_{t-1}, \mathsf{AGG}_{x_{1,i}^b, x_{1,i}^1, \underbrace{T, \dots, T}_{t-1 \text{ times}}, \tau_{1,i}, K_i^{\mathsf{msk}}, K_i^{\mathsf{enc}}, \underbrace{\perp, \dots, \perp}_{t-1 \text{ times}}, \perp})$$

- Ciphertexts $(i = j)$

$$\mathsf{ct}_{1,i} \leftarrow \mathsf{FE}_t^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_t, (\boxed{K_i^{\mathsf{msk}}|_{\{\tau_{2,k_2}\dots\tau_{t,k_t}\}}}, \boxed{K_i^{\mathsf{key}}|_{\{\tau_{2,k_2}\dots\tau_{t,k_t}\}}}, \tau_{1,i}, k_2, \dots, k_t), 1)$$

$$\mathsf{sk}_{1,i} \leftarrow \mathsf{FE}_{t-1}.\mathsf{KG}(\mathsf{msk}_{t-1}, \mathsf{AGG}_{x_{1,i}^b, x_{1,i}^1, k_2, \dots, k_t, \tau_{1,i}, K_i^{\mathsf{msk}}|_{\{\tau_{2,k_2}\dots\tau_{t,k_t}\}}, K_i^{\mathsf{enc}}|_{\{\tau_{2,k_2}\dots\tau_{t,k_t}\}}, \tau_{2,k_2},\dots,\tau_{t,k_t}, \gamma})$$

$$\mathsf{msk}_{\tau_{1,j},\tau_{2,k_2}\dots\tau_{t,k_t}} = \mathsf{FE}_1.\mathsf{S}(1^\lambda; \mathsf{PRF.Eval}(K_i^{\mathsf{msk}}, \tau_{k_2}\dots\tau_{k_t}))$$
$$\gamma = \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}_{\tau_{1,j},\tau_{2,k_2}\dots\tau_{t,k_t}}, (x_{1,j}^b, x_{2,k_2}^b, \dots, x_{t,k_t}^b); \mathsf{PRF.Eval}(K_i^{\mathsf{enc}}, \tau_{2,k_2}\dots\tau_{t,k_t}))$$

- Ciphertexts $(i = j+1, \dots, T)$

$$\mathsf{ct}_{1,i} \leftarrow \mathsf{FE}_t^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_t, (K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}, \tau_{1,i}, \underbrace{0, \dots, 0}_{t-1 \text{ times}}), 1)$$

$$\mathsf{sk}_{1,i} \leftarrow \mathsf{FE}_{t-1}.\mathsf{KG}(\mathsf{msk}_{t-1}, \mathsf{AGG}_{x_{1,i}^b, x_{1,i}^1, \underbrace{0,\dots,0}_{t-1 \text{ times}}, \tau_{1,i}, K_i^{\mathsf{msk}}, K_i^{\mathsf{enc}}, \underbrace{\perp,\dots,\perp}_{t-1 \text{ times}}, \perp})$$

- Ciphertext $(i = 1, \dots, T,\ \ell = 2, \dots, t)$:

$$\mathsf{ct}_{\ell,i} \leftarrow \mathsf{FE}_t^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_t, (i, \tau_{\ell,i}), \ell)$$
$$\mathsf{ct}'_{\ell,i} \leftarrow \mathsf{FE}_{t-1}.\mathsf{E}(\mathsf{msk}_{t-1}, (x_{\ell,i}^b, x_{\ell,i}^1, i, \tau_{\ell,i}, \underbrace{\perp, \dots, \perp}_{t-1 \text{ times}}, \perp), \ell - 1).$$

- Functional keys $(i = 1, \dots, T)$:

$$\mathsf{sk}_{f_i} \leftarrow \mathsf{FE}_t^{\mathsf{sel}}.\mathsf{KG}(\mathsf{msk}_t, D_{f_i^b, f_i^1, i, \boxed{\tau_{1,j}, \tau_{2,k_2} \dots, \tau_{t,k_t}, \delta}})$$
$$\mathsf{msk}_{\tau_{1,j}, \tau_{2,k_2} \dots \tau_{t,k_t}} = \mathsf{FE}_1.\mathsf{S}(1^\lambda; \mathsf{PRF.Eval}(K_i^{\mathsf{msk}}, \tau_{k_2} \dots \tau_{k_t}))$$
$$\delta = \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk}_{\tau_{1,j}, \tau_{2,k_2} \dots \tau_{t,k_t}}, C_{f_i^b}; \mathsf{PRF.Eval}(K_j^{\mathsf{key}}, \tau_{k_2} \dots \tau_{k_t}))$$

As in Claim 4.5 we have the following claim:

Claim A.21. *There exists a probabilistic polynomial-time adversary $\mathcal{B}^{(4,j,k_2 \dots, k_t) \to (5,j,k_2 \dots, k_t)}$ such that*

$$\left| \Pr\left[\mathcal{H}^{(4,j,k_2 \dots, k_t)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(5,j,k_2 \dots, k_t)}(\lambda) = 1\right] \right| \leq \mathsf{Adv}^{\mathsf{selFE_t}}_{\mathsf{FE}_t^{\mathsf{sel}}, \mathcal{F}', \mathcal{B}^{(4,j,k_2 \dots, k_t) \to (5,j,k_2 \dots, k_t)}}(\lambda).$$

Experiment $\mathcal{H}^{(6,j,k_2 \dots, k_t)}(\lambda)$. This experiment is obtained from the experiment $\mathcal{H}^{(5,j,k_2 \dots, k_t)}(\lambda)$ by modifying the encryptions as follows. Instead of using randomness generated using a PRF we use randomness sampled uniformly at random. That is, $\mathsf{msk}_{\tau_{1,j}, \tau_{2,k_2}, \dots, \tau_{t,k_t}}$, γ and δ are generated using randomness that is sampled uniformly at random rather than generated using a PRF. We emphasize that $\mathsf{msk}_{\tau_{1,j}, \tau_{2,k_2}, \dots, \tau_{t,k_t}}$ is computed in advance once as $\mathsf{msk}_{\tau_{1,j}, \tau_{2,k_2}, \dots, \tau_{t,k_t}} \leftarrow \mathsf{1FE.S}(1^\lambda)$.

- Ciphertexts $(i = 1, \dots, j-1)$:

$$\mathsf{ct}_{1,i} \leftarrow \mathsf{FE}_t^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_t, (K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}, \tau_{1,i}, \underbrace{T, \dots, T}_{t-1 \text{ times}}), 1)$$

$$\mathsf{sk}_{1,i} \leftarrow \mathsf{FE}_{t-1}.\mathsf{KG}(\mathsf{msk}_{t-1}, \mathsf{AGG}_{x_{1,i}^b, x_{1,i}^1, \underbrace{T,\dots,T}_{t-1 \text{ times}}, \tau_{1,i}, K_i^{\mathsf{msk}}, K_i^{\mathsf{enc}}, \underbrace{\perp,\dots,\perp}_{t-1 \text{ times}}, \perp})$$

- Ciphertexts $(i = j)$

$$\mathsf{ct}_{1,i} \leftarrow \mathsf{FE}_t^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_t, (K_i^{\mathsf{msk}}|_{\{\tau_{2,k_2} \dots \tau_{t,k_t}\}}, K_i^{\mathsf{key}}|_{\{\tau_{2,k_2} \dots \tau_{t,k_t}\}}, \tau_{1,i}, k_2, \dots, k_t), 1)$$
$$\mathsf{sk}_{1,i} \leftarrow \mathsf{FE}_{t-1}.\mathsf{KG}(\mathsf{msk}_{t-1}, \mathsf{AGG}_{x_{1,i}^b, x_{1,i}^1, k_2, \dots, k_t, \tau_{1,i}, K_i^{\mathsf{msk}}|_{\{\tau_{2,k_2} \dots \tau_{t,k_t}\}}, K_i^{\mathsf{enc}}|_{\{\tau_{2,k_2} \dots \tau_{t,k_t}\}}, \tau_{2,k_2}, \dots, \tau_{t,k_t}, \gamma})$$
$$\boxed{\mathsf{msk}_{\tau_{1,j}, \tau_{2,k_2} \dots \tau_{t,k_t}}} = \mathsf{FE}_1.\mathsf{S}(1^\lambda)$$
$$\boxed{\gamma} = \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}_{\tau_{1,j}, \tau_{2,k_2} \dots \tau_{t,k_t}}, (x_{1,j}^b, x_{2,k_2}^b, \dots, x_{t,k_t}^b))$$

- Ciphertexts $(i = j+1, \ldots, T)$

$$\mathsf{ct}_{1,i} \leftarrow \mathsf{FE}_t^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_t, (K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}, \tau_{1,i}, \underbrace{0, \ldots, 0}_{t-1 \text{ times}}), 1)$$

$$\mathsf{sk}_{1,i} \leftarrow \mathsf{FE}_{t-1}.\mathsf{KG}(\mathsf{msk}_{t-1}, \mathsf{AGG}_{x_{1,i}^b, x_{1,i}^1, \underbrace{0, \ldots, 0}_{t-1 \text{ times}}, \tau_{1,i}, K_i^{\mathsf{msk}}, K_i^{\mathsf{enc}}, \underbrace{\perp, \ldots, \perp}_{t-1 \text{ times}}, \perp})$$

- Ciphertext $(i = 1, \ldots, T,\ \ell = 2, \ldots, t)$:

$$\mathsf{ct}_{\ell,i} \leftarrow \mathsf{FE}_t^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_t, (i, \tau_{\ell,i}), \ell)$$
$$\mathsf{ct}'_{\ell,i} \leftarrow \mathsf{FE}_{t-1}.\mathsf{E}(\mathsf{msk}_{t-1}, (x_{\ell,i}^b, x_{\ell,i}^1, i, \tau_{\ell,i}, \underbrace{\perp, \ldots, \perp}_{t-1 \text{ times}}, \perp), \ell - 1).$$

- Functional keys $(i = 1, \ldots, T)$:

$$\mathsf{sk}_{f_i} \leftarrow \mathsf{FE}_t^{\mathsf{sel}}.\mathsf{KG}(\mathsf{msk}_t, D_{f_i^b, f_i^1, i, \tau_{1,j}, \tau_{2,k_2} \ldots, \tau_{t,k_t}, \delta})$$
$$\boxed{\delta} = \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk}_{\tau_{1,j}, \tau_{2,k_2} \ldots \tau_{t,k_t}}, C_{f_i^b})$$

As in Claim 4.6 we have the following claim:

Claim A.22. *There exists a probabilistic polynomial-time adversary $\mathcal{B}^{(5,j,k_2 \ldots,k_t) \to (6,j,k_2 \ldots,k_t)}$ such that*

$$\left| \Pr\left[\mathcal{H}^{(5,j,k_2 \ldots,k_t)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(6,j,k_2 \ldots,k_t)}(\lambda) = 1\right] \right| \leq 3 \cdot \mathsf{Adv}_{\mathsf{PRF}, \mathcal{B}^{(5,j,k_2 \ldots,k_t) \to (6,j,k_2 \ldots,k_t)}}(\lambda).$$

Experiment $\mathcal{H}^{(7,j,k_2 \ldots,k_t)}(\lambda)$. This experiment is obtained from the experiment $\mathcal{H}^{(6,j,k_2 \ldots,k_t)}(\lambda)$ by modifying the encryptions as follows. Instead of having $(x_{1,j}^b, x_{2,k_2}^b, \ldots, x_{t,k_t}^b)$ hardwired in γ and $D_{f_i^b}$ in δ, we hardwire the values $(x_{1,j}^1, x_{2,k_2}^1, \ldots, x_{t,k_t}^1)$ and $D_{f_i^1}$, respectively.

