Toward RSA-OAEP without Random Oracles

Nairen Cao[1], Adam O'Neill[2], and Mohammad Zaheri[3]

[1] Dept. of Computer Science, Georgetown University, USA
nc645@georgetown.edu
[2] College of Information and Computer Sciences, University of Massachusetts Amherst, USA
adamo@cs.umass.edu
[3] Dept. of Computer Science, Georgetown University, USA
mz394@georgetown.edu

Abstract. We show new partial and full instantiation results *under chosen-ciphertext security* for the widely implemented and standardized RSA-OAEP encryption scheme of Bellare and Rogaway (EUROCRYPT 1994) and two variants. Prior work on such instantiations either showed negative results or settled for "passive" security notions like IND-CPA. More precisely, recall that RSA-OAEP adds redundancy and randomness to a message before composing two rounds of an underlying Feistel transform, whose round functions are modeled as random oracles (ROs), with RSA. Our main results are:

- Either of the two oracles (while still modeling the other as a RO) can be instantiated in RSA-OAEP under IND-CCA2 using mild standard-model assumptions on the round functions and generalizations of algebraic properties of RSA shown by Barthe, Pointcheval, and Báguelin (CCS 2012). The algebraic properties are only shown to hold at practical parameters for small encryption exponent ($e = 3$), but we argue they have value for larger e as well.
- Both oracles can be instantiated simultaneously for two variants of RSA-OAEP, called "t-clear" and "s-clear" RSA-OAEP. For this we use extractability-style assumptions in the sense of Canetti and Dakdouk (TCC 2010) on the round functions, as well as novel yet plausible "XOR-type" assumptions on RSA. While admittedly strong, such assumptions may nevertheless be necessary at this point to make positive progress.

In particular, our full instantiations evade impossibility results of Shoup (J. Cryptology 2002), Kiltz and Pietrzak (EUROCRYPT 2009), and Bitansky *et al.* (STOC 2014). Moreover, our results for s-clear RSA-OAEP yield the most efficient RSA-based encryption scheme proven IND-CCA2 in the standard model (using bold assumptions on cryptographic hashing) to date.

1 Introduction

In this paper, we show new partial and full instantiations *under chosen-ciphertext attack* (CCA) for the RSA-OAEP encryption scheme [10] and some variants.

This helps explain why the scheme, which so far has only been shown to have such security in the random oracle (RO) model, has stood up to cryptanalysis despite the existence of "uninstantiable" RO model schemes and other negative results. It also leads to the fastest CCA-secure RSA-based public-key encryption scheme in the standard model (where one assumes standard-model properties of cryptographic hash functions) to date. We now discuss some background and motivation before an overview of our results.

1.1 Background and Motivation

In the random oracle (RO) model of Bellare and Rogaway [9], every algorithm has oracle access to the same truly random functions. This model has been enormously enabling in the design of practical protocols for various goals; examples include public-key encryption [9, 10, 43], digital signatures [9, 11], and identity-based encryption [21]. When a RO model scheme is implemented, one "instantiates" the oracles, that is, replaces their invocations with invocations of functions with publicly-available code. Thus, there are many possible "instantiations" of a protocol, depending on the choice of the latter. To obtain a practical instantiation, it was suggested by [9] to build these functions from cryptographic hashing in an appropriate way. We call this the *canonical instantiation.* The *RO model thesis* of [9] is that if a protocol is secure in the RO model then its canonical instantiation remains secure in the standard (RO devoid) sense.

Unfortunately, the RO model thesis has been refuted in a strong sense, starting with the work of Canetti *et al.* [28]. These works show that there exist RO model schemes for which *any* instantiation, let alone the canonical one, yields a scheme that can be broken efficiently in the standard model. However, the consensus of the community is that such schemes always seem contrived or artificial in some way. Indeed, RO model schemes that have been standardized have stood up to decades of cryptanalysis. If the RO model thesis is false, what explains this? This leads to what may be called the *practical RO model thesis:* For a "practical" scheme proven secure in the RO model scheme, its canonical instantiation remains secure in the standard model. However, from a scientific standpoint this thesis is unsatisfactory because it lacks a *definition* of "practical."[4] This shortcoming is the starting point for our work.

1.2 Our Thesis

Candidate differentiating properties. It seems problematic to try to define practicality in the above sense. Instead, we propose some candidate properties that we conjecture to differentiate schemes to which the RO model thesis applies from those to which it does not. Here are some such properties, some of which are inspired by our work described below:

[4] Here we do not mean "practical" in the sense of efficient enough to use in practice, but rather "does not do anything contrived."

1. There exist standard-model properties of the constituent functions that together suffice to prove security of the scheme, ideally as well as realizations of such functions under standard assumptions.
2. *Each* individual constituent function can be separately instantiated as above, while possibly modeling the others as ROs.
3. Variants of the scheme that fall under the same framework satisfy one of the above properties.
4. There exist constructions of standard-model hash functions that allow to prove security of the scheme when replacing the ROs, ideally these constructions being under standard assumptions.

The revised thesis. Our *revised RO model thesis* is that a scheme satisfying one of the above properties is such that the canonical instantiation yields a secure scheme in the standard model, where we relax the notion of instantiation to allow stronger assumptions on non-RO constituent functions. That is, "constituent functions" refers not only to those modeled as ROs but possibly other functions associated with the scheme, like RSA. Thus, one may search for novel assumptions on RSA, for example. Indeed, if one looks at the question of why some RSA-based RO scheme is secure in practice, it could very well have to do with properties of RSA (which has a lot of algebraic structure) beyond mere one-wayness. We have seen the same strategy used to explain security of schemes, without transitioning between the RO and standard models, for example with Chaum's blind signature scheme [7] and Damgård's ElGamal [33]. It was also advocated by Pandey *et al.* [54] to resolve some long-standing theoretical questions.

It is also worth mentioning that there are impossibility results in the standard model for RSA-OAEP [49] and RSA-FDH, RSA-PSS [36, 35]. However, these are *black-box* impossibility results that demonstrate that a proof treating the functions as black-boxes cannot suffice. As in other areas of cryptography [2] this motivates looking at non-blackbox assumptions.

1.3 Discussion of The Properties and Our Goals

Our focus: RSA-OAEP. We focus our study on whether the RO model thesis applies to a very influential scheme, namely *RSA-OAEP* [10]. Roughly, RSA-OAEP is defined as follows. RSA-OAEP encrypts a message as $f(s\|t)$ where f is the RSA function, where for functions $\mathcal{G}$ and $\mathcal{H}$ (originally modeled as ROs) we have $s = \mathcal{G}(r) \oplus m \| 0^\zeta$ for randomness $r \in \{0,1\}^\rho$ and message $m \in \{0,1\}^\mu$, $t = \mathcal{H}(s) \oplus r$. (We denote $s = s_1 \| s_2$.) Thus, we would like to examine whether RSA-OAEP satisfies the properties listed above.

The first property. Here we seek standard model properties of RSA, $\mathcal{G}$, and $\mathcal{H}$ that suffice to prove IND-CCA. For this property, we mentioned that ideally we would also have theoretical realizations of such functions under standard assumptions. We make it clear that we do not advocate *using* these theoretical realizations in practice, but they would show that the goal is not impossible to achieve. The importance of this is illustrated by the fact that the most general forms of assumptions such as correlation intractability (CI) [28] and universal computational extraction (UCE) [5, 23] have been shown (likely) impossible. (But special cases of CI and UCE which suffice for the schemes considered remain plausible [5, 23, 25].) Unfortunately, we do not know how to achieve the first property for RSA-OAEP, even without such theoretical realizations.

The second property. The second property asks for so-called "partial instantiations" for each one of $\mathcal{G}$ or $\mathcal{H}$, while still modeling the other as a RO. Partial instantiations are valuable because ROs are used in different ways in a scheme, and instantiating one of them isolates a property it relies on. Moreover, we ask that *every* oracle can be (separately) instantiated. This has provable implications in practice as well, as now an attacker would need to exploit weakness in the *interaction* between these functions in order to break the scheme in the standard model. In our eyes this makes a standard model attack much less plausible. We show that RSA-OAEP satisfies this property under suitable assumptions.

The third property. The third property is more subjective than the others, as it hinges on what constitutes a scheme falling under the same framework. The aim is to capture the scheme designers' intent or their general approach. Again, the idea is not to use the modified schemes in practice necessarily (although one certainly could if the efficiency penalty is acceptable), but to validate the framework more than simply proving the original scheme is secure in the RO model. An upshot is that this approach can indeed lead to variants of the scheme that offer better security with similar efficiency. We show the third property holds for RSA-OAEP, and in fact our results for one of our variants, namely s-clear RSA-OAEP, leads to the most efficient IND-CCA secure scheme in the standard model, albeit under bold assumptions on cryptographic hashing.

The fourth property. Note that this property differs from the first in that it does not require giving higher-level properties that the hash functions should satisfy in order to make the scheme secure. Thus, it does not really give insight into what properties hash functions used in the canonical instantiation should satisfy to do this. Still, existence of such hash functions refutes uninstantiability of the scheme, showing that the job of the hash functions in making the scheme secure is at least plausible. As with the first property, we leave it as an open problem to show this for RSA-OAEP. We note that this property has been shown for other RO model schemes in, *e.g*, [46, 61].

We proceed to describe our approach and results in more detail.

1.4 Using PA + IND-CPA

Using PA + IND-CPA. A common thread running through our analyses is the use of *plaintext awareness* (PA) [10, 4, 8]. PA captures the intuition that an adversary who produces a ciphertext must "know" the corresponding plaintext. It is not itself a notion of privacy, but, at a high level, combined with IND-CPA it implies IND-CCA. We use this approach to obtain modularity in proofs, isolate assumptions needed, and make overall analyses more tractable. Moreover, while it seems that PA necessitates using knowledge assumptions, this is somewhat inherent anyway due to black-box impossibility results discussed below.

Flavors and implications. PA comes in various flavors: PA-RO [4], and PA0, PA1, and PA2 [8]. PA-RO refers to a notion in the RO model, while PA0, PA1, and PA2 refer to standard model notions that differ in what extent the adversary can query its decryption or encryption oracles. (In particular, in PA2 the adversary can query for encryptions of unknown plaintexts.) Similarly, IND-CCA comes in flavors [56, 4]: IND-CCA0, IND-CCA1, and IND-CCA2. We use that [4, 8] show that IND-CPA + PA-RO implies IND-CCA2 in the RO model, IND-CPA + PA0 implies IND-CCA1 with one decryption query, IND-CPA + PA1 implies IND-CCA1, and IND-CPA + PA2 implies IND-CCA2.

1.5 Partial Instantiation Results

High-level approach. We first give partial instantiation results of RSA-OAEP under IND-CCA2. Such results have been sought after in prior work [24, 17, 18] but have proven negative results or settled for weaker security notions. The heroes for us here are new generalizations of the notions of "second-input extractability" (SIE) and "common-input extractability" (CIE) proven by Barthe *et al.* [3] to hold for small-exponent RSA ($e = 3$). SIE says that an RSA image point can be inverted given a sufficiently-long (depending on e) part of the preimage, whereas CIE says that two RSA images can be inverted if the preimages share a common part. They were used by [3] where the "part" is the least-significant bits to analyze a no-redundancy, one-round version of RSA-OAEP in the RO model. The assumptions are proven via Coppersmith's algorithm to find small roots of a univariate polynomial modulo N [30].

We show that generalized versions where the "part" refers to some of the middle or most-significant bits, rather than least-significant bits, is useful for analyzing RSA-OAEP more generally. We show these versions also hold for small-exponent RSA, but based on the *bivariate* Coppersmith algorithm [30, 15, 31]. Moreover, despite the similarity of assumptions, our proof strategies in the partial instantiations are somewhat different than that of Barthe *et al.* [3]. Another interesting point is that while (generalized) SIE and CIE hold for $e = 3$, we argue they have practical value for larger e as well. Namely, while $e > 3$ would require an impractical "part" length using Coppersmith's technique, they could possibly hold for practical parameters via other (in particular, non-blackbox) techniques. At least, we do not see how to refute that, which could lend insight into why there is no IND-CCA2 attack on the scheme for general e. [5]

[5] Moreover, we conjecture this is different from the case of "lossiness" [55, 48] as shown for RSA and used to analyze IND-CPA security of RSA-OAEP in [48]. Namely, to get sufficient lossiness it seems to inherently require large e, since the *only* way to make RSA parameters lossy is to have $e \mid \phi(N)$.

