1 Hard Core Predicate

Let $f : \{0,1\}^n \to \{0,1\}^n$ be a OWF and $f' : \{0,1\}^{2n} \to \{0,1\}^{2n}$ be $s.t.$ for every $x \in \{0,1\}^{2n}$, $f'(x) = f(x[0:n]) \| x[n:2n]$. As has been proved in previous homework, we know f' is also a OWF [1].
Then we show

$$g(x,r) = (f'(x), r) = (f(x[0:n]) \| x[n:2n], r)$$

Now we can calculate the probability by

$$\begin{aligned}
\Pr\left[x \leftarrow \{0,1\}^{2n} : \mathcal{A}(1^n, f(x)) = h(x)\right] &= \Pr\left[x \leftarrow \{0,1\}^{2n}, b \leftarrow \{0,1\} : b = \langle x[0:n], r\rangle\right] && (1)\\
&= \frac{1}{2} && (2)
\end{aligned}$$

Therefore, we show that this does not satisfy the requirement for 2-bit hard core predicate.

2 Pseudorandom Functions

2.1 Counterexample

No, it is not.
We need to specify the Adversary A by

$$\begin{aligned}
&\underline{\mathcal{A}}: && (3)\\
&\quad y_1 \leftarrow \mathbf{f}_k\left(1^\ell\right) && (4)\\
&\quad y_2 \leftarrow \mathbf{f}_k\left(0^\ell\right) && (5)\\
&\quad \text{Parse } y_1 \text{ as } y_1 = y_{1,1} \| y_{1,2} \quad (|y_{1,1}| = |y_{1,2}| = l) && (6)\\
&\quad \text{Parse } y_2 \text{ as } y_2 = y_{2,1} \| y_{2,2} \quad (|y_{2,1}| = |y_{2,2}| = l) && (7)\\
&\quad \text{return 1 if } y_{1,1} = y_{2,2} \text{ else return 0} && (8)
\end{aligned}$$

Now we have

$$g_k(1^\ell) = f_k(1^\ell) \| f_k(0^\ell)$$

$$g_k(0^\ell) = f_k(0^\ell) \| f_k(1^\ell)$$

As in the adversary, it checks whether the first half of f_1 equals to the second half of f_2. If we generate a random 2l-bit, A will output 1 when the first half in the first string matches the second half of the second string ($y_{1,1} = y_{2,2}$), where both are l-bit long. For a random string, such probability should be 2^{-l}. Then we show:

$$\begin{aligned}
\Pr\left[\mathrm{Real}_G^A \Rightarrow 1\right] &= 1 && (9)\\
\Pr\left[\mathrm{Rand}_R^A \Rightarrow 1\right] &= 2^{-l} && (10)
\end{aligned}$$

Therefore, $\{g_k\}_k$ is not a family of PRFs.

2.2 Proof

Yes, it is.
Before we proceed the formal proof, we need to define a random function R by

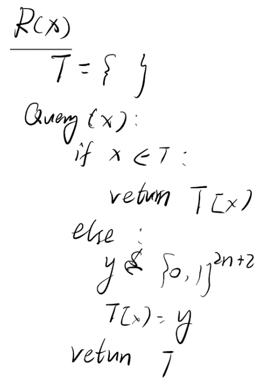

Figure 1: 2.2 Random

We now prove this via reduction. Let adversary A distinguish between $g_k(x)$ and $R(x)$, then we show there exists adversary B which builds upon A can break the PRF f_k. Now we show via reduction by

