From Selective to Adaptive Security in Functional Encryption

Prabhanjan Ananth[1], Zvika Brakerski[2], Gil Segev[3](✉), and Vinod Vaikuntanathan[4]

[1] University of California, Los Angeles, USA
prabhanjan@cs.ucla.edu
[2] Weizmann Institute of Science, Rehovot, Israel
zvika.brakerski@weizmann.ac.il
[3] Hebrew University of Jerusalem, Jerusalem, Israel
segev@cs.huji.ac.il
[4] Massachusetts Institute of Technology, Cambridge, USA
vinodv@mit.edu

Abstract. In a functional encryption (FE) scheme, the owner of the secret key can generate restricted decryption keys that allow users to learn specific functions of the encrypted messages and nothing else. In many known constructions of FE schemes, security is guaranteed only for messages that are fixed ahead of time (i.e., before the adversary even interacts with the system). This so-called *selective security* is too restrictive for many realistic applications. Achieving *adaptive security* (also called *full security*), where security is guaranteed even for messages that are adaptively chosen at any point in time, seems significantly more challenging. The handful of known adaptively-secure schemes are based on specifically tailored techniques that rely on strong assumptions (such as obfuscation or multilinear maps assumptions).

We show that any sufficiently-expressive *selectively-secure* FE scheme

P. Ananth–This work was done in part while visiting MIT, and was supported in part by the Northrop Grumman Cybersecurity Consortium. Research supported in part from a DARPA/ONR PROCEED award, NSF Frontier Award 1413955, NSF grants 1228984, 1136174, 1118096, and 1065276. This material is based upon work supported by the Defense Advanced Research Projects Agency through the U.S. Office of Naval Research under Contract N00014-11- 1-0389. The views expressed are those of the author and do not reflect the official policy or position of the Department of Defense, the National Science Foundation, or the U.S. Government.
Z. Brakerski–Supported by the Israel Science Foundation (Grant No. 468/14) and by the Alon Young Faculty Fellowship.
G. Segev–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).
V. Vaikuntanathan–Research supported in part by DARPA Grant number FA8750-11-2-0225, an Alfred P. Sloan Research Fellowship, the Northrop Grumman Cybersecurity Research Consortium (CRC), Microsoft Faculty Fellowship, and a Steven and Renee Finn Career Development Chair from MIT.

R. Gennaro and M. Robshaw (Eds.): CRYPTO 2015, Part II, LNCS 9216, pp. 657–677, 2015.
DOI: 10.1007/978-3-662-48000-7_32

can be transformed into an *adaptively-secure* one without introducing any additional assumptions. We present a black-box transformation, for both public-key and private-key schemes, making novel use of *hybrid encryption*, a classical technique that was originally introduced for improving the efficiency of encryption schemes. We adapt the hybrid encryption approach to the setting of functional encryption via a technique for embedding a "hidden execution thread" in the decryption keys of the underlying scheme, which will only be activated within the proof of security of the resulting scheme. As an additional application of this technique, we show how to construct functional encryption schemes for arbitrary circuits starting from ones for shallow circuits (NC1 or even TC0).

Keywords: Functional encryption · Adaptive security · Generic constructions

1 Introduction

Traditional notions of public-key encryption provide all-or-nothing access to data: owners of the secret key can recover the entire message from a ciphertext, whereas those who do not know the secret key learn nothing at all. Functional encryption, a revolutionary notion originating from the work of Sahai and Waters [SW05], is a modern type of encryption scheme where the owner of the (master) secret key can release function-specific secret keys sk_f, referred to as *functional keys*, which enable a user holding an encryption of a message x to compute $f(x)$ but nothing else (see [KSW08,LOS+10,BSW11,O'N10] and many others). Intuitively, in terms of indistinguishability-based security, encryptions of any two messages, x_0 and x_1, should be computationally indistinguishable given access to functional keys for any function f such that $f(x_0) = f(x_1)$.

While initial constructions of functional encryption schemes [BF03,BCO+04, KSW08,LOS+10] were limited to restricted function classes such as point functions and inner products, recent developments have dramatically improved the state of the art. In particular, the works of Sahai and Seyalioglu [SS10] and Gorbunov, Vaikuntanathan and Wee [GVW12] showed that a scheme supporting a single functional key can be based on any semantically-secure encryption scheme. This result can be extended to the case where the number of functional keys is polynomial and known a-priori [GVW12]. Goldwasser, Kalai, Popa, Vaikuntanathan and Zeldovich [GKP+13] constructed a scheme with succinct ciphertexts based on a specific hardness assumption (Learning with Errors).

The first functional encryption scheme that supports a-priori unbounded number of functional keys was constructed by Garg, Gentry, Halevi, Raykova, Sahai and Waters [GGH+13], based on the existence of a general-purpose indistinguishability obfuscator (for which a heuristic construction is presented in the same paper). Garg et al. showed that given any such obfuscator, their functional encryption scheme is *selectively secure*. At a high level, selective security guarantees security only for messages that are fixed ahead of time (i.e., before the adversary even interacts with the system). Whereas security only for such messages may be justified in some cases, it is typically too restrictive for realistic applications. A more realistic notion is that of *adaptive security* (often called *full security*), which guarantees security even for messages that can be adaptively chosen at any point in time.

Historically, the first functional encryption schemes were only proven selectively secure [BB04, GPS+06, KSW08, GVW13, GKP+13]. The problem of constructing adaptively secure schemes seems significantly more challenging and only few approaches are known. A simple observation is that if a selectively-secure scheme's message space is not too large, e.g., $\{0,1\}^n$ for a relatively small n, then any adaptively-chosen message x can be guessed ahead of time with probability 2^{-n}. Starting with a *sub-exponential* hardness assumption, and taking the security parameter to be polynomial in n allows us to argue that the selectively-secure scheme is in fact also adaptively secure. This observation is known as "complexity leveraging" and is clearly not satisfactory in general.

The powerful "dual system" approach, put forward by Waters [Wat09], has been used to construct adaptively-secure attribute-based encryption scheme (a restricted notion of functional encryption) for formulas, as well as an adaptively-secure functional encryption scheme for linear functions [LOS+10]. However, this method is a general outline, and each construction was so far required to tailor the solution based on its specialized assumption. In some cases, such as attribute-based encryption for circuits, it is still not known how to implement dual system encryption to achieve adaptive security (although Garg, Gentry, Halevi and Zhandry [GGH+14a] show how to do this with custom-built methods and hardness assumptions).

Starting with [GGH+13], there has been significant effort in the research community to construct an adaptively-secure general-purpose functional encryption scheme with an unbounded number of functional keys. Boyle, Chung and Pass [BCP14] constructed an adaptively secure scheme, under the assumption that differing-input obfuscators exist (these are stronger primitives than the indistinguishability obfuscators used by [GGH+13]). Following their work, Waters [Wat14] and Garg, Gentry, Halevi and Zhandry [GGH+14b] constructed specific adaptively-secure schemes assuming indistinguishability obfuscation and assuming non-standard assumptions on multilinear maps, respectively. Despite this significant progress, each of these constructions relies on somewhat tailored methods and techniques.

1.1 Our Results: From Selective to Adaptive Security

We show that any selectively-secure functional encryption scheme implies an adaptively-secure one, without relying on any additional assumptions. Our transformation applies equally to public-key schemes and to private-key ones, where the resulting adaptive scheme inherits the public-key or private-key flavor of the underlying scheme. The following theorem informally summarizes our main contribution.

Theorem 1.1 (Informal). *Given any public-key (resp. private-key) selectively-secure functional encryption scheme for the class of all polynomial size circuits, there exists an adaptively-secure public-key (resp. private-key) functional encryption scheme with similar properties.*

Specifically, the adaptive scheme supports slightly smaller circuits than those supported by the selective scheme we started with.

Our transformation can be applied, in particular, to the selectively-secure schemes of Garg et al. [GGH+13] and Waters [Wat14], resulting in adaptively-secure schemes based on indistinguishability obfuscation (and one-way functions).[1]

We view the significance of our result in a number of dimensions. First of all, it answers the basic call of cryptographic research to substantiate the existence of rather complex primitives on that of somewhat simpler ones. We feel that this is of special interest in the case of adaptive security, where it seemed that ad-hoc methods were required. Secondly, our construction, being of fairly low overhead, will allow to focus the attention of the research community in studying selectively-secure functional encryption schemes, rather than investing unwarranted efforts in obtaining adaptively-secure ones. Lastly, we hope that our methods will be extended towards weaker forms of functional encryption schemes for which adaptive security is yet unattained generically, such as attribute-based encryption for all polynomial-size circuits.

