Instantiability of Classical Random-Oracle-Model Encryption Transforms

Alice Murphy[1], Adam O'Neill[2], and Mohammad Zaheri[3]

[1] Dept. of Computer Science, University of Waterloo, Canada
anlmurph@uwaterloo.ca
[2] Manning CICS, University of Massachusetts Amherst, USA
adamo@cs.umass.edu
[3] Snap Inc., USA
mohammad.zaheri@gmail.com

Abstract. Extending work leveraging program obfuscation to instantiate random-oracle-based transforms (*e.g.*, Hohenberger *et al.*, EUROCRYPT 2014, Kalai *el al.*, CRYPTO 2017), we show that, using obfuscation and other assumptions, there exist standard-model hash functions that suffice to instantiate the classical RO-model encryption transforms OAEP (Bellare and Rogaway, EUROCRYPT 1994) and Fujisaki-Okamoto (CRYPTO 1999, J. Cryptology 2013) for specific public-key encryption (PKE) schemes to achieve IND-CCA security. Our result for Fujisaki-Okamoto employs a simple modification to the scheme.
Our instantiations do not require much stronger assumptions on the base schemes compared to their corresponding RO-model proofs. For example, to instantiate low-exponent RSA-OAEP, the assumption we need on RSA is sub-exponential partial one-wayness, matching the assumption (partial one-wayness) on RSA needed by Fujisaki *et al.* (J. Cryptology 2004) in the RO model up to sub-exponentiality. For the part of Fujisaki-Okamoto that upgrades public-key encryption satisfying indistinguishability against plaintext checking attack to IND-CCA, we again do not require much stronger assumptions up to sub-exponentiality.
We obtain our hash functions in a unified way, extending a technique of Brzuska and Mittelbach (ASIACRYPT 2014). We incorporate into their technique: (1) extremely lossy functions (ELFs), a notion by Zhandry (CRYPTO 2016), and (2) *multi-bit* auxiliary-input point function obfuscation (MB-AIPO). While MB-AIPO is impossible in general (Brzuska and Mittelbach, ASIACRYPT 2014), we give plausible constructions for the special cases we need, which may be of independent interest.

Keywords. Fujisaki-Okamoto, RSA-OAEP, Random Oracle, Standard Model, Chosen-Ciphertext Security, Extremely Lossy Functions

1 Introduction

1.1 Background and Goal

The random oracle model and uninstantiability. The random oracle (RO) model [10] is a popular paradigm for designing practical cryptographic

schemes. The idea is that in the design and analysis of a scheme all parties are assumed to have access to one or more oracles that implement independent random functions (called ROs). The hope is that when the scheme is implemented in practice, using cryptographic hashing in place of the ROs, then the scheme retains security. (Replacing the ROs with some functions is said to "instantiate" the scheme via these functions.) Unfortunately, this paradigm has been shown to be false in a strong sense, starting with the work of Canetti, Goldreich, and Halevi [28]. They exhibit schemes that are secure in the RO model but are insecure when instantiated with *any* efficient function, let alone cryptographic hashing. Such unfortunate schemes are called *uninstantiable*. Thus, it is crucial to demonstrate *instantiatiability* of popular RO model schemes by giving efficient functions that can provably replace their ROs. This not only gives us better evidence of their security, but also provides insights into their security that were previously obscured in the ROM. This insight can lead to tweaks that increase their security and new design goals for cryptographic hashing.

Before proceeding, it should be clarified that our hash functions made to replace ROs are not practically efficient. Thus, we do not propose that our hash functions are actually used. Rather, their *existence* makes it more plausible that the schemes we instantiate meet their goals when using cryptographic hashing.

RO MODEL TRANSFORMS. A particularly vexing case of uninstantiability concerns *transforms* in the RO model; in other words, compilers that take one or more "base schemes" (that may or may not use ROs) and output a "target scheme" that uses ROs. We say that the transform "works" if for any secure base schemes the output target scheme is secure (under the appropriate security notions). The instantiated scheme should have the same security property, so we refer to the transform as uninstantiable if for any standard-model hash functions replacing the ROs, there exist secure base schemes such that the corresponding target scheme is insecure. This means the transform cannot "work" in the standard model in general.

OUR FOCUS: CLASSICAL ENCRYPTION TRANSFORMS. We are concerned with instantiability of two highly influential RO model transforms that output a (public-key) encryption scheme, the Optimal Asymmetric Encryption Padding (OAEP) trapdoor permutation-based transform [11] and the Fujisaki-Okamoto (FO) hybrid-encryption transform [37]. These are considered two of the "crown jewels" of the RO model, but their instantiability has not been established. In fact, there exist *uninstantiability* results to some extent. Accordingly, the main question we study is:

> *Do there exist standard-model hash functions that suffice to instantiate IND-CCA2 secure OAEP and FO?*

We briefly recall how these transforms work. OAEP takes a trapdoor permutation (TDP) $\mathcal{F}$ (typically RSA) and produces a public-key encryption scheme whose public key is an instance f of the TDP. It uses two ROs $\mathcal{G}, \mathcal{H}$ and the encryption algorithm has the form:

$$\mathcal{E}_f^{\mathsf{OAEP}}(m;r) = f(s\|t) \quad \text{where} \quad s = \mathcal{G}(r) \oplus m\|0^{\zeta} \quad \text{and} \quad t = \mathcal{H}(s) \oplus r \ ,$$

where $\zeta \in \mathbb{N}$ is a redundancy parameter.

FO uses a public-key encryption scheme and a symmetric-key encryption scheme to produce a new public-key encryption scheme. We modify the original encryption algorithm [37] by incorporating changes from Hofheinz, Hövelmanns, and Kiltz [49] to obtain the form:

$$\mathcal{E}^{\mathsf{hy}}_{pk}(m;r) = \mathcal{E}^{\mathsf{asy}}_{pk}(r;\mathcal{H}(r)) \| \mathcal{E}^{\mathsf{sy}}_{K}(m) \quad \text{where} \quad K = \mathcal{G}(r\|c_1), c_1 = \mathcal{E}^{\mathsf{asy}}_{pk}(r;\mathcal{H}(r)) \ ,$$

where $\mathcal{E}^{\mathsf{asy}}$ denotes the encryption algorithm of the starting public-key scheme and $\mathcal{E}^{\mathsf{sy}}$ denotes the encryption algorithm of the starting symmetric-key scheme.

Instantiability results for OAEP and FO are challenging because there are negative results known. Notably, Kiltz and Pietrzak [61] show a black-box separation for OAEP in the ideal TDP model, and Brzuska *et al.* [23] show the FO transform to be uninstantiable, even assuming IND-CPA security of the base PKE scheme. Further results about the schemes are discussed below.

1.2 Further Related Work and Open Questions

Attempts at instantiability of OAEP and FO. The question of instantiability of OAEP and FO was posed by Canetti [26] and Boldyreva and Fischlin [18, 19]. The latter gave partial instantiations of variants of the transforms, where only *one* of the ROs is instantiated. Kiltz *et al.* [60] showed IND-CPA security of RSA-OAEP using lossiness of RSA, while Bellare, Hoang, and Keelveedhi [7] showed RSA-OAEP is the same for public-key-independent messages assuming the round functions meet their UCE notion. Cao *et al.* [29] gave partial instantiations of RSA-OAEP, as well as full instantiations for some variants of it.

On the negative side, Brown [22] and Paillier and Villar [64] showed negative results for proving RSA-OAEP is IND-CCA secure in restricted models, and Kiltz and Pietrzak [61] showed a general black-box impossibility result. Their results do not contradict ours because we use non-blackbox assumptions. Furthermore, they do not apply to TDP's satisfying properties common-inputs extractability (CIE) and second-inputs extractability (SIE). Shoup [70] exhibited a black-box separation showing that a form of *non-malleability* for the TDP is necessary. On the other hand, Fujisaki *et al.* [39] show that the seemingly stronger assumption of *partial one-wayness* (POW) on the TDP is sufficient.

FO has evaded any positive results in the standard model, despite its growing importance. The assumptions needed by Brzuska *et al.* [23] were later relaxed by Goyal *et al.* [46]. We evade these results by exploiting the fact that they do not apply when the PKE scheme is OW-PCA or lossy. Brzuska *et al.* [23] actually show uninstantiability of the underlying "Encrypt-with-Hash" (EwH) [6] portion of the transform, namely $\mathcal{E}^{\mathsf{asy}}_{pk}(r;\mathcal{H}(r))$. Thus, our main focus is on the "hybrid encryption" part of the transform $\mathcal{E}^{\mathsf{asy}}_{pk}(r)\|\mathcal{E}^{\mathsf{sy}}_{K}(m)$ where $K = \mathcal{G}(r\|c_1), c_1 = \mathcal{E}^{\mathsf{asy}}_{pk}(r;\mathcal{H}(r))$. We also consider the first part by making other assumptions on the base scheme. Concurrently, Zhandry [73] introduced a negative result for the FO transform when using *random oracles* in his augmented random oracle model (AROM). We use structured hash functions instead.

We have previously seen success in instantiating classical RO-based transforms outside the encryption domain, such as the full-domain hash (FDH) signature scheme [50, 72] and Fiat-Shamir (*e.g.*, [58]). In particular, we have seen such lines of work first use obfuscation and later drop it (*e.g*, by Zhandry [72] in the case of FDH); we are hopeful the same pattern will emerge for our results.

Results in the (Q)ROM. Results about the security of RSA-OAEP in the RO model were shown in [11, 39, 70]. Ultimately, these works showed RSA-OAEP is IND-CCA2 secure in the RO model assuming only one-wayness of RSA, but with a loose security reduction.

The original security bound for FO is lossy. With the recent interest in post-quantum cryptography and FO's applications to it, there has been work on getting tight reductions for FO and variants in the quantum RO model, *e.g.* [49, 51, 55, 56, 69], all of which are set in the ROM. Our security bound for the instantiated FO is also lossy.[4] An interesting question is whether "implicit rejection" can help with this, as it does in the RO case.

1.3 Our Results

A unified paradigm. Our standard-model hash functions for OAEP and FO are obtained via a unified paradigm that uses indistinguishability obfuscation (iO) [3, 41] to obfuscate the composition of a punctured pseudorandom function (PPRF) [21, 59, 68] and extremely lossy function (ELF) [72]. In our proofs, we extend an idea of Brzuska and Mittelbach [25] to construct universal computational extractors [7]. In our extension, we utilize *multi-bit* auxiliary-input point function obfuscation (MB-AIPO) [27], as well as ELFs.

ELFs and their applicability. To explain ELFs [72], we first recall the notion of a lossy function, a trapdoor-less version of lossy trapdoor functions [65]. A lossy function key can be generated in one of two modes, the injective or the lossy mode, where the first induces an injective function and the second induces a highly non-injective one. Furthermore, keys generated via these two modes are indistinguishable to any efficient adversary. Note that the lossy function image cannot be *too* small, else there would be a trivial distinguisher. ELFs achieve *much more lossiness* by reversing the order of quantifiers. Namely, for an ELF, for every adversary there exists an (adversary-dependent) indistinguishable lossy key-generation mode. The induced function can even have an appropriate *polynomial*-size image. Zhandry [72] constructs ELFs based on exponential DDH, where the lossy mode depends on the run-time of the adversary.

We observe ELFs seem useful for "answering decryption queries" in a proof of IND-CCA security. Indeed, a high-level strategy in the reduction could be, on answering a decryption query, to iterate over all possible ELF outputs in the lossy mode to see which one permits correct decryption. But there is a problem:

[4] Looking ahead, we do not obtain a *post-quantum* secure instantiation of FO in this work based on known realizations of our hash functions. Yet, clearly a classically secure one is a step forward.

the ELF output used in the challenge ciphertext would not look random to a reduction running the IND-CCA adversary and simulating the decryption oracle this way. This is because the reduction must be able to enumerate the entire lossy ELF image. To solve this problem, we wrap the ELF into a higher-level program that we obfuscate. This program outputs a special, truly random point on the input used in forming the challenge ciphertext, and otherwise evaluates the ELF.

Results on OAEP. For simplicity, consider the case of public-key-independent messages; we later explain how to deal with the public-key-dependent case. We show that low-exponent RSA-OAEP is fully instanitiable under the same assumption on the base scheme (RSA) used by Fujisaki *et al.* [38] in the RO model, namely partial one-wayness. Here we instantiate $\mathcal{G}$ in OAEP as $\mathsf{iO}(\mathsf{ELF}(\mathsf{PRF}_K(\cdot)))$ where iO is an indistinguishability obfuscator [3, 41], ELF is an injective-mode ELF, and PRF is a puncturable pseudorandom function [21, 59, 68]. The PRF key and ELF function are hardcoded into the obfuscated program. To instantiate $\mathcal{H}$ we use a one-wayness extractor [52] with polynomial-length output (see below). In the proof (and not in the construction), multi-bit point function obfuscation with auxiliary input (MB-AIPO) is used.

Results on Fujisaki-Okamoto. We focus on the part of the transform from OW-PCA to IND-CCA2 (cf. transform 3.2.2 of Hofheinz *et al.* [49]), which is *not* subject to uninstantiability results. Moreover, we propose a modified version of this part of the FO transform:

$$\mathcal{E}^{\mathsf{hy}}_{pk}(m;r) = \mathcal{E}^{\mathsf{asy}}_{pk}(r;z) \| \mathcal{E}^{\mathsf{sy}}_{K}(m\|r) \quad \text{where} \quad K = \mathcal{G}(r\|\mathcal{E}^{\mathsf{asy}}_{pk}(r;z)) \ .$$

Decryption recovers r from the asymmetric ciphertext, computes the symmetric key with the hash function, and then decrypts the symmetric ciphertext $m\|r'$, m is returned iff $r = r'$. Moreover, if the symmetric-key encryption is already *randomized* and *randomness-recovering*, then r can safely be used as its coins as there is no additional overhead (cf. Remark 3).

We show this modified part of the FO transform is fully instantiable under suitable assumptions. To describe the assumptions, we introduce a new notion of cryptography with "adaptive" auxiliary input. This refers to an adversary being given auxiliary input that includes access to an oracle. Specifically, for our instantiation we require MB-AIPO with adaptive auxiliary input where the input point has the form $r^*\|c^*_1$, the output point is K^*, and the auxiliary input has the form (t, d, c^*, pk', m) where $c^* = c^*_1\|c^*_2$ is an encryption of m. Furthermore, the oracle provided to the adversary is either a public-key ciphertext validity checker or, as a separate assumption, a symmetric-key ciphertext validity checker. Beyond this, we need that the public-key encryption scheme is sub-exponentially OW-PCA and the symmetric-key encryption scheme is sub-exponentially secure authenticated encryption [9]. Notably, we later show that our new ELF-based MB-AIPO is secure for the adaptive auxiliary input needed, albeit for public-key-independent messages.

New MB-AIPOs. We wish to justify the existence of MB-AIPOs for the distributions needed in the OAEP and FO instantiation proofs. This is challenging

because in general MB-AIPO for computationally unpredictable auxiliary input is likely impossible [24]. To circumvent this result for OAEP, we provide a new and simple RSA-based MB-AIPO. The auxiliary input contains an RSA ciphertext, and it is plausible this combination is secure. For FO, we show a new MB-AIPO for *statistically unpredictable* auxiliary input (which is not subject to the [24] result) based on ELFs that we further prove is sufficient for us when the PKE scheme is *lossy* [8] and the one-time AE scheme is *information-theoretic* and *leakage-resilient* in the sense of [2]. Of course, one can simply assume security of our MB-AIPO wrt. the *specific* computationally unpredictable auxiliary input needed. Then information-theoretic security of the AE and lossiness of the PKE can be removed, which yields a more practical result.

Leveraging sub-exponential security assumptions. Finally, we leverage sub-exponential security assumptions to handle public-key-dependent messages. To see the reason, consider that the auxiliary information given to an MB-AIPO adversary in our proofs should contain an encryption of the challenge message. However, the challenge message depends on the obfuscation itself, the latter being in the public key. Thus, we have to *guess* the message in the auxiliary information. A generic argument to this effect would require sub-exponential security assumptions on *all* of the primitives, whereas for us it is crucial to avoid this assumption on ELFs, for which we do not know sub-exponentially secure instantiations. Thus, we use a tailored argument at this step of the proof. While we do not view sub-exponential assumptions as too devastating, it is an important open problem to handle public-key-dependent messages without them. Current techniques to remove sub-exponential iO [1] do not seem applicable to our case, because the message is not hashed or fed through an obfuscation.

On the assumptions. Arguably, our assumptions are strong, but not unreasonably so. We note that new constructions of iO have recently emerged [43, 53, 54, 71] under safer assumptions. ELFs have been built from exponential DDH [72], which is a common assumption on elliptic curves. To construct a sub-exponential one-wayness extractor with polynomial output length, we can use diO with short auxiliary input as per [13], which is stronger than iO but is plausibly satisfied by the same constructions.[5] (diO with short auxiliary input is weaker than full-fledged diO, which is implausible [42].) Perhaps the most exotic assumption we need are MB-AIPOs for specific auxiliary input distributions. However, we lend plausibility by suggesting specific constructions.

2 Preliminaries

We overview notations and definitions used; some of which are taken from the prior work of Cao *et al.* [29].

[5] Unfortunately, for another construction of a one-wayness extractor with polynomial-length output from ELFs due to Zhandry [72], it does not seem possible to set parameters to get sub-exponential security.

2.1 Notation and Conventions

For a probabilistic algorithm A, by $y \leftarrow\!\!\$\ A(x)$ we mean that A is executed on input x and the output is assigned to y. We sometimes use $y \leftarrow A(x;r)$ to make A's random coins explicit. We denote by $\Pr\left[A(x) = y : x \leftarrow\!\!\$\ X\right]$ the probability that A outputs y on input x when x is sampled according to X. We denote by $[A(x)]$ the set of possible outputs of A when run on input x. The security parameter is denoted $k \in \mathbb{N}$ and 1^k denotes the unary encoding of the security parameter. Integer parameters often implicitly depend on k.

Unless otherwise specified, all algorithms must run in probabilistic polynomial time (PPT) in k, and an algorithm's run time includes that of any overlying experiment as well as the size of its code.

The length of a string s is denoted $|s|$. We denote by $s|_i^j$ the substring of s from the i-th least significant bit (LSB) to the j-th most significant bit (MSB) of s (inclusive), where $1 \le i \le j \le |s|$. For convenience, we denote by $s|_\ell = s|_1^\ell$ the ℓ LSBs of s and $s|^\ell = s|_{|s|-\ell}^{|s|}$ the ℓ MSBs of s, for $1 \le \ell \le |s|$. Vectors are denoted in boldface, for example $\mathbf{x}$. If $\mathbf{x}$ is a vector then $|\mathbf{x}|$ denotes the number of components of $\mathbf{x}$ and $\mathbf{x}[i]$ denotes its i-th component, for $1 \le i \le |\mathbf{x}|$. Note that we begin indexing at 1, not 0. For convenience, we extend algorithmic notation to operate on each vector of inputs component-wise. For example, if A is an algorithm and $\mathbf{x}, \mathbf{y}$ are vectors then $\mathbf{z} \leftarrow\!\!\$\ A(\mathbf{x}, \mathbf{y})$ denotes that $\mathbf{z}[i] \leftarrow\!\!\$\ A(\mathbf{x}[i], \mathbf{y}[i])$ for all $1 \le i \le |\mathbf{x}|$. Unless otherwise specified, ε denotes the empty string. A function $f\colon \mathbb{N} \to [0,1]$ is *negligible* if for every constant c and all but finitely many $k \in \mathbb{N}$ we have $f(k) < 1/k^c$.

Many games return a value like $(b' = b)$. This means that the boolean truth value of the statement $b' = b$ is returned. Define the *left-or-right selector function* as $\mathsf{LR}(x_0, x_1, b) = x_b$ for $x_0, x_1 \in \{0,1\}^*$ and $b \in \{0,1\}$.

Indistinguishability. Let $\mathcal{X} = \{X_k\}_{k\in\mathbb{N}}$ and $\mathcal{Y} = \{Y_k\}_{k\in\mathbb{N}}$ be distribution ensembles. We say that $\mathcal{X}$ is *computationally indistinguishable* from $\mathcal{Y}$, denoted $\mathcal{X} \approx_c \mathcal{Y}$, if for all PPT distinguishers D

$$|\Pr[\, D(x_k) \Rightarrow 1\,] - \Pr[\, D(Y_k) \Rightarrow 1\,]| \le \mathsf{negl}(k)$$

We say that $\mathcal{X}$ is *statistically indistinguishable* from $\mathcal{Y}$, denoted $\mathcal{X} \approx_s \mathcal{Y}$, if for all (even bounded) distinguishers D

$$|\Pr[\, D(x_k) \Rightarrow 1\,] - \Pr[\, D(Y_k) \Rightarrow 1\,]| \le \mathsf{negl}(k)\ .$$

2.2 Encryption Schemes and Their Security

Symmetric-key encryption. A *symmetric-key (or private key) encryption scheme* SE with message space Msg is a tuple of algorithms $(\mathcal{K}, \mathcal{E}, \mathcal{D})$. The key-generation algorithm $\mathcal{K}$ on input 1^k outputs a private key K. The encryption algorithm $\mathcal{E}$ on inputs K and a message $m \in \mathsf{Msg}(1^k)$ outputs a ciphertext c. The deterministic decryption algorithm $\mathcal{D}$ on inputs K and ciphertext c outputs

Game $\mathcal{AE}^{A,1}_{\mathsf{SE}}(k)$	**Game** $\mathcal{AE}^{A,0}_{\mathsf{SE}}(k)$
$K \leftarrow\!\!\$\ \mathcal{K}(1^k)$	$K \leftarrow\!\!\$\ \mathcal{K}(1^k)$
$b' \leftarrow\!\!\$\ A^{\mathcal{E}_K(\cdot),\mathcal{V}_K(\cdot)}(1^k)$	$b' \leftarrow\!\!\$\ A^{\$(\cdot),\perp(\cdot)}(1^k)$
Return b'	Return b'
Oracle $\mathcal{E}_K(m)$	**Oracle** $\$(m)$
$c \leftarrow\!\!\$\ \mathcal{E}_K(m)$	$c \leftarrow\!\!\$\ \mathcal{E}_K(m)$
Return c	$u \leftarrow\!\!\$\ \{0,1\}^{\lvert c\rvert}$
Oracle $\mathcal{V}_K(c)$	Return u
$m \leftarrow \mathcal{D}_K(c)$	**Oracle** $\perp(c)$
If $m = \perp$ return 0	Return $\perp$
Return 1	

Fig. 1: **Games to define $\mathcal{AE}$ for private-key encryption.**

a message m or $\perp$. We require that for all $K \in [\mathcal{K}(1^k)]$ and all $m \in \mathsf{Msg}(1^k)$, $\mathcal{D}_K(\mathcal{E}_K(m)) = m$ with probability 1.

Authenticated encryption. Let $\mathsf{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be a symmetric key encryption scheme. To define authenticated encryption [9], we give a combined definition of privacy and authenticity following Rogaway and Shrimpton [67]. Let A be an adversary. For every $k \in \mathbb{N}$, the experiments in Fig. 1 define the AE game. Define the *AE-advantage* of A against SE as

$$\mathbf{Adv}^{\mathrm{ae}}_{\mathsf{SE},A}(k) = \left|\Pr\left[\mathcal{AE}^{A,1}_{\mathsf{SE}}(k) \Rightarrow 1\right] - \Pr\left[\mathcal{AE}^{A,0}_{\mathsf{SE}}(k) \Rightarrow 1\right]\right| .$$

We say that SE is AE-secure if $\mathbf{Adv}^{\mathrm{ae}}_{\mathsf{SE},A}(k)$ is negligible in k for all PPT A.

Public-key encryption. A *public-key encryption scheme* PKE is a tuple of algorithms $(\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec})$, with message space Msg and coin space Coins. The key-generation algorithm Kg on input 1^k outputs a public key pk and matching secret key sk. The encryption algorithm Enc on inputs pk and a message $m \in \mathsf{Msg}(1^k)$ outputs a ciphertext c. The deterministic decryption algorithm Dec on inputs sk and ciphertext c outputs a message m or $\perp$. We require that for all $(pk, sk) \in [\mathsf{Kg}(1^k)]$ and all $m \in \mathsf{Msg}(1^k)$, $\mathsf{Dec}(sk, (\mathsf{Enc}(pk, m)) = m$ with probability 1. When multiple primitives are being used, algorithms of PKE will be denoted $\mathsf{PKE.Kg}$, $\mathsf{PKE.Enc}$, etc. to avoid confusion.

Privacy of public-key encryption [45, 66]. Let $\mathsf{PKE} = (\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec})$ be a public key encryption scheme and let $A = (A_1, A_2)$ be an adversary. Let $\mathcal{M}$ be a PPT algorithm that takes inputs 1^k and a public key pk to return a message $m \in \mathsf{Msg}(1^k)$. For all $k \in \mathbb{N}$ and ATK $\in$ {CPA, CCA1, CCA2}, the experiment in Fig. 2 (left) defines the IND-ATK security game. The *ind-atk advantage* of A against PKE is defined as

$$\mathbf{Adv}^{\text{ind-atk}}_{\mathsf{PKE},A}(k) = 2 \cdot \Pr\left[\text{IND-ATK}^{A}_{\mathsf{PKE}}(k) \Rightarrow 1\right] - 1 .$$

Game IND-ATK$^{A}_{\mathsf{PKE}}(k)$	**Game** OW-PCA$^{A}_{\mathsf{PKE}}(k)$
$b \leftarrow\!\!\$\ \{0,1\}$; $(pk, sk) \leftarrow\!\!\$\ \mathsf{Kg}(1^k)$	$(pk, sk) \leftarrow\!\!\$\ \mathsf{Kg}(1^k)$
$(st, m_0, m_1) \leftarrow\!\!\$\ A_1^{\mathcal{O}_1(\cdot)}(1^k, pk)$	$m \leftarrow\!\!\$\ \mathsf{Msg}(1^k)$; $r \leftarrow\!\!\$\ \mathsf{Coins}(1^k)$
$c \leftarrow\!\!\$\ \mathsf{Enc}(pk, m_b)$	$c \leftarrow \mathsf{Enc}(pk, m; r)$
$b' \leftarrow\!\!\$\ A_2^{\mathcal{O}_2(\cdot)}(st, pk, c)$	$m' \leftarrow\!\!\$\ A^{\mathsf{PCO}_{sk}(\cdot,\cdot)}(pk, c)$
Return $(b = b')$	If $m = m'$ then return 1
	Else return 0

Fig. 2: **Games to define** IND-ATK **(left) and** OW-PCA **(right) security for public-key encryption.**

If atk = cpa, then $\mathcal{O}_1(\cdot) = \varepsilon$ and $\mathcal{O}_2(\cdot) = \varepsilon$. In this case, we say PKE is *secure against chosen-plaintext attack* (IND-CPA) if $\mathbf{Adv}^{\text{ind-cpa}}_{\mathsf{PKE},A}(k)$ is negligible in k for all PPT A.
Similarly, if atk = cca1, then $\mathcal{O}_1(\cdot) = \mathsf{Dec}(sk, \cdot)$, and $\mathcal{O}_2(\cdot) = \varepsilon$; if atk = cca2, then $\mathcal{O}_1(\cdot) = \mathsf{Dec}(sk, \cdot)$, and $\mathcal{O}_2(\cdot) = \mathsf{Dec}(sk, \cdot)$. In the case of cca2, A_2 is not allowed to ask $\mathcal{O}_2$ to decrypt c. We say that PKE is secure against non-adaptive chosen-ciphertext attack or IND-CCA1 (resp. adaptive chosen-ciphertext attack or IND-CCA2), if $\mathbf{Adv}^{\text{ind-cca1}}_{\mathsf{PKE},A}(k)$ (resp. $\mathbf{Adv}^{\text{ind-cca2}}_{\mathsf{PKE},A}(k)$) is negligible in k for all PPT A.

One-wayness under plaintext checking attack. Let $\mathsf{PKE} = (\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec})$ be a public key encryption scheme. For every $k \in \mathbb{N}$, the experiment in Fig. 2 (right) defines the OW-PCA security game. We say PKE is OW-PCA secure if for any PPT adversary A

$$\mathbf{Adv}^{\text{ow-pca}}_{\mathsf{PKE},A}(k) = \Pr\left[\,\text{OW-PCA}^{A}_{\mathsf{PKE}}(k) \Rightarrow 1\,\right] ,$$

is negligible in k. Here $\mathsf{PCO}_{sk}(\cdot,\cdot)$ is the plaintext-checking oracle that on input (c, m) outputs 1 iff $\mathsf{Dec}(sk, c) = m$. We say that PKE is *sub-exponentially* OW-PCA if for every PPT A we have $\mathbf{Adv}^{\text{ow-pca}}_{\mathsf{PKE},A}(k) = O(2^{-k^{\alpha}})$ for a constant $0 \leq \alpha \leq 1$.

2.3 Trapdoor Permutations and Their Security

Trapdoor permutations. A trapdoor permutation (TDP) family with domain $\mathsf{T.Dom}$ is a tuple of algorithms $\mathcal{F} = (\mathsf{Kg}, \mathsf{Eval}, \mathsf{Inv})$. Algorithm Kg on input 1^k outputs a pair (F, F^{-1}), where $F\colon \mathsf{T.Dom}(k) \to \mathsf{T.Dom}(k)$. Algorithm Eval on inputs a function F and $x \in \mathsf{T.Dom}(k)$ outputs $y \in \mathsf{T.Dom}(k)$. We often write $F(x)$ instead of $\mathsf{Eval}(F, x)$. Algorithm Inv on inputs a function F^{-1} and $y \in \mathsf{T.Dom}(k)$ outputs $x \in \mathsf{T.Dom}(k)$. We often write $F^{-1}(y)$ instead of $\mathsf{Inv}(F^{-1}, y)$. We require that for any $(F, F^{-1}) \in [\mathsf{Kg}(1^k)]$ and any $x \in \mathsf{T.Dom}(k)$, $F^{-1}(F(x)) = x$.

One-wayness. Let $\mathcal{F} = (\mathsf{Kg}, \mathsf{Eval}, \mathsf{Inv})$ be a trapdoor permutation family with domain $\mathsf{T.Dom}$. We say $\mathcal{F}$ is *one-way* if for every PPT inverter I

$$\mathbf{Adv}^{\mathrm{owf}}_{\mathcal{F},I}(k) = \Pr_{\substack{(F,F^{-1}) \leftarrow\$ \mathsf{Kg}(1^k) \\ x \leftarrow\$ \mathsf{T.Dom}(k)}} \left[\begin{array}{c} x' \leftarrow I(F, F(x)) \\ x' = x \end{array} \right] \leq \mathsf{negl}(k) \ .$$

Partial one-wayness [38]. Let $\mathcal{F} = (\mathsf{Kg}, \mathsf{Eval}, \mathsf{Inv})$ be a trapdoor permutation family with domain $\mathsf{T.Dom}$. We say $\mathcal{F}$ is $(\mu, \mu+\zeta)$-*partial one way* ($(\mu, \mu+\zeta)$-POW) if for every PPT inverter I

$$\mathbf{Adv}^{\mathrm{pow}}_{\mathcal{F},I}(k) = \Pr_{\substack{(F,F^{-1}) \leftarrow\$ \mathsf{Kg}(1^k) \\ x \leftarrow\$ \mathsf{T.Dom}(k)}} \left[\begin{array}{c} x' \leftarrow I(F, F(x)) \\ x' = x|_{\mu}^{\mu+\zeta} \end{array} \right] \leq \mathsf{negl}(k) \ .$$

We additionally say that $\mathcal{F}$ is sub-exponentially $(\mu, \mu+\zeta)$-POW if for all PPT inverters I and all $k \in \mathbb{N}$, there exists some constant $0 < \alpha < 1$ such that the advantage of I is bounded by $O(2^{-k^{\alpha}})$. Fujisaki *et al.* [38] show that in the case of RSA one-wayness implies partial one-wayness.

2.4 Algebraic Properties of RSA

We recall algebraic properties of RSA that hold in the low-exponent regime for appropriate parameters. For generality of our results, we state them for abstract TDPs. We adapt them from Cao *et al.* [29].

Second-input extractability. Informally, a TDP is SIE if there is an efficient extractor that given a TDP function F, an image $F(x)$, and some portion of the preimage, can return the entire preimage. Formally: Let $\mathcal{F} = (\mathsf{Kg}, \mathsf{Eval}, \mathsf{Inv})$ be a trapdoor permutation family with domain $\{0,1\}^n$. For $1 \leq i \leq j \leq n$, we say $\mathcal{F}$ is (i,j)-*second-input-extractable* ((i,j)-SIE) if there exists an efficient extractor $\mathcal{E}$ such that for every $k \in \mathbb{N}$, every $F \in [\mathsf{Kg}(1^k)]$, and every $x \in \{0,1\}^n$, extractor $\mathcal{E}$ on inputs $F, F(x), x|_{i+1}^{j}$ outputs x. We often write ζ-SIE instead of $(n-\zeta, n)$-SIE.

Common-inputs extractability. Informally, a TDP is CIE if there is an efficient extractor that on inputs an instance of the TDP family F, two image points $F(x_1), F(x_2)$, returns the preimages x_1, x_2 if a run of bits of both preimages are equal. Formally: Let $\mathcal{F} = (\mathsf{Kg}, \mathsf{Eval}, \mathsf{Inv})$ be a trapdoor permutation family with domain $\mathsf{T.Dom}$. For $1 \leq i \leq j \leq n$, we say $\mathcal{F}$ is (i,j)-*common-input-extractable* ((i,j)-CIE) if there exists an efficient extractor $\mathcal{E}$ such that for every $k \in \mathbb{N}$, every $F \in [\mathsf{Kg}(1^k)]$, and every $x_1, x_2 \in \mathsf{T.Dom}$, extractor $\mathcal{E}$ on inputs $F, F(x_1), F(x_2)$ outputs (x_1, x_2) if $x_1|_{i+1}^{j} = x_2|_{i+1}^{j}$. We often write ζ-CIE instead of $(n-\zeta, n)$-CIE.