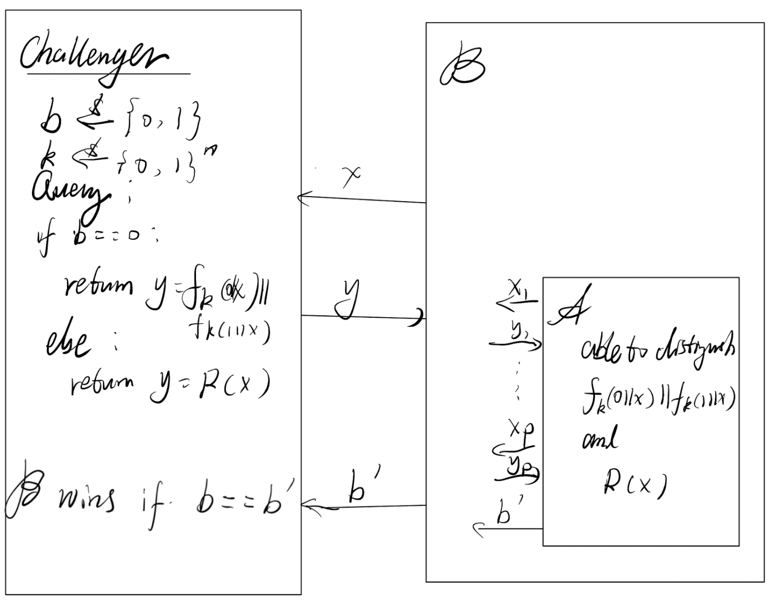

Figure 2: 2.2 Reduction

We show that B has the same advantage of breaking PRF f_k as A is able to distinguish between $g_k(x)$ and $R(x)$, where the assumption contradicts with the precondition that f_k is PRF. Therefore, there exists no adversary A such that A is able to distinguish between $g_k(x)$ and $R(x)$, which further proves that $\{g_k\}_k$ is a family of PRFs.

2.3 Reduction

Before we show formal proof, we firstly need to define the construction the random functions R_1 and R_2 by

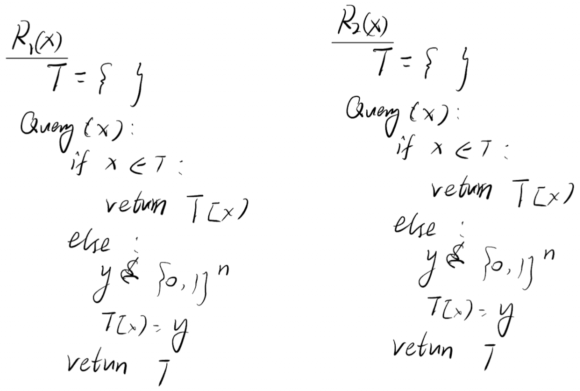

Figure 3: 2.3 Random

First, we show the hybrids by

$$\mathcal{H}_0 : \{g(f_k(x_1)), g(f_k(x_2)), \ldots, g(f_k(x_p))\}$$

$$\mathcal{H}_1 : \{g(R_2(x_1)), g(R_2(x_2)), \ldots, g(R_2(x_p))\}$$

$$\mathcal{H}_2 : \{R_1(x_1), g(R_2(x_2)), g(R_2(x_3)), \ldots, g(R_2(x_p))\}$$

$$\mathcal{H}_i : \{R_1(x_1), R_1(x_2), \ldots, R_1(x_{i-1}), g(R_2(x_i)), \ldots, g(R_2(x_p))\}$$

$$\mathcal{H}_{i+1} : \{R_1(x_1), R_1(x_2), \ldots, R_1(x_i), g(R_2(x_{i+1})), \ldots, g(R_2(x_p))\}$$

$$\mathcal{H}_p : \{R_1(x_1), R_1(x_2), \ldots, R_1(x_p)\}$$

In order to show $\{h_k\}_k$ is a family of PRFs, we need to show that $\mathcal{H}_0$ is indistinguishable from $\mathcal{H}_p$. Firstly, we need to prove $\mathcal{H}_0$ is indistinguishable from $\mathcal{H}_1$ on the PRF problem by assuming there exists adversary A such that could distinguish between them and then construct an adversary B which will break the security of PRF f_k. Then we show the following hybrids are indistinguishable between each other by reduction process on the PRG problem.
Let A distinguish between $\mathcal{H}_0$ and $\mathcal{H}_1$ with non-negligible advantage $\nu(n)$. Then we show the reduction by:

