On Selective-Opening Security of Deterministic Primitives

Adam O'Neill[1] Mohammad Zaheri[2]

February 13, 2020

Abstract

Classically, selective-opening attack (SOA) has been studied for *randomized* primitives, like randomized encryption schemes and commitments. The study of SOA for deterministic primitives, which presents some unique challenges, was initiated by Bellare *et al.* (PKC 2015), who showed negative results. Subsequently, Hoang *et al.* (ASIACRYPT 2016) showed positive results in the non-programmable random oracle model. Here we show the first positive results for SOA security of deterministic primitives in the *standard* (RO devoid) model. Our results are:

- Any $2t$-wise independent hash function is SOA secure for an unbounded number of "t-correlated" messages, meaning any group of up to t messages are arbitrarily correlated.
- An analogous result for deterministic encryption, from close variant of a NPROM scheme proposed by Hoang *et al.*
- We connect the one-more-RSA problem of Bellare *et al.* (J. Cryptology 2003) to this context and demonstrate this problem is hard under the Φ-Hiding Assumption with large enough encryption exponent.

Our results indicate that SOA for deterministic primitives in the standard model is more tractable than prior work would indicate.

Keywords: Selective Opening Security, One-More RSA, Randomness Extractor, Deterministic Public-Key Encryption, Information Theoretic Setting.

[1] Dept. of Computer Science, University of Massachusetts Amherst, Email: `adamo@cs.umass.edu`
[2] Dept. of Computer Science, Georgetown University, Email: `mz394@georgetown.edu`

Contents

1 Introduction

In this paper, we study selective-opening-attack (SOA) security of some *deterministic* primitives, namely hash functions and (public-key) deterministic encryption, extending the work of Hoang *et al.* [19] in addition to answering some open questions there.

1.1 Background and Motivation

SOA security. Roughly, SOA security of a cryptographic primitive refers to giving the adversary the power to adaptively choose instances of the primitive to corrupt and considering security of the uncorrupted instances. SOA grew out of work on non-committing and deniable primitives [15, 10, 24, 13, 11, 9, 25, 6, 28], which are even stronger forms of security. Namely, SOA has been studied in a line of work on public-key encryption and commitments started by Bellare, Hofheinz, and Yilek [3, 2, 20, 18, 7, 21]. When considering adaptive corruption, SOA arguably captures the security one wants in practice. Here we only consider *sender* SOA (*i.e.*, sender, not receiver, corruption), which we just refer to SOA security in the remainder of the paper for simplicity.

SOA for deterministic encryption. SOA security has usually been studied for *randomized* primitives, where the parties use random coins that are given to the adversary when corrupted, in particular randomized encryption. The study of SOA for deterministic primitives, namely deterministic encryption was initiated by Bellare *et al.* [1], who showed an impossibility result wrt. a simulation based definition. Subsequently, Hoang *et al.* [19] proposed a comparison based definition and showed positive results in the non programmable random oracle (RO) model [5, 23]. They left open the problem of constructions in the standard (RO devoid) model, which we study in this work. In particular, Hoang *et al.* emphasized this problem is open even for uniform and independent messages.

SOA for hash functions. In addition to randomized encryption, SOA security has often been considered for randomized commitments. Note that a simple construction of a commitment in the RO model is $H(x\|r)$ where x is the input and r is the randomness (decommitment). Analogously to the case of encryption, we study SOA security of hash functions. This can also be seen as studying the more basic case compared to deterministic encryption, as Goyal *et al.* [17] did in the non-SOA setting. The practical motivation is *password hashing* — note some passwords may be recovered by coercion, and one would like to say something about security of the other passwords.

One-more RSA inversion problem. Finally, an influential problem that we cast in the framework of SOA (this problem has not been explicitly connected to SOA before as far as we are aware) is the *one-more RSA inversion problem* of Bellare *et al.* [4]. Informally, the problem asks that an adversary with many RSA challenges and an inversion oracle cannot produce more preimages than number of oracle calls. Bellare *et al.* show this leads to a proof of security of Chaum's blind signature scheme in the RO model.

Challenges. For randomized primitives, a key challenge in security proofs has been that at the time the simulator prepares the challenge ciphertexts it does not know the subset that the adversary will corrupt. Compared to randomized primitives, deterministic primitives additionally presents some unique challenges in the SOA setting. To see why, say for encryption, a common strategy is for the simulator to "lie" about the randomness in order to make the message encrypt to the right ciphertext. However, in the deterministic case the adversary there is no randomness to fake.

1.2 Our Contributions

Results for hash functions. We start with the study of a more basic primitive than deterministic encryption, namely hash functions (which in some sense are the deterministic analogue of commitments). We note that SOA notion for hash functions is stronger than the one-wayness notion. We point that the SOA adversary without any opening could simply run the one-wayness adversary on each image challenge and recover the preimages. Thus, SOA notion is strictly stronger than one-wayness. Here we show results for an unbounded number of "t-correlated" messages, meaning each set of up to t messages may be arbitrarily correlated. Namely, we show that $2t$-wise independent hash functions, which can be realized information-theoretically by a classical construction of polynomial evaluation. We also consider the notion of t-correlated messages to be interesting in its own right, and it captures a setting with password hashing where a password is correlated with a small number of others (and it is even stronger than that, in that a password may be correlated with *any* small number of others).

To show $2t$-wise independent hash functions are SOA secure, we first show that in the information theoretic setting, knowing the content of opened messages increases the upper-bound for advantage of adversary by at most factor of 2. This is because the messages are independent and knowing the opened messages does not increase the advantage of adversary on guessing the unopened messages. Then, we show that for any hash key s in the set of "good hash keys", the probability of $H(s, X) = y$ is almost equally distributed over all hash value y. Therefore, we can show for any hash key s in the set of "good hash keys" and any vector of hash values, opening does not increases the upper-bound for advantage of adversary. Thus, it is only enough to bound the advantage of adversary without any opening.

Constructions in the standard model. In the setting of deterministic encryption, it is easy to see the same strategy as above works using lossy trapdoor functions [27] that are $2t$-wise independent in the lossy mode. However, for $t > 1$ we are not aware of any such construction and highlight this as an interesting open problem.[1] Hence, we turn to build a D-SO-CPA secure scheme in the standard model. We give a new DPKE scheme using $2t$-wise independent hash functions and regular lossy trapdoor function [27], which has practical instantiations, e.g., RSA is regular lossy [22]. A close variant of our scheme is shown to be D-SO-CPA secure in the NPROM [19]. The proof strategy here is very similar to proof of hash function. We start by switching to the lossy mode and then bound the advantage of adversary in the information theoretic setting.

Results for one-more-RSA. Bellare *et al.* [4] were first to introduce one-more-RSA problem. They show assuming hardness of one-more-RSA inversion problem leads to a proof of security of Chaum's blind signature scheme [12] in the random oracle model. This problem is natural SOA extension of the one-wayness of RSA. Intuitively, in the one-more inversion problem, the adversary gets a number of image points, and must output the inverses of all image points, while it has access to the corruption oracle and can see the preimage of image points of its choice. We note that the number of corruption queries is less than the number of image points. We show that one-more inversion problem is hard for RSA with a large enough encryption exponent e. In particular, we show that one-more inversion problem is hard for any regular lossy trapdoor function. Intuitively, we show that in the lossy mode the images are uniformly distributed. Then we show that inverting even one of the images is hard, since any preimage x is equally likely.

1.3 Discussion and Related Work

Seeing us as replacing random oracles. Another way of seeing our treatment of hash functions is as isolating a property of random oracles and realizing it in the standard model, building on a line of work in this vein started by Canetti [8]. In this context, it would be interesting to consider *adaptive* SOA security for hash functions similar to [26] who consider adaptive commitments. We leave this as another open problem. Additionally, it would be interested in our results allow replacing ROs in any particular higher-level protocol.

2 Preliminaries

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. If A is deterministic we denote this instead by $y \leftarrow A(x)$. We denote by $[A(x)]$ the set of all possible outputs of A when run on input x. For a finite set S, we denote by $s \leftarrow\!\!\$\ S$ the choice of a uniformly random element from S and assigning it to s.

Let $\mathbb{N}$ denote the set of all non-negative integers. For any $n \in \mathbb{N}$ we denote by $[n]$ the set $\{1, \ldots, n\}$. For a vector $\mathbf{x}$, we denote by $|\mathbf{x}|$ its length (number of components) and by $\mathbf{x}[i]$ its i-th component. For a vector $\mathbf{x}$ of length n and any $I \subseteq [n]$, we denote by $\mathbf{x}[I]$ the vector of length $|I|$ such that $\mathbf{x}[I] = (\mathbf{x}[i])_{i \in I}$, and by $\mathbf{x}[\overline{I}]$ the vector of length $n - |I|$ such that $\mathbf{x}[\overline{I}] = (\mathbf{x}[i])_{i \notin I}$. For a string X, we denote by $|X|$ its length.

Let X, Y be random variables taking values on a common finite domain. The *statistical distance* between X and Y is given by

$$\Delta(X, Y) = \frac{1}{2} \sum_{x} \left| \Pr\left[\, X = x \,\right] - \Pr\left[\, Y = x \,\right] \right| .$$

[1] It is tempting to give a Paillier-based construction with a degree $2t$ polynomial in the exponent, but unfortunately the coefficients don't lie in a field so the classical proof of $2t$-wise independence does not work.

```
Game D-CPA1-REAL$^{A,\mathcal{M}}_{\mathsf{DE}}(k)$
    $param \leftarrow\!\!\$\; A.\mathrm{pg}(1^k)$
    $(pk, sk) \leftarrow\!\!\$\; \mathsf{Kg}(1^k)$
    $\mathbf{m}_1 \leftarrow\!\!\$\; \mathcal{M}(1^k, param)$
    For $i = 1$ to $|\mathbf{m}|$ do
      $\mathbf{c}[i] \leftarrow \mathsf{Enc}(pk, \mathbf{m}_1[i])$
    $(state, I) \leftarrow\!\!\$\; A.\mathrm{cor}(pk, \mathbf{c}, param)$
    $\omega \leftarrow\!\!\$\; A.\mathrm{g}(state, \mathbf{m}_1[I], param)$
    Return $(\omega = A.\mathrm{f}(\mathbf{m}_1, param))$
```

```
Game D-CPA1-IDEAL$^{A,\mathcal{M}}_{\mathsf{DE}}(k)$
    $param \leftarrow\!\!\$\; A.\mathrm{pg}(1^k)$
    $(pk, sk) \leftarrow\!\!\$\; \mathsf{Kg}(1^k)$
    $\mathbf{m}_1 \leftarrow\!\!\$\; \mathcal{M}(1^k, param)$
    For $i = 1$ to $|\mathbf{m}|$ do
      $\mathbf{c}[i] \leftarrow \mathsf{Enc}(pk, \mathbf{m}_1[i])$
    $(state, I) \leftarrow\!\!\$\; A.\mathrm{cor}(pk, \mathbf{c}, param)$
    $\mathbf{m}_0 \leftarrow\!\!\$\; \mathsf{Resamp}_{\mathcal{M}}(1^k, \mathbf{m}_1[I], I, param)$
    $\omega \leftarrow\!\!\$\; A.\mathrm{g}(state, \mathbf{m}_1[I], param)$
    Return $(\omega = A.\mathrm{f}(\mathbf{m}_0, param))$
```

Figure 1: **Games to define the D-SO-CPA security.**

We also define $\Delta(X, Y \mid S) = \frac{1}{2}\sum_{x \in S} \big|\Pr[\, X = x\,] - \Pr[\, Y = x\,]\big|$, for a set S. The *min-entropy* of a random variable X is $\mathrm{H}_\infty(X) = -\log(\max_x \Pr[\, X = x\,])$. The *average conditional min-entropy* of X given Y is

$$\widetilde{\mathrm{H}}_\infty(X|Y) = -\log(\sum_y P_Y(y) \max_x \Pr[\, X = x \mid Y = y\,]) \ .$$

Entropy after information leakage. Dodis *et al.* [14] characterized the effect of auxiliary information on average min-entropy:

Lemma 2.1 [14] Let X, Y, Z be random variables and $\delta > 0$ be a real number.
(a) If Y has at most 2^λ possible values then we have $\widetilde{\mathrm{H}}_\infty(X \mid Z, Y) \geq \widetilde{\mathrm{H}}_\infty(X \mid Z) - \lambda$.
(b) Let S be the set of values b such that $\mathrm{H}_\infty(X \mid Y = b) \geq \widetilde{\mathrm{H}}_\infty(X \mid Y) - \log(1/\delta)$. Then it holds that $\Pr[Y \in S] \geq 1 - \delta$.

