J Cryptol (2017) 30:889–919
DOI: 10.1007/s00145-016-9238-4

Journal of CRYPTOLOGY

Instantiability of RSA-OAEP Under Chosen-Plaintext Attack*

Eike Kiltz
Ruhr-Universität Bochum, Bochum, Germany
eike.kiltz@ruhr-uni-bochum.de
Url: http://www.kiltz.net

Adam O'Neill
Georgetown University, Washington, DC, USA
adam@cs.georgetown.edu
Url: http://www.cs.georgetown.edu/∼adam

Adam Smith
Pennsylvania State University, University Park, PA, USA
asmith@cse.psu.edu
Url: http://www.cse.psu.edu/∼asmith

Communicated by Kenneth Paterson.

Received 7 November 2011 / Revised 21 April 2016
Online publication 19 September 2016

Abstract. We show that the widely deployed RSA-OAEP encryption scheme of Bellare and Rogaway (Eurocrypt 1994), which combines RSA with two rounds of an underlying Feistel network whose hash (i.e., round) functions are modeled as random oracles, meets indistinguishability under chosen-plaintext attack (IND-CPA) in the *standard model* based on simple, non-interactive, and non-interdependent assumptions on RSA and the hash functions. To prove this, we first give a result on a more general notion called "padding-based" encryption, saying that such a scheme is IND-CPA if (1) its underlying padding transform satisfies a "fooling" condition against small-range distinguishers on a class of high-entropy input distributions, and (2) its trapdoor permutation is sufficiently *lossy* as defined by Peikert and Waters (STOC 2008). We then show that the first round of OAEP satisfies condition (1) if its hash function is t-wise independent for t roughly proportional to the allowed message length. We clarify that this result requires the hash function to be keyed, and for its key to be included in the public key of RSA-OAEP. We also show that RSA satisfies condition (2) under the Φ-Hiding Assumption of Cachin et al. (Eurocrypt 1999). This is the first *positive* result about the instantiability of RSA-OAEP. In particular, it increases confidence that chosen-plaintext attacks are unlikely to be found against the scheme. In contrast, RSA-OAEP's predecessor in PKCS #1 v1.5 was shown to be vulnerable to such attacks by Coron et al. (Eurocrypt 2000).

*A preliminary version of this paper appears in *Advances in Cryptology—CRYPTO 2010, 30th Annual International Cryptology Conference,* T. Rabin ed., LNCS, Springer, 2010. This is the full version.

Keywords. RSA, OAEP, Padding-based encryption, Lossy trapdoor functions, Left-over hash lemma, Standard model.

1. Introduction

Bellare and Rogaway [5] designed the RSA-OAEP encryption scheme as a drop-in replacement for RSA PKCS #1 v1.5 [55] with provable security. In particular, it follows the same paradigm as RSA PKCS #1 v1.5 in that it encrypts a message of less than k bits to a k-bit ciphertext (where k is the modulus length) by first applying a fast, randomized, and invertible "padding transform" to the message before applying RSA. In the case of RSA-OAEP, the underlying padding transform (which is itself called 'OAEP'[1]) embeds a message m and random coins r as $s\|(H(s)\oplus r)$ where '$\|$' denotes concatenation, $s=(m\|0^{k_1})\oplus G(r)$ for some parameter k_1, and G and H are hash functions (see Fig. 2 on p. 12). In contrast, PKCS #1 v1.5 essentially just concatenates m with r.

RSA-OAEP was designed using the random oracle (RO) methodology [6]. This means that the hash functions are modeled as independent truly random functions, available to all parties via oracle access. When the scheme is implemented in practice, these oracles are heuristically "instantiated" in certain ways using a cryptographic hash function. In particular, this means that any oracle call by the scheme's algorithms is replaced by the computation of a concrete function. In terms of security, a cryptographic hash function (or a function built from one) is of course not random nor computable only via an oracle (it has a short, public description), but schemes designed using this methodology are hoped to be secure. Unfortunately, a series of works, starting with the seminal paper of Canetti et al. [20], showed that there are schemes secure in the RO model that are insecure under *every* instantiation of the oracles; such RO model schemes are called *uninstantiable*. Thus, to gain confidence in an RO model scheme, we should show that it is instantiable, i.e., that the oracles admit a secure instantiation by efficiently computable functions under well-defined assumptions. Then, when we instantiate the scheme, we know that our goal is at least plausible. We feel this is especially important for a scheme such as RSA-OAEP, which is by now widely standardized and implemented (e.g., in SSH [32]).

Yet, while RO model schemes continue to be proposed, relatively few have been shown to be instantiable. In particular, we are not aware of *any* result showing instantiability of RSA-OAEP, even under a relatively modest security model. In fact, the scheme has come under criticism lately due to several works (discussed in Sect. 1.2) showing the impossibility of certain types of instantiations under chosen-ciphertext attack (IND-CCA) [52]. Fortunately, we bring some good news: We give reasonable assumptions under which RSA-OAEP is secure against *chosen-plaintext attack* (IND-CPA) [31]. We believe this is an important step toward a better understanding of the scheme's security.

[1] We often use the same terminology for 'f-OAEP,' which refers to OAEP using an abstract TDP f, with the meaning hopefully clear from context.

1.1. *Our Contributions*

Our result on the instantiability of RSA-OAEP is obtained via three steps or other results. (These other results may also be of independent interest.) First, we show a general result on the instantiability of "padding-based encryption," of which f-OAEP is a special case, under the assumption that the underlying padding transform is what we call a *fooling extractor* and the trapdoor permutation is *lossy* [49]. We then show (as the second and third steps, respectively) that OAEP and RSA satisfy the respective conditions under suitable assumptions.

Padding-based encryption without ROs. Our first result is a general theorem about *padding-based encryption* (PBE), a notion formalized recently by Kiltz and Pietrzak [38].[2] PBE generalizes the design methodology of PKCS #1 and RSA-OAEP we already mentioned. Namely, we start with a k-bit to k-bit trapdoor permutation (TDP) that satisfies a weak security notion like one-wayness. To "upgrade" the TDP to an encryption scheme satisfying a strong security notion like IND-CPA, we design an invertible "padding transform" which embeds a plaintext and random coins into a k-bit string, to which we then apply the TDP. This methodology is quite natural and has long been prevalent in practice, motivating the design of OAEP and later schemes such as SAEP [13] and PSS-E [23]. The latter were all designed and analyzed in the RO model.

We show that the RO model is *unnecessary* in the design and analysis of IND-CPA secure PBE. To do so, we formulate a connection between PBE and a new notion we call "fooling extractor for small-range distinguishers." or just "fooling extractor," and *lossy* trapdoor functions as defined by Peikert and Waters [49]. Lossiness means that there is an alternative, "lossy" key generation algorithm that outputs a public key indistinguishable from a normal one, but which induces a small ("lossy") range function. This is powerful because it allows one to prove security with respect to the lossy key generation algorithm, where information-theoretic arguments apply. A fooling extractor is a kind of randomness extractor (a concept introduced in [46]) whose output on a high-entropy source looks random to any function (or distinguisher) with a *small range*.[3] Our result says that if the padding transform of a PBE scheme is an "adaptive" fooling extractor for sources of the form (m, R)—where m is a plaintext and R is the random coins (which we call "encryption sources")—and its TDP is sufficiently lossy (the logarithm of its lossy range size should be slightly less than the length of R), then the PBE scheme is IND-CPA. Here "adaptive" means that m may *depend* on the choice of the extractor seed. We call such padding transforms "encryption-compatible."

OAEP fools small-range distinguishers. Our second result says that the OAEP padding transform is encryption-compatible if the hash function G is t-wise independent for appropriate t (roughly, proportional to the allowed message length).[4] Note that no

[2] Such schemes were called "simple embedding schemes" by Bellare and Rogaway [5], who discussed them only on an intuitive level.

[3] In the formal definition, we actually consider an "external" distinguisher who gets the extractor seed; see Sect. 3 for details.

[4] In particular, this result requires that G is a *keyed* hash function whose key is included in the public key for OAEP. On the other hand, cryptographic hash functions are typically unkeyed. But see "Using unkeyed hash functions" below.

restriction is put on hash function H; in particular, neither hash function is modeled as an RO. The inspiration for our proof comes from the "Crooked" Leftover Hash Lemma (LHL) of Dodis and Smith [26], especially its application to deterministic encryption by Boldyreva et al. [10] (who also gave a simpler proof). Qualitatively, the Crooked LHL says that $(K, f(\Pi(K, X)))$ looks like $(K, f(U))$ for any small-range function f, pairwise-independent function Π keyed by K, and high-entropy source X; in our terminology, this says that a pairwise-independent function is a fooling extractor for such X. In our application, we might naïvely view Π as the OAEP. There are two problems with this. First, OAEP is *not* pairwise independent, even in the RO model. Second, showing that OAEP is encryption-compatible entails showing adaptivity (as defined above), whereas in the lemma K is independent of X.

To solve the first problem, we show that the Crooked LHL can be strengthened to say that $K, f(X, \Pi(K, X))$ looks like $K, f(X, U)$; i.e., that $\Pi(K, X)$ looks random to f *even given* X. The proof is a careful extension of the proof of the Crooked LHL in [10]. Then, by viewing X as the random coins in OAEP and Π as the hash function G, we can conclude that OAEP is a fooling extractor for any fixed encryption source (m, R), where m is *independent* of K (note that our analysis does not use any properties of H—the only fact we use about the second Feistel round is that it is invertible).

To solve the second problem, we extend an idea of Trevisan and Vadhan [61] to our setting and show that if G is t-*wise* independent for large enough t, the probability that the chosen seed (or key) is "bad" for a particular encryption source is so small that we can take a union bound over all possible m and conclude that OAEP is in fact adaptive, meaning it is indeed encryption-compatible. Interestingly, we obtain better parameters in the case that f is *regular*, meaning every preimage set has the same size. However, our analysis still goes through assuming that every preimage set is sufficiently large, which we show can always be assumed with some loss in parameters.

Lossiness of RSA. To instantiate RSA-OAEP, it remains to show lossiness of RSA. Our final result is that RSA is indeed lossy under reasonable assumptions. We first show lossiness of RSA under the Φ-Hiding Assumption (ΦA) of Cachin, Micali, and Stadler [16]. ΦA has been used as the basis for a number of efficient protocols, e.g., [15,16,29,33]. ΦA states roughly that given an RSA modulus $N = pq$, it is hard to distinguish primes e that divide $\phi(N) = (p-1)(q-1)$ from those that do not. Normal RSA parameters (N, e) are such that $\gcd(e, \phi(N) = 1$. Under ΦA, we may alternatively choose (N, e) such that e *divides* $p-1$. The range of the RSA function is then reduced by a factor $1/e$. To resist known attacks, we can take the bit-length of e up to almost $1/4$ that of N, giving RSA lossiness of almost $k/4$ bits, where k is the modulus length.[5] We also stress that even though the only currently known algorithm to break the ΦA with such parameters is to factor the modulus N, it is considerably stronger than the standard factoring/RSA assumptions.

In practice, e is usually chosen to be small for efficiency reasons. We observe that in this case more lossiness can be achieved by considering *multi-prime* RSA where $N = p_1 \cdots p_m$ for $m \geq 2$ (for a fixed modulus length). In the lossy case, we choose (N, e) such that e divides p_i for *all* $1 \leq i \leq m-1$; the range of the RSA function is then

[5] We remark that the recent attacks on ΦA [56] are for moduli of a special form that does not include RSA.

reduced by a factor $1/e^{m-1}$. In a preliminary version of this paper [37], we showed that the maximum bit-length of e in this case to avoid our best attack was roughly $k(1/m-2/m^2)$ where k is the modulus length. By devising better attacks, this value was subsequently reduced to $k(2/3m^{2/3})$ by Herrmann [35] and $k(1/m - 2/(em \log(m+1)))$, where e is the base of the natural logarithm, by Tosu and Kunihiro [60]. So, for a fixed modulus size we gain in lossiness only for small e. If we assume such multi-prime RSA moduli are indistinguishable from two-prime ones, we can achieve such a gain in lossiness in the case of standard (two-prime) RSA as well.

Implications for RSA-OAEP. Combining the results above gives that RSA-OAEP is IND-CPA in the standard model under (rather surprisingly, at least to us) simple, non-interactive, and non-interdependent assumptions on RSA and the hash functions. The parameters for RSA-OAEP supported by our proofs are discussed in Sect. 6. While they are considerably worse than what is expected in practice, we view the upshot of our results not as the concrete parameters they support, but rather that they increase the theoretical backing for the scheme's security at a more qualitative level, showing it can be instantiated at least for larger parameters. In particular, our results give us greater confidence that chosen-plaintext attacks are unlikely to be found against the scheme; such attacks are known against the predecessor of RSA-OAEP in PKCS #1 v1.5 [22]. That said, we strongly encourage further research to try to improve the concrete parameters. Indeed, initial steps in this direction have already been taken; see Sect. 1.3 below.

Moreover, our analysis brings to light to some simple modifications that may increase the scheme's security. The first is to key the hash function G. Although our results have some interpretation in the case that G is a fixed function (see below), it may be preferable for G to have an explicit, randomly selected key. It is in an interesting open question whether our proof can be extended to function families that use shorter keys. The second possible modification is to increase the length of the randomness versus that of the redundancy in the message when encrypting short messages under RSA-OAEP. Of course, we suggest these modifications only in cases where they do not impact efficiency too severely.

