COMP547A Homework set #3

Due Thursday November 12th, 2020, 23:59:59

Exercises (from Katz and Lindell's book)

[15%]

3.6 Let G be a pseudorandom generator with expansion factor $\ell(n) > 2n$. In each of the following cases, say whether G' is necessarily a pseudorandom generator. If yes, give a proof; if not, show a counterexample.

(a) Define $G'(s) \stackrel{\text{def}}{=} G(s_1 \ldots s_n)$, where $s = s_1 \ldots s_{2n}$.

(b) Define $G'(s) \stackrel{\text{def}}{=} G\left(0^{|s|} \| s\right)$, where $s = s_1 \ldots s_{n/2}$.

(c) Define $G'(s) \stackrel{\text{def}}{=} G(s) \,\|\, G(s+1 \bmod 2^n)$

[5%]

3.13 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 $F_{A,b} : \{0,1\}^n \to \{0,1\}^n$ 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.

[5%]

3.18 Let F be a pseudorandom permutation, and define a fixed-length encryption scheme (Enc, Dec) as follows: On input $m \in \{0,1\}^{n/2}$ 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 prove that this scheme is CPA-secure for messages of length $n/2$. (If you are looking for a real challenge, prove that this scheme is CCA-secure if F is a *strong* pseudorandom permutation.)

[+10% bonus]

[15%]

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

(b) To encrypt $m \in \{0,1\}^n$, output the ciphertext $m \oplus F_k(0^n)$.

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

More on back…

[5%]

3.17 Assume pseudorandom permutations exist. Show that there exists a function F' that is a pseudorandom permutation but is *not* a strong pseudorandom permutation.

Hint: Construct F' such that $F'_k(k) = 0^{|k|}$.

[5%]

3.29 Let $\Pi_1 = (\mathsf{Enc}_1, \mathsf{Dec}_1)$ and $\Pi_2 = (\mathsf{Enc}_2, \mathsf{Dec}_2)$ be two encryption schemes for which it is known that at least one is CPA-secure (but you don't know which one). Show how to construct an encryption scheme Π that is guaranteed to be CPA-secure as long as at least one of Π_1 or Π_2 is CPA-secure. Provide a full proof of your solution.

Hint: Generate two plaintext messages from the original plaintext so that knowledge of either one reveals nothing about the original plaintext, but knowledge of both enables the original plaintext to be computed.

[5%]

5.5 What is the output of an r-round Feistel network when the input is (L_0, R_0) in each of the following two cases:

(a) Each round function outputs all 0s, regardless of the input.

(b) Each round function is the identity function.

[5%]

5.6 Show that DES has the property that $DES_k(x) = \overline{DES_{\overline{k}}(\overline{x})}$ for every key k and input x (where $\overline{z}$ denotes the bitwise complement of z). This is called the *complementarity property* of DES. (The description of DES given in this chapter is sufficient for this exercise.)

[20%]

5.12 This question illustrates an attack on two-key triple encryption. Let F be a block cipher with n-bit block length and key length, and set $F'_{k_1,k_2}(x) = F_{k_1}(F^{-1}_{k_2}(F_{k_1}(x)))$.

(a) Assume that given a pair (m_1, m_2) it is possible to find in *constant* time all keys k_2 such that $m_2 = F^{-1}_{k_2}(m_1)$. Show how to recover the entire key for F' (with high probability) in time roughly 2^n using three known input/output pairs.

(b) In general, it will *not* be possible to find k_2 as above in constant time. However, show that by using a pre-processing step taking 2^n time it is possible, given m_2, to find in (essentially) constant time all keys k_2 such that $m_2 = F^{-1}_{k_2}(0^n)$.

(c) Assume k_1 is known and that the pre-processing step above has already been run. Show how to use a single pair (x, y) for a *chosen* input value x to determine k_2 in constant time.

(d) Put the above components together to devise an attack that recovers the entire key by running in roughly 2^n time and requesting the encryption of roughly 2^n chosen inputs.

More on back…

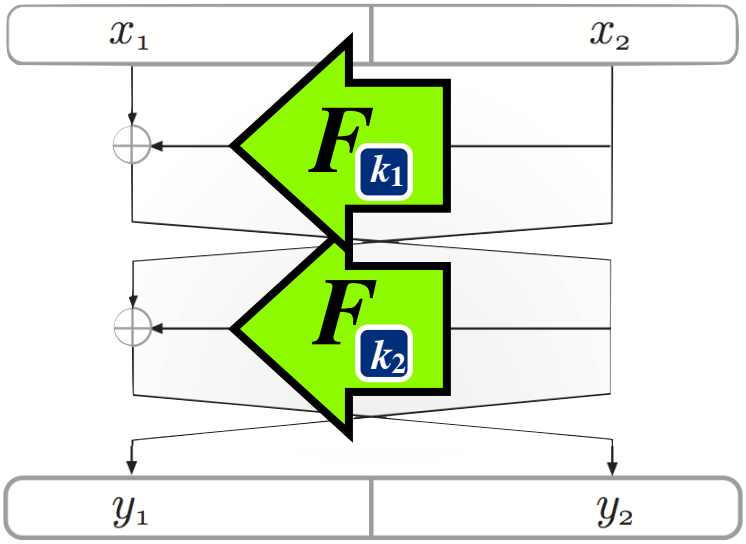
Homemade Exercises: non Pseudo-Random Permutation

[5%]

1. Let F be a pseudo-random family of functions. Let k_1 and k_2 be two independent random keys. Prove that

$$\pi_{k_1,k_2}(x_1, x_2) := \langle x_1 \oplus F_{k_1}(x_2), x_2 \oplus F_{k_2}(x_1 \oplus F_{k_1}(x_2)) \rangle$$

is not a pseudo-random permutation family.