1.2 Our Techniques

Our result is achieved by incorporating a number of techniques which will be explained in this section. In a nutshell, our main observation is that *hybrid encryption* (a.k.a key encapsulation) can be employed in the context of functional encryption, and has great potential in going from selective to adaptive security of encryption schemes. At a first glance, *hybrid functional encryption* should lead to a selective-to-adaptive transformation, given an additional weak component: A *symmetric* FE which is adaptively secure when only a single message query is allowed. We show that the latter can be constructed from any one-way function as a corollary of [GVW12,BS15]. However, the intuitive reasoning fails to translate into a proof of security. To resolve this issue, we use a technique we call *The Trojan Method*, which originates from De Caro et al.'s "trapdoor circuits" [CIJ+13] (similar ideas had been since used by Gentry et al. [GHR+14] and Brakerski and Segev [BS15]).

We conclude this section with a short comparison of our technique with the aforementioned "dual system encryption" technique that had been used to achieve adaptively secure attribute based encryption.

Hybrid Functional Encryption. Hybrid encryption is a veteran technique in cryptography and has been used in a variety of settings. We show that in the context of functional encryption it is especially powerful.

[1] Waters [Wat14] also constructed an adaptively-secure scheme, but using specific ad-hoc techniques and in a significantly more complicated manner.

The idea in hybrid encryption is to combine two encryption schemes: An "external" scheme (sometimes called KEM – Key Encapsulation Mechanism) and an "internal" scheme (sometimes called DEM – Data Encapsulation Mechanism). In order to encrypt a message in the hybrid scheme, a fresh key is generated for the internal scheme, and is used to encrypt the message. Then the key itself is encrypted using the external scheme. The final hybrid ciphertext contains the two ciphertexts: $(\mathsf{Enc}_{\mathsf{ext}}(k), \mathsf{Enc}_{\mathsf{int},k}(m))$ (all external ciphertexts use the same key). To decrypt, one first decrypts the external ciphertext, retrieves k and applies it to the internal ciphertext. Note that if, for example, the external scheme is public-key and the internal is symmetric key, then the resulting scheme will also be public key. Hybrid encryption is often used in cases where the external scheme is less efficient (e.g. in encrypting long messages) and thus there is an advantage in using it to encrypt only a short key, and encrypt the long message using the more efficient internal scheme. Lastly, note that the internal scheme only needs to be able to securely encrypt a single message.

The intuition as to why hybrid encryption may be good for achieving adaptive security is that the external scheme only encrypts keys for the internal scheme. Namely, it only encrypts messages from a predetermined and known distribution, so selective security should be enough for the external scheme. The hardness of adaptive security is "pushed" to the internal scheme, but there the task is easier since the internal scheme only needs to be able to encrypt a single message, and it can be private-key rather than public-key.

Let us see how to employ this idea in the case where both the internal and external schemes are FE schemes. To encrypt, we will generate a fresh master secret key for the internal scheme, and encrypt it under the external scheme. To generate a key for the function f, the idea is to generate a key for the function $G_f(\mathsf{msk}_{\mathsf{int}})$ which takes a master key for the internal scheme, and outputs a secret key for function f under the internal scheme, using $\mathsf{msk}_{\mathsf{int}}$ (randomness is handled using a PRF). This will allow to decrypt in a two-step process as above. First apply the external secret-key for G_f to the external ciphertext, this will give you an internal secret key for f, which is in turn applied to the internal ciphertext to produce $f(x)$.

For the external scheme, we will use a selectively secure FE scheme (for the sake of concreteness, let us say public-key FE). As explained above, selective security is sufficient here since all the messages encrypted using the external scheme can be generated ahead of time (i.e. they do not depend on the actual x's that the user wishes to encrypt).

For the internal scheme, we require an FE scheme that is *adaptively secure*, but only supports the encryption of a single message. Fortunately, such a primitive can be derived from the works of [GVW12,BS15]. In [GVW12], the authors present an adaptively secure one-time bounded FE scheme. This scheme allows to only generate a key for one function, and to encrypt as many messages as the user wishes. This construction is based on the existence of semantically secure encryption, so the public-key version needs public-key encryption and the symmetric version needs symmetric encryption. While this primitive seems dual to what we need for our purposes, [BS15] shows how to transform private-key FE schemes into *function private* FE. In function-private FE, messages and functions enjoy the same level of privacy, in the sense that a user that produces x_0, x_1, f_0, f_1 such that $f_0(x_0) = f_1(x_1)$ cannot distinguish between $(\mathsf{Enc}(x_0), \mathsf{sk}_{f_0})$ and $(\mathsf{Enc}(x_1), \mathsf{sk}_{f_1})$. Therefore, after applying the [BS15] transformation, we can switch the roles of the functions and messages, and obtain a symmetric FE scheme which is adaptively secure for a *single message and many functions*. (We note that the symmetric version of the [GVW12] scheme can be shown to be function private even without the [BS15] transformation, however since this claim is not made explicitly in the paper we choose not to rely on it.)

Whereas intuitively this should solve the problem, it is not clear how to prove security of the new construction. Standard security proofs for hybrid encryption follow by first relying on the security of the external scheme and removing the encapsulated key, and then relying on the security of the internal scheme and removing the message. However, in our case, removing the encapsulated key is easily distinguishable, since the adversary is allowed to obtain functional keys and apply them to the ciphertext (so long as $f(x_0) = f(x_1)$). Without the internal key, the decryption process no longer works. To resolve this difficulty, we use the Trojan method.

Before we describe the Trojan method, we pause to note that our idea so far can be thought of as "boosting" a single-message, many-key, adaptive symmetric-key FE into a many-message, many-key, adaptive public-key FE (using a selective public-key FE as a "catalyst"). The recent work of Waters [Wat14] proceeds along a similar train of thought, and indeed, motivated our approach. However, while our transformation is simple and general, Waters has to rely on a powerful catalyst, namely an indistinguishability obfuscator.

The Trojan Method. The Trojan Method, which is a generalization of techniques used in [CIJ+13] and later in [GHR+14,BS15], is a way to embed a hidden functionality thread in an FE secret-key that can only be invoked by special ciphertexts generated using special (secret) back-door information. This thread remains completely unused in the normal operation of the scheme (and can be instantiated with meaningless functionality). In the proof, however, the secret thread will be activated by the challenge ciphertext in such a way that is indistinguishable to the user (= attacker). Namely, the user will not be able to tell that it is executing the secret thread and not the main thread. This will be extremely beneficial to prove security. We wish to argue that in the view of the user, the execution of the main thread does not allow to distinguish between the encryption of two messages x_0, x_1. The problem is that for functionality purposes, the main thread has to know which input it is working on. This is where the hidden thread comes into the play. We will design the hidden thread so that in the eyes of the user, it is computationally indistinguishable from the main thread on the special messages x_0, x_1. However, in the hidden thread, the output can be computed in a way that does not distinguish between x_0 and x_1 (either by a statistical or a computational argument), which will allow us to conclude that encryptions of x_0, x_1 are indistinguishable.

In particular, this method will resolve the aforementioned conundrum in our proof outline above. In the proof, we will use the Trojan method to embed a hidden thread in which $\mathsf{msk}_{\mathsf{int}}$ is not used at all, but rather G_f produces a precomputed internal sk_f. This will allow us to remove $\mathsf{msk}_{\mathsf{int}}$ from the challenge ciphertext and use the security properties of the internal scheme to argue that a internal encryption of x_0, x_1 are identical so long as $f(x_0) = f(x_1)$.

We note that an important special case of the above outline is when the trojan thread is a constant function. This had been the case in [CIJ+13, GHR+14], and this is the case in this work as well. However, we emphasize that our description here allows for greater generality since we allow the trojan thread to implement functionality that depends on the input x. We feel that this additional power may be useful for future applications.

Technically, the hidden thread is implemented using (standard) symmetric-key encryption, which in turn can be constructed starting with any one-way function. In the functional secret-key generation process for a function f, the secret-key generation process will produce a symmetric-key ciphertext c (which can just be encryption of 0 or another fixed message, since it only needs to have meaningful content in the security proof). It will then consider the function $G_{f,c}$ that takes as input a pair (x, s), and first checks whether it can decrypt c using s as a symmetric key. If it cannot, then it just runs f on x and returns the output. If s actually decrypts c, we consider $f^* = \mathsf{Dec}_s(c)$ (i.e. c encrypts a description of a function), and the output is the execution of $f^*(x)$. The value c is therefore used as a Trojan Horse: Its contents are hidden from the users of the scheme, however given a hidden command (in the form of the symmetric s) it can embed functionality that "takes over" the functional secret-key.

