Devote a Lifetime to Playing Games

Emanuele Di Giandomenico

e.di.giandomenico@tue.nl

Dipartimento di Matematica
Università di Genova

PhD Seminar
21st December 2023

Outline

Outline

What is a Game?

A tool to prove the security of cryptographic primitives.

The definition of security is tied to some particular event S.
$\Pr[S]$ has to be very close to some specified target probability.

Outline

To prove the security we use a sequence of games Game 0, Game 1, $\ldots$, Game n, which are related to the events $S_0, S_1, \ldots, S_n$.

- $\Pr[S_i]$ negligibly close to $\Pr[S_{i+1}]$.
- $\Pr[S_n]$ negligibly close to the target probability.

Transition based on Indistinguishability

A small change, if detected by the adversary, would imply an efficient method of distinguishing two distributions that are indistinguishable.

- P_1, P_2 are computationally indistinguishable distribution related respectively to S_i, S_{i+1}.
- Distinguish algorithm $\mathcal{D}$ s.t
  $\Pr[\mathcal{D}(x) \Rightarrow 1 \mid x \leftarrow P_1] = \Pr[S_i]$ and
  $\Pr[\mathcal{D}(y) \Rightarrow 1 \mid y \leftarrow P_2] = \Pr[S_{i+1}]$.

The indistiguishability assumption implies that $|\Pr[S_i] - \Pr[S_{i+1}]|$ is negligible.

Transition based on Failure Events

Game i and Game $i+1$ proceed identically unless a certain failure events F occurs. It is equivalent to saying that $S_i \wedge \neg F \iff S_{i+1} \wedge \neg F$.

Difference Lemma

Let S, S', F be events defined in some probability distribution, and suppose that $S \wedge \neg F \iff S' \wedge \neg F$. Then

$$|\Pr[S] - \Pr[S']| \leq \Pr[F].$$

Bridging Steps

This change is purely conceptual and $\Pr[S_i] = \Pr[S_{i+1}]$. It prepares the ground for one of the previous transition.

Outline

Public Key Encryption

Syntax

A public key encryption scheme PKE $:=$ (KeyGen, Enc, Dec) consists on three algorithms

- $(pk, sk) \leftarrow \mathsf{KeyGen}(1^\lambda)$.
- $c \leftarrow \mathsf{Enc}(pk, m)$.
- $m \leftarrow \mathsf{Dec}(sk, c)$.

Correctness

We say that PKE is ρ-correct if we have

$$\Pr\left[m = m' \;\middle|\; \begin{array}{l} (pk, sk) \leftarrow \mathsf{KeyGen}(1^\lambda), \\ c \leftarrow \mathsf{Enc}(pk, m), \\ m' \leftarrow \mathsf{Dec}(sk, c) \end{array} \right] \geq \rho$$

Security Game

<u>IND − PKE</u>

$(pk, sk) \leftarrow \mathsf{KeyGen}(1^\lambda)$
$(m_0, m_1) \leftarrow \mathcal{A}(pk)$
$b \leftarrow \{0, 1\}$
$c \leftarrow \mathsf{Enc}(pk, m_b)$
$b' \leftarrow \mathcal{A}(pk, c)$
return b'

The advantage of an adversary $\mathcal{A}$ against the above game is defined as

$$\mathsf{Adv}_{\mathsf{IND-PKE}}(\mathcal{A}) := \left| \Pr[b = b'] - \frac{1}{2} \right| .$$

Outline

ElGamal Encryption Scheme

Let G be a multiplicative group of prime order p, and let $g \in G$ be a generator.

KeyGen(1^λ)

$x \leftarrow \mathbb{Z}_p$
$h := g^x$
return $(pk, sk) := (h, x)$

Enc$(pk, m \in G)$

$y \leftarrow \mathbb{Z}_p$
$j := g^y$
$k := h^y$
$l := km$
$c := (j, l)$
return c

Dec(sk, c)

$m := l(j^x)^{-1}$
return m

Outline

Security of ElGamal

Let G be a multiplicative group of prime order p, and let $g \in G$ be a generator.

DDH Assumption

Let $\mathcal{D}$ be an algorithm that takes as input triples of group elements and outputs a bit. We define the advantage of $\mathcal{A}$ against DDH as

$$\mathsf{Adv}_{\mathsf{DDH}}(\mathcal{D}) := \begin{array}{l} |\Pr[x, y \leftarrow \mathbb{Z}_p \colon \mathcal{D}(g^x, g^y, g^{xy}) = 1] \\ - \Pr[x, y, z \leftarrow \mathbb{Z}_p \colon \mathcal{D}(g^x, g^y, g^z) = 1]| \end{array}$$

Security Proof

Game 0

$x \leftarrow \mathbb{Z}_p$
$h := g^x$
$(pk, sk) := (h, x)$
$(m_0, m_1) \leftarrow \mathcal{A}(pk)$
$b \leftarrow \{0, 1\}$
$y \leftarrow \mathbb{Z}_p$
$j := g^y$
$k := h^y$
$l := km_b$
$c := (j, l)$
$b' \leftarrow \mathcal{A}(pk, c)$
return b'

Security Proof

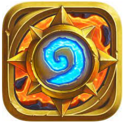
Game 1

$x \leftarrow \mathbb{Z}_p$
$h := g^x$
$(pk, sk) := (h, x)$
$(m_0, m_1) \leftarrow \mathcal{A}(pk)$
$b \leftarrow \{0, 1\}$
$y \leftarrow \mathbb{Z}_p$
$j := g^y$
$z \leftarrow \mathbb{Z}_p$
$k := g^z$
$l := km_b$
$c := (j, l)$
$b' \leftarrow \mathcal{A}(pk, c)$
return b'

Security Proof

- $\Pr[S_1] = \frac{1}{2}$: this follows from the fact that b' is independent from b.
- $|\Pr[S_0] - \Pr[S_1]| \leq \mathsf{Adv}_{\mathsf{DDH}}$.
- $\mathsf{Adv}^{\mathsf{ElGamal}}_{\mathsf{IND-PKE}} \leq \mathsf{Adv}_{\mathsf{DDH}}$.

Thanks for your attention!



I still prefer this game.