*

Index of Security Definitions

One-time secrecy for symmetric-key encryption (Definition 2.6):

 $\mathcal{L}_{ ext{ots-L}}^{\Sigma}$ $\underbrace{ ext{QUERY}(m_L, m_R \in \Sigma.\mathcal{M}):}_{k \leftarrow \Sigma. ext{KeyGen}}_{c \leftarrow \Sigma. ext{Enc}(k, m_L)}_{ ext{return } c}$

 $\mathcal{L}_{\text{ots-R}}^{\Sigma}$ $\underline{\text{QUERY}(m_L, m_R \in \Sigma.\mathcal{M}):}$ $k \leftarrow \Sigma.\text{KeyGen}$ $c \leftarrow \Sigma.\text{Enc}(k, m_R)$ return c

t-out-of-*n* secret sharing (Definition 3.3):

 $\mathcal{L}_{\text{tsss-L}}^{\Sigma}$ $\underline{\text{QUERY}(m_L, m_R \in \Sigma.\mathcal{M}, U):}$ $\text{if } |U| \geqslant \Sigma.t: \text{ return err}$ $s \leftarrow \Sigma.\text{Share}(m_L)$ $\text{return } \{s_i \mid i \in U\}$

 $\mathcal{L}_{tsss-R}^{\Sigma}$ $\underline{\text{QUERY}(m_L, m_R \in \Sigma.\mathcal{M}, U):}_{if |U| \geqslant \Sigma.t: \text{ return err}}$ $s \leftarrow \Sigma.\text{Share}(m_R)$ $\text{return } \{s_i \mid i \in U\}$

Pseudorandom generator (Definition 5.1):

 $\mathcal{L}_{prg-real}^{G}$ $\underline{\frac{QUERY():}{s \leftarrow \{0,1\}^{\lambda}}}$ $\underline{return \ G(s)}$

 $\mathcal{L}_{\mathsf{prg-rand}}^{G}$ $\underbrace{\mathsf{QUERY():}}_{\substack{z \leftarrow \{\mathbf{0}, \mathbf{1}\}^{\lambda + \ell} \\ \mathsf{return} \ z}}$

Pseudorandom function (Definition 6.1):

 $\mathcal{L}_{\text{prf-real}}^{F}$ $k \leftarrow \{0, 1\}^{\lambda}$ $\underbrace{\text{QUERY}(x \in \{0, 1\}^{in}):}_{\text{return } F(k, x)}$

 $\mathcal{L}_{prf-rand}^{F}$ T := empty assoc. array $\underbrace{\text{QUERY}(x \in \{0,1\}^{in}):}_{\text{if } T[x] \text{ undefined:}}$ $T[x] \leftarrow \{0,1\}^{out}$ return T[x]

Pseudorandom permutation (Definition 7.2):

```
\mathcal{L}_{\text{prp-rand}}^{F}
L_{\text{prp-rand}}^{F}
T := \text{empty assoc. array}
\underline{\text{QUERY}(x \in \{0,1\}^{blen}):}
\underline{\text{return } F(k,x)}
\underline{\text{If } T[x] \text{ undefined:}}
T[x] \leftarrow \{0,1\}^{blen} \setminus \text{range}(T)
\underline{\text{return } T[x]}
```

Strong pseudorandom permutation (Definition 7.6):

$$\mathcal{L}_{\text{sprp-real}}^{F}$$

$$\mathcal{L}_{\text{sprp-real}}^{F}$$

$$T, T^{-1} := \text{empty assoc. arrays}$$

$$\underbrace{QUERY(x \in \{0,1\}^{blen}):}_{\text{if } T[x] \text{ undefined:}}_{\text{undefined:}}$$

$$\underbrace{y \leftarrow \{0,1\}^{blen} \setminus \text{range}(T)}_{T[x] := y; T^{-1}[y] := x}$$

$$\underbrace{T[x] := y; T^{-1}[y] := x}_{\text{return } T[x]}$$

$$\underbrace{T[x] := y; T^{-1}[y] := x}_{\text{return } T^{-1}[y] \text{ undefined:}}_{\text{undefined:}}$$