Results and intuition. Namely, we show partial instantiations of both oracles $\mathcal{G}, \mathcal{H}$ under very mild assumptions on the round functions — roughly, that $\mathcal{G}$ is a pseudorandom generator and $\mathcal{H}$ is a hardcore function for RSA, respectively — in both cases assuming RSA is SIE and CIE. We first prove IND-CPA security in these cases. Interestingly, the instantiation of $\mathcal{G}$ under IND-CPA uses that RSA is SIE while the instantiation of $\mathcal{H}$ does not, the intuition being that in the latter case we assume $\mathcal{H}$ is a hardcore function so its output masks $r \in \{0,1\}^\rho$ used in the challenge ciphertext unconditionally. Now for PA-RO, in both cases we use SIE and CIE, but wrt. different bits of the input. In the case of instantiating $\mathcal{G}$, it is wrt. the redundancy bits s_2. Intuitively, for a decryption query there are two cases. Firstly, that it has a *different* r-part than the challenge and therefore this must have been queried to the RO, in which case the SIE extractor works. Secondly, that it has the *same* r-part as the challenge, but it therefore shares s_2, in which case the CIE extractor works. In the case of instantiating $\mathcal{H}$, there are again two cases for an encryption query depending on whether it shares the same s-part of the challenge or not; thus the assumption is wrt. the whole s-part.

1.6 Full Instantiation Results

High-level approach. We next give full instantiation results for two variants of RSA-OAEP, called t-clear and s-clear RSA-OAEP. Prior results on t-clear RSA-OAEP [18] showed only partial instantiations or relatively weak security notions, and s-clear RSA-OAEP was only considered indirectly by Shoup [59] for negative results. In t-clear RSA-OAEP, a message is encrypted as $f(s_1)\|s_2\|t$ where f is the RSA function $s_1\|s_2 = \mathcal{G}(r)\oplus m\|0^\zeta$ for randomness $r \in \{0,1\}^\rho$ and message $m \in \{0,1\}^\mu$, $t = \mathcal{H}(s_1\|s_2)\oplus r$. Here we divide s into $s_1\|s_2$, where $s_2 \in \{0,1\}^\zeta$, so the name "t-clear" while consistent with prior work [18], is somewhat of a misnomer. On the other hand, in s-clear RSA OAEP a message is encrypted as $s\|f(t)$. One of the heroes for us here is a hierarchy of "extractability" notions we define and assume for the round functions, called EXT-RO, EXT0, EXT1, EXT2, roughly paralleling PA-RO, PA0, PA1, PA2 respectively, and generalizing prior work [26, 27, 34, 12], although we mention that [34] already has our EXT1 definition. Besides this parallel, our generalizations consider adversaries that output only part of an image point or an image point along with part of a pre-image. These are bold assumptions to make on (functions constructed out of) cryptographic hash functions, but, as discussed above, we believe studying their implications is justified. In the case of s-clear, another hero is a family of new "XOR-type" assumptions we introduce, and give intuitive justifications for in light of the multiplicative structure of RSA. Again, we view part of our contribution as putting forth novel assumptions that the research community can analyze (say in the generic ring model) in the future.

We make several remarks about our results, particularly how they avoid known impossibility results, before detailing them:

- Extractability is a non-blackbox assumption (saying for every adversary there exists a non-blackbox "extractor") so we avoid the impossibility result of Kiltz and Pietrzak [49].[6]. That is, the fact we use extractable hash functions (extractability being an intuitive property used in the original RO model proof) is somewhat unavoidable.

- While extractability of $\mathcal{H}$ would *prima facie* be false, we use it only in a plausible way for a cryptographic hash function. Namely, the adversary also outputs *part of the preimage.* Extractability assumptions we use on $\mathcal{G}$, even where the adversary outputs only part of an image point, remain plausible as it is an expanding function with a sparse range (usually constructed something like $\mathcal{G}(x) = (\mathcal{H}(0\|x)\|\mathcal{H}(1\|x), \ldots)$.
- For extractability we use only bounded key-independent auxiliary input (basically, the keys for the other functions in the scheme), so we avoid the impossibility result of Bitansky *et al.* [14]. Moreover, the key-dependent auxiliary information is just one image query (at least in the proof of IND-CCA2).
- Our "XOR-type" assumptions on RSA avoid a negative result of Shoup [59], showing that there is an attack if the general trapdoor permutation is "XOR-malleable."[7]
- We typically use the various forms of extractability in combination with (at least) collision-resistance, so that the extractor returns the "right" preimage. The collision-resistant construction of [52] based on knowledge assumptions, albeit where the adversary outputs the entire image point, is on the lowest level of our hierarchy (EXT0); furthermore, it is not known to work when the adversary outputs part of the image point. Any theoretical constructions for higher levels (EXT1, EXT2) are similarly open. We hope these are targeted in future work.

Results and intuition for t-clear. Our results for t-clear RSA-OAEP are weaker than those for s-clear RSA-OAEP. First, for t-clear we prove IND-CPA for high-entropy, public key independent messages, under mild assumptions on the round functions, namely that $\mathcal{H}$ is a hardcore function for RSA and $\mathcal{G}$ is a pseudorandom generator. Intuitively, the high-entropy requirement comes from the fact that the adversary attacking $\mathcal{H}$ needs to know r to prepare its challenge ciphertext, so the randomness of the input to $\mathcal{H}$ needs to come from m. (We could avoid it using the stronger assumption of UCE as per the result of [5], which could be viewed as a hedge.) Furthermore, m needs to be public-key independent so as to not bias the output. Then we can prove PA0 based on forms of EXT0 for $\mathcal{G}$ and $\mathcal{H}$, the intuition being that the plaintext extractor first extracts from the part $\mathcal{G}(r)$ that is left in clear by the redundancy to get r and then runs the extractor for $\mathcal{H}$ on $t \oplus r$ from which it can compute m, with the above part of the pre-image to get s. Note that when running the extractor here and below we have to be careful that the constructed extractor uses the same coins as the

[6] As acknowledged by the authors there was a bug in the proceedings version of this paper, but this has been fixed for the full version [50].

[7] In more detail, note that for s-clear the "overall" TDP (including the part output in the clear) is not partial one-way [39] so their security proof does *not* apply. In fact, Shoup [59] considers the scheme in his proof that RSA-OAEP is not IND-CCA2-secure for general one-way TDPs, exhibiting the above-mentioned attack.

starting one for consistency (otherwise we won't end up with the right extractor). We can also prove PA1, although we have to make an extractability assumption directly on the padding scheme.[8] Interestingly, even this approach does not work for PA2, which we leave completely open for t-clear (cf. Remark 14).

Results and intuition for s-clear. We find s-clear is much more friendly to a full instantiation by making novel but plausible assumptions on RSA. One is XOR-nonmalleability (XOR-NM), saying that from $\mathcal{F}(x)$ it is hard to find some $\mathcal{F}(x')$ and z such that $z = x \oplus x'$. Another is XOR-indistinguishability (XOR-IND), saying for random x and adversarially-chosen z one cannot tell $\mathcal{F}(x)$ from $\mathcal{F}(x \oplus z)$ given "hint" $\mathcal{G}(x)$. In our results, $\mathcal{G}$ is a PRG, which we show also implies $\mathcal{G}$ is a HCF for $\mathcal{F}$. So, the notion can be viewed as an extension of the classical notion of HCF. In fact, we use XOR-IND just to show IND-CPA. The intuition is that it allows breaking the dependency of s in the input to OAEP with the input to RSA. The proofs of PA0 and PA1 are very similar, and showcase one reason s-clear is much more friendly to a full instantiation, namely it heavily depends on the extractability of $\mathcal{G}$. That is, if $\mathcal{G}$ is suitably extractable, the plaintext extractor can simply recover r and then compute the plaintext as $s \oplus \mathcal{G}(r)$. For PA2, one has to be careful as when the adversary makes an encryption query, the plaintext extractor should call the image oracle for $\mathcal{G}$, where in addition to $\mathcal{G}(x)$ for random x it receives the hint of RSA on x. We show that if RSA is XOR-IND then this implies the adversary can get the whole ciphertext as a hint to simulate the encryption oracle. Then we also have the worry about the adversary querying "mauled" ciphertexts to the extract oracle. Intuitively, if the r-part is the same then it cannot run the extractor for $\mathcal{G}$, but we show this violates XOR-NM of RSA. On the other hand, if the s-part is the same then we cannot break XOR-NM but this creates a collision for $\mathcal{G}$.

1.7 Discussion and Perspective

We summarize and compare our results to prior work in Fig. 1. Note that we get a lot of mileage from assuming the trapdoor permutation is specifically RSA, whereas prior work, which has mostly shown negative results CCA-style security notions, went for a general approach. We also highlight that while our assumptions on both RSA and the round functions for our full instantiability results are expectedly stronger than what we need for partial instantiations, they still compare favorably to prior work. In particular, while our assumption of EXT2 for $\mathcal{G}$ in our s-clear result is already "PA2-flavored," prior work [18, Definition 3.3] made CCA-style assumptions on the round functions even to obtain relatively weak notions of non-malleability. It can also be viewed as a strengthening of "adaptive" (CCA-style) security notions on one-way functions [54, 47].[9] Plus,

[8] At a very high level, we can prove EXT0 of $\mathcal{G}, \mathcal{H}$ implies EXT0 for the padding scheme, but we do not know how to do this for EXT1 because of an "extractor blow-up" problem.

[9] These works do not precisely match our setting as [54] consider keyless functions and [47] consider functions with a trapdoor.

Scheme	Assumptions on OAEP	Assumptions on $\mathcal{F}$	Security	Size	Ref
RSA-OAEP	**$\mathcal{G}$: PRG and $\mathcal{H}$: RO**	**OW, SIE and CIE**	**IND-CCA2**	n	**Section 3**
RSA-OAEP	**$\mathcal{G}$: RO and $\mathcal{H}$: PHCF**	**OW, SIE and CIE**	**IND-CCA2**	n	**Section 3**
RSA-OAEP	$\mathcal{G}$: t-wise independent	Lossy TDP	IND-CPA	n	[48]
RSA-OAEP	$\mathcal{G}, \mathcal{H}$: UCE	OW	IND-CPA-KI	n	[5]
RSA-OAEP ***t*-clear**	**$\mathcal{G}$: PRG, EXT0 and NCR** **$\mathcal{H}$: HCF, EXT0 and CR**	**OW**	**$IND-CCA0-KI**	$3n + 3k$	**Full version**
RSA-OAEP ***t*-clear**	OAEP **: EXT1 and NCR** **$\mathcal{G}$: PRG and $\mathcal{H}$: HCF**	**OW**	**$IND-CCA1-KI**	$3n + 3k$	**Full version**
RSA-OAEP *t*-clear	$\mathcal{G}$: PRG and NCR $\mathcal{H}$: RO	OW	IND-CCA2	$n + k$	[18]
RSA-OAEP *t*-clear	$\mathcal{G}$: RO $\mathcal{H}$: NM PRG with hint	OW	IND-CCA2	$n + k$	[18]
RSA-OAEP *t*-clear	$\mathcal{G}$: PRG and NCR $\mathcal{H}$: NM PRG with hint	OW	$NM-CPA	$n + k$	[18]
RSA-OAEP ***s*-clear**	**$\mathcal{G}$: PRG, EXT1 and NCR**	**XOR-IND0**	**IND-CCA1**	$2n + k + \mu$	**Section 6**
RSA-OAEP ***s*-clear**	**$\mathcal{G}$: PRG, EXT2 and NCR** **$\mathcal{H}$: CR**	**XOR-IND1,2** **and XOR-NM0**	**IND-CCA2**	$2n + k + \mu$	**Section 6**

Fig. 1: Instantiability results for RSA-OAEP, where n is modulus length, k is security param and μ is message length. Typically $n = 2048, k = 128$ and $\mu = 128$.

it is not clear how to get an IND-CCA2 encryption scheme from EXT2 functions in a simpler way.

1.8 Related Work

RO model results. Results about security of $\mathcal{F}$-OAEP for an abstract TDP $\mathcal{F}$ with applications to RSA-OAEP in the RO model were shown in [10, 59, 39]. 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. Interestingly, Shoup [59] considers s-clear RSA-OAEP indirectly in a negative result about RSA-OAEP with a general one-way TDP. Security of t-clear RSA-OAEP (under the name “RSA-OAEP++‘’) has been analyzed in the RO model by Boldyreva, Imai and Kobara [19], who show tight security in the multi-challenge setting.

Partial instantiation results. Canetti [24] conjectured that his notion of perfect one-wayness sufficed to instantiate *one* of the two oracles in $\mathcal{F}$-OAEP. This was disproved in general by Boldyreva and Fischlin [17], but their results do not contradict ours because they use a contrived TDP $\mathcal{F}$. Subsequently, Boldyreva and Fischlin [18] gave partial instantiations for t-clear $\mathcal{F}$-OAEP under stronger assumptions on the round functions.