We note that in order to support the Trojan method, the decryption keys of our FE scheme need to perform symmetric decryption, branch operations, and execution of the function f^*. Thus we need to start with an FE scheme which allows for the generation of sufficiently expressive keys.

Our Trojan method can be seen as a weak form of function privacy in FE, but one that can be applied even in the context of public-key FE. In essence, we cannot hide the main thread of the evaluated function (this is unavoidable in public-key FE). However, we can hide the secret thread and thus allow the function to operate in a designated way for specially generated ciphertexts. (This interpretation is not valid for previous variants of this method such as "trapdoor circuits" [CIJ+13].)

A simple application of the Trojan method is our reduction in Sect. 4, showing that FE that only supports secret-keys for functions with shallow circuits (e.g. logarithmic depth) implies a scheme that works for circuits of arbitrary depth (although with a size bound). Essentially, instead of producing a secret key for the desired functionality, we output a key for the function that computes a *randomized encoding* of that functionality. A *(computational) randomized encoding* [IK00, AIK05] of an input-function pair $\mathsf{RE}(f, x)$ is, in a nutshell, a representation of $f(x)$ that reveals no information except $f(x)$ on one hand, but can be computed with less resources on the other (in our case, lower depth).

To make the proof work, the Trojan thread will contain a precomputed $\mathsf{RE}(f, x_0)$ value, which will allow us to use the security property of the encoding scheme and switch it to $\mathsf{RE}(f, x_1)$. See Sect. 4 for details. We note that a similar approach is used in [GHR+14] to achieve FE that works for RAM machines.

Relation to Dual-System Encryption. Our approach takes some resemblance to the "Dual-System Encryption" method of Waters [Wat09] and followup works [LW10,LW12]. This method had been used to prove adaptive security for Identity Based Encryption and Attribute Based Encryption, based on the hardness of some problems on groups with bilinear-maps. In broad terms, in their proof the distribution of the ciphertext is changed into "semi-functional" mode in a way that is indiscoverable by an observer. A semi-functional ciphertext is still decryptable by normal secret keys. Then, the secret-keys are modified into semi-functional form, which is useless in decrypting semi-functional ciphertexts. This is useful since in IBE and ABE, the challenge ciphertext is not supposed to be decryptable by those keys given to the adversary. Still, a host of algebraic techniques are used to justify the adversary's inability to produce other semi-functional ciphertexts in addition to the challenge, which would foil the reduction.

Our proof technique also requires changing the distributions of the keys and challenge ciphertext. However, there are also major differences. Our modified ciphertext is not allowed to interact with properly generated secret keys, and therefore the distinction between "normal" and "semi-functional" does not fit here. Furthermore, in Identity Based and Attribute Based Encryption, the attacker in the security game is not allowed to receive keys that reveal any information on the message, which allows to generate semi-functional ciphertexts that do not contain any information, whereas in our case, there is a structured and well-defined output for any ciphertext and any key. This means that the information required for decryption (which can be a-priori unbounded) needs to be embedded in the keys. Lastly, our proof is completely generic and does not rely on the algebraic structure of the underlying hardness assumption as in previous implementations of this method.

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 $f(x)$. A function $\mathsf{negl} : \mathbb{N} \to \mathbb{R}$ is *negligible* if for any polynomial $p(\lambda)$ it holds that $\mathsf{negl}(\lambda) < 1/p(\lambda)$ for all sufficiently large $\lambda \in \mathbb{N}$.

2.1 Pseudorandom Functions and Symmetric Encryption

Pseudorandom Functions. We rely on the following standard notion of a pseudorandom function family [GGM86], asking that a pseudorandom function be computationally indistinguishable from a truly random function via oracle access.

Definition 2.1. *A family* $\mathcal{F} = \left\{\mathsf{PRF_K} : \{0,1\}^n \to \{0,1\}^m : \mathsf{K} \in \mathcal{K}\right\}$ *of efficiently-computable functions is* pseudorandom *if for every PPT adversary* $\mathcal{A}$ *there exists a negligible function* $\mathsf{negl}(\cdot)$ *such that*

$$\left| \Pr_{\mathsf{K} \leftarrow \mathcal{K}} \left[\mathcal{A}^{\mathsf{PRF_K}(\cdot)}(1^\lambda) = 1\right] - \Pr_{\mathsf{R} \leftarrow \mathcal{U}} \left[\mathcal{A}^{\mathsf{R}(\cdot)}(1^\lambda) = 1\right] \right| \leq \mathsf{negl}(\lambda),$$

for all sufficiently large $\lambda \in \mathbb{N}$*, where* $\mathcal{U}$ *is the set of all functions from* $\{0,1\}^n$ *to* $\{0,1\}^m$*.*

We say that a pseudorandom function family $\mathcal{F}$ is implementable in NC^1 if every function in $\mathcal{F}$ can be implemented by a circuit of depth $c \cdot \log(n)$, for some constant c. We also consider the notion of a *weak* pseudorandom function family, asking that the above definition holds for adversaries that may access the functions on random inputs (that is, the oracles $\mathsf{PRF_K}(\cdot)$ and $\mathsf{R}(\cdot)$ take no input, and on each query they sample a uniform input r and output $\mathsf{PRF_K}(r)$ and $\mathsf{R}(r)$, respectively).

Symmetric Encryption with Pseudorandom Ciphertexts. A symmetric encryption scheme consists of a tuple of PPT algorithms $(\mathsf{Sym.Setup}, \mathsf{Sym.Enc}, \mathsf{Sym.Dec})$. The algorithm $\mathsf{Sym.Setup}$ takes as input a security parameter λ in unary and outputs a key K_E. The encryption algorithm $\mathsf{Sym.Enc}$ takes as input a symmetric key K_E and a message m and outputs a ciphertext CT. The decryption algorithm $\mathsf{Sym.Dec}$ takes as input a symmetric key K_E and a ciphertext CT and outputs the message m.

In this work, we require a symmetric encryption scheme Π where the ciphertexts produced by $\mathsf{Sym.Enc}$ are pseudorandom strings. Let $\mathsf{OEnc}_K(\cdot)$ denote the (randomized) oracle that takes as input a message m, chooses a random string r and outputs $\mathsf{Sym.Enc}(\mathsf{Sym.K}, m; r)$. Let $R_{\ell(\lambda)}(\cdot)$ denote the (randomized) oracle that takes as input a message m and outputs a uniformly random string of length $\ell(\lambda)$ where $\ell(\lambda)$ is the length of the ciphertexts. More formally, we require that for every PPT adversary $\mathcal{A}$ the following advantage is negligible in λ:

$$\mathsf{Adv}^{\mathsf{symPR}}_{\Pi,\mathcal{A}}(\lambda) = \left| \mathsf{Pr}\left[\mathcal{A}^{\mathsf{OEnc}_{\mathsf{Sym.K}}(\cdot)}(1^\lambda) = 1\ \right] - \mathsf{Pr}\left[\mathcal{A}^{\mathsf{R}_{\ell(\lambda)}(\cdot)}(1^\lambda) = 1\ \right] \right|$$

where the probability is taken over the choice of $\mathsf{Sym.K} \leftarrow \mathsf{Sym.Setup}(1^\lambda)$, and over the internal randomness of $\mathcal{A}$, OEnc and $\mathsf{R}_{\ell(\lambda)}$.

We note that such a symmetric encryption scheme with pseudorandom ciphertexts can be constructed from one-way functions, e.g. using weak pseudorandom functions by defining $\mathsf{Sym.Enc}(\mathsf{K}, m; r) = (r, \mathsf{PRF_K}(r) \oplus m)$ (see [Gol04] for more details).

2.2 Public-Key Functional Encryption

A public-key functional encryption (FE) scheme Π_{Pub} over a message space $\mathcal{M} = \{\mathcal{M}_\lambda\}_{\lambda \in \mathbb{N}}$ and a function space $\mathcal{F} = \{\mathcal{F}_\lambda\}_{\lambda \in \mathbb{N}}$ is a tuple $(\mathsf{Pub.Setup}, \mathsf{Pub.KeyGen}, \mathsf{Pub.Enc}, \mathsf{Pub.Dec})$ of PPT algorithms with the following properties:

– $\mathsf{Pub.Setup}(1^\lambda)$: The setup algorithm takes as input the unary representation of the security parameter, and outputs a public key MPK and a secret key MSK.
– $\mathsf{Pub.KeyGen}(\mathsf{MSK}, f)$: The key-generation algorithm takes as input a secret key MSK and a function $f \in \mathcal{F}_\lambda$, and outputs a functional key sk_f.
– $\mathsf{Pub.Enc}(\mathsf{MPK}, m)$: The encryption algorithm takes as input a public key MPK and a message $m \in \mathcal{M}_\lambda$, and outputs a ciphertext CT.
– $\mathsf{Pub.Dec}(sk_f, \mathsf{CT})$: The decryption algorithm takes as input a functional key sk_f and a ciphertext CT, and outputs $m' \in \mathcal{M}_\lambda \cup \{\perp\}$.

