Introduction to Modern Cryptography

Michele Ciampi

(Slides courtesy of Prof. Jonathan Katz)

Lecture 8
CPA-secure Encryption from PRF
CPA-security (recall)

Experiment $\text{PrivK}_{A,\Pi}^{\text{cpa}}(n)$

Fix $\Pi, A$. Define a randomized experiment $\text{PrivK}_{A,\Pi}^{\text{cpa}}(n)$:

- $k \leftarrow \text{Gen}(1^n)$
- $A(1^n)$ interacts with an encryption oracle $\text{Enc}_k(\cdot)$, and then outputs $m_0, m_1$ of the same length
- $b \leftarrow \{0, 1\}$, $c \leftarrow \text{Enc}_k(m_b)$, give $c$ to $A$
- $A$ can continue to interact with $\text{Enc}_k(\cdot)$
- $A$ outputs $b'$; $A$ succeeds if $b = b'$, and the experiment evaluates to $1$ in this case
Security Against Chosen-plaintext Attacks

\( \Pi \) is secure against chosen-plaintext attacks (CPA-secure) if for all PPT attackers \( A \), there is a negligible function \( \epsilon \) such that

\[
\Pr[\text{PrivK}_{A, \Pi}^{\text{cpa}}(n) = 1] \leq \frac{1}{2} + \epsilon(n)
\]
EAV-secure Encryption (POTP) (recall)

- Solves OTP limitation 1 (key as long as the message)
- Not solve OTP limitation 2 (key used only once)
- EAV-secure, but **not** CPA-secure
CPA-secure Encryption
CPA-secure Encryption

- Not solve OTP limitation 1 (key as long as the message)
- Solves OTP limitation 2 (key used only once)
- \( \implies \) CPA-secure \( \implies \) EAV-secure
CPA-secure Encryption (Formal)

### Encryption Scheme $\Pi$

Let $F$ be a length-preserving keyed function.

- **Gen**($1^n$): choose a uniform key $k \in \{0, 1\}^n$
- **Enc$_k$**($m$), where $|m| = |k| = n$:
  - Choose uniform $r \in \{0, 1\}^n$ (nonce/initialization vector)
  - Output ciphertext $\langle r, F_k(r) \oplus m \rangle$
- **Dec$_k$**($c_1$, $c_2$): output $c_2 \oplus F_k(c_1)$
- Correctness is immediate

- The key is as long as the message...
- ...but the same key can be used to securely encrypt multiple messages
<table>
<thead>
<tr>
<th>Theorem</th>
</tr>
</thead>
<tbody>
<tr>
<td>If $F$ is a pseudorandom function, then $\Pi$ is CPA-secure</td>
</tr>
</tbody>
</table>

$\implies$ proof by reduction
Proof by Reduction

Reduction $A'$

Instance $x$ of problem $X$

Instance of scheme II

“Break”

Solution to $x$
Proof by Reduction

High level

- Attacker $A$ attacks $\Pi$ (as was defined)
- Design distinguisher $D$ that uses $A$ as a subroutine to attack the PRF $F$
  - i.e. $D$ tries to distinguish $F$ from a random function (RF)
- $D$ simulates to $A$ the steps in the $\text{PrivK}_{A,\Pi}^{\text{cpa}}(n)$ experiment for $F$ and for a RF
- Relate the success $\Pr$ of $A$ to the success $\Pr$ of $D$
- If $A$ succeeds $\implies$ $D$ succeeds $\implies$ $F \neq \text{PRF}$
- contradicts $F$ PRF $\implies$ $A$ can not succeed $\implies$ $\Pi$ CPA-secure
The Reduction
The Reduction
The Reduction

PR/random
The Reduction

\[ A \] interacts with an encryption oracle simulated by \( D \)
The Reduction

$A$ interacts with an encryption oracle simulated by $D$
A interacts with an encryption oracle simulated by $D$
The Reduction

$A$ interacts with an encryption oracle simulated by $D$
The Reduction

\[ A \text{ interacts with an encryption oracle simulated by } D \]
The Reduction

\[ A \text{ interacts with an encryption oracle simulated by } D \]
The Reduction

A outputs two messages $m_0, m_1$
The Reduction

\[ D \text{ simulates the encryption oracle for } m_b \]
The Reduction

\[ D \text{ simulates the encryption oracle for } m_b \]
The Reduction

\[ D \text{ simulates the encryption oracle for } m_b \]
The Reduction

\( D \) simulates the encryption oracle for \( m_b \)
The Reduction

$D$ simulates the encryption oracle for $m_b$
The Reduction

\[ A \text{ outputs its result } b' \]
The Reduction

\[ D \text{ outputs 1 if } b = b' \]
## CPA-security Proof

### High level

- Replace $F_k$ with a random function $f$ and denote the modified scheme $\tilde{\Pi}$
- Whenever $f$ is evaluated on a new input, the result is uniform and independent of everything else
- Prove security assuming $f$ is never evaluated on the same input twice
- Argue that $f$ is never evaluated on the same input except with negligible probability
The Distinguisher $D$ Using $A$ as a Subroutine