Full instantiation results. Brown [22] and Paillier and Villar [53] showed negative results for proving RSA-OAEP is IND-CCA secure in restricted models, and Kiltz and Pietrzak [49] showed a general black-box impossibility result. As mentioned above, their results do not contradict ours because we use non-blackbox assumptions. Moving to weaker notions, Kiltz *et al.* [47] show IND-CPA security of RSA-OAEP using lossiness [55], while Bellare, Hoang, and Keelveedhi [5] show RSA-OAEP is IND-CPA secure for public-key independent messages assuming the round functions meet their notion of universal computational extraction. Boldyreva and Fischlin [18] show a weak form of non-malleability for t-clear $\mathcal{F}$-OAEP, again using very strong assumptions on the round functions. Lewko *et al.* [51] show IND-CPA security of the RSA PKCS v1.5 scheme, with the bounds later being corrected and improved by Smith and Zhang [60].

Candidate instantiability assumptions. General notions for function families geared toward instantiating ROs that have been proposed include correlation intractability [28, 25], extractable hash functions [26, 27, 12, 14], perfect one-wayness [24, 29, 37], seed incompressibility [42], non-malleability [16, 1], and universal computational extraction (UCE) [5, 23, 6].

1.9 Organization

In Section 2, we give the preliminaries. In Section 3, we formalize the algebraic properties of RSA we use and our partial instantiation results for RSA-OAEP. In Section 4, we give a new hierarchy of extractable functions. In Section 5, we abstract out some properties of the OAEP padding scheme we use. Then, in Section 6 we give novel "XOR-type" assumptions on RSA and combine them with the above to give our full instantiation result s-clear RSA-OAEP. Due to space constraints, our results for t-clear RSA-OAEP are deferred to the supplementary materials. We also defer all detailed proofs to the supplementary materials.

2 Preliminaries and Some Generalizations

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 $\Pr\big[A(x) = y : x \leftarrow_{\$} X\big]$ 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 $k \in \mathbb{N}$. Unless otherwise specified, all algorithms must run in probabilistic polynomial-time (PPT) in k, and an algorithm's running-time includes that of any overlying experiment as well as the size of its code. Integer parameters often implicitly depend on k. The length of a string s is denoted $|s|$. We denote by $s|_i^j$ the i-th least significant bits(LSB) to j-th least significant bits of s(including i-th and j-th bits), where $1 \leq i \leq j \leq |s|$. For convenience, we denote by $s|_\ell = s|_1^\ell$ the ℓ least significant bits of s and $s|^\ell = s|_{|s|-\ell}^{|s|}$ the ℓ most significant bits(MSB) of s, for $1 \leq \ell \leq |s|$. We write P_X for the distribution of random variable X and $P_X(x)$ for the probability that X puts on value x, i.e. $P_X(x) = \Pr[X = x]$. We denote by U_ℓ the uniform distribution on $\{0,1\}^\ell$.

```
**Game** PA-RO$^{A,\mathsf{Ext}}_{\mathsf{PKE}}(k)$
$b \leftarrow_\$ \{0,1\}$ ; $i \leftarrow 1$ ; $j \leftarrow 1$
$(pk, sk) \leftarrow_\$ \mathsf{Kg}(1^k)$
$b' \leftarrow_\$ A^{\mathrm{RO}(\cdot,1),\textsc{Enc}(pk,\cdot),\mathcal{D}(sk,\cdot)}(pk)$
Return $(b = b')$

**Procedure** $\mathrm{RO}(x, i)$
If $H[x] = \bot$ then $H[x] \leftarrow_\$ \{0,1\}^\ell$
If $i = 1$ then
    $\mathbf{x}[j] \leftarrow x$ ; $\mathbf{h}[j] \leftarrow H[x]$ ; $j \leftarrow j + 1$
Return $H[x]$
```

```
**Procedure** $\textsc{Enc}(pk, \mathcal{M})$
$m \leftarrow_\$ \mathcal{M}(1^k, pk)$
$c \leftarrow_\$ \mathsf{Enc}^{\mathrm{RO}(\cdot,2)}(pk, m)$
$\mathbf{c}[i] \leftarrow c$ ; $i \leftarrow i + 1$
Return $c$

**Procedure** $\mathcal{D}(sk, c)$
If $c \in \mathbf{c}$ then return $\bot$
$m_0 \leftarrow \mathsf{Dec}(sk, c)$
$m_1 \leftarrow_\$ \mathsf{Ext}^{\mathrm{RO}(\cdot,3)}(\mathbf{x}, \mathbf{h}, \mathbf{c}, c, pk)$
Return $m_b$
```

Fig. 2: **Game to define PA-RO security.**

We write U_S for the uniform distribution on the set 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 $1 \leq i \leq |\mathbf{x}|$. 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 $1 \leq i \leq |\mathbf{x}|$. Let X be random variables taking values on a common finite domain. The min-entropy of a random variable X is $\mathrm{H}_\infty(X) = -\log(\max_x \Pr[\, X = x \,])$.

2.2 Public-Key Encryption and its Security

Public-key encryption. A *public-key encryption scheme* PKE with message space Msg is a tuple of algorithms $(\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec})$. 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 $\bot$. 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.

PA-RO security. We first define plaintext-awareness in the RO model following [4], which builds on the definition in [10] and is strictly stronger than IND-CCA2 security in general. Let $\mathsf{PKE} = (\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec})$ be a public key encryption scheme and let $\mathcal{M}$ be a PPT algorithm that takes as inputs 1^k and a public key pk, and outputs a message $m \in \mathsf{Msg}(1^k)$. To adversary A and extractor Ext, we associate the experiment in Fig. 2 for every $k \in \mathbb{N}$. We say that PKE is PA-RO secure if for every PPT adversary A there exists an extractor Ext such that

$$\mathbf{Adv}^{\mathsf{pa\text{-}ro}}_{\mathsf{PKE},A,\mathsf{Ext}}(k) = 2 \cdot \Pr\left[\text{PA-RO}^{A,\mathsf{Ext}}_{\mathsf{PKE}}(k) \Rightarrow 1\right] - 1 \ .$$

is negligible in k.

Remark 1. Our definition of plaintext awareness in the random oracle model differs from the definition given in [4] in the following way. In our definition,

Game $\mathrm{PAI}_{\mathsf{PKE}}^{A,\mathsf{Ext}}(k)$	**Procedure** $\mathcal{D}(sk, c)$	**Procedure** $\textsc{Enc}(pk, \mathcal{M})$
$(pk, sk) \leftarrow_{\$} \mathsf{Kg}(1^k)$	If $c \in \mathbf{c}$ then return $\perp$	$m \leftarrow_{\$} \mathcal{M}(1^k, pk)$
$b \leftarrow_{\$} \{0,1\}$; $i \leftarrow 1$; $\mathbf{c} \leftarrow \varepsilon$	$m_0 \leftarrow \mathsf{Dec}(sk, c)$	$c \leftarrow_{\$} \mathsf{Enc}(pk, m)$
$r \leftarrow_{\$} \mathsf{Coins}(k)$; $st \leftarrow (pk, r)$	$(m_1, st) \leftarrow_{\$} \mathsf{Ext}(st, \mathbf{c}, c)$	$\mathbf{c}[i] \leftarrow c$; $i \leftarrow i + 1$
$b' \leftarrow A^{\mathcal{D}(sk,\cdot),\mathcal{O}}(pk; r)$	Return m_b	Return c
Return $(b = b')$		

Fig. 3: **Games to define PAI security.**

we are giving the extractor access to the random oracle. We observe that the analogous result of [4, Theorem 4.2] that IND-CPA and PA-RO together imply IND-CCA2 still holds for our modified definition, since in the proof the IND-CPA adversary could query its own random oracle to answer to the random oracle queries of the extractor.

We now turn to definitions of plaintext awareness in the standard model, following [8].

PA SECURITY. Let $\mathsf{PKE} = (\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec})$ be a public key encryption scheme. For $\mathrm{PAI} \in \{\mathrm{PA0}, \mathrm{PA1}, \mathrm{PA2}\}$, we associate the experiment in Fig. 3 to adversary A and extractor Ext, for every $k \in \mathbb{N}$. Define the PAI advantage of A

$$\mathbf{Adv}^{\mathrm{pai}}_{\mathsf{PKE},A,\mathsf{Ext}}(k) = 2 \cdot \Pr\left[\, \mathrm{PAI}^{A,\mathsf{Ext}}_{\mathsf{PKE}}(k) \Rightarrow 1 \,\right] - 1 \ .$$

If PAI = PA1, then $\mathcal{O} = \varepsilon$. PA0 is defined similarly to PA1, except A is only allowed to make a single decryption query. If PAI = PA2, then $\mathcal{O} = \textsc{Enc}$. We say that PKE is PAI secure if for every PPT adversary A with coin space Coins there exists an extractor Ext such that, $\mathbf{Adv}^{\mathrm{pai}}_{\mathsf{PKE},A,\mathsf{Ext}}(k)$ is negligible in k.

Remark 2. Our PA2 definition comes from [8]. We give PA2 adversary extra access to encryption oracle. This models the ability that IND-CCA2 adversary obtains ciphertext without knowing the randomness.

2.3 Trapdoor Permutations and Their Security

TRAPDOOR PERMUTATIONS. A trapdoor permutation family with domain TDom is a tuple of algorithms $\mathcal{F} = (\mathsf{Kg}, \mathsf{Eval}, \mathsf{Inv})$ that work as follows. Algorithm Kg on input a unary encoding of the security parameter 1^k outputs a pair (f, f^{-1}), where $f\colon \mathsf{TDom}(k) \to \mathsf{TDom}(k)$. Algorithm Eval on inputs a function f and $x \in \mathsf{TDom}(k)$ outputs $y \in \mathsf{TDom}(k)$. We often write $f(x)$ instead of $\mathsf{Eval}(f, x)$. Algorithm Inv on inputs a function f^{-1} and $y \in \mathsf{TDom}(k)$ outputs $x \in \mathsf{TDom}(k)$. 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 $x \in \mathsf{TDom}(k)$, $f^{-1}(f(x)) = x$. We call $\mathcal{F}$ an n-bit trapdoor permutation family if $\mathsf{TDom} = \{0,1\}^n$. We will think of the RSA trapdoor permutation family [57] n-bit for simplicity, although its domain is $\mathbb{Z}_N^*$ for an n-bit integer N. Additionally, for convenience we define the following. For an ν-bit trapdoor permutation family and $\ell \in \mathbb{N}$, we define $\mathcal{F}|_\ell = (\mathsf{Kg}|_\ell, \mathsf{Eval}|_\ell, \mathsf{Inv}|_\ell)$

as the $(\nu + \ell)$-bit trapdoor permutation families such that for all $k \in \mathbb{N}$, all $(f|_\ell, f^{-1}|_\ell) \in [\mathsf{Kg}|_\ell(1^k)]$, and all $x \in \{0,1\}^{\nu+\ell}$, we have $f(x)|_\ell = f(x|^{n-\ell})\|x|_\ell$, and analogously for $\mathcal{F}|^\ell$.

2.4 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 $\mathcal{F}\colon \mathcal{K}_F \times \mathsf{F.Dom} \to \mathsf{F.Rng}$. We call $\mathcal{F}$ an *ℓ-injective* function if for all distinct $x_1, x_2 \in \mathsf{F.Dom}(k)$ and $K_F \in [\mathcal{K}_F(1^k)]$, we have $F(K_F, x_1)|_\ell \neq F(K_F, x_2)|_\ell$.

Near-collision resistance. Let $\mathcal{H}\colon \mathcal{K}_H \times \mathsf{HDom} \to \mathsf{HRng}$ be a function family. For $m \in \mathbb{N}$ suppose $\mathsf{HRng} = \{0,1\}^m$. For $1 \le \ell \le m$ we say $\mathcal{H}$ is *near-collision resistant* with respect to ℓ-least significant bits of the outputs (NCR$_\ell$) if for any PPT adversary A:

$$\mathbf{Adv}^{\text{n-cr}_\ell}_{\mathcal{H},A}(k) = \Pr_{K_H \leftarrow\!\$\, \mathcal{K}_H(1^k)}\left[\begin{array}{c} (x_1,x_2) \leftarrow A(K_H) \\ x_1, x_2 \in \mathsf{HDom}(k) \end{array} \wedge \begin{array}{c} \mathcal{H}(K_H,x_1)|_\ell = \mathcal{H}(K_H,x_2)|_\ell \\ x_1 \neq x_2 \end{array}\right]$$

is negligible in k. We note that our definition differs slightly from [18] as both x_1, x_2 are adversarially chosen. In terms of feasibility, the same construction based on one-way permutations given in [18] works in our case as well. Similarly, we define NCR$^\ell$ where the adversary tries to find collision on the ℓ-most significant bits of the output.