We say that such a scheme is defined for a complexity class $\mathcal{C}$ if it supports all the functions that can be implemented in $\mathcal{C}$. In terms of correctness, we require that there exists a negligible function $\mathsf{negl}(\cdot)$ such that for all sufficiently large $\lambda \in \mathbb{N}$, for every message $m \in \mathcal{M}_\lambda$, and for every function $f \in \mathcal{F}_\lambda$ it holds that $\Pr[\mathsf{Pub.Dec}(\mathsf{Pub.KeyGen}(\mathsf{MSK}, f), \mathsf{Pub.Enc}(\mathsf{MPK}, m)) = f(m)] \geq 1 - \mathsf{negl}(\lambda)$, where $(\mathsf{MPK}, \mathsf{MSK}) \leftarrow \mathsf{Pub.Setup}(1^\lambda)$, and the probability is taken over the random choices of all algorithms.

We consider the standard selective and adaptive indistinguishability-based notions for functional encryption (see, for example, [BSW11, O'N10]). Intuitively, these notions ask that encryptions of any two messages, m_0 and m_1, should be computationally indistinguishable given access to functional keys for any function f such that $f(m_0) = f(m_1)$. In the case of selective security, adversaries are required to specify the two messages in advance (i.e., before interacting with the system). In the case of adaptive security, adversaries are allowed to specify the two messages even after obtaining the public key and functional keys.[2]

Definition 2.2. (Selective Security). *A public-key functional encryption scheme* $\Pi = (\mathsf{Sel.Setup}, \mathsf{Sel.KeyGen}, \mathsf{Sel.Enc}, \mathsf{Sel.Dec})$ *over a function space* $\mathcal{F} = \{\mathcal{F}_\lambda\}_{\lambda \in \mathbb{N}}$ *and a message space* $\mathcal{M} = \{\mathcal{M}_\lambda\}_{\lambda \in \mathbb{N}}$ *is* selectively secure *if for any PPT adversary* $\mathcal{A}$ *there exists a negligible function* $\mathsf{negl}(\cdot)$ *such that*

$$\mathsf{Adv}^{\mathsf{Sel}}_{\Pi,\mathcal{A}}(\lambda) = \left| \Pr[\mathsf{Expt}^{\mathsf{Sel}}_{\Pi,\mathcal{A}}(\lambda, 0) = 1] - \Pr[\mathsf{Expt}^{\mathsf{Sel}}_{\Pi,\mathcal{A}}(\lambda, 1) = 1] \right| \leq \mathsf{negl}(\lambda)$$

for all sufficiently large $\lambda \in \mathbb{N}$*, where for each* $b \in \{0,1\}$ *and* $\lambda \in \mathbb{N}$ *the experiment* $\mathsf{Expt}^{\mathsf{Sel}}_{\Pi,\mathcal{A}}(\lambda, b)$*, modeled as a game between the adversary* $\mathcal{A}$ *and a challenger, is defined as follows:*

1. **Setup phase:** *The challenger samples* $(\mathsf{Sel.MPK}, \mathsf{Sel.MSK}) \leftarrow \mathsf{Sel.Setup}(1^\lambda)$.

[2] Our notions of security consider a single challenge, and in the public-key setting these are known to be equivalent to their multi-challenge variants via a standard hybrid argument.

2. **Challenge phase:** *On input* 1^λ *the adversary submits* (m_0, m_1)*, and the challenger replies with* $\mathsf{Sel.MPK}$ *and* $\mathsf{CT} \leftarrow \mathsf{Sel.Enc}(\mathsf{Sel.MPK}, m_b)$*.*
3. **Query phase:** *The adversary adaptively queries the challenger with any function* $f \in \mathcal{F}_\lambda$ *such that* $f(m_0) = f(m_1)$*. For each such query, the challenger replies with* $\mathsf{Sel}.sk_f \leftarrow \mathsf{Sel.KeyGen}(\mathsf{Sel.MSK}, f)$*.*
4. **Output phase:** *The adversary outputs a bit* b' *which is defined as the output of the experiment.*

Definition 2.3. (Adaptive Security). *A public-key functional encryption scheme* $\Pi = (\mathsf{Ad.Setup}, \mathsf{Ad.KeyGen}, \mathsf{Ad.Enc}, \mathsf{Ad.Dec})$ *over a function space* $\mathcal{F} = \{\mathcal{F}_\lambda\}_{\lambda \in \mathbb{N}}$ *and a message space* $\mathcal{M} = \{\mathcal{M}_\lambda\}_{\lambda \in \mathbb{N}}$ *is* adaptively secure *if for any PPT adversary* $\mathcal{A}$ *there exists a negligible function* $\mathsf{negl}(\cdot)$ *such that*

$$\mathsf{Adv}^{\mathsf{Ad}}_{\Pi,\mathcal{A}}(\lambda) = \left| \Pr[\mathsf{Expt}^{\mathsf{Ad}}_{\Pi,\mathcal{A}}(\lambda, 0) = 1] - \Pr[\mathsf{Expt}^{\mathsf{Ad}}_{\Pi,\mathcal{A}}(\lambda, 1) = 1] \right| \leq \mathsf{negl}(\lambda)$$

for all sufficiently large $\lambda \in \mathbb{N}$*, where for each* $b \in \{0,1\}$ *and* $\lambda \in \mathbb{N}$ *the experiment* $\mathsf{Expt}^{\mathsf{Ad}}_{\Pi,\mathcal{A}}(1^\lambda, b)$*, modeled as a game between the adversary* $\mathcal{A}$ *and a challenger, is defined as follows:*

1. **Setup phase:** *The challenger samples* $(\mathsf{Ad.MPK}, \mathsf{Ad.MSK}) \leftarrow \mathsf{Ad.Setup}(1^\lambda)$*, and sends* $\mathsf{Ad.MPK}$ *to the adversary.*
2. **Query phase I:** *The adversary adaptively queries the challenger with any function* $f \in \mathcal{F}_\lambda$*. For each such query, the challenger replies with* $\mathsf{Ad}.sk_f \leftarrow \mathsf{Ad.KeyGen}(\mathsf{Ad.MSK}, f)$*.*
3. **Challenge Phase***: The adversary submits* (m_0, m_1) *such that* $f(m_0) = f(m_1)$ *for all function queries* f *made so far, and the challenger replies with* $\mathsf{CT} \leftarrow \mathsf{Ad.Enc}(\mathsf{Ad.MSK}, m_b)$*.*
4. **Query phase II:** *The adversary adaptively queries the challenger with any function* $f \in \mathcal{F}_\lambda$ *such that* $f(m_0) = f(m_1)$*. For each such query, the challenger replies with* $\mathsf{Ad}.sk_f \leftarrow \mathsf{Ad.KeyGen}(\mathsf{Ad.MSK}, f)$*.*
5. **Output phase:** *The adversary outputs a bit* b' *which is defined as the output of the experiment.*

3 Our Transformation in the Public-Key Setting

In this section we present our transformation from selective security to adaptive security for public-key functional encryption schemes. In addition to any selectively-secure public-key functional encryption scheme (see Definition 2.2), our transformation requires a *private-key* functional encryption scheme that is adaptively-secure for a single message query and many function queries. Based on [GVW12,BS15], such a scheme can be based on any one-way function[3].

[3] Gorbunov et al. [GVW12] constructed a private-key functional encryption scheme that is adaptively secure for a single function query and many message queries based on any private-key encryption scheme (and thus based on any one-way function). Any such scheme can be turned into a function private one using the generic transformation of Brakerski and Segev [BS15], and then one can simply switch the roles of functions and messages [AAB+13,BS15]. This results in a private-key scheme that is adaptively secure for a single message query and many function queries.

More specifically, we rely on the following building blocks (all of which are implied by any selectively-secure public-key functional encryption scheme):

1. A selectively-secure public-key functional encryption scheme $\mathsf{Sel} = (\mathsf{Sel.Setup}, \mathsf{Sel.KeyGen}, \mathsf{Sel.Enc}, \mathsf{Sel.Dec})$.
2. An adaptively-secure single-ciphertext private-key functional encryption scheme[4] $\mathsf{OneCT} = (\mathsf{OneCT.Setup}, \mathsf{OneCT.KeyGen}, \mathsf{OneCT.Enc}, \mathsf{OneCT.Dec})$.
3. A symmetric encryption scheme with pseudorandom ciphertexts $\mathsf{SYM} = (\mathsf{Sym.Setup}, \mathsf{Sym.Enc}, \mathsf{Sym.Dec})$.
4. A pseudorandom function family $\mathcal{F}$ with a key space $\mathcal{K}$.

