Recap

PRG: $G: \{0,1\}^n \to \{0,1\}^{\ell(n)}$

$$\forall PPT\ \mathcal{D},\ \left| \Pr_{s \xleftarrow{\$} \{0,1\}^n}[\mathcal{D}(G(s))=1] - \Pr_{r \xleftarrow{\$} \{0,1\}^{\ell(n)}}[\mathcal{D}(r)=1] \right|$$

COTP(m,k): $c = G(k) \oplus m$ $\leq negl(n)$

↳ IND-EAV secure but not IND-CPA secure.

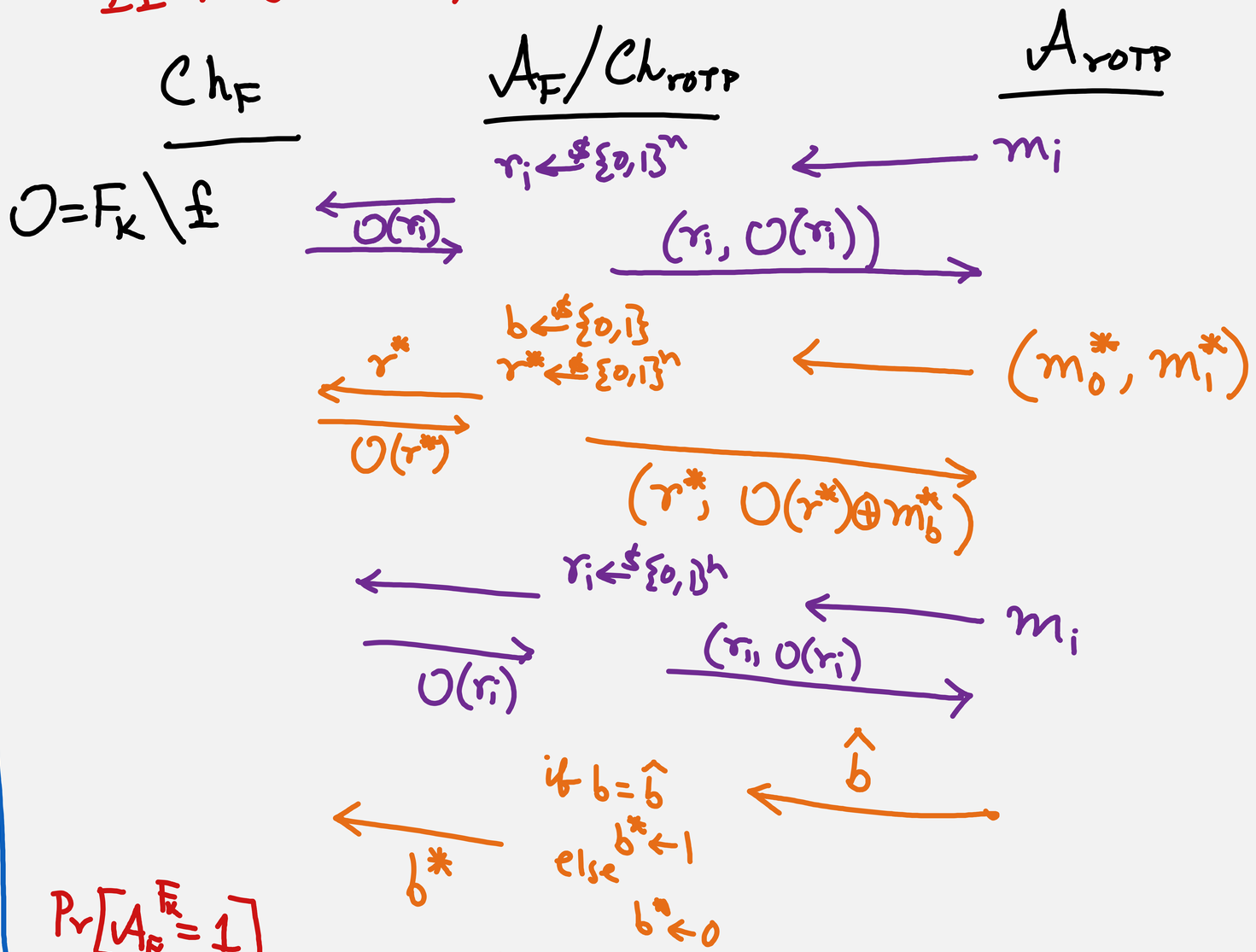
PRF: $F: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$

$$\forall PPT\ \mathcal{D},\ \left| \Pr_{k \leftarrow K_\lambda}[\mathcal{D}^{F_k(\cdot)}=1] - \Pr_{f \leftarrow Func_n}[\mathcal{D}^{f(\cdot)}=1] \right| \leq negl(n)$$

