Introduction to Cryptology

3.3 - CPA Security and Pseudorandom Permutations

Federico Pintore

Mathematical Institute, University of Oxford (UK)

Michaelmas term 2020

More security definitions are needed...

Both perfect and computational indistinguishability focus on an adversary $\mathcal{A}$ who knows one ciphertext.

What are the security definitions for more powerful adversaries?

More security definitions are needed...

For example, the adversary $\mathcal{A}$ could be challenged on two lists of messages instead of two messages m_0,m_1.

More security definitions are needed...

For example, the adversary $\mathcal{A}$ could be challenged on two lists of messages instead of two messages m_0,m_1.

- If Enc is deterministic, $\mathcal{A}$ trivially wins the game (two equal messages only in one vector).
- Deterministic encryption schemes are not secure under the multiple encryptions threat model.

More security definitions are needed...

For example, the adversary $\mathcal{A}$ could be challenged on two lists of messages instead of two messages m_0,m_1.

- If Enc is deterministic, $\mathcal{A}$ trivially wins the game (two equal messages only in one vector).
- Deterministic encryption schemes are not secure under the multiple encryptions threat model.

What about the Chosen Plaintext Attack (CPA) and the Chosen Ciphertext Attack (CCA) threat models?

CPA-Security

CPA Indistinguishability Experiment $\text{PrivK}^{\text{cpa}}_{\mathcal{A},E}$

Challenger Ch		Adversary $\mathcal{A}$
$k \leftarrow \text{KeyGen(n)}$		
		Queries to $\text{Enc}(k, \cdot)$
	$\xleftarrow{m_0, m_1, \lvert m_0\rvert = \lvert m_1\rvert}$	
$b \leftarrow_{\$} \{0,1\}$		
	$\xrightarrow{c = \text{Enc}(k, m_b)}$	
		Queries to $\text{Enc}(k, \cdot)$
		Outputs their guess b'

CPA-Security

CPA Indistinguishability Experiment $\mathrm{PrivK}^{\mathrm{cpa}}_{\mathcal{A},E}$

Challenger Ch		Adversary $\mathcal{A}$
$k \leftarrow \mathrm{KeyGen}(\mathrm{n})$		
		Queries to $\mathrm{Enc}(k,\cdot)$
	$\xleftarrow{m_0,m_1,\lvert m_0\rvert=\lvert m_1\rvert}$	
$b \leftarrow_{\$} \{0,1\}$		
	$\xrightarrow{c=\mathrm{Enc}(k,m_b)}$	
		Queries to $\mathrm{Enc}(k,\cdot)$
		Outputs their guess b'

Definition

An encryption scheme E is CPA-secure if, for every PPT adversary $\mathcal{A}$, it holds:

$$\mathrm{Adv}^{\mathrm{cpa}}_{\mathcal{A},E}(n) = \Pr(\mathrm{PrivK}^{\mathrm{cpa}}_{\mathcal{A},E}(n) = 1) \leq 1/2 + \mathrm{negl}(n)\,,$$

where $\mathrm{PrivK}^{\mathrm{cpa}}_{\mathcal{A},E}(n) = 1$ if $b' = b$, and 0 otherwise.

CPA-security for multiple encryptions

- Ch runs $k \leftarrow \mathrm{KeyGen}(n)$ and uniformly samples $b \in \{0,1\}$;
- $\mathcal{A}$ has access to the oracle $\mathrm{LR}_{k,b}$: on a query $(m_{0,i}, m_{1,i})$, with $i = 1, 2, \ldots,$ $\mathrm{Enc}(k, m_{b,i})$ is returned;
- $\mathcal{A}$ submits their guess $b' \in \{0,1\}$.

CPA-security for multiple encryptions

- Ch runs $k \leftarrow \mathrm{KeyGen}(n)$ and uniformly samples $b \in \{0,1\}$;
- $\mathcal{A}$ has access to the oracle $\mathrm{LR}_{k,b}$: on a query $(m_{0,i}, m_{1,i})$, with $i = 1, 2, \ldots,$ $\mathrm{Enc}(k, m_{b,i})$ is returned;
- $\mathcal{A}$ submits their guess $b' \in \{0,1\}$.

Theorem

If an encryption scheme E is CPA-secure, it is CPA-secure for multiple encryptions.

CPA-security for multiple encryptions

- Ch runs $k \leftarrow \mathrm{KeyGen}(n)$ and uniformly samples $b \in \{0,1\}$;
- $\mathcal{A}$ has access to the oracle $\mathrm{LR}_{k,b}$: on a query $(m_{0,i}, m_{1,i})$, with $i = 1, 2, \ldots,$ $\mathrm{Enc}(k, m_{b,i})$ is returned;
- $\mathcal{A}$ submits their guess $b' \in \{0,1\}$.

Theorem

If an encryption scheme E is CPA-secure, it is CPA-secure for multiple encryptions.