Our adaptively-secure scheme $\mathsf{Ad} = (\mathsf{Ad.Setup}, \mathsf{Ad.KeyGen}, \mathsf{Ad.Enc}, \mathsf{Ad.Dec})$ is defined as follows.

– **The setup algorithm:** On input 1^λ the setup algorithm $\mathsf{Ad.Setup}$ samples $(\mathsf{Sel.MPK}, \mathsf{Sel.MSK}) \leftarrow \mathsf{Sel.Setup}(1^\lambda)$, and outputs $\mathsf{Ad.MPK} = \mathsf{Sel.MPK}$ and $\mathsf{Ad.MSK} = \mathsf{Sel.MSK}$.
– **The key-generation algorithm:** On input the secret key $\mathsf{Ad.MSK} = \mathsf{Sel.MSK}$ and a function f, the key-generation algorithm $\mathsf{Ad.KeyGen}$ first samples $C_E \leftarrow \{0,1\}^{\ell_1(\lambda)}$ and $\tau \leftarrow \{0,1\}^{\ell_2(\lambda)}$ uniformly and independently. Then, it computes and outputs $\mathsf{Ad}.sk_f = \mathsf{Sel}.sk_G \leftarrow \mathsf{Sel.KeyGen}(\mathsf{Sel.MSK}, G_{f,C_E,\tau})$, where the function $G_{f,C_E,\tau}$ is defined in Fig. 1.
– **The encryption algorithm:** On input the public key $\mathsf{Ad.MPK} = \mathsf{Sel.MPK}$ and a message m, the encryption algorithm $\mathsf{Ad.Enc}$ first samples $\mathsf{K} \leftarrow \mathcal{K}_\lambda$ and $\mathsf{OneCT.MSK} \leftarrow \mathsf{OneCT.Setup}(1^\lambda)$. Then, it outputs $\mathsf{CT} = (\mathsf{CT}_0, \mathsf{CT}_1)$, where

$$\mathsf{CT}_0 \leftarrow \mathsf{OneCT.Enc}(\mathsf{OneCT.MSK}, m) \text{ and}$$
$$\mathsf{CT}_1 \leftarrow \mathsf{Sel.Enc}(\mathsf{Sel.MPK}, (\mathsf{OneCT.MSK}, \mathsf{K}, 0^\lambda, 0)).$$

– **The decryption algorithm:** On input a functional key $\mathsf{Ad}.sk_f = \mathsf{Sel}.sk_G$ and a ciphertext $\mathsf{CT} = (\mathsf{CT}_0, \mathsf{CT}_1)$, the decryption algorithm $\mathsf{Ad.Dec}$ first computes $\mathsf{OneCT}.sk_f \leftarrow \mathsf{Sel.Dec}(\mathsf{Sel}.sk_G, \mathsf{CT}_1)$. Then, it computes $m \leftarrow \mathsf{OneCT.Dec}(\mathsf{OneCT}.sk_f, \mathsf{CT}_0)$ and outputs m.

```
$G_{f,C_E,\tau}(\mathsf{OneCT.MSK}, \mathsf{K}, \mathsf{Sym.K}, \beta)$:

1. If $\beta = 1$ output $\mathsf{OneCT}.sk_f \leftarrow \mathsf{Sym.Dec}(\mathsf{Sym.K}, C_E)$.
2. Otherwise, output $\mathsf{OneCT}.sk_f \leftarrow \mathsf{OneCT.KeyGen}(\mathsf{OneCT.MSK}, f; \mathsf{PRF}_\mathsf{K}(\tau))$.
```

Fig. 1. The function $G_{f,C_E,\tau}$.

The correctness of the above scheme easily follows from that of its underlying building blocks, and in the remainder of this section we prove the following theorem:

[4] That is, a private-key functional encryption scheme that is adaptively-secure for a single message query and many function queries (as discussed above).

Theorem 3.1. *Assuming that: (1)* Sel *is a selectively-secure public-key functional encryption scheme, (2)* OneCT *is an adaptively-secure single-ciphertext private-key functional encryption scheme, (3)* SYM *is a symmetric encryption scheme with pseudorandom ciphertexts, and (4)* $\mathcal{F}$ *is a pseudorandom function family, then* Ad *is an* adaptively-secure *public-key functional encryption scheme.*

Proof. We show that any PPT adversary $\mathcal{A}$ succeeds in the adaptive security game (see Definition 2.3) with only negligible probability. We will show this in a sequence of hybrids. The advantage of the adversary in $\mathsf{Hybrid}_{i.b}$ is defined to be probability that the adversary outputs 1 in $\mathsf{Hybrid}_{i.b}$ and this quantity is denoted by $\mathsf{Adv}^{\mathcal{A}}_{i.b}$. For $b \in \{0,1\}$, we define the following hybrids.

$\mathsf{\mathbf{Hybrid}}_{\mathbf{1}.\boldsymbol{b}}$: This corresponds to the real experiment when the challenger encrypts the message m_b. More precisely, the challenger produces an encryption $\mathsf{CT} = (\mathsf{CT}_0, \mathsf{CT}_1)$ where

$$\mathsf{CT}_0 \leftarrow \mathsf{OneCT.Enc}(\mathsf{OneCT.MSK}, m) \text{ and}$$
$$\mathsf{CT}_1 \leftarrow \mathsf{Sel.Enc}(\mathsf{Sel.MPK}, (\mathsf{OneCT.MSK}, \mathsf{K}, 0^\lambda, 0)).$$

$\mathsf{\mathbf{Hybrid}}_{\mathbf{2}.\boldsymbol{b}}$: The challenger replaces the hard-coded ciphertext C_E in every functional key corresponding to a query f made by the adversary, with a symmetric key encryption of $\mathsf{OneCT}.sk_f$ (note that each key has its own different C_E). Here, $\mathsf{OneCT}.sk_f$ is the output of $\mathsf{OneCT.KeyGen}(\mathsf{OneCT.MSK}^*, f; \mathsf{PRF}_{\mathsf{K}^*}(\tau))$ and K^* is a PRF key drawn from the key space $\mathcal{K}$. Further, the symmetric encryption is computed with respect to $\mathsf{Sym.K}^*$, where $\mathsf{Sym.K}^*$ is the output of $\mathsf{Sym.Setup}(1^\lambda)$ and τ is the tag associated to the functional key of f. The same $\mathsf{Sym.K}^*$ and K^* are used while generating all the functional keys, and K^* is used for generating the challenge ciphertext $\mathsf{CT}^* = (\mathsf{CT}^*_0, \mathsf{CT}^*_1)$ (that is, $\mathsf{CT}^*_0 \leftarrow \mathsf{OneCT.Enc}(\mathsf{OneCT.MSK}^*, m_b)$ and $\mathsf{CT}^*_1 \leftarrow \mathsf{Sel.Enc}(\mathsf{Sel.MSK}, (\mathsf{OneCT.MSK}^*, \mathsf{K}^*, 0^\lambda, 0)))$. The rest of the hybrid is the same as the previous hybrid, $\mathsf{Hybrid}_{1.b}$.

Note that the symmetric key $\mathsf{Sym.K}^*$ is not used for any purpose other than generating the values C_E. Therefore, the pseudorandom ciphertexts property of the symmetric scheme implies that $\mathsf{Hybrid}_{2.b}$ and $\mathsf{Hybrid}_{1.b}$ are indistinguishable.

