Constructing Lossy Trapdoor Functions

Brett Hemenway    Rafail Ostrovsky

December 5th, 2013
Introduction

Lossy Encryption and Lossy Trapdoor Functions

LTFs from Lossy Encryption

Randomness Dependent Message (RDM) Security

Conclusion and Open Problems
Derandomizing encryption schemes

Trying to build injective trapdoor functions

Enc_{pk}(x, r)

CPA secure encryption of

Enc_{pk}(x, f(x))

Randomness is a function of message

Is this one-way?

In general this is a bad idea!
Derandomizing encryption schemes

Trying to build injective trapdoor functions

$\text{Enc}_{pk}(x, r)$

CPA secure encryption of $x$

Is this one-way?

In general this is a bad idea!
Derandomizing encryption schemes

Trying to build injective trapdoor functions

\[ \text{Enc}_{pk}(x, f(x)) \]

Randomness is a function of message
Derandomizing encryption schemes

Trying to build injective trapdoor functions

\[ \text{Enc}_{pk}(x, f(x)) \]

Is this one-way?

Randomness is a function of message
Derandomizing encryption schemes

Trying to build injective trapdoor functions

\[ \text{Enc}_{pk}(x, f(x)) \]

In general this is a bad idea!

Randomness is a function of message
Encrypting randomness dependent messages is a bad idea

A simple example: using message as randomness

Suppose:

- \( \text{Enc}_{pk}(\cdot, \cdot) \) is CPA secure
- Messages and randomness are the same length
Encrypting randomness dependent messages is a bad idea

A simple example: using message as randomness

Suppose:
- $\text{Enc}_{pk}(\cdot, \cdot)$ is CPA secure
- Messages and randomness are the same length

\[
\begin{align*}
\text{If } x &= r \\
& \quad c = x \\
\text{Else} \\
& \quad c = \text{Enc}_{pk}(x, r)
\end{align*}
\]
Encrypting randomness dependent messages is a bad idea

A simple example: using message as randomness

Suppose:

- \( \text{Enc}_{pk}(\cdot, \cdot) \) is CPA secure
- Messages and randomness are the same length

\[
\begin{align*}
\text{If } x &= r \\
& \quad \Rightarrow c = x \\
\text{Else} & \quad c = \text{Enc}_{pk}(x, r)
\end{align*}
\]

\( x \mapsto \text{Enc}'_{pk}(\cdot, \cdot) \) is \textbf{not} one-way
Message-dependent randomness

- $x \mapsto \text{Enc}_{pk}(x, x)$ is not one-way
- What about $x \mapsto \text{Enc}_{pk}(x, h(x))$?
This approach is doomed to fail

**Theorem ([GMR01])**

There is no black-box construction of injective trapdoor functions from IND-CPA secure cryptosystems
Random oracles break message dependency

If $\text{Enc}$ is IND-CPA secure, and $h$ is a RO, then

- $x \mapsto \text{Enc}(x, h(x))$ is a one-way trapdoor function [BHSV98]
- $x \mapsto \text{Enc}(x, h(pk, x))$ is deterministic encryption [BBO07]
Dependencies between messages and randomness

- \( x \mapsto \text{Enc}(x, x) \) may not be one-way
- \( x \mapsto \text{Enc}(x, h(x)) \) is one-way when \( h \) is a RO
- What if \( h \) is a some other function?
Main result

If:

- Enc is *lossy encryption*
- $h$ is a pairwise independent hash function

Then:

$x \mapsto Enc(x, h(x))$ is an injective trapdoor function
Main result

If:

- Enc is *lossy encryption*
- $h$ is a pairwise independent hash function
- Message space is larger than the randomness space

Then:

$x \mapsto \text{Enc}(x, h(x))$ is an injective trapdoor function
Introduction

Lossy Encryption and Lossy Trapdoor Functions

LTFs from Lossy Encryption

Randomness Dependent Message (RDM) Security

Conclusion and Open Problems
Lossy Cryptographic Primitives

- Lossy primitives have two types of public-keys
  - **Injective keys** - these allow decryption / inversion
  - **Lossy keys** - these *statistically* lose information about the message / input