Enc cannot be deterministic ($\mathcal{A}$ can query on (m, m) and (m', m))

CCA-Security

CCA Indistinguishability Experiment $\mathrm{PrivK}^{\mathrm{cca}}_{\mathcal{A},E}$

Challenger Ch		Adversary $\mathcal{A}$
$k \leftarrow \mathrm{KeyGen(n)}$		
		Queries to $\mathrm{Enc}(k,\cdot)$ and $\mathrm{Dec}(k,\cdot)$
	$\xleftarrow{m_0,m_1,\lvert m_0\rvert=\lvert m_1\rvert}$	
$b \leftarrow_{\$} \{0,1\}$		
	$\xrightarrow{c=\mathrm{Enc}(k,m_b)}$	
		Queries to $\mathrm{Enc}(k,\cdot)$ and $\mathrm{Dec}(k,\cdot)$
		Outputs their guess b'

Definition

An encryption scheme E is CCA-secure if for, every PPT $\mathcal{A}$, it holds $\mathrm{Adv}^{\mathrm{cca}}_{\mathcal{A},E}(n) = \Pr(\mathrm{PrivK}^{\mathrm{cca}}_{\mathcal{A},E}(n) = 1) \leq 1/2 + \mathrm{negl}(n)$.

CPA-secure encryption from Pseudorandom Permutations

Pseudorandom Functions

Generalisation to functions of the notion of pseudorandomness, i.e. *random-looking* functions are considered.

Pseudorandom Functions

Generalisation to functions of the notion of pseudorandomness, i.e. *random-looking* functions are considered.

The focus is on keyed functions, i.e. functions of the form

$$F : I \to O$$

where $I \subset \{0,1\}^* \times \{0,1\}^*$ and $O \subset \{0,1\}^*$.

Pseudorandom Functions

Generalisation to functions of the notion of pseudorandomness, i.e. *random-looking* functions are considered.

The focus is on keyed functions, i.e. functions of the form

$$F : I \to O$$

where $I \subset \{0,1\}^* \times \{0,1\}^*$ and $O \subset \{0,1\}^*$.

- given $k \in \{0,1\}^*$ and $I_k = \{x | (k,x) \in I\}$, $F_k : I_k \to O_k$ defined by $x \mapsto F(k,x)$ is a single-input function.
- we require the existence of $\ell_{key}(n), \ell_{in}(n), \ell_{out}(n) \in \mathbb{Z}[n]$ s.t., for any $k \in \{0,1\}^{\ell_{key}(n)}$, $I_k = \{0,1\}^{\ell_{in}(n)}$ and $O_k = \{0,1\}^{\ell_{out}(n)}$.
- F is length-preserving if $\ell_{key}(n) = \ell_{in}(n) = \ell_{out}(n)$.

Pseudorandom Functions

Definition

$F : I \to O$ is a pseudorandom function (PRF) if it is length-preserving, efficiently computable and, for every PPT distinguisher D, there exists a negligible function $\mathrm{negl}(n)$ *s.t.*

$$\mathrm{Adv}^{PRF}_{F,\mathrm{D}}(n) = |\Pr(\mathrm{D}^{f()}(n) = 1) - \Pr(\mathrm{D}^{F_k()}(n) = 1)| \leq \mathrm{negl}(n)$$

where the first probability is taken over uniform choice of $f \in Func_n$ and the randomness of D, while the second one over uniform choice of $k \in \{0,1\}^n$ and the randomness of D.

- $Func_n$ is the set of all functions from $\{0,1\}^n$ to $\{0,1\}^n$.
- $\mathrm{D}^{f()}$ means that D has access to an evaluating oracle for f.

Pseudorandom Permutations

F is a pseudorandom permutation (PRP) if:

- $\ell_{in}(n) = \ell_{out}(n)$;
- F_k is a bijection for every $k \in \{0,1\}^{\ell_{key}(n)}$;
- F_k and F_k^{-1} are efficiently computable for every $k \in \{0,1\}^{\ell_{key}(n)}$;
- for a uniform k, F_k is indistinguishable from a uniform permutation of $\{0,1\}^{\ell_{in}(n)}$.

Pseudorandom Permutations

F is a pseudorandom permutation (PRP) if:

- $\ell_{in}(n) = \ell_{out}(n)$;
- F_k is a bijection for every $k \in \{0,1\}^{\ell_{key}(n)}$;
- F_k and F_k^{-1} are efficiently computable for every $k \in \{0,1\}^{\ell_{key}(n)}$;
- for a uniform k, F_k is indistinguishable from a uniform permutation of $\{0,1\}^{\ell_{in}(n)}$.

F is a strong pseudorandom permutation if it is a PRP and the distinguisher D is given access to both f and f^{-1}, or F_k and F_k^{-1}.