Parameters. Barthe *et al.* [4] show via the univariate Coppersmith algorithm [31] that RSA is ζ-SIE and ζ-CIE for sufficiently large ζ. Specifically, they show RSA is ζ_1-SIE for $\zeta_1 > n(e-1)/e$, and ζ_2-CIE for $\zeta_2 > n(e^2-1)/e^2$. Cao *et al.* [29] show a generalization to runs of arbitrary consecutive bits using the (heuristic)

bivariate Coppersmith algorithm [17, 31, 32]. Specifically, they show that RSA is (i,j)-SIE for $(j-i) > n(e-1)/e$, and (i,j)-CIE for $(j-i) > n(e^2-1)/e^2$, assuming the bivariate Coppersmith algorithm is efficient. Although its efficiency is heuristic, it works well in practice [16, 20, 35, 57].

2.5 Function Families and Associated Security Notions

Function families. A function family with domain $\mathsf{F.Dom}$ and range $\mathsf{F.Rng}$ is a tuple of algorithms $\mathcal{F} = (\mathcal{K}_F, F)$ that work as follows. Algorithm $\mathcal{K}_F$ on input a unary encoding of the security parameter 1^k outputs a key K_F. Deterministic algorithm F on inputs K_F and $x \in \mathsf{F.Dom}(k)$ outputs $y \in \mathsf{F.Rng}(k)$. We alternatively write $\mathcal{F}$ as a function $\mathcal{F}\colon \mathcal{K}_F \times \mathsf{F.Dom} \to \mathsf{F.Rng}$.

One-wayness extractors. Let $\mathcal{F}\colon \mathcal{K}_F \times \mathsf{F.Dom} \to \mathsf{F.Rng}$ be a function family. We say $\mathcal{F}$ is a *one-wayness extractor* [52] if for any PPT adversary A and any unpredictable distribution D we have

$$\mathbf{Adv}^{\mathsf{cdist}}_{\mathcal{F},A,D} = |\Pr[A(K_F, z, F(K_F, x)) = 1] - \Pr[A(K_F, z, R) = 1]| \ ,$$

is negligible in k, where $K_F \leftarrow\!\!\$\ \mathcal{K}_F(1^k)$, $(z,x) \leftarrow\!\!\$\ D_k$, and $R \leftarrow\!\!\$\ \mathsf{F.Rng}(k)$.

We additionally say that $\mathcal{F}$ is a sub-exponential one-wayness extractor if for any PPT adversary A, any sub-exponentially unpredictable distribution D and all $k \in \mathbb{N}$, there exists some constant $0 < \alpha < 1$ such that the advantage of A is bounded by $O(2^{-k^\alpha})$.

We explain how to build a sub-exponential one-wayness extractor, which is essentially a sub-exponentially secure universal hardcore function. The construction due to Bellare *et al.* [13] from diO + PPRFs has polynomial output length as desired. The form of diO needed has short auxiliary input, evading impossibility results of [42]. Moreover, the construction is sub-exponentially secure if the underlying primitives are also. It is not clear how to make an alternative construction from ELFs [72] sub-exponentially secure. However, it suffices for public-key-independent messages in our results.

2.6 The OAEP Transform

Padding scheme. We define a general notion of a padding scheme following [11, 61]. For $\nu, \rho, \mu \in \mathbb{N}$, the associated *padding scheme* is a triple of algorithms $\mathsf{PAD} = (\Pi, \mathsf{PAD}, \mathsf{PAD}^{-1})$ defined as follows. Algorithm Π on input 1^k outputs a pair $(\pi, \hat{\pi})$ where $\pi : \{0,1\}^{\mu+\rho} \to \{0,1\}^\nu$ and $\hat{\pi} : \{0,1\}^\nu \to \{0,1\}^\mu \cup \{\bot\}$ such that π is injective and for all $m \in \{0,1\}^\mu$ and $r \in \{0,1\}^\rho$ we have $\hat{\pi}(\pi(m\|r)) = m$. Algorithm PAD on inputs π and $m \in \{0,1\}^\mu$ outputs $y \in \{0,1\}^\nu$. Algorithm PAD^{-1} on inputs a mapping $\hat{\pi}$ and $y \in \{0,1\}^\nu$ outputs $m \in \{0,1\}^\mu$ or $\bot$.

Padding-based encryption. Let PAD be a padding transform from domain $\{0,1\}^{\mu+\rho}$ to range $\{0,1\}^\nu$. Let $\mathcal{F}$ be a TDP with domain $\{0,1\}^\nu$. The associated *padding-based encryption scheme* is a triple of algorithms $\mathsf{PAD}[\mathcal{F}] = (\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec})$ defined in Fig. 3.

$\underline{\mathsf{Kg}(1^k)}$	$\underline{\mathsf{Enc}(pk, m\|\|r)}$	$\underline{\mathsf{Dec}(sk, c)}$
$(\pi, \hat{\pi}) \leftarrow\!\!\$\ \Pi$	$(\pi, F) \leftarrow pk$	$(\hat{\pi}, F^{-1}) \leftarrow sk$
$(F, F^{-1}) \leftarrow\!\!\$\ \mathsf{Kg}(1^k)$	$y \leftarrow \pi(m\|\|r)$	$y \leftarrow F^{-1}(c)$
$pk \leftarrow (\pi, F)$	$c \leftarrow F(y)$	$m \leftarrow \hat{\pi}(y)$
$sk \leftarrow (\hat{\pi}, F^{-1})$	Return c	Return m
Return (pk, sk)		

Fig. 3: **Padding based encryption scheme** $\mathsf{PAD}[\mathcal{F}] = (\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec})$**.**

Algorithm $\mathsf{OAEP}_{(K_G, K_H)}(m\|r)$	**Algorithm** $\mathsf{OAEP}^{-1}_{(K_G, K_H)}(x)$
$s \leftarrow (m\|0^\zeta) \oplus G(K_G, r)$	$s\|t \leftarrow x\ ;\ r \leftarrow t \oplus H(K_H, s)$
$t \leftarrow r \oplus H(K_H, s)$	$m' \leftarrow s \oplus G(K_G, r)$
$x \leftarrow s\|t$	If $m'|_\zeta = 0^\zeta$ then return $m'|^\mu$
Return x	Return $\perp$

Fig. 4: **OAEP padding scheme** $\mathsf{OAEP}[\mathcal{G}, \mathcal{H}]$**.**

OAEP PADDING SCHEME. We recall the OAEP padding scheme [11]. Let message length μ, randomness length ρ, and redundancy length ζ be integer parameters, and $\nu = \mu + \rho + \zeta$. Let $\mathcal{G}\colon \mathcal{K}_G \times \{0,1\}^\rho \to \{0,1\}^{\mu+\zeta}$ and $\mathcal{H}\colon \mathcal{K}_H \times \{0,1\}^{\mu+\zeta} \to \{0,1\}^\rho$ be function families. The associated *OAEP padding scheme* is a triple of algorithms $\mathsf{OAEP}[\mathcal{G}, \mathcal{H}] = (\mathcal{K}_{\mathsf{OAEP}}, \mathsf{OAEP}, \mathsf{OAEP}^{-1})$ defined as follows. On input 1^k, $\mathcal{K}_{\mathsf{OAEP}}$ returns (K_G, K_H) where $K_G \leftarrow\!\!\$\ \mathcal{K}_G(1^k)$ and $K_H \leftarrow\!\!\$\ \mathcal{K}_H(1^k)$, and $\mathsf{OAEP}, \mathsf{OAEP}^{-1}$ are as defined in Fig. 4.

OAEP ENCRYPTION SCHEME. As in Fig. 3, we denote by $\mathsf{OAEP}[\mathcal{G}, \mathcal{H}, \mathcal{F}] = (\mathsf{OAEP.Kg}, \mathsf{OAEP.Enc}, \mathsf{OAEP.Dec})$ the OAEP-based encryption scheme $\mathcal{F}$-OAEP with $n = \nu$. We typically think of $\mathcal{F}$ as RSA, and all our results apply to this case under suitable assumptions.

2.7 The Fujisaki-Okamoto Transform

The Fujisaki-Okamoto (FO) transformation [36, 37] is a technique to convert weak public-key encryption schemes into strong ones which resist chosen-ciphertext attack (i.e., are IND-CCA2 secure). Let $\mathsf{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be a private-key encryption scheme and let $\mathsf{PKE} = (\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec})$ be a public-key encryption scheme. Assume $\mathcal{K}(1^k)$ outputs a key $K \in \{0,1\}^k$ and $\mathsf{PKE.Coins} \subseteq \mathsf{PKE.Msg}$. Moreover, let $\mathcal{H}\colon \mathcal{K}_H \times \mathsf{H.Dom} \to \mathsf{H.Rng}$ and $\mathcal{G}\colon \mathcal{K}_G \times \mathsf{PKE.Coins} \to \{0,1\}^k$ be hash function families. The FO transform $\mathsf{FO}[\mathcal{H}, \mathcal{G}, \mathsf{PKE}, \mathsf{SE}] = (\mathsf{FO.Kg}, \mathsf{FO.Enc}, \mathsf{FO.Dec})$ is defined in Fig. 5.

2.8 Program Obfuscation

Here we present three different types of obfuscation used in this paper. We start by recalling the definition of indistinguishability obfuscation from [3, 41].

$\underline{\mathsf{FO.Kg}(1^k)}$	$\underline{\mathsf{FO.Enc}(pk, m; r)}$	$\underline{\mathsf{FO.Dec}(sk, c)}$
$(pk', sk') \leftarrow\!\!\$\ \mathsf{PKE.Kg}(1^k)$	$(pk', K_H, K_G) \leftarrow pk$	$(sk', K_H, K_G) \leftarrow sk$
$K_H \leftarrow\!\!\$\ \mathcal{K}_H(1^k)$	$y \leftarrow H(K_H, r)$	$r \leftarrow \mathsf{PKE.Dec}(sk', c_1)$
$K_G \leftarrow\!\!\$\ \mathcal{K}_G(1^k)$	$c_1 \leftarrow \mathsf{PKE.Enc}(pk', r; y)$	If $r = \perp$ then return $\perp$
$pk \leftarrow (pk', K_H, K_G)$	$K \leftarrow G(K_G, r)$	$c_1' \leftarrow \mathsf{PKE.Enc}(pk', r; H(K_H, r))$
$sk \leftarrow (sk', K_H, K_G)$	$c_2 \leftarrow\!\!\$\ \mathcal{E}^{\mathsf{sy}}_K(m)$	If $c_1' \neq c_1$ then return $\perp$
Return (pk, sk)	$c \leftarrow (c_1, c_2)$	$K \leftarrow G(K_G, r)$
	Return c	$m \leftarrow \mathcal{D}^{\mathsf{sy}}_K(c_2)$
		Return m

Fig. 5: **FO transform** $\mathsf{FO}[\mathcal{H}, \mathcal{G}, \mathsf{PKE}, \mathsf{SE}] = (\mathsf{FO.Kg}, \mathsf{FO.Enc}, \mathsf{FO.Dec})$.

Indistinguishability obfuscation. A PPT algorithm iO is called an indistinguishability obfuscator for a circuit ensemble $\mathcal{C} = \{\mathcal{C}_k\}_{k\in\mathbb{N}}$ if the following conditions hold:

- **Correctness:** For all security parameters $k \in \mathbb{N}$, for all $C \in \mathcal{C}_k$, and for all inputs x, we have that

$$\Pr\left[\, C'(x) = C(x) : C' \leftarrow\!\!\$\ \mathsf{iO}(1^k, C) \,\right] = 1 \ .$$

- **Security:** For any PPT distinguisher D, for all pairs of circuits $C_0, C_1 \in \mathcal{C}_k$ such that $|C_0| = |C_1|$ and $C_0(x) = C_1(x)$ on all inputs x, we have that

$$\begin{aligned}\mathbf{Adv}^{\mathsf{io}}_{\mathsf{iO},D,\mathcal{C}}(k) &= |\Pr\left[\, D(1^k, \mathsf{iO}(1^k, C_0)) = 1 \,\right] - \Pr\left[\, D(1^k, \mathsf{iO}(1^k, C_1)) = 1 \,\right]| \\ &\leq \mathsf{negl}(k) \ .\end{aligned}$$

One can also represent security as a game that picks a random bit b and gives the adversary, who can make exactly one query, oracle access to $\mathsf{iO}(\mathsf{LR}(\cdot,\cdot,b))$. Both circuits in the query must be the same size and functionally equivalent.

We additionally say that iO is a sub-exponentially indistinguishability obfuscator for a circuit ensemble $\mathcal{C} = \{\mathcal{C}_k\}_{k\in\mathbb{N}}$ if for every PPT distinguisher D, for all $k \in \mathbb{N}$ and for all pairs of functionally equivalent circuits $C_0, C_1 \in \mathcal{C}_k$, there exists some constant $0 < \alpha < 1$ such that the advantage of D is bounded by $O(2^{-k^\alpha})$.

We now formalize the definition of unpredictable distributions which are used to define obfuscators for point functions.

Computationally unpredictable distribution. We call distribution ensemble $\mathcal{D} = \{D_k = (Z_k, X_k)\}_{k\in\mathbb{N}}$, on tuples of strings, computationally unpredictable (cup) if for every PPT algorithm A, we have

$$\Pr\left[\, A(1^k, z) \Rightarrow x : \ (z, x) \leftarrow\!\!\$\ D_k \,\right] \leq \mathsf{negl}(k) \ .$$

We call it *sub-exponentially unpredictable* if there exists some constant $0 < \alpha < 1$ such that the above probability is bounded by $O(2^{-k^\alpha})$.

Statistically unpredictable distributions. We call distribution ensemble $\mathcal{D} = \{D_k = (Z_k, X_k)\}_{k\in\mathbb{N}}$, on tuples of strings, statistically unpredictable (sup) if for every (even unbounded) algorithm A, we have that

$$\Pr\left[\, A(1^k, z) \Rightarrow x : \ (z, x) \leftarrow\!\!\$\ D_k \,\right] \leq \mathsf{negl}(k) \ .$$

Point obfuscation with auxiliary information. Although indistinguishability obfuscation applies to general circuits, we can also study obfuscation schemes for particular classes of functions, such as point functions. A point function p_x for some value x is defined as follows: $p_x(\tilde{x}) = 1$ iff $\tilde{x} = x$ and equals $\perp$ otherwise.

We now give the definition of point function obfuscation following [15]. A PPT algorithm AIPO is a point function obfuscator for the class of distributions $\mathcal{D} = \{D_k = (Z_k, X_k)\}_{k\in\mathbb{N}}$, where X_k is the input point distribution and Z_k is the auxiliary information distribution, if the following conditions hold:

- **Correctness:** For all security parameters $k \in \mathbb{N}$, for all $(z, x) \leftarrow\!\!\$\ D_k$, AIPO on input x outputs a polynomial-size circuit p_x that returns 1 on x and $\perp$ everywhere else.
- **Security:** To distinguisher A we associate the experiment in Fig. 6, for every $k \in \mathbb{N}$. We require that for every PPT distinguisher A

$$\mathbf{Adv}^{\text{aipo}}_{\mathsf{AIPO},A,D}(k) = 2 \cdot \Pr\left[\, \text{AIPO}^{D,A}_{\mathsf{AIPO}}(k) \Rightarrow 1 \,\right] - 1 \leq \mathsf{negl}(k) \ .$$

Sub-exponential security. We additionally say AIPO is a *sub-exponentially secure* point obfuscator if for any sub-exponentially unpredictable distribution ensemble $\{D_k = (Z_k, X_k)\}_{k\in\mathbb{N}}$ there exists some constant $\alpha > 0$ such that for every PPT A, and for all $k \in \mathbb{N}$, the advantage of every PPT adversary A is bounded by $O(2^{-k^\alpha})$.

Auxiliary-input point obfuscation with multi-bit output. A multi-bit point function $p_{x,y}$ is similar to a regular point function p_x in that $\perp$ is returned for all inputs $x' \neq x$. But unlike p_x, which just returns a single bit 1 input x, $p_{x,y}$ returns the multi-bit string y.

A PPT algorithm $\mathsf{MB\text{-}AIPO}$ is a multi-bit point obfuscator for the distribution ensemble $\mathcal{D} = \{D_k = (Z_k, X_k, Y_k)\}_{k\in\mathbb{N}}$, on triples of strings, if the following conditions hold:

- **Correctness:** For all security parameters $k \in \mathbb{N}$, for all $(z, x, y) \leftarrow\!\!\$\ D_k$, $\mathsf{MB\text{-}AIPO}$ on input x, y outputs a polynomial-size circuit that returns y on x and $\perp$ on all other inputs.
- **Security:** To distinguisher A, we associate the experiment in Fig. 6, for every $k \in \mathbb{N}$. We require that for every PPT distinguisher A,

$$\mathbf{Adv}^{\text{mb-aipo}}_{\mathsf{MB\text{-}AIPO},A,\mathcal{D}}(k) = 2 \cdot \Pr\left[\, \text{MB-AIPO}^{\mathcal{D},A}_{\mathsf{MB\text{-}AIPO}}(k) \Rightarrow 1 \,\right] - 1 \leq \mathsf{negl}(k) \ .$$

Game $\text{AIPO}^{\mathcal{D},A}_{\mathsf{AIPO}}(k)$	**Game** $\text{MB-AIPO}^{\mathcal{D},A}_{\mathsf{MB\text{-}AIPO}}(k)$
$b \leftarrow\!\!\$\ \{0,1\}\ ;\ (z, x_0) \leftarrow\!\!\$\ D_k$	$b \leftarrow\!\!\$\ \{0,1\}\ ;\ (z, x, y_0) \leftarrow\!\!\$\ D_k$
$x_1 \leftarrow\!\!\$\ \{0,1\}^{\lvert x_0\rvert}$	$y_1 \leftarrow\!\!\$\ \{0,1\}^{\lvert y_0\rvert}$
$p \leftarrow\!\!\$\ \mathsf{AIPO}(x_b)$	$p \leftarrow\!\!\$\ \mathsf{MB\text{-}AIPO}(x, y_b)$
$b' \leftarrow\!\!\$\ A(1^k, z, p)$	$b' \leftarrow\!\!\$\ A(1^k, z, p)$
Return $(b = b')$	Return $(b = b')$

Fig. 6: **Games to define AIPO (left) and MB-AIPO (right) security.**

Game $\text{PRF-DIST}^{A}_{\mathsf{PRF}}(k)$
$b \leftarrow\!\!\$\ \{0,1\}\ ;\ (S, st) \leftarrow\!\!\$\ A_1(1^k)$
$K \leftarrow\!\!\$\ \mathsf{PRF.Kg}(1^k)$
$K_S \leftarrow\!\!\$\ \mathsf{PRF.Punct}(K, S)$
$\mathbf{y}_0 \leftarrow \mathsf{PRF.Eval}(K, S)$
$\mathbf{y}_1 \leftarrow\!\!\$\ \mathsf{PRF.Rng}(k)^{\times \lvert S\rvert}$
$b' \leftarrow\!\!\$\ A_2(st, S, K_S, \mathbf{y}_b)$
Return $(b = b')$

Fig. 7: **Game to define PRF-DIST security.**

We omit definitions of unpredictability and sub-exponential security in the context of MB-AIPOs since they extend naturally from their AIPO counterparts. Although we will note that in the case of MB-AIPO the unpredictable sampling distribution has the form $\mathcal{D} = \{D_k = (Z_x, X_k, Y_k)\}_{k\in\mathbb{N}}$ where Y_k represents the multi-bit output point. Unpredictability is defined the same way as above, in particular, the attacker is not given the point sampled from Y_k, nor are they required to predict it. MB-AIPO for computationally unpredictable auxiliary inputs is likely impossible in general [24]. Our choice is therefore to use statistical unpredictability or assume MB-AIPO for a *specific* computationally unpredictable auxiliary input.

2.9 Puncturable PRFs

A family of puncturable pseudorandom functions (PPRFs) [21, 59, 68] with domain $\mathsf{PRF.Dom}$ and range $\mathsf{PRF.Rng}$ is a tuple of algorithms $\mathsf{PRF} = (\mathsf{PRF.Kg}, \mathsf{PRF.Punct}, \mathsf{PRF.Eval})$ that work as follows. Algorithm $\mathsf{PRF.Kg}$ on input 1^k outputs a key K. Algorithm $\mathsf{PRF.Eval}$ takes as inputs a key K and $x \in \mathsf{PRF.Dom}(k)$ and outputs $y \in \mathsf{PRF.Rng}(k)$. We often write $\mathsf{PRF}_K(x)$ instead of $\mathsf{PRF.Eval}(K, x)$. Additionally, there is a PPT puncturing algorithm $\mathsf{PRF.Punct}$ which on inputs a key K and a polynomial-size set $S \subseteq \mathsf{PRF.Dom}(k)$, outputs a special, punctured key K_S. We say PRF is puncturable PRF if the following two properties hold:

– **Functionality preserved under puncturing:** For every PPT adversary $A = (A_1, A_2)$ such that adversary $A_1(1^k)$ outputs a polynomial-size set $S \subseteq$

$\mathsf{PRF.Dom}(k)$, it holds for all $x \in \mathsf{PRF.Dom}(k)$ where $x \notin S$ that

$$\Pr[\mathsf{PRF.Eval}(K, x) = \mathsf{PRF.Eval}(K_S, x) : K \leftarrow\!\!\$\ \mathsf{PRF.Kg}(1^k),\ K_S \leftarrow\!\!\$\ \mathsf{PRF.Punct}(K, S)] = 1 \ .$$

– **Pseudorandom at punctured points:** To attacker $A = (A_1, A_2)$, we associate the experiment in Fig. 7 for every $k \in \mathbb{N}$. We require that for every PPT adversary $A = (A_1, A_2)$,

$$\mathbf{Adv}^{\mathrm{pprf}}_{\mathsf{PRF},A}(k) = 2 \cdot \Pr\left[\,\text{PRF-DIST}^{A}_{\mathsf{PRF}}(k) \Rightarrow 1\,\right] - 1 \leq \mathsf{negl}(k) \ .$$

The works [21, 59, 68] construct PPRFs from one-way functions.

2.10 Extremely Lossy Functions

A family of extremely lossy functions (ELFs) ELF with domain $\mathsf{ELF.Dom}$ and range $\mathsf{ELF.Rng}$ is a tuple of algorithms $\mathsf{ELF} = (\mathsf{ELF.IKg}, \mathsf{ELF.LKg}, \mathsf{ELF.Eval})$ that work as follows. Algorithm $\mathsf{ELF.IKg}$ on input 1^k outputs the description of a function $f\colon \mathsf{ELF.Dom}(k) \to \mathsf{ELF.Rng}(k)$. Algorithm $\mathsf{ELF.LKg}$ on inputs 1^k and polynomial r outputs the description of a function $f\colon \mathsf{ELF.Dom}(k) \to \mathsf{ELF.Rng}(k)$. Algorithm $\mathsf{ELF.Eval}$ on inputs a function f and $x \in \mathsf{ELF.Dom}(k)$ outputs $y \in \mathsf{ELF.Rng}(k)$. We often write $f(x)$ instead of $\mathsf{ELF.Eval}(f, x)$. An ELF has the following properties:

– **Correctness:** For f output by (1^k), the function f is injective.
– **Key-indistinguishability:** For any polynomial p and inverse polynomial function δ, there is a polynomial q such that, for any adversary A running in time at most p, and any $r \geq q$, we have that

$$|\ \Pr[A(f) \Rightarrow 1 : f \leftarrow\!\!\$\ \mathsf{ELF.IKg}(1^k)] - \Pr[A(f) \Rightarrow 1 : f \leftarrow\!\!\$\ \mathsf{ELF.LKg}(1^k, r)]\ | < \delta \ .$$

– **Lossiness:** for all polynomials r, over $f \leftarrow\!\!\$\ \mathsf{ELF.LKg}(1^k, r)$ the function f has image of at most r.
– **Efficiently enumerable image:** For any polynomial r, let f be an output of $\mathsf{ELF.LKg}(1^k, r)$. Then on inputs f, r and in time $\mathsf{poly}(|\mathsf{ELF.Dom}|, r)$, $f([\mathsf{ELF.Dom}])$ can be output.

Zhandry gives a construction from the exponential DDH assumption.

3 Low-Exponent RSA-OAEP Instantiation

In this section, we show low-exponent (*e.g.*, $e = 3$) RSA-OAEP is fully instantiable using its algebraic properties described in Section 2.4. We leave the instantiability of high-exponent RSA-OAEP for future work.

$\underline{\mathsf{ELF}'.\mathsf{IKg}(1^k)}$	$\underline{\mathsf{ELF}'.\mathsf{LKg}(1^k, r)}$	$\underline{\mathsf{ELF}'.\mathsf{Eval}(K, f, x)}$
$f \leftarrow\!\!\$\ \mathsf{ELF.IKg}(1^k)$	$f \leftarrow\!\!\$\ \mathsf{ELF.LKg}(1^k, r)$	$y \leftarrow \mathsf{ELF.Eval}(f, x)$
$K \leftarrow\!\!\$\ \mathcal{K}_{\mathsf{PI}}(1^k)$	$K \leftarrow\!\!\$\ \mathcal{K}_{\mathsf{PI}}(1^k)$	Return $\mathsf{PRG}(\mathsf{PI}_K(y))$
Return (K, f)	Return (K, f)	

Fig. 8: **Augmented ELF construction** $\mathsf{ELF}'[\mathsf{PRG}, \mathsf{PI}, \mathsf{ELF}] = (\mathsf{ELF}'.\mathsf{IKg}, \mathsf{ELF}'.\mathsf{LKg}, \mathsf{ELF}'.\mathsf{Eval})$.

Procedure $\mathcal{K}_G(1^k)$	**Procedure** $G(K_G, x)$
$K \leftarrow\!\!\$\ \mathsf{PRF.Kg}(1^k)$	$C_G \leftarrow\!\!\$\ K_G(1^k)$
$f \leftarrow\!\!\$\ \mathsf{ELF.IKg}(1^k)$	Return $C_G(x)$
$K_G \leftarrow\!\!\$\ \mathsf{iO}(pad(s(k), f(\mathsf{PRF}_K(\cdot))))$	
Return K_G	

Fig. 9: **The hash function family** $\mathcal{G}$.

3.1 Augmented ELFs

For convenience, we define a notion of *augmented* ELFs to make the evaluation of the ELF in injective mode on a uniform input to be uniform on an appropriate *binary* range. We will need this below. The idea is to compose the ELF, f, with a pairwise-independent hash and pseudorandom generator, *i.e.* $\mathsf{PRG}(\mathsf{PI}_K(f(\cdot)))$. Namely, let $\mathsf{ELF} = (\mathsf{ELF.IKg}, \mathsf{ELF.LKg}, \mathsf{ELF.Eval})$ be an ELF, $\mathsf{PI}\colon \mathcal{K}_{\mathsf{PI}} \times \{0,1\}^n \to \{0,1\}^m$ be a function family such that $m \leq |\mathsf{ELF.Dom}| - 2\log(1/\epsilon) + 1$ for negligible ϵ, and $\mathsf{PRG}\colon \{0,1\}^m \to \{0,1\}^r$ be a function. Define the associated *augmented* ELF $\mathsf{ELF}'[\mathsf{PRG}, \mathsf{PI}, \mathsf{ELF}] = (\mathsf{ELF}'.\mathsf{IKg}, \mathsf{ELF}'.\mathsf{LKg}, \mathsf{ELF}'.\mathsf{Eval})$ as in Fig. 8.

Proposition 1. *Suppose* ELF *is a secure ELF,* PI *is pairwise-independent hash, and* PRG *is a secure PRG. Then the associated augmented ELF* $\mathsf{ELF}'[\mathsf{PRG}, \mathsf{PI}, \mathsf{ELF}]$*, as defined in Fig. 8, is such that the output of the following experiment is computationally indistinguishable from* (f', z) *where* $z \in \{0,1\}^r$ *is independent and uniform:*

$$f' \leftarrow\!\!\$\ \mathsf{ELF}'.\mathsf{IKg}(1^k)\ ;\ x \leftarrow\!\!\$\ \mathsf{ELF.Dom}(x)\ ;\ \textit{Return}\ (f', f'(x))\ .$$

This follows by first applying the Leftover Hash Lemma [47] and then the security of the PRG.

3.2 The Result

We will need MB-AIPO for the following distribution ensemble. We suggest using our new RSA-based construction in the full version of Section 5; in particular, this RSA-based obfuscator "plays well" with the auxiliary input in this case. Define the distribution ensemble $\mathcal{D}^{\mathcal{OAEP}} = \{D_k^{\mathcal{OAEP}}\}_{k\in\mathbb{N}}$ be as follows:

Distribution $D_k^{\mathcal{OAEP}}$
$r^* \leftarrow\!\!\$\ \{0,1\}^\rho\ ;\ z^* \leftarrow\!\!\$\ \{0,1\}^{\mu+\zeta}$
$K_H \leftarrow\!\!\$\ \mathcal{K}_H(1^k)\ ;\ (F, F^{-1}) \leftarrow\!\!\$\ \mathsf{Kg}(1^k)$
$m \leftarrow\!\!\$\ \{0,1\}^\mu$
$s^* \leftarrow z^* \oplus (m \| 0^\zeta)\ ;\ y^* \leftarrow H(K_H, s^*)$
$t^* \leftarrow r^* \oplus y^*\ ;\ c^* \leftarrow F(s^* \| t^*)$
$L \leftarrow (c^*, K_H, F, m)$
Return (L, r^*, z^*)

$\underline{\mathsf{OAEP.Kg}(1^k)}$	$\underline{\mathsf{OAEP.Enc}(pk, m)}$	$\underline{\mathsf{OAEP.Dec}(sk, c)}$
$K_G \leftarrow\!\!\$\ \mathcal{K}_G(1^k)$	$(F, K_G, K_H) \leftarrow pk$	$(F^{-1}, K_G, K_H) \leftarrow sk$
$K_H \leftarrow\!\!\$\ \mathcal{K}_H(1^k)$	$r \leftarrow\!\!\$\ \{0,1\}^\rho$	$s \| t \leftarrow F^{-1}(c)$
$(F, F^{-1}) \leftarrow\!\!\$\ \mathsf{Kg}(1^k)$	$z \leftarrow G(K_G, r)$	$r \leftarrow t \oplus H(K_H, s)$
$pk \leftarrow (F, K_G, K_H)$	$s \leftarrow z \oplus (m \| 0^\zeta)$	$m' \leftarrow s \oplus G(K_G, r)$
$sk \leftarrow (F^{-1}, K_G, K_H)$	$t \leftarrow r \oplus H(K_H, s)$	If $m'|_\zeta = 0^\zeta$ then return $m'|^\mu$
Return (pk, sk)	$c \leftarrow F(s \| t)$	Return $\perp$
	Return c	

Fig. 10: $\mathsf{OAEP}[\mathcal{G}, \mathcal{H}, \mathcal{F}] = (\mathsf{OAEP.Kg}, \mathsf{OAEP.Enc}, \mathsf{OAEP.Dec})$ **where $\mathcal{G}$ is defined in Fig. 9.**

Theorem 1. *Let n, μ, ζ, ρ be integer parameters. Let $\mathcal{F}$ be a family of trapdoor permutations with domain $\{0,1\}^n$, where $n = \mu + \zeta + \rho$. Assume $\mathcal{F}$ is sub-exponentially OW, $(\mu, \mu+\zeta)$-SIE, and $(\mu, \mu+\zeta)$-CIE. Assume* ELF *is a secure augmented ELF with* $\mathsf{ELF.Rng} = \{0,1\}^{\mu+\zeta}$, PRF *is a secure puncturable PRF with* $\mathsf{PRF.Dom} = \{0,1\}^\rho$, iO *is a sub-exponentially secure iO for $\mathcal{P}/poly$, and sub-exponential MB-AIPO for the distribution ensemble $\mathcal{D}^{\mathcal{OAEP}}$ exists. Let $\mathcal{G} : \mathcal{K}_G \times \{0,1\}^\rho \to \{0,1\}^{\mu+\zeta}$ and $\mathcal{H} : \mathcal{K}_H \times \{0,1\}^{\mu+\zeta} \to \{0,1\}^\rho$ be hash function families, where $\mathcal{G}$ is in Fig. 9* [6] *and $\mathcal{H}$ is a sub-exponentially secure one-wayness extractor. Then* $\mathsf{OAEP}[\mathcal{G}, \mathcal{H}, \mathcal{F}] = (\mathsf{OAEP.Kg}, \mathsf{OAEP.Enc}, \mathsf{OAEP.Dec})$*, as defined in Fig. 10, is IND-CCA2 secure.*

The full proof can be found in the full version of the paper; below we present a proof sketch. At a high-level, the idea is to change ELF to lossy mode so that a simulator can answer decryption queries by exhaustively searching the lossy image and using algebraic properties of RSA.

Game G_1: This is the standard IND-CCA2 security game, shown in Fig. 11. $\mathcal{G}$ is computed by the circuit $\mathcal{C}_1[K, f] = f(\mathsf{PRF}_K(\cdot))$ where f is in injective mode and the PRF key K is not punctured. Note that in G_1, $z^* = G(K_G, r^*)$.

Game G_2: The PRF key K is replaced with a key K^* which is punctured at r^* and the circuit $\mathcal{C}_1$ is switched to $\mathcal{C}_2$. $\mathcal{C}_2$ depends on an MB-AIPO of the point

[6] Here the function $pad(\cdot,\cdot)$ pads the circuit specified by the second argument to the length specified by the first argument. Here we implicitly set $s(k)$ to what is needed in the proof; cf. [24].

