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

Derandomizing encryption schemes

Trying to build injective trapdoor functions

CPA secure encryption of x

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

Derandomizing encryption schemes

Trying to build injective trapdoor functions

$\mathrm{Enc}_{pk}(x, f(x))$

Randomness is a function of message

Derandomizing encryption schemes

Trying to build injective trapdoor functions

Is this one-way?

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

Randomness is a function of message

Derandomizing encryption schemes

Trying to build injective trapdoor functions

$\mathsf{Enc}_{pk}(x, f(x))$

$\boxed{\text{In general this is a bad idea!}}$

Randomness is a function of message

Encrypting randomness dependent messages is a bad idea

A simple example: using message as randomness

Suppose:

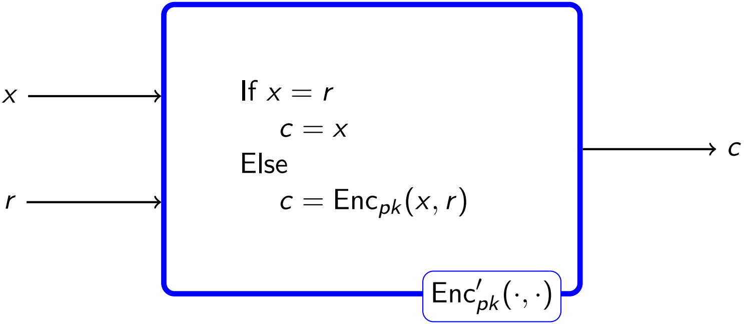
- $\text{Enc}_{pk}(\cdot, \cdot)$ is CPA secure
- Messages and randomness are the same length

Encrypting randomness dependent messages is a bad idea

A simple example: using message as randomness

Suppose:

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

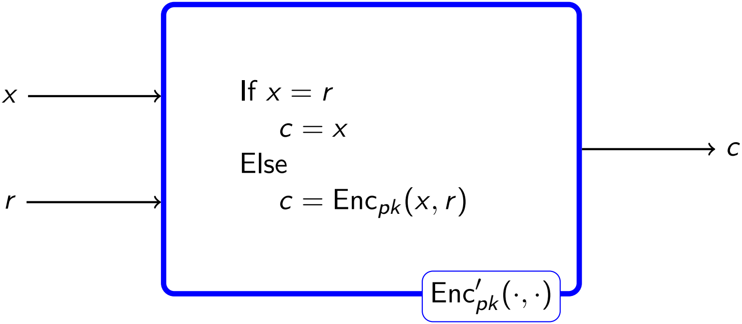


Encrypting randomness dependent messages is a bad idea

A simple example: using message as randomness

Suppose:

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



$x \mapsto \mathsf{Enc}'_{pk}(x, x)$ is **not** one-way

Message-dependent randomness

- $x \mapsto \mathsf{Enc}_{pk}(x, x)$ is not one-way
- What about

$$x \mapsto \mathsf{Enc}_{pk}(x, h(x))?$$

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 Enc is IND-CPA secure, and h is a RO, then

- $x \mapsto \mathrm{Enc}(x, h(x))$ is a one-way trapdoor function [BHSV98]
- $x \mapsto \mathrm{Enc}(x, h(pk, x))$ is deterministic encryption [BBO07]

Dependencies between messages and randomness

- $x \mapsto \mathsf{Enc}(x, x)$ may not be one-way
- $x \mapsto \mathsf{Enc}(x, h(x))$ 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:

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

Main result

If:

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

Then:

$x \mapsto \mathsf{Enc}(x, h(x))$ 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]

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

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

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

Lossy Encryption

[GOS06, PW08, PVW08, KN08, BHY09]

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

Correctness:

For all m, r

$$\boxed{D(E(pk_I, m, r)) = m}$$

Lossiness:

For all m_0, m_1

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

Indistinguishability

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

Lossy Encryption

[GOS06, PW08, PVW08, KN08, BHY09]

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

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

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

Lossy Encryption

[GOS06, PW08, PVW08, KN08, BHY09]

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

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

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

Lossy Encryption

[GOS06, PW08, PVW08, KN08, BHY09]

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

Correctness:

For all m, r

$$D(E(pk_I, m, r)) = m$$

Lossiness:

For all m_0, m_1

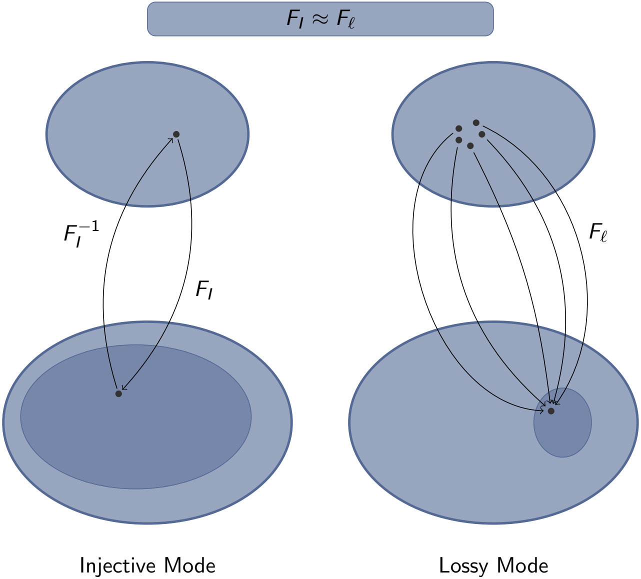
$$\{E(pk_L, m_0, r)\} \approx^s \{E(pk_L, m_1, r)\}$$

Indistinguishability

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

Notice: Indistinguishability + Lossiness $\Longrightarrow$ IND-CPA security

Lossy Trapdoor Functions [PW08]



Lossy Trapdoor Functions in Detail

$$(s, t) \longleftarrow G_{LTDF}(1^\lambda, inj)$$

Lossy Trapdoor Functions in Detail

$$(s, t) \longleftarrow G_{LTDF}(1^{\lambda}, inj) \qquad\qquad (s, \perp) \longrightarrow G_{LTDF}(1^{\lambda}, lossy)$$

Lossy Trapdoor Functions in Detail

$$(s, t) \longleftarrow G_{LTDF}(1^{\lambda}, inj) \qquad\qquad (s, \perp) \longrightarrow G_{LTDF}(1^{\lambda}, lossy)$$

Trapdoor:

$$F^{-1}(t, F(s, x)) = x$$

Lossy Trapdoor Functions in Detail

$$(s, t) \longleftarrow G_{LTDF}(1^\lambda, inj) \qquad (s, \perp) \longrightarrow G_{LTDF}(1^\lambda, lossy)$$

Trapdoor:

$$F^{-1}(t, F(s, x)) = x$$

Lossiness:

$$|\operatorname{im} F(s, \cdot)| \leq 2^r$$

Lossy Trapdoor Functions in Detail

$$(s, t) \longleftarrow G_{LTDF}(1^{\lambda}, inj) \qquad (s, \perp) \longrightarrow G_{LTDF}(1^{\lambda}, lossy)$$

Trapdoor:
$$F^{-1}(t, F(s, x)) = x$$

Lossiness:
$$|\operatorname{im} F(s, \cdot)| \leq 2^{r}$$

The first outputs of $G_{LTDF}(1^{\lambda}, inj)$, and $G_{LTDF}(1^{\lambda}, lossy)$ 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,CRHFs,OT,PRGs) [PW08]
- Deterministic Encryption [BFO08]
- Correlated Product Security [RS09, MY09]
- Replace RO in RSA-OAEP [KOS10]
- Leaky Pseudo-entropy Functions [BHK11]

Introduction

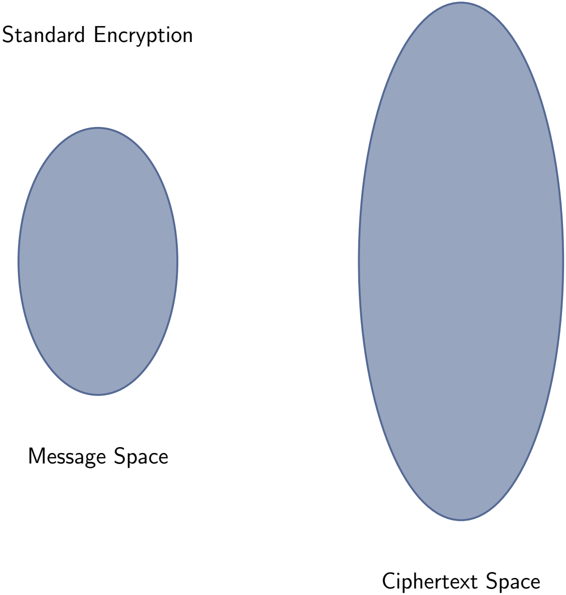
Lossy Encryption and Lossy Trapdoor Functions