- Ciphertexts $(i = 1, \ldots, j-1)$:

$$\mathsf{ct}_{1,i} \leftarrow \mathsf{FE}_t^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_t, (K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}, \tau_{1,i}, \underbrace{T, \ldots, T}_{t-1 \text{ times}}), 1)$$

$$\mathsf{sk}_{1,i} \leftarrow \mathsf{FE}_{t-1}.\mathsf{KG}(\mathsf{msk}_{t-1}, \mathsf{AGG}_{x_{1,i}^b, x_{1,i}^1, \underbrace{T, \ldots, T}_{t-1 \text{ times}}, \tau_{1,i}, K_i^{\mathsf{msk}}, K_i^{\mathsf{enc}}, \underbrace{\perp, \ldots, \perp}_{t-1 \text{ times}}, \perp})$$

- Ciphertexts $(i = j)$

$$\mathsf{ct}_{1,i} \leftarrow \mathsf{FE}_t^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_t, (K_i^{\mathsf{msk}}|_{\{\tau_{2,k_2} \ldots \tau_{t,k_t}\}}, K_i^{\mathsf{key}}|_{\{\tau_{2,k_2} \ldots \tau_{t,k_t}\}}, \tau_{1,i}, k_2, \ldots, k_t), 1)$$
$$\mathsf{sk}_{1,i} \leftarrow \mathsf{FE}_{t-1}.\mathsf{KG}(\mathsf{msk}_{t-1}, \mathsf{AGG}_{x_{1,i}^b, x_{1,i}^1, k_2, \ldots, k_t, \tau_{1,i}, K_i^{\mathsf{msk}}|_{\{\tau_{2,k_2} \ldots \tau_{t,k_t}\}}, K_i^{\mathsf{enc}}|_{\{\tau_{2,k_2} \ldots \tau_{t,k_t}\}}, \tau_{2,k_2}, \ldots, \tau_{t,k_t}, \gamma})$$
$$\mathsf{msk}_{\tau_{1,j}, \tau_{2,k_2} \ldots \tau_{t,k_t}} = \mathsf{FE}_1.\mathsf{S}(1^\lambda)$$
$$\gamma = \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}_{\tau_{1,j}, \tau_{2,k_2} \ldots \tau_{t,k_t}}, (\boxed{x_{1,j}^1, x_{2,k_2}^1, \ldots, x_{t,k_t}^1}))$$

- Ciphertexts $(i = j+1, \ldots, T)$

$$\mathsf{ct}_{1,i} \leftarrow \mathsf{FE}_t^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_t, (K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}, \tau_{1,i}, \underbrace{0, \ldots, 0}_{t-1 \text{ times}}), 1)$$

$$\mathsf{sk}_{1,i} \leftarrow \mathsf{FE}_{t-1}.\mathsf{KG}(\mathsf{msk}_{t-1}, \mathsf{AGG}_{x_{1,i}^b, x_{1,i}^1, \underbrace{0, \ldots, 0}_{t-1 \text{ times}}, \tau_{1,i}, K_i^{\mathsf{msk}}, K_i^{\mathsf{enc}}, \underbrace{\perp, \ldots, \perp}_{t-1 \text{ times}}, \perp})$$

- Ciphertext ($i = 1, \dots, T$, $\ell = 2, \dots, t$):

$$\mathsf{ct}_{\ell,i} \leftarrow \mathsf{FE}_t^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_t, (i, \tau_{\ell,i}), \ell)$$
$$\mathsf{ct}'_{\ell,i} \leftarrow \mathsf{FE}_{t-1}.\mathsf{E}(\mathsf{msk}_{t-1}, (x^b_{\ell,i}, x^1_{\ell,i}, i, \tau_{\ell,i}, \underbrace{\bot, \dots, \bot}_{t-1 \text{ times}}, \bot), \ell - 1).$$

- Functional keys ($i = 1, \dots, T$):

$$\mathsf{sk}_{f_i} \leftarrow \mathsf{FE}_t^{\mathsf{sel}}.\mathsf{KG}(\mathsf{msk}_t, D_{f_i^b, f_i^1, i, \tau_{1,j}, \tau_{2,k_2} \dots, \tau_{t,k_t}, \delta})$$
$$\delta = \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk}_{\tau_{1,j}, \tau_{2,k_2} \dots \tau_{t,k_t}}, \boxed{C_{f_i^1}})$$

As in Claim 4.7 we have the following claim:

Claim A.23. *There exists a probabilistic polynomial-time adversary $\mathcal{B}^{(6,j,k_2\dots,k_t)\to(7,j,k_2\dots,k_t)}$ such that*

$$\left|\Pr\left[\mathcal{H}^{(6,j,k_2\dots,k_t)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(7,j,k_2\dots,k_t)}(\lambda) = 1\right]\right| \leq \mathsf{Adv}^{\mathsf{full1FE}}_{\mathsf{FE}_1, \mathcal{F}', \mathcal{B}^{(6,j,k_2\dots,k_t)\to(7,j,k_2\dots,k_t)}}(\lambda).$$

Experiment $\mathcal{H}^{(8,j,k_2\dots,k_t)}(\lambda)$. This experiment is obtained from the experiment $\mathcal{H}^{(7,j,k_2\dots,k_t)}(\lambda)$ by modifying the encryptions as follows. Instead of using randomness sampled uniformly at random we use randomness generated using a PRF. That is, $\mathsf{msk}_{\tau_{1,j}, \tau_{2,k_2}, \dots, \tau_{t,k_t}}$, γ and δ are generated using a PRF.

- Ciphertexts ($i = 1, \dots, j - 1$):

$$\mathsf{ct}_{1,i} \leftarrow \mathsf{FE}_t^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_t, (K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}, \tau_{1,i}, \underbrace{T, \dots, T}_{t-1 \text{ times}}), 1)$$
$$\mathsf{sk}_{1,i} \leftarrow \mathsf{FE}_{t-1}.\mathsf{KG}(\mathsf{msk}_{t-1}, \mathsf{AGG}_{x^b_{1,i}, x^1_{1,i}, \underbrace{T, \dots, T}_{t-1 \text{ times}}, \tau_{1,i}, K_i^{\mathsf{msk}}, K_i^{\mathsf{enc}}, \underbrace{\bot, \dots, \bot}_{t-1 \text{ times}}, \bot})$$

- Ciphertexts ($i = j$)

$$\mathsf{ct}_{1,i} \leftarrow \mathsf{FE}_t^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_t, (K_i^{\mathsf{msk}}|_{\{\tau_{2,k_2} \dots \tau_{t,k_t}\}}, K_i^{\mathsf{key}}|_{\{\tau_{2,k_2} \dots \tau_{t,k_t}\}}, \tau_{1,i}, k_2, \dots, k_t), 1)$$
$$\mathsf{sk}_{1,i} \leftarrow \mathsf{FE}_{t-1}.\mathsf{KG}(\mathsf{msk}_{t-1}, \mathsf{AGG}_{x^b_{1,i}, x^1_{1,i}, k_2, \dots, k_t, \tau_{1,i}, K_i^{\mathsf{msk}}|_{\{\tau_{2,k_2} \dots \tau_{t,k_t}\}}, K_i^{\mathsf{enc}}|_{\{\tau_{2,k_2} \dots \tau_{t,k_t}\}}, \tau_{2,k_2}, \dots, \tau_{t,k_t}, \gamma})$$
$$\boxed{\mathsf{msk}_{\tau_{1,j}, \tau_{2,k_2} \dots \tau_{t,k_t}}} = \mathsf{FE}_1.\mathsf{S}(1^\lambda; \mathsf{PRF.Eval}(K_i^{\mathsf{msk}}, \tau_{k_2} \dots \tau_{k_t}))$$
$$\boxed{\gamma} = \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}_{\tau_{1,j}, \tau_{2,k_2} \dots \tau_{t,k_t}}, (x^1_{1,j}, x^1_{2,k_2}, \dots, x^1_{t,k_t}); \mathsf{PRF.Eval}(K_i^{\mathsf{enc}}, \tau_{k_2} \dots \tau_{k_t}))$$

- Ciphertexts ($i = j + 1, \dots, T$)

$$\mathsf{ct}_{1,i} \leftarrow \mathsf{FE}_t^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_t, (K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}, \tau_{1,i}, \underbrace{0, \dots, 0}_{t-1 \text{ times}}), 1)$$
$$\mathsf{sk}_{1,i} \leftarrow \mathsf{FE}_{t-1}.\mathsf{KG}(\mathsf{msk}_{t-1}, \mathsf{AGG}_{x^b_{1,i}, x^1_{1,i}, \underbrace{0, \dots, 0}_{t-1 \text{ times}}, \tau_{1,i}, K_i^{\mathsf{msk}}, K_i^{\mathsf{enc}}, \underbrace{\bot, \dots, \bot}_{t-1 \text{ times}}, \bot})$$

- Ciphertext ($i = 1, \dots, T$, $\ell = 2, \dots, t$):

$$\mathsf{ct}_{\ell,i} \leftarrow \mathsf{FE}_t^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_t, (i, \tau_{\ell,i}), \ell)$$
$$\mathsf{ct}'_{\ell,i} \leftarrow \mathsf{FE}_{t-1}.\mathsf{E}(\mathsf{msk}_{t-1}, (x^b_{\ell,i}, x^1_{\ell,i}, i, \tau_{\ell,i}, \underbrace{\bot, \dots, \bot}_{t-1 \text{ times}}, \bot), \ell - 1).$$

- Functional keys ($i = 1, \ldots, T$):

$$\mathsf{sk}_{f_i} \leftarrow \mathsf{FE}_t^{\mathsf{sel}}.\mathsf{KG}(\mathsf{msk}_t, D_{f_i^b, f_i^1, i, \tau_{1,j}, \tau_{2,k_2} \ldots, \tau_{t,k_t}, \delta})$$
$$\boxed{\mathsf{msk}_{\tau_{1,j}, \tau_{2,k_2} \ldots \tau_{t,k_t}}} = \mathsf{FE}_1.\mathsf{S}(1^\lambda; \mathsf{PRF.Eval}(K_j^{\mathsf{msk}}, \tau_{k_2} \ldots \tau_{k_t}))$$
$$\boxed{\delta} = \mathsf{FE}_1.\mathsf{KG}(\mathsf{msk}_{\tau_{1,j}, \tau_{2,k_2} \ldots \tau_{t,k_t}}, C_{f_i^1}; \mathsf{PRF.Eval}(K_j^{\mathsf{key}}, \tau_{k_2} \ldots \tau_{k_t}))$$

As in Claim 4.8 we have the following claim:

Claim A.24. *There exists a probabilistic polynomial-time adversary $\mathcal{B}^{(7,j,k_2 \ldots, k_t) \to (8,j,k_2 \ldots, k_t)}$ such that*

$$\left| \Pr\left[\mathcal{H}^{(7,j,k_2 \ldots, k_t)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(8,j,k_2 \ldots, k_t)}(\lambda) = 1\right] \right| \leq 3 \cdot \mathsf{Adv}_{\mathsf{PRF}, \mathcal{B}^{(7,j,k_2 \ldots, k_t) \to (8,j,k_2 \ldots, k_t)}}(\lambda).$$

Experiment $\mathcal{H}^{(9,j,k)}(\lambda)$. This experiment is obtained from the experiment $\mathcal{H}^{(8,j,k_2 \ldots, k_t)}(\lambda)$ by modifying the ciphertexts as follows. First, instead of using a punctured keys $K_j^{\mathsf{msk}}|_{\{\tau_{2,k_2}, \ldots, \tau_{t,k_t}\}}$ and $K_j^{\mathsf{key}}|_{\{\tau_{2,k_2}, \ldots, \tau_{t,k_t}\}}$ in the j^{th} encryption with respect to msk_2, we use the original keys K_j^{msk} and K_j^{key}. Second, we set the threshold thr in $\mathsf{ct}_{1,j}$ to $k+1$. Lastly, we hardwire into every functional key for a pair $(f_i^0 . f_i^1)$ the sequence $(\perp, \ldots, \perp, \perp)$ instead of $(\tau_{1,j}, \tau_{2,k_2} \ldots, \tau_{t,k_t}, \delta)$.

- Ciphertexts ($i = 1, \ldots, j-1$):

$$\mathsf{ct}_{1,i} \leftarrow \mathsf{FE}_t^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_t, (K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}, \tau_{1,i}, \underbrace{T, \ldots, T}_{t-1 \text{ times}}), 1)$$
$$\mathsf{sk}_{1,i} \leftarrow \mathsf{FE}_{t-1}.\mathsf{KG}(\mathsf{msk}_{t-1}, \mathsf{AGG}_{x_{1,i}^b, x_{1,i}^1, \underbrace{T, \ldots, T}_{t-1 \text{ times}}, \tau_{1,i}, K_i^{\mathsf{msk}}, K_i^{\mathsf{enc}}, \underbrace{\perp, \ldots, \perp}_{t-1 \text{ times}}, \perp})$$

- Ciphertexts ($i = j$)

$$\mathsf{ct}_{1,i} \leftarrow \mathsf{FE}_t^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_t, (\boxed{K_i^{\mathsf{msk}}}, \boxed{K_i^{\mathsf{key}}}, \tau_{1,i}, k_2, \ldots, k_{t-1}, \boxed{k_t + 1}), 1)$$
$$\mathsf{sk}_{1,i} \leftarrow \mathsf{FE}_{t-1}.\mathsf{KG}(\mathsf{msk}_{t-1}, \mathsf{AGG}_{x_{1,i}^b, x_{1,i}^1, k_2, \ldots, k_t, \tau_{1,i}, K_i^{\mathsf{msk}}|_{\{\tau_{2,k_2} \ldots \tau_{t,k_t}\}}, K_i^{\mathsf{enc}}|_{\{\tau_{2,k_2} \ldots \tau_{t,k_t}\}}, \tau_{2,k_2}, \ldots, \tau_{t,k_t}, \gamma})$$
$$\mathsf{msk}_{\tau_{1,j}, \tau_{2,k_2} \ldots \tau_{t,k_t}} = \mathsf{FE}_1.\mathsf{S}(1^\lambda; \mathsf{PRF.Eval}(K_i^{\mathsf{msk}}, \tau_{k_2} \ldots \tau_{k_t}))$$
$$\gamma = \mathsf{FE}_1.\mathsf{E}(\mathsf{msk}_{\tau_{1,j}, \tau_{2,k_2} \ldots \tau_{t,k_t}}, (x_{1,j}^1, x_{2,k_2}^1, \ldots, x_{t,k_t}^1); \mathsf{PRF.Eval}(K_i^{\mathsf{enc}}, \tau_{k_2} \ldots \tau_{k_t}))$$