$$\underbrace{x \leftarrow \{0,1\}^{blen} \setminus \text{range}(T^{-1})}_{T^{-1}[y] := x; T[x] := y}$$

$$\underbrace{T[x] := y; T^{-1}[y] := x}_{\text{return } T^{-1}[y]}$$

CPA security for symmetric-key encryption (Definition 8.1, Section 9.2):

$$\mathcal{L}_{\text{cpa-L}}^{\Sigma}$$

$$k \leftarrow \Sigma. \text{KeyGen}$$

$$\frac{\text{CHALLENGE}(m_L, m_R \in \Sigma.\mathcal{M}):}{\text{if } |m_L| \neq |m_R| \text{ return null}}$$

$$c \coloneqq \Sigma. \text{Enc}(k, m_L)$$

$$\text{return } c$$

$$\mathcal{L}_{\text{cpa-R}}^{\Sigma}$$

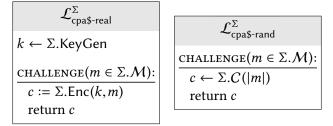
$$k \leftarrow \Sigma. \text{KeyGen}$$

$$\frac{\text{CHALLENGE}(m_L, m_R \in \Sigma.\mathcal{M}):}{\text{if } |m_L| \neq |m_R| \text{ return null}}$$

$$c \coloneqq \Sigma. \text{Enc}(k, m_R)$$

$$\text{return } c$$

CPA\$ security for symmetric-key encryption (Definition 8.2, Section 9.2):



CCA security for symmetric-key encryption (Definition 10.1):

 $k \leftarrow \Sigma$.KeyGen $k \leftarrow \Sigma$.KeyGen $S := \emptyset$ $S := \emptyset$ CHALLENGE $(m_L, m_R \in \Sigma.\mathcal{M})$: CHALLENGE $(m_L, m_R \in \Sigma.\mathcal{M})$: if $|m_L| \neq |m_R|$ return null if $|m_L| \neq |m_R|$ return null $c := \Sigma.\operatorname{Enc}(k, m_L)$ $c := \Sigma.\operatorname{Enc}(k, m_R)$ $\mathcal{S} := \mathcal{S} \cup \{c\}$ $\mathcal{S} := \mathcal{S} \cup \{c\}$ return creturn c $\text{DEC}(c \in \Sigma.C)$: $\text{DEC}(c \in \Sigma.C)$: if $c \in \mathcal{S}$ return null if $c \in \mathcal{S}$ return null return Σ . Dec(k,c)return Σ . Dec(k,c)

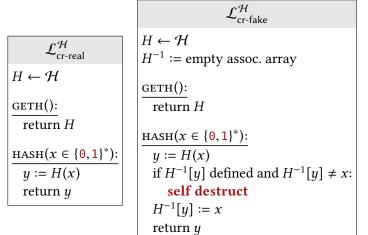
CCA\$ security for symmetric-key encryption (Definition 10.2):

 $\mathcal{L}^{\Sigma}_{\mathsf{cca\$-real}}$ $\mathcal{L}^{\Sigma}_{\text{cca\$-rand}}$ $k \leftarrow \Sigma$.KeyGen $k \leftarrow \Sigma$.KeyGen $S := \emptyset$ $S := \emptyset$ CHALLENGE($m \in \Sigma.\mathcal{M}$): CHALLENGE($m \in \Sigma.\mathcal{M}$): $c := \Sigma.\mathsf{Enc}(k,m)$ $c \leftarrow \Sigma.C(|m|)$ $\mathcal{S} \coloneqq \mathcal{S} \cup \{c\}$ $\mathcal{S} := \mathcal{S} \cup \{c\}$ return creturn c $\text{DEC}(c \in \Sigma.C)$: $\mathrm{DEC}(c \in \Sigma.C)$: if $c \in \mathcal{S}$ return null if $c \in \mathcal{S}$ return null return Σ . Dec(k, c)return Σ . Dec(k, c)

