Randomness-Dependent Message Security

Eleanor Birrell, Kai-Min Chung, Rafael Pass[*], and Sidharth Telang

Cornell University
{eleanor,chung,rafael,sidtelang}@cs.cornell.edu

Abstract. Traditional definitions of the security of encryption schemes assume that the messages encrypted are chosen independently of the randomness used by the encryption scheme. Recent works, implicitly by Myers and Shelat (FOCS'09) and Bellare et al (AsiaCrypt'09), and explicitly by Hemmenway and Ostrovsky (ECCC'10), consider *randomness-dependent message (RDM) security* of encryption schemes, where the message to be encrypted may be selected as a function—referred to as the RDM function—of the randomness used to encrypt this particular message, or other messages, but in a circular way. We carry out a systematic study of this notion. Our main results demonstrate the following:

- *Full RDM security*—where the RDM function may be an arbitrary polynomial-size circuit—is not possible.
- Any secure encryption scheme can be slightly modified, by just performing some *pre-processing to the randomness*, to satisfy *bounded-RDM* security, where the RDM function is restricted to be a circuit of *a priori* bounded polynomial size. The scheme, however, requires the randomness r needed to encrypt a message m to be slightly longer than the length of m (i.e., $|r| > |m| + \omega(\log k)$, where k is the security parameter).
- We present a black-box provability barrier to compilations of *arbitrary* public-key encryption into RDM-secure ones using just pre-processing of the randomness, whenever $|m| > |r| + \omega(\log k)$. On the other hand, under the DDH assumption, we demonstrate the existence of bounded-RDM secure schemes that can encrypt arbitrarily "long" messages using "short" randomness.

We finally note that the existence of public-key encryption schemes imply the existence of a fully RDM-secure encryption scheme in an "ultra-weak" Random-Oracle Model—where the security reduction need not "program" the oracle, or see the queries made by the adversary to the oracle; combined with our impossibility result, this yields the first example of a cryptographic task that has a secure implementation in such a weak Random-Oracle Model, but does not have a secure implementation without random oracles.

1   Introduction

Traditional definitions of secure encryption, including semantic (or CPA) security and CCA security, address the problem of how to securely communicate a message in the presence of a polynomially-bounded adversary that observes encrypted messages. In the standard approach, it is assumed that the message, the keys, and the randomness used to encrypt the message, are all chosen independently.

More recently, new definitions have emerged that relax some of these independence assumptions. Most notably, a line of work initiated independently by Camenisch and Lysyanskaya [21] and by Black, Rogaway, and Shrimpton [14] addresses the problem of "key-dependent" messages (KDM): namely, they consider the security of a public-key encryption scheme in a setting where the message to be encrypted may (adversarially) depend on the secret-key. A variant of this notion instead considers "circular" security: here, the adversary may observe a "cycle" of q messages $\overrightarrow{m}$ encrypted using different keys $(\overrightarrow{pk}, \overrightarrow{sk})$, but where m_i may depend on the depends on the secret-key $sk_{(i+1 \mod q)}$. One motivation for studying key-dependence arises in the context of hard-drive encryption: you want to encrypt your hard-drive, on which your secret-key is also found. Circular security arises naturally in a situation when two parties want to share their secret keys with each other (but not with the rest of the world): a natural solution to the problem would be for player 1 to send an encrypted version of his secret key using player 2's public key, and vice versa. For this protocol to be secure, circular security is needed. More recently, circular security has found important applications in the context of fully-homomorphic encryptions (indeed, to date, all known FHE schemes rely on the assumption that some underlying encryption scheme is circularly secure).

We here focus on an alternative relaxation of the classic independence assumptions, first implicitly considered by Myers and Shelat [36] and Bellare et al [10], and explicitly by Hemmenway and Ostrovsky [31]: We study of the security of encryption schemes in a scenario where the message to be encrypted may be selected as a function—referred to as the *RDM function*—of the randomness used to encrypt this particular message, or other messages, but in a circular way. More precisely, in analogy with KDM security and circular security, we consider two notions of randomness dependent message security.

- *Randomness-dependent message (RDM) security*: roughly speaking, a public-key encryption scheme is said to be RDM-secure if indistinguishability of ciphertexts holds even if the encrypted messages are chosen as a function of the randomness used to encrypt *this particular* message.
- *Circular randomness-dependent (circular-RDM) security*: roughly speaking, a public-key encryption scheme is said to be circular RDM-secure if indistinguishability of ciphertexts holds even if the encrypted messages are chosen as a function of the randomness used to encrypt *other* messages, but in a circular way. More precisely, we consider a scenario where q messages $\overrightarrow{m}$ are encrypted using randomness $\overrightarrow{r}$, where m_1 is chosen as a function of r_q and

each other message m_i is chosen as a function of r_{i-1} and the "previous" ciphertext $c_{i-1} = \text{Enc}_{pk}(m_{i-1}, r_{i-1})$.

Why Care about Randomness-Dependent Message Security. We consider two reasons to study RDM security:

1. *involuntary RDM attacks:* Implementations of secure protocols are prone to programming mistakes; attacks exploiting such programming mistakes (e.g., buffer overflow attacks) have been demonstrated on secure protocols. Attacks of this type may allow an attacker to see encryptions of randomness dependent messages, even if the original protocol chooses messages independently of the randomness used to encrypt it. RDM security would block such "involuntary" RDM attacks.

   To prevent against these we need to be able to handle sufficiently general classes of RDM functions that may be produced by the attackers.

2. *voluntary RDM attacks* As shown in the beautiful work by Myers and She-lat [36], the possibility of encrypting the randomness used in other encryptions, in a circular way, leads to new powerful techniques in the design of encryption schemes. This techniques was further refined in a recent work by Hohenberger, Lewko and Waters [33]. Another application is found in the work of Hemmenway and Ostrovsky [31], that explicitly considers a notion of circular randomness dependent "one-wayness" and show its usefulness for constructing injective trapdoor functions. In this context, the protocol designer is "voluntarily" creating a (circular-)RDM attack. The above-mentioned works either implicitly (as in [36] and [33]), or explicitly (as in [31]) consider and design encryption schemes that are circular-RDM secure for the specific randomness-dependent messages selected by their protocols. Although for this particular application it suffices to consider specific RDM functions, having general-purpose RDM-secure encryption schemes simplifies the design and the security analysis of protocols.

   Another motivation stems from non-black-box simulation techniques pioneered in the work by Barak [5]; in a variant of Barak's simulation technique due to [41], the simulator commits to its own code (that, in particular, contains the randomness used for the commitment, and thus circularity arises). In this particular application, the circularity could be broken, but having general techniques for dealing with RDM security may simplify future applications.

Before explaining our result, let us also point out that RDM secure encryption is very related to *hedged encryption schemes* introduced by Bellare et al [10]—encryption schemes that remain secure as long as the joint message-randomness distribution comes from a high-entropy source, that is independent of the public-key of the encryption scheme (which in turn are very related to *deterministic encryption* [8,11,15]; see [10] for more details). Hedged encryption schemes are RDM-secure if restricting the attacker to using RDM functions that do not

depend on the public-key.[1] Our focus here is on notions of RDM security where the RDM function may depend also on the public-key.

1.1   Our Results

Full RDM Security. Our first result shows that if the RDM function may be an arbitrary polynomial-size circuit (chosen by the adversary), then RDM security, as defined by Hemmenway and Ostrovsky [31], is impossible to achieve.

Theorem 1 (Informal Statement). *There does not exist an encryption scheme that is (fully) RDM-secure.*

We next show that if there exists some polynomial q such that an encryption scheme is q-circular RDM secure, then the encryption scheme is also RDM secure; thus q-circular RDM security is impossible for all polynomials q.