Game $G_1(k)$
$b \leftarrow\!\!\$\ \{0,1\}$; $K \leftarrow\!\!\$\ \mathsf{PRF.Kg}(1^k)$
$r^* \leftarrow\!\!\$\ \{0,1\}^\rho$; $f \leftarrow\!\!\$\ \mathsf{ELF.IKg}(1^k)$
$x^* \leftarrow \mathsf{PRF}_K(r^*)$; $z^* \leftarrow f(x^*)$
$K_G \leftarrow\!\!\$\ \mathsf{iO}(pad(\mathcal{C}_1[K, f]))$
$K_H \leftarrow\!\!\$\ \mathcal{K}_H(1^k)$; $(F, F^{-1}) \leftarrow\!\!\$\ \mathsf{Kg}(1^k)$
$pk \leftarrow (F, K_H, K_G)$; $sk \leftarrow (F^{-1}, K_H, K_G)$
$(st, m_0, m_1) \leftarrow\!\!\$\ A_1^{\mathsf{Dec}(\cdot)}(1^k, pk)$
$s^* \leftarrow z^* \oplus (m_b \| 0^\zeta)$; $y^* \leftarrow H(K_H, s^*)$
$t^* \leftarrow r^* \oplus y^*$; $c^* \leftarrow F(s^* \| t^*)$
$b' \leftarrow\!\!\$\ A_2^{\mathsf{Dec}(\cdot)}(st, pk, c^*)$
Return $(b = b')$

Fig. 11: **IND-CCA2 security game for OAEP with adversary** $A = (A_1, A_2)$**.**

function p_{r^*,z^*} so that on inputs not equal to r^*, $f(\mathsf{PRF}_{K^*}(\cdot))$ is evaluated and on input r^*, the obfuscated point function p_{r^*,z^*} is evaluated (and $p_{r^*,z^*}(r^*) = z^*$). The input-output behavior of the circuits in G_1 and G_2 are identical and they are the same size (using padding), only their descriptions differ. Since the adversary gets obfuscated versions of these circuits, games G_1 and G_2 are indistinguishable by the security of iO.

Game G_3: Previously, z^* was given by $f(\mathsf{PRF}_K(r^*))$. In G_3, r^* is defined as $f(x^*)$ where x^* is sampled randomly from the PRF range. This change is indistinguishable by the pseudorandomness at punctured points of the puncturable PRF.

Game G_4: In G_3 we had $z^* = f(x^*)$, where x^* was random. In this game, z^* is changed to a randomly sampled string from the range of G. This game is indistinguishable from the previous because f is a secure augmented ELF.

Game G_5: The circuit $\mathcal{C}_2$ now uses the un-punctured PRF key K instead of K^*, the key punctured at r^*. Like the transition to G_2, this update to $\mathcal{C}_2$ does not change its input-output behavior and is therefore undetected due to iO security.

Game G_6: By considering the running time of the IND-CCA adversary A, the ELF is switched to lossy mode. This reduces the range of $f(\mathsf{PRF}_K(\cdot))$ to polynomial size. This game also updates A_1's decryption oracle to include a "bad" flag which is silently set to true if A_1 makes a decryption query $\overline{c} = F(\overline{s} \| (\overline{r} \oplus H(K_H, \overline{s})))$, where $\overline{s} = \overline{z} \oplus (\overline{m} \| 0^\zeta)$, in which the last ζ bits of $\overline{z}$ are equal to the last ζ bits of z^*. So the bad flag condition can be written as $\overline{z}|_\zeta = z^*|_\zeta$.

This flag does not change the input-output behavior of the decryption oracle. Thus to bound the probability the switch from G_5 to G_6 is detected, we only need to invoke indistinguishability of the ELF injective and lossy modes.

Game G_7: We further update A_1's decryption oracle to return $\perp$ if the bad flag introduced in G_6 is true. Hence G_6 and G_7 follow the "identical-until-bad" of [12], allowing the game transition to be bounded by the probability bad is set.

Let us consider what it means for bad to be set to true. As stated in G_6, this occurs when A_1 queries their decryption oracle with a ciphertext $\overline{c} = F(\overline{s} \| (\overline{r} \oplus H(K_H, \overline{s})))$, where $\overline{s} = \overline{z} \oplus (\overline{m} \| 0^{\zeta})$, such that $\overline{z}|_{\zeta} = z^*|_{\zeta}$. A_1 gets as input the function F, the hash keys K_H and K_G. At this point, K_G is the circuit described in G_3 under iO. The last ζ bits of z^* are encoded in this circuit as the last ζ bits of the MB-AIPO output point (since the output point is z^*). Hence the only way A_1 can obtain z^* (with non-negligible probability) is by breaking MB-AIPO security. So, the security of the MB-AIPO is used to bound the probability the switch from G_6 to G_7 is detected.

Game G_8: In this game both A_1 and A_2's decryption oracles are changed to decrypt using only the public key (F, K_H, K_G) and no secret keys. These decryption oracles have the same input-output behavior as the oracles in G_7, and hence their change is undetectable to the adversary. Decryption without the private key is achieved by exploiting three properties: the polynomial-sized ELF range, second-input extractability (SIE), common-inputs extractability (CIE), which are algebraic properties of RSA defined by Barthe *et al.* [4] that hold due to the Coppersmith algorithm [31]; we actually use generalizations due to Cao *et al.* [29] that hold due to the bivariate Coppersmith algorithm [17, 31, 32].

First, note the polynomial ELF range allows $\overline{z} = f(\mathsf{PRF}_K(\overline{r}))$ to be found via exhaustive search instead of by using F^{-1}, *unless* $\overline{z} = z^*$*, the challenge point.* In G_7, all valid ciphertexts were decrypted by A_1's oracles except for those with $\overline{z}|_{\zeta} = z^*|_{\zeta}$. In G_8, with overwhelming probability, z^* will not be in the lossy ELF range and hence will not be found through exhaustively searching the range. So if A_1 makes a decryption query in G_8 that cannot be decrypted using exhaustive search, $\perp$ is returned. But if A_2 makes a valid query $\overline{c}$ in G_7 with $\overline{z}|_{\zeta} = z^*|_{\zeta}$, then their decryption oracle will decrypt. So to achieve this behavior in G_8 we run a CIE extractor on inputs $F, \overline{c}, c^*$. The extractor returns $\overline{s} \| \overline{t}$ and $s^* \| t^*$ if $\overline{z}|_{\zeta} = z^*|_{\zeta}$ and $\perp$ otherwise. If $\perp$ is returned then the query was not a valid ciphertext and $\perp$ is returned by the oracle. If $\overline{s} \| \overline{t}$ is returned then decryption can be completed using the hash keys.

Game G_9: In this final game the MB-AIPO output point in the circuit $\mathcal{C}_2$ is switched from z^* to random $\overline{z}$ (while z^* is still used in the formation of s^*). Since $\overline{z}$ is the MB-AIPO output point and z^* was the output point in G_8, the security of MB-AIPO is used to bound the probability the adversary detects this transition.

A_2's challenge ciphertext is $c^* = F(s^* \| (r^* \oplus H(K_H, s^*)))$ where $s^* = z^* \oplus (m_b \| 0^{\zeta})$. At this point, z^* is randomly sampled and is independent of r^*. Moreover, K_G given to A is independent of z^*. So m_b is hidden in c^* by z^* acting as a one-time-pad. So the challenge bit b is hidden and hence c^* looks random to A_2, concluding the proof sketch.

4 Fujisaki-Okamoto Instantiation

Inspired by Hofheinz, Hövelmanns, and Kiltz [49], we take a modular approach to instantiating FO. Our main contribution is to instantiate the part of the

PKE transform from OW-PCA to IND-CCA. Here we need to assume the SE is information-theoretic and leakage-resilient AE. Then we observe how to instantiate a transform from OW-CPA to OW-PCA based on prior work assuming the PKE is lossy. Composing these transforms provides an instantiation of FO under the foregoing assumptions. As a point of comparison, Matsuda and Hanaoka [62] also construct IND-CCA encryption from lossy encryption, but their construction follows a different blueprint than FO.

4.1 Cryptography with Adaptive Auxiliary Input

We define primitives in a setting where the adversary gets auxiliary information depending on the secrets. Such a setting was considered by Dodis *et al.* [33]. We further extend it to consider what we call *adaptive* auxiliary input, where the adversary is given an oracle that depends on the secrets.

Adaptive distribution ensembles. An *adaptive distribution ensemble* is a pair $(\mathcal{O}, \mathcal{D})$ where $\mathcal{O}$ is an oracle and $\mathcal{D} = \{D_k = (Z_k, X_k)\}_{k\in\mathbb{N}}$ is a distribution ensemble. We call $(\mathcal{O}, \mathcal{D})$ *adaptive computationally unpredictable* (acup) if for every PPT algorithm A,

$$\Pr\left[\, A^{\mathcal{O}(z,x,\cdot)}(1^k, z) \Rightarrow x : \ (z, x) \leftarrow\!\!\$\ D_k \,\right] \leq \mathsf{negl}(k) \ .$$

We call it *sub-exponentially unpredictable* if there exists some constant $0 < \alpha < 1$ such that the above probability is bounded by $O(2^{-k^\alpha})$. Adaptive statistically unpredictable (asup) is defined similarly.

AE with adaptive auxiliary input. Let $\mathsf{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be a private-key encryption scheme and let A be an adversary. Let $(\mathcal{O}, \mathcal{D})$ be an adaptive distribution ensemble where $\mathcal{O}$ is an oracle and distribution ensemble $\mathcal{D} = \{D_k = (Z_k, K_k)\}_{k\in\mathbb{N}}$ is such that K_k is uniform on $\mathcal{K}(1^k)$. For every $k \in \mathbb{N}$, the experiments in Fig. 12 define the AE-AUX game (where the code of $\mathcal{O}$ is elided). Define the *AE-AUX advantage* of A against SE wrt. $(\mathcal{O}, \mathcal{D})$ as

$$\mathbf{Adv}^{\text{ae-aux}}_{\mathsf{SE},A,\mathcal{O},D}(k) = \left|\Pr\left[\,\text{AE-AUX}^{A,1}_{\mathsf{SE},\mathcal{O},D}(k) \Rightarrow 1\,\right] - \Pr\left[\,\text{AE-AUX}^{A,0}_{\mathsf{SE},\mathcal{O},D}(k) \Rightarrow 1\,\right]\right| \ .$$

We say that SE is secure under AE-AUX wrt. $(\mathcal{O}, \mathcal{D})$ if $\mathbf{Adv}^{\text{ae-aux}}_{\mathsf{SE},A,\mathcal{O},D}(k)$ is negligible in k for all PPT A.

Leakage-resilient AE. Leakage resilience [2] corresponds to the case in which the oracle is empty ($\mathcal{O} = \varepsilon$) and $\mathcal{D}$ is statistically unpredictable. We are not aware if such a definition has appeared in the literature before. Leakage-resilient AE has been studied, *e.g.*, by Bartwell *et al.* [5], but they use the weaker "only computation leaks" paradigm of Micali and Reyzin [63].

MB-AIPO with adaptive auxiliary input. MB-AIPOs with adaptive auxiliary input are similarly defined wrt. adaptive distribution ensembles, meaning that in the MB-AIPO experiment (Fig. 6), A gets oracle $\mathcal{O}$. We believe this to be a natural progression of the notion, capturing the intuition that if the

Game AE-AUX$^{A,1}_{\mathsf{SE},D}(k)$	**Game** AE-AUX$^{A,0}_{\mathsf{SE},D}(k)$
$(w, K) \leftarrow\!\!\$\ D_k$	$(w, K) \leftarrow\!\!\$\ D_k$
$b' \leftarrow\!\!\$\ A^{\mathcal{E}_K(\cdot),\mathcal{V}_K(\cdot),\mathcal{O}(\cdot)}(1^k, w)$	$b' \leftarrow\!\!\$\ A^{\$(\cdot),\perp(\cdot),\mathcal{O}(\cdot)}(1^k, w)$
Return b'	Return b'
Oracle $\mathcal{E}_K(m)$	**Oracle** $\$(m)$
$c \leftarrow\!\!\$\ \mathcal{E}_K(m)$	$c \leftarrow\!\!\$\ \mathcal{E}_K(m)$
Return c	$u \leftarrow\!\!\$\ \{0,1\}^{\lvert c\rvert}$
Oracle $\mathcal{V}_K(c)$	Return u
$m \leftarrow \mathcal{D}_K(c)$	**Oracle** $\perp(c)$
If $m = \perp$ return 0	Return 0
Return 1	**Oracle** $\mathcal{O}(w, K, \cdot)$
Oracle $\mathcal{O}(w, K, \cdot)$	$\ldots$
$\ldots$	

Fig. 12: **Games to define** AE-AUX **for private-key encryption.**

input point is unpredictable relative to an oracle, the MB-AIPO is secure relative to the same oracle. The notions of acup-MB-AIPO and asup-MB-AIPO are defined naturally. Note that in this work we only consider MB-AIPOs with adaptive auxiliary input relative to *specific* adaptive distribution ensembles.

4.2 From OW-PCA to IND-CCA

Here we consider instantiability of the part of the Fujisaki-Okamoto (FO) transform that upgrades OW-PCA to IND-CCA, as in Section 3.2.2 of [49]. In the full version, we also consider insantiability of the part of the FO transform that upgrades OW-CPA to OW-PCA, showing a positive result by making the stronger assumption of lossiness [8] (compared to OW-CPA) on the base PKE scheme. In fact, we show that by assuming lossiness of the base PKE scheme, we can also construct an MB-AIPO from ELFs (mentioned in Section 5) that is secure wrt. each of the three (adaptive) distribution ensembles required in Theorem 2.

We slightly tweak the part of the Fujisaki-Okamoto (FO) transform that upgrades OW-PCA to IND-CCA, as in Section 3.2.2 of [49]. Note that this part is not subject to an uninstantiability result. Here we encrypt $m\|r$ instead of m under the symmetric encryption scheme. Our version of this part of FO, which we call $\overline{\mathsf{FO}}$, also differs from the original in that the symmetric key is set to be the hash of $r\|c_1$ (where c_1 is the asymmetric ciphertext), instead of just the hash of r, which is also done in [49]. Let $\mathsf{SE} = (\mathcal{K}^{\mathsf{sy}}, \mathcal{E}^{\mathsf{sy}}, \mathcal{D}^{\mathsf{sy}})$ and $\mathsf{PKE} = (\mathsf{PKE.Kg}, \mathsf{PKE.Enc}, \mathsf{PKE.Dec})$ be private and public-key encryption schemes, respectively. Let $\{0,1\}^k$ and $\{0,1\}^\mu$ be the SE key-space and message-space, respectively. Let $\mathcal{G}\colon K_G \times (\mathsf{PKE.Msg} \times \mathsf{PKE.Ctxt}) \to \{0,1\}^k$ be the hash function family as constructed in Fig. 14. $\overline{\mathsf{FO}}[\mathcal{G}, \mathsf{PKE}, \mathsf{SE}] = (\overline{\mathsf{FO}}.\mathsf{Kg}, \overline{\mathsf{FO}}.\mathsf{Enc}, \overline{\mathsf{FO}}.\mathsf{Dec})$ is defined in Fig. 13.

$\underline{\overline{\mathsf{FO}}.\mathsf{Kg}(1^k)}$	$\underline{\overline{\mathsf{FO}}.\mathsf{Enc}(pk, m; r)}$	$\underline{\overline{\mathsf{FO}}.\mathsf{Dec}(sk, c)}$
$(pk', sk') \leftarrow\!\!\$\ \mathsf{PKE}.\mathsf{Kg}(1^k)$	$(pk', K_G) \leftarrow pk$	$(c_1, c_2) \leftarrow c\,;\ (sk', K_G) \leftarrow sk$
$K_G \leftarrow\!\!\$\ \mathcal{K}_G(1^k)$	$z \leftarrow\!\!\$\ \mathsf{PKE}.\mathsf{Coins}(1^k)$	$r \leftarrow \mathsf{PKE}.\mathsf{Dec}(sk', c_1)$
$pk \leftarrow (pk', K_G)$	$c_1 \leftarrow \mathsf{PKE}.\mathsf{Enc}(pk', r; z)$	If $r = \perp$ then return $\perp$
$sk \leftarrow (sk', K_G)$	$K \leftarrow G(K_G, r\|c_1)$	$K \leftarrow G(K_G, r\|c_1)$
Return (pk, sk)	$c_2 \leftarrow \mathcal{E}^{\mathsf{sy}}_K(m\|r)$	$m\|r' \leftarrow \mathcal{D}^{\mathsf{sy}}_K(c_2)$
	$c \leftarrow (c_1, c_2)$	If $r = r'$ then return m
	Return c	Return $\perp$

Fig. 13: **Modified part of FO transform $\overline{\mathsf{FO}}[\mathcal{G}, \mathsf{PKE}, \mathsf{SE}] = (\overline{\mathsf{FO}}.\mathsf{Kg}, \overline{\mathsf{FO}}.\mathsf{Enc}, \overline{\mathsf{FO}}.\mathsf{Dec})$.**

Procedure $\mathcal{K}_G(1^k)$	**Procedure** $G(K_G, x)$
$K_{\mathsf{PRF}} \leftarrow\!\!\$\ \mathsf{PRF}.\mathsf{Kg}(1^k)$	$C_G \leftarrow\!\!\$\ K_G(1^k)$
$f \leftarrow\!\!\$\ \mathsf{ELF}.\mathsf{IKg}(1^k)$	Return $C_G(x)$
$K_G \leftarrow\!\!\$\ \mathsf{iO}(pad(s(k), f(\mathsf{PRF}_{K_{\mathsf{PRF}}}(\cdot))))$	
Return K_G	

Fig. 14: **The hash function family $\mathcal{G}$.**

Theorem 2. *Assume that* ELF *is a secure augmented ELF,* PRF *is a secure puncturable PRF and* iO *is a sub-exponentially secure indistinguishability obfuscator. Assume sub-exponentially secure MB-AIPO (1) for the adaptive distribution ensemble $(\mathsf{PCO}_{sk'}(\cdot,\cdot), \mathcal{D}_1^{\mathcal{F}^{\mathcal{O}}})$, (2) for adaptive distribution ensemble $(\mathcal{V}_{K^*}(\cdot), \mathcal{D}_1^{\mathcal{F}^{\mathcal{O}}})$, and (3) for the distribution $\mathcal{D}_7$ (Fig. 22). Moreover, assume* PKE *is sub-exponentially OW-PCA and* SE *is sub-exponentially secure one-time AE. Then if $\mathcal{G}$ is instantiated as in Fig. 14* [7] *, $\overline{\mathsf{FO}}$ as defined in Fig. 13 is IND-CCA2 secure.*

The full proof can be found in the full version of the paper; below we present a proof sketch.

Game G_1: We start with the standard IND-CCA2 security game with PPT adversary $A = (A_1, A_2)$, shown in Fig. 15, in which the hash function G is given by $\mathsf{iO}(\mathcal{C}_1[K, f])$. Our goal in this game chain is to show that ciphertext $c_2^* = \mathcal{E}^{\mathsf{sy}}_{K^*}(m\|r^*)$ looks uniformly random to any efficient adversary given the corresponding public-key ciphertext c_1^* and K_G. To do so, we again use our new approach, incorporating an ELF and MB-AIPO into the technique of [25].

Game G_2: First, we change $\mathcal{C}_1$ to $\mathcal{C}_2$ in a manner that does not change the input/output behavior. The PRF key K_{PRF} is replaced with a key K^*_{PRF} which is punctured at $r^*\|c_1^*$. $\mathcal{C}_2$ depends on an MB-AIPO of the point function with input point $r^*\|c_1^*$ and output point K^*. On inputs $x \neq r^*\|c_1^*$, $G(K_G, x)$ is evaluated as $f(\mathsf{PRF}_{K^*_{\mathsf{PRF}}}(x))$. On inputs $x = r^*\|c_1^*$, $G(K_G, x)$ is evaluated as the MB-AIPO and hence outputs K^*. Therefore, this game is functionally equivalent

[7] Here the function $pad(\cdot\cdot)$ pads the circuit specified by the second argument to the length specified by the first argument. We implicitly set $s(k)$ to what is needed in the proof; cf. [24].

Game $G_1(k)$
$K_{\mathsf{PRF}} \leftarrow\!\!\$\ \mathsf{PRF.Kg}(1^k)\ ;\ f \leftarrow\!\!\$\ \mathsf{ELF.IKg}(1^k)$
$r^* \leftarrow\!\!\$\ \mathsf{G.Dom}(k)\ ;\ z^* \leftarrow\!\!\$\ \mathsf{PKE.Coins}(1^k)$
$(pk', sk') \leftarrow\!\!\$\ \mathsf{PKE.Kg}(1^k)$
$c_1^* \leftarrow \mathsf{PKE.Enc}(pk', r^*; z^*)$
$t^* \leftarrow \mathsf{PRF}_{K_{\mathsf{PRF}}}(r^* \| c_1^*)\ ;\ K^* \leftarrow f(t^*)$
$K_G \leftarrow\!\!\$\ \mathsf{iO}(pad(\mathcal{C}_1[K_{\mathsf{PRF}}, f]))$
$pk \leftarrow (pk', K_G)\ ;\ sk \leftarrow (sk', K_G)$
$b \leftarrow\!\!\$\ \{0,1\}\ ;\ (st, m_0, m_1) \leftarrow\!\!\$\ A_1^{\mathsf{Dec}(\cdot)}(1^k, pk)$
$c_2^* \leftarrow \mathcal{E}^{\mathsf{sy}}_{K^*}(m_b \| r^*)\ ;\ c^* \leftarrow (c_1^*, c_2^*)$
$b' \leftarrow\!\!\$\ A_2^{\mathsf{Dec}(\cdot)}(st, pk, c^*)$
Return $(b = b')$

Fig. 15: **IND-CCA2 security game for FO with adversary** $A = (A_1, A_2)$**.**

to the previous game and the circuits in G_1 and G_2 are indistinguishable by the security of iO.

Game G_3: The symmetric encryption key and MB-AIPO output point is K^*, where, previously, $f(\mathsf{PRF}_{K_{\mathsf{PRF}}}(r^* \| c_1^*)) = K^*$. In the third game, K^* becomes $K^* = f(t^*)$ where t^* is sampled uniformly at random from the PRF range. This change is indistinguishable by the security of the PRF at punctured points.

Game G_4: Next, K^*, the symmetric encryption key and MB-AIPO output point, is switched to random. This game is indistinguishable from the previous because f is a secure augmented ELF.

Game G_5: In this game the PRF key used in the obfuscated circuit $\mathcal{C}_2$ is switched from K^*_{PRF} (punctured at $r^* \| c_1^*$) to K_{PRF} which is unpunctured. In the previous game when evaluated at $r^* \| c_1^*$, $\mathcal{C}_2$ would return the output of the MB-AIPO at this point, not the ELF PRF composition. As in the transition from G_2 to G_3, the circuit input-output behavior in G_5 is identical to that of G_4. The difference in circuit descriptions is indistinguishable by the security property of iO.

Game G_6: By considering the running time of the IND-CCA adversary A, the ELF is switched to lossy mode, shrinking the range of $f(\mathsf{PRF}_{K_{\mathsf{PRF}}}(\cdot))$ down to polynomial size. Previously in G_5, the symmetric encryption key K^* was sampled randomly from the *injective* ELF range, so in G_6 when K^* is sampled from this same range, with overwhelming probability this value of K^* will not be in the image of $f(\mathsf{PRF}_{K_{\mathsf{PRF}}}(\cdot))$.

At this point we introduce three flags to the FO decryption oracle to track A's nefarious activities. In G_6 these flags, bad_0, bad_1, and bad_2, are all "silent," meaning their states do not affect the behavior of the oracles. Using three game transitions, we show that the probability of each flag being set to true is negligible. Since the transitions from G_i to G_{i+1} for $i \in \{6, 7, 8\}$ follow the "identical-until-$\mathsf{bad}_{\{0,1,2\}}$" model of [12], the game transitions can be bounded by the probability $\mathsf{bad}_{\{0,1,2\}}$ is set.

Game G_7: In the first of these three transitions, A_1's decryption oracle is changed so that it returns $\perp$ when bad_0 is true, which occurs when A_1 makes a decryption query $\overline{c} = (\overline{c}_1, \overline{c}_2)$ where the symmetric key computed in the decryption procedure, $\overline{K} = G(K_G, \overline{r} \| \overline{c}_1)$, is such that $\overline{K} = K^*$. Recall from G_6 that f is in lossy mode and thus with high probability the only way the current hash circuit could output the key K^* is if the MB-AIPO input point $r^* \| c_1^*$ was used as input. In other words, if bad_0 is set to true, then $\overline{r} \| \overline{c}_1 = r^* \| c_1^*$. Thus, the probability bad_0 is set to true is bounded by the security of MB-AIPO.
Game G_8: This game continues from G_7 and differs in A_2's decryption oracle, which returns $\perp$ when bad_1 is set to true. This occurs when A_2 makes a query $\overline{c} = (\overline{c}_1, \overline{c}_2)$ where $\overline{K} = K^*$ (as in G_7) and $\overline{c}_1 \neq c_1^*$. This can only happen if K^* is in the image of f, which is in lossy mode. In this game K^* is randomly sampled from the injective ELF range and so with high probability will not be in the polynomial-sized lossy ELF range, and hence w.h.p. bad_1 will not be set to true.
Game G_9: This game continues from G_8 and differs in A_2's decryption oracle, which returns $\perp$ when bad_2 is set to true. This occurs when A_2 makes a query $\overline{c} = (\overline{c}_1, \overline{c}_2)$ where $\overline{K} = K^*$ (as in G_7), $\overline{c}_1 = c_1^*$, $\overline{c}_2 \neq c_2^*$, and $\overline{c}_2$ is a valid symmetric ciphertext. If bad_2 is set to true, then A_2 has found a valid symmetric ciphertext different from their challenge ($\overline{c}_2 \neq c_2^*$). To set bad_2, A_2 must find a valid symmetric ciphertext under the same key as the challenge key, K^*, hence we bound the probability bad_2 is true with an AE-AUX adversary.
Game G_{10}: In this final game, the output point of the MB-AIPO in K_G is switched from the symmetric key K^* to a uniformly random string $\overline{K}$. The challenge ciphertext is still formed using K^* but the obfuscated output point in the hash circuit $\overline{K}$ is now independent of the challenge ciphertext given to A. The probability that A detects the transition from G_9 to G_{10} is bounded by the security of MB-AIPO.

Now that the K^* is uniformly random and independent of the public key, c_2^* looks uniformly random by virtue of the symmetric-key encryption scheme being IND-CPA secure concluding the proof sketch.

5 New Auxiliary-Input Multi-Bit Point Function Obfuscators and Applications

Recall that in both our OAEP and FO instantiations we need a point function obfuscation with multi-bit output (MB-AIPO), for uniformly random input and output points, that is secure wrt. certain auxiliary inputs, even though MB-AIPO is impossible in general [24]. We first show how to obtain an MB-AIPO for statistically unpredictable inputs (albeit only polynomially secure), as needed for our FO instantiation, from ELFs. We then show that the MB-AIPO required for the RSA-OAEP instantiation can be built from RSA itself under a strong yet reasonable assumption on RSA. As far as we are aware, before our work there was only one candidate MB-AIPO, due to Bitansky and Canetti [14].

The full section can be found in the full version of the paper.

Acknowledgements

We thank Dakshita Khurana for collaboration in the early stages of this work. Furthermore, we are indebted to Pooya Farshim for helpful insights. A.O. was supported in part by a gift from Cisco Systems. Most of this work was done while M.Z. was at Georgetown University.

References

1. T. Agrikola, G. Couteau, and D. Hofheinz. The usefulness of sparsifiable inputs: How to avoid subexponential iO. In A. Kiayias, M. Kohlweiss, P. Wallden, and V. Zikas, editors, *PKC 2020, Part I*, volume 12110 of *LNCS*, pages 187–219. Springer, Heidelberg, May 2020.
2. A. Akavia, S. Goldwasser, and V. Vaikuntanathan. Simultaneous hardcore bits and cryptography against memory attacks. In O. Reingold, editor, *TCC 2009*, volume 5444 of *LNCS*, pages 474–495. Springer, Heidelberg, Mar. 2009.
3. B. Barak, O. Goldreich, R. Impagliazzo, S. Rudich, A. Sahai, S. P. Vadhan, and K. Yang. On the (im)possibility of obfuscating programs. In J. Kilian, editor, *CRYPTO 2001*, volume 2139 of *LNCS*, pages 1–18. Springer, Heidelberg, Aug. 2001.
4. G. Barthe, D. Pointcheval, and S. Zanella-Béguelin. Verified security of redundancy-free encryption from rabin and RSA. Cryptology ePrint Archive, Report 2012/308, 2012. `http://eprint.iacr.org/2012/308`.
5. G. Barwell, D. P. Martin, E. Oswald, and M. Stam. Authenticated encryption in the face of protocol and side channel leakage. In T. Takagi and T. Peyrin, editors, *ASIACRYPT 2017, Part I*, volume 10624 of *LNCS*, pages 693–723. Springer, Heidelberg, Dec. 2017.
6. M. Bellare, A. Boldyreva, and A. O'Neill. Deterministic and efficiently searchable encryption. In A. Menezes, editor, *CRYPTO 2007*, volume 4622 of *LNCS*, pages 535–552. Springer, Heidelberg, Aug. 2007.
7. M. Bellare, V. T. Hoang, and S. Keelveedhi. Instantiating random oracles via UCEs. In R. Canetti and J. A. Garay, editors, *CRYPTO 2013, Part II*, volume 8043 of *LNCS*, pages 398–415. Springer, Heidelberg, Aug. 2013.
8. M. Bellare, D. Hofheinz, and S. Yilek. Possibility and impossibility results for encryption and commitment secure under selective opening. In A. Joux, editor, *EUROCRYPT 2009*, volume 5479 of *LNCS*, pages 1–35. Springer, Heidelberg, Apr. 2009.
9. M. Bellare and C. Namprempre. Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. In T. Okamoto, editor, *ASIACRYPT 2000*, volume 1976 of *LNCS*, pages 531–545. Springer, Heidelberg, Dec. 2000.
10. M. Bellare and P. Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In D. E. Denning, R. Pyle, R. Ganesan, R. S. Sandhu, and V. Ashby, editors, *ACM CCS 93*, pages 62–73. ACM Press, Nov. 1993.
11. M. Bellare and P. Rogaway. Optimal asymmetric encryption. In A. D. Santis, editor, *EUROCRYPT'94*, volume 950 of *LNCS*, pages 92–111. Springer, Heidelberg, May 1995.
12. M. Bellare and P. Rogaway. The security of triple encryption and a framework for code-based game-playing proofs. In S. Vaudenay, editor, *EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 409–426. Springer, Heidelberg, May / June 2006.

13. M. Bellare, I. Stepanovs, and S. Tessaro. Poly-many hardcore bits for any one-way function and a framework for differing-inputs obfuscation. In P. Sarkar and T. Iwata, editors, *ASIACRYPT 2014, Part II*, volume 8874 of *LNCS*, pages 102–121. Springer, Heidelberg, Dec. 2014.
14. N. Bitansky and R. Canetti. On strong simulation and composable point obfuscation. In T. Rabin, editor, *CRYPTO 2010*, volume 6223 of *LNCS*, pages 520–537. Springer, Heidelberg, Aug. 2010.
15. N. Bitansky and O. Paneth. Point obfuscation and 3-round zero-knowledge. In R. Cramer, editor, *TCC 2012*, volume 7194 of *LNCS*, pages 190–208. Springer, Heidelberg, Mar. 2012.
16. D. Bleichenbacher. On the security of the KMOV public key cryptosystem. In B. S. Kaliski Jr., editor, *CRYPTO'97*, volume 1294 of *LNCS*, pages 235–248. Springer, Heidelberg, Aug. 1997.
17. J. Blömer and A. May. A tool kit for finding small roots of bivariate polynomials over the integers. In R. Cramer, editor, *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 251–267. Springer, Heidelberg, May 2005.
18. A. Boldyreva and M. Fischlin. Analysis of random oracle instantiation scenarios for OAEP and other practical schemes. In V. Shoup, editor, *CRYPTO 2005*, volume 3621 of *LNCS*, pages 412–429. Springer, Heidelberg, Aug. 2005.
19. A. Boldyreva and M. Fischlin. On the security of OAEP. In X. Lai and K. Chen, editors, *ASIACRYPT 2006*, volume 4284 of *LNCS*, pages 210–225. Springer, Heidelberg, Dec. 2006.
20. D. Boneh and G. Durfee. Cryptanalysis of RSA with private key d less than $N^{0.292}$. In J. Stern, editor, *EUROCRYPT'99*, volume 1592 of *LNCS*, pages 1–11. Springer, Heidelberg, May 1999.
21. E. Boyle, N. Gilboa, and Y. Ishai. Function secret sharing. In E. Oswald and M. Fischlin, editors, *EUROCRYPT 2015, Part II*, volume 9057 of *LNCS*, pages 337–367. Springer, Heidelberg, Apr. 2015.
22. D. R. L. Brown. A weak-randomizer attack on rsa-oaep with e = 3. Cryptology ePrint Archive, Report 2005/189, 2005. `http://eprint.iacr.org/2005/189`.
23. C. Brzuska, P. Farshim, and A. Mittelbach. Random-oracle uninstantiability from indistinguishability obfuscation. In Y. Dodis and J. B. Nielsen, editors, *TCC 2015, Part II*, volume 9015 of *LNCS*, pages 428–455. Springer, Heidelberg, Mar. 2015.
24. C. Brzuska and A. Mittelbach. Indistinguishability obfuscation versus multi-bit point obfuscation with auxiliary input. In P. Sarkar and T. Iwata, editors, *ASIACRYPT 2014, Part II*, volume 8874 of *LNCS*, pages 142–161. Springer, Heidelberg, Dec. 2014.
25. C. Brzuska and A. Mittelbach. Using indistinguishability obfuscation via UCEs. In P. Sarkar and T. Iwata, editors, *ASIACRYPT 2014, Part II*, volume 8874 of *LNCS*, pages 122–141. Springer, Heidelberg, Dec. 2014.
26. R. Canetti. Towards realizing random oracles: Hash functions that hide all partial information. In B. S. Kaliski Jr., editor, *CRYPTO'97*, volume 1294 of *LNCS*, pages 455–469. Springer, Heidelberg, Aug. 1997.
27. R. Canetti and R. R. Dakdouk. Obfuscating point functions with multibit output. In N. P. Smart, editor, *EUROCRYPT 2008*, volume 4965 of *LNCS*, pages 489–508. Springer, Heidelberg, Apr. 2008.
28. R. Canetti, O. Goldreich, and S. Halevi. The random oracle methodology, revisited. *J. ACM*, 51(4):557–594, 2004.
29. N. Cao, A. O'Neill, and M. Zaheri. Toward RSA-OAEP without random oracles. In A. Kiayias, M. Kohlweiss, P. Wallden, and V. Zikas, editors, *PKC 2020, Part I*, volume 12110 of *LNCS*, pages 279–308. Springer, Heidelberg, May 2020.