$D$ simulates to $A$ the steps in the $\text{PrivK}_{A,\Pi}^{\text{cpa}}(n)$ and $\text{PrivK}_{A,\Pi}^{\text{cpa}}(n)$ experiments

World 0: $D$ simulates $\text{PrivK}_{A,\Pi}^{\text{cpa}}(n)$

- $D$ is given access to a RF $f \in \mathcal{F}_n$
- As if $A$ is interacting with the OTP

World 1: $D$ simulates $\text{PrivK}_{A,\Pi}^{\text{cpa}}(n)$

- $D$ is given access to the PRF $F_k$
- As if $A$ is interacting with $\Pi$
World 0: $D$ with a Truly Random Function

$D^f$ simulates $\text{PrivK}_{A,\tilde{\Pi}}^{\text{cpa}}(n)$ for $A(1^n)$ (truly random $f$)

- $A$ interacts with $O$ for $i = 1, 2, \ldots, q(n)$: choose $m_i$
- Simulation:
  1. $D$ generates $r_i \leftarrow \{0, 1\}^n$
  2. $D$ queries $f$ on $r_i$: gets $f(r_i)$
  3. $D$ computes $c_i = m_i \oplus f(r_i)$; sends $(r_i, c_i)$ to $A$
- $A$ outputs $(m_0, m_1)$
- Simulation:
  1. $D$ generates $b \leftarrow \{0, 1\}$
  2. $D$ generates $r_c \leftarrow \{0, 1\}^n$; gets $f(r_c)$
  3. $D$ computes $c = m_b \oplus f(r_c)$; sends $(r_c, c)$ to $A$
- $A$ continues to interact with $O$
- $b' \leftarrow A(c)$
- If $b = b'$ then $D(y) = 1$
World 0: \( D \) with a Truly Random Function

\( D \) simulates \( \text{PrivK}_{A,\Pi}^{\text{cpa}} \) for \( A \)

Let \( r_c \) be the random value used in generating the challenge ciphertext \( c \):

\[
c = \tilde{E}_k(m_b) = m_b \oplus f(r_c)
\]

Two cases

1. \( r_c \) was used in at least one previous query of \( A \) (event Repeat)
2. \( r_c \) was used in none of the previous queries of \( A \)
World 0: $D$ with a Truly Random Function

Case 1: $r_c$ used before (Repeat)

- $A$ has a pair $(m', c')$ s.t. $c' = m' \oplus f(r_c)$
- $A$ computes $f(r_c) = m' \oplus c'$
- $A$ computes $m_b = c \oplus f(r_c)$
- $A$ succeeds with

$$\Pr[\text{PrivK}_{A, \pi}^{\text{cpa}}(n) = 1] = 1$$
**Case 2: \( r_c \) not used before (\( \neg \text{Repeat} \))**

- \( r_c \) random \( \implies \) \( f(r_c) \) random
- \( A \) learns nothing from its interaction with \( f \)
- \( \implies \) \( \widetilde{E}_k(m_b) = m_b \oplus f(r_c) \) is equivalent to OTP
- \( A \) succeeds with

\[
\Pr[\text{PrivK}_{A,\Pi}^{\text{cpa}}(n) = 1] = \Pr[\text{PrivK}_{A,\text{OTP}} = 1] = \frac{1}{2}
\]
World 0: \( D \) with a Truly Random Function

**Pr[Repeat] and Pr[\( \neg \)Repeat]**

- \( A \) is PPT \( \implies \) \( A \) can make at most \( q(n) \) polynomial number of queries

- As \( r_c \) is chosen uniformly, it follows that

\[
\Pr[\text{Repeat}] = \frac{q(n)}{2^n}
\]

\[
\Pr[\neg \text{Repeat}] = 1 - \frac{q(n)}{2^n} = 1 - \text{negl} \approx 1
\]
World 0: $D$ with a Truly Random Function

$$\text{Pr}[\text{PrivK}_{A,\tilde{\Pi}}^{\text{cpa}}(n) = 1]$$

\[
\begin{align*}
\text{Pr}[\text{PrivK}_{A,\tilde{\Pi}}^{\text{cpa}}(n) = 1] & \\
\overset{LTP}{=} & \text{Pr}[(\text{PrivK}_{A,\tilde{\Pi}}^{\text{cpa}}(n) = 1) \land \text{Repeat}] + \\
& \text{Pr}[(\text{PrivK}_{A,\tilde{\Pi}}^{\text{cpa}}(n) = 1) \land \neg\text{Repeat}] \\
\overset{\text{Cond.P.}}{=} & \text{Pr}[(\text{PrivK}_{A,\tilde{\Pi}}^{\text{cpa}}(n) = 1)|\text{Repeat}] \text{ Pr}[\text{Repeat}] + \\
& \text{Pr}[(\text{PrivK}_{A,\tilde{\Pi}}^{\text{cpa}}(n) = 1)|\neg\text{Repeat}] \text{ Pr}[\neg\text{Repeat}] \\
\leq & \text{Pr}[\text{Repeat}] + \text{Pr}[(\text{PrivK}_{A,\tilde{\Pi}}^{\text{cpa}}(n) = 1)|\neg\text{Repeat}] \\
= & \frac{q(n)}{2^n} + \frac{1}{2}
\end{align*}
\]
World 1: $D$ with a Pseudorandom Function

