

Mid-Sem Solutions

Problem 1

a) Π perfectly secure or not? $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$:

$\text{Gen}(1^n)$: Pick $k \in \{0, 1\}^n \setminus \{0^n\}$

$\text{Enc}(k, m) := k \oplus m$

$\text{Dec}(k, c) := k \oplus c$

Solution: No, not perfect secure.

Take uniform random distribution $\mathcal{U}_M$ on message space M .

Then, for any fixed $m \in M$

$$\Pr[\mathcal{U}_M = m | C = m] = 0 \neq \Pr[\mathcal{U}_M = m]$$

% you excluded $k=0^n$

b) Is F' a PRF?

$F = \{f_k : \{0, 1\}^n \rightarrow \{0, 1\}^n \mid k \in \{0, 1\}^n\}$ is a PRF.

$$f'_k(x) := \begin{cases} f_k(x) & \text{if } \bigoplus_{i=1}^n x_i = 0 \\ f_k(x \oplus 0^n \| 1) & \text{if } \bigoplus_{i=1}^n x_i = 1 \end{cases}$$

Solution: No, not a PRF

Attack: Eve can query the oracle on x & $x \oplus 0^n \| 1$.
If the outputs are same $\Rightarrow$ PRF else random function.
Clearly Eve wins this with non-negl. prob.

c) G' PRG or not?

$G : \{0, 1\}^n \rightarrow \{0, 1\}^{\ell}$ be a PRG

$$G'(s) := \begin{cases} G(s) & \text{if } \bigoplus_{i=1}^{\ell} s_i = 0 \text{ (even parity)} \\ G(s \oplus 0^{\ell-1} \| 1) & \text{if } \bigoplus_{i=1}^{\ell} s_i = 1 \text{ (odd parity)} \end{cases}$$

called parity of s

Solution: Remark: this question is an example which shows the importance of writing a complete formal proof.

My earlier "proof" was hand-waived & hence I didn't catch a mistake in the reduction. Here, intuition was actually deceptive. Thanks to Aditya, who gave the seed to launch a complete attack (although it uses a "leakage-resilient" PRF, which I haven't taught in class)

Let $\{f_k: \{0,1\}^n \rightarrow \{0,1\}^n\}_{k \in \{0,1\}^n}$ be a PRF that remains secure, even when Eve gets a single bit dependent on k .
 (In particular, say Eve gets $\bigoplus_{i=1}^n k_i$ in addition to the oracle access to either f_k or a random function and the security guarantee is that Eve still cannot win)

called
"leakage-
resilient"
PRFs

Now, $G(s) = f_s(0^n) \parallel \bigoplus_{i=1}^n s_i$ is a PRG (assuming the special PRF above)

But now the last bit of $G'(s)$ = $\begin{cases} \bigoplus_{i=1}^n s_i = 0 & \text{if } \bigoplus_{i=1}^n s_i = 0 \\ \bigoplus_{i=1}^n s_i \oplus 1 = 0 & \text{if } \bigoplus_{i=1}^n s_i = 1 \end{cases}$

$\Rightarrow$ Last-bit is predictable
 $\Rightarrow G'$ is not a PRG.

Moral of the story: Think intuitively, but only believe it if you can completely prove it! Sometimes, intuitions can be wrong!

d) Is Π COA-secure or not?

Π is CTR-mode, instantiated with the specific function F' in b)

Solution: Not COA-secure.

If you encrypt 3-blocks $m_1 \parallel m_2 \parallel m_3$, then $\because f'_k(\text{ctr}+1) = f'_k(\text{ctr}+2)$
 $c_2 \oplus c_3 = m_2 \oplus m_3$ which will lead to a COA-attack

Problem 2: Let (Gen, H) be collision resistant

a) $H_1^k(x) := H^k(x) \oplus 1^k$

Solution: Yes

Given a collision for H $x \neq x' : H^k(x) = H^k(x')$
 $\rightarrow x \neq x' : H^k(x) \oplus 1^k = H^k(x') \oplus 1^k$
 $\rightarrow x \neq x' : H_1^k(x) = H_1^k(x')$
 which gives a collision for H

b) $H_2^k(x) := H^k(x_1 || x_2 || \dots || x_n)$ where $x = x_1 || x_2 || \dots || x_n || x_n$.

Solution: No

$x = x_1 || x_2 || \dots || x_n || 0 \neq x' = x_1 || x_2 || \dots || x_n || 1$ is a collision for any $x_1 || x_2 || \dots || x_n$.

c) $H_3^k(x) := y_1 || y_2 || \dots || y_n$ where $y_1 || y_2 || \dots || y_n || y_n = H^k(x)$.