- Ciphertexts ($i = j+1, \ldots, T$)

$$\mathsf{ct}_{1,i} \leftarrow \mathsf{FE}_t^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_t, (K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}, \tau_{1,i}, \underbrace{0, \ldots, 0}_{t-1 \text{ times}}), 1)$$
$$\mathsf{sk}_{1,i} \leftarrow \mathsf{FE}_{t-1}.\mathsf{KG}(\mathsf{msk}_{t-1}, \mathsf{AGG}_{x_{1,i}^b, x_{1,i}^1, \underbrace{0, \ldots, 0}_{t-1 \text{ times}}, \tau_{1,i}, K_i^{\mathsf{msk}}, K_i^{\mathsf{enc}}, \underbrace{\perp, \ldots, \perp}_{t-1 \text{ times}}, \perp})$$

- Ciphertext ($i = 1, \ldots, T$, $\ell = 2, \ldots, t$):

$$\mathsf{ct}_{\ell,i} \leftarrow \mathsf{FE}_t^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_t, (i, \tau_{\ell,i}), \ell)$$
$$\mathsf{ct}'_{\ell,i} \leftarrow \mathsf{FE}_{t-1}.\mathsf{E}(\mathsf{msk}_{t-1}, (x_{\ell,i}^b, x_{\ell,i}^1, i, \tau_{\ell,i}, \underbrace{\perp, \ldots, \perp}_{t-1 \text{ times}}, \perp), \ell - 1).$$

- Functional keys ($i = 1, \ldots, T$):

$$\mathsf{sk}_{f_i} \leftarrow \mathsf{FE}_t^{\mathsf{sel}}.\mathsf{KG}(\mathsf{msk}_t, D_{f_i^b, f_i^1, i, \underbrace{\boxed{\bot, \ldots, \bot}}_{t \text{ times}}, \boxed{\bot}})$$

As in Claim 4.9 we have the following claim:

Claim A.25. *There exists a probabilistic polynomial-time adversary $\mathcal{B}^{(8,j,k_2\ldots,k_t)\to(9,j,k_2\ldots,k_t)}$ such that*

$$\left|\Pr\left[\mathcal{H}^{(8,j,k_2\ldots,k_t)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(9,j,k_2\ldots,k_t)}(\lambda) = 1\right]\right| \leq \mathsf{Adv}^{\mathsf{selFE_t}}_{\mathsf{FE}_t^{\mathsf{sel}}, \mathcal{F}', \mathcal{B}^{(8,j,k_2\ldots,k_t)\to(9,j,k_2\ldots,k_t)}}(\lambda).$$

Next, as in Claim 4.10, we observe that $\mathcal{H}^{(9,j,k_2\ldots,k_t)}(\lambda)$ and $\mathcal{H}^{(3,j,k_2\ldots,k_{t-1},k_t+1)}(\lambda)$ are indistinguishable. Moreover, we notice that $\mathcal{H}^{(3,j,k_2\ldots,T)}(\lambda) = \mathcal{H}^{(3,j,k_2\ldots,k_{t-1}+1,0)}(\lambda)$ and more generally $\mathcal{H}^{(3,j,k_2\ldots,k_i,T,0,\ldots,0)}(\lambda) = \mathcal{H}^{(3,j,k_2\ldots,k_i+1,0,\ldots,0)}(\lambda)$.

Claim A.26. *There exists a probabilistic polynomial-time adversary $\mathcal{B}^{(9,j,k_2\ldots,k_t)\to(3,j,k_2\ldots,k_{t-1},k_t+1)}$ such that*

$$\left|\Pr\left[\mathcal{H}^{(9,j,k_2\ldots,k_t)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(3,j,k_2\ldots,k_{t-1},k_t+1))}(\lambda) = 1\right]\right|$$
$$\leq \mathsf{Adv}^{\mathsf{fullFE_{t-1}}}_{\mathsf{FE}_{t-1}, \mathcal{F}', \mathcal{B}^{(9,j,k_2\ldots,k_t)\to(3,j,k_2\ldots,k_{t-1},k_t+1))}}(\lambda).$$

Experiment $\mathcal{H}^{(10)}(\lambda)$. This experiment is obtained from the experiment $\mathcal{H}^{(3,T+1,0,\ldots,0)}(\lambda)$ by modifying the ciphertexts *not* to include f_i^b at all.

- Ciphertexts ($i = 1, \ldots, T$):

$$\mathsf{ct}_{1,i} \leftarrow \mathsf{FE}_t^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_t, (K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}, \tau_{1,i}, \underbrace{T, \ldots, T}_{t-1 \text{ times}}), 1)$$
$$\mathsf{sk}_{1,i} \leftarrow \mathsf{FE}_{t-1}.\mathsf{KG}(\mathsf{msk}_{t-1}, \mathsf{AGG}_{x_{1,i}^b, x_{1,i}^1, \underbrace{T, \ldots, T}_{t-1 \text{ times}}, \tau_{1,i}, K_i^{\mathsf{msk}}, K_i^{\mathsf{enc}}, \underbrace{\bot, \ldots, \bot}_{t-1 \text{ times}}, \bot})$$

- Ciphertext ($i = 1, \ldots, T$, $\ell = 2, \ldots, t$):

$$\mathsf{ct}_{\ell,i} \leftarrow \mathsf{FE}_t^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_t, (i, \tau_{\ell,i}), \ell)$$
$$\mathsf{ct}'_{\ell,i} \leftarrow \mathsf{FE}_{t-1}.\mathsf{E}(\mathsf{msk}_{t-1}, (x_{\ell,i}^b, x_{\ell,i}^1, i, \tau_{\ell,i}, \underbrace{\bot, \ldots, \bot}_{t-1 \text{ times}}, \bot), \ell - 1).$$

- Functional keys ($i = 1, \ldots, T$):

$$\mathsf{sk}_{f_i} \leftarrow \mathsf{FE}_t^{\mathsf{sel}}.\mathsf{KG}(\mathsf{msk}_t, D_{\boxed{\bot}, f_i^1, i, \underbrace{\bot, \ldots, \bot}_{t \text{ times}}, \bot})$$

As in Claim 4.11 we have the following claim:

Claim A.27. *There exists a probabilistic polynomial-time adversary $\mathcal{B}^{(3,T+1,0,\ldots,0)\to(10)}$ such that*

$$\left|\Pr\left[\mathcal{H}^{(3,T+1,0,\ldots,0)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(10)}(\lambda) = 1\right]\right| \leq \mathsf{Adv}^{\mathsf{selFE_t}}_{\mathsf{FE}_t^{\mathsf{sel}}, \mathcal{F}', \mathcal{B}^{(3,T+1,0,\ldots,0)\to(10)}}(\lambda).$$

Experiment $\mathcal{H}^{(11)}(\lambda)$. This experiment is obtained from the experiment $\mathcal{H}^{(10)}(\lambda)$ by modifying the ciphertexts *not* to include $x^b_{\mathsf{i},i}$ at all for $\mathsf{i} \in [t]$ and $i \in [T]$ Notice that this experiment is completely independent of the bit b, and therefore $\Pr[\mathcal{H}^{(11)}(\lambda) = 1] = 1/2$.

- Ciphertexts ($i = 1, \ldots, T$):

$$\mathsf{ct}_{1,i} \leftarrow \mathsf{FE}^{\mathsf{sel}}_t.\mathsf{E}(\mathsf{msk}_t, (K^{\mathsf{msk}}_i, K^{\mathsf{key}}_i, \tau_{1,i}, \underbrace{T, \ldots, T}_{t-1 \text{ times}}), 1)$$

$$\mathsf{sk}_{1,i} \leftarrow \mathsf{FE}_{t-1}.\mathsf{KG}(\mathsf{msk}_{t-1}, \mathsf{AGG}_{\boxed{\bot}, x^1_{1,i}, \underbrace{T, \ldots, T}_{t-1 \text{ times}}, \tau_{1,i}, K^{\mathsf{msk}}_i, K^{\mathsf{enc}}_i, \underbrace{\bot, \ldots, \bot}_{t-1 \text{ times}}, \bot})$$

- Ciphertext ($i = 1, \ldots, T$, $\ell = 2, \ldots, t$):

$$\mathsf{ct}_{\ell,i} \leftarrow \mathsf{FE}^{\mathsf{sel}}_t.\mathsf{E}(\mathsf{msk}_t, (i, \tau_{\ell,i}), \ell)$$
$$\mathsf{ct}'_{\ell,i} \leftarrow \mathsf{FE}_{t-1}.\mathsf{E}(\mathsf{msk}_{t-1}, (\boxed{\bot}, x^1_{\ell,i}, i, \tau_{\ell,i}, \underbrace{\bot, \ldots, \bot}_{t-1 \text{ times}}, \bot), \ell - 1).$$

- Functional keys ($i = 1, \ldots, T$):

$$\mathsf{sk}_{f_i} \leftarrow \mathsf{FE}^{\mathsf{sel}}_t.\mathsf{KG}(\mathsf{msk}_t, D_{\bot, f^1_i, i, \underbrace{\bot, \ldots, \bot}_{t \text{ times}}, \bot})$$

As in Claim 4.12 we have the following claim:

Claim A.28. *There exists a probabilistic polynomial-time adversary $\mathcal{B}^{(10)\to(11)}$ such that*

$$\left|\Pr\left[\mathcal{H}^{(10)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(11)}(\lambda) = 1\right]\right| \leq \mathsf{Adv}^{\mathsf{fullFE_{t-1}}}_{\mathsf{FE}_{t-1}, \mathcal{F}', \mathcal{B}^{(10)\to(11)}}(\lambda).$$

Finally, putting together Claims A.18–A.28 with the facts that $\mathsf{Adv}^{\mathsf{fullFE_t}}_{\mathsf{FE}_t, \mathcal{F}, \mathcal{A}}(\lambda) = \mathcal{H}^{(0)}(\lambda)$, $\mathcal{H}^{(2)}(\lambda) = \mathcal{H}^{(3,1,0,\ldots,0)}(\lambda)$, and $\Pr\left[\mathcal{H}^{(11)}(\lambda) = 1\right] = 1/2$, and that t is a fixed constant, we observe that

$$\begin{aligned}
\mathsf{Adv}^{\mathsf{fullFE_t}}_{\mathsf{FE}_t, \mathcal{F}, \mathcal{A}} &\stackrel{\mathsf{def}}{=} \left|\Pr\left[\mathsf{Exp}^{\mathsf{fullFE_t}}_{\mathsf{FE}_t, \mathcal{F}, \mathcal{A}}(\lambda) = 1\right] - \frac{1}{2}\right| \\
&= \left|\Pr\left[\mathcal{H}^{(0)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(11)}(\lambda) = 1\right]\right| \\
&\leq \sum_{i=0}^{1} \left|\Pr\left[\mathcal{H}^{(i)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(i+1)}(\lambda) = 1\right]\right| \\
&\quad + \sum_{j=1}^{T} \sum_{k_2=0}^{T} \cdots \sum_{k_t=0}^{T} \sum_{i=3}^{8} \left|\Pr\left[\mathcal{H}^{(i,j,k_2,\ldots,k_t)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(i+1,j,k_2,\ldots,k_t)}(\lambda) = 1\right]\right| \\
&\quad + \left|\Pr\left[\mathcal{H}^{(3,T+1,0,\ldots,0)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(10)}(\lambda) = 1\right]\right| \\
&\quad + \left|\Pr\left[\mathcal{H}^{(10)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(11)}(\lambda) = 1\right]\right| \\
&\leq T^t \cdot \mathsf{neg}(\lambda) \leq \mathsf{neg}(\lambda).
\end{aligned}$$

■

B Deferred Proofs

B.1 Proofs of Claims 3.2–3.7

Proof of Claim 3.2. The adversary $\mathcal{B}^{(0)\to(1)} = \mathcal{B}$ given input 1^λ is defined as follows. First, $\mathcal{B}$ samples $\mathsf{msk_{out}} \leftarrow \mathsf{1FE.S}(1^\lambda)$, $b \leftarrow \{0,1\}$ and emulates the execution of $\mathcal{A}_1$ on input 1^λ by simulating the encryptions as follows: When $\mathcal{A}_1$ requests the encryption of the pair $(x^0, x^1) \in \mathcal{X}_\lambda$ (with respect to index $\mathsf{i} = 1$), $\mathcal{B}$ samples $s \in \{0,1\}^\lambda$, $\mathsf{msk}^\star \leftarrow \mathsf{1FE.S}(1^\lambda)$, $K \leftarrow \mathsf{PRF.Gen}(1^\lambda)$, queries the key-generation oracle $\mathsf{KG}_\sigma(\mathsf{msk_{in}}, \cdot, \cdot)$ with the pair $(\mathsf{AGG}_{x^b,\perp,0,s,\mathsf{msk}^\star,K}, \mathsf{AGG}_{x^b,x^1,0,s,\mathsf{msk}^\star,K})$ and returns the output to $\mathcal{A}_1$. Moreover, $\mathcal{B}$ runs $\mathsf{1FE.E}(\mathsf{msk_{out}}, (\mathsf{msk}^\star, K^{\mathsf{key}}, 0))$ and returns the output to $\mathcal{A}_1$. When $\mathcal{A}_1$ requests an encryption of $(y^0, y^1) \in \mathcal{Y}_\lambda$ (with respect to index $\mathsf{i} = 2$), $\mathcal{B}$ samples $t \in \{0,1\}^\lambda$, queries the encryption oracle $\mathsf{Enc}_\sigma(\mathsf{msk_{in}}, \cdot, \cdot)$ with the pair $((y^b, \perp, t, \perp, \perp), (y^b, y^1, t, \perp, \perp))$ and returns the output to $\mathcal{A}_1$. We do the above with all input pairs until $\mathcal{A}_1$ outputs state and halts.

