Compositional Analysis of Protocol Equivalence in the Applied π-calculus using Quasi-Open Bisimilarity

18th International Colloquium on Theoretical Aspects of Computing (ICTAC'21)

Sjouke Mauw, Ross Horne, **Semyon Yurkov**

Department of Computer Science, University of Luxembourg

September 6-10, 2021

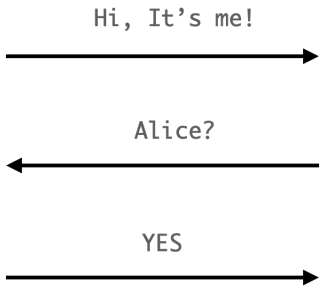
Communication protocols

Hi, It's me!

Alice?

YES

Communication protocols

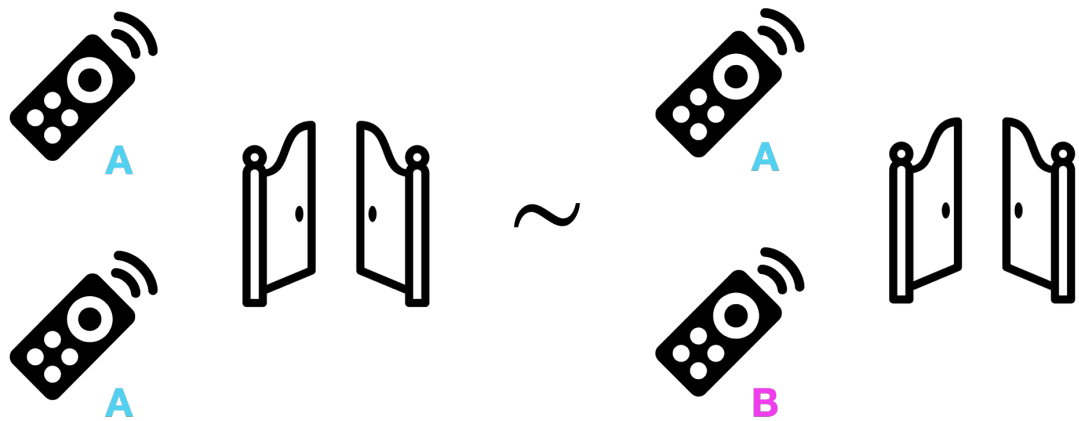


We use applied π-calculus to define a protocol as a process and security goals as properties of this process.

Security properties

Secrecy, authentication, privacy ...

