Hardware-Oriented Security and Trust
ECE 4156 HST / ECE 6156 HST
Spring 2024
Assoc. Prof. Vincent John Mooney III
Georgia Institute of Technology
Homework 3, 65 pts. (ECE 4156) 90 pts. (ECE 6156)
Due Friday February 2 prior to 11:55pm

1) (5 pts.) In the Media Gallery on Canvas, listen to the lecture "05MerkleDamgard." There is no need to notify Professor Mooney that you have done so **unless** you have problems. Canvas provides information regarding which GT usernames have accessed / listened to lectures, so there is no need to turn anything in if you have been successful.

Watch the video in Media Gallery

2) (15 pts.) Consider the following keyed function F: for security parameter n, the key is an n x n Boolean matrix A and an n-bit Boolean vector b. Define $F_{A,b}$: $\{0,1\}^n \rightarrow \{0,1\}^n$ by $F_{A,b}(x) \stackrel{\text{def}}{=} Ax + b$, where all operations are done modulo 2. Show that F is not a pseudorandom function. (NOTE: this is problem 3.13 on page 103 of Katz and Lindell.)

Solution

Given,
$F_{A,b}(x) \stackrel{\text{def}}{=} Ax + b$
Where $F_{A,b} : \{0,1\}^n \rightarrow \{0,1\}^n$
This function is **not a pseudorandom function.**

Proof:
$F_{A,b}(x) \stackrel{\text{def}}{=} Ax + b$
Plugging in a zero vector $0^n = [0,0,...,0^{n-1}]$ will reveal the vector b.
$F_{A,b}(0^n) = A(0^n) + b$
$= b$

Therefore, inserting a zero vector revealed the b vector.

Similarly, the keyed function can be solved for A.
By plugging in with only 1 one and the rest zeros, it is possible to find the columns of A.

For example:

$F_{A,b}([1,0,\ldots,0^{n-1}]) = A(1,0,\ldots,0^{n-1}) + b$

As the b vector values are already known, taking the result from the calculation above and subtracting the corresponding b vector value will yield the 1st column of A.

Similarly, calculate $F_{A,b}([0,1,\ldots,0^{n-1}) = A(0,1,\ldots,0^{n-1}) + b$
Taking the result and subtracting the b vector value will yield the 2nd column of A.

Solving for all n columns in this manner, we shall obtain the vector A.

With both the A and b vectors known, it is possible to create a distinguisher which makes the function deterministic and not pseudorandom.

As the function $F_{A,b}(x)$ is deterministic, $\Pr\left[D^{F_k(.)}(1^n) = 1\right] = 1$

It does not satisfy the condition $\left|\Pr\left[D^{F_k(.)}(1^n) = 1\right] - \Pr\left[D^{f(.)}(1^n) = 1\right]\right| \leq negl(n)$,

$$\left|\Pr\left[D^{F_k(.)}(1^n) = 1\right] - \Pr\left[D^{f(.)}(1^n) = 1\right]\right| > negl(n),$$

∴ $F_{A,b} : \{0,1\}^n \rightarrow \{0,1\}^n$ is not a pseudorandom function.

3) (25 pts.) Let F be a pseudorandom permutation and define a fixed-length encryption scheme (Enc, Dec) as follows: On input $m = \{0,1\}^{n/2}$ and key $k \in \{0,1\}^n$, algorithm Enc chooses a uniform string $r \in \{0,1\}^{n/2}$ of length $n/2$ and computes $c := F_k(r||m)$.

Show how to decrypt and provide an intuitive reason why this scheme is CPA-secure for messages of length n/2. (NOTE1: $r||m$ denotes For example, if $r = 0110$ and $m = 1100$ then one possibility is $r||m = 01101100$.) (NOTE2: this problem is very similar to problem 3.18 on page 104 of Katz and Lindell.) (NOTE3: the "intuitive reason" requested will not be graded in a harsh manner – in other words, if you provide a solid reason you will receive full credit even if there are a variety of solid, intuitive reasons possible. Of course, if you provide a "reason" which is vague or incorrect, you will lose points.)

Solution

Given,
input $m = \{0,1\}^{n/2}$
key $k \in \{0,1\}^n$
$r \in \{0,1\}^{n/2}$
$c := F_k(r||m)$
Need to decipher the ciphertext $c := F_k(r||m)$.
Why is this scheme CPA-secure?

Proof:

The ciphertext can be decrypted for a message m, where $m = \{0,1\}^{n/2}$, by first applying the inverse of the encryption scheme $c := F_k(r||m)$

$$dec := F_k^{-1}(c)$$
$$:= (r||m)$$

where $||$ denotes unambiguous concatenation of r followed by m.