2.2 Public-Key Encryption

Public-key encryption. A public-key encryption scheme PKE with message-space Msg is a tuple of algorithms $(\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec})$ defined as follows. The key-generation algorithm Kg on input unary encoding of the security parameter 1^k outputs a public key pk and matching secret key sk. The encryption algorithm Enc on inputs a public key pk and message $m \in \mathsf{Msg}(1^k)$ outputs a ciphertext c. The deterministic decryption algorithm Dec on inputs a secret key sk and ciphertext c outputs a message m or $\perp$. We require that for all $(pk, sk) \in [\mathsf{Kg}(1^k)]$ and all $m \in \mathsf{Msg}(1^k)$, it holds that $\mathsf{Dec}(sk, (\mathsf{Enc}(pk, m)) = m$. We say that PKE is *deterministic* if Enc is deterministic.

D-SO-CPA security. Let $\mathsf{DE} = (\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec})$ be a D-PKE scheme. To a message sampler $\mathcal{M}$ and an adversary $A = (A.\mathrm{pg}, A.\mathrm{cor}, A.\mathrm{g}, A.\mathrm{f})$, we associate the experiment in Figure 1 for every $k \in \mathbb{N}$. We say that DE is D-SO-CPA secure for a class $\mathscr{M}$ of efficiently resamplable message samplers and a class $\mathscr{A}$ of adversaries if for every $\mathcal{M} \in \mathscr{M}$ and any $A \in \mathscr{A}$,

$$\begin{aligned} &\mathbf{Adv}^{\text{d-so-cpa}}_{\mathsf{DE},A,\mathcal{M}}(k) \\ = \ &\Pr\left[\text{D-CPA1-REAL}^{A,\mathcal{M}}_{\mathsf{DE}}(k) \Rightarrow 1\right] - \Pr\left[\text{D-CPA1-IDEAL}^{A,\mathcal{M}}_{\mathsf{DE}}(k) \Rightarrow 1\right] \end{aligned}$$

is negligible in k.

2.3 Lossy Trapdoor Functions and Their Security

Lossy trapdoor functions. A lossy trapdoor function [27] with domain LDom, range LRng and lossiness τ is a tuple of algorithms $\mathsf{LT} = (\mathsf{IKg}, \mathsf{LKg}, \mathsf{Eval}, \mathsf{Inv})$ that work as follows. Algorithm IKg on input a unary encoding of the security parameter 1^k outputs an "injective" evaluation key ek and matching trapdoor td. Algorithm LKg on input 1^k outputs a "lossy" evaluation key lk. Algorithm Eval on inputs an (either injective or lossy) evaluation key ek and $x \in \mathsf{LDom}(k)$ outputs $y \in \mathsf{LRng}(k)$. Algorithm Inv on inputs a trapdoor td and a $y \in \mathsf{LRng}(k)$ outputs $x \in \mathsf{LDom}(k)$. We denote by $\mathsf{Img}(lk)$ the co-domain of $\mathsf{Eval}(lk, \cdot)$. We require the following properties:

Correctness: For all $k \in \mathbb{N}$, all $(ek, td) \in [\mathsf{IKg}(1^k)]$ and all $x \in \mathsf{LDom}(k)$ it holds that $\mathsf{Inv}(td, \mathsf{Eval}(ek, x)) = x$.

Key indistinguishability: We require that for every PPT distinguisher D, the following advantage be negligible in k.

$$\mathbf{Adv}^{\mathrm{ltdf}}_{\mathsf{LT},D}(k) = \Pr\left[\, D(ek) \Rightarrow 1 \,\right] - \Pr\left[\, D(lk) \Rightarrow 1 \,\right] \ .$$

where $(ek, td) \leftarrow_{\$} \mathsf{IKg}(1^k)$ and $lk \leftarrow_{\$} \mathsf{LKg}(1^k)$.

Lossiness: The size of the co-domain of $\mathsf{Eval}(lk, \cdot)$ is at most $|\mathsf{LRng}(k)|/2^{\tau(k)}$ for all $k \in \mathbb{N}$ and all $lk \in [\mathsf{LKg}(1^k)]$. We call τ the *lossiness* of LT.

t-WISE INDEPENDENT. Let LT be a lossy trapdoor function with domain LDom, range LRng and lossiness τ. We say LT is t-wise independent if for all $lk \in [\mathsf{LKg}(1^k)]$ and all distinct $x_1, \ldots, x_{t(k)} \in \mathsf{LDom}(k)$

$$\Delta\left((\mathsf{Eval}(lk, x_1), \ldots, \mathsf{Eval}(lk, x_{t(k)})), (U_1, \ldots, U_{t(k)})\right) = 0$$

where $lk \leftarrow_{\$} \mathsf{LKg}(1^k)$ and $U_1, \ldots, U_{t(k)}$ are uniform and independent on $\mathsf{LRng}(k)$.

REGULARITY. Let LT be a lossy trapdoor function with domain LDom, range LRng and lossiness τ. We say LT is regular if for all $lk \in [\mathsf{LKg}(1^k)]$ and all $y \in \mathsf{Img}(lk)$, we have $\Pr\left[\, \mathsf{Eval}(lk, U) = y \,\right] = 1/|\mathsf{Img}(lk)|$, where U is uniform on $\mathsf{LDom}(k)$.

2.4 Hash Functions and Associated Security Notions

HASH FUNCTIONS. A *hash function* with domain HDom and range HRng is a pair of algorithms $\mathsf{H} = (\mathsf{HKg}, \mathsf{h})$ that work as follows. Algorithm HKg on input a unary encoding of the security parameter 1^k outputs a key K. Algorithm h on inputs a key K and $x \in \mathsf{HDom}(k)$ outputs $y \in \mathsf{HRng}(k)$. We say that H is *t-wise independent* if for all $k \in \mathbb{N}$ and all distinct $x_1, \ldots, x_{t(k)} \in \mathsf{HDom}(k)$

$$\Delta\left((\mathsf{h}(K, x_1), \ldots, \mathsf{h}(K, x_{t(k)})), (U_1, \ldots, U_{t(k)})\right) = 0$$

where $K \leftarrow_{\$} \mathsf{HKg}(1^k)$ and $U_1, \ldots, U_{t(k)}$ are uniform and independent in $\mathsf{HRng}(k)$.

3 Selective Opening Security for Hash Functions

Bellare, Dowsley, and Keelveedhi [1] were the first to consider selective-opening security of deterministic PKE. They propose a "simulation-based" semantic security notion, but then show that this definition is unachievable in both the standard model and the non-programmable random-oracle model. Later in [19] Hoang *et al.* introduce an alternative, "comparison-based" semantic-security notion and show that this definition is achievable in the non-programmable random-oracle model but leave it open in the standard model. In this section, we extend their definitions to hash function families and show that t-wise independent hash functions are selective opening secure under this notion.

3.1 Security Notion

MESSAGE SAMPLERS. A *message sampler* $\mathcal{M}$ is a PPT algorithm that takes as input the unary representation 1^k of the security parameter and a string $param \in \{0,1\}^*$, and outputs a vector $\mathbf{m}$ of messages. We require that $\mathcal{M}$ be associated with functions v and n such that for any $param \in \{0,1\}^*$, for any $k \in \mathbb{N}$, and any $\mathbf{m} \in [\mathcal{M}(1^k, param)]$, we have $|\mathbf{m}| = v(k)$ and $|\mathbf{m}[i]| = n(k)$, for every $i \leq |\mathbf{m}|$. Moreover, the components of $\mathbf{m}$ must be distinct. Let $\mathsf{Coins}[k]$ be the set of coins for $\mathcal{M}(1^k, \cdot)$. Define $\mathsf{Coins}[k, \mathbf{m}, I, param] = \{\omega \in \mathsf{Coins}[k] \mid \mathbf{m}[I] = \mathbf{m}'[I],$ where $\mathbf{m}' \leftarrow \mathcal{M}(1^k, param; \omega)\}$.

A message sampler $\mathcal{M}$ is (μ, d)-*correlated* if

- For any $k \in \mathbb{N}$, any $param \in \{0,1\}^*$, every $\mathbf{m} \in [\mathcal{M}(1^k, param)]$ and any $i \in [v]$, $\mathbf{m}[i]$ have min-entropy at least μ and is independent of at least $v - d$ messages.
- Messages $\mathbf{m}[1], \ldots, \mathbf{m}[v(k)]$ must be distinct, for any $param \in \{0,1\}^*$ and any $\mathbf{m} \in [\mathcal{M}(1^k, param)]$.

Note that in this definition, d can be 0, which corresponds to a message sampler in which each message is independent of all other messages and has at least μ bits of min-entropy.

```
Game H-SO-REAL$_{\mathsf{H}}^{A,\mathcal{M}}(k)$
    $param \leftarrow\$ A.\mathrm{pg}(1^k)$
    $K \leftarrow\$ \mathsf{HKg}(1^k)$
    $\mathbf{m}_1 \leftarrow\$ \mathcal{M}(1^k, param)$
    For $i = 1$ to $|\mathbf{m}_1|$ do
        $\mathsf{h}[i] \leftarrow \mathsf{h}(K, \mathbf{m}_1[i])$
    $(state, I) \leftarrow\$ A.\mathrm{cor}(K, \mathbf{h}, param)$
    $\omega \leftarrow\$ A.\mathrm{g}(state, \mathbf{m}_1[I], param)$
    Return $(\omega = A.\mathrm{f}(\mathbf{m}_1, param))$
```

```
Game H-SO-IDEAL$_{\mathsf{H}}^{A,\mathcal{M}}(k)$
    $param \leftarrow\$ A.\mathrm{pg}(1^k)$
    $K \leftarrow\$ \mathsf{HKg}(1^k)$
    $\mathbf{m}_1 \leftarrow\$ \mathcal{M}(1^k, param)$
    For $i = 1$ to $|\mathbf{m}_1|$ do
        $\mathsf{h}[i] \leftarrow \mathsf{h}(K, \mathbf{m}_1[i])$
    $(state, I) \leftarrow\$ A.\mathrm{cor}(K, \mathbf{h}, param)$
    $\omega \leftarrow\$ A.\mathrm{g}(state, \mathbf{m}_1[I], param)$
    $\mathbf{m}_0 \leftarrow\$ \mathsf{Resamp}_{\mathcal{M}}(1^k, \mathbf{m}_1[I], I, param)$
    Return $(\omega = A.\mathrm{f}(\mathbf{m}_0, param))$
```

Figure 2: **Games to define the H-SO security.**

RESAMPLING. Following [3], let $\mathsf{Resamp}_{\mathcal{M}}(1^k, I, \mathbf{x}, param)$ be the algorithm that samples $r \leftarrow\$ \mathsf{Coins}[k, \mathbf{m}, I, param]$ and returns $\mathcal{M}(1^k, param; r)$. (We note that Resamp may run in exponential time.) A *resampling algorithm* of $\mathcal{M}$ is an algorithm Rsmp such that $\mathsf{Rsmp}(1^k, I, \mathbf{x}, param)$ is identically distributed as $\mathsf{Resamp}_{\mathcal{M}}(1^k, I, \mathbf{x}, param)$. A message sampler $\mathcal{M}$ is *efficiently resamplable* if it admits a PT resampling algorithm.

H-SO SECURITY. Let $\mathsf{H} = (\mathsf{HKg}, \mathsf{h})$ be a hash function family with domain HDom and range HRng. To an adversary $A = (A.\mathrm{pg}, A.\mathrm{cor}, A.\mathrm{g}, A.\mathrm{f})$ and a message sampler $\mathcal{M}$, we associate the experiment in Figure 2 for every $k \in \mathbb{N}$. We say that H is H-SO secure for a class $\mathscr{M}$ of efficiently resamplable message samplers and a class $\mathscr{A}$ of adversaries if for every $\mathcal{M} \in \mathscr{M}$ and any $A \in \mathscr{A}$,

$$\begin{aligned}&\mathbf{Adv}^{\text{h-so}}_{\mathsf{H},A,\mathcal{M}}(k)\\ =\ &\Pr\left[\text{H-SO-REAL}_{\mathsf{H}}^{A,\mathcal{M}}(k) \Rightarrow 1\right] - \Pr\left[\text{H-SO-IDEAL}_{\mathsf{H}}^{A,\mathcal{M}}(k) \Rightarrow 1\right]\end{aligned}$$

is negligible in k.

DISCUSSION. We refer to the messages indexed by I as the "opened" messages. For every message $\mathbf{m}[i]$ that adversary A opens, we require that every message correlated to $\mathbf{m}[i]$ to also be opened.