Theorem 2 (Informal Statement). *There does not exist an encryption scheme that is (fully) q-circular RDM-secure for any polynomial q.*

Bounded RDM Security. Since "unbounded" RDM security is impossible, we consider RDM security with respect to restricted classes of RDM functions.

   Our first positive result demonstrates that if the RDM function is restricted to be a circuit of *a priori* polynomially bounded size, then any secure encryption scheme can be modified to satisfy both RDM and circular-RDM security.

Theorem 3 (Informal Statement). *Assume the existence of a secure public key encryption scheme. Then, for every polynomial s, there exists an encryption scheme Π that is RDM secure when restricting the RDM function to be computed by a circuit of size at most $s(k)$ where k is the security parameter. Additionally Π is q-circular RDM secure for every polynomial q under the same restrictions on the RDM function.*

Theorem 3 is proven by modifying any secure encryption scheme to first "hash" the randomness using a t-wise independent hash-function. The same transformation was previously used by Hemmenway and Ostrovsky [31] to transform "lossy encryption schemes" [42], that can encrypt messages longer than the randomness, into schemes that satisfy a notion of circular-RDM "one-wayness"[2] (as opposed to semantic security) with respect to a particular circular-RDM function (the identity function).

---

[1] However, it is not clear in general whether hedged encryption schemes are *circular* RDM secure, even if we restrict to RDM functions that do not depend on the public-key.

[2] The notion of q-circular RDM one-wayness of Hemmenway and Ostrovsky requires that no polynomial-time attacker can recover $r_1, r_2, \ldots r_q$ given $\mathrm{Enc}_{pk}(r_q; r_1), \mathrm{Enc}_{pk}(r_1; r_2), \ldots, \mathrm{Enc}_{pk}(r_{q-1}; r_q)$ except with negligible probability, over the choice of pk and uniform $r_1, \ldots r_q$.

In order to encrypt a message m, our encryption scheme requires using $|m| + \omega(\log k)$ bits; that is, the randomness used to encrypt a message needs to be sufficiently longer than the message being encrypted (as such, the encryption scheme of Theorem 3 does not handle "the identity function" as an RDM function.) Our next positive result strictly strengthens the conclusion of Theorem 3 (but under a stronger assumption) and the results of [31]: the existence of *lossy trapdoor functions* [43] implies the existence of both bounded RDM-secure and bounded circular-RDM secure encryption schemes that can encrypt also "long" messages using "short" randomness—the ratio between the message-length and the randomness length is proportional to the lossiness of the trapdoor function. Our construction mirrors a construction of hedged encryption of Bellare et al [10]; roughly, the encryption is done by first "hashing" the message-randomness pair and then applying a lossy trapdoor function to the hashed value. The key difference is that we replace the use of univeral hashing (in the construction of [10]) with t-wise independent hashing.[3]

Theorem 4 (Informal Statement). *Assume the existence of "sufficiently" lossy trapdoor functions (the existence of which are implied e.g., by the DDH assumption). Then, for every polynomials s, l, there exists a $l(k)$-bit encryption scheme Π using only k-bits of randomness that is RDM secure (and q-circular RDM secure for every polynomial q), when restricting the RDM function to be computed by a circuit of size at most $s(k)$ where k is the security parameter.*

To prove the above two theorems we develop several new information-theoretic tools regarding t-wise independent hash functions, that may be of independent interests. For instance, with very high probability, a t-wise independent hash functions is a "good" randomness extractor for any min-entropy source with *with computationally-bounded leakage* (mirroring a lemma of Trevisan-Vadhan [44]). We also present "crooked" versions of such deterministic extraction lemmas (mirroring the "crooked left-over-hash lemma of [25]).

An interesting question is whether any encryption schemes can be modified by simply performing some pre-processing to the randomness (as in Theorem 3) to become bounded RDM secure, but still handle long messages using short randomness. At first sight, it may seem like we could use a pseudorandom generator to "stretch" a small seed into the required long random string for the construction in Theorem 3. We have no attack against this construction. However, we show that security reductions that only use the attacker and the RDM function as a black-box—following [28], we refer to such reductions as *strongly black-box*—cannot be used to demonstrate RDM security of encryption schemes with *perfect correctness* and *efficiently recognizable public-keys* that can encrypt long messages using short randomness, based on a falsifiable intractability assumption [37]; for instance, this means that the El-Gamal crypto system cannot be

---

[3] The construction of [10] actually requires universal hash *permutations*. As far as we know, constructions of t-wise independent permutations are not known, which requires us to further modify the scheme to guarantee correctness.

modified (by performing pre-processing to the randomness) to become bounded RDM secure for long messages.

Theorem 5 (Informal statement). *Assume the existence of one-way functions secure against subexponential-sized circuits. For every polynomials m and r such that $m(k) \geq r(k) + \omega(\log k)$, there exists a polynomial s such that for every $m(\cdot)$-bit encryption scheme Π with perfect correctness and efficiently recognizable public-keys that uses $r(\cdot)$ bits of randomness to encrypt a message, s-bounded security of Π cannot be based on any falsifiable assumption using a strongly black-box reduction, unless the assumption is false.*

Let us point out that the reason Theorem 5 does not contradict Theorem 4 is that in the construction used to prove Theorem 4, valid ("injective") public-keys are indistinguisbale from invalid ("lossy") public-keys, and thus the schemes does not have efficiently recognizable public-keys.

RDM Security beyond Encryption. We note that the notion of RDM security applies not only to encryption but makes sense also in the context of more general cryptographic protocols. For instance, the notion of RDM security directly extends to commitments—just as in the case of encryption, we here let the RDM function select the messages to be committed to as a function of the committer's randomness. We remark that Theorem 1 readily extends also to rule out (even computationally binding and computationally-hiding) RDM-secure commitments. Additionally, Theorem 3 extends to show that any commitment scheme in the CRS model can be turned into a bounded RDM secure commitment scheme in the CRS model. However, Theorem 5 does not extend to the setting to commitments—using a collision-resistant hash function, any RDM secure commitment for short messages can be turned into a RDM-secure commitment for long messages. The above results for commitment schemes can be found in the full version of this work.

We leave an exploration of RDM security for other tasks (e.g., zero-knowledge and witness indistinguishability—where the RDM function may select the statement and witness to the proved as a function of the prover's randomness, or secure computation—where the RDM function may select a player's input as a function of his randomness) for future work.

On the Soundness of the Random-Oracle Methodology. Starting with the work of Canetti, Goldreich and Halevi [22,23], there are several "uninstantiability results" for the random oracle model [7], showing schemes that are secure in the random oracle model, but where every instantiation of random oracle with a concrete (efficient) function leads to an insecure protocol (see e.g., [5,27,34]). Another vein of work shows *tasks* (as opposed to schemes) that can be securely implemented in the random oracle model, but for which there are no secure implementations in the standard model (see e.g., [39,40,9]). As far as we know, all these separations for tasks, however, make a relatively strong use of the random oracle model; [39,9] rely on the security reduction "programming the random

oracle", and [40] relies on the security reduction "seeing all the queries to the random oracle". Thus, it is conceivable that a weaker usage of random oracles may circumvent these uninstantiability results. For instance, Unruh [45] introduced a weaker random oracle model where the adversary may get an (inefficient) non-uniform advice about the random oracle, and suggested that proofs of security in this weaker random oracle model may still be "sound". We here address this question using RDM-secure encryption as a task.