Using unkeyed hash functions. Formally, our results assume G is randomly chosen from a large family (i.e., it is a keyed hash function). However, our analysis actually shows that *almost every* function (i.e. all but a very small fraction) from the family yields a secure instantiation; we just do not know an explicit member that works. In other words, it is not strictly necessary that G be randomly chosen. When G is instantiated in practice using a fixed cryptographic hash function like MD5 or SHA1, it is plausible that the resulting instantiation is secure. One can also assume the fixed cryptographic hash function to be implicitly keyed, where the key (in this context called the initialization vector) is chosen and fixed by its designer, and hard-coded into its implementation.

On chosen-ciphertext security. Any extension of our results to security under chosen-ciphertext attack (IND-CCA) must get around the negative results of Kiltz and Pietrzak [38] (which we discuss in more detail in Sect. 1.2). One possible approach to this is based on the fact that, by the results of Bellare and Palacio [4], the notion of plaintext awareness (PA) + IND-CPA implies IND-CCA. Thus, in order to show IND-CCA security of RSA-OAEP in the standard model it suffices, by our results, to show PA (which is an orthogonal property to privacy). To show the latter one could try to use non-black-box assumptions on H along the lines of [18]. We leave a detailed investigation to future work.

1.2. *Related Work*

SECURITY OF OAEP IN THE RO MODEL. In their original paper [5], Bellare and Rogaway showed that OAEP is IND-CPA assuming the TDP is one-way. They further showed it achieves a notion they called "plaintext awareness." Subsequently, Shoup [58] observed that the latter notion is too weak to imply security against chosen-ciphertext attacks, and in fact there is no black-box proof of IND-CCA security of OAEP based on one-wayness of the TDP. Fortunately, Fujisaki al. [28] proved that OAEP is nevertheless IND-CCA assuming so-called "partial-domain" one-wayness and that partial-domain one-wayness and (standard) one-wayness of RSA are equivalent.

SECURITY OF OAEP WITHOUT ROS. Results on instantiability of OAEP have so far mainly been negative. Boldyreva and Fischlin [11] showed that (contrary to a conjecture of Canetti [17]) one cannot securely instantiate even *one* of the two hash functions (while still modeling the other as an RO) of OAEP under IND-CCA by a "perfectly one-way" hash function [17,19] if one assumes only that f is partial-domain one-way. Brown [14] and Paillier and Villar [47] later showed that there are no "key-preserving" black-box proofs of IND-CCA security of RSA-OAEP based on one-wayness of RSA. Recently, Kiltz and Pietrzak [38] (building on the earlier work of Dodis et al. [24] in the signature context) generalized these results and showed that there is no black-box proof of IND-CCA (or even NM-CPA) security of OAEP based on any property of the TDP satisfied by an *ideal* (truly random) permutation.[6] In fact, their result can be extended to rule out a black-box proof of NM-CPA security of OAEP assuming the TDP is lossy [39], so our results are in some sense *optimal* given our assumptions.

INSTANTIATIONS OF RELATED SCHEMES. A positive instantiation result about a variant of OAEP called OAEP++ [40] (where part of the transform is output in the clear) was obtained by Boldyreva and Fischlin in [12]. They showed an instantiation that achieves (some weak form of) non-malleability under chosen-plaintext attacks (NM-CPA) for random messages, assuming the existence of non-malleable pseudorandom generators (NM-PRGs).[7] We note that the approach of trying to obtain positive results for instantiations under security notions weaker than IND-CCA originates from their work, and the authors explicitly ask whether OAEP can be shown IND-CPA in the standard model based on reasonable assumptions on the TDP and hash functions.

Another line of work has looked at instantiating other RO model schemes related at least in spirit to OAEP. Canetti [17] showed that the IND-CPA scheme in [6] can be instantiated using (a strong form of) perfectly one-way probabilistic hash functions. More recently, the works of Canetti and Dakdouk [18], Pandey al. [48], and Boldyreva et

---

[6] Note, however, that their result does not rule out such a proof based on other properties of the TDP, non-black-box assumptions on the hash functions, or in the case of a specific TDP like RSA.

[7] In particular, their security notion does *not* imply IND-CPA since they consider random messages. We also point out that it remains an open question whether NM-PRGs can be constructed.

al. [9] obtained (partial) instantiations of the earlier IND-CCA scheme of [6]. Hofheinz and Kiltz [36] recently showed an IND-CCA secure instantiation of a variant of the DHIES scheme of [51].

1.3. *Subsequent Work*

Subsequent to the preliminary version of this paper [37], our results have been improved in several ways. First, as mentioned above, Hermann [35] and Tosu and Kunihiro [60] gave better cryptanalyses of our extension of ΦA to the case of multiple primes. Furthermore, Lewko al. [42] resolved an open problem raised by our work and proved "approximate regularity" of lossy RSA on arithmetic progressions of sufficient length, leading to improved security bounds for RSA-OAEP; see Sect. 6. They also showed that this result gives a proof of IND-CPA security of RSA PKCS #1 v1.5. Subsequently, Smith and Zhang [59] proved a stronger result on approximate regularity of lossy RSA under a stronger assumption on RSA, leading to better parameters. They also fixed an erroneous claim of [42] about an "average-case" version of approximate regularity of lossy RSA, which can be used to prove large consecutive runs of input bits simultaneously hardcore without the stronger assumption on RSA.

Seurin [57] (building additionally on Freeman et al. [27]) showed how to extend our results to the case of the Rabin trapdoor function [50] instead of RSA. Hemenway *el al.* [34] showed how to use our result on the lossiness of RSA under ΦA to obtain new constructions of non-committing encryption under this assumption. Bellare et al. [3] proved IND-CPA security of RSA-OAEP under standard one-wayness of RSA, but making a much stronger assumption on the hash functions than we do.

2. Preliminaries

NOTATION AND CONVENTIONS. For a probabilistic algorithm A, by $y \stackrel{\$}{\leftarrow} A(x)$, we mean that A is executed on input x and the output is assigned to y, whereas if S is a finite set then by $s \stackrel{\$}{\leftarrow} S$, we mean that s is assigned a uniform element of S. We sometimes use $y \leftarrow A(x; \mathsf{Coins})$ to make A's random coins explicit. We denote by $\Pr\big[A(x) \Rightarrow y : \ldots\big]$ the probability that A outputs y on input x when x is sampled according to the elided experiment. Unless otherwise specified, an algorithm may be probabilistic and its running-time includes that of any overlying experiment. We denote by 1^k the unary encoding of the security parameter k. We sometimes suppress dependence on k for readability. For $i \in \mathbb{N}$ we denote by $\{0, 1\}^i$ the set of all binary strings of length i. If s is a string, then $|s|$ denotes its length in bits, whereas if S is a set then $|S|$ denotes its cardinality. By '$\|$' we denote string concatenation. All logarithms are base 2.

BASIC DEFINITIONS. Writing $P_X(x)$ for the probability that a random variable X puts on x, the *statistical distance* between random variables X and Y with the same range is given by $\Delta(X, Y) = \frac{1}{2}\sum_x |P_X(x) - P_Y(x)|$. If $\Delta(X, Y)$ is at most ε then we say X, Y are *ε-close* and write $X \approx_\varepsilon Y$. We say that X is *independent* if it is independent of all other random variables under consideration. The *min-entropy* of X is $\mathrm{H}_\infty(X) = -\log(\max_x P_X(x))$. A random variable X over $\{0, 1\}^n$ is called an (n, ℓ)-*source* if $\mathrm{H}_\infty(X) \geq \ell$. If $\ell = n$ then

X is said to be *uniform*. Let $f : A \to B$ be a function. We denote by $R(f)$ the *range* of f, i.e., $\{b \in B \mid \exists a \in A, f(a) = b\}$. We call $|R(f)|$ the *range size* of f. We call f *regular* if each pre-image set is the same size, i.e., $|\{x \in D \mid f(x) = y\}|$ is the same for all $y \in R$.

Public-key encryption and its security. A *public-key encryption scheme* with message-space MsgSp is a triple of algorithms $\mathcal{AE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$. The key generation algorithm $\mathcal{K}$ returns a public key pk and matching secret key sk. The encryption algorithm $\mathcal{E}$ takes pk and a plaintext m to return a ciphertext. The deterministic decryption algorithm $\mathcal{D}$ takes sk and a ciphertext c to return a plaintext. We require that for all messages $m \in$ MsgSp

$$\Pr\left[\mathcal{D}(sk, \mathcal{E}(pk, m)) \Rightarrow m \ :\ (pk, sk) \xleftarrow{\$} \mathcal{K}\right]$$

is (very close to) 1.

To an encryption scheme $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ and an adversary $A = (A_1, A_2)$, we associate a chosen-plaintext attack experiment,

$$
\begin{array}{l}
\textbf{Experiment } \mathbf{Exp}^{\text{ind-cpa}}_{\Pi,A}(k) \\
\quad b \xleftarrow{\$} \{0,1\}\,;\ (pk, sk) \xleftarrow{\$} \mathcal{K}(1^k) \\
\quad (m_0, m_1, \text{state}) \xleftarrow{\$} A_1(pk) \\
\quad c \xleftarrow{\$} \mathcal{E}(pk, m_b) \\
\quad d \xleftarrow{\$} A_2(pk, c, \text{state}) \\
\quad \text{If } d = b \text{ then return 1 else return 0}
\end{array}
$$

where we require A's output to satisfy $|m_0| = |m_1|$. Define the *ind-cpa advantage* of A against Π as

$$\mathbf{Adv}^{\text{ind-cpa}}_{\Pi,A}(k) = 2 \cdot \Pr\left[\mathbf{Exp}^{\text{ind-cpa}}_{\Pi,A}(k) \Rightarrow 1\right] - 1.$$

Lossy trapdoor permutations. A *lossy trapdoor permutation (LTDP) generator* [49][8] is a pair $\mathsf{LTDP} = (\mathcal{F}, \mathcal{F}')$ of algorithms. Algorithm $\mathcal{F}$ is a usual trapdoor permutation (TDP) generator, namely it outputs a pair (f, f^{-1}) where f is a (description of a) permutation on $\{0,1\}^k$ and f^{-1} its inverse. Algorithm $\mathcal{F}'$ outputs a (description of a) function f' on $\{0,1\}^k$. We call $\mathcal{F}$ the "injective mode" and $\mathcal{F}'$ the "lossy mode" of LTDP respectively, and we call $\mathcal{F}$ "lossy" if it is the first component of some lossy TDP. For a distinguisher D, define its *ltdp-advantage* against LTDP as

$$\mathbf{Adv}^{\text{ltdp}}_{\mathsf{LTDP},D}(k) = \Pr\left[D(f) \Rightarrow 1 \ :\ (f, f^{-1}) \xleftarrow{\$} \mathcal{F}\right] - \Pr\left[D(f') \Rightarrow 1 \ :\ f' \xleftarrow{\$} \mathcal{F}'\right].$$

[8] We note that [49] actually defines lossy trapdoor *functions*, but the extension to permutations is straightforward.

We say LTDP has *residual leakage* s if for all f' output by $\mathcal{F}'$ we have $|R(f')| \leq 2^s$. The *lossiness* of LTDP is $\ell = k - s$.

t-WISE INDEPENDENT HASHING. Let $H : \mathcal{K} \times D \to R$ be a (keyed) hash function. We say that H is *t-wise independent* [62] if for all distinct $x_1, \ldots, x_t \in D$ and all $y_1, \ldots, y_t \in R$

$$\Pr\left[\, H(K, x_1) = y_1 \;\wedge\; \ldots \;\wedge\; H(K, x_t) = y_t \,:\, K \xleftarrow{\$} \mathcal{K} \,\right] = \frac{1}{|R|^t}.$$

In other words, $H(K, x_1), \ldots, H(K, x_t)$ are all uniform and independent.

3. Padding-Based Encryption from Lossy TDP + Fooling Extractor

In this section, we show a general result on how to build IND-CPA secure padding-based encryption (PBE) without using random oracles, by combining a lossy TDP with a “fooling extractor" for small-range distinguishers.

3.1. *Background and Tools*

We first provide the definitions relevant to our result.

PADDING-BASED ENCRYPTION. The idea behind padding-based encryption (PBE) is as follows: We start with a k-bit to k-bit trapdoor permutation (e.g., RSA) and wish to build a secure encryption scheme. As in [5], we are interested in encrypting messages of less than k bits to ciphertexts of length k. It is well-known that we cannot simply encrypt messages under the TDP directly to achieve strong security. So, in a PBE scheme we “upgrade" the TDP by first applying a randomized and invertible “padding transform" to a message prior to encryption.