Claim 3.2. *Assuming the pseudorandom ciphertexts property of* SYM*, for each* $b \in \{0,1\}$ *we have* $|\mathsf{Adv}^{\mathcal{A}}_{1.b} - \mathsf{Adv}^{\mathcal{A}}_{2.b}| \leq \mathsf{negl}(\lambda)$*.*

Proof. Suppose there exists an adversary such that the difference in the advantages is non-negligible, then we construct a reduction that can break the security of SYM. The reduction internally executes the adversary by simulating the role of the challenger in the adaptive public-key FE game. It answers both the message and the functional queries made by the adversary as follows. The reduction first executes $\mathsf{OneCT.Setup}(1^\lambda)$ to obtain $\mathsf{OneCT.MSK}^*$. It then samples K^* from $\mathcal{K}$. Further, the reduction generates $\mathsf{Sel.MSK}$, which is the output of

$\mathsf{Sel.Setup}(1^\lambda)$ and $\mathsf{Sym.K}^*$, which is the output of $\mathsf{Sym.Setup}(1^\lambda)$. When the adversary submits a functional query f, the reduction first picks τ at random. The reduction executes $\mathsf{OneCT.KeyGen}(\mathsf{OneCT.MSK}^*, f; \mathsf{PRF}(\mathsf{K}^*(\tau)))$ to obtain $\mathsf{OneCT}.sk_f$. It then sends $\mathsf{OneCT}.sk_f$ to the challenger of the symmetric encryption scheme. The challenger returns back with C_E, where C_E is either a uniformly random string or it is an encryption of $\mathsf{OneCT}.sk_f$. The reduction then generates a selectively-secure FE functional key of $G_{f,C_E,\tau}$ and denote the result by $\mathsf{Sel}.sk_G$ which is sent to the adversary. The message queries made by the adversary are handled as in Hybrid_1. That is, the adversary submits the message-pair query (m_0, m_1) and the reduction sends $\mathsf{CT}^* = (\mathsf{CT}_0^*, \mathsf{CT}_1^*)$ back to the adversary, where $\mathsf{CT}_0^* = \mathsf{OneCT.Enc}(\mathsf{OneCT.MSK}^*, m_b)$ and $\mathsf{CT}_1^* = \mathsf{Sel.Enc}(\mathsf{Sel.MSK}, (\mathsf{OneCT.MSK}^*, \mathsf{K}^*, 0^\lambda, 0))$.

If the challenger of the symmetric key encryption scheme sends a uniformly random string back to the reduction every time the reduction makes a query to the challenger then we are in $\mathsf{Hybrid}_{1.b}$, otherwise we are in $\mathsf{Hybrid}_{2.b}$. Since the adversary can distinguish both the hybrids with non-negligible probability, we have that the reduction breaks the security of the symmetric key encryption scheme with non-negligible probability. From our hypothesis, we have that the reduction breaks the security of the symmetric key encryption scheme with non-negligible probability. This proves the claim. □

$\mathsf{\mathbf{Hybrid}}_{\mathbf{3.b}}$: The challenger modifies the challenge ciphertext $\mathsf{CT}^* = (\mathsf{CT}_0^*, \mathsf{CT}_1^*)$ so that CT_1^* is an encryption of $(0^\lambda, 0^\lambda, \mathsf{Sym.K}^*, 1)$. The ciphertext component CT_0^* is not modified (i.e., $\mathsf{CT}_0^* = \mathsf{OneCT.Enc}(\mathsf{OneCT.MSK}^*, m_b)$). The rest of the hybrid is the same as the previous hybrid, $\mathsf{Hybrid}_{2.b}$.

Note that the functionality of the functional keys generated using the underlying selectively-secure scheme is unchanged with the modified CT_1^*. Therefore, its selective security implies that $\mathsf{Hybrid}_{3.b}$ and $\mathsf{Hybrid}_{2.b}$ are indistinguishable.

Claim 3.3. *Assuming the selective security of* Sel*, for each* $b \in \{0,1\}$ *we have* $|\mathsf{Adv}_{2.b}^{\mathcal{A}} - \mathsf{Adv}_{3.b}^{\mathcal{A}}| \leq \mathsf{negl}(\lambda)$.

Proof. Suppose the claim is not true for some adversary $\mathcal{A}$, we construct a reduction that breaks the security of Sel. Our reduction will internally execute $\mathcal{A}$ by simulating the role of the challenger of the adaptive FE game.

Our reduction first executes $\mathsf{OneCT.Setup}(1^\lambda)$ to obtain $\mathsf{OneCT.MSK}^*$. It then samples K^* from $\mathcal{K}$. It also executes $\mathsf{Sym.Setup}(1^\lambda)$ to obtain $\mathsf{Sym.K}^*$. The reduction then sends the message pair $\big((\mathsf{OneCT.MSK}^*, \mathsf{K}^*, 0^\lambda, 0), (0^\lambda, 0^\lambda, \mathsf{Sym.K}^*, 1)\big)$ to the challenger of the selective game. The challenger replies back with the public key $\mathsf{Sel.MPK}$ and the challenge ciphertext CT_1^*. The reduction is now ready to interact with the adversary $\mathcal{A}$. If $\mathcal{A}$ makes a functional query f then the reduction constructs the circuit $G_{f,C_E,\tau}$ as in $\mathsf{Hybrid}_{2.b}$. It then queries the challenger of the selective game with the function G and in return it gets the key $\mathsf{Sel}.sk_G$. The reduction then sets $\mathsf{Ad}.sk_f$ to be $\mathsf{Sel}.sk_G$ which it then sends back to $\mathcal{A}$. If $\mathcal{A}$ submits a message pair (m_0, m_1), the reduction executes $\mathsf{OneCT.Enc}(\mathsf{OneCT.MSK}^*, m_0)$ to obtain CT_0^*. It then sends the ciphertext

$\mathsf{CT}^* = (\mathsf{CT}_0^*, \mathsf{CT}_1^*)$ to the adversary. The output of the reduction is the output of $\mathcal{A}$.

We claim that the reduction is a legal adversary in the selective security game of Sel, i.e., for challenge message query $(M_0 = (\mathsf{OneCT.MSK}^*, \mathsf{K}^*, 0^\lambda, 0)$, $M_1 = (0^\lambda, 0^\lambda, \mathsf{Sym.K}^*, 1))$ and every functional query of the form $G_{f,C_E,\tau}$ made by the reduction, we have that $G_{f,C_E,\tau}(M_0) = G_{f,C_E,\tau}(M_1)$: By definition, $G_{f,C_E,\tau}(M_0)$ is the functional key of f, with respect to key $\mathsf{OneCT.MSK}^*$ and randomness $\mathsf{PRF}_{\mathsf{K}^*}(\tau)$. Further, $G_{f,C_E,\tau}(M_1)$ is the decryption of C_E which is nothing but the functional key of f, with respect to key $\mathsf{OneCT.MSK}^*$ and randomness $\mathsf{PRF}_{\mathsf{K}^*}(\tau)$. This proves that the reduction is a legal adversary in the selective security game.

If the challenger of the selective game sends back an encryption of $(\mathsf{OneCT.MSK}^*, \mathsf{K}^*, 0^\lambda, 0)$ then we are in $\mathsf{Hybrid}_{2.b}$ else if the challenger encrypts $(0^\lambda, 0^\lambda, \mathsf{Sym.K}^*, 1)$ then we are in $\mathsf{Hybrid}_{3.b}$. By our hypothesis, this means the reduction breaks the security of the selective game with non-negligible probability that contradicts the security of Sel. This completes the proof of the claim.

$\mathsf{Hybrid}_{4.b}$: For every function query f made by the adversary, the challenger generates C_E by executing $\mathsf{Sym.Enc}(\mathsf{Sym.K}^*, \mathsf{OneCT}.sk_f)$, with $\mathsf{OneCT}.sk_f$ being the output of $\mathsf{OneCT.KeyGen}(\mathsf{OneCT.MSK}^*, f; R)$, where R is picked at random. The rest of the hybrid is the same as the previous hybrid.

Note that the PRF key K^* is not explicitly needed in the previous hybrid, and therefore the pseudorandomness of $\mathcal{F}$ implies that $\mathsf{Hybrid}_{4.b}$ and $\mathsf{Hybrid}_{3.b}$ are indistinguishable.

Claim 3.4. *Assuming that $\mathcal{F}$ is a pseudorandom function family, for each $b \in \{0,1\}$ we have $|\mathsf{Adv}_{3.b}^{\mathcal{A}} - \mathsf{Adv}_{4.b}^{\mathcal{A}}| \le \mathsf{negl}(\lambda)$.*

Proof. Suppose the claim is false for some PPT adversary $\mathcal{A}$, we construct a reduction that internally executes $\mathcal{A}$ and breaks the security of the pseudorandom function family $\mathcal{F}$. The reduction simulates the role of the challenger of the adaptive game when interacting with $\mathcal{A}$. The reduction answers the functional queries, made by the adversary as follows; the message queries are answered as in $\mathsf{Hybrid}_{3.b}$ (or $\mathsf{Hybrid}_{4.b}$). For every functional query f made by the adversary, the reduction picks τ at random which is then forwarded to the challenger of the PRF security game. In response it receives R^*. The reduction then computes C_E to be $\mathsf{Sym.Enc}(\mathsf{Sym.K}^*, \mathsf{OneCT}.sk_f)$, where $\mathsf{OneCT}.sk_f = \mathsf{OneCT.KeyGen}(\mathsf{OneCT.MSK}^*, f; R^*)$. The reduction then proceeds as in the previous hybrids to compute the functional key $\mathsf{Ad}.sk_f$ which it then sends to $\mathcal{A}$.

