Electronic Colloquium on Computational Complexity, Report No. 127 (2010)

Building Injective Trapdoor Functions From Oblivious Transfer

Brett Hemenway and Rafail Ostrovsky

August 9, 2010

Abstract

Injective one-way trapdoor functions are one of the most fundamental cryptographic primitives. In this work we give a novel construction of injective trapdoor functions based on oblivious transfer for long strings.

Our main result is to show that *any* 2-message statistically sender-private semi-honest oblivious transfer (OT) for strings longer than the sender randomness implies the existence of *injective* one-way trapdoor functions. This is perhaps surprising given given the black box separation of injective one-way trapdoor functions from many common cryptographic protocols, e.g. IND-CCA encryption.

As a tool for creating injective one-way trapdoor functions, we define a new notion of security for a public key encryption scheme called **Randomness Dependent Message** (RDM) security, and use it as a stepping stone for creating injective one-way trapdoor functions.

Our main result has a number of interesting corollaries:

- Applying the results of Mol and Yilek (PKC '10), we also show that Lossy Encryption with long plaintexts implies correlated product secure functions and IND-CCA secure encryption.
- Lossy encryption with long plaintexts implies a weak form of RDM security.

In addition, Hemenway, Libert, Ostrovsky and Vergnaud (ePrint '09) showed that statistically-hiding 2-round Oblivious Transfer (OT) is equivalent to Lossy Encryption, where if OT uses randomness shorter than the message so does Lossy Encryption and vice versa. Thus, our main result also implies an injective one-way trapdoor function from any lossy encryption with short randomness. This is somewhat surprising since injective trapdoor functions are *deterministic* and, given the trapdoor, allow recovery of a complete inverse, while public-key encryptions are probabilistic and recover only the plaintext and not necessarily the randomness used in the encryption process. Our result corroborates the previous result of Bellare, Halevi, Sahai and Vadhan (CRYPTO '98) showing that IND-CPA secure encryption implies injective one-way trapdoor permutations in the random oracle model. We stress that in our work we do not make use of a random oracle.

Keywords: injective trapdoor functions, oblivious transfer, public-key cryptography, lossy trapdoor functions

ISSN 1433-8092

1 Introduction

One-way functions are the most basic cryptographic primitive, and their existence is necessary for essentially all of modern cryptography. Despite their immense value in cryptography, one-way functions are not sufficient for many useful cryptographic applications [IR89, RTV04], and in many situations a *trapdoor* is needed as well as the requirement that the function should be *injective*. In this work we provide a novel construction of *injective one-way trapdoor functions* from the following simple secure *protocol*.

A Simple Protocol: We describe a simple protocol between a sender S and receiver R. The sender S has two strings m_0, m_1, and the receiver has a bit b. The receiver sends a message q to the sender, and the sender generates responds with rsp. We require four properties: no efficient sender can recover b from q, the receiver R, can efficiently recover m_b from rsp, the response rsp is statistically independent of m_{1-b}, and finally, the randomness used by the sender in generating rsp is shorter than the length of the messages.

The first three properties describe a *statistically sender-private 2-message* $\binom{2}{1}$*-oblivious transfer protocol* for honest players[1] [Rab81, EGL85]. The fourth property, that the sender randomness must be shorter than the length of the transmitted message is new and is required for technical reasons.

Our main result is showing that this protocol implies injective one-way trapdoor functions. In fact, we show a stronger result, that this protocol implies lossy trapdoor functions as defined by Peikert and Waters [PW08].

Constructing injective one-way trapdoor functions (a deterministic primitive) from a secure protocol, e.g. public-key encryption or oblivious transfer (randomized primitives) has received much attention over the years with little success. One step in this direction was given by Bellare, Halevi, Sahai and Vadhan [BHSV98], who showed that in the *Random Oracle Model* IND-CPA secure encryption implies injective one-way trapdoor permutations. Since it is known ([GKM$^+$00]) 2-message OT implies IND-CPA encryption, the results of Bellare et al. can be viewed as a construction of injective one-way trapdoor permutations from 2-message oblivious transfer in the *random oracle model*. Our results, on the other hand, are in the *standard model*, and do not rely on random oracles.

To achieve the connection between this secure protocol and injective one-way trapdoor functions, we consider an alternative formulation of oblivious transfer. In [PVW08], Peikert, Vaikuntanathan and Waters defined a primitive called *lossy encryption*, and showed that lossy encryption implies statistically sender-private 2-message oblivious transfer. In [HLOV09], Hemenway, Libert, Ostrovsky and Vergnaud showed that the two primitives are, in fact, identical. Their construction of lossy encryption from OT also preserves the randomness and message lengths, so if the OT uses sender randomness shorter than the messages so does the lossy encryption (for completeness, we include their proof in Appendix A). Throughout this work, we will use the terminology of lossy encryption because it makes the constructions more transparent.

[1] Throughout this work, when we refer to oblivious transfer, we refer to oblivious transfer with respect to honest-but-curious parties, i.e. semi-honest OT. Since we are using OT to construct other protocols, using the weaker notion of OT makes our results *stronger*.

Lossy Encryption [KN08, PVW08, BHY09], is a public-key encryption protocol with two indistinguishable types of public keys, injective keys and lossy keys. Ciphertexts created under injective keys can be decrypted, while ciphertexts created under lossy keys are statistically independent of the underlying plaintext. The security of the encryption is then guaranteed by the indistinguishability of the two types of keys.

If $\mathcal{PKE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is a lossy encryption scheme, (which by results of [HLOV09] is equivalent to the simple OT protocol described above) our construction has a simple description: we choose as our function candidate,

$$F_{pk,h}(x) = \mathsf{Enc}(pk, x, h(x))$$

where h is some 2-wise independent hash function. Our main theorem shows that $F_{pk,h}(\cdot)$ is a family of injective one-way trapdoor functions. That is, interestingly, we are able to prove that this is secure even though the randomness is *dependent on the message*. This is somewhat surprising given how difficult it has been to realize other forms of circular security, e.g. Key Dependent Message (KDM) security [CL01],[BRS03],[BHHO08].

1.1 Previous Work

Injective one-way trapdoor functions were one of the first abstract cryptographic primitives to be defined, and their value is well recognized. In [Yao82], Yao showed that injective trapdoor functions imply IND-CPA secure encryption, and Gertner, Malkin and Reingold [GMR01] showed a black-box separation between injective (also poly-to-one) trapdoor functions and public-key encryption schemes. Gertner, Kannan, Malkin, Reingold, and Viswanathan [GKM$^+$00] showed a black-box separation between 2-message oblivious transfer (OT) and injective trapdoor functions, in both directions.

In this work, we show that statistically sender-private OT for long strings implies injective one-way trapdoor functions. Combining our results with the separation results of [GKM$^+$00] gives a separation between standard OT and statistically sender-private OT for long strings.

In this work, we actually construct lossy trapdoor functions (LTDFs) as defined by Peikert and Waters [PW08]. Lossy trapdoor functions imply injective trapdoor functions [PW08, MY09], but appear to be a strictly stronger primitive, as they cannot be constructed in a black-box manner from even one-way trapdoor permutations as shown by Rosen and Segev [RS09]. This separation was later extended by Vahlis in [Vah10]. A family of lossy trapdoor functions, contains two computationally indistinguishable types of functions: injective functions with a trapdoor, and lossy functions, which are functions that statistically lose information about their input. The indistinguishability of the two types of functions shows that the injective functions are, in fact, one-way.

A similar property can be defined for cryptosystems [GOS06, PVW08, KN08, BHY09]. A cryptosystem is called lossy encryption, if there are two indistinguishable types of public keys, injective keys which behave normally, and lossy keys, which have the property that ciphertexts created under a lossy key are statistically independent of the plaintext. It was shown in Bellare, Hofheinz and Yilek [BHY09] that just as injective trapdoor functions imply IND-CPA secure encryption, LTDFs imply lossy encryption. One interpretation of our main theorem is as a partial converse of that result.

Although LTDFs immediately imply injective one-way trapdoor functions, Rosen and Segev [RS09] showed that LTDFs cannot be constructed from one-way trapdoor permutations in a black-box manner, and currently the only known generic construction of LTDFs is from homomorphic smooth hash proof systems [HO09]. In this work, we construct lossy trapdoor functions, and hence injective one-way trapdoor functions from lossy encryption with long plaintexts.

