MPRI 2.30: Proofs of Security Protocols

2. The CCSA Logic

Adrien Koutsos

2024/2025

Outline

The CCSA Logic

The CCSA Logic

We now present a logic, to state (and later prove) **properties** about **bitstring distributions**.

This is a first-order logic with a predicate $\sim$[1] representing **computational indistinguishability**.

$$\begin{aligned}\Phi := & \ \tilde{\top} \mid \tilde{\bot} \\ & \mid \Phi \mathbin{\tilde{\wedge}} \Phi \mid \Phi \mathbin{\tilde{\vee}} \Phi \mid \Phi \mathbin{\tilde{\rightarrow}} \Phi \mid \tilde{\neg}\, \Phi \\ & \mid \tilde{\forall} \mathsf{x}.\Phi \mid \tilde{\exists} \mathsf{x}.\Phi & (\mathsf{x} \in \mathcal{X}) \\ & \mid t_1, \ldots, t_n \sim_n t_{n+1}, \ldots, t_{2n} & (t_1, \ldots, t_{2n} \in \mathcal{T}(\mathcal{S}))\end{aligned}$$

Remark: we use $\tilde{\wedge}, \tilde{\vee}, \tilde{\rightarrow}, \ldots$ for the logical *connectives*, to avoid confusion with the boolean *function symbols* $\wedge, \vee, \rightarrow, \ldots$ in terms.

[1] Actually, one predicate $\sim_n$ of arity $2n$ for every $n \in \mathbb{N}$.

Semantics of the Logic

The logic has a **standard FO semantics**, using $\mathcal{D}$ as interpretation domain and interpreting $\sim$ as **computational indistinguishability**.

The **satisfaction** $\mathbb{M} \models \Phi$ of Φ in $\mathbb{M}$ is as expected for **boolean connective** and FO **quantifiers**. E.g.:

$$\mathbb{M} \models \tilde{\top} \qquad \mathbb{M} \models \Phi \mathbin{\tilde{\wedge}} \Psi \quad \text{if } \mathbb{M} \models \Phi \text{ and } \mathbb{M} \models \Psi$$

$$\mathbb{M} \models \tilde{\neg}\Phi \quad \text{if not } \mathbb{M} \models \Phi \qquad \mathbb{M} \models \tilde{\forall} \mathsf{x}.\Phi \quad \text{if } \forall m \in \mathcal{D},\ \mathbb{M}[\mathsf{x} \mapsto m] \models \Phi$$

Semantics of the Logic

Finally, $\sim_n$ is interpreted as **computational indistinguishability**.

$$\mathbb{M} \models t_1, \ldots, t_n \sim_n s_1, \ldots, s_n$$

if, for every PPTM $\mathcal{A}$ with a $n+1$ input (and working) tapes, and a **single** random tape:

$$\left| \begin{array}{rl} & \mathrm{Pr}_\rho\left(\mathcal{A}(1^\eta, ([\![t_i]\!]^{\eta,\rho}_{\mathbb{M}})_{1 \leq i \leq n}, \rho_\mathsf{a}) = 1\right) \\ - & \mathrm{Pr}_\rho\left(\mathcal{A}(1^\eta, ([\![s_i]\!]^{\eta,\rho}_{\mathbb{M}})_{1 \leq i \leq n}, \rho_\mathsf{a}) = 1\right) \end{array} \right| \qquad (\star)$$

is a **negligible** function of η.

*The quantity in $(\star)$ is called the **advantage** of $\mathcal{A}$ against the left/right game $t_1, \ldots, t_n \sim_n s_1, \ldots, s_n$*

Negligible Functions

A function $f(\eta)$ is **negligible**, which we write $f \in \text{negl}(\eta)$, if it is **asymptotically smaller** than the **inverse** of any **polynomial**, i.e.:

$$\forall c \in \mathbb{N}, \exists N \in \mathbb{N} \text{ s.t. } \forall n \geq N, f(n) \leq \frac{1}{n^c}$$

Example

Let f be the function defined by:

$$f(\eta) \stackrel{\text{def}}{=} \Pr_\rho\left(\llbracket \mathsf{n}_0 \rrbracket^{\eta,\rho} = \llbracket \mathsf{n}_1 \rrbracket^{\eta,\rho}\right)$$

If $\mathsf{n}_0 \not\equiv \mathsf{n}_1$, then $f(\eta) = \frac{1}{2^\eta}$, and f is negligible.

Satisfiability and Validity

A formula Φ is **satisfied** by a model $\mathbb{M}$ when $\mathbb{M} \models \Phi$.

Φ is **valid**, denoted by $\models \Phi$, if it is **satisfied** by **every model**.

Φ is **$\mathcal{C}$-valid** if it is satisfied by every model $\mathbb{M} \in \mathcal{C}$.

Protocol Indistinguishability

$\mathcal{P}$ and $\mathcal{Q}$ are **indistinguishable**, written $\mathcal{P} \approx \mathcal{Q}$, if for any τ:

$$\models \mathsf{s\text{-}exec}(\mathcal{P}, \tau) \sim \mathsf{s\text{-}exec}(\mathcal{Q}, \tau)$$

Remark

While there are countably many observable traces τ, the **set** of **foldings** of a protocol P is always **finite**:[2]

$$\left|\left\{\mathsf{s\text{-}exec}(\mathcal{P}, \tau) \mid \tau\right\}\right| < +\infty$$

[2] If we remove trailing sequences of `error` terms.

Exercise: Negligibility

Exercise

Show the following properties:

- If $f \in \text{negl}(\eta)$ and $g \in \text{negl}(\eta)$ then $f + g \in \text{negl}(\eta)$.
- Idem, but for $\max(f, g)$ and $\min(f, g)$.
- Take a polynomial P. If, for every $1 \leq i \leq P(\eta)$, $f_i \in \text{negl}(\eta)$, then $\sum_{1 \leq i \leq P(\eta)} f_i$ is not necessarily negligible.
- Show that $\sum_{1 \leq i \leq P(\eta)} f_i$ is negligible if there exists $f \in \text{negl}(\eta)$ uniformly bounding the f_i's, i.e. s.t. $f_i(\eta) \leq f(\eta)$ for every i, η.