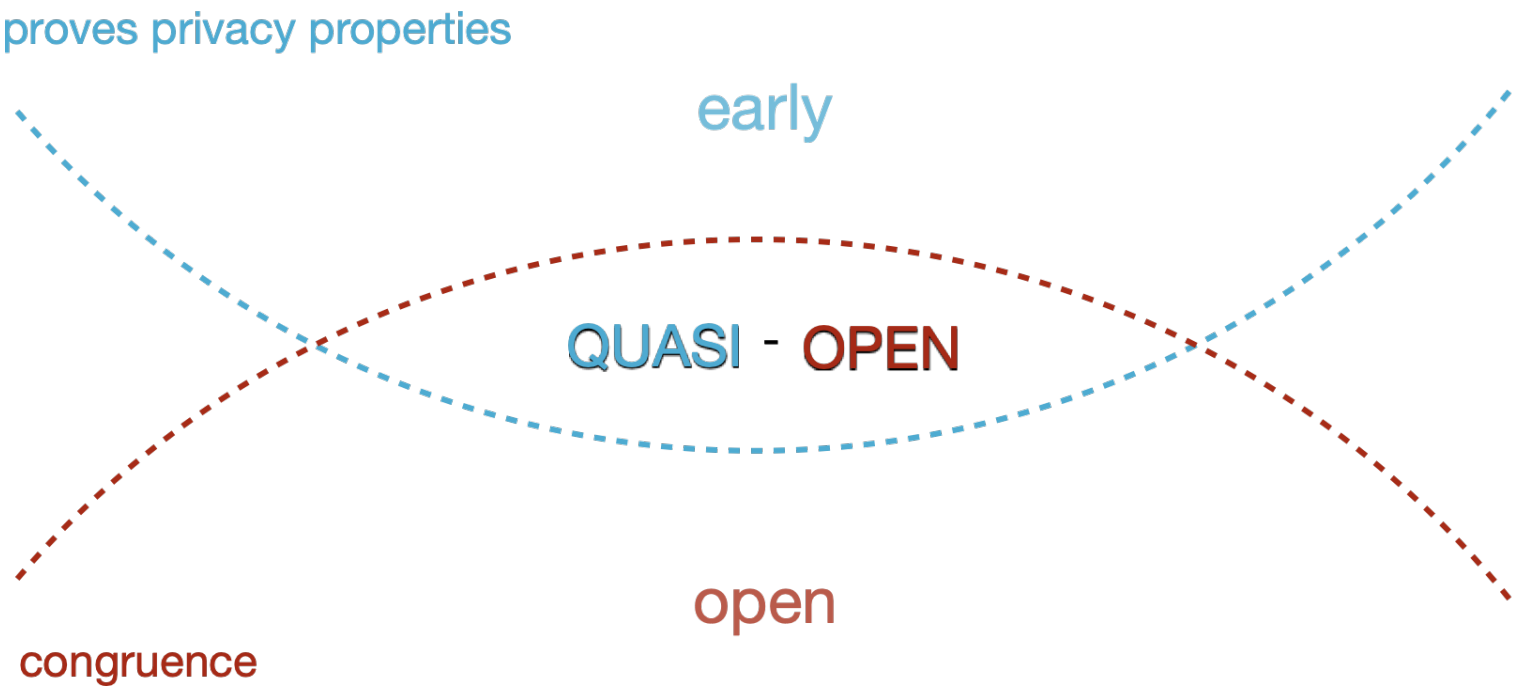
P satisfies privacy if it **behaves like** the *ideal*, definitely private P'.



Implementation $\sim$ Specification

Q: What is $\sim$ exactly?

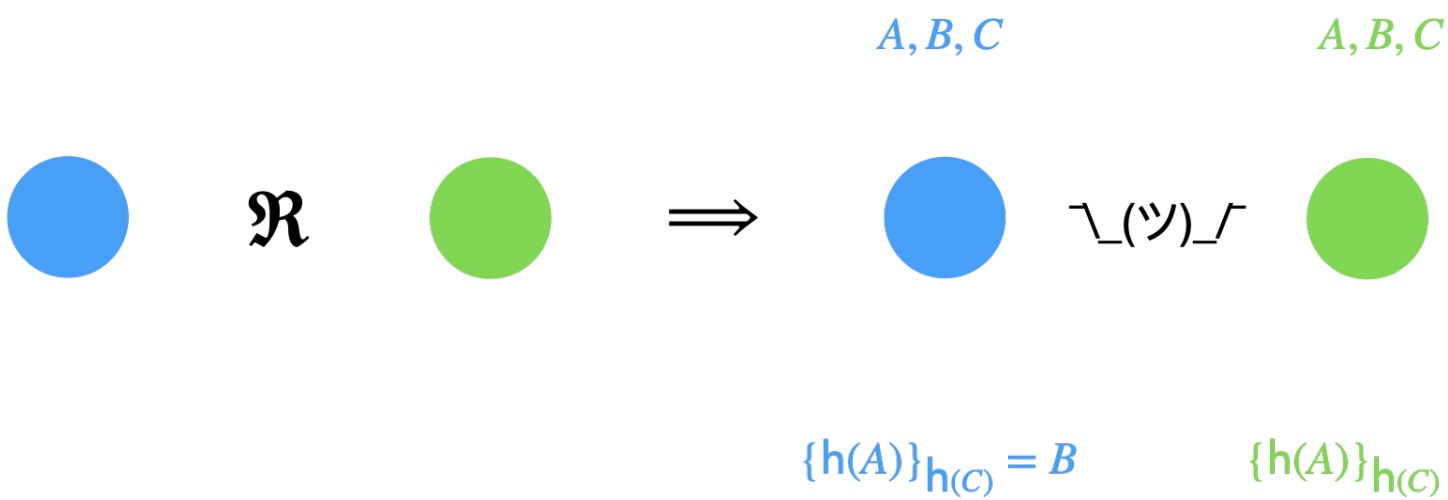
Bisimilarity Zoo



We suggest that $\sim$ is **quasi-open bisimilarity**.

