$F:$
$\{0,1\}^n\times$
$\{0,1\}^n\rightarrow$
$\{0,1\}^n$
D
$|\Pr[D^{F_k(\cdot)}(1^n)=1]{-}\Pr[D^{f(\cdot)}(1^n)=1]|\leq(n)$

$k\leftarrow$
$\{0,1\}^n$
$f\leftarrow_n$
n
$\{0,1\}^n\rightarrow$
$\{0,1\}^n$
n
$|_n|$
$2^{n\cdot 2^n}$
$\{0,1\}^n$
2^n
$\{0,1\}^n$
2^n
2^n
2^n
$(2^n)^{2^n}=2^{2\cdot 2^n}.$

D
$F(\cdot)$
$F(\cdot)$
$F_k(\cdot)$
$f(\cdot)$
D
$_distinguisher.jpg$
$_construction.jpg$
F
$\Pi=$
$(,,)$
(1^n)
$k\in$
$\{0,1\}^n$
(k,m)
$m\in$
$\{0,1\}^n$
$r\in$
$\{0,1\}^n$
$s=$
$F_k(r)\oplus$
m
$c=$
(r,s)
(k,c)
$c=$
(r,s)
$m=$
$F_k(r)\oplus$
s
F
Π
Π
F
$\widetilde{\Pi=}$
$(,,)$
D
A

$$\Pr[D^{F_k(\cdot)}(1^n)=1]=\Pr[PrivK^{cpa}_{A,\Pi}(n)=1]$$

$$\Pr[D^{f(\cdot)}(1^n)=1]=\Pr[PrivK^{cpa}_{A,\widetilde{\Pi}}(n)=1]$$

$$|\Pr[D^{F_k(\cdot)}(1^n)=1]{-}\Pr[D^{f(\cdot)}(1^n)=1]|\leq(n)$$

$\Pr[PrivK^{cpa}_{A,\widetilde{\Pi}}(n)=$
$1]=$
$?$
r^*
$\Pr[A^{case1}_{win}]=$
$\frac{1}{2}$
$_CPA-$
$secure_case1.jpg$
r^*
$\Pr[A^{case2}_{win}]=$
1
$_CPA-$
$secure_case2.jpg$
$Repeat$
r^*
$\Pr[PrivK^{cpa}_{A,\widetilde{\Pi}(n)=1]=\Pr[PrivK^{cpa}_{A,\widetilde{\Pi}}(n)=1\wedge Repeat]+\Pr[PrivK^{cpa}_{A,\widetilde{\Pi}}(n)=1\wedge\neg Repeat]\leq\Pr[Repeat]+\Pr[PrivK^{cpa}_{A,\widetilde{\Pi}}(n)=1\wedge\neg Repeat]=\frac{q(n)}{2^n}+\frac{1}{2}=(r}}$