Then, we emulate the execution of $\mathcal{A}_2$ on input 1^λ, state and all the ciphertexts that were already generated by simulating the key-generation oracle as follows: When $\mathcal{A}_2$ requests a functional key for $(f^0, f^1) \in \mathcal{F} \times \mathcal{F}$, $\mathcal{B}$ samples a random $z \leftarrow \{0,1\}^\lambda$, runs the key-generation procedure $\mathsf{1FE.KG}(\mathsf{msk_{out}}, D_{f^b,\perp,z,\perp})$ and returns the output to $\mathcal{A}_2$. We do the above until $\mathcal{A}_2$ outputs b' and halts. Finally, $\mathcal{B}$ outputs 1 if $b' = b$ and otherwise it outputs 0.

Note that when $\sigma = 0$ then $\mathcal{A}$'s view is identical to its view in the experiment $\mathcal{H}^{(0)}$, and when $\sigma = 1$ then $\mathcal{A}$'s view is identical to its view in the modified experiment $\mathcal{H}^{(1)}$ described above. Therefore,

$$\left|\Pr\left[\mathcal{H}^{(0)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(1)}(\lambda) = 1\right]\right| = \mathsf{Adv}^{\mathsf{full1FE}}_{\mathsf{1FE},\mathcal{F}',\mathcal{B}^{(0)\to(1)}}(\lambda).$$

■

Proof of Claim 3.3. The adversary $\mathcal{B}^{(1)\to(2)} = \mathcal{B}$ given input 1^λ is defined as follows. First, $\mathcal{B}$ samples $\mathsf{msk_{in}} \leftarrow \mathsf{1FE.S}(1^\lambda)$, $b \leftarrow \{0,1\}$ and emulates the execution of $\mathcal{A}_1$ on input 1^λ by simulating the encryptions as follows: When $\mathcal{A}_1$ requests the encryption of $(x^0, x^1) \in \mathcal{X}_\lambda$ (with respect to index $\mathsf{i} = 1$), $\mathcal{B}$ samples $s \in \{0,1\}^\lambda$, $\mathsf{msk}^\star \leftarrow \mathsf{1FE.S}(1^\lambda)$, $K \leftarrow \mathsf{PRF.Gen}(1^\lambda)$, runs the key-generation procedure $\mathsf{1FE.KG}(\mathsf{msk_{in}}, \cdot)$ with the input $\mathsf{AGG}_{x^b,x^1,0,s,\mathsf{msk}^\star,K}$ and returns the output to $\mathcal{A}_1$. Moreover, $\mathcal{B}$ queries the encryption oracle $\mathsf{Enc}_\sigma(\mathsf{msk_{out}}, \cdot, \cdot)$ with the pair $((\mathsf{msk}^\star, K^{\mathsf{key}}, 0), (\mathsf{msk}^\star, K^{\mathsf{key}}, 0))$ and returns the output to $\mathcal{A}_1$. When $\mathcal{A}_1$ requests an encryption of $(y^0, y^1) \in \mathcal{Y}_\lambda$ (with respect to index $\mathsf{i} = 2$), $\mathcal{B}$ samples $t \in \{0,1\}^\lambda$, runs the encryption oracle $\mathsf{1FE.E}(\mathsf{msk_{in}}, \cdot)$ with the input $(y^b, y^1, t, \perp, \perp)$ and returns the output to $\mathcal{A}_1$.

Then, we emulates the execution of $\mathcal{A}_2$ on input 1^λ, state and all the ciphertexts generated before by simulating the key-generation oracle as follows: When $\mathcal{A}_2$ requests a functional key for $(f^0, f^1) \in \mathcal{F} \times \mathcal{F}$, $\mathcal{B}$ samples a random $z \leftarrow \{0,1\}^\lambda$, queries the key-generation oracle $\mathsf{KG}_\sigma(\mathsf{msk_{out}}, \cdot, \cdot)$ with the pair $(D_{f^b,\perp,z,\perp}, D_{f^b,f^1,z,\perp})$ and returns the output to $\mathcal{A}_2$. We do the above until $\mathcal{A}_2$ outputs b' and halts. Finally, $\mathcal{B}$ outputs 1 if $b' = b$ and otherwise it outputs 0.

Note that when $\sigma = 0$ then $\mathcal{A}$'s view is identical to its view in the experiment $\mathcal{H}^{(1)}$, and when $\sigma = 1$ then $\mathcal{A}$'s view is identical to its view in the modified experiment $\mathcal{H}^{(2)}$ described above. Therefore,

$$\left|\Pr\left[\mathcal{H}^{(1)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(2)}(\lambda) = 1\right]\right| = \mathsf{Adv}^{\mathsf{full1FE}}_{\mathsf{1FE},\mathcal{F}',\mathcal{B}^{(1)\to(2)}}(\lambda).$$

■

Proof of Claim 3.4. The adversary $\mathcal{B}^{(3,j)\to(4,j)} = \mathcal{B}$ given input 1^λ is defined as follows. First, $\mathcal{B}$ samples $\mathsf{msk_{out}} \leftarrow \mathsf{1FE.S}(1^\lambda)$, $b \leftarrow \{0,1\}$, $s_j \leftarrow \{0,1\}^\lambda$, $\mathsf{msk}^\star_j \leftarrow \mathsf{1FE.S}(1^\lambda)$ and $K_j \leftarrow \mathsf{PRF.Eval}(1^\lambda)$, and emulates the execution of $\mathcal{A}_1$ on input 1^λ by simulating the encryptions as follows: When $\mathcal{A}_1$ requests for the encryption of the i^{th} input pair $(x^0, x^1) \in \mathcal{X}_\lambda$ (with respect to index $\mathsf{i} = 1$) for $i \leq j-1$, $\mathcal{B}$ samples $s \in \{0,1\}^\lambda$, $\mathsf{msk}^\star \leftarrow \mathsf{1FE.S}(1^\lambda)$, $K \leftarrow \mathsf{PRF.Gen}(1^\lambda)$, queries the key-generation oracle $\mathsf{KG}_\sigma(\mathsf{msk_{in}}, \cdot, \cdot)$ with the pair $(\mathsf{AGG}_{x^b,x^1,1,s,\mathsf{msk}^\star,K}, \mathsf{AGG}_{x^b,x^1,1,s,\mathsf{msk}^\star,K})$ and returns the output to $\mathcal{A}_1$. Moreover, $\mathcal{B}$ runs $\mathsf{1FE.E}(\mathsf{msk_{out}}, (\mathsf{msk}^\star, K^{\mathsf{key}}, 1))$ and returns the output to $\mathcal{A}_1$. When $\mathcal{A}_1$ requests for the encryption of the i^{th} input pair $(x^0, x^1) \in \mathcal{X}_\lambda$ (with respect to index $\mathsf{i} = 1$) for $i = j$, $\mathcal{B}$ sets $s = s_j$, $\mathsf{msk}^\star = \mathsf{msk}^\star_j$, $K = K_j$, queries the key-generation oracle $\mathsf{KG}_\sigma(\mathsf{msk_{in}}, \cdot, \cdot)$ with the pair $(\mathsf{AGG}_{x^b,x^1,0,s,\mathsf{msk}^\star,K}, \mathsf{AGG}_{x^b,x^1,1,s,\perp,\perp})$ and returns the output to $\mathcal{A}_1$. Moreover, $\mathcal{B}$ runs $\mathsf{1FE.E}(\mathsf{msk_{out}}, (\mathsf{msk}^\star, K^{\mathsf{key}}, 0))$ and returns the output to $\mathcal{A}_1$. When $\mathcal{A}_1$ requests for the encryption of the i^{th} input pair $(x^0, x^1) \in \mathcal{X}_\lambda$ (with respect to index $\mathsf{i} = 1$) for $i \geq j+1$, $\mathcal{B}$ samples $s \in \{0,1\}^\lambda$, $\mathsf{msk}^\star \leftarrow \mathsf{1FE.S}(1^\lambda)$, $K \leftarrow \mathsf{PRF.Gen}(1^\lambda)$, queries the key-generation oracle $\mathsf{KG}_\sigma(\mathsf{msk_{in}}, \cdot, \cdot)$ with the pair $(\mathsf{AGG}_{x^b,x^1,0,s,\mathsf{msk}^\star,K}, \mathsf{AGG}_{x^b,x^1,0,s,\mathsf{msk}^\star,K})$ and returns the output to $\mathcal{A}_1$. Moreover, $\mathcal{B}$ runs $\mathsf{1FE.E}(\mathsf{msk_{out}}, (\mathsf{msk}^\star, K^{\mathsf{key}}, 0))$ and returns the output to $\mathcal{A}_1$. When $\mathcal{A}_1$ requests an encryption of $(y^0, y^1) \in \mathcal{Y}_\lambda$ (with respect to index $\mathsf{i} = 2$) $\mathcal{B}$ samples $t \in \{0,1\}^\lambda$, queries the encryption oracle $\mathsf{Enc}_\sigma(\mathsf{msk_{in}}, \cdot, \cdot)$ with the pair $((y^b, y^1, t, \perp, \perp), (y^b, y^1, t, s_j, \gamma))$, where $\gamma = \mathsf{1FE.E}(\mathsf{msk}^\star_j, (x^b_j, y^b); \mathsf{PRF.Eval}(K_j, t))$ and returns the output to $\mathcal{A}_1$.

Denote by (x^0_j, x^1_j) the j^{th} ciphertext pair issued with index $\mathsf{i} = 1$. $\mathcal{B}$ emulates the execution of $\mathcal{A}_2$ on input 1^λ, state and all the ciphertexts from before by simulating the key-generation oracle as follows: When $\mathcal{A}_2$ requests a functional key for $(f^0, f^1) \in \mathcal{F} \times \mathcal{F}$, $\mathcal{B}$ samples a random $z \leftarrow \{0,1\}^\lambda$, runs the key-generation procedure $\mathsf{1FE.KG}(\mathsf{msk_{out}}, \cdot)$ with the circuit $D_{f^b,f^1,z,\perp}$ and returns the output to $\mathcal{A}_2$. We do the above until $\mathcal{A}_2$ outputs b' and halts. Finally, $\mathcal{B}$ outputs 1 if $b' = b$ and otherwise it outputs 0.

Note that when $\sigma = 0$ then $\mathcal{A}$'s view is identical to its view in the experiment $\mathcal{H}^{(3,j)}$, and when $\sigma = 1$ then $\mathcal{A}$'s view is identical to its view in the modified experiment $\mathcal{H}^{(4,j)}$ described above. Therefore,

$$\left|\Pr\left[\mathcal{H}^{(3,j)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(4,j)}(\lambda) = 1\right]\right| \leq \mathsf{Adv}^{\mathsf{full1FE}}_{\mathsf{1FE},\mathcal{F}',\mathcal{B}^{(3,j)\to(4,j)}}(\lambda).$$