We show that in the random-oracle model the existence of public-key encryption schemes imply the existence of "fully" RDM secure encryption schemes (i.e., without restricting the RDM function); our scheme is essentially identical to the hedged encryption scheme of [10] (but the analysis is quite different given the different security goals).[4] Our use of the random oracle model is extremely weak: we do not need to "program it", or "see queries to it", and security holds even the attacker may get any inefficient non-uniform advice about it (as in the model of [45]). (The only property we need of the random oracle is that it acts as a $k^{\log k}$-wise indepedent hash function.) We refer to such a model as the "ultra-weak" Random Oracle Model.

Theorem 6 (Informal Statement). *Assume the existence of a secure public key encryption scheme. Then, there exists a encryption scheme Π that is "fully" RDM secure in the "ultra-weak" Random Oracle Model.*

Theorem 6, combined with our impossibility result (Theorem 1), thus yields an example of an arguably natural task (i.e., RDM-secure encryption) that can be securely implemented in the ultra-weak random-oracle model, but not in the standard model. Let us point out that a cruicial aspect of the security proof of our RO-based scheme is that the RDM function is not allowed to query the random oracle; in case we allow it to query the random oracle, our impossibility result still holds.

1.2   Related Work

As mentioned in the introduction, (circular) RDM security was first implicitly considered by Myers and Shelat [36] and explicitly by Hemmenway and Ostrovsky [31]. [36] [33] demonstrate semantic security of encryption schemes of a specific type of circular RDM attack, but do not formally introduce a notion of RDM security. Hemmenway and Ostrovsky [31] provide the first formal definition of RDM-secure encryption schemes, but only investigate, and provide constructions of, schemes satisfying the weaker notion of "circular-RDM one-wayness". As far as we know, we are the first to explicitly study the feasibility of satisfying (circular-)RDM *semantic* security (as opposed to one-wayness). As mentioned above, Bellare et al [10] study *hedged encryption schemes* that are closely related to RDM-secure encryption schemes; such encryption schemes are RDM secure if restricting the attacker to using RDM functions that do not depend on the

---

[4] Hedged encryption exists also in the plain model so we cannot hope to get a separation by directly appealing to the results of [10].

public-key. Nevertheless, as mentioned, the constructions of both Bellare et al and Hemmenway and Ostrovsky are very useful to us.

As mentioned in the introduction, the related notion of key-dependent message (KDM) security was first introduced by Black, Rogaway, and Shrimpton in 2002 [14], who demonstrated the possibility of achieving their definition in the random-oracle model. The related notion of circular security (in which there exists a cycle of ciphertexts where each message depends on the previous secret key) was independently and concurrently introduced by Camenisch and Lysyanskaya [21], who also showed constructions in the random-oracle model. Follow-up work considered message-dependent PRFs [30] and symmetric encryption [32,4] in the standard model. In [29] barriers to constructing KDM secure schemes for general classes of key-dependencies. In 2008, Boneh, Halevi, Hamburg, and Ostrovsky presented the first KDM-secure public-key encryption scheme [16]; their construction was based on the DDH assumption. Subsequent work developed schemes that were KDM secure and CCA2 secure [20], KDM secure and resilient to leakage on the secret key [6], circular secure under alternative assumptions [17], and circular secure against larger classes of functions [18]. Recent work has also shown that there exist schemes that are secure under standard definitions but which are not 2-circular secure [1,24].

A separate, but related line of related work focuses on leakage-resilient encryption (see e.g., [35,26,2,3,38,19]). In a sense, RDM security can be viewed as a CPA security game where the attacker gets to see some leakage on the encryptor's randomness before selecting the messages; indeed, in our positive results, this view will be instrumental.

Overview of the Paper. Some preliminaries are found in Section 2. We provide formal definitions of RDM and circular RDM security in Section 3. Our impossibility results regarding RDM and circular RDM security are found in Section 4. Finally, in Section 5 we present our positive results. The black-box unprovability results are postponed to the full version. All full proofs are found in the full version.

2   Preliminaries

For a distribution S, $s \leftarrow S$ means that s is chosen according to distribution S. For a set S, $s \leftarrow S$ means that s is chosen uniformly from the set S. U_n denotes the uniform distribution over n-bit strings. For a probabilistic algorithm A, $A(x; r)$ denotes the output of A running on input x with randomness r; $A(x)$ denotes the output of A on input x with uniformly chosen randomness. All logarithms are base 2 unless otherwise specified. We say that a function $\varepsilon : \mathbb{N} \rightarrow [0, 1]$ is negligible if for every constant $c \in \mathbb{N}$, $\varepsilon(n) < k^{-c}$ for sufficiently large k.

The *statistical difference* between two probability distributions X, Y is defined by $\Delta(X, Y) = (1/2) \cdot \sum_x |\Pr[x \leftarrow X] - \Pr[x \leftarrow Y]|$. X and Y are ε-close if $\Delta(X, Y) \leq \varepsilon$. The *statistical difference* between two ensembles $\{X_k\}_k$ and

$\{Y_k\}_k$ is a function δ defined by $\delta(k) = \Delta(X_k, Y_k)$. Two probability ensembles are said to be *statistically close* if their statistical difference is negligible. We also say X_k and Y_k are statistically close if $\Delta(X_k, Y_k) \leq \epsilon(k)$ for some negligible function ϵ. Two ensembles $\{X_k\}, \{Y_k\}$ are *computationally indistinguishable* if for every PPT distinguisher D, there exists a negligible function μ such that for every $k \in \mathbb{N}$,

$$|\Pr[D(1^k, X_k) = 1] - \Pr[D(1^k, Y_k) = 1]| \leq \mu(k).$$

The *min-entropy* of a random variable X, denoted $H_\infty(X)$ is defined by $H_\infty(X) = -\log(max_x \Pr[x \leftarrow X])$. A random variable X is a *k-source* if $H_\infty(X) \geq k$.

A family of hash functions $\mathcal{H} = \{h : S_1 \to S_2\}$ is *t-wise independent* if the following two conditions hold:

1. $\forall x \in S_1$, the random variable $h(x)$ is uniformly distributed over S_2, where $h \leftarrow \mathcal{H}$.
2. $\forall x_1 \neq \cdots \neq x_t \in S_1$, the random variables $h(x_1), \ldots, h(x_t)$ are independent, where $h \leftarrow \mathcal{H}$.

A function $\text{Ext}\{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ is a *strong (k, ε)-extractor* if for every k-source X over $\{0,1\}^n$, $(U_d, \text{Ext}(X, U_d))$ is ε-close to (U_d, U_m).

Definition 1 (Public-Key Encryption). *An l-bit public-key encryption scheme consists of a triple $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ of PPT algorithms where (i) Gen takes a security parameter 1^k as input and generates a pair of public and secret key $(pk, sk) \leftarrow \text{Gen}(1^k)$, (ii) Enc takes a public key pk and a message m in a message space $\{0,1\}^{l(k)}$ as input and generates a ciphertext $c \leftarrow \text{Enc}_{pk}(m)$, (iii) Dec is a deterministic algorithm that takes a secret key sk and a ciphertext c as input and outputs $m' = \text{Dec}_{sk}(c)$, and (iv) there exists a negligible function μ such that for every $k \in \mathbb{N}$, for random $(pk, sk) \leftarrow \text{Gen}(1^k)$,*

$$\Pr\left[\exists m \in \{0,1\}^{l(k)} s.t. \text{Dec}_{sk}(\text{Enc}_{pk}(m)) \neq m\right] \leq \mu(k),$$

where the probability is taken over the randomness of Gen and the randomness of the encryption. We say that Π has perfect correctness if the above condition holds for $\mu(k) = 0$.