As the decryption is unambiguously concatenated, both the uniform string and message will be of equal length n/2 and will be able to be distinguished. This means that the decrypted text's n/2 bits corresponding to the message can be obtained from the decryption result.

The given scheme is CPA-secure as the adversary can only make a polynomial set of queries to the encryption oracle, and so the chance that the encryption oracle picks the same random number r is negligible. If the selected same random number r is not the same, the query yields no useful information for the adversary. Since the probability of guessing r is negligible,

$$\Pr\left[\text{PrivK}_{A,\Pi}^{cpa}(n) = 1\right] \leq \frac{1}{2} + negl(n)$$

Therefore, the given pseudorandom permutation is CPA-secure.

4) (15 pts.) Let F be a pseudorandom function and G be a pseudorandom generator with expansion factor $\ell(n) = n + 1$. For the following encryption schemes, state whether the scheme has indistinguishable encryptions in the presence of an eavesdropper and whether it is CPA-secure. (In each case, the shared key is a uniform $k \in \{0,1\}^n$.) Explain your answer.

Encryption scheme: To encrypt $m \in \{0,1\}^n$, choose uniform $r \in \{0,1\}^n$ and output the ciphertext $\langle r, G(r) \oplus m \rangle$.

(NOTE: this is part a of problem 3.19 on page 104 of Katz and Lindell.)

Solution

Given,
ciphertext C = $\langle r, G(r) \oplus m \rangle$
$m \in \{0,1\}^n$
$k \in \{0,1\}^n$
$r \in \{0,1\}^n$

The given encryption scheme is **distinguishable and is not CPA-secure**.

Proof:

The text in the ciphertext is sent without a key so the adversary can obtain r via eavesdropping. Once r is obtained it can be used to find (r) using the generator. With $G(\text{r})$, finding m is straightforward. m is obtained by performing an XOR of c with $G(r)$.

$$G(r) \oplus c = m$$

As the text is distinguishable, the scheme is not CPA-secure.

5) [ECE 6156 only!] (20 pts.) Let F be a pseudorandom function and G be a pseudorandom generator with expansion factor $\ell(n) = n + 1$. For each of the following encryption schemes, state whether the scheme has indistinguishable encryptions in the presence of an eavesdropper and whether it is CPA-secure. (In each case, the shared key is a uniform $k \in \{0,1\}^n$.) Explain your answer.

a. To encrypt $m \in \{0,1\}^n$, output the ciphertext $m \oplus F_k(0^n)$.
b. To encrypt $m \in \{0,1\}^{2n}$, parse m as $m_1 || m_2$ with $|m_1| = |m_2|$, then choose uniform $r \in \{0,1\}^n$ and output the ciphertext $\langle r, m_1 \oplus F_k(r), m_2 \oplus F_k(r+1) \rangle$.

(NOTE: this is part b and part c of problem 3.19 on page 104 of Katz and Lindell.)

Solution

a. Given
$c = m \oplus F_k(0^n)$
note that $F_k(0^n)$ will always output the same value. The cipher text $c = m \oplus F_k(0^n)$ will always output the same value for a given message m. When the adversary has access to the oracle, the adversary can solve for $F_k(0^n)$ and m by finding the XOR of the cipher with m and $F_k(0^n)$ respectively. Therefore, the given scheme is **not CPA-secure**.
But the scheme is indistinguishable for an eavesdropper as $F_k(x^n)$ is a pseudorandom function. Thus, the message cannot be guessed even though the ciphertext c is known. $m \oplus F_k(0^n)$ acts as a one-time pad and is **indistinguishable.**

b. Given
$c = \langle r, m_1 \oplus F_k(r), m_2 \oplus F_k(r+1) \rangle$

If the adversary has access to the oracle, as F_k is a psuedorandom function and is **indistinguishable** in the presence of an eavesdropper. Thus, $F_k(r+1)$ and $F_k(r)$ have negligible probability of being distinguished.

The scheme is also **CPA-secure**. The scheme uses pseudorandom function F_k and has negligible probability $\left(\frac{q(n)}{2^n}\right)$ to find m_1 or m_2 where $q(n)$ is the number of queries to the oracle. As a result, there is negligible probability of finding m. Therefore, the given scheme is indistinguishable and CPA-secure.

A proof of this is very similar to the proof of Theorem 3.31 except that **Repeat** denotes the event that r-1, r or r+1 is chosen in another ciphertext.