CS 6160 Cryptology Lectu
Pseudorandom Functions &
Security

Maria Francis

September 11, 2025

10/09/202

Security for Multiple Encryptions

- We looked at a weak model of passive eavesdrop ciphertext.
- Next we consider communicating parties sending ciphertexts to each other using same key and an observing all of them.
- Description of multiple encryption ttack game:
  1. $\mathcal{A}$ outputs a pairs of equal length lists of messag $M_0 = \ m_0 \ , \quad , m_{0\ t})$ and $M \ = \ m \quad , \quad , m$ $|m_{0\ i}| = |m \ \ _i| \ \forall i$.
  2. k is generated and a uniform bit $b \in \{0, 1\}$ is ch $c_i \leftarrow Enc_k \ \ m_{b\ i})$ and the list $C = \ c \ , \quad , c_t)$ is
  3. $\mathcal{A}$ outputs a bit b .
  4. $MultSec^*_{\mathcal{A}\ \mathcal{E}} \ \ 1^n)$ - the corresponding advantage winning this bit guessing game better than 1/2.

10/09/202

Security for Multiple Encryptions

- How do this experiment come in the picture of se definitions?

efinition

cipher $\mathcal{E} = \ \mathit{Gen}, \mathit{Enc}, \mathit{Dec})$ has indistinguishable m encryptions in the presence of an eavesdropper if for a polynomial-time adversaries $\mathcal{A}$,

$$\mathit{MultSec}^{*}_{\mathcal{A}\ \mathcal{E}}\ 1^{n}) \leq \mathrm{negl}\ n)$$

10/09/202

Security for Multiple Encryptions stronger?

- ny scheme that is secure w.r.t. the ttack gam encryptions is also secure w.r.t. ttack Game of security. The list has only one message.
- But is our new definition strictly stronger?

Theorem

There is a cipher that has indistinguishable encryption presence of an eavesdropper but not indistinguishable encryptions in the presence of an eavesdropper.

- sematically secure scheme that is deterministic outputting $M_0 = 0^\ell, 0^\ell)$ and $M = 0^\ell, 1^\ell)$.
- Let $C = c , c_2)$ be the ciphertexts $\mathcal{A}$ receives.
- If $c = c_2$, then $\mathcal{A}$ says $b' = 0$ else 1.

10/09/202

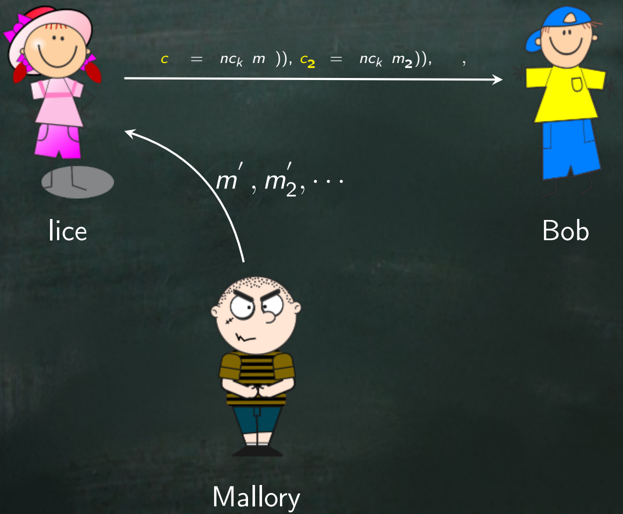
Security for Multiple Encryptions
stronger?

- What is the probability that $b^{'} = b$?
- The same message encrypted twice will yield the ciphertext.
- Thus if $b = 0$ then $c \ = c_2$ and so $\mathcal{A}$ outputs 0 i
- If $b = 1$ then a different message is encrypted ea so $c \ \neq c_2$ and $\mathcal{A}$ outputs 1.
- So probability is 1 that the adversary will succeed
- We need probabilistic encryption.

Theorem

f $\mathcal{E}$ is a encryption scheme in which Enc is a determi of the key and message then $\mathcal{E}$ cannot have indistingu multiple encryptions in the presence of an eavesdropp

Chosen-Plaintext ttacks



$c \quad = \quad nc_k \ m \ )), c_2 \quad = \quad nc_k \ m_2)), \quad ,$

$m' , m_2', \cdots$

lice

Bob

Mallory

Mallory gets lice to encrypt m , m_2, and eavesdrops for the corresponding cip

Chosen-Plaintext ttacks

lice

$c = Enc_k\ m)$, m is m_0 or m

Bob

Mallory

Can Mallory tell which message was enc with probability better random guessing?