Definition 2 (CPA and CCA Security). *An l-bit public-key encryption scheme $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ is CPA-secure if for every probabilistic polynomial time adversary $A = (A_1, A_2)$, the ensembles $\{IND_0^{\Pi}(A, k)\}_k$ and $\{IND_1^{\Pi}(A, k)\}_k$ are computationally indistinguishable, where*

$$\begin{aligned}
IND_b^{\Pi}(A, k) := \ &(pk, sk) \leftarrow \text{Gen}(1^k) \\
&(m_0, m_1, \textsf{state}) \leftarrow A_1(1^k, pk) \\
&c \leftarrow \text{Enc}_{pk}(m_b) \\
&o \leftarrow A_2(c, \textsf{state}) \\
&Output\ o
\end{aligned}$$

We say Π is CCA-secure *if the above holds when A_2 has access to a decryption oracle but is not allowed to query the decryption oracle with the challenge ciphertext c.*

Remark 1. In the above definition and for essentially all the results in this paper, we consider a *uniform* polynomial-time attacker A. In case security holds against also *non-uniform* polynomial-time attackers, we refer to the scheme as being non-uniformly CPA/CCA secure. As is often the case, all our constructions in uniform setting directly extend also to the case of non-uniform security (if assuming that the underlying schemes are non-uniformly secure).

Note that the above definition assumes that messages encrypted are chosen independently of the randomness used by the encryption algorithm.

3   Definition of RDM Security

In this section, we formally define two notions of randomness-dependent message security for encryption schemes.

Our first definition is essentially equivalent to the definition of RDM security due to Hemmenway and Ostrovsky [31]. In this definition, messages are adversarially chosen functions (after seeing the public key) of the randomness used for encryption: we say the encryption scheme is secure if the adversary cannot distinguish between encryptions of different functions of the randomness.

Definition 3. *[RDM-Security] An l-bit public-key encryption scheme $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ is* randomness-dependent message secure (RDM-secure) *if for every* PPT *adversary $A = (A_1, A_2)$, the ensembles $\{RDM_0^{\Pi}(A, k)\}_{k \in \mathbb{N}}$ and $\{RDM_1^{\Pi}(A, k)\}_{k \in \mathbb{N}}$ are computationally indistinguishable where*

$$RDM_b^{\Pi}(A, k) := (pk, sk) \leftarrow \text{Gen}(1^k)$$
$$(f_0, f_1, \text{state}) \leftarrow A_1(1^k, pk)$$
$$r \leftarrow U_R$$
$$c \leftarrow \text{Enc}_{pk}(f_b(r); r)$$
$$o \leftarrow A_2(c, \text{state})$$
$$Output\ o$$

and R is the encryption randomness length of Π. The RDM functions f_b are represented as circuits from $\{0, 1\}^{|r|}$ to $\{0, 1\}^{l(k)}$ We say Π is RDM-CCA-secure if the above holds when A_2 has access to a decryption oracle but is not allowed to query the decryption oracle with the challenge ciphertext c.

We remark that by a standard hybrid argument, we can assume without loss of generality that the adversary A_1 always choose f_1 to be a constant function $f_1 = 0$. As mentioned, Definition 3 is essentially identical to the notion of RDM security defined by Hemmenway and Ostrovsky [31]: the definition of [31] is a multi-message version of Definition 3 where the attacker gets to see a sequence of encrypted messages (that may depend in a correlated way on the randomness

used to encrypt them), and thus the definition of [31] implies Definition 3. (Looking forward, since we are proving an impossibility result regarding Definition 3, considering a weaker definition makes our results stronger.)

Consider a sequence of encryptions where messages are functions of the previous (but most recent) encryption randomness and ciphertext. Security in this setting is guaranteed by CPA security, since encryption randomness is still independent of the messages. However if this dependency is circular, it is unclear whether or not we have security. We now formally introduce this notion of circular randomness dependent message security.

Definition 4 (q-circular RDM Security). *Let $q : \mathbb{N} \to \mathbb{N}$ be efficiently computable. An l-bit public-key encryption scheme $\Pi = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ is q-circular RDM secure if for every PPT adversary $A = (A_1, A_2)$, the following two ensembles $\{CIR_0^\Pi(A, k)\}_{k \in \mathbb{N}}$ and $\{CIR_1^\Pi(A, k)\}_{k \in \mathbb{N}}$ are computationally indistinguishable, where*

$$
\begin{aligned}
CIR_b^\Pi(A, k) := \ &(pk, sk) \leftarrow \mathrm{Gen}(1^k) \\
&(f_0^1, f_0^2, \dots, f_0^{q(k)}, f_1^1, f_1^2, \dots, f_1^{q(k)}, \mathsf{state}) \leftarrow A_1(1^k, pk) \\
&r^1, r^2, \dots, r^{q(k)} \leftarrow U_R^{q(k)} \\
&c^1 \leftarrow \mathrm{Enc}_{pk}(f_b^1(r^q); r^1) \\
&for\ i = 2, \dots, q \\
&\quad c^i \leftarrow \mathrm{Enc}_{pk}(f_b^i(r^{i-1}, c^{i-1}); r^i) \\
&o \leftarrow A_2(\bar{c}, \mathsf{state}) \\
&Output\ o
\end{aligned}
$$

and R is the encryption randomness length of Π. The RDM functions f_b^i are represented as circuits as defined in Definition 3. $\bar{c}$ denotes the vector $(c^1, c^2, \dots c^n)$. Furthermore, Π is circular RDM secure *if Π is k^c-circular RDM secure for every constant c. q-circular-CCA and circular-CCA RDM security are defined in analogous way.*

Remark 2. Note that by a hybrid argument, we can assume without loss of generality that A always choose $f_1^i = 0$ for every $i \in [q]$. We will use this observation later in the proof of Theorem 11.

We also define relaxations of RDM security and circular RDM security where we restrict the RDM function to be computable by circuits of *a priori* bounded size.

Definition 5. *Let $s : \mathbb{N} \to \mathbb{N}$ be efficiently computable. An l-bit public key encryption scheme Π is* s-bounded RDM secure *(resp., s-bounded (q-)circular RDM secure) if Π is RDM secure (resp., (q-)circular RDM secure) under the additional restriction that in the corresponding security game, the adversary A_1 can only output RDM functions computable by circuits of size bounded by $s(k)$. CCA security is defined analogously.*

4   Impossibility Results

In this section we prove that both RDM-security and q-circular security are impossible to achieve. Throughout this section, we focus on bit-encryption schemes; this only makes our results stronger. We first establish the impossibility result on the RDM-secure encryption schemes; our techniques (of using pairwise independent hashfunctions to signal a message) are similar to those used by Bellare and Keelveedhi [12] in a different context.

Theorem 7. *For every* 1-*bit encryption scheme* $\Pi = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$, Π *is not RDM-secure.*

Proof. Let $\Pi = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ be a 1-bit encryption scheme. We construct a PPT adversary $A = (A_1, A_2)$ that breaks the RDM security of Π. The idea is to use f_b to signal the bit b in the RDM_b^Π experiment by pairwise independent hash functions.

Fix a security parameter $k \in \mathbb{N}$. Let C denotes the ciphertext space of Π for the corresponding security parameter k, and let $\mathcal{H} = \{h : C \to \{0,1\}\}$ be a pairwise independent hash function family that hashes ciphertexts to a bit. Our adversary A uses $h \leftarrow \mathcal{H}$ to construct functions $f_{b,h}$ for $b \in \{0,1\}$ that signals the bit b as follows.