LTFs from Lossy Encryption

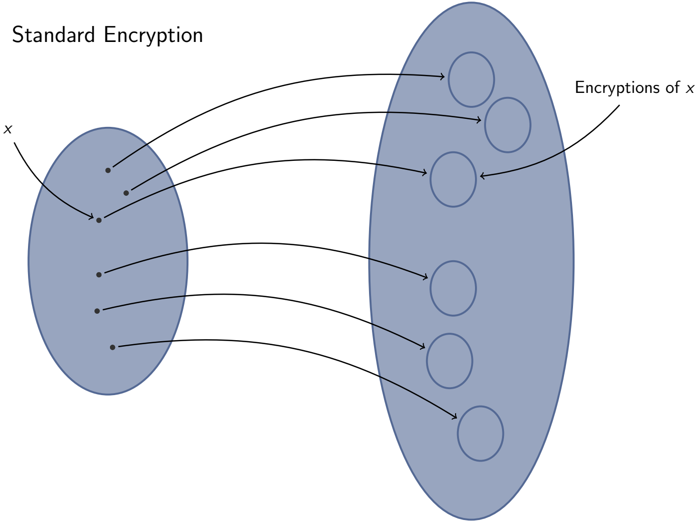
Randomness Dependent Message (RDM) Security

Conclusion and Open Problems

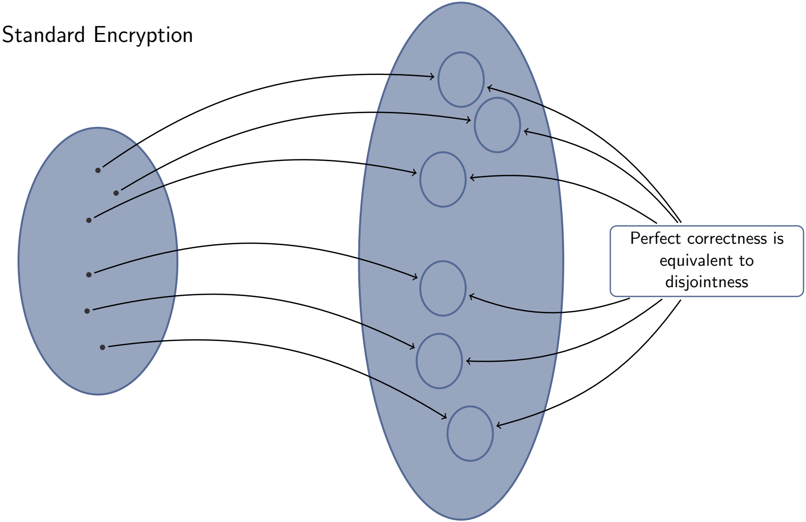
Lossy Encryption



Lossy Encryption

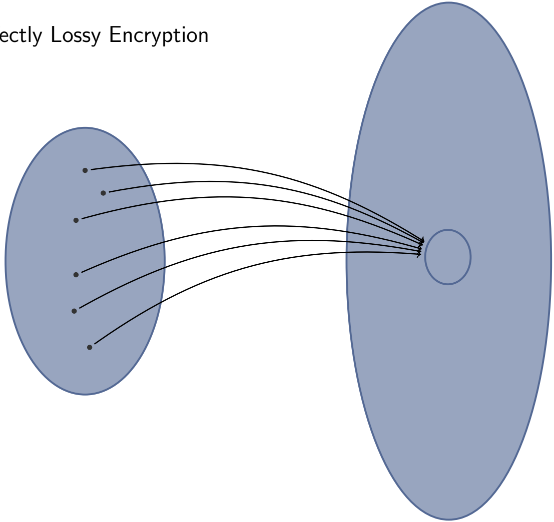


Lossy Encryption



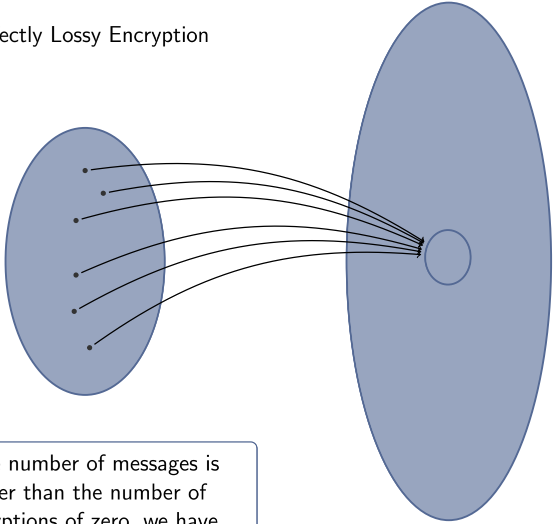
Lossy Encryption

Perfectly Lossy Encryption



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*.
  - $|\mathcal{M}| > |\mathcal{R}|$ (|Message Space| > |Randomness Space|)
- Define:

$$F_{pk}(x) = \mathsf{Enc}_{pk}(x, 0)$$

Perfectly Lossy Encryption Implies LTFs

A simple warmup

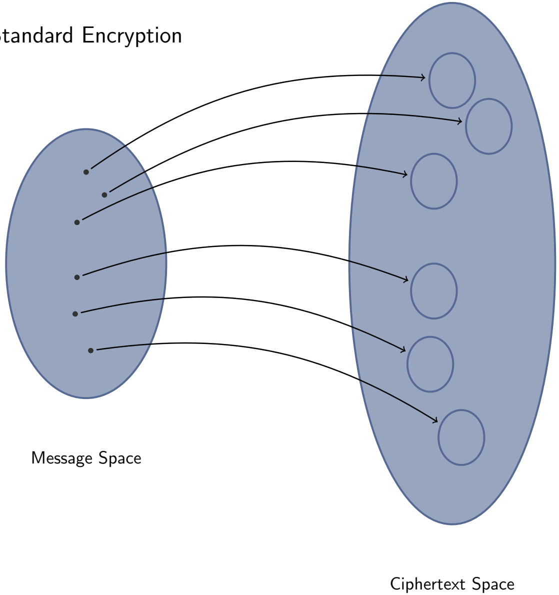
- Suppose
  - Enc is a *perfectly lossy encryption*.
  - $|\mathcal{M}| > |\mathcal{R}|$ ($|$Message Space$| > |$Randomness Space$|$)
- Define:

$$F_{pk}(x) = \mathrm{Enc}_{pk}(x, 0)$$

  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.