30. D. Coppersmith. Finding a small root of a bivariate integer equation; factoring with high bits known. In U. M. Maurer, editor, *EUROCRYPT'96*, volume 1070 of *LNCS*, pages 178–189. Springer, Heidelberg, May 1996.
31. D. Coppersmith. Finding a small root of a univariate modular equation. In U. M. Maurer, editor, *EUROCRYPT'96*, volume 1070 of *LNCS*, pages 155–165. Springer, Heidelberg, May 1996.
32. J.-S. Coron, A. Kirichenko, and M. Tibouchi. A note on the bivariate Coppersmith theorem. *Journal of Cryptology*, 26(2):246–250, Apr. 2013.
33. Y. Dodis, Y. T. Kalai, and S. Lovett. On cryptography with auxiliary input. In M. Mitzenmacher, editor, *Proceedings of the 41st Annual ACM Symposium on Theory of Computing, STOC 2009, Bethesda, MD, USA, May 31 - June 2, 2009*, pages 621–630. ACM, 2009.
34. Y. Dodis and A. Smith. Entropic security and the encryption of high entropy messages. In J. Kilian, editor, *TCC 2005*, volume 3378 of *LNCS*, pages 556–577. Springer, Heidelberg, Feb. 2005.
35. G. Durfee and P. Q. Nguyen. Cryptanalysis of the RSA schemes with short secret exponent from asiacrypt '99. In T. Okamoto, editor, *ASIACRYPT 2000*, volume 1976 of *LNCS*, pages 14–29. Springer, Heidelberg, Dec. 2000.
36. E. Fujisaki and T. Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In M. J. Wiener, editor, *CRYPTO'99*, volume 1666 of *LNCS*, pages 537–554. Springer, Heidelberg, Aug. 1999.
37. E. Fujisaki and T. Okamoto. Secure integration of asymmetric and symmetric encryption schemes. *Journal of Cryptology*, 26(1):80–101, Jan. 2013.
38. E. Fujisaki, T. Okamoto, D. Pointcheval, and J. Stern. RSA-OAEP is secure under the RSA assumption. In J. Kilian, editor, *CRYPTO 2001*, volume 2139 of *LNCS*, pages 260–274. Springer, Heidelberg, Aug. 2001.
39. E. Fujisaki, T. Okamoto, D. Pointcheval, and J. Stern. RSA-OAEP is secure under the RSA assumption. *Journal of Cryptology*, 17(2):81–104, Mar. 2004.
40. B. Fuller, A. O'Neill, and L. Reyzin. A unified approach to deterministic encryption: New constructions and a connection to computational entropy. In R. Cramer, editor, *TCC 2012*, volume 7194 of *LNCS*, pages 582–599. Springer, Heidelberg, Mar. 2012.
41. S. Garg, C. Gentry, S. Halevi, M. Raykova, A. Sahai, and B. Waters. Candidate indistinguishability obfuscation and functional encryption for all circuits. *SIAM J. Comput.*, 45(3):882–929, 2016.
42. S. Garg, C. Gentry, S. Halevi, and D. Wichs. On the implausibility of differing-inputs obfuscation and extractable witness encryption with auxiliary input. In J. A. Garay and R. Gennaro, editors, *CRYPTO 2014, Part I*, volume 8616 of *LNCS*, pages 518–535. Springer, Heidelberg, Aug. 2014.
43. R. Gay and R. Pass. Indistinguishability obfuscation from circular security. In S. Khuller and V. V. Williams, editors, *STOC '21: 53rd Annual ACM SIGACT Symposium on Theory of Computing, Virtual Event, Italy, June 21-25, 2021*, pages 736–749. ACM, 2021.
44. O. Goldreich and L. A. Levin. A hard-core predicate for all one-way functions. In D. S. Johnson, editor, *Proceedings of the 21st Annual ACM Symposium on Theory of Computing, May 14-17, 1989, Seattle, Washington, USA*, pages 25–32. ACM, 1989.
45. S. Goldwasser and S. Micali. Probabilistic encryption. *Journal of Computer and System Sciences*, 28(2):270–299, 1984.
46. R. Goyal, V. Koppula, and B. Waters. Lockable obfuscation. In C. Umans, editor, *58th FOCS*, pages 612–621. IEEE Computer Society Press, Oct. 2017.

47. J. Håstad, R. Impagliazzo, L. A. Levin, and M. Luby. A pseudorandom generator from any one-way function. *SIAM J. Comput.*, 28(4):1364–1396, 1999.
48. B. Hemenway and R. Ostrovsky. Building lossy trapdoor functions from lossy encryption. In K. Sako and P. Sarkar, editors, *ASIACRYPT 2013, Part II*, volume 8270 of *LNCS*, pages 241–260. Springer, Heidelberg, Dec. 2013.
49. D. Hofheinz, K. Hövelmanns, and E. Kiltz. A modular analysis of the Fujisaki-Okamoto transformation. In Y. Kalai and L. Reyzin, editors, *TCC 2017, Part I*, volume 10677 of *LNCS*, pages 341–371. Springer, Heidelberg, Nov. 2017.
50. S. Hohenberger, A. Sahai, and B. Waters. Replacing a random oracle: Full domain hash from indistinguishability obfuscation. In P. Q. Nguyen and E. Oswald, editors, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 201–220. Springer, Heidelberg, May 2014.
51. K. Hövelmanns, E. Kiltz, S. Schäge, and D. Unruh. Generic authenticated key exchange in the quantum random oracle model. In A. Kiayias, M. Kohlweiss, P. Wallden, and V. Zikas, editors, *PKC 2020, Part II*, volume 12111 of *LNCS*, pages 389–422. Springer, Heidelberg, May 2020.
52. C.-Y. Hsiao, C.-J. Lu, and L. Reyzin. Conditional computational entropy, or toward separating pseudoentropy from compressibility. In M. Naor, editor, *EUROCRYPT 2007*, volume 4515 of *LNCS*, pages 169–186. Springer, Heidelberg, May 2007.
53. A. Jain, H. Lin, and A. Sahai. Simplifying constructions and assumptions for $i\mathcal{O}$. Cryptology ePrint Archive, Report 2019/1252, 2019. `https://eprint.iacr.org/2019/1252`.
54. A. Jain, H. Lin, and A. Sahai. Indistinguishability obfuscation from well-founded assumptions. In S. Khuller and V. V. Williams, editors, *STOC '21: 53rd Annual ACM SIGACT Symposium on Theory of Computing, Virtual Event, Italy, June 21-25, 2021*, pages 60–73. ACM, 2021.
55. H. Jiang, Z. Zhang, L. Chen, H. Wang, and Z. Ma. IND-CCA-secure key encapsulation mechanism in the quantum random oracle model, revisited. In H. Shacham and A. Boldyreva, editors, *CRYPTO 2018, Part III*, volume 10993 of *LNCS*, pages 96–125. Springer, Heidelberg, Aug. 2018.
56. H. Jiang, Z. Zhang, and Z. Ma. Tighter security proofs for generic key encapsulation mechanism in the quantum random oracle model. In J. Ding and R. Steinwandt, editors, *Post-Quantum Cryptography - 10th International Conference, PQCrypto 2019, Chongqing, China, May 8-10, 2019 Revised Selected Papers*, volume 11505 of *Lecture Notes in Computer Science*, pages 227–248, 2019.
57. C. S. Jutla. On finding small solutions of modular multivariate polynomial equations. In K. Nyberg, editor, *EUROCRYPT'98*, volume 1403 of *LNCS*, pages 158–170. Springer, Heidelberg, May / June 1998.
58. Y. T. Kalai, G. N. Rothblum, and R. D. Rothblum. From obfuscation to the security of Fiat-Shamir for proofs. In J. Katz and H. Shacham, editors, *CRYPTO 2017, Part II*, volume 10402 of *LNCS*, pages 224–251. Springer, Heidelberg, Aug. 2017.
59. A. Kiayias, S. Papadopoulos, N. Triandopoulos, and T. Zacharias. Delegatable pseudorandom functions and applications. In A.-R. Sadeghi, V. D. Gligor, and M. Yung, editors, *ACM CCS 2013*, pages 669–684. ACM Press, Nov. 2013.
60. E. Kiltz, A. O'Neill, and A. Smith. Instantiability of RSA-OAEP under chosen-plaintext attack. In T. Rabin, editor, *CRYPTO 2010*, volume 6223 of *LNCS*, pages 295–313. Springer, Heidelberg, Aug. 2010.
61. E. Kiltz and K. Pietrzak. On the security of padding-based encryption schemes - or - why we cannot prove OAEP secure in the standard model. In A. Joux, editor,

EUROCRYPT 2009, volume 5479 of *LNCS*, pages 389–406. Springer, Heidelberg, Apr. 2009.
62. T. Matsuda and G. Hanaoka. Chosen ciphertext security via point obfuscation. In Y. Lindell, editor, *TCC 2014*, volume 8349 of *LNCS*, pages 95–120. Springer, Heidelberg, Feb. 2014.
63. S. Micali and L. Reyzin. Physically observable cryptography (extended abstract). In M. Naor, editor, *TCC 2004*, volume 2951 of *LNCS*, pages 278–296. Springer, Heidelberg, Feb. 2004.
64. P. Paillier and J. L. Villar. Trading one-wayness against chosen-ciphertext security in factoring-based encryption. In X. Lai and K. Chen, editors, *ASIACRYPT 2006*, volume 4284 of *LNCS*, pages 252–266. Springer, Heidelberg, Dec. 2006.
65. C. Peikert and B. Waters. Lossy trapdoor functions and their applications. *SIAM J. Comput.*, 40(6):1803–1844, 2011.
66. C. Rackoff and D. R. Simon. Cryptographic defense against traffic analysis. In *25th ACM STOC*, pages 672–681. ACM Press, May 1993.
67. P. Rogaway and T. Shrimpton. A provable-security treatment of the key-wrap problem. In S. Vaudenay, editor, *EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 373–390. Springer, Heidelberg, May / June 2006.
68. A. Sahai and B. Waters. How to use indistinguishability obfuscation: deniable encryption, and more. In D. B. Shmoys, editor, *46th ACM STOC*, pages 475–484. ACM Press, May / June 2014.
69. T. Saito, K. Xagawa, and T. Yamakawa. Tightly-secure key-encapsulation mechanism in the quantum random oracle model. In J. B. Nielsen and V. Rijmen, editors, *EUROCRYPT 2018, Part III*, volume 10822 of *LNCS*, pages 520–551. Springer, Heidelberg, Apr. / May 2018.
70. V. Shoup. OAEP reconsidered. *Journal of Cryptology*, 15(4):223–249, Sept. 2002.
71. H. Wee and D. Wichs. Candidate obfuscation via oblivious LWE sampling. In A. Canteaut and F. Standaert, editors, *Advances in Cryptology - EUROCRYPT 2021 - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17-21, 2021, Proceedings, Part III*, volume 12698 of *Lecture Notes in Computer Science*, pages 127–156. Springer, 2021.
72. M. Zhandry. The magic of ELFs. In M. Robshaw and J. Katz, editors, *CRYPTO 2016, Part I*, volume 9814 of *LNCS*, pages 479–508. Springer, Heidelberg, Aug. 2016.
73. M. Zhandry. Augmented random oracles. Cryptology ePrint Archive, Paper 2022/783, 2022. `https://eprint.iacr.org/2022/783`.

Supplementary Material

A Proof of Theorem 1

Remark 1. When $\mathcal{F}$ is RSA, for $\zeta \geq k(e^2-1)/e^2$ we have that $(\mu, \mu+\zeta)$-SIE and $(\mu, \mu+\zeta)$-CIE hold under the assumption that the bivariate Coppersmith algorithm [17, 30, 32] is efficient. Therefore, under this assumption, the assumptions on RSA are reduced to solely sub-exponential OW (which implies sub-exponential POW) matching the result in the RO model by Fujisaki *et al.* [39] up to sub-exponentiality. Although this could be viewed as "trading heuristics,"

Games $G_1(k)$, $G_2(k)$	**Games** $G_3(k)$, $G_4(k)$
$b \leftarrow\!\!\$\ \{0,1\}$; $K \leftarrow\!\!\$\ \mathsf{PRF.Kg}(1^k)$	$b \leftarrow\!\!\$\ \{0,1\}$; $K \leftarrow\!\!\$\ \mathsf{PRF.Kg}(1^k)$
$r^* \leftarrow\!\!\$\ \{0,1\}^\rho$; $K^* \leftarrow\!\!\$\ \mathsf{PRF.Punct}(K, r^*)$	$r^* \leftarrow\!\!\$\ \{0,1\}^\rho$; $K^* \leftarrow\!\!\$\ \mathsf{PRF.Punct}(K, r^*)$
$f \leftarrow\!\!\$\ \mathsf{ELF.IKg}(1^k)$; $x^* \leftarrow \mathsf{PRF}_K(r^*)$	$f \leftarrow\!\!\$\ \mathsf{ELF.IKg}(1^k)$; $\boxed{x^* \leftarrow\!\!\$\ \mathsf{PRF.Rng}(k)}$
$z^* \leftarrow f(x^*)$; $p \leftarrow\!\!\$\ \mathsf{MB\text{-}AIPO}(r^*, z^*)$	$z^* \leftarrow f(x^*)$; $z^* \leftarrow\!\!\$\ \mathsf{G.Rng}(k)$
$K_G \leftarrow\!\!\$\ \mathsf{iO}(pad(\mathcal{C}_1[K, f]))$	$p \leftarrow\!\!\$\ \mathsf{MB\text{-}AIPO}(r^*, z^*)$
$K_G \leftarrow\!\!\$\ \mathsf{iO}(\mathcal{C}_2[K^*, f, p])$	$K_G \leftarrow\!\!\$\ \mathsf{iO}(\mathcal{C}_2[K^*, f, p])$
$K_H \leftarrow\!\!\$\ \mathcal{K}_H(1^k)$; $(F, F^{-1}) \leftarrow\!\!\$\ \mathsf{Kg}(1^k)$	$K_H \leftarrow\!\!\$\ \mathcal{K}_H(1^k)$; $(F, F^{-1}) \leftarrow\!\!\$\ \mathsf{Kg}(1^k)$
$pk \leftarrow (F, K_H, K_G)$; $sk \leftarrow (F^{-1}, K_H, K_G)$	$pk \leftarrow (F, K_H, K_G)$; $sk \leftarrow (F^{-1}, K_H, K_G)$
$(st, m_0, m_1) \leftarrow\!\!\$\ A_1^{\mathsf{Dec}(\cdot)}(1^k, pk)$	$(st, m_0, m_1) \leftarrow\!\!\$\ A_1^{\mathsf{Dec}(\cdot)}(1^k, pk)$
$s^* \leftarrow z^* \oplus (m_b \| 0^\zeta)$; $y^* \leftarrow H(K_H, s^*)$	$s^* \leftarrow z^* \oplus (m_b \| 0^\zeta)$; $y^* \leftarrow H(K_H, s^*)$
$t^* \leftarrow r^* \oplus y^*$; $c^* \leftarrow F(s^* \| t^*)$	$t^* \leftarrow r^* \oplus y^*$; $c^* \leftarrow F(s^* \| t^*)$
$b' \leftarrow\!\!\$\ A_2^{\mathsf{Dec}(\cdot)}(st, pk, c^*)$	$b' \leftarrow\!\!\$\ A_2^{\mathsf{Dec}(\cdot)}(st, pk, c^*)$
Return $(b = b')$	Return $(b = b')$

Games $G_5(k)$, $G_6(k)$	**Games** $G_7(k)$, $G_8(k)$
$b \leftarrow\!\!\$\ \{0,1\}; K \leftarrow\!\!\$\ \mathsf{PRF.Kg}(1^k); r^* \leftarrow\!\!\$\ \{0,1\}^\rho$	$b \leftarrow\!\!\$\ \{0,1\}; K \leftarrow\!\!\$\ \mathsf{PRF.Kg}(1^k); r^* \leftarrow\!\!\$\ \{0,1\}^\rho$
$z^* \leftarrow\!\!\$\ \mathsf{G.Rng}(k)$; $p \leftarrow\!\!\$\ \mathsf{MB\text{-}AIPO}(r^*, z^*)$	$z^* \leftarrow\!\!\$\ \mathsf{G.Rng}(k)$; $p \leftarrow\!\!\$\ \mathsf{MB\text{-}AIPO}(r^*, z^*)$
$f \leftarrow\!\!\$\ \mathsf{ELF.IKg}(1^k)$; $f \leftarrow\!\!\$\ \mathsf{ELF.LKg}(1^k)$	$f \leftarrow\!\!\$\ \mathsf{ELF.LKg}(1^k)$; $K_G \leftarrow\!\!\$\ \mathsf{iO}(\mathcal{C}_2[K, f, p])$
$\boxed{K_G \leftarrow\!\!\$\ \mathsf{iO}(\mathcal{C}_2[K, f, p])}$	$K_H \leftarrow\!\!\$\ \mathcal{K}_H(1^k)$; $(F, F^{-1}) \leftarrow\!\!\$\ \mathsf{Kg}(1^k)$
$K_H \leftarrow\!\!\$\ \mathcal{K}_H(1^k)$; $(F, F^{-1}) \leftarrow\!\!\$\ \mathsf{Kg}(1^k)$	$pk \leftarrow (F, K_H, K_G)$; $sk \leftarrow (F^{-1}, K_H, K_G)$
$pk \leftarrow (F, K_H, K_G)$; $sk \leftarrow (F^{-1}, K_H, K_G)$	$\boxed{(st, m_0, m_1) \leftarrow\!\!\$\ A_1^{\mathsf{Dec}'(G_7,\cdot)}(1^k, pk)}$
$(st, m_0, m_1) \leftarrow\!\!\$\ A_1^{\mathsf{Dec}(\cdot)}(1^k, pk)$	$(st, m_0, m_1) \leftarrow\!\!\$\ A_1^{\mathsf{Dec}''_1(\cdot)}(1^k, pk)$
$(st, m_0, m_1) \leftarrow\!\!\$\ A_1^{\mathsf{Dec}'(G_6,\cdot)}(1^k, pk)$	$s^* \leftarrow z^* \oplus (m_b \| 0^\zeta)$; $y^* \leftarrow H(K_H, s^*)$
$s^* \leftarrow z^* \oplus (m_b \| 0^\zeta)$; $y^* \leftarrow H(K_H, s^*)$	$t^* \leftarrow r^* \oplus y^*$; $c^* \leftarrow F(s^* \| t^*)$
$t^* \leftarrow r^* \oplus y^*$; $c^* \leftarrow F(s^* \| t^*)$	$b' \leftarrow\!\!\$\ A_2^{\mathsf{Dec}(\cdot)}(st, pk, c^*)$
$b' \leftarrow\!\!\$\ A_2^{\mathsf{Dec}(\cdot)}(st, pk, c^*)$	$b' \leftarrow\!\!\$\ A_2^{\mathsf{Dec}''_2(\cdot)}(st, pk, c^*)$
Return $(b = b')$	Return $(b = b')$

Fig. 16: **Games G_1–G_8 in the proof of Theorem 1. Uses procedures in Fig. 17. The boxes highlight the difference between adjacent games in different cells.**

efficiency of an algorithm can be studied and hopefully *proven*. It is also supported experimentally. Indeed, the bivariate Coppersmith algorithm works well in practice [16, 20, 35, 57]. Interestingly, this entire issue can be avoided if the order of the messages bits and redundancy bits in OAEP are swapped.

Remark 2. We use sub-exponential assumptions when the challenge message depends on the public-key (more precisely, when the message depends on the key for hash function G). This is because the MB-AIPO auxiliary input should contain the encrypted challenge message, but the latter depends on the public key. To solve this, the MB-AIPO *guess* the challenge message to be able to properly simulate the games. So we have an exponential security loss, which we compen-

Game $G_9(k)$
$b \leftarrow\!\!\$\ \{0,1\}$; $K \leftarrow\!\!\$\ \mathsf{PRF.Kg}(1^k)$
$r^* \leftarrow\!\!\$\ \{0,1\}^\rho$; $z^* \leftarrow\!\!\$\ \mathsf{G.Rng}(k)$
$\boxed{\overline{z} \leftarrow\!\!\$\ \mathsf{G.Rng}(k)\ ;\ \overline{p} \leftarrow\!\!\$\ \mathsf{MB\text{-}AIPO}(r^*, \overline{z})}$
$f \leftarrow\!\!\$\ \mathsf{ELF.LKg}(1^k)$; $\boxed{K_G \leftarrow\!\!\$\ \mathsf{iO}(\mathcal{C}_2[K, f, \overline{p}])}$
$K_H \leftarrow\!\!\$\ \mathcal{K}_H(1^k)$; $(F, F^{-1}) \leftarrow\!\!\$\ \mathsf{Kg}(1^k)$
$pk \leftarrow (F, K_H, K_G)$; $sk \leftarrow (F^{-1}, K_H, K_G)$
$(st, m_0, m_1) \leftarrow\!\!\$\ A_1^{\mathsf{Dec}_1''(\cdot)}(1^k, pk)$
$s^* \leftarrow z^* \oplus (m_b \| 0^\zeta)$; $y^* \leftarrow H(K_H, s^*)$
$t^* \leftarrow r^* \oplus y^*$; $c^* \leftarrow F(s^* \| t^*)$
$b' \leftarrow\!\!\$\ A_2^{\mathsf{Dec}_2''(\cdot)}(st, pk, c^*)$
Return $(b = b')$

Circuit $\mathcal{C}_1[K, f](r)$
Return $f(\mathsf{PRF}_K(r))$

Circuit $\mathcal{C}_2[K, f, p](r)$
If $p(r) = \perp$ then return $f(\mathsf{PRF}_K(r))$
Return $p(r)$

Procedure $\mathsf{Dec}'(G_X, c)$
$(F^{-1}, K_H, K_G) \leftarrow sk$; $s \leftarrow F^{-1}(c)|^{\mu+\zeta}$
$t \leftarrow F^{-1}(c)|_\rho$; $r \leftarrow t \oplus H(K_H, s)$
If $s|_\zeta = z^*|_\zeta$ then
  $\mathsf{bad} \leftarrow \mathsf{true}$
  If $X = 7$ then return $\perp$
$m' \leftarrow s \oplus G(K_G, r)$
If $m'|_\zeta = 0^\zeta$ then return $m'|^\mu$
Else return $\perp$

Procedure $\mathsf{Dec}''_{\mathsf{flag}}(c)$
$(F, K_H, K_G) \leftarrow pk$
For all $z \in [f(\cdot)]$ do
  $s \| t \leftarrow \mathsf{Ext}_{\mathsf{sie}}(F, c, z|_\zeta)$
  $r \leftarrow t \oplus H(K_H, s)$
  $\overline{m} \leftarrow G(K_G, r) \oplus s$; $m \leftarrow \overline{m}|^\mu$
  If $\mathsf{OAEP.Enc}(pk, m; r) = c$ then return m
If $\mathsf{flag} = 1$ then return $\perp$
$(s \| t, s^* \| t^*) \leftarrow \mathsf{Ext}_{\mathsf{cie}}(F, c, c^*)$
If $F(s\|t) \neq c \ \vee\ F(s^*\|t^*) \neq c^* \ \vee\ s|_\zeta \neq s^*|_\zeta$ then
  Return $\perp$
$r \leftarrow t \oplus H(K_H, s)$
$\overline{m} \leftarrow G(K_G, r) \oplus s$; $m \leftarrow \overline{m}|^\mu$
Return m

Fig. 17: **Game G_9 and related procedures for the proof of Theorem 1. The boxes in G_9 highlight the differences from G_8.**

sate for with sub-exponential security assumptions. In the case that messages do *not* depend on the public key[8] we can remove all sub-exponential assumptions.

Proof. We use that OW and $(\mu, \mu+\zeta)$-SIE together imply $(\mu, \mu+\zeta)$-POW (recall POW means partial one-way). The proof of the latter implication is straightforward. Consider the games G_1–G_9 in Figures 16 and 17.

Game G_1: This is the standard IND-CCA2 game. For contradiction, suppose PPT adversary $A = (A_1, A_2)$ runs in time v and wins game G_1 with non-negligible probability ϵ. Let δ be an inverse polynomial in k such that $\epsilon \geq \delta$ infinitely often.

[8] Which is called IND-CCA-KI in [60].

Adversary $D_1^{\mathsf{iO}(\mathsf{LR}(\cdot,\cdot,d))}(1^k)$	**Adversary** $D_2(r^*, K^*, x^*)$
$r^* \leftarrow\!\!\$\ \{0,1\}^\rho$; $K \leftarrow\!\!\$\ \mathsf{PRF.Kg}(1^k)$	$f \leftarrow\!\!\$\ \mathsf{ELF.IKg}(1^k)$; $z^* \leftarrow f(x^*)$
$f \leftarrow\!\!\$\ \mathsf{ELF.IKg}(1^k)$; $z^* \leftarrow f(\mathsf{PRF}_K(r^*))$	$p \leftarrow\!\!\$\ \mathsf{MB\text{-}AIPO}(r^*, z^*)$
$K^* \leftarrow\!\!\$\ \mathsf{PRF.Punct}(K, r^*)$	$K_G \leftarrow\!\!\$\ \mathsf{iO}(\mathcal{C}_2[K^*, f, p])$
$p \leftarrow\!\!\$\ \mathsf{MB\text{-}AIPO}(r^*, z^*)$	$K_H \leftarrow\!\!\$\ \mathcal{K}_H(1^k)$; $(F, F^{-1}) \leftarrow\!\!\$\ \mathsf{Kg}(1^k)$
$C^1 \leftarrow\!\!\$\ \mathcal{C}_1[K, f]$; $C^2 \leftarrow\!\!\$\ \mathcal{C}_2[K^*, f, p]$	$pk \leftarrow (F, K_H, K_G)$
$K_H \leftarrow\!\!\$\ \mathcal{K}_H(1^k)$; $(F, F^{-1}) \leftarrow\!\!\$\ \mathsf{Kg}(1^k)$	$sk \leftarrow (F^{-1}, K_H, K_G)$; $b \leftarrow\!\!\$\ \{0,1\}$
$K_G \leftarrow \mathsf{iO}(\mathsf{LR}(C^1, C^2, d))$	$(st, m_0, m_1) \leftarrow\!\!\$\ A_1^{\mathsf{Dec}(\cdot)}(1^k, pk)$
$pk \leftarrow (F, K_H, K_G)$; $sk \leftarrow (F^{-1}, K_H, K_G)$	$s^* \leftarrow z^* \oplus (m_b \| 0^\zeta)$; $y^* \leftarrow H(K_H, s^*)$
$b \leftarrow\!\!\$\ \{0,1\}$; $(st, m_0, m_1) \leftarrow\!\!\$\ A_1^{\mathsf{Dec}(\cdot)}(1^k, pk)$	$t^* \leftarrow r^* \oplus y^*$; $c^* \leftarrow F(s^* \| t^*)$
$s^* \leftarrow z^* \oplus (m_b \| 0^\zeta)$; $y^* \leftarrow H(K_H, s^*)$	$b' \leftarrow\!\!\$\ A_2^{\mathsf{Dec}(\cdot)}(st, pk, c^*)$
$t^* \leftarrow r^* \oplus y^*$; $c^* \leftarrow F(s^* \| t^*)$	Return $(b = b')$
$b' \leftarrow\!\!\$\ A_2^{\mathsf{Dec}(\cdot)}(st, pk, c^*)$	
Return $(b = b')$	

Circuit $\mathcal{C}_1[K, f](r)$	**Procedure** $\mathsf{Dec}(c)$
Return $f(\mathsf{PRF}_K(r))$	$m \leftarrow \mathsf{Dec}(sk, c)$
Circuit $\mathcal{C}_2[K^*, f, p](r)$	Return m
If $p(r) = \perp$ then return $f(\mathsf{PRF}_{K^*}(r))$	
Return $p(r)$	

Fig. 18: **iO adversary D_1 (left) and PRF adversary D_2 (right) in the proof of Theorem 1 (cf. G_2 and G_3).**

Game G_2: Game G_2 is similar to game G_1 except that the PRF key K is punctured at r^*. Moreover, the hash key K_G does not consist of an obfuscation of $\mathcal{C}_1[K, f]$, but rather of an obfuscation of the circuit $\mathcal{C}_2[K^*, f, p]$. Note that the two circuits are functionally equivalent and the same size by *pad*. Therefore, considering an iO adversary D_1 in Fig. 18, we get that $|\Pr[G_1 \Rightarrow 1] - \Pr[G_2 \Rightarrow 1]| \leq \mathbf{Adv}^{\mathrm{io}}_{\mathsf{iO}, D_1, \mathcal{C}}(k)$.

Game G_3: Game G_3 is similar to game G_2 except that x^* is chosen randomly in $\mathsf{PRF.Rng}(k)$. Considering the adversary D_2 attacking pseudorandom function PRF at the punctured points in Fig. 18, we get that $|\Pr[G_2 \Rightarrow 1] - \Pr[G_3 \Rightarrow 1]| \leq \mathbf{Adv}^{\mathrm{pprf}}_{\mathsf{PRF}, D_2}(k)$.

Game G_4: Game G_4 is similar to game G_3 except that z^* is chosen randomly in $\{0,1\}^{\mu+\zeta}$. Recalling that ELF is augmented (cf. Section 3.1) and Proposition 1, consider the adversary D_3 in Fig. 19 that distinguishes the output of augmented ELF from random. We get that $|\Pr[G_3 \Rightarrow 1] - \Pr[G_4 \Rightarrow 1]|$ is less than advantage of adversary D_3 and hence is negligible.

Game G_5: Game G_5 is similar to game G_4 except that an obfuscation of circuit $\mathcal{C}_2[K, f, p]$ is used as the hash key K_G. Note that circuit $\mathcal{C}_2[K, f, p]$ is identical to circuit $\mathcal{C}_2[K^*, f, p]$, except that it uses the original PRF key K instead of the punctured key K^*. The two circuits are functionally equivalent and the same size by *pad*. Therefore, considering the adversary D_4 attacking iO, we

Adversary $D_3(f, z^*)$	**Adversary** $D_5(f)$
$b \leftarrow\$ \{0,1\}$; $K \leftarrow\$ \mathsf{PRF.Kg}(1^k)$	$b \leftarrow\$ \{0,1\}$; $r^* \leftarrow\$ \{0,1\}^\rho$
$r^* \leftarrow\$ \{0,1\}^\rho$; $K^* \leftarrow\$ \mathsf{PRF.Punct}(K, r^*)$	$z^* \leftarrow\$ \mathsf{G.Rng}(k)$; $p \leftarrow\$ \mathsf{MB\text{-}AIPO}(r^*, z^*)$
$p \leftarrow\$ \mathsf{MB\text{-}AIPO}(r^*, z^*)$	$K \leftarrow\$ \mathsf{PRF.Kg}(1^k)$; $K_G \leftarrow\$ \mathsf{iO}(\mathcal{C}_2[K, f, p])$
$K_G \leftarrow\$ \mathsf{iO}(\mathcal{C}_2[K^*, f, p])$	$K_H \leftarrow\$ \mathcal{K}_H(1^k)$; $(F, F^{-1}) \leftarrow\$ \mathsf{Kg}(1^k)$
$K_H \leftarrow\$ \mathcal{K}_H(1^k)$; $(F, F^{-1}) \leftarrow\$ \mathsf{Kg}(1^k)$	$pk \leftarrow (F, K_H, K_G)$
$pk \leftarrow (F, K_H, K_G)$; $sk \leftarrow (F^{-1}, K_H, K_G)$	$sk \leftarrow (F^{-1}, K_H, K_G)$
$(st, m_0, m_1) \leftarrow\$ A_1^{\mathsf{Dec}(\cdot)}(1^k, pk)$	$(st, m_0, m_1) \leftarrow\$ A_1^{\mathsf{Dec}(\cdot)}(1^k, pk)$
$s^* \leftarrow z^* \oplus (m_b \| 0^\zeta)$; $y^* \leftarrow H(K_H, s^*)$	$s^* \leftarrow z^* \oplus (m_b \| 0^\zeta)$; $y^* \leftarrow H(K_H, s^*)$
$t^* \leftarrow r^* \oplus y^*$; $c^* \leftarrow F(s^* \| t^*)$	$t^* \leftarrow r^* \oplus y^*$; $c^* \leftarrow F(s^* \| t^*)$
$b' \leftarrow\$ A_2^{\mathsf{Dec}(\cdot)}(st, pk, c^*)$	$b' \leftarrow\$ A_2^{\mathsf{Dec}(\cdot)}(st, pk, c^*)$
Return $(b = b')$	Return $(b = b')$

Circuit $\mathcal{C}_1[K, f](r)$	**Procedure** $\mathsf{Dec}(c)$
Return $f(\mathsf{PRF}_K(r))$	$m \leftarrow \mathsf{Dec}(sk, c)$
Circuit $\mathcal{C}_2[K^*, f, p](r)$	Return m
If $p(r) = \perp$ then return $f(\mathsf{PRF}_{K^*}(r))$	
Return $p(r)$	

Fig. 19: **ELF adversary D_3 (left) and ELF adversary D_5 (right) in the proof of Theorem 1 (cf. G_4 and G_6).**

get that $|\Pr[G_4 \Rightarrow 1] - \Pr[G_5 \Rightarrow 1]| \leq \mathbf{Adv}^{\mathrm{io}}_{\mathsf{iO}, D_4, \mathcal{C}}(k)$. We omit the code of adversary D_4 due to its similarity to adversary D_1 (Fig. 18).

