Symbolic Verification of Cryptographic Protocols

A Computationally Complete Symbolic Attacker

David Baelde

LSV, ENS Paris-Saclay

2018–2019

Intro

What would it take to make symbolic analyses of equivalences relevant to the computational model ?

- Interpret terms as computations of probabilistic Turing machine.
- Make precise assumptions about primitives e.g. IND-CCA1.
- Interpret equality as the almost-always coincidence of two computations, which may be larger than $=_E$.
- Give up non-determinism: determinate processes only.
- Do not reason explicitly about these machines and interpretations.

Semantics: terms

We want to interpret t as probabilistic Turing computation $[\![t]\!]^{\sigma}_{\eta,\rho}$

- with security parameter $\eta \in \mathbb{N}$;
- with read-only infinite binary tapes $\rho = \rho_1, \rho_2$ of protocol and attacker randomness;
- where σ interprets free variables as Turing machines.

Definition

- $[\![x]\!]^{\sigma}_{\eta,\rho} = \sigma(x)(1^{\eta}; \rho)$
- names interpreted as non-overlapping portions $[\![n]\!]^{\sigma}_{\eta,\rho}$ of ρ_1
- any function symbol f of arity n interpreted as deterministic polynomial-time n-ary computation

Semantics: LTS

We modify the LTS for this computational setting:

$$(\mathbf{out}(c,u).P \mid Q, \Phi, \sigma) \xrightarrow{\mathbf{out}(c,w)} (P \mid Q, \Phi + \{w \mapsto u\}, \sigma)$$

$$(\mathbf{in}(c,x).P \mid Q, \Phi, \sigma) \xrightarrow{\mathbf{in}(c,x)} (P \mid Q, \Phi, \sigma + \{x \mapsto \mathcal{A}_x(\llbracket \Phi \rrbracket^{\sigma}_{\eta,\rho}, \eta, \rho)\})$$
where $\mathcal{A}_x$ is a PPTIME Turing machine

$$(\mathbf{if}\ u = v\ \mathbf{then}\ P\ \mathbf{else}\ Q \mid R, \Phi, \sigma) \xrightarrow{\tau} (P \mid R, \Phi, \sigma) \quad \text{if } \llbracket u \rrbracket^{\sigma}_{\eta,\rho} = \llbracket v \rrbracket^{\sigma}_{\eta,\rho}$$

$$(\mathbf{if}\ u = v\ \mathbf{then}\ P\ \mathbf{else}\ Q \mid R, \Phi, \sigma) \xrightarrow{\tau} (Q \mid R, \Phi, \sigma) \quad \text{if } \llbracket u \rrbracket^{\sigma}_{\eta,\rho} \neq \llbracket v \rrbracket^{\sigma}_{\eta,\rho}$$

$$(\mathbf{new}\ n.P \mid Q, \Phi, \sigma) \xrightarrow{\tau} (P \mid Q, n.\Phi, \sigma) \quad \text{if } n \notin \mathrm{bn}(\Phi)$$

Define $K \overset{\alpha}{\Rightarrow} K'$ to hold iff $K \xrightarrow{\alpha} K_\alpha \xrightarrow{\tau}^{*} K'$ and $K' \not\xrightarrow{\tau}$.

Semantics: indistinguishability

We say that $P \sim_{\mathcal{M}} Q$ when, for any PPTIME adversary $\mathcal{A}$, the following advantage is negligible in η:

$$|\mathbf{Pr}\{\rho\ :\ \mathcal{A}^{P}_{\eta,\rho} = 1\} - \mathbf{Pr}\{\rho\ :\ \mathcal{A}^{Q}_{\eta,\rho} = 1\}|$$

Here $\mathcal{A}^{P}_{\eta,\rho}$ may extract randomness from ρ_2, interact with P by choosing observable actions and input values, and receiving output values.

Equivalently: for any tr, for any PPTIME machines $(\mathcal{A}_x)_{\mathbf{in}(c,x)\in \mathrm{tr}}$ and $\mathcal{A}$, the following is well-defined and negligible in η:

$$|\mathbf{Pr}\{\rho\ :\ \mathcal{A}([\![\Phi(P^{\mathrm{tr}})]\!]^{\sigma}_{\eta,\rho}) = 1\} - \mathbf{Pr}\{\rho\ :\ \mathcal{A}([\![\Phi(Q^{\mathrm{tr}})]\!]^{\sigma}_{\eta,\rho}) = 1\}|$$

where P^{tr} is the result of executing tr with inputs given by $(\mathcal{A}_x)_x$.

