Provable Anonymity

Epistemic Logic for Anonymizing Protocols

Ichiro Hasuo

Radboud University Nijmegen
The Netherlands

Introduction

Concern about **on-line privacy** is growing...

- ISPs in EU might soon start logging all the URLs you browse

A number of **anonymizing protocols** have been introduced

- Chaum Mix, Onion Routing, Crowds,...

Introduction

A lot of work in formal verification of **authentication** protocols (e.g. Needham-Schroeder, Otway-Rees, ...) but

Formulation and verification of anonymity
is still quite immature

Our work is first to

- comprehensively formulate competing notions for "anonymity", and
- actually verify real protocols,

using **crypto-conscious epistemic logic**

Coauthors

Peter va? Rossum

Wolt?r Pieters

?lavio D. Garcia

Coauthors

Peter va? Rossum

Wolt?r Pieters

?lavio D. Garcia

Full paper available:

Provable Anonymity.
F. Garcia, I. Hasuo, W. Pieters, and P. van Rossum.
To appear in FMSE 2005.

Motivating example: onion routing

Introduced by [Chaum, '81] and
[Goldschlag, Reed, Syverson, '96]

Practical implementation available as
TOR (The Onion Router), **`http://tor.eff.org`**

Motivating example: onion routing

A tries to send a message m to B **anonymously**

$\{\!|-|\!\}_X$: public-key encryption n_i: nonce

$$A \xrightarrow{(((m)))} R_1 \xrightarrow{((m))} R_2 \xrightarrow{(m)} B$$

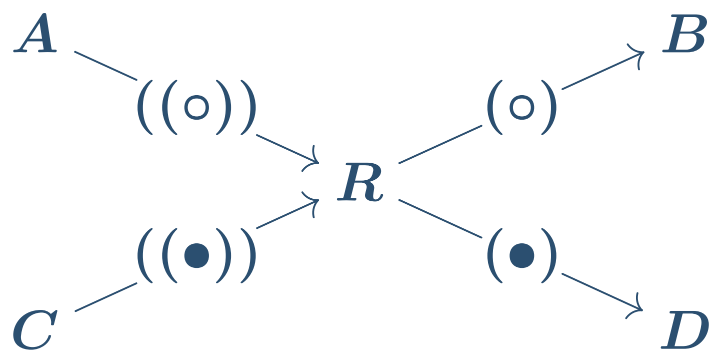
$$(m) = \{\!|m|\!\}_B$$

$$((m)) = \{\!|n_1, B, (m)|\!\}_{R_2}$$

$$(((m))) = \{\!|n_0, R_2, ((m))|\!\}_{R_1}$$

Onion routing

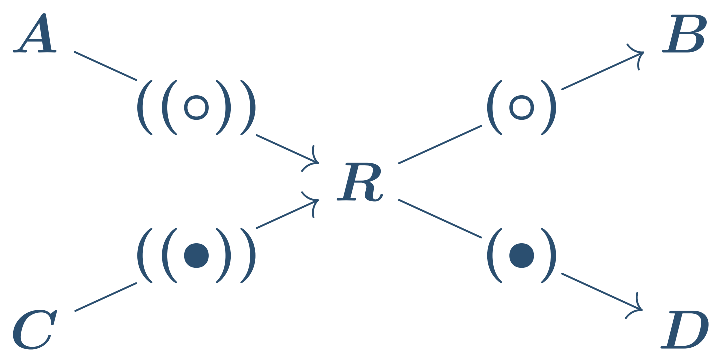
actual run



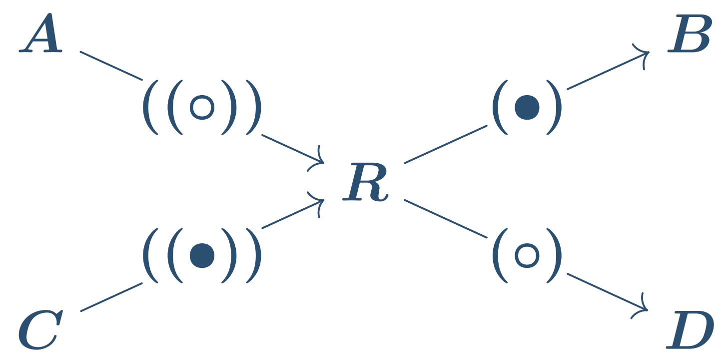
where $((\circ)) = \{\!|\, n, X, (\circ) \,|\!\}_R$

