Public-key encryption
The details

Foundations of Cryptography
Computer Science Department
Wellesley College

Fall 2016

Table of contents

Introduction

Public-key encryption

CPA Secure

Multiple Encryptions
Public-key encryption scheme

**Definition 11.1.** A public-key encryption scheme is a tuple of probabilistic polynomial-time algorithms \( (\text{Gen}, \text{Enc}, \text{Dec}) \) such that:

1. The key generation algorithm \( \text{Gen} \) takes as input the security parameter \( 1^n \) and outputs a pair of keys \( (pk, sk) \) with \( \|pk\| = n = \|sk\| \). We refer to these as the public key and the private key respectively.

2. The encryption algorithm \( \text{Enc} \) takes as input a public key \( pk \) and a message \( m \) from some underlying plaintext space. It outputs a ciphertext \( c \); we write \( c = \text{Enc}_{pk}(m) \).

3. The decryption algorithm \( \text{Dec} \) takes as input a private key \( sk \) and a ciphertext \( c \), and outputs a message \( m \) or a special symbol \( \perp \) denoting failure. We assume WLOG that \( \text{Dec} \) is deterministic and write \( m = \text{Dec}_{sk}(c) \).

We require that, except with negligible probability,
\[
\text{Dec}_{sk}(\text{Enc}_{pk}(m)) = m
\]

---

The eavesdropping indistinguishability experiment

Given a public-key encryption scheme \( \Pi = (\text{Gen}, \text{Enc}, \text{Dec}) \) and an adversary \( A \) consider the following:

**The eavesdropping indistinguishability experiment** \( \text{PubK}^{\text{eav}}_{A, \Pi}(n) \):

1. \( \text{Gen}(1^n) \) is run to obtain keys \( (pk, sk) \).
2. Adversary \( A \) is given \( pk \), and outputs a pair of messages \( m_0, m_1 \) of the same length.
3. A random bit \( b \leftarrow \{0, 1\} \) is chosen, and then a ciphertext \( c = \text{Enc}_{pk}(m_b) \) is computed and given to \( A \). We call \( c \) the challenge ciphertext.
4. \( A \) outputs a bit \( b' \).
5. The output of the experiment is defined to be \( 1 \) if \( b' = b \), and \( 0 \) otherwise.

*Giving \( pk \) to \( A \) effectively gives \( A \) encryption oracle access for free.*
**Indistinguishable encryptions in the presence of an eavesdropper**

**Definition 11.2.** A public-key encryption scheme $\text{PubK}^{\text{eav}}_{\mathcal{A}, n}(n)$ has *indistinguishable encryptions in the presence of an eavesdropper* if for all probabilistic polynomial-time adversaries $\mathcal{A}$ there exists a negligible function $\text{negl}$ such that

$$\Pr[\text{PubK}^{\text{eav}}_{\mathcal{A}, n}(n) = 1] \leq \frac{1}{2} + \text{negl}(n).$$

**Storming the Bastille**

- Of course there is more than one form of attack ...
- And hence, more one definition of security.
- For example, we may wish our public-key encryption schemes for be secure against CPA or even CCA attacks.
Introduction
Public-key encryption
CPA Secure
Multiple Encryptions

More experiments and definitions

The CPA indistinguishability experiment PubK$^{'cpa}_{A, \Pi}(n)$:

1. Gen($1^n$) is run to obtain keys ($pk, sk$).
2. Adversary $A$ is given $pk$ as well as oracle access to $Enc_{pk}(\cdot)$. The adversary outputs a pair of messages $m_0, m_1$ of the same length.
3. A random bit $b \leftarrow \{0, 1\}$ is chosen, and then a ciphertext $c \leftarrow Enc_{pk}(m_b)$ is computed and given to $A$.
4. $A$ continues to have access to $Enc_{pk}(\cdot)$, and outputs a bit $b'$.
5. The output of the experiment is defined to be 1 if $b' = b$, and 0 otherwise.