10/09/202

CP in the real world

- CP encompasses known-plaintext attacks and th see in the real world.
- How can adversary have significant influence over messages got encrypted?
- $\mathcal{A}$ types on a terminal which in turns encrypts wh using the shared key of the server.
- In WWII, British placed mines in certain locations locations will get encrypted by Germans and they to break the scheme.
- More examples from WWII and real world!

10/09/202

CP security

- $\mathcal{A}$ has access to an encryption oracle Enc_k), it is blackbox that encrypts messages of $\mathcal{A}$'s choice us but won't show how it is done to $\mathcal{A}$.
- $\mathcal{A}$ queries this oracle with m and Enc_k) returns c
- For a randomized encryption, the oracle also uses randomness each time.
- $\mathcal{A}$ can interact with this oracle as many times as long as its polynomial in the security parameter).
- We do not worry about the efficiency of the orac

10/09/202

CP indistinguishability experime

1. key k is generated considering the security para
2. $\mathcal{A}$ has oracle access Enc_k) and outputs a pair of m_0, m of the same length.
3. uniform bit $b \in \{0, 1\}$ is chosen and then a cip $c \leftarrow Enc_k\ m_b)$ given to $\mathcal{A}$.
4. $\mathcal{A}$ continues to have oracle access to Enc_k) and b'.
5. $CP\ \ adv^*_{\mathcal{A}\ \mathcal{E}}\ 1^n)$ is defined as usual.

private-key encryption scheme $\mathcal{E}$ has indistinguishab under a CP or is CP -secure if for all PPT $\mathcal{A}$ CP a negligible.

10/09/202

CP indistinguishability experime

- Big advantage for CP -security – enough to shov single encryption.
- Security against CP is a minimal requirement fo schemes!
- ny private-key encryption scheme that is CP -s CP -secure for multiple encryptions.
- We skip the proof.

10/09/202

Block Ciphers

- Block ciphers are the “work horse” of practical cr
- They are used to build ciphers with stronger secu – stronger than semantic security.
- For all practical purposes we want block ciphers t random permutation.
- the definition of security of block cipher is like a test.

  The adversary is given a black box, instead of w permutation f that can be either E $k, \cdot)$ for a ra generated k or f is a truly random permutation, uniformly from all permutations on the domain. $\mathcal{A}$ cannot see inside the box but can probe it wi polynomial number of them.

10/09/202

Infinite (?) Pseudo randomness

- We want to have an infinite amount of shared ran just a short key.
- So when we get a message of length ℓ we can sp randomness into blocks of length ℓ and use each
- lice just tells Bob which location of the shared she used to encrypt and then Bob decrypts using information.
- s long as lice does not repeat the block, we ar eavesdroppers.
- Infinite means exponential amount! Typically a lo 2^{ℓ} OTP keys!

Pseudorandom Functions

- Pseudorandom functions are a neat abstraction o ciphers.
- High level idea:

  PRG: short random seed s gives G s) a long ran output.

  PRF: short random key K gives E_k $\dot{)}$ random lo
- We have keyed functions E_k with key length(ℓ_k 1 length(ℓ_{in} 1^n)) and output length(ℓ_{out} 1^n)).
- We assume all are length preserving, ℓ_k $1^n) = \ell_{in}$ $1^n) = \ell_{out}$ $1^n) = n$, but not necessa permutation!

Pseudorandom Functions

- E_k induces a natural distribution E on functions choosing a uniform key $k \in \{0,1\}^n$.
- We call E pseudorandom if the function E_k is inc from a function f chosen uniformly at random fro all functions with the same domain and range (i.e $f : \{0,1\}^n \to \{0,1\}^n$).
- How to choose a function at random? How big is $|\ \mathrm{unc}_n| = 2^{n\,2^n}$.

10/09/202

Pseudorandom Functions

pseudorandom function (PRF) is a family of functic
$\{E_k : \{0,1\}^{\ell_{in} \quad n)} \rightarrow \{0,1\}^{\ell_{out} \quad n)}$ where $n \in \quad , k \in \{0$
that:

- Efficiency: One can compute $E_K \ x)$ in poly $n)$-ti and x.
- Security: For any PPT adversary $\mathcal{A}$:

$$|Pr[\mathcal{A}^{\ \ k \ )} \ 1^n) = 1] \quad Pr[\mathcal{A}^{f \ )} \ 1^n) = 1]| \leq$$

where $k \leftarrow \{0,1\}^n$ and $f \leftarrow Func_n$, where $Func_n$
all the functions mapping ℓ_{in} bits to ℓ_{out} bits.