Partial hardcore functions. For convenience, we also generalize the notion of hardcore function in the following way. Let $\mathcal{F} = (\mathsf{Kg}, \mathsf{Eval}, \mathsf{Inv})$ be n-bit trapdoor permutation family. Let $\mathcal{H}\colon \mathcal{K}_H \times \{0,1\}^{n-\ell} \to \mathsf{HRng}$ be a function family, for some $\ell < n$. To attacker A, we associate the experiment in Fig. 4 for every $k \in \mathbb{N}$. We say that $\mathcal{H}$ is a *ℓ-partial hardcore function* for the trapdoor permutation family $\mathcal{F}$ if for every PPT adversary A,

$$\mathbf{Adv}^{\text{phcf}}_{\mathcal{F},\mathcal{H},A}(k) = 2 \cdot \Pr\left[\text{PHCF-DIST}^{A}_{\mathcal{F},\mathcal{H}}(k) \Rightarrow 1\right] - 1 \ .$$

is negligible in k. Note if $(f(x), x|_{n-\ell})$ is a one-way function of x, then $\mathcal{H}$ is a ℓ-partial hardcore function for $\mathcal{F}$ when $\mathcal{H}$ is a computational randomness extractor [32]. This is plausible for the case that $\mathcal{F}$ is RSA when $n - \ell$ is small enough that Coppersmith's techniques do not apply. This means $n - \ell \le n(e-1)/e - \log 1/\epsilon$ such that $N^\epsilon \ge 2^k$ for security parameter k.

2.5 The OAEP Framework

OAEP padding scheme. We recall the OAEP padding scheme [10]. 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 $\mathcal{H}\colon \mathcal{K}_H \times \{0,1\}^{\mu+\zeta} \to$

```
**Game** PHCF-DIST$^A_{\mathcal{F},\mathcal{H}}(k)$
$b \xleftarrow{\$} \{0,1\}$ ; $K_H \xleftarrow{\$} \mathcal{K}_H(1^k)$ ; $(f, f^{-1}) \xleftarrow{\$} \mathsf{Kg}(1^k)$
$x \xleftarrow{\$} \{0,1\}^n$ ; $h_0 \leftarrow H(K_H, x|^{\ell})$ ; $h_1 \xleftarrow{\$} \mathsf{HRng}(k)$
$b' \xleftarrow{\$} A(K_H, f, f(x), x|_{n-\ell}, h_b)$
Return $(b = b')$
```

Fig. 4: **Games to define PHCF-DIST security.**

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 $m'|_{\zeta} = 0^{\zeta}$ return $m'|^{\mu}$
Return x	Else return $\bot$

Fig. 5: **OAEP padding scheme** $\mathsf{OAEP}[G, H]$**.**

$\{0,1\}^{\rho}$ 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 $K_G \xleftarrow{\$} \mathcal{K}_G(1^k)$ and $K_H \xleftarrow{\$} \mathcal{K}_H(1^k)$, and $\mathsf{OAEP}, \mathsf{OAEP}^{-1}$ are as defined in Fig. 5.

OAEP ENCRYPTION SCHEME AND VARIANTS. Slightly abusing notation, we denote by $\mathsf{OAEP}[\mathcal{G},\mathcal{H},\mathcal{F}]$ the OAEP-based encryption scheme $\mathcal{F}$-OAEP with $n = \nu$. We also consider two other OAEP-based encryption schemes, called *t-clear* and *s-clear* $\mathcal{F}$-OAEP, and denoted $\mathsf{OAEP}_{\mathsf{t\text{-}clear}}[\mathcal{G},\mathcal{H},\mathcal{F}|_{\zeta+\rho}]$ and $\mathsf{OAEP}_{\mathsf{s\text{-}clear}}$ $[\mathcal{G},\mathcal{H},\mathcal{F}|^{\mu+\zeta}]$. Here $n = \mu$ and $n = \rho$, respectively. We often write $\mathsf{OAEP}_{\mathsf{t\text{-}clear}}$ and $\mathsf{OAEP}_{\mathsf{s\text{-}clear}}$ instead of $\mathsf{OAEP}_{\mathsf{t\text{-}clear}}[\mathcal{G},\mathcal{H},\mathcal{F}|_{\zeta+\rho}]$ and $\mathsf{OAEP}_{\mathsf{s\text{-}clear}}[\mathcal{G},\mathcal{H},\mathcal{F}|^{\mu+\zeta}]$. We typically think of $\mathcal{F}$ as RSA, and all our results apply to this case under suitable assumptions. Note that, following prior work, despite its name t-clear $\mathcal{F}$-OAEP we actually apply $\mathcal{F}$ to only the μ most significant bits of the output of the underlying padding scheme, leaving the redundancy part of s in the clear as well.

3 Partial Instantiation Results for RSA-OAEP

In this section, we give partial instantiations of either $\mathcal{G}$ or $\mathcal{H}$ for RSA-OAEP under IND-CCA2. Our results use only mild standard model properties of $\mathcal{G}$ or $\mathcal{H}$. We also use (generalizations of) algebraic properties of RSA proven by Barthe *et al.* [3] for small enough e. For example, using a 2048-bit modulus and encrypting a 128-bit AES key, our results hold for $e = 3$. They might be true for larger e; at least, they cannot be disproved. Note that our results first necessitate a separate proof of IND-CPA — the standard model IND-CPA results of Kiltz *et al.* [48] and Bellare *et al.* [5] are not suitable, the first requiring large e and the second holding only for public-key independent messages.

3.1 Algebraic Properties of RSA

We first give generalizations of algebraic properties of RSA from Barthe *et al.* [3] that we use, and their parameters. They used these assumptions to analyze security of a zero-redudancy one-round version of RSA-OAEP. We show that generalizations are useful for analyzing security of full RSA-OAEP.

Second-input extractability. 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* (BB (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-input extractability. 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)-*common-input-extractable* 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 $x_1, x_2 \in \mathsf{TDom}(k)$, 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.

Comparison to Barthe *et al.* Compared to [3], we generalize the notions of SIE and CIE to consider arbitrary runs of consecutive bits. That is, [3] only considers the most significant bits; *i.e.*, ζ-SIE and ζ-CIE in our notation.

Parameters. Barthe *et al.* [3] show via the univariate Coppersmith algorithm [30] 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 $\zeta_2 > n(e^2-1)/e^2$. We show that a generalization to runs of arbitrary consecutive bits using the *bivariate* Coppersmith algorithm [30, 15, 31]. Specifically, we show that RSA is (i,j)-SIE for $(j-i) > n(e-1)/e$, and (i,j)-CIE for $(j-i) > n(e^2-1)/e^2$, Due to space constraints, this is shown in the full version. Note that in our partial instantiation results for RSA-OAEP, $j-i$ refers to the length of the redundancy ζ.

3.2 Main Results

Main results. We now give our main results, namely partial instantiations for RSA-OAEP of either oracle $\mathcal{G}$ or $\mathcal{H}$. These results refer to IND-CCA2 security for simplicity, whereas we actually prove PA-RO + IND-CPA.

Theorem 3. Let n, μ, ζ, ρ be integer parameters. Let $\mathcal{G} : \mathcal{K}_G \times \{0,1\}^\rho \to \{0,1\}^{\mu+\zeta}$ be a pseudorandom generator and $\mathcal{H} : \{0,1\}^{\mu+\zeta} \to \{0,1\}^\rho$ be a RO. Let $\mathcal{F}$ be a family of trapdoor permutations with domain $\{0,1\}^n$, where $n = \mu + \zeta + \rho$. Suppose $\mathcal{F}$ is one-way, $(\mu+\zeta)$-second input and $(\mu+\zeta)$-common input extractable. Then $\mathsf{OAEP}[\mathcal{G}, \mathcal{H}, \mathcal{F}]$ is IND-CCA2 secure. In particular, for any adversary A, there is an adversary D and an inverter I such that

$$\mathbf{Adv}^{\text{ind-cca2}}_{\mathsf{OAEP}[\mathcal{G},\mathcal{H},\mathcal{F}],A}(k) \leq 2 \cdot \mathbf{Adv}^{\text{owf}}_{\mathcal{F},I}(k) + 10 \cdot \mathbf{Adv}^{\text{prg}}_{\mathcal{G},D}(k) + \frac{2p}{2^{\mu+\zeta}} + \frac{4q}{2^{\zeta}} \ .$$

where q is the total number of the decryption queries and p is the total number of RO queries made by A. Furthermore, the running time of D and I are about that of A plus the time to run SIE and CIE extractors.

Theorem 4. Let n, μ, ζ, ρ be integer parameters. Let $\mathcal{H} : \mathcal{K}_H \times \{0,1\}^{\mu+\zeta} \rightarrow \{0,1\}^{\rho}$ be a hash function family and $\mathcal{G} : \{0,1\}^{\rho} \rightarrow \{0,1\}^{\mu+\zeta}$ be a RO. Let $\mathcal{F}$ be a family of trapdoor permutations with domain $\{0,1\}^n$, where $n = \mu+\zeta+\rho$. Suppose $\mathcal{F}$ is $(\rho, \rho+\zeta)$-second input and $(\rho, \rho+\zeta)$-common input extractable. Suppose further $\mathcal{H}$ is a $(\mu+\zeta)$-partial hardcore function for $\mathcal{F}$. Then $\mathsf{OAEP}[\mathcal{G}, \mathcal{H}, \mathcal{F}]$ is IND-CCA2. In particular, for any adversary $A = (A_1, A_2)$, there exists an adversary B such that

$$\mathbf{Adv}^{\text{ind-cca2}}_{\mathsf{OAEP}[\mathcal{G},\mathcal{H},\mathcal{F}],A}(k) \le 2 \cdot \mathbf{Adv}^{\text{phcf}}_{\mathcal{F},\mathcal{H},B}(k) + \frac{2p}{2^{\rho}} + \frac{4q}{2^{\zeta}} \ .$$

where q the total number of the decryption queries and p is the total number of RO queries made by A. Furthermore, the running time of B is about that of A plus the time to run SIE and CIE extractors.

The proofs of both theorems follow from below.

Parameters for RSA-OAEP. We discuss when our results support RSA-OAEP encryption of an AES key of appropriate length, based on Subsection 3.1. The main requirement is encryption exponent $e = 3$. In this case, with length 2048 bits we can use randomness and message length 128 bits, and for modulus length 4096 we can use randomness length 256. The choice that $e = 3$ is sometimes used in practice but it is an interesting open problem to extend our results to other common choices such as $e = 2^{16} + 1$. In particular, it may be possible that SIE and CIE hold in this case for the same parameters. Interestingly, we have a "flipped" situation vs. [48] who show IND-CPA security of RSA-OAEP in the standard model using *large exponent* RSA. We hope future work will help reconcile these differences.

3.3 Partial Instantiation of G

We first show how to instantiate $\mathcal{G}$ when modeling $\mathcal{H}$ as a RO. In particular, we show $\mathsf{OAEP}[\mathcal{G}, \mathcal{H}, \mathcal{F}]$ is IND-CPA + PA-RO when $\mathcal{G}$ is a pseudorandom generator and $\mathcal{F}$ is one-way, $(\mu+\zeta)$-SIE and $(\mu+\zeta)$-CIE.

IND-CPA result. Under IND-CPA, we show a tight reduction when $\mathcal{G}$ is a pseudorandom generator and $\mathcal{F}$ is one-way and $(\mu+\zeta)$-SIE. Alternatively, we give result where $\mathcal{F}$ is only partial one-way, but the reduction is lossy (due to space constraints, this is shown in the full version). Note that it is shown in [38] that one-wayness of RSA implies partial one-wayness, but the reduction is even more lossy, while SIE and CIE unconditionally hold for appropriate parameters.

Theorem 5. Let n, μ, ζ, ρ be integer parameters. Let $\mathcal{G} : \mathcal{K}_G \times \{0,1\}^{\rho} \rightarrow \{0,1\}^{\mu+\zeta}$ be a pseudorandom generator and $\mathcal{H} : \{0,1\}^{\mu+\zeta} \rightarrow \{0,1\}^{\rho}$ be a RO. Let $\mathcal{F}$ be a family of trapdoor permutations with domain $\{0,1\}^n$, where

$n = \mu + \zeta + \rho$. Suppose $\mathcal{F}$ is one-way and $(\mu+\zeta)$-second input extractable. Then $\mathsf{OAEP}[\mathcal{G}, \mathcal{H}, \mathcal{F}]$ is IND-CPA. In particular, for any adversary $A = (A_1, A_2)$, there are an adversary D and an inverter I such that

$$\mathbf{Adv}^{\text{ind-cpa}}_{\mathsf{OAEP}[\mathcal{G},\mathcal{H},\mathcal{F}],A}(k) \leq 2 \cdot \mathbf{Adv}^{\text{owf}}_{\mathcal{F},I}(k) + 6 \cdot \mathbf{Adv}^{\text{prg}}_{\mathcal{G},D}(k) + \frac{2q}{2^{\mu+\zeta}} \ .$$

where q is the total number of RO queries made by A. Furthermore, the running time of D is about that of A and the running time of I is about that of A plus the time to run SIE extractor.

Proof idea. Let $c = f(s\|t)$ be the challenge ciphertext. Note that, it is unlikely that A queries value s to $\mathcal{H}$ since one could use SIE extractor to invert challenge c knowing s. Thus, value t looks random to A. Moreover, we know $\mathcal{G}$ is PRG, then value s looks random. Therefore, challenge c looks random to A.