Game G_6: Game G_6 is similar to game G_5 except that we change ELF to lossy mode. That is, we generate $f \leftarrow \mathsf{ELF.LKg}(1^k, \mathsf{poly}(\mathsf{v}, 2/\delta))$, where $\mathsf{poly}(\mathsf{v}, 2/\delta)$ is a polynomial in two variables.[9] This means no adversary running in time v can distinguish the mode of f with more than a $\delta/2$ probability. Considering a standard ELF adversary D_5, running in time v, attacking the key-indistinguishability property of ELF in Fig. 19, we get that $|\Pr[G_5 \Rightarrow 1] - \Pr[G_6 \Rightarrow 1]| \leq \delta/2$. A_1's decryption oracle changed to $\mathsf{Dec}'(G_6, \cdot)$, defined in Fig. 17 (left). This oracle silently sets a bad flag which is used in the analysis of the G_6 to G_7 transition.

Game G_7: Game G_7 is similar to game G_6 except that A_1's decryption oracle $\mathsf{Dec}'(G_7, \cdot)$ returns $\perp$ after bad is set, as defined in Fig. 17 (left). Games G_6 and G_7 are identical-until-bad, and so by the fundamental lemma of game-playing [12], we have $|\Pr[G_6 \Rightarrow 1] - \Pr[G_7 \Rightarrow 1]| \leq \Pr[G_6 \text{ sets } \mathsf{bad}]$. bad is set when A_1 makes a decryption query c with the same "preimage redundancy bits," $s|_\zeta$, as the preimage of c^*. In other words, A_1 makes a query $c = F(s \| r \oplus H(K_H, s))$ where $s = z \oplus (m \| 0^\zeta)$ such that the ζ least significant bits of z equal the ζ LSB of z^* (i.e. $z|_\zeta = z^*|_\zeta$).

[9] The argument $\mathsf{poly}(\mathsf{v}, 2/\delta)$ is omitted from the G_6 pseudo code in Fig. 16 due to its dependence on the adversary run-time, v.

Distribution $\mathsf{Samp}(1^k)$	**Adversary** $D_6(1^k, L, p)$
$r^* \leftarrow\!\!\$\ \{0,1\}^\rho$; $z^* \leftarrow\!\!\$\ \mathsf{G.Rng}(k)$	$f \leftarrow\!\!\$\ \mathsf{ELF.LKg}(1^k)$
$K_H \leftarrow\!\!\$\ \mathcal{K}_H(1^k)$; $(F, F^{-1}) \leftarrow\!\!\$\ \mathsf{Kg}(1^k)$	$K \leftarrow\!\!\$\ \mathsf{PRF.Kg}(1^k)$; $(c^*, K_H, F) \leftarrow L$
$m \leftarrow\!\!\$\ \{0,1\}^\mu$; $s^* \leftarrow z^* \oplus (m \| 0^\zeta)$	$K_G \leftarrow\!\!\$\ \mathsf{iO}(\mathcal{C}_2[K, f, p])$
$y^* \leftarrow H(K_H, s^*)$; $t^* \leftarrow r^* \oplus y^*$	$pk \leftarrow (F, K_H, K_G)$; $b' \leftarrow 0$
$c^* \leftarrow F(s^* \| t^*)$; $L \leftarrow (c^*, K_H, F)$	Run $A_1^{\mathsf{Dec}_{D_6}(\cdot)}(1^k, pk)$
Return (L, r^*, z^*)	Return b'

Procedure $\mathsf{Dec}_{D_6}(c)$
$(F, K_H, K_G) \leftarrow pk$
For all $z \in [f(\cdot)]$ do
  $s \| t \leftarrow \mathsf{Ext}_{\mathsf{sie}}(F, c, z|_\zeta)$; $r \leftarrow t \oplus H(K_H, s)$
  $\overline{m} \leftarrow G(K_G, r) \oplus s$; $m' \leftarrow \overline{m}|^\mu$
  If $\mathsf{OAEP.Enc}(pk, m'; r) = c$ then return m'
$(s^* \| t^*, s \| t) \leftarrow \mathsf{Ext}_{\mathsf{cie}}(F, c^*, c)$
If $(F(s^* \| t^*) = c^*) \ \wedge \ (F(s \| t) = c) \ \wedge (s^*|_\zeta = s|_\zeta)$ then $b' \leftarrow 1$
Return $\perp$

Fig. 20: **Distribution** Samp **(left), MB-AIPO adversary** D_6 **(right), and the decryption oracle simulated by** D_6 **in the proof of Theorem 1 (cf.** G_7**).**

A_1's input includes the MB-AIPO with output point z^*. So, to bound the probability bad is set, consider the MB-AIPO adversary D_6 and associated distribution Samp in Fig. 20. (Note that Samp is a restriction of $\mathcal{D}^{\mathcal{OAEP}}$, not an additional assumption on the MB-AIPO.) To simulate the decryption oracle for A, D_6 uses $\mathsf{Dec}_{D_6}(\cdot)$ shown in Fig. 20 (bottom). In this simulated decryption oracle, the polynomial-size of the lossy range of ELF is exploited. D_6 can iterate over the whole range of f and check if each possible value of z works to decrypt. We claim that

$$\Pr[\, G_6 \text{ sets } \mathsf{bad} \,] \le \mathbf{Adv}^{\text{mb-aipo}}_{\mathsf{MB\text{-}AIPO}, D_6, \mathsf{Samp}}(k) + q_d/2^\zeta \ ,$$

where q_d is the number of decryption queries A_1 makes. To see this by a standard conditioning argument let's write

$$\mathbf{Adv}^{\text{mb-aipo}}_{\mathsf{MB\text{-}AIPO}, D_6, \mathsf{Samp}}(k)$$
$$= |\Pr\left[\, \text{MB-AIPO}^{\mathsf{Samp}, D_6, 1}_{\mathsf{MB\text{-}AIPO}}(k) \Rightarrow 1 \,\right] - \Pr\left[\, \text{MB-AIPO}^{\mathsf{Samp}, D_6, 0}_{\mathsf{MB\text{-}AIPO}}(k) \Rightarrow 1 \,\right]| \ ,$$

where the third superscript $d \in \{0,1\}$ on the RHS terms indicates the challenge bit b is fixed to d in the game. We next claim

$$\Pr\left[\, \text{MB-AIPO}^{\mathsf{Samp}, D_6, 1}_{\mathsf{MB\text{-}AIPO}}(k) \Rightarrow 1 \,\right] \ge \Pr[\, G_6 \text{ sets } \mathsf{bad} \,] \, .$$

Indeed, for any execution of A in G_6 that sets bad, the same coin sequence will also cause D_6 to return $b' = 1$. Finally

$$\Pr\left[\, \text{MB-AIPO}^{\mathsf{Samp}, D_6, 0}_{\mathsf{MB\text{-}AIPO}}(k) \Rightarrow 1 \,\right] \le q_d/2^\zeta \ .$$

This is because $z^*|_\zeta$ is random and independent of A_1's view. Each query thus causes bad to be set with probability $2^{-\zeta}$, and we take a union bound across queries.

Game G_8**:** Game G_8 is similar to game G_7 except that A's decryption oracles are changed to $\mathsf{Dec}''_{\mathsf{flag}}(\cdot)$ for $\mathsf{flag} \in \{1,2\}$ given to $A_{\mathsf{flag}=1}$ and $A_{\mathsf{flag}=2}$ respectively, as defined in Fig. 17 (bottom right). We claim that $\Pr[\,G_7 \Rightarrow 1\,] = \Pr[\,G_8 \Rightarrow 1\,]$ and show this by arguing that the respective decryption oracles have the same input-output behavior. Unlike the previous decryption oracles, $\mathsf{Dec}''_{\mathsf{flag}}(\cdot)$ decrypts using the public key, not the private key, by running in more time than the adversary A. $\mathsf{Dec}''_{\mathsf{flag}}(\cdot)$ exhaustively searches over all points in the polynomial-size range of the lossy-mode ELF and runs the second-input extractor $\mathsf{Ext}_{\mathsf{sie}}$ for $\mathcal{F}$. Recall that on inputs $F, c = F(s\|t)$, and $(s\|t)|_\mu^{\mu+\zeta}$, $\mathsf{Ext}_{\mathsf{sie}}$ returns $s\|t$.

If no message m is found via exhaustive search that encrypts to the input ciphertext and $\mathsf{flag} = 1$ (indicating A_1 is making queries), then $\mathsf{Dec}''_1(\cdot)$ returns $\perp$. Hence, decryption oracles $\mathsf{Dec}''_1(\cdot)$ and $\mathsf{Dec}'(G_7, \cdot)$ have identical input-output behavior.

Next A_2's interaction with the oracle is considered. If no message is found via exhaustive search and $\mathsf{flag} = 2$ (indicating A_2 is making queries), the procedure runs the common-inputs extractor $\mathsf{Ext}_{\mathsf{cie}}$ on the input ciphertext c and challenge ciphertext c^* to decrypt the former. Recall that on inputs $F, c = F(s\|t)$ and $c^* = F(s^*\|t^*)$, $\mathsf{Ext}_{\mathsf{cie}}$ returns $s\|t$ and $s^*\|t^*$ if $(s\|t)|_\mu^{\mu+\zeta} = (s^*\|t^*)|_\mu^{\mu+\zeta}$. This final equality can be rewritten as $s|_\zeta = s^*|_\zeta$.[10] If the CIE extractor also fails to produce the decryption of c, $\mathsf{Dec}''_2(\cdot)$ returns $\perp$. This means A_2's query was not a valid ciphertext and so the decryption oracle $\mathsf{Dec}(\cdot)$ in G_7 would have also returned $\perp$. On the other hand, if $\mathsf{Ext}_{\mathsf{cie}}$ outputs preimages of c and c^* such that $s|_\zeta = s^*|_\zeta$, then $\mathsf{Dec}''_2(\cdot)$ can output the decryption m, just as $\mathsf{Dec}(\cdot)$ would have in G_7. So, $\mathsf{Dec}''_2(\cdot)$ and $\mathsf{Dec}(\cdot)$ also have identical input-output behavior. Now we can conclude $\Pr[\,G_7 \Rightarrow 1\,] = \Pr[\,G_8 \Rightarrow 1\,]$ as desired.

Game G_9**:** Game G_9 is similar to game G_8 except that the hash key K_G consists of an obfuscation of the circuit $\mathcal{C}_2[K, f, \overline{p}]$, where $\overline{p}$ has random output point $\overline{z}$, instead of z^* (but the challenge c^* still depends on z^*). Circuits $\mathcal{C}_2[K, f, p]$ and $\mathcal{C}_2[K, f, \overline{p}]$ only differ only on the single point where $p(r)$ is not equal to $\perp$, that is, r^*. The difference in the outcome of games G_8 and G_9 is bounded by the security of the MB-AIPO. Consider distribution Samp and MB-AIPO adversary D_8 in Fig. 21.

We start by showing that Samp is a sub-exponentially unpredictable distribution. Assume that there exists an adversary that outputs r^* on input $L = (c^*, K_H, F, m)$ with probability greater than δ. Then we can construct a distinguisher against $\mathcal{H}$ with advantage more than δ. However, we know that $\mathcal{H}$ is a sub-exponential one-wayness extractor and $\mathcal{F}$ is sub-exponentially $(\mu, \mu+\zeta)$-POW. Hence, $\delta \leq 2^{-k^\alpha}$ for some $0 < \alpha < 1$. Thus, Samp is

[10] Or written as $z|_\zeta = z^*|_\zeta$, since $s = z \oplus (m\|0^\zeta)$ and hence the last ζ bits of s are equal to the last ζ bits of z, i.e., $s|_\zeta = z|_\zeta$.

Distribution $\mathsf{Samp}(1^k)$	**Adversary** $D_8(1^k, L, p)$
$r^* \leftarrow\!\!\$\ \{0,1\}^\rho$; $z^* \leftarrow\!\!\$\ \mathsf{G.Rng}(k)$	$f \leftarrow\!\!\$\ \mathsf{ELF.LKg}(1^k)$; $K \leftarrow\!\!\$\ \mathsf{PRF.Kg}(1^k)$
$K_H \leftarrow\!\!\$\ \mathcal{K}_H(1^k)$; $(F, F^{-1}) \leftarrow\!\!\$\ \mathsf{Kg}(1^k)$	$(c^*, K_H, F, m) \leftarrow L$
$m \leftarrow\!\!\$\ \{0,1\}^\mu$	$K_G \leftarrow\!\!\$\ \mathsf{iO}(\mathcal{C}_2[K, f, p])$
$s^* \leftarrow z^* \oplus (m \Vert 0^\zeta)$; $y^* \leftarrow H(K_H, s^*)$	$pk \leftarrow (F, K_H, K_G)$; $b \leftarrow\!\!\$\ \{0,1\}$
$t^* \leftarrow r^* \oplus y^*$; $c^* \leftarrow F(s^* \Vert t^*)$	$(st, m_0, m_1) \leftarrow\!\!\$\ A_1^{\mathsf{Dec}_1''(\cdot)}(1^k, pk)$
$L \leftarrow (c^*, K_H, F, m)$	If $m_b \neq m$ then $b' \leftarrow\!\!\$\ \{0,1\}$
Return (L, r^*, z^*)	Else $b' \leftarrow\!\!\$\ A_2^{\mathsf{Dec}_2''(\cdot)}(st, pk, c^*)$
	Return $(b = b')$

Fig. 21: **Distribution Samp (left) and MB-AIPO adversary D_8 (right) in the proof of Theorem 1 (cf. Game G_9).**

sub-exponentially unpredictable. Next, consider adversary D_8 attacking MB-AIPO obfuscator in Fig. 21. We get that

$$|\Pr[G_8 \Rightarrow 1] - \Pr[G_9 \Rightarrow 1]| \leq 2^\mu \cdot \mathbf{Adv}^{\text{mb-aipo}}_{\mathsf{MB\text{-}AIPO}, D_8, \mathsf{Samp}}(k) .$$

The loss factor of 2^μ in the advantage arises from Samp *guessing* the challenge message for A. This is needed because the auxiliary input for MB-AIPO cannot depend on the challenge obfuscation. However, A selects challenge messages after seeing the public key, which contains this challenge obfuscation. To make up for this, we use sub-exponential assumptions. Let α_{iO} be the security constant of the iO and let MB-AIPO be sub-exponentially secure with parameter α_{iO}. Then when iO is initialized with parameter greater than $(\mu + k)^{1/\alpha_{\mathsf{iO}}}$, we get that $|\Pr[G_8 \Rightarrow 1] - \Pr[G_9 \Rightarrow 1]| \leq 2^{-k}$.

Observe that adversary A running in time v wins in game G_9 with probability at least $\delta/2 - \mathsf{negl}(k)$. This quantity is at least $\delta/3$ infinitely often, and is therefore non-negligible.

However, we know that ciphertext c^* in game G_9 is independent of bit b. Therefore, advantage of adversary A winning in game G_9 is zero, contradicting our initial assumption. Hence, no PPT adversary can win game G_1 with non-negligible probability. This completes the proof of Theorem 1.

B Proof of Theorem 2

Remark 3. If SE is randomized and randomness-recovering (meaning the decryptor recovers the same coins used by the encryptor), then in $\overline{\mathsf{FO}}.\mathsf{Enc}$, $\mathcal{E}^{\mathsf{sy}}_K(m \Vert r)$ can be safely changed to $\mathcal{E}^{\mathsf{sy}}_K(m; r)$ and our modified transform introduces *no additional overhead*. Essentially the same proof works as the game hops are unaffected.

Remark 4. We comment on the existence of MB-AIPO secure wrt. the above auxiliary input distributions. Distribution $\mathcal{D}_7$ (Fig. 22) is unconditionally sub-exponentially statistically unpredictable, so any sup-MB-AIPO will meet the corresponding requirement. We argue in Section B.1 that if PKE is sub-exponentially

lossy, then the oracle $\mathsf{PCO}_{sk'}(\cdot,\cdot)$ can be eliminated in $(\mathsf{PCO}_{sk'}(\cdot,\cdot), \mathcal{D}_1^{\mathcal{FO}})$, and we show in Section C.3 that under this assumption $\mathcal{D}_1^{\mathcal{FO}}$ is also sub-exponentially statistically unpredictable. In Section 5 we give a new ELF-based sup-MB-AIPO construction that we show in Section C.3 is secure wrt. $(\mathcal{V}_{K^*}(\cdot), \mathcal{D}_1^{\mathcal{FO}})$ under appropriate assumptions that make $\mathcal{D}_1^{\mathcal{FO}}$ statistically unpredictable. Unfortunately, it is not known to be *sub-exponentially* secure (but nevertheless suffices for public-key-independent messages); for that, we conjecture one can use the MB-AIPO of Bitansky and Canetti [14] under a sub-exponential version of their assumption.

Remark 5. As in the RSA-OAEP instantiation, in our FO instantiation one can remove all sub-exponential assumptions at the price of only handling public-key-independent message security.

Fig. 22 defines the distributions $\mathcal{D}_1^{\mathcal{FO}} = \{D_{1,k}^{\mathcal{FO}}\}_{k\in\mathbb{N}}$ and $\mathcal{D}_7 = \{D_{7,k}\}_{k\in\mathbb{N}}$ that will be needed for the proof.

Distribution $D_{1,k}^{\mathcal{FO}}$	**Distribution** $D_{7,k}$
$r^* \leftarrow\!\!\$\ \mathsf{G.Dom}(k)\ ;\ z^* \leftarrow\!\!\$\ \mathsf{PKE.Coins}(1^k)$	$K^* \leftarrow\!\!\$\ \{0,1\}^k\ ;\ t \leftarrow\!\!\$\ \{0,1\}^k$
$K^* \leftarrow\!\!\$\ \{0,1\}^k\ ;\ \ m \leftarrow\!\!\$\ \{0,1\}^\mu$	$d \leftarrow \langle t, K^*\rangle\ ;\ r^* \leftarrow\!\!\$\ \mathsf{G.Dom}(k)$
$(pk', sk') \leftarrow\!\!\$\ \mathsf{PKE.Kg}(1^k)$	$z^* \leftarrow\!\!\$\ \mathsf{PKE.Coins}(1^k)$
$c_1^* \leftarrow \mathsf{PKE.Enc}(pk', r^*; z^*)$	$(pk', sk') \leftarrow\!\!\$\ \mathsf{PKE.Kg}(1^k)$
$c_2^* \leftarrow\!\!\$\ \mathcal{E}_{K^*}^{\mathsf{sy}}(m\|r^*)\ ;\ \ c^* \leftarrow (c_1^*, c_2^*)$	$c_1^* \leftarrow \mathsf{PKE.Enc}(pk', r^*; z^*)$
$aux \leftarrow (c^*, pk', m)$	$aux \leftarrow (t, d, pk', sk')$
Return $(aux, r^*\|c_1^*, K^*)$	Return $(aux, r^*\|c_1^*, K^*)$

Fig. 22: **MB-AIPO distributions** $\mathcal{D}_1^{\mathcal{FO}} = \{D_{1,k}^{\mathcal{FO}}\}_{k\in\mathbb{N}}$ **and** $\mathcal{D}_7 = \{D_{7,k}\}_{k\in\mathbb{N}}$**.**

Proof. Consider games G_1–G_{10} in Fig. 23 and Fig. 24.

Game G_1**:** This is the standard IND-CCA2 game. Suppose PPT adversary $A = (A_1, A_2)$ runs in time v and wins game G_1 with non-negligible probability ϵ. Let δ be an inverse polynomial in k such that $\epsilon \geq \delta$ infinitely often.

Game G_2**:** Game G_2 is similar to game G_1 except that we puncture the PRF key K_{PRF} at $r^*\|c_1^*$. Moreover, the hash key K_G does not consist of an obfuscation of $\mathcal{C}_1[K_{\mathsf{PRF}}, f]$, but rather of an obfuscation of the circuit $\mathcal{C}_2[K_{\mathsf{PRF}}^*, f, p]$. Here, p is the MB-AIPO obfuscation of the multi-bit point function $p_{r^*\|c_1^*,\, K^*}$ and thus, $p(x)$ outputs K^* if and only if $x = r^*\|c_1^*$. The two circuits are functionally equivalent and the same size by *pad*. Therefore, considering the iO adversary D_1 in Fig. 25 (left) we get $|\Pr[\,G_1 \Rightarrow 1\,] - \Pr[\,G_2 \Rightarrow 1\,]| \leq \mathbf{Adv}^{\mathrm{io}}_{\mathsf{iO},D_1,\mathcal{C}}(k)$.

Game G_3**:** Game G_3 is similar to game G_2 except that t^* is chosen randomly from $\mathsf{PRF.Rng}(k)$. Considering the adversary D_2 attacking pseudorandom function PRF at the punctured points in Fig. 25 (right), we get that $|\Pr[\,G_2 \Rightarrow 1\,] - \Pr[\,G_3 \Rightarrow 1\,]| \leq \mathbf{Adv}^{\mathrm{pprf}}_{\mathsf{PRF},D_2}(k)$.

Games $G_1(k)$, $G_2(k)$	**Games** $G_3(k)$, $G_4(k)$
$K_{\mathsf{PRF}} \leftarrow\!\$\ \mathsf{PRF.Kg}(1^k)$; $f \leftarrow\!\$\ \mathsf{ELF.IKg}(1^k)$	$K_{\mathsf{PRF}} \leftarrow\!\$\ \mathsf{PRF.Kg}(1^k)$; $f \leftarrow\!\$\ \mathsf{ELF.IKg}(1^k)$
$r^* \leftarrow\!\$\ \mathsf{G.Dom}(k)$; $z^* \leftarrow\!\$\ \mathsf{PKE.Coins}(1^k)$	$r^* \leftarrow\!\$\ \mathsf{G.Dom}(k)$; $z^* \leftarrow\!\$\ \mathsf{PKE.Coins}(1^k)$
$(pk', sk') \leftarrow\!\$\ \mathsf{PKE.Kg}(1^k)$	$(pk', sk') \leftarrow\!\$\ \mathsf{PKE.Kg}(1^k)$
$c_1^* \leftarrow \mathsf{PKE.Enc}(pk', r^*; z^*)$	$c_1^* \leftarrow \mathsf{PKE.Enc}(pk', r^*; z^*)$
$t^* \leftarrow \mathsf{PRF}_{K_{\mathsf{PRF}}}(r^* \Vert c_1^*)$; $K^* \leftarrow f(t^*)$	$\boxed{t^* \leftarrow\!\$\ \mathsf{PRF.Rng}(k)}$; $K^* \leftarrow f(t^*)$
$K^*_{\mathsf{PRF}} \leftarrow\!\$\ \mathsf{PRF.Punct}(K_{\mathsf{PRF}}, r^* \Vert c_1^*)$	$K^* \leftarrow\!\$\ \{0,1\}^k$
$p \leftarrow\!\$\ \mathsf{MB\text{-}AIPO}(r^* \Vert c_1^*, K^*)$	$K^*_{\mathsf{PRF}} \leftarrow\!\$\ \mathsf{PRF.Punct}(K_{\mathsf{PRF}}, r^* \Vert c_1^*)$
$K_G \leftarrow\!\$\ \mathsf{iO}(pad(\mathcal{C}_1[K_{\mathsf{PRF}}, f]))$	$p \leftarrow\!\$\ \mathsf{MB\text{-}AIPO}(r^* \Vert c_1^*, K^*)$
$K_G \leftarrow\!\$\ \mathsf{iO}(\mathcal{C}_2[K^*_{\mathsf{PRF}}, f, p])$	$K_G \leftarrow\!\$\ \mathsf{iO}(\mathcal{C}_2[K^*_{\mathsf{PRF}}, f, p])$
$pk \leftarrow (pk', K_G)$; $sk \leftarrow (sk', K_G)$	$pk \leftarrow (pk', K_G)$; $sk \leftarrow (sk', K_G)$
$b \leftarrow\!\$\ \{0,1\}$; $(st, m_0, m_1) \leftarrow\!\$\ A_1^{\mathsf{Dec}(\cdot)}(1^k, pk)$	$b \leftarrow\!\$\ \{0,1\}$; $(st, m_0, m_1) \leftarrow\!\$\ A_1^{\mathsf{Dec}(\cdot)}(1^k, pk)$
$c_2^* \leftarrow \mathcal{E}^{\mathsf{sy}}_{K^*}(m_b \Vert r^*)$; $c^* \leftarrow (c_1^*, c_2^*)$	$c_2^* \leftarrow \mathcal{E}^{\mathsf{sy}}_{K^*}(m_b \Vert r^*)$; $c^* \leftarrow (c_1^*, c_2^*)$
$b' \leftarrow\!\$\ A_2^{\mathsf{Dec}(\cdot)}(st, pk, c^*)$	$b' \leftarrow\!\$\ A_2^{\mathsf{Dec}(\cdot)}(st, pk, c^*)$
Return $(b = b')$	Return $(b = b')$

Games $G_5(k)$, $G_6(k)$	**Games** $G_7(k)$, $G_8(k)$
$K_{\mathsf{PRF}} \leftarrow\!\$\ \mathsf{PRF.Kg}(1^k)$; $f \leftarrow\!\$\ \mathsf{ELF.IKg}(1^k)$	$K_{\mathsf{PRF}} \leftarrow\!\$\ \mathsf{PRF.Kg}(1^k)$; $f \leftarrow\!\$\ \mathsf{ELF.LKg}(1^k)$
$f \leftarrow\!\$\ \mathsf{ELF.LKg}(1^k)$; $z^* \leftarrow\!\$\ \mathsf{PKE.Coins}(1^k)$	$r^* \leftarrow\!\$\ \mathsf{G.Dom}(k)$; $z^* \leftarrow\!\$\ \mathsf{PKE.Coins}(1^k)$
$r^* \leftarrow\!\$\ \mathsf{G.Dom}(k)$; $(pk', sk') \leftarrow\!\$\ \mathsf{PKE.Kg}(1^k)$	$(pk', sk') \leftarrow\!\$\ \mathsf{PKE.Kg}(1^k)$
$c_1^* \leftarrow \mathsf{PKE.Enc}(pk', r^*; z^*)$; $K^* \leftarrow\!\$\ \{0,1\}^k$	$c_1^* \leftarrow \mathsf{PKE.Enc}(pk', r^*; z^*)$; $K^* \leftarrow\!\$\ \{0,1\}^k$
$p \leftarrow\!\$\ \mathsf{MB\text{-}AIPO}(r^* \Vert c_1^*, K^*)$	$p \leftarrow\!\$\ \mathsf{MB\text{-}AIPO}(r^* \Vert c_1^*, K^*)$
$\boxed{K_G \leftarrow\!\$\ \mathsf{iO}(\mathcal{C}_2[K_{\mathsf{PRF}}, f, p])}$	$K_G \leftarrow\!\$\ \mathsf{iO}(\mathcal{C}_2[K_{\mathsf{PRF}}, f, p])$; $pk \leftarrow (pk', K_G)$
$pk \leftarrow (pk', K_G)$; $sk \leftarrow (sk', K_G)$	$sk \leftarrow (sk', K_G)$; $b \leftarrow\!\$\ \{0,1\}$
$b \leftarrow\!\$\ \{0,1\}$; $(st, m_0, m_1) \leftarrow\!\$\ A_1^{\mathsf{Dec}(\cdot)}(1^k, pk)$	$\boxed{(st, m_0, m_1) \leftarrow\!\$\ A_1^{\mathsf{Dec}'_1(G_7,\cdot)}(1^k, pk)}$
$(st, m_0, m_1) \leftarrow\!\$\ A_1^{\mathsf{Dec}'_1(G_6,\cdot)}(1^k, pk)$	$(st, m_0, m_1) \leftarrow\!\$\ A_1^{\mathsf{Dec}'_1(G_8,\cdot)}(1^k, pk)$
$c_2 \leftarrow \mathcal{E}^{\mathsf{sy}}_{K^*}(m_b \Vert r^*)$; $c^* \leftarrow (c_1^*, c_2^*)$	$c_2 \leftarrow \mathcal{E}^{\mathsf{sy}}_{K^*}(m_b \Vert r^*)$; $c^* \leftarrow (c_1^*, c_2^*)$
$b' \leftarrow\!\$\ A_2^{\mathsf{Dec}(\cdot)}(st, pk, c^*)$	$\boxed{b' \leftarrow\!\$\ A_2^{\mathsf{Dec}'_2(G_7,\cdot)}(st, pk, c^*)}$
$b' \leftarrow\!\$\ A_2^{\mathsf{Dec}'_2(G_6,\cdot)}(st, pk, c^*)$	$b' \leftarrow\!\$\ A_2^{\mathsf{Dec}'_2(G_8,\cdot)}(st, pk, c^*)$
Return $(b = b')$	Return $(b = b')$

Circuit $\mathcal{C}_1[K_{\mathsf{PRF}}, f](x)$	**Circuit** $\mathcal{C}_2[K_{\mathsf{PRF}}, f, p](x)$
Return $f(\mathsf{PRF}_{K_{\mathsf{PRF}}}(x))$	If $p(x) = \perp$ then return $f(\mathsf{PRF}_{K_{\mathsf{PRF}}}(x))$
	Return $p(x)$

Fig. 23: **Games G_1–G_8 in the proof of Theorem 2. The boxes highlight the difference between adjacent games in different cells.**

Game G_4: Game G_4 is similar to game G_3 except that K^* is chosen randomly from $\{0,1\}^k$. By Proposition 1 (since ELF is augmented, cf. Section 3.1), we get that $|\Pr[G_3 \Rightarrow 1] - \Pr[G_4 \Rightarrow 1]|$ is negligible.

Game G_5: Game G_5 is similar to game G_4 except that an obfuscation of circuit $\mathcal{C}_2[K_{\mathsf{PRF}}, f, p]$ is used as the hash key K_G, instead of $\mathcal{C}_2[K^*_{\mathsf{PRF}}, f, p]$, where

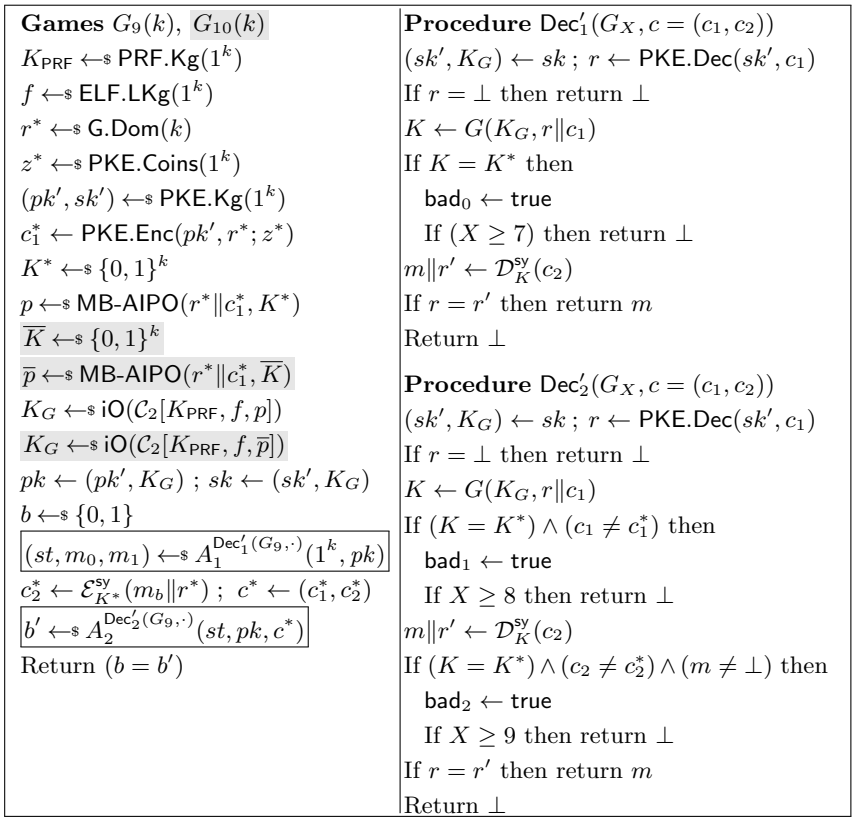

Fig. 24: **Games G_9, G_{10} and bad flag decryption oracles for games $G_6 - G_{10}$ in the proof of Theorem 2. Boxes in G_9 highlight the differences from G_8.**

K_{PRF} is the original key and K^*_{PRF} is punctured at $r^* \| c_1^*$. The two circuits are functionally equivalent since they both output $f(\mathsf{PRF}_{K_{\mathsf{PRF}}}(x))$ when $x \neq r^* \| c_1^*$, and output K^* otherwise. Therefore, considering the iO adversary D_4, we get that $|\Pr[\, G_4 \Rightarrow 1\,] - \Pr[\, G_5 \Rightarrow 1\,]| \leq \mathbf{Adv}^{\mathsf{io}}_{\mathsf{iO}, D_4, \mathcal{C}}(k)$. A description of adversary D_4 is omitted due to its similarity to D_1 (Fig. 25, left).