Exercise: Validity

Exercise

Which of the formulas below are **valid**? Which are not?

$$\mathsf{true} \sim \mathsf{false} \qquad \mathsf{n}_0 \sim \mathsf{n}_0 \qquad \mathsf{n}_0 \sim \mathsf{n}_1 \qquad \mathsf{n}_0 = \mathsf{n}_1 \sim \mathsf{false}$$

$$\mathsf{n}_0, \mathsf{n}_0 \sim \mathsf{n}_0, \mathsf{n}_1 \qquad f(\mathsf{n}_0) \sim f(\mathsf{n}_1) \ \text{ where } f \in \mathcal{F} \cup \mathcal{G}$$

$$\pi_1(\langle \mathsf{n}_0\ ,\ \mathsf{n}_1 \rangle) = \mathsf{n}_0 \sim \mathsf{true}$$

Exercise: Validity

Exercise

Which of the formulas below are **valid**? Which are not?

$\not\models \mathsf{true} \sim \mathsf{false}$ $\quad \models \mathsf{n}_0 \sim \mathsf{n}_0$ $\quad \models \mathsf{n}_0 \sim \mathsf{n}_1$ $\quad \models \mathsf{n}_0 = \mathsf{n}_1 \sim \mathsf{false}$

$\not\models \mathsf{n}_0, \mathsf{n}_0 \sim \mathsf{n}_0, \mathsf{n}_1$ $\quad \models f(\mathsf{n}_0) \sim f(\mathsf{n}_1)$ where $f \in \mathcal{F} \cup \mathcal{G}$

$\not\models \pi_1(\langle \mathsf{n}_0 , \mathsf{n}_1 \rangle) = \mathsf{n}_0 \sim \mathsf{true}$

Exercise: Protocol Indistinguishability

Exercise

Informally, determine which of the following protocols **indistinguishabilities** hold, and under what **assumptions**:

$$\mathbf{out}(\mathsf{c}, t_1) \approx \mathbf{out}(\mathsf{c}, t_2) \qquad \mathbf{out}(\mathsf{c}, t) \approx \mathbf{null} \qquad \mathbf{in}(\mathsf{c}, \mathsf{x}) \approx \mathbf{null}$$

$$\mathbf{out}(\mathsf{c}, t) \approx \text{if } b \text{ then } \mathbf{out}(\mathsf{c}, t_1) \text{ else } \mathbf{out}(\mathsf{c}, t_2)$$

Proof System

Cryptographic Arguments

High-level structure of a **game-hopping** proof:

$$\mathcal{G}_0 \sim_{\epsilon_1} \ldots \sim_{\epsilon_n} \mathcal{G}_n \quad \Rightarrow$$

$$\mathcal{G}_0 \sim_{\epsilon_1 + \cdots + \epsilon_n} \mathcal{G}_n$$

where each **game-hop** $\mathcal{G}_i \sim_{\epsilon_{i+1}} \mathcal{G}_{i+1}$ is justified by:

- **bridging steps** showing that $\mathcal{G} \sim_0 \mathcal{G}'$.
- **up-to-bad argument** $|\Pr(\mathcal{G}) - \Pr(\mathcal{G}')| \leq \Pr(\text{bad})$.
  - $\Pr(\text{bad}) \leq \epsilon$ through a **probabilistic argument** (e.g. collision probability).
  - ...
- a **cryptographic reduction** to some hardness assumption.
- ...

$\Longrightarrow$ how to **capture these arguments in the logic**?

Soundness

A rule:

$$\frac{\phi_1 \quad \dots \quad \phi_n}{\phi}$$

is **sound** if ϕ is **valid** whenever $\phi_1, \dots, \phi_n$ are **valid**.

Example

$$\frac{y \sim x}{x \sim y} \quad \text{is sound}$$

These are typically **structural rules**, which are valid in all **models**.

Other rules, e.g. rules relying on **cryptographic hardness assumptions**, which only hold in a subset of all models.

Proof System

Structuring Rules

Structuring Rules

Structuring rules allow to:

- capture the **high-level structure** of a cryptographic proof;
- handle **low-level manipulation** of the proof-goal (**bookkeeping**).

Structuring Rules

Computational indistinguishability is an **equivalence relation**:

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

Alpha-renaming.

$$\frac{}{\vec{u} \sim \vec{u}\alpha}\ \alpha\text{-}\textsc{equ}$$

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

Proofs. Basic properties of indistinguishability.

Structuring Rules

Permutation. If π is a permutation of $\{1, \ldots, n\}$ then:

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

Restriction. The adversary can throw away some values:

$$\frac{\vec{u}, s \sim \vec{v}, t}{\vec{u} \sim \vec{v}} \ \textsc{Restr}$$

Structuring Rules

Duplication. Giving twice the same value to the adversary is useless:

$$\frac{\vec{u}, s \sim \vec{v}, t}{\vec{u}, s, s \sim \vec{v}, t, t}\ \text{Dup}$$

Function application. If the arguments of a function are indistinguishable, so is the image:

$$\frac{\vec{u_1}, \vec{v_1} \sim \vec{u_1}, \vec{v_2}}{f(\vec{u_1}), \vec{v_1} \sim f(\vec{u_2}), \vec{v_2}}\ \text{FA}$$

where $f \in \mathcal{F} \cup \mathcal{G}$.

Proofs. These last four rules are proved by cryptographic reductions.

