Pseudo-Random Function (PRF)

A function F: $\mathcal{K}\times\mathcal{X}\rightarrow\mathcal{Y}$ such that:

1. $\forall\, k \in \mathcal{K}, x \in \mathcal{X}$, ∃ a PPT algorithm that (efficiently) computes $F_k(x)$ *(efficiency)*
2. ∀ algorithm PPT $\mathcal{D}$, ∃ $\varepsilon(n)$ negligible such that

$$\mathrm{Adv}^{\mathrm{PRF}}_{\mathcal{D},F}(n) = |\Pr[\mathcal{D}(f) = 1] - \Pr[\mathcal{D}(F_k(.)) = 1]| \leq \varepsilon(n)$$

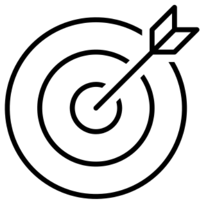
where $f \leftarrow^{R} \mathrm{Func}(\mathcal{X}, \mathcal{Y})$ and $k \leftarrow^{R} \mathcal{K}$ *(pseudo-randomness)*

Pseudo-Random Permutation (PRP)

A bijection F: $\mathcal{X}\times\mathcal{K}\rightarrow\mathcal{X}$, with F PRF

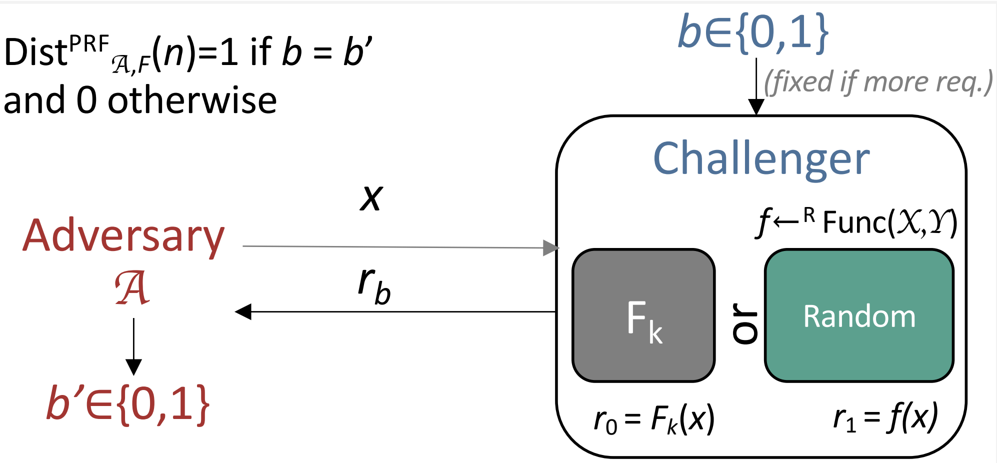
$(\mathcal{Y} = \mathcal{X})$

$\mathcal{D}$: distinguisher
$\mathcal{D}()$ output: 0 = not random, 1 = random
PPT: Probabilistic Polynomial in Time
$\mathrm{Func}(\mathcal{X}, \mathcal{Y})$: the set of all functions from $\mathcal{X}$ to $\mathcal{Y}$, $\mathcal{K}=\{0,1\}^n$
$f \leftarrow^{R} \mathrm{Func}(\mathcal{X}, \mathcal{Y})$: f is random function in $\mathrm{Func}(\mathcal{X}, \mathcal{Y})$
$k \leftarrow^{R} \mathcal{K}$: k is random key



Indistinguishability from random functions / permutations

$\mathrm{Dist}^{\mathrm{PRF}}_{\mathcal{A},F}(n)=1$ if $b = b'$ and 0 otherwise



F is PRF if $\forall\mathcal{A}$ PPT, ∃ $\varepsilon(n)$ negligible such that:

$$\Pr[\mathrm{Dist}^{\mathrm{PRF}}_{\mathcal{A},F}(n)=1] \leq ½ + \varepsilon(n)$$