

Midterm 1 Review Questions

1 PRG Reduction Failure

Let $G(s) : \{0,1\}^\lambda \rightarrow \{0,1\}^{\ell(\lambda)}$ be a PRG. Define the following candidate PRG $G'(s) : \{0,1\}^\lambda \rightarrow \{0,1\}^{\ell(\lambda)+\lambda}$:

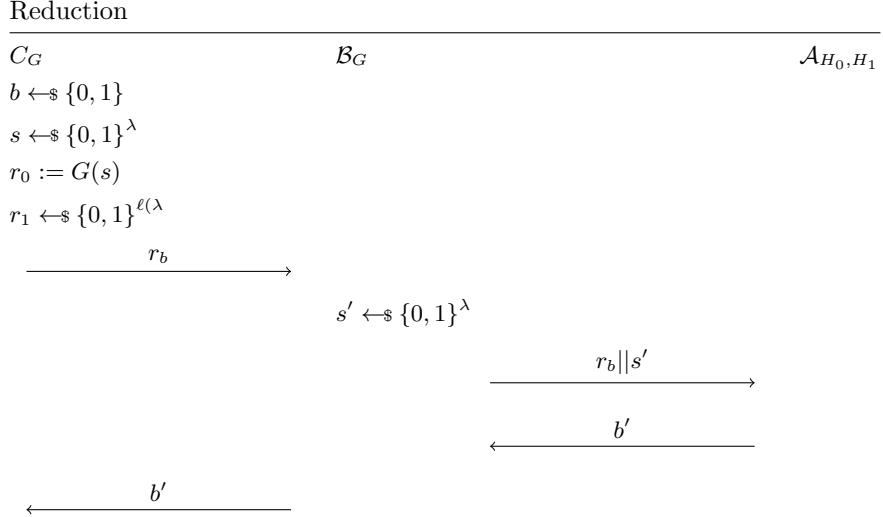
$$\boxed{\begin{array}{c} G'(S) \\ \hline \text{return } G(s)||s \end{array}}$$

We previously saw that G' is *not* a secure PRG. We will show how, if we attempt to prove that G' is secure, the proof breaks down.

We first define our hybrids:

$$H_0 = \{G(s)||s : s \xleftarrow{\$} \{0,1\}^\lambda\}$$
$$H_1 = \left\{ r||s : \begin{array}{l} s \xleftarrow{\$} \{0,1\}^\lambda \\ r \xleftarrow{\$} \{0,1\}^{\ell(\lambda)} \end{array}\right\}$$

We now must prove that H_0 is computationally indistinguishable from H_1 . To do so, we build a reduction. Assume that there exists an adversary \mathcal{A}_{H_0, H_1} that distinguishes between H_0 and H_1 . We will build an adversary \mathcal{B}_G that distinguishes between the output of G and a random string.



Our next step is to look at the input mapping. When $b = 1$, $r_b || s'$ is a truly random string, exactly what \mathcal{A}_{H_0, H_1} expects to see in H_1 .

However, when $b = 0$, $r_b || s' = G(s) || s'$. Note that this is *not* what \mathcal{A}_{H_0, H_1} would expect to see in H_0 , which is $G(s) || s$ (the seed passed to the PRG is *the exact same* as the value concatenated to the output). Therefore the input mapping fails, and our reduction cannot go forward.

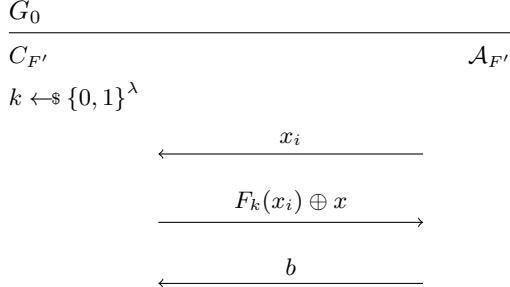
When working through a problem yourself, this would be the point to ask whether the scheme is indeed *insecure*. The reason the reduction fails can often give you a hint as to how to attack the scheme. In this case, the reduction fails because the seed s is the same as the seed that is passed to G . As we saw in class, we can use this fact to attack the scheme.