We suggest that $\sim$ is quasi-open bisimilarity I (definition)

Two processes are $\sim$ if there is a symmetric $\mathfrak{R}$, s.t.



i. Static equivalence

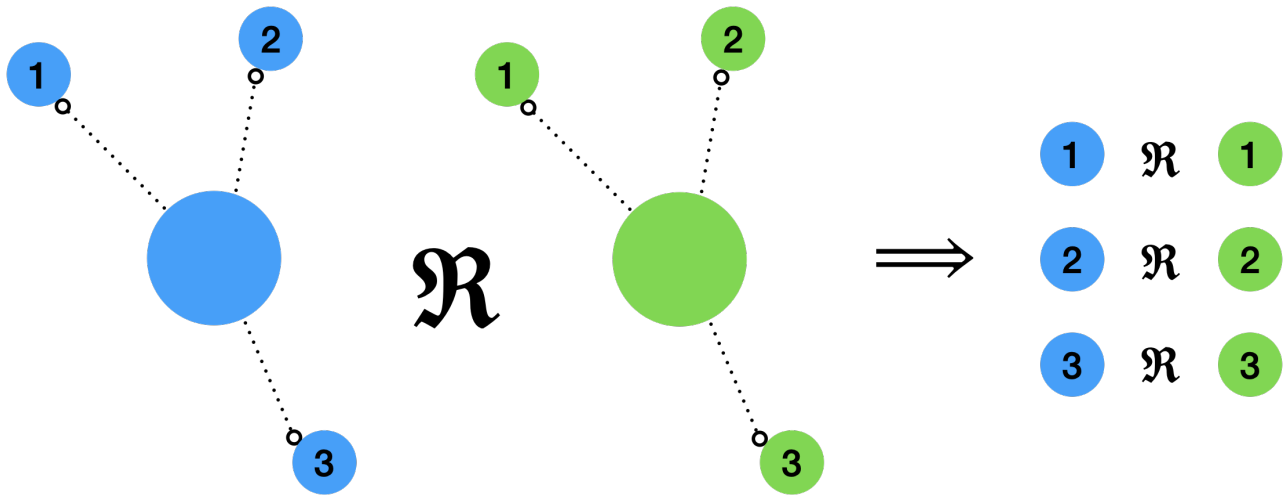
We suggest that $\sim$ is quasi-open bisimilarity I (definition)

Two processes are $\sim$ if there is a symmetric $\mathfrak{R}$, s.t.