First-order logic

Turing machines are just one particular model for our terms.

Introduce attacker terms for a given tr:

- for each $\mathbf{in}(c, x) \in \mathrm{tr}$,
  take symbol g_x of arity the number of preceding outputs;
- conceptually replace $\mathcal{A}_x(\Phi, \eta, \rho)$ by $[\![g_x]\!]([\![\Phi]\!]^{\sigma}_{\eta,\rho}, \rho_2) \stackrel{def}{=} [\![g_x(\Phi)]\!]^{\sigma}_{\eta,\rho}$.

First-order logic

Turing machines are just one particular model for our terms.
Introduce attacker terms for a given tr:

- for each $\mathbf{in}(c, x) \in \mathrm{tr}$,
  take symbol g_x of arity the number of preceding outputs;
- conceptually replace $\mathcal{A}_x(\Phi, \eta, \rho)$ by $[\![g_x]\!]([\![\Phi]\!]^{\sigma}_{\eta,\rho}, \rho_2) \stackrel{def}{=} [\![g_x(\Phi)]\!]^{\sigma}_{\eta,\rho}$.

Theorem

P and Q are computationally indistinguishable if:

- P and Q must perform the same traces tr;
- for each such tr, $\mathrm{fold}(P, \mathrm{tr}) \sim \mathrm{fold}(Q, \mathrm{tr})$ is valid.

Example

$P = \mathbf{new}\ m.\ \mathbf{in}(c, x).\mathbf{out}(c, m)$
$Q = \mathbf{new}\ n.\ \mathbf{in}(c, x).\mathbf{if}\ x = n\ \mathbf{then}\ \mathbf{out}(c, \mathbf{0})\ \mathbf{else}\ \mathbf{out}(c, n)$
$\mathrm{tr} = \mathbf{in}(c, x).\mathbf{out}(c, w)$ induces $m \sim \mathbf{if}\ \mathrm{EQ}(g_x(), n)\ \mathbf{then}\ \mathbf{0}\ \mathbf{else}\ n$.

First-order logic

Turing machines are just one particular model for our terms.
Introduce attacker terms for a given tr:

- for each $\mathbf{in}(c, x) \in \mathrm{tr}$,
  take symbol g_x of arity the number of preceding outputs;
- conceptually replace $\mathcal{A}_x(\Phi, \eta, \rho)$ by $[\![g_x]\!]([\![\Phi]\!]^{\sigma}_{\eta,\rho}, \rho_2) \stackrel{def}{=} [\![g_x(\Phi)]\!]^{\sigma}_{\eta,\rho}$.

Theorem

P and Q are computationally indistinguishable if:

- P and Q must perform the same traces tr;
- for each such tr, $\mathrm{fold}(P, \mathrm{tr}) \not\sim \mathrm{fold}(Q, \mathrm{tr})$ inconsistent with Axioms.

Example

$P = \mathbf{new}\ m.\ \mathbf{in}(c, x).\mathbf{out}(c, m)$
$Q = \mathbf{new}\ n.\ \mathbf{in}(c, x).\mathbf{if}\ x = n\ \mathbf{then}\ \mathbf{out}(c, \mathbf{0})\ \mathbf{else}\ \mathbf{out}(c, n)$
$\mathrm{tr} = \mathbf{in}(c, x).\mathbf{out}(c, w)$ induces $m \sim \mathbf{if}\ \mathrm{EQ}(g_x(), n)\ \mathbf{then}\ \mathbf{0}\ \mathbf{else}\ n$.