We show that it is suffices to consider balanced H-SO adversaries where output of A.f is boolean. We call A *δ-balanced* boolean H-SO adversary if for all $b \in \{0,1\}$,

$$\left|\Pr\left[\, t = b \ : \ t \leftarrow\$ A.\mathrm{f}(m, param) \,\right] - \frac{1}{2}\right| \leq \delta \ .$$

for all *param* and m output by A.pg and $\mathcal{M}$, respectively.

Theorem 3.1 Let $\mathsf{H} = (\mathsf{HKg}, \mathsf{h})$ be a hash function family with domain HDom and range HRng. Let A be a H-SO adversary against H with respect to message sampler $\mathcal{M}$. Then for any $0 \leq \delta < 1/2$, there is a *δ-balanced* boolean H-SO adversary B such that for all $k \in \mathbb{N}$

$$\mathbf{Adv}^{\text{h-so}}_{\mathsf{H},A,\mathcal{M}}(k) \leq \left(\frac{2\sqrt{2}}{\delta} + \sqrt{2}\right)^2 \cdot \mathbf{Adv}^{\text{h-so}}_{\mathsf{H},B,\mathcal{M}}(k) \ .$$

where the running time of A is about that of B plus $\mathcal{O}(1/\delta)$.

We refer to Appendix A for the proof of Theorem 3.1. Next, we give a useful lemma that we later use in our proofs.

Lemma 3.2 Let X, Y be random variables where $\widetilde{\mathrm{H}}_\infty(X \mid Y) \geq \mu$. For any $0 \leq \delta < 1/2$, random variable Y is a δ-balanced boolean. Then, $\mathrm{H}_\infty(X \mid Y = b) \geq \mu - \log(\frac{1}{2} - \delta)$ for all $b \in \{0,1\}$.

Proof: We know that $\Pr\left[\, Y = b \,\right] \geq 1/2 - \delta$, for all $b \in \{0,1\}$. We also have that $\sum_b \Pr\left[\, Y = b \,\right] \max_x \Pr\left[\, X = x \mid Y = b \,\right] \leq 2^{-\mu}$. Therefore, we obtain that $\max_x \Pr\left[\, X = x \mid Y = b \,\right] \leq 2^{-\mu}(1/2 - \delta)$ for all $b \in \{0,1\}$. Summing up, we get $\mathrm{H}_\infty(X \mid Y = b) \geq \mu - \log(\frac{1}{2} - \delta)$ for all $b \in \{0,1\}$. □ ▮

3.2 Achieving H-SO Security

We show in Theorem 3.3 that pair-wise independent hash functions are selective opening secure when the messages are independent and have high min-entropy. Specifically, we give an upper-bound for the advantage of H-SO adversary attacking the pair-wise independent hash function. We first show that in the information theoretic setting, knowing the content of opened messages increases the upper-bound for advantage of adversary by at most factor of 2. This is because the messages are independent and knowing the opened messages does not increase the advantage of adversary on guessing the unopened messages. We point that for any vector of hash values and hash key, value I is uniquely defined (unbounded adversary can be assumed deterministic) and based on the independence of the messages, we could drop the probability of opened messages in the upper-bound for the advantage of adversary. Note that the adversary still may increase its advantage by choosing I adaptively without seeing the opened messages, we later prove this is not the case.

We show in Lemma 3.4 that for any hash key s in the set of "good hash keys", the probability of $H(s,X)=y$ is almost equally distributed over all hash value y. Therefore, we can show for any hash key s in the set of "good hash keys" and any vector of hash values, opening does not increases the upper-bound for advantage of adversary. Thus, it is only enough to bound the advantage of adversary without any opening.

Theorem 3.3 Let $\mathsf{H} = (\mathsf{HKg}, \mathsf{h})$ be a family of pair-wise independent hash function with domain HDom and range HRng. Let $\mathcal{M}$ be a $(\mu, 0)$-correlated, efficiently resamplable message sampler. Then for any computationally unbounded adversary A,

$$\mathbf{Adv}^{\text{h-so}}_{\mathsf{H},A,\mathcal{M}}(k) \le 2592v\sqrt[3]{2^{1-\mu}|\mathsf{HRng}(k)|^2}\ .$$

Proof: We need the following lemma whose proof we'll give later.

Lemma 3.4 Let $\mathsf{H} = (\mathsf{HKg}, \mathsf{h})$ be a pair-wise independent hash function with domain HDom and range HRng. Let X be a random variable over HDom such that $\mathrm{H}_\infty(X) \ge \eta$. Then, for all $y \in \mathsf{HRng}(k)$ and for any $\epsilon > 0$,

$$\left|\Pr\left[\, H(K,X) = y \,\right] - |\mathsf{HRng}(k)|^{-1}\right| \ge \epsilon|\mathsf{HRng}(k)|^{-1}\ .$$

for at most 2^{-u} fraction of $K \in [\mathsf{HKg}(1^k)]$, where $u = \eta - 2\log|\mathsf{HRng}(k)| - 2\log(1/\epsilon)$.

We begin by showing H is H-SO secure against any $\frac{1}{4}$-balanced boolean adversary B. Observe that for computationally unbounded adversary B, we can assume wlog that B.cor, B.g and B.f are deterministic. Moreover, we can also assume that adversary B.cor pass $K, \mathbf{h}[\bar{I}]$ as state st to adversary B.g. We denote by $\mathbf{Adv}^{\text{h-so}}_{\mathsf{H},B,\mathcal{M},s}(k)$, advantage of B when $K = s$. For any fix key s we have

$$\begin{aligned}
&\Pr[\text{H-SO-REAL}^{B}_{\mathsf{H},s}(k) \Rightarrow 1] \\
=\ &\sum_{b=0}^{1}\sum_{I}\Pr[B.\mathrm{cor}(s,\mathbf{h}) \Rightarrow I \ \wedge\ B.\mathrm{g}(s,\mathbf{m}_1[I],\mathbf{h}[\bar{I}]) \Rightarrow b \ \wedge\ B.\mathrm{f}(\mathbf{m}_1) \Rightarrow b]
\end{aligned}$$

For any $\mathbf{y} \in (\mathsf{HRng}(k))^{\times v}$ and $s \in [\mathsf{HKg}(1^k)]$, we define $I_{s,\mathbf{y}}$ to be output of B.cor on input $s, \mathbf{y}$. We also define $M^b_{s,\mathbf{y}} = \{\mathbf{m}[I_{s,\mathbf{y}}] \mid B.\mathrm{g}(s,\mathbf{m}_1[I_{s,\mathbf{y}}],\mathbf{y}) \Rightarrow b\}$, for $b \in \{0,1\}$. Thus,

$$\begin{aligned}
&\Pr[\text{H-SO-REAL}^{B}_{\mathsf{H},s}(k) \Rightarrow 1] \\
=\ &\sum_{b=0}^{1}\sum_{\mathbf{y}}\Pr[\mathbf{h} = \mathbf{y} \ \wedge\ \mathbf{m}_1[I_{s,\mathbf{y}}] \in M^b_{s,\mathbf{y}} \ \wedge\ B.\mathrm{f}(\mathbf{m}_1) \Rightarrow b]
\end{aligned}$$

The above probability is over the choice of $\mathbf{m}_1$. Similarly, we can define the probability of the experiment H-SO-IDEAL outputting 1. Therefore, we obtain

$$\begin{aligned}
\mathbf{Adv}^{\text{h-so}}_{\mathsf{H},B,\mathcal{M},s}(k) \ =\ &\sum_{b=0}^{1}\sum_{\mathbf{y}}\Pr[\mathbf{h} = \mathbf{y} \ \wedge\ \mathbf{m}_1[I_{s,\mathbf{y}}] \in M^b_{s,\mathbf{y}} \ \wedge\ B.\mathrm{f}(\mathbf{m}_1) \Rightarrow b] \\
&\qquad - \Pr[\mathbf{h} = \mathbf{y} \ \wedge\ \mathbf{m}_1[I_{s,\mathbf{y}}] \in M^b_{s,\mathbf{y}} \ \wedge\ B.\mathrm{f}(\mathbf{m}_0) \Rightarrow b]
\end{aligned}$$

Assume wlog that above difference is maximized when $b = 1$. For $d \in \{0,1\}$, we define E_d as an event where $\mathbf{h}[I_{s,\mathbf{y}}] = \mathbf{y}[I_{s,\mathbf{y}}]$ and $\mathbf{m}_1[I_{s,\mathbf{y}}] \in M^1_{s,\mathbf{y}}$ and $B.\mathrm{f}(\mathbf{m}_d) = 1$. Note that the messages are independent and has μ bits of min-entropy. For convenience, we write I instead of $I_{s,\mathbf{y}}$. Then, we obtain

$$\begin{aligned}\mathbf{Adv}^{\text{h-so}}_{\mathsf{H},B,\mathcal{M},s}(k) \quad \leq \quad & 2 \cdot \sum_{\mathbf{y}} \Pr[E_1] \cdot \Pr[\mathbf{h}[\overline{I}] = \mathbf{y}[\overline{I}] \mid B.\mathrm{f}(\mathbf{m}_1) = 1] \\ & \qquad - \Pr[E_0] \cdot \Pr[\mathbf{h}[\overline{I}] = \mathbf{y}[\overline{I}]]\end{aligned}$$

Note that $\mathbf{m}_0$ and $\mathbf{m}_1$ have the same distribution. Then, we have $\Pr[E_0] = \Pr[E_1]$ and $\Pr[E_0] \leq \Pr[\mathbf{h}[I] = \mathbf{y}[I]]$. Therefore, we obtain

$$\begin{aligned}& \mathbf{Adv}^{\text{h-so}}_{\mathsf{H},B,\mathcal{M},s}(k) \\ \leq \quad & 2 \cdot \sum_{\mathbf{y}} \Pr[\mathbf{h}[I] = \mathbf{y}[I]] \cdot \Big(\Pr[\mathbf{h}[\overline{I}] = \mathbf{y}[\overline{I}] \mid B.\mathrm{f}(\mathbf{m}_1) = 1] - \Pr[\mathbf{h}[\overline{I}] = \mathbf{y}[\overline{I}]]\Big)\end{aligned}$$

We define random variable $\mathbf{X}[i] = (\mathbf{m}_1[i] \mid B.\mathrm{f}(\mathbf{m}_1) = 1)$, for all $i \in [v]$. From property (a) of Lemma 2.1 and Lemma 3.2, we obtain that $\mathrm{H}_\infty(\mathbf{X}[i]) \geq \mu - 3$. For all $i \in [v]$, we also have $\mathrm{H}_\infty(\mathbf{m}_1[i]) \geq \mu \geq \mu - 3$. Moreover, we know Lemma 3.4 holds for at most 2^{-u} fraction of $K \in [\mathsf{HKg}(1^k)]$, where $u = \mu - 3 - 2\log|\mathsf{HRng}(k)| - 2\log(1/\epsilon)$; we shall determine the value of ϵ later. Using union bound, for all $\mathbf{X}[i], \mathbf{m}[i]$, where $i \in [v]$ and for any $\epsilon > 0$, we obtain that for at least $1 - 2v2^{-u}$ fraction of K, we have $\big|\Pr\left[\, H(K, x[i]) = \mathbf{y}[i]\,\right] - |\mathsf{HRng}(k)|^{-1}\big| \leq \epsilon|\mathsf{HRng}(k)|^{-1}$, for all $i \in [v]$ and $x \in \{\mathbf{m}_1, \mathbf{X}\}$. Let S be the set of such K.