MAC (Definition 11.2):

 $\mathcal{L}_{\text{mac-real}}^{\Sigma}$ $k \leftarrow \Sigma. \text{KeyGen}$ $\frac{GETMAC(m \in \Sigma.\mathcal{M}):}{\text{return } \Sigma. \text{MAC}(k, m)}$ $\frac{VER(m \in \Sigma.\mathcal{M}, t):}{\text{return } t \stackrel{?}{=} \Sigma. \text{MAC}(k, m)}$ $\frac{VER(m \in \Sigma.\mathcal{M}, t):}{\text{return } t \stackrel{?}{=} \Sigma. \text{MAC}(k, m)}$ $\frac{VER(m \in \Sigma.\mathcal{M}, t):}{\text{return } t \stackrel{?}{=} \Sigma. \text{MAC}(k, m)}$

Collision resistance (Definition 12.1):

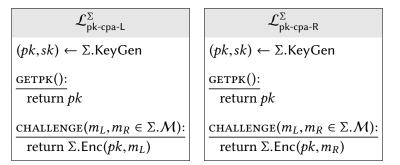


Key agreement (Definition 14.4):

$$\frac{\mathcal{L}_{\text{ka-real}}^{\Sigma}}{\underbrace{\frac{\text{QUERY}():}{(t,K) \leftarrow \text{EXECPROT}(\Sigma)}}_{\text{return } (t,K)} + \underbrace{\frac{\text{QUERY}():}{(t,K) \leftarrow \text{EXECPROT}(\Sigma)}}_{K' \leftarrow \Sigma.\mathcal{K}} + \underbrace{\frac{\text{QUERY}():}{(t,K) \leftarrow \text{EXECPROT}(\Sigma)}}_{\text{return } (t,K')}$$

Decisional Diffie-Hellman assumption (Definition 14.5):

CPA security for public-key encryption (Definition 15.1):



CPA\$ security for public-key encryption (Definition 15.2):

$$\mathcal{L}_{\text{pk-cpa\$-real}}^{\Sigma}$$

$$(pk, sk) \leftarrow \Sigma.\text{KeyGen}$$

$$\frac{\text{GETPK}():}{\text{return } pk}$$

$$\frac{\text{CHALLENGE}(m \in \Sigma.\mathcal{M}):}{\text{return } \Sigma.\text{Enc}(pk, m)}$$

$$\frac{\text{CHALLENGE}(m \in \Sigma.\mathcal{M}):}{\text{return } \Sigma.\text{Enc}(pk, m)}$$

$$\mathcal{L}^{\Sigma}_{\text{pk-cpa\$-rand}}$$

$$(pk,sk) \leftarrow \Sigma.\text{KeyGen}$$

$$\frac{\text{GETPK():}}{\text{return }pk}$$

$$\frac{\text{CHALLENGE}(m \in \Sigma.\mathcal{M}):}{c \leftarrow \Sigma.C}$$

$$\text{return }c$$

One-time secrecy for public-key encryption (Definition 15.4):

$$\mathcal{L}_{ ext{pk-ots-L}}^{\Sigma}$$
 $(pk, sk) \leftarrow \Sigma. \text{KeyGen}$
 $count := 0$

$$\frac{\text{GETPK():}}{\text{return } pk}$$

$$\frac{\text{CHALLENGE}(m_L, m_R \in \Sigma. \mathcal{M}):}{count := count + 1}$$

$$\text{if } count > 1: \text{ return null}$$

$$\text{return } \Sigma. \text{Enc}(pk, m_L)$$

$$\mathcal{L}^{\Sigma}_{ ext{pk-ots-R}}$$
 $(pk,sk) \leftarrow \Sigma. \text{KeyGen}$
 $count := 0$

$$\frac{\text{GETPK():}}{\text{return } pk}$$

$$\frac{\text{CHALLENGE}(m_L, m_R \in \Sigma.\mathcal{M}):}{count := count + 1}$$
if $count > 1$: return null return $\Sigma. \text{Enc}(pk, m_R)$