PA-RO result. We show RSA-OAEP is PA-RO when modeling $\mathcal{H}$ as a RO if $\mathcal{G}$ is a pseudorandom generator and $\mathcal{F}$ is both second-input extractable and common-input extractable.

Theorem 6. Let n, μ, ζ, ρ be integer parameters. Let $\mathcal{G} : \mathcal{K}_G \times \{0,1\}^\rho \rightarrow \{0,1\}^{\mu+\zeta}$ be a pseudorandom generator and $\mathcal{H} : \{0,1\}^{\mu+\zeta} \rightarrow \{0,1\}^\rho$ be a RO. Let $\mathcal{F}$ be a family of trapdoor permutations with domain $\{0,1\}^n$, where $n = \mu + \zeta + \rho$. Suppose $\mathcal{F}$ is $(\mu+\zeta)$-second input and $(\mu+\zeta)$-common input extractable. Then $\mathsf{OAEP}[\mathcal{G}, \mathcal{H}, \mathcal{F}]$ is PA-RO secure. In particular, for any adversary A, there exists an adversary D and an extractor Ext such that

$$\mathbf{Adv}^{\text{pa-ro}}_{\mathsf{OAEP}[\mathcal{G},\mathcal{H},\mathcal{F}],A,\mathsf{Ext}}(k) \leq 2 \cdot \mathbf{Adv}^{\text{prg}}_{\mathcal{G},D}(k) + \frac{2q}{2^{\zeta}} \ .$$

where q is the total number of the extraction queries made by A. Furthermore, the running time of D is about that of A and the running time of Ext is about that of SIE and CIE extractors.

Proof idea. Let $c = f(s\|t)$ be the extract query made by A. If there is a prior query s to $\mathcal{H}$, then one could use SIE or CIE extractor to extract message m. Otherwise the challenge c is invalid whp, since the ζ-lsb of $G(K_G, r)$ and s are not equal on random r whp, when $\mathcal{G}$ is PRG.

3.4 Partial Instantiation of *H*

Now, we instantiate the hash function $\mathcal{H}$ when modeling only $\mathcal{G}$ as a RO. In particular, we show $\mathsf{OAEP}[\mathcal{G}, \mathcal{H}, \mathcal{F}]$ is IND-CPA + PA-RO when $\mathcal{H}$ is a special type of hardcore function and $\mathcal{F}$ is one-way, second-input and common-input extractable. Note that Boneh [20] previously showed a simplified RSA-OAEP with one Feistel round $\mathcal{G}$ is IND-CCA2 secure and Barthe *et al.* [3] showed such a scheme does not even need redundancy, but these proof do not translate to the case of $\mathcal{H}$ as a cryptographic hash function.

IND-CPA RESULT. Under IND-CPA, we show a tight reduction when $\mathcal{H}$ is a $(\mu + \zeta)$-partial hardcore function for $\mathcal{F}$. In particular, it is plausible for $\mathcal{H}$ as a computational randomness extractor [32] and that $\mathcal{F}$ is RSA in the common setting $\rho = k$ (*e.g.*, $\rho = 128$ for modulus length $n = 2048$), since Coppersmith's technique fails.

Theorem 7. Let n, μ, ζ, ρ be integer parameters. Let $\mathcal{H} : \mathcal{K}_H \times \{0,1\}^{\mu+\zeta} \to \{0,1\}^{\rho}$ be a hash function family and $\mathcal{G} : \{0,1\}^{\rho} \to \{0,1\}^{\mu+\zeta}$ be a RO. Let $\mathcal{F}$ be a family of trapdoor permutations with domain $\{0,1\}^n$, where $n = \mu + \zeta + \rho$. Suppose $\mathcal{H}$ is a $(\mu + \zeta)$-partial hardcore function for $\mathcal{F}$. Then $\mathsf{OAEP}[\mathcal{G}, \mathcal{H}, \mathcal{F}]$ is IND-CPA. In particular, for any adversary $A = (A_1, A_2)$, there exists an adversary B such that

$$\mathbf{Adv}^{\text{ind-cpa}}_{\mathsf{OAEP}[\mathcal{G},\mathcal{H},\mathcal{F}],A}(k) \leq 2 \cdot \mathbf{Adv}^{\text{phcf}}_{\mathcal{F},\mathcal{H},B}(k) + \frac{2q}{2^{\rho}} \ ,$$

where q is the total number of RO queries made by A. The running time of B is about that of A.

PROOF IDEA. Let $c = f(s\|t)$ be the challenge ciphertext. Note that, it is unlikely that A queries r to $\mathcal{G}$, since one can build an adversary B attacking $\mathcal{H}$. Moreover, if A does not query r to $\mathcal{G}$, value s looks random and A won't be able to obtain any information about b.

PA-RO RESULT. We show another partial instantiation result modeling only $\mathcal{G}$ as a RO. Namely, we show RSA-OAEP is PA-RO if $\mathcal{F}$ is second-input extractable, and common-input extractable. Note that this does not require any assumption on $\mathcal{H}$.

Theorem 8. Let n, μ, ζ, ρ be integer parameters. Let $\mathcal{H} : \{0,1\}^{\mu+\zeta} \to \{0,1\}^{\rho}$ be a hash function family and $\mathcal{G} : \mathcal{K}_G \times \{0,1\}^{\rho} \to \{0,1\}^{\mu+\zeta}$ be a RO. Let $\mathcal{F}$ be a family of trapdoor permutations with domain $\{0,1\}^n$, where $n = \mu + \zeta + \rho$. Suppose $\mathcal{F}$ is $(\rho, \rho + \zeta)$-second input and $(\rho, \rho + \zeta)$-common input extractable. Then $\mathsf{OAEP}[\mathcal{G}, \mathcal{H}, \mathcal{F}]$ is PA-RO secure. In particular, for any adversary A, there exists an extractor Ext such that,

$$\mathbf{Adv}^{\text{pa-ro}}_{\mathsf{OAEP}[\mathcal{G},\mathcal{H},\mathcal{F}],A,\mathsf{Ext}}(k) \leq \frac{2q}{2^{\zeta}} \ .$$

where q is the total number of the extract queries made by A. The running time of Ext is about that of SIE and CIE extractors.

PROOF IDEA. Let $c = f(s\|t)$ be the extract query made by A. If there is a prior query r to $\mathcal{G}$, then one with knowledge of $\mathcal{G}(r)|_{\zeta}$ could use SIE or CIE extractor to extract message m. Otherwise, the challenge c is invalid whp, since the ζ-lsb of $\mathcal{G}(H(K_H, s) \oplus t)$ and s are not equal whp.

4 A Hierarchy of Extractability Notions

Intuitively, extractability of a function formalizes the idea that an adversary that produces a point in the image must "know" a corresponding preimage, as there being a non-blackbox extractor that produces one. Previous work on extractability starting with [26, 27] considers a "one-shot" adversary. Inspired by the related notion of plaintext awareness for encryption schemes [4, 8], we define a hierarchy of extractability notions called EXT0, EXT1, EXT2, and EXT-RO, which will in particular be useful for our full instantiation results. Even our notion of EXT0 generalizes prior work, as explained below.

EXT FUNCTIONS. Let η, ζ, μ be integer parameters. Let $\mathcal{H} : \mathcal{K}_H \times \mathsf{HDom} \to \mathsf{HRng}$ be a hash function family. For $\mathrm{EXTI} \in \{\mathrm{EXT0}, \mathrm{EXT1}, \mathrm{EXT2}\}$, we associate the experiment in Fig. 6 to an adversary A and extractor Ext, for every $k \in \mathbb{N}$. For any key independent auxiliary input $z \in \{0,1\}^\eta$, we define

$$\begin{aligned}&\mathbf{Adv}^{(\eta,\mu)\text{-exti}_\zeta}_{\mathcal{H},\mathcal{F},A,\mathsf{Ext},z}(k)\\ &= \Pr_{\substack{K_H \leftarrow\!\!\$\, \mathcal{K}_H(1^k)\\ r \leftarrow\!\!\$\, \mathsf{Coins}(k)}}\left[\begin{array}{c}(\mathbf{x},\mathbf{y}) \leftarrow \mathrm{EXTI}^{A,\mathcal{E},z}_{\mathcal{H},\mathcal{F}}(K_H, r)\\ \exists i, \exists x : H(K_H, x)|_\zeta = \mathbf{y}[i] \wedge \mathbf{x}[i]|_\mu = x|_\mu \wedge H(K_H, \mathbf{x}[i])|_\zeta \neq \mathbf{y}[i]\end{array}\right]\end{aligned}$$

We define the EXTI advantage of A to be $\mathbf{Adv}^{(\eta,\mu)\text{-exti}_\zeta}_{\mathcal{H},\mathcal{F},A,\mathsf{Ext}}(k) = \max_{z \in \{0,1\}^\eta} \mathbf{Adv}^{(\eta,\mu)\text{-exti}_\zeta}_{\mathcal{H},\mathcal{F},A,\mathsf{Ext},z}(k)$. If EXTI = EXT1, then $\mathcal{O} = \varepsilon$. Note that, in EXT1 definition, adversary A have only access to extract oracle $\mathcal{E}$. EXT0 is defined similarly to EXT1, except A is only allowed to make a single extract query. If EXTI = EXT2, then $\mathcal{O} = \mathcal{I}$, where $\mathcal{I}$ is an image oracle. We say $\mathcal{H}$ is (η, μ)-EXTI$_\zeta$ if for any PPT adversary A with coin space Coins, there exists a stateful extractor $\mathcal{E}$ such that $\mathbf{Adv}^{(\eta,\mu)\text{-exti}_\zeta}_{\mathcal{H},\mathcal{F},A,\mathsf{Ext}}(k)$ is negligible in k.

Similarly, we define the analogous notion (η, μ)-EXTI$^\zeta$ where the adversary outputs the ζ *most* significant bits of the image point. We often write η-EXTI$_\zeta$ and η-EXTI$^\zeta$ instead of $(\eta, 0)$-EXTI$_\zeta$ and $(\eta, 0)$-EXTI$^\zeta$, respectively. We also often write (η, μ)-EXTI instead of (η, μ)-EXTI$_\zeta$ when $\zeta = \log|\mathsf{HRng}|$.

We generalized the notion of extractable functions in two ways. First, the extractor should work when the adversary outputs ζ least significant bits of an image point and μ bits of a preimage, given η bits of auxiliary information. Previous work considered $\zeta = \log|\mathsf{HRng}|$ and $\mu = 0$. Next, we give a definition of "many-times" extractability. We note that a central open problem in the theory of extractable functions to construct a "many-times" extractable function from a "one-time" extractable function, see *e.g.* [41]; the obvious approach suffers an extractor "blow-up" issue. For practical purposes, we simply formalize and assume this property for an appropriate construction from cryptographic hashing.

In the EXT2 notion, we extend the definition of EXT1 and give the adversary access to an oracle $\mathcal{I}$ that outputs the function evaluation of a random point from its domain along with an uninvertible hint about the corresponding preimage

```
Game $\mathrm{EXTI}^{A,\mathcal{E},z}_{\mathcal{H},\mathcal{F}}(K_H, r)$
    $i \leftarrow 1$ ; $j \leftarrow 1$ ; $st \leftarrow \varepsilon$
    $\mathbf{x} \leftarrow \varepsilon$ ; $\mathbf{y} \leftarrow \varepsilon$ ; $\mathbf{h} \leftarrow \varepsilon$
    $\mathbf{h}_1 \leftarrow \varepsilon$ ; $\mathbf{w} \leftarrow \varepsilon$
    $(f, f^{-1}) \leftarrow_{\$} \mathsf{Kg}(1^k)$
    Run $A^{\mathcal{E}(\cdot,\cdot),\mathcal{O}}(K_H, f, z; r)$
    Return $(\mathbf{x}, \mathbf{y})$

Procedure $\mathcal{E}(x_2, y)$
    If $y \in \mathbf{h}_1$ then return $\perp$
    $(st, x_1) \leftarrow \mathsf{Ext}(st, K_H, f, z, \mathbf{h}, \mathbf{w}, x_2, y; r)$
    $\mathbf{x}[i] \leftarrow x_1 \| x_2$ ; $\mathbf{y}[i] \leftarrow y$ ; $i \leftarrow i + 1$
    Return $x_1$

Procedure $\mathcal{I}(1^k)$
    $v \leftarrow_{\$} \mathsf{HDom}(k)$ ; $h \leftarrow H(K_H, v)$
    $\mathbf{h}[j] \leftarrow h$ ; $\mathbf{w}[j] \leftarrow f(v)$ ; $\mathbf{h}_1[j] \leftarrow h|_\zeta$ ; $j \leftarrow j + 1$
    Return $(h, f(v))$
```

Fig. 6: **Game to define EXTI security.**

(We also consider EXT2 notion without a hint, where the uninvertable hint is an empty function). The adversary is not allowed to query any such point to the extract oracle $\mathcal{E}$. In other words, this is a form of extractability with key dependent auxiliary information that parallels PA2 for encryption schemes. Note that we avoid the impossibility result of [13] since in all of our EXT definitions, we consider only bounded independent auxiliary information.

