COMP 4140 (Fall 2022) Assignment 2

Due date: Thursday October 20, by 11:59 PM (CST) Late assignments will not be accepted.

This pdf copy is provided for convenience only. You must use the crowdmark link provided for submission.

Notation:

- $||$ means concatentation. Eg. $0010||110010 = 0010110010$.
- NOT is the negation operator. Eg. $\mathsf{NOT}(0010) = 1101$.
- If $m = m_1 m_2 ... m_n$ is a n-bit binary string, then $\oplus_{i=1}^{n} m_i$ is the XOR of all the bits of m. Eg. If $m = 1011$, then $\oplus_{i=1}^{n} m_i = 1 \oplus 0 \oplus 1 \oplus 1 = 1$.

Required Questons - Please submit solutions to the following questions.

1. Suppose $F : \{0,1\}^n \to \{0,1\}^{2n}$ is a PRG that is also an injection (that is, one-to-one). Define G to be a deterministic polynomial-time algorithm such that for any n and any input $s \in \{0,1\}^n$, the output of $G(s)$ is $F(s)||s$.

Prove that G is not a pseudorandom generator.

Hint: The distinguisher has access to F.

2. Let $F : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$ be a length-preserving pseudorandom function. Let $G : \{0,1\}^n \times \{0,1\}^{n-1} \to \{0,1\}^{3n}$ be the keyed function defined as
$$G_k(x) = F_k(0||x)||\mathsf{NOT}(F_k(0||x))||F_k(1||x).$$

Prove that G is not a pseudorandom function.

3. Let $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be an private-key encryption scheme that is EAV-secure. Define a new scheme $\Pi^{'} = (\mathsf{Gen}^{'}, \mathsf{Enc}^{'}, \mathsf{Dec}^{'})$ where $\mathsf{Gen}^{'}$ is the same as Gen, $\mathsf{Enc}^{'}_k(m) = \mathsf{Enc}_k(m)||(\oplus_{i=1}^{n} m_i)$, where $m = m_1 m_2 ... m_n$, and $\mathsf{Dec}^{'}_k(c) = \mathsf{Dec}_k(c_1 c_2 ... c_{|c|-1})$.

Show that the scheme $\Pi^{'}$ is *not* EAV-Secure?

4. Suppose G is a PRG with expansion factor $l(n)$ for every positive integer n.

Prove that the function $G^{'}(s) = \mathsf{NOT}\ G(s)$ is also a PRG for all s where $|s| > 0$.

5. Consider the following variation of the one-time pad for $n \geq 6$.

$\mathsf{Gen}(1^n)$ takes as input 1^n and outputs an uniformly and randomly chosen key from $\{0,1\}^n$...

$\mathsf{Enc}_k(m)$ takes as input $k, m \in \{0,1\}^n$, uniformly and randomly chooses a string l from $\{100...0, 0100...0, 0010...0, ..., 000...01\}$, the set of n-bit strings where exactly one of the n bits is 1. The output of $\mathsf{Enc}_k(m)$ is the 2-tuple $(m \oplus k \oplus l, l)$. Note that $\mathsf{Enc}_k(m)$ is a randomized algorithm.

$\mathsf{Dec}_k(c, l)$ takes as input k, c, l and outputs $c \oplus k \oplus l$.

Answer the following questions.

a. Show that this scheme is correct. That is, for each $n \geq 6$, $\mathsf{Dec}_k(\mathsf{Enc}_k(m)) = m$ for each $m \in \{0,1\}^n$.

b. Show that this scheme **does not** have indistinguishable multiple encryptions in the presence of an eavesdropper. That is, show it is not secure under multiple encryptions with the same key.

Hint: For $n \geq 6$, you may assume it is possible to construct a set of $n+1$ n-bit binary strings $w_1, w_2, ..., w_{n+1}$ in polynomial-time with respect to n, where any pair of these strings differ in at least 3 positions. You don't need to give an algorithm for doing this, you can just assume a polynomial-time algorithm exists for doing this.

Optional Questions - The following questions will not be graded but you should try them.

1. Suppose $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is a private-key encryption scheme, n is the security parameter and $\mathcal{A}$ is a PPT adversary.

We define $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n, b)$ be the same experiment at $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n)$ except that the fixed bit $b\{0,1\}$ is used (random than being chosen at random). Let $out_{\mathcal{A}}(\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n, b))$ denote the output bit $b^{'}$ the adversary in this experiment.

Show that if for all PPT adversaries $\mathcal{A}$, there exists a negligible function negl such that the following condition holds

$$|\Pr[out_{\mathcal{A}}(\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n, 0) = 1] - \Pr[out_{\mathcal{A}}(\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n, 1) = 1]| \leq \mathsf{negl}(n),$$

then Π is EAV-secure (as defined by Definition 3.8 of textbook and in the lecture slides).

2. Consider the following encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ where F is a pseudorandom function.

   - Gen: On input 1^n, choose k, s uniformly from $\{0,1\}^n$ and outputs (k, s).
   - Enc: For the key (k, s) and a message $m \in \{0,1\}$ do the following:

     1. If $m = s$, output the ciphertext $(0, k, s, s)$.

2. If $m \neq s$, then choose uniformly and randomly $r \in \{0,1\}^n$ and output the ciphertex $(1, s, r, F_k(r) \oplus m)$.

- Dec: For the key (k, s) and ciphertext $c = (b, c_1, c_2, c_3)$ do the following:
  1. If $b = 0$ output s.
  2. If $b = 1$ output $m = F_k(c_2) \oplus c_3$.

Show that:

- Decryption always succeeds. That is, for any key (k, s) and message m, $\mathsf{Dec}_{(k,s)}(\mathsf{Enc}_{(k,s)}(m)) = m$.
- Show that Π is not secure under chosen-plaintext attack. That is, show Π is not CPA-secure.

3. Show that if G is not a pseudorandom generator then Construction of the EAV-secure scheme (pseudo one-time pad on slide 107 of the lectures slides) is not EAV-Secure.

4. Given a stream cipher $(\texttt{Init}, \texttt{Next})$ and a parameter $l = l(n) > n$, define the deterministic function G^l by

$$G^l(s) = GetBits_1(Init(s), 1^l).$$

We say the stream cipher is *secure* if G^l is a PRG for any polynomial l.

Let F be a pseudo-random funcyion, and consider the following stream cipher which accepts an n-bit initialization vecture IV:

- $\texttt{Init}(s, IV)$ outputs $\texttt{st} = (s, IV)$.
- $\texttt{Next}(s, IV)$ outputs $y = F_s(IV)$ and $\texttt{st}' = (s, IV + 1)$.

Show that this stream cipher is not secure.