Introduction to Modern Cryptography

Michele Ciampi

(Slides courtesy of Prof. Jonathan Katz)

Lecture 7, Part 1
Security Against Chosen-Plaintext Attacks (CPA)
Pseudo One-time Pad (POTP) (previous lecture)
Security of POTP (previous lecture)

Theorem

*If* $G$ *is a pseudorandom generator, then the pseudo one-time pad* $\Pi$ *is EAV-secure (i.e. computationally indistinguishable)*
So far

- Proof that the pseudo OTP is secure...
- ...with some caveats
  - Assuming $G$ is a pseudorandom generator
  - Relative to our definition
- The only ways the scheme can be broken are:
  - If a weakness is found in $G$
  - If the definition isn’t sufficiently strong (this lecture!)
Have we gained anything?

▶ Yes! The POTP has a key shorter than the message
  ▶ $n$ bits vs. $p(n)$ bits
  ▶ $\implies$ Solved one of the limitations of the OTP

▶ The fact that the parties internally generate a $p(n)$-bit temporary string to encrypt/decrypt is irrelevant
▶ The $n$-bit key is what the parties share in advance
▶ Parties do not store the $p(n)$-bit temporary value
Stepping Back

- Perfect secrecy has two limitations:
  1. Key as long as the message
  2. Key can only be used once
- We have seen how to circumvent the first (cf. POTP)
- Does the POTP have the second limitation?
- How can we circumvent the second?
But first...

- Develop an appropriate **security definition**
- Recall that security definitions have two parts
  - **Security goal**: what we want to prevent the attacker from doing
  - **Threat model**: the abilities the attacker is assumed to have
- Keep the security goal the same
  - as in indistinguishable encryption
- Strengthen the threat model
Single-message Secrecy (SMS)

SMS captures perfect secrecy and indistinguishability

Parties share $k$; single $m$ encrypted under $k$

- **Threat model:** attacker observes single ciphertext $c$
- **Security goal:** given $c$ attacker can not derive any information on $m$
Multiple-message Secrecy (MMS)

MMS strengthens the threat model of SMS

Parties share $k$; multiple $m_i$ encrypted under $k$

- **Threat model**: attacker observes multiple ciphertexts $c_i$
- **Security goal**: given $c_i$, attacker cannot derive any information on any $m_i$
Fix $\Pi, A$. Define a randomized experiment $\text{PrivK}^\text{mult}_{A, \Pi}(n)$:

1. $A(1^n)$ outputs two vectors $(m_{0,1} \ldots m_{0,t})$ and $(m_{1,1} \ldots m_{1,t})$
   - Require that $\forall i : |m_{0,i}| = |m_{1,i}|$

2. $k \leftarrow \text{Gen}(1^n), b \leftarrow \{0, 1\}, \forall i : c_i = \text{Enc}_k(m_{b,i})$

3. $b' = A(c_1 \ldots c_t)$; $A$ succeeds if $b = b'$, and experiment evaluates to 1 in this case
A Formal Definition

Multiple-message Indistinguishability

\( \Pi \) is multiple-message indistinguishable if for all PPT attackers \( A \), there is a negligible function \( \epsilon \) such that

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

Claim

*POTP* is not multiple-message indistinguishable

Attack

\( A \) outputs \((m_{0,0}, m_{0,1})\) and \((m_{1,0}, m_{1,1})\) s.t.

\[
m_{0,0} = m_{0,1} = m_{1,0} \neq m_{1,1}
\]

If \(c_0 = c_1\) then \(A\) outputs \(b' = 0\); otherwise \(b' = 1\) i.e. \(A\) wins the \(\text{PrivK}_{A,\Pi}^{\text{mult}}(n)\) game with \(Pr = 1\)
Multiple-message Secrecy

Fact

No **deterministic** encryption scheme is multiple-message indistinguishable

- The issue is not an artefact of our definition
- It is a problem in practise if an attacker can tell when **the same message** is encrypted twice
- Need to consider **randomized** schemes!
Multiple-message Secrecy

- We shall not work with **multiple-message indistinguishability**
- Instead, define something stronger:
- Security against chosen-plaintext attacks (CPA-security)
- CPA is the minimal notion of security an encryption scheme should satisfy

If $\Pi$ is CPA-secure $\implies \Pi$ is multiple-message indist.
CPA-security

Threat model

- Attacker $A$ can request encryption of any $m_i$ of his choice
- i.e. $A$ is given access to an encryption oracle $E_k$
CPA-security

A submits \( m_1 \) \( \implies \) obtains \( c_1 = E_k(m_1) \)
CPA-security

\[
A \text{ submits } m_2 \implies \text{ obtains } c_2 = E_k(m_2)
\]
CPA-security

\[ A \text{ submits } m_i \implies \text{ obtains } c_i = E_k(m_i): i = 1, 2, \ldots \]
CPA-security

Threat model

- At some point an unknown (to A) message $m$ is encrypted
- Attacker observes $c = E_k(m)$
CPA-security

Security goal

- Given $c$ attacker can not derive any information on $m$
Is the threat model too strong?

- In practice, there are many ways an attacker can influence what gets encrypted
- Not clear how best to model this
- **Chosen-plaintext attacks encompass any such influence**
- In some cases an attacker may have complete control over what gets encrypted
Experiment $\text{PrivK}_{A,\Pi}^{\text{cpa}}(n)$

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

1. $k \leftarrow \text{Gen}(1^n)$
2. $A(1^n)$ interacts with an encryption oracle $\text{Enc}_k(\cdot)$, and then outputs $m_0, m_1$ of the same length
3. $b \leftarrow \{0, 1\}, c \leftarrow \text{Enc}_k(m_b)$, give $c$ to $A$
4. $A$ can continue to interact with $\text{Enc}_k(\cdot)$
5. $A$ 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

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

- CPA-security is stronger than multiple-message indistinguishability
- i.e. if $\Pi$ is CPA-secure then it is also multiple-message indistinguishable

Fact
No deterministic encryption scheme is multiple-message indistinguishable

Corollary
No deterministic encryption scheme can be CPA-secure
Attacker $A$ attacks deterministic scheme $\Pi = (\text{Gen, Enc, Dec})$

1. Query the encryption oracle on $m_0$ and $m_1$
2. Obtain $c_0 = \text{Enc}_k(m_0)$, $c_1 = \text{Enc}_k(m_1)$
3. Output $m_0, m_1$; get challenge $c$
4. If $c = c_0$ output 0; if $c = c_1$ output 1

$A$ succeeds with $Pr = 1$

Is CPA-security impossible to achieve?
End

References: Section 3.4 until Pag. 76