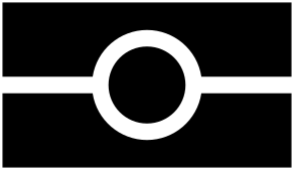
Automated Verification of Privacy

Laouen Fernet

SSE Research Workshop, DTU Compute
lpkf@dtu.dk

June 13, 2024



A Logical Approach for Automated Reasoning about Privacy in Security Protocols


L. Fernet, S. Mödersheim, and L. Viganò.
A decision procedure for alpha-beta privacy for a bounded number of transitions.
In *CSF 2024 (to appear)*. IEEE, 2024.
Extended version at `https://people.compute.dtu.dk/lpkf`.


L. Fernet and S. Mödersheim.
Private authentication with alpha-beta-privacy.
In *OID 2023*, LNI. GI, 2023.


L. Fernet, S. Mödersheim, and L. Viganò.
A typing result for alpha-beta privacy.
Technical report, DTU Compute; KCL Informatics, 2024.
Will be submitted as journal extension.


L. Fernet, S. Mödersheim, and L. Viganò.
A compositionality result for alpha-beta privacy.
Submitted to CSF 2025.

Encrypted messages: $\mathsf{scrypt}(k, m, r), \mathsf{crypt}(k, m, r)$

where

$\mathsf{dscrypt}(k, \mathsf{scrypt}(k, m, r)) \approx m$

$\mathsf{dcrypt}(\mathsf{inv}(k), \mathsf{crypt}(k, m, r)) \approx m$

$$\mathit{struct} = [l_1 \mapsto \mathsf{inv}(\mathsf{pk}(\mathsf{i})), l_2 \mapsto \mathsf{crypt}(\mathsf{pk}(x), \mathsf{pair}(y, \mathsf{n}), \mathsf{r})]$$
$$\mathit{concr} = [l_1 \mapsto \mathsf{inv}(\mathsf{pk}(\mathsf{i})), l_2 \mapsto \mathsf{crypt}(\mathsf{pk}(\mathsf{a}), \mathsf{pair}(\mathsf{b}, \mathsf{n}), \mathsf{r})]$$




v_1 v_2 v_3 v_4

- $\alpha \equiv v_1, v_2, v_3, v_4 \in \{0, 1\} \wedge v_1 + v_2 + v_3 + v_4 \doteq 2$
- β includes α and encrypted ballots etc.




v_1 v_2 v_3 v_4

- $\alpha \equiv v_1, v_2, v_3, v_4 \in \{0, 1\} \wedge v_1 + v_2 + v_3 + v_4 \doteq 2$
- β includes α and encrypted ballots etc.
- If $\beta \Rightarrow v_1 \doteq v_4 \wedge v_2 \doteq v_3$: privacy violation

$\star\ x \in \mathsf{Agent}.$

$\star\ y \in \{\mathsf{yes}, \mathsf{no}\}.$

$\mathsf{rcv}(M).$

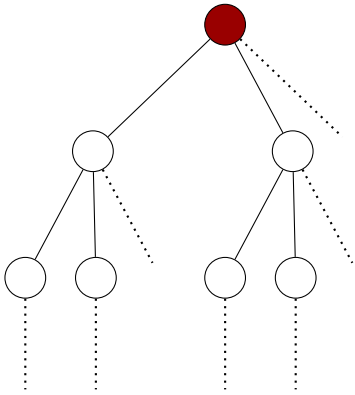
$\mathsf{try}\ N := \mathsf{dcrypt}(\mathsf{inv}(\mathsf{pk}(\mathsf{s})), M)\ \mathsf{in}$

$\mathsf{if}\ y \doteq \mathsf{yes}\ \mathsf{then}$

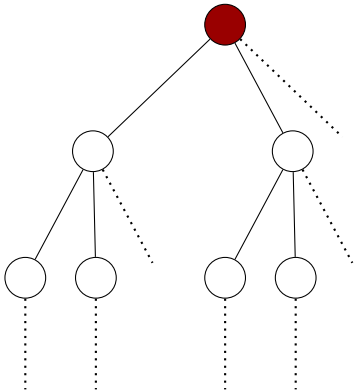
$\quad \nu R.\ \mathsf{snd}(\mathsf{crypt}(\mathsf{pk}(x), \mathsf{pair}(\mathsf{yes}, N), R))$

else

$\quad \nu R.\ \mathsf{snd}(\mathsf{crypt}(\mathsf{pk}(x), \mathsf{no}, R))$

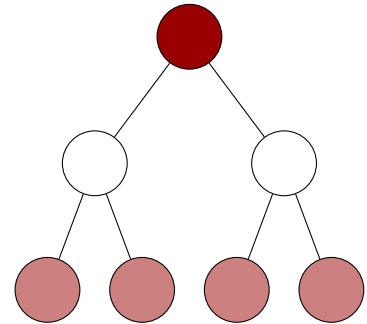


(α, β) in every state



(α, β) in every state

$\longrightarrow$



Several (α_i, β_i) in every symbolic state

$\star\ x \in \mathsf{Agent}.$

$\star\ y \in \{\mathsf{yes}, \mathsf{no}\}.$

$\mathsf{rcv}(\mathsf{crypt}(\mathsf{pk}(\mathsf{s}), N, \_)).$

if $y \doteq \mathsf{yes}$ then

$\quad \nu R.\ \mathsf{snd}(\mathsf{crypt}(\mathsf{pk}(x), \mathsf{pair}(\mathsf{yes}, N), R))$

else

$\quad \nu R.\ \mathsf{snd}(\mathsf{crypt}(\mathsf{pk}(x), \mathsf{pair}(\mathsf{no}, N), R))$

$Spec = Spec_1 \parallel Spec_2$

If $Spec$ is composable and $Spec|_1$ and $Spec|_2$ are secure, then $Spec$ is secure.

A Logical Approach for Automated Reasoning about Privacy in Security Protocols

Opportunities for future work: case studies, alpha-beta privacy models, tool user interface, optimizations, new procedures...