$D^{F_k}$ simulates $\text{PrivK}_{A,\Pi}^{\text{cpa}}(n)$ for $A(1^n)$ (pseudorandom $F_k$)

- $A$ interacts with $\mathcal{O}$ for $i = 1, 2, \ldots, q(n)$: choose $m_i$
- Simulation:
  1. $D$ generates $r_i \leftarrow \{0, 1\}^n$
  2. $D$ queries $F_k$ on $r_i$: gets $F_k(r_i)$
  3. $D$ computes $c_i = m_i \oplus F_k(r_i)$; sends $(r_i, c_i)$ to $A$
- $A$ outputs $(m_0, m_1)$
- Simulation:
  1. $D$ generates $b \leftarrow \{0, 1\}$
  2. $D$ generates $r_c \leftarrow \{0, 1\}^n$; gets $F_k(r_c)$
  3. $D$ computes $c = m_b \oplus F_k(r_c)$; sends $(r_c, c)$ to $A$
- $A$ continues to interact with $\mathcal{O}$
- $b' \leftarrow A(c)$
- If $b = b'$ then $D(y) = 1$
World 1: $D$ with a Pseudorandom Function

$D$ simulates $\text{PrivK}_{A,\Pi}^{\text{cpa}}$ for $A$

The $\text{Pr}$ with which $A$ succeeds in this case is

$$\Pr[\text{PrivK}_{A,\Pi}^{\text{cpa}}(n) = 1]$$

Note

This is the $\text{Pr}$ that we want to bound!
Proof.

By the assumption that $F$ is a PRF $\exists \epsilon(n) = \text{negl}$:

$$|\Pr_{k \leftarrow \{0,1\}^n}[D^F_k(\cdot) = 1] - \Pr_{f \leftarrow F_n}[D^f(\cdot) = 1]| \leq \epsilon(n)$$

By the simulation of $\text{PrivK}_{A,\Pi}^{\text{cpa}}(n)$ by $D^f$:

$$\Pr_{f \leftarrow F_n}[D^f(\cdot) = 1] = \Pr[\text{PrivK}_{A,\Pi}^{\text{cpa}}(n) = 1] = \frac{q(n)}{2^n} + \frac{1}{2}$$

By the simulation of $\text{PrivK}_{A,\Pi}^{\text{cpa}}(n)$ by $D^{F_k}$:

$$\Pr_{k \leftarrow \{0,1\}^n}[D^{F_k}(\cdot) = 1] = \Pr[\text{PrivK}_{A,\Pi}^{\text{cpa}}(n) = 1]$$
Proof.

Therefore

\[
\Pr[\text{PrivK}_{A,\Pi}^{\text{cpa}}(n) = 1] \leq \frac{1}{2} + \frac{q(n)}{2^n} + \epsilon(n)
\]

\[= \frac{1}{2} + \text{negl}(n)\]

\[\implies \Pi \text{ is CPA-secure.} \]
Real-world Security?

- What happens if a nonce $r$ is ever reused?
- What happens to the bound if the nonce is chosen non-uniformly?
Attacks?

Nonce $r$ not used correctly

- If $r$ repeats, security fails
  - Exactly analogous to multiple encryptions using the (pseudo)one-time pad scheme
- When $r$ is a uniform, $n$-bit string, the probability of a repeat is **negligible**
- If $r$ is too short, or is chosen from another distribution, repeats may happen
  - May make scheme insecure
**Attacks?**

<table>
<thead>
<tr>
<th>$F$ not used correctly</th>
</tr>
</thead>
<tbody>
<tr>
<td>▶ (Function of) plaintext directly leaked in ciphertext</td>
</tr>
<tr>
<td>e.g. $\langle m, F_k(m) \rangle$</td>
</tr>
<tr>
<td>▶ $F$ not used with a random, unknown key</td>
</tr>
<tr>
<td>e.g. $\text{Enc}_k(m) = \langle r, F_r(m) \rangle$</td>
</tr>
</tbody>
</table>
## CPA-secure Encryption Summary

### Practical CPA-secure Scheme

We have shown a CPA-secure encryption scheme based on any PRF:

\[
\text{Enc}_k(m) = \langle r, F_k(r) \oplus m \rangle
\]

### Drawbacks?

- A 1-block plaintext results in a 2-block ciphertext
- Only defined for encryption of \(n\)-bit messages
- (Both key and message of length \(n\) i.e. OTP limitation 1)
- Solution: Modes of Operation (next lecture!)
End

Reference: Section 3.5.2