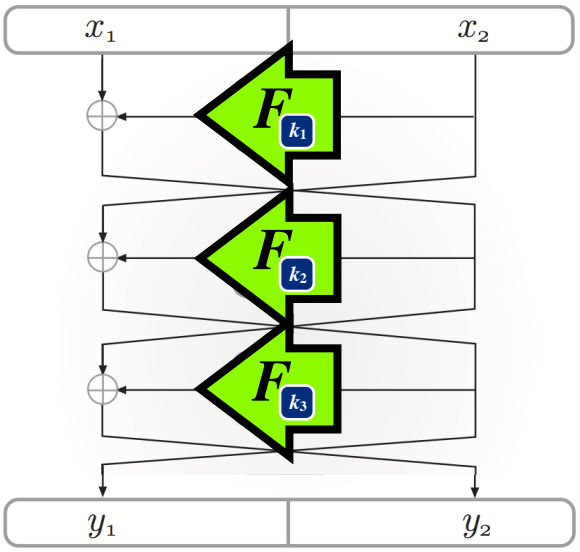


[5%]

2. Let F be a pseudo-random family of functions. Let k_1, k_2 and k_3 be three independent random keys. Prove that

$\pi_{k_1,k_2,k_3}(x_1, x_2) := \langle x_2 \oplus F_{k_2}(x_1 \oplus F_{k_1}(x_2)), x_1 \oplus F_{k_1}(x_2) \oplus F_{k_3}(x_2 \oplus F_{k_2}(x_1 \oplus F_{k_1}(x_2))) \rangle$

is not a **strong** pseudo-random permutation family.

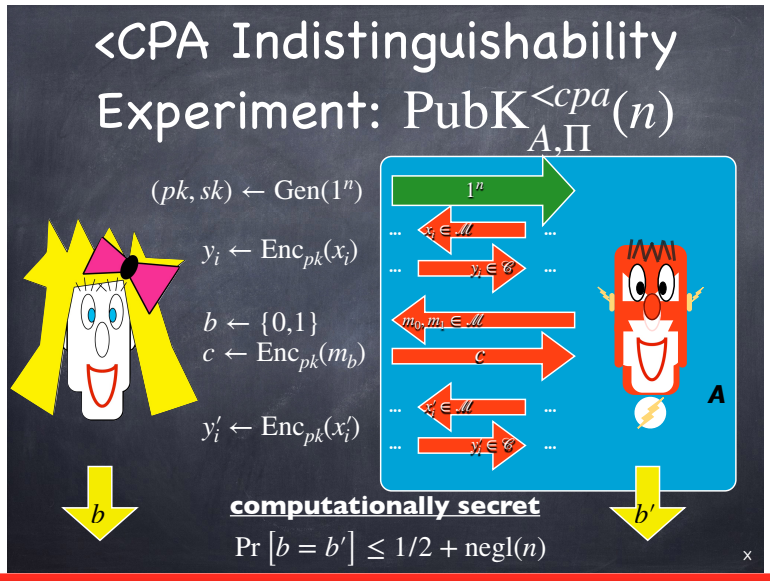


More on back…

Homemade Exercises: <CPA and >CPA

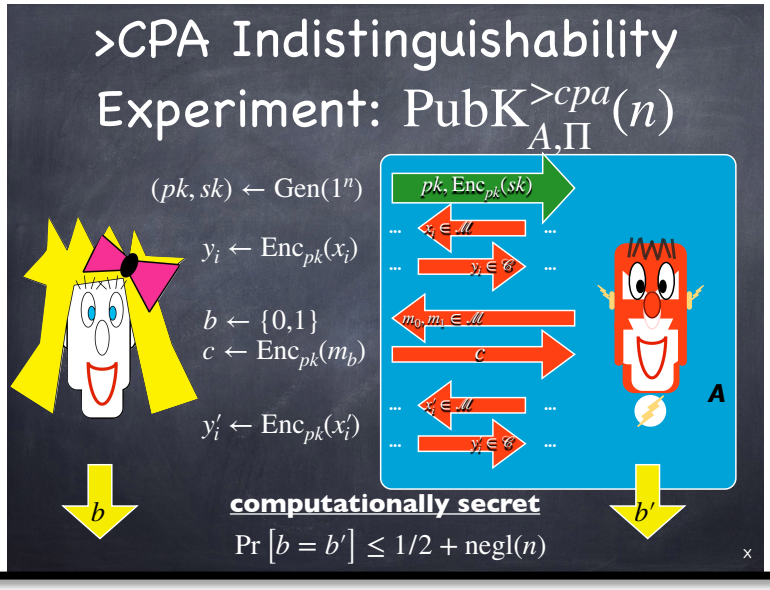
[5%]

3. Consider the definition below of the <CPA indistinguishability experiment leading to <CPA-security. Instead of providing the public-key pk to the adversary, it only provides an oracle access to the encryption algorithm. I give you a <u>private-key</u> scheme Π that is CPA-secure. Construct from Π a <u>public-key</u> scheme Π' that is <CPA-secure but does not have indistinguishable encryptions in the presence of an eavesdropper.



[5%]

4. Consider the definition below of the >CPA indistinguishability experiment leading to >CPA-security. Instead of providing only pk to the adversary, it also provides $\text{Enc}_{pk}(sk)$ (an encryption of the private-key). I give you a <u>public-key</u> scheme Π that has indistinguishable encryptions in the presence of an eavesdropper. Construct from Π a <u>public-key</u> scheme Π' that still has indistinguishable encryptions in the presence of an eavesdropper but is not >CPA-secure.



More on back…