Now, we have for all $s \in S$ and $i \in [v]$, we obtain $(1-\epsilon)|\mathsf{HRng}(k)|^{-1} \leq \Pr\left[\,\mathbf{h}[i] = \mathbf{y}[i]\,\right] \leq (1+\epsilon)|\mathsf{HRng}(k)|^{-1}$. Let $|I_{s,\mathbf{y}}| = \ell$. Then,

$$\begin{aligned}\mathbf{Adv}^{\text{h-so}}_{\mathsf{H},B,\mathcal{M},s}(k) \quad & \leq \quad 2 \cdot \sum_{\mathbf{y}} |\mathsf{HRng}(k)|^{-v}(1+\epsilon)^{\ell}\Big((1+\epsilon)^{v-\ell} - (1-\epsilon)^{v-\ell}\Big) \\ & \leq \quad 2\Big((1+\epsilon)^{v} - (1-\epsilon)^{v}\Big)\end{aligned}$$

We also have $(1+\epsilon)^v = 1 + \sum_i \binom{v}{i}\epsilon^i \leq 1 + \sum_i \epsilon^i v^i$. For $\epsilon v < 1/2$, we obtain that $(1+\epsilon)^v \leq 1 + 2\epsilon v$. Similarly, we obtain that $(1-\epsilon)^v \geq 1 - 2\epsilon v$. Therefore, we have that $\mathbf{Adv}^{\text{h-so}}_{\mathsf{H},B,\mathcal{M},s}(k) \leq 8\epsilon v$. Then,

$$\begin{aligned}\mathbf{Adv}^{\text{h-so}}_{\mathsf{H},B,\mathcal{M}}(k) \quad & = \quad \sum_{s \in S} \Pr\left[\, K = s\,\right] \cdot \mathbf{Adv}^{\text{h-so}}_{\mathsf{H},B,\mathcal{M},s}(k) \\ & \qquad + \sum_{s \in \overline{S}} \Pr\left[\, K = s\,\right] \cdot \mathbf{Adv}^{\text{h-so}}_{\mathsf{H},B,\mathcal{M},s}(k) \\ & \leq \quad \max_{s \in S} \mathbf{Adv}^{\text{h-so}}_{\mathsf{H},B,\mathcal{M},s}(k) + 2v2^{-u} \;\; .\end{aligned}$$

Finally, by substituting $\epsilon = \sqrt[3]{2^{1-\mu}|\mathsf{HRng}(k)|^2}$, we obtain

$$\mathbf{Adv}^{\text{h-so}}_{\mathsf{H},B,\mathcal{M}}(k) \leq 16v\sqrt[3]{2^{1-\mu}|\mathsf{HRng}(k)|^2} \;\; .$$

Using Theorem 3.1, we obtain for any unbounded adversary A

$$\mathbf{Adv}^{\text{h-so}}_{\mathsf{H},A,\mathcal{M}}(k) \leq 2592v\sqrt[3]{2^{1-\mu}|\mathsf{HRng}(k)|^2} \;\; .$$

This completes the proof of Theorem 3.3. ▌

Proof of Lemma 3.4. We will need the following tail inequality for pair-wise independent distributions

Claim 3.5 Let $A_1, \cdots, A_n$ be pair-wise independent random variables in the interval $[0,1]$. Let $A = \sum_i A_i$ and

$\mathbb{E}(A) = \mu$ and $\delta > 0$. Then,

$$\Pr[\,|A-\mu| > \delta\mu\,] \le \frac{1}{\delta^2\mu} \ .$$

Proof of Claim 3.5. From Chebychev's inequality, for any $\delta > 0$ we have

$$\Pr[\,|A-\mu| > \delta\mu\,] \le \frac{\mathbf{Var}[A]}{\delta^2\mu^2} \ .$$

Note that $A_1, \cdots, A_n$ are pair-wise independent random variables. Thus, we have $\mathbf{Var}[A] = \sum_i \mathbf{Var}[A_i]$. Moreover, we know that $\mathbf{Var}[A_i] \le \mathbb{E}(A_i)$ for all $i \in [n]$, since the random variable A_i is in the interval $[0,1]$. Therefore, we have $\mathbf{Var}[A] \le \mu$. This completes the proof of Claim 3.5.

We define $p_x = \Pr[\,X = x\,]$, for any $x \in \mathsf{HDom}(k)$. We consider the probability over the choice of key K. For every $x \in \mathsf{HDom}(k)$ and $y \in \mathsf{HRng}(k)$, we also define the following random variable

$$Z_{x,y} = \begin{cases} p_x & \text{if } \ H(K,x) = y \\ 0 & \text{otherwise} \end{cases}$$

We define random variable $A_{x,y} = Z_{x,y}2^\eta$. Note that for every x, $H(K,x)$ is uniformly distributed, over the uniformly random choice of K. Therefore, we have $\mathbb{E}(Z_{x,y}) = p_x/|\mathsf{HRng}(k)|$, for every x, y. Let $Z_y = \sum_x Z_{x,y}$ and $A_y = \sum_x A_{x,y}$. Then, we have $\mathbb{E}(Z_y) = 1/|\mathsf{HRng}(k)|$ and $\mathbb{E}(A_y) = 2^\eta/|\mathsf{HRng}(k)|$. Moreover, for every x, y, we know $A_{x,y} \in [0,1]$ and for every y, the variables $A_{x,y}$ are pair-wise independent. Applying Claim 3.5, we obtain that for every y and $\delta > 0$

$$\Pr\left[\left|A_y - \frac{2^\eta}{|\mathsf{HRng}(k)|}\right| \ge \frac{\delta 2^\eta}{|\mathsf{HRng}(k)|}\right] \le \frac{|\mathsf{HRng}(k)|}{\delta^2 2^\eta} \ .$$

Substituting Z_y for A_y and choosing $\delta = \epsilon$, we obtain that for every $\epsilon > 0$,

$$\Pr\left[\left|Z_y - \frac{1}{|\mathsf{HRng}(k)|}\right| \ge \frac{\epsilon}{|\mathsf{HRng}(k)|}\right] \le \frac{|\mathsf{HRng}(k)|}{\epsilon^2 2^\eta} \ .$$

Using union bound, we obtain that with probability $|\mathsf{HRng}(k)|^2/\epsilon^2 2^\eta = 2^{-u}$ over the choice of K that $|Z_y - 1/|\mathsf{HRng}(k)|| \ge \epsilon/|\mathsf{HRng}(k)|$, for all $y \in |\mathsf{HRng}(k)|$. This completes the proof of Lemma 3.4. □

We show in Theorem 3.6 that the $2d$-wise independent hash functions are selective opening secure for (μ, d)-correlated message samplers.

Theorem 3.6 Let $\mathsf{H} = (\mathsf{HKg}, \mathsf{h})$ be a family of $2d$-wise independent hash function with domain HDom and range HRng. Let $\mathcal{M}$ be a (μ, d)-correlated, efficiently resamplable message sampler. Then for any computationally unbounded adversary A,

$$\mathbf{Adv}^{\text{h-so}}_{\mathsf{H},A,\mathcal{M}}(k) \le 2592v\sqrt[3]{2^{1-\mu}|\mathsf{HRng}(k)|^{2d}} \ .$$

Proof: We need the following lemma whose proof we'll give later.

Lemma 3.7 Let $\mathsf{H} = (\mathsf{HKg}, \mathsf{h})$ be a $2d$-wise independent hash function with domain HDom and range HRng. Let $\mathbf{X} = (X_1, \cdots, X_t)$, where $t \le d$ and X_i is a random variable over HDom such that $\mathrm{H}_\infty(X_i) \ge \eta$, for $i \in [t]$. Then, for all $\mathbf{y} = (y_1, \cdots, y_t)$, where $y_i \in \mathsf{HRng}(k)$ and for any $\epsilon > 0$,

$$\left|\Pr[\,H(K,\mathbf{X}) = \mathbf{y}\,] - |\mathsf{HRng}(k)|^{-t}\right| \ge \epsilon|\mathsf{HRng}(k)|^{-t} \ .$$

for at most 2^{-w} fraction of $K \in [\mathsf{HKg}(1^k)]$, where $w = \eta - 2t\log|\mathsf{HRng}(k)| - 2\log(1/\epsilon)$.

We begin by showing H is H-SO secure against any $\frac{1}{4}$-balanced boolean adversary B. Observe that for computationally unbounded adversary B, we can assume wlog that B.cor, B.g and B.f are deterministic. Moreover, we can also assume that adversary B.cor pass $K, \mathbf{h}[\bar{I}]$ as state st to adversary B.g. We denote by $\mathbf{Adv}^{\text{h-so}}_{\mathsf{H},B,\mathcal{M},s}(k)$, advantage of B when $K = s$. For any fix key s we have

$$\begin{aligned} & \Pr[\text{H-SO-REAL}^{B}_{\mathsf{H},s}(k) \Rightarrow 1] \\ = \; & \sum_{b=0}^{1} \sum_{I} \Pr[B.\mathrm{cor}(s, \mathbf{h}) \Rightarrow I \;\wedge\; B.\mathrm{g}(s, \mathbf{m}_1[I], \mathbf{h}[\bar{I}]) \Rightarrow b \;\wedge\; B.\mathrm{f}(\mathbf{m}_1) \Rightarrow b] \end{aligned}$$

For any $\mathbf{y} \in (\mathsf{HRng}(k))^{\times v}$ and $s \in [\mathsf{HKg}(1^k)]$, we define $I_{s,\mathbf{y}}$ to be output of B.cor on input $s, \mathbf{y}$. We also define $M^{b}_{s,\mathbf{y}} = \{\mathbf{m}[I_{s,\mathbf{y}}] \mid B.\mathrm{g}(s, \mathbf{m}_1[I_{s,\mathbf{y}}], \mathbf{y}) \Rightarrow b\}$, for $b \in \{0, 1\}$. Thus,

$$\begin{aligned} & \Pr[\text{H-SO-REAL}^{B}_{\mathsf{H},s}(k) \Rightarrow 1] \\ = \; & \sum_{b=0}^{1} \sum_{\mathbf{y}} \Pr[\mathbf{h} = \mathbf{y} \;\wedge\; \mathbf{m}_1[I_{s,\mathbf{y}}] \in M^{b}_{s,\mathbf{y}} \;\wedge\; B.\mathrm{f}(\mathbf{m}_1) \Rightarrow b] \end{aligned}$$

The above probability is over the choice of $\mathbf{m}_1$. Similarly, we can define the probability of the experiment H-SO-IDEAL outputting 1. Therefore, we obtain

$$\begin{aligned} \mathbf{Adv}^{\text{h-so}}_{\mathsf{H},B,\mathcal{M},s}(k) \;=\; & \sum_{b=0}^{1} \sum_{\mathbf{y}} \Pr[\mathbf{h} = \mathbf{y} \;\wedge\; \mathbf{m}_1[I_{s,\mathbf{y}}] \in M^{b}_{s,\mathbf{y}} \;\wedge\; B.\mathrm{f}(\mathbf{m}_1) \Rightarrow b] \\ & \qquad - \Pr[\mathbf{h} = \mathbf{y} \;\wedge\; \mathbf{m}_1[I_{s,\mathbf{y}}] \in M^{b}_{s,\mathbf{y}} \;\wedge\; B.\mathrm{f}(\mathbf{m}_0) \Rightarrow b] \end{aligned}$$

Assume wlog that the above difference is maximized when $b = 1$. For $d \in \{0, 1\}$, we define E_d as an event where $\mathbf{h}[I_{s,\mathbf{y}}] = \mathbf{y}[I_{s,\mathbf{y}}]$ and $\mathbf{m}_1[I_{s,\mathbf{y}}] \in M^{1}_{s,\mathbf{y}}$ and $B.\mathrm{f}(\mathbf{m}_d) = 1$. Note that the messages are independent and has μ bits of min-entropy. For convenience, we write I instead of $I_{s,\mathbf{y}}$. Then, we obtain

$$\begin{aligned} \mathbf{Adv}^{\text{h-so}}_{\mathsf{H},B,\mathcal{M},s}(k) \;\le\; & 2 \cdot \sum_{\mathbf{y}} \Pr[E_1] \cdot \Pr[\mathbf{h}[\bar{I}] = \mathbf{y}[\bar{I}] \mid B.\mathrm{f}(\mathbf{m}_1) = 1] \\ & \qquad - \Pr[E_0] \cdot \Pr[\mathbf{h}[\bar{I}] = \mathbf{y}[\bar{I}]] \end{aligned}$$

Note that $\mathbf{m}_0$ and $\mathbf{m}_1$ have the same distribution. Then, we have $\Pr[E_0] = \Pr[E_1]$ and $\Pr[E_0] \le \Pr[\mathbf{h}[I] = \mathbf{y}[I]]$. We define random variable $\mathbf{X}[i] = (\mathbf{m}_1[i] \mid B.\mathrm{f}(\mathbf{m}_1) = 1)$, for all $i \in [v]$. From property (a) of Lemma 2.1 and Lemma 3.2, we obtain that $\mathrm{H}_\infty(\mathbf{X}[i]) \ge \mu - 3$. For all $i \in [v]$, we also have $\mathrm{H}_\infty(\mathbf{m}_1[i]) \ge \mu \ge \mu - 3$

Moreover, we know Lemma 3.4 holds for at most 2^{-u} fraction of $K \in [\mathsf{HKg}(1^k)]$, where $u = \mu - 3 - 2d \log |\mathsf{HRng}(k)| - 2 \log(1/\epsilon)$; we shall determine the value of ϵ later. Partition $[v]$ to $L_1, \cdots, L_v$ such that $|L_k| \le d$ and for all $i, j \in L_k$, messages $\mathbf{m}[i]$ and $\mathbf{m}[j]$ are correlated. Using union bound, for all $\mathbf{y}[L_i] \in (\mathsf{HRng}(k))^{\times |L_i|}$, where $i \in [v]$ and for any $\epsilon > 0$, we obtain that for at least $1 - 2v2^{-u}$ fraction of K, we have $\big|\Pr[\, H(K, x[L_i]) = \mathbf{y}[L_i]\,] - |\mathsf{HRng}(k)|^{-|L_i|}\big| \le \epsilon |\mathsf{HRng}(k)|^{-|L_i|}$, for all $i \in [v]$ and $x \in \{\mathbf{m}_1, \mathbf{X}\}$. Let S be the set of such K.