Our definition of PBE largely follows the recent formalization in [38]. Let k, μ, ρ be three integers such that $\mu + \rho \leq k$. A *padding transform* $(\pi, \hat{\pi})$ consists of two mappings $\pi : \{0,1\}^{\mu+\rho} \to \{0,1\}^k$ and $\hat{\pi} : \{0,1\}^k \to \{0,1\}^\mu \cup \{\perp\}$ such that π is injective and the following consistency requirement is fulfilled:

$$\forall m \in \{0,1\}^\mu, r \in \{0,1\}^\rho \;:\; \hat{\pi}(\pi(m \,\|\, r)) = m.$$

A *padding transform generator* is an algorithm Π that on input 1^k outputs a (description of a) padding transform $(\pi, \hat{\pi})$. Let $\mathcal{F}$ be a k-bit trapdoor permutation generator and Π be a padding transform generator. Define the associated *padding-based encryption scheme* $\mathcal{AE}_\Pi[\mathcal{F}] = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ with message-space $\{0,1\}^\mu$ by

Alg $\mathcal{K}(1^k)$	**Alg** $\mathcal{E}((\boldsymbol{\pi}, f), m)$	**Alg** $\mathcal{D}((\boldsymbol{\pi}, f^{-1}), y)$
$(\pi, \hat{\pi}) \xleftarrow{\$} \Pi(1^k)$	$r \xleftarrow{\$} \{0,1\}^\rho$; $x \leftarrow \pi(m \| r)$	$x \leftarrow f^{-1}(y)$
$\boldsymbol{\pi} \leftarrow (\pi, \hat{\pi})$	$y \leftarrow f(x)$	$m \leftarrow \hat{\pi}(x)$
$(f, f^{-1}) \xleftarrow{\$} \mathcal{F}(1^k)$	Return y	Return m
Return $((\boldsymbol{\pi}, f), (\boldsymbol{\pi}, f^{-1}))$		

Padding-based encryption schemes have long been prevalent in practice, for example PKCS #1 [55]. While OAEP [5] is the best-known, the notion also captures later schemes such as SAEP [13] and PSS-E [23].

FOOLING EXTRACTORS. We define a new notion that we call "fooling extractor for small-range distinguishers" or just "fooling extractor." Intuitively, fooling extractors are a type of randomness extractor [46] that "fools" distinguishers with small-range output. We give some more intuition after the formal definition.

Definition 3.1. Let $\mathsf{FExt}\colon \{0,1\}^c \times \{0,1\}^n \to \{0,1\}^k$ be a function and let $\mathcal{X} = \{X_1, \ldots, X_q\}$ be a class of (n,ℓ)-sources (as defined in Sect. 2). We say that FExt *fools range-*2^s *distinguishers on* $\mathcal{X}$ *with probability* $1-\varepsilon$ (or is an (s,ε)-fooling extractor for $\mathcal{X}$) if for all functions f' on $\{0,1\}^k$ with range size at most 2^s and all $1 \le i \le q$:

$$(K, f'(\mathsf{FExt}(K, X_i)) \approx_\varepsilon (K, f'(U))\,,$$

where K is uniform on $\{0,1\}^c$ and U is uniform and independent on $\{0,1\}^n$. We call K the *key* or *seed* of FExt. Note that K is *independent* of i above.

We say that FExt *adaptively* fools range-2^s distinguishers on $\mathcal{X}$ with probability $1-\varepsilon$ (or is an adaptive (s,ε)-fooling extractor for $\mathcal{X}$) if for all functions f' on $\{0,1\}^k$ with range size at most 2^s:

$$\mathop{\mathbf{E}}_{k' \xleftarrow{\$} \{0,1\}^c}\left[\max_{1\le i\le q} \Delta\Big(f'(\mathsf{FExt}(k', X_i))\,,\; f'(U)\Big)\right] \le \varepsilon.$$

Since $\Delta(K, f'(\mathsf{FExt}(K, X_i)), (K, f'(U))) = \mathbf{E}_{k'}\, \Delta(k', f(\mathsf{FExt}(k', X_i)), (k', f(U)))$, the above implies that $(K, f'(\mathsf{FExt}(K, X_i)) \approx_\varepsilon (K, f'(U))$ for i *depending* on K (or, put differently, $(K, f'(\mathsf{FExt}(K, X_i)) \approx_\varepsilon (K, f'(U))$ holds for every i over the *same* choice of K).

As a useful special case, we say that FExt fools range-2^s regular distinguishers on $\mathcal{X}$ with probability $1-\varepsilon$ (or is a regular (s,ε)-fooling extractor for $\mathcal{X}$) if we quantify only over *regular* f in the definition. An *adaptive regular* (s,ε)-fooling extractor for $\mathcal{X}$ is defined analogously.

We note that while the intuition given prior to the definition describes fooling the function f, it actually requires fooling an "implicit" or "external" distinguisher that sees both the output $f'(\mathsf{FExt}(K, X_i))$ of f and the extractor seed K. This crucial for the definition to be meaningful. Indeed, just asking that $f'(\mathsf{FExt}(K, X_i))$ be indistinguishable from $f(U)$ for all small-range functions f is equivalent to asking only that $\mathsf{FExt}(K, X_i)$ be indistinguishable from U. This latter requirement is trivial to achieve (if one is not concerned with key length)–for example, by using K as a one-time pad.

We also note that the concept of fooling extractors was implicit in the work of Dodis and Smith [26] on error-correction without leaking partial information, whose "Crooked" Leftover Hash Lemma establishes in our language that a pairwise-independent function is a (s,ε)-fooling extractor for every singleton (n,ℓ)-source X where $s \le \ell - 2\log(1/\varepsilon)+$

2. This lemma was later applied in the context of deterministic public-key encryption by Boldyreva et al. [10], who also gave a simpler proof.

3.2. *The Result*

To state our result, we first formalize the concept of *encryption-compatible* padding transforms.

Definition 3.2. Let Π be a padding transform generator whose coins are drawn from Coins. Define the associated function $h_\Pi : \mathsf{Coins} \times \{0,1\}^{\mu+\rho} \to \{0,1\}^k$ by $h(cc, m\|r) = \pi(m\|r)$ for all $cc \in \mathsf{Coins}$, $m \in \{0,1\}^\mu$, $r \in \{0,1\}^\rho$, where $(\pi, \hat{\pi}) \leftarrow \Pi(1^k; cc)$. Define the class $\mathcal{X}_\Pi$ of *encryption sources* associated to Π as containing all sources of the form (m, R), where $m \in \{0,1\}^\mu$ is fixed and $R \in \{0,1\}^\rho$ is uniform. (Note that the class $\mathcal{X}_\Pi$ therefore contains 2^μ distinct $(\mu+\rho, \rho)$-sources.) We say that Π is (s, ε)-*encryption-compatible* if h_Π as above is an adaptive (s, ε)-fooling extractor for $\mathcal{X}_\Pi$. (Here Coins plays the role of $\{0,1\}^c$ in Definition 3.1.) A *regular* (s, ε)-encryption-compatible padding transform generator is defined analogously.

Theorem 3.3. *Let* $\mathsf{LTDP} = (\mathcal{F}, \mathcal{F}')$ *be an LTDP with residual leakage s, and let* Π *be an* (s, ε)*-encryption-compatible padding transform generator. Then, for any IND-CPA adversary A against* $\mathcal{AE}_\Pi[\mathcal{F}]$*, there is an adversary D against* LTDP *such that for all* $k \in \mathbb{N}$

$$\mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{AE},A}(k) \le \mathbf{Adv}^{\text{ltdp}}_{\mathsf{LTDP},D}(k) + \varepsilon.$$

Furthermore, the running-time of D is the time to run A.

Proof. Given $A = (A_1, A_2)$, we define three games, called G_0, G_1, G_2, in Fig. 1. Note that game G_0 is the experiment $\mathbf{Exp}^{\text{ind-cpa}}_{\Pi,A}(k)$ defining IND-CPA security. We claim that for a distinguisher D against LTDP that is simple to construct, we have

$$\begin{aligned} \frac{1}{2} + \mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{AE}_\Pi[\mathcal{F}],A}(k) &= \Pr[\,G_0 \Rightarrow 1\,] && (1)\\ &\le \Pr[\,G_1 \Rightarrow 1\,] + \mathbf{Adv}^{\text{ltdp}}_{\mathsf{LTDP},D}(k) && (2)\\ &\le \Pr[\,G_2 \Rightarrow 1\,] + \mathbf{Adv}^{\text{ltdp}}_{\mathsf{LTDP},D}(k) + \varepsilon && (3)\\ &= \frac{1}{2} + \mathbf{Adv}^{\text{ltdp}}_{\mathsf{LTDP},D}(k) + \varepsilon\,, && (4) \end{aligned}$$

from which the theorem follows by re-arranging terms. So let us justify the above.

Equation (1) is true by the definition of IND-CPA security.

For (2) we can construct a distinguisher D as required since G_0, G_1 do not use f^{-1} in any way.

Game G_0:	Game G_1:	Game G_2:
$b \xleftarrow{\$} \{0,1\}$; $(f, f^{-1}) \xleftarrow{\$} \mathcal{F}$	$b \xleftarrow{\$} \{0,1\}$; $\boxed{f \xleftarrow{\$} \mathcal{F}'}$	$b \xleftarrow{\$} \{0,1\}$; $f \xleftarrow{\$} \mathcal{F}'$
$(\pi, \hat{\pi}) \xleftarrow{\$} \Pi$; $\mathbf{\Pi} \leftarrow (\pi, \hat{\pi})$	$(\pi, \hat{\pi}) \xleftarrow{\$} \Pi$; $\mathbf{\Pi} \leftarrow (\pi, \hat{\pi})$	$(\pi, \hat{\pi}) \xleftarrow{\$} \Pi$; $\mathbf{\Pi} \leftarrow (\pi, \hat{\pi})$
$(m_0, m_1, \text{state}) \xleftarrow{\$} A_1(f, \mathbf{\Pi})$	$(m_0, m_1, \text{state}) \xleftarrow{\$} A_1(f, \mathbf{\Pi})$	$(m_0, m_1, \text{state}) \xleftarrow{\$} A_1(f, \mathbf{\Pi})$
$r \leftarrow \{0,1\}^\rho$; $x \leftarrow \hat{\pi}(m_b \| r)$	$r \xleftarrow{\$} \{0,1\}^\rho$; $x \leftarrow \hat{\pi}(m_b \| r)$	$\boxed{x \xleftarrow{\$} \{0,1\}^k}$
$d \xleftarrow{\$} A_2((f, \mathbf{\Pi}), f(x), \text{state})$	$d \xleftarrow{\$} A_2((f, \mathbf{\Pi}), f(x), \text{state})$	$d \xleftarrow{\$} A_2((f, \mathbf{\Pi}), f(x), \text{state})$
If $d = b$ then Return 1	If $d = b$ then Return 1	If $d = b$ then Return 1
Else Return 0	Else Return 0	Else Return 0

Fig. 1. Games for the proof of Theorem 3.3. *Shaded* areas indicate the differences between games.

Equation (3) is true by the definition of encryption compatibility. Namely, since h_Π in the definition is an adaptive (s, ε)-fooling extractor for $\mathcal{X}_\Pi$, we know the expectation over the coins cc is at most ε for m *depending* on cc (and hence π), where $(\pi, \hat{\pi}) \leftarrow \Pi(1^k; cc)$, of $\Delta(f'(\pi(m, R)), f'(U))$, so in particular it holds for $m = m_b$ in game G_1.

Finally, (4) uses the fact that in G_2 no information about b is given to A. Note that the final two steps in the proof are information-theoretic, meaning they do not use any assumption about A's running-time. $\square$

Remark 3.4. The analogous result holds for regular LTDPs and regular encryption-compatible padding transforms. That is, if the LTDP is *regular*, then it suffices to use a regular encryption-compatible padding transform to obtain the same conclusion. The latter may be easier to design or more efficient than in the general case; indeed, we get better parameters for OAEP in the regular case in Sect. 4. Furthermore, known examples of LTDPs (including RSA, as shown in Sect. 5) are regular, although a technical issue about the domain of RSA versus the output range of OAEP makes it challenging to exploit this for RSA-OAEP; see Sect. 6.

4. OAEP as a Fooling Extractor

In this section, we show that the OAEP padding transform of Bellare and Rogaway [5] is encryption-compatible as defined in Sect. 3 if its initial hash function is t-wise independent for t depending on the message length and lossiness of the TDP.

4.1. *OAEP*

We recall the OAEP padding transform of Bellare and Rogaway [5], lifted to the "instantiated" setting, i.e., where its hash functions may be keyed. (The original scheme was defined for unkeyed hash functions.) Let $G\colon \mathcal{K}_G \times \{0,1\}^\rho \to \{0,1\}^\mu$ and $H\colon \mathcal{K}_H \times \{0,1\}^\mu \to \{0,1\}^\rho$ be hash functions. The associated padding transform generator $\mathsf{OAEP}[G, H]$ on input 1^k returns $(\pi_{K_G,K_H}, \hat{\pi}_{K_G,K_H})$, where $K_G \xleftarrow{\$} \mathcal{K}_G(1^k)$ and $K_H \xleftarrow{\$} \mathcal{K}_H(1^k)$, defined via

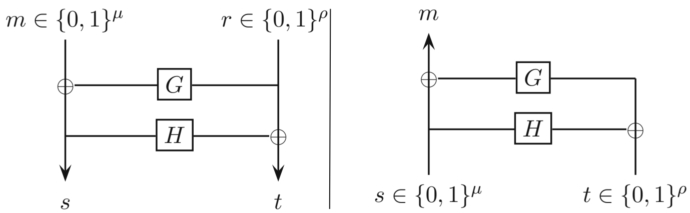

Fig. 2. Algorithms $\pi_{K_G,K_H}(m,r)$ and $\hat{\pi}_{K_G,K_H}(s,t)$ for $\mathsf{OAEP}[G,H]$.