■

Proof of Claim 3.5. The adversary $\mathcal{B}^{(4,j)\to(5,j)} = \mathcal{B}$ given input 1^λ is defined as follows. First, $\mathcal{B}$ samples $\mathsf{msk_{in}} \leftarrow \mathsf{1FE.S}(1^\lambda)$, $b \leftarrow \{0,1\}$, $s_j \leftarrow \{0,1\}^\lambda$, $\mathsf{msk}^\star_j \leftarrow \mathsf{1FE.S}(1^\lambda)$ and $K_j \leftarrow \mathsf{PRF.Eval}(1^\lambda)$, and emulates the execution of $\mathcal{A}_1$ on input 1^λ by simulating the encryptions as follows: When $\mathcal{A}_1$ requests for the encryption of the i^{th} input pair $(x^0, x^1) \in \mathcal{X}_\lambda$ (with respect to index $\mathsf{i} = 1$) for $i \leq j-1$, $\mathcal{B}$ samples $s \in \{0,1\}^\lambda$, $\mathsf{msk}^\star \leftarrow \mathsf{1FE.S}(1^\lambda)$, $K \leftarrow \mathsf{PRF.Gen}(1^\lambda)$, runs the key-generation procedure $\mathsf{1FE.KG}(\mathsf{msk_{in}}, \cdot)$ with the input $\mathsf{AGG}_{x^b,x^1,1,s,\mathsf{msk}^\star,K}$ and returns the output to $\mathcal{A}_1$. Moreover, $\mathcal{B}$ queries the encryption oracle $\mathsf{Enc}_\sigma(\mathsf{msk_{out}}, \cdot, \cdot)$ with the pair $((\mathsf{msk}^\star, K^{\mathsf{key}}, 0), (\mathsf{msk}^\star, K^{\mathsf{key}}, 1))$ and returns the output to $\mathcal{A}_1$. When $\mathcal{A}_1$ requests for the encryption of the i^{th} input pair $(x^0, x^1) \in \mathcal{X}_\lambda$ (with respect to index $\mathsf{i} = 1$) for $i = j$, $\mathcal{B}$ sets $s = s_j$, $\mathsf{msk}^\star = \mathsf{msk}^\star_j$, $K = K_j$, runs the key-generation procedure $\mathsf{1FE.KG}(\mathsf{msk_{in}}, \cdot)$ with the input $\mathsf{AGG}_{x^b,x^1,0,s,\mathsf{msk}^\star,K}$ and returns the output to $\mathcal{A}_1$. Moreover, $\mathcal{B}$ queries the encryption oracle $\mathsf{Enc}_\sigma(\mathsf{msk_{out}}, \cdot, \cdot)$ with the pair $((\mathsf{msk}^\star, K^{\mathsf{key}}, 0), (\perp, \perp, 0))$ and returns the output to $\mathcal{A}_1$. When $\mathcal{A}_1$ requests for the encryption of the i^{th} input pair $(x^0, x^1) \in \mathcal{X}_\lambda$ (with respect to index $\mathsf{i} = 1$) for $i \leq j-1$, $\mathcal{B}$ samples $s \in \{0,1\}^\lambda$, $\mathsf{msk}^\star \leftarrow \mathsf{1FE.S}(1^\lambda)$, $K \leftarrow \mathsf{PRF.Gen}(1^\lambda)$, runs the key-generation procedure $\mathsf{1FE.KG}(\mathsf{msk_{in}}, \cdot)$ with the input $\mathsf{AGG}_{x^b,x^1,0,s,\mathsf{msk}^\star,K}$ and returns the output to $\mathcal{A}_1$. Moreover, $\mathcal{B}$ queries the encryption oracle $\mathsf{Enc}_\sigma(\mathsf{msk_{out}}, \cdot, \cdot)$ with the pair $((\mathsf{msk}^\star, K^{\mathsf{key}}, 0), (\mathsf{msk}^\star, K^{\mathsf{key}}, 0))$ and returns the output to $\mathcal{A}_1$. When $\mathcal{A}_1$ requests an encryption of $(y^0, y^1) \in \mathcal{Y}_\lambda$ (with respect to index $\mathsf{i} = 2$) $\mathcal{B}$ samples $t \in \{0,1\}^\lambda$, runs the encryption procedure

$\mathsf{1FE.E}(\mathsf{msk_{in}}, \cdot)$ with the input $(y^b, y^1, t, s_j, \gamma)$, where $\gamma = \mathsf{1FE.E}(\mathsf{msk}_j^\star, (x_j^b, y^b); \mathsf{PRF.Eval}(K_j, t))$ and returns the output to $\mathcal{A}_1$

Denote by (x_j^0, x_j^1) the j^{th} ciphertext pair issued with index $\mathsf{i} = 1$. $\mathcal{B}$ emulates the execution of $\mathcal{A}_2$ on input 1^λ, state and all the ciphertexts from before by simulating the key-generation oracle as follows: When $\mathcal{A}_2$ requests a functional key for $(f^0, f^1) \in \mathcal{F} \times \mathcal{F}$, $\mathcal{B}$ samples a random $z \leftarrow \{0,1\}^\lambda$, queries the key-generation oracle $\mathsf{KG}_\sigma(\mathsf{msk_{out}}, \cdot, \cdot)$ with the pair $(D_{f^b,f^1,z,\perp}, D_{f^b,f^1,z,\delta})$, where $\delta = \mathsf{1FE.KG}(\mathsf{msk}_j^\star, D_{f^b}; \mathsf{PRF}(K_j^{\mathsf{key}}, z_i))$, and returns the output to $\mathcal{A}_2$. We do the above until $\mathcal{A}_2$ outputs b' and halts. Finally, $\mathcal{B}$ outputs 1 if $b' = b$ and otherwise it outputs 0.

Note that when $\sigma = 0$ then $\mathcal{A}$'s view is identical to its view in the experiment $\mathcal{H}^{(4,j)}$, and when $\sigma = 1$ then $\mathcal{A}$'s view is identical to its view in the modified experiment $\mathcal{H}^{(5,j)}$ described above. Therefore,

$$\left|\Pr\left[\mathcal{H}^{(4,j)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(5,j)}(\lambda) = 1\right]\right| \leq \mathsf{Adv}^{\mathsf{full1FE}}_{\mathsf{1FE},\mathcal{F}',\mathcal{B}^{(4,j)\to(5,j)}}(\lambda).$$

■

Proof of Claim 3.6. The adversary $\mathcal{B}^{(5,j)\to(6,j)} = \mathcal{B}$ given input 1^λ is defined as follows. Recall that $\mathcal{B}$ has access to an oracle, denoted $R(\cdot)$, that is either a random function or a PRF and its goal is to distinguish between the two cases. First, $\mathcal{B}$ samples $\mathsf{msk_{in}}, \mathsf{msk_{out}} \leftarrow \mathsf{1FE.S}(1^\lambda)$, $b \leftarrow \{0,1\}$, $s_j \leftarrow \{0,1\}^\lambda$ and $\mathsf{msk}_j^\star \leftarrow \mathsf{1FE.S}(1^\lambda)$, and emulates the execution of $\mathcal{A}_1$ on input 1^λ by simulating the encryptions as follows: When $\mathcal{A}_1$ requests for the encryption of the i^{th} input pair $(x^0, x^1) \in \mathcal{X}_\lambda$ (with respect to index $\mathsf{i} = 1$) for $i \leq j - 1$, $\mathcal{B}$ samples $s \in \{0,1\}^\lambda$, $\mathsf{msk}^\star \leftarrow \mathsf{1FE.S}(1^\lambda)$, $K \leftarrow \mathsf{PRF.Gen}(1^\lambda)$, runs the key-generation procedure $\mathsf{1FE.KG}(\mathsf{msk_{in}}, \cdot)$ with the input $\mathsf{AGG}_{x^b,x^1,1,s,\mathsf{msk}^\star,K}$ and returns the output to $\mathcal{A}_1$. Moreover, $\mathcal{B}$ runs the encryption procedure $\mathsf{1FE.E}(\mathsf{msk_{out}}, \cdot)$ with the input $(\mathsf{msk}^\star, K^{\mathsf{key}}, 1)$ and returns the output to $\mathcal{A}_1$. When $\mathcal{A}_1$ requests for the encryption of the i^{th} input pair $(x^0, x^1) \in \mathcal{X}_\lambda$ (with respect to index $\mathsf{i} = 1$) for $i \leq j - 1$, $\mathcal{B}$ sets $s = s_j$, $\mathsf{msk}^\star = \mathsf{msk}_j^\star$, $K = K_j$, runs the key-generation procedure $\mathsf{1FE.KG}(\mathsf{msk_{in}}, \cdot)$ with the input $\mathsf{AGG}_{x^b,x^1,0,s,\perp,\perp}$ and returns the output to $\mathcal{A}_1$. Moreover, $\mathcal{B}$ runs the encryption procedure $\mathsf{1FE.E}(\mathsf{msk_{out}}, \cdot)$ with the input $(\perp, \perp, 0)$ and returns the output to $\mathcal{A}_1$. When $\mathcal{A}_1$ requests for the encryption of the i^{th} input pair $(x^0, x^1) \in \mathcal{X}_\lambda$ (with respect to index $\mathsf{i} = 1$) for $i \geq j + 1$, $\mathcal{B}$ samples $s \in \{0,1\}^\lambda$, $\mathsf{msk}^\star \leftarrow \mathsf{1FE.S}(1^\lambda)$, $K \leftarrow \mathsf{PRF.Gen}(1^\lambda)$, runs the key-generation procedure $\mathsf{1FE.KG}(\mathsf{msk_{in}}, \cdot)$ with the input $\mathsf{AGG}_{x^b,x^1,0,s,\mathsf{msk}^\star,K}$ and returns the output to $\mathcal{A}_1$. Moreover, $\mathcal{B}$ runs the encryption procedure $\mathsf{1FE.E}(\mathsf{msk_{out}}, \cdot)$ with the input $(\mathsf{msk}^\star, K^{\mathsf{key}}, 0)$ and returns the output to $\mathcal{A}_1$. When $\mathcal{A}_1$ requests an encryption of $(y^0, y^1) \in \mathcal{Y}_\lambda$ (with respect to index $\mathsf{i} = 2$) $\mathcal{B}$ samples $t \in \{0,1\}^\lambda$, runs the encryption procedure $\mathsf{1FE.E}(\mathsf{msk_{in}}, \cdot)$ with the input $(y^b, y^1, t, s_j, \gamma)$, where $\gamma = \mathsf{1FE.E}(\mathsf{msk}_j^\star, (x_j^b, y^b); R(t_i)))$, where $R(t_i)$ is either the output of a PRF or a uniformly random string, and returns the output to $\mathcal{A}_1$.

Denote by (x_j^0, x_j^1) the j^{th} ciphertext pair issued with index $\mathsf{i} = 1$. $\mathcal{B}$ emulates the execution of $\mathcal{A}_2$ on input 1^λ and state by simulating the key-generation oracle as follows: When $\mathcal{A}_2$ requests a functional key for $(f^0, f^1) \in \mathcal{F} \times \mathcal{F}$, $\mathcal{B}$ samples a random $z \leftarrow \{0,1\}^\lambda$, queries the key-generation oracle $\mathsf{1FE.KG}(\mathsf{msk_{out}}, \cdot)$ with the circuit $D_{f^b,f^1,z,\delta}$, where $\delta = \mathsf{1FE.KG}(\mathsf{msk}_j^\star, D_{f^b}; R(z_i)))$, where $R(z_i)$ is either the output of a PRF or a uniformly random string, and returns the output to $\mathcal{A}_2$. We do the above until $\mathcal{A}_2$ outputs b' and halts. Finally, $\mathcal{B}$ outputs 1 if $b' = b$ and otherwise it outputs 0.

Note that when $R(\cdot)$ corresponds to a pseudorandom function then $\mathcal{A}$'s view is identical to its view in the experiment $\mathcal{H}^{(5,j)}$, and when $R(\cdot)$ corresponds to a uniformly random function then $\mathcal{A}$'s view is identical to its view in the modified experiment $\mathcal{H}^{(6,j)}$. Therefore,

$$\left|\Pr\left[\mathcal{H}^{(5,j)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(6,j)}(\lambda) = 1\right]\right| \leq \mathsf{Adv}_{\mathsf{PRF},\mathcal{B}^{(5,j)\to(6,j)}}(\lambda).$$

■

Proof of Claim 3.7. The adversary $\mathcal{B}^{(6,j)\to(7,j)} = \mathcal{B}$ given input 1^λ is defined as follows. First, $\mathcal{B}$ samples $\mathsf{msk_{in}}, \mathsf{msk_{out}} \leftarrow \mathsf{1FE.S}(1^\lambda)$, $b \leftarrow \{0,1\}$, $s_j \leftarrow \{0,1\}^\lambda$ and $K_j \leftarrow \mathsf{PRF.Eval}(1^\lambda)$, and emulates the execution of $\mathcal{A}_1$ on input 1^λ by simulating the encryptions as follows: When $\mathcal{A}_1$ requests for the encryption of the i^{th} input pair $(x^0, x^1) \in \mathcal{X}_\lambda$ (with respect to index $\mathsf{i} = 1$) for $i \leq j-1$, $\mathcal{B}$ samples $s \in \{0,1\}^\lambda$, $\mathsf{msk}^\star \leftarrow \mathsf{1FE.S}(1^\lambda)$, $K \leftarrow \mathsf{PRF.Gen}(1^\lambda)$, runs the key-generation procedure $\mathsf{1FE.KG}(\mathsf{msk_{in}}, \cdot)$ with the input $\mathsf{AGG}_{x^b, x^1, 1, s, \mathsf{msk}^\star, K}$ and returns the output to $\mathcal{A}_1$. Moreover, $\mathcal{B}$ runs the encryption procedure $\mathsf{1FE.E}(\mathsf{msk_{out}}, \cdot)$ with the input $(\mathsf{msk}^\star, K^{\mathsf{key}}, 1)$ and returns the output to $\mathcal{A}_1$. When $\mathcal{A}_1$ requests for the encryption of the i^{th} input pair $(x^0, x^1) \in \mathcal{X}_\lambda$ (with respect to index $\mathsf{i} = 1$) for $i = j$, $\mathcal{B}$ sets $s = s_j$ and $K = K_j$, runs the key-generation procedure $\mathsf{1FE.KG}(\mathsf{msk_{in}}, \cdot)$ with the input $\mathsf{AGG}_{x^b, x^1, 0, s, \perp, \perp}$ and returns the output to $\mathcal{A}_1$. Moreover, $\mathcal{B}$ runs the encryption procedure $\mathsf{1FE.E}(\mathsf{msk_{out}}, \cdot)$ with the input $(\perp, \perp, 0)$ and returns the output to $\mathcal{A}_1$. When $\mathcal{A}_1$ requests for the encryption of the i^{th} input pair $(x^0, x^1) \in \mathcal{X}_\lambda$ (with respect to index $\mathsf{i} = 1$) for $i \geq j+1$, $\mathcal{B}$ samples $s \in \{0,1\}^\lambda$, $\mathsf{msk}^\star \leftarrow \mathsf{1FE.S}(1^\lambda)$, $K \leftarrow \mathsf{PRF.Gen}(1^\lambda)$, runs the key-generation procedure $\mathsf{1FE.KG}(\mathsf{msk_{in}}, \cdot)$ with the input $\mathsf{AGG}_{x^b, x^1, 0, s, \mathsf{msk}^\star, K}$ and returns the output to $\mathcal{A}_1$. Moreover, $\mathcal{B}$ runs the encryption procedure $\mathsf{1FE.E}(\mathsf{msk_{out}}, \cdot)$ with the input $(\mathsf{msk}^\star, K^{\mathsf{key}}, 0)$ and returns the output to $\mathcal{A}_1$. When $\mathcal{A}_1$ requests for the encryption of $(y^0, y^1) \in \mathcal{Y}_\lambda$ (with respect to index $\mathsf{i} = 2$) $\mathcal{B}$ samples $t \in \{0,1\}^\lambda$, queries the encryption oracle $\mathsf{Enc}_\sigma(\mathsf{msk}^\star_j, \cdot, \cdot)$ with the pair $((x^b_j, y^b), (x^1_j, y^1))$ to get γ, runs the encryption procedure $\mathsf{1FE.E}(\mathsf{msk_{in}}, \cdot)$ with the input $(y^b, y^1, t, s_j, \gamma)$ and returns the output to $\mathcal{A}_1$.