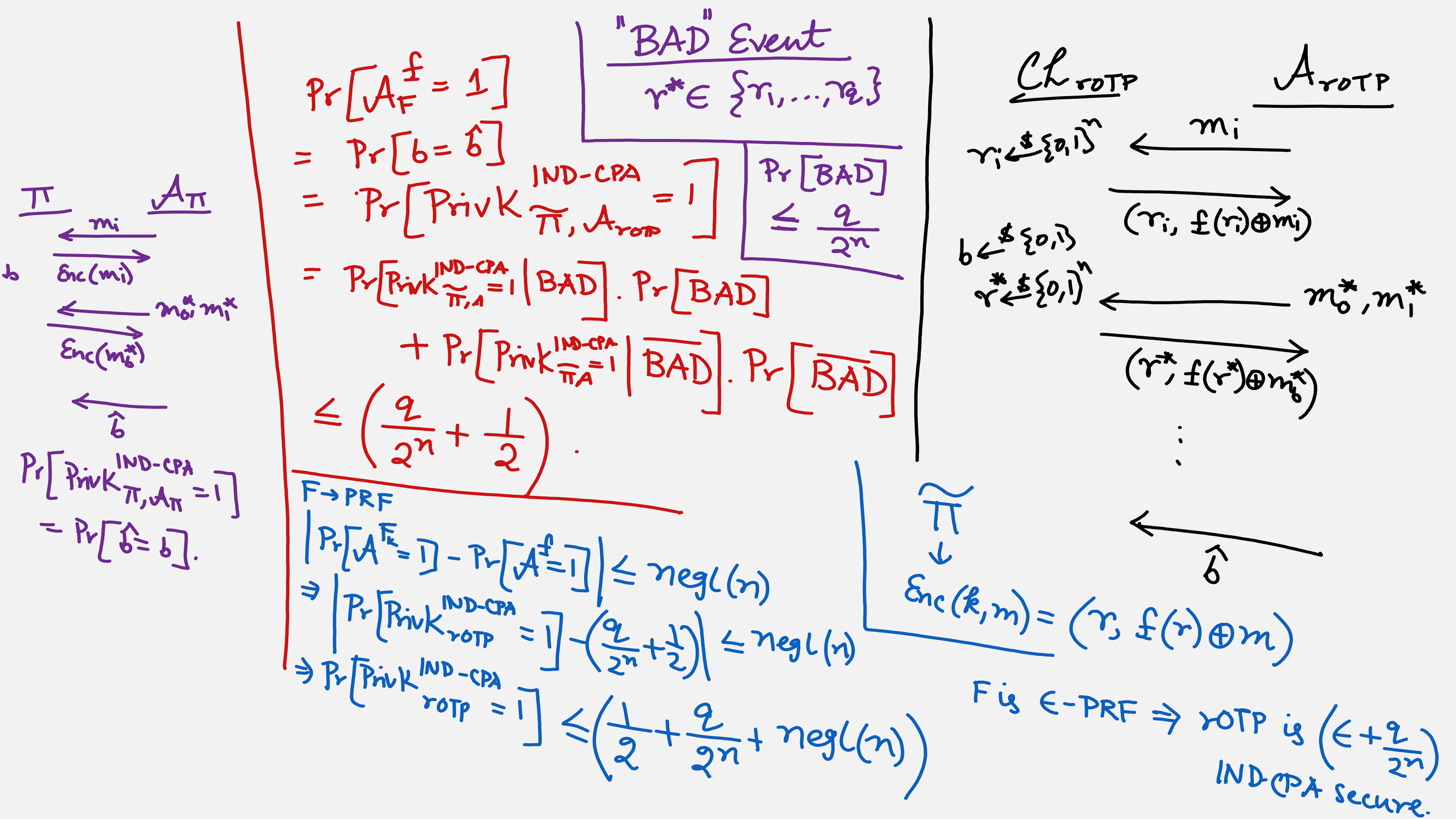
rOTP(m,k): $r \xleftarrow{\$} \{0,1\}^n$, $(c_1, c_2) \leftarrow (r, F_k(r) \oplus m)$.

