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

Adrien Koutsos, Inria Paris

2025/2026

Structural

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

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

Where α is an injective renaming of names in $\mathcal{N}$.

Basic reductions

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

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

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

Rewriting

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

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

Freshness

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

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