Now, we have for all $s \in S$ and $i \in [v]$, we obtain $(1-\epsilon)|\mathsf{HRng}(k)|^{-|L_i|} \le \Pr[\, \mathbf{h}[L_i] = \mathbf{y}[L_i]\,] \le (1+\epsilon)|\mathsf{HRng}(k)|^{-|L_i|}$. Let $|I_{s,\mathbf{y}}| = \ell$. Then,

$$\begin{aligned} \mathbf{Adv}^{\text{h-so}}_{\mathsf{H},B,\mathcal{M},s}(k) \;&\le\; 2 \cdot \sum_{\mathbf{y}} |\mathsf{HRng}(k)|^{-v} (1+\epsilon)^{\ell} \Big((1+\epsilon)^{v-\ell} - (1-\epsilon)^{v-\ell} \Big) \\ &\le\; 2 \Big((1+\epsilon)^{v} - (1-\epsilon)^{v} \Big) \end{aligned}$$

We also have $(1+\epsilon)^v = 1 + \sum_i \binom{v}{i} \epsilon^i \le 1 + \sum_i \epsilon^i v^i$. For $\epsilon v < 1/2$, we obtain that $(1+\epsilon)^v \le 1 + 2\epsilon v$. Similarly, we obtain that $(1-\epsilon)^v \geq 1 - 2\epsilon v$. Therefore, we have that $\mathbf{Adv}^{\text{h-so}}_{\mathsf{H},B,\mathcal{M},s}(k) \leq 8\epsilon v$. Then,

$$\begin{aligned}\mathbf{Adv}^{\text{h-so}}_{\mathsf{H},B,\mathcal{M}}(k) &= \sum_{s \in S} \Pr\left[K = s\right] \cdot \mathbf{Adv}^{\text{h-so}}_{\mathsf{H},B,\mathcal{M},s}(k) \\ &\quad + \sum_{s \in \overline{S}} \Pr\left[K = s\right] \cdot \mathbf{Adv}^{\text{h-so}}_{\mathsf{H},B,\mathcal{M},s}(k) \\ &\leq \max_{s \in S} \mathbf{Adv}^{\text{h-so}}_{\mathsf{H},B,\mathcal{M},s}(k) + 2v2^{-u} \ .\end{aligned}$$

Finally, by substituting $\epsilon = \sqrt[3]{2^{1-\mu}|\mathsf{HRng}(k)|^2}$, we obtain

$$\mathbf{Adv}^{\text{h-so}}_{\mathsf{H},B,\mathcal{M}}(k) \leq 16v\sqrt[3]{2^{1-\mu}|\mathsf{HRng}(k)|^{2d}} \ .$$

Using Theorem 3.1, we obtain for any unbounded adversary A

$$\mathbf{Adv}^{\text{h-so}}_{\mathsf{H},A,\mathcal{M}}(k) \leq 2592v\sqrt[3]{2^{1-\mu}|\mathsf{HRng}(k)|^{2d}} \ .$$

This completes the proof of Theorem 3.6.

▌

Proof of Lemma 3.7. We define $p_{\mathbf{x}} = \Pr\left[\mathbf{X} = \mathbf{x}\right]$, for any $\mathbf{x} = (x_1, \cdots, x_t)$, where $x_i \in \mathsf{HDom}(k)$. We consider the probability over the choice of key K. For every $\mathbf{x}$ and $\mathbf{y}$, we also define the following random variable

$$Z_{\mathbf{x},\mathbf{y}} = \begin{cases} p_{\mathbf{x}} & \text{if } \ H(K, \mathbf{x}) = \mathbf{y} \\ 0 & \text{otherwise} \end{cases}$$

Let $A_{\mathbf{x},\mathbf{y}} = Z_{\mathbf{x},\mathbf{y}}2^{\eta}$. Note that for all $i \in [t]$ and for every x_i, $H(K, x_i)$ is uniformly distributed, over the uniformly random choice of K. Moreover, H is t-wise independent. Therefore, we have $\mathbb{E}(Z_{\mathbf{x},\mathbf{y}}) = p_{\mathbf{x}}/|\mathsf{HRng}(k)|^t$, for every $\mathbf{x}, \mathbf{y}$. Let $Z_{\mathbf{y}} = \sum_{\mathbf{x}} Z_{\mathbf{x},\mathbf{y}}$ and $A_{\mathbf{y}} = \sum_{\mathbf{x}} A_{\mathbf{x},\mathbf{y}}$. Then, we have $\mathbb{E}(Z_{\mathbf{y}}) = 1/|\mathsf{HRng}(k)|^t$ and $\mathbb{E}(A_{\mathbf{y}}) = 2^{\eta}/|\mathsf{HRng}(k)|^t$. Moreover, for every $\mathbf{x}, \mathbf{y}$, we know $A_{\mathbf{x},\mathbf{y}} \in [0, 1]$ and for every $\mathbf{y}$, the variables $A_{\mathbf{x},\mathbf{y}}$ are pair-wise independent. Applying Claim 3.5, we obtain that for every $\mathbf{y}$ and $\delta > 0$

$$\Pr\left[\left|A_{\mathbf{y}} - \frac{2^{\eta}}{|\mathsf{HRng}(k)|^t}\right| \geq \frac{\delta 2^{\eta}}{|\mathsf{HRng}(k)|^t}\right] \leq \frac{|\mathsf{HRng}(k)|^t}{\delta^2 2^{\eta}} \ .$$

Substituting $Z_{\mathbf{y}}$ for $A_{\mathbf{y}}$ and choosing $\delta = \epsilon$, we obtain that for every $\epsilon > 0$,

$$\Pr\left[\left|A_{\mathbf{y}} - \frac{2^{\eta}}{|\mathsf{HRng}(k)|^t}\right| \geq \frac{\epsilon 2^{\eta}}{|\mathsf{HRng}(k)|^t}\right] \leq \frac{|\mathsf{HRng}(k)|^t}{\epsilon^2 2^{\eta}} \ .$$

Using union bound, we obtain that with probability $|\mathsf{HRng}(k)|^{2t}/\epsilon^2 2^{\eta} = 2^{-w}$ over the choice of K that $|Z_{\mathbf{y}} - |\mathsf{HRng}(k)|^{-t}| \geq \epsilon|\mathsf{HRng}(k)|^{-t}$, for all $\mathbf{y}$. Thus,

$$\left|\Pr\left[H(K, \mathbf{X}) = \mathbf{y}\right] - |\mathsf{HRng}(k)|^{-t}\right| \geq \epsilon|\mathsf{HRng}(k)|^{-t} \ .$$

with probability at most 2^{-w} over the choice of K. This completes the proof of Lemma 3.7. □

4 Selective Opening Security for Deterministic Encryption

In this section, we give two different constructions of deterministic public key encryption and show that they achieve D-SO-CPA security. First, we show that lossy trapdoor functions that are $2t$-wise independent in the lossy mode are selective opening secure for t-correlated messages. However, it is an open problem to construct them for $t > 1$.

```
Game $G_0(k)$
    $b \leftarrow\$ \{0,1\}$ ; $param \leftarrow\$ A.\mathrm{pg}(1^k)$
    $\mathbf{m}_1 \leftarrow\$ \mathcal{M}(1^k, param)$
    $(ek, td) \leftarrow\$ \mathsf{IKg}(1^k)$
    $\mathbf{c} \leftarrow \mathsf{Eval}(ek, \mathbf{m}_1)$
    $(state, I) \leftarrow\$ A.\mathrm{cor}(ek, \mathbf{c}, param)$
    $\mathbf{m}_0 \leftarrow\$ \mathsf{Rsmp}(1^k, \mathbf{m}_1[I], I, param)$
    $\omega \leftarrow\$ A.\mathrm{g}(state, \mathbf{m}_1[I], param)$
    $t \leftarrow\$ A.\mathrm{f}(\mathbf{m}_b, param)$
    If $(t = \omega)$ then return $b$
    Else return $(1 - b)$
```

```
Game $G_1(k)$
    $b \leftarrow\$ \{0,1\}$ ; $param \leftarrow\$ A.\mathrm{pg}(1^k)$
    $\mathbf{m}_1 \leftarrow\$ \mathcal{M}(1^k, param)$
    $lk \leftarrow\$ \mathsf{LKg}(1^k)$
    $\mathbf{c} \leftarrow \mathsf{Eval}(lk, \mathbf{m}_1)$
    $(state, I) \leftarrow\$ A.\mathrm{cor}(lk, \mathbf{c}, param)$
    $\mathbf{m}_0 \leftarrow\$ \mathsf{Rsmp}(1^k, \mathbf{m}_1[I], I, param)$
    $\omega \leftarrow\$ A.\mathrm{g}(state, \mathbf{m}_1[I], param)$
    $t \leftarrow\$ A.\mathrm{f}(\mathbf{m}_b, param)$
    If $(t = \omega)$ then return $b$
    Else return $(1 - b)$
```

Figure 3: **Games G_0, G_1 of the proof of Theorem 4.1.**

Hence, we give another construction of deterministic public key encryption using hash functions and lossy trapdoor permutation and show it is selective opening secure. A close variant of this scheme is shown to be D-SO-CPA secure in the NPROM [19]. Our scheme is efficient and only public-key primitive that it uses is a regular lossy trapdoor function, which has practical instantiations, e.g., both Rabin and RSA are regular lossy.

4.1 Achieving D-SO-CPA Security

We start by showing that $2t$-wise independent lossy trapdoor functions are selective opening secure. It was previously shown by Hoang *et al.* [19] that D-SO-CPA notion is achievable under the random oracle model. They leave it open to construct a D-SO-CPA secure scheme in the standard model. Here, we show that that a pair-wise independent lossy trapdoor function is D-SO-CPA secure for independent messages. We also show that that a $2d$-wise independent lossy trapdoor function is D-SO-CPA secure for (μ, d)-correlated message samplers.

First, we show in Theorem 4.1 that a pair-wise independent lossy trapdoor functions is D-SO-CPA secure for $(\mu, 0)$-correlated message samplers.

Theorem 4.1 Let $\mathcal{M}$ be a $(\mu, 0)$-correlated, efficiently resamplable message sampler. Let LT be a lossy trapdoor function with domain LDom, range LRng and lossiness τ. Suppose LT is pair-wise independent. Then for any adversary A,

$$\mathbf{Adv}^{\text{d-so-cpa}}_{\mathsf{LT},A,\mathcal{M}}(k) \le 2 \cdot \mathbf{Adv}^{\text{ltdf}}_{\mathsf{LT},B}(k) + 2592v \sqrt[3]{2^{1-\mu-2\tau}|\mathsf{LRng}(k)|^2} \ .$$

Proof: Consider games G_0, G_1 in Figure 3. Then

$$\mathbf{Adv}^{\text{d-so-cpa}}_{\mathsf{LT},A,\mathcal{M}}(k) = 2 \cdot \Pr\left[\, G_0(k) \Rightarrow 1 \,\right] - 1 \ .$$

We now explain the game chain. Game G_1 is identical to game G_0, except that instead of generating an injective key for the lossy trapdoor function, we generate a lossy one. Consider the following adversary B attacking the key indistinguishability of LT. It simulates game G_0, but uses its given key instead of generating a new one. It outputs 1 if the simulated game returns 1, and outputs 0 otherwise. Then

$$\Pr[G_0(k) \Rightarrow 1] - \Pr[G_1(k) \Rightarrow 1] \le \mathbf{Adv}^{\text{ltdf}}_{\mathsf{LT},B}(k) \ .$$

Note that game G_1 is identical to games H-SO-REAL or H-SO-IDEAL, when $b = 1$ or $b = 0$, respectively. Then

$$\mathbf{Adv}^{\text{h-so}}_{\mathsf{LT},A,\mathcal{M}}(k) = 2 \cdot \Pr\left[\, G_1(k) \Rightarrow 1 \,\right] - 1 \ .$$

Note that LT is pair-wise independent and τ-lossy. Then, size of the range of LT in the lossy mode is at most $2^{-\tau}|\mathsf{LRng}(k)|$. From Theorem 3.3

$$\mathbf{Adv}^{\text{h-so}}_{\mathsf{LT},A,\mathcal{M}}(k) \le 2592v \sqrt[3]{2^{1-\mu-2\tau}|\mathsf{LRng}(k)|^2} \ .$$