→ F is PRF ⇒ rOTP IND-CPA secure

If F is a PRF, rOTP is IND-CPA Secure



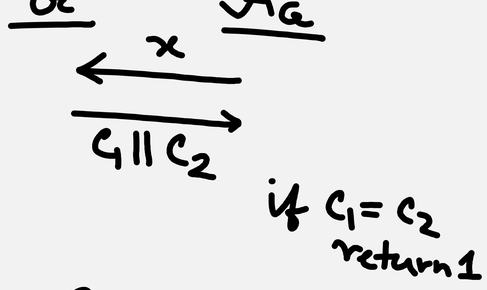
$$\Pr[\mathcal{A}_F^{F_k}=1] = \Pr[b=\hat{b}] \simeq \Pr[PrivK^{IND\text{-}CPA}_{rOTP, \mathcal{A}_{rOTP}}=1]$$


"BAD" Event
$r^* \in \{r_1, \ldots, r_q\}$
$\Pr[BAD] \le \frac{q}{2^n}$
$\Pr[A_F^f = 1]$
$= \Pr[b = \hat{b}]$
$= \Pr[PrivK^{IND\text{-}CPA}_{\tilde{\pi}, A_{rOTP}} = 1]$
$= \Pr[PrivK^{IND\text{-}CPA}_{\tilde{\pi},A} = 1 \mid BAD] \cdot \Pr[BAD]$
$+ \Pr[PrivK^{IND\text{-}CPA}_{\tilde{\pi}A} = 1 \mid \overline{BAD}] \cdot \Pr[\overline{BAD}]$
$\le \left(\frac{q}{2^n} + \frac{1}{2}\right)$.
π
A_π
m_i
b
$Enc(m_i)$
m_0^*, m_1^*
$Enc(m_b^*)$
$\hat{b}$
$\Pr[PrivK^{IND\text{-}CPA}_{\pi, A_\pi} = 1]$
$= \Pr[\hat{b} = b]$.
Ch_{rOTP}
A_{rOTP}
$r_i \xleftarrow{\$} \{0,1\}^n$
m_i
$(r_i, f(r_i) \oplus m_i)$
$b \xleftarrow{\$} \{0,1\}$
$r^* \xleftarrow{\$} \{0,1\}^n$
m_0^*, m_1^*
$(r^*, f(r^*) \oplus m_b^*)$
$\hat{b}$
$F \to PRF$
$\left|\Pr[A^{F_k} = 1] - \Pr[A^f = 1]\right| \le negl(n)$
$\Rightarrow \left|\Pr[PrivK^{IND\text{-}CPA}_{rOTP} = 1] - \left(\frac{q}{2^n} + \frac{1}{2}\right)\right| \le negl(n)$
$\Rightarrow \Pr[PrivK^{IND\text{-}CPA}_{rOTP} = 1] \le \left(\frac{1}{2} + \frac{q}{2^n} + negl(n)\right)$
$\tilde{\pi}$
$Enc(k, m) = (r, f(r) \oplus m)$
F is ϵ-PRF $\Rightarrow$ rOTP is $\left(\epsilon + \frac{q}{2^n}\right)$ IND-CPA secure.

Some Problems on PRF

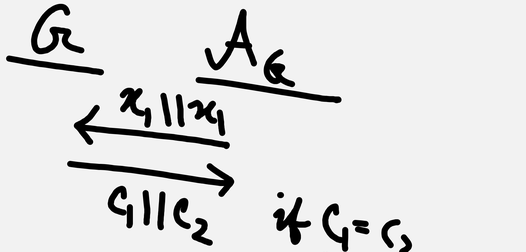
Let $F: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a PRF. Are the following functions PRF?