Algorithm $\pi_{K_G,K_H}(m\|r)$	**Algorithm** $\hat{\pi}_{K_G,K_H}(x)$
$s \leftarrow m \oplus G(K_G, r)$	$s\|t \leftarrow x$
$t \leftarrow r \oplus H(K_H, s)$	$r \leftarrow t \oplus H(K_H, s)$
$x \leftarrow s\|t$	$m \leftarrow s \oplus G(K_G, r)$
Return x	Return m

See Fig. 2 for a graphical illustration.

Remark 4.1. Since we mainly study IND-CPA security, for simplicity we define above the "no-redundancy" version of OAEP, i.e., corresponding to the "basic scheme" in [5]. However, all our results also holds for the redundant version. Additionally, as is typical in the literature, we have defined OAEP to apply the G-function to the least-significant bits of the input; in standards and implementations, it is typically the most significant bits (where the order of m and r are switched). Again, we stress that our results hold in either case.

4.2. *Analysis*

The following establishes that OAEP is encryption-compatible if the hash function G is t-wise independent for appropriate t. No restriction is put on the other hash function H. Indeed, our result also applies to SAEP [13] (although the latter is neither standardized nor known to provide CCA security in the RO model, except in certain cases).

Theorem 4.2. *Let $G: \mathcal{K}_G \times \{0,1\}^\rho \to \{0,1\}^\mu$ and $H: \mathcal{K}_H \times \{0,1\}^\mu \to \{0,1\}^\rho$ be hash functions, and suppose G is t-wise independent. Let $\mathsf{OAEP} = \mathsf{OAEP}[G,H]$. Then*

(1) OAEP *is (s,ε)-encryption-compatible where $\varepsilon = 2^{-u}$ for $u = \frac{t}{3t+2}(\rho - s - \log t + 2) - \frac{2(\mu+s)}{3t+2} - 1$.*
(2) OAEP *is* regular *(s,ε)-encryption-compatible where $\varepsilon = 2^{-u}$ for $u = \frac{t}{2t+2}(\rho - s - \log t + 2) - \frac{\mu+s+2}{t+1} - 1$.*
(3) When $t = 2$, OAEP *is (s,ε)-encryption-compatible where $\varepsilon = 2^{-u}$ for $u = (\rho - s - 2\mu)/4 - 1$.*

Note that parts (2) and (3) capture special cases of (1) in which we get better bounds. The techniques used in the proof were first developed in the context of the classical LHL by Trevisan and Vadhan [61] and Dodis, Sahai and Smith [25], though the style of presentation of our theorem statement and proof are inspired by Barak al. [1, Lemma1]. We mention that due to our use of (variants of) the Crooked LHL rather than the classical one and the stucture of OAEP, some of the technical details differ in our case and require new ideas.

Corollary 4.3. *Let* $G: \mathcal{K}_G \times \{0,1\}^\rho \to \{0,1\}^\mu$ *and* $H: \mathcal{K}_H \times \{0,1\}^\mu \to \{0,1\}^\rho$ *be hash functions and suppose that* G *is* t*-wise independent for* $t \geq 3\frac{\mu+s}{\rho-s}$. *Then* $\mathsf{OAEP}[G, H]$ *is* (s, ε)*-encryption-compatible where* $\varepsilon = \exp(-c(\rho - s - \log t))$ *for a constant* $c > 0$.

In particular, $c \approx 1/2$ for regular functions. For such a function, if $\rho - s$ is at least 180, then ε is roughly 2^{-80} for $t = 10$ and message lengths $\mu \leq 2^{15}$ (which for practical purposes does not restrict the message-space). Applying Theorem 3.3, we see that if G is 10-wise independent and the number of random bits used in OAEP is at least 180 bits larger than the residual lossiness of the TDP, then the security of OAEP is tightly related to that of the lossy TDP.

Remark 4.4. To show security of OAEP against what we call *key-independent* chosen-plaintext attack, it suffices to argue that $\mathsf{OAEP}[G, H]$ is a fooling extractor for any *fixed* encryption source $X = (m, R)$ where $m \in \{0,1\}^\mu$. The latter holds for any $\varepsilon > 0$ and $s \leq \rho - 2\log(1/\varepsilon) + 2$ assuming G is only pairwise-independent (i.e., $t = 2$). See Appendix 8 for details.

Proof. (of Theorem 4.2) We now prove the above theorem.

Overview. We write OAEP for $\mathsf{OAEP}[G, H]$. The high-level idea for all three parts of the theorem is the same. Fix a lossy function f' with range size at most 2^s. We first show that for every *fixed* message $m \in \{0,1\}^\mu$, with high probability (say $1 - \delta$) over the choice of K_G, the statistical distance between $f'(\mathsf{OAEP}(m, R))$ and $f'(U)$ is small (say $\hat{\varepsilon}$). This aspect of the proof changes from part to part. We then take a union bound to show that the above holds for *all* messages over the same choice of K_G with probability at least $1 - 2^\mu\delta$. This means that the statistical distance between the pair $(K_G, f'(\mathsf{OAEP}(m, R)))$ and $(K_G, f'(\mathsf{OAEP}(U)))$ is at most $\varepsilon = \hat{\varepsilon} + 2^\mu\delta$ for all messages over the same choice of K_G. Finally, we express δ as a function of $\hat{\varepsilon}$, and select $\hat{\varepsilon}$ to minimize this sum. Note that the entire argument works for any choice of H.

We first prove part (3) of the theorem, then part (2), and finally part (1).

Proof of part (3). To prove part (3) of the theorem, we strengthen the Crooked LHL of [26] to give the distinguisher access to the *input* to the fooling function as well its output.

Lemma 4.5. *(Augmented Crooked LHL.) Let* $h: \mathcal{K} \times A \to B$ *be a pairwise-independent function and let* $g: A \times B \to S$ *be a function. Let* X *be a random variable on* A *such that* $\mathrm{H}_\infty(X) \geq \lg|S| + 2\lg(1/\hat{\varepsilon}) - 2$ *for some* $\hat{\varepsilon} > 0$. *Then*

$$\Delta((K, g(X, h(K, X)), (K, g(X, U)) \le \hat{\varepsilon},$$

where $K \xleftarrow{\$} \mathcal{K}$ *and* $U \xleftarrow{\$} B$.

The proof, which extends the proof of the Crooked LHL given in [10], is in Appendix 1.

Now we let G play the role of h in Lemma 4.5 and let $\{0, 1\}^\rho$ and $\{0, 1\}^\mu$ play the roles of A and B, respectively. Let g in the lemma be defined by $g(a, b) = f(m \oplus a \| b \oplus H(K_H, m \oplus a))$ for arbitrary but *fixed* $m \in \{0, 1\}^\mu$, $K_H \in \mathcal{K}_H$. It follows that OAEP is a $(s, \hat{\varepsilon})$-fooling extractor for every *fixed* encryption source X of the form (m, R). Part (3) of the theorem now follows by applying Markov's inequality and taking a union bound over *all* such sources.

In more detail, let f' be any function on $\{0, 1\}^k$ to a set $\mathcal{Y}$ of size at most 2^s, and let $X = (m, R)$ be any $(\mu + \rho, \rho)$-source, where $m \in \{0, 1\}^\mu$ is fixed and R is uniform over $\{0, 1\}^\rho$. Define random variable Z_{K_G, K_H} to take value $\Delta(f'(\pi_{k_G, k_H}(m \| R), f'(U))$ for U uniform on $\{0, 1\}^k$, if $K_G = k_G$ and $K_H = k_H$, where here and in what follows the probability is over the random choices of K_G and K_H (although as the distribution on K_H does not matter – we use only the fact that it is independent of m, R, K_G). Then applying Lemma 4.5 as explained above, we have $\mathbf{E}\left[Z_{K_G, K_H} \right] \le 1/2\sqrt{|S| \cdot 2^{-\rho}}$. Thus by Markov's inequality

$$\Pr\left[Z_{K_G, K_H} \ge \hat{\varepsilon} \right] \le \frac{\sqrt{2^{s-\rho}}}{2\hat{\varepsilon}}$$

for any $\hat{\varepsilon} > 0$. By a union bound, the probability that the above holds simultaneously for all 2^μ possible $(\mu + \rho, \rho)$-sources $X = (m, R)$ is at least $1 - \delta_{\hat{\varepsilon}}$, where

$$\delta_{\hat{\varepsilon}} = \frac{2^\mu \cdot \sqrt{2^{s-\rho}}}{2\hat{\varepsilon}}.$$

It now follows (by a conditioning argument) that OAEP is (s, ε)-encryption-compatible with $\varepsilon = \hat{\varepsilon} + \delta_{\hat{\varepsilon}}$. Note that $\delta_{\hat{\varepsilon}}$ can be written in the form $\gamma \cdot \hat{\varepsilon}^{-1}$ (where γ depends on ρ, s, μ but not $\hat{\varepsilon}$). Setting $\hat{\varepsilon} = \gamma^{1/2}$ yields $\varepsilon \le 2\gamma^{1/2}$ and part (3) of the Theorem follows by observing that

$$\begin{aligned} u = -\log \varepsilon &\ge -\frac{1}{2} \cdot \log \gamma - 1 \\ &= -\frac{1}{2} \cdot (\mu + 1/2(s - \rho)) - 1 \\ &= (\rho - s - 2\mu)/4 - 1. \end{aligned}$$

Proof of part (2). Instead of Markov's inequality, the proof of part (2) of the theorem uses a stronger tail inequality for t-wise independent random variables, due to Bellare and Rompel [7] (our application was inspired by the use of t-wise independence by Trevisan and Vadhan [61] and Dodis, Sahai, and Smith [25]).

Let f' be any function on $\{0, 1\}^k$ to a set $\mathcal{Y}$ of size at most 2^s. For this part of the theorem, assume that f' is regular, that is, that each preimage set has size exactly 2^{k-s}.

Let $X = (m, R)$ be any $(\mu + \rho, \rho)$-source, where $m \in \{0, 1\}^\mu$ is fixed and R is uniform over $\{0, 1\}^\rho$. For each $r \in \{0, 1\}^\rho$ and $y \in \mathcal{Y}$, define the random variable

$$Z_{r,y} = \begin{cases} 2^{-\rho} & \text{if } f'(\pi_{K_G,K_H}(m\|r)) = y\,, \\ 0 & \text{otherwise,} \end{cases}$$

where as before the probability is over the random choices of K_G and K_H (although as before the distribution on K_H does not matter – we use only the fact that it is independent of m, R, K_G). Let $Z_y = \sum_r Z_{r,y}$. We claim that $\mathbf{E}\left[\, Z_y \,\right] = 2^{-s}$. To see this, note that

$$\mathbf{E}\left[\, Z_y \,\right] = \sum_r 2^{-\rho} \cdot \Pr\left[\, f'(U\|r) = y \,\right] = \Pr\left[\, f'(U\|R) = y \,\right] = 2^{-s}$$

where we use the fact that R is uniform and f' is regular.

To bound the deviation of Z_y from its mean, note that for a fixed y, the variables $\{Z_{r,y}\}_{r\in\{0,1\}^\rho}$ are t-wise independent (by the t-wise independence of G) and take values in $[0, 2^{-\rho}]$. We can apply the following tail bound (modified from the original to apply to random variables in $[0, M]$ rather than $[0, 1]$).

Lemma 4.6. *(Bellare and Rompel [7]) Let $A_1, \ldots A_n$ be t-wise independent random variables taking values in $[0, M]$. Let $A = \sum_i A_i$ and $\delta \le 1$. Then*

$$\Pr\left[\, |A - \mathbf{E}[\, A \,]| \ge \delta \cdot \mathbf{E}[\, A \,] \,\right] \le c_t \left(\frac{t \cdot M}{\delta^2 \cdot \mathbf{E}[\, A \,]} \right)^{t/2}$$

where $c_t < 3$ and $c_t < 1$ when $t \ge 8$.

Setting $\delta = 2\hat{\varepsilon}$, we get that for every $y \in \mathcal{Y}$,

$$\Pr\left[\, |Z_y - 2^{-s}| \ge 2\hat{\varepsilon} \cdot 2^{-s} \,\right] \le c_t \left(\frac{t}{4\hat{\varepsilon}^2 \cdot 2^{-s+\rho}} \right)^{t/2}. \tag{5}$$

By a union bound, the probability that there exists a $y \in \mathcal{Y}$ such that $|Z_y - 2^{-s}| \ge 2\hat{\varepsilon} \cdot 2^{-s}$ is at most

$$2^s c_t \left(\frac{t}{4\hat{\varepsilon}^2 \cdot 2^{-s}} \right)^{t/2}.$$

Observe that if $|Z_y - 2^{-s}| \ge 2\hat{\varepsilon} \cdot 2^{-s}$ for all $y \in \mathcal{Y}$ then, letting Y denote the random variable $f'(\pi_{K_G,K_H}(m, R))$, we have

$$\Delta((K_G, K_H, Y), (K_G, K_H, f'(U)) \;\le\; \frac{1}{2} \sum_{y\in\mathcal{Y}} |Z_y - 2^{-s}| \;=\; \sum_{y\in\mathcal{Y}} \hat{\varepsilon} \cdot 2^{-s} \;=\; \hat{\varepsilon}.$$

By another union bound, the probability that the above holds simultaneously for all 2^{μ} possible $(\mu+\rho, \rho)$-sources $X = (m, R)$ is at least $1 - \delta_{\hat{\varepsilon}}$, where

$$\delta_{\hat{\varepsilon}} = 2^{\mu+s} c_t \left(\frac{t}{4\hat{\varepsilon}^2 \cdot 2^{-s+\rho}} \right)^{t/2}. \tag{6}$$

It now follows (by a conditioning argument) that OAEP is (s, ε)-encryption-compatible with $\varepsilon = \hat{\varepsilon} + \delta_{\hat{\varepsilon}}$. Note that $\delta_{\hat{\varepsilon}}$ can be written in the form $\gamma \cdot \hat{\varepsilon}^{-t}$ (where γ depends on t, ρ, s, μ but not $\hat{\varepsilon}$). Setting $\hat{\varepsilon} = \gamma^{1/(t+1)}$ yields $\varepsilon \leq 2\gamma^{1/(t+1)}$ and part (2) of the Theorem follows by observing that

$$\begin{aligned} u = -\log \varepsilon &\geq -\frac{1}{t+1} \cdot \log \gamma - 1 \\ &= -\frac{1}{t+1} \cdot (\frac{t}{2}(\rho - s - \log t + 2) + \mu + s + \log c_t) - 1 \\ &\geq \frac{t}{2t+2} \cdot (\rho - s - \log t + 2) - \frac{\mu + s + 2}{t+1} - 1. \end{aligned}$$

Proof of part (1). We now turn to proving the lemma for general (not necessarily balanced) functions f'. We first give a proof for approximately balanced functions, in which no pre-image set is too small; we then show that this implies a bound for arbitrary functions.