2 Proving a PRF Secure

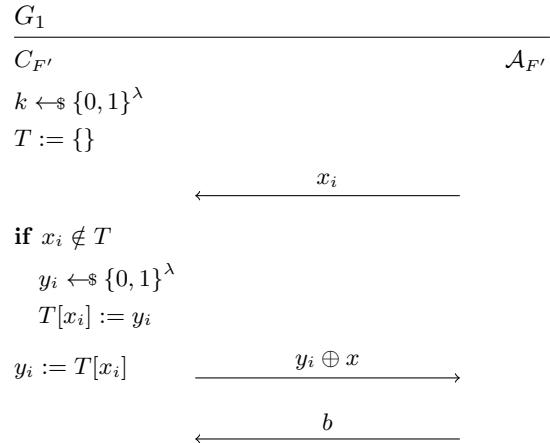
Let $\{F_k\}_{k \in \{0,1\}^\lambda}$, where $F_k : \{0, 1\}^\lambda \rightarrow \{0, 1\}^\lambda$ be a secure PRF. We will prove that $F'_k(x) := F_k(x) \oplus x$ is a secure PRF.

We do this proof via a series of games. For a game G_i , let W_i be the event that an NUPPT adversary \mathcal{A} outputs 1 in G_i .

Let G_0 be the PRF Game₀ for F'_k , shown below (there may be any polynomial number of queries from $\mathcal{A}_{F'}$ to $C_{F'}$).



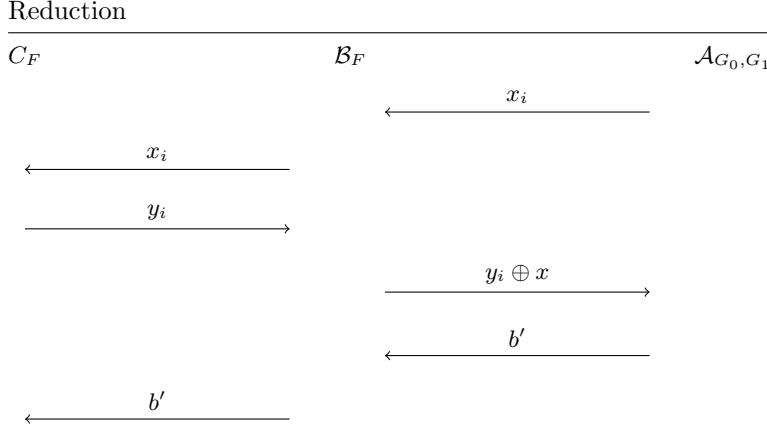
We now define G_1 , where the output of $F'_k(x_i)$ is replaced with a random function.



We now prove that G_0 is computationally indistinguishable from G_1 . To do this, we must show that there exists a negligible function $\nu(\lambda)$ such that:

$$|\Pr[W_0] - \Pr[W_1]| \leq \nu(\lambda)$$

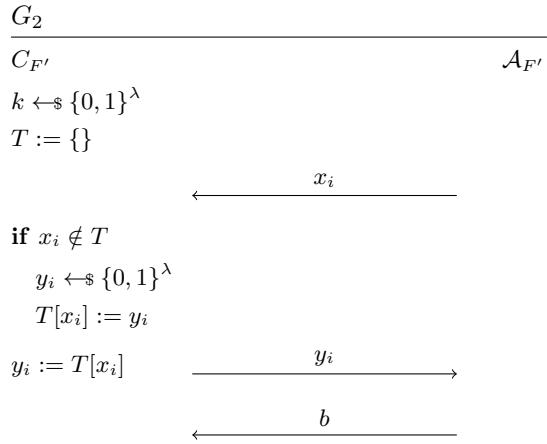
We do this via a reduction to the security of F . Let \mathcal{A}_{G_0, G_1} be an adversary that distinguishes between G_0 and G_1 . We will construct an adversary \mathcal{B}_F that distinguishes between the PRF Game₀ and Game₁ for F .



When \mathcal{B}_F is in Game_0 , it sends $F'_k(x_i) \oplus x_i$ to \mathcal{A}_{G_0, G_1} , exactly what it would expect to see in G_0 . When \mathcal{B}_F is in Game_1 it sends $T[x_i] \oplus x_i$ to \mathcal{A}_{G_0, G_1} (where T is the “table implementation” of a random function), exactly what it would expect to see in G_1 .