While lossy trapdoor functions were created as a building block for IND-CCA secure encryption, lossy encryption was initially created to help prove security against an active adversary in the Multiparty Computation Setting. Lossy encryption has gone by many names. Groth, Ostrovsky and Sahai called it "parameter-switching" in the context of perfect non-interactive zero knowledge proofs [GOS06]. In [KN08], Kol and Naor called it "Meaningful/Meaningless" encryption, in [PVW08], Peikert, Vaikuntanathan and Waters called it "Dual-Mode Encryption", and in [BHY09] Bellare, Hofheinz and Yilek called it "Lossy Encryption". We follow the example of [BHY09] and call it *lossy encryption*. Despite the seeming power of this primitive, it has proven rather easy to construct, and in [HLOV09], Hemenway, Libert, Ostrovsky and Vergnaud give constructions of lossy encryption from, rerandomizable encryption, statistically-hiding oblivious transfer, universal hash proofs, private information retrieval schemes and homomorphic encryption. Combining the results of [PVW08] and [HLOV09], shows that lossy encryption with short randomness can be viewed exactly as a statistically sender private $\binom{2}{1}$-oblivious transfer with short randomness. Thus, throughout this work, we will use the terminology of lossy encryption because it preserves the intuition of our construction, but it should be noted that lossy encryption can be substituted throughout the paper by 2-message statistically sender-private $\binom{2}{1}$-oblivious transfer and all of our results remain valid.

1.2 Our Contributions

One of the most fundamental techniques in modern cryptography is the use of randomization in protocols to achieve higher levels of security. On the other hand, because randomized protocols cannot always be applied, and good randomness is difficult to generate, a significant body of research has explored the question of where deterministic primitives can be created from their randomized counterparts. One (negative) example of this type was the results of Gertner, Malkin and Reingold showing that IND-CPA secure encryption cannot be used in a black-box way to construct injective one-way trapdoor functions. Our work is perhaps best viewed in this light. We show that lossy encryption, a randomized primitive, which is a strengthening of the standard IND-CPA secure encryption, can be used to construct lossy trapdoor functions, a deterministic primitive, which is the analogous strengthening of injective one-way trapdoor functions.

Our main result is to give a black-box construction of LTDFs (and hence injective one-way trapdoor functions, and IND-CCA secure encryption) from any lossy encryption over a plaintext space which is (at least 1-bit) larger than its randomness space. This is a somewhat surprising connection because lossy encryption has proven to be fairly easy to construct ([PVW08, HLOV09]), while injective one-way trapdoor functions have proven difficult to construct and are black-box separated from many common primitives ([Rud89, IR89, GKM$^+$00, GMR01]).

Theorem (Main Theorem (Informal))**.** *Suppose* $\mathcal{PKE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *is a lossy encryption scheme over message space* $\mathcal{M}$*, randomness space* $\mathcal{R}$ *and ciphertext space* $\mathcal{C}$*. If* $|\mathcal{M}| > 2|\mathcal{R}|$*, i.e. messages are at least one bit longer than the randomness, and* $\mathcal{H}$ *is a* 2*-wise independent hash family, with* $h : \mathcal{M} \to \mathcal{R}$*, for* $h \in \mathcal{H}$*, then the function*

$$\begin{aligned} F_{pk,h} : \mathcal{M} &\to \mathcal{C} \\ x &\mapsto \mathsf{Enc}(pk, x, h(x)) \end{aligned}$$

is a slightly lossy trapdoor function.

While these functions are fairly simple to describe, the circular nature of the construction makes the proof very delicate.

Applying the results of Mol and Yilek [MY09], we have the following corollaries:

Corollary. *If there exists a lossy encryption scheme with messages at least one bit longer than the encryption randomness, then there exists Correlated Product secure functions.*

Corollary. *If there exists a lossy encryption scheme with messages at least one bit longer than the encryption randomness, then there exists IND-CCA secure encryption.*

2 Preliminaries

2.1 Notation

If $f : X \to Y$ is a function, for any $Z \subset X$, we let $f(Z) = \{f(x) : x \in Z\}$. If A is a PPT machine, then we use $a \xleftarrow{\$} A$ to denote running the machine A and obtaining an output, where a is distributed according to the internal randomness of A. If R is a set, and no distribution is specified, we use $r \xleftarrow{\$} R$ to denote sampling from the uniform distribution on R.

If X and Y are families of distributions indexed by a security parameter λ, we say that X is statistically close to Y, (written $X \approx_s Y$) to mean that for all polynomials p and sufficiently large λ, we have $\sum_x |\Pr[X = x] - \Pr[Y = x]| < \frac{1}{p(\lambda)}$.

We say that X and Y are computationally close (written $X \approx_c Y$) to mean that for all PPT adversaries A, for all polynomials p, and for all sufficiently large λ, we have $|\Pr[A^X = 1] - \Pr[A^Y = 1]| < 1/p(\lambda)$.

2.2 Oblivious Transfer

We briefly recall the definition of oblivious transfer (OT) [Rab81, EGL85]. In particular honest-receiver two-message statistically-hiding $\binom{2}{1}$-OT. Throughout this work, we use the term oblivious transfer to mean 2-message (i.e. 1 round) $\binom{2}{1}$-OT for semi-honest players. Oblivious transfer is a protocol between a sender Sen and a receiver $\mathsf{Rec} = (\mathsf{Rec}_q, \mathsf{Rec}_d)$. The sender Sen has two strings m_0, m_1, and the receiver has a bit b. The receiver Rec_q generates a query q along with some state information sk and sends q to the sender. The sender generates randomness r and evaluates $\mathsf{rsp} = \mathsf{Sen}(\mathsf{q}, m_0, m_1, r)$ and sends rsp to the receiver Rec_d who uses sk to obtain m_b.

- **Correctness:** For all $m_0, m_1 \in \{0,1\}^k$, for all $b \in \{0,1\}$, there is a negligible function ν such that

$$\Pr[(\mathsf{q}, sk) \xleftarrow{\$} \mathsf{Rec}_q(1^\lambda, b);\ \mathsf{rsp} \xleftarrow{\$} \mathsf{Sen}(\mathsf{q}, m_0, m_1, r) : \mathsf{Rec}_d(sk, \mathsf{rsp}) = m_b] \geq 1 - \nu(\lambda).$$

- **Receiver Privacy:** b remains computationally hidden from Sen's view. Specifically, we must have

$$\{(\mathsf{q}, sk) \xleftarrow{\$} \mathsf{Rec}_q(1^\lambda, 0) : \mathsf{q}\} \approx_c \{(\mathsf{q}, sk) \xleftarrow{\$} \mathsf{Rec}_q(1^\lambda, 1) : \mathsf{q}\},$$

  where the distributions are taken over the internal randomness of Rec_q.

- **Sender Privacy:** for any $b \in \{0,1\}$, for any strings m_0, m_1, m_0', m_1' such that $m_b = m_b'$ and any honest receiver's query $\mathsf{q} = \mathsf{Rec}_q(1^\lambda, b)$, it must hold that

$$\{(\mathsf{q}, sk) \xleftarrow{\$} \mathsf{Rec}_q(1^\lambda, b); \mathsf{rsp} \xleftarrow{\$} \mathsf{Sen}(\mathsf{q}, m_0, m_1, r) : \mathsf{rsp}\} \approx_s$$

$$\{(\mathsf{q}, sk) \xleftarrow{\$} \mathsf{Rec}_q(1^\lambda, b); \mathsf{rsp} \xleftarrow{\$} \mathsf{Sen}(\mathsf{q}, m_0', m_1', r) : \mathsf{rsp}\}$$

  where the distributions are taken over the internal randomness of Rec_q and the choice of r.

Our constructions will require the sender randomness r to be shorter than the messages m_0, m_1. Schemes that satisfy this property exist under Paillier's Decisional Composite Residuosity (DCR) assumption. See Appendix B for a discussion.

2.3 Lossy Trapdoor Functions

We briefly review the notion of *Lossy Trapdoor Functions* (LTDFs) as described in [PW08].

Intuitively, a family of Lossy Trapdoor Functions is a family of functions which have two modes, injective mode, which has a trapdoor, and lossy mode which is guaranteed to have a small image size. This implies that with high probability, the preimage of an element in the image will have a large size. Formally we have:

Definition 1. A tuple $(S_{\text{ltdf}}, F_{\text{ltdf}}, F_{\text{ltdf}}^{-1})$ of PPT algorithms is called a family of (n,k)-Lossy Trapdoor Functions if the following properties hold:

- **Sampling Injective Functions:** $S_{\text{ltdf}}(1^\lambda, 1)$ outputs s, t where s is a function index, and t its trapdoor. We require that $F_{\text{ltdf}}(s, \cdot)$ is an injective deterministic function on $\{0,1\}^n$, and $F_{\text{ltdf}}^{-1}(t, F_{\text{ltdf}}(s, x)) = x$ for all x.