- The two types of keys are computationally indistinguishable
Lossy Encryption

[GOS06, PW08, PVW08, KN08, BHY09]

\[ G(1^\lambda, \text{mode}), E(pk, m, r), D(sk, c) \]

**Correctness:**

For all \( m, r \)

\[ D(E(pk_I, m, r)) = m \]

**Lossiness:**

For all \( m_0, m_1 \)

\[ \{ E(pk_L, m_0, r) \} \approx^s \{ E(pk_L, m_1, r) \} \]

**Indistinguishability**

\[ \{ pk_I : pk_I \leftarrow G(1^\lambda, \text{Injective}) \} \approx^c \{ pk_L : pk_L \leftarrow G(1^\lambda, \text{Lossy}) \} \]
Lossy Encryption
[GOS06, PW08, PVW08, KN08, BHY09]

\[ G(1^\lambda, \text{mode}), E(pk, m, r), D(sk, c) \]

**Correctness:**
For all \( m, r \)
\[ D(E(pk_I, m, r)) = m \]

**Lossiness:**
For all \( m_0, m_1 \)
\[ \{ E(pk_L, m_0, r) \} \approx_s \{ E(pk_L, m_1, r) \} \]

**Indistinguishability**
\[ \{ pk_I : pk_I \leftarrow G(1^\lambda, \text{Injective}) \} \approx_c \{ pk_L : pk_L \leftarrow G(1^\lambda, \text{Lossy}) \} \]
Lossy Encryption

[GOS06, PW08, PVW08, KN08, BHY09]

\[ G(1^\lambda, \text{mode}), E(pk, m, r), D(sk, c) \]

**Correctness:**
For all \( m, r \)
\[ D(E(pk_I, m, r)) = m \]

**Lossiness:**
For all \( m_0, m_1 \)
\[ \{E(pk_L, m_0, r)\} \approx_s \{E(pk_L, m_1, r)\} \]

**Indistinguishability**
\[ \{pk_I : pk_I \leftarrow G(1^\lambda, \text{Injective})\} \approx^c \{pk_L : pk_L \leftarrow G(1^\lambda, \text{Lossy})\} \]
Lossy Encryption  
[GOS06, PW08, PVW08, KN08, BHY09]

\[
G(1^\lambda, \text{mode}), E(pk, m, r), D(sk, c)
\]

**Correctness:**  
For all \( m, r \)
\[
D(E(pk_I, m, r)) = m
\]

**Lossiness:**  
For all \( m_0, m_1 \)
\[
\{ E(pk_L, m_0, r) \} \approx_s \{ E(pk_L, m_1, r) \}
\]

**Indistinguishability**
\[
\{ pk_I : pk_I \leftarrow G(1^\lambda, \text{Injective}) \} \approx^c \{ pk_L : pk_L \leftarrow G(1^\lambda, \text{Lossy}) \}
\]
Lossy Encryption
[GOS06, PW08, PVW08, KN08, BHY09]

G(1^\lambda, \text{mode}), E(pk, m, r), D(sk, c)

**Correctness:**
For all \( m, r \)

\[ D(E(pk_I, m, r)) = m \]

**Lossiness:**
For all \( m_0, m_1 \)

\[ \{E(pk_L, m_0, r)\} \approx^s \{E(pk_L, m_1, r)\} \]

**Indistinguishability**

\[ \{pk_I : pk_I \leftarrow G(1^\lambda, \text{Injective})\} \approx^c \{pk_L : pk_L \leftarrow G(1^\lambda, \text{Lossy})\} \]

Notice: Indistinguishability + Lossiness \( \Rightarrow \) IND-CPA security
Lossy Trapdoor Functions [PW08]

$F_I \approx F_\ell$

Injective Mode

Lossy Mode

$F_I^{-1}$

$F_I$
Lossy Trapdoor Functions in Detail

\[(s, t) \leftarrow G_{LTDF}(1^\lambda, inj)\]
Lossy Trapdoor Functions in Detail

\[(s, t) \leftarrow G_{LTDF}(1^\lambda, inj) \quad (s, \bot) \rightarrow G_{LTDF}(1^\lambda, lossy)\]
Lossy Trapdoor Functions in Detail

\[(s, t) \leftarrow G_{LTDF}(1^\lambda, inj) \quad (s, \perp) \rightarrow G_{LTDF}(1^\lambda, lossy)\]