EXT-RO FUNCTIONS. Finally, we give a notion of extractability in the RO model, inspired by PA-RO for encryption schemes. In particular, here the adversary has access to an oracle F to which it queries a sampling algorithm, the oracle returning the image of a point in the domain sampled accordingly. Moreover, instead of the adversary's random coins the extractor gets a transcript of its RO queries and responses, but *not* those made by F. Due to space constraints, we refer to the full version for the complete definition.

PLAUSIBILITY. We typically use EXT notions in tandem with other properties such as collision-resistance. In terms of feasibility, there are several constructions proposed for EXT0 with $\zeta = \log|\mathsf{HRng}|$ and $\mu = 0$ and collision-resistance in [52] based on knowledge assumptions. (In the weaker case of EXT0 with only one-wayness, which does not suffice for us, the notion is actually achievable for these parameters under standard assumptions [13].) However, for our generalizations and notions of EXT1, EXT2, we are not aware of any constructions in the standard model. Despite the fact that they are difficult to judge, it may be a reality that as a community we need to move to such assumptions in order to make progress on some difficult problems. A similar strategy was used for very different goals by Pandey *et al.* [54]. It would be interesting for future work to explore relations between our assumptions and theirs.

5 Results for Padding Schemes and OAEP

We abstract properties of the OAEP padding scheme and prove them based on corresponding notions for the round functions. Namely, we study near-collision resistance, $\mathrm{EXT0}_{\zeta+\rho}$, $\mathrm{EXT1}^{\mu+\zeta}$ and $(\zeta+\rho)$-EXT-RO. In particular, note that while the OAEP padding scheme is invertible these notions are non-trivial because we consider adversaries that only produce part of the output. Proving the other notions, $\text{EXT1}_{\zeta+\rho}$, $\text{EXT2}^{\mu+\zeta}$ and $\text{EXT2}_{\zeta+\rho}$, in the standard model based on assumptions on the round functions remains open. However, they could be justified as assumptions by the fact that OAEP is $(\zeta+\rho)$-EXT-RO, similarly to showing a RO is UCE [5, Section 6.1]. Due to space constraints, these are shown in the full version.

6 Full Instantiation Results for s-Clear RSA-OAEP

In this section, we give full instantiation results for s-clear RSA-OAEP. Note that we are the first to consider this variant. We show that s-clear is IND-CCA2 if $\mathcal{G}$ is a pseudorandom generator, near-collision resistant, and "many-times" extractable with dependent auxiliary information, $\mathcal{H}$ is collision-resistant, and $\mathcal{F}$ meets novel "XOR-nonmalleability" and "XOR-indistinguishability" notions that seem plausible for RSA. Also note that we avoid the several impossibility results here. First, we avoid the impossibility result of [58] by using XOR-nonmalleability of $\mathcal{F}$. Second, we avoid the impossibility result of [13] since the dependent auxiliary information is bounded.

6.1 XOR Assumptions on Trapdoor Permutations and RSA

Here, we give classes of novel assumptions on RSA (and trapdoor permutations in general), which are stronger than one-wayness and needed for RSA-OAEP s-clear.

XOR-IND. Our first class of assumptions speaks to the fact that addition or XOR operations "break up" the multiplicative structure of RSA. Indeed, in a related context of arithmetic progressions on $\mathbb{Z}_N$ we have seen formal evidence of this [51, 60]. It is interesting for future work to give formal evidence in our case as well. Let $\mathcal{F} = (\mathsf{Kg}, \mathsf{Eval}, \mathsf{Inv})$ be a trapdoor permutation family with domain TDom. Let $\mathcal{G} : \mathcal{K}_G \times \mathsf{TDom} \to \mathsf{GRng}$ be a function family. For $\text{ATK} \in \{\text{IND0}, \text{IND1}, \text{IND2}\}$, we associate the experiment in Fig. 7, for every $k \in \mathbb{N}$. Define the xor-atk advantage of A against $\mathcal{F}$ with the hint function family $\mathcal{G}$

$$\mathbf{Adv}^{\text{xor-atk}}_{\mathcal{F},\mathcal{G},A}(k) = 2 \cdot \Pr\left[\text{XOR-ATK}^{A}_{\mathcal{F},\mathcal{G}}(k) \Rightarrow 1\right] - 1 \ .$$

If $\text{atk} = \text{ind0}$, then $\mathcal{O} = \varepsilon$. We say that $\mathcal{F}$ is XOR-IND0 with respect to hint function family $\mathcal{G}$ if for every PPT attacker A, $\mathbf{Adv}^{\text{xor-ind0}}_{\mathcal{F},\mathcal{G},A}(k)$ is negligible in k. Similarly, if $\text{atk} = \text{ind1}$, then $\mathcal{O} = \mathcal{C}$, where $\mathcal{C}$ is a relation checker oracle that on input y_1, y_2 and ω outputs 1, if $\omega = f^{-1}(y_1) \oplus f^{-1}(y_2)$, otherwise outputs 0. Similarly, if $\text{atk} = \text{ind2}$, then $\mathcal{O} = \mathcal{V}_\ell$, where $\mathcal{V}_\ell$ is an ℓ-bit image verifier oracle that on input y outputs 1, if there exists x such that $y = G(K_G, x)|_\ell$, otherwise outputs 0. Note that A is not allowed to query for the challenge to $\mathcal{V}$. We say that $\mathcal{F}$ is XOR-IND1 (resp. XOR-IND2_ℓ) with respect to hint function family $\mathcal{G}$ if for every PPT attacker A, $\mathbf{Adv}^{\text{xor-ind1}}_{\mathcal{F},\mathcal{G},A}(k)$ (resp. $\mathbf{Adv}^{\text{xor-ind2}_\ell}_{\mathcal{F},\mathcal{G},A}(k)$) is negligible in k.

```
Game XOR-ATK$^A_{\mathcal{F},\mathcal{G}}(k)$
$b \leftarrow\!\!\$ \{0,1\}$ ; $(f, f^{-1}) \leftarrow \mathsf{Kg}(1^k)$
$K_G \leftarrow \mathcal{K}_G(1^k)$ ; $x \leftarrow\!\!\$ \mathsf{TDom}(k)$
$(state, z) \leftarrow\!\!\$ A_1(f, K_G, G(K_G, x))$
$y_0 \leftarrow f(x)$ ; $y_1 \leftarrow f(x \oplus z)$
$b' \leftarrow\!\!\$ A_2^{\mathcal{O}}(state, y_b)$
Return $(b = b')$
```

Fig. 7: **Games to define XOR-ATK security.**

Observe that the hint is *crucial*, as otherwise the assumption would trivially hold. In our results, $\mathcal{G}$ is a PRG. In this case, we show that $\mathcal{G}$ is also a HCF function for $\mathcal{F}$. In other words, the assumption in our use-case can be viewed an extension of the classical notion of HCF — $\mathcal{G}$ is "robust" not in the sense of [40], but in the sense that the view of the adversary is also indistinguishable given $\mathcal{F}$ applied to either the real input or *related one*. Note that not all hardcore functions have this property, even when $\mathcal{F}$ is partial one-way. For example, consider a hardcore function $\mathcal{G}$ that reveals first bit of its input x. Then if a partial one-way function $\mathcal{F}$ also reveals the first bit of x, XOR-indistinguishability clearly does not hold.

Theorem 9. Let $\mathcal{F}$ be a family of one-way trapdoor permutations with domain TDom. Suppose $\mathcal{G} : \mathcal{K}_G \times \mathsf{TDom} \to \mathsf{GRng}$ is a pseudorandom generator and $\mathcal{F}$ is XOR-IND0 with respect to hint function family $\mathcal{G}$. Then $\mathcal{G}$ is a hardcore function for $\mathcal{F}$ on the uniform distribution. In particular, for any adversary A, there are adversaries B, C such that

$$\mathbf{Adv}^{\mathrm{hcf}}_{\mathcal{F},\mathcal{G},U,A}(k) \leq 2 \cdot \mathbf{Adv}^{\mathrm{xor\text{-}ind0}}_{\mathcal{F},\mathcal{G},B}(k) + 2 \cdot \mathbf{Adv}^{\mathrm{prg}}_{\mathcal{G},C}(k) \ .$$

XOR-NM0. Our second class of assumptions speak to the fact that RSA is non-malleable wrt. XOR. Intuitively, if RSA was XOR malleable, then since it is multiplicatively homomorphic it would be (something like) fully homomorphic, which is unlikely. (Although we do not claim the exact formulation of our definitions imply a formal definition of fully homomorphic.) A similar argument was made by Hofheinz for a non-malleability assumption on the Paillier trapdoor permutation (which is additively homomorphic) wrt. multiplication [Assumption 4.2][44]. Let $\mathcal{F} = (\mathsf{Kg}, \mathsf{Eval}, \mathsf{Inv})$ be a trapdoor permutation family with domain TDom. To attacker A, we associate the experiment in Fig. 8 for every $k \in \mathbb{N}$. We say that $\mathcal{F}$ is XOR-NM0 if for every PPT attacker A,

$$\mathbf{Adv}^{\mathrm{xor\text{-}nm0}}_{\mathcal{F},A}(k) = \Pr\left[\,\mathrm{XOR\text{-}NM0}^A_{\mathcal{F}}(k) \Rightarrow 1\,\right] \ .$$

is negligible in k.

XOR-NM1. Let $\mathcal{F} = (\mathsf{Kg}, \mathsf{Eval}, \mathsf{Inv})$ be a trapdoor permutation family with domain TDom. Let $\mathcal{G} : \mathcal{K}_G \times \mathsf{TDom} \to \mathsf{GRng}$ be a hash function family. To

```
$\textbf{Game}$ XOR-NM0$^A_{\mathcal{F}}(k)$
$(f, f^{-1}) \leftarrow \mathsf{Kg}(1^k)$
$x \leftarrow_\$ \mathsf{TDom}(k)$
$(\omega, y') \leftarrow_\$ A(f, f(x))$
$x' \leftarrow f^{-1}(y')$
If $(\omega = x \oplus x') \wedge (\omega \neq 0)$
    Return 1
Else return 0
```

```
$\textbf{Game}$ XOR-NM1$^A_{\mathcal{F},\mathcal{G}}(k)$
$(f, f^{-1}) \leftarrow \mathsf{Kg}(1^k)$ ; $K_G \leftarrow \mathcal{K}_G(1^k)$
$x \leftarrow_\$ \mathsf{TDom}(k)$ ; $z \leftarrow G(K_G, x)$
$(\alpha, st) \leftarrow_\$ A_1(f, K_G, z)$
$(\omega, y') \leftarrow_\$ A_2(st, f(x \oplus \alpha))$
$x' \leftarrow f^{-1}(y')$
If $(\omega \oplus \alpha = x \oplus x') \wedge (\omega \neq 0)$ then return 1
Else return 0
```

Fig. 8: **Games to define XOR-NM security.**

attacker A, we associate the experiment in Fig. 8 for every $k \in \mathbb{N}$. We say that $\mathcal{F}$ is XOR-NM1 with respect to $\mathcal{G}$ if for every PPT attacker A,

$$\mathbf{Adv}^{\text{xor-nm1}}_{\mathcal{F},\mathcal{G},A}(k) = \Pr\left[\, \text{XOR-NM1}^A_{\mathcal{F},\mathcal{G}}(k) \Rightarrow 1 \,\right] \ .$$

is negligible in k.

Relations between definitions. Interestingly, we show XOR-NM0 and XOR-IND1 together imply XOR-NM1.

Theorem 10. Let $\mathcal{F} = (\mathsf{Kg}, \mathsf{Eval}, \mathsf{Inv})$ be a trapdoor permutation family with domain TDom. Let $\mathcal{G} : \mathcal{K}_G \times \mathsf{TDom} \to \mathsf{GRng}$ be a function family. Suppose $\mathcal{F}$ is XOR-NM0 and XOR-IND1 with respect to $\mathcal{G}$. Then, $\mathcal{F}$ is XOR-NM1 with respect to $\mathcal{G}$. In particular, for any adversary A, there are adversaries B, C such that

$$\mathbf{Adv}^{\text{xor-nm1}}_{\mathcal{F},\mathcal{G},A}(k) \leq \mathbf{Adv}^{\text{xor-nm0}}_{\mathcal{F},\mathcal{G},B}(k) + 2 \cdot \mathbf{Adv}^{\text{xor-ind1}}_{\mathcal{F},\mathcal{G},C}(k) \ .$$

Discussion. We caution that these are new assumptions and must be treated with care, although they have some intuitive appeal as discussed where they are introduced. It would be interesting for future work to establish theoretical constructions meeting them or show that RSA meets them under more well-studied assumptions.