Therefore, the advantage of \mathcal{A}_{G_0, G_1} is exactly equal to the advantage of \mathcal{B}_F , and so by the security of F the advantage of \mathcal{A}_{G_0, G_1} must be negligible.

We now define G_2 , where the output of the PRF is replaced with only the output of the random function. Note that G_2 is identical to the PRF Game_1 .



We know that the xor of random value with an adversarially chosen value is perfectly indistinguishable from a random value, and so

$$|\Pr[W_1] - \Pr[W_2]| = 0$$

for all adversaries.

We then have by the hybrid lemma that $|\Pr[W_0] - \Pr[W_2]| \leq \nu(\lambda)$ for some negligible function ν , and so F' is a secure PRF.

3 Proving a PRF Insecure

Let $\{F_k\}_{k \in \{0,1\}^\lambda}$, where $F_k : \{0,1\}^\lambda \rightarrow \{0,1\}^\lambda$ be a secure PRF. We will prove that $F'_{k_1||k_2}(x_1||x_2) := F_{k_1}(x_1) \oplus F_{k_2}(x_2)$ is *not* a secure PRF.

We will use the function $\text{Query}(x_i) \rightarrow y_i$ to indicate the ability of an adversary to issue queries to the PRF challenger in the PRF game. Consider the following PRF adversary $\mathcal{A}_{F'}$:

$\mathcal{A}_{F'}(1^\lambda)$
<hr/>
$y_1 \leftarrow \text{Query}(0^\lambda 0^\lambda)$
$y_2 \leftarrow \text{Query}(0^\lambda 1^\lambda)$
$y_3 \leftarrow \text{Query}(1^\lambda 0^\lambda)$
$y_4 \leftarrow \text{Query}(1^\lambda 1^\lambda)$
if $y_1 \oplus y_2 = y_3 \oplus y_4$ then return 0
else return 1

We now analyze the advantage of $\mathcal{A}_{F'}$. Let W_b be the event that \mathcal{A} outputs 0 in PRF Game_b. We begin by looking at W_0 (the game where the challenger responds to queries with $F'_{k_1||k_2}(x_1||x_2)$).

In Game₀ we have that $\Pr[W_0] = \Pr[y_1 \oplus y_2 = y_3 \oplus y_4]$. Then:

$$\begin{aligned} y_1 \oplus y_2 &= y_3 \oplus y_4 \\ F'_{k_1||k_2}(0^\lambda||0^\lambda) \oplus F'_{k_1||k_2}(0^\lambda||1^\lambda) &= F'_{k_1||k_2}(1^\lambda||0^\lambda) \oplus F'_{k_1||k_2}(1^\lambda||1^\lambda) \\ F_{k_1}(0^\lambda) \oplus F_{k_2}(0^\lambda) \oplus F_{k_1}(0^\lambda) \oplus F_{k_2}(1^\lambda) &= F_{k_1}(1^\lambda) \oplus F_{k_2}(0^\lambda) \oplus F_{k_1}(1^\lambda) \oplus F_{k_2}(1^\lambda) \\ F_{k_2}(0^\lambda) \oplus F_{k_2}(1^\lambda) &= F_{k_2}(0^\lambda) \oplus F_{k_2}(1^\lambda) \end{aligned}$$

and so $\Pr[W_0] = \Pr[y_1 \oplus y_2 = y_3 \oplus y_4] = \Pr[F_{k_2}(0^\lambda) \oplus F_{k_2}(1^\lambda) = F_{k_2}(0^\lambda) \oplus F_{k_2}(1^\lambda)] = 1$.

We now turn to W_1 . In this case, each y_i is a uniformly random value, as each is the result of a distinct query. Therefore, $\Pr[W_1] = \Pr[y_1 \oplus y_2 = y_3 \oplus y_4] = \frac{1}{2^\lambda}$.

We then have that, for $\mathcal{A}_{F'}$:

$$\begin{aligned} &|\Pr[W_0] - \Pr[W_1]| \\ &= \left| 1 - \frac{1}{2^\lambda} \right| \\ &= 1 - \frac{1}{2^\lambda} \end{aligned}$$

which is clearly not negligible in λ . Therefore, F' is not a secure PRF.