Assume for now that $\min_{y \in \mathcal{Y}} |\mathsf{preimg}_{f'}(y)| \geq \lambda \cdot 2^{k-s}$ for some real number $0 < \lambda \leq 1$ (note that regularity corresponds to $\lambda = 1$), where $\mathsf{preimg}_{f'}(y) = \{x \in \{0,1\}^k \mid f(x) = y\}$ We sketch how to modify the proof of part (2) under this assumption; essentially, we end up with an extra factor of λ in the denominator of Eq. 6. We use the same definition of Z_y as in part (2). Instead of $\mathbf{E}\left[\, Z_y \,\right] = 2^{-s}$, we now have $\mathbf{E}\left[\, Z_y \,\right] = \Pr[\, f(U \| R) = y\,] = |\mathsf{preimg}_{f'}(y)|/2^k$. Thus, instead of Eq. (5), we have

$$\begin{aligned} &\Pr\left[\, |Z_y - |\mathsf{preimg}_{f'}(y)|/2^k| \geq 2\hat{\varepsilon} \cdot |\mathsf{preimg}_{f'}(y)|/2^k \,\right] \\ &\quad \leq c_t \left(\frac{t}{4\hat{\varepsilon}^2 \cdot |\mathsf{preimg}_{f'}(y)|/2^k \cdot 2^{\rho}} \right)^{t/2}. \end{aligned}$$

Using $\min_{y \in \mathcal{Y}} |\mathsf{preimg}_{f'}(y)| \geq \lambda \cdot 2^{k-s}$ and taking a union bound, we get that the probability that there exists $y \in \mathcal{Y}$ such that

$$|Z_y - |\mathsf{preimg}_{f'}(y)|/2^k| \geq 2\hat{\varepsilon} \cdot |\mathsf{preimg}_{f'}(y)|/2^k| \tag{7}$$

is at most

$$2^s c_t \left(\frac{t}{4\hat{\varepsilon}^2 \cdot \lambda \cdot 2^{-s} \cdot 2^{\rho}} \right)^{t/2}. \tag{8}$$

We can obtain a bound for arbitrary functions f' by noting that every function f' is "close" to a function with no small pre-images. Specifically:

Claim 4.7. Let $f'\colon \{0,1\}^k \to \mathcal{Y}$ where $|\mathcal{Y}| \le 2^s$ be a function. For any real number $\lambda > 0$, there exists a function $g'\colon \{0,1\}^k \to \mathcal{Y}$ such that (i) $\min_{y\in\mathcal{Y}} |\mathsf{preimg}_{g'}(y)| \ge \lambda \cdot 2^{k-s}$; and (ii) the function g' agrees with f' on a $1-\lambda$ fraction of its domain. In particular, $\Delta(f'(U), g'(U)) \le \lambda$.

We can now prove part (3) of the Theorem from Eq. (8) by choosing $\lambda = \hat{\varepsilon}$ in the claim and then completing the analysis as in part (2). It remains to prove the claim.

Proof (of Claim 4.7): The idea is that we will take all the small pre-image sets of f' and merge them together with some larger preimage set (e.g., if 0 has a large pre-image set, then for all elements x such that $\mathsf{preimg}_{f'}(f'(x))$ is small, we set $f(x) = 0$). How many elements can belong to small pre-image sets? There are at most 2^s pre-image sets, each of which contains at most $\lambda \cdot 2^{k-s}$ elements. So there are at most $\lambda \cdot 2^k$ elements of the domain on which f' has to be changed. □

This concludes the proof of the Theorem.

5. Lossiness of RSA

In this section, we show that the RSA trapdoor permutation is lossy under reasonable assumptions. In particular, we show that, for large enough encryption exponent e, RSA is considerably lossy under the Φ-Hiding Assumption of [16]. We then show that by generalizing this assumption to multi-prime RSA we can get even more lossiness. Finally, we propose a "Two-Or-m-Primes" Assumption that, when combined with the former, amplifies the lossiness of standard (two-prime) RSA for small e.

5.1. *Background on RSA and Notation*

We denote by $\mathcal{RSA}_k$ the set of all tuples (N, p, q) such that $N = pq$ is the product of two distinct $k/2$-bit primes. Such an N is called an *RSA modulus*. By $(N, p, q) \xleftarrow{\$} \mathcal{RSA}_k$ we mean that (N, p, q) is sampled according to the uniform distribution on $\mathcal{RSA}_k$. An *RSA TDP generator* [53] is an algorithm $\mathcal{F}$ that returns $(N, e), (N, d)$, where N is an RSA modulus and $ed \equiv 1 \pmod{\phi(N)}$. (Here $\phi(\cdot)$ denotes Euler's totient function, so in particular $\phi(N) = (p-1)(q-1)$.) The tuple (N, e) defines the permutation on $\mathbb{Z}_N^*$ given by $f(x) = x^e \bmod N$, and similarly (N, d) defines its inverse. We say that a lossy TDP generator $\mathsf{LTDP} = (\mathcal{F}, \mathcal{F}')$ is an RSA LTDP if $\mathcal{F}$ is an RSA TDP generator.

To define the Φ-Hiding Assumption and later some extensions of it, the following notation is also useful. For $i \in \mathbb{N}$ we denote by $\mathcal{P}_i$ the set of all i-bit primes. Let R be a relation on p and q. By $\mathcal{RSA}_k[R]$ we denote the subset of $\mathcal{RSA}_k$ for that the relation R holds on p and q. For example, let e be a prime. Then $\mathcal{RSA}_k[p = 1 \bmod e]$ is the set of all (N, p, q), where $N = pq$ is the product of two distinct $k/2$-bit primes p, q and $p = 1 \bmod e$. That is, the relation $R(p, q)$ is true if $p = 1 \bmod e$ and q is arbitrary. By $(N, p, q) \xleftarrow{\$} \mathcal{RSA}_k[R]$ we mean that (N, p, q) is sampled according to the uniform distribution on $\mathcal{RSA}_k[R]$.

5.2. *RSA Lossy TDP from Φ-Hiding*

Φ-HIDING ASSUMPTION (ΦA). We recall the Φ-Hiding Assumption of [16]. For an RSA modulus N, we say that N *ϕ-hides* a prime e if $e \mid \phi(N)$. Intuitively, the assumption is that, given RSA modulus N, it is hard to distinguish primes which are ϕ-hidden by N from those that are not. Formally, let $0 < c < 1/2$ be a (public) constant determined later. Consider the following two distributions:

$$\mathcal{R}_1 = \{(e, N) : e, e' \xleftarrow{\$} \mathcal{P}_{ck}\,;\ (N, p, q) \xleftarrow{\$} \mathcal{RSA}_k[p = 1 \bmod e']\}$$
$$\mathcal{L}_1 = \{(e, N) : e \xleftarrow{\$} \mathcal{P}_{ck}\,;\ (N, p, q) \xleftarrow{\$} \mathcal{RSA}_k[p = 1 \bmod e])\}.$$

To a distinguisher D, we associate its Φ*A advantage* defined as

$$\mathbf{Adv}^{\Phi\mathrm{A}}_{c,D}(k) \;=\; \Pr[\, D(\mathcal{R}_1) \Rightarrow 1\,] - \Pr[\, D(\mathcal{L}_1) \Rightarrow 1\,]\,.$$

As shown in [16], distributions $\mathcal{R}_1, \mathcal{L}_1$ can be sampled efficiently assuming the widely accepted Extended Riemann Hypothesis (as we need a density estimate on the number of primes of a particular form).[9]

RSA LTDP FROM ΦA. We construct an RSA LTDP based on ΦA. In injective mode the public key is (N, e) where e is not ϕ-hidden by N, whereas in lossy mode it is. Namely, define $\mathsf{LTDP}_1 = (\mathcal{F}_1, \mathcal{F}'_1)$ as follows:

Algorithm $\mathcal{F}_1$	**Algorithm** $\mathcal{F}'_1$
$e, e' \xleftarrow{\$} \mathcal{P}_{ck}$	$e \xleftarrow{\$} \mathcal{P}_{ck}$
$(N, p, q) \xleftarrow{\$} \mathcal{RSA}_k[p = 1 \bmod e']$	$(N, p, q) \xleftarrow{\$} \mathcal{RSA}_k[p = 1 \bmod e]$
If $\gcd(e, \phi(N)) \neq 1$ then return $\perp$	Return (N, e)
$d \leftarrow e^{-1} \bmod \phi(N)$	
Return $((N, e), (N, d))$	

The fact that algorithm $\mathcal{F}_1$ has only a very small probability of failure (returning $\perp$) follows from the fact that $\phi(N)$ can have only a constant number of prime factors of length ck and Bertrand's Postulate.

Proposition 5.1. *Suppose there is a distinguisher D against* LTDP_1*. Then there is a distinguisher D' such that for all $k \in \mathbb{N}$*

$$\mathbf{Adv}^{\mathrm{ltdp}}_{\mathsf{LTDP}_1, D}(k) \;\leq\; \mathbf{Adv}^{\Phi\mathrm{A}}_{c,D'}(k).$$

Furthermore, the running-time of D' is that of D. LTDP_1 *has lossiness ck.*

The proof is straightforward.

From a practical perspective, a drawback of LTDP_1 is that $\mathcal{F}_1$ chooses $N = pq$ in a non-standard way, so that it hides a prime of the same length as e. Moreover, for small values of e it returns $\perp$ with high probability. This is done for consistency

[9] This is done by choosing a uniform $(1/2 - c)k$-bit number x until $p = xe + 1$ is a prime.

with how [16] formulated ΦA. But, to address this, we also propose what we call the *Enhanced* ΦA (EΦA), which says that N generated in the non-standard way (i.e., by $\mathcal{F}_1$) is indistinguishable from one chosen at random subject to $\gcd(e, \phi(N)) = 1$.[10] We conjecture that EΦA holds for all values of c that ΦA does. Details follow.

ENHANCED Φ-HIDING ASSUMPTION. We say that the *Enhanced Φ-Hiding Assumption* (EΦA) holds for c if the following two distributions $\mathcal{R}_{1^*}$ and $\mathcal{L}_{1^*}$ are computationally indistinguishable:

$$\mathcal{R}_{1^*} = \{(e, N) \,:\, e \xleftarrow{\$} \mathcal{P}_{ck}\,;\ (N, p, q) \xleftarrow{\$} \mathcal{RSA}_k\}$$
$$\mathcal{L}_{1^*} = \{(e, N) \,:\, e \xleftarrow{\$} \mathcal{P}_{ck}\,;\ (N, p, q) \xleftarrow{\$} \mathcal{RSA}_k[p = 1 \bmod e])\}.$$

To a distinguisher D, we associate its *EΦA advantage* defined as

$$\mathbf{Adv}^{\mathrm{E\Phi A}}_{c,D}(k) \;=\; \Pr[\,D(\mathcal{R}_{1^*}) \Rightarrow 1\,] - \Pr[\,D(\mathcal{L}_{1^*}) \Rightarrow 1\,]\,.$$

As before, distributions $\mathcal{R}_{1^*}, \mathcal{L}_{1^*}$ can be sampled efficiently assuming the widely accepted Extended Riemann Hypothesis. We conjecture that EΦA holds for all values of $\mathcal{K}_\phi$, c that ΦA does.

RSA LTDP FROM EΦA. Now define $\mathsf{LTDP}_{1^*} = (\mathcal{F}_{1^*}, \mathcal{F}'_{1^*})$ where

Algorithm $\mathcal{F}_{1^*}$
$e \xleftarrow{\$} \mathcal{P}_{ck}$
$(N, p, q) \xleftarrow{\$} \mathcal{RSA}_k$
If $\gcd(e, \phi(N)) \neq 1$ then Return $\perp$
Else Return $(N, e), (N, d)$

and $\mathcal{F}'_{1^*} = \mathcal{F}'_1$ in Sect. 5.2. Again we have the probability that $\mathcal{F}_{1^*}$ returns $\perp$ is very small. We stress that $\mathcal{F}_{1^*}$, unlike $\mathcal{F}_1$, chooses p, q at random as is typical in practice. We have the following proposition.