- $A_1(1^k, pk)$: A_1 samples $h \leftarrow \mathcal{H}$ and outputs $(f_{0,h}, f_{1,h}, h)$, where for $b \in \{0,1\}$, $f_{b,h}$ on input r, outputs a message $m \in \{0,1\}$ such that $h(\mathrm{Enc}_{pk}(m, r)) = b$ if such an m exists; otherwise $f_{b,h}$ outputs $m = 0$.
- $A_2(c, h)$: A_2 simply outputs one bit $h(c)$.

To show that A breaks the RDM security of Π, it suffices to show the following claim, which clearly implies $\mathrm{RDM}_0^\Pi(A, k)$ and $\mathrm{RDM}_1^\Pi(A, k)$ are distinguishable.

Claim. $\Pr[\mathrm{RDM}_b^\Pi(A, k) = b] \geq 3/4 - \mathrm{negl}(k)$ for $b \in \{0,1\}$.

Proof. Note that the output of $\mathrm{RDM}_b^\Pi(A, k)$ is simply $h(\mathrm{Enc}_{pk}(f_b(r), r))$ where $(pk, sk) \leftarrow \mathrm{Gen}(1^k)$, $r \leftarrow U_{|r|}$, and $h \leftarrow \mathcal{H}$. The correctness of Π implies that,

$$\Pr_{pk,r}[\mathrm{Enc}_{pk}(0, r) \neq \mathrm{Enc}_{pk}(1, r)] \geq 1 - \mathrm{negl}(k). \tag{1}$$

When this is the case, by the pairwise independence,

$$\Pr_h[\exists\, m \text{ s.t. } h(\mathrm{Enc}_{pk}(m, r)) = b] = 3/4.$$

It follows by an union bound that

$$\Pr[\mathrm{RDM}_b^\Pi(A, k) = b]$$
$$\geq \Pr_{pk,r,h}[(\mathrm{Enc}_{pk}(0, r) \neq \mathrm{Enc}_{pk}(1, r)) \wedge (\exists\, m \text{ s.t. } h(\mathrm{Enc}_{pk}(m, r)) = b)]$$
$$\geq 3/4 - \mathrm{negl}(k).$$

$\square$

We proceed to establish the impossibility result on the circular RDM-secure encryption schemes.

Theorem 8. *For every 1-bit encryption scheme $\Pi = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$, Π is not q-circular RDM-secure for every efficiently computable and polynomially bounded q.*

We prove Theorem 8 by showing that in fact, circular RDM security implies RDM security. Theorem 8 follows by combining Theorem 7 and 9.

Theorem 9. *Let $\Pi = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ be a 1-bit encryption scheme, and $q : \mathbb{N} \to \mathbb{N}$ be efficiently computable and polynomially bounded. If Π is q-circular RDM-secure, then Π is RDM-secure.*

Proof. (Sketch) The formal proof can be found in the full version; we here just provide a proof sketch. Let us first sketch the proof for the special case that Π has perfect correctness and that $q = 2$, to illustrate the idea behind the proof. Suppose there exists a PPT adversary A that breaks the RDM security of Π, we want to construct a PPT adversary B that breaks the 2-circular security of Π.

The idea is to let B simulate the attack of A in the circular RDM security game using the second message (in general, using the last message). More precisely, recall that in the RDM security game RDM_b^Π, A generates RDM functions f_0 and f_1, and receives $c = \mathrm{Enc}_{pk}(f_b(r); r)$. To simulate the attack of A in CIR_b^π, B generates $f_0^1, f_0^2, f_1^1, f_1^2$ in a way so that B will receive $\bar{c} = (c^1, c^2)$ with $c^2 = \mathrm{Enc}_{pk}(f_b(r^2); r^2)$. Then B can output whatever A_2 outputs on input c^2, and break the circular RDM security with the same advantage as A.

Now, the key observation is that the RDM function $f_b^2(r^1, c^1)$ can in fact decrypt c^1 to get the message $f_b^1(r^2)$ by checking whether c^1 equals to $\mathrm{Enc}_{pk}(0, r^1)$ or $\mathrm{Enc}_{pk}(1, r^1)$ (the perfect correctness implies $\mathrm{Enc}_{pk}(0, r^1) \neq \mathrm{Enc}_{pk}(1, r^1)$ and the decryption will be always correct). Thus, B can let $f_b^1 = f_b$ and let $f_b^2(r^1, c^1) = f_b^1(r^2)$, and by doing so B will receive $c^2 = \mathrm{Enc}_{pk}(f_b^2(r^1, c^1), r^2) = \mathrm{Enc}_{pk}(f_b(r^2), r^2)$, as desired. This completes the proof of the special case.

We can readily extend the proof to the general q-circular RDM security, by letting B set $f_b^1 = f_b$ and $f_b^{i+1}(r^i, c^i) = f_b^i(r^{i-1}, c^{i-1})$ for $i = 1, \ldots, q-1$. On the other hand, imperfect correctness only causes negligible probability of decryption errors, and thus only reduces the advantage of B by a negligible amount.   □

5   Positive Results

5.1   Bounded RDM Security

In the previous sections we have seen that RDM security and circular RDM security are impossible to achieve. In this section we see how we can achieve the weaker notions of bounded RDM security and bounded circular RDM security. In fact we achieve a stronger notion of RDM security which implies both of the above.

This strong RDM security is in fact security in the presence of randomness leakage (such that the leakage function size is *a priori* bounded by a polynomial) which is available to the adversary when it chooses the messages to encrypt.

Definition 6. *For every $s, p : \mathbb{N} \to \mathbb{N}$ an l-bit public-key encryption scheme $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ is s-bounded p-strong RDM secure (BSRDM-secure) if for every PPT adversary $A = (A_1, A_2)$, the ensembles $\{BSRDM_0^{\Pi}(A, k)\}_{k \in \mathbb{N}}$ and $\{BSRDM_1^{\Pi}(A, k)\}_{k \in \mathbb{N}}$ are computationally indistinguishable where*

$$
\begin{aligned}
BSRDM_b^{\Pi}(A, k) := \ &(pk, sk) \leftarrow \text{Gen}(1^k) \\
&r \leftarrow U_R \\
&(f, \text{state}_1) \leftarrow A_1(1^k, pk) \\
&(m_0, m_1, \text{state}_2) \leftarrow A_2(f(r), \text{state}_1) \\
&c \leftarrow \text{Enc}_{pk}(m_b; r) \\
&o \leftarrow A_3(c, \text{state}_2) \\
&Output\ o,
\end{aligned}
$$

R is the encryption randomness length of Π and $f : \{0,1\}^{|r|} \to \{0,1\}^{p(k)}$ is a function computed by a circuit of size at most $s(k)$. CCA security is defined analogously.

We show that any secure encryption scheme can be compiled to a bounded strong RDM-secure encryption scheme (with "long" encryption randomness).

Theorem 10. *Assume the existence of a CPA (resp., CCA) secure public key encryption scheme. Then, there exists a l-bit s-bounded p-strong RDM-secure (resp., RDM-CCA-secure) encryption scheme for every polynomial l, s and p.*

We start by providing a construction that converts any secure encryption scheme to bounded strong RDM secure encryption scheme. The main idea is that though leakage degrades the randomness, the randomness is long enough to have enough residual min-entropy so that the random bits necessary for encryption can be extracted from it. The problem with this is that the extractor seed will have to be part of the public key, and the adversary can choose a leakage function after seeing the public key. Hence the leakage could be such that the seed always fails to extract randomness from the source. This is where we exploit the fact that the set of possible leakage functions is bounded: using a union bound, we show that if the randomness used by the encryption scheme is long enough, then with overwhelming probability a random seed can extract randomness from the source resulting from any leakage function. The following lemma captures the above idea.