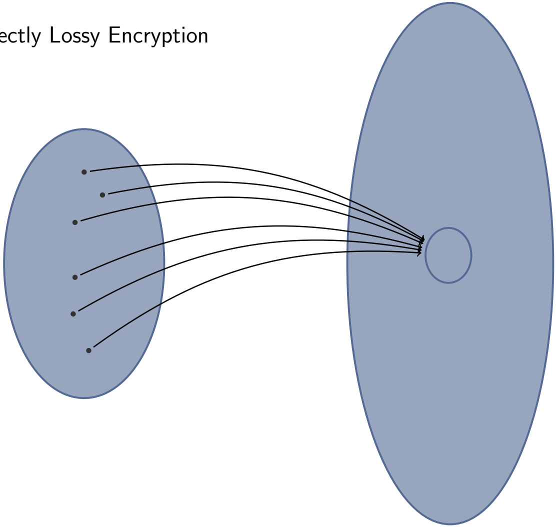
Lossy Encryption

Standard Encryption



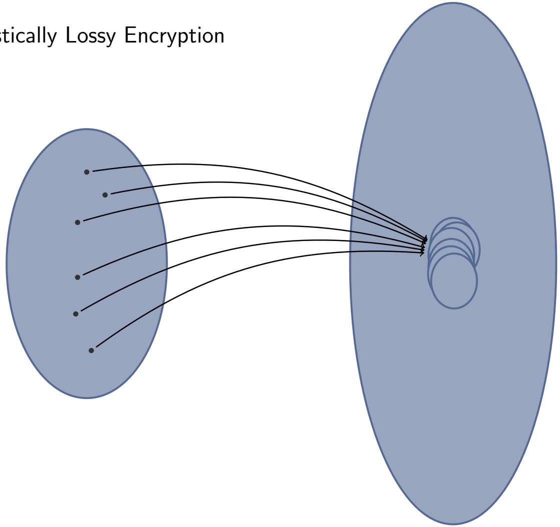
Lossy Encryption

Perfectly Lossy Encryption



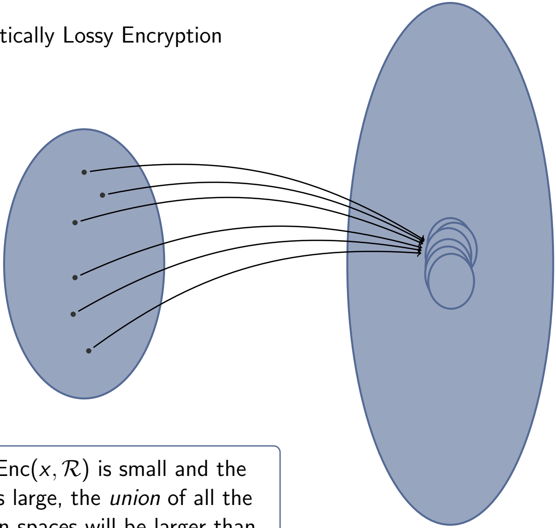
Lossy Encryption

Statistically Lossy Encryption



Lossy Encryption

Statistically Lossy Encryption



Even if $\mathrm{Enc}(x, \mathcal{R})$ 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
  - Enc is a *lossy encryption*.
  - The plaintext space, $\mathcal{M}$ is larger than the randomness space $\mathcal{R}$.
- Define: $F_{pk}(x) = \mathsf{Enc}_{pk}(x, h(x))$
  where h is a pairwise independent hash function. Then $F_{pk}(x)$ is a lossy trapdoor function.

Lossy Trapdoor Functions from Lossy Encryption

- **Proof Sketch:**
  We must show that in lossy mode, with high probability over the choice of h, the size of $\left|\bigcup_{x \in \mathcal{M}} \mathsf{Enc}_{pk}(x, h(x))\right| < |\mathcal{M}|$.
  Let $C_0 = \mathsf{Enc}_{pk}(0, \mathcal{R})$ (the set of encryptions of 0).
- In lossy mode, with high probability over x, $\mathsf{Enc}_{pk}(x, h(x)) \in C_0$.
- 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.

Lossy Trapdoor Functions from Lossy Encryption

Consequences

- **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, $F_{pk}(x) = \mathsf{Enc}_{pk}(x, h(x))$ is an injective trapdoor function.
- [BBO07]: when Enc is an IND-CPA secure cryptosystem, and h is a random oracle, $F_{pk}(x) = \mathsf{Enc}_{pk}(x, h(x||pk))$ 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]

$$pk \xleftarrow{\$} \mathsf{Gen}(1^\lambda)$$

$$\vec{r} = (r_1, \ldots, r_n) \xleftarrow{\$} \mathsf{coins}(\mathsf{Enc})$$

$$(f_1, \ldots, f_n) \xleftarrow{\$} \mathcal{A}_1(pk)$$

$$\vec{c} = (\mathsf{Enc}(pk, f_1(\vec{r}), r_1), \ldots, \mathsf{Enc}(pk, f_n(\vec{r}), r_n))$$

$$b \leftarrow A_2(\vec{c})$$

Real

Randomness dependent message security

See also [BCPT13]

$$pk \xleftarrow{\$} \mathsf{Gen}(1^\lambda)$$

$$\vec{r} = (r_1, \ldots, r_n) \xleftarrow{\$} \mathsf{coins}(\mathsf{Enc})$$

$$(f_1, \ldots, f_n) \xleftarrow{\$} \mathcal{A}_1(pk)$$

$$\boxed{\vec{c} = (\mathsf{Enc}(pk, 0, r_1), \ldots, \mathsf{Enc}(pk, 0, r_n))}$$

$$b \leftarrow A_2(\vec{c})$$

Ideal

Randomness dependent message security

See also [BCPT13]

$pk \xleftarrow{\$} \mathsf{Gen}(1^\lambda)$

$\vec{r} = (r_1, \ldots, r_n) \xleftarrow{\$} \mathsf{coins}(\mathsf{Enc})$

$(f_1, \ldots, f_n) \xleftarrow{\$} \mathcal{A}_1(pk)$

$\boxed{\vec{c} = (\mathsf{Enc}(pk, 0, r_1), \ldots, \mathsf{Enc}(pk, 0, r_n))}$

$b \leftarrow A_2(\vec{c})$

Parallels KDM security [BRS03, BHHO08, HU08, ACPS09]

Randomness Circular Security

Definition

A cryptosystem is Randomness Circular Secure if

$$\{pk, \mathrm{Enc}(pk, r_2, r_1), \mathrm{Enc}(pk, r_3, r_2), \ldots, \mathrm{Enc}(pk, r_n, r_{n-1}), \mathrm{Enc}(pk, r_1, r_n)\}$$
$$\approx_c$$
$$\{pk, \mathrm{Enc}(pk, 0, r_1), ..., \mathrm{Enc}(pk, 0, r_n)\}$$