Denote by (x^0_j, x^1_j) the j^{th} ciphertext pair issued with index $\mathsf{i} = 1$. $\mathcal{B}$ emulates the execution of $\mathcal{A}_2$ on input 1^λ and state by simulating the key-generation oracle as follows: When $\mathcal{A}_2$ requests a functional key for $(f^0, f^1) \in \mathcal{F} \times \mathcal{F}$, $\mathcal{B}$ samples a random $z \leftarrow \{0,1\}^\lambda$, queries the key generation oracle $\mathsf{KG}_\sigma(\mathsf{msk}^\star_j, \cdot, \cdot)$ with the pair (C_{f^b}, C_{f^1}) to get δ, runs the key-generation procedure $\mathsf{1FE.KG}(\mathsf{msk_{out}}, \cdot)$ with the input $D_{f^b, f^1, z, \delta}$ and returns the output to $\mathcal{A}_2$. We do the above until $\mathcal{A}_2$ outputs b' and halts. Finally, $\mathcal{B}$ outputs 1 if $b' = b$ and otherwise it outputs 0.

Note that when $\sigma = 0$ then $\mathcal{A}$'s view is identical to its view in the experiment $\mathcal{H}^{(6,j)}$, and when $\sigma = 1$ then $\mathcal{A}$'s view is identical to its view in the modified experiment $\mathcal{H}^{(7,j)}$ described above. Therefore,

$$\left|\Pr\left[\mathcal{H}^{(6,j)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(7,j)}(\lambda) = 1\right]\right| \leq \mathsf{Adv}^{\mathsf{full1FE}}_{\mathsf{1FE}, \mathcal{F}', \mathcal{B}^{(6,j)\to(7,j)}}(\lambda).$$

■

B.2 Proofs of Claims 4.2–4.7

Proof of Claim 4.2. The adversary $\mathcal{B}^{(0)\to(1)} = \mathcal{B}$ given input 1^λ is defined as follows. First, $\mathcal{B}$ samples $\mathsf{msk}_2 \leftarrow \mathsf{2FE^{sel}.S}(1^\lambda)$, $b \leftarrow \{0,1\}$ and emulates the execution of $\mathcal{A}$ on input 1^λ by simulating the encryption oracle as follows: When $\mathcal{A}$ queries the encryption oracle with $(x^0, x^1) \in \mathcal{X}_\lambda$ (with respect to index $\mathsf{i} = 1$), $\mathcal{B}$ samples $s \in \{0,1\}^\lambda$, $K^{\mathsf{msk}}, K^{\mathsf{key}}, K^{\mathsf{enc}} \leftarrow \mathsf{PRF.Gen}(1^\lambda)$, queries the key-generation oracle $\mathsf{KG}_\sigma(\mathsf{msk}_1, \cdot, \cdot)$ with the pair $(\mathsf{AGG}_{x^b, \perp, 0, s, K^{\mathsf{msk}}, K^{\mathsf{enc}}, \perp, \perp}, \mathsf{AGG}_{x^b, x^1, 0, s, K^{\mathsf{msk}}, K^{\mathsf{enc}}, \perp, \perp})$ and returns the output to $\mathcal{A}$. Moreover, $\mathcal{B}$ runs $\mathsf{2FE^{sel}.E}(\mathsf{msk}_2, (K^{\mathsf{msk}}, K^{\mathsf{key}}, s, 0), 1)$ and returns the output to $\mathcal{A}$. When $\mathcal{A}$ requests the i^{th} encryption of $(y^0, y^1) \in \mathcal{Y}_\lambda$ (with respect to index $\mathsf{i} = 2$), $\mathcal{B}$ samples $t \in \{0,1\}^\lambda$, queries the encryption oracle $\mathsf{Enc}_\sigma(\mathsf{msk}_1, \cdot, \cdot)$ with the pair $((y^b, \perp, 1, t, \perp, \perp), (y^b, y^1, i, t, \perp, \perp))$ and returns the output to $\mathcal{A}$. Moreover, $\mathcal{B}$ runs $\mathsf{2FE^{sel}.E}(\mathsf{msk}_2, (1, t), 2)$ and returns the output to $\mathcal{A}$. When $\mathcal{A}$ requests a functional key for $(f^0, f^1) \in \mathcal{F} \times \mathcal{F}$, $\mathcal{B}$ runs the key-generation procedure $\mathsf{2FE^{sel}.KG}(\mathsf{msk}_2, D_{f^b, \perp, 1, \perp, \perp, \perp})$ and returns the output to $\mathcal{A}$.

Note that when $\sigma = 0$ then $\mathcal{A}$'s view is identical to its view in the experiment $\mathcal{H}^{(0)}$, and when $\sigma = 1$ then $\mathcal{A}$'s view is identical to its view in the modified experiment $\mathcal{H}^{(1)}$ described above. Therefore,

$$\left|\Pr\left[\mathcal{H}^{(0)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(1)}(\lambda) = 1\right]\right| = \mathsf{Adv}^{\mathsf{full1FE}}_{\mathsf{1FE},\mathcal{F}',\mathcal{B}^{(0)\to(1)}}(\lambda).$$

■

Proof of Claim 4.3. The adversary $\mathcal{B}^{(1)\to(2)} = (\mathcal{B}_1, \mathcal{B}_2)$ given input 1^λ is defined as follows. First, $\mathcal{B}_1$ samples $\mathsf{msk}_1 \leftarrow \mathsf{1FE.S}(1^\lambda)$ and $b \leftarrow \{0,1\}$. Then, $\mathcal{B}_1$ samples $K^{\mathsf{msk}}_1, \ldots, K^{\mathsf{msk}}_T, K^{\mathsf{key}}_1, \ldots, K^{\mathsf{key}}_T$, $K^{\mathsf{enc}}_1, \ldots, K^{\mathsf{enc}}_T \leftarrow \mathsf{PRF.Gen}(1^\lambda)$, $s_1, \ldots, s_T \leftarrow \{0,1\}^\lambda$ and $t_1, \ldots, t_T \leftarrow \{0,1\}^\lambda$, where T is upper bounded by the running time of $\mathcal{A}$. For $i \in [T]$ the adversary $\mathcal{B}_1$ requests the encryption of the pair $((K^{\mathsf{msk}}_i, K^{\mathsf{key}}_i, s_i, 0), (K^{\mathsf{msk}}_i, K^{\mathsf{key}}_i, s_i, 0))$ with respect to index $\mathsf{i} = 1$ and with the pairs $((1, t_i), (i, t_i))$ with respect to index $\mathsf{i} = 2$ to get $\mathsf{ct}_{1,1}, \ldots, \mathsf{ct}_{1,T}, \mathsf{ct}_{2,1}, \ldots, \mathsf{ct}_{2,T}$. Finally, $\mathcal{B}_1$ outputs the state information state which is all its memory.

Next, $\mathcal{B}_2$ given as input 1^λ, state and $\mathsf{ct}_{1,1}, \ldots, \mathsf{ct}_{1,T}, \mathsf{ct}_{2,1}, \ldots, \mathsf{ct}_{2,T}$ emulates the execution of $\mathcal{A}$ on input 1^λ by simulating the encryption oracle as follows: When $\mathcal{A}$ queries for the i^{th} time the encryption oracle with $(x^0, x^1) \in \mathcal{X}_\lambda$ (with respect to index $\mathsf{i} = 1$), $\mathcal{B}_2$ runs the key-generation procedure $\mathsf{1FE.KG}(\mathsf{msk}_1, \cdot)$ with the input $\mathsf{AGG}_{x^b, x^1, 0, s_i, K^{\mathsf{msk}}_i, K^{\mathsf{enc}}_i, \perp, \perp}$ to get $\mathsf{sk}_{1,i}$ and returns $(\mathsf{ct}_{1,i}, \mathsf{sk}_{1,i})$ to $\mathcal{A}$. When $\mathcal{A}$ queries for the i^{th} time the encryption oracle with $(y^0, y^1) \in \mathcal{Y}_\lambda$ (with respect to index $\mathsf{i} = 2$), $\mathcal{B}_2$ runs the encryption procedure $\mathsf{1FE.E}(\mathsf{msk}_1, \cdot)$ with the input $(y^b, y^1, i, t, \perp, \perp)$ to get $\mathsf{ct}_{3,i}$ and returns the pair $(\mathsf{ct}_{2,i}, \mathsf{ct}_{3,i})$ to $\mathcal{A}$. When $\mathcal{A}$ requests for the i^{th} time a functional key for $(f^0, f^1) \in \mathcal{F} \times \mathcal{F}$, $\mathcal{B}_2$ queries the key-generation oracle $\mathsf{KG}_\sigma(\mathsf{msk}_2, \cdot, \cdot)$ with the pair $(D_{f^b, \perp, 1, \perp, \perp, \perp}, D_{f^b, f^1, i, \perp, \perp, \perp})$ and returns the output to $\mathcal{A}$.

Note that when $\sigma = 0$ then $\mathcal{A}$'s view is identical to its view in the experiment $\mathcal{H}^{(1)}$, and when $\sigma = 1$ then $\mathcal{A}$'s view is identical to its view in the modified experiment $\mathcal{H}^{(2)}$ described above. Therefore,

$$\left|\Pr\left[\mathcal{H}^{(1)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(2)}(\lambda) = 1\right]\right| \leq \mathsf{Adv}^{\mathsf{sel2FE}}_{\mathsf{2FE^{sel}},\mathcal{F}',\mathcal{B}^{(1)\to(2)}}(\lambda).$$

■

Proof of Claim 4.4. The adversary $\mathcal{B}^{(3,j,k)\to(4,j,k)} = \mathcal{B}$ given input 1^λ is defined as follows. First, $\mathcal{B}$ samples $\mathsf{msk}_2 \leftarrow \mathsf{2FE^{sel}.S}(1^\lambda), s_j, t_k \leftarrow \{0,1\}^\lambda$, $K^{\mathsf{msk}}_j, K^{\mathsf{key}}_j, K^{\mathsf{enc}}_j \leftarrow \mathsf{PRF.Gen}(1^\lambda)$, $b \leftarrow \{0,1\}$, computes $\mathsf{msk}_{s_j,t_k} = \mathsf{1FE.S}(1^\lambda; \mathsf{PRF.Eval}(K^{\mathsf{msk}}_j, t_k))$ and emulates the execution of $\mathcal{A}$ on input 1^λ by simulating the encryption oracle as follows.

When $\mathcal{A}$ queries the encryption oracle with $(x^0, x^1) \in \mathcal{X}_\lambda$ (with respect to index $\mathsf{i} = 1$) for the i^{th} time for $i \leq j - 1$, $\mathcal{B}$ samples $s \in \{0,1\}^\lambda$, $K^{\mathsf{msk}}, K^{\mathsf{key}}, K^{\mathsf{enc}} \leftarrow \mathsf{PRF.Gen}(1^\lambda)$, queries the key-generation oracle $\mathsf{KG}_\sigma(\mathsf{msk}_1, \cdot, \cdot)$ with the pair $(\mathsf{AGG}_{x^b, x^1, T, s, K^{\mathsf{msk}}, K^{\mathsf{enc}}, \perp, \perp}, \mathsf{AGG}_{x^b, x^1, T, s, K^{\mathsf{msk}}, K^{\mathsf{enc}}, \perp, \perp})$ and returns the output to $\mathcal{A}$. Moreover, $\mathcal{B}$ runs $\mathsf{2FE^{sel}.E}(\mathsf{msk}_2, (K^{\mathsf{msk}}, K^{\mathsf{key}}, s, T), 1)$ and returns the output to $\mathcal{A}$.