10/09/202

Pseudorandom Functions

- function is specified by giving its value on each domain.
- We can view the function f as a lookup table tha in the row of the table labeled x.
- For each $f \in \mathrm{unc}_n$, the look-up table for f has one for each string in the domain $\{0,1\}^n$.
- Each row contains an n-bit string since the range $\{0,1\}^n$.
- If we concatenate all the entries of this table, we function in unc_n can be represented by a string $2^n \times n$.
- Each string of length $2^n \cdot n$ is a unique function i $|\mathrm{unc}_n| = 2^{n\,2^n}$.

Pseudorandom Functions

- pseudorandom function is a keyed function, i.e E_k ·) is a function from $E_k : \{0,1\}^n \rightarrow \{0,1\}^n$ s. $k \in \{0,1\}^n$ is indistinguishable from f for a unifo $f \in$ unc$_n$.
- The former is a chosen from a distribution of 2^n whereas the latter is chosen from $2^{n\,2^n}$ functions!
- Despite this, every polynomial time distinguisher receives the *description* of pseudorandom functio 1 with “almost ” same probability as when it is gi description of random function f.

Oracle to avoid exponential descri

- But description of f could be exponential since $|\ \mathrm{unc}_n| = 2^{n\,2^n}$, we need lookup table of $n \cdot 2^n$.
- We give $\mathcal{A}$ an access to oracle $\mathcal{O}$ which is either
- $\mathcal{A}$ queries oracle at any point with x and the orac $\mathcal{O}\ x)$.
- The oracle is a black-box but deterministic and g output for same input.
- $\mathcal{A}$ can only do polynomial number of queries.
- $\mathcal{A}$ is not given key k, else distinguishing is trivial.

  $\mathcal{A}$ will query oracle with x, obtain y,
  heck $E_k\ x) = y$ if yes then conclude it was the
  else oracle for f.

10/09/202

Oracle to avoid exponential descri

- No matter how big the table is since we only hav polynomial number of queries we need to have or amount of the table.
- Basically we fill the table in a lazy/on-demand wa
- The lookup table is initially uninitialized and valu only when the calling program requests them.
- It changes when each entry is sampled (if at all) it is sampled (which is uniformly & independently

10/09/202

Security Definitions

- We have to define an attack game for security de PRF.
- We define two experiments just like before, but h adversary submits a sequence of queries x , x_2, challenger.
- $\mathcal{C}$ responds to query x_i with f x_i), where f in Exp and in Exp 1 it is randomly selected function fron
- The same f is used to answer all the queries.
- When the adversary tires itself of querying (note adversary so it will tire for sure) it outputs a bit.

10/09/202

ttack Game

Experiment b:

- The challenger selects $f \in \;\mathrm{unc}_n$ as follows:
  if $b = 0$ $k \leftarrow \mathcal{K}$, $f := E_k\; \cdot)$
  if $b = 1$ $f \leftarrow \;\mathrm{unc}_n$
- $\mathcal{A}$ submits a sequence of queries to the challenge
  $i = 1, 2, \quad$, the ith query is a data block x_i
- $\mathcal{C}$ computes $y_i = f\;\, x_i)$ and gives y_i to $\mathcal{A}$
- $\mathcal{A}$ computes and outputs a bit $\hat{b} \in \{0, 1\}$.

10/09/202

ttack Game

- For $b = 0, 1$, let W_b be the event that $\mathcal{A}$ outputs Experiment b. We define $\mathcal{A}$'s advantage as :

$$PRFadv_{\mathcal{A}\ \mathcal{E}}\ 1^k) = |Pr[W_0] \quad Pr[W\ ]$$

- We say that $\mathcal{A}$ is a Q-query PRF adversary if $\mathcal{A}$ Q queries.
- PRF $\mathcal{E}$ is secure if for all PPT adversaries $\mathcal{A}$, $PRFadv_{\mathcal{A}\ \mathcal{E}}\ 1^k)$ is negligible.
- The queries can be adaptive, i.e. they need not b advance and can be adapted to change based on

NOT a Pseudorandom Function

- Let $E_k\ \ x) = k \oplus x$.
- If k is uniform $E_k\ \ x)$ is also uniformly distributed
- Consider the following adversary $\mathcal{A}$ that queries $\mathcal{O}$
  distinct points $x\ \ , x_2$ to get $y\ \ = \mathcal{O}\ \ x\ \ )$ and $y_2 =$

  It outputs 1 iff $y\ \ \oplus y_2 = x\ \ \oplus x_2$
  If $\mathcal{O} = E_k$, for any k, $\mathcal{A}$ is correct is 1.
  For $\mathcal{O} = f$, the probability $f\ \ x\ \ ) \oplus f\ \ x_2) = x\ \ \oplus$
  as probability $f\ \ x_2) = x\ \ \oplus x_2 \oplus f\ \ x\ \ )$, which is
  The difference is $|1\quad 2\ \ ^n|$, not negligible.

