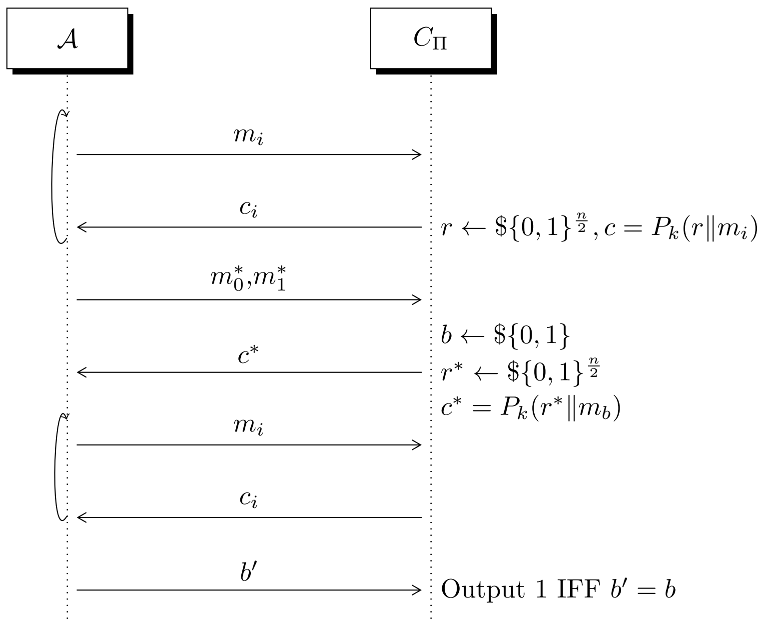
Contents

Chapter 1

Exercise 1

1.1 point a

Suppose we have the given scheme Π and the CPA game



If P is a PRP family, Π is always CPA secure unless a *bad event* happens.

Suppose m_0^* and m_1^* have already been sent multiple times to $\mathcal{C}_\Pi$ and that $\mathcal{A}$ collected , at most, *poly* couples containing (m_0^* or m_1^*, c'). It could happen that, sent m_0^* and m_1^* as challenge messages, $\mathcal{A}$ receives one of the previuosly received c'. In that case, $\mathcal{A}$ knows which message has been encrypted, then he can easily win the game.

What is the probability $\mathcal{A}$ can win in this way?
When $c^* = P_k(r^* \| m_b)$ where r^* was already chosen by $\mathcal{C}$ in a previuos request

of m_b (where b can be 0 or 1), $\mathcal{A}$ can win. Let's call r_b a random number chosen when m_b was sent to $\mathcal{C}$:

$$\begin{aligned}\mathcal{P}[wins] = \mathcal{P}[r^* = r_b \wedge m_b \text{ is chosen for encryption }] = \\ = \mathcal{P}[m_b]\mathcal{P}[r^* = r_b] = \\ = \frac{1}{2}\frac{1}{2^{\frac{n}{2}}}(\text{for } m_b \text{ asked just once}) \\ = \frac{1}{2}\frac{q}{2^{\frac{n}{2}}}(\text{for } m_b \text{ asked q times})\end{aligned}$$

Since $b \leftarrow \$\{0,1\}$ and $\mathcal{P}[r^* = r_0 \wedge m_0$ is chosen for encryption] and $\mathcal{P}[r^* = r_1 \wedge m_1$ is chosen for encryption] are disjoint probabilities, the probabilities of the two events is the sum of single probabilities.

So, $\mathcal{A}$ wins with probability at least $\frac{1}{2^{\frac{n}{2}}}$, at most $\frac{q}{2^{\frac{n}{2}}}$, which is still negligible since q can be , at most, *poly*.

1.2 point b

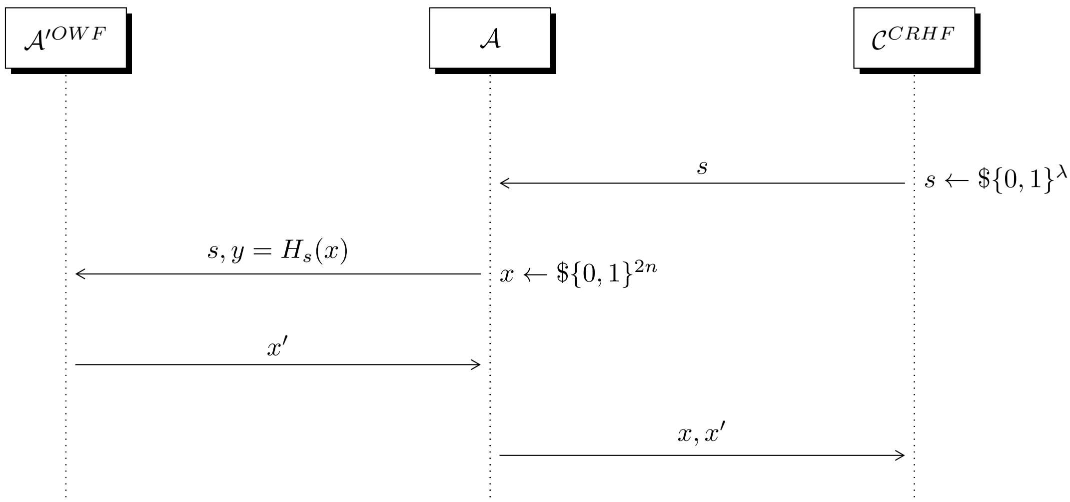
Exercise 2

1.3 point a

1.3.1 i

$$\mathcal{H} \text{ is CRHF } \Rightarrow \mathcal{H} \text{ is OWF}$$

To show this property, let's make a reduction:



When does not $\mathcal{A}$ win?
Since CRHF game wants the final couple (x, x') with $x \neq x'$, if $\mathcal{A}'^{OWF}$ returns $x' = x$ the CRHF game doesn't work.

This **BAD** event happens with

$$\mathcal{P}[x = x'] = Col(X, X') = \sum_x \mathcal{P}[X = x \wedge X' = x] = \sum_x \mathcal{P}[X = x]\mathcal{P}[X' = x] = \frac{1}{2^{2n}}$$

.

1.3.2 ii

If functions from $\mathcal{H}$ family aren't compressing, the probability of **BAD** event changes:

$$\mathcal{P}[x = x'] = Col(X, X') = \sum_x \mathcal{P}[X = x \wedge X' = x] = \sum_x \mathcal{P}[X = x]\mathcal{P}[X' = x] = \frac{1}{2^n}$$

.

Now, if our functions from $\mathcal{H}$ were compressing (from 2n bits to n bits), the best CRHF function (the function with the minimum number of collisions) had $2^n + 1$ inputs generating a collision (in the same codomain's element).

In this case, the best possible CRHF function is bijective (since it could be a permutation over 2^n elements).

In general, for non-compressing functions we can show that

$$\mathcal{H} \text{ is CRHF mapping n bits to n bits} \Rightarrow \mathcal{H} \text{ is OWF}$$

with the same reduction of the above **point i** .