ii. Matching transitions

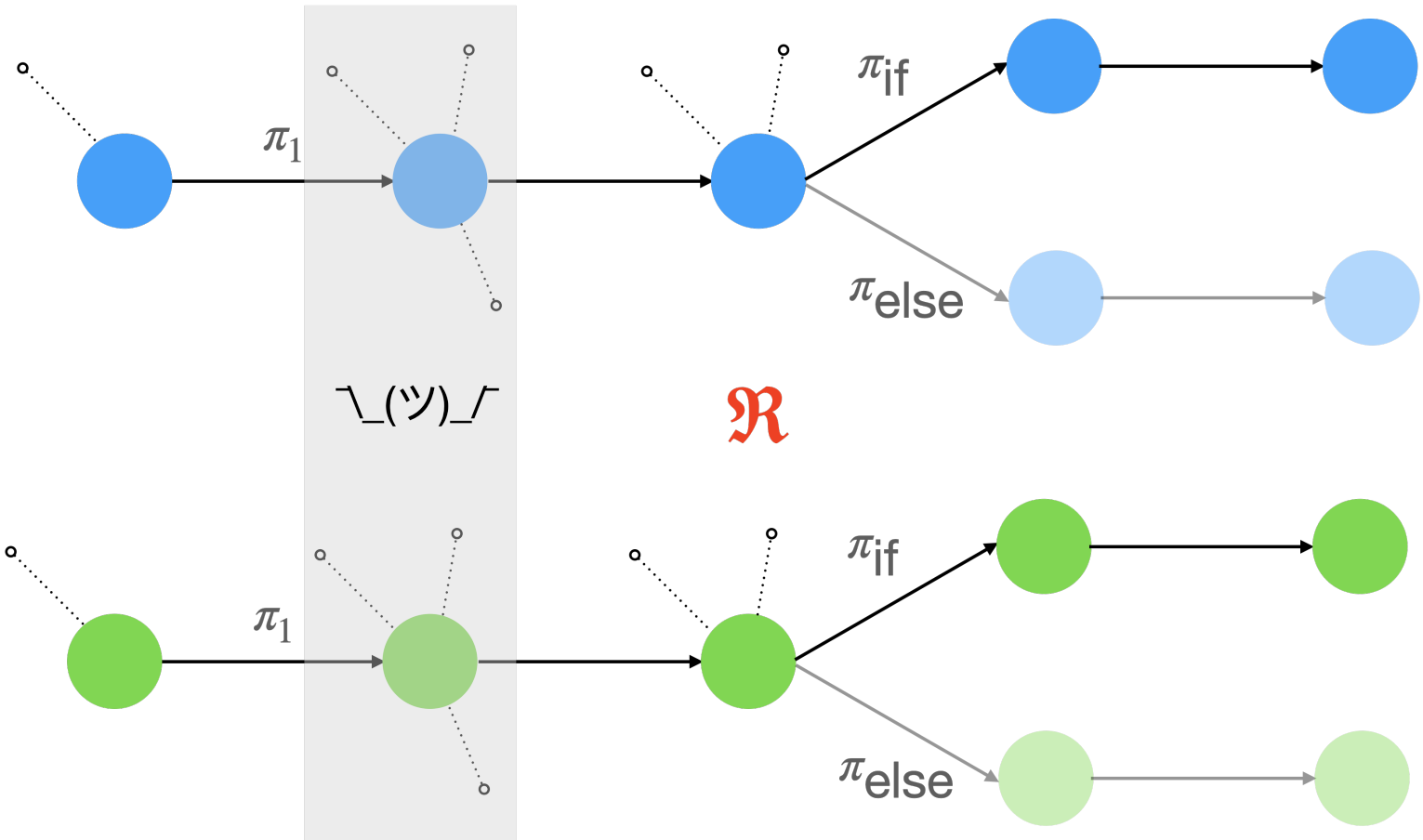
We suggest that $\sim$ is quasi-open bisimilarity I (definition)

Two processes are $\sim$ if there is a symmetric $\mathfrak{R}$, s.t.



iii. Reachability

We suggest that $\sim$ is quasi-open bisimilarity I (definition)



We suggest that $\sim$ is quasi-open bisimilarity II (motivation)

We suggest that $\sim$ is quasi-open bisimilarity II (motivation)

- $\sim$ is a bisimilarity: reach class of attacker-defender games is covered.

We suggest that $\sim$ is quasi-open bisimilarity II (motivation)

- $\sim$ is a bisimilarity: reach class of attacker-defender games is covered.
- $\sim$ is a congruence: compositional approach to prove the equivalence.

We suggest that $\sim$ is quasi-open bisimilarity II (motivation)

- $\sim$ is a bisimilarity: reach class of attacker-defender games is covered.
- $\sim$ is a congruence: compositional approach to prove the equivalence.
- $\sim$ is coarse enough bisimilarity congruence: bogus attacks are ignored.

We suggest that $\sim$ is quasi-open bisimilarity II (motivation)

- $\sim$ is a bisimilarity: reach class of attacker-defender games is covered.
- $\sim$ is a congruence: compositional approach to prove the equivalence.
- $\sim$ is coarse enough bisimilarity congruence: bogus attacks are ignored.

The coarsest.

Bisimilarity.

Congruence.

We suggest that $\sim$ is quasi-open bisimilarity II (motivation)

- $\sim$ is a bisimilarity: reach class of attacker-defender games is covered.
- $\sim$ is a congruence: compositional approach to prove the equivalence.
- $\sim$ is coarse enough bisimilarity congruence: bogus attacks are ignored.

The coarsest.