Trapdoor:
\[F^{-1}(t, F(s, x)) = x\]
Lossy Trapdoor Functions in Detail

\[(s, t) \leftarrow G_{LTDF}(1^\lambda, inj) \quad (s, \bot) \rightarrow G_{LTDF}(1^\lambda, lossy)\]

Trapdoor:
\[F^{-1}(t, F(s, x)) = x\]

Lossiness:
\[|\text{im } F(s, \cdot)| \leq 2^r\]
Lossy Trapdoor Functions in Detail

\[(s, t) \leftarrow \text{GLTDF}(1^\lambda, inj) \quad \quad (s, \bot) \rightarrow \text{GLTDF}(1^\lambda, \text{lossy})\]

Trapdoor:
\[F^{-1}(t, F(s, x)) = x\]

Lossiness:
\[|\text{im } F(s, \cdot)| \leq 2^r\]

The first outputs of \(\text{GLTDF}(1^\lambda, inj)\), and \(\text{GLTDF}(1^\lambda, \text{lossy})\) are computationally indistinguishable.
Constructions of LTFs

- DDH, LWE [PW08]
- DCR [RS08, BFO08]
- D-Linear, QR [FGK+10]
- Φ-Hiding [KOS10]
- EDDH [HO12]
Implications of LTFs

- IND-CCA encryption (also IND-CPA, CRHF, OT, PRG) [PW08]
- Deterministic Encryption [BFO08]
- Correlated Product Security [RS09, MY09]
- Replace RO in RSA-OAEP [KOS10]
- Leaky Pseudo-entropy Functions [BHK11]
Introduction

Lossy Encryption and Lossy Trapdoor Functions

LTFs from Lossy Encryption

Randomness Dependent Message (RDM) Security

Conclusion and Open Problems
Lossy Encryption

Standard Encryption

Message Space

Ciphertext Space

Perfect correctness is equivalent to disjointness.

Perfectly Lossy Encryption

If the number of messages is larger than the number of encryptions of zero, we have lossiness.
Lossy Encryption

Perfect correctness is equivalent to disjointness.

If the number of messages is larger than the number of encryptions of zero, we have lossiness.
Lossy Encryption

Perfect correctness is equivalent to disjointness if the number of messages is larger than the number of encryptions of zero, we have lossiness.
Lossy Encryption

Perfectly Lossy Encryption

Perfect correctness is equivalent to disjointness

If the number of messages is larger than the number of encryptions of zero, we have lossiness.
Lossy Encryption

Perfectly Lossy Encryption

If the number of messages is larger than the number of encryptions of zero, we have lossiness.
Perfectly Lossy Encryption Implies LTFs
A simple warmup

- Suppose
  - Enc is a *perfectly lossy encryption*.
  - $|\mathcal{M}| > |\mathcal{R}|$ ($|\text{Message Space}| > |\text{Randomness Space}|$)
- Define:
  $$F_{pk}(x) = Enc_{pk}(x, 0)$$
Perfectly Lossy Encryption Implies LTFs

A simple warmup

- Suppose
  - Enc is a *perfectly lossy encryption*.
  - $|\mathcal{M}| > |\mathcal{R}|$ (|Message Space| > |Randomness Space|)
- Define:
  $$F_{pk}(x) = Enc_{pk}(x, 0)$$

Then $F_{pk}(x)$ is a lossy trapdoor function.

**Proof:**
In lossy mode, the image of $F$ is bounded by $|\mathcal{R}| < |\mathcal{M}|$. 
Injective and lossy modes are indistinguishable because Enc is a lossy encryption.
Lossy Encryption

- Standard Encryption

Message Space

Ciphertext Space

Even if $\text{Enc}(x, R)$ is small and the overlap is large, the union of all the encryption spaces will be larger than $|M|$, so the previous argument fails.
Even if $\text{Enc}(x, R)$ is small and the overlap is large, the union of all the encryption spaces will be larger than $|M|$, so the previous argument fails.
Lossy Encryption

Statistically Lossy Encryption

Even if $\text{Enc}(x, R)$ is small and the overlap is large, the union of all the encryption spaces will be larger than $|M|$, so the previous argument fails.
Even if $\text{Enc}(x, R)$ is small and the overlap is large, the union of all the encryption spaces will be larger than $|\mathcal{M}|$, so the previous argument fails.
Lossy Trapdoor Functions from Lossy Encryption

Main result

- Suppose
  - \textit{Enc} is a \textit{lossy encryption}.
  - The plaintext space, \( \mathcal{M} \) is larger than the randomness space \( \mathcal{R} \).