Summing up,

$$\mathbf{Adv}^{\text{d-so-cpa}}_{\mathsf{LT},A,\mathcal{M}}(k) \le 2 \cdot \mathbf{Adv}^{\text{ltdf}}_{\mathsf{LT},B}(k) + 2592v \sqrt[3]{2^{1-\mu-2\tau}|\mathsf{LRng}(k)|^2} \ .$$

```
$\underline{\mathsf{DE.Kg}(1^k)}$
$(ek, td) \leftarrow\!\!\$\ \mathsf{IKg}(1^k)$
$K_H \leftarrow\!\!\$\ \mathsf{HKg}(1^k)$
$K_G \leftarrow\!\!\$\ \mathsf{GKg}(1^k)$
$pk \leftarrow (K_H, K_G, ek)$
$sk \leftarrow (K_H, K_G, td)$
Return $(pk, sk)$
```

```
$\underline{\mathsf{DE.Enc}(pk, m)}$
$(K_H, K_G, ek) \leftarrow pk$
$r \leftarrow \mathsf{h}(K_H, m)$
$y \leftarrow \mathsf{g}(K_G, r) \oplus m$
$c \leftarrow \mathsf{Eval}(ek, y||r)$
Return $c$
```

```
$\underline{\mathsf{DE.Dec}(sk, c)}$
$(K_H, K_G, td) \leftarrow sk$
$y||r \leftarrow \mathsf{Inv}(td, c)$
$m \leftarrow \mathsf{g}(K_G, r) \oplus y$
Return $m$
```

Figure 4: **D-PKE scheme** $\mathsf{DE}[\mathsf{H}, \mathsf{G}, \mathsf{LT}]$**.**

This completes the proof of Theorem 4.1. ▌

Next, we show in Theorem 4.2 that a $2d$-wise independent lossy trapdoor functions is D-SO-CPA secure for (μ, d)-correlated message samplers.

Theorem 4.2 Let $\mathcal{M}$ be a (μ, d)-correlated, efficiently resamplable message sampler. Let LT be a lossy trapdoor function with domain LDom, range LRng and lossiness τ. Suppose LT is $2d$-wise independent. Then for any adversary A,

$$\mathbf{Adv}^{\text{d-so-cpa}}_{\mathsf{LT},A,\mathcal{M}}(k) \le 2 \cdot \mathbf{Adv}^{\text{ltdf}}_{\mathsf{LT},B}(k) + 2592v\sqrt[3]{2^{1-\mu-2d\tau}|\mathsf{LRng}(k)|^{2d}} \ .$$

The proof of Theorem 4.2 is very similar to the proof of Theorem 4.1.

Although that $2t$-wise independent trapdoor functions are very efficient and secure against selective opening attack, it is an open problem to construct them for $t > 1$. Hence, we give a new construction of deterministic public key encryption that is selective opening secure. Our scheme $\mathsf{DE}[\mathsf{H}, \mathsf{G}, \mathsf{LT}]$ is shown in Figure 4, where LT is a lossy trapdoor function and H, G are hash functions. We begin by showing in Theorem 4.3 that DE is D-SO-CPA secure for independent messages when H, G are pair-wise independent hash functions and LT is a regular lossy trapdoor function.

Theorem 4.3 Let $\mathcal{M}$ be a $(\mu, 0)$-correlated, efficiently resamplable message sampler. Let $\mathsf{H} = (\mathsf{HKg}, \mathsf{h})$ with domain $\{0,1\}^n$ and range $\{0,1\}^\ell$ and $\mathsf{G} = (\mathsf{GKg}, \mathsf{g})$ with domain $\{0,1\}^\ell$ and range $\{0,1\}^n$ be hash function families. Suppose H and G are pair-wise independent. Let LT be a regular lossy trapdoor function with domain $\{0,1\}^{n+\ell}$, range $\{0,1\}^p$ and lossiness τ. Let $\mathsf{DE}[\mathsf{H}, \mathsf{G}, \mathsf{LT}]$ be as above. Then for any adversary A,

$$\mathbf{Adv}^{\text{d-so-cpa}}_{\mathsf{DE},A,\mathcal{M}}(k) \le 2 \cdot \mathbf{Adv}^{\text{ltdf}}_{\mathsf{LT},B}(k) + 2592v\sqrt[3]{2^{1-\mu-2\tau+2p}} \ .$$

Proof: We begin by showing the following lemma.

Lemma 4.4 Let $\mathsf{H} = (\mathsf{HKg}, \mathsf{h})$ with domain $\{0,1\}^n$ and range $\{0,1\}^\ell$ and $\mathsf{G} = (\mathsf{GKg}, \mathsf{g})$ with domain $\{0,1\}^\ell$ and range $\{0,1\}^n$ be hash function families. Suppose H and G are pair-wise independent. Let LT be a regular lossy trapdoor function with domain $\{0,1\}^{n+\ell}$, range $\{0,1\}^p$ and lossiness τ. Let X be a random variable over $\{0,1\}^n$ such that $\mathrm{H}_\infty(X) \ge \eta$. Then, for all $lk \in [\mathsf{LKg}(1^k)]$, all $c \in \mathsf{Img}(lk)$ and any $\epsilon > 0$,

$$\Big|\Pr\left[\,\mathsf{DE.Enc}(pk, X) = c\,\right] - 2^{\tau-p}\Big| \ge \epsilon 2^{\tau-p} \ .$$

for at most 2^{-u} fraction of public key pk, where $u = \eta + 2\tau - 2p - 2\log(1/\epsilon)$.

Proof of Lemma 4.4. We define $p_x = \Pr\left[\,X = x\,\right]$, for any $x \in \{0,1\}^n$. We consider the probability over the choice of public key pk. fix the lossy key $lk \in [\mathsf{LKg}(1^k)]$, we consider the probability over the choice of K_H, K_G. For every $x \in \{0,1\}^n$ and $c \in \mathsf{Img}(lk)$, we also define the following random variable

$$Z_{x,c} = \begin{cases} p_x & \text{if } \ \mathsf{DE.Enc}(pk, x) = c \\ 0 & \text{otherwise} \end{cases}$$

Let $A_{x,c} = Z_{x,c}2^\eta$. Note that that for every x, $\mathsf{h}(K_H, x)$ is uniformly distributed, over the uniformly random choice of K_H. Moreover, for every x and K_H, $\mathsf{g}(K_G, \mathsf{h}(K_H, x))$ is uniformly distributed, over the uniformly random choice of K_G. Since LT is a regular LTDF, we have $\mathbb{E}(Z_{x,c}) = p_x \cdot 2^{\tau-p}$, for every x, c. Let $Z_c = \sum_x Z_{x,c}$

```
Game $G_0(k)$
    $b \leftarrow_\$ \{0,1\}$ ; $param \leftarrow_\$ A.\mathrm{pg}(1^k)$
    $\mathbf{m}_1 \leftarrow_\$ \mathcal{M}(1^k, param)$
    $(ek, td) \leftarrow_\$ \mathsf{IKg}(1^k)$ ; $K_H \leftarrow_\$ \mathsf{HKg}(1^k)$
    $K_G \leftarrow_\$ \mathsf{GKg}(1^k)$ ; $pk \leftarrow (K_H, K_G, ek)$
    $\mathbf{c} \leftarrow \mathsf{DE.Enc}(pk, \mathbf{m}_1)$
    $(state, I) \leftarrow_\$ A.\mathrm{cor}(pk, \mathbf{c}, param)$
    $\mathbf{m}_0 \leftarrow_\$ \mathsf{Rsmp}(1^k, \mathbf{m}_1[I], I, param)$
    $\omega \leftarrow_\$ A.\mathrm{g}(state, \mathbf{m}_1[I], param)$
    $t \leftarrow_\$ A.\mathrm{f}(\mathbf{m}_b, param)$
    If $(t = \omega)$ then return $b$
    Else return $(1 - b)$
```

```
Game $G_1(k)$
    $b \leftarrow_\$ \{0,1\}$ ; $param \leftarrow_\$ A.\mathrm{pg}(1^k)$
    $\mathbf{m}_1 \leftarrow_\$ \mathcal{M}(1^k, param)$
    $lk \leftarrow_\$ \mathsf{LKg}(1^k)$ ; $K_H \leftarrow_\$ \mathsf{HKg}(1^k)$
    $K_G \leftarrow_\$ \mathsf{GKg}(1^k)$ ; $pk \leftarrow (K_H, K_G, lk)$
    $\mathbf{c} \leftarrow \mathsf{DE.Enc}(pk, \mathbf{m}_1)$
    $(state, I) \leftarrow_\$ A.\mathrm{cor}(pk, \mathbf{c}, param)$
    $\mathbf{m}_0 \leftarrow_\$ \mathsf{Rsmp}(1^k, \mathbf{m}_1[I], I, param)$
    $\omega \leftarrow_\$ A.\mathrm{g}(state, \mathbf{m}_1[I], param)$
    $t \leftarrow_\$ A.\mathrm{f}(\mathbf{m}_b, param)$
    If $(t = \omega)$ then return $b$
    Else return $(1 - b)$
```

Figure 5: **Games G_0, G_1 of the proof of Theorem 4.3.**

and $A_c = \sum_x A_{x,c}$. Then, we have $\mathbb{E}(Z_c) = 2^{\tau - p}$ and $\mathbb{E}(A_c) = 2^{\eta+\tau-p}$. Moreover, for every x, c, we know $A_{x,c} \in [0,1]$ and for every c, the variables $A_{x,c}$ are pair-wise independent. Applying Claim 3.5, we obtain that for every c and $\delta > 0$

$$\Pr\left[\, \left|A_c - 2^{\eta+\tau-p}\right| \geq \delta \cdot 2^{\eta+\tau-p} \,\right] \leq \frac{2^{p-\eta-\tau}}{\delta^2} \ .$$

Substituting Z_c for A_c and choosing $\delta = \epsilon$, we obtain that for every $\epsilon > 0$,

$$\Pr\left[\, \left|Z_c - 2^{\tau-p}\right| \geq \epsilon \cdot 2^{\tau-p} \,\right] \leq \frac{2^{p-\eta-\tau}}{\epsilon^2} \ .$$

Using union bound, we obtain that $|Z_c - 2^{\tau-p}| \geq \epsilon \cdot 2^{\tau-p}$ with probability $2^{2p-\eta-2\tau}/\epsilon^2 = 2^{-u}$ over the choice of K_H, K_G, for all $lk \in [\mathsf{LKg}(1^k)]$, all $c \in \mathsf{Img}(lk)$. This completes the proof of Lemma 4.4. □

Consider games G_0, G_1 in Figure 5. Then

$$\mathbf{Adv}^{\text{d-so-cpa}}_{\mathsf{DE},A,\mathcal{M}}(k) = 2 \cdot \Pr\left[\, G_0(k) \Rightarrow 1 \,\right] - 1 \ .$$

We now explain the game chain. Game G_1 is identical to game G_0, except that instead of generating an injective key for the lossy trapdoor function, we generate a lossy one. Consider the following adversary B attacking the key indistinguishability of LT. It simulates game G_0, but uses its given key instead of generating a new one. It outputs 1 if the simulated game returns 1, and outputs 0 otherwise. Then

$$\Pr[G_0(k) \Rightarrow 1] - \Pr[G_1(k) \Rightarrow 1] \leq \mathbf{Adv}^{\text{ltdf}}_{\mathsf{LT},B}(k) \ .$$

Similar to proof of Theorem 3.3, using Lemma 4.4, we obtain that

$$\Pr\left[\, G_1(k) \Rightarrow 1 \,\right] \leq 1296v\sqrt[3]{2^{1-\mu-2\tau+2p}} + \frac{1}{2} \ .$$

Summing up,

$$\mathbf{Adv}^{\text{d-so-cpa}}_{\mathsf{DE},A,\mathcal{M}}(k) \leq 2 \cdot \mathbf{Adv}^{\text{ltdf}}_{\mathsf{LT},B}(k) + 2592v\sqrt[3]{2^{1-\mu-2\tau+2p}} \ .$$

This completes the proof of Theorem 4.3. ▌

We now extend our result to include correlated messages. We show that it is enough to use $2t$-wise independent hash functions to extend the security to t-correlated messages. Let $\mathsf{DE}[\mathsf{H}, \mathsf{G}, \mathsf{LT}]$ be PKE scheme shown in Figure 4, where LT is a lossy trapdoor function and H, G are hash functions. We show in Theorem 4.5 that DE is D-SO-CPA secure for t-correlated messages when H, G are $2t$-wise independent hash functions and LT is a regular lossy trapdoor function.