- **Sampling Lossy Functions:** $S_{\text{ltdf}}(1^\lambda, 0)$ outputs $(s, \perp)$ where s is a function index and $F_{\text{ltdf}}(s, \cdot)$ is a function on $\{0,1\}^n$, where the image of $F_{\text{ltdf}}(s, \cdot)$ has size at most 2^{n-k}.

- **Indistinguishability:** The first outputs of $S_{\text{ltdf}}(1^\lambda, 0)$ and $S_{\text{ltdf}}(1^\lambda, 1)$ are computationally indistinguishable.

We recall a basic result about Lossy Trapdoor Functions from from [PW08].

Lemma 1. Let λ be a security parameter. If $(S_{\text{ltdf}}, F_{\text{ltdf}}, F^{-1}_{\text{ltdf}})$ is a family of (n, k) Lossy Trapdoor Functions, and $k = \omega(\log(\lambda))$, then the injective branches form a family of injective one-way trapdoor functions.

The intuition is that if the lossiness is large enough, then the preimage of *any* element in the image has more than one element in it. Thus an adversary who can invert the function can be used to distinguish whether the functions are in injective or lossy modes simply by calculating $y = F_{\text{ltdf}}(s, x)$, and sending it to the inverter and checking if the inverter responds with x or a different preimage of y. It is important to notice that this proof does not go through if the lossiness is too small. If the preimage has size one with polynomial probability, then the inverter could simply refuse to invert on any element which has preimage of size greater than one.

In [MY09], Mol and Yilek observed that if f is an (n, k)-LTDF, then defining $\vec{f}(x_1, \ldots, x_t) = (f(x_1), \ldots, f(x_t))$, is a (tn, tk)-LTDF. Thus if $k > 1/\operatorname{poly}$, t can be chosen such that $tk = \omega(\log(\lambda))$, and hence $\vec{f}$ is a injective one-way trapdoor function by Lemma 1. Mol and Yilek went on to show how to construct correlated product secure functions, and hence IND-CCA secure cryptosystems from these *slightly lossy trapdoor functions*.

2.4 Lossy Encryption

In [PVW08], Peikert, Vaikuntanathan and Waters defined Dual-Mode Encryption, a type of cryptosystem with two types public-keys, injective keys on which the cryptosystem behaves normally and "lossy" or "messy" keys on which the system loses information about the plaintext. In particular they require that the encryptions of any two plaintexts under a lossy key yield distributions that are statistically close, yet injective and lossy keys remain computationally indistinguishable. Groth, Ostrovsky and Sahai [GOS06] previously used a similar notion in the context of non-interactive zero knowledge.

In [BHY09] Bellare, Hofheinz and Yilek defined *Lossy Encryption*, expanding on the definitions of Dual-Mode Encryption in [PVW08], Meaningful/Meaningless Encryption in [KN08] and Parameter-Switching in [GOS06]. At a high level, a 'lossy' (or 'messy' in the terminology of [PVW08]) cryptosystem is one which has two types of public keys which specify two different modes of operation. In the normal mode, encryption is injective, while in the lossy (or 'messy') mode, the ciphertexts generated by the encryption algorithm are independent of the plaintext. We also require that no efficient adversary can distinguish normal keys from lossy keys. In [BHY09], they also require openability, which basically allows the decryptor to decrypt a ciphertext generated from a lossy key to *any* plaintext.

Definition 2. Formally, a *lossy public-key encryption scheme* is a tuple $\mathcal{PKE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ of polynomial-time algorithms such that

- $\mathsf{Gen}(1^\lambda, inj)$ outputs keys (pk, sk), keys generated by $\mathsf{Gen}(1^\lambda, inj)$ are called *injective keys*.
- $\mathsf{Gen}(1^\lambda, lossy)$ outputs keys $(pk_{\mathsf{lossy}}, sk_{\mathsf{lossy}})$, keys generated by $\mathsf{Gen}(1^\lambda, lossy)$ are called *lossy keys*.
- $\mathsf{Enc}(pk, \cdot, \cdot) : \mathcal{M} \times \mathcal{R} \to \mathcal{C}$.

Additionally, the algorithms must satisfy the following properties:

1. *Correctness on injective keys.* For all $x \in \mathcal{M}$,

$$\Pr\left[(pk, sk) \xleftarrow{\$} \mathsf{Gen}(1^\lambda, inj); r \xleftarrow{\$} \mathcal{R} : \mathsf{Dec}(sk, \mathsf{Enc}(pk, x, r)) = x\right] = 1.$$

2. *Indistinguishability of keys.* We require that the public key, pk in lossy mode and injective mode are computationally indistinguishable. Specifically, if $\text{proj} : (pk, sk) \mapsto pk$ is the projection map, then the two distributions

$$\{\text{proj}(\mathsf{Gen}(1^\lambda, inj))\} \approx_c \{\text{proj}(\mathsf{Gen}(1^\lambda, lossy))\}$$

3. *Lossiness of lossy keys.* If $(pk_{\mathsf{lossy}}, sk_{\mathsf{lossy}}) \xleftarrow{\$} \mathsf{Gen}(1^\lambda, lossy)$, then for all $x_0, x_1 \in \mathcal{M}$, the two distributions $\mathsf{Enc}(pk_{\mathsf{lossy}}, x_0, \mathcal{R})$ and $\mathsf{Enc}(pk_{\mathsf{lossy}}, x_1, \mathcal{R})$ are statistically close, i.e. the statistical distance is negligible in λ.

We call a cryptosystem ν-lossy if

$$\max_{x_0, x_1 \in \mathcal{M}} \Delta(\{r \xleftarrow{\$} \mathcal{R} : \mathsf{Enc}(pk_{\mathsf{lossy}}, x_0, r)\}, \{r \xleftarrow{\$} \mathcal{R} : \mathsf{Enc}(pk_{\mathsf{lossy}}, x_1, r)\} < \nu.$$

We call a cryptosystem *perfectly lossy* if the distributions $\mathsf{Enc}(pk_{\mathsf{lossy}}, x_0, \mathcal{R})$ and $\mathsf{Enc}(pk_{\mathsf{lossy}}, x_1, \mathcal{R})$ are identical.

In [PVW08], Peikert, Vaikuntanathan and Waters showed that essentially the same construction that creates IND-CPA secure encryption from injective trapdoor functions, will provide lossy encryption from lossy trapdoor functions. In [HLOV09], Hemenway, Libert, Ostrovsky and Vergnaud showed that lossy encryption is identical to statistically sender private $\binom{2}{1}$-OT. A review of the equivalence can be found in Appendix A.

2.5 k-wise independent hash functions

We recall the definition of k-wise independent hash functions.

Definition 3. A family of functions $\mathcal{H}$ is called *k-wise independent* if for all $h \in \mathcal{H}$ $h : X \to Y$, and for all $y_1, \ldots, y_k \in Y$, and all *distinct* $x_1, \ldots, x_k \in X$, we have

$$\Pr_{h \in \mathcal{H}}[h(x_1) = y_1, \ldots, h(x_k) = y_k] = \frac{1}{|Y|^k}.$$

It is easy to construct, k-wise independent hash functions. In particular, recall that if $X = \mathbb{F}_q$ is a finite field then the family of polynomials of degree less than k in $\mathbb{F}_q[x]$ is a k-wise independent hash family from X to X.

3 Randomness Dependent Message (RDM) Security

The (semantic) security of a public-key cryptosystem holds only when the messages being encrypted can be efficiently computed from the public key. Previous work has explored the notion of security when the plaintext is allowed to depend on the secret key (dubbed key dependent message (KDM) security) [BRS03],[BHHO08],[HU08],[CS09]. In this work we consider new notions of security when the plaintext may depend on the encryption randomness. While the need for KDM security arises naturally in practical applications, the notion of Randomness Dependent Message (RDM) security arises naturally in cryptographic *constructions*.