Lemma 1. *[Deterministic Extraction From Bounded Leakage Sources] Let $\mathcal{F} = \{f : \{0,1\}^n \to \{0,1\}^{\ell}\}$ be a class of (leakage) functions. Let $\mathcal{H} = \{h : \{0,1\}^n \to \{0,1\}^m\}$ be a t-wise independent hash function family. If*

$$
\begin{cases}
t \geq 2(m + \ell + \log|\mathcal{F}| + \log(1/\delta) + 3), \\
m \leq n - \ell - 3\log(1/\varepsilon) - \log t - 5,
\end{cases}
$$

then with probability at least $(1 - \delta)$ over $h \leftarrow \mathcal{H}$, it holds that for every $f \in \mathcal{F}$,

$$
\Delta((f(U_n), h(U_n)), (f(U_n), U_m)) \leq \varepsilon.
$$

The proof of the lemma can be found in the full version, and relies on the ideas similar to those used by [44] to demonstrate deterministic extraction from sources computable by bounded size circuits. We now see how we can get a bounded-SRDM-secure encryption scheme from any secure encryption scheme.

The following transformation is essentially identical to the one used in [31] but using different parameters and using a different analysis.[5]

Definition 7. *For every polynomial s and p and encryption scheme $\Pi = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$, define a new encryption scheme $\Pi' = (\mathrm{Gen}', \mathrm{Enc}', \mathrm{Dec}')$ as follows:*

- $\mathrm{Gen}'(1^k) : (pk, sk) \leftarrow \mathrm{Gen}(1^k), h_k \leftarrow \mathcal{H}_k$ *where* $\mathcal{H}_k = \{h_k : \{0,1\}^{R'(k)} \to \{0,1\}^{R(k)}\}$ *is a $t(k)$-wise independent family of hash functions where $R(.)$ is the length of the randomness of Enc, $R'(.)$ is the length of the randomness of Enc',*

$$t(k) \geq 2(R(k) + k + s(k) + p(k) + 3)$$

  and

$$R'(k) = p(k) + R(k) + 3k + \log t(k) + 5$$

  Output $((pk, h_k), sk)$.
- $\mathrm{Enc}'_{(pk,h_k)}(m) : r \leftarrow U_{R'(k)};$ *output* $\mathrm{Enc}_{pk}(m; h_k(r))$.
- $\mathrm{Dec}'_{sk}(c) :$ *output* $\mathrm{Dec}_{sk}(c)$.

In the full version we show, by appealing to Lemma 1 that the above construction transforms a CPA (resp., CCA) secure scheme to a bounded strong RDM (resp., CCA-RDM) secure scheme (thus implying Theorem 10).

Lemma 2. *Let s, p be polynomials. Let Π be a CPA (resp., CCA) secure public key encryption scheme, and Π' be the transformed encryption scheme obtained from Definition 7. Then, Π' is s-bounded p-strong RDM (resp., CCA-RDM) secure.*

It is clear that bounded strong RDM security implies RDM security. Additionally, in the full version we demonstrate that bounded strong RDM security implies also bounded circular RDM security.

Theorem 11. *For all l-bit public key encryption schemes $\Pi = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$, if Π is s-bounded l-strong RDM secure (resp., CCA-RDM secure) then Π is s-bounded circular RDM secure (resp., CCA-RDM secure).*

Full RDM Security in the Random Oracle Model. In the full version of this paper, we demonstrate that the above scheme actually yeilds a fully (as opposed to bounded) RDM secure encryption scheme in the random oracle model [7], if replacing the t-wise independent hashfunction with a random oracle. Our use of

---

[5] As mentioned in Section 1.2, the results of [31] require the underlying encryption schemes to satisfy additional properties (e.g., "lossiness") and the results established about the resulting encryption scheme are very different.

the random oracle model is extremely weak: we do not need to "program it", or "see queries to it". Additionally, security holds even if the attacker may get any inefficient non-uniform advice about the random oracle (as in the model of [45]). The only property we need of the random oracle is that it acts as a $k^{\log k}$-wise indepedent hash function (to be able to apply Lemma 1).

This result, combined with Theorem 7, show the existence of a task—RDM secure encryption—that can be achieved in such an "ultra-weak" random oracle model (assuming the existence of CPA secure encryption schemes), but cannot be achieved in the plain model. As far as we know, this is the first separation between tasks achievable in such a weak random oracle model, and the plain model.

5.2   Bounded RDM Security with Short Randomness

The above construction yields strong bounded RDM-secure encryption schemes where the length of the randomness is longer than the length of the message. We now provide a construction of a bounded RDM-secure and bounded circular RDM-secure encryption scheme that can encrypt arbitrarily long messages using "short" randomness. This construction, however, relies on stronger cryptographic assumption—namely, we require the existence of "lossy" trapdoor functions.

Definition 8 ([43]). *A tuple* $(\text{GenLossy}, \text{GenInj}, F, \text{invert}))$ *is an* (n, u)-*lossy trapdoor function if the following holds:*

- *(Injection mode) For every* $k \in \mathbb{N}$, $\Pr[(pk, sk) \leftarrow \text{GenInj}(1^k) : x \leftarrow U_{n(k)} :$ $\text{invert}_{sk}(F_{pk}(x)) = x] = 1$
- *(Lossy mode) For every* $k \in \mathbb{N}$ *and* $pk \leftarrow \text{GenLossy}(1^k)$, *the size of the range of* $F_{pk}(.)$ *(which takes as input strings of length* $n(k)$*) is at most* $2^{u(k)}$.
- *The following ensembles are computationally indistinguishable*

$$\{(pk, sk) \leftarrow \text{GenInj}(1^k) : pk\}_{k \in \mathbb{N}}$$

$$\{pk \leftarrow \text{GenLossy}(1^k) : pk\}_{k \in \mathbb{N}}$$

We turn to providing our construction of a bounded-RDM secure encryption scheme that can encrypt also "long" messages using "short" randomness—the ratio between the message-length and the randomness length is proportional to the lossiness of the trapdoor function. Formally, we establish the following theorem.

Theorem 12. *Let* l *and* R *be the message length and randomness length parameters with* $R(k) \geq k$. *Assuming the existence of* (n, u)-*lossy trapdoor functions with* $n \geq 3(l + R)$ *and* $u \leq R/8$, *then for every polynomial* s, *there exist a* l-*bit* s-*bounded circular RDM secure encryption scheme with randomness length* R.

In particular, assuming the DDH assumption holds, for every polynomial l, R, s *with* $R(k) \geq k$, *there exist a* l-*bit* s-*bounded circular RDM secure encryption scheme with randomness length* R.

We mention that the "in particular" part of the theorem follows by the DDH-based construction of lossy trapdoor functions in [43]. Our construction is closely related to the "pad-then-deterministic" construction of hedged encryption schemes of Bellare et al [10], where the encryption is done by first applying a *invertible* universal hash *permutation* h to the message-randomness pair $(m||r)$ and then applying a lossy trapdoor function F_{pk} to the hashed value. Recall that hedged encryption scheme already satisfy a notion of RDM security when restricting to RDM functions that do not depend on the public-key. To deal with RDM functions that depend on the public key, our key modification to their scheme is to replace the use of univeral hashing with t-wise independent hashing. However, since constructions of t-wise independent *permutations* are not known, to deal with arbitrary t-wise independent hash functions, we further modify the scheme to "pad" the message-randomness pair with a sufficiently long sequence of 0's.