Proof of Function Application

$$\frac{\vec{u}_1, \vec{v}_1 \sim \vec{u}_1, \vec{v}_2}{f(\vec{u}_1), \vec{v}_1 \sim f(\vec{u}_2), \vec{v}_2} \text{ FA}$$

Proof. Assume $f \in \mathcal{F}$ (the case $f \in \mathcal{G}$ is similar). The proof is by contrapositive. Let $\mathbb{M}$ and $\mathcal{A}$ s.t. its advantage against:

$$f(\vec{u}_1), \vec{v}_1 \sim f(\vec{u}_2), \vec{v}_2 \tag{$\dagger$}$$

is not negligible. Let $\mathcal{B}$ be the *distinguisher* defined by, for any bitstrings $\vec{w}_u, \vec{w}_v$ and tape ρ_a:

$$\mathcal{B}(1^\eta, \vec{w}_u, \vec{w}_v, \rho_a) \stackrel{\text{def}}{=} \mathcal{A}(1^\eta, (\!|f|\!)_{\mathbb{M}}(1^\eta, \vec{w}_u), \vec{w}_v, \rho_a)$$

$\mathcal{B}$ is a PPTM since $\mathcal{A}$ is and $(\!|f|\!)_{\mathbb{M}}$ can be evaluated in pol. time. Then:

$$\begin{aligned} & \mathcal{B}(1^\eta, [\![\vec{u}_i]\!]_{\mathbb{M}}^{\eta,\rho}, [\![\vec{v}_i]\!]_{\mathbb{M}}^{\eta,\rho}, \rho_a) \\ = \; & \mathcal{A}(1^\eta, [\![f(\vec{u}_i)]\!]_{\mathbb{M}}^{\eta,\rho}, [\![\vec{v}_i]\!]_{\mathbb{M}}^{\eta,\rho}, \rho_a) \end{aligned} \qquad (i \in \{1, 2\})$$

Hence the advantage of $\mathcal{B}$ in distinguishing $\vec{u}_1, \vec{v}_1 \sim \vec{u}_1, \vec{v}_2$ is exactly the advantage of $\mathcal{A}$ in distinguishing ($\dagger$). $\square$

Structuring Rules

Case Study. We can do case disjunction over branching terms:

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

Proof of Case Study

$$\frac{b_0, u_0 \sim b_1, u_1 \qquad b_0, v_0 \sim b_1, v_1}{t_0 \equiv \text{if } b_0 \text{ then } u_0 \text{ else } v_0 \sim t_1 \equiv \text{if } b_1 \text{ then } u_1 \text{ else } v_1} \text{ CS}$$

Proof. (by contrapositive) Assume $\mathbb{M}$ and $\mathcal{A}$ s.t. its advantage against:

$$\text{if } b_0 \text{ then } u_0 \text{ else } v_0 \sim \text{if } b_1 \text{ then } u_1 \text{ else } v_1 \qquad (\dagger)$$

is non-negligible. Let $\mathcal{B}_\top$ be the distinguisher:

$$\mathcal{B}_\top(1^\eta, w_b, w, \rho_a) \stackrel{\text{def}}{=} \begin{cases} \mathcal{A}(1^\eta, w, \rho_a) & \text{if } w_b = 1 \\ 0 & \text{otherwise} \end{cases}$$

$\mathcal{B}_\top$ is trivially a PPTM. Moreover, for any $i \in \{1, 2\}$:

$$\begin{aligned} & \Pr_\rho\Big(\mathcal{B}_\top(1^\eta, [\![b_i]\!]^{\eta,\rho}_{\mathbb{M}}, [\![u_i]\!]^{\eta,\rho}_{\mathbb{M}}, \rho_a) = 1\Big) \\ = \; & \left.\Pr_\rho\Big(\mathcal{A}(1^\eta, [\![t_i]\!]^{\eta,\rho}_{\mathbb{M}}, \rho_a) = 1 \wedge [\![b_i]\!]^{\eta,\rho}_{\mathbb{M}} = 1\Big)\right\} p_{\top,i} \end{aligned}$$

Proof of Case Study (continued)

Hence the advantage of $\mathcal{B}_\top$ against $b_0, u_0 \sim b_1, u_1$ is $|p_{\top,1} - p_{\top,0}|$.

Similarly, let $\mathcal{B}_\perp$ be the distinguisher:

$$\mathcal{B}_\perp(1^\eta, w_b, w, \rho_a) \stackrel{\text{def}}{=} \begin{cases} \mathcal{A}(1^\eta, w, \rho_a) & \text{if } w_b \neq 1 \\ 0 & \text{otherwise} \end{cases}$$

By an identical reasoning, we get that the advantage of $\mathcal{B}_\perp$ against $b_0, v_0 \sim b_1, v_1$ is $|p_{\perp,1} - p_{\perp,0}|$, where $p_{\perp,i}$ is:

$$\Pr_\rho\Big(\mathcal{A}(1^\eta, [\![t_i]\!]_{\mathbb{M}}^{\eta,\rho}, \rho_a) = 1 \land [\![b_i]\!]_{\mathbb{M}}^{\eta,\rho} \neq 1\Big)$$

Proof of Case Study (continued)

The advantage of $\mathcal{A}$ against $t_0 \sim t_1$ is, by partitioning and triangular inequality:

$$|(p_{\top,1} + p_{\bot,1}) - (p_{\top,0} + p_{\bot,1})| \leq |p_{\top,1} - p_{\top,0}| + |p_{\bot,1} - p_{\bot,1}|$$

Since $\mathcal{A}$'s advantage is non-negligible, at least one of the two quantity above is non-negligible. Hence either $\mathcal{B}_\top$ or $\mathcal{B}_\bot$ has a non-negligible advantage against a premise of the CS rule. $\square$.

Counter-Examples

Remark that b is **necessary** in CS

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

We have:

$$\models \langle 0\,,\, \mathsf{n}_0 \rangle \sim \langle 0\,,\, \mathsf{n}_0 \rangle \qquad \models \langle 1\,,\, \mathsf{n}_0 \rangle \sim \langle 1\,,\, \mathsf{n}_0 \rangle \qquad \models \mathtt{even}(\mathsf{n}_0) \sim \mathtt{odd}(\mathsf{n}_0)$$

But:

$$\not\models \begin{array}{l} \ \text{if } \mathtt{even}(\mathsf{n}_0) \text{ then } \langle 0\,,\, \mathsf{n}_0 \rangle \text{ else } \langle 1\,,\, \mathsf{n}_0 \rangle \\ \sim \text{if } \ \mathtt{odd}(\mathsf{n}_0) \text{ then } \langle 0\,,\, \mathsf{n}_0 \rangle \text{ else } \langle 1\,,\, \mathsf{n}_0 \rangle \end{array}$$

Why is the later formula not valid?

Proof System

Basic Single-Step Reasoning Rules

Equality Reasoning

If $\models (s = t) \sim \text{true}$, then s and t are **equal with overwhelming probability**. Hence we can **safely replace** s by t in **any context**.