When $\mathcal{A}$ queries the encryption oracle with $(x^0, x^1) \in \mathcal{X}_\lambda$ (with respect to index $\mathsf{i} = 1$) for the i^{th} time for $i = j$, $\mathcal{B}$ queries the key-generation oracle $\mathsf{KG}_\sigma(\mathsf{msk}_1, \cdot, \cdot)$ with $(\mathsf{AGG}_{x^b, x^1, k, s_j, K^{\mathsf{msk}}_j, K^{\mathsf{enc}}_j, \perp, \perp}$, $\mathsf{AGG}_{x^b, x^1, k, s_j, K^{\mathsf{msk}}_j|_{\{t_k\}}, K^{\mathsf{enc}}_j|_{\{t_k\}}, t_k, \gamma})$, where $\gamma = \mathsf{1FE.E}(\mathsf{msk}_{s_j,t_k}, (x^b_j, y^b_k); \mathsf{PRF.Eval}(K^{\mathsf{enc}}_i, t_k))$, and returns the output to $\mathcal{A}$. Moreover, $\mathcal{B}$ runs $\mathsf{2FE^{sel}.E}(\mathsf{msk}_2, (K^{\mathsf{msk}}_j, K^{\mathsf{key}}_j, s_j, k), 1)$ and returns the output to $\mathcal{A}$.

When $\mathcal{A}$ queries the encryption oracle with $(x^0, x^1) \in \mathcal{X}_\lambda$ (with respect to index $\mathsf{i} = 1$) for the i^{th} time for $i \geq j + 1$, $\mathcal{B}$ samples $s \in \{0,1\}^\lambda$, $K^{\mathsf{msk}}, K^{\mathsf{key}}, K^{\mathsf{enc}} \leftarrow \mathsf{PRF.Gen}(1^\lambda)$, queries the key-generation oracle $\mathsf{KG}_\sigma(\mathsf{msk}_1, \cdot, \cdot)$ with the pair $(\mathsf{AGG}_{x^b, x^1, 0, s, K^{\mathsf{msk}}, K^{\mathsf{enc}}, \perp, \perp}, \mathsf{AGG}_{x^b, x^1, 0, s, K^{\mathsf{msk}}, K^{\mathsf{enc}}, \perp, \perp})$

and returns the output to $\mathcal{A}$. Moreover, $\mathcal{B}$ runs $\mathsf{2FE^{sel}.E}(\mathsf{msk}_2, (K^{\mathsf{msk}}, K^{\mathsf{key}}, s, 0), 1)$ and returns the output to $\mathcal{A}$. When $\mathcal{A}$ requests the i^{th} encryption of $(y^0, y^1) \in \mathcal{Y}_\lambda$ (with respect to index $\mathsf{i} = 2$), $\mathcal{B}$ samples $t_i \in \{0,1\}^\lambda$ (unless $i = k$ in which case t_i is already known), queries the encryption oracle $\mathsf{Enc}_\sigma(\mathsf{msk}_1, \cdot, \cdot)$ with the pair $((y^b, y^1, 1, t_i, \perp, \perp), (y^b, y^1, i, t_i, \perp, \perp))$ and returns the output to $\mathcal{A}$. Moreover, $\mathcal{B}$ runs $\mathsf{2FE^{sel}.E}(\mathsf{msk}_2, (i,t), 2)$ and returns the output to $\mathcal{A}$. When $\mathcal{A}$ requests a functional key for $(f^0, f^1) \in \mathcal{F} \times \mathcal{F}$, $\mathcal{B}$ runs the key-generation procedure $\mathsf{2FE^{sel}.KG}(\mathsf{msk}_2, D_{f^b, f^1, i, \perp, \perp, \perp})$ and returns the output to $\mathcal{A}$.

Note that when $\sigma = 0$ then $\mathcal{A}$'s view is identical to its view in the experiment $\mathcal{H}^{(3,j,k)}$, and when $\sigma = 1$ then $\mathcal{A}$'s view is identical to its view in the modified experiment $\mathcal{H}^{(4,j,k)}$ described above. Therefore,

$$\left| \Pr\left[\mathcal{H}^{(3,j,k)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(4,j,k)}(\lambda) = 1\right] \right| \leq \mathsf{Adv}^{\mathsf{full1FE}}_{\mathsf{1FE}, \mathcal{F}', \mathcal{B}^{(3,j,k)\to(4,j,k)}}(\lambda).$$

■

Proof of Claim 4.5. The adversary $\mathcal{B}^{(4,j,k)\to(5,j,k)} = (\mathcal{B}_1, \mathcal{B}_2)$ given input 1^λ is defined as follows. First, $\mathcal{B}_1$ samples $\mathsf{msk}_1 \leftarrow \mathsf{1FE.S}(1^\lambda)$, $b \leftarrow \{0,1\}$, $K_1^{\mathsf{msk}}, \ldots, K_T^{\mathsf{msk}}, K_1^{\mathsf{key}}, \ldots, K_T^{\mathsf{key}}, K_1^{\mathsf{enc}}, \ldots, K_T^{\mathsf{enc}} \leftarrow \mathsf{PRF.Gen}(1^\lambda)$, $s_1, \ldots, s_T \leftarrow \{0,1\}^\lambda$ and $t_1, \ldots, t_T \leftarrow \{0,1\}^\lambda$, where T is upper bounded by the running time of $\mathcal{A}$. Then, $\mathcal{B}_1$ computes $\mathsf{msk}_{s_j, t_k} = \mathsf{1FE.S}(1^\lambda; \mathsf{PRF.Eval}(K_j^{\mathsf{msk}}, t_k))$.

The adversary $\mathcal{B}_1$ proceeds as follows: For $i \leq j-1$ it requests the encryption of the pair $((K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}, s_i, T), (K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}, s_i, T))$ with respect to index $\mathsf{i} = 1$. For $i = j$ it requests the encryption of the pair $((K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}, s_i, k), (K_i^{\mathsf{msk}}|_{\{t_k\}}, K_i^{\mathsf{key}}|_{\{t_k\}}, s_i, k))$, where $K_i^{\mathsf{msk}}|_{\{t_k\}}$ and $K_i^{\mathsf{key}}|_{\{t_k\}}$ are the keys K_i^{msk} and K_i^{key} punctured at the point t_k. For $i \geq j+1$ it requests the encryption of the pair $((K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}, s_i, 0), (K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}, s_i, 0))$ with respect to index $\mathsf{i} = 1$. All the above results with $\mathsf{ct}_{1,1}, \ldots, \mathsf{ct}_{1,T}$. Then, the adversary $\mathcal{B}_1$ requests the encryption of the pair $((i, t_i), (i, t_i))$ with respect to index $\mathsf{i} = 2$ for $i \in [T]$ to get $\mathsf{ct}_{2,1}, \ldots, \mathsf{ct}_{2,T}$. Finally, $\mathcal{B}_1$ outputs the state information state which is all its memory.

Next, $\mathcal{B}_2$ emulates the execution of $\mathcal{A}$ on input 1^λ by simulating the encryption oracle as follows: When $\mathcal{A}$ queries the encryption oracle with $(x^0, x^1) \in \mathcal{X}_\lambda$ (with respect to index $\mathsf{i} = 1$) for the i^{th} time for $i \leq j-1$, $\mathcal{B}_2$ runs the key-generation procedure $\mathsf{1FE.KG}(\mathsf{msk}_1, \cdot)$ with the pair $\mathsf{AGG}_{x^b, x^1, T, s_i, K_i^{\mathsf{msk}}, K_i^{\mathsf{enc}}, \perp, \perp}$ to get $\mathsf{sk}_{1,i}$ and returns the pair $(\mathsf{ct}_{1,i}, \mathsf{sk}_{1,i})$ to $\mathcal{A}$. When $\mathcal{A}$ queries the encryption oracle with $(x^0, x^1) \in \mathcal{X}_\lambda$ (with respect to index $\mathsf{i} = 1$) for the i^{th} time for $i = j$, $\mathcal{B}_2$, runs the key-generation procedure $\mathsf{1FE.KG}(\mathsf{msk}_1, \cdot)$ with the input $\mathsf{AGG}_{x^b, x^1, k, s_j, K_j^{\mathsf{msk}}|_{\{t_k\}}, K_j^{\mathsf{enc}}|_{\{t_k\}}, t_k, \gamma})$, where $\gamma = \mathsf{1FE.E}(\mathsf{msk}_{s_j, t_k}, (x_j^b, y_k^b); \mathsf{PRF.Eval}(K_i^{\mathsf{enc}}, t_k))$, to get $\mathsf{sk}_{1,i}$ and returns the pair $(\mathsf{ct}_{1,i}, \mathsf{sk}_{1,i})$ to $\mathcal{A}$. When $\mathcal{A}$ queries the encryption oracle with $(x^0, x^1) \in \mathcal{X}_\lambda$ (with respect to index $\mathsf{i} = 1$) for the i^{th} time for $i \leq j-1$, $\mathcal{B}_2$ runs the key-generation procedure $\mathsf{1FE.KG}(\mathsf{msk}_1, \cdot)$ with the pair $\mathsf{AGG}_{x^b, x^1, 0, s_i, K_i^{\mathsf{msk}}, K_i^{\mathsf{enc}}, \perp, \perp}$ to get $\mathsf{sk}_{1,i}$ and returns the pair $(\mathsf{ct}_{1,i}, \mathsf{sk}_{1,i})$ to $\mathcal{A}$. When $\mathcal{A}$ requests the i^{th} encryption of $(y^0, y^1) \in \mathcal{Y}_\lambda$ (with respect to index $\mathsf{i} = 2$), $\mathcal{B}_2$ runs the encryption procedure $\mathsf{1FE.E}(\mathsf{msk}_1, \cdot)$ with the input $(y^b, y^1, i, t_i, \perp, \perp))$ to get $\mathsf{ct}_{3,i}$ and returns the pair $(\mathsf{ct}_{2,i}, \mathsf{ct}_{3,i})$ to $\mathcal{A}$. When $\mathcal{A}$ requests a functional key for $(f^0, f^1) \in \mathcal{F} \times \mathcal{F}$, $\mathcal{B}_2$ queries the key-generation oracle $\mathsf{KG}(\mathsf{msk}_2, \cdot, \cdot)$ with the pair $(D_{f^b, f^1, i, \perp, \perp, \perp}, D_{f^b, f^1, i, s_j, t_k, \delta})$, where $\delta = \mathsf{1FE.KG}(\mathsf{msk}_{s_j, t_k}, C_{f_i^b}; \mathsf{PRF.Eval}(K_j^{\mathsf{key}}, t_k))$ and returns the output to $\mathcal{A}$.

Note that when $\sigma = 0$ then $\mathcal{A}$'s view is identical to its view in the experiment $\mathcal{H}^{(4,j,k)}$, and when $\sigma = 1$ then $\mathcal{A}$'s view is identical to its view in the modified experiment $\mathcal{H}^{(5,j,k)}$ described above. Therefore,

$$\left| \Pr\left[\mathcal{H}^{(4,j,k)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(5,j,k)}(\lambda) = 1\right] \right| \leq \mathsf{Adv}^{\mathsf{sel2FE}}_{\mathsf{2FE^{sel}}, \mathcal{F}', \mathcal{B}^{(4,j,k)\to(5,j,k)}}(\lambda).$$

■

Proof of Claim 4.6. The proof of this claim proceeds by three hybrid experiments, which we denote by $\mathcal{H}^{(5.1,j,k)}$,$\mathcal{H}^{(5.2,j,k)}$ and $\mathcal{H}^{(5.3,j,k)} = \mathcal{H}^{(6,j,k)}$, such that in each we replace only one PRF evaluation with sampling a string uniformly at random. Experiment $\mathcal{H}^{(5.1,j,k)}$ corresponds to replacing $\mathsf{PRF.Eval}(K_j^{\mathsf{msk}}, t_k)$ with a uniform string, experiment $\mathcal{H}^{(5.2,j,k)}$ corresponds to replacing $\mathsf{PRF.Eval}(K_j^{\mathsf{msk}}, t_k)$ and $\mathsf{PRF.Eval}(K_j^{\mathsf{enc}}, t_k))$, and finally experiment $\mathcal{H}^{(5.3,j,k)}$ corresponds to $\mathcal{H}^{(6,j,k)}$. Since the three proofs of indistinguishability are very similar, we provide the proof for the first one and omit the missing details. That is, in what follows we prove that the experiment $\mathcal{H}^{(5,j,k)}$ is indistinguishable from an experiment $\mathcal{H}^{(5.1,j,k)}$ in which we only replace the value of msk_{s_j,t_k} to be computed using a uniform random string rather than as $\mathsf{PRF.Eval}(K_j^{\mathsf{msk}}, t_k)$.

The adversary $\mathcal{B}^{(5,j,k)\to(5.1,j,k)} = \mathcal{B}$ given input 1^λ is defined as follows. First, $\mathcal{B}$ samples $\mathsf{msk}_1 \leftarrow \mathsf{1FE.S}(1^\lambda), \mathsf{msk}_2 \leftarrow \mathsf{2FE^{sel}.S}(1^\lambda)$, $b \leftarrow \{0,1\}$ and $s_j, t_k \leftarrow \{0,1\}^\lambda$. Now, $\mathcal{B}$ is given $R(t_k)$, a punctures PRF key $K_j^{\mathsf{msk}}|_{\{t_k\}}$ and its goal is to guess if $R(t_k)$ is uniformly random or the output of a PRF.