If the challenger of the PRF game sent $R^* = \mathsf{PRF}_{\mathsf{K}^*}(\tau)$ back to the reduction then we are in $\mathsf{Hybrid}_{3.b}$ else if R^* is generated at random by the challenger then we are in $\mathsf{Hybrid}_{4.b}$. From our hypothesis this means that the probability that the reduction distinguishes the pseudorandom value from random (at the point τ) is non-negligible, contradicting the security of the pseudorandom function family.□

We now conclude the proof of the theorem by showing that $\mathsf{Hybrid}_{4.0}$ is computationally indistinguishable from $\mathsf{Hybrid}_{4.1}$ based on the adaptive security of the underlying single-ciphertext scheme.

Claim 3.5. *Assuming the adaptive security of the scheme* OneCT*, we have* $|\mathsf{Adv}^{\mathcal{A}}_{4.0} - \mathsf{Adv}^{\mathcal{A}}_{4.1}| \leq \mathsf{negl}(\lambda)$.

Proof. Suppose there exists a PPT adversary $\mathcal{A}$, such that the claim is false. We design a reduction $\mathcal{B}$ that internally executes $\mathcal{A}$ to break the adaptive security of OneCT.

The reduction simulates the role of the challenger of the adaptive public-key FE game. It answers both the functional as well as message queries made by the adversary as follows. If $\mathcal{A}$ makes a functional query f then it forwards it to the challenger of the adaptively-secure single-ciphertext FE scheme. In return it receives $\mathsf{OneCT}.sk_f$. It then encrypts it using the symmetric encryption scheme, where the symmetric key is picked by the reduction itself, and denote the resulting ciphertext to be C_E. The reduction then constructs the circuit $G_{f,C_E,\tau}$, with τ being picked at random, as in the previous hybrids. Finally, the reduction computes the selective public-key functional key of $G_{f,C_E,\tau}$, where the reduction itself picks the master secret key of selective public-key FE scheme. The resulting functional key is then sent to $\mathcal{A}$. If $\mathcal{A}$ makes a message-pair query (m_0, m_1), the reduction forwards this message pair to the challenger of the adaptive game. In response it receives CT_0^*. The reduction then generates CT_1^* on its own where CT_1^* is the selective FE encryption of $(0^\lambda, 0^\lambda, \mathsf{Sym.K}^*, 1)$. The reduction then sends $\mathsf{CT}^* = (\mathsf{CT}_0^*, \mathsf{CT}_1^*)$ to $\mathcal{A}$. The output of the reduction is the output of $\mathcal{A}$.

We note that the reduction is a legal adversary in the adaptive game of OneCT, i.e., for every challenge message query (m_0, m_1), functional query f, we have that $f(m_0) = f(m_1)$: this follows from the fact that (i) the functional queries (resp., challenge message query) made by the adversary (of Ad) is the same as the functional queries (resp., challenge message query) made by the reduction, and (ii) the adversary (of Ad) is a legal adversary. This proves that the reduction is a legal adversary in the adaptive game.

If the challenger sends an encryption of m_0 then we are in $\mathsf{Hybrid}_{4.0}$ and if the challenger sends an encryption of m_1 then we are in $\mathsf{Hybrid}_{4.1}$. From our hypothesis, this means that the reduction breaks the security of OneCT. This proves the claim. □

4 From Shallow Circuits to All Circuits

In this section we show that a functional encryption scheme that supports functions computable by shallow circuits can be transformed into one that supports functions computable by arbitrarily deep circuits. In particular, the shallow class can be any class in which weak pseudorandom functions can be computed and has some composition properties.[5] For concreteness we consider here the class NC^1, which can compute weak pseudorandom functions under standard cryptographic assumptions such as DDH or LWE (a lower complexity class such as TC^0 is also sufficient under standard assumptions). We focus here on private-key

[5] Similarly to the class WEAK defined in [App14].

functional encryption schemes, and note that an essentially identical transformation applies for public-key scheme.

While we present a direct reduction below, we notice that this property can be derived from the transformation in Sect. 3, by recalling some properties of Gorbunov et al.'s [GVW12] single-key functional encryption scheme. One can verify that their setup algorithm can be implemented in NC^1 (under the assumption that it can evaluate weak pseudorandom functions), regardless of the depth of the function being implemented. This property carries through even after applying the function privacy transformation of Brakerski and Segev [BS15]. Lastly, to implement our approach we need a symmetric encryption scheme with decryption in NC^1, which again translates to the evaluation of a weak pseudorandom function [NR04, BPR12].

(Computational) Randomized Encodings [IK00, AIK05]**.** A (computational) randomized encoding scheme for a function class $\mathcal{F}$ consists of two PPT algorithms $(\mathsf{RE.Encode}, \mathsf{RE.Decode})$. The PPT algorithm $\mathsf{RE.Encode}$ takes as input $(1^\lambda, F, x, r)$, where λ is the security parameter, $F : \{0,1\}^\lambda \rightarrow \{0,1\}$ is a function in $\mathcal{F}$, instance $x \in \{0,1\}^\lambda$ and randomness r. The output is denoted by $\hat{F}(x;r)$. The PPT algorithm $\mathsf{RE.Decode}$ takes as input $\hat{F}(x;r)$ and outputs $y = F(x)$.

The security property states that there exists a PPT algorithm $\mathsf{RE.Sim}$ that takes as input $(1^\lambda,\ F(x))$ and outputs $\mathsf{SimOut}_{F(x)}$ such that any PPT adversary cannot distinguish the distribution $\{\hat{F}(x;r)\}$ from the distribution $\{\mathsf{SimOut}_{F(x)}\}$. The following corollary is derived from applying Yao's garbled circuit technique using a weak PRF based encryption algorithm.

Corollary 4.1. *Assuming a family of weak pseudorandom functions that can be evaluated in* NC^1*, there exists a randomized encoding scheme* $(\mathsf{RE.Encode}, \mathsf{RE.Decode})$ *for the class of polynomial size circuits, such that* $\mathsf{RE.Encode}$ *is computable in* NC^1*.*

Our Transformation. Let $\mathcal{NCFE} = (\mathsf{NCFE.Setup}, \mathsf{NCFE.KeyGen}, \mathsf{NCFE.Enc}, \mathsf{NCFE.Dec})$ be a private-key functional encryption scheme for the class NC^1. We assume that $\mathcal{NCFE}$ supports functions with multi-bit outputs, as otherwise it is always possible to produce a functional key for each output bit separately. We also use a pseudorandom function family denoted by $\mathcal{F} = \{\mathsf{PRF}_\mathsf{K}(\cdot)\}_{\mathsf{K}\in\mathcal{K}}$ and a symmetric encryption scheme $\mathsf{SYM} = (\mathsf{Sym.Setup}, \mathsf{Sym.Enc}, \mathsf{Sym.Dec})$. We construct a private-key functional encryption scheme $\mathcal{PFE} = (\mathsf{PFE.Setup}, \mathsf{PFE.KeyGen}, \mathsf{PFE.Enc}, \mathsf{PFE.Dec})$ as follows.

- **The setup algorithm:** On input 1^λ the algorithm $\mathsf{PFE.Setup}$ samples and outputs $MSK \leftarrow \mathsf{NCFE.Setup}(1^\lambda)$.
- **The key-generation algorithm:** On input the secret key MSK and a circuit F, the algorithm $\mathsf{PFE.KeyGen}$ first samples $C_E \leftarrow \{0,1\}^{\ell_1(\lambda)}$ and $\tau \leftarrow \{0,1\}^\lambda$ uniformly and independently. Then, it computes a functional key $SK_G \leftarrow \mathsf{NCFE.KeyGen}(MSK, G_{F,C_E,\tau})$, where the function $G_{F,C_E,\tau}$ is defined in Fig. 2, and outputs SK_G.

– **The encryption algorithm:** On input the secret key MSK and a message x, the algorithm $\mathsf{PFE.Enc}$ first samples $K_P \leftarrow \{0,1\}^\lambda$, and then computes and outputs $C \leftarrow \mathsf{NCFE.Enc}(MSK, (x, K_P, 0^\lambda, 0))$.
– **The decryption algorithm:** On input a functional key $SK_F = SK_G$, and a ciphertext C, the decryption algorithm $\mathsf{PFE.Dec}$ computes $\widehat{F}(x) \leftarrow \mathsf{NCFE.Dec}(SK_G, C)$ and then outputs $\mathsf{RE.Decode}(\widehat{F}(x))$.

