CSA E0 235: Cryptography (30.1.2016)

Scribe for Lecture 6

Instructor: Arpita Patra *Submitted by: Subhajit Bhar*

Contents

1 Introduction of CPA and CPA-security :

During World War II the British placed mines at certain locations, knowing that the Germans, when finding those mines,would encrypt the locations and send them back to headquarters. These encrypted messages were used by cryptanalysts at Bletchley Park to break the German encryption scheme.This is one of the historical example of CPA where as CPA was developed by Mihir Bellare, Anand Desai, E. Jokipii, Phillip Rogaway(A Concrete Security Treatment of Symmetric Encryption. FOCS,1997).

In ***C***hosen ***P***laintext ***A***ttacks (***CPA***), the attacker can influence the two parties to encrypt messages m_1,m_2,..... using same key k, which is shared between the two parties. In future the attacker observes ciphertext corresponding to some messages encrypted using same key k.The goal of the attacker is then decrypt messages using previous knowledge.

Security against CPA means that the attacker cannot tell which message was encrypted with probability significantly better than random guessing.

2 Formal definition of CPA security:

2.1 CPA security for single message encryption:

We imagine ***A***dversary($\boldsymbol{A}$) has access to an encryption oracle, viewed as a "black box".The adversary is allowed to interact with the oracle adaptively, as many times as it likes.

Consider the following experiment defined for any encryption scheme $\prod$ = (Gen, Enc, Dec), adversary $\boldsymbol{A}$, and value n for the security parameter:

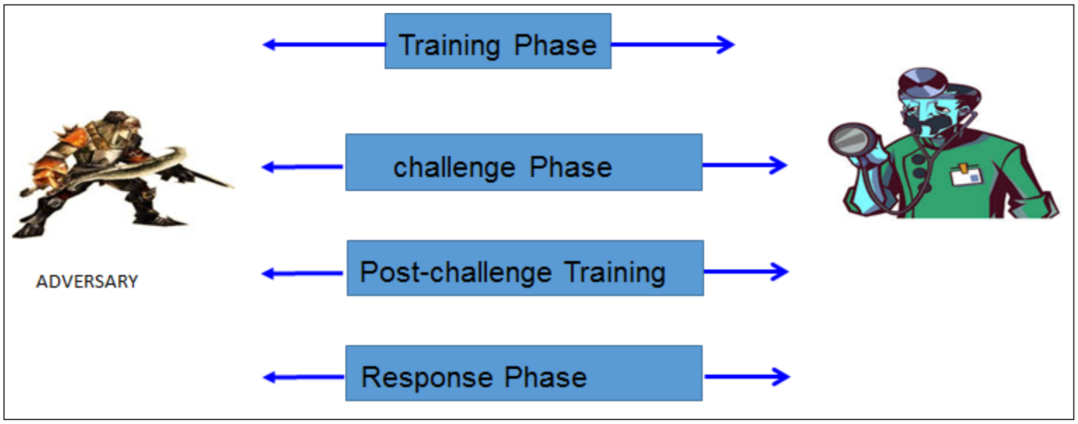


Figure 1: CPA indistinguishability Experiment

Training Phase:

$\boldsymbol{A}$ adaptively submits its query and receives their encryption..

(m_1, c_1),(m_2, c_2),....,(m_l, c_l): $c_l := Enc_k(m_l)$

Challenge Phase:

- $\boldsymbol{A}$ submits two equal length challenge plain-text (m_0,m_1).
- A uniform bit b $\in$ (0, 1) is chosen by verifier and then one of the challenge plain-text m_b is encrypted according to that for $\boldsymbol{A}$

Post Challenge Training Phase:

$\boldsymbol{A}$ adaptively submits its query and receives their encryption..

Response phase:

$\boldsymbol{A}$ finally submits its guess regarding encrypted challenge plain-text. Now adversary will win the game if his/her guess is correct.