10/09/202

PRFs and PRGs

- PRFs and PRGs are closely related.

  PRG guarantees that a single output appears ra
  input is chosen at random, i.e. G x) is pseudo-u
  uniform.

  PRF guarantees all its outputs appear random r
  input provided the function is drawn at random,
  by choosing a k at random, not its inputs!

- PRG can be constructed from PRF by simply eva
  different inputs.

- PRF from PRG? GGM construction given by Gol
  Goldwasser, and Micali.

10/09/202

PRFs and PRGs

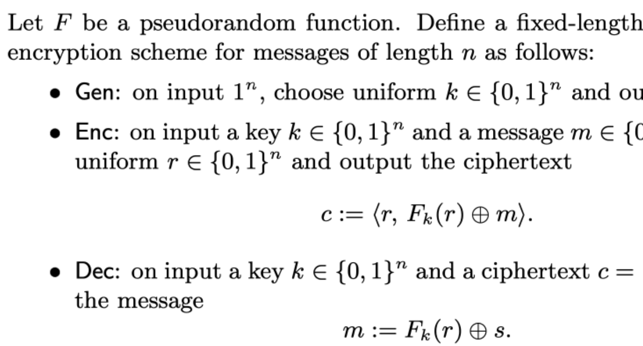
- PRFs are a compact representation of an exponen
pseudorandom string. PRGs always run in poly ti
only have outputs which are $\mathrm{poly}\ k$, the security
- PRFs remove the need of the sender and receiver
state and stay in synch to make sure that the pse
pad is not reused.
- PRFs allow for random-access, direct access to a
output stream, output of a function $f_k\ i)$, ith blo
pseudorandom string with seed k.
- PRFs are a way to achieve random access to a ve
pseudorandom string.

CP -security from a Pseudorando
Function

- PRFs give us access to infinite (not really infinite
  with one short key.
- How can one construct an encryption scheme fro
  pseudorandom function?
- $Enc_k \ m) = E_k \ m)$, where E_k is a PRF.
- The encryption reveals nothing about m, so it is
  checkbox cleared but it is deterministic.

10/09/202

CP -security from a Pseudorando
Function



Let F be a pseudorandom function. Define a fixed-length
encryption scheme for messages of length n as follows:

- Gen: on input 1^n, choose uniform $k \in \{0,1\}^n$ and ou
- Enc: on input a key $k \in \{0,1\}^n$ and a message $m \in \{($
uniform $r \in \{0,1\}^n$ and output the ciphertext

$$c := \langle r,\ F_k(r) \oplus m \rangle.$$

- Dec: on input a key $k \in \{0,1\}^n$ and a ciphertext $c =$
the message

$$m := F_k(r) \oplus s.$$

CP -security from a Pseudorando
Function

- Two things to note here that we have not previou
  the other ciphers:

  For a given key k, every message m has 2^n corre
  ciphertexts and still the receiver can decrypt cor
  The ciphertext is longer than the plaintext.

- To prove :If F is a (secure) PRF, then the above
  is a CP -secure symmetric encryption scheme.

Security Proof

Proof idea:

- Using the assumption that F is a PRF, we can ef
  replace F by a truly random function.
- We assume $\mathcal{A}$ is an efficient CP adversary that
  most q n) queries to the challenger, we argue tha
  negligible probability, no two r values are ever the

10/09/202

Security Proof

Games 0 and 1

- Game 0 considers the pseudorandom function an
  considers f from unc.
- The bit b referred in these games denotes the ra
  chosen by the challenger.
- $\hat{b}$ chooses the output bit of the adversary $\mathcal{A}$.
- Let W_j be the event that $\hat{b} = b$ in Game j.
- We show that the $|Pr[W\ ]\quad Pr[W_0]|$ is same as
  which we assume is negligible for a secure PRF.