Definition. A public-key encryption scheme PubK$^{'cpa}_{A, \Pi}(n)$ has indistinguishable encryptions under a chosen-plaintext attack if for all probabilistic polynomial-time adversaries $A$ there exists a negligible function $negl$ such that

$$Pr[PubK^{'cpa}_{A, \Pi}(n) = 1] \leq \frac{1}{2} + negl(n).$$

But you told me ...

Proposition 11.3 If a public-key encryption scheme PubK$^{'eav}_{A, \Pi}(n)$ has indistinguishable encryptions in the presence of an eavesdropper then $\Pi$ also has indistinguishable encryptions under a chosen plain-text attack.
Perfectly-secret public-key encryption

**Definition.** A public-key encryption scheme $\text{PubK}_{\mathcal{A},n}^{\text{eav}}$ is *perfectly secret* if for every PPT adversary $\mathcal{A}$

$$\Pr[\text{PubK}_{\mathcal{A},n}^{\text{eav}}(n) = 1] = \frac{1}{2}.$$ 

**Sad but true.** Unfortunately, perfectly-secret public-key encryption schemes are pipe dreams.*

*We leave this for an exercise.

More pipes: Insecurity of deterministic public-key encryption

**Remark.** For the same reason that no deterministic private-key encryption scheme can be CPA-secure, we have

**Theorem 11.7.** No deterministic public-key encryption scheme has indistinguishability in the presence of an eavesdropper.

**Warning!** This is not a mere "artifact" of our security definition. Deterministic public-key encryption schemes are vulnerable to practical attacks in realistic scenarios.
CPA security for multiple encryptions

The definition for indistinguishable encryptions under a chosen-plaintext can easily be extended to indistinguishable multiple encryptions in the same way that indistinguishability encryption in the presence of an eavesdropper was.

The text takes a somewhat simpler approach that can model attackers that can adaptively choose plaintexts to be encrypted, even after observing previous ciphertext.

The attacker has access to a "left-or-right" oracle $LR_{k,b}$ that, on input a pair of equal-length messages $m_0, m_1$, computes the ciphertext $c \leftarrow Enc_k(m_b)$ and returns $c$.*

*Here $b$ is a random bit chosen at the beginning of the experiment.

One more experiment

The LR-oracle experiment $\text{PubK}^{LR-\text{cpa}}_{\mathcal{A},\Pi}(n)$:

1. $\text{Gen}(1^n)$ is run to obtain keys $(pk, sk)$.
2. A uniform bit $b \leftarrow \{0, 1\}$ is chosen.
3. The adversary $\mathcal{A}$ is given input $pk$ and oracle access to $LR_{pk,b}(\cdot, \cdot)$.
4. Adversary $\mathcal{A}$ outputs a bit $b'$.
5. The output of the experiment is defined to be 1 if $b' = b$, and 0 otherwise. If $\text{PubK}^{LR-\text{cpa}}_{\mathcal{A},\Pi}(n) = 1$, we say that $\mathcal{A}$ succeeds.

Definition 11.5. A public-key encryption scheme $\text{PubK}^{\text{PR-\text{cpa}}}_{\mathcal{A},\Pi}(n)$ has indistinguishable multiple encryptions if for all probabilistic polynomial-time adversaries $\mathcal{A}$ there exists a negligible function $\text{negl}$ such that

$$\Pr[\text{PubK}^{\text{LP-\text{cpa}}}_{\mathcal{A},\Pi}(n) = 1] \leq \frac{1}{2} + \text{negl}(n).$$
**CPA-secure implies indistinguishable multiple encryptions**

**Theorem 11.6.** If a public-key encryption scheme $\Pi$ is CPA-secure then $\Pi$ has indistinguishable multiple encryptions.

**Remark.** Theorem 11.6 implies that a CPA-secure public-key encryption scheme for *fixed-length* messages implies a public-key encryption scheme for *arbitrary-length* messages satisfying the same notion of security.