Game G_6: Game G_6 is similar to game G_5 except that ELF is switched to lossy mode. That is, we generate $f \leftarrow\$ \mathsf{ELF.LKg}(1^k, \mathsf{poly}(\mathsf{v}, 2/\delta))$, where $\mathsf{poly}(\mathsf{v}, 2/\delta)$ is a polynomial in two variables. This means no adversary running in time v can distinguish the mode of f with more than a $\delta/2$ probability. Considering a standard ELF adversary D_5 attacking lossiness of ELF running in time v, we get that $|\Pr[\, G_5 \Rightarrow 1\,] - \Pr[\, G_6 \Rightarrow 1\,]| \leq \delta/2$. In Figure 23 the second input to $\mathsf{ELF.LKg}$ is omitted since $\mathsf{poly}(\mathsf{v}, 2/\delta)$ depends on the adversary's running time, v.

Game G_6 also introduces flags bad_0, bad_1, and bad_2 to the decryption oracles (Fig. 24, right) which do not affect the output of G_6. These flags are used to analyze later game transitions. Let $\bar{c} = (\bar{c}_1, \bar{c}_2)$ be a decryption query made

Adversary $D_1^{\mathsf{iO}(\mathsf{LR}(\cdot,\cdot,d))}(1^k)$
$K_{\mathsf{PRF}} \leftarrow\!\$\ \mathsf{PRF.Kg}(1^k)\ ;\ f \leftarrow\!\$\ \mathsf{ELF.IKg}(1^k)$
$r^* \leftarrow\!\$\ \mathsf{G.Dom}(k)\ ;\ z^* \leftarrow\!\$\ \mathsf{PKE.Coins}(1^k)$
$(pk', sk') \leftarrow\!\$\ \mathsf{PKE.Kg}(1^k)$
$c_1^* \leftarrow \mathsf{PKE.Enc}(pk', r^*; z^*)$
$t^* \leftarrow \mathsf{PRF}_{K_{\mathsf{PRF}}}(r^* \| c_1^*)\ ;\ K^* \leftarrow f(t^*)$
$K^*_{\mathsf{PRF}} \leftarrow\!\$\ \mathsf{PRF.Punct}(K_{\mathsf{PRF}}, r^* \| c_1^*)$
$p \leftarrow\!\$\ \mathsf{MB\text{-}AIPO}(r^* \| c_1^*, K^*)$
$C' \leftarrow\!\$\ pad(\mathcal{C}_1[K_{\mathsf{PRF}}, f])\ ;\ C'' \leftarrow\!\$\ \mathcal{C}_2[K^*_{\mathsf{PRF}}, f, p]$
$K_G \leftarrow \mathsf{iO}(\mathsf{LR}(C', C''))$
$pk \leftarrow (pk', K_G)\ ;\ sk \leftarrow (sk', K_G)$
$b \leftarrow\!\$\ \{0,1\}\ ;\ (st, m_0, m_1) \leftarrow\!\$\ A_1^{\mathsf{Dec}(\cdot)}(1^k, pk)$
$c_2^* \leftarrow \mathcal{E}^{\mathsf{sy}}_{K^*}(m_b \| r^*)\ ;\ c^* \leftarrow (c_1^*, c_2^*)$
$b' \leftarrow\!\$\ A_2^{\mathsf{Dec}(\cdot)}(st, pk, c^*)$
Return $(b = b')$

Adversary $D_2(r^* \| c_1^*, K^*_{\mathsf{PRF}}, t^*)$
$f \leftarrow\!\$\ \mathsf{ELF.IKg}(1^k)\ ;\ K^* \leftarrow f(t^*)$
$p \leftarrow\!\$\ \mathsf{MB\text{-}AIPO}(r^* \| c_1^*, K^*)$
$K_G \leftarrow\!\$\ \mathsf{iO}(\mathcal{C}_2[K^*_{\mathsf{PRF}}, f, p])$
$(pk', sk') \leftarrow\!\$\ \mathsf{PKE.Kg}(1^k)$
$pk \leftarrow (pk', K_G)\ ;\ sk \leftarrow (sk', K_G)$
$b \leftarrow\!\$\ \{0,1\}$
$(st, m_0, m_1) \leftarrow\!\$\ A_1^{\mathsf{Dec}(\cdot)}(1^k, pk)$
$c_2^* \leftarrow \mathcal{E}^{\mathsf{sy}}_{K^*}(m_b \| r^*)\ ;\ c^* \leftarrow (c_1^*, c_2^*)$
$b' \leftarrow\!\$\ A_2^{\mathsf{Dec}(\cdot)}(st, pk, c^*)$
Return $(b = b')$

Circuit $\mathcal{C}_1[K_{\mathsf{PRF}}, f](x)$
Return $f(\mathsf{PRF}_{K_{\mathsf{PRF}}}(x))$

Circuit $\mathcal{C}_2[K^*_{\mathsf{PRF}}, f, p](x)$
If $p(x) = \perp$ then return $f(\mathsf{PRF}_{K^*_{\mathsf{PRF}}}(x))$
Return $p(x)$

Procedure $\mathsf{Dec}(c)$
$m \leftarrow \overline{\mathsf{FO}}.\mathsf{Dec}(sk, c)$
Return m

Fig. 25: iO **adversary** D_1 **(left) and punctured** PRF **adversary** D_2 **(right) (cf. Theorem 2, games** G_2**,** G_3 **resp.).**

to A's oracle. Moreover, let $\overline{K}$ be the symmetric-key generated during the decryption process of $\overline{c}$ (which could be $\perp$). Game G_6 sets...

- Flag bad_0 when A_1 makes a decryption query such that $\overline{K} = K^*$.
- Flag bad_1 when A_2 makes a decryption query such that $\overline{K} = K^*$ and $\overline{c}_1 \neq c_1^*$.
- Flag bad_2 when A_2 makes a decryption query such that $\overline{K} = K^*$, $\overline{c}_1 = c_1^*$, $\overline{c}_2 \neq c_2^*$, and $\overline{c}_2$ is a valid ciphertext.

Game G_7**:** Game G_7 is similar to game G_6 except that in G_7 oracle $\mathsf{Dec}'_1(G_7, c)$ returns $\perp$ after bad_0 is set. As G_6, G_7 are identical-until-bad_0, by the fundamental lemma of game-playing [12], we have $\Pr[G_6 \Rightarrow 1] \leq \Pr[G_7 \Rightarrow 1] + \Pr[G_6 \text{ sets } \mathsf{bad}_0]$. bad_0 being set indicates that A_1 was able to find K^*. The only information on K^* A_1 gets is K_G, which depends on p, which is an MB-AIPO with output point K^*. In Fig. 26, we construct an MB-AIPO adversary B_7 for which we claim that

$$\Pr[G_6 \text{ sets } \mathsf{bad}_0] \ \leq\ \mathbf{Adv}^{\text{mb-aipo}}_{\mathsf{MB\text{-}AIPO}, B_7, \mathcal{D}_7}(k) + q_d/2^k\ .$$

Distribution $D_{7,k}$	**Adversary** $B_7(1^k, aux, p)$
$K^* \leftarrow\!\!\$\ \{0,1\}^k\ ;\ t \leftarrow\!\!\$\ \{0,1\}^k$	$(t, d, pk', sk') \leftarrow aux$
$d \leftarrow \langle t, K^* \rangle\ ;\ r^* \leftarrow\!\!\$\ \mathsf{G.Dom}(k)$	$f \leftarrow\!\!\$\ \mathsf{ELF.LKg}(1^k)\ ;\ b' \leftarrow 0$
$z^* \leftarrow\!\!\$\ \mathsf{PKE.Coins}(1^k)$	$K_{\mathsf{PRF}} \leftarrow\!\!\$\ \mathsf{PRF.Kg}(1^k)$
$(pk', sk') \leftarrow\!\!\$\ \mathsf{PKE.Kg}(1^k)$	$K_G \leftarrow\!\!\$\ \mathsf{iO}(\mathcal{C}_2[K_{\mathsf{PRF}}, f, p])$
$c_1^* \leftarrow \mathsf{PKE.Enc}(pk', r^*; z^*)$	$pk \leftarrow (pk', K_G)\ ;\ sk \leftarrow (sk', K_G)$
$aux \leftarrow (t, d, pk', sk')$	$(st, m_0, m_1) \leftarrow\!\!\$\ A_1^{\mathsf{Dec}_{B_7}(\cdot)}(1^k, pk)$
Return $(aux, r^* \| c_1^*, K^*)$	Return b'

Procedure $\mathsf{Dec}_{B_7}(c = (c_1, c_2))$
$r \leftarrow \mathsf{PKE.Dec}(sk', c_1)$
If $p(r\|c_1) = \perp$ then return $\overline{\mathsf{FO}}.\mathsf{Dec}(sk, c)$
$K \leftarrow p(r\|c_1)$
If $\langle\, t, K \,\rangle = d$ then $b' \leftarrow 1$
Return $\perp$

Fig. 26: **MB-AIPO adversary B_7, its simulated decryption oracle Dec_{B_7}, and associated distribution $\mathcal{D}_7 = \{D_{7,k}\}_{k\in\mathbb{N}}$ (cf. Theorem 2, game G_7).**

Adversary B_7 does not run A_2 since only A_1 has the ability to set bad_0. To justify the claim, first write

$$\mathbf{Adv}^{\text{mb-aipo}}_{\mathsf{MB\text{-}AIPO},B_7,\mathcal{D}_7}(k) = |\Pr\left[\,\text{MB-AIPO}^{\mathcal{D}_7,B_7,1}_{\mathsf{MB\text{-}AIPO}}(k) \Rightarrow 1\,\right] - \Pr\left[\,\text{MB-AIPO}^{\mathcal{D}_7,B_7,0}_{\mathsf{MB\text{-}AIPO}}(k) \Rightarrow 1\,\right]|\ ,$$

where the 0 and 1 superscripts represent the games with random and real MB-AIPO challenges, respectively. Observe that

$$\Pr\left[\,\text{MB-AIPO}^{\mathcal{D}_7,B_7,1}_{\mathsf{MB\text{-}AIPO}}(k) \Rightarrow 1\,\right] = \Pr\left[\,G_6 \text{ sets } \mathsf{bad}_0\,\right].$$

This is because both events occur if and only if A_1 obtains K^* from K_G. In the random challenge case, A_1 gets no information on K^* so,

$$\Pr\left[\,\text{MB-AIPO}^{\mathcal{D}_7,B_7,0}_{\mathsf{MB\text{-}AIPO}}(k) \Rightarrow 1\,\right] \ \le\ q_d/2^k$$

where q_d bounds A_1's number of decryption queries. Rearranging yields the claim. Note that the MB-AIPO distribution $\mathcal{D}_7$ (Fig. 26, left) is statistically unpredictable.

Game G_8: Game G_8 is similar to game G_7 except that in G_8 A_1 and A_2 have updated decryption oracles $\mathsf{Dec}'_{\mathsf{flag}}(G_8, \cdot)$ where $\mathsf{flag} \in \{1, 2\}$ (shown in Fig. 24, right). $\mathsf{Dec}'_1(G_8, \cdot)$ is the same as $\mathsf{Dec}'_1(G_7, \cdot)$, but $\mathsf{Dec}'_2(G_8, c)$ returns $\perp$ when bad_1 is set. As G_7, G_8 are identical-until-bad_1, by the fundamental lemma of game-playing [12] we have $\Pr[\,G_7 \Rightarrow 1\,] \le \Pr[\,G_8 \Rightarrow 1\,] + \Pr[\,G_7 \text{ sets } \mathsf{bad}_1\,]$. We claim that

$$\Pr[\,G_7 \text{ sets } \mathsf{bad}_1\,] \le \frac{\mathsf{poly}(\mathsf{v}, 2/\delta)}{2^k}\ .$$

To see this, note that for a bad_1 decryption query $(\overline{c}_1 \neq c_1^*, \overline{c}_2)$ with $\overline{K} = K^*$, we have

$$\mathsf{iO}(\mathcal{C}_2[K_{\mathsf{PRF}}, f, p])(\overline{r}\|\overline{c}_1) = f(\mathsf{PRF}_{K_{\mathsf{PRF}}}(\overline{r}\|\overline{c}_1)) = K^* \ ,$$

where $f \leftarrow\!\!\$\ \mathsf{ELF.LKg}(1^k, \mathsf{poly}(\mathsf{v}, 2/\delta))$ and $\overline{r} \leftarrow \mathsf{PKE.Dec}(sk', \overline{c}_1)$. Since K^* is sampled independently and uniformly at random from the injective ELF range, the probability K^* is in the lossy ELF range is at most $\mathsf{poly}(\mathsf{v}, 2/\delta)/2^k$, giving us the claim.

Game G_9**:** Game G_9 is similar to game G_8 except that $\mathsf{Dec}_2'(G_9, \cdot)$ returns $\perp$ when bad_2 is set (shown in Fig. 24, right). As G_8, G_9 are identical-until-bad_2, by the fundamental lemma of game-playing [12] we have $|\Pr[\,G_8 \Rightarrow 1\,] - \Pr[\,G_9 \Rightarrow 1\,]| \leq \Pr[\,G_8 \text{ sets } \mathsf{bad}_2\,]$. bad_2 being set indicates that A_2 has found a valid symmetric key ciphertext under K^* not equal to the challenge symmetric ciphertext, c_2^*.
So, consider the AE-AUX adversary $\overline{B}_9$ wrt. $(\mathsf{PCO}_{sk'}(\cdot,\cdot), \mathcal{D}_2^{\mathcal{F}\mathcal{O}})$ in Fig. 27. In this game $\overline{B}_9$ has, in additional to its usual two oracles, access to the $\mathsf{PCO}_{sk'}(\cdot,\cdot)$ oracle[11] and the auxiliary information given by the distribution $\mathcal{D}_2^{\mathcal{F}\mathcal{O}}$ (Fig. 27). It follows from the theorem assumptions that SE is secure wrt. $(\mathsf{PCO}_{sk'}(\cdot,\cdot), \mathcal{D}_2^{\mathcal{F}\mathcal{O}})$ (proven in Lemma 1). Note that $\overline{B}_9$'s decryption oracle $\mathsf{Dec}_{\overline{B}_9}$ uses $\mathcal{O}_2(\cdot)$ (either the verification oracle $\mathcal{V}_K(\cdot)$ or $\perp(\cdot)$ depending on the game world) to determine if bad_2 would have been set in G_8. $\overline{B}_9$ does not use oracle $\mathcal{O}_1(\cdot)$ because SE is only *one-time* AE. c_2^* and m are in *aux* given as input to $\overline{B}_9$. This takes the place of one $\mathcal{O}_1(\cdot)$ query.
Recall the advantage definition,

$$\mathbf{Adv}^{\text{ae-aux}}_{\mathsf{SE},\overline{B}_9,\mathcal{D}_2^{\mathcal{F}\mathcal{O}},\mathsf{PCO}_{sk'}}(k) = \Big|\Pr\Big[\,\text{AE-AUX}^{\overline{B}_9,1}_{\mathsf{SE},\mathcal{D}_2^{\mathcal{F}\mathcal{O}},\mathsf{PCO}_{sk'}}(k) \Rightarrow 1\,\Big] - \Pr\Big[\,\text{AE-AUX}^{\overline{B}_9,0}_{\mathsf{SE},\mathcal{D}_2^{\mathcal{F}\mathcal{O}},\mathsf{PCO}_{sk'}}(k) \Rightarrow 1\,\Big]\Big| \ ,$$

where the 0 and 1 superscripts represent the games in which $\overline{B}_9$ has random (i.e. $\$(\cdot), \perp(\cdot)$) and real (i.e. $\mathcal{E}_{K^*}(\cdot), \mathcal{V}_{K^*}(\cdot)$) oracles, respectively.
Consider a G_8 coin sequence on which bad_2 gets set. When $\overline{B}_9$'s game is run on the corresponding coin sequence, and when $m = m_b$, $\overline{B}_9$ then correctly guesses the challenge bit b. If $m \neq m_b$, then $\overline{B}_9$ outputs 0. Since $m \in \{0,1\}^\mu$ is random and independent of the view of A, we have

$$\Pr[\,G_8 \text{ sets } \mathsf{bad}_2\,] \leq 2^\mu \cdot \mathbf{Adv}^{\text{ae-aux}}_{\mathsf{SE},\overline{B}_9,\mathcal{D}_2^{\mathcal{F}\mathcal{O}},\mathsf{PCO}_{sk'}}(k) \ .$$

We compensate for the 2^μ factor using sub-exponential assumptions.

Game G_{10}**:** Game G_{10} is similar to game G_9 except that the hash key K_G consists of an obfuscation of the circuit $\mathcal{C}_2[K_{\mathsf{PRF}}, f, \overline{p}]$, where $\overline{p}$ has random output point $\overline{K}$, instead of K^*. K^* is still used as the symmetric encryption key. Circuits $\mathcal{C}_2[K_{\mathsf{PRF}}, f, p]$ and $\mathcal{C}_2[K_{\mathsf{PRF}}, f, \overline{p}]$ only differ on the single point

[11] Recall $\mathsf{PCO}_{sk'}(\cdot,\cdot)$ is a plaintext-checking oracle that on input (c, m) outputs 1 iff $\mathsf{PKE.Dec}(sk', c) = m$.

Adv $\overline{B}_9^{\mathcal{O}_1(\cdot),\mathcal{O}_2(\cdot),\mathsf{PCO}_{sk'}(\cdot,\cdot)}(1^k, aux)$	**Distribution** $D_{2,k}^{\mathcal{F}\mathcal{O}}$
$(p, c_1^*, c_2^*, pk', m) \leftarrow aux$	$K^* \leftarrow\!\!\$\ \{0,1\}^k$; $r^* \leftarrow\!\!\$\ \mathsf{G.Dom}(k)$
$K_{\mathsf{PRF}} \leftarrow\!\!\$\ \mathsf{PRF.Kg}(1^k)$	$z^* \leftarrow\!\!\$\ \mathsf{PKE.Coins}(1^k)$
$f \leftarrow\!\!\$\ \mathsf{ELF.LKg}(1^k)$	$(pk', sk') \leftarrow\!\!\$\ \mathsf{PKE.Kg}(1^k)$
$K_G \leftarrow\!\!\$\ \mathsf{iO}(\mathcal{C}_2[K_{\mathsf{PRF}}, f, p])$	$c_1^* \leftarrow \mathsf{PKE.Enc}(pk', r^*; z^*)$
$pk \leftarrow (pk', K_G)$; $b \leftarrow\!\!\$\ \{0,1\}$	$p \leftarrow\!\!\$\ \mathsf{MB\text{-}AIPO}(r^* \| c_1^*, K^*)$
$(st, m_0, m_1) \leftarrow\!\!\$\ A_1^{\mathsf{Dec}_{\overline{B}_9}(1,\cdot)}(1^k, pk)$	$m \leftarrow\!\!\$\ \{0,1\}^\mu$; $c_2^* \leftarrow \mathcal{E}_{K^*}^{\mathsf{sy}}(m \| r^*)$
If $m \neq m_b$ then return 0	$aux \leftarrow (p, c_1^*, c_2^*, pk', m)$
$c^* \leftarrow (c_1^*, c_2^*)$; $\mathsf{win} \leftarrow 0$	Return (aux, K^*)
Run $A_2^{\mathsf{Dec}_{\overline{B}_9}(2,\cdot)}(st, pk, c^*)$	
Return win	

Procedure $\mathsf{Dec}_{\overline{B}_9}(\mathsf{flag}, c = (c_1, c_2))$
If $\mathsf{flag} = 2 \ \wedge \ c_2 \neq c_2^*$ then
  $d \leftarrow \mathcal{O}_2(c_2)$
  If $d = 1$ then $\mathsf{win} \leftarrow 1$
For all $K \in [f(\cdot)]$ do
  $m \| r \leftarrow \mathcal{D}_K^{\mathsf{sy}}(c_2)$
  If $m \| r \neq \perp \wedge \mathsf{PCO}_{sk'}(c_1, r) = 1 \wedge G(K_G, r \| c_1) = K$ then
    Return m
Return $\perp$

Fig. 27: AE-AUX **with adaptive auxiliary-input adversary** $\overline{B}_9$ **(top left), decryption oracle (bottom), and auxiliary information distribution** $\mathcal{D}_2^{\mathcal{F}\mathcal{O}} = \{D_{2,k}^{\mathcal{F}\mathcal{O}}\}_{k\in\mathbb{N}}$ **(top right) (cf. Theorem 2, game** G_9**).**

where $p(x) \neq \perp$. We bound the difference between games G_9 and G_{10} by the security of the MB-AIPO. Consider the $\mathsf{MB\text{-}AIPO}$ adversary D_9 wrt. adaptive auxiliary input distribution $(\mathsf{PCO}_{sk'}(\cdot,\cdot), \mathcal{D}_1^{\mathcal{F}\mathcal{O}})$ in Fig. 28. We claim

$$|\Pr[\, G_9 \Rightarrow 1\,] - \Pr[\, G_{10} \Rightarrow 1\,]| \leq 2^\mu \cdot \mathbf{Adv}^{\text{mb-aipo}}_{\mathsf{MB\text{-}AIPO}, D_9, \mathsf{PCO}_{sk'}, \mathcal{D}_1^{\mathcal{F}\mathcal{O}}}(k)\ .$$

To justify this, we write

$$\mathbf{Adv}^{\text{mb-aipo}}_{\mathsf{MB\text{-}AIPO}, D_9, \mathsf{PCO}_{sk'}, \mathcal{D}_1^{\mathcal{F}\mathcal{O}}}(k) = |\Pr\left[\,\text{MB-AIPO}^{\mathsf{PCO}_{sk'}, \mathcal{D}_1^{\mathcal{F}\mathcal{O}}, D_9, 1}_{\mathsf{MB\text{-}AIPO}}(k) \Rightarrow 1\,\right] - \Pr\left[\,\text{MB-AIPO}^{\mathsf{PCO}_{sk'}, \mathcal{D}_1^{\mathcal{F}\mathcal{O}}, D_9, 0}_{\mathsf{MB\text{-}AIPO}}(k) \Rightarrow 1\,\right]|\ ,$$

where the 0 and 1 superscripts represent the games with random (i.e. $\overline{p}$) and real (i.e. p) MB-AIPO challenges, respectively. Now observe

$$\Pr\left[\,\text{MB-AIPO}^{\mathsf{PCO}_{sk'}, \mathcal{D}_1^{\mathcal{F}\mathcal{O}}, D_9, 1}_{\mathsf{MB\text{-}AIPO}}(k) \Rightarrow 1\,\right] = 1/2^\mu \cdot \Pr[\, G_9 \Rightarrow 1\,]\ .$$

To see this, consider running $\text{MB-AIPO}^{\mathsf{PCO}_{sk'}, \mathcal{D}_1^{\mathcal{F}\mathcal{O}}, D_9, 1}_{\mathsf{MB\text{-}AIPO}}(k)$ and G_9 over the same sequence of coins. On a coin sequence where the challenge message

Distribution $D_{1,k}^{\mathcal{FO}}$	**Adversary** $D_9^{\mathsf{PCO}_{sk'}(\cdot,\cdot)}(1^k, aux, p)$
$r^* \leftarrow\!\!\$\ \mathsf{G.Dom}(k)\ ;\ z^* \leftarrow\!\!\$\ \mathsf{Coins}(1^k)$	$K_{\mathsf{PRF}} \leftarrow\!\!\$\ \mathsf{PRF.Kg}(1^k)\,;\ f \leftarrow\!\!\$\ \mathsf{ELF.LKg}(1^k)$
$K^* \leftarrow\!\!\$\ \{0,1\}^k\ ;\ m \leftarrow\!\!\$\ \{0,1\}^\mu$	$(c^*, pk', m) \leftarrow aux$
$(pk', sk') \leftarrow\!\!\$\ \mathsf{PKE.Kg}(1^k)$	$K_G \leftarrow\!\!\$\ \mathsf{iO}(\mathcal{C}_2[K_{\mathsf{PRF}}, f, p])$
$c_1^* \leftarrow \mathsf{PKE.Enc}(pk', r^*; z^*)$	$pk \leftarrow (pk', K_G)\ ;\ b \leftarrow\!\!\$\ \{0,1\}$
$c_2^* \leftarrow \mathcal{E}_{K^*}^{\mathsf{sy}}(m\|r^*)\ ;\ c^* \leftarrow (c_1^*, c_2^*)$	$(st, m_0, m_1) \leftarrow\!\!\$\ A_1^{\textsc{DecSim}(\cdot)}(1^k, pk)$
$aux \leftarrow (c^*, pk', m)$	If $m_b \neq m$ then $b' \leftarrow\!\!\$\ \{0,1\}$
Return $(aux, r^*\|c_1^*, K^*)$	Else $b' \leftarrow\!\!\$\ A_2^{\textsc{DecSim}(\cdot)}(st, pk, c^*)$
	Return $(b = b')$

Procedure $\textsc{DecSim}(c = (c_1, c_2))$
For all $K \in [f(\cdot)]$ do
  $m\|r \leftarrow \mathcal{D}_K^{\mathsf{sy}}(c_2)$
  If $m\|r \neq \perp \wedge \mathsf{PCO}_{sk'}(c_1, r) = 1 \wedge G(K_G, r\|c_1) = K$ then
    Return m
Return $\perp$

Fig. 28: **MB-AIPO adversary D_9, associated distribution $\mathcal{D}_1^{\mathcal{FO}} = \{D_{1,k}^{\mathcal{FO}}\}_{k\in\mathbb{N}}$, and simulated decryption oracle** DecSim **(cf. Theorem 2, game G_{10}).**

chosen by $D_{1,k}^{\mathcal{FO}}$ is correct ($m = m_b$), A's view is the same in both G_9 and in $\text{MB-AIPO}_{\mathsf{MB\text{-}AIPO}}^{\mathsf{PCO}_{sk'}, \mathcal{D}_1^{\mathcal{FO}}, D_9, 1}(k)$. The factor of $2^{-\mu}$ is present because $\Pr[\, m = m_b \mid m \leftarrow\!\!\$\ \{0,1\}^\mu \,] = 2^{-\mu}$ where m_b is one of the two messages output by A_1. A similar argument yields

$$\Pr\left[\, \text{MB-AIPO}_{\mathsf{MB\text{-}AIPO}}^{\mathsf{PCO}_{sk'}, \mathcal{D}_1^{\mathcal{FO}}, D_9, 0}(k) \Rightarrow 1 \,\right] = 1/2^\mu \cdot \Pr[\, G_{10} \Rightarrow 1 \,]\ .$$

To make up for the 2^μ factor we use sub-exponential assumptions. In particular, since MB-AIPO is sub-exponentially secure with parameter α_{iO} (let α_{iO} be the security constant of the iO) when iO is initialized with parameter greater than $(\mu + k)^{1/\alpha_{\mathsf{iO}}}$, we get that $|\Pr[\, G_9 \Rightarrow 1 \,] - \Pr[\, G_{10} \Rightarrow 1 \,]| \leq 2^{-k}$.

Adversary A running in time v wins in game G_{10} with probability at least $\delta/2 - \mathsf{negl}(k)$. This quantity is at least $\delta/3$ infinitely often, and is therefore non-negligible. However, considering the SE IND-CPA[12] adversary D_{10}, we obtain that $\Pr[\, G_{10} \Rightarrow 1 \,] \leq \mathbf{Adv}_{\mathsf{SE}, D_{10}}^{\text{ind-cpa}}(k)$. We omit the construction of D_{10} and note that since c_1^*, c_2^* look independent of each other to A in game G_{10} it is straight forward to construct. Therefore, we have that $\delta/3 \leq \mathbf{Adv}_{\mathsf{SE}, D_{10}}^{\text{ind-cpa}}(k)$. Since SE is assumed to be IND-CCA secure (and hence IND-CPA secure), $\mathbf{Adv}_{\mathsf{SE}, D_{10}}^{\text{ind-cpa}}(k)$ is negligible, which is a contradiction. Hence, there are no PPT adversaries that can win game G_1 with non-negligible probability.
To complete the proof we prove the following lemma (invoked in game G_9 above).

[12] SE is assumed to be AE, implying it is IND-CCA secure, which in turn implies it is also IND-CPA secure.

Adv $B^{\mathcal{V}_{K^*}(\cdot)}(1^k, aux, p)$	**Procedure** SIM-$\mathcal{V}_{K^*}(c)$
$\mathsf{win} \leftarrow 0$; $(c_1^*, c_2^*, pk', m) \leftarrow aux$	If $\mathcal{V}_{K^*}(c) = 1 \ \wedge \ c \neq c_2^*$ then
$L \leftarrow (p, c_1^*, c_2^*, pk', m)$	$\mathsf{win} \leftarrow 1$
Run $A^{\mathcal{E}_{K^*}(\cdot), \text{SIM-}\mathcal{V}_{K^*}(\cdot), \mathsf{PCO}_{sk'}(\cdot,\cdot)}(1^k, L)$	Return $\mathcal{V}_{K^*}(c)$
Return win	

Distribution $D_{1,k}^{\mathcal{FO}}$	**Distribution** $D_{2,k}^{\mathcal{FO}}$
$r^* \leftarrow\!\!\$\ \mathsf{G.Dom}(k)$; $K^* \leftarrow\!\!\$\ \{0,1\}^k$	$K^* \leftarrow\!\!\$\ \{0,1\}^k$; $r^* \leftarrow\!\!\$\ \mathsf{G.Dom}(k)$
$m \leftarrow\!\!\$\ \{0,1\}^\mu$; $(pk', sk') \leftarrow\!\!\$\ \mathsf{LPKE.Kg}(1^k)$	$z^* \leftarrow\!\!\$\ \mathsf{PKE.Coins}(1^k)$
$c_1^* \leftarrow\!\!\$\ \mathsf{LPKE.Enc}(pk', r^*)$	$(pk', sk') \leftarrow\!\!\$\ \mathsf{PKE.Kg}(1^k)$
$c_2^* \leftarrow\!\!\$\ \mathcal{E}_{K^*}^{\mathsf{sy}}(m \| r^*)$; $c^* \leftarrow (c_1^*, c_2^*)$	$c_1^* \leftarrow \mathsf{PKE.Enc}(pk', r^*; z^*)$
$aux \leftarrow (c^*, pk', m)$	$p \leftarrow\!\!\$\ \mathsf{MB\text{-}AIPO}(r^* \| c_1^*, K^*)$
Return $(aux, r^* \| c_1^*, K^*)$	$m \leftarrow\!\!\$\ \{0,1\}^\mu$; $c_2^* \leftarrow \mathcal{E}_{K^*}^{\mathsf{sy}}(m \| r^*)$
	$aux \leftarrow (p, c_1^*, c_2^*, pk', m)$
	Return (aux, K^*)

Fig. 29: **MB-AIPO adversary B and the simulated $\mathcal{V}_{K^*}$ oracle for running A (cf. Lemma 1).**

Lemma 1. *Let* SE *be sub-exponentially secure AE, and let* MB-AIPO *be a sub-exponentially secure MB-AIPO wrt. adaptive distribution ensemble* $(\mathcal{V}_{K^*}(\cdot), \mathcal{D}_1^{\mathcal{FO}})$. *Then* SE *is sub-exponentially secure AE-AUX wrt.* $(\mathsf{PCO}_{sk'}(\cdot,\cdot), \mathcal{D}_2^{\mathcal{FO}})$.

Proof. The idea is to show that the adaptive auxiliary information looks random to an AE-AUX adversary A and hence does not significantly increase its advantage. In order to do so, we give an MB-AIPO adversary B in Fig. 29 wrt. $(\mathcal{V}_{K^*}(\cdot), \mathcal{D}_1^{\mathcal{FO}})$ that runs A. When $p \leftarrow\!\!\$\ \mathsf{MB\text{-}AIPO}(r^* \| c_1^*, K)$, the auxiliary information is independent of the symmetric key K^*. Hence, there is an AE adversary B' such that

$$\mathbf{Adv}^{\text{ae-aux}}_{\mathsf{SE},A,\mathsf{PCO}_{sk'}}(k) \leq \mathbf{Adv}^{\text{ae}}_{\mathsf{SE},B'}(k) + \mathbf{Adv}^{\text{mb-aipo}}_{\mathsf{MB\text{-}AIPO},B,\mathcal{V}_{K^*},\mathcal{D}}(k) \ .$$

B.1 From Lossy to OW-PCA

In the proof of Theorem 2 we assumed OW-PCA is satisfied by PKE. However, this may not be the case for a candidate PKE scheme. The step missing in Fig. 13 vs. the original is Encrypt-with-Hash $\mathsf{EwH}[\mathsf{PKE}, \mathcal{H}]$ [6], which converts a randomized PKE scheme PKE into a deterministic one by using the hash $\mathcal{H}$ on the message as the encryption coins. See [49, Section 3.1].

Unfortunately, scheme $\mathsf{EwH}[\mathsf{PKE}, \mathcal{H}]$ is *uninstantiable* [23] for IND-CPA secure PKE, in that there exists an IND-CPA PKE such that for every choice of $\mathcal{H}$, $\mathsf{EwH}[\mathsf{PKE}, \mathcal{H}]$ is insecure. Thus, in order to instantiate it, we need to make assumptions on PKE that do not follow from IND-CPA.

INSTANTIATING EWH. Interestingly, Hemenway and Ostrovsky [48, Corollary 2] show that $\mathsf{EwH}[\mathsf{PKE}, \mathcal{H}]$, where PKE is lossy and $\mathcal{H}$ is a pairwise independent hash, is a sufficiently lossy TDF [65] to be OW-CPA. The result requires that the

PKE messages are $\omega(\log k)$-bits longer than the coins. We further need to assume *sub-exponential* indistinguishability and *sub-exponential* lossiness of PKE, which can be built from a variety of sub-exponential assumptions.