Solution: No

for a collision resistant (Gen, H) , define $H^k(x || b) := \hat{H}^k(x) || b$ for $b \in \{0, 1\}$.

Now (Gen, H) is also collision resistant (easy to show)

Instantiate H_3 with this H gives an attack:

for any $x_1 || x_2 || \dots || x_n$, $x = x_1 || \dots || x_n || 0 \neq x' = x_1 || \dots || x_n || 1$ is a collision.

Problem 3: $F = \{f_k : \{0, 1\}^n \rightarrow \{0, 1\}^n\}_{k \in \{0, 1\}^n}$ be a PRF. Is $\Pi = (\text{Gen}, \text{Mac}, \text{Verify})$ EU-CMA secure in each case below?

a) $\text{Gen}(m)$ outputs $k \in \{0, 1\}^n$ (fixed-length MAC)
 $\text{Mac}_k(m_1 || m_2) :$ where $|m_1| = |m_2| = n-1$
 outputs $t = f_k(0 || m_1) \oplus f_k(1 || m_2)$

Solution: No

Malloy: query $m_1 || m_1$ to get $t = f_k(0 || m_1) \oplus f_k(1 || m_1)$
 $m_2 || m_2$ to get $t' = f_k(0 || m_2) \oplus f_k(1 || m_2)$
 $m_1 || m_2$ to get $t'' = f_k(0 || m_1) \oplus f_k(1 || m_2)$

Forgery: $(m_2 || m_2, t'' = t \oplus t' \oplus t'')$

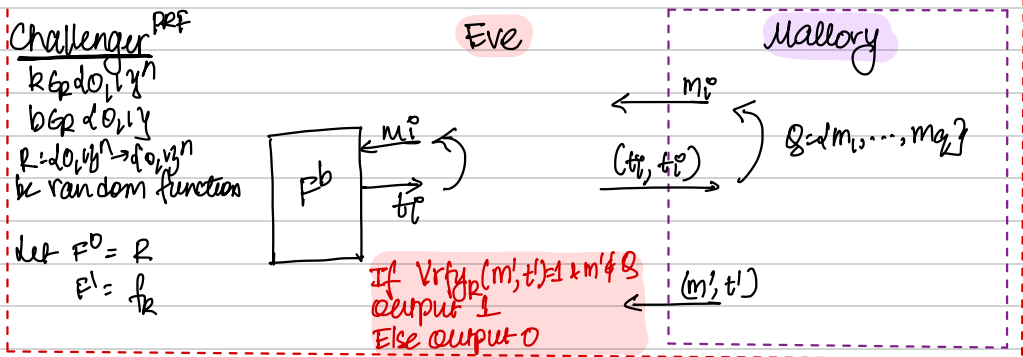
b) $\text{Gen}(1^n)$ outputs $k \in \{0,1\}^n$.

$\text{Mac}_k(m)$: output $t = (f_k(m), f_k(m))$.

Solution: Yes, it is EUCMA Secure.

Reduction: Assume $\exists$ Mallory against Π

Here is an **Eve**, breaking the PRF security!



$$\Pr_{\mathcal{E}}[\text{Eve}^{\text{rel.}}(n) = 1] = \Pr[\text{MacForge}_{\text{Mallory}, \pi}^{\text{ema}}(n) = 1]$$

$$\Pr\{E_{\text{ver}}^{R(L)}(1^n) = 1\} = \frac{1}{2^n}$$

Problem 4: $G: \{0,1\}^n \rightarrow \{0,1\}^{n+1}$ be a pseudorandom generator.

TL = (Gen, Enc, Dec) defined as:

$\text{Gen}(C^n)$: outputs $k \in \{0, 1\}^n$

$\text{Enc}(k, m)$: for $m \in \{0, 1\}^{n+1}$

output: $c = m$, if $k = 0^{100} || k$, (i.e. first 100-bits of k are 0)
 $c = m \oplus G(k)$, otherwise

Solution: Π is not CPA secure $\because \Pi$ is deterministic

with challenge messages m_0, m_1 , Eve gets c_b

Eve can query $Enc_f(\cdot)$ on m_0 & m_1 to get c_0 & c_1

If $C_b = C_0$ output 0 else if $C_b = C_1$ output 1.

Π does not have ciphertext integrity: query $\text{Enc}_K(\cdot)$ to get C
output $C' = C \oplus 1^n$.