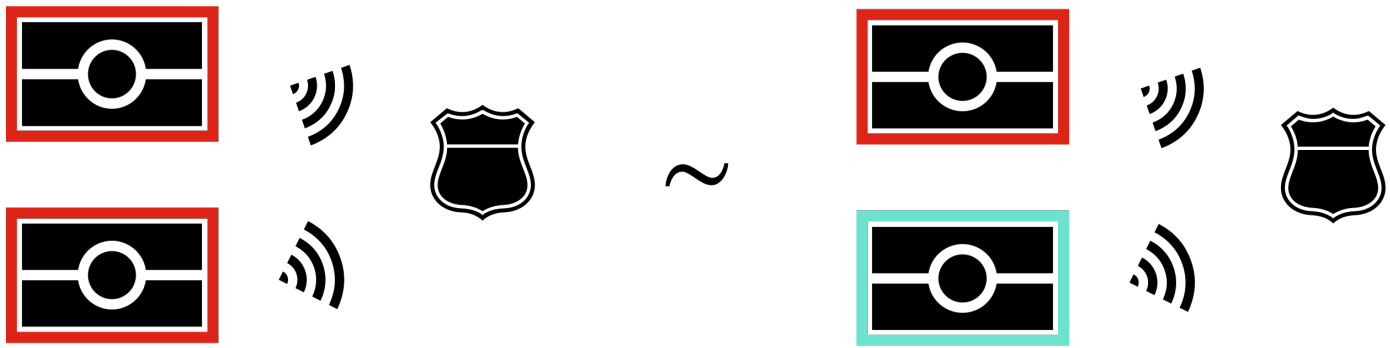
Bisimilarity.

Congruence.

- $\sim$ is *complete* with respect to a powerful notion of testing equivalence (open barbed bisimilarity).

Too coarse equivalence leads to missing attacks

Unlinkability = no one can relate two observed protocol sessions.



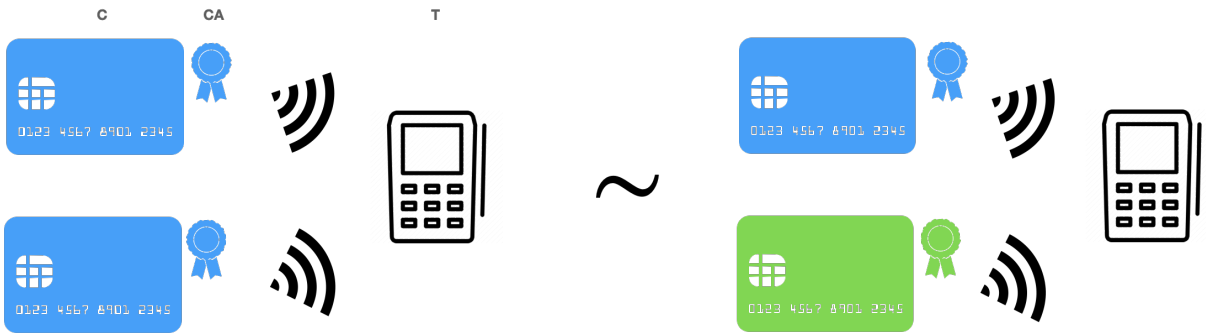
Too coarse equivalence leads to missing attacks

ICAO BAC protocol

- is unlinkable in trace equivalence model: Hirschi, Delaune, Baelde. S&P'16
- is not unlinkable in bisimilarity model and the attack found is *practical*: Filimonov, Horne, Mauw, Smith. ESORICS'19

Congruence enables compositional reasoning

Goal: C presents credentials multiple times without the risk of being reidentified.



$$\mathit{Impl} \triangleq \nu s.\ \Big(!\nu a.\ !\nu ch_c.\overline{c_C}\langle ch_c\rangle.C(s, ch_c, a) \mid \overline{out}\langle \mathtt{pk}(s)\rangle.\ !\nu ch_t.\overline{c_T}\langle ch_t\rangle.T(\mathtt{pk}(s), ch_t) \Big)$$

$$\sim$$

$$\mathit{Spec} \triangleq \nu s.\ \Big(!\nu a.\ \nu ch_c.\overline{c_C}\langle ch_c\rangle.C(s, ch_c, a) \mid \overline{out}\langle \mathtt{pk}(s)\rangle.\ !\nu ch_t.\overline{c_T}\langle ch_t\rangle.T(\mathtt{pk}(s), ch_t) \Big)$$

Congruence enables compositional reasoning

Goal: C presents credentials multiple times without the risk of being reidentified.