$\mathcal{B}$ emulates the execution of $\mathcal{A}$ on input 1^λ by simulating the encryption oracle as follows: When $\mathcal{A}_1$ requests for the encryption of the i^{th} input pair $(x^0, x^1) \in \mathcal{X}_\lambda$ (with respect to index $\mathsf{i} = 1$) for $i \leq j-1$, $\mathcal{B}$ samples $K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}, K_i^{\mathsf{enc}} \leftarrow \mathsf{PRF.Gen}(1^\lambda,\ s_i \leftarrow \{0,1\}^\lambda$, executes the procedure $\mathsf{2FE^{sel}.E}(\mathsf{msk}_2, (K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}, s_i, T), 1)$ to get $\mathsf{ct}_{1,i}$ and the procedure $\mathsf{1FE.KG}(\mathsf{msk}_1, \cdot)$ with the input $\mathsf{AGG}_{x^b,x^1,T,s_i,K_i^{\mathsf{msk}},K_i^{\mathsf{enc}},\perp,\perp}$ to get $\mathsf{sk}_{1,i}$, and returns to $\mathcal{A}$ the pair $(\mathsf{ct}_{1,i}, \mathsf{sk}_{1,i})$. When $\mathcal{A}_1$ requests for the encryption of the i^{th} input pair $(x^0, x^1) \in \mathcal{X}_\lambda$ (with respect to index $\mathsf{i} = 1$) for $i = j$, $\mathcal{B}$ samples $K_i^{\mathsf{key}}, K_i^{\mathsf{enc}} \leftarrow \mathsf{PRF.Gen}(1^\lambda,$, punctures K_i^{enc} and K_i^{key} at the point t_k to get $K_i^{\mathsf{enc}}|_{\{t_k\}}$ and $K_i^{\mathsf{key}}|_{\{t_k\}}$, respectively, executes the procedure $\mathsf{2FE^{sel}.E}(\mathsf{msk}_2, (K_i^{\mathsf{msk}}|_{\{t_k\}}, K_i^{\mathsf{key}}|_{\{t_k\}}, s_i, k), 1)$ to get $\mathsf{ct}_{1,i}$ and the procedure $\mathsf{1FE.KG}(\mathsf{msk}_1, \mathsf{AGG}_{x^b,x^1,k,s_i,K_i^{\mathsf{msk}}|_{\{t_k\}},K_i^{\mathsf{enc}}|_{\{t_k\}},t_k,\gamma})$, where $\gamma = \mathsf{1FE.E}(\mathsf{msk}_{s_j,t_k},$ $(x_j^b, y_k^b); \mathsf{PRF.Eval}(K_i^{\mathsf{enc}}, t_k))$ and $\mathsf{msk}_{s_j,t_k} = \mathsf{1FE.S}(1^\lambda; R(t_k))$ to get $\mathsf{sk}_{1,i}$, and returns to $\mathcal{A}$ the pair $(\mathsf{ct}_{1,i}, \mathsf{sk}_{1,i})$. When $\mathcal{A}_1$ requests for the encryption of the i^{th} input pair $(x^0, x^1) \in \mathcal{X}_\lambda$ (with respect to index $\mathsf{i} = 1$) for $i \geq j+1$, $\mathcal{B}$ samples $K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}, K_i^{\mathsf{enc}} \leftarrow \mathsf{PRF.Gen}(1^\lambda,\ s_i \leftarrow \{0,1\}^\lambda$, executes the procedure $\mathsf{2FE^{sel}.E}(\mathsf{msk}_2, (K_i^{\mathsf{msk}}, K_i^{\mathsf{key}}, s_i, 0), 1)$ to get $\mathsf{ct}_{1,i}$ and the procedure $\mathsf{1FE.KG}(\mathsf{msk}_1, \cdot)$ with the circuit $\mathsf{AGG}_{x^b,x^1,0,s_i,K_i^{\mathsf{msk}},K_i^{\mathsf{enc}},\perp,\perp}$ to get $\mathsf{sk}_{1,i}$, and returns to $\mathcal{A}$ the pair $(\mathsf{ct}_{1,i}, \mathsf{sk}_{1,i})$. When $\mathcal{A}$ requests the i^{th} encryption of $(y^0, y^1) \in \mathcal{Y}_\lambda$ (with respect to index $\mathsf{i} = 2$), $\mathcal{B}$ samples $t_i \leftarrow \{0,1\}^\lambda$, runs the encryption procedure $\mathsf{1FE.E}(\mathsf{msk}_1, \cdot)$ with the input $(y^b, y^1, i, t_i, \perp, \perp))$ to get $\mathsf{ct}_{3,i}$ and the encryption procedure $\mathsf{2FE^{sel}.E}(\mathsf{msk}_2, (i, t_i), 2)$ to get $\mathsf{ct}_{2,i}$ and returns the pair $(\mathsf{ct}_{2,i}, \mathsf{ct}_{3,i})$ to $\mathcal{A}$. When $\mathcal{A}$ requests a functional key for $(f^0, f^1) \in \mathcal{F} \times \mathcal{F}$, $\mathcal{B}$ runs the key-generation procedure $\mathsf{2FE^{sel}.KG}(\mathsf{msk}_2, \cdot)$ with the input $D_{f^b,f^1,i,s_j,t_k,\delta}$, where $\delta = \mathsf{1FE.KG}(\mathsf{msk}_{s_j,t_k}, C_{f_i^b}; \mathsf{PRF.Eval}(K_j^{\mathsf{key}}, t_k))$ and returns the output to $\mathcal{A}$.

Note that when $\sigma = 0$ then $\mathcal{A}$'s view is identical to its view in the experiment $\mathcal{H}^{(5,j,k)}$, and when $\sigma = 1$ then $\mathcal{A}$'s view is identical to its view in the modified experiment $\mathcal{H}^{(5.1,j,k)}$ described above. The same argument applied to $\mathcal{H}^{(5.2,j,k)}$ and $\mathcal{H}^{(5.3,j,k)}$ to get

$$\left|\Pr\left[\mathcal{H}^{(5,j,k)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(6,j,k)}(\lambda) = 1\right]\right| \leq 3 \cdot \mathsf{Adv}_{\mathsf{PRF},\mathcal{B}^{(5,j,k)\to(6,j,k)}}(\lambda).$$

■

Proof of Claim 4.7. The adversary $\mathcal{B}^{(6,j,k)\to(7,j,k)} = \mathcal{B}$ given input 1^λ is defined as follows. First, $\mathcal{B}$ samples $\mathsf{msk}_2 \leftarrow \mathsf{2FE^{sel}.S}(1^\lambda), s_j, t_k \leftarrow \{0,1\}^\lambda,\ K_j^{\mathsf{msk}}, K_j^{\mathsf{key}}, K_j^{\mathsf{enc}} \leftarrow \mathsf{PRF.Gen}(1^\lambda),\ b \leftarrow \{0,1\}$ and punctures the PRF keys at t_k to get $K_j^{\mathsf{msk}}|_{\{t_k\}}, K_j^{\mathsf{key}}|_{\{t_k\}}$ and $K_j^{\mathsf{enc}}|_{\{t_k\}}$, emulates the execution of $\mathcal{A}$ on input 1^λ by simulating the encryption oracle as follows: When $\mathcal{A}$ queries the encryption oracle with $(x^0, x^1) \in \mathcal{X}_\lambda$ (with respect to index $\mathsf{i} = 1$) for the i^{th} time for $i \leq j-1$, $\mathcal{B}$ samples $s \in \{0,1\}^\lambda$, $K^{\mathsf{msk}}, K^{\mathsf{key}}, K^{\mathsf{enc}} \leftarrow \mathsf{PRF.Gen}(1^\lambda)$, queries the key-generation oracle $\mathsf{KG}_\sigma(\mathsf{msk}_1, \cdot, \cdot)$ with the pair $(\mathsf{AGG}_{x^b,x^1,T,s,K^{\mathsf{msk}},K^{\mathsf{enc}},\perp,\perp}, \mathsf{AGG}_{x^b,x^1,T,s,K^{\mathsf{msk}},K^{\mathsf{enc}},\perp,\perp})$ and returns the output to $\mathcal{A}$. Moreover, $\mathcal{B}$ runs $\mathsf{2FE}^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_2, (K^{\mathsf{msk}}, K^{\mathsf{key}}, s, T), 1)$ and returns the output to $\mathcal{A}$. When $\mathcal{A}$ queries the encryption oracle with $(x^0, x^1) \in \mathcal{X}_\lambda$ (with respect to index $\mathsf{i} = 1$) for the i^{th} time for $i = j$, $\mathcal{B}$, queries the key-generation oracle $\mathsf{KG}_\sigma(\mathsf{msk}_1, \cdot, \cdot)$ with the pair $(\mathsf{AGG}_{x^b,x^1,k,s_j,K_j^{\mathsf{msk}}|_{\{t_k\}},K_j^{\mathsf{enc}}|_{\{t_k\}},t_k,\gamma}, \mathsf{AGG}_{x^b,x^1,k,s_j,K_j^{\mathsf{msk}}|_{\{t_k\}},K_j^{\mathsf{enc}}|_{\{t_k\}},t_k,\gamma})$, where γ is the output of the encryption oracle $\mathsf{Enc}_\sigma(\mathsf{msk}_{s_j,t_k}, \cdot, \cdot)$ on the pair $((x_j^b, y_k^b), (x_j^1, y_k^1))$, and returns the output to $\mathcal{A}$. Moreover, $\mathcal{B}$ runs $\mathsf{2FE}^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_2, (K_j^{\mathsf{msk}}|_{\{t_k\}}, K_j^{\mathsf{key}}|_{\{t_k\}}, s_j, k), 1)$ and returns the output to $\mathcal{A}$. When $\mathcal{A}$ queries the encryption oracle with $(x^0, x^1) \in \mathcal{X}_\lambda$ (with respect to index $\mathsf{i} = 1$) for the i^{th} time for $i \leq j-1$, $\mathcal{B}$ samples $s \in \{0,1\}^\lambda$, $K^{\mathsf{msk}}, K^{\mathsf{key}}, K^{\mathsf{enc}} \leftarrow \mathsf{PRF.Gen}(1^\lambda)$, queries the key-generation oracle $\mathsf{KG}_\sigma(\mathsf{msk}_1, \cdot, \cdot)$ with the pair $(\mathsf{AGG}_{x^b,x^1,0,s,K^{\mathsf{msk}},K^{\mathsf{enc}},\perp,\perp}, \mathsf{AGG}_{x^b,x^1,0,s,K^{\mathsf{msk}},K^{\mathsf{enc}},\perp,\perp})$ and returns the output to $\mathcal{A}$. Moreover, $\mathcal{B}$ runs $\mathsf{2FE}^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_2, (K^{\mathsf{msk}}, K^{\mathsf{key}}, s, 0), 1)$ and returns the output to $\mathcal{A}$. When $\mathcal{A}$ requests the i^{th} encryption of $(y^0, y^1) \in \mathcal{Y}_\lambda$ (with respect to index $\mathsf{i} = 2$), $\mathcal{B}$ samples $t_i \in \{0,1\}^\lambda$ (unless $i = k$ in which case t_i is already known), runs the encryption procedure $\mathsf{1FE.E}(\mathsf{msk}_1, \cdot)$ with the input $(y^b, y^1, i, t_i, \perp, \perp)$ and returns the output to $\mathcal{A}$. Moreover, $\mathcal{B}$ runs $\mathsf{2FE}^{\mathsf{sel}}.\mathsf{E}(\mathsf{msk}_2, (i, t), 2)$ and returns the output to $\mathcal{A}$. When $\mathcal{A}$ requests a functional key for $(f^0, f^1) \in \mathcal{F} \times \mathcal{F}$, $\mathcal{B}$ runs the key-generation procedure $\mathsf{2FE}^{\mathsf{sel}}.\mathsf{KG}(\mathsf{msk}_2, D_{f^b,f^1,i,s_j,t_k,\delta})$, where δ is the output of the key-generation oracle $\mathsf{KG}_\sigma(\mathsf{msk}_{s_j,t_j}, \cdot, \cdot)$ with the pair (C_{f^b}, C_{f^1}), and returns the output to $\mathcal{A}$.

Note that when $\sigma = 0$ then $\mathcal{A}$'s view is identical to its view in the experiment $\mathcal{H}^{(6,j,k)}$, and when $\sigma = 1$ then $\mathcal{A}$'s view is identical to its view in the modified experiment $\mathcal{H}^{(7,j,k)}$ described above. Therefore,

$$\left|\Pr\left[\mathcal{H}^{(6,j,k)}(\lambda) = 1\right] - \Pr\left[\mathcal{H}^{(7,j,k)}(\lambda) = 1\right]\right| \leq \mathsf{Adv}^{\mathsf{full1FE}}_{\mathsf{1FE},\mathcal{F}',\mathcal{B}^{(6,j,k)\to(7,j,k)}}(\lambda).$$

■