Hardware-Oriented Security and Trust
ECE 4156 HST / ECE 6156 HST
Spring 2025

Assoc. Prof. Vincent John Mooney III
Georgia Institute of Technology

Homework 3, 55 pts. (ECE 4156) 75 pts. (ECE 6156)
Due Friday January 31 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 the Media Gallery on Canvas.

2) (15 pts.) Consider the following keyed function F: for security parameter n, the key is an $n \times n$ 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 3.15 on page 102 of the 3rd edition of Katz and Lindell; alternatively, this is problem 3.13 on page 103 of the 2nd edition.)

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.**

Informal Proof:
$F_{A,b}(x) \stackrel{\text{def}}{=} Ax + b$
Plugging in a zero vector will reveal the vector b.
$F_{A,b}(0) = A(0) + b$
$= b$
Therefore inserting a zero vector reveals the b vector.

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

For Example:
$F_{A,b}(1,0^{n-1}) = F_{A,b}(1,0,\ldots,0) = A(1,0^{n-1}) + b$
As the b vector values are already known, subtracting the first column with corresponding b vector value will yield the 1st column of A.

Similarly, $F_{A,b}(0,1,0^{n-2}) = A(0,1,0^{n-2}) + b$
Subtracting the second column with the corresponding b vector value will yield the 2nd column of A.

Solving for all n values we shall obtain the matrix A.

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

Since the Function is deterministic, $\Pr\left[D^{F_k(.)}(1^n) = 1\right] = 1$

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

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

$\therefore$ $F_{A,b} : \{0,1\}^n \rightarrow \{0,1\}^n$ 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 (i) how to decrypt and (ii) provide an intuitive reason why this scheme is CPA-secure for messages of length $n/2$. (NOTE1: $r||m$ denotes unambiguous concatenation of r and m. For example, if $r = 0110$ and $m = 1100$ then one possibility is $r||m = 01101100$.) (NOTE2: this problem is very similar to 3.19 on page 102 of the 3rd edition of Katz and Lin-dell; alternatively, this problem is very similar to problem 3.18 on page 104 of the 2nd edition 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 the following:
input $m = \{0,1\}^{n/2}$
key $k \in \{0,1\}^n$
$r \in \{0,1\}^{n/2}$
$c := F_k(r||m)$
Show how to decipher the ciphertext $c := F_k(r||m)$.
Also, explain why this scheme is CPA- Secure.

Informal Proof / Reason / Intuition:
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 it is unambiguously concatenated, both the uniform string and message will be of equal length n/2. This means that the decrypted text contains in a known fashion the n/2 bits that are the message text.

We now show that the given scheme is CPA-Secure. In order to show this, we first consider an encryption scheme $\widetilde{\Pi}_E$ that is identical to the above encryption scheme except that a truly random permutation is used instead of a pseudorandom one. Let A be an adversary and let $q(\cdot)$ be a polynomial upper bounding the runtime of A. We claim the following:

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

Let r_c denote the random string used to generate the challenge ciphertext $c := F_k(r||m)$.

There are two cases:

a) *The value r_c is used by the encryption oracle to answer at least one of A's queries*: In this case, A can know which message was encrypted, but the probability of this event occurring is upper bounded by $\frac{q(n)}{2^{\frac{n}{2}}}$ (this is obtained by applying the union bound).

b) *The value r_c is not used by the encryption oracle to answer any of A's queries*: In this case, A learns nothing about the plaintext because the challenge ciphertext is a uniform string (subject to being distinct from all other ciphertexts).

Using a similar argument as in the proof of Theorem 3.31, the above equation follows. The rest of the proof follows as in the proof of Theorem 3.31 by showing that the difference when using a pseudorandom permutation instead is at most negligible.

In summary, the probability of guessing *r* is negligible,

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

Therefore, the given pseudorandom permutation is CPA-secure.

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

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

(NOTE: this is problem 3.20a on page 102 of the 3rd edition of Katz and Lindell; alternatively, this is problem 3.19a on page 104 of the 2nd edition of Katz and Lindell.)

Solution

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

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

Informal Proof / Explanation:

The text in the ciphertext is sent without a key so the adversary can get r via eavesdropping. Once r is obtained it can be used to find $G(r)$ using the generator. With $G(r)$, finding m is straightforward. m is obtained from the 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 (EAV-secure) 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 $m \oplus F_k(0^n)$.

Given
c := $m \oplus F_k(0^n)$
As $F_k(0^n)$ 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. Since the adversary has access to an encryption 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 since $F_k(0^n)$ 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. 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: these are problems 3.20b and 3.20c on page 102 of the 3rd edition of Katz and Lindell; alternatively, these are problems 3.19b and 3.19c on page 104 of the 2nd edition.)

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

F_k is a psuedorandom function and thus 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. 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.