Axioms: basic examples

Force enough things that are valid in computational models, using recursive axiom schemes. For example:

$$\forall \vec{x}, \vec{y}, \vec{z}, \vec{w}. \quad \vec{x}, \vec{z} \sim \vec{y}, \vec{w} \Rightarrow f(\vec{x}), \vec{z} \sim f(\vec{y}), \vec{w}$$

$$\forall \vec{x}, \vec{y}, z, z'. \quad \vec{x}, z \sim \vec{y}, z' \Rightarrow \vec{x}, z, z \sim \vec{y}, z', z'$$

$$\forall \vec{x}, \vec{y}. \quad x_1, \ldots, x_n \sim y_1, \ldots, y_n \Rightarrow x_{\pi(1)}, \ldots, x_{\pi(n)} \sim y_{\pi(1)}, \ldots, y_{\pi(n)}$$

where π is any permutation

$$\vec{u} \sim \vec{v} \Rightarrow \vec{u}, n \sim \vec{v}, m$$

for any terms such that $n \notin \mathrm{fn}(\vec{u})$, $m \notin \mathrm{fn}(\vec{v})$

$$\forall x, y, z, \vec{u}, \vec{v}. \quad \textbf{if } \mathrm{EQ}(x, y) \textbf{ then } t[x] \textbf{ else } z, \vec{u} \sim \vec{v} \Rightarrow \textbf{if } \mathrm{EQ}(x, y) \textbf{ then } t[y] \textbf{ else } z, \vec{u} \sim \vec{v}$$

$$\forall b, \vec{w}, x, z. \quad b, \vec{w}, x \sim b, \vec{w}, z \wedge b, \vec{w}, y \sim b, \vec{w}, z \Rightarrow \vec{w}, \textbf{if } b \textbf{ then } x \textbf{ else } y \sim \vec{w}, z$$

Axioms: a counter-example

Removing b from hypotheses in previous axiom yields an unsound one:

$$\begin{array}{ll}\forall b, \vec{w}, x, z. & \vec{w}, x \sim \vec{w}, z \wedge \vec{w}, y \sim \vec{w}, z \\ & \Rightarrow \vec{w}, \textbf{if } b \textbf{ then } x \textbf{ else } y \sim \vec{w}, z\end{array}$$

Assume we have symbols fst and neg, interpreted in some model as the extraction of the first bit and negation respectively. Then we have

$$\mathsf{fst}(n) \sim \mathsf{fst}(n) \quad \text{and} \quad \mathsf{neg}(\mathsf{fst}(n)) \sim \mathsf{fst}(n)$$

but

$$\textbf{if } \mathsf{fst}(n) \textbf{ then } \mathsf{fst}(n) \textbf{ else } \mathsf{neg}(\mathsf{fst}(n)) \not\sim \mathsf{fst}(n).$$

The previous (sound) axiom would not allow to derive this incorrect indistinguishability, since $\mathsf{fst}(n), \mathsf{fst}(n) \not\sim \mathsf{fst}(n), \mathsf{neg}(\mathsf{fst}(n)).$

Axioms: equality

In a computational model,

- $[\![\mathsf{EQ}(u,v)]\!]^{\sigma}_{\eta,\rho} = [\![\mathit{true}]\!]^{\sigma}_{\eta,\rho}$ iff $[\![u]\!]^{\sigma}_{\eta,\rho} = [\![v]\!]^{\sigma}_{\eta,\rho}$;
- $\mathsf{EQ}(u,v) \sim \mathsf{true}$: $[\![u]\!]^{\sigma}_{\eta,\rho} = [\![v]\!]^{\sigma}_{\eta,\rho}$ with overwhelming probability;
- $u = v$: shorthand for $\mathsf{EQ}(u,v) \sim \mathsf{true}$.

Example axioms on equality:

$$
\begin{array}{rll}
\forall x,y. & x = y \wedge \Phi[x] \Rightarrow \Phi[y] & \\
\forall x. & \mathsf{EQ}(x,x) = \mathsf{true} & \\
 & \mathsf{EQ}(n,u) = \mathsf{false} & \text{when } n \notin \mathsf{fn}(u) \\
\forall x,y. & \textbf{if } \mathsf{true} \textbf{ then } x \textbf{ else } y = x & \\
\forall x,y. & \textbf{if } \mathsf{false} \textbf{ then } x \textbf{ else } y = y & \\
\forall b,x,y,z,. & \textbf{if } b \textbf{ then if } b \textbf{ then } x \textbf{ else } y \textbf{ else } z = \textbf{if } b \textbf{ then } x \textbf{ else } z & \\
\forall x,y. & \mathbf{proj}_1(\mathbf{pair}(x,y)) = x &
\end{array}
$$