Definition:

A private-key encryption scheme $\prod$ = (Gen, Enc, Dec) has indistinguishable encryptions under a chosen-plaintext attack, or is **CPA** secure, if for all probabilistic polynomial-time adversaries A there is a negligible function negl such that

$$\boxed{\Pr[\ PrivK_A^{cpa}\ (\mathrm{n}) = 1] \leqslant \frac{1}{2} + \mathrm{negl(n)}}$$

where the probability is taken over the randomness used by A, as well as the randomness used in the experiment.

2.2 CPA security for multiple message encryption:

Definition:

A private-key encryption scheme $\prod$ = (Gen, Enc, Dec) has indistinguishable encryptions under a chosen-plaintext attack, or is **CPA**-multiple secure, if for all probabilistic polynomial-time adversaries A there is a negligible function negl such that

$$\boxed{\Pr[\ PrivK_A^{cpa-mult}\ (\mathrm{n}) = 1] \leqslant \frac{1}{2} + \mathrm{negl(n)}}$$

where the probability is taken over the randomness used by A, as well as the randomness used in the experiment.

2.3 Relation between CPA single message and CPA multiple messages security:

Theorem :

Any private-key encryption scheme that is CPA-secure is also CPA-secure for multiple encryptions.

3 Advantage of CPA security:

I. We can use the same key for encrypting arbitrary number of messages.

II. Key size need not be same as message size.This is useful for large message size.In particular, given any CPA-secure fixed-length encryption scheme $\prod$ = (Gen, Enc, Dec), it is possible to construct a CPA-secure encryption scheme $\prod^{'}$ = $(Gen^{'}, Enc^{'}, Dec^{'})$ for arbitrary-length messages quite easily. For simplicity, say $\prod$ encrypts messages that are 1-bit long. Leave $Gen^{'}$ the same as Gen. Define $Enc_k^{'}$ for any message m (having some arbitrary length l) as $Enc_k^{'}(m) = Enc_k^{'}(m_1)$, . . . , $Enc_k^{'}(m_l)$, where m_i denotes the i-th bit of m.

4 Requirement of CPA security scheme:

Encryption procedure must be randomized. For this we need fresh randomness for each run of Enc.This results different ciphertexts for the same message. At the same time want to use a single key.

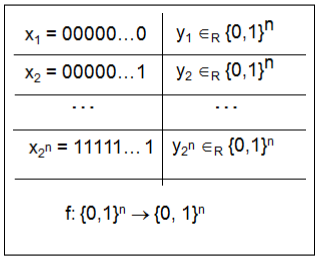
4.1 Random function-generation-problem:

Random function:

A truly Random function is such a function whose output behavior is completely unpredictable and every string of length n is a possible image with equal probability.

Generation of TRF:

Suppose we flip a coin n-times and according to the result of each time we can make n-bit x.Now using function f:$\{0,1\}^n \rightarrow \{0,1\}^n$ we can form y. Such a table is showing in the figure.

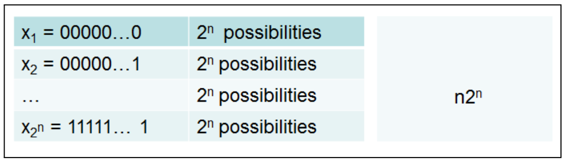


x_1 = 00000...0	$y_1 \in_R \{0,1\}^n$
x_2 = 00000...1	$y_2 \in_R \{0,1\}^n$
...	...
x_{2^n} = 11111...1	$y_{2^n} \in_R \{0,1\}^n$

f: $\{0,1\}^n \rightarrow \{0, 1\}^n$

Problem with the size of function:

In domain we have 2^n choices since every element is n-bit long. Thus table for f containing 2^n rows with each row containing an n-bit string.Thus, the size of f is exactly the number of strings of length n.2^n, or $|f| = 2^{n.2^n}$ This is not possible to construct in poly-time !