6.2 Main Results

After establishing its security in the RO model, we show that s-clear RSA-OAEP is IND-CCA1 and IND-CCA2 under respective suitable assumptions. As in Section 3 we actually prove corresponding notions of IND-CPA + PA, yielding stronger results. The results in Section follow from those below.

IND-CCA2 result in RO model. First, note that the partial one-wayness result of [39] does not apply to this variant, and in fact the negative result of [59] *does* apply, demonstrating that one-wayness of the trapdoor permutation is not enough for the scheme to achieve IND-CCA2 security *even in the RO model*. We show that XOR-nonmalleability is sufficient.

Theorem 11. Let μ, ζ, ρ be integer parameters. Let $\mathcal{F}$ be a XOR-NM0 family of one-way trapdoor permutations with domain $\{0,1\}^{\rho}$. Suppose $\mathcal{G} : \mathcal{K}_G \times \{0,1\}^{\rho} \to \{0,1\}^{\mu+\zeta}$ is a RO and $\mathcal{H} : \mathcal{K}_H \times \{0,1\}^{\mu+\zeta} \to \{0,1\}^{\rho}$ is collision-resistant. Then $\mathsf{OAEP}_{\mathsf{s\text{-}clear}}[\mathcal{G}, \mathcal{H}, \mathcal{F}|^{\mu+\zeta}]$ is IND-CCA2 secure in the random oracle model. In particular, for any adversary A, there are adversaries B, C such that

$$\mathbf{Adv}^{\text{ind-cca2}}_{\mathsf{OAEP}_{\mathsf{s\text{-}clear}},A}(k) \leq \frac{2q}{2^{\rho}} + \frac{4p}{2^{\zeta}} + 2 \cdot \mathbf{Adv}^{\text{cr}}_{\mathcal{H},C}(k) + 4 \cdot \mathbf{Adv}^{\text{xor-nm0}}_{\mathcal{F},B}(k) \ .$$

where p is the number of decryption-oracle queries of A and q is the total number of random-oracle queries of A and $\mathcal{M}$. Adversary B and C makes at most q random-oracle queries.

IND-CCA1 RESULT. To prove IND-CCA1, we use EXT1 and near-collision resistance of the overall OAEP padding scheme (which follows from assumptions on the round functions as per Section 5), as well as the assumption that $\mathcal{G}$ is a pseudorandom generator and $\mathcal{F}$ is XOR-IND (as defined in Section 6.1).

Theorem 12. Let η, μ, ζ, ρ be integer parameters. Let $\mathcal{F}$ be a family of trapdoor permutations with domain $\{0,1\}^{\mu}$, and let $\eta = |[\mathsf{Kg}(1^k)]|$. 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 function families. Suppose $\mathcal{G}$ is a pseudorandom generator, and let $\mathcal{F}$ is XOR-IND0 with respect to hint function $\mathcal{G}$ (as defined in Section 6.1). Also suppose $\mathsf{OAEP}[\mathcal{G}, \mathcal{H}]$ is η-EXT1$^{\mu+\zeta}$ and NCR$^{\mu+\zeta}$. Then $\mathsf{OAEP}_{\mathsf{s\text{-}clear}}[\mathcal{G}, \mathcal{H}, \mathcal{F}|^{\mu+\zeta}]$ is IND-CCA1 secure. In particular, for any adversary A that makes q decryption queries, there exist adversaries C, D, E, and EXT1 adversary B that makes q extract queries such that for all extractors Ext,

$$\mathbf{Adv}^{\text{ind-cca1}}_{\mathsf{OAEP}_{\mathsf{s\text{-}clear}},A}(k) \leq 2 \cdot \mathbf{Adv}^{\eta\text{-ext1}^{\mu+\zeta}}_{\mathsf{OAEP}[\mathcal{G},\mathcal{H}],B,\mathsf{Ext}}(k) + 2 \cdot \mathbf{Adv}^{\text{n-cr}^{\mu+\zeta}}_{\mathsf{OAEP}[\mathcal{G},\mathcal{H}],C}(k)$$
$$+6 \cdot \mathbf{Adv}^{\text{xor-ind0}}_{\mathcal{F},\mathcal{G},D}(k) + 4 \cdot \mathbf{Adv}^{\text{prg}}_{\mathcal{G},E}(k) \ .$$

IND-CCA2 RESULT. To prove IND-CCA2, we use EXT2 and near-collision resistance of $\mathcal{G}$, as well as the assumptions that $\mathcal{G}$ is a pseudorandom generator, $\mathcal{H}$ is collision-resistant and $\mathcal{F}$ is XOR-IND and XOR-NM (as defined in Section 6.1). Note that, EXT2 adversary only makes one image query. Thus, the dependent auxiliary information is bounded by the size of the image.

Theorem 13. Let η, μ, ζ, ρ be integer parameters. Let $\mathcal{F}$ be a family of trapdoor permutations with domain $\{0,1\}^{\mu}$ and $\eta = |[\mathsf{Kg}(1^k)]| + |[\mathcal{K}_H(1^k)]|$. 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 function families. Suppose $\mathcal{G}$ is PRG, NCR$_{\zeta}$, EXT2$_{\zeta}$ and η-EXT2$_{\zeta}$ with respect to $\mathcal{F}$, and $\mathcal{H}$ is collision-resistant. Suppose $\mathcal{F}$ is XOR-NM0, XOR-IND1 and XOR-IND2$_{\zeta}$ with respect to $\mathcal{G}$. Then $\mathsf{OAEP}_{\mathsf{s\text{-}clear}}[\mathcal{G}, \mathcal{H}, \mathcal{F}|^{\mu+\zeta}]$ is IND-CCA2 secure. In particular, for any adversary A that makes q decryption queries, there exists adversaries $C_H, C_G, D_1, D_2, D_3, E$, and adversary B_1, B_2 that makes q extract queries such that for all extractors $\mathsf{Ext}_1, \mathsf{Ext}_2$,

$$\begin{aligned}\mathbf{Adv}^{\text{ind-cca2}}_{\mathsf{OAEP}_{\mathsf{s\text{-}clear}},A}(k) \leq{} & 6 \cdot \mathbf{Adv}^{\eta\text{-ext2}_\zeta}_{\mathcal{G},\mathcal{F},B_1,\mathsf{Ext}_1}(k) + 18 \cdot \mathbf{Adv}^{\text{xor-ind2}_\zeta}_{\mathcal{F},\mathcal{G},D_1}(k) \\ & + 10 \cdot \mathbf{Adv}^{\text{n-cr}_\zeta}_{\mathcal{G},C_G}(k) + 4 \cdot \mathbf{Adv}^{\text{cr}}_{\mathcal{H},C_H}(k) + 4 \cdot \mathbf{Adv}^{\text{xor-nm0}}_{\mathcal{F},\mathcal{G},D_3}(k) \\ & + 14 \cdot \mathbf{Adv}^{\text{xor-ind1}}_{\mathcal{F},\mathcal{G},D_2}(k) + 16 \cdot \mathbf{Adv}^{\text{prg}}_{\mathcal{G},E}(k) + 24 \cdot \mathbf{Adv}^{\text{ext2}_\zeta}_{\mathcal{G},B_2,\mathsf{Ext}_2}(k)\end{aligned}$$

Efficiency. The ciphertext length is $2n + k + \mu$ where n is the length of the RSA modulus, k is the security parameter, and μ is the message length. For example, if $n = 2048$, $k = 128$, and we encrypt an AES key with $\mu = 128$ (*i.e.*, we use RSA-OAEP as a key encapsulation mechanism, which is typical in practice then the ciphertext length is 4352). It is interesting to compare this with the standard model IND-CCA2 secure key encapsulation mechanism of Kiltz *et al.* [45]. They describe their scheme based on modular squaring (factoring), but it is straightforward to derive a scheme based on RSA with large hardcore function and a cryptographic hash function being target collision-resistant, which results in the most efficient prior standard-model RSA-based encryption scheme we are aware of. It performs one "small" exponentiation wrt. e and one "full" exponentiation modulo N, so is much more computationally expensive than our scheme. Thus, one could arguably say ours is the most computationally efficient RSA-based encryption scheme under "plausible standard-model assumptions" (where one takes the liberty of making bold assumptions on cryptographic hash functions) to date. On the other hand, the scheme of [45] has ciphertext length only $2n$.

Remark 14. It is worth mentioning why we are able to get IND-CCA2 (*i.e.*, adaptive) security for s-clear RSA-OAEP but not t-clear. The point is that, in the t-clear setting, it is not even clear how to define EXT2 of OAEP in a useful way. Since OAEP is invertible, the image oracle should output only *part* of the image point. But then it is not clear how the EXT2 adversary against OAEP can simulate the encryption oracle for the PA2 adversary against t-clear RSA-OAEP. On the other hand, for EXT2 of $\mathcal{G}$, the image oracle can output the *full* image point since $\mathcal{G}$ is not invertible. This then allows proving that s-clear RSA-OAEP is PA2 directly (without using monolithic assumptions on the padding scheme not known to follow from assumptions on the round functions).

6.3 IND-CPA, PA0 and PA1 Result

We show that s-clear RSA-OAEP is IND-CPA secure under suitable assumptions. Then, we show either PA0, PA1 and PA2 security depending on the strength of assumptions on $\mathcal{G}, \mathcal{H}$ and $\mathcal{F}$. Interestingly, even our IND-CPA result uses an XOR-based assumption on the trapdoor permutation. We also give a full instantiation result for s-clear RSA-OAEP and show that it is PA0 and PA1 under suitable assumptions. We show that s-clear RSA-OAEP "inherits" the extractability of the underlying padding transform, in the form of PA1 and

EXT1, as long as the latter is also near-collision resistant. Here we state the result for an abstract padding scheme rather than specifically for OAEP. Note that results for OAEP then follow from the round functions as per Section 5. Due to space constraints, these are shown in the full version.

6.4 PA2 Result

We give a full instantiation result for s-clear RSA-OAEP and show that it is PA2 under stronger assumptions on $\mathcal{G}, \mathcal{H}$ and $\mathcal{F}$. We note that we can reduce assumptions as per Theorem 10.

Theorem 15. Let η, μ, ζ, ρ be integer parameters. Let $\mathcal{F}$ be a family of trapdoor permutations with domain $\{0,1\}^\rho$. 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. Let $\eta = |[\mathsf{Kg}(1^k)]| + |[\mathcal{K}_H(1^k)]|$. Suppose $\mathcal{G}$ is PRG, NCR$_\zeta$, EXT2$_\zeta$ and η-EXT2$_\zeta$ with respect to $\mathcal{F}$ and $\mathcal{H}$ is collision-resistant. Suppose $\mathcal{F}$ is XOR-NM1 and XOR-IND2$_\zeta$ with respect to $\mathcal{G}$. Then $\mathsf{OAEP}_{\mathsf{s\text{-}clear}}[\mathcal{G}, \mathcal{H}, \mathcal{F}|^{\mu+\zeta}]$ is PA2 secure. In particular, for any adversary A that makes at most q decryption queries and p encryption queries, there are extractor Ext, adversaries B_F, B_G, B_H, C, D, adversary A_G, C_G that makes at most q extract queries and p image queries such that for all extractors $\mathsf{Ext}_G, \mathsf{Ext}'_G$

$$\begin{aligned}\mathbf{Adv}^{\mathrm{pa2}}_{\mathsf{OAEP}_{\mathsf{s\text{-}clear}}, A, \mathsf{Ext}}(k) \le\ & 3 \cdot \mathbf{Adv}^{\eta\text{-}\mathrm{ext2}_\zeta}_{\mathcal{G}, \mathcal{F}, A_G, \mathsf{Ext}_G}(k) + 9p \cdot \mathbf{Adv}^{\mathrm{xor\text{-}ind2}_\zeta}_{\mathcal{F}, \mathcal{G}, C}(k) \\ & + 6p \cdot \mathbf{Adv}^{\mathrm{prg}}_{\mathcal{G}, D}(k) + 12p \cdot \mathbf{Adv}^{\mathrm{ext2}_\zeta}_{\mathcal{G}, C_G, \mathsf{Ext}'_G}(k) \\ & + 5 \cdot \mathbf{Adv}^{\mathrm{n\text{-}cr}_\zeta}_{\mathcal{G}, B_G}(k) + 2 \cdot \mathbf{Adv}^{\mathrm{cr}}_{\mathcal{H}, B_H}(k) + 2p \cdot \mathbf{Adv}^{\mathrm{xor\text{-}nm1}}_{\mathcal{F}, \mathcal{G}, B_F}(k)\end{aligned}$$

PROOF IDEA. Let $c = (s, y)$ be the random ciphertext that A obtains from it's encryption oracle. Let $c' = (s', y')$ be the extract query made by A. Note that if $s|_\zeta \neq s'|_\zeta$ then we use Ext_G on input $s|_\zeta$ to recover r and then m. Note that if $s|_\zeta = s'|_\zeta$ then there is 2 cases. First, if $y = y'$ then we can find collision on $\mathcal{H}$. Next, if $y \neq y'$ then we can build an XOR-NM adversary. Note that, there are two obstacles in the proof. First, EXT2 adversary need to simulate the encryption oracle for PA2 adversary using its image oracle. Moreover, PA2 adversary may query for the key-dependent messages to the encryption oracle. We were able to enable EXT2 adversary to simulate the encryption oracle assuming $\mathcal{G}$ is PRG and EXT2.