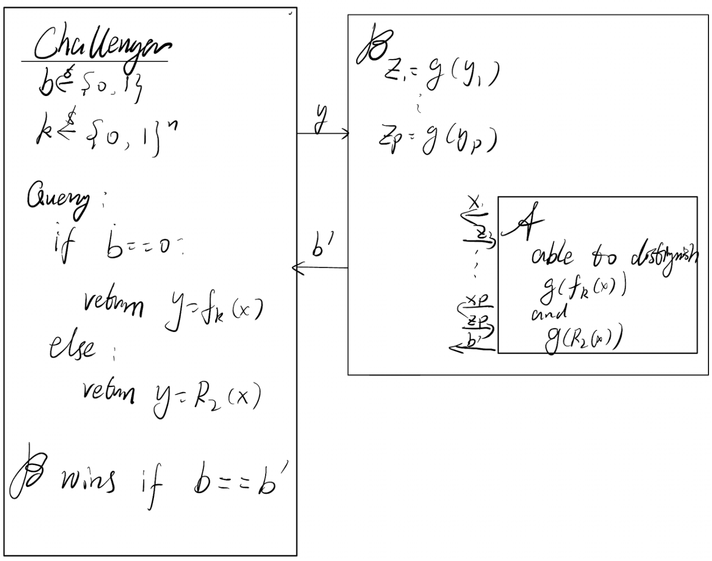

Figure 4: 2.3 Reduction I

We show that B has the same advantage of breaking PRF f_k as A is able to distinguish between $g(f_k(x))$ and $g(R_2(x))$, where the assumption contradicts with the precondition that f_k is PRF. Therefore, $\mathcal{H}_0$ and $\mathcal{H}_1$ are indistinguishable.
Let A_1 distinguish between $\mathcal{H}_1$ and $\mathcal{H}_2$ with non-negligible advantage $\nu_1(n)$. Then we show the reduction by:

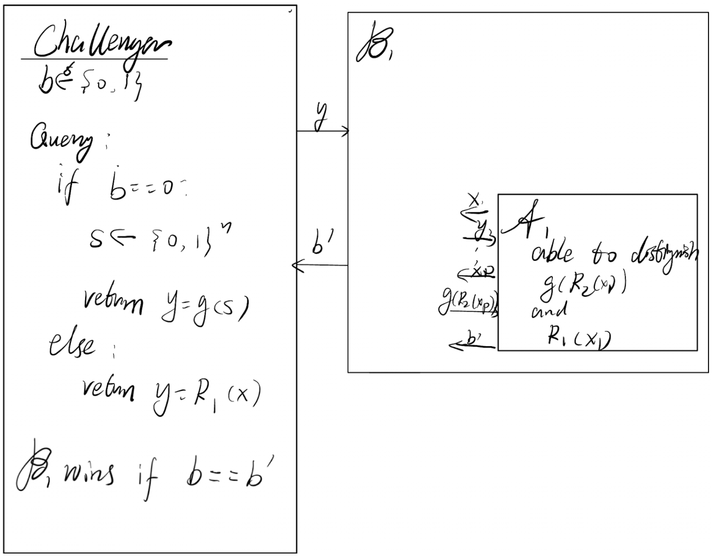

Figure 5: 2.3 Reduction II

We show that B_1 has the same advantage of breaking PRG g as A_1 is able to distinguish between $g(R_2(x_1))$ and $R_1(x_1)$, where the assumption contradicts with the precondition that g is PRG. Therefore, $\mathcal{H}_1$ and $\mathcal{H}_2$ are indistinguishable.
Let A_i distinguish between $\mathcal{H}_i$ and $\mathcal{H}_{i+1}$ with non-negligible advantage $\nu_i(n)$. Then we show the reduction by:

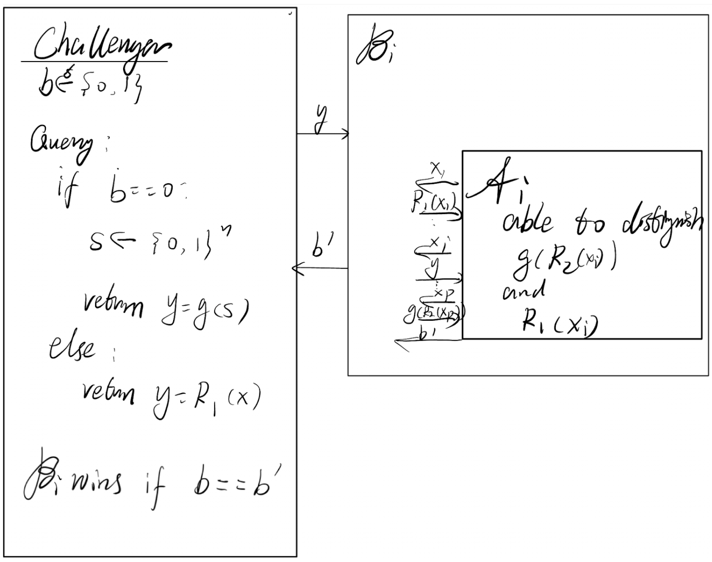

Figure 6: 2.3 Reduction III

Similar to what we explained in proving $\mathcal{H}_1$ and $\mathcal{H}_2$ are indistinguishable. We show that B_i has the same advantage of breaking PRG g as A_i is able to distinguish between $g(R_2(x_i))$ and $R_1(x_i)$, where the assumption contradicts with the precondition that g is PRG. Therefore, $\mathcal{H}_i$ and $\mathcal{H}_{i+1}$ are indistinguishable.
Up to now, we show $\mathcal{H}_0 \approx_c \mathcal{H}_1 \approx_c \ldots \approx_c \mathcal{H}_i \approx_c \mathcal{H}_{i+1}$. Therefore, there exists no adversary A such

that A is able to distinguish between $\mathcal{H}_0$ and $\mathcal{H}_p$ with non-negligible advantage, which further proves that $\{h_k\}_k$ is a family of PRFs.

3 Discrete Log

Since $X \in G$, we have $X = g^i$ where $i \in \mathbb{Z}_q$. And to solve the discrete log problem is equivalent to find such i.
Let $X' = g * X$, then we have

$$X = \frac{X'}{g}$$

Now we show that

$$\begin{aligned}
\log_g X &= \log_g \frac{X'}{g} && (11)\\
&= \log_g X' - \log_g g \quad \text{(Logarithm quotient rule)} && (12)\\
&= \log_g X' - 1 && (13)
\end{aligned}$$

Since the discrete log of X', $\log_g X'$ above, can be learned, we can also learn the discrete log of X by $\log_g X' - 1$.

4 Diffie Hellman

4.1 Explanation

The argument is very wrong. From the perspective of calculating product of exponentials, the result of $(g^a) \cdot (g^b)$ should be g^{a+b}. Also, this will not work in the context of DH key agreement process where we calculate the shared key with modulus. Besides, calculating $A \cdot B$ does not make sense. Therefore, the argument is totally wrong.

4.2 Proof

Consider the following hybrids, where $a_1, a_2, b, r_1, r_2 \xleftarrow{\$} \{0, ..., p-1\}$:

$$\begin{aligned}
\mathcal{H}_0 &= \{g, g^{a_1}, g^{a_2}, g^{a_1 \cdot b}, g^{a_2 \cdot b}\} && (14)\\
\mathcal{H}_1 &= \{g, g^{a_1}, g^{a_2}, g^{r_1}, g^{a_2 \cdot b}\} && (15)\\
\mathcal{H}_2 &= \{g, g^{a_1}, g^{a_2}, g^{r_1}, g^{r_2}\} && (16)
\end{aligned}$$

In order to prove the two distributions are indistinguishable, we need to show that $\mathcal{H}_0$ and $\mathcal{H}_2$ are indistinguishable. Firstly, we need to prove via reduction by assuming there exists adversary A_1 such that A_1 is able to distinguish between $\mathcal{H}_0$ and $\mathcal{H}_1$ with non-negligible advantage. Then, we show that we could construct another adversary B_1 such that B_1 is able to break DDH assumption. After that, we show similar process to prove the indistinguishability between H_1 and H_2.
Let A_1 distinguish between H_0 and H_1 with non-negligible advantage and we show via reduction by