If ϕ is a term of type `bool`, let $[\phi] \stackrel{\text{def}}{=} \phi \sim \text{true}$.
$\Rightarrow$ i.e. ϕ is *overwhelmingly true* (equivalently, $\neg\phi$ is *negligible*).

Then the following rule is sound:

$$\frac{\vec{u}, t \sim \vec{v} \qquad [s = t]}{\vec{u}, s \sim \vec{v}}\ \mathrm{R}$$

Equality Reasoning

Proof

First, for any model $\mathbb{M}$, we have:

$$\mathbb{M} \models [\phi] \text{ iff. } \Pr_\rho\left(\llbracket\phi\rrbracket_{\mathbb{M}}^{\eta,\rho}\right) \text{ is overwhelming.}$$

- Left-to-right:

$$\begin{aligned}
& \mathbb{M} \models [\phi] \\
\Rightarrow\ & \forall A \in \mathcal{D}.\ \left|\Pr_\rho\left(\mathcal{A}(1^\eta, \llbracket\phi\rrbracket_{\mathbb{M}}^{\eta,\rho}, \rho_a)\right) - \Pr_\rho\left(\mathcal{A}(1^\eta, \llbracket\mathsf{true}\rrbracket_{\mathbb{M}}^{\eta,\rho}, \rho_a)\right)\right| \in \mathsf{negl}(\eta) \\
\Rightarrow\ & \left|\Pr_\rho\left(\llbracket\phi\rrbracket_{\mathbb{M}}^{\eta,\rho}\right) - 1\right| \in \mathsf{negl}(\eta) \qquad \text{(taking } \mathcal{A}(1^\eta, w, \rho_a) = w\text{)} \\
\Rightarrow\ & \Pr_\rho\left(\llbracket\phi\rrbracket_{\mathbb{M}}^{\eta,\rho}\right) \in \mathsf{o.w.}(\eta)
\end{aligned}$$

- Right-to-left, assume $\Pr_\rho\left(\llbracket\phi\rrbracket_{\mathbb{M}}^{\eta,\rho}\right) \in \mathsf{o.w.}(\eta)$ and take $\mathcal{A} \in \mathcal{D}$:

$$\begin{aligned}
& \left|\Pr_\rho\left(\mathcal{A}(1^\eta, \llbracket\phi\rrbracket_{\mathbb{M}}^{\eta,\rho}, \rho_a)\right) - \Pr_\rho\left(\mathcal{A}(1^\eta, \llbracket\mathsf{true}\rrbracket_{\mathbb{M}}^{\eta,\rho}, \rho_a)\right)\right| \\
\leq\ & \Pr_\rho\left(\neg\llbracket\phi\rrbracket_{\mathbb{M}}^{\eta,\rho}\right) \qquad \text{(up-to-bad)} \\
\in\ & \mathsf{negl}(\eta)
\end{aligned}$$

Equality Reasoning

This allows to conclude immediately since:

$$
\begin{aligned}
& |\Pr(\mathcal{A}([\![\vec{u}, t]\!])) - \Pr(\mathcal{A}([\![\vec{v}]\!]))| \\
\leq\ & |\Pr(\mathcal{A}([\![\vec{u}, s]\!])) - \Pr(\mathcal{A}([\![\vec{v}]\!]))| + \Pr\left([\![s]\!] \neq [\![t]\!]\right) \qquad \text{(up-to-bad)}
\end{aligned}
$$

Reminder: up-to-bad argument

If B, E, E' are events such that:

$$(E \wedge \neg B) \Leftrightarrow (E' \wedge \neg B), \qquad (\diamond)$$

then $|\Pr(E) - \Pr(E')| \leq \Pr(B)$.

Indeed, by triangular inequality and total probabilities:

$$|\Pr(E) - \Pr(E')| \leq |\Pr(E \wedge B) - \Pr(E' \wedge B)| + |\Pr(E \wedge \neg B) - \Pr(E' \wedge \neg B)|$$

We conclude by observing that:

- $|\Pr(E \wedge \neg B) - \Pr(E' \wedge \neg B)| = 0$ by $(\diamond)$;
- $|\Pr(E \wedge B) - \Pr(E' \wedge B)| \leq \max(\Pr(E \wedge B), \Pr(E' \wedge B)) \leq \Pr(B)$.

Generic Equality Reasoning

To prove $\models [s = t]$ (or more generally $\models [\phi]$), we use the rule:

$$\frac{\mathcal{A}_{\mathsf{th}} \vdash_{\textsc{Gen}} \phi}{[\phi]}\ \textsc{GEN}$$

where $\vdash_{\textsc{Gen}}$ is any **sound proof system** for generic mathematical reasoning (e.g. higher-order logic).

This allows **exact** (i.e. non-probabilistic) mathematical reasoning.

We allow additional axioms using $\mathcal{A}_{\mathsf{th}}$ (e.g. for if $\cdot$ then $\cdot$ else$\cdot$).

Example

$$\mathcal{A}_{\mathsf{th}} \vdash_{\textsc{Gen}} v = w \rightarrow \begin{pmatrix} \text{if } u = v \text{ then } u \text{ else } t \ = \\ \text{if } u = v \text{ then } w \text{ else } t \end{pmatrix}$$

Equality Reasoning

Up-to-bad arguments (game-hop style)

Two games $\mathcal{G}, \mathcal{G}'$ such that:

$$\Pr(\mathcal{G} \wedge \neg \mathsf{bad}) = \Pr(\mathcal{G}' \wedge \neg \mathsf{bad}).$$

Then $|\Pr(\mathcal{G}) - \Pr(\mathcal{G}')| \leq \Pr(\mathsf{bad})$.

In the **CCSA** logic:

$$\frac{[\neg \phi_{\mathsf{bad}}] \qquad [\neg \phi_{\mathsf{bad}} \rightarrow u = v]}{u \sim v}\ \mathrm{U2B}$$

Proof. Rewriting rule + some basic reasoning.

Equality Reasoning

Up-to-bad arguments (game-hop style)

Two games $\mathcal{G}, \mathcal{G}'$ such that:

$$\Pr(\mathcal{G} \wedge \neg\mathsf{bad}) = \Pr(\mathcal{G}' \wedge \neg\mathsf{bad}).$$

Then $|\Pr(\mathcal{G}) - \Pr(\mathcal{G}')| \leq \Pr(\mathsf{bad})$.