Axioms: encryption

The following axiom scheme is satisfied when $[\![\mathbf{aenc}]\!]$ is IND-CCA1:

$$\vec{v}, \textbf{if}\ \mathsf{EQL}(u, u')\ \textbf{then}\ \{u\}^{r}_{\mathsf{pk}_a}\ \textbf{else}\ u'' \sim \vec{v}, \textbf{if}\ \mathsf{EQL}(u, u')\ \textbf{then}\ \{u'\}^{r'}_{\mathsf{pk}_a}\ \textbf{else}\ u''$$

provided:

- r and r' do not appear in other terms;
- sk_a only occurs in decryption position in $\vec{v}, u, u', u''$.

If $[\![\mathbf{aenc}]\!]$ ensures key privacy, then

$$\vec{v}, \{u\}^{r}_{\mathsf{pk}_a} \sim \vec{v}, \{u\}^{r'}_{\mathsf{pk}_{a'}}$$

holds whenever r and r' are fresh and secret keys for a and a' do not occur, in particular there are no decryptions using these keys.

Private authentication: attacks / counter-models

$I(sk_a, pk_b)$	$R(sk_b, pk_a)$
new r, n_a.	**new** r, n_b.
let $pk_a = \mathbf{pub}(sk_a)$ **in**	**let** $pk_b = \mathbf{pub}(sk_b)$ **in**
$\mathbf{out}(c, \{\mathbf{pair}(n_a, pk_a)\}^r_{pk_b}))$.	$\mathbf{in}(c, x)$.**let** $y = \mathbf{adec}(x, sk_b)$ **in**
$\ldots$	**if** $\mathbf{proj}_2(y) = pk_a$
	then $\mathbf{out}(c, \{\langle \mathbf{proj}_1(y), n_b \rangle\}^r_{pk_a})$
	else $\mathbf{out}(c, \{n_b\}^r_{pk_a}))$

Anonymity

$R(sk_b, \mathbf{pub}(sk_a)) \approx^? R(sk_b, \mathbf{pub}(sk_c))$

$I(sk_a, pk_b)$	$R(sk_b, pk_a)$
new r, n_a.	**new** r, n_b.
let $pk_a = \mathbf{pub}(sk_a)$ **in**	**let** $pk_b = \mathbf{pub}(sk_b)$ **in**
$\mathbf{out}(c, \{\mathbf{pair}(n_a, pk_a)\}^r_{pk_b}))$.	$\mathbf{in}(c, x)$.**let** $y = \mathbf{adec}(x, sk_b)$ **in**
$\ldots$	**if** $\mathbf{proj}_2(y) = pk_a$
	then $\mathbf{out}(c, \{\langle \mathbf{proj}_1(y), n_b \rangle\}^r_{pk_a})$
	else $\mathbf{out}(c, \{n_b\}^r_{pk_a}))$

Anonymity

Φ_0, **if** $\mathrm{EQ}(\mathbf{proj}_2(h), pk_a)$ **then** $\{\langle \mathbf{proj}_1(h), n_b \rangle\}^r_{pk_a}$ **else** $\{n_b\}^r_{pk_a} \sim^?$
Φ_0, **if** $\mathrm{EQ}(\mathbf{proj}_2(h), pk_c)$ **then** $\{\langle \mathbf{proj}_1(h), n_b \rangle\}^r_{pk_c}$ **else** $\{n_b\}^r_{pk_c}$
where $h = \mathbf{adec}(g_x(\Phi_0), sk_b)$.