Recall that the standard construction of t-wise independent hash functions is a degree $t-1$ univariate polynomial over a prime field, which is invertible by the Berlekamp algorithm [13].

Definition 9. *Let l, R, and s be the message length, randomness length, and size parameters with $R(k) \geq k$. Let (GenLossy, GenInj, F, invert) be an (n, u)-lossy trapdoor function with public-key length v such that $u \leq R/8$ and $n = 3(l + R)$. Let $t = 8(s + u + v + R)$ and $\mathcal{H}_n = \{h : \{0,1\}^n \to \{0,1\}^n\}$ be an* invertible *family of $t(\cdot)$-wise independent hash functions. Define an l-bit s-bounded (circular) RDM-secure encryption scheme $\Pi = $ (Gen, Enc, Dec) with randomness length R as follows[6]:*

- Gen$(1^k) : (pk, sk) \leftarrow$ GenInj$(1^k), h \leftarrow \mathcal{H}_n$; *output* $((pk, h), (sk, h))$.
- Enc$_{(pk,h)}(m) : r \leftarrow U_{R(k)}$; *output* $c = F_{pk}(h(m||r||0^{2(l+R)}))$.
- Dec$_{(sk,h)}(c) :$ *output the first $l(k)$ bits of $h^{-1}(\text{invert}_{sk}(c))$.*

While our construction is bounded circular RDM secure, it is instructive to first focus on the bounded RDM security. Recall the security of the [10] scheme (which relies on a construction of deterministic encryption from [15]) relies on a "crooked" version of leftover hash lemma [25], which asserts that when F_{pk} has small range size (which is the case in the lossy mode) and the source $(m||r)$ has sufficient min-entropy and is independent of h, then $F_{pk}(h(m||r))$ is statistically close to the "crooked" distribution $F_{pk}(U_{|m|+|r|})$.

In our context, however, the adversary selects a s-bounded RDM function f after seeing the public key, and thus the source $(f(r)||r||0^{2(l+R)})$ may be correlated with the hash function h (and also F_{pk}). We overcome this issue by using t-wise independent hashing and proving a crooked version of the deterministic extraction lemma from computationally bounded source of Trevisan and Vadhan [44]. The lemma asserts that with overwhelming probability over

---

[6] In fact, to achieve only bounded RDM security (as opposed to circular RDM security), it suffices to, say, satisfy $u \leq R/5$ and set $t = 4(s+u+v)$. We do not optimize the parameters here.

$h \leftarrow \mathcal{H}$, the encryption $F_{pk}(f(r)||r||0^{2(l+R)})$ is statistically close to a corresponding crooked distribution $F_{pk}(U_n)$ for *every lossy* function F_{pk} and *every s*-bounded RDM function f. Therefore, the s-bounded RMD security follows by switching to the lossy mode and applying the crooked deterministic extraction lemma. We proceed to state the crooked deterministic extraction lemma and prove the s-bounded RDM security of our scheme. The proof of Lemma 3 can be found in the full version and follows similar techniques to those used by [44].

Lemma 3 (Crooked Deterministic Extraction). *Let* $\mathcal{H} = \{h : \{0,1\}^n \rightarrow \{0,1\}^n\}$ *be a t-wise independent hash function family. Let* $\mathcal{F} = \{f : \{0,1\}^n \rightarrow R_f\}$ *be a family of functions where each* $f \in \mathcal{F}$ *has range* R_f *of size* $|R_f| \leq 2^m$. *Let* $\mathcal{C}$ *be a family of distributions over* $\{0,1\}^n$ *such that every* $X \in \mathcal{C}$ *has min-entropy* $H_\infty(X) \geq k$. *If*

$$\begin{cases} t \geq 2(m + \log|\mathcal{F}| + \log|\mathcal{C}| + \log(1/\delta) + 3), \\ m \leq k - 2\log(1/\varepsilon) - \log t - 2, \end{cases}$$

then with probability at least $(1 - \delta)$ *over* $h \leftarrow \mathcal{H}$, *it holds that for every* $f \in \mathcal{F}$ *and every* $X \in \mathcal{C}$,

$$\Delta(f(h(X)), f(U_n)) \leq \varepsilon.$$

In the full version we show the following lemma, by appealing to Lemma 3.

Lemma 4. *The l-bit encryption scheme* $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *constructed in Definition 9 is correct and s-bounded RDM secure.*

We now turn to prove also circular RDM security of our scheme. To do this, we require the use of a generalized form of the above crooked deterministic extraction lemma that also deals with leakage (just as our "plain" deterministic extraction of leakage-source lemma, lemma 1).

Lemma 5. *Let* $\mathcal{H} = \{h : \{0,1\}^n \rightarrow \{0,1\}^n\}$ *be a t-wise independent hash function family. Let* $\mathcal{F} = \{f : \{0,1\}^n \rightarrow R_f\}$ *be a family of functions where each* $f \in \mathcal{F}$ *has range* R_f *of size* $|R_f| \leq 2^m$. *Let* $\mathcal{G} = \{g : \{0,1\}^n \rightarrow \{0,1\}^n\}$ *be a family of functions. Let* $\mathcal{C}$ *be a family of distributions over* $\{0,1\}^n$ *such that every* $X \in \mathcal{C}$ *has min-entropy* $H_\infty(X) \geq k$. *If*

$$\begin{cases} t \geq 2(2m + \log|\mathcal{F}| + \log|\mathcal{G}| + \log|\mathcal{C}| + \log(1/\delta) + 3), \\ m \leq (k - 3\log(1/\varepsilon) - \log t - 5)/2, \end{cases}$$

then with probability at least $(1 - \delta)$ *over* $h \leftarrow \mathcal{H}$, *it holds that for every* $f \in \mathcal{F}$, $g \in \mathcal{G}$, *and* $X \in \mathcal{C}$,

$$\Delta((f(g(X)), f(h(X))), (f(g(X)), f(U_n))) \leq \varepsilon.$$

In the full version we show the following lemma, by appealing to Lemma 5.

Lemma 6. *The l-bit encryption scheme* $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *constructed in Definition 9 is s-bounded circular RDM secure.*

References

1. Acar, T., Belenkiy, M., Bellare, M., Cash, D.: Cryptographic Agility and Its Relation to Circular Encryption. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 403–422. Springer, Heidelberg (2010)
2. Akavia, A., Goldwasser, S., Vaikuntanathan, V.: Simultaneous Hardcore Bits and Cryptography against Memory Attacks. In: Reingold, O. (ed.) TCC 2009. LNCS, vol. 5444, pp. 474–495. Springer, Heidelberg (2009)
3. Alwen, J., Dodis, Y., Wichs, D.: Leakage-Resilient Public-Key Cryptography in the Bounded-Retrieval Model. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 36–54. Springer, Heidelberg (2009)
4. Applebaum, B., Harnik, D., Ishai, Y.: Semantic security under related-key attacks and applications. In: ICS, pp. 45–60 (2011)
5. Barak, B.: How to go beyond the black-box simulation barrier. In: FOCS, pp. 106–115 (2001)
6. Barak, B., Haitner, I., Hofheinz, D., Ishai, Y.: Bounded Key-Dependent Message Security. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 423–444. Springer, Heidelberg (2010)
7. Bellare, M., Rompel, J.: Randomness-efficient oblivious sampling. In: Proceedings of the 35th Annual Symposium on Foundations of Computer Science, pp. 276–287 (1994)
8. Bellare, M., Boldyreva, A., O'Neill, A.: Deterministic and Efficiently Searchable Encryption. In: Menezes, A. (ed.) CRYPTO 2007. LNCS, vol. 4622, pp. 535–552. Springer, Heidelberg (2007)
9. Bellare, M., Boldyreva, A., Palacio, A.: An Uninstantiable Random-Oracle-Model Scheme for a Hybrid-Encryption Problem. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 171–188. Springer, Heidelberg (2004)
10. Bellare, M., Brakerski, Z., Naor, M., Ristenpart, T., Segev, G., Shacham, H., Yilek, S.: Hedged Public-Key Encryption: How to Protect against Bad Randomness. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 232–249. Springer, Heidelberg (2009)
11. Bellare, M., Fischlin, M., O'Neill, A., Ristenpart, T.: Deterministic Encryption: Definitional Equivalences and Constructions without Random Oracles. In: Wagner, D. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 360–378. Springer, Heidelberg (2008)
12. Bellare, M., Keelveedhi, S.: Authenticated and Misuse-Resistant Encryption of Key-Dependent Data. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 610–629. Springer, Heidelberg (2011)
13. Berlekamp, E.R.: Factoring polynomials over finite fields. Bell System Technical Journal 46, 1853–1859 (1967)
14. Black, J., Rogaway, P., Shrimpton, T.: Encryption-Scheme Security in the Presence of Key-Dependent Messages. In: Nyberg, K., Heys, H.M. (eds.) SAC 2002. LNCS, vol. 2595, pp. 62–75. Springer, Heidelberg (2003)