Definition 4 (Strong RDM Security)**.** We consider two experiments:

RDM (Real)	**RDM (Ideal)**
$pk \xleftarrow{\$} \mathsf{Gen}(1^\lambda)$	$pk \xleftarrow{\$} \mathsf{Gen}(1^\lambda)$
$\vec{r} = (r_1, \ldots, r_n) \xleftarrow{\$} \mathsf{coins}(\mathsf{Enc})$	$\vec{r} = (r_1, \ldots, r_n) \xleftarrow{\$} \mathsf{coins}(\mathsf{Enc})$
$(f_1, \ldots, f_n) \xleftarrow{\$} \mathcal{A}_1(pk)$	$(f_1, \ldots, f_n) \xleftarrow{\$} \mathcal{A}_1(pk))$
$\vec{c} = (\mathsf{Enc}(pk, f_1(\vec{r}), r_1), \ldots, \mathsf{Enc}(pk, f_n(\vec{r}), r_n))$	$\vec{c} = (\mathsf{Enc}(pk, 0, r_1), \ldots, \mathsf{Enc}(pk, 0, r_n))$
$b \leftarrow A_2(\vec{c})$	$b \xleftarrow{\$} A_2(\vec{c})$.

Figure 1: RDM security

A cryptosystem $\mathcal{PKE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is called *Strongly RDM Secure* with respect to $\mathcal{F}$ if for all polynomial $n = n(\lambda)$, and all PPT adversaries $A = (A_1, A_2)$ for which A_1 only outputs $f_i \in \mathcal{F}$, we have

$$\left|\Pr[A^{RDM_{\mathsf{real}}} = 1] - \Pr[A^{RDM_{\mathsf{ideal}}} = 1]\right| < \nu$$

for some negligible function $\nu = \nu(\lambda)$.

It is natural as well to consider a weakened notion of RDM security, called RDM One-wayness.

Definition 5 (RDM One-Way)**.** Let $\mathcal{PKE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a public key cryptosystem. Consider the following experiment

RDM One-Way
$pk \xleftarrow{\$} \mathsf{Gen}(1^\lambda)$
$\vec{r} = (r_1, \ldots, r_n) \xleftarrow{\$} \mathcal{R}$
$(f_1, \ldots, f_n) \xleftarrow{\$} \mathcal{A}_1(pk)$
$\vec{c} = (\mathsf{Enc}(pk, f_1(\vec{r}), r_1), \ldots, \mathsf{Enc}(pk, f_n(\vec{r}), r_n))$
$\vec{r}' \leftarrow A_2(\vec{c})$

Figure 2: RDM One-Way

A cryptosystem $\mathcal{PKE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is called *RDM One-Way* with respect to family $\mathcal{F}$ if for all polynomials $n = n(\lambda)$, and all PPT adversaries $A = (A_1, A_2)$ for which A_1 only outputs $f_i \in \mathcal{F}$, we have $\Pr[\vec{r} = \vec{r}'] < \nu$ for some negligible function $\nu = \nu(\lambda)$.

A special case of RDM one-wayness, is the encryption of a randomness cycle. As before we can consider both the decision and the search variants.

Definition 6 (RCIRC Security)**.** A cryptosystem $\mathcal{PKE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ will be called *randomness circular secure* (RCIRC secure) if we have

$$\{pk, \mathsf{Enc}(pk, r_2, r_1), \mathsf{Enc}(pk, r_3, r_2), \ldots, \mathsf{Enc}(pk, r_n, r_{n-1}), \mathsf{Enc}(pk, r_1, r_n)\} \approx_c$$

$$\{pk, \mathsf{Enc}(pk, 0, r_1), \ldots, \mathsf{Enc}(pk, 0, r_n)\},$$

where $pk \xleftarrow{\$} \mathsf{Gen}(1^\lambda)$, and $r_i \xleftarrow{\$} \mathsf{coins}(\mathsf{Enc})$ for $i = 1, \ldots, n$.

When using a cryptosystem as a building block in a more complicated protocol, it is sometimes desirable to encrypt messages that are correlated with the randomness. Similar to the notion of circular security ([CL01],[BRS03],[BHHO08]), which talks about security when encrypting *key cycles*, we define a notion of security related to encrypting *randomness cycles*. We call this property RCIRC One-Wayness.

Definition 7 (RCIRC One-wayness)**.** We say that a cryptosystem is RCIRC One-Way if the function

$$\begin{aligned} F_{pk} : \mathsf{coins}(\mathsf{Enc})^n &\to \mathcal{C}^n \\ (r_1, \ldots, r_n) &\mapsto (\mathsf{Enc}(pk, r_2, r_1), \ldots, \mathsf{Enc}(pk, r_1, r_n)), \end{aligned}$$

is a one-way function.

It is not hard to see that a cryptosystem that is RCIRC One-Way gives rise to an injective one-way trapdoor function.

3.1 Comparing RDM and KDM Security

It is tempting to define Randomness Dependent Message (RDM) Security in a manner exactly analogous to Key Dependent Message (KDM) Security. For example, if we parallel the definition of KDM security given in [HU08],[BHHI10], we obtain

Definition 8 (RDM Security (flawed))**.** Let $\mathcal{PKE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a public-key encryption scheme with message space $\mathcal{M}$ and randomness space $\mathcal{R}$. Let $\vec{pk} = (pk_1, \ldots, pk_n)$, and $\vec{r} = (r_1, \ldots, r_n)$, for some integer $n = n(\lambda)$. Define:

- $\mathsf{Real}_{\vec{pk},\vec{r}}$ to be the oracle that on input $f : \mathcal{R}^n \to \mathcal{M}$, and $i \in [n]$ returns $C = \mathsf{Enc}(pk_i, f(\vec{r}), r_i)$.
- $\mathsf{Ideal}_{\vec{pk},\vec{r}}$ to be the oracle that on input f, i returns $E(pk_i, f(\vec{r}), r_i)$.

For a PPT Machine A, we define the KDM advantage of A to be

$$\mathcal{A}^{RDM}_{\mathcal{PKE},A} = \left|\Pr\left[A^{\mathsf{Real}_{\vec{pk},\vec{r}}}(\vec{pk}) = 1\right] - \Pr\left[A^{\mathsf{Ideal}_{\vec{pk},\vec{sk}}}(\vec{pk}) = 1\right]\right|.$$

Where $pk_i \xleftarrow{\$} G(1^\lambda)$, for $i \in [n]$. We say that $\mathcal{PKE}$ is RDM secure with respect to a class of functions $\mathcal{F}$ if for every polynomial n and every PPT A, that only queries its oracle with $f \in \mathcal{F}$, the advantage $\mathcal{A}^{RDM}_{\mathcal{PKE},A}$ is a negligible function of λ.

This definition can never be satisfied because the oracles answers are deterministic. In particular, in the ideal world, the oracle's response to a query (f, i) will be identical to its response to the query (g, i).

4 Constructing Slightly Lossy Trapdoor Functions

In this section we give a generic construction of a slightly lossy trapdoor functions from lossy encryption.

Let $\mathcal{PKE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a Lossy Encryption, with $\mathsf{Enc}(pk, \cdot, \cdot) : \mathcal{M} \times \mathcal{R} \to \mathcal{C}_{pk}$. Let $\mathcal{H}$ be a family of pairwise independent hash functions, with $h : \mathcal{M} \to \mathcal{R}$, for all $h \in \mathcal{H}$. The construction is described in Figure 3.

- **Sampling an Injective Function:**
  $(pk, sk) \xleftarrow{\$} \mathsf{Gen}(1^\lambda, inj)$
  $h \xleftarrow{\$} \mathcal{H}$
- **Sampling a Slightly Lossy Function:**
  $(pk, \perp) \xleftarrow{\$} \mathsf{Gen}(1^\lambda, lossy)$
  $h \xleftarrow{\$} \mathcal{H}$
- **Evaluation:**
  $F_{pk,h} : \mathcal{M} \to \mathcal{C}$,
  $F_{pk,h}(x) = (\mathsf{Enc}(pk, x, h(x))$
- **Trapdoor:**
  $F^{-1}_{pk,h}(c) = \mathsf{Dec}(sk, c)$

Figure 3: Slightly Lossy Trapdoor Functions from Lossy Encryption

The injectivity, and correctness of inversion of the functions described in Figure 3 is clear, it remains only to show that the lossy branch of $F_{pk,h}$ is slightly lossy.

This is not at all obvious because we are applying the cryptosystem $\mathcal{PKE}$ in a randomness circular manner.

5 Proof of Security

In this section we prove that the function family defined in Figure 3 is slightly lossy.

This will require a number of combinatorial lemmas.

To build intuition, we begin by considering the case when the encryption scheme $\mathcal{PKE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is *perfectly* lossy, i.e. for a lossy key pk, the distributions $\mathsf{Enc}(pk, x)$ and $\mathsf{Enc}(pk, y)$ are identical for any $x, y \in \mathcal{M}$.