- Define: \( F_{pk}(x) = \text{Enc}_{pk}(x, h(x)) \)
where \( h \) is a pairwise independent hash function. Then \( F_{pk}(x) \) is a lossy trapdoor function.
Proof Sketch:
We must show that in lossy mode, with high probability over the choice of $h$, the size of $\left| \bigcup_{x \in \mathcal{M}} \text{Enc}_{pk}(x, h(x)) \right| < |\mathcal{M}|$. Let $C_0 = \text{Enc}_{pk}(0, \mathcal{R})$ (the set of encryptions of 0).

- In lossy mode, with high probability over $x$, $\text{Enc}_{pk}(x, h(x)) \in C_0$.
- Expected number of points $F_{pk}(x) \in C_0$ is large.
- Pairwise independence shows variance is small.
- With high probability most of the evaluations $F_{pk}(x)$ lie in the small space $C_0$. 


Main Result: Lossy encryption with plaintexts at least one bit longer than the randomness implies LTFs.

Lossy Encryption is equivalent to statistically sender private 1-2-OT, so statistically hiding OT with long messages implies lossy trapdoor functions and hence injective trapdoor functions.

The primary open question is whether we can relax the requirement on plaintext length.
Comparison to Non-Lossy Case

- [BHSV98]: when Enc is an IND-CPA secure cryptosystem, and $h$ is a random oracle, $F_{pk}(x) = \text{Enc}_{pk}(x, h(x))$ is an injective trapdoor function.
- [BBO07]: when Enc is an IND-CPA secure cryptosystem, and $h$ is a random oracle, $F_{pk}(x) = \text{Enc}_{pk}(x, h(x||pk))$ is deterministic encryption.
- Our results do not require a random oracle.
Introduction

Lossy Encryption and Lossy Trapdoor Functions

LTFs from Lossy Encryption

Randomness Dependent Message (RDM) Security

Conclusion and Open Problems
Randomness dependent message security
See also [BCPT13]

\[pk \leftarrow \text{Gen}(1^\lambda)\]
\[\vec{r} = (r_1, \ldots, r_n) \leftarrow \text{coins(Enc)}\]
\[(f_1, \ldots, f_n) \leftarrow A_1(pk)\]
\[\vec{c} = (\text{Enc}(pk, f_1(\vec{r}), r_1), \ldots, \text{Enc}(pk, f_n(\vec{r}), r_n))\]
\[b \leftarrow A_2(\vec{c})\]

Real
Randomness dependent message security

See also [BCPT13]

\[
pk \leftarrow \text{Gen}(1^\lambda)
\]

\[
\vec{r} = (r_1, \ldots, r_n) \leftarrow \text{coins}(\text{Enc})
\]

\[
(f_1, \ldots, f_n) \leftarrow A_1(pk)
\]

\[
\vec{c} = (\text{Enc}(pk, 0, r_1), \ldots, \text{Enc}(pk, 0, r_n))
\]

\[
b \leftarrow A_2(\vec{c})
\]
Randomness dependent message security
See also [BCPT13]

\[
pk \overset{\$}{\leftarrow} \text{Gen}(1^\lambda)
\]
\[
\vec{r} = (r_1, \ldots, r_n) \overset{\$}{\leftarrow} \text{coins(Enc)}
\]
\[
(f_1, \ldots, f_n) \overset{\$}{\leftarrow} A_1(pk)
\]
\[
\vec{c} = (\text{Enc}(pk, 0, r_1), \ldots, \text{Enc}(pk, 0, r_n))
\]
\[
b \leftarrow A_2(\vec{c})
\]

Parallels KDM security [BRS03, BHOO08, HU08, ACPS09]
Randomness Circular Security