$I(sk_a, pk_b)$	$R(sk_b, pk_a)$
new r, n_a.	**new** r, n_b.
let $pk_a = \mathbf{pub}(sk_a)$ **in**	**let** $pk_b = \mathbf{pub}(sk_b)$ **in**
$\mathbf{out}(c, \{\mathbf{pair}(n_a, pk_a)\}^r_{pk_b}))$.	$\mathbf{in}(c, x)$.**let** $y = \mathbf{adec}(x, sk_b)$ **in**
$\ldots$	**if** $\mathbf{proj}_2(y) = pk_a$
	then $\mathbf{out}(c, \{\langle \mathbf{proj}_1(y), n_b \rangle\}^r_{pk_a})$
	else $\mathbf{out}(c, \{\langle n_b, n_b \rangle\}^r_{pk_a}))$

Anonymity

Φ_0, **if** $\mathrm{EQ}(\mathbf{proj}_2(h), pk_a)$ **then** $\{\langle \mathbf{proj}_1(h), n_b \rangle\}^r_{pk_a}$ **else** $\{\langle n_b, n_b \rangle\}^r_{pk_a} \sim^?$
Φ_0, **if** $\mathrm{EQ}(\mathbf{proj}_2(h), pk_c)$ **then** $\{\langle \mathbf{proj}_1(h), n_b \rangle\}^r_{pk_c}$ **else** $\{\langle n_b, n_b \rangle\}^r_{pk_c}$
where $h = \mathbf{adec}(g_x(\Phi_0), sk_b)$.

$I(sk_a, pk_b)$	$R(sk_b, pk_a)$
new r, n_a.	**new** r, n_b.
let $pk_a = \mathbf{pub}(sk_a)$ **in**	**let** $pk_b = \mathbf{pub}(sk_b)$ **in**
$\mathbf{out}(c, \{\mathbf{pair}(n_a, pk_a)\}^r_{pk_b}))$.	$\mathbf{in}(c, x)$.**let** $y = \mathbf{adec}(x, sk_b)$ **in**
$\ldots$	**if** $\mathbf{proj}_2(y) = pk_a \wedge \mathrm{EQL}(\mathbf{proj}_1(y), n_b)$
	then $\mathbf{out}(c, \{\langle \mathbf{proj}_1(y), n_b \rangle\}^r_{pk_a})$
	else $\mathbf{out}(c, \{\langle n_b, n_b \rangle\}^r_{pk_a}))$

Anonymity

Φ_0, **if** $\mathrm{EQ}(\mathbf{proj}_2(h), pk_a)$ **then** $\{\langle \mathbf{proj}_1(h), n_b \rangle\}^r_{pk_a}$ **else** $\{\langle n_b, n_b \rangle\}^r_{pk_a} \sim^?$
Φ_0, **if** $\mathrm{EQ}(\mathbf{proj}_2(h), pk_c)$ **then** $\{\langle \mathbf{proj}_1(h), n_b \rangle\}^r_{pk_c}$ **else** $\{\langle n_b, n_b \rangle\}^r_{pk_c}$
where $h = \mathbf{adec}(g_x(\Phi_0), sk_b)$.

Private authentication: proof / validity

$$\begin{aligned}\Phi_a = \Phi_0, \textbf{if}\ & \mathrm{EQ}(\mathbf{proj}_2(h), pk_a) \wedge \\ & \mathrm{EQL}(\mathbf{proj}_1(h), n_b)\ \textbf{then}\ \{\langle \mathbf{proj}_1(h), n_b \rangle\}^r_{pk_a}\ \textbf{else}\ \{\langle n_b, n_b \rangle\}^r_{pk_a} \\ \Phi_c = \Phi_0, \textbf{if}\ & \mathrm{EQ}(\mathbf{proj}_2(h), pk_c) \wedge \\ & \mathrm{EQL}(\mathbf{proj}_1(h), n_b)\ \textbf{then}\ \{\langle \mathbf{proj}_1(h), n_b \rangle\}^r_{pk_c}\ \textbf{else}\ \{\langle n_b, n_b \rangle\}^r_{pk_c}\end{aligned}$$

$\Phi_a \sim \Phi_c$ in any model of the axioms, in particular in any computational model whose encryption scheme satisfies IND-CCA1 and key privacy.