Theorem 4.5 Let $\mathcal{M}$ be a (μ, d)-correlated, efficiently resamplable message sampler. Let $\mathsf{H} = (\mathsf{HKg}, \mathsf{h})$ with domain $\{0,1\}^n$ and range $\{0,1\}^\ell$ and $\mathsf{G} = (\mathsf{GKg}, \mathsf{g})$ with domain $\{0,1\}^\ell$ and range $\{0,1\}^n$ be hash function

```
Game ONE-MORE-INV$^A_{\mathsf{TDF}}(k)$
    $j \leftarrow 0$ ; $(ek, td) \leftarrow\$ \mathsf{Kg}(1^k)$
    For $i = 1$ to $v$ do
        $\mathbf{x}[i] \leftarrow\$ \mathsf{TDom}(k)$
        $\mathbf{y}[i] \leftarrow \mathsf{Eval}(ek, \mathbf{x}[i])$
    $\mathbf{x}' \leftarrow\$ A^{\mathcal{C}}(ek, \mathbf{y})$
    Return $(\mathbf{x} = \mathbf{x}')$

Oracle $\mathcal{C}(i)$
    $j \leftarrow j + 1$
    If $j \geq v$ then
        Return $\perp$
    Return $\mathbf{x}[i]$
```

Figure 6: **Games to define the One-More security.**

families. Suppose H and G are $2d$-wise independent. Let LT be a regular lossy trapdoor function with domain $\{0,1\}^{n+\ell}$, range $\{0,1\}^p$ and lossiness τ. Let $\mathsf{DE}[\mathsf{H},\mathsf{G},\mathsf{LT}]$ be as above. Then for any adversary A,

$$\mathbf{Adv}^{\text{d-so-cpa}}_{\mathsf{DE},A,\mathcal{M}}(k) \leq 2 \cdot \mathbf{Adv}^{\text{ltdf}}_{\mathsf{LT},B}(k) + 2592v\sqrt[3]{2^{1-\mu+2d(-\tau+p)}} \ .$$

The proof of Theorem 4.5 is very similar to the proof of Theorem 4.3.

5 The One-More-RSA Inversion Problem

In this section, we recall the definition of one-more-RSA inversion problem. This problem is a natural extensions of the RSA-inversion problem underlying the notion of one-wayness to a setting where the adversary has access to a corruption oracle. Bellare *et al.* [4] first introduce this notion and show that assuming hardness of one-more-RSA inversion problem leads to a proof of security of Chaum's blind signature scheme in the random oracle model. Here we show that one-more inversion problem is hard for RSA with a large enough encryption exponent e. In particular, we show that one-more inversion problem is hard for any regular lossy trapdoor function.

5.1 Security Notion

Here we give a formal definition of one-more-RSA inversion problem. Our definition is more general and consider this problem for any trapdoor function. Intuitively, in the one-more inversion problem, the adversary gets a number of image points, and must output the inverses of all image points, while it has access to the corruption oracle and can see the preimage of image points of its choice. We note that the number of corruption queries is less than the number of image points.

Note that the special case of the one-more inversion problem in which there is only one image point is exactly the problem underlying the notion of one-wayness.

One-more inversion problem. Let $\mathsf{TDF} = (\mathsf{Kg}, \mathsf{Eval}, \mathsf{Inv})$ be a trapdoor function with domain $\mathsf{TDom}(\cdot)$ and range $\mathsf{TRng}(\cdot)$. To an adversary A, we associate the experiment in Figure 6 for every $k \in \mathbb{N}$. We say that TDF is one-more$[v]$ secure for a class $\mathscr{A}$ of adversaries if for every any $A \in \mathscr{A}$,

$$\mathbf{Adv}^{\text{one-more}}_{\mathsf{TDF},A,v}(k) = \Pr\left[\text{ONE-MORE-INV}^{A,v}_{\mathsf{TDF}}(k) \Rightarrow 1\right]$$

is negligible in k.

5.2 Achieving One-More Security

We show in Theorem 5.1 that a regular lossy trapdoor function is one-more secure. We point out that, for large enough encryption exponent e, RSA is a regular lossy trapdoor function.

Theorem 5.1 Let LT be a regular lossy trapdoor function with domain LDom, range LRng and lossiness τ. Then for any adversary A and any $v \in \mathbb{N}$,

$$\mathbf{Adv}^{\text{one-more}}_{\mathsf{LT},A,v}(k) \leq \mathbf{Adv}^{\text{ltdf}}_{\mathsf{LT},B}(k) + 2^{-\tau} \ .$$

Proof: Consider games G_1–G_3 in Figure 7. Then

$$\mathbf{Adv}^{\text{one-more}}_{\mathsf{LT},A,v}(k) = \Pr\left[\,G_0(k) \Rightarrow 1\,\right] \ .$$

```
Game $G_0(k)$
    $j \leftarrow 0$
    $(ek, td) \stackrel{\$}{\leftarrow} \mathsf{IKg}(1^k)$
    For $i = 1$ to $v$ do
      $\mathbf{x}[i] \stackrel{\$}{\leftarrow} \mathsf{LDom}(k)$
      $\mathbf{y}[i] \leftarrow \mathsf{Eval}(ek, \mathbf{x}[i])$
    $\mathbf{x}' \stackrel{\$}{\leftarrow} A^{\mathcal{C}}(ek, \mathbf{y})$
    Return $(\mathbf{x} = \mathbf{x}')$
```

```
Game $G_1(k)$
    $j \leftarrow 0$
    $lk \stackrel{\$}{\leftarrow} \mathsf{LKg}(1^k)$
    For $i = 1$ to $v$ do
      $\mathbf{x}[i] \stackrel{\$}{\leftarrow} \mathsf{LDom}(k)$
      $\mathbf{y}[i] \leftarrow \mathsf{Eval}(lk, \mathbf{x}[i])$
    $\mathbf{x}' \stackrel{\$}{\leftarrow} A^{\mathcal{C}}(lk, \mathbf{y})$
    Return $(\mathbf{x} = \mathbf{x}')$
```

```
Oracle $\mathcal{C}(i)$ // $G_0$–$G_2$
    $j \leftarrow j + 1$
    If $j \geq v$ then
      Return $\bot$
    Return $\mathbf{x}[i]$
```

```
Game $G_2(k)$
    $j \leftarrow 0$
    $lk \stackrel{\$}{\leftarrow} \mathsf{LKg}(1^k)$
    For $i = 1$ to $v$ do
      $\mathbf{y}[i] \stackrel{\$}{\leftarrow} \mathsf{Img}(lk)$
      $\mathbf{x}[i] \stackrel{\$}{\leftarrow} \mathsf{P}(lk, y)$
    $\mathbf{x}' \stackrel{\$}{\leftarrow} A^{\mathcal{C}}(lk, \mathbf{y})$
    Return $(\mathbf{x} = \mathbf{x}')$
```

```
Game $G_3(k)$
    $j \leftarrow 0$ ; $I \leftarrow \bot$
    $lk \stackrel{\$}{\leftarrow} \mathsf{LKg}(1^k)$
    For $i = 1$ to $v$ do
      $\mathbf{y}[i] \stackrel{\$}{\leftarrow} \mathsf{Img}(lk)$
    $\mathbf{x}' \stackrel{\$}{\leftarrow} A^{\mathcal{C}}(lk, \mathbf{y})$
    For $i \notin I$ do
      $\mathbf{x}[i] \stackrel{\$}{\leftarrow} \mathsf{P}(lk, y)$
    Return $(\mathbf{x} = \mathbf{x}')$
```

```
Oracle $\mathcal{C}(i)$ // $G_3$
    $j \leftarrow j + 1$
    $I \leftarrow I \cup \{i\}$
    If $j \geq v$ then
      Return $\bot$
    $\mathbf{x}[i] \stackrel{\$}{\leftarrow} \mathsf{P}(lk, y)$
    Return $\mathbf{x}[i]$
```

Figure 7: **Games G_2, G_3 of the proof of Theorem 5.1.**

We now explain the game chain. Game G_1 is identical to game G_0, except that instead of generating an injective key for the lossy trapdoor function, we generate a lossy one. Consider the following adversary B attacking the key indistinguishability of LT. It simulates game G_0, but uses its given key instead of generating a new one. It outputs 1 if the simulated game returns 1, and outputs 0 otherwise. Then

$$\Pr[G_0(k) \Rightarrow 1] - \Pr[G_1(k) \Rightarrow 1] \leq \mathbf{Adv}^{\mathrm{ltdf}}_{\mathsf{LT},B}(k) \ .$$

Let $\mathsf{P}(lk, y) = \{x \mid \mathsf{Eval}(lk, x) = y\}$. In game G_2, we reorder the code of game G_1 producing vector $\mathbf{y}$. Note that LT is a regular lossy trapdoor function. Then, distribution of vector $\mathbf{y}$ is uniformly random on $\mathsf{Img}(lk)$ in game G_1. Thus, vectors $\mathbf{x}$ and $\mathbf{y}$ have the same distribution in game G_1 and G_2. Hence, the change is conservative, meaning that $\Pr[G_1(k) \Rightarrow 1] = \Pr[G_2(k) \Rightarrow 1]$. Moreover, game G_3 is identical to game G_2. Thus, we have $\Pr[G_2(k) \Rightarrow 1] = \Pr[G_3(k) \Rightarrow 1]$.

Let $\mathbf{y}[\overline{I}]$ be the unopened images, where $|\overline{I}| \geq 1$. Note that in game G_3, for all $i \in \overline{I}$, $\mathbf{x}[i]$ is chosen uniformly at random after adversary A outputs $\mathbf{x}'$. Therefore, we obtain $\Pr[G_3(k) \Rightarrow 1] \leq 2^{-\tau}$. Summing up,

$$\mathbf{Adv}^{\text{one-more}}_{\mathsf{LT},A,v}(k) \leq \mathbf{Adv}^{\mathrm{ltdf}}_{\mathsf{LT},B}(k) + 2^{-\tau} \ .$$

This completes the proof of Theorem 5.1. ▌

Acknowledgments

We thank Jonathan Katz for insightful conversations.

References

[1] M. Bellare, R. Dowsley, and S. Keelveedhi. How secure is deterministic encryption? In *Public-Key Cryptography — PKC 2015*, volume 9020 of *LNCS*, pages 52–73. Springer, Heidelberg, Germany, 2015. (Cited on page 3, 6.)

[2] M. Bellare, R. Dowsley, B. Waters, and S. Yilek. Standard security does not imply security against selective-opening. In D. Pointcheval and T. Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 645–662, Cambridge, UK, Apr. 15–19, 2012. Springer, Heidelberg, Germany. (Cited on page 3.)

[3] 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, Cologne, Germany, Apr. 26–30, 2009. Springer, Heidelberg, Germany. (Cited on page 3, 7.)

[4] M. Bellare, C. Namprempre, D. Pointcheval, and M. Semanko. The one-more-RSA-inversion problems and the security of Chaum's blind signature scheme. *Journal of Cryptology*, 16(3):185–215, June 2003. (Cited on page 3, 4, 16.)

[5] M. Bellare and P. Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In V. Ashby, editor, *ACM CCS 93*, pages 62–73, Fairfax, Virginia, USA, Nov. 3–5, 1993. ACM Press. (Cited on page 3.)

[6] R. Bendlin, J. B. Nielsen, P. S. Nordholt, and C. Orlandi. Lower and upper bounds for deniable public-key encryption. In D. H. Lee and X. Wang, editors, *ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 125–142, Seoul, South Korea, Dec. 4–8, 2011. Springer, Heidelberg, Germany. (Cited on page 3.)

[7] F. Böhl, D. Hofheinz, and D. Kraschewski. On definitions of selective opening security. In M. Fischlin, J. Buchmann, and M. Manulis, editors, *PKC 2012*, volume 7293 of *LNCS*, pages 522–539, Darmstadt, Germany, May 21–23, 2012. Springer, Heidelberg, Germany. (Cited on page 3.)

[8] 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, Santa Barbara, CA, USA, Aug. 17–21, 1997. Springer, Heidelberg, Germany. (Cited on page 4.)

[9] R. Canetti, C. Dwork, M. Naor, and R. Ostrovsky. Deniable encryption. In B. S. Kaliski Jr., editor, *CRYPTO'97*, volume 1294 of *LNCS*, pages 90–104, Santa Barbara, CA, USA, Aug. 17–21, 1997. Springer, Heidelberg, Germany. (Cited on page 3.)

[10] R. Canetti, U. Feige, O. Goldreich, and M. Naor. Adaptively secure multi-party computation. In *28th ACM STOC*, pages 639–648, Philadephia, PA, USA, May 22–24, 1996. ACM Press. (Cited on page 3.)

