3 PRP versus Left-or-Right

Given a security parameter (which is implicit and omitted from notations for better readability), we consider a pair $(\mathsf{Enc}, \mathsf{Dec})$ of functions from $\{0,1\}^k \times \{0,1\}^n$ to $\{0,1\}^n$ (k and n are functions of the security parameter). These functions are such that for all K and X, we have

$$\mathsf{Dec}(K, \mathsf{Enc}(K, X)) = X$$

It is assumed that there are implementations which can evaluate both functions in polynomial time complexity (in terms of the security parameter). We define several security notions.

PRP. We say that this pair is a *pseudorandom permutation* (PRP) if there exists a negligible function negl such that for all probabilistic polynomial time (PPT) algorithm $\mathcal{A}$, we have $\Pr[\Gamma^{\mathsf{PRP}}(\mathcal{A}, 0) \to 1] - \Pr[\Gamma^{\mathsf{PRP}}(\mathcal{A}, 1) \to 1] \leq \mathsf{negl}$, where $\Gamma^{\mathsf{PRP}}(\mathcal{A}, b)$ is the PRP game defined as follows:

$\Gamma^{\mathsf{PRP}}(\mathcal{A}, b)$:
- initialize a list $\mathcal{L}$ to empty
- pick $K \in \{0,1\}^k$ uniformly at random
- pick a permutation Π over $\{0,1\}^n$ uniformly at random
- run $b' \leftarrow \mathcal{A}^{\mathcal{O}}$
- return b'

subroutine $\mathcal{O}(x)$:
- if $x \in \mathcal{L}$ abort
- insert x in $\mathcal{L}$
- **if** $b = 0$ **then**
  - return $\mathsf{Enc}(K, x)$
- **else**
  - return $\Pi(x)$
- **end if**

LoR. We say that this pair is *LoR-secure* if there exists a negligible function negl such that for all probabilistic polynomial time (PPT) algorithm $\mathcal{A}$, we have $\Pr[\Gamma^{\mathsf{LoR}}(\mathcal{A}, 0) \to 1] - \Pr[\Gamma^{\mathsf{LoR}}(\mathcal{A}, 1) \to 1] \leq \mathsf{negl}$, where $\Gamma^{\mathsf{LoR}}(\mathcal{A}, b)$ is the left-or-right game defined as follows:

$\Gamma^{\mathsf{LoR}}(\mathcal{A}, b)$:
- initialize two lists $\mathcal{L}_l$ and $\mathcal{L}_r$ to empty
- pick $K \in \{0,1\}^k$ uniformly at random
- run $b' \leftarrow \mathcal{A}^{\mathcal{O}}$
- return b'

subroutine $\mathcal{O}(x_l, x_r)$:
- if $x_l \in \mathcal{L}_l$ or $x_r \in \mathcal{L}_r$, abort
- insert x_r in $\mathcal{L}_l$ and x_r in $\mathcal{L}_r$
- **if** $b = 0$ **then**
  - return $\mathsf{Enc}(K, x_l)$

else
  return $\mathsf{Enc}(K, x_r)$
end if

We want to show the equivalence between these notions.

Q.1 Is the list management important in each security definition (or: what happens with modified definitions in which we remove the lists)? Justify your answer.

Q.2 We consider the following hybrid game:

$\Gamma^{\mathsf{hyb}}(\mathcal{A}, b)$:
initialize a list $\mathcal{L}$ to empty
pick $K \in \{0,1\}^k$ uniformly at random
pick a permutation Π over $\{0,1\}^n$ uniformly at random
run $b' \leftarrow \mathcal{A}^{\mathcal{O}}$
return b'

subroutine $\mathcal{O}(x)$:
if $x \in \mathcal{L}$ abort
insert x in $\mathcal{L}$
if $b = 0$ **then**
  return $\mathsf{Enc}(K, x)$
else
  return $\mathsf{Enc}(K, \Pi(x))$
end if

Show that for all $\mathcal{A}$ playing the PRP game and any b, we have $\Pr[\Gamma^{\mathsf{PRP}}(\mathcal{A}, b) \to 1] = \Pr[\Gamma^{\mathsf{hyb}}(\mathcal{A}, b) \to 1]$.

Q.3 Given $\mathcal{A}$ playing the PRP game, we define $\mathcal{B}$ playing the LoR game as follows:

$\mathcal{B}^{\mathcal{O}}$:
pick a permutation Π over $\{0,1\}^n$ uniformly at random
run $\mathcal{A}$
  when $\mathcal{A}$ makes a query x to its oracle, answer by $\mathcal{O}(x, \Pi(x))$
return the same output as $\mathcal{A}$

Show that $\Pr[\Gamma^{\mathsf{hyb}}(\mathcal{A}, b) \to 1] = \Pr[\Gamma^{\mathsf{LoR}}(\mathcal{B}, b) \to 1]$ for any b.

Q.4 Deduce that LoR-security implies PRP.
CAUTION: adversaries must be PPT.

Q.5 Using the following game, show that PRP security implies LoR security. Give a precise proof with the reductions.

$\Gamma^{\mathsf{generic}}(\mathcal{A}, b, c)$:
initialize two lists $\mathcal{L}_l$ and $\mathcal{L}_r$ to empty
pick $K \in \{0,1\}^k$ uniformly at random
pick a permutation Π over $\{0,1\}^n$ uniformly at random
run $b' \leftarrow \mathcal{A}^{\mathcal{O}}$
return b'

subroutine $\mathcal{O}(x_l, x_r)$:

```
if $x_l \in \mathcal{L}_l$ or $x_r \in \mathcal{L}_r$, abort
insert $x_r$ in $\mathcal{L}_l$ and $x_r$ in $\mathcal{L}_r$
if $b = 0$ then
    if $c = 0$ then
        return $\mathsf{Enc}(K, x_l)$
    else
        return $\Pi(x_l)$
    end if
else
    if $c = 0$ then
        return $\mathsf{Enc}(K, x_r)$
    else
        return $\Pi(x_r)$
    end if
end if
```