In the **CCSA** logic:

$$\frac{[\neg\phi_{\mathsf{bad}}] \qquad [\neg\phi_{\mathsf{bad}} \rightarrow u = v]}{u \sim v}\ \text{U2B}$$

Proof. Rewriting rule + some basic reasoning.

Other direction $[\,\cdot\,] \Rightarrow (\cdot \sim \cdot)$ also exists:

$$\frac{[\psi] \qquad \phi \sim \psi}{[\phi]}\ \textsc{Rewrite-Equiv}$$

$\Longrightarrow$ enables **back-and-forth between both predicates**.

Probabilistic Independence

Two rules exploiting the **independence** of bitstring distributions:

$$\frac{}{[t \neq \mathsf{n}]}\ =\text{-}\textsc{Ind} \quad \text{when } \mathsf{n} \notin \mathsf{st}(t)$$

$$\frac{\vec{u} \sim \vec{v}}{\vec{u}, \mathsf{n}_0 \sim \vec{v}, \mathsf{n}_1}\ \textsc{Fresh} \quad \text{when } \mathsf{n}_0 \notin \mathsf{st}(\vec{u}) \text{ and } \mathsf{n}_1 \notin \mathsf{st}(\vec{v})$$

Remark

To check that the rules side-conditions hold, we require that they do not contain free variables. Hence we actually have a countable, recursive, set of **ground rules** (i.e. rule **schemata**).

Probability Independence

We give the proof of the first rule:

$$\frac{}{[t \neq \mathsf{n}]}\ {=}\text{-IND} \quad \text{when } \mathsf{n} \notin \mathsf{st}(t)$$

Proof. For any model $\mathbb{M}$ (we omit it below):

$$\begin{aligned}
& \mathsf{Pr}_\rho([\![t = \mathsf{n}]\!]^{\eta,\rho}) \\
= \ & \mathsf{Pr}_\rho([\![t]\!]^{\eta,\rho} = [\![\mathsf{n}]\!]^{\eta,\rho}) \\
= \ & \textstyle\sum_{w \in \{0,1\}^*} \mathsf{Pr}_\rho([\![t]\!]^{\eta,\rho} = w \wedge [\![\mathsf{n}]\!]^{\eta,\rho} = w) \\
= \ & \textstyle\sum_{w \in \{0,1\}^*} \mathsf{Pr}_\rho([\![t]\!]^{\eta,\rho} = w) \cdot \mathsf{Pr}_\rho([\![\mathsf{n}]\!]^{\eta,\rho} = w) \\
= \ & \tfrac{1}{2^\eta} \cdot \textstyle\sum_{w \in \{0,1\}^\eta} \mathsf{Pr}_\rho([\![t]\!]^{\eta,\rho} = w) \\
= \ & \frac{1}{2^\eta}
\end{aligned}$$

□

Exercise

Exercise

Give a **derivation** of the following formula:

$$\mathsf{n}_0 \sim \text{if } b \text{ then } \mathsf{n}_0 \text{ else } \mathsf{n}_1 \quad (\text{when } \mathsf{n}_0, \mathsf{n}_1 \notin \mathrm{st}(b))$$

Proof System

Implementation Rules

Rules: Soundness

A rule is $\mathcal{C}$-**sound** if ϕ is $\mathcal{C}$-**valid** whenever $\phi_1, \ldots, \phi_n$ are $\mathcal{C}$-**valid**.

Example

$$\frac{}{[\pi_1\langle x\,,\,y\rangle = x]}$$

is **not** sound, because we do not require anything on the interpretation of π_1 and the pair.

Obviously, it is $\mathcal{C}_\pi$-sound, where $\mathcal{C}_\pi$ is the set of model where π_1 computes the first projection of the pair $\langle \_\,,\,\_\rangle$.

Implementation Assumptions

The **general philosophy** of the CCSA approach is to make the minimum number of assumptions possible on the interpretations of function symbols in a model.

Any additional necessary assumption is added through rules, which restrict the set of model for which the formula holds (hence limit the scope of the final security result).

Typically, this is used for:

- **functional properties**, which must be satisfied by the protocol functions (e.g. the projection/pair rule).
- **cryptographic hardness assumptions**, which must be satisfied by the cryptographic primitives (e.g. IND-CCA).

Functional Properties

Example. **Equational theories** for protocol functions:

- $\pi_i(\langle x_1, x_2 \rangle) = x_i$ $\qquad i \in \{1, 2\}$
- $\mathsf{dec}(\{x\}^z_{\mathsf{pk}(y)}, \mathsf{sk}(y)) = x$
- $(x \oplus y) \oplus z = x \oplus (y \oplus z)$
- $\ldots$

Proof System

Cryptographic Rules

Cryptographic Reduction

Cryptographic reductions are the main tool used in proofs of computational security.

Cryptographic Reduction $\mathcal{S} \leq_{\textsf{red}} \mathcal{H}$

*If you can break the **cryptographic design** $\mathcal{S}$, then you can break the **hardness assumption** $\mathcal{H}$ using roughly the same **time**.*

- We assume that $\mathcal{H}$ cannot be broken in a reasonable time:
  - Low-level assumptions: D-Log, DDH, ...
  - Higher-level assumptions: IND-CCA, EUF-MAC, PRF, ...
- Hence, $\mathcal{S}$ **cannot be broken in a reasonable time**.

Cryptographic Reduction $\mathcal{S} \leq_{\textsf{red}} \mathcal{H}$

$\mathcal{S}$ reduces to a hardness hypothesis $\mathcal{H}$ (e.g. IND-CCA, DDH) if:

$$\forall \mathcal{A}.\, \exists \mathcal{B}.\ \mathsf{Adv}^{\eta}_{\mathcal{S}}(\mathcal{A}) \leq P(\mathsf{Adv}^{\eta}_{\mathcal{H}}(\mathcal{B}), \eta)$$

where $\mathcal{A}$ and $\mathcal{B}$ are taken among PPTMs and P is a polynomial.

Cryptographic Rules

We are now going to give **rules** which capture some **cryptographic hardness hypotheses**.

The validity of these rules will be established through a **cryptographic reduction**.

