

## Problem 1

Let  $G : \{0, 1\}^n \rightarrow \{0, 1\}^{2n}$  be a pseudorandom generator. Let  $s \xleftarrow{\$} \{0, 1\}^n, r \xleftarrow{\$} \{0, 1\}^{2n}$  and  $y = G(s)$ . Consider the function  $P_{r,y}$  defined by:

1. On input  $x \in \{0, 1\}^n$ , check that  $G(x) \oplus r = y$ .
2. If true output 1; otherwise, output 0.

Show for any PPT  $\mathcal{A}$  with input  $(r, y)$  and output  $x \in \{0, 1\}^n$ ,

$$\Pr[P_{r,y}(x) = 1 : x \leftarrow \mathcal{A}(r, y)] \leq \nu(n).$$

**Solution:** Consider the following sequence of manipulations:

$$\begin{aligned}
 & \Pr[P_{r,y}(x) = 1 : x \leftarrow \mathcal{A}(r, y), r \leftarrow \{0, 1\}^{2n}, y \leftarrow G(s), s \leftarrow \{0, 1\}^n] \\
 &= \Pr[G(x) \oplus r = y : x \leftarrow \mathcal{A}(r, y), r \leftarrow \{0, 1\}^{2n}, y \leftarrow G(s), s \leftarrow \{0, 1\}^n] \\
 &= \Pr[G(x) \oplus r = G(s) : x \leftarrow \mathcal{A}(r, G(s)), r \leftarrow \{0, 1\}^{2n}, s \leftarrow \{0, 1\}^n] \\
 &= \Pr[G(x) = r \oplus G(s) : x \leftarrow \mathcal{A}(r, G(s)), r \leftarrow \{0, 1\}^{2n}, s \leftarrow \{0, 1\}^n] \\
 &= \Pr[G(x) = r \oplus a : x \leftarrow \mathcal{A}(r, a), r \leftarrow \{0, 1\}^{2n}, a \leftarrow \{0, 1\}^{2n}] \\
 &= \Pr[G(x) = r \oplus a : x \leftarrow \mathcal{A}(r \oplus a, a), r \leftarrow \{0, 1\}^{2n}, a \leftarrow \{0, 1\}^{2n}] \\
 &= \Pr[G(x) = b : x \leftarrow \mathcal{A}(b, a), b \leftarrow \{0, 1\}^{2n}, a \leftarrow \{0, 1\}^{2n}] \\
 &= \Pr[G(x) = G(d) : x \leftarrow \mathcal{A}(G(d), a), d \xleftarrow{\$} \{0, 1\}^{2n}, a \xleftarrow{\$} \{0, 1\}^{2n}] \Pr[b \in G(\{0, 1\}^{2n}) : b \xleftarrow{\$} \{0, 1\}^{2n}] \\
 &\quad + 0 \cdot \Pr[b \notin G(\{0, 1\}^{2n}) : b \xleftarrow{\$} \{0, 1\}^{2n}] \\
 &\leq \Pr[G(x) = G(d) : x \leftarrow \mathcal{A}(G(d), a), d \xleftarrow{\$} \{0, 1\}^{2n}, a \xleftarrow{\$} \{0, 1\}^{2n}] \\
 &= \Pr[G(\mathcal{A}(G(d), a)) = G(d) : d \xleftarrow{\$} \{0, 1\}^{2n}, a \xleftarrow{\$} \{0, 1\}^{2n}] \\
 &\leq \nu(n),
 \end{aligned}$$

where  $\nu(n)$  is a negligible function. Notice we used the fact that  $G$  is a one-way function because it's a pseudorandom generator. Further, we equated  $\mathcal{A}(r, a)$  and  $\mathcal{A}(r \oplus a, a)$ , since the adversary  $\mathcal{A}$  can recover  $r$  with  $(r \oplus a) \oplus a$ . Therefore, we have that for any PPT  $\mathcal{A}$  with input  $(r, y)$  and output  $x \in \{0, 1\}^n$ , we have

$$\Pr[P_{r,y}(x) = 1 : x \leftarrow \mathcal{A}(r, y)] \leq \nu(n).$$