F
D
R
Pseudorandomness.
$\mathcal{A}$
$$= \Pr\left[b = b' : \begin{array}{l} pp \leftarrow \mathsf{Setup}(1^\lambda); \\ k \leftarrow \mathsf{KeyGen}(pp); \\ b \leftarrow \{0,1\}; \\ b' \leftarrow \mathcal{A}^{\mathcal{O}_{\mathsf{ror}}(b,\cdot)}(\lambda); \end{array}\right] - \frac{1}{2},$$
$\mathcal{O}_{\mathsf{ror}}(0, x) =$
$F_k(x)$
$\mathcal{O}_{\mathsf{ror}}(1, x) =$
$\mathsf{H}(x)$
H
D
R^1
$\mathcal{A}$
$\mathcal{O}_{\mathsf{ror}}(b, \cdot)$
F
λ
weak pseudorandomness
$\mathcal{O}_{\mathsf{ror}}(b, \cdot)$
D
$\mathcal{A}$
weak PRFs
Composable.
F
F
$R \subseteq$
D
$k_1, k_2 \in$
K
$F_{k_1}(F_{k_2}(\cdot))$
$R =$
D
Commutative.
$\forall k_1, k_2 \in$
$K, \forall x \in$
$X :$
$F_{k_1}(F_{k_2}(x)) =$
$F_{k_2}(F_{k_1}(x))$
F_k
$\mathcal{A}$
$k' K$

To efficiently simulate access to a uniformly random function H from D to R, one may think of a process in which the adversary's