**Remark.** For example, suppose $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ is an encryption scheme for a single-bit message. We construction $\Pi' = (\text{Gen}, \text{Enc}', \text{Dec'})$ for messages in $\{0, 1\}^*$

$$\text{Enc}'_{pk}(m) = \text{Enc}_{pk}(m_1), \ldots, \text{Enc}_{pk}(m_{\ell}),$$

where $m = m_1, \ldots, m_{\ell}$.

---

**Intuition behind Theorem 11.6**

**Theorem 11.6.** If a public-key encryption scheme $\Pi$ is CPA-secure then $\Pi$ has indistinguishable multiple encryptions.

**Proof.** Fix an arbitrary PPT adversary $\mathcal{A}$ and a CPA-secure public-key encryption scheme $\Pi$. Consider experiment PubK$^{\text{LR-cpa2}}_{\mathcal{A}, \Pi}(n)$ where $\mathcal{A}$ can only make two queries: $(m_{1,0}, m_{1,1})$ and $(m_{2,0}, m_{2,1})$. In the experiment $\mathcal{A}$ receives either the pair

$$(\text{Enc}_{pk}(m_{1,0}), \text{Enc}_{pk}(m_{2,0})) \text{ or } (\text{Enc}_{pk}(m_{1,1}), \text{Enc}_{pk}(m_{2,1})).$$

We write $\mathcal{A}(pk, \text{Enc}_{pk}(m_{1,0}), \text{Enc}_{pk}(m_{2,0}))$ in the first case and analogously for the second.

We show that there exists a negligible function $\text{negl}$ such that

$$| \Pr[\mathcal{A}(pk, \text{Enc}_{pk}(m_{1,0}), \text{Enc}_{pk}(m_{2,0})) = 1] - \Pr[\mathcal{A}(pk, \text{Enc}_{pk}(m_{1,1}), \text{Enc}_{pk}(m_{2,1})) = 1] | \leq \text{negl}(n).$$

*For simplicity we assume the adversary make only two calls to the LR oracle.*
To prove this, we will show that

Let $\tilde{C}_0$ denote the distribution of ciphertext pairs $(\text{Enc}_{pk}(m_1,0), \text{Enc}_{pk}(m_2,0))$, and $\tilde{C}_1$ the distribution of ciphertext pairs $(\text{Enc}_{pk}(m_1,1), \text{Enc}_{pk}(m_2,1))$. We show

1. CPA-security of $\Pi$ implies $\mathcal{A}$ cannot distinguish between when it is given a pair of ciphertexts distributed according to $\tilde{C}_0$, or a pair of ciphertexts $(\text{Enc}_{pk}(m_1,0), \text{Enc}_{pk}(m_2,1))$. Denote the distribution of these ciphertexts by $\tilde{C}_{01}$.

2. Similarly, CPA-security of $\Pi$ implies that $\mathcal{A}$ cannot distinguish between when it is given a pair of ciphertexts distributed according to $\tilde{C}_{01}$, or a pair distributed according to $\tilde{C}_1$.

We conclude that $\mathcal{A}$ cannot distinguish between distributions $\tilde{C}_0$ and $\tilde{C}_1$.

The long and the short of it

We must show that there is a negligible function $\text{negl}$ for which

\[
\left| \Pr[\mathcal{A}(pk, \text{Enc}_{pk}(m_1,0), \text{Enc}_{pk}(m_2,0)) = 1] - \Pr[\mathcal{A}(pk, \text{Enc}_{pk}(m_1,0), \text{Enc}_{pk}(m_2,1)) = 1] \right| \leq \text{negl}(n).*
\]

*Intuitively this follows from the single message case since these two inputs differ only in the second element and $\mathcal{A}$ can generate $\text{Enc}_{pk}(m_1,0)$ on its own.
To prove our claim, consider the following PPT adversary

Adversary \( A' \) against the single message experiment \( \text{PubK}^{\text{eav}}_{A', \Pi}(n) \):