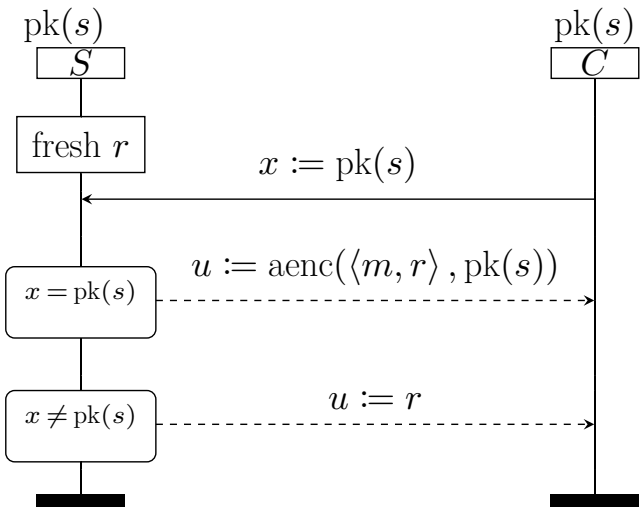
$\sim$

$$Small\_Impl \triangleq \nu s.\ \overline{out}\langle \mathrm{pk}(s)\rangle.\ !\nu a.\ !\nu ch_c.\overline{c_C}\langle ch_c\rangle.C(s, ch_c, a)$$

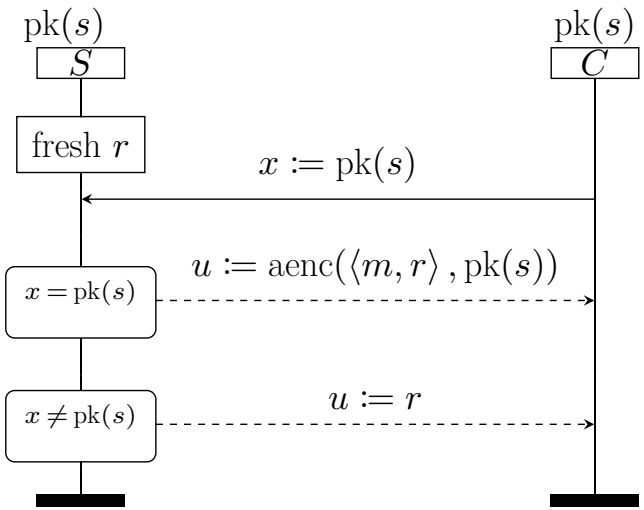
$\sim$

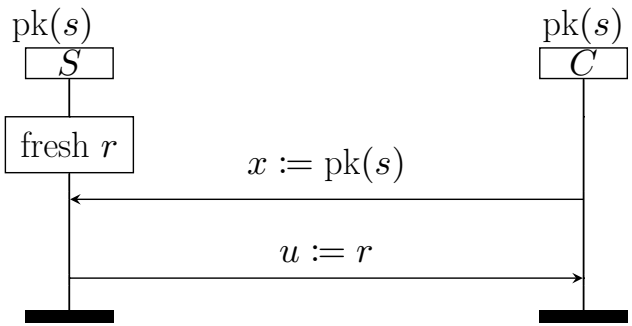
$$Small\_Spec \triangleq \nu s.\ \overline{out}\langle \mathrm{pk}(s)\rangle.\ !\nu a.\ \nu ch_c.\overline{c_C}\langle ch_c\rangle.C(s, ch_c, a)$$

Too fine equivalence discovers bogus attacks



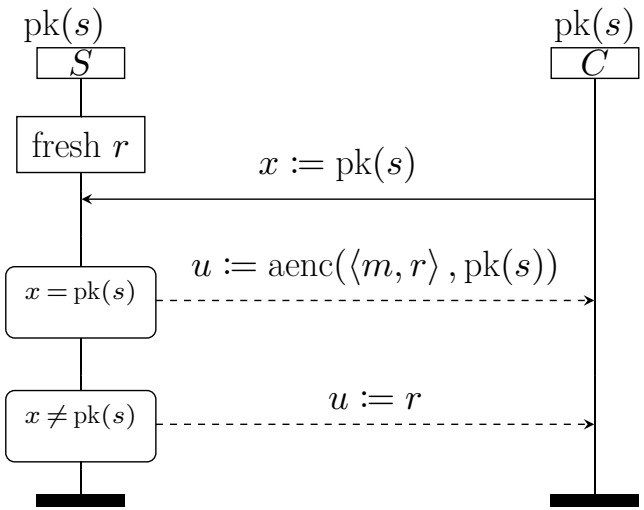
Too fine equivalence discovers bogus attacks