Definition

A cryptosystem is Randomness Circular Secure if

\[
\{pk, \text{Enc}(pk, r_2, r_1), \text{Enc}(pk, r_3, r_2), \ldots, \text{Enc}(pk, r_n, r_{n-1}), \text{Enc}(pk, r_1, r_n)\}
\approx_c
\{pk, \text{Enc}(pk, 0, r_1), \ldots, \text{Enc}(pk, 0, r_n)\}
\]
Randomness Circular Security

Definition

A cryptosystem is Randomness Circular Secure if

\[
\{ pk, \text{Enc}(pk, r_2, r_1), \text{Enc}(pk, r_3, r_2), \ldots, \text{Enc}(pk, r_n, r_{n-1}), \text{Enc}(pk, r_1, r_n) \} \\
\approx_c \\
\{ pk, \text{Enc}(pk, 0, r_1), \ldots, \text{Enc}(pk, 0, r_n) \}
\]

Similar to (key) circular security [CL01, BRS03, BHHO08]
A cryptosystem is RCIRC-one-way if the map

\[(r_1, \ldots, r_n) \mapsto (\text{Enc}(pk, r_2, r_1), \ldots, \text{Enc}(pk, r_1, \ldots, r_n))\]

is one-way.
A cryptosystem is RCIRC-one-way if the map

\[(r_1, \ldots, r_n) \mapsto (\text{Enc}(pk, r_2, r_1), \ldots, \text{Enc}(pk, r_1, \ldots, r_n))\]

is one-way

Implies one-way trapdoor functions
Introduction

Lossy Encryption and Lossy Trapdoor Functions

LTFs from Lossy Encryption

Randomness Dependent Message (RDM) Security

Conclusion and Open Problems
Conclusions

- Lossy Encryption with long plaintexts implies LTFs
- OT with long messages implies injective trapdoor functions
Open Problems

- Does Lossy Encryption imply LTFs?
  i.e. can we drop the restriction on plaintext length?
Thanks!
Benny Applebaum, David Cash, Chris Peikert, and Amit Sahai. 
Fast Cryptographic Primitives and Circular-Secure Encryption Based on Hard Learning Problems. 

Mihir Bellare, Alexandra Boldyreva, and Adam O’Neill. 
Deterministic and Efficiently Searchable Encryption. 
Eleanor Birrell, Kai-Min Chung, Rafael Pass, and Sidharth Telang.  
Randomness-Dependent Message Security.  

Alexandra Boldyreva, Serge Fehr, and Adam O’Neill.  
References III


References V

David M. Freeman, Oded Goldreich, Eike Kiltz, Alon Rosen, and Gil Segev.
More Constructions of Lossy and Correlation-Secure Trapdoor Functions.
In *Public Key Cryptography 2010 (PKC 2010)*, Lecture Notes in Computer Science, 2010.

Yael Gertner, Tal Malkin, and Omer Reingold.
On the Impossibility of Basing Trapdoor Functions on Trapdoor Predicates.

Jens Groth, Rafail Ostrovsky, and Amit Sahai.
Perfect non-interactive zero knowledge for NP.
References VI

Brett Hemenway and Rafail Ostrovsky.
Building Injective Trapdoor Functions From Oblivious Transfer.

Brett Hemenway and Rafail Ostrovsky.
Extended-DDH and Lossy Trapdoor Functions.
In PKC 2012, 2012.

Dennis Hofheinz and Dominique Unruh.
Towards Key-Dependent Message Security in the Standard Model.
Gillat Kol and Moni Naor.
Cryptography and Game Theory: Designing Protocols for Exchanging Information.

Eike Kiltz, Adam O’Neill, and Adam Smith.
Instantiability of RSA-OAEP under chosen-plaintext attack.

Petros Mol and Scott Yilek.
Chosen-Ciphertext Security from Slightly Lossy Trapdoor Functions.
References VIII

Chris Peikert, Vinod Vaikuntanathan, and Brent Waters.
A Framework for Efficient and Composable Oblivious Transfer.

Chris Peikert and Brent Waters.
Lossy trapdoor functions and their applications.

Alon Rosen and Gil Segev.
Efficient Lossy Trapdoor Functions Based on the Composite Residuosity Assumption.
Alon Rosen and Gil Segev.
Chosen-Ciphertext Security via Correlated Products.