1. $G_k(x) = F_k(x) \| F_k(x)$ $\Rightarrow$

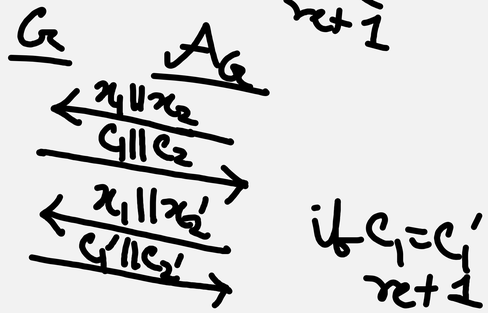


$$Pr\left[A_G^G = 1\right] - Pr\left[A_G^{\$} = 1\right] = 1 - \frac{1}{2^n}$$

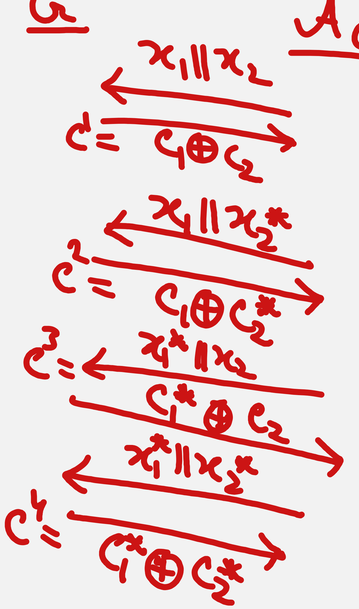
2. $G_k(x_1 \| x_2) = F_k(x_1) \| F_k(x_2)$ $\Rightarrow$



3. $G_{k_1,k_2}(x_1 \| x_2) = F_{k_1}(x_1) \| F_{k_2}(x_2)$ $\Rightarrow$



4. $G_{k_1,k_2}(x_1 \| x_2) = F_{k_1}(x_1) \oplus F_{k_2}(x_2)$



If $c^1 \oplus c^2 \oplus c^3 \oplus c^4 = 0$ ret 1

O/W —

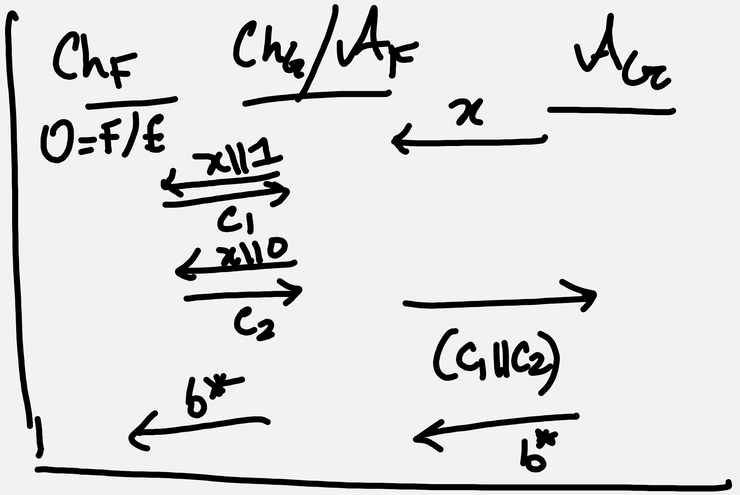
⑤ $G_K(x) = F_K(x \| 1) \| F_K(x \| 0)$

$G: \{0,1\}^{n-1} \times \{0,1\}^n \to \{0,1\}^{2n}$

⑥ $G_K(x) = F_K(x \| 1) \| F_K(0 \| x)$

(*) ⑦ $G_K(x) = F_K(x \| 1) \oplus F_K(0 \| x)$

$\Rightarrow$ (PRF)



$x = 0^{n-2}1$

$c_1 \| c_2$

$F_K(0^{n-2}11) \| F_K(0^{n-1}1)$

$x = 0^{n-3}11$

$c_1' \| c_2'$

$F_K(0^{n-3}111) \| F_K(0^{n-2}11)$

if $c_1 = c_2'$

$n+1$