Proposition 5.2. *If the Enhanced Φ-Hiding Assumption holds for c, then* $\mathsf{LTDP}_{1^*} = (\mathcal{F}_{1^*}, \mathcal{F}'_{1^*})$ *is an RSA LTDP with lossiness ck. In particular, suppose there is a distinguisher D against* LTDP_{1^*}*. Then there is a distinguisher D' such that*

$$\mathbf{Adv}^{\mathrm{ltdp}}_{\mathsf{LTDP}_{1^*},D}(k) \;\le\; \mathbf{Adv}^{\mathrm{E\Phi A}}_{c,D'}(k).$$

Furthermore, the running-time of D' is that of D.

Again, the proof is straightforward.

PARAMETERS FOR LTDP_1. When e is too large, ΦA can be broken by using Coppersmith's method for finding small roots of a univariate modulo an unknown divisor of N [21,43].

[10] Additionally, in practice the encryption exponent e is usually fixed. This can be addressed by parameterizing EΦA by a fixed e instead of choosing it at random. Note that for $e = 3$ one should make both $e \mid p - 1$ and $e \mid q - 1$ in the lossy case (otherwise the assumption is false [16]).

Namely, consider the polynomial $r(x) = ex+1 \mod p$. Coppersmith's method allows us to find all roots of r smaller than $N^{1/4}$, and thus factor N, in lossy mode in polynomial time if $c \geq 1/4$. (This is essentially the "factoring with high bits known" attack.) More specifically, applying [43, Theorem1], N can be factored in time poly($\log N$) and $O(N^{\varepsilon})$ if $c = 1/4 - \varepsilon$ (i.e., $\log e \geq \log N(1/4 - \varepsilon)$). For example, with modulus size $k = 2048$, we can set $\varepsilon = .04$ for 80-bit security (to enforce $k\varepsilon \geq 80$) and obtain $2048(1/4 - 0.04) = 430$ bits of lossiness.

5.3. *RSA Lossy TDP from Multi-prime Φ-Hiding*

Multi-prime RSA (according to [41] the earliest reference is [54]) is a generalization of RSA to moduli $N = p_1 \cdots p_m$ of length k with $m \geq 2$ prime factors of equal bit-length. Multi-prime RSA is of interest to practitioners since it allows to speed up decryption and is included in RSA PKCS #1 v2.1. We are interested in it here because for it we can show greater lossiness, in particular with smaller encryption exponent e.

Notation and terminology. Let $m \geq 2$ be fixed. We denote by $\mathcal{MRSA}_k$ the set of all tuples $(N, p_1, \ldots, p_m)$, where $N = p_1 \cdots p_m$ is the product of distinct k/m-bit primes. Such an N is called an *m-prime RSA modulus*. By $(N, p_1, \ldots, p_m) \stackrel{\$}{\leftarrow} \mathcal{MRSA}_k$ we mean that $(N, p_1, \ldots, p_m)$ is sampled according to the uniform distribution on $\mathcal{MRSA}_k$. The rest of the notation and terminology of Sect. 5 is extended to the multi-prime setting in the obvious way.

Multi Φ-hiding assumption. For an m-prime RSA modulus N, let us say that N *mϕ-hides* a prime e if $e \mid p_i - 1$ for all $1 \leq i \leq m-1$. Intuitively, the assumption is that, given such N, it is hard to distinguish primes which are $m\phi$-hidden by N from those that do not divide $p_i - 1$ for any $1 \leq i \leq m$. Formally, let $m = m(k) \geq 2$ be a polynomial and let $c = c(k)$ be an inverse polynomial determined later. Consider the following two distributions:

$$\mathcal{R}_2 = \{(e, N) \; : \; e, e' \stackrel{\$}{\leftarrow} \mathcal{P}_{ck} \, ; \; (N, p_1, \ldots, p_t) \stackrel{\$}{\leftarrow} \mathcal{MRSA}_k[p_{i \leq m-1} = 1 \bmod e']\}$$
$$\mathcal{L}_2 = \{(e, N) \; : \; e \stackrel{\$}{\leftarrow} \mathcal{P}_{ck} \, ; \; (N, p_1, \ldots, p_t) \stackrel{\$}{\leftarrow} \mathcal{MRSA}_k[p_{i \leq m-1} = 1 \bmod e]\}.$$

Above and in what follows, by $p_{i \leq m-1} = 1 \bmod e$ we mean that $p_i = 1 \bmod e$ for all $1 \leq i \leq m-1$. To a distinguisher D, we associate its $M\Phi A$ *advantage* defined as

$$\mathbf{Adv}^{\mathrm{M\Phi A}}_{m,c,D}(k) \; = \; \Pr[\, D(\mathcal{R}_2) \Rightarrow 1\,] - \Pr[\, D(\mathcal{L}_2) \Rightarrow 1\,]\,.$$

As before, distributions $\mathcal{R}_2$, $\mathcal{L}_2$ can be sampled efficiently assuming the widely accepted Extended Riemann Hypothesis.

Note that if we had required that in the lossy case $N = p_1 \cdots p_m$ is such that $e \mid p_i$ for all $1 \leq i \leq m$, then in this case we would always have $N = 1 \bmod e$. But in the injective case N mod e is random, which would lead to a trivial distinguishing algorithm. This explains why we do not impose $e \mid p_m$ in the lossy case above.

Multi-prime RSA LTDP from MΦA. We construct a multi-prime RSA LTDP based on MΦA having lossiness $(m-1)\log e$, where in lossy mode N $m\phi$-hides e. Namely, define $\mathsf{LTDP}_2 = (\mathcal{F}_2, \mathcal{F}_2')$ as follows:

Algorithm $\mathcal{F}_2$	**Algorithm** $\mathcal{F}_2'$
$e, e' \xleftarrow{\$} \mathcal{P}_{ck}$	$e \xleftarrow{\$} \mathcal{P}_{ck}$
$(N, p_1, \ldots, p_m) \xleftarrow{\$} \mathcal{MRSA}_k[p_{i\le m-1} = 1 \bmod e']$	$(N, p_1, \ldots, p_m) \xleftarrow{\$} \mathcal{MRSA}_k [p_{i\le m-1} = 1 \bmod e]$
If $\gcd(e, \phi(N)) \ne 1$ then Return $\perp$	Return (N, e)
$d \leftarrow e^{-1} \bmod \phi(N)$	
Else return $(N, e), (N, d)$	

Proposition 5.3. *Suppose there is a distinguisher D against* LTDP_2. *Then there is a distinguisher D' such that for all $k \in \mathbb{N}$*

$$\mathbf{Adv}^{\mathrm{ltdp}}_{\mathsf{LTDP}_2, D}(k) \le \mathbf{Adv}^{\mathrm{M\Phi A}}_{m,c,D'}(k).$$

Furthermore, the running-time of D' is that of D. LTDP_2 *has lossiness $(m-1)ck$.*

The proof is straightforward.

Parameters for LTDP_2. Using [35, Section 3] we can break the MΦA in time poly$(\log N)$ and $O(N^{\varepsilon})$ if

$$c \ge 1/m - \frac{2}{3\sqrt{m^3}} - \varepsilon.$$

For $m \ge 3$ this improves the bound with $c \ge 1/m - 1/m^2 - \varepsilon$ obtained from "factoring with high bits known"; for $m \ge 4$ this improves the bound with $c \ge 1/m - 2\frac{(1/m)^{(1/(m-1)} - (1/m)^{m/(m-1)}}{m(m-1)} - \varepsilon$ from the preliminary version [37]. We also note that Tosu and Kunihiro [60] showed a bound with $c \ge 1/m - \frac{2}{em\log(m+1)}$ where e is the base of the natural logarithm, which is better than [35] for $m \ge 6$ (see [60, Section4.4] for comparison).

For example, with modulus size $k = 2048$ and $m = 3$ $(m = 4, 5)$ we set $\varepsilon = .04$ (for about 80-bit security) and obtain 676 (778, 822) bits of lossiness for LTDP_2, according to Proposition 5.3.

5.4. *Small-Exponent RSA LTDP from* 2*-vs-m Primes*

For efficiency reasons, the public RSA exponent e is typically not chosen to be too large in practice. (For example, researchers at UC San Diego [63] found that 99.5 % of the certificates in the campus's TLS corpus had $e = 2^{16} + 1$.) Therefore, we investigate the possibility of using an additional assumption to "amplify" the lossiness of RSA for small e.

Our high-level idea is to assume that it is hard to distinguish $N = pq$ where p, q are primes of length $k/2$ from $N = p_1 \cdots p_m$ for $m > 2$, where $p_1, \ldots, p_m$ are primes of length k/m (which we call the "2-vs-m Primes" Assumption). This assumption is a generalization of the "2-vs-3 Primes" Assumptions introduced in [8] and used independently to construct a "slightly lossy" TDF based on modular squaring [45]. Combined with the MΦA Assumption of Sect. 5.3, we obtain $(m-1)\log e$ bits of lossiness from *standard* (two-prime) RSA. Let us state our assumption and construction formally.

2-VS-m PRIMES ASSUMPTION. We say that the *2-vs-m primes assumption* holds for m if the following two distributions $\mathcal{N}_2$ and $\mathcal{N}_m$ are computationally indistinguishable:

$$\mathcal{N}_2 = \{N \,:\, e \xleftarrow{\$} \mathcal{P}_{ck}\,;\; (N, p, q) \xleftarrow{\$} \mathcal{RSA}_k[p = 1 \bmod e]\}$$
$$\mathcal{N}_m = \{N \,:\, e \xleftarrow{\$} \mathcal{P}_{ck}\,;\; (N, p, q) \xleftarrow{\$} \mathcal{MRSA}_k[p_{i \le m-1} = 1 \mod e]\}.$$

To a distinguisher D, we associate its *HFA-advantage* defined as

$$\mathbf{Adv}_m^{\mathrm{2vmp}}(D) \;=\; \Pr[\, D(\mathcal{N}_2) \Rightarrow 1\,] - \Pr[\, D(\mathcal{N}_m) \Rightarrow 1\,]\,.$$

RSA LTDP FROM 2-VS-m PRIMES + MΦA. Define $\mathsf{LTDP}_3 = (\mathcal{F}_3, \mathcal{F}_3')$ as follows:

Algorithm $\mathcal{F}_3$	**Algorithm** $\mathcal{F}_3'$
$e, e' \xleftarrow{\$} \mathcal{P}_{ck}$	$e \xleftarrow{\$} \mathcal{P}_{ck}$
$(N, p, q) \xleftarrow{\$} \mathcal{RSA}_k[p = 1 \bmod e']$	$(N, p_1, \ldots, p_m) \xleftarrow{\$} \mathcal{MRSA}_k[p_{i \le m-1}$ $= 1 \bmod e]$
If $\gcd(e, \phi(N)) \neq 1$ then Return $\perp$	Return (N, e)
Else Return $(N, e), (N, d)$	

Proposition 5.4. *If the 2-vs-m Primes Assumption holds for m and the Multi-Prime Φ-Hiding Assumption holds for m, e, then* $\mathsf{LTDP}_3 = (\mathcal{F}_3, \mathcal{F}_3')$ *is an RSA LTDP with lossiness* $(m-1)ck$*. In particular, suppose there is a distinguisher D against* LTDP_3*. Then there is a distinguisher* D_1, D_2 *such that*

$$\mathbf{Adv}_{\mathsf{LTDP}_3}^{\mathrm{ltdp}}(D) \;\le\; \mathbf{Adv}_m^{\mathrm{2vmp}}(D_1) + \mathbf{Adv}_{m,c}^{\mathrm{M\Phi A}}(D_2).$$

Furthermore, the running-time of D_1, D_2 *is that of D.*

Again, the proof is a straightforward.

PARAMETERS FOR LTDP_3. We note that m in the construction cannot be too large; otherwise, a small factor of N in the lossy case can be recovered by the elliptic curve factoring method due to Lenstra [41], whose running-time is proportional to the smallest factor of N. The largest factor recovered by the method so far was 223-bits in length [64]. Thus, for example using 2048-bit RSA with $e = 2^{16} - 1$, if we assume it is hard to recover factors larger than that we can get $8 \cdot 16 = 128$ bits of lossiness under the HFA plus MΦA where $m = 9$.

Enhanced HFA. As in the previous cases, to address the fact that in practice $N = pq$ is chosen at random and not subject to p hiding a prime of the same bit-length as e, we may define an *enhanced* version of HFA. Then under the enhanced HFA + enhanced MΦA assumptions, we obtain the same amount of lossiness for standard 2-prime RSA.

6. Instantiating RSA-OAEP

By combining the results of Sects. 3, 4, and 5, we obtain standard model instantiations of RSA-OAEP under chosen-plaintext attack.

Regularity. In particular, we would like to apply part (2) of Theorem 4.2 in this case, as it is not hard to see that under all of the assumptions discussed in Sect. 5, RSA is a *regular* lossy TDP on the domain $\mathbb{Z}_N^*$. Unfortunately, this is different from $\{0, 1\}^{\rho+\mu}$ (identified as integers), the range of OAEP. In RSA PKCS #1 v2.1, the mismatch is handled by selecting $\rho + \mu = \lfloor \log N \rfloor - 16$, and viewing OAEP's output as an integer less than $2^{\rho+\mu} < N/2^{16}$ (i.e., the most significant two bytes of the output are zeroed out). The problem is that in the lossy case RSA may not be regular on the subdomain $\{0, \ldots, 2^{\rho+\mu}\}$ (although this has been proven in subsequent work; see below). So, we just detail the weaker parameters given by part (1) of Theorem 4.2 here.