$\boldsymbol{G_{F,C_E,\tau}(x, K_P, K_E, \beta)}$:

1. If $\beta = 1$ output $\mathsf{Sym.Dec}_{K_E}(C_E)$.
2. Otherwise, output $\widehat{F}(x; \mathsf{PRF}_{K_P}(\tau)) = \mathsf{RE.Encode}(F, x; \mathsf{PRF}_{K_P}(\tau))$.

Fig. 2. The function $G_{F,C_E,\tau}$.

The correctness of the above scheme easily follows from that of its underlying building blocks, and in the remainder of this section we provide a sketch for proving the following theorem:

Theorem 4.2. *Assuming that: (1) $\mathcal{NCFE}$ is a selectively-secure private-key functional encryption scheme for* NC^1*, (2)* SYM *is a symmetric encryption scheme with pseudorandom ciphertexts whose decryption circuit is in* NC^1*, (3)* PRF *is a weak pseudorandom function family which can be evaluated in* NC^1*, and (4)* $(\mathsf{RE.Encode}, \mathsf{RE.Decode})$ *is a randomized encoding scheme with encoding in* NC^1*, then $\mathcal{PFE}$ is a selectively-secure private-key functional encryption scheme for P.*

Proof Sketch. The proof proceeds by a sequence of hybrids. For simplicity, we consider the case when the adversary submits a single challenge pair (m_0, m_1), and the argument can be easily generalized to the case of multiple challenges.

$\mathsf{\mathbf{Hybrid}}_\mathbf{0}$: This corresponds to the real experiment where the challenger sends an encryption of m_0 to the adversary.

$\mathsf{\mathbf{Hybrid}}_\mathbf{1}$: For every functional query F, the challenger replaces C_E with a symmetric encryption $\mathsf{Sym.Enc}(K_E, \widehat{F}(m_0; \mathsf{PRF}_{K_P}(t))$ in the functional key for F. By a sequence of intermediate hybrids (as many as the number of function queries), Hybrid_1 can be shown to be computationally indistinguishable from Hybrid_0 based on the pseudorandom ciphertexts property of the symmetric encryption scheme.

$\mathsf{\mathbf{Hybrid}}_\mathbf{2}$: The challenge ciphertext will consist of an encryption of $(m_0, 0, K_E, 1)$ instead of $(m_0, K_P, 0^\lambda, 0)$. This hybrid is computationally indistinguishable from Hybrid_1 by the security of the underlying functional encryption scheme.

Hybrid_3: For every function query F, the challenger replaces C_E in all the functional keys with $\mathsf{Sym.Enc}(K_E, \widehat{F}(m_0; r))$ for a uniform r. By a sequence of intermediate hybrids (as many as the number of function queries), Hybrid_3 can be shown to be computationally indistinguishable from Hybrid_2 based on the security of PRF.

Hybrid_4: Finally, for every function query F, the challenger replaces $\widehat{F}(m_0; r)$ in the ciphertext hardwired in the functional key for F by the simulated randomized encoding $\mathsf{RE.Sim}(1^\lambda, F(m_0))$. By a sequence of intermediate hybrids (as many as the number of function queries), Hybrid_4 can be shown to be computationally indistinguishable from Hybrid_3 based on the security of randomized encodings. Note that the this hybrid does not depend on whether m_0 or m_1 was encrypted since for all function queries F it holds that $F(m_0) = F(m_1)$, and this proves the security of $\mathcal{PFE}$.

References

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

[AIK05] Applebaum, B., Ishai, Y., Kushilevitz, E.: Computationally private randomizing polynomials and their applications. In: CCC, pp. 260–274. IEEE Computer Society (2005)

[App14] Applebaum, B.: Bootstrapping obfuscators via fast pseudorandom functions. In: Sarkar, P., Iwata, T. (eds.) ASIACRYPT 2014, Part II. LNCS, vol. 8874, pp. 162–172. Springer, Heidelberg (2014)

[BB04] Boneh, D., Boyen, X.: Efficient selective-ID secure identity-based encryption without random oracles. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 223–238. Springer, Heidelberg (2004)

[BCO+04] Boneh, D., Di Crescenzo, G., Ostrovsky, R., Persiano, G.: Public key encryption with keyword search. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 506–522. Springer, Heidelberg (2004)

[BCP14] Boyle, E., Chung, K.-M., Pass, R.: On extractability obfuscation. In: Lindell, Y. (ed.) TCC 2014. LNCS, vol. 8349, pp. 52–73. Springer, Heidelberg (2014)

[BF03] Boneh, D., Franklin, M.K.: Identity-based encryption from the Weil pairing. SIAM J. Comput. **32**(3), 586–615 (2003)

[BPR12] Banerjee, A., Peikert, C., Rosen, A.: Pseudorandom functions and lattices. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 719–737. Springer, Heidelberg (2012)

[BS15] Brakerski, Z., Segev, G.: Function-private functional encryption in the private-key setting. In: Dodis, Y., Nielsen, J.B. (eds.) TCC 2015, Part II. LNCS, vol. 9015, pp. 306–324. Springer, Heidelberg (2015)

[BSW11] Boneh, D., Sahai, A., Waters, B.: Functional encryption: definitions and challenges. In: Ishai, Y. (ed.) TCC 2011. LNCS, vol. 6597, pp. 253–273. Springer, Heidelberg (2011)

[CIJ+13] De Caro, A., Iovino, V., Jain, A., O'Neill, A., Paneth, O., Persiano, G.: On the achievability of simulation-based security for functional encryption. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013, Part II. LNCS, vol. 8043, pp. 519–535. Springer, Heidelberg (2013)

[GGH+13] Garg, S., Gentry, C., Halevi, S., Raykova, M., Sahai, A., Waters, B.: Candidate indistinguishability obfuscation and functional encryption for all circuits. In: FOCS, pp. 40–49 (2013)

[GGH+14a] Garg, S., Gentry, C., Halevi, S., Zhandry, M.: Fully secure attribute based encryption from multilinear maps. IACR Cryptol. ePrint Arch. **2014**, 622 (2014)

[GGH+14b] Garg, S., Gentry, C., Halevi, S., Zhandry, M.: Fully secure functional encryption without obfuscation. Cryptology ePrint Archive, report 2014/666 (2014)

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

[GHR+14] Gentry, C., Halevi, S., Raykova, M., Wichs, D.: Outsourcing private RAM computation. In: FOCS, pp. 404–413. IEEE Computer Society (2014)

[GKP+13] Goldwasser, S., Kalai, Y., Popa, R.A., Vaikuntanathan, V., Zeldovich, N.: Reusable garbled circuits and succinct functional encryption. In: ACM STOC, pp. 555–564 (2013)

[Gol04] Goldreich, O.: Foundations of Cryptography - Volume 2: Basic Applications. Cambridge University Press, Cambridge (2004)

[GPS+06] Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. In: ACM CCS, pp. 89–98 (2006)

[GVW12] Gorbunov, S., Vaikuntanathan, V., Wee, H.: Functional encryption with bounded collusions via multi-party computation. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 162–179. Springer, Heidelberg (2012)

[GVW13] Gorbunov, S., Vaikuntanathan, V., Wee, H.: Attribute-based encryption for circuits. In : ACM STOC, pp. 545–554 (2013)

[IK00] Ishai, Y., Kushilevitz, E.: Randomizing polynomials: a new representation with applications to round-efficient secure computation. In: FOCS, pp. 294–304 (2000)

[KSW08] Katz, J., Sahai, A., Waters, B.: Predicate encryption supporting disjunctions, polynomial equations, and inner products. In: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 146–162. Springer, Heidelberg (2008)

[LOS+10] Lewko, A., Okamoto, T., Sahai, A., Takashima, K., Waters, B.: Fully Secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 62–91. Springer, Heidelberg (2010)

[LW10] Lewko, A., Waters, B.: New techniques for dual system encryption and fully secure HIBE with short ciphertexts. In: Micciancio, D. (ed.) TCC 2010. LNCS, vol. 5978, pp. 455–479. Springer, Heidelberg (2010)

[LW12] Lewko, A., Waters, B.: New proof methods for attribute-based encryption: achieving full security through selective techniques. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 180–198. Springer, Heidelberg (2012)

[NR04] Naor, M., Reingold, O.: Number-theoretic constructions of efficient pseudo-random functions. J. ACM **51**(2), 231–262 (2004)

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

[SS10] Sahai, A., Seyalioglu, H.: Worry-free encryption: functional encryption with public keys. In: ACM CCS, pp. 463–472 (2010)

[SW05] Sahai, A., Waters, B.: Fuzzy identity-based encryption. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 457–473. Springer, Heidelberg (2005)

[Wat09] Waters, B.: Dual system encryption: realizing fully secure IBE and HIBE under simple assumptions. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 619–636. Springer, Heidelberg (2009)

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