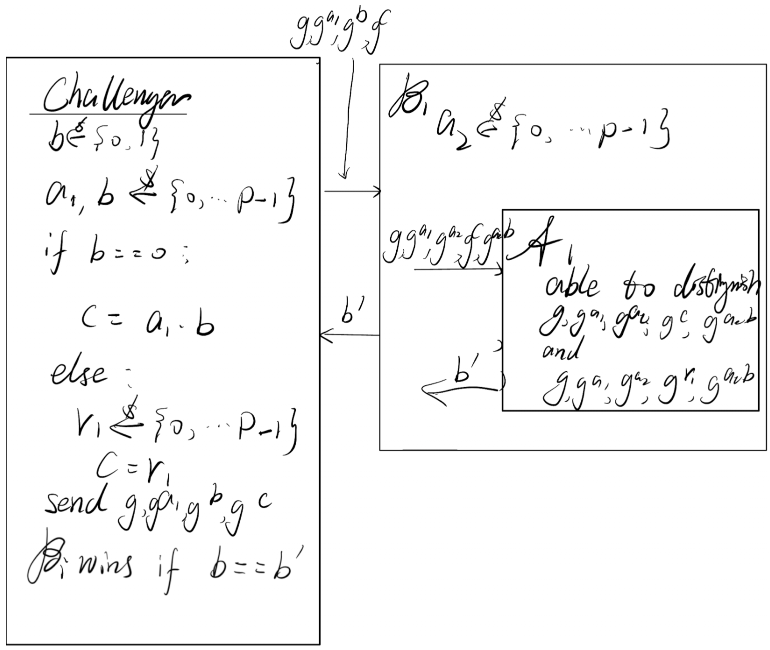

Figure 7: 4.2 Reduction I

We show that B_1 has the same advantage of breaking DDH assumption as A_1 is able to distinguish between $\mathcal{H}_0$ and $\mathcal{H}_1$, where the assumption contradicts with the DDH assumption. Therefore, $\mathcal{H}_0$ and $\mathcal{H}_1$ are indistinguishable.
Let $\mathcal{A}_2$ distinguish between $\mathcal{H}_1$ and $\mathcal{H}_2$ with some non-negligible advantage, based on which there is another adversary $\mathcal{B}_2$ that will break the DDH assumption.

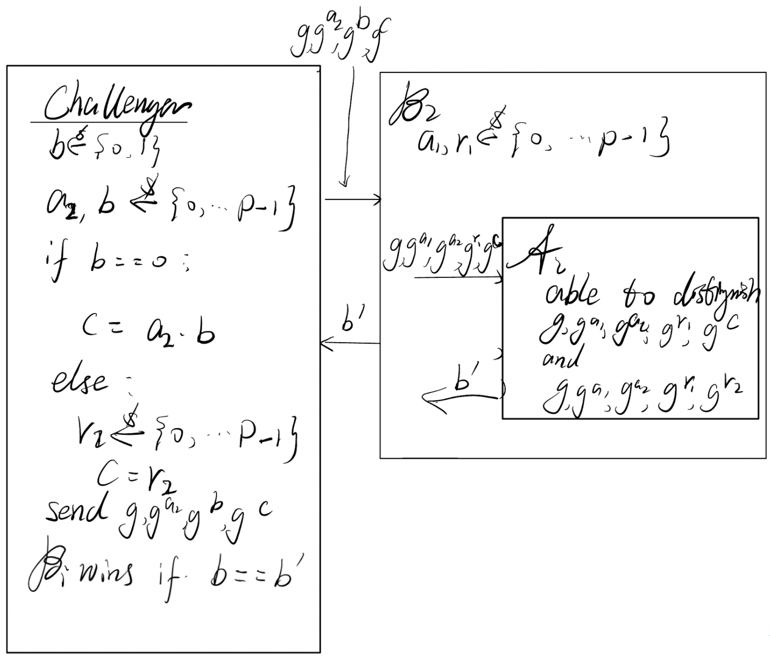

Figure 8: 4.2 Reduction II

We show that B_2 has the same advantage of breaking DDH assumption as A_2 is able to distinguish between $\mathcal{H}_1$ and $\mathcal{H}_2$, where the assumption contradicts with the DDH assumption. Therefore, $\mathcal{H}_1$ and $\mathcal{H}_2$ are indistinguishable.
Up to now, we show $\mathcal{H}_0 \approx_c \mathcal{H}_1 \approx_c \mathcal{H}_2$. Therefore, there exists no adversary A such that A is able to distinguish between $\mathcal{H}_0$ and $\mathcal{H}_2$ with non-negligible advantage, which further proves that D_1 and D_2

are indistinguishable under the DDH assumption

References

[1] Homework 2 Q4.1, https://github.com/heldridge/ModernCryptography-Fall2022/blob/main/homeworks/hw2.pdf