Problem 5: Let (Gen, h) be fixed-length CRHF with input length $2n-1$ and output length $n-1$. Define (Gen, h) on inputs of length $2n$:

$$h^k(b \| x) := \begin{cases} b \| h^k(x) & \text{if } b=0 \\ x & \text{otherwise} \end{cases}$$

- a) Is (Gen, h) collision resistant?
 b) Is (Gen, h) obtained using Merkle-Damgård transform to (Gen, h) collision resistant?

Solution (Sketch):

- a) No, for any $x \neq x' \in \{0,1\}^{2n-1}$
 $(0 \| x, 1 \| x')$ gives a collision.

- b) Yes,

$\therefore$ Merkle-Damgård sets $z_0 := 0^n$, & computes
 $z_p := h^k(z_{p-1} \| x_p) \quad \forall p = 1, \dots, l+1$, where $x_{l+1} = (x)$.

$$\therefore z_1 = h^k(0^n \| x_1) = 0 \| h^k(0^n \| x_1) \quad (\text{denote by } 0 \| z_1')$$

$$\Rightarrow \forall p = 2, \dots, l+1, \quad z_p = h^k(0 \| z_{p-1}' \| x_p) = 0 \| h^k(z_{p-1}' \| x_p)$$

$\therefore$ The proof is exactly same as Merkle Damgård for $(\text{Gen}, \hat{h})$ with just the bit 0 pre-pended at each step.
 No argument changes!

Problem b: $F: \{f_k: \{0,1\}^n \rightarrow \{0,1\}^n\}_{k \in \{0,1\}^n}$ be a weak PRF.

a) $\Pi = (\text{Gen}, \text{Mac}, \text{Vrfy})$ for $\mathcal{M} = \{0,1\}^n$

$\text{Gen}(1^n)$: output $k \in \{0,1\}^n$

$\text{Mac}_k(m)$: output $t = f_k(m)$.

Solution: not EU-CMA secure. take the F from the hint.

$$f_k(x) := \begin{cases} 0^n & \text{if } x = 0^n \\ f_k(x) & \text{o.w.} \end{cases}$$

for a PRF

$$F = \{f'_k: \{0,1\}^n \rightarrow \{0,1\}^n\}_{k \in \{0,1\}^n}$$

Show that: F is a weak PRF (via reduction)

The for this F , Π has the following forgery:
Mallory can just output $(m = 0^n, t = 0^n)$.

b) $\Pi' = (\text{Gen}', \text{Mac}', \text{Vrfy}')$ for $\mathcal{M} = \{0,1\}^n$

$\text{Gen}'(1^n)$: outputs $k \in \{0,1\}^n$

$\text{Mac}'(k, m)$: generate $r \in \{0,1\}^n$ & output $t = (r, f_k(r \| m))$

$\text{Vrfy}'(k, m, t)$: for $t = (r, s)$ if $f_k(r \| m) = s$ output 1
else output 0.

Solution: Modify the F from a) slightly:

$$\text{for } x_1, x_2 \in \{0,1\}^n, f_k(x_1 \| x_2) := \begin{cases} 0^n & \text{if } x_2 = 0^n \\ f'_k(x_1 \| x_2), & \text{otherwise} \end{cases}$$

for a PRF

$$F' = \{f'_k: \{0,1\}^n \rightarrow \{0,1\}^n\}_{k \in \{0,1\}^n}$$

Again, show that:

F is a weak PRF (via reduction)

Then, for this F , a clear forgery is:

Mallory outputs $(m = 0^n, t = 0^n)$ as a forgery

c) Can you build an EU-CMA secure Π just assuming that F is a weak PRF.

Solution:

Step I: weak PRF $\Rightarrow$ length doubling PRG.

$F = \{f_k: \{0,1\}^{n/2} \rightarrow \{0,1\}^{2n/2}\}_{k \in \{0,1\}^{n/2}}$ be weak PRF
Consider $G: \{0,1\}^n \rightarrow \{0,1\}^{2n}$:

$$G(s_1 \| s_2) := f_{s_1}(s_2) \quad \text{for } s_1, s_2 \in \{0,1\}^{n/2}$$

Prove that if F is a weak PRF $\Rightarrow G$ is a PRG.

Step II: You can now use GGM with G above to get a PRF $F' = \{f'_k: \{0,1\}^n \rightarrow \{0,1\}^{2n}\}_{k \in \{0,1\}^n}$

Step III: Now, the construction Π in a) is EU-CMA secure for $M = \{0,1\}^n$ when instantiated with F'

Intuition: Essentially GGM helps you transform a primitive (PRG or weak PRF) with "average-case" security (meaning only on random inputs) to "worst-case" security of PRFs (meaning for inputs of adv's choice). For MAC this "worst-case" security is needed!

Think about CPA-encryption & if all this is needed for that!