Acknowledgments

We thank the PKC reviewers for their insightful comments. Mohammad Zaheri was partially supported by NSF grant No. 1565387, No. 1149832 and No. 1718498.

References

1. P. Baecher, M. Fischlin, and D. Schröder. Expedient non-malleability notions for hash functions. In A. Kiayias, editor, *CT-RSA 2011*, volume 6558 of *LNCS*, pages 268–283, San Francisco, CA, USA, Feb. 14–18, 2011. Springer, Heidelberg, Germany.
2. B. Barak. How to go beyond the black-box simulation barrier. In *42nd FOCS*, pages 106–115, Las Vegas, NV, USA, Oct. 14–17, 2001. IEEE Computer Society Press.
3. G. Barthe, D. Pointcheval, and S. Zanella Béguelin. Verified security of redundancy-free encryption from rabin and rsa. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, CCS '12, pages 724–735, New York, NY, USA, 2012. ACM.
4. M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway. Relations among notions of security for public-key encryption schemes. In H. Krawczyk, editor, *CRYPTO'98*, volume 1462 of *LNCS*, pages 26–45, Santa Barbara, CA, USA, Aug. 23–27, 1998. Springer, Heidelberg, Germany.
5. 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, Santa Barbara, CA, USA, Aug. 18–22, 2013. Springer, Heidelberg, Germany.
6. M. Bellare, V. T. Hoang, and S. Keelveedhi. Cryptography from compression functions: The UCE bridge to the ROM. In J. A. Garay and R. Gennaro, editors, *CRYPTO 2014, Part I*, volume 8616 of *LNCS*, pages 169–187, Santa Barbara, CA, USA, Aug. 17–21, 2014. Springer, Heidelberg, Germany.
7. 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.
8. M. Bellare and A. Palacio. Towards plaintext-aware public-key encryption without random oracles. In P. J. Lee, editor, *ASIACRYPT 2004*, volume 3329 of *LNCS*, pages 48–62, Jeju Island, Korea, Dec. 5–9, 2004. Springer, Heidelberg, Germany.
9. 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.
10. M. Bellare and P. Rogaway. Optimal asymmetric encryption. In A. D. Santis, editor, *EUROCRYPT'94*, volume 950 of *LNCS*, pages 92–111, Perugia, Italy, May 9–12, 1994. Springer, Heidelberg, Germany.
11. M. Bellare and P. Rogaway. The exact security of digital signatures: How to sign with RSA and Rabin. In U. M. Maurer, editor, *EUROCRYPT'96*, volume 1070 of *LNCS*, pages 399–416, Saragossa, Spain, May 12–16, 1996. Springer, Heidelberg, Germany.
12. N. Bitansky, R. Canetti, A. Chiesa, and E. Tromer. From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again. In S. Goldwasser, editor, *ITCS 2012*, pages 326–349, Cambridge, MA, USA, Jan. 8–10, 2012. ACM.
13. N. Bitansky, R. Canetti, O. Paneth, and A. Rosen. On the existence of extractable one-way functions. In D. B. Shmoys, editor, *46th ACM STOC*, pages 505–514, New York, NY, USA, May 31 – June 3, 2014. ACM Press.
14. N. Bitansky, R. Canetti, O. Paneth, and A. Rosen. On the existence of extractable one-way functions. *SIAM Journal on Computing*, 45(5):1910–1952, 2016.

15. 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, Aarhus, Denmark, May 22–26, 2005. Springer, Heidelberg, Germany.
16. A. Boldyreva, D. Cash, M. Fischlin, and B. Warinschi. Foundations of non-malleable hash and one-way functions. In M. Matsui, editor, *ASIACRYPT 2009*, volume 5912 of *LNCS*, pages 524–541, Tokyo, Japan, Dec. 6–10, 2009. Springer, Heidelberg, Germany.
17. 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, Santa Barbara, CA, USA, Aug. 14–18, 2005. Springer, Heidelberg, Germany.
18. 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, Shanghai, China, Dec. 3–7, 2006. Springer, Heidelberg, Germany.
19. A. Boldyreva, H. Imai, and K. Kobara. How to strengthen the security of RSA-OAEP. *IEEE Trans. Information Theory*, 56(11):5876–5886, 2010.
20. D. Boneh. Simplified OAEP for the RSA and Rabin functions. In J. Kilian, editor, *CRYPTO 2001*, volume 2139 of *LNCS*, pages 275–291, Santa Barbara, CA, USA, Aug. 19–23, 2001. Springer, Heidelberg, Germany.
21. D. Boneh and M. K. Franklin. Identity based encryption from the Weil pairing. *SIAM Journal on Computing*, 32(3):586–615, 2003.
22. D. R. L. Brown. A weak-randomizer attack on rsa-oaep with e = 3, 2005.
23. C. Brzuska, P. Farshim, and A. Mittelbach. Indistinguishability obfuscation and UCEs: The case of computationally unpredictable sources. In J. A. Garay and R. Gennaro, editors, *CRYPTO 2014, Part I*, volume 8616 of *LNCS*, pages 188–205, Santa Barbara, CA, USA, Aug. 17–21, 2014. Springer, Heidelberg, Germany.
24. 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.
25. R. Canetti, Y. Chen, and L. Reyzin. On the correlation intractability of obfuscated pseudorandom functions. In *Theory of Cryptography - 13th International Conference, TCC*, pages 389–415, 2016.
26. R. Canetti and R. R. Dakdouk. Extractable perfectly one-way functions. In L. Aceto, I. Damgård, L. A. Goldberg, M. M. Halldórsson, A. Ingólfsdóttir, and I. Walukiewicz, editors, *ICALP 2008, Part II*, volume 5126 of *LNCS*, pages 449–460, Reykjavik, Iceland, July 7–11, 2008. Springer, Heidelberg, Germany.
27. R. Canetti and R. R. Dakdouk. Towards a theory of extractable functions. In O. Reingold, editor, *TCC 2009*, volume 5444 of *LNCS*, pages 595–613. Springer, Heidelberg, Germany, Mar. 15–17, 2009.
28. R. Canetti, O. Goldreich, and S. Halevi. The random oracle methodology, revisited. *J. ACM*, 51(4):557–594, 2004.
29. R. Canetti, D. Micciancio, and O. Reingold. Perfectly one-way probabilistic hash functions (preliminary version). In *30th ACM STOC*, pages 131–140, Dallas, TX, USA, May 23–26, 1998. ACM Press.
30. D. Coppersmith. Finding a small root of a univariate modular equation. In *Proceedings of the 15th Annual International Conference on Theory and Application of Cryptographic Techniques*, EUROCRYPT'96, pages 155–165, Berlin, Heidelberg, 1996. Springer-Verlag.

31. J.-S. Coron, A. Kirichenko, and M. Tibouchi. A note on the bivariate Coppersmith theorem. *Journal of Cryptology*, 26(2):246–250, Apr. 2013.
32. D. Dachman-Soled, R. Gennaro, H. Krawczyk, and T. Malkin. Computational extractors and pseudorandomness. In R. Cramer, editor, *TCC 2012*, volume 7194 of *LNCS*, pages 383–403, Taormina, Sicily, Italy, Mar. 19–21, 2012. Springer, Heidelberg, Germany.
33. I. Damgård. Towards practical public key systems secure against chosen ciphertext attacks. In J. Feigenbaum, editor, *CRYPTO'91*, volume 576 of *LNCS*, pages 445–456, Santa Barbara, CA, USA, Aug. 11–15, 1991. Springer, Heidelberg, Germany.
34. I. Damgård, S. Faust, and C. Hazay. Secure two-party computation with low communication. In R. Cramer, editor, *TCC 2012*, volume 7194 of *LNCS*, pages 54–74, Taormina, Sicily, Italy, Mar. 19–21, 2012. Springer, Heidelberg, Germany.
35. Y. Dodis, I. Haitner, and A. Tentes. On the instantiability of hash-and-sign RSA signatures. In R. Cramer, editor, *TCC 2012*, volume 7194 of *LNCS*, pages 112–132, Taormina, Sicily, Italy, Mar. 19–21, 2012. Springer, Heidelberg, Germany.
36. Y. Dodis, R. Oliveira, and K. Pietrzak. On the generic insecurity of the full domain hash. In V. Shoup, editor, *CRYPTO 2005*, volume 3621 of *LNCS*, pages 449–466, Santa Barbara, CA, USA, Aug. 14–18, 2005. Springer, Heidelberg, Germany.
37. M. Fischlin. Pseudorandom function tribe ensembles based on one-way permutations: Improvements and applications. In J. Stern, editor, *EUROCRYPT'99*, volume 1592 of *LNCS*, pages 432–445, Prague, Czech Republic, May 2–6, 1999. Springer, Heidelberg, Germany.
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, Santa Barbara, CA, USA, Aug. 19–23, 2001. Springer, Heidelberg, Germany.
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, Taormina, Sicily, Italy, Mar. 19–21, 2012. Springer, Heidelberg, Germany.
41. D. Gupta and A. Sahai. On constant-round concurrent zero-knowledge from a knowledge assumption. In *Progress in Cryptology—INDOCRYPT 2014*, pages 71–88, 2014.
42. S. Halevi, S. Myers, and C. Rackoff. On seed-incompressible functions. In R. Canetti, editor, *TCC 2008*, volume 4948 of *LNCS*, pages 19–36, San Francisco, CA, USA, Mar. 19–21, 2008. Springer, Heidelberg, Germany.
43. V. T. Hoang, J. Katz, A. O'Neill, and M. Zaheri. Selective-opening security in the presence of randomness failures. In J. H. Cheon and T. Takagi, editors, *Advances in Cryptology – ASIACRYPT 2016*, pages 278–306, Berlin, Heidelberg, 2016. Springer Berlin Heidelberg.
44. D. Hofheinz. All-but-many lossy trapdoor functions. In D. Pointcheval and T. Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 209–227, Cambridge, UK, Apr. 15–19, 2012. Springer, Heidelberg, Germany.
45. D. Hofheinz, E. Kiltz, and V. Shoup. Practical chosen ciphertext secure encryption from factoring. *Journal of Cryptology*, 26(1):102–118, Jan. 2013.
46. 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, Copenhagen, Denmark, May 11–15, 2014. Springer, Heidelberg, Germany.

47. E. Kiltz, P. Mohassel, and A. O'Neill. Adaptive trapdoor functions and chosen-ciphertext security. In H. Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 673–692, French Riviera, May 30 – June 3, 2010. Springer, Heidelberg, Germany.
48. 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.
49. 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, Cologne, Germany, Apr. 26–30, 2009. Springer, Heidelberg, Germany.
50. E. Kiltz and K. Pietrzak. Personal communication, 2019.
51. M. Lewko, A. O'Neill, and A. Smith. *Regularity of Lossy RSA on Subdomains and Its Applications*, pages 55–75. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.
52. A. C. S. G. H. L. A. R. Nir Bitansky, Ran Canetti and E. Tromer. The hunting of the SNARK. In *J. Cryptology*, volume 30, pages 989–1066, 2017.
53. 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, Shanghai, China, Dec. 3–7, 2006. Springer, Heidelberg, Germany.
54. 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.
55. 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.
56. C. Rackoff and D. R. Simon. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. In J. Feigenbaum, editor, *CRYPTO'91*, volume 576 of *LNCS*, pages 433–444, Santa Barbara, CA, USA, Aug. 11–15, 1991. Springer, Heidelberg, Germany.
57. R. L. Rivest, A. Shamir, and L. M. Adleman. A method for obtaining digital signature and public-key cryptosystems. *Communications of the Association for Computing Machinery*, 21(2):120–126, 1978.
58. V. Shoup. OAEP reconsidered. In J. Kilian, editor, *CRYPTO 2001*, volume 2139 of *LNCS*, pages 239–259, Santa Barbara, CA, USA, Aug. 19–23, 2001. Springer, Heidelberg, Germany.
59. V. Shoup. OAEP reconsidered. *Journal of Cryptology*, 15(4):223–249, 2002.
60. A. Smith and Y. Zhang. *On the Regularity of Lossy RSA*, pages 609–628. Springer Berlin Heidelberg, Berlin, Heidelberg, 2015.
61. M. Zhandry. The magic of ELFs. *J. Cryptology*, 32(3):825–866, 2019.