CSC 591 Cryptography October 18th 2018

Lecture Mid-Term Review

Lecturer: Alessandra Scafuro *Scribe: Gauraang Khurana*

Psuedo-Randomness and Encyrption Security

This lecture is a review of the concepts covered in the first half of the semester. We briefly discuss the concepts behind pseudo-randomness and encryption schemes before we dive into sample problems and security proofs.

Definition

Pseudo-Randomness: Our goal is to output random looking strings. There are three sub-types when we talk about pseudo-randomness. These can be categorized as,

1. PRG: Given as input, a short truly random string called *seed*, the goal is to output a longer pseudo-random string.
2. PRF: Given as input a short truly random string called key, the goal is to output many pseudo-random strings.
   $F_K(X_1) \to y_1$
   $F_K(X_2) \to y_2$
   .
   .
   One key $\to$ Many outputs
3. PRP: It is similar to PRF but it gives us more functionality since it is a two-way function.
   $F_K(X_i) \to y_i$
   $X \leftarrow F_K^{-1}(y_1)$ [if K is known, we can go back]

CPA Security: Encryption - Our goal is to hide a message.

Private Key: $A \xrightarrow{c_1,c_2,c_i,c_n} B$
Pick $r \in \{0,1\}^n$
c $= m \oplus r \xrightarrow{c} B^r$
To prove alot of randomness, we don't need many keys but we need one r. Now we use,
$c = m_i \oplus F_k(r_i) \xrightarrow{r_i,c_i}$

Examples of PRF:

Given that F is a PRF, state whether F' is also a PRF.

1. $F'_K(x) = F_K(0) \oplus F_K(x)$

2. $F_K^{'}(x) = F_K(0x)$
3. $F_K^{'}(x) = F_K(0)||F_K(x)$
4. $F_K^{'}(x) = F_K(x) \oplus F_K(\bar{x})$
5. $F_K^{'}(x) = F_K(\bar{x})$

Before moving to the solutions, let's revise the functionality of a PRF function. We will construct a Distinguisher $D^{'}$ which has access to an Oracle $(F^{'}, TF)$. There are two phases involved,

- Query Phase
- Decision Phase

Solution 1:

Query Phase: Query$(X_1) \rightarrow Y_1$ (output), where $X_1 \in (0)^n$
Decision Phase:

- If $Y^1 = (0)^n$, then output 1
  Else output 0

Analysis Phase:

- Case 1: Oracle = $F^{'}$
  $$Pr[D^{'F^{'}}] = 1$$
- Case 2: Oracle is a Truly Random Function
  $$Pr[D^{TR} \rightarrow 1] = \frac{1}{2^n}$$

The difference between the probabilities in Case 1 and Case 2 is less than negligible, therefore we can say that this PRF is not secure.

Solution 2: Theorem : If F is a PRF then $F^{'}$ is also a PRF. Proof: Towards a contradiction. Assume $\exists$ PPT $D^{'}$ that distinguishes the Output of $F^{'}$.
$Pr[D^{'F^{'}} \rightarrow 1] - Pr[D^{TF} \rightarrow 1] = p(n)$

1. Reduction: From $D^{'}$ to D, where D is a distinguisher for F. D has oracle access to F and TF.
   - When $D^{'}$ queries X to his oracle, D queries $O(0x)$ (= y) and gives y to $D^{'}$.
   - When $D^{'}$ outputs a bit b, D outputs a b.
2. Analysis -
   - Case 1: Oracle = F, D simulates exactly behaviour of $F^{'}$.
   - Case 2: Oracle = TF, D simulates exactly a truly random function.

D wins with P(n) which is non-negligible. Therefore, it contradicts our assumption and hence we prove that it is a secure PRF.

Solution 3: Query Phase - Query(X_1) $\rightarrow Y_1$ (output)
Query(X_2) $\rightarrow Y_2$ (output)

Decision Phase:

- Parse Y_1 as y_{L_1} and y_{R_1} where $Y_1 = y_{L_1}||y_{R_1}$ and $|y_{L_1}| = |y_{R_1}|$.
- Parse Y_2 as y_{L_2} and y_{R_2} where $Y_2 = y_{L_2}||y_{R_2}$ and $|y_{L_2}| = |y_{R_2}|$.
- If $y_L^1 = y_R^2$, then output 1
  Else output 0

Analysis:

1. Case 1: Oracle = $F^{'}$
   $$Pr[D^{'F^{'}}] = 1$$
2. Case 2: Oracle is a Truly Random Function
   $$Pr[D^{TR} \rightarrow 1] = \frac{2^n}{2^2 n} = \frac{1}{2^n}$$

The difference between the probabilities in Case 1 and Case 2 is less than negligible, therefore we can say that this PRF is not secure.

Solution 4: Query Phase - Query(X_1) $\rightarrow Y_1$
Query($\bar{(}X_1)$) $\rightarrow Y_2$

Decision Phase:

- If $y_L^1 = y_R^2$, then output 1
  Else output 0

Analysis Phase:

- Case 1: Oracle = $F^{'}$
  $$Pr[D^{'F^{'}}] = 1$$
- Case 2: Oracle is a Truly Random Function
  $$Pr[D^{TR} \rightarrow 1] = \frac{2}{2^n}$$

The difference between the probabilities in Case 1 and Case 2 is less than negligible, therefore we can say that this PRF is not secure.

Examples of Encryption Scheme:

1. $Enc(K, m_1, ...m_n)$ $C_0 \leftarrow \{0,1\}^n$; $m_0 = c_0$

   For $i = 1..l$ $\qquad C_i = F_K(m_i) \oplus m_{i-1}$

   return $c_0, c_1..c_l$

2. $\text{Enc}(K, m)$ $S_1 \leftarrow \{0,1\}^K$ $S_2 \leftarrow S_1 \oplus m$

   $x = F_K(S_1)$; $Y = F_K(S_2)$ return x_1, y

Before moving to the solutions, let's revise the functionality of the A_{CPA}

- Training Stage
- Challenge Phase

  Sends m_0, m_1

  gets cipher, c^*
- Make Decision

Solution 2:
Training : No training required.
Challenge : Query $m_0 = 0^n$
$m_1 = 1^n$
Obtain $c^* = x^*, y^*$
Decision: If $x^* = y^*$, Output 1
Else Output 0
Analysis:

- Case 1: C^* is an encryption of $m_0 = 0^n$

  $X^* = F_K(S_1)$

  $Y^* = F_K(S_1 \oplus 0) = F_K(S_1)$

  $X^* = Y^*$

  A_{CPA} output 0 with Pr = 1

- Case 2: C^* is an encryption of $m_1 = 1^n$

  $X^* = F_K(S_1)$

  $Y^* = F_K(S_1 \oplus 1^n) \Rightarrow Y^* \neg X^*$

  A_{CPA} outputs 1 with Pr = 1