Randomness Circular Security

Definition

A cryptosystem is Randomness Circular Secure if

$$\{pk, \mathsf{Enc}(pk, r_2, r_1), \mathsf{Enc}(pk, r_3, r_2), \ldots, \mathsf{Enc}(pk, r_n, r_{n-1}), \mathsf{Enc}(pk, r_1, r_n)\}$$
$$\approx_c$$
$$\{pk, \mathsf{Enc}(pk, 0, r_1), ..., \mathsf{Enc}(pk, 0, r_n)\}$$

Similar to (key) circular security [CL01, BRS03, BHHO08]

RCIRC One-wayness

Definition

A cryptosystem is RCIRC-one-way if the map

$$(r_1, \ldots, r_n) \mapsto (\mathsf{Enc}(pk, r_2, r_1), \ldots, \mathsf{Enc}(pk, r_1, \ldots, r_n))$$

is one-way

RCIRC One-wayness

Definition

A cryptosystem is RCIRC-one-way if the map

$$(r_1, \ldots, r_n) \mapsto (\mathsf{Enc}(pk, r_2, r_1), \ldots, \mathsf{Enc}(pk, r_1, \ldots, r_n))$$

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

Thanks!

References I

Benny Applebaum, David Cash, Chris Peikert, and 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.

Mihir Bellare, Alexandra Boldyreva, and Adam O'Neill.
Deterministic and Efficiently Searchable Encryption.
In *CRYPTO '07*, volume 4622 of *Lecture Notes in Computer Science*, pages 535–552. Springer Berlin / Heidelberg, 2007.

References II

Eleanor Birrell, Kai-Min Chung, Rafael Pass, and Sidharth Telang.
Randomness-Dependent Message Security.
In Amit Sahai, editor, *Theory of Cryptography*, volume 7785 of *Lecture Notes in Computer Science*, pages 700–720. Springer Berlin Heidelberg, 2013.

Alexandra Boldyreva, Serge Fehr, and Adam O'Neill.
On Notions of Security for Deterministic Encryption, and Efficient Constructions without Random Oracles.
In David Wagner, editor, *CRYPTO '08*, volume 5157 of *Lecture Notes in Computer Science*, pages 335–359. Springer, 2008.

References III

Dan Boneh, Shai Halevi, Michael Hamburg, and Rafail Ostrovsky.
Circular-secure encryption from Decision Diffie-Hellman.
In *CRYPTO '08*, volume 5157 of *Lecture Notes in Computer Science*, pages 108–125, 2008.

Mark Braverman, Avinatan Hassidim, and Yael T. Kalai.
Leaky Pseudo-Entropy Functions.
In *ICS'11*, pages 353–366, 2011.

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.

References IV

Mihir Bellare, Dennis Hofheinz, and Scott Yilek.
Possibility and Impossibility Results for Encryption and Commitment Secure under Selective Opening.
In *Eurocrypt '09*. Springer, 2009.

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.

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.

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.
In *FOCS '01*, page 126, Washington, DC, USA, 2001. IEEE Computer Society.

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.

References VI

Brett Hemenway and Rafail Ostrovsky.
Building Injective Trapdoor Functions From Oblivious Transfer.
ECCC TR10-127, 2010.

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.
In *Eurocrypt '08*, volume 4965 of *Lecture Notes in Computer Science*, pages 108–126, 2008.

References VII

Gillat Kol and Moni Naor.
Cryptography and Game Theory: Designing Protocols for Exchanging Information.
In *TCC '08*, pages 320–339. Springer Berlin / Heidelberg, 2008.

Eike Kiltz, Adam O'Neill, and Adam Smith.
Instantiability of RSA-OAEP under chosen-plaintext attack.
In *Proceedings of the 30th annual conference on Advances in cryptology*, CRYPTO'10, pages 295–313, Berlin, Heidelberg, 2010. Springer-Verlag.

Petros Mol and Scott Yilek.
Chosen-Ciphertext Security from Slightly Lossy Trapdoor Functions.
Cryptology ePrint Archive, Report 2009/524, 2009.

References VIII

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.

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.

Alon Rosen and Gil Segev.
Efficient Lossy Trapdoor Functions Based on the Composite Residuosity Assumption.
http://eprint.iacr.org/2008/134, 2008.

References IX

Alon Rosen and Gil Segev.
Chosen-Ciphertext Security via Correlated Products.
In *TCC '09*, pages 419–436, Berlin, Heidelberg, 2009.
Springer-Verlag.