15. Boldyreva, A., Fehr, S., O'Neill, A.: On Notions of Security for Deterministic Encryption, and Efficient Constructions without Random Oracles. In: Wagner, D. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 335–359. Springer, Heidelberg (2008)

16. Boneh, D., Halevi, S., Hamburg, M., Ostrovsky, R.: Circular-Secure Encryption from Decision Diffie-Hellman. In: Wagner, D. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 108–125. Springer, Heidelberg (2008)

17. Brakerski, Z., Goldwasser, S.: Circular and Leakage Resilient Public-Key Encryption under Subgroup Indistinguishability. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 1–20. Springer, Heidelberg (2010)

18. Brakerski, Z., Goldwasser, S., Kalai, Y.T.: Black-Box Circular-Secure Encryption beyond Affine Functions. In: Ishai, Y. (ed.) TCC 2011. LNCS, vol. 6597, pp. 201–218. Springer, Heidelberg (2011)

19. Brakerski, Z., Kalai, Y.T., Katz, J., Vaikuntanathan, V.: Overcoming the hole in the bucket: Public-key cryptography resilient to continual memory leakage. In: Proceedings of the 2010 IEEE 51st Annual Symposium on Foundations of Computer Science, FOCS 2010, pp. 501–510 (2010)

20. Camenisch, J., Chandran, N., Shoup, V.: A Public Key Encryption Scheme Secure against Key Dependent Chosen Plaintext and Adaptive Chosen Ciphertext Attacks. In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 351–368. Springer, Heidelberg (2009)

21. Camenisch, J.L., Lysyanskaya, A.: An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 93–118. Springer, Heidelberg (2001)

22. Canetti, R., Goldreich, O., Halevi, S.: On the Random-Oracle Methodology as Applied to Length-Restricted Signature Schemes. In: Naor, M. (ed.) TCC 2004. LNCS, vol. 2951, pp. 40–57. Springer, Heidelberg (2004)

23. Canetti, R., Goldreich, O., Halevi, S.: The random oracle methodology, revisited. J. ACM 51(4), 557–594 (2004)

24. Cash, D., Green, M., Hohenberger, S.: New Definitions and Separations for Circular Security. In: Fischlin, M., Buchmann, J., Manulis, M. (eds.) PKC 2012. LNCS, vol. 7293, pp. 540–557. Springer, Heidelberg (2012)

25. Dodis, Y., Smith, A.: Correcting errors without leaking partial information. In: STOC, pp. 654–663 (2005)

26. Dziembowski, S., Pietrzak, K.: Leakage-resilient cryptography. In: Proceedings of the 2008 49th Annual IEEE Symposium on Foundations of Computer Science, pp. 293–302 (2008)

27. Goldwasser, S., Kalai, Y.T.: On the (in)security of the fiat-shamir paradigm. In: FOCS, pp. 102–113 (2003)

28. Haitner, I., Holenstein, T.: On the (Im)Possibility of Key Dependent Encryption. In: Reingold, O. (ed.) TCC 2009. LNCS, vol. 5444, pp. 202–219. Springer, Heidelberg (2009)

29. Haitner, I., Holenstein, T.: On the (Im)Possibility of Key Dependent Encryption. In: Reingold, O. (ed.) TCC 2009. LNCS, vol. 5444, pp. 202–219. Springer, Heidelberg (2009)

30. Halevi, S., Krawczyk, H.: Security under key-dependent inputs. In: Proceedings of the 14th ACM Conference on Computer and Communications Security, CCS 2007, pp. 466–475 (2007)

31. Hemenway, B., Ostrovsky, R.: Building injective trapdoor functions from oblivious transfer. Electronic Colloquium on Computational Complexity (ECCC) 17 (2010)

32. Hofheinz, D., Unruh, D.: Towards Key-Dependent Message Security in the Standard Model. In: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 108–126. Springer, Heidelberg (2008)
33. Hohenberger, S., Lewko, A., Waters, B.: Detecting Dangerous Queries: A New Approach for Chosen Ciphertext Security. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 663–681. Springer, Heidelberg (2012)
34. Maurer, U.M., Renner, R.S., Holenstein, C.: Indifferentiability, Impossibility Results on Reductions, and Applications to the Random Oracle Methodology. In: Naor, M. (ed.) TCC 2004. LNCS, vol. 2951, pp. 21–39. Springer, Heidelberg (2004)
35. Micali, S., Reyzin, L.: Physically Observable Cryptography (Extended Abstract). In: Naor, M. (ed.) TCC 2004. LNCS, vol. 2951, pp. 278–296. Springer, Heidelberg (2004)
36. Myers, S., Shelat, A.: Bit encryption is complete. In: FOCS, pp. 607–616 (2009)
37. Naor, M.: On Cryptographic Assumptions and Challenges. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 96–109. Springer, Heidelberg (2003)
38. Naor, M., Segev, G.: Public-Key Cryptosystems Resilient to Key Leakage. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 18–35. Springer, Heidelberg (2009)
39. Nielsen, J.B.: Separating Random Oracle Proofs from Complexity Theoretic Proofs: The Non-committing Encryption Case. In: Yung, M. (ed.) CRYPTO 2002. LNCS, vol. 2442, pp. 111–126. Springer, Heidelberg (2002)
40. Pass, R.: On Deniability in the Common Reference String and Random Oracle Model. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 316–337. Springer, Heidelberg (2003)
41. Pass, R., Rosen, A., Tseng, W.l.D.: Public-coin parallel zero-knowledge for np (2011)
42. Peikert, C., Vaikuntanathan, V., Waters, B.: A Framework for Efficient and Composable Oblivious Transfer. In: Wagner, D. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 554–571. Springer, Heidelberg (2008)
43. Peikert, C., Waters, B.: Lossy trapdoor functions and their applications. SIAM J. Comput. 40(6), 1803–1844 (2011)
44. Trevisan, L., Vadhan, S.: Extracting randomness from samplable distributions. In: Proceedings of the 41st Annual Symposium on Foundations of Computer Science, pp. 32–42 (2000)
45. Unruh, D.: Random Oracles and Auxiliary Input. In: Menezes, A. (ed.) CRYPTO 2007. LNCS, vol. 4622, pp. 205–223. Springer, Heidelberg (2007)