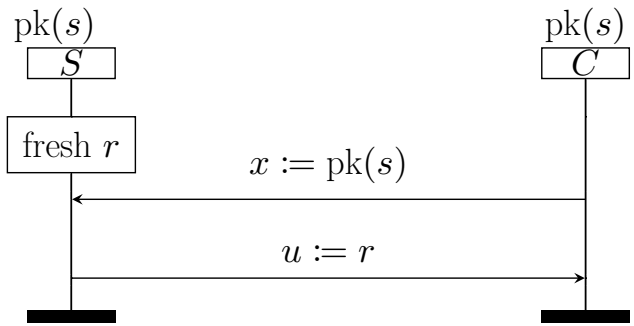


Too fine equivalence discovers bogus attacks

Open bisimilarity $\asymp_o$ is a finer bisimilarity congruence.

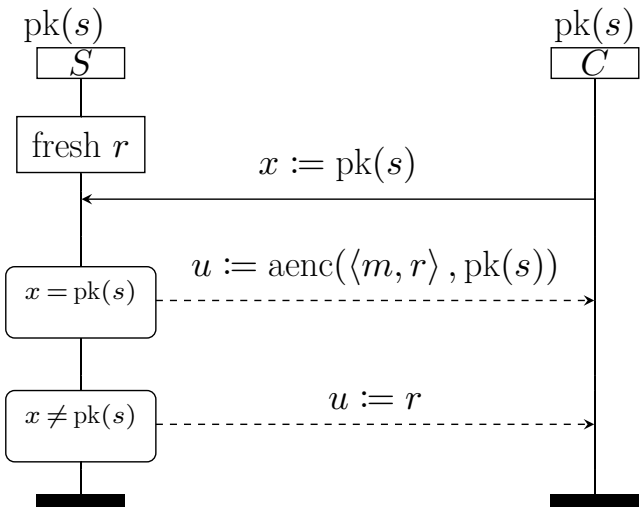


$\asymp_o$



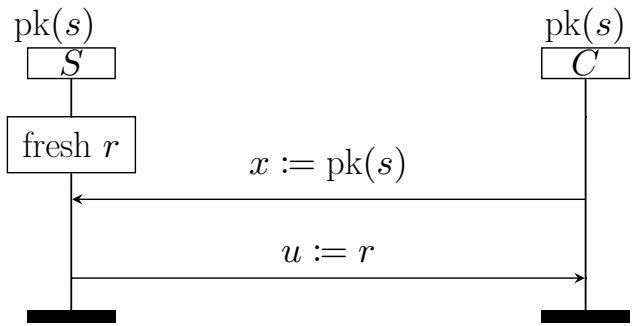
Too fine equivalence discovers bogus attacks

Open bisimilarity $\asymp_o$ is a finer bisimilarity congruence.



$\asymp_o$

$\sim_{qo}$



Quasi-open bisimilarity $\sim_{qo}$ is the coarsest bisimilarity congruence

Conclusions

- Privacy properties are sensitive to equivalence notion.
- Quasi-open bisimilarity is optimal.
  - Bisimilarity $\Rightarrow$ wide range of practical attacks.
  - Congruence $\Rightarrow$ compositional reasoning.
  - Coarsest bisimilarity congruence $\Rightarrow$ no spurious attacks.

Conclusions

- Privacy properties are sensitive to equivalence notion.
- Quasi-open bisimilarity is optimal.
  - Bisimilarity $\Rightarrow$ wide range of practical attacks.
  - Congruence $\Rightarrow$ compositional reasoning.
  - Coarsest bisimilarity congruence $\Rightarrow$ no spurious attacks.
  - Canonical: independent of any internal constraint system.