Concrete parameters. Since the results in Sect. 5 have several cases and the parameter settings are rather involved, we avoid stating an explicit theorem about RSA-OAEP. If we use part (1) of Theorem 4.2, one can see that for $u = 80$ bits security, messages of roughly $\mu \approx k - s - 3 \cdot 80$ bits can be encrypted (for sufficiently large t). For concreteness, we give two example parameter settings. Using the Multi Φ-Hiding Assumption with $k = 1024$ bits and 3 primes, we obtain $\ell = k - s = 291$ bits of lossiness and hence can encrypt messages of length $\mu = 40$ bits (for $t \approx 400$). Using the Φ-Hiding Assumption with $k = 2048$, we obtain $\ell = k - s = 430$ bits of lossiness and hence can encrypt messages of length $\mu = 160$ bits (for $t \approx 150$).

Subsequent improvements. The approximately regularity of RSA on the above subdomain (and, more generally, on arithmetic progressions of sufficient length) has subsequently been shown by Lewko et al. [42]. This allows us to obtain essentially the better parameters given by part (2) of Theorem 4.2. For example, using the Φ-Hiding Assumption with $k = 2048$, we can encrypt messages of length 274 bits (see [42, Section5.3]).

Acknowledgements

We thank Mihir Bellare, Alexandra Boldyreva, Dan Brown, Yevgeniy Dodis, Mathias Herrmann, Jason Hinek, Arjen Lenstra, Alex May, Phil Rogaway, and the anonymous reviewers of Crypto 2010 and the Journal of Cryptology for helpful comments. In particular, we thank Dan for reminding us of [16, Remark2,p. 6], Alex and Mathias for pointing out the improved attacks in Sect. 5.3, Phil for encouraging us to consider the case of small e more closely and for telling us that KI security as defined in Appendix 8 was previously considered by [44], and Yevgeniy for suggesting the statement of Lemma 4.5 (our original lemma was specific to OAEP).

Part of this work was done, while E.K. was at CWI, Amsterdam. E.K. is funded by ERC Project ERCC (FP7/615074) and the German Federal Ministry for Education and Research. Part of this work was done while A.O. was at Georgia Institute of Technology, supported in part by NSF award #0545659 and NSF Cyber Trust award #0831184. A.S. was supported in part by NSF awards #0747294, 0729171.

Eike Kiltz was partially supported by DFG grant KI 795/4-1 and ERC Project ERCC (FP7/615074). Adam Smith was funded by US National Science Foundation award CCF-0747294.

7. Appendix 1: Proof of Lemma 4.5

We introduce the following notation for the proof. For a random variable V with range $\mathcal{V}$, we define the *collision probability* of V as $\mathrm{Col}(V) = \Pr\left[\, V = V' \,\right] = \sum_{v\in\mathcal{V}} P_V(v)^2$ where V' is an independent copy of V, and for an event $\mathcal{E}$ we define the *conditional collision probability* $\mathrm{Col}_{\mathcal{E}}(V) = \Pr\left[\, V = V' \mid \mathcal{E} \,\right]$. For random variables V, W, we define the *square of the 2-distance* as $D(V, W) = \sum_v \left(P_V(v) - P_W(v)\right)^2$.

Writing $\mathbf{E}_k$ for expectation over the choice of random k from $\mathcal{K}$, we have

$$\begin{aligned}
\Delta\big((K, g(X, h(K, X))), (K, g(X, U))\big) \;&=\; \mathbf{E}_k\big[\Delta\big(g(X, h(k, X)), g(X, U)\big)\big] \qquad (9)\\
\le\; \frac{1}{2}\mathbf{E}_k&\left[\sqrt{|S|\, D\big(g(X, h(k, X)), g(X, U)\big)}\right]\\
\le\; \frac{1}{2}&\sqrt{|S|\,\mathbf{E}_k\big[D\big(g(X, h(k, X)), g(X, U)\big)\big]} \qquad (10)
\end{aligned}$$

where the first inequality is by Cauchy-Swartz and the second is by Jensen's inequality. We now show

$$\mathbf{E}_k\big[D\big(g(X, h(k, X)), g(X, U)\big)\big] \le \mathrm{Col}(X)$$

from which the theorem follows. Write $(X, Y_k) = (X, h(k, X))$ for an arbitrary but fixed k. Then

$$\begin{aligned}
D\big(g(X, Y_k), g(X, U)\big) \;&=\; \sum_s \big(P_{g(X,Y_k)}(s) - P_{g(X,U)}(s)\big)^2\\
&= \sum_s P_{g(X,Y_k)}(s)^2 - 2\sum_s P_{g(X,Y_k)}(s)P_{g(X,U)}(s)\\
&\quad + \sum_s P_{g(X,U)}(s)^2\,.
\end{aligned}$$

Using the Kronecker delta $\delta_{s,s'}$ which equals 1 if $s = s'$ and else 0 for all $s, s' \in S$, we can write $P_{g(X,Y_k)}(s) = \sum_x P_X(x)\delta_{g(x,h(k,x)),s}$, and thus

$$\begin{aligned}\sum_s P_{g(X,Y_k)}(s)^2 &= \sum_s \Big(\sum_x P_X(x)\delta_{g(x,h(k,x)),s}\Big)\Big(\sum_{x'} P_X(x')\delta_{g(x',h(k,x')),s}\Big)\\ &= \sum_{x,x'} P_X(x)P_X(x')\delta_{g(h(k,x)),g(h(k,x'))}.\end{aligned}$$

We use the pairwise independence of h to rewrite this in terms of collision probabilities:

$$\begin{aligned}\mathbf{E}_k\Big[\sum_s P_{g(X,Y_k)}(s)^2\Big] &= \sum_{x,x'} P_X(x)P_X(x')\mathbf{E}_k[\delta_{g(x,h(k,x)),g(x',h(k,x'))}]\\ &= \mathrm{Col}(X) \;+\; \mathrm{Col}_{\mathcal{E}}(g(X,U))(1-\mathrm{Col}(X))\,, \qquad (11)\end{aligned}$$

where the subscript $\mathcal{E}$ denotes (conditioning on) the event that $X \neq X'$. That is,

$$\mathrm{Col}_{\mathcal{E}}(g(X,U)) \;=\; \Pr\big[\,g(X,U) = g(X',U') \;|\; X \neq X'\,\big]\,.$$

Similarly,

$$\begin{aligned}\sum_s P_{g(X,Y_k)}(s)P_{g(X,U)}(s) &= \sum_s \Big(\sum_x P_X(x)\delta_{g(x,h(k,x)),s}\Big)\\ &\quad \Big(\sum_{x',u} P_X(x')P_U(u)\delta_{g(x',u),s}\Big)\\ &= \sum_x\sum_{x'}\sum_u P_X(x)P_X(x')P_U(u)\delta_{g(x,h(k,x)),g(x',u)}\end{aligned}$$

so that

$$\begin{aligned}\mathbf{E}_k\Big[\sum_s P_{g(X,Y_k)}(s)P_{g(X,U)}(s)\Big] &= \sum_x\sum_{x'}\sum_u P_X(x)P_X(x')P_U(u)\mathbf{E}_k[\delta_{g(x,h(k,x)),g(x',u)}]\\ &= \mathrm{Col}(g(X,U)) \;=\; \mathrm{Col}_{\overline{\mathcal{E}}}(g(X,U))\mathrm{Col}(X)\\ &\quad + \mathrm{Col}_{\mathcal{E}}(g(X,U))(1-\mathrm{Col}(X))\,.\end{aligned}$$

where $\mathcal{E}$ is defined as above. Note that the only difference between the expression above and that in (11) is that even when $X = X'$, a collision is not guaranteed.

Finally,

$$\begin{aligned}\sum_s P_{g(X,U)}(s)^2 &= \mathrm{Col}(g(X,U))\\ &= \mathrm{Col}_{\overline{\mathcal{E}}}(g(X,U))\mathrm{Col}(X) + \mathrm{Col}_{\mathcal{E}}(g(X,U))(1-\mathrm{Col}(X))\end{aligned}$$

as well. By combining the above, we have

$$\begin{aligned}
\mathbf{E}_k\big[D\big(g(X, Y_k), f(X, U)\big)\big] &= \mathrm{Col}(X) + \mathrm{Col}_{\mathcal{E}}(g(X, U))(1 - \mathrm{Col}(X)) \\
&\quad - 2(\mathrm{Col}_{\overline{\mathcal{E}}}(g(X, U))\mathrm{Col}(X) \\
&\quad + \mathrm{Col}_{\mathcal{E}}(g(X, U))(1 - \mathrm{Col}(X))) \\
&\quad + \mathrm{Col}_{\overline{\mathcal{E}}}(g(X, U))\mathrm{Col}(X) + \mathrm{Col}_{\mathcal{E}}(g(X, U))(1-\mathrm{Col}(X)) \\
&= (1 - \mathrm{Col}_{\overline{\mathcal{E}}}(g(X, U)))\mathrm{Col}(X) \\
&\le \mathrm{Col}(X).
\end{aligned}$$

To complete the proof, we can plug the bound above into (10):

$$\begin{aligned}
\Delta\big((K, g(X, h(K, X))), (K, g(X, U))\big) &\le \frac{1}{2}\sqrt{|S|\,\mathbf{E}_k\big[D\big(g(X, h(k, X)), g(X, U)\big)\big]} \\
&\le \frac{1}{2}\sqrt{|S|\mathrm{Col}(X)}.
\end{aligned}$$

By the assumption on the min-entropy of X, the collision probability $\mathrm{Col}(X)$ is at most $4\hat{\varepsilon}^2/|S|$. So the statistical distance $\Delta\big((K, g(X, h(K, X))), (K, g(X, U))\big)$ is at most $\hat{\varepsilon}$, as desired. □

8. Appendix 2: Security of OAEP Under Key-Independent Chosen-Plaintext Attack

The commonly-accepted notions of security for encryption ask for privacy with respect to messages that may depend on the public key. We define here a notion of privacy for messages *not* depending on the public key. We mention that such a definition appears for example in the work of Micali et al. [44] (under the name "three-pass," versus "one-pass," cryptosystem), in the text of Goldreich [30], and in the context of the recent work on deterministic encryption [2].

THE DEFINITION. To an encryption scheme $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ and an adversary $B = (B_1, B_2)$ we associate

$$\begin{array}{l}
\textbf{Experiment } \mathbf{Exp}^{\text{indki-cpa}}_{\Pi,B}(k) \\
\quad b \xleftarrow{\$} \{0,1\}\,;\ (m_0, m_1, s) \xleftarrow{\$} B_1 \\
\quad (pk, sk) \xleftarrow{\$} \mathcal{K}\,;\ c \xleftarrow{\$} \mathcal{E}(pk, m_b) \\
\quad d \xleftarrow{\$} B_2(pk, c, s) \\
\quad \text{If } d = b \text{ then Return 1 Else Return 0}
\end{array}$$

We require $|m_0| = |m_1|$ above. Define the *indki-cpa advantage* of B against Π as

$$\mathbf{Adv}^{\text{indki-cpa}}_{\Pi,B}(k) = 2 \cdot \Pr\Big[\mathbf{Exp}^{\text{indki-cpa}}_{\Pi,B}(k) \Rightarrow 1\Big] - 1.$$

Remarks. While non-standard, KI security seems adequate for some applications. For example, in [30] Goldreich points out that high-level applications that use encryption as a tool do so in a key-oblivious manner, and Bellare et al. [2] argue that in real life public keys are abstractions hidden in our software, so messages are unlikely to depend on them. KI security also suffices for hybrid encryption.

The result. We can show a standard model instantiation under KI security directly from Lemma 4.5, where G is any *pairwise-independent* function. This is captured by the theorem below.

Theorem 8.1. *Let* $\mathsf{LTDP} = (\mathcal{F}, \mathcal{F}')$ *be an LTDP with residual leakage* ℓ*, and let* OAEP *be the encryption scheme associated to* $\mathcal{F}$*, hash functions* G, H*, and a parameter* $k_0 < k$*. Suppose* G *is pairwise-independent. Let* $\varepsilon > 0$*. Then for any* $k_0 \geq \ell + 2\log(1/\varepsilon) - 2$ *and any INDKI-CPA adversary* B *against* OAEP*, there is a distinguisher* D *against* LTDP *such that*

$$\mathbf{Adv}^{\text{indki-cpa}}_{\mathsf{OAEP},B}(k) \leq \mathbf{Adv}^{\text{ltdp}}_{\mathsf{LTDP},D}(k) + \varepsilon.$$

Furthermore, the running-time of D *is the time to run* B.

As we mentioned, the proof is a simple hybrid argument concluding by Lemma 4.5.