Private authentication: proof / validity

$$\Phi_a = \Phi_0, \textbf{if } \mathrm{EQ}(\mathbf{proj}_2(h), pk_a) \wedge \mathrm{EQL}(\mathbf{proj}_1(h), n_b) \textbf{ then } \{\langle \mathbf{proj}_1(h), n_b \rangle\}^r_{pk_a} \textbf{ else } \{\langle n_b, n_b \rangle\}^r_{pk_a}$$

$$\Phi_c = \Phi_0, \textbf{if } \mathrm{EQ}(\mathbf{proj}_2(h), pk_c) \wedge \mathrm{EQL}(\mathbf{proj}_1(h), n_b) \textbf{ then } \{\langle \mathbf{proj}_1(h), n_b \rangle\}^r_{pk_c} \textbf{ else } \{\langle n_b, n_b \rangle\}^r_{pk_c}$$

$\Phi_a \sim \Phi_c$ in any model of the axioms, in particular in any computational model whose encryption scheme satisfies IND-CCA1 and key privacy.

- $\Phi_0, \mathrm{EQ}_a, \textbf{if } \mathrm{EQL} \textbf{ then } \{\langle n_b, n_b \rangle\}^r_{pk_a} \textbf{ else } \{\langle n_b, n_b \rangle\}^r_{pk_a} \sim \Phi_0, \mathrm{EQ}_a, \{\langle n_b, n_b \rangle\}^r_{pk_a}$;

Private authentication: proof / validity

$$\Phi_a = \Phi_0, \textbf{if } \mathrm{EQ}(\textbf{proj}_\textbf{2}(h), pk_a) \wedge \mathrm{EQL}(\textbf{proj}_\textbf{1}(h), n_b) \textbf{ then } \{\langle \textbf{proj}_\textbf{1}(h), n_b\rangle\}^r_{pk_a} \textbf{ else } \{\langle n_b, n_b\rangle\}^r_{pk_a}$$

$$\Phi_c = \Phi_0, \textbf{if } \mathrm{EQ}(\textbf{proj}_\textbf{2}(h), pk_c) \wedge \mathrm{EQL}(\textbf{proj}_\textbf{1}(h), n_b) \textbf{ then } \{\langle \textbf{proj}_\textbf{1}(h), n_b\rangle\}^r_{pk_c} \textbf{ else } \{\langle n_b, n_b\rangle\}^r_{pk_c}$$

$\Phi_a \sim \Phi_c$ in any model of the axioms, in particular in any computational model whose encryption scheme satisfies IND-CCA1 and key privacy.

- $\Phi_0, \mathrm{EQ}_a, \textbf{if } \mathrm{EQL} \textbf{ then } \{\langle n_b, n_b\rangle\}^r_{pk_a} \textbf{ else } \{\langle n_b, n_b\rangle\}^r_{pk_a} \sim \Phi_0, \mathrm{EQ}_a, \{\langle n_b, n_b\rangle\}^r_{pk_a}$;
- $\Phi_0, \mathrm{EQ}_a, \textbf{if } \mathrm{EQL} \textbf{ then } \{\langle \textbf{proj}_\textbf{1}(h), n_b\rangle\}^r_{pk_a} \textbf{ else } \{\langle n_b, n_b\rangle\}^r_{pk_a} \sim \Phi_0, \mathrm{EQ}_a, \textbf{if } \mathrm{EQL} \textbf{ then } \{\langle n_b, n_b\rangle\}^r_{pk_a} \textbf{ else } \{\langle n_b, n_b\rangle\}^r_{pk_a}$ by IND-CCA1;

Private authentication: proof / validity

$$\Phi_a = \Phi_0, \textbf{if } \mathrm{EQ}(\mathbf{proj}_2(h), pk_a) \wedge \mathrm{EQL}(\mathbf{proj}_1(h), n_b) \textbf{ then } \{\langle \mathbf{proj}_1(h), n_b \rangle\}^r_{pk_a} \textbf{ else } \{\langle n_b, n_b \rangle\}^r_{pk_a}$$

$$\Phi_c = \Phi_0, \textbf{if } \mathrm{EQ}(\mathbf{proj}_2(h), pk_c) \wedge \mathrm{EQL}(\mathbf{proj}_1(h), n_b) \textbf{ then } \{\langle \mathbf{proj}_1(h), n_b \rangle\}^r_{pk_c} \textbf{ else } \{\langle n_b, n_b \rangle\}^r_{pk_c}$$

$\Phi_a \sim \Phi_c$ in any model of the axioms, in particular in any computational model whose encryption scheme satisfies IND-CCA1 and key privacy.