1. \( A' \), given \( pk \), runs \( A(pk) \).
2. When \( A(pk) \) makes its first query \((m_{1,0}, m_{1,1})\) to the LR oracle, \( A' \) computes \( c_1 \leftarrow \text{Enc}_{pk}(m_{1,0}) \) and returns \( c_1 \) to \( A \).
3. When \( A(pk) \) makes its second query \((m_{2,0}, m_{2,1})\) to the LR oracle, \( A' \) outputs \((m_{2,0}, m_{2,1})\) and receives back a challenge ciphertext \( c_2 \). This is returned to \( A \).
4. \( A' \) outputs the bit \( b' \) that is output by \( A \).

When \( b = 0 \) adversary \( A' \) is given \( \text{Enc}_{pk}(m_{2,0}) \), and

\[
\Pr[A'(\text{Enc}_{pk}(m_{2,0})) = 0] = \Pr[A(pk, \text{Enc}_{pk}(m_{1,0}), \text{Enc}_{pk}(m_{2,0})) = 0].
\]

When \( b = 1 \) adversary \( A' \) is given \( \text{Enc}_{pk}(m_{1}^2) \), and

\[
\Pr[A'(\text{Enc}_{pk}(m_{2,1})) = 1] = \Pr[A(pk, \text{Enc}_{pk}(m_{1,0}), \text{Enc}_{pk}(m_{2,1})) = 1].
\]

Completing the proof of Claim 10.8

By the security of \( \Pi \) in the sense of single-message indistinguishability, there exists a negligible function \( \text{negl} \) such that

\[
\frac{1}{2} + \text{negl}(n) \geq \Pr[\text{PubK}^{\text{eav}}_{A', \Pi}(n) = 1] \\
= \frac{1}{2} \cdot (\Pr[A'(\text{Enc}_{pk}(m_{2,0})) = 0] + \Pr[A'(\text{Enc}_{pk}(m_{2,1})) = 1]) \\
= \frac{1}{2} \cdot (1 - \Pr[A'(\text{Enc}_{pk}(m_{2,0})) = 1] + \Pr[A'(\text{Enc}_{pk}(m_{2,1})) = 1])
\]

So that (after some fiddling to get other side of the absolute values)

\[
|\Pr[A'(\text{Enc}_{pk}(m_{2,0})) = 1] - \Pr[A'(\text{Enc}_{pk}(m_{2,1})) = 1]| \leq \text{negl}(n).
\]

This, together with results from previous page proves:

\[
|\Pr[A(pk, \text{Enc}_{pk}(m_{1,0}), \text{Enc}_{pk}(m_{2,0})) = 1] - \Pr[A(pk, \text{Enc}_{pk}(m_{1,0}), \text{Enc}_{pk}(m_{2,1})) = 1]| \leq \text{negl}(n).
\]
A very similar argument proves

From the previous slide we have

$$|\Pr[A(pk, \text{Enc}_{pk}(m_{1,0}), \text{Enc}_{pk}(m_{2,0})) = 1] - \Pr[A(pk, \text{Enc}_{pk}(m_{1,0}), \text{Enc}_{pk}(m_{2,1})) = 1]| \leq \text{negl}(n).$$

An almost identical arguments show the existence of a negligible function negl such that

$$|\Pr[A(pk, \text{Enc}_{pk}(m_{1,0}), \text{Enc}_{pk}(m_{2,1})) = 1] - \Pr[A(pk, \text{Enc}_{pk}(m_{1,1}), \text{Enc}_{pk}(m_{2,1})) = 1]| \leq \text{negl}(n).$$

Combining these two inequalities yields

$$|\Pr[A(pk, \text{Enc}_{pk}(m_{1,0}), \text{Enc}_{pk}(m_{2,0})) = 1] - \Pr[A(pk, \text{Enc}_{pk}(m_{1,1}), \text{Enc}_{pk}(m_{2,1})) = 1]| \leq \text{negl}(n).$$