Security Proof

Game 0 corresponding to encryption scheme $\mathcal{E}$

- Choose $k \leftarrow \mathcal{K}$ and E be a PRF and message len
- $\mathcal{A}$ queries the Enc-oracle on several messages. Fo $m \in \{0,1\}^n$, the oracle answers the query:

  hoose $r \leftarrow \{0,1\}^n$

  Returns $E_k \ r) \oplus m$
- $\mathcal{A}$ outputs $m_0, m \ \in \{0,1\}^n$ to the challenger $\mathcal{C}$
- Challenger chooses $b \leftarrow \{0,1\}$ and $r \leftarrow \{0,1\}^n$.
- Returns $\langle r, E_k \ r) \oplus m_b \rangle$
- $\mathcal{A}$ returns $\hat{b} \in \{0,1\}$
- W_0 is the event that $\hat{b} = b$ in Game 0.

Security Proof

Game 1 corresponding to encryption scheme $\mathcal{E}'$

- Choose $f \leftarrow \ \mathrm{unc}_n$, where message length is n.
- $\mathcal{A}$ queries the Enc-oracle on several messages. Fo
  $m \in \{0,1\}^n$, the oracle answers the query:

  hoose $r \in \{0,1\}^n$

  Returns $\langle r, f\ \ r) \oplus m \rangle$
- $\mathcal{A}$ outputs $m_0, m\ \ \in \{0,1\}^n$ to the challenger $\mathcal{C}$.
- Challenger chooses $b \leftarrow \{0,1\}$ and $r \leftarrow \{0,1\}^n$.
- Returns $\langle r, f\ \ r) \oplus m_b \rangle$
- $\mathcal{A}$ returns $\hat{b} \in \{0,1\}$
- $W\ \$ is the event that $\hat{b} = b$ in Game 1.

10/09/202

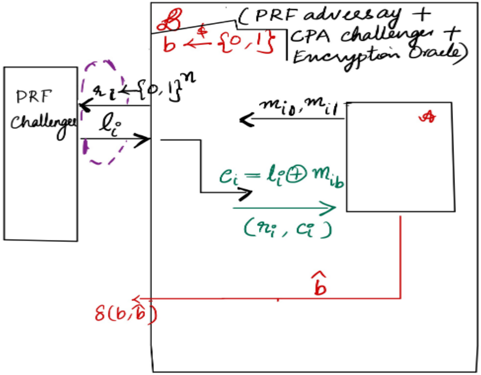
Security Proof

Claim 1 : $|Pr[W\ ]\quad Pr[W_0]| = negl\ 1^n)$

- We show in the next figure that $|Pr[W\ ]\quad Pr[W_0]| = PRFadv\ \mathcal{B})$ where $\mathcal{B}$ is an wrapper around $\mathcal{A}$ that attacks the underlying P
- Since we assume E to be a secure PRF, $PRFadv$ negligible implies $|Pr[W\ ]\quad Pr[W_0]| = negl\ 1^n)$.

10/09/202

Security Proof



Claim: $|\Pr[W_1] - \Pr[W_0]| = \mathrm{PRFadv}$
$(\mathcal{B}, E_k$

10/09/202

Security Proof

Claim 2: $Pr[W\ ] \leq 1/2 + q\ \ n)/2^n$

- Every time m is encrypted (either by Enc-oracle o
  ciphertext), a uniform r is chosen and ciphertext
  $\langle r, f\ \ r) \oplus m\rangle$.
- Let r^* be used for the challenge ciphertext (m_b).
  two cases:
  1. r^* is never used when answering any of $\mathcal{A}$'s Enc

     $\mathcal{A}$ learns nothing about $f\ \ r\ \ )$ by interacting w
     For $\mathcal{A}$, $f\ \ r\ \ )$ $\quad m_b$ is uniformly distributed anc
     the experiment so probability that $\quad = \ \hat{}$ is 1

10/09/202

CP -security proof contd.

2. r^* came up at least once in $\mathcal{A}$'s Enc-oracle queries

$\mathcal{A}$ gets $\langle r^*, s\rangle$ as response for m, $\Rightarrow f\ \ r^*) = s \oplus$

Probability of that happening: $q\ \ n)/2^n$, $r^* \in \{0, 1$

Let *Repeat* be the event corresponding to Case 2.

$$
\begin{aligned}
Pr[W\ ] &= Pr[W\ \ \cap Repeat] + Pr[W\ \ \cap \overline{Rep} \\
&\leq Pr[Repeat] + Pr[W\ |\overline{Repeat}] \\
&\leq q\ \ n)/2^n + 1/2
\end{aligned}
$$

This implies $|Pr[W_0]\quad 1/2| = CP\ \ adv^*_{\mathcal{A}\,\mathcal{E}\quad n)} = negl$