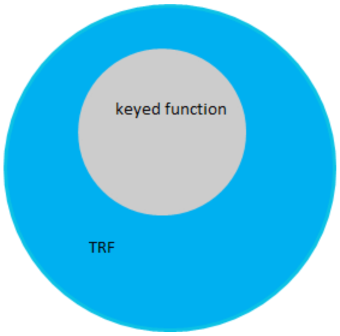
x_1 = 00000…0	2^n possibilities	n2^n
x_2 = 00000…1	2^n possibilities	
…	2^n possibilities	
x_{2^n} = 11111… 1	2^n possibilities	

5 Pseudorandom Functions :

A Pseudorandom Functions is a such function whose output behavior looks like a True random function and this function is chosen from a set of function according to some distribution(not true random distribution).Those function specification must be concise.

5.1 Keyed function:

A keyed function F induces a natural distribution on functions given by choosing a uniform key k ∈ $\{0, 1\}^n$ and then considering the resulting single input function F_k. The size of F is, $|F|$ = size of key space = 2^n



5.2 Indistinguishability Game for PRF:

We call F is pseudorandom if the function F_k(for a uniform key k) is indistinguishable from a function chosen uniformly at random from the set of all functions having the same domain and range; that is, if no efficient adversary can distinguish whether it is interacting with F_k (for uniform k) or f (where f is chosen uniformly from the set of all functions mapping n-bit inputs to n-bit outputs).

To define the indistinguishability scheme formally we perform following experiment:

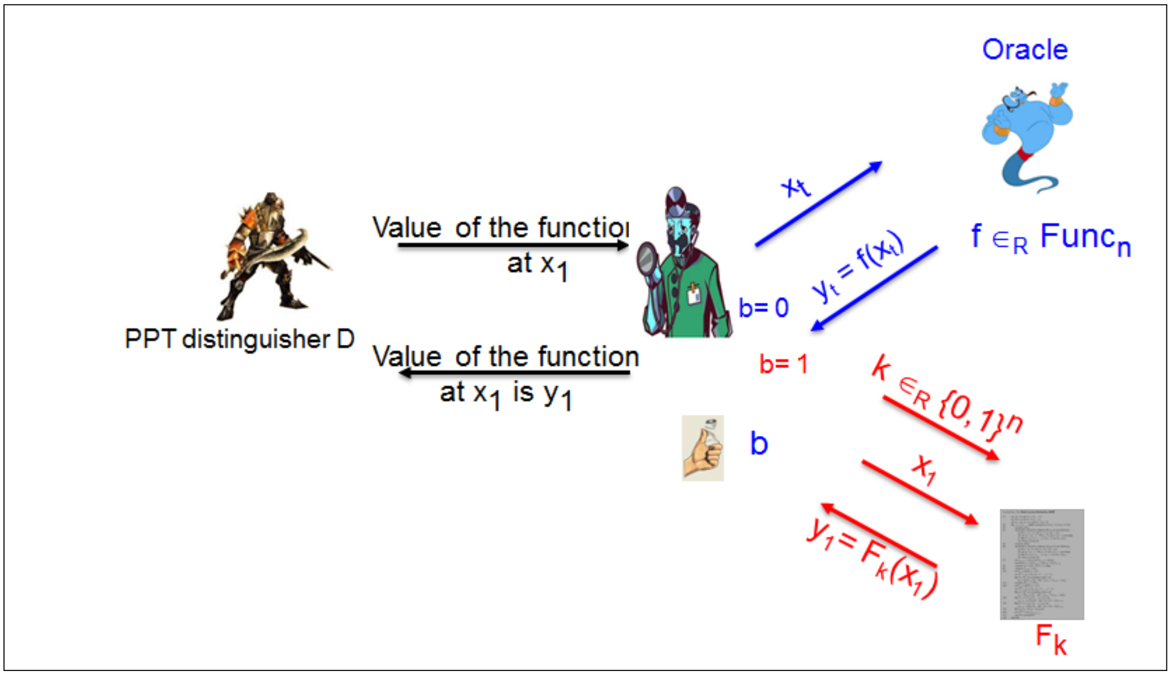


Figure 2: PRF indistinguishability Experiment

- PPT distinguisher ***D*** is allowed to ask polynomial number of queries.
- Verifier will flip a coin and result b $\in \{0, 1\}$.
- If b= 0 then he choose the value of function from oracle (i.e truly random function f)
- If b= 1 then he choose the value of function from keyed space (i.e F_k).
- If ***D*** guess is correct then ***D*** will win the game.