- $\Phi_0, \mathrm{EQ}_a, \textbf{if } \mathrm{EQL} \textbf{ then } \{\langle n_b, n_b \rangle\}^r_{pk_a} \textbf{ else } \{\langle n_b, n_b \rangle\}^r_{pk_a} \sim \Phi_0, \mathrm{EQ}_a, \{\langle n_b, n_b \rangle\}^r_{pk_a}$;
- $\Phi_0, \mathrm{EQ}_a, \textbf{if } \mathrm{EQL} \textbf{ then } \{\langle \mathbf{proj}_1(h), n_b \rangle\}^r_{pk_a} \textbf{ else } \{\langle n_b, n_b \rangle\}^r_{pk_a} \sim \Phi_0, \mathrm{EQ}_a, \textbf{if } \mathrm{EQL} \textbf{ then } \{\langle n_b, n_b \rangle\}^r_{pk_a} \textbf{ else } \{\langle n_b, n_b \rangle\}^r_{pk_a}$ by IND-CCA1;
- $\Phi_0, \mathrm{EQ}_a, \textbf{if } \mathrm{EQL} \textbf{ then } \{\langle \mathbf{proj}_1(h), n_b \rangle\}^r_{pk_a} \textbf{ else } \{\langle n_b, n_b \rangle\}^r_{pk_a} \sim \Phi_0, \mathrm{EQ}_a, \{\langle n_b, n_b \rangle\}^r_{pk_a}$ by transitivity;

Private authentication: proof / validity

$$\Phi_a = \Phi_0, \textbf{if } \mathrm{EQ}(\textbf{proj}_2(h), pk_a) \wedge \\ \mathrm{EQL}(\textbf{proj}_1(h), n_b) \textbf{ then } \{\langle \textbf{proj}_1(h), n_b\rangle\}^r_{pk_a} \textbf{ else } \{\langle n_b, n_b\rangle\}^r_{pk_a}$$

$$\Phi_c = \Phi_0, \textbf{if } \mathrm{EQ}(\textbf{proj}_2(h), pk_c) \wedge \\ \mathrm{EQL}(\textbf{proj}_1(h), n_b) \textbf{ then } \{\langle \textbf{proj}_1(h), n_b\rangle\}^r_{pk_c} \textbf{ else } \{\langle n_b, n_b\rangle\}^r_{pk_c}$$

$\Phi_a \sim \Phi_c$ in any model of the axioms, in particular in any computational model whose encryption scheme satisfies IND-CCA1 and key privacy.

- $\Phi_0, \mathrm{EQ}_a, \textbf{if } \mathrm{EQL} \textbf{ then } \{\langle n_b, n_b\rangle\}^r_{pk_a} \textbf{ else } \{\langle n_b, n_b\rangle\}^r_{pk_a} \sim \Phi_0, \mathrm{EQ}_a, \{\langle n_b, n_b\rangle\}^r_{pk_a}$;
- $\Phi_0, \mathrm{EQ}_a, \textbf{if } \mathrm{EQL} \textbf{ then } \{\langle \textbf{proj}_1(h), n_b\rangle\}^r_{pk_a} \textbf{ else } \{\langle n_b, n_b\rangle\}^r_{pk_a} \sim \Phi_0, \mathrm{EQ}_a, \textbf{if } \mathrm{EQL} \textbf{ then } \{\langle n_b, n_b\rangle\}^r_{pk_a} \textbf{ else } \{\langle n_b, n_b\rangle\}^r_{pk_a}$ by IND-CCA1;
- $\Phi_0, \mathrm{EQ}_a, \textbf{if } \mathrm{EQL} \textbf{ then } \{\langle \textbf{proj}_1(h), n_b\rangle\}^r_{pk_a} \textbf{ else } \{\langle n_b, n_b\rangle\}^r_{pk_a} \sim \Phi_0, \mathrm{EQ}_a, \{\langle n_b, n_b\rangle\}^r_{pk_a}$ by transitivity;
- $\Phi_a \sim \Phi_0, \{\langle n_b, n_b\rangle\}^r_{pk_a}$ by basic axiom on conditional;
- $\Phi_a \sim \Phi_b$ by the previous item for a and a' and key privacy.