[11] R. Canetti, S. Halevi, and J. Katz. Adaptively-secure, non-interactive public-key encryption. In J. Kilian, editor, *TCC 2005*, volume 3378 of *LNCS*, pages 150–168, Cambridge, MA, USA, Feb. 10–12, 2005. Springer, Heidelberg, Germany. (Cited on page 3.)

[12] D. Chaum. Blind signatures for untraceable payments. In D. Chaum, R. L. Rivest, and A. T. Sherman, editors, *CRYPTO'82*, pages 199–203, Santa Barbara, CA, USA, 1982. Plenum Press, New York, USA. (Cited on page 4.)

[13] I. Damgård and J. B. Nielsen. Improved non-committing encryption schemes based on a general complexity assumption. In M. Bellare, editor, *CRYPTO 2000*, volume 1880 of *LNCS*, pages 432–450, Santa Barbara, CA, USA, Aug. 20–24, 2000. Springer, Heidelberg, Germany. (Cited on page 3.)

[14] Y. Dodis, L. Reyzin, and A. Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In C. Cachin and J. Camenisch, editors, *EUROCRYPT 2004*, volume 3027 of *LNCS*, pages 523–540, Interlaken, Switzerland, May 2–6, 2004. Springer, Heidelberg, Germany. (Cited on page 5.)

[15] C. Dwork, M. Naor, O. Reingold, and L. J. Stockmeyer. Magic functions. *J. ACM*, 50(6):852–921, 2003. (Cited on page 3.)

[16] 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, Taormina, Sicily, Italy, Mar. 19–21, 2012. Springer, Heidelberg, Germany. (Cited on page 19.)

[17] V. Goyal, A. O'Neill, and V. Rao. Correlated-input secure hash functions. In Y. Ishai, editor, *TCC 2011*, volume 6597 of *LNCS*, pages 182–200, Providence, RI, USA, Mar. 28–30, 2011. Springer, Heidelberg, Germany. (Cited on page 3.)

[18] F. Heuer, E. Kiltz, and K. Pietrzak. Standard security does imply security against selective opening for markov distributionss. Cryptology ePrint Archive, Report 2015/853, 2015. `http://eprint.iacr.org/2015/853`. (Cited on page 3.)

[19] V. T. Hoang, J. Katz, A. O'Neill, and M. Zaheri. Selective-opening security in the presence of randomness failures. In *Advances in Cryptology – ASIACRYPT 2016*, pages 278–306. Springer, 2016. (Cited on page 3, 4, 6, 13.)

[20] D. Hofheinz, V. Rao, and D. Wichs. Standard security does not imply indistinguishability under selective opening. Cryptology ePrint Archive, Report 2015/792, 2015. `http://eprint.iacr.org/2015/792`. (Cited on page 3.)

[21] D. Hofheinz and A. Rupp. Standard versus selective opening security: Separation and equivalence results. In Y. Lindell, editor, *TCC 2014*, volume 8349 of *LNCS*, pages 591–615, San Diego, CA, USA, Feb. 24–26, 2014. Springer, Heidelberg, Germany. (Cited on page 3.)

[22] 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, Santa Barbara, CA, USA, Aug. 15–19, 2010. Springer, Heidelberg, Germany. (Cited on page 4.)

[23] J. B. Nielsen. Separating random oracle proofs from complexity theoretic proofs: The non-committing encryption case. In M. Yung, editor, *CRYPTO 2002*, volume 2442 of *LNCS*, pages 111–126, Santa Barbara, CA, USA, Aug. 18–22, 2002. Springer, Heidelberg, Germany. (Cited on page 3.)

[24] J. B. Nielsen. A threshold pseudorandom function construction and its applications. In M. Yung, editor, *CRYPTO 2002*, volume 2442 of *LNCS*, pages 401–416, Santa Barbara, CA, USA, Aug. 18–22, 2002. Springer, Heidelberg, Germany. (Cited on page 3.)

```
Algorithm $B.\mathrm{pg}(1^k)$
$\mathit{param} \leftarrow_{\$} A.\mathrm{pg}(1^k)$
$r \leftarrow_{\$} \{0,1\}^{\mathsf{A.f.rl}(k)}$
$\mathit{pars} \leftarrow (r, \mathit{param})$
Return $\mathit{pars}$

Algorithm $B.\mathrm{cor}(k, \mathbf{h}, \mathit{pars})$
$(r, \mathit{param}) \leftarrow \mathit{pars}$
$(I, \mathit{st}) \leftarrow_{\$} A.\mathrm{cor}(k, \mathbf{h}, \mathit{param})$
Return $(I, \mathit{st})$

Algorithm $B.\mathrm{g}(\mathit{st}, \mathbf{m}[I], \mathit{pars})$
$(r, \mathit{param}) \leftarrow \mathit{pars}$
$\omega \leftarrow_{\$} A.\mathrm{g}(\mathit{st}, \mathbf{m}[I], \mathit{param})$
Return $\langle r, \omega \rangle$

Algorithm $B.\mathrm{f}(\mathbf{m}, \mathit{pars})$
$(r, \mathit{param}) \leftarrow \mathit{pars}$
$t \leftarrow_{\$} A.\mathrm{f}(\mathbf{m}, \mathit{param})$
Return $\langle r, t \rangle$
```

Figure 8: **H-SO adversary B in the proof of Claim A.1.**

[25] A. O'Neill, C. Peikert, and B. Waters. Bi-deniable public-key encryption. In P. Rogaway, editor, *CRYPTO 2011*, volume 6841 of *LNCS*, pages 525–542, Santa Barbara, CA, USA, Aug. 14–18, 2011. Springer, Heidelberg, Germany. (Cited on page 3.)

[26] O. Pandey, R. Pass, and V. Vaikuntanathan. Adaptive one-way functions and applications. In D. Wagner, editor, *CRYPTO 2008*, volume 5157 of *LNCS*, pages 57–74, Santa Barbara, CA, USA, Aug. 17–21, 2008. Springer, Heidelberg, Germany. (Cited on page 4.)

[27] C. Peikert and B. Waters. Lossy trapdoor functions and their applications. In R. E. Ladner and C. Dwork, editors, *40th ACM STOC*, pages 187–196, Victoria, British Columbia, Canada, May 17–20, 2008. ACM Press. (Cited on page 4, 5.)

[28] 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, New York, NY, USA, May 31 – June 3, 2014. ACM Press. (Cited on page 3.)

A Deferred Proofs

Proof of Theorem 3.1. The proof is similar to the proof of Theorem 3.1 from [16]. The proof of Theorem 3.1 follows from the following claims. We begin by showing that it is suffices to consider H-SO adversaries where the output of A.f is boolean.

Claim A.1 Let $\mathsf{H} = (\mathsf{HKg}, \mathsf{h})$ be a hash function family with domain HDom and range HRng. Let A be a H-SO adversary against H with respect to message sampler $\mathcal{M}$. Then, there is a boolean H-SO adversary B such that for all $k \in \mathbb{N}$

$$\mathbf{Adv}^{\text{h-so}}_{\mathsf{H},A,\mathcal{M}}(k) \leq 2 \cdot \mathbf{Adv}^{\text{h-so}}_{\mathsf{H},B,\mathcal{M}}(k) \ .$$

where the running time of B is about that of A.

Proof: Consider adversary B in Figure 8. We define E_A and E_B to be events where games H-SO-REAL$^{A,\mathcal{M}}_{\mathsf{H}}$ and H-SO-REAL$^{B,\mathcal{M}}_{\mathsf{H}}$ output 1, respectively. Hence,

$$\begin{aligned} \Pr[\,E_B\,] &= \Pr[\,E_A\,] + \frac{1}{2}(1 - \Pr[\,E_A\,]) \\ &= \frac{1}{2}\Pr[\,E_A\,] + \frac{1}{2} \ . \end{aligned}$$

We also define T_A and T_B to be the events where games H-SO-IDEAL$^{A,\mathcal{M}}_{\mathsf{H}}$ and H-SO-IDEAL$^{B,\mathcal{M}}_{\mathsf{H}}$ output 1, respectively. Similarly, we have $\Pr[\,T_B\,] = \Pr[\,T_A\,]/2 + 1/2$. Thus, we have $\mathbf{Adv}^{\text{h-so}}_{\mathsf{H},A,\mathcal{M}}(k) \leq 2 \cdot \mathbf{Adv}^{\text{h-so}}_{\mathsf{H},B,\mathcal{M}}(k)$. This completes the proof. ▌

Next, we claim that it is suffices to consider balanced H-SO adversaries meaning the probability the partial information is 1 or 0 is approximately 1/2.

Claim A.2 Let $\mathsf{H} = (\mathsf{HKg}, \mathsf{h})$ be a hash function family with domain HDom and range HRng. Let B be a boolean H-SO adversary against H with respect to the message sampler $\mathcal{M}$. Then for any $0 \leq \delta < 1/2$, there is a *δ-balanced* boolean H-SO adversary C such that for all $k \in \mathbb{N}$

$$\mathbf{Adv}^{\text{h-so}}_{\mathsf{H},B,\mathcal{M}}(k) \leq \left(\frac{2}{\delta} + 1\right)^2 \cdot \mathbf{Adv}^{\text{h-so}}_{\mathsf{H},C,\mathcal{M}}(k) \ .$$

```
**Algorithm** $C.\mathrm{pg}(1^k)$
$param \leftarrow\$\ B.\mathrm{pg}(1^k)$
Return $param$

**Algorithm** $C.\mathrm{f}(m, param)$
$t \leftarrow\$\ B.\mathrm{f}(m, param)$
$j \leftarrow\$\ \{1, \cdots 2(1/\delta) + 1\}$
If $j \leq 1/\delta$ then return 0
If $j \leq 2(1/\delta)$ return 1
Return $t$
```

```
**Algorithm** $C.\mathrm{cor}(k, \mathbf{h}, param)$
$(I, st) \leftarrow\$\ B.\mathrm{cor}(k, \mathbf{h}, param)$
Return $(I, st)$

**Algorithm** $C.\mathrm{g}(st, \mathbf{m}[I], param)$
$\omega \leftarrow\$\ B.\mathrm{g}(st, \mathbf{m}[I], param)$
$i \leftarrow\$\ \{1, \cdots 2(1/\delta) + 1\}$
If $i \leq 1/\delta$ then return 0
If $i \leq 2(1/\delta)$ return 1
Return $\omega$
```

Figure 9: **H-SO adversary C in the proof of Claim A.2.**

where the running time of C is about that of B plus $\mathcal{O}(1/\delta)$

Proof: For simplicity, we assume $1/\delta$ is an integer. Consider adversary C in Figure 9. Note that C is δ-*balanced*, since for all $b \in \{0, 1\}$

$$\left|\Pr\left[\, t = b \ : \ t \leftarrow\$\ C.\mathrm{f}(m, param) \,\right] - \frac{1}{2}\right| \leq \frac{1}{2/\delta + 1} \ .$$

We define E_B and E_C to be events where games H-SO-REAL$_{\mathsf{H}}^{B,\mathcal{M}}$ and H-SO-REAL$_{\mathsf{H}}^{C,\mathcal{M}}$ output 1, respectively. Let T be the event that $i, j = 2/\delta + 1$. Therefore we have

$$\begin{aligned} \Pr\left[\, E_C \,\right] &= \Pr\left[\, E_C \mid T \,\right] \cdot \Pr\left[\, T \,\right] + \Pr\left[\, E_C \mid \overline{T} \,\right] \cdot \Pr\left[\, \overline{T} \,\right] \\ &= \left(\frac{1}{2/\delta + 1}\right)^2 \Pr\left[\, E_B \,\right] + \frac{1}{2}\Pr\left[\, \overline{T} \,\right] \ . \end{aligned}$$

We also define T_B and T_C to be the events where games H-SO-IDEAL$_{\mathsf{H}}^{B,\mathcal{M}}$ and H-SO-IDEAL$_{\mathsf{H}}^{C,\mathcal{M}}$ output 1, respectively. Similarly, we have

$$\Pr\left[\, T_C \,\right] = \left(\frac{1}{2/\delta + 1}\right)^2 \Pr\left[\, T_B \,\right] + \frac{1}{2}\Pr\left[\, \overline{T} \,\right] \ .$$

Summing up, we obtain that $\mathbf{Adv}^{\text{h-so}}_{\mathsf{H},B,\mathcal{M}}(k) \leq \left(\frac{2}{\delta} + 1\right)^2 \cdot \mathbf{Adv}^{\text{h-so}}_{\mathsf{H},C,\mathcal{M}}(k)$. This completes the proof of Claim A.2. ■