- Asymmetric encryption: indistinguishability ($\mathsf{IND\text{-}CCA}_1$) and key-privacy ($\mathsf{KP\text{-}CCA}_1$);
- Hash function: collision-resistance (CR-HK);
- MAC: unforgeability (EUF-CMA).

Asymmetric Encryption Scheme

An **asymmetric encryption scheme** contains:

- public and private key generation functions $\mathsf{pk}(\_), \mathsf{sk}(\_)$;
- **randomized**[3] encryption function $\{\_\}_{\_}^{\_}$;
- a decryption function $\mathsf{dec}(\_, \_)$

It must satisfies the functional equality:

$$\mathsf{dec}(\{x\}_{\mathsf{pk}(y)}^{z}, \mathsf{sk}(y)) = x$$

[3] The role of the randomization will become clear later.

IND-CCA$_1$ Security

An encryption scheme is **indistinguishable against chosen cipher-text attacks** (IND-CCA$_1$) iff. for every PPTM $\mathcal{A}$ with access to:

- a left-right oracle $\mathcal{O}_{\mathsf{LR}}^{b,\mathsf{n}}(\cdot,\cdot)$:

$$\mathcal{O}_{\mathsf{LR}}^{b,\mathsf{n}}(m_0, m_1) \stackrel{\text{def}}{=} \begin{cases} \{m_b\}_{\mathsf{pk}(\mathsf{n})}^{\mathsf{r}} & \text{if } \mathsf{len}(m_1) = \mathsf{len}(m_2) \quad (\mathsf{r}\ \textit{fresh}) \\ 0 & \text{otherwise} \end{cases}$$

- and a decryption oracle $\mathcal{O}_{\mathsf{dec}}^{\mathsf{n}}(\cdot)$,

where $\mathcal{A}$ can call $\mathcal{O}_{\mathsf{LR}}$ once, and cannot call $\mathcal{O}_{\mathsf{dec}}$ after $\mathcal{O}_{\mathsf{LR}}$, then:

$$\left| \Pr_{\mathsf{n}}\left(\mathcal{A}^{\mathcal{O}_{\mathsf{LR}}^{1,\mathsf{n}},\mathcal{O}_{\mathsf{dec}}^{\mathsf{n}}}(1^\eta, \mathsf{pk}(\mathsf{n})) = 1\right) - \Pr_{\mathsf{n}}\left(\mathcal{A}^{\mathcal{O}_{\mathsf{LR}}^{0,\mathsf{n}},\mathcal{O}_{\mathsf{dec}}^{\mathsf{n}}}(1^\eta, \mathsf{pk}(\mathsf{n})) = 1\right) \right|$$

is negligible in η, where n is drawn uniformly in $\{0,1\}^\eta$.

IND-CCA$_1$ Security: Exercise

Exercise

Show that if the encryption **ignore its randomness**, i.e. there exists aenc(_, _) s.t. for all x, y, r:

$$\{x\}_y^r = \mathsf{aenc}(x, y)$$

then the encryption does not satisfy IND-CCA$_1$.

Indistinguishability Against Chosen Ciphertexts Attacks

If the encryption scheme is IND-CCA$_1$, then the *ground* rule:

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

is sound, when:

- r does not appear in $\vec{u}, t_0, t_1$, i.e. $\mathsf{r} \not\in \mathsf{st}(\vec{u}, t_0, t_1)$;
- n appears only in $\mathsf{pk}(\cdot)$ or $\mathsf{dec}(\_, \mathsf{sk}(\cdot))$ positions in $\vec{u}, t_0, t_1$, which we write:

$$\mathsf{n} \sqsubseteq_{\mathsf{pk}(\cdot),\mathsf{dec}(\_,\mathsf{sk}(\cdot))} \vec{u}, t_0, t_1$$

IND-CCA$_1$ Rule: Conditions

Definition: Positions

We write $\text{pos}(t) \in \{\epsilon\} \cup \mathbb{N}\,(\cdot\,\mathbb{N})^*$ the set of *positions* of t and $t_{|p}$ the sub-term of t at position p.

Example

if $t \equiv f(g(a,b),h(c))$ then $\text{pos}(t) = \{\epsilon, 0, 1, 0\cdot 0, 0\cdot 1, 1, 1\cdot 0\}$ and:

$$t_{|\epsilon} \equiv t \qquad t_{|0} \equiv g(a,b) \qquad t_{|0\cdot 0} \equiv a \qquad t_{|0\cdot 1} \equiv b \qquad t_{|1} \equiv h(c)$$

$$t_{|1\cdot 0} \equiv c$$

IND-CCA$_1$ Rule: Conditions

Definition: CCA$_1$ Side-Condition

$(\mathsf{n} \sqsubseteq_{\mathsf{pk}(\cdot),\mathsf{dec}(\_,\mathsf{sk}(\cdot))} u)$ iff. for any $p \in \mathsf{pos}(u)$, if $t_{|p} \equiv \mathsf{n}$, either:

- $p = p_0 \cdot 0$ and $t_{|p_0} \equiv \mathsf{pk}(\mathsf{n})$;
- or $p = p_0 \cdot 1 \cdot 0$ and $t_{|p_0} \equiv \mathsf{dec}(s, \mathsf{sk}(\mathsf{n}))$.

Examples (writing $\sqsubseteq$ instead of $\sqsubseteq_{\mathsf{pk}(\cdot),\mathsf{dec}(\_,\mathsf{sk}(\cdot))}$)

$\mathsf{n} \not\sqsubseteq \mathsf{n}$ $\quad$ $\mathsf{n} \sqsubseteq \mathsf{pk}(\mathsf{pk}(\mathsf{n}))$ $\quad$ $\mathsf{n} \sqsubseteq \mathsf{dec}(\mathsf{pk}(\mathsf{n}), \mathsf{sk}(\mathsf{n}))$

$\mathsf{n} \not\sqsubseteq \mathsf{dec}(\mathsf{sk}(\mathsf{n}), \mathsf{sk}(\mathsf{n}))$ $\quad$ $\mathsf{n} \sqsubseteq t$ if $\mathsf{n} \notin \mathsf{st}(t)$