Encryption using PRPs

Let F be a PRP. We define the following symmetric-key encryption scheme $E = (\text{KeyGen}, \text{Enc}, \text{Dec})$:

- $k \leftarrow \text{KeyGen}(n)$: on input n, it outputs a uniformly random key $k \in \{0,1\}^{\ell_k(n)}$.
- $c \leftarrow \text{Enc}(k, m)$: given a key k and a message $m \in \{0,1\}^{\ell_{in}(n)}$, it uniformly samples $r \leftarrow \{0,1\}^{\ell_{in}(n)}$, and outputs

$$(c_0, c_1) \leftarrow (r, F_k(r) \oplus m).$$

- $m \leftarrow \text{Dec}(k, (c_0, c_1))$: on input a key k and a ciphertext $c = (c_0, c_1)$, it returns

$$m \leftarrow (F_k(c_0) \oplus c_1).$$

Encryption using PRP

Theorem

If F is a PRP with $\ell_{in}(n) \geq n$, then the encryption scheme E is CPA-secure.

Proof (by reduction)

Let $\mathcal{A}$ a PPT adversary against the CPA-security of E. $\mathcal{A}$ can make a polynomial number $q(n)$ of encryption queries.

We use $\mathcal{A}$ as a subroutine for a distinguisher D for the PRP.

On a query $m \in \{0,1\}^n$, D queries the oracle on a uniform $r \in \{0,1\}^{\ell_{in}(n)}$, receiving the image y. They reply with $(r, y \oplus m)$.

If $\mathcal{A}$ wins the game, D outputs 1 (0 otherwise).

Encryption using PRP

$$\Pr(\mathrm{D}^{F_k()}(n) = 1) = \Pr(\mathrm{PrivK}^{\mathrm{cpa}}_{\mathcal{A},E}(n) = 1)$$

If E' denotes a variant of E with a uniform permutation f instead of F_k, then we have:

$$\Pr(\mathrm{D}^{f()}(n) = 1) = \Pr(\mathrm{PrivK}^{\mathrm{cpa}}_{\mathcal{A},E'}(n) = 1)$$

Since F is a PRP we deduce

$$\begin{aligned}
&\left|\Pr(\mathrm{D}^{F_k()}(n) = 1) - \Pr(\mathrm{D}^{f()}(n) = 1)\right| = \\
&\left|\Pr(\mathrm{PrivK}^{\mathrm{cpa}}_{\mathcal{A},E}(n) = 1) - \Pr(\mathrm{PrivK}^{\mathrm{cpa}}_{\mathcal{A},E'}(n) = 1)\right| \leq \mathrm{negl}(n)
\end{aligned}$$

Encryption using PRP

For the case when $\mathcal{A}$ is interacting with E', let r_c be the first component of the challenge ciphertext.

- case 1: r_c did not appear in any of the answers to the encryption queries. Then $f(r_c)$ is a uniform string and the probability to win the game is $1/2$ (OTP is perfectly secret)
- case 2: r_c appeared in at least one of the queries. The probability of this event is at most $q(n)/2^{\ell_{in}(n)}$.

Thus

$$\Pr(\mathrm{PrivK}^{\mathrm{cpa}}_{\mathcal{A},E'}(n) = 1) \leq 1/2 + q(n)/2^{\ell_{in}(n)}$$

and therefore

$$\Pr(\mathrm{PrivK}^{\mathrm{cpa}}_{\mathcal{A},E}(n) = 1) \leq 1/2 + q(n)/2^{\ell_{in}(n)} n + \mathrm{negl}(n)\,.$$

Notes

- The product of a positive polynomial in $\mathbb{Z}[n]$ and a negligible function is a negligible function.
- The sum of two negligible functions is a negligible function.

Further Reading I

Nadhem J AlFardan, Daniel J Bernstein, Kenneth G Paterson, Bertram Poettering, and Jacob CN Schuldt.
On the security of RC4 in TLS.
In 22nd USENIX Security Symposium (USENIX Security 13), pages 305–320, 2013.

Boaz Barak and Shai Halevi.
A model and architecture for pseudo-random generation with applications to/dev/random.
In Proceedings of the 12th ACM conference on Computer and communications security, pages 203–212. ACM, 2005.

Daniel J Bernstein.
The Salsa20 Family of Stream Ciphers.
In New stream cipher designs, pages 84–97. Springer, 2008.

Further Reading II


Lenore Blum, Manuel Blum, and Mike Shub.
A simple unpredictable pseudo-random number generator.
SIAM Journal on computing, 15(2):364–383, 1986.


Christian Cachin.
Entropy measures and unconditional security in cryptography.
PhD thesis, ETH Zurich, 1997.


Scott Fluhrer, Itsik Mantin, and Adi Shamir.
Weaknesses in the key scheduling algorithm of RC4.
In Selected areas in cryptography, pages 1–24. Springer, 2001.

Further Reading III

Christina Garman, Kenneth G Paterson, and Thyla Van der Merwe.
Attacks only get better: Password recovery attacks against RC4 in TLS.
In 24th USENIX Security Symposium (USENIX Security 15), pages 113–128, 2015.

Itsik Mantin and Adi Shamir.
A practical attack on broadcast RC4.
In Fast Software Encryption, pages 152–164. Springer, 2002.