5.1 The Perfectly Lossy Case

Lemma 2. If $\mathcal{PKE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$, be a *perfectly* lossy encryption scheme, and $pk \xleftarrow{\$} \mathsf{Gen}(1^\lambda)$, the sets $\mathsf{Enc}(pk, \mathcal{M}, \mathcal{R})$ and $\mathsf{Enc}(pk, 0, \mathcal{R})$ are equal.

Proof. The perfect lossiness property says that

$$\Pr[r \xleftarrow{\$} \mathcal{R} : \mathsf{Enc}(pk, x) = c] = \Pr[r \xleftarrow{\$} \mathcal{R} : \mathsf{Enc}(pk, y) = c],$$

for all $x, y \in \mathcal{M}$ and all $c \in \mathcal{C}$, thus we have that *as sets* $\mathsf{Enc}(pk, x, \mathcal{R}) = \mathsf{Enc}(pk, y, \mathcal{R})$. Since $\mathsf{Enc}(pk, \mathcal{M}, \mathcal{R}) = \bigcup_{x \in \mathcal{M}} \mathsf{Enc}(pk, x, \mathcal{R})$, the claim follows. □

Lemma 3. If $\mathcal{PKE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$, be a *perfectly* lossy encryption scheme, and h is *any* function from $\mathcal{M}$ to $\mathcal{R}$, then the function

$$\begin{aligned} F_{pk,h} : \mathcal{M} &\to \mathcal{C} \\ x &\mapsto \mathsf{Enc}(pk, x, h(x)), \end{aligned}$$

is a $(\log|\mathcal{M}|, \log|\mathcal{M}| - \log|\mathcal{R}|)$-LTDF.

Proof. The indistinguishability of injective and lossy modes follows from the indistinguishability of injective and lossy keys for $\mathcal{PKE}$. The trapdoor follows from the correctness of decryption for $\mathcal{PKE}$.

Notice that for any function h, the image of $F_{pk,h}$ is a subset of the ciphertext space $\mathcal{C} = \mathsf{Enc}(pk, \mathcal{M}, \mathcal{R})$. In lossy mode, from Lemma 2 we have that the set $\mathsf{Enc}(pk, \mathcal{M}, \mathcal{R})$ is equal to the set $\mathsf{Enc}(pk, 0, \mathcal{R})$, but $|\mathsf{Enc}(pk, 0, \mathcal{R})| \leq |\mathcal{R}|$, so if pk is a lossy key, the image size of $F_{pk,h}$ is at most $|\mathcal{R}|$, and the result follows. □

Notice that the specific form of the function h was never used in the proof of Lemma 3. For example, we could choose h to be a constant function, and the result would still hold! It is instructive to examine this a little further. For any ordinary encryption scheme, the function $F_{pk,h}(x) = \mathsf{Enc}(pk, x, 0)$, i.e. encrypting the message x using some fixed randomness (in this case the zero string), will not be a one-way function. To see this, we can take any IND-CPA secure encryption scheme and modify it so that if the zero string is used for the randomness, the encryption algorithm simply outputs the message in the clear. This will not affect the CPA security of the encryption scheme, but it will mean the function $F_{pk,h}$ defined in this way will be the identity function, and hence trivially invertible. On the other hand, if $\mathcal{PKE}$ is a perfectly lossy encryption, and $|\mathcal{M}| > |\mathcal{R}|$, then this modification will break the perfect lossiness of $\mathcal{PKE}$.

It is tempting to conclude that if $\mathcal{PKE}$ is not perfectly lossy, but only statistically lossy, then Lemma 3 will still hold. To see that the proof of Lemma 3 does not hold in the statistically lossy case, notice that the counterexample given in the previous paragraph still applies. In the next section, we will construct a lossy trapdoor functions from statistically lossy encryption, but significantly more machinery is needed.

The perfect lossiness property is so strong that we can actually extend Lemma 3.

Lemma 4. If $\mathcal{PKE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$, be a *perfectly* lossy encryption scheme, $0 < t \in \mathbb{Z}$, and h is *any* function from $\mathcal{M}^t$ to $\mathcal{R}$, then the function

$$\begin{aligned} &F_{pk,h} : \mathcal{M}^t \to \mathcal{C}^t \\ &(x_1, \ldots, x_t) \mapsto (\mathsf{Enc}(pk, x_1, h(x_1, \ldots, x_t)), \ldots, \mathsf{Enc}(pk, x_t, h(x_1, \ldots, x_t))), \end{aligned}$$

is a $(t \log |\mathcal{M}|, t(\log |\mathcal{M}| - \log |\mathcal{R}|))$-LTDF.

The proof is essentially identical to the proof of Lemma 3. One consequence of Lemma 4 is

Lemma 5. If $\mathcal{PKE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$, be a *perfectly* lossy encryption scheme, $0 < t \in \mathbb{Z}$, and $\log(|\mathcal{M}|/|\mathcal{R}|) = \omega(\log(\lambda))$, and $0 < t \in \mathbb{Z}$, is strongly t-RCIRC-One Way.

Proof. By Lemma 4, the function $F_{pk,h}$ as defined in Lemma 4 is a $(t \log(|\mathcal{M}|), t(\log(|\mathcal{M}|) - \log(|\mathcal{R}|)))$-LTDF. Since the lossiness, $t((\log |\mathcal{M}|) - \log(|\mathcal{R}|)) = t \log\left(\frac{|\mathcal{M}|}{|\mathcal{R}|}\right) = \omega(\log(\lambda))$, by Lemma 1, the function $F_{pk,h}$ is a one-way function for *any* choice of h. □

As remarked above, this argument *does not* trivially extend to the statistically-lossy case. This is because the distributions $\{r \xleftarrow{\$} \mathcal{R} : \mathsf{Enc}(pk, x, r)\}$ and $\{r \xleftarrow{\$} \mathcal{R} : \mathsf{Enc}(pk, y, r)\}$, will be statistically close for any $x, y \in \mathcal{M}$, but we are not choosing the randomness uniformly, in fact, the randomness is uniquely defined by the message, so new techniques are needed.

5.2 The Statistically Lossy Case

In the preceding section, we examined the perfectly lossy case. There, we were free to choose the function h arbitrarily, even a constant function sufficed to prove security! In the statistical setting we will make use of the fact that h is a pairwise independent hash function.

We begin with a number of basic combinatorial lemmas.

First, we recall a basic fact about sums of squares.

Lemma 6.

$$\text{If } \{d_1, \ldots, d_m\} \in \mathbb{R} \text{ and } d = \frac{1}{m}\sum_{i=1}^{m} d_i, \text{ then } \sum_{i=1}^{m} d_i^2 \geq \sum_{i=1}^{m} d^2.$$

Proof.

$$0 \leq \sum_{i=1}^{m} (d_i - d)^2 = \sum_{i=1}^{m} d_i^2 - 2d\sum_{i=1}^{m} d_i + md^2 = \sum_{i=1}^{m} d_i^2 - md^2.$$

Thus we have

$$\sum_{i=1}^{m} d^2 = md^2 \leq \sum_{i=1}^{m} d_i^2.$$

□

For the following, consider a fixed (lossy) public key pk. Let C_0 be the set of encryptions of 0, i.e.

$$C_0 = \mathsf{Enc}(pk, 0, \mathcal{R}).$$

So $|C_0| \leq |\mathcal{R}|$. For $x \in \mathcal{M}$, define A_x to be the event (over the random choice of $h \xleftarrow{\$} \mathcal{H}$) that $F_{pk,h}(x) \notin C_0$. Let $d_x = \Pr[A_x] = \mathbb{E}(1_{A_x})$. Let $d = \frac{1}{|\mathcal{M}|}\sum_{x\in\mathcal{M}} d_x$. Thus Lemma 6 says that $\sum_{x\in X} d_x^2 \geq |\mathcal{M}|d^2$. Let Z be the random variable denoting the number of elements in the domain that map outside of C_0, so

$$Z = \sum_{x\in\mathcal{M}} 1_{A_x} = \sum_{x\in\mathcal{M}} 1_{x\notin C_0}.$$

Thus the image of $F_{pk,h}$ has size bounded by $|C_0| + Z$.