Claim. Let $\mathsf{LPKE} = (\mathsf{Kg}, \mathsf{Kg}', \mathsf{Enc}, \mathsf{Dec})$ be a lossy encryption scheme and let $\mathcal{H}$ be a pairwise independent hash. Then $\mathsf{PKE} = \mathsf{EwH}[\mathsf{LPKE}, \mathcal{H}]$ is OW-PCA.

Proof. Consider the OW-PCA adversary A against PKE in Fig. 30, we argue its advantage is negligible. First we switch the PCA oracle to a "public" mode, which uses pk instead of sk: $\mathsf{PCO}'_{pk}(m, c)$ returns 1 iff $\mathsf{Enc}(pk, m; r') = c$ for some $r' \in \mathsf{Coins}(1^k)$. (The oracle can be eliminated at this point.) Next, LPKE is switched to lossy mode. If A's advantage changes, we can build a corresponding distinguisher against LPKE: On input pk, the distinguisher simulates the PCA game for A given the input pk. In the final game we know that by Hemenway-Ostrovsky [48] PKE is a lossy TDF and hence OW-PCA advantage is small (the PCO oracle uses pk, so it does not affect this step). □

Games $G_1(k)$, $G_2(k)$	Game $G_3(k)$
$(pk, sk) \leftarrow\!\!\$\ \mathsf{Kg}(1^k)$	$pk \leftarrow\!\!\$\ \mathsf{Kg}'(1^k)$
$m \leftarrow\!\!\$\ \mathsf{Msg}(1^k)\ ;\ r \leftarrow\!\!\$\ \mathsf{Coins}(1^k)$	$m \leftarrow\!\!\$\ \mathsf{Msg}(1^k)\ ;\ r \leftarrow\!\!\$\ \mathsf{Coins}(1^k)$
$c \leftarrow \mathsf{Enc}(pk, m; r)$	$c \leftarrow \mathsf{Enc}(pk, m; r)$
$m' \leftarrow\!\!\$\ A^{\mathsf{PCO}_{sk}(\cdot,\cdot)}(pk, c)$	$m' \leftarrow\!\!\$\ A^{\mathsf{PCO}'_{pk}(\cdot,\cdot)}(pk, c)$
$m' \leftarrow\!\!\$\ A^{\mathsf{PCO}'_{pk}(\cdot,\cdot)}(pk, c)$	If $m = m'$ then return 1
If $m = m'$ then return 1	Else return 0
Else return 0	

Fig. 30: Game chain for the above claim.

Getting OW-PCA with public checkability. Observe that any instantiation of EwH that is OW-CPA is also OW-PCA. Intuitively, this is because of "re-encrypt on decryption." Namely, given (pk, K, c, m) *anyone* can determine whether or not $\mathsf{Enc}(pk, m; H_K(m)) = c$, which can be seen as identical to the check made by $\mathsf{Dec}'(sk, c)$. In other words, the $\mathsf{PCO}_{sk'}(\cdot,\cdot)$ oracle can be publicly computed in an equivalent way, which we call public checkability. OW-PCA with public checkability allows us to eliminate the $\mathsf{PCO}_{sk'}(\cdot,\cdot)$ oracle from $(\mathsf{PCO}_{sk'}(\cdot,\cdot), \mathcal{D}_1^{\mathcal{F}\mathcal{O}})$ in Theorem 2 when PKE is lossy. That is, the distribution ensemble is no longer adaptive.

C New Auxiliary-Input Multi-Bit Point Function Obfuscators and Applications

C.1 Canonical Point Function Obfuscators

Canonical AIPO. We define a special kind of AIPO called *canonical*[13], which is specified by a triple of algorithms $\mathsf{AIPO} = (\mathsf{AIPO.Kg}, \mathsf{AIPO.Obf}, \mathsf{AIPO.Ver})$. Algorithm $\mathsf{AIPO.Kg}$ on input 1^k returns a key K. Algorithm $\mathsf{AIPO.Obf}$ on inputs K, x returns c. Algorithm $\mathsf{AIPO.Ver}$ on inputs K, c, x' returns a bit b. We call $\mathsf{AIPO.Ver}$ *trivial* if it returns $\mathsf{AIPO.Obf}(K, x') = c$, in which case we usually omit it. For correctness, we additionally require that for all $k \in \mathbb{N}$, $\mathsf{AIPO.Ver}(K, c, x')$ returns 1 when $x' = x$ and returns $\perp$ otherwise, for all possible outcomes of $K \leftarrow\!\!\$\ \mathsf{AIPO.Kg}(1^k)$ and $c \leftarrow \mathsf{AIPO.Obf}(K, x)$.

This formalism is loosely taken from [26]. One can think of c as the "obfuscated program" which can be run on x' via $\mathsf{AIPO.Ver}$ with K. Moreover, a fresh key K must be generated for each run of $\mathsf{AIPO.Obf}$.

Canonical MB-AIPO. A canonical MB-AIPO is similarly defined by a triple of algorithms $\mathsf{MB\text{-}AIPO} = (\mathsf{MB\text{-}AIPO.Kg}, \mathsf{MB\text{-}AIPO.Obf}, \mathsf{MB\text{-}AIPO.Ver})$. Algorithm $\mathsf{MB\text{-}AIPO.Kg}$ takes as input 1^k and outputs a key K. $\mathsf{MB\text{-}AIPO.Obf}$ takes as inputs K, x, y returns c. Algorithm $\mathsf{MB\text{-}AIPO.Ver}$ on inputs K, c, x' returns y or $\perp$. For correctness, we additionally require that for all $k \in \mathbb{N}$, $\mathsf{MB\text{-}AIPO.Ver}(K, c, x')$ returns y when $x' = x$ and returns $\perp$ otherwise, for all possible outcomes of $(z, x, y) \leftarrow\!\!\$\ D_k$, $K \leftarrow\!\!\$\ \mathsf{MB\text{-}AIPO.Kg}(1^k)$, and $c \leftarrow \mathsf{MB\text{-}AIPO.Obf}(K, x, y)$.

C.2 MB-AIPO from ELFs

Our construction is based on a sup-AIPO of Zhandry and a slight variant of the Correlated Cooked Leftover Hash Lemma, so we first provide these.

Zhandry's AIPO. Let ELF be an ELF with domain $\mathsf{ELF.Dom}(k)$, where k is the security parameter. Let $\mathcal{H}$ be a family of pairwise independent hash functions with $\mathcal{H} : \mathcal{K}_H \times \{0,1\}^n \to \mathsf{ELF.Dom}(k)$, where $|\{0,1\}^n|^2/|\mathsf{ELF.Dom}(k)|$ is negligible. It then follows with overwhelming probability that for all $K_H \in \mathcal{K}_H$, $H(K_H, \cdot)$ is injective. With this hash function, we recreate a construction due to Zhandry [72][14] as the canonical AIPO $\mathsf{sAIPO}[\mathcal{H}, \mathsf{ELF}] = (\mathsf{sAIPO.Kg}, \mathsf{sAIPO.Obf}, \mathsf{sAIPO.Ver})$ in Figure 31. Note that we will often write $f(H(K_H, x))$ instead of $\mathsf{sAIPO.Obf}(x, K_H, f)$.

[13] Which are, in essence, just a different type of notation to express AIPOs.
[14] Specifically, construction 4.3 in [72].

$\underline{\mathsf{sAIPO.Kg}(1^k)}$	$\underline{\mathsf{sAIPO.Obf}(K_H, f, x)}$	$\underline{\mathsf{sAIPO.Ver}(K_H, f, c, x')}$
$K_H \leftarrow\!\!\$\ \mathcal{K}_H(1^k)$	$c \leftarrow f(H(K_H, x))$	$c' \leftarrow \mathsf{sAIPO.Obf}(K_H, f, x')$
$f \leftarrow\!\!\$\ \mathsf{ELF.IKg}(1^k)$	Return c	If $c' = c$ then return 1
Return (K_H, f)		Else return $\perp$

Fig. 31: **Point function obfuscator** $\mathsf{sAIPO}[\mathcal{H}, \mathsf{ELF}] = (\mathsf{sAIPO.Kg}, \mathsf{sAIPO.Obf}, \mathsf{sAIPO.Ver})$.

A CROOKED LEFTOVER HASH LEMMA FOR CORRELATED SOURCES. Fuller *et al.* [40] prove a generalization of the crooked leftover hash lemma [34] to correlated sources. We present a modified version of this lemma that extends it to multiple functions:

Lemma 2. *Let $\mathcal{H} : \mathcal{K} \times D \to R$ be a 2τ-wise function for $t > 0$, and let $\mathcal{F} = (f_1, \ldots, f_\tau)$ be a tuple of functions, where $f_i : R \to S_i$ for $1 \le i \le \tau$. Let $\mathbf{X} = (X_1, \ldots, X_\tau)$ where the X_i's are random variables over D with min-entropy $\mathbf{H}_\infty(X_i) \ge \mu$ for all $1 \le i \le \tau$ and $\Pr[X_i = X_j] = 0$ for all $1 \le i \ne j \le \tau$. Then*

$$\Delta((K, \mathcal{F}(\mathcal{H}(K, \mathbf{X}))), (K, \mathcal{F}(\mathbf{U}))) \le \frac{1}{2}\sqrt{\frac{\tau^2 (\max_i |S_i|)^\tau}{2^\mu}},$$

where $K \leftarrow\!\!\$\ \mathcal{K}$ and $\mathbf{U} = (U_1, ..., U_\tau)$ where the U_i's are all uniform and independent over R. Here the functions in $\mathcal{F}$ operate in order on the corresponding components.

The proof of Lemma 2 is omitted due to its similarity to the original proof in [40], which only differs from the above bound in that $|S|^\tau$ takes the place of $\max_i |S_i|^\tau$. This change is a result of allowing each function $f_1, \ldots, f_\tau$ to be a different function with a different co-domain (in [40] these functions were all equal, $f_1 = \cdots = f_\tau$).

OUR CONSTRUCTION. To define our MB-AIPO we use a modification of the transformation due to Canetti-Dakdouk [27] that builds an MB-AIPO from an AIPO.

Let ELF be an ELF and let $\mathcal{H} : \mathcal{K}_H \times \{0,1\}^n \to \mathsf{ELF.Dom}$ be a family of $(2t+2)$-wise independent hash functions indexed by keys in $\mathcal{K}_H$. In Figure 32 we define our sup-MB-AIPO as the canonical MB-AIPO $\mathsf{sMB\text{-}AIPO}[\mathcal{H}, \mathsf{ELF}] = (\mathsf{sMB\text{-}AIPO.Kg}, \mathsf{sMB\text{-}AIPO.Obf}, \mathsf{sMB\text{-}AIPO.Ver})$. On input 1^k algorithm $\mathsf{sMB\text{-}AIPO.Kg}$ returns $K_H \leftarrow\!\!\$\ \mathcal{K}_H(1^k)$. Algorithm $\mathsf{sMB\text{-}AIPO.Obf}$ on inputs (K_H, x, y, φ) returns a pair $(\mathbf{f}, \mathbf{c})$; vs. the syntax in Section C.1, we introduce an additional "mode" input bit φ to specify the ELF mode of operation in the proof of security. Algorithm $\mathsf{sMB\text{-}AIPO.Ver}$ on inputs $(K_H, (\mathbf{f}, \mathbf{c}), x')$ returns the string y or $\perp$. We ensure that each AIPO building the sequence is an obfuscation of a different point function. This additional requirement is in place to ensure the conditions of Lemma 2 are met so it may be used in the proof of security.

Theorem 3. *Let $\mathcal{D} = \{D_k = (Z_k, X_k, Y_k)\}_{k \in \mathbb{N}} \in \mathcal{D}^{\mathsf{sup}}$. Let ELF be a secure ELF and let $\mathcal{H} : \mathcal{K}_H \times \{0,1\}^n \to \mathsf{ELF.Dom}$ be $(2t+2)$-wise independent.*

$\underline{\mathsf{sMB\text{-}AIPO.Obf}(K_H, x, y, \varphi)}$	$\underline{\mathsf{sMB\text{-}AIPO.Ver}(K_H, (\mathbf{f}, \mathbf{c}), x')}$
$t \leftarrow \lvert y \rvert$	$(f_1^{\varphi}, \ldots, f_{t+1}^{\varphi}) \leftarrow \mathbf{f}$
For i from 1 to t do	$(c_1, \ldots, c_{t+1}) \leftarrow \mathbf{c}$
$f_i^{\mathsf{inj}} \leftarrow\!\!\$\ \mathsf{ELF.IKg}(1^k)$; $f_i^{\mathsf{los}} \leftarrow\!\!\$\ \mathsf{ELF.LKg}(1^k, r)$	If $f_{t+1}^{\varphi}(H(K_H, x' + t + 1)) \neq c_{t+1}$
If $y[i] = 1$ then	then
$x_{i,y} \leftarrow x + i$; $c_i \leftarrow f_i^{\varphi}(H(K_H, x_{i,y}))$	Return $\perp$
Else	Else
$x_{i,y} \leftarrow\!\!\$\ \{0,1\}^n$	For i from 1 to t do
While $\exists\, j \in [1, i-1]$ such that $x_{i,y} = x_{j,y}$ do	If $f_i^{\varphi}(H(K_H, x' + i)) = c_i$
While $\exists\, j \in [1, t+1]$ such that $x_{i,y} = x + j$ do	then $y_i \leftarrow 1$
$x_{i,y} \leftarrow\!\!\$\ \{0,1\}^n$	Else $y_i \leftarrow 0$
$c_i \leftarrow f_i^{\varphi}(H(K_H, x_{i,y}))$	$y \leftarrow y_1, \ldots, y_t$
$f_{t+1}^{\mathsf{inj}} \leftarrow\!\!\$\ \mathsf{ELF.IKg}(1^k)$; $f_{t+1}^{\mathsf{los}} \leftarrow\!\!\$\ \mathsf{ELF.LKg}(1^k, r)$	Return y
$x_{t+1,y} \leftarrow x + t + 1$; $c_{t+1} \leftarrow f_{t+1}^{\varphi}(H(K_H, x_{t+1,y}))$	
$\mathbf{c} \leftarrow [c_1, \ldots, c_{t+1}]$; $\mathbf{f} \leftarrow [f_1^{\varphi}, \ldots, f_{t+1}^{\varphi}]$	
Return $(\mathbf{f}, \mathbf{c})$	

Fig. 32: **Construction** $\mathsf{sMB\text{-}AIPO}[\mathcal{H}, \mathsf{ELF}] = (\mathsf{sMB\text{-}AIPO.Kg}, \mathsf{sMB\text{-}AIPO.Obf}, \mathsf{sMB\text{-}AIPO.Ver})$**.** $\mathsf{sMB\text{-}AIPO.Kg}$ **returns** $K \leftarrow\!\!\$\ \mathcal{K}_H(1^k)$ **on input** 1^k**.**

Then, $\mathsf{sMB\text{-}AIPO}[\mathcal{H}, \mathsf{ELF}] = (\mathsf{sMB\text{-}AIPO.Kg}, \mathsf{sMB\text{-}AIPO.Obf}, \mathsf{sMB\text{-}AIPO.Ver})$ *defined in Fig. 32 is a secure canonical MB-AIPO for* $\mathcal{D}$ *when* $\mathbf{H}_{\infty}(X_k) \geq 2\log[t+1] + (t+1)\log[\max_i |S_i|] - 2\log\epsilon - 2$*, where* ϵ *is negligible in the security parameter* k*.*

Remark 6. Our MB-AIPO construction is similar to the Canetti-Dakdouk (CD) transform [27] applied to the sup-AIPO of Zhandry [72], except that we use the same hash key for each AIPO instead of a fresh one, and we have to ensure each hash input is distinct. It may also be possible to analyze the MB-AIPO construction actually obtained by applying the CD transform to Zhandry's sup-AIPO, which uses a fresh pairwise independent hash key for each AIPO, by modifying and proving a correlated CLHL accordingly. (It does *not* work to treat the underlying AIPO as a black-box in the analysis.) However, we chose our MB-AIPO to be most compatible with the existing correlated CLHL.

Proof. In this proof we often refer to $\mathsf{sAIPO}[\mathcal{H}, \mathsf{ELF}]$ and $\mathsf{sMB\text{-}AIPO}[\mathcal{H}, \mathsf{ELF}]$ simply as sAIPO and $\mathsf{sMB\text{-}AIPO}$, respectively, since the definitions of $\mathcal{H}$ and ELF remain unchanged throughout.

For the sake of contradiction, suppose a PPT MB-AIPO adversary A runs in time v and distinguishes between the distributions

$$(1^k, z, f_1^{\mathsf{inj}}(H(K_H, x_{1,y})), \ldots, f_{t+1}^{\mathsf{inj}}(H(K_H, x_{t+1,y})))$$

$$\text{and } (1^k, z, f_1^{\mathsf{inj}}(u_1), \ldots, f_{t+1}^{\mathsf{inj}}(u_{t+1}))$$

Game $G_1(k)$	**Games** $G_{2.i}(k)$ **for** $1 \le i \le t+1$
$b \leftarrow\!\!\$\ \{0,1\}$; $(z,x,y_0) \leftarrow\!\!\$\ D_k$	$b \leftarrow\!\!\$\ \{0,1\}$; $(z,x,y_0) \leftarrow\!\!\$\ D_k$
$y_1 \leftarrow\!\!\$\ \{0,1\}^{\lvert y_0\rvert}$	$y_1 \leftarrow\!\!\$\ \{0,1\}^{\lvert y_0\rvert}$; $K_H \leftarrow\!\!\$\ \mathsf{sMB\text{-}AIPO.Kg}(1^k)$
$K_H \leftarrow\!\!\$\ \mathsf{sMB\text{-}AIPO.Kg}(1^k)$	$(\mathbf{f},\mathbf{c}) \leftarrow\!\!\$\ \mathsf{sMB\text{-}AIPO.Obf}(K_H,x,y_b,\mathsf{inj})$
$(\mathbf{f},\mathbf{c}) \leftarrow\!\!\$\ \mathsf{sMB\text{-}AIPO.Obf}(K_H,x,y_b,\mathsf{inj})$	$(\mathbf{f}^{\mathsf{los}},\mathbf{c}^{\mathsf{los}}) \leftarrow\!\!\$\ \mathsf{sMB\text{-}AIPO.Obf}(K_H,x,y_b,\mathsf{los})$
$b' \leftarrow\!\!\$\ A(1^k,z,K_H,\mathbf{f},\mathbf{c})$	For j from 1 to i do
Return $(b=b')$	$\quad \mathbf{f}[j] \leftarrow \mathbf{f}^{\mathsf{los}}[j]$; $\mathbf{c}[j] \leftarrow \mathbf{c}^{\mathsf{los}}[j]$
	$b' \leftarrow\!\!\$\ A(1^k,z,K_H,\mathbf{f},\mathbf{c})$
	Return $(b=b')$

Game $G_3(k)$	**Games** $G_{4.i}(k)$ **for** $1 \le i \le t+1$
$b \leftarrow\!\!\$\ \{0,1\}$; $(z,x,y_0) \leftarrow\!\!\$\ D_k$	$b \leftarrow\!\!\$\ \{0,1\}$; $(z,x,y_0) \leftarrow\!\!\$\ D_k$
$y_1 \leftarrow\!\!\$\ \{0,1\}^{\lvert y_0\rvert}$	$y_1 \leftarrow\!\!\$\ \{0,1\}^{\lvert y_0\rvert}$; $K_H \leftarrow\!\!\$\ \mathsf{sMB\text{-}AIPO.Kg}(1^k)$
$K_H \leftarrow\!\!\$\ \mathsf{sMB\text{-}AIPO.Kg}(1^k)$	$(\mathbf{f},\mathbf{c}) \leftarrow\!\!\$\ \mathsf{sMB\text{-}AIPO.Obf}(K_H,x,y_b,\mathsf{inj})$
$(\mathbf{f},\mathbf{c}) \leftarrow\!\!\$\ \mathsf{sMB\text{-}AIPO.Obf}(K_H,x,y_b,\mathsf{los})$	$(\mathbf{f}^{\mathsf{los}},\mathbf{c}^{\mathsf{los}}) \leftarrow\!\!\$\ \mathsf{sMB\text{-}AIPO.Obf}(K_H,x,y_b,\mathsf{los})$
$(f_1^{\mathsf{los}},\ldots,f_{t+1}^{\mathsf{los}}) \leftarrow \mathbf{f}$	$(f_1^{\mathsf{inj}},\ldots,f_{t+1}^{\mathsf{inj}}) \leftarrow \mathbf{f}$; $(f_1^{\mathsf{los}},\ldots,f_{t+1}^{\mathsf{los}}) \leftarrow \mathbf{f}^{\mathsf{los}}$
For j from 1 to $t+1$ do	For j from 1 to i do
$\quad u_j \leftarrow\!\!\$\ \mathsf{ELF.Dom}(k)$; $\mathbf{c}[j] \leftarrow f_j^{\mathsf{los}}(u_j)$	$\quad u_j \leftarrow\!\!\$\ \mathsf{ELF.Dom}(k)$; $\mathbf{c}[j] \leftarrow f_j^{\mathsf{inj}}(u_j)$
$b' \leftarrow\!\!\$\ A(1^k,z,K_H,\mathbf{f},\mathbf{c})$	For j from $i+1$ to $t+1$ do
Return $(b=b')$	$\quad u_j \leftarrow\!\!\$\ \mathsf{ELF.Dom}(k)$
	$\quad \mathbf{c}[j] \leftarrow f_j^{\mathsf{los}}(u_j)$; $\mathbf{f}[j] \leftarrow f_j^{\mathsf{los}}$
	$b' \leftarrow\!\!\$\ A(1^k,z,K_H,\mathbf{f},\mathbf{c})$
	Return $(b=b')$

Fig. 33: **Game chain for the proof of Theorem 3.**

with non-negligible advantage at least ϵ, for all $k \in \mathbb{N}$, $K_H \leftarrow\!\!\$\ \mathsf{sMB\text{-}AIPO.Kg}(1^k)$, $(z,x,y) \leftarrow\!\!\$\ D_k$, and $f_i \leftarrow\!\!\$\ \mathsf{ELF.IKg}(1^k)$ and $u_i \leftarrow\!\!\$\ \mathsf{ELF.Dom}(k)$ for all $1 \le i \le |y|+1$. This means there exists an inverse polynomial in the security parameter, δ, such that $\epsilon \ge \delta$ infinitely often. We now describe the game chain in Fig. 33 where A is a PPT MB-AIPO adversary.

Game G_1: This is the standard MB-AIPO security game.

Games $G_{2.i}$ for $1 \le i \le t+1$: Game $G_{2.i}$ is similar to game G_1 except that the first i ELFs in $\mathbf{f}$ are in lossy mode and the first i strings in $\mathbf{c}$ were computed using these lossy-mode ELFs. Note that $G_{2.t+1}$ is the game in which the MB-AIPO given to A is generated with all ELFs in lossy mode. The lossy mode ELFs are generated via $\mathsf{ELF.LKg}(1^k, \mathsf{poly}(\mathsf{v}, \delta/(3t+3)))$ where $\mathsf{poly}(\mathsf{v}, \delta/(3t+3))$ is a polynomial chosen such that an ELF adversary running in time v cannot distinguish between ELFs generated from $\mathsf{ELF.LKg}(1^k, \mathsf{poly}(\mathsf{v}, \delta/(3t+3)))$ vs. $\mathsf{ELF.IKg}(1^k)$ except with probability less than $\delta/(3t+3)$.

We can bound the difference in A's distinguishing advantage between games $G_{2.i-1}$ and $G_{2.i}$ for $1 \le i \le t+1$ (where we let $G_{2.0} = G_1$) with an

ELF adversary, B running in time v, as shown in Figure 34. Hence, we get $|\Pr[\,G_{2.i-1} \Rightarrow 1\,] - \Pr[\,G_{2.i} \Rightarrow 1\,]| < \delta/(3t+3)$.

Adversary $B(1^k, f_i)$
$b \leftarrow\!\!\$\ \{0,1\}$; $(z, x, y_0) \leftarrow\!\!\$\ D_k$
$y_1 \leftarrow\!\!\$\ \{0,1\}^{|y_0|}$; $K_H \leftarrow\!\!\$\ \mathsf{sMB\text{-}AIPO.Kg}(1^k)$
$(\mathbf{f}, \mathbf{c}) \leftarrow\!\!\$\ \mathsf{sMB\text{-}AIPO.Obf}(K_H, x, y_b, \mathsf{inj})$
$(\mathbf{f}^{\mathsf{los}}, \mathbf{c}^{\mathsf{los}}) \leftarrow\!\!\$\ \mathsf{sMB\text{-}AIPO.Obf}(K_H, x, y_b, \mathsf{los})$
For j from 1 to $i-1$ do
  $\mathbf{f}[j] \leftarrow \mathbf{f}^{\mathsf{los}}[j]$; $\mathbf{c}[j] \leftarrow \mathbf{c}^{\mathsf{los}}[j]$
$\mathbf{f}[i] \leftarrow f_i$; $\mathbf{c}[i] \leftarrow f_i(H(K_H, x_{i,y_b}))$
$b' \leftarrow\!\!\$\ A(1^k, z, K_H, \mathbf{f}, \mathbf{c})$
Return $(b = b')$

Fig. 34: **ELF adversary B running MB-AIPO adversary A in the proof of Theorem 3 (cf. $G_{2.i}$).**

Game G_3: G_3 is similar to game $G_{2.t+1}$ except all AIPOs in the sequence have been switched to a version of sAIPO without the hash function and the inputs have all been switched to random. By the Crooked LHL for correlated sources (Lemma 2) we know that

$$\Delta(\,(K_H, (f_1^{\mathsf{los}}(H(K_H, x_{1,y_b})), \ldots, f_{t+1}^{\mathsf{los}}(H(K_H, x_{t+1,y_b})))\,),$$
$$(K_H, (f_1^{\mathsf{los}}(u_1), \ldots, f_{t+1}^{\mathsf{los}}(u_{t+1})))\,) \leq \frac{1}{2}\sqrt{\frac{(t+1)^2\,(\max_i |S_i|)^{t+1}}{2^{\mu}}}\,,$$

where $\mu = 2\log[t+1] + (t+1)\log[\max_i |S_i|] - 2\log\epsilon - 2$. Hence $G_{2.t+1}$ and G_3 are indistinguishable except with probability $\frac{1}{2}\sqrt{(t+1)^2\,(\max_i |S_i|)^{t+1}\,2^{-\mu}}$, which is negligible in k. We then may write $|\Pr[\,G_{2.t+1} \Rightarrow 1\,] - \Pr[\,G_3 \Rightarrow 1\,]| \leq \mathsf{negl}(k)$.

Games $G_{4.i}$ for $1 \leq i \leq t+1$: Game $G_{4.i}$ is similar to game G_3 except that the first i elements in the MB-AIPO sequence where generated in injective mode instead of lossy mode. By a similar argument as in Figure 34 used for $G_{2.i}$, we get that for $1 \leq i \leq t+1$, $|\Pr[\,G_{4.i-1} \Rightarrow 1\,] - \Pr[\,G_{4.i} \Rightarrow 1\,]| < \delta/(3t+3)$ (where we let $G_{4.0} = G_3$).

Putting the game chain together gives

$$
\begin{aligned}
&|\Pr[G_1 \Rightarrow 1] - \Pr[G_3 \Rightarrow 1]| = \\
&\quad |\Pr[G_1 \Rightarrow 1] - \Pr[G_{2.1} \Rightarrow 1]| + |\Pr[G_{2.1} \Rightarrow 1] - \Pr[G_{2.2} \Rightarrow 1]| + \dots \\
&\quad + |\Pr[G_{2.t+1} \Rightarrow 1] - \Pr[G_3 \Rightarrow 1]| + |\Pr[G_3 \Rightarrow 1] - \Pr[G_{4.1} \Rightarrow 1]| + \\
&\quad \cdots + |\Pr[G_{4.t} \Rightarrow 1] - \Pr[G_{4.t+1} \Rightarrow 1]| \\
&\quad < \frac{(t+1)\delta}{3t+3} + \mathsf{negl}(k) + \frac{(t+1)\delta}{3t+3} \\
&\quad < \frac{2\delta}{3} + \mathsf{negl}(k)\ .
\end{aligned}
$$

Since $\mathsf{negl}(k) < \delta/3$, the RHS of the above inequality is strictly less than δ, meaning $\epsilon < \delta$, contradicting our initial assumption about the adversary.

C.3 Application of the ELF-based MB-AIPO to Fujisaki-Okamoto

We show that under suitable assumptions, our ELF-based-MB-AIPO is secure wrt. the first and second adaptive auxiliary inputs that we require in Theorem 2; the third is statistically unpredictable so it directly follows from Theorem 3. Note that the above is not sub-exponential security and only suffices for public-key-independent messages. To achieve sub-exponential security, we conjecture the prior MB-AIPO of Bitansky and Canetti [14] suffices under sub-exponential security of their assumption.

Security wrt. the first adaptive auxiliary input. We argued in Section B.1 that we can remove oracle $\mathsf{PCO}_{sk'}(\cdot,\cdot)$ by assuming PKE is lossy. We therefore concentrate on showing $\mathcal{D}_1^{\mathcal{FO}}$ is statistically unpredictable. It suffices to show the distribution ensemble is *indistinguishable* from statistically a unpredictable distribution.

Proposition 2. *Suppose* LPKE *is lossy and* SE *is one-time information-theoretic AE. Then there exists* $\mathcal{D}_1^{\mathcal{FO}'} \in \mathcal{D}^{\mathsf{sup}}$ *such that* $\mathcal{D}_1^{\mathcal{FO}} \approx_c \mathcal{D}_1^{\mathcal{FO}'}$.

Proof. We recall the distribution

Distribution $D_{1,k}^{\mathcal{FO}}$
$r^* \leftarrow\!\!\$\ \mathsf{G.Dom}(k)\ ;\ K^* \leftarrow\!\!\$\ \{0,1\}^k$
$m \leftarrow\!\!\$\ \{0,1\}^\mu\ ;\ (pk', sk') \leftarrow\!\!\$\ \mathsf{LPKE.Kg}(1^k)$
$c_1^* \leftarrow\!\!\$\ \mathsf{LPKE.Enc}(pk', r^*)$
$c_2^* \leftarrow\!\!\$\ \mathcal{E}_{K^*}^{\mathsf{sy}}(m\|r^*)\ ;\ c^* \leftarrow (c_1^*, c_2^*)$
$aux \leftarrow (c^*, pk', m)$
Return $(aux, r^*\|c_1^*, K^*)$

Let $\mathcal{D}_1^{\mathcal{FO}'}$ be like $\mathcal{D}_1^{\mathcal{FO}}$ except pk' is generated in lossy mode. We need to show that there is a computationally indistinguishable $\mathcal{D}_1^{\mathcal{FO}'}$ such that for any *unbounded* predictor P, $\Pr\left[P(1^k, aux) \Rightarrow r^*\|c_1^*\right]$ (over the coins for sampling from

$\mathcal{D}_1^{\mathcal{F}\mathcal{O}'}$ and those of P) is negligibly small. Observe that c_1^* is given in aux so we focus on the probability of P outputting r^*.

Consider a game chain where: In game H_0, P gets aux as in $\mathcal{D}_1^{\mathcal{F}\mathcal{O}'}$. In game H_1 we change c_1^* to an encryption of the zero string of length $|r^*|$ rather than an encryption of r^*. Finally, in game H_2 we change c_2^* to an encryption of $m\|0$ rather than $m\|r^*$. Note that in H_2, P has no information on r^* so,

$$\Pr[\, H_2 \Rightarrow 1\,] = 1/|\mathsf{G.Dom}(k)|\ .$$

It remains to argue that

$$|\Pr[\, H_i \Rightarrow 1\,] - \Pr[\, H_{i+1} \Rightarrow 1\,]|$$

is negligible for $i \in \{0,1\}$. For $i = 0$, let $A = (A_1, A_2)$ be the IND-CPA adversary against LPKE that works as follows. On inputs $1^k, pk'$, A_1 outputs $m_0 = r^*, m_1 = 0$ where $r^* \leftarrow\!\!\$\ \mathsf{G.Dom}(k)$. A_2 is then given $pk', m_0, m_1, c_1 \leftarrow\!\!\$\ \mathsf{LPKE.Enc}(pk', m_b)$. A_2 samples $K^* \leftarrow\!\!\$\ \{0,1\}^k, m \leftarrow\!\!\$\ \{0,1\}^\mu$ and computes $c_2 \leftarrow\!\!\$\ \mathcal{E}^{\mathsf{sy}}_{K^*}(m\|m_0)$. Finally, A_2 runs the predictor $P(1^k, ((c_1, c_2), pk', m))$.

When $b = 0$, A simulates H_0 for the predictor and when $b = 1$, A simulates H_1 for the predictor. If P returns $m_0\|c_1$, then A_2 outputs $b' = 0$. If P returns $m_1\|c_1$, then A_2 outputs $b' = 1$. Thus $|\Pr[\, H_0 \Rightarrow 1\,] - \Pr[\, H_1 \Rightarrow 1\,]| \leq \mathbf{Adv}^{\text{ind-cpa}}_{\mathsf{LPKE},A}(k)$. Note that LPKE is lossy and hence this quantity is negligible.

Case $i = 1$ represents the probability of detecting the change from $c_2^* \leftarrow\!\!\$\ \mathcal{E}^{\mathsf{sy}}_{K^*}(m\|r^*)$ to $c_2 \leftarrow\!\!\$\ \mathcal{E}^{\mathsf{sy}}_{K^*}(m\|0)$. This probability is bounded using the information-theoretic IND-CPA security of SE. Let A be an IND-CPA adversary against SE. A generates $r^* \leftarrow\!\!\$\ \mathsf{G.Dom}(k), m \leftarrow\!\!\$\ \{0,1\}^\mu$, and $c_1 \leftarrow\!\!\$\ \mathsf{LPKE.Enc}(pk', 0)$. A runs their IND-CPA game oracle $\mathcal{E}^{\mathsf{sy}}_{K^*}(\mathsf{LR}(\cdot,\cdot,b))$ on the two inputs $m_0 = m\|r^*$ and $m_1 = m\|0$, and gets a ciphertext $c_2' = \mathcal{E}^{\mathsf{sy}}_{K^*}(m_b\|r^*)$ in return. A then runs the predictor $P(1^k, ((c_1, c_2'), pk'.m))$.