IND-CCA$_1$ Rule: Proof

Proof sketch

Proof by contrapositive. Let $\mathbb{M}$ be a model, $\mathcal{A}$ an adversary and $\vec{u}, t_0, t_1$ ground terms such that:

$$\left| \begin{array}{l} \quad \Pr_\rho(\mathcal{A}(1^\eta, [\![\vec{u}]\!]_{\mathbb{M}}^{\eta,\rho}, [\![\{t_0\}_{\mathsf{pk}(\mathsf{n})}^{\mathsf{r}}]\!]_{\mathbb{M}}^{\eta,\rho}, \rho_\mathsf{a}) \\ - \Pr_\rho(\mathcal{A}(1^\eta, [\![\vec{u}]\!]_{\mathbb{M}}^{\eta,\rho}, [\![\{t_1\}_{\mathsf{pk}(\mathsf{n})}^{\mathsf{r}}]\!]_{\mathbb{M}}^{\eta,\rho}, \rho_\mathsf{a}) \end{array} \right|$$

is not negligible, and $\mathbb{M} \models [\mathsf{len}(t_0) = \mathsf{len}(t_1)]$.

We must build a PPTM $\mathcal{B}$ s.t. $\mathcal{B}$ wins the IND-CCA$_1$ security game.

IND-CCA$_1$ Rule: Proof

Let $\mathcal{B}^{\mathcal{O}_{\mathsf{LR}}^{b,\mathsf{n}},\mathcal{O}_{\mathsf{dec}}^{\mathsf{n}}}(1^\eta, [\![\mathsf{pk}(\mathsf{n})]\!]_{\mathbb{M}}^{\eta,\rho})$ be the following program:

i) **lazily**[4] samples the random tapes $(\rho_{\mathsf{a}}, \rho'_{\mathsf{h}})$ where:

$$\rho'_{\mathsf{h}} := \rho_{\mathsf{h}}[\mathsf{n} \mapsto 0, \mathsf{r} \mapsto 0]$$

ii) compute[5]:

$$w_{\vec{u}}, w_{t_0}, w_{t_1} := [\![\vec{u}, t_0, t_1]\!]_{\mathbb{M}}^{\eta,\rho}$$

using $(\rho_{\mathsf{a}}, \rho'_{\mathsf{h}})$, $[\![\mathsf{pk}(\mathsf{n})]\!]_{\mathbb{M}}^{\eta,\rho}$ and calls to $\mathcal{O}_{\mathsf{dec}}^{\mathsf{n}}$.

iii) return 0 if $\mathsf{len}(t_0) \neq \mathsf{len}(t_1)$.

iii) otherwise, compute:

$$w_{lr} := \mathcal{O}_{\mathsf{LR}}^{b,\mathsf{n}}(w_{t_0}, w_{t_1}) = [\![\{t_b\}_{\mathsf{pk}(\mathsf{n})}^{\mathsf{r}}]\!]_{\mathbb{M}}^{\eta,\rho}$$

iv) return $\mathcal{A}(1^\eta, w_{\vec{u}}, w_{lr}, \rho_{\mathsf{a}})$.

[4] Why do we need this?

[5] We describe how later.

IND-CCA$_1$ Rule: Proof

Then:

$$\begin{aligned}\mathsf{Adv}(\mathcal{A}) &\leq \mathsf{Adv}(\mathcal{A} \wedge \mathsf{len}(t_0) = \mathsf{len}(t_1)) + \mathsf{Pr}(\mathsf{len}(t_0) \neq \mathsf{len}(t_1)) && \text{(up-to-bad)}\\ &= \mathsf{Adv}(\mathcal{B} \wedge \mathsf{len}(t_0) = \mathsf{len}(t_1)) + \mathsf{Pr}(\mathsf{len}(t_0) \neq \mathsf{len}(t_1))\\ &= \mathsf{Adv}(\mathcal{B}) + \mathsf{Pr}(\mathsf{len}(t_0) \neq \mathsf{len}(t_1))\end{aligned}$$

Hence $\mathcal{B}$'s advantage against IND-CCA$_1$ is at least $\mathcal{A}$'s advantage against:

$$\vec{u}, \{t_0\}^{\mathsf{r}}_{\mathsf{pk(n)}} \sim \vec{u}, \{t_1\}^{\mathsf{r}}_{\mathsf{pk(n)}} \qquad (\dagger)$$

up-to a negligible quantity (the probability that $\mathsf{len}(t_0) \neq \mathsf{len}(t_1)$).

Since ($\dagger$) is assumed non-negligible, so is $\mathcal{B}$'s advantage.

IND-CCA$_1$ Rule: Proof

It only remains to explain how to do step *ii*) in polynomial time.

We prove by **structural induction** that for any subterm s of $\vec{u}, t_0, t_1$:

- either s is a forbidden subterm r, n, or sk(n);
- or $\mathcal{B}$ can compute $w_s := [\![s]\!]_{\mathbb{M}}^{\eta,\rho}$ in polynomial time.

Assuming this holds, we conclude by observing that IND-CCA$_1$ side conditions guarantees that $\vec{u}, t_0, t_1$ are not forbidden subterms.

IND-CCA$_1$ Rule: Proof

Induction. We are in one of the following cases:

- $s \in \mathcal{X}$ is not possible, since $\vec{u}, t_0, t_1$ are ground.
- $s \in \{\mathsf{r}, \mathsf{n}\}$ are forbidden, hence the induction hypothesis holds.
- $s \in \mathcal{N} \backslash \{\mathsf{r}, \mathsf{n}\}$, then $\mathcal{B}$ computes s directly from $\rho'_{\mathsf{h}} = \rho_{\mathsf{h}}[\mathsf{n} \mapsto 0, \mathsf{r} \mapsto 0]$.
- $s \equiv f(t_1, \ldots, t_n)$ and $t_1, \ldots, t_n$ are not forbidden. Then, by induction hypothesis, $\mathcal{B}$ can compute $w_i := [\![t_i]\!]^{\eta,\rho}_{\mathbb{M}}$ for any $1 \leq i \leq n$. Then $\mathcal{B}$ simply computes:

$$w_s := \begin{cases} (\!|f|\!)_{\mathbb{M}}(1^\eta, w_1, \ldots, w_n) & \text{if } f \in \mathcal{F} \\ (\!|f|\!)_{\mathbb{M}}(1^\eta, w_1, \ldots, w_n, \rho_{\mathsf{a}}) & \text{if } f \in \mathcal{G} \end{cases}$$

IND-CCA$_1$ Rule: Proof

case disjunction (continued):

- $s \equiv f(t_1, \ldots, t_n)$ and at least one of the t_i is forbidden.