To show that $F_{pk,h}$ is a lossy trapdoor function, we must show that with high probability (over the choice of h), the image of $F_{pk,h}$ is small (relative to the domain $\mathcal{M}$). We begin with the easy observation:

$$\mathbb{E}(Z) = \mathbb{E}\left(\sum_{x\in\mathcal{M}} 1_{A_x}\right) = \sum_{x\in\mathcal{M}} d_x = |\mathcal{M}|d. \tag{1}$$

Notice as well, that since h is 1-universal, $\Pr[h \xleftarrow{\$} \mathcal{H} : F_{pk,h}(x) = c] = \Pr[r \leftarrow \mathcal{R} : \mathsf{Enc}(pk, x, r) = c]$ for all $x \in \mathcal{M}$, $c \in \mathcal{C}$. We will use this fact to show that d is small. In fact, it's not hard to see that d is bounded by the lossiness of $\mathcal{PKE}$.

This shows that the expected image size is small, but we wish to show that with high probability the image size of $F_{pk,h}$ is small. To do this we examine the variance of Z.

Recall the basic probabilistic fact that if Z is a random Variable, and $Z = \sum_{i=1}^{m} 1_{A_i}$, then

$$\binom{Z}{2} = \sum_{i<j} 1_{A_i\cap A_j},$$

so

$$\mathbb{E}(Z^2) = 2\mathbb{E}\left(\binom{Z}{2}\right) + \mathbb{E}(Z) = 2\mathbb{E}\left(\sum_{i<j} 1_{A_i\cap A_j}\right) + \mathbb{E}(Z),$$

which yields the identity

$$\mathrm{Var}(Z) = \mathbb{E}(Z^2) - \mathbb{E}(Z)^2 = 2\mathbb{E}\left(\sum_{i<j} 1_{A_i\cap A_j}\right) + \mathbb{E}(Z) - \mathbb{E}(Z)^2. \tag{2}$$

To use equation (2), we need to be able to calculate the first summation of $1_{A_i \cap A_j}$. Since h is pairwise independent we have that

$$\begin{aligned}\Pr[A_x \cap A_y] &= \Pr[\mathsf{Enc}(pk, x, h(x)) \notin C_0, \mathsf{Enc}(pk, y, h(y)) \notin C_0] \\ &= \Pr[\mathsf{Enc}(pk, x, h(x)) \notin C_0] \Pr[\mathsf{Enc}(pk, y, h(y)) \notin C_0] \\ &= d_x d_y,\end{aligned}$$

whenever $x \neq y$.

Thus we have

$$\begin{aligned}\mathrm{Var}(Z) &= \mathbb{E}(Z^2) - \mathbb{E}(Z)^2 \\ &= 2\mathbb{E}\left(\binom{Z}{2}\right) + \mathbb{E}(Z) - \mathbb{E}(Z)^2 \\ &= 2\mathbb{E}\sum_{x<y} 1_{A_x \cap A_y} + \mathbb{E}(Z) - \mathbb{E}(Z)^2 \\ &= 2\sum_{x<y} d_x d_y + |\mathcal{M}|d - \left(\sum_{x \in \mathcal{M}} d_x\right)^2 \\ &= |\mathcal{M}|d - \sum_{x \in \mathcal{M}} d_x^2\end{aligned}$$

Thus by Lemma 6, we arrive at the upper bound

$$\mathrm{Var}(Z) \leq |\mathcal{M}|d - |\mathcal{M}|d^2 = |\mathcal{M}|(d - d^2). \tag{3}$$

On the other hand, we have

$$\begin{aligned}\mathrm{Var}(Z) &= \sum_{z=0}^{|\mathcal{M}|} (z - \mathbb{E}(Z))^2 \Pr[Z = z] \\ &= \sum_{z=0}^{|\mathcal{M}|} (z - |\mathcal{M}|d)^2 \Pr[Z = z] \\ &\geq \sum_{z=(1-\epsilon)|\mathcal{M}|}^{|\mathcal{M}|} (z - |\mathcal{M}|d)^2 \Pr[Z = z] \\ &\geq \sum_{z=(1-\epsilon)|\mathcal{M}|}^{|\mathcal{M}|} ((1-\epsilon)|\mathcal{M}| - |\mathcal{M}|d)^2 \Pr[Z = z] \\ &= (1 - \epsilon - d)^2 |\mathcal{M}|^2 \sum_{z=(1-\epsilon)|\mathcal{M}|}^{|\mathcal{M}|} \Pr[Z = z]\end{aligned}$$

Where, here we have used the fact that $1-\epsilon > d$. Since the parameter ϵ is under our control, we can always ensure that this is the case. This will not be a stringent restriction, however, because d is bounded by the statistical lossiness of $\mathcal{PKE}$, and hence will be negligible. In the proof of the following, we will find another restriction on ϵ, namely to achieve a useful degree of lossiness, ϵ must be chosen so that $\epsilon > \frac{|\mathcal{R}|}{|\mathcal{M}|}$.

Rearranging, we have

$$\sum_{z=(1-\epsilon)|\mathcal{M}|}^{|\mathcal{M}|} \Pr[Z = z] \leq \frac{\mathrm{Var}(Z)}{(1-\epsilon-d)^2|\mathcal{M}|^2}.$$

Applying the bound on the variance obtained in Equation 3, we have

$$\sum_{z=(1-\epsilon)|\mathcal{M}|}^{|\mathcal{M}|} \Pr[Z = z] \leq \frac{|\mathcal{M}|(d-d^2)}{(1-\epsilon-d)^2|\mathcal{M}|^2} \leq \frac{d(1-d)}{(1-\epsilon-d)^2|\mathcal{M}|}. \tag{4}$$

Lemma 7. If $\mathcal{PKE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is a ν-lossy encryption, and if $|\mathcal{M}| = t|\mathcal{R}|$, for some $t > 1$, then for any $0 < \epsilon < 1$ such that $1-\epsilon$ is noticeable, and $\epsilon > \frac{1}{t}$, the function $F_{pk,h}$ is a $(\log|\mathcal{M}|, -\log((1-\epsilon+\frac{1}{t})))$-almost always LTDF family.

Proof. Suppose $\mathcal{PKE}$ is ν-Lossy, i.e. $\Delta(\{r \xleftarrow{\$} \mathcal{R} : \mathsf{Enc}(pk, x, r)\}, \{r \xleftarrow{\$} \mathcal{R} : \mathsf{Enc}(pk, y, r)\}) < \nu$. Then by the 1-universality of h, $\Delta(\{h \xleftarrow{\$} \mathcal{H} : F_{pk,h}(0)\}, \{h \xleftarrow{\$} \mathcal{H} : F_{pk,h}(x)\}) < \nu$ for all $x \in \mathcal{M}$. In particular, $d_x = \Pr(A_x) < \nu$ for all d_x, so $d = \frac{1}{|\mathcal{M}|}\sum_{x\in\mathcal{M}} d_x < \nu$. Because the random variable Z represents the number of $x \in \mathcal{M}$ such that $F_{pk,h}(x) \notin C_0$, we have $|F_{pk,h}(\mathcal{M})| \leq |C_0| + Z$. Since $|C_0| \leq |\mathcal{R}| = \frac{1}{t}|\mathcal{M}|$, by Equation 4, we have

$$\Pr[|F_{pk,h}(\mathcal{M})| > (1-\epsilon+\frac{1}{t})|\mathcal{M}|] < \frac{(\nu-\nu^2)}{(1-\epsilon-\nu)^2|\mathcal{M}|}.$$

We would like to choose ϵ as close to 1 as possible but subject to the constraint that $\frac{\nu-\nu^2}{(1-\epsilon-\nu)^2|\mathcal{M}|}$ is negligible. Since ν is negligible, and $\frac{1}{|\mathcal{M}|}$ is negligible, the right hand side will certainly be negligible if $1-\epsilon-\nu$ is non-negligible. But this holds because ν is negligible, and $1-\epsilon$ is non-negligible. Thus with all but negligible probability, the residual leakage is $\log((1-\epsilon+\frac{1}{t})|\mathcal{M}|)$, so the lossiness is $\log(|\mathcal{M}|) - \log((1-\epsilon+\frac{1}{t})|\mathcal{M}|) = -\log(1-\epsilon+\frac{1}{t})$. □

From Lemma 7, we see that if $1-\frac{1}{t}$ is non-negligible, such an ϵ will exist. This immediately implies the result:

Theorem 1 (Main Theorem)**.** If $\mathcal{PKE}$ is a ν-Lossy Encryption with $|\mathcal{M}| = t|\mathcal{R}|$, for some $t > 1$ with $1-\frac{1}{t}$ non-negligible, then the functions described in Figure 3 is a family of lossy trapdoor functions.

Proof. From the proof of Lemma 7, it suffices to find an ϵ such that $1-\epsilon$ is noticeable, and $\epsilon - \frac{1}{t}$ is noticeable.