F is a PRF if for every PPT D there is an negl(n), for n number of queries

$$\boxed{\mid \text{Pr}[D^{F_k}(1^n) = 1] \text{ - } \text{Pr}[D^f(1^n) = 1] \mid \leq \text{negl(n)}}$$

5.3 Formation of PRF:

For an input x we form a keyed function like y = k $\oplus$ x.
Now for two input x_1,x_2 we following relationship between input and output,

$$x_1 \oplus x_2 = y_1 \oplus y_2$$

If we play same game as described above then for PPT distinguisher always Pr$[D^{F_k}(1^n) = 1]$ = 1 , if verifier choose the value of function from keyed space and Pr$[D^f(1^n) = 1] = 2^{-n}$ if verifier choose the value of function from oracle. So then,

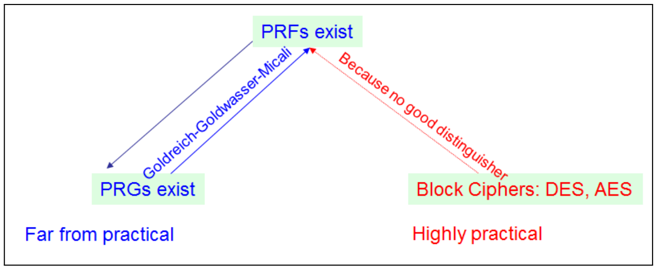
$$| \Pr[D^{F_k}(1^n) = 1] \text{ - } \Pr[D^f(1^n) = 1] \, |= 1\text{-}2^{-n}$$

This is not a negligible function of n.

6 Assumption for CPA security scheme:

PRFs exist

There is no proof but we strongly believe they do... The relation among PRF, PRG, Block cipher are shown in figure.



7 Condition for Pseudo Random Permutation (PRP):

F is a PRp if for every PPT D there is an negl(n), for n number of queries

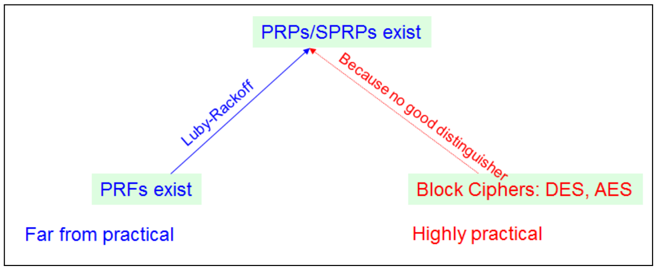
$$| \Pr[D^{F_k}(1^n) = 1] \text{ - } \Pr[D^f(1^n) = 1] \, | \leq \text{negl(n)}$$

8 Condition for Strong Pseudo Random Permutation (SPRP):

F is a Strong PRP if for every PPT D there is an negl(n), for n number of queries

$$| \Pr[D^{F_k, F_k^{-1}}(1^n) = 1] \text{ - } \Pr[D^{f, f^{-1}}(1^n) = 1] \, | \leq \text{negl(n)}$$

There is no proof but we strongly believe PRP and SPRP exist... The relation among PRF, PRP/SPRP, Block cipher are shown in figure.



References

(I) Katz, Jonathan, and Yehuda Lindell. Introduction to modern cryptography. CRC Press, 2014.

(II) Arpita Patra. http://drona.csa.iisc.ernet.in/arpita/Cryptography16.html. Course Materials.