2 /0 /2025

S 6160 ryptology Lectu
omputational Securit

Maria Francis

ugust 28, 2025

Computationally Secure Cryptogra

The goal is to define encryption schemes that a computationally constrained adversary cannot dis some bounded probability (i.e. probability less th of an asteroid hitting the earth).

ll schemes are parameterized by a security para gets bigger the scheme should asymptotically bec secure. For example, the scheme can set the size key to depend on n.

dversaries are PPT (probabilistic polynomial tim access to randomness (uniformly random bits).

For a PPT algorithm $\mathcal{A}$ we write $\mathcal{A}$ x) to denote variable for $\mathcal{A}$'s output and $\mathcal{A}$ $x; r$) is the executi randomized algorithm for a particular input x and randomness r.

The adversary's success probability is negligible.

2 /0 /2025

Computational Indistinguishability

Consider the sequence $X = \{X_n\}$ and $Y = \{Y_n\}$

X, Y are computationally indistinguishable if all
distinguishers , $\exists$ n), a negligible function such

$$|Pr[\quad X_n) = 1] \quad Pr[\quad Y_n) = 1]| \leq$$

denoted by $X \approx Y$ and sometimes $X \approx_c Y$.

Theorem : If $X \approx Y$ and $f : \{0, 1\} \quad \rightarrow \{0, 1\}$ is
function then $f\ X) \approx f\ Y)$.

Reduction proof : Suppose $\exists$ PPT distinguisher

$$|Pr[\quad f\ X_n)) = 1] \quad Pr[\quad f\ Y_n)) = 1]| \neq$$

We then construct a new PPT distinguisher
get that $|Pr[\quad X_n) = 1] \quad Pr[\quad Y_n) = 1]| \neq$
$poly\ n)negl\ n)$ is negligible.

Computational Indistinguishability

Hybrid rgument If $X \approx Y$ and $Y \approx Z$ then $X \approx$

For any distinguisher let

$$
\begin{aligned}
n) &= |Pr[\quad X_n) = 1] \quad Pr[\quad Z_n) = \\
&= |Pr[\quad X_n) = 1] \quad Pr[\quad Y_n) = \\
&+ |Pr[\quad Y_n) = 1] \quad Pr[\quad Z_n) = \\
&\leq \quad n) + \ _2 \ n).
\end{aligned}
$$

$X \approx Y$ implies $n)$ is negligible and $Y \approx Z$ im negligible.

Since sum of two negligible functions are negligi $n)$ is negligible and $X \approx Z$.

Security Games

We usually define security via games which are in
protocols between an adversary $\mathcal{A}$ trying to brea
and the world running the system which we call t
$\mathcal{C}$.

For some such Game – or sometimes called Expe
an adversary $\mathcal{A}$ we define $Game_{\mathcal{A}}\ 1^n)$ to denote
game, usually this will be the output of the adve
end of the game.

We define often security via two games, $Game^0$,
represent two possible options for what the world
doing – encryptions of two different messages – a
that the adversary cannot tell them apart.

Security Games

We say that two games, $Game^0$, $Game$ are com
indistinguishable denoted as $Game^0 \approx Game$ if

$\forall PPT\ \mathcal{A}\ \exists$ a negligible function $n)$ s.t.
$|Pr[Game^0_{\mathcal{A}}\ 1^n) = 1] \quad Pr[Game_{\mathcal{A}}\ 1^n) = 1]$

If $Game^0 \approx Game$ and $Game \approx Game^2$ then
$Game^0 \approx Game^2$.

Computational indisitnguishability of games is an
computational indistinguishability of random vari
particular, the same hybrid argument works for ga

Computationally Secure Encryptio

Consider an encryption scheme with $\mathcal{K}_n = \{0, 1\}$
$\mathcal{M}_n = \{0, 1\}^{\ell(n)}$ where ℓ is a polynomial and $\mathcal{C}_n$.

The scheme consists of the algorithms to encrypt
$Enc : \mathcal{K}_n \times \mathcal{M}_n \to \mathcal{C}_n$ and $ec : \mathcal{K}_n \times \mathcal{C}_n \to \mathcal{M}_n$

We define the following game for proving comput
security

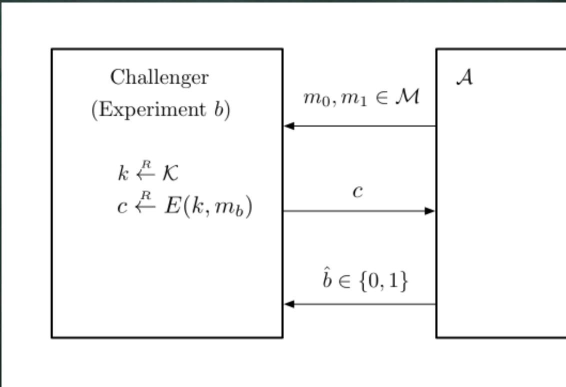
One-time Security Game $OneSec$, $b \in \{0, 1\}$:

dversary $\mathcal{A}$ chooses $m_0, m \;\in \mathcal{M}_n$ and sends to
$\mathcal{C}$ samples a uniformly random key from the key
and sends $\mathcal{A}$, $c = Enc\;\; k, m\;\;)$ of the message m
$\mathcal{A}$ outputs some $b \;\in \{0, 1\}$.

n encryption scheme is one time computational
sem ntic lly secure if $OneSec^0 \approx OneSec$.

2 /0 /2025

ttack Game for Semantic Securit



Formal Definitions

For $b = 0, 1$, let W be the event that $\mathcal{A}$ outputs 1 in Game/Experiment b. We define $\mathcal{A}$'s semantic security w.r.t. $\mathcal{E}$ as

$$SSadv_{\mathcal{A}\ \mathcal{E}}\ 1^n) := |Pr[W_0] \quad Pr[W\ ]|.$$

The value $SSadv_{\mathcal{A}\ \mathcal{E}}\ 1^n)$ is a number between 0 and 1

Definition (Semantic Security)

cipher $\mathcal{E}$ is semantically secure if all the efficient ad
the value $SSadv_{\mathcal{A}\ \mathcal{E}}\ 1^n)$ is negligible.

lternate Characterization

more convenient and common definition.

Just one experiment.

In this bit guessing version the challenger chooses
random and runs Experiment b and the adversary
which bit b has been used with probability better

2 /0 /2025

lternate Characterization

For a given cipher $\mathcal{E} =$ $Enc,$ $ec)$ defined over $\mathcal{K}, \mathcal{M}$
a given adversary $\mathcal{A}$ the attack game runs as follows:

- $\mathcal{A}$ computes m_0, m $\in \mathcal{M}$ of the same length and
  to the challenger, $\mathcal{C}$.
- $\mathcal{C}$ computes $b \leftarrow$ $\{0,1\}, k \leftarrow$ $\mathcal{K}$, $c \leftarrow$ E k, m
  to the adversary.
- The adversary outputs a bit $b' \in \{0,1\}$.

We say $\mathcal{A}$ wins the game if $b' = b$.
nyone can guess with $1/2$ probability and we want th
to be much better than a random guess.
If W denotes the event that the adversary wins the at
then we are interested in $|Pr[W]$ $1/2|$ and denote it
$SSadv_{\mathcal{A}\ \mathcal{E}}$ $1^n)$.

Relation between two characteriza

Exercise – For every cipher $\mathcal{E}$ and every adversary $\mathcal{A}$,
$SSadv_{\mathcal{A}\ \mathcal{E}}\ 1^n) = 2 \cdot SSadv_{\mathcal{A}\ \mathcal{E}}\ 1^n)$.