In this case, we can take $\epsilon = \frac{1}{2} + \frac{1}{2t}$. In this case $1-\epsilon = \epsilon - \frac{1}{t} = \frac{1-\frac{1}{t}}{2}$ which is noticeable since $1-\frac{1}{t}$ was assumed to be noticeable. In this case, the lossiness of the function will be $-\log(1-\epsilon+\frac{1}{t}) = \sum_{j=1}^{\infty} \frac{(\epsilon-\frac{1}{t})^j}{j} \geq \epsilon - \frac{1}{t} = \frac{1}{2}(1-\frac{1}{t})$, which is noticeable. □

Taking $t = 2$, and applying the results of [MY09], we have

Corollary 1. If there exists Lossy Encryption with $|\mathcal{M}| > 2|\mathcal{R}|$, and there is an efficiently computable family of 2-wise independent hash functions from $\mathcal{M}$ to $\mathcal{R}$, then there exists injective one-way trapdoor functions, Correlated Product secure functions and IND-CCA2 secure encryption.

Although Theorem 1 provides lossy trapdoor functions and hence IND-CCA secure encryption [MY09], we would like to see exactly how lossy the functions can be.

Corollary 2. If $|\mathcal{M}| = t|\mathcal{R}|$, and $\frac{1}{t}$ is negligible, i.e. the messages are $\omega(\log \lambda)$ bits longer than the randomness, then the functions described in Figure 3 is a family of injective one-way trapdoor functions.

Proof. From Equation 4, we have

$$\Pr[|F_{pk,h}(\mathcal{M})| > (1 - \epsilon + \frac{1}{t})|\mathcal{M}|] < \frac{(\nu - \nu^2)}{(1 - \epsilon - \nu)^2|\mathcal{M}|}.$$

If we set $\epsilon = 1 - \nu - \frac{1}{\sqrt{|\mathcal{M}|}}$, then the right hand side becomes $\nu - \nu^2$, which is negligible. The lossiness is then $-\log\left(1 - \epsilon + \frac{1}{t}\right) = -\log\left(\nu + \frac{1}{t} - \frac{1}{\sqrt{|\mathcal{M}|}}\right) > -\log(\nu + \frac{1}{t})$. Since both ν and $\frac{1}{t}$ were assumed to be negligible, so is the sum $\nu + \frac{1}{t}$. But this means that $-\log(\nu + \frac{1}{t}) \in \omega(\log \lambda)$. Thus we can apply Lemma 1 to conclude that $F_{pk,h}$ is a family of injective one-way trapdoor functions.

□

If the functions described in Figure 3 are a family of injective one-way trapdoor functions, that means that the underlying cryptosystem, is RCIRC One-Way

Corollary 3. If $\mathcal{PKE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is a lossy encryption, and if $|\mathcal{M}| = t|\mathcal{R}|$, and $\frac{1}{t}$ is negligible, if we define $\widetilde{\mathcal{PKE}} = (\widetilde{\mathsf{Gen}}, \widetilde{\mathsf{Enc}}, \widetilde{\mathsf{Dec}})$, with

- $\widetilde{\mathsf{Gen}}(1^\lambda)$, generates $(pk, sk) \xleftarrow{\$} \mathsf{Gen}(1^\lambda)$, and $h \xleftarrow{\$} \mathcal{H}$ and sets $\tilde{pk} = (pk, h)$, $\tilde{sk} = sk$.
- $\widetilde{\mathsf{Enc}}(\tilde{pk}, m, r) = \mathsf{Enc}(pk, m, h(r))$.
- $\widetilde{\mathsf{Dec}}(\tilde{sk}, c) = \mathsf{Dec}(sk, c)$.

Then $\widetilde{\mathcal{PKE}}$ is RCIRC One-Way.

We remark that the construction outlined above is RCIRC-OW for one input. A straightforward modification of the above arguments shows that if h is a $2k$-wise independent hash family, then $\widetilde{\mathcal{PKE}}$ is RCIRC-OW for k inputs.

6 Conclusion

The results of Gertner, Malkin and Reingold [GMR01] show that injective one-way trapdoor functions cannot be constructed in a black-box manner from IND-CPA secure encryption. Our results show that when the cryptosystem is indistinguishable from a one which loses information about the plaintext (i.e. lossy encryption), then we can construct injective trapdoor functions from it which are indistinguishable from functions that statistically lose information about their inputs (i.e. lossy trapdoor functions). The only requirement we have is that the plaintext space of the cryptosystem be larger than its randomness space.

This result is somewhat surprising because it does not parallel the standard (non-lossy) case. This is surprising as well given the number of generic primitives that imply lossy encryption, and the lack of constructions of injective one-way trapdoor functions from general assumptions. Our proof relies crucially on showing that lossy encryption with long plaintexts remains one-way even when encrypting with *randomness that is dependent on the message*. The notion of security in the presence of randomness dependent messages is an interesting one, and we hope it will prove useful in other constructions.

Applying the results of [MY09] to our constructions immediately gives a construction of IND-CCA secure encryption from lossy encryption with long plaintexts.

References

[BHHI10] Boaz Barak, Iftach Haitner, Dennis Hofheinz, and Yuval Ishai. Bounded key-dependent message security. In *Eurocrypt '10*, Lecture Notes in Computer Science, 2010. To Appear.

[BHHO08] Dan Boneh, Shai Halevi, Mike Hamburg, and Rafail Ostrovsky. Circular-secure encryption from decision diffie-hellman. In *Crypto '08*, pages 108–125. Springer Berlin / Heidelberg, 2008.

[BHSV98] Mihir Bellare, Shai Halevi, Amit Sahai, and Salil Vadhan. Many-to-one trapdoor functions and their relation to public-key cryptosystems. In *Crypto '98*, volume 1462 of *LNCS*, pages 283–298. Springer Berlin / Heidelberg, 1998.

[BHY09] Mihir Bellare, Dennis Hofheinz, and Scott Yilek. Possibility and impossibility results for encryption and commitment secure under selective opening. In *Eurocrypt '09*. Springer, 2009.

[BRS03] John Black, Phillip Rogaway, and Thomas Shrimpton. Encryption-scheme security in the presence of key-dependent messages. In *SAC '02: Revised Papers from the 9th Annual International Workshop on Selected Areas in Cryptography*, pages 62–75, London, UK, 2003. Springer-Verlag.

[CL01] Jan Camenisch and Anna Lysyanskaya. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In *Eurocrypt '01*, volume 2045 of *Lecture Notes in Computer Science*, pages 93+, 2001.

[CS09] Benny Applebaum David Cash and Chris Peikert Amit Sahai. Fast cryptographic primitives and circular-secure encryption based on hard learning problems. In *Crypto '09*, pages 595–618, Berlin, Heidelberg, 2009. Springer-Verlag.

[EGL85] Shimon Even, Oded Goldreich, and Abraham Lempel. A randomized protocol for signing contracts. *Communications of the ACM*, 28(6):637–647, 1985.

[GKM+00] Yael Gertner, Sampath Kannan, Tal Malkin, Omer Reingold, and Mahesh Viswanathan. The relationship between public key encryption and oblivious transfer. In *FOCS '00*, page 325, Washington, DC, USA, 2000. IEEE Computer Society.

[GMR01] Yael Gertner, Tal Malkin, and Omer Reingold. On the impossibility of basing trapdoor functions on trapdoor predicates. In *FOCS '01*, page 126, Washington, DC, USA, 2001. IEEE Computer Society.

[GOS06] Jens Groth, Rafail Ostrovsky, and Amit Sahai. Perfect non-interactive zero knowledge for np. In *Proceedings of Eurocrypt 2006, volume 4004 of LNCS*, pages 339–358. Springer, 2006.

[HLOV09] Brett Hemenway, Benoît Libert, Rafail Ostrovsky, and Damien Vergnaud. Lossy encryption: Constructions from general assumptions and efficient selective opening chosen ciphertext security. ePrint Archive 2009/088, 2009.

[HO09] Brett Hemenway and Rafail Ostrovsky. Lossy trapdoor functions from smooth homomorphic hash proof systems. ECCC Report TR09-127, 2009.

[HU08] Dennis Hofheinz and Dominique Unruh. Towards key-dependent message security in the standard model. In *Eurocrypt '08*, volume 4965 of *Lecture Notes in Computer Science*, pages 108–126, 2008.

[IR89] Russell Impagliazzo and Steven Rudich. Limits on the provable consequences of one-way permutations. In *STOC '89*, pages 44–61. ACM, 1989.