When $b = 0$, A simulates H_1 for the predictor and when $b = 1$, A simulates H_2 for the predictor. If P returns $m\|r^*$, then A outputs $b' = 0$. If P returns $m\|0$, then A outputs $b' = 1$. Thus $|\Pr[\, H_1 \Rightarrow 1\,] - \Pr[\, H_2 \Rightarrow 1\,]| \leq \mathbf{Adv}^{\text{ind-cpa}}_{\mathsf{SE},A}(k)$, which is negligible by security of SE, completing the proof.

Security wrt. the second adaptive auxiliary input. We now establish that our ELF-based sup-MB-AIPO is secure wrt. the second auxiliary input under appropriate assumptions. Before our main theorem we start with the following lemma.

Lemma 3. *Let* $\mathsf{LPKE} = (\mathsf{Kg}, \mathsf{Kg}', \mathsf{Enc}, \mathsf{Dec})$ *be a lossy PKE scheme. Let* SE *be information-theoretic one-time AE. Let* ELF *be an ELF and let* $\mathcal{H} : \mathcal{K}_H \times \{0,1\}^n \to \mathsf{ELF.Dom}$ *be a family of* $(2t+2)$*-wise independent hash functions. Let* $\mathsf{sMB\text{-}AIPO}[\mathcal{H}, \mathsf{ELF}] = (\mathsf{sMB\text{-}AIPO.Kg}, \mathsf{sMB\text{-}AIPO.Obf}, \mathsf{sMB\text{-}AIPO.Ver})$ *be the sup-MB-AIPO constructed in Section C.2. Let* v *be a polynomial in* k*. Consider the two distribution ensembles* $\mathcal{D}^0 = \{D_k^0\}_{k\in\mathbb{N}}$ *and* $\mathcal{D}^1 = \{D_k^1\}_{k\in\mathbb{N}}$ *defined below.*

Then $\mathcal{D}^0 \approx_s \mathcal{D}^1$.

Distribution D_k^0	**Distribution** D_k^1
$r^* \leftarrow\!\!\$\ \mathsf{G.Dom}(k)\ ;\ m \leftarrow\!\!\$\ \{0,1\}^\mu$	$r^* \leftarrow\!\!\$\ \mathsf{G.Dom}(k)\ ;\ m \leftarrow\!\!\$\ \{0,1\}^\mu$
$K_0 \leftarrow\!\!\$\ \{0,1\}^k\ ;\ K_1 \leftarrow\!\!\$\ \{0,1\}^k$	$K_1 \leftarrow\!\!\$\ \{0,1\}^k$
$pk' \leftarrow\!\!\$\ \mathsf{LPKE.Kg}'(1^k)$	$pk' \leftarrow\!\!\$\ \mathsf{LPKE.Kg}'(1^k)$
$c_1^* \leftarrow\!\!\$\ \mathsf{LPKE.Enc}(pk', r^*)$	$c_1^* \leftarrow\!\!\$\ \mathsf{LPKE.Enc}(pk', r^*)$
$c_2^* \leftarrow\!\!\$\ \mathcal{E}^{\mathsf{sy}}_{K_1}(m\|r^*)\ ;\ c^* \leftarrow (c_1^*, c_2^*)$	$c_2^* \leftarrow\!\!\$\ \mathcal{E}^{\mathsf{sy}}_{K_1}(m\|r^*)\ ;\ c^* \leftarrow (c_1^*, c_2^*)$
$K_H \leftarrow\!\!\$\ \mathsf{sMB\text{-}AIPO.Kg}(1^k)$	$K_H \leftarrow\!\!\$\ \mathsf{sMB\text{-}AIPO.Kg}(1^k)$
$(\mathbf{f}^{\mathsf{los}'}, \mathbf{c}^{\mathsf{los}'}) \leftarrow\!\!\$\ \mathsf{sMB\text{-}AIPO.Obf}^{\mathsf{los(v)}}_{K_H}(r^*\|c_1^*, K_0)$	$(\mathbf{f}^{\mathsf{los}}, \mathbf{c}^{\mathsf{los}}) \leftarrow\!\!\$\ \mathsf{sMB\text{-}AIPO.Obf}^{\mathsf{los(v)}}_{K_H}(r^*\|c_1^*, K_1)$
Return $(c^*, \mathbf{f}^{\mathsf{los}'}, \mathbf{c}^{\mathsf{los}'}, K_H, pk', m)$	Return $(c^*, K_H, \mathbf{f}^{\mathsf{los}}, \mathbf{c}^{\mathsf{los}}, pk', m)$

Proof. Let D be an unbounded distinguisher for $\mathcal{D}^0, \mathcal{D}^1$. We invoke the remainder of the proof of Theorem 3, following switching all instances of ELF to the appropriate lossy mode, with auxiliary input (c^*, pk', m), which we show below to be statistically unpredictable. Further, note this remainder of the above-mentioned proof is statistical as desired.

To complete the proof, we need to show that for any unbounded predictor P',

$$\Pr\left[\, P'(1^k, (c_1^*\|c_2^*, pk', m)) \Rightarrow K_1 \,\right]$$

is negligible. To show this, first note that by information-theoretic security of SE we have that,

$$|\Pr\left[\, P'(1^k, (c_1^*\|c_2^*, pk', m)) \Rightarrow K_1 \,\right] - \Pr\left[\, P'(1^k, (c_1^*\|\$, pk', m)) \Rightarrow K_1 \,\right]|$$

is negligible, where \$ is a random string of length $|c_2^*|$. Since pk' is a lossy key,

$$|\Pr\left[\, P'(1^k, (c_1^*\|\$, pk', m)) \Rightarrow K_1 \,\right] - \Pr\left[\, P'(1^k, (c_0\|\$, pk', m)) \Rightarrow K_1 \,\right]|$$

is negligible, where c_0 is an encryption under pk' of a fixed message. At this point, the auxiliary information contains no information on K_1, completing the proof.

Theorem 4. *Let* $\mathsf{LPKE} = (\mathsf{Kg}, \mathsf{Kg}', \mathsf{Enc}, \mathsf{Dec})$ *be a secure lossy PKE scheme. Let* SE *be a zero-time information-theoretic leakage-resilient AE scheme. Let* ELF *be an ELF and let* $\mathcal{H} : \mathcal{K}_H \times \{0,1\}^n \to \mathsf{ELF.Dom}$ *be a family of* $(2k+2)$*-wise independent hash functions. Let* $\mathsf{sMB\text{-}AIPO}[\mathcal{H}, \mathsf{ELF}] = (\mathsf{sMB\text{-}AIPO.Kg}, \mathsf{sMB\text{-}AIPO.Obf}, \mathsf{sMB\text{-}AIPO.Ver})$ *be the corresponding sup-MB-AIPO constructed in Section C.2. Then* $\mathsf{sMB\text{-}AIPO}$ *is secure MB-AIPO wrt. adaptive auxiliary input* $(\mathcal{V}_{K_1}(\cdot), \mathcal{D}_1^{\mathcal{FO}})$.

Remark 7. It seems unusual that the AE is zero-time in the above theorem, but the leakage provides the adversary with a ciphertext in this case.

Proof. Consider the game chain in Fig. 37.

Game G_1**:** This is the standard MB-AIPO security game wrt. $(\mathcal{V}_{K_1}(\cdot), \mathcal{D}_1^{\mathcal{FO}})$. For contradiction, suppose a PPT MB-AIPO adversary A runs in time v and wins game G_1 with non-negligible probability ϵ. Let δ be an inverse polynomial in the security parameter such that $\epsilon \geq \delta$ infinitely often.

Games $G_{2.i}$ **for** $1 \leq i \leq k+1$**:** Game $G_{2.i}$ is similar to game G_1 except that the first i ELFs in the MB-AIPO construction are switched to lossy mode. Each of the $k+1$ ELFs in the MB-AIPO construction are switched to lossy mode one at a time. Note that $G_{2.k+1}$ is the game in which the MB-AIPO given to A is generated with all ELFs in lossy mode. The lossy-mode ELFs are generated via $\mathsf{ELF.LKg}(1^k, \mathsf{poly}(\mathsf{v}, \delta/(k+1)))$ where $\mathsf{poly}(\mathsf{v}, \delta/(k+1))$ is a polynomial chosen such that an ELF adversary running in time v cannot distinguish between the ELF lossy and injective modes except with probability less than $\delta/(k+1)$.

Consider the ELF adversary in Fig. 35 running the MB-AIPO adversary to determine if their challenge ELF, f_i, is in injective or lossy mode. Hence, $|\Pr[G_{2.i-1} \Rightarrow 1] - \Pr[G_{2.i} \Rightarrow 1]| < \delta/(k+1)$ (letting $G_{2.0} = G_1$).

Adversary $B(1^k, f_i)$
$m \leftarrow\!\!\$\ \{0,1\}^\mu$; $r^* \leftarrow\!\!\$\ \mathsf{G.Dom}(k)$
$K_1 \leftarrow\!\!\$\ \{0,1\}^k$; $K_0 \leftarrow\!\!\$\ \{0,1\}^k$
$(pk', sk') \leftarrow\!\!\$\ \mathsf{LPKE.Kg}(1^k)$; $c_1^* \leftarrow\!\!\$\ \mathsf{LPKE.Enc}(pk', r^*)$
$c_2^* \leftarrow\!\!\$\ \mathcal{E}_{K_1}^{\mathsf{sy}}(m\|r^*)$; $c^* \leftarrow (c_1^*, c_2^*)$
$aux \leftarrow (c^*, pk', m)$
$K_H \leftarrow\!\!\$\ \mathsf{sMB\text{-}AIPO.Kg}(1^k)$
$(\mathbf{f}, \mathbf{c}) \leftarrow\!\!\$\ \mathsf{sMB\text{-}AIPO.Obf}_{K_H}^{\mathsf{inj}}(m\|r^*, K_1)$
$(\mathbf{f}^{\mathsf{los}}, \mathbf{c}^{\mathsf{los}}) \leftarrow\!\!\$\ \mathsf{sMB\text{-}AIPO.Obf}_{K_H}^{\mathsf{los(v)}}(m\|r^*, K_1)$
For j from 1 to $i-1$ do $\mathbf{f}[j] \leftarrow \mathbf{f}^{\mathsf{los}}[j]$; $\mathbf{c}[j] \leftarrow \mathbf{c}^{\mathsf{los}}[j]$
$\mathbf{f}[i] \leftarrow f_i$; $\mathbf{c}[i] \leftarrow f_i(H(K_H, m\|r^*_{i,K_1}))$
$b' \leftarrow\!\!\$\ A^{\mathcal{V}_{K_1}(\cdot)}(1^k, aux, K_H, \mathbf{f}, \mathbf{c})$
Return $(b = b')$

Fig. 35: **ELF adversary** B **running MB-AIPO adversary** A **in the proof of Theorem 4 (cf.** $G_{2.i}$**).**

Game G_3**:** G_3 is similar to $G_{2.k+1}$ except the public key encryption scheme is switched to lossy mode. By assumption on the lossy encryption scheme, the distinguishing probability of the injective and lossy keys is negligible. So, $|\Pr[G_{2.k+1} \Rightarrow 1] - \Pr[G_3 \Rightarrow 1]|$ is negligible.

Game G_4**:** Next, the symmetric-key ciphertext c_2^* is switched to a random c_2 of length $|c_2^*|$ and the MB-AIPO adversary's verification oracle is changed to $\perp(\cdot)$, which outputs $\perp$ on all inputs. To bound the probability this switch is detected, we use AE with leakage consisting of $(c^*, K_H, \mathbf{f}^{\mathsf{los}}, \mathbf{c}^{\mathsf{los}}, pk', m)$. Consider such an adversary B_1 in Fig. 36. (Here B_1's oracles $(\mathcal{O}_1, \mathcal{O}_2)$ are either $(\mathcal{E}_{K_1}^*(\cdot), \mathcal{V}_{K_1}(\cdot))$ or $(\$(\cdot), \perp(\cdot))$.)

To invoke leakage-resilient AE security, we must prove that the leakage is statistically unpredictable. In particular, we must prove that

$$\Pr\left[\, P(1^k, (c^*, K_H, \mathbf{f}^{\mathsf{los}}, \mathbf{c}^{\mathsf{los}}, pk', m)) \Rightarrow K_1 \,\right]$$

is negligible for any unbounded predictor P. It suffices to prove

$$(c^*, K_H, \mathbf{f}^{\mathsf{los}}, \mathbf{c}^{\mathsf{los}}, pk', m) \approx_s (c^*, K_H, \mathbf{f}^{\mathsf{los}'}, \mathbf{c}^{\mathsf{los}'}, pk', m)$$

where $(\mathbf{f}^{\mathsf{los}'}, \mathbf{c}^{\mathsf{los}'}) \leftarrow\!\!\$\ \mathsf{sMB\text{-}AIPO.Obf}^{\mathsf{los}}_{K_H}(r^* \| c_1^*, K_0)$, which is shown in Lemma 3. Hence we have $|\Pr[\, G_4 \Rightarrow 1\,] - \Pr[\, G_{3.t+1} \Rightarrow 1\,]| \leq \mathbf{Adv}^{\text{ae-aux}}_{\mathsf{SE},B_1,D^0}(k)$.

Adv $B_1^{\mathcal{O}_1(\cdot),\mathcal{O}_2(\cdot)}(1^k, (c^*, K_H, \mathbf{f}^{\mathsf{los}}, \mathbf{c}^{\mathsf{los}}, pk', m))$	**Distribution** D_k^1
$aux \leftarrow (c^*, pk', m)$	$r^* \leftarrow\!\!\$\ \mathsf{G.Dom}(k)\ ;\ m \leftarrow\!\!\$\ \{0,1\}^\mu$
$b' \leftarrow\!\!\$\ A(1^k, aux, (K_H, \mathbf{f}^{\mathsf{los}}, \mathbf{c}^{\mathsf{los}}))$	$K_1 \leftarrow\!\!\$\ \{0,1\}^k$
Return $(b = b')$	$pk' \leftarrow\!\!\$\ \mathsf{LPKE.Kg}'(1^k)$
	$c_1^* \leftarrow\!\!\$\ \mathsf{LPKE.Enc}(pk', r^*)$
	$c_2^* \leftarrow\!\!\$\ \mathcal{E}^{\mathsf{sy}}_{K_1}(m \| r^*)\ ;\ c^* \leftarrow (c_1^*, c_2^*)$
	$K_H \leftarrow\!\!\$\ \mathsf{sMB\text{-}AIPO.Kg}(1^k)$
	$(\mathbf{f}^{\mathsf{los}}, \mathbf{c}^{\mathsf{los}}) \leftarrow\!\!\$\ \mathsf{sMB\text{-}AIPO.Obf}^{\mathsf{los(v)}}_{K_H}(r^* \| c_1^*, K_1)$
	Return $(c^*, K_H, \mathbf{f}^{\mathsf{los}}, \mathbf{c}^{\mathsf{los}}, pk', m)$

Fig. 36: **AE-AUX adversary in the proof of Theorem 4, game G_4.**

Game G_5: G_5 is similar to G_4 except the point function obfuscation $(\mathbf{f}^{\mathsf{los}}, \mathbf{c}^{\mathsf{los}}) \leftarrow\!\!\$\ \mathsf{sMB\text{-}AIPO.Obf}^{\mathsf{los(v)}}_{K_H}(r^* \| c_1^*, K_1)$ is changed to the obfuscation $(\mathbf{f}^{\mathsf{los}}, \mathbf{c}^{\mathsf{los}}) \leftarrow\!\!\$\ \mathsf{sMB\text{-}AIPO.Obf}^{\mathsf{los(v)}}_{K_H}(r^* \| c_1^*, K_0)$, where K_0 is independent and random. For this transition, we invoke sup-MB-AIPO security of sMB-AIPO wrt. (c^*, pk', m). To do so, we argue that for any unbounded predictor P,

$$\Pr\left[\, P(1^k, (c_1^* \| c_2, pk', m)) \Rightarrow K_1 \,\right]$$

is negligible. Consider changing c_1^* in P's input to c_1, a LPKE encryption of a fixed message under pk'. It is easy to see that

$$|\Pr\left[\, P(1^k, (c_1^* \| c_2, pk', m)) \Rightarrow K_1 \,\right] - \Pr\left[\, P(1^k, (c_1 \| c_2, pk', m)) \Rightarrow K_1 \,\right]|$$

is negligible by the lossiness of LPKE. Now P's input contains no information on K_1. Therefore, $|\Pr[\, G_5 \Rightarrow 1\,] - \Pr[\, G_4 \Rightarrow 1\,]| \leq \mathbf{Adv}^{\text{mb-aipo}}_{\mathsf{sMB\text{-}AIPO},A,\mathcal{D}_1^{\mathcal{F}\mathcal{O}}}(k)$, which is negligible by the security of sMB-AIPO.

We can complete the proof by "reversing" the game chain.

C.4 MB-AIPO from Low-Exponent RSA and its Application to Low-Exponent RSA-OAEP

We show that TDPs (such as low-exponent RSA) that satisfy SIE can be used to implement a multi-bit point function obfuscator. When used in our RSA-OAEP

Game $G_1(k)$	**Games** $G_{2.i}(k)$ **for** $1 \le i \le k+1$
$m \leftarrow\!\!\$\ \{0,1\}^\mu\ ;\ r^* \leftarrow\!\!\$\ \mathsf{G.Dom}(k)$	$m \leftarrow\!\!\$\ \{0,1\}^\mu\ ;\ r^* \leftarrow\!\!\$\ \mathsf{G.Dom}(k)$
$K_1 \leftarrow\!\!\$\ \{0,1\}^k\ ;\ K_0 \leftarrow\!\!\$\ \{0,1\}^k$	$K_1 \leftarrow\!\!\$\ \{0,1\}^k\ ;\ K_0 \leftarrow\!\!\$\ \{0,1\}^k$
$(pk', sk') \leftarrow\!\!\$\ \mathsf{LPKE.Kg}(1^k)$	$(pk', sk') \leftarrow\!\!\$\ \mathsf{LPKE.Kg}(1^k)$
$c_1^* \leftarrow\!\!\$\ \mathsf{LPKE.Enc}(pk', r^*)$	$c_1^* \leftarrow\!\!\$\ \mathsf{LPKE.Enc}(pk', r^*)$
$c_2^* \leftarrow\!\!\$\ \mathcal{E}^{\mathsf{sy}}_{K_1}(m\|r^*)\ ;\ c^* \leftarrow (c_1^*, c_2^*)$	$c_2^* \leftarrow\!\!\$\ \mathcal{E}^{\mathsf{sy}}_{K_1}(m\|r^*)\ ;\ c^* \leftarrow (c_1^*, c_2^*)$
$aux \leftarrow (c^*, pk', m)$	$aux \leftarrow (c^*, pk', m)$
$K_H \leftarrow\!\!\$\ \mathsf{sMB\text{-}AIPO.Kg}(1^k)$	$K_H \leftarrow\!\!\$\ \mathsf{sMB\text{-}AIPO.Kg}(1^k)$
$(\mathbf{f}, \mathbf{c}) \leftarrow\!\!\$\ \mathsf{sMB\text{-}AIPO.Obf}^{\mathsf{inj}}_{K_H}(r^*\|c_1^*, K_1)$	$(\mathbf{f}, \mathbf{c}) \leftarrow\!\!\$\ \mathsf{sMB\text{-}AIPO.Obf}^{\mathsf{inj}}_{K_H}(r^*\|c_1^*, K_1)$
$b' \leftarrow\!\!\$\ A^{\mathcal{V}_{K_1}(\cdot)}(1^k, aux, K_H, \mathbf{f}, \mathbf{c})$	$(\mathbf{f}^{\mathsf{los}}, \mathbf{c}^{\mathsf{los}}) \leftarrow\!\!\$\ \mathsf{sMB\text{-}AIPO.Obf}^{\mathsf{los(v)}}_{K_H}(r^*\|c_1^*, K_1)$
Return $(b' = 1)$	For j from 1 to i do
	$\quad \mathbf{f}[j] \leftarrow \mathbf{f}^{\mathsf{los}}[j]\ ;\ \mathbf{c}[j] \leftarrow \mathbf{c}^{\mathsf{los}}[j]$
	$b' \leftarrow\!\!\$\ A^{\mathcal{V}_{K_1}(\cdot)}(1^k, aux, K_H, \mathbf{f}, \mathbf{c})$
	Return $(b' = 1)$

Game $G_3(k)$	**Games** $G_4(k)$, $G_5(k)$
$m \leftarrow\!\!\$\ \{0,1\}^\mu\ ;\ r^* \leftarrow\!\!\$\ \mathsf{G.Dom}(k)$	$m \leftarrow\!\!\$\ \{0,1\}^\mu\ ;\ r^* \leftarrow\!\!\$\ \mathsf{G.Dom}(k)$
$K_1 \leftarrow\!\!\$\ \{0,1\}^k\ ;\ K_0 \leftarrow\!\!\$\ \{0,1\}^k$	$K_1 \leftarrow\!\!\$\ \{0,1\}^k\ ;\ K_0 \leftarrow\!\!\$\ \{0,1\}^k$
$pk' \leftarrow\!\!\$\ \mathsf{LPKE.Kg'}(1^k)$	$pk' \leftarrow\!\!\$\ \mathsf{LPKE.Kg'}(1^k)$
$c_1^* \leftarrow\!\!\$\ \mathsf{LPKE.Enc}(pk', r^*)$	$c_1^* \leftarrow\!\!\$\ \mathsf{LPKE.Enc}(pk', r^*)$
$c_2^* \leftarrow\!\!\$\ \mathcal{E}^{\mathsf{sy}}_{K_1}(m\|r^*)\ ;\ c^* \leftarrow (c_1^*, c_2^*)$	$c_2^* \leftarrow\!\!\$\ \mathcal{E}^{\mathsf{sy}}_{K_1}(m\|r^*)\ ;\ c_2 \leftarrow\!\!\$\ \{0,1\}^{\lvert c_2^*\rvert}$
$aux \leftarrow (c^*, pk', m)$	$c^* \leftarrow (c_1^*, c_2)\ ;\ aux \leftarrow (c^*, pk', m)$
$K_H \leftarrow\!\!\$\ \mathsf{sMB\text{-}AIPO.Kg}(1^k)$	$K_H \leftarrow\!\!\$\ \mathsf{sMB\text{-}AIPO.Kg}(1^k)$
$(\mathbf{f}^{\mathsf{los}}, \mathbf{c}^{\mathsf{los}}) \leftarrow\!\!\$\ \mathsf{sMB\text{-}AIPO.Obf}^{\mathsf{los(v)}}_{K_H}(r^*\|c_1^*, K_1)$	$(\mathbf{f}^{\mathsf{los}}, \mathbf{c}^{\mathsf{los}}) \leftarrow\!\!\$\ \mathsf{sMB\text{-}AIPO.Obf}^{\mathsf{los(v)}}_{K_H}(r^*\|c_1^*, K_0)$
$b' \leftarrow\!\!\$\ A^{\mathcal{V}_{K_1}(\cdot)}(1^k, aux, K_H, \mathbf{f}, \mathbf{c})$	$(\mathbf{f}^{\mathsf{los}}, \mathbf{c}^{\mathsf{los}}) \leftarrow\!\!\$\ \mathsf{sMB\text{-}AIPO.Obf}^{\mathsf{los(v)}}_{K_H}(r^*\|c_1^*, K_1)$
Return $(b' = 1)$	$b' \leftarrow\!\!\$\ A^{\perp(\cdot)}(1^k, aux, K_H, \mathbf{f}^{\mathsf{los}}, \mathbf{c}^{\mathsf{los}})$
	Return $(b' = 0)$
	Return $(b' = 1)$

Fig. 37: **Game chain for the proof of Theorem 4.**

instantiation, it "plays nicely" with the auxiliary input we need for the the MB-AIPO, the latter already containing a similar RSA-OAEP ciphertext. We take this as evidence that MB-AIPO for such distributions exists.

Basic RSA-based construction. For concreteness, we use the RSA function here rather than a general TDP. Consider the RSA parameter generator RSAgen that on input 1^k outputs $(N, p, q, 3, d)$ where $|N| = k$. Recall from Section 2.4 that RSAgen is unconditionally $(2k/3)$-SIE; let Ext denote the corresponding SIE extractor. Given RSAgen, in Figure 38 we define a canonical MB-AIPO $\mathsf{MB\text{-}AIPO}[\mathsf{RSAgen}] = (\mathsf{MB\text{-}AIPO.Kg}, \mathsf{MB\text{-}AIPO.Obf}, \mathsf{MB\text{-}AIPO.Ver})$ for a distribution $\mathcal{D} = \{D_k = (Z_k, X_k, Y_k)\}_{k\in\mathbb{N}}$ where X_k is uniform on $\{0,1\}^{2k/3}$ and Y_k is uniform on $\{0,1\}^{k/3}$, for all $k \in \mathbb{N}$. Here Z_k denotes the distribution on the auxiliary input. The reason why the order of x and y are switched in the argument

to RSA is because of how we will use it in conjunction with our RSA-OAEP instantiation. As an aside, if there is no auxiliary input, it is easy to see that the presented MB-AIPO is secure — under a *stronger* definition where the adversary *gets* either the output point or a random one — assuming the function $\mathsf{hcf}_{k/3}(x) = x|_{k/3}$ for $x \in \mathbb{Z}_N^*$ is hardcore. Indeed, in the absence of auxiliary input, a uniform output distribution makes the standard security notion vacuous. However, since we *do* have auxiliary input in our application, we do not pursue such a definition further.

Enhanced construction. The major problem with the basic RSA-based MB-AIPO in our application is that in RSA-OAEP $r^* \in \{0,1\}^\rho$ is the input point and $z^* \in \{0,1\}^{\mu+\zeta}$ is the output point for the MB-AIPO, and the latter is *longer*. It is tempting to try to get a result for the opposite regime (long r^*, short z^*), but this runs into the problem that we need $(\mu, \mu+\zeta)$-SIE for the instantiation, so z^* *must* be long. To address this, we process z^* in "chunks." Namely, given RSAgen, again in Figure 38 (bottom) we define a canonical *enhanced* MB-AIPO $\mathsf{MB\text{-}AIPO}^*[\mathsf{RSAgen}] = (\mathsf{MB\text{-}AIPO}^*.\mathsf{Kg}, \mathsf{MB\text{-}AIPO}^*.\mathsf{Obf}, \mathsf{MB\text{-}AIPO}^*.\mathsf{Ver})$ for a distribution $\mathcal{D} = \{D_k = (Z_k, X_k, Y_k)\}_{k\in\mathbb{N}}$ where X_k is uniform on $\{0,1\}^{k/3}$ and Y_k is uniform on $\{0,1\}^{2k/3}$. Note that the modulus N for a "chunk" is such $7k/9$. meaning to use this MB-AIPO one needs a correspondingly larger modulus size for the same security level.

Security of the enhanced construction. Security of the enhanced RSA-based MB-AIPO is a question of *composability*. Namely, for $q \in \mathbb{N}$ we say $\mathsf{MB\text{-}AIPO}$ is *q-same-input-point (q-SIP) composable* for $\mathcal{D} = \{D_k = (X_k, Y_k^{(1)}, \ldots, Y_k^{(q)}, Z_k)\}_{k\in\mathbb{N}}$ if for any PPT distinguisher A, the associated advantage

$$\mathbf{Adv}^{\mathrm{comp}}_{\mathsf{MB\text{-}AIPO},A,\mathcal{D}}(k) = 2 \cdot \Pr\left[\mathrm{SIP\text{-}COMP}^{\mathcal{D},A,q}_{\mathsf{MB\text{-}AIPO}}(k) \Rightarrow 1\right] - 1 \ ,$$

is negligible in k, where the experiment is defined in Figure 39. We next reduce security of the enhanced RSA-based MB-AIPO to SIP-composability of the basic RSA-based MB-AIPO.

Proposition 3. *Suppose* $\mathsf{MB\text{-}AIPO}[\mathsf{RSAgen}]$ *is 6-SIP composable for* $\mathcal{D} = \{D_k = (X_k, Y_k^{(1)}, \ldots, Y_k^{(6)}, Z_k)\}_{k\in\mathbb{N}}$ *where* $X_k \in \{0,1\}^{k/3}, Y_k^{(i)} \in \{0,1\}^{k/9}$ $\forall i \in [6]$ *are all uniform and independent. Then* $\mathsf{MB\text{-}AIPO}^*[\mathsf{RSAgen}]$ *is secure for* $\mathcal{D}^* = \{D_k^* = (X_k, Y_k, Z_k)\}_{k\in\mathbb{N}}$ *where* X_k *is uniform on* $\{0,1\}^{2k/3}$ *and* Y_k *is independent and uniform on* $\{0,1\}^{k/3}$.

We conjecture:

Conjecture 1. $\mathsf{MB\text{-}AIPO}[\mathsf{RSAgen}]$ is 6-SIP-composable for the above distribution where Z_k is as in $\mathcal{D}^{\mathcal{OAEP}}$. Thus, by Proposition 3 $\mathsf{MB\text{-}AIPO}^*[\mathsf{RSAgen}]$ is secure for $\mathcal{D}^{\mathcal{OAEP}}$.

To reason about this, recall $\mathcal{D}^{\mathcal{OAEP}}$:

$\underline{\mathsf{MB\text{-}AIPO.Kg}(1^k)}$:	$\underline{\mathsf{MB\text{-}AIPO.Obf}(N,x,y)}$:	$\underline{\mathsf{MB\text{-}AIPO.Ver}(N,x',c)}$:
$(N,p,q,3,d) \leftarrow\!\$\ \mathsf{RSAgen}(1^k)$	$c \leftarrow (y\|x)^3 \bmod N$	$y' \leftarrow \mathsf{Ext}(N,c,x')$
Return N	Return c	If $(y'\|x')^3 \bmod N = c$ then
		Return y'
		Else return $\perp$

$\underline{\mathsf{MB\text{-}AIPO}^*.\mathsf{Kg}(1^k)}$:	$\underline{\mathsf{MB\text{-}AIPO}^*.\mathsf{Obf}(\perp,x,y)}$:	$\underline{\mathsf{MB\text{-}AIPO}^*.\mathsf{Ver}(\perp,x',(c,N))}$:
Return $\perp$	$o \leftarrow k/9$	$(c_1,N_1\ldots,c_6,N_6) \leftarrow c$
	For $i = 1$ to 6 do	If for all $i = 1$ to 6
	$y' \leftarrow y\|_i^{i+o}$	$\mathsf{MB\text{-}AIPO.Ver}(N_i,x',c_i) \Rightarrow 1$
	$(N,p,q,3,d) \leftarrow\!\$\ \mathsf{RSAgen}(1^{7k/9})$	Then return 1
	$c \leftarrow (y'\|x)^e \bmod N$	Else return 0
	$\mathbf{c}$.append(c,N)	
	$i \leftarrow i+o$	

Fig. 38: **MB-AIPO construction** MB-AIPO[RSAgen].

Game $\text{SIP-COMP}^{\mathcal{D},A}_{\mathsf{MB\text{-}AIPO}}(k)$
$b \leftarrow\!\$\ \{0,1\}$; $(x,y_1\ldots,y_q,z) \leftarrow\!\$\ D_k$
If $b = 0$ then $y_i \leftarrow\!\$\ \{0,1\}^{|y_i|}\ \forall i \in [q]$
$p_i \leftarrow\!\$\ \mathsf{MB\text{-}AIPO}(x,y_i)\ \forall i \in [q]$
$b' \leftarrow\!\$\ A(p_1,\ldots,p_q,z)$
Return $(b = b')$

Fig. 39: **Game to define SIP-COMP security.**

Distribution $D_k^{\mathcal{OAEP}}$
$r^* \leftarrow\!\$\ \{0,1\}^\rho$; $z^* \leftarrow\!\$\ \{0,1\}^{\mu+\zeta}$
$K_H \leftarrow\!\$\ \mathcal{K}_H(1^k)$; $(F,F^{-1}) \leftarrow\!\$\ \mathsf{Kg}(1^k)$
$m \leftarrow\!\$\ \{0,1\}^\mu$
$s^* \leftarrow z^* \oplus (m\|0^\zeta)$; $y^* \leftarrow H(K_H,s^*)$
$t^* \leftarrow r^* \oplus y^*$; $c^* \leftarrow F(s^*\|t^*)$
$t \leftarrow\!\$\ \{0,1\}^{\mu+\zeta}$; $d \leftarrow \langle t,z^*\rangle$
$L \leftarrow (t,d,c^*,K_H,F,m)$
Return (L,r^*,z^*)

We expand out the terms the adversary is given in this case:

$$L = (t,d,c^*,K_H,F,m,c_1,\ldots,c_6)$$

where c^* is the RSA-OAEP encryption for m modulo $|N| = k$ using r^* and z^* appropriately and $c_1,\ldots,c_6$ are $(z_i^*||r^*)^3 \mod N_i$ for $i = 1$ to 6 where z_i^* are the "chunks" of z^* of length $|N|/9$ and $|N_i| = 7|N|/9$. It suffices to argue that z^* is hard to recover from

$$L' = (c^*,K_H,F,m,c_1,\ldots,c_6)$$

because then we can replace d with an independent random bit by the Goldreich-Levin [44]. That z^* is hard to recover from L seems to us a reasonable conjecture about RSA; it is also reasonable to conjecture sub-exponential security.