MPRI
SECURE: Proofs of Security Protocols
Cheatsheet: rules of the logic (week 2)

Adrien Koutsos, Inria Paris

2026/2027

Structural

$$\frac{}{\vec{u} \sim \vec{u}}\ \textsc{Refl} \qquad \frac{\vec{v} \sim \vec{u}}{\vec{u} \sim \vec{v}}\ \textsc{Sym} \qquad \frac{\vec{u} \sim \vec{w} \qquad \vec{w} \sim \vec{v}}{\vec{u} \sim \vec{v}}\ \textsc{Trans} \qquad \frac{}{\vec{u} \sim \vec{u}\alpha}\ \alpha\text{-EQU}$$

$$\frac{\vec{w}_0, b_0, u_0 \sim \vec{w}_1, b_1, u_1 \qquad \vec{w}_0, b_0, v_0 \sim \vec{w}_1, b_1, v_1}{\vec{w}_0, \mathsf{if}\ b_0\ \mathsf{then}\ u_0\ \mathsf{else}\ v_0 \sim \vec{w}_1, \mathsf{if}\ b_1\ \mathsf{then}\ u_1\ \mathsf{else}\ v_1}\ \text{CS}$$

α is an injective renaming of names in $\mathcal{N}$. Terms $\vec{u}$ must be ground in α-EQU.

Basic reductions

$$\frac{\vec{u}, s \sim \vec{v}, t}{\vec{u}, s, s \sim \vec{v}, t, t}\ \textsc{Dup} \qquad \frac{\vec{u}_1, \vec{v}_1 \sim \vec{u}_1, \vec{v}_2}{f(\vec{u}_1), \vec{v}_1 \sim f(\vec{u}_2), \vec{v}_2}\ \text{FA} \qquad \frac{\vec{u}, s \sim \vec{v}, t}{\vec{u} \sim \vec{v}}\ \textsc{Restr}$$

$$\frac{u_{\pi(1)}, \ldots, u_{\pi(n)} \sim v_{\pi(1)}, \ldots, v_{\pi(n)}}{u_1, \ldots, u_n \sim v_1, \ldots, v_n}\ \textsc{Perm}$$

Where π is a permutation of $\{1, \ldots, n\}$.

Rewriting

$$\frac{\vec{u}, t \sim \vec{v} \qquad [s = t]}{\vec{u}, s \sim \vec{v}}\ \text{R} \qquad \frac{\mathcal{A}_{\mathsf{th}} \vdash_{\textsc{Gen}} \phi}{[\phi]}\ \text{GEN}$$

Where $\vdash_{\textsc{Gen}}$ is a sound proof system for generic mathematical reasoning.

Freshness

$$\frac{}{[t \neq \mathsf{n}]}\ =\text{-IND} \quad \text{when } \mathsf{n} \notin \mathsf{st}(t) \qquad \frac{\vec{u} \sim \vec{v}}{\vec{u}, \mathsf{n}_0 \sim \vec{v}, \mathsf{n}_1}\ \textsc{Fresh} \quad \text{when } \mathsf{n}_0 \notin \mathsf{st}(\vec{u}) \text{ and } \mathsf{n}_1 \notin \mathsf{st}(\vec{v})$$

We require that all terms are ground *terms, and that n, n_0, n_1 are names.*

IND-CCA1 *If* $(\{\cdot\}^{\cdot}_{\cdot}, \mathsf{dec}(\cdot,\cdot), \mathsf{pk}(\cdot), \mathsf{sk}(\cdot))$ *is an IND-CCA1 asymmetric encryption scheme*

$$\frac{[\mathsf{len}(t_0) = \mathsf{len}(t_1)]}{\vec{u}, \{t_0\}^{\mathsf{r}}_{\mathsf{pk}(\mathsf{n})} \sim \vec{u}, \{t_1\}^{\mathsf{r}}_{\mathsf{pk}(\mathsf{n})}}\ \text{IND-CCA}_1$$

We require that all terms are ground, that n, r *are names, and that:*

- $\mathsf{r} \notin \mathsf{st}(\vec{u}, t_0, t_1)$*;*
- $\mathsf{n} \sqsubseteq_{\mathsf{pk}(\cdot),\mathsf{dec}(_,\mathsf{sk}(\cdot))} \vec{u}, t_0, t_1$*,*
  i.e. n *appears only has* $\mathsf{pk}(\cdot)$ *or* $\mathsf{dec}(_, \mathsf{sk}(\cdot))$ *in* $\vec{u}, t_0, t_1$*.*

IND-KP *If* $(\{\cdot\}^{\cdot}_{\cdot}, \mathsf{dec}(\cdot,\cdot), \mathsf{pk}(\cdot), \mathsf{sk}(\cdot))$ *is an IND-KP asymmetric encryption scheme*

$$\frac{}{\vec{u}, \{t\}^{\mathsf{r}}_{\mathsf{pk}(\mathsf{n}_0)} \sim \vec{u}, \{t\}^{\mathsf{r}}_{\mathsf{pk}(\mathsf{n}_1)}}\ \text{KP-CCA}_1$$

We require that all terms are ground, that $\mathsf{n}_0, \mathsf{n}_1, \mathsf{r}$ *are names, and that:*

- $\mathsf{r} \notin \mathsf{st}(\vec{u}, t)$*;*
- $\mathsf{n}_i \sqsubseteq_{\mathsf{pk}(\cdot),\mathsf{dec}(_,\mathsf{sk}(\cdot))} \vec{u}, t$ *for both* $i \in \{0, 1\}$
  i.e. n_0 *and* n_1 *appear only has* $\mathsf{pk}(\cdot)$ *or* $\mathsf{dec}(_, \mathsf{sk}(\cdot))$ *in* $\vec{u}, t$*.*

EUF-CMA *If* $(\mathsf{mac}.(\cdot), \mathsf{verify}.(\cdot,\cdot))$ *is a EUF-CMA MAC scheme*

$$\frac{}{\mathsf{verify}_{\mathsf{k}}(s, m) \vdash \bigvee_{u \in \mathcal{S}} m = u}\ \text{EUF-MAC}$$

We require that all terms are ground, that k *is a name, and that:*

- $\mathcal{S} = \mathbb{S}_{\mathsf{mac}}(s, m)$ *where* $\mathbb{S}_{\mathsf{mac}}(u) = \{v \mid \mathsf{mac}_{\mathsf{k}}(v) \in \mathsf{st}(u)\}$*;*
- $\mathsf{k} \sqsubseteq_{\mathsf{mac}.(_),\mathsf{verify}.(_,_)} s, m$
  i.e. k *appears only in* mac *or* verify *key positions in* s, m*.*

CR-HK *If* $\mathsf{H}(\cdot,\cdot)$ *is a CR-HK hash function*

$$\frac{}{\mathsf{H}(m_1, \mathsf{k}) = \mathsf{H}(m_2, \mathsf{k}) \vdash m_1 = m_2}\ \text{CR}$$

We require that all terms are ground, that k *is a name, and that:*

- $\mathsf{k} \sqsubseteq_{\mathsf{H}(_,\cdot)} m_1, m_2$
  i.e. k *appears only in hash key position in* m_1, m_2*.*