  Using IND-CCA$_1$ side conditions, either s is either $\mathsf{pk}(\mathsf{n})$ or $\mathsf{dec}(m, \mathsf{sk}(\mathsf{n}))$.

  The first case is immediate since $\mathcal{B}$ receives $[\![\mathsf{pk}(\mathsf{n})]\!]_{\mathbb{M}}^{\eta,\rho}$ as argument.

  For the second case, from IND-CCA$_1$ side conditions, we know that $m \neq \mathsf{n}$ and $m \neq \mathsf{sk}(\mathsf{n})$. Hence, by **induction hypothesis**, $\mathcal{B}$ can compute $w_m = [\![m]\!]_{\mathbb{M}}^{\eta,\rho}$. We conclude using:

$$w_s := \mathcal{O}_{\mathsf{dec}}^{\mathsf{n}}(w_m) \qquad \square$$

IND-CCA$_1$ Rule: Exercise

Exercise

Which of the following formulas can be proven using IND-CCA$_1$?

$$\mathsf{pk}(n), \{0\}^{r}_{\mathsf{pk}(n)} \sim \mathsf{pk}(n), \{1\}^{r}_{\mathsf{pk}(n)}$$

$$\mathsf{pk}(n), \{0\}^{r}_{\mathsf{pk}(n)}, \{0\}^{r_0}_{\mathsf{pk}(n)} \sim \mathsf{pk}(n), \{1\}^{r}_{\mathsf{pk}(n)}, \{0\}^{r_0}_{\mathsf{pk}(n)}$$

$$\mathsf{pk}(n), \{0\}^{r}_{\mathsf{pk}(n)}, \{0\}^{r}_{\mathsf{pk}(n)} \sim \mathsf{pk}(n), \{0\}^{r}_{\mathsf{pk}(n)}, \{1\}^{r}_{\mathsf{pk}(n)}$$

$$\mathsf{pk}(n), \{0\}^{r}_{\mathsf{pk}(n)} \sim \mathsf{pk}(n), \{\mathsf{sk}(n)\}^{r}_{\mathsf{pk}(n)}$$

IND-CCA$_1$ Rule: Exercise

Exercise (Hybrid Argument)

Prove the following formula using IND-CCA$_1$:

$$\{0\}^{r_0}_{pk(n)}, \{1\}^{r_1}_{pk(n)}, \ldots, \{n\}^{r_n}_{pk(n)} \sim \{0\}^{r_0}_{pk(n)}, \{0\}^{r_1}_{pk(n)}, \ldots, \{0\}^{r_n}_{pk(n)}$$

Note: we assume that all plain-texts above have the same length (e.g. they are all represented over L bits, for L large enough)

KP-CCA$_1$ Security

A scheme provides **key privacy against chosen cipher-text attacks** (KP-CCA$_1$) iff for every PPTM $\mathcal{A}$ with access to:

- a left-right encryption oracle $\mathcal{O}_{\mathsf{LR}}^{b,\mathsf{n}_0,\mathsf{n}_1}(\cdot)$:

$$\mathcal{O}_{\mathsf{LR}}^{b,\mathsf{n}_0,\mathsf{n}_1}(m) \stackrel{\mathsf{def}}{=} \{m\}_{\mathsf{pk}(\mathsf{n}_b)}^{\mathsf{r}} \qquad (\mathsf{r}\ \textit{fresh})$$

- and two decryption oracles $\mathcal{O}_{\mathsf{dec}}^{\mathsf{n}_0}(\cdot)$ and $\mathcal{O}_{\mathsf{dec}}^{\mathsf{n}_1}(\cdot)$,

where $\mathcal{A}$ can call $\mathcal{O}_{\mathsf{LR}}$ once, and cannot call the decryption oracles after $\mathcal{O}_{\mathsf{LR}}$, then:

$$\left| \begin{array}{l} \quad \Pr_{\mathsf{n}_0,\mathsf{n}_1}\left(\mathcal{A}^{\mathcal{O}_{\mathsf{LR}}^{1,\mathsf{n}_0,\mathsf{n}_1},\mathcal{O}_{\mathsf{dec}}^{\mathsf{n}_0},\mathcal{O}_{\mathsf{dec}}^{\mathsf{n}_1}}(1^\eta, \mathsf{pk}(\mathsf{n}_0), \mathsf{pk}(\mathsf{n}_1)) = 1\right) \\ - \Pr_{\mathsf{n}_0,\mathsf{n}_1}\left(\mathcal{A}^{\mathcal{O}_{\mathsf{LR}}^{0,\mathsf{n}_0,\mathsf{n}_1},\mathcal{O}_{\mathsf{dec}}^{\mathsf{n}_0},\mathcal{O}_{\mathsf{dec}}^{\mathsf{n}_1}}(1^\eta, \mathsf{pk}(\mathsf{n}_0), \mathsf{pk}(\mathsf{n}_1)) = 1\right) \end{array} \right|$$

is negligible in η, where $\mathsf{n}_0, \mathsf{n}_1$ are drawn in $\{0,1\}^\eta$.

Security Notions: Exercise

Exercise

Show that $\text{IND-CCA}_1 \not\Rightarrow \text{KP-CCA}_1$ and $\text{KP-CCA}_1 \not\Rightarrow \text{IND-CCA}_1$.

KP-CCA$_1$ Rule

Key Privacy Against Chosen Ciphertexts Attacks

If the encryption scheme is KP-CCA$_1$, then the *ground* rule:

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

is sound, when:

- r does not appear in $\vec{u}, t$;
- $\mathsf{n}_0, \mathsf{n}_1$ appear only in $\mathsf{pk}(\cdot)$ or $\mathsf{dec}(\_, \mathsf{sk}(\cdot))$ positions in $\vec{u}, t$.

The **proof** is similar to the IND-CCA$_1$ soundness proof. We omit it.