[KN08] Gillat Kol and Moni Naor. Cryptography and game theory: Designing protocols for exchanging information. In *TCC '08*, pages 320–339. Springer Berlin / Heidelberg, 2008.

[MY09] Petros Mol and Scott Yilek. Chosen-ciphertext security from slightly lossy trapdoor functions. Cryptology ePrint Archive, Report 2009/524, 2009. http://eprint.iacr.org/2009/524/.

[PVW08] Chris Peikert, Vinod Vaikuntanathan, and Brent Waters. A framework for efficient and composable oblivious transfer. In David Wagner, editor, *Crypto '08*, volume 5157 of *Lecture Notes in Computer Science*, pages 554–571. Springer, 2008.

[PW08] Chris Peikert and Brent Waters. Lossy trapdoor functions and their applications. In *STOC '08: Proceedings of the 40th annual ACM symposium on Theory of computing*, pages 187–196, New York, NY, USA, 2008. ACM.

[Rab81] Michael Rabin. How to exchange secrets by oblivious transfer. Technical Report TR-81, Harvard University, 1981.

[RS09] Alon Rosen and Gil Segev. Chosen-ciphertext security via correlated products. In *TCC '09*, pages 419–436, Berlin, Heidelberg, 2009. Springer-Verlag.

[RTV04] Omer Reingold, Luca Trevisan, and Salil Vadhan. Notions of reducibility between cryptographic primitives. In *TCC '04*, pages 1–20. Springer, 2004.

[Rud89] Steven Rudich. *Limits on the Provable Consequences of One-way Permutations*. PhD thesis, University of California, Berkeley, 1989.

[Vah10] Yevgeniy Vahlis. Two is a crowd? a black-box separation of one-wayness and security under correlated inputs. In *TCC '10*, volume 5978 of *Lecture Notes in Computer Science*. Springer Berlin / Heidelberg, 2010.

[Yao82] Andrew Yao. Theory and applications of trapdoor functions. In *FOCS '82*, pages 82–91. IEEE Computer Society, 1982.

Appendix

A Equivalence of Oblivious Transfer and Lossy Encryption

We briefly recall the definition of honest-receiver two-round statistically-hiding $\binom{2}{1}$-OT. Oblivious transfer is a protocol between a sender Sen and a receiver $\mathsf{Rec} = (\mathsf{Rec}_q, \mathsf{Rec}_d)$. The sender Sen has two strings m_0, m_1, and the receiver has a bit b. The receiver Rec_q generates a query q along with some state information sk and sends q to the sender. The sender generates randomness r evaluates $\mathsf{rsp} = \mathsf{Sen}(\mathsf{q}, m_0, m_1, r)$ and sends rsp to the receiver Rec_d who uses sk to obtain m_b.

- **Correctness:** For all $m_0, m_1 \in \{0,1\}^k$, for all $b \in \{0,1\}$, there is a negligible function ν such that

$$\Pr[(\mathsf{q}, sk) \xleftarrow{\$} \mathsf{Rec}_q(1^\lambda, b);\ \mathsf{rsp} \xleftarrow{\$} \mathsf{Sen}(\mathsf{q}, m_0, m_1) : \mathsf{Rec}_d(sk, \mathsf{rsp}) = m_b] \geq 1 - \nu(\lambda).$$

- **Receiver Privacy:** b remains computationally hidden from Sen's view. Specifically, we must have

$$\{(\mathsf{q}, sk) \xleftarrow{\$} \mathsf{Rec}_q(1^\lambda, 0) : \mathsf{q}\} \approx_c \{(\mathsf{q}, sk) \xleftarrow{\$} \mathsf{Rec}_q(1^\lambda, 1) : \mathsf{q}\},$$

  where the distributions are taken over the internal randomness of Rec_q.

- **Sender Privacy:** for any $b \in \{0,1\}$, for any strings m_0, m_1, m_0', m_1' such that $m_b = m_b'$ and any honest receiver's query $\mathsf{q} = \mathsf{Rec}_q(1^\lambda, b)$, it must hold that

$$\{(\mathsf{q}, sk) \xleftarrow{\$} \mathsf{Rec}_q(1^\lambda, b); \mathsf{rsp} \xleftarrow{\$} \mathsf{Sen}(\mathsf{q}, m_0, m_1) : \mathsf{rsp}\} \approx_s \{(\mathsf{q}, sk) \xleftarrow{\$} \mathsf{Rec}_q(1^\lambda, b); \mathsf{rsp} \xleftarrow{\$} \mathsf{Sen}(\mathsf{q}, m_0', m_1') : \mathsf{rsp}\}$$

  where the distributions are taken over the internal randomness of Rec_q and Sen.

A.1 $\binom{2}{1}$-OT Implies Lossy Encryption

We briefly review the construction in [HLOV09]. Let $(\mathsf{Sen}, \mathsf{Rec})$ be a two-round honest-receiver statistically-hiding $\binom{2}{1}$-OT. We construct a lossy encryption as follows:

- **Key Generation:**
  Define $G(1^\lambda, \mathsf{inj}) = \mathsf{Rec}_q(1^\lambda, 0)$. Set $pk = \mathsf{q}$, and $sk = sk$. Define $G(1^\lambda, \mathsf{lossy}) = \mathsf{Rec}_q(1^\lambda, 1)$. Set $pk = \mathsf{q}$, and $sk = \perp$.

- **Encryption:**
  Define $E(pk, m, r) = \mathsf{Sen}(\mathsf{q}, m, 0^{|m|}; r)$, where r is the randomness used in $\mathsf{Sen}(\mathsf{q}, m, 0)$.

- **Decryption:**
  To decrypt $c = \mathsf{rsp}$ in injective mode, we define $D(sk, \mathsf{rsp}) = \mathsf{Rec}_d(sk, \mathsf{rsp})$.

Notice that the sender randomness from the OT protocol becomes the encryption randomness in the lossy encryption scheme. Thus if the sender randomness is shorter than the messages in the OT, the encryption randomness will be shorter than the messages in the lossy encryption.

A.2 Lossy Encryption is $\binom{2}{1}$-OT

We briefly review the construction of statistically sender private $\binom{2}{1}$-OT from lossy encryption given in [PVW08].

Let $\mathcal{PKE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a lossy encryption scheme. Then define an oblivious transfer protocol as follows:

- **Query:** For a given bit b, the receiver generates a query (pk_0, pk_1) where $pk_b \xleftarrow{\$} \mathsf{Gen}(1^\lambda, inj)$, and $pk_{1-b} \xleftarrow{\$} \mathsf{Gen}(1^\lambda, lossy)$.
- **Response:** For given strings x_0, x_1, the sender responds to a query (pk_0, pk_1) by choosing $r_0, r_1 \xleftarrow{\$} \mathcal{R}$, and sending $E(pk_0, x_0, r_0), E(pk_1, x_1, r_1)$ to the receiver.

Note that in this direction, the randomness used by the OT is twice the randomness used by the lossy encryption since an OT response consists of two ciphertexts. This does not affect our results, however, since we make use of the implication in the opposite direction.

B Constructing Lossy Encryption With Long Plaintexts

In [HLOV09], Hemenway et al. showed that lossy encryption can be constructed from statistically rerandomizable encryption and from statistically sender private $\binom{2}{1}$-oblivious transfer. This immediately yields constructions of lossy encryption from homomorphic encryption and smooth universal hash proof systems. Using the generic transformation from re-randomizable encryption to lossy encryption given in [HLOV09], we have efficient Lossy Encryption from the Damgård-Jurik cryptosystem. Unfortunately none of the other constructions immediately yield lossy encryption with long plaintexts.

Recall, that with a standard IND-CPA secure cryptosystem $\mathcal{PKE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ we can arbitrarily extend the plaintext space by expanding the randomness with a pseudorandom generator. Specifically, if PRG is pseudorandom generator, such that $\mathsf{PRG} : \mathcal{R} \to \mathcal{R}^k$, we can define a new cryptosystem, with encryption of $(m_1, \ldots, m_k)$ under randomness r given by setting $r_1, \ldots, r_k = \mathsf{PRG}(r)$, and setting the ciphertext as $\mathsf{Enc}(m_1, r_1), \ldots, \mathsf{Enc}(m_k, r_k)$. It is important to notice that applying this construction to a lossy encryption scheme, will yield an IND-CPA secure scheme, but not necessarily a lossy encryption scheme.

ECCC ISSN 1433-8092

http://eccc.hpi-web.de