References

[1] M. Abdalla, M. Bellare, P. Rogaway, The oracle Diffie–Hellman assumptions and an analysis of DHIES, in D. Naccache, editor, *CT-RSA 2001*. LNCS, vol. 2020 (Springer, Heidelberg, April 2001), pp. 143–158

[2] B. Barak, R. Shaltiel, E. Tromer, True random number generators secure in a changing environment, in C.D. Walter, Ç.K. Koç, C. Paar, editors, *CHES 2003*. LNCS, vol. 2779 (Springer, Heidelberg, September 2003), pp. 166–180

[3] M. Bellare, A. Boldyreva, A. O'Neill, Deterministic and efficiently searchable encryption, in A. Menezes, editor, *CRYPTO 2007*. LNCS, vol. 4622 (Springer, Heidelberg, August 2007), pp. 535–552

[4] M. Bellare, V.T. Hoang, S. Keelveedhi, Instantiating random oracles via UCEs, in R. Canetti, J.A. Garay, editors, *CRYPTO 2013, Part II*. LNCS, vol. 8043 (Springer, Heidelberg, August 2013), pp. 398–415

[5] M. Bellare, A. Palacio, Towards plaintext-aware public-key encryption without random oracles, in P.J. Lee, editor, *ASIACRYPT 2004*. LNCS, vol. 3329 (Springer, Heidelberg, December 2004), pp. 48–62

[6] M. Bellare, P. Rogaway, Random oracles are practical: a paradigm for designing efficient protocols. in V. Ashby, editor, *ACM CCS 93*. (ACM Press, November 1993), pp. 62–73

[7] M. Bellare, P. Rogaway, Optimal asymmetric encryption, in A. De Santis, editor, *EUROCRYPT'94*. LNCS, vol. 950 (Springer, Heidelberg, May 1995), pp. 92–111

[8] M. Bellare, J. Rompel, Randomness-efficient oblivious sampling, in *35th FOCS*. (IEEE Computer Society Press, November 1994), pp. 276–287

[9] M. Blum, P. Feldman, S. Micali, Proving security against chosen cyphertext attacks, in S. Goldwasser, editor, *CRYPTO'88*. LNCS, vol. 403 (Springer, Heidelberg, August 1990), pp. 256–268

[10] A. Boldyreva, D. Cash, M. Fischlin, B. Warinschi, Foundations of non-malleable hash and one-way functions, in M. Matsui, editor, *ASIACRYPT 2009*. LNCS, vol. 5912 (Springer, Heidelberg, December 2009), pp. 524–541

[11] A. Boldyreva, S. Fehr, A. O'Neill, On notions of security for deterministic encryption, and efficient constructions without random oracles, in D. Wagner, editor, *CRYPTO 2008*. LNCS, vol. 5157 (Springer, Heidelberg, August 2008), pp. 335–359

[12] A. Boldyreva, M. Fischlin, Analysis of random oracle instantiation scenarios for OAEP and other practical schemes, in V. Shoup, editor, *CRYPTO 2005*. LNCS, vol. 3621 (Springer, Heidelberg, August 2005), pp. 412–429

[13] A. Boldyreva, M. Fischlin, On the security of OAEP, in X. Lai, K. Chen, editors, *ASIACRYPT 2006*. LNCS, vol. 4284 (Springer, Heidelberg, December 2006), pp. 210–225

[14] D. Boneh, Simplified OAEP for the RSA and Rabin functions, in J. Kilian, editor, *CRYPTO 2001*. LNCS, vol. 2139 (Springer, Heidelberg, August 2001), pp. 275–291

[15] D.R.L. Brown, What hashes make RSA-OAEP secure? Cryptology ePrint Archive. Report 2006/223. http://eprint.iacr.org/ (2006)

[16] C. Cachin, Efficient private bidding and auctions with an oblivious third party, in *ACM CCS 99*. (ACM Press, November 1999), pp. 120–127

[17] C. Cachin, S. Micali, M. Stadler, Computationally private information retrieval with polylogarithmic communication, in J. Stern, editor, *EUROCRYPT'99*. LNCS, vol. 1592 (Springer, Heidelberg, May 1999), pp. 402–414

[18] R. Canetti, Towards realizing random oracles: hash functions that hide all partial information, in B.S. Kaliski Jr., editor, *CRYPTO'97*. LNCS, vol. 1294 (Springer, Heidelberg, August 1997), pp. 455–469

[19] R. Canetti, R.R. Dakdouk, Extractable perfectly one-way functions, in L. Aceto, I. Damgård, L.A. Goldberg, M.M. Halldórsson, A. Ingólfsdóttir, I. Walukiewicz, editors, *ICALP 2008, Part II*. LNCS, vol. 5126 (Springer, Heidelberg, July 2008), pp. 449–460

[20] R. Canetti, O. Goldreich, S. Halevi, The random oracle methodology, revisited. *J. ACM*, **51**(4), 557–594 (2004)

[21] R. Canetti, D. Micciancio, O. Reingold, Perfectly one-way probabilistic hash functions (preliminary version), in *30th ACM STOC*. (ACM Press, May 1998), pp. 131–140

[22] D. Coppersmith, Small solutions to polynomial equations, and low exponent RSA vulnerabilities. *J. Cryptol.*, **10**(4), 233–260 (1997)

[23] J.-S. Coron, M. Joye, D. Naccache, P. Paillier, New attacks on PKCS#1 v1.5 encryption, in B. Preneel, editor, *EUROCRYPT 2000*. LNCS, vol. 1807 (Springer, Heidelberg, May 2000), pp. 369–381

[24] J.-S. Coron, M. Joye, D. Naccache, P. Paillier, Universal padding schemes for RSA, in M. Yung, editor, *CRYPTO 2002*. LNCS, vol. 2442 (Springer, Heidelberg, August 2002), pp. 226–241

[25] Y. Dodis, R. Oliveira, K. Pietrzak, On the generic insecurity of the full domain hash, in V. Shoup, editor, *CRYPTO 2005*. LNCS, vol. 3621 (Springer, Heidelberg, August 2005), pp. 449–466

[26] Y. Dodis, A. Sahai, A. Smith, On perfect and adaptive security in exposure-resilient cryptography, in B. Pfitzmann, editor, *EUROCRYPT 2001*. LNCS, vol. 2045 (Springer, Heidelberg, May 2001), pp. 301–324

[27] Y. Dodis, A. Smith, Correcting errors without leaking partial information, in H.N. Gabow, R. Fagin, editors, *37th ACM STOC*. (ACM Press, May 2005), pp. 654–663

[28] D.M. Freeman, O. Goldreich, E. Kiltz, A. Rosen, G. Segev, More constructions of lossy and correlation-secure trapdoor functions. *J. Cryptol.*, **26**(1), 39–74 (2013)

[29] E. Fujisaki, T. Okamoto, D. Pointcheval, J. Stern, RSA-OAEP is secure under the RSA assumption. *J. Cryptol.*, **17**(2), 81–104 (2004)

[30] C. Gentry, P.D. Mackenzie, Z. Ramzan, Password authenticated key exchange using hidden smooth subgroups, in V. Atluri, C. Meadows, A. Juels, editors, *ACM CCS 05*. (ACM Press, November 2005), pp. 299–309

[31] O. Goldreich, *Foundations of Cryptography: Basic Applications*, vol. 2 (Cambridge University Press, Cambridge, UK, 2004)

[32] S. Goldwasser, S. Micali, Probabilistic encryption. *J. Comput. Syst. Sci.*, **28**(2), 270–299 (1984)

[33] B. Harris, RSA Key Exchange for the Secure Shell (SSH) Transport Layer Protocol. RFC 4432

[34] B. Hemenway, R. Ostrovsky, Public-key locally-decodable codes, in D. Wagner, editor, *CRYPTO 2008*. LNCS, vol. 5157 (Springer, Heidelberg, August 2008), pp. 126–143

[35] B. Hemenway, R. Ostrovsky, A. Rosen, Non-committing encryption from ϕ-hiding, in Y. Dodis, J.B. Nielsen, editors, *TCC 2015, Part I*. LNCS, vol. 9014 of (Springer, Heidelberg, March 2015), pp. 591–608

[36] M. Herrmann, Improved cryptanalysis of the multi-prime ϕ-hiding assumption. in A. Nitaj, D. Pointcheval, editors, *AFRICACRYPT 11*. LNCS, vol. 6737 (Springer, Heidelberg, July 2011), pp. 92–99

[37] D. Hofheinz, E. Kiltz, The group of signed quadratic residues and applications, in S. Halevi, editor, *CRYPTO 2009*. LNCS, vol. 5677 (Springer, Heidelberg, August 2009), pp. 637–653
[38] E. Kiltz, K. Pietrzak, Personal communication (2009)
[39] E. Kiltz, A. O'Neill, A. Smith, Instantiability of RSA-OAEP under chosen-plaintext attack, in T. Rabin, editor, *CRYPTO 2010*. LNCS, vol. 6223 (Springer, Heidelberg, August 2010), pp. 295–313
[40] E. Kiltz, 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*. LNCS, vol. 5479 (Springer, Heidelberg, April 2009), pp. 389–406
[41] K. Kobara, H. Imai, OAEP++ : a very simple way to apply oaep to deterministic ow-cpa primitives. Cryptology ePrint Archive, Report 2002/130. http://eprint.iacr.org/ (2002)
[42] A.K. Lenstra, Unbelievable security. Matching AES security using public key systems (invited talk), in C. Boyd, editor, *ASIACRYPT 2001*. LNCS, vol. 2248 (Springer, Heidelberg, December 2001), pp. 67–86
[43] M. Lewko, A. O'Neill, A. Smith, Regularity of lossy RSA on subdomains and its applications, in T. Johansson, P.Q. Nguyen, editors, *EUROCRYPT 2013*. LNCS, vol. 7881 (Springer, Heidelberg, May 2013), pp. 55–75
[44] A. May, Using lll-reduction for solving rsa and factorization problems: a survey, in *LLL+25 Conference in Honour of the 25th Birthday of the LLL Algorithm* (2007)
[45] S. Micali, C. Rackoff, B. Sloan, The notion of security for probabilistic cryptosystems, in A.M. Odlyzko, editor, *CRYPTO'86*. LNCS, vol. 263 (Springer, Heidelberg, August 1987), pp. 381–392
[46] P. Mol, S. Yilek, Chosen-ciphertext security from slightly lossy trapdoor functions, in P.Q. Nguyen, D. Pointcheval, editors, *PKC 2010*. LNCS, vol. 6056 (Springer, Heidelberg, May 2010), pp. 296–311
[47] N. Nisan, D. Zuckerman, Randomness is linear in space. *J. Comput. Syst. Sci.*, **52**(1), 43–52 (1996)
[48] P. Paillier, J.L. Villar, Trading one-wayness against chosen-ciphertext security in factoring-based encryption, in X. Lai, K. Chen, editors, *ASIACRYPT 2006*. LNCS, vol. 4284 (Springer, Heidelberg, December 2006), pp. 252–266
[49] O. Pandey, R. Pass, V. Vaikuntanathan, Adaptive one-way functions and applications, in D. Wagner, editor, *CRYPTO 2008*. LNCS, vol. 5157 (Springer, Heidelberg, August 2008), pp. 57–74
[50] C. Peikert, B. Waters, Lossy trapdoor functions and their applications. *SIAM J. Comput.*, **40**(6), 1803–1844 (2011)
[51] Rsa public-key cryptography standards (pkcs). http://www.rsa.com/rsalabs/node.asp?id=2124
[52] M.O. Rabin, Digitalized signatures and public-key functions as intractable as factorization. Technical report (1979)
[53] C. Rackoff, D.R. Simon, Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack, in J. Feigenbaum, editor, *CRYPTO'91*. LNCS. vol. 576 (Springer, Heidelberg, August 1992), pp. 433–444
[54] R.L. Rivest, A. Shamir, L. Adelman, U.S. patent 4405829: cryptographic communications system and method
[55] R.L. Rivest, A. Shamir, L. Adelman, A method for obtaining public-key cryptosystems and digital signatures. Technical Memo MIT/LCS/TM-82, Massachusetts Institute of Technology, Laboratory for Computer Science (1977)
[56] C. Schridde, B. Freisleben, On the validity of the phi-hiding assumption in cryptographic protocols, in J. Pieprzyk, editor, *ASIACRYPT 2008*. LNCS, vol. 5350 (Springer, Heidelberg, December 2008), pp. 344–354
[57] Y. Seurin, On the lossiness of the Rabin trapdoor function, in H. Krawczyk, editor, *PKC 2014*. LNCS, vol. 8383 (Springer, Heidelberg, March 2014), pp. 380–398
[58] V. Shoup, OAEP reconsidered. *J. Cryptol.*, **15**(4), 223–249 (2002)
[59] A. Smith, Y. Zhang, On the regularity of lossy RSA—improved bounds and applications to padding-based encryption, in Y. Dodis, J.B. Nielsen, editors, *TCC 2015, Part I*. LNCS, vol. 9014 (Springer, Heidelberg, March 2015), pp. 609–628
[60] K. Tosu, N. Kunihiro, Optimal bounds for multi-prime phi-hiding assumption, in *Information Security and Privacy—17th Australasian Conference, ACISP 2012, Wollongong, NSW, Australia, July 9–11, 2012. Proceedings* (2012), pp. 1–14
[61] L. Trevisan, S.P. Vadhan, Extracting randomness from samplable distributions, in *41st FOCS* (IEEE Computer Society Press, November 2000), pp. 32–42

[62] M.N. Wegman, L. Carter, New hash functions and their use in authentication and set equality. *J. Comput. Syst. Sci.* **22**(3), 265–279 (1981)

[63] S. Yilek, E. Rescorla, H. Shacham, B. Enright, S. Savage, When private keys are public: results from the 2008 debian openssl vulnerability, in *Internet Measurement Conference*

[64] P. Zimmerman, Integer factoring records. http://www.loria.fr/~zimmerma/records/factor.html