Game $\mathrm{KR}_{\Sigma}^{Alice}$

$K \leftarrow\!\!\$\ \boldsymbol{K}$

$K' \leftarrow\!\!\$\ \boldsymbol{K'}$

$\sigma \leftarrow \epsilon$

$K_0 \leftarrow\!\!\$\ Alice^{\mathtt{Enc}}(K')$

Return $(K = K_0)$

procedure $\mathtt{Enc}(M)$

$(C, \sigma) \leftarrow\!\!\$\ \boldsymbol{E'}(K', K, M, \sigma)$

Return C

Game $\mathrm{SDET}_{\Pi,\Sigma}^{Bob}$

$b \leftarrow\!\!\$\ \{0, 1\}$

$K' \leftarrow\!\!\$\ \boldsymbol{K'}$

$\sigma \leftarrow \epsilon$

$b' \leftarrow\!\!\$\ Bob^{\mathtt{Enc}}$

Return $(b = b')$

procedure $\mathtt{Enc}(K, M)$

If $(b = 1)$ then $(C, \sigma) \leftarrow\!\!\$\ \boldsymbol{E}(K, M, \sigma)$

Else $(C, \sigma) \leftarrow\!\!\$\ \boldsymbol{E'}(K', K, M, \sigma)$

Return (C, σ)

$$\mathbf{Adv}_{\Sigma}^{\mathrm{kr}}(Alice) = \Pr[\mathrm{KR}_{\Sigma}^{Alice} \Rightarrow \mathrm{true}]$$

$$\mathbf{Adv}_{\Pi,\Sigma}^{\mathrm{sdet}}(Bob) = 2\Pr[\mathrm{SDET}_{\Pi,\Sigma}^{Bob} \Rightarrow \mathrm{true}] - 1$$

$$\mathbf{Adv}_{\Pi,\Sigma}^{\mathrm{surv}}(Alice) = 1$$

$$\mathbf{Adv}_{\Pi,\Sigma}^{\mathrm{det}}(Bob) \leq \frac{q^2}{2^{n-l-1}} + \mathbf{Adv}_{\boldsymbol{B}}^{\mathrm{prf}}(Bob\text{-}PRF)$$

$$\mathbf{Adv}_{\Pi,\Sigma}^{\mathrm{det}}(Bob) \leq \frac{q^2}{2^{(2^r)}} + \mathbf{Adv}_{\boldsymbol{F}}^{\mathrm{prf}}(Bob\text{-}PRF)$$

$$\mathbf{Adv}_{\Sigma}^{\mathrm{kr}}(Alice) + \mathbf{Adv}_{H}^{\mathrm{prf}}(Alice\text{-}PRF) \geq 1 - \delta(q, s, n)$$

$$2^{-\mathbf{H}_{\infty}(\boldsymbol{E})} = \max_{K,M,C} \Pr[E(K, M) =_{\$} C]$$

$$\delta(q, s, n) \leq ne^{-\frac{q}{n}} + q2^{-s} + (q^2 s^2)2^{-\mathbf{H}_{\infty}(\boldsymbol{E})-1}$$

Game $\mathrm{DETECT}^{Bob}_{\Pi,\Pi'}$

$b \leftarrow\!\!\$\ \{0,1\}$

$K' \leftarrow\!\!\$\ \boldsymbol{K'}$

$b' \leftarrow\!\!\$\ Bob^{\mathtt{Enc}}$

Return $(b = b')$

procedure $\mathtt{Key}(i)$

If$(K_i = \perp)$ then $(K_i \leftarrow\!\!\$\ \boldsymbol{K}; \sigma_i \leftarrow \epsilon)$

Return K_i

procedure $\mathtt{Enc}(M, i)$

If$(K_i = \perp)$ then Return $\perp$

If $(b = 1)$ then $(C, \sigma_i) \leftarrow\!\!\$\ \boldsymbol{E}(K_i, M, \sigma_i)$

Else $(C, \sigma_i) \leftarrow\!\!\$\ \boldsymbol{E'}(K', K_i, M, \sigma_i, i)$

Return C

procedure $\boldsymbol{E}(K', K, M)$

$x \leftarrow\!\!\$\ \{0, 1, \ldots (n-1)\}$

$r \leftarrow\!\!\$\ \{0,1\}^{n-l-1}$

$IV \leftarrow \boldsymbol{B}(K', K[x]||\langle x \rangle||r)$

$C \leftarrow E^*(K, M, IV)$

Return C

procedure $\boldsymbol{A}(K', (C_1, C_2 \ldots C_{\lfloor n \ln n \rfloor}))$

For $j = 1, 2, \ldots \lfloor n \ln n \rfloor \{$

$b||x||r \leftarrow \boldsymbol{B}^{-1}(K', X(C_j))$

$K[x] = b\}$

Return K

$$\mathbf{Adv}^{\mathrm{sdet}}_{\Pi,\Sigma}(Bob) \leq 2\mathbf{Adv}^{\mathrm{prf}}_{H}(Bob\text{-}PRF) + (k^2 s^2) 2^{-\mathbf{H}_\infty(\boldsymbol{E})}$$

$$\mathbf{Adv}^{\mathrm{surv}}_{\Pi,\Sigma}(Alice) = 0$$

procedure $\boldsymbol{E}(K', K, (M_0, M_1 \ldots M_{n-1}))$	**procedure** $\boldsymbol{A}(K', (C_0, C_1 \ldots C_{n-1}))$
For $j = 0, 1, \ldots (n-1)\{$	For $j = 0, 1, \ldots (n-1)\{$
$C_j \leftarrow \perp$	$K[j] \leftarrow F(K', C_j)\}$
While $(C_j = \perp)\{$	Return K
$C' \leftarrow\!\!\$\ E(K, M_j)$	
If $(F(K', C') = K[j])$ then $C_j \leftarrow C'$	
$\}\}$	
Return $C_0, C_1 \ldots C_{n-1}$	

procedure $\boldsymbol{E}(K', K, M)$	**procedure** $\boldsymbol{A}(K', (C_1 \ldots C_q))$
$C \leftarrow \perp; \quad j \leftarrow 0$	For $j = 1, \ldots q\{$
While $((C = \perp) \wedge (j < s))\{$	$(v, t) \leftarrow H(K', C_j)\}$
$j \leftarrow j + 1$	$K[t] \leftarrow v$
$C' \leftarrow\!\!\$\ E(K, M)$	Return K
$(v, t) \leftarrow H(K', C')$	
If $(K[t] = v)$ then $C \leftarrow C'$	
$\}\}$	
Return C	