Onion routing

actual run



"counter" run

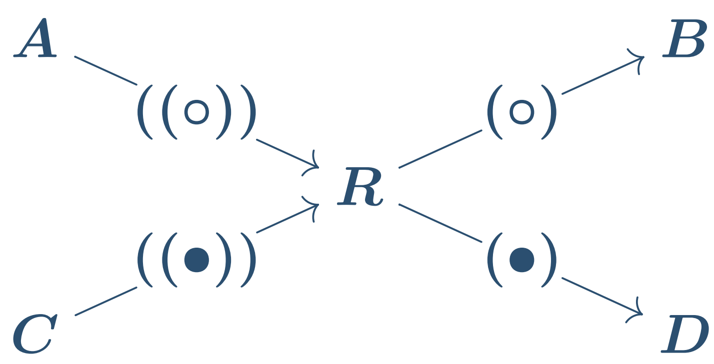


where $((\circ)) = \{\!|\, n, X, (\circ) \,|\!\}_R$

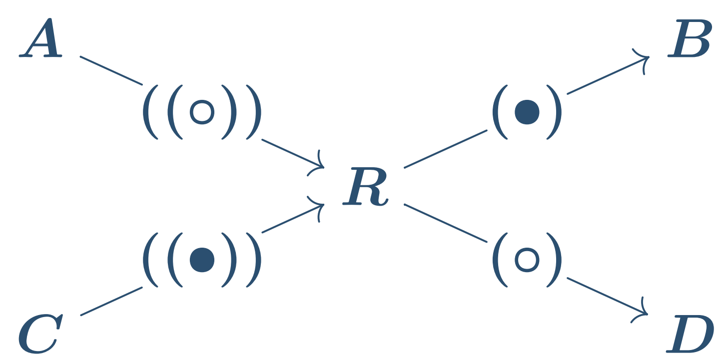
This is "anonymous" because the counter run is equally possible, so adversary is not sure whether A sent something to B or C

Onion routing

actual run



"counter" run



where $((\circ)) = \{\!|n, X, (\circ)|\!\}_R$

Anonymity fails when:

- private key of R is compromised
- we omit nonces, $((\circ)) = \{\!|X, (\circ)|\!\}_R$
- not enough padding, e.g. C is absent

Various "anonymity"

A number of proposals and objections...

Anonymity, Unobservability, Pseudonymity, and Identity Management – A Proposal for Terminology
(Ongoing draft from July 2000)
`http://dud.inf.tu-dresden.de/Literatur_V1.shtml`

Various "anonymity"

A number of proposals and objections...

Anonymity, Unobservability, Pseudonymity, and Identity Management – A Proposal for Terminology
(Ongoing draft from July 2000)
`http://dud.inf.tu-dresden.de/Literatur_V1.shtml`

With **epistemic language** we can formulate and verify competing notions in a uniform manner! [Halpern, O'Neill]

Epistemic logic

$\Box_A \varphi$		A **knows** φ
$\Diamond_A \varphi$	$(:= \quad \neg \Box_A \neg \varphi)$	A **suspects** φ

Semantics $\quad (W, \quad \{\cong_A \mid A : \text{agent}\})$

- W: set of possible worlds
- $\cong_A$: observational equivalence for A

$$x \models \Box_A \varphi \quad \stackrel{\text{def}}{\Longleftrightarrow} \quad \forall y \cong_A x.\quad y \models \varphi$$

$$x \models \Diamond_A \varphi \quad \stackrel{\text{def}}{\Longleftrightarrow} \quad \exists y \cong_A x.\quad y \models \varphi$$

"Anonymity" expressed with epistemic logic

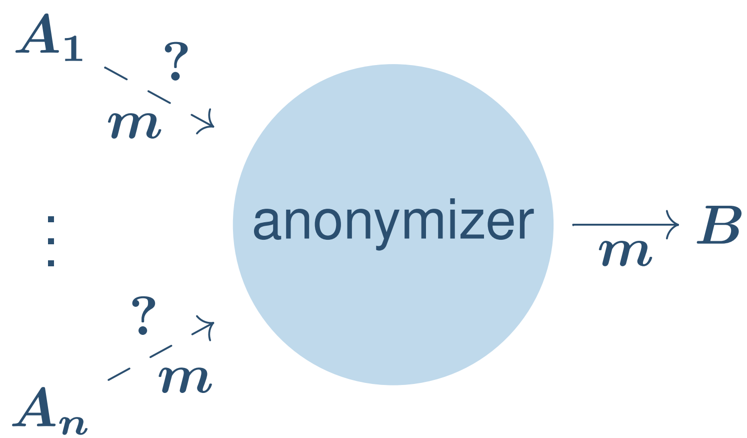
Sender anonymity

Given: B receives message (containing) m.

Weak ver.

Not sure if A sent m

Anonymity set $\{A_1, \ldots, A_n\}$



Each A_i is suspected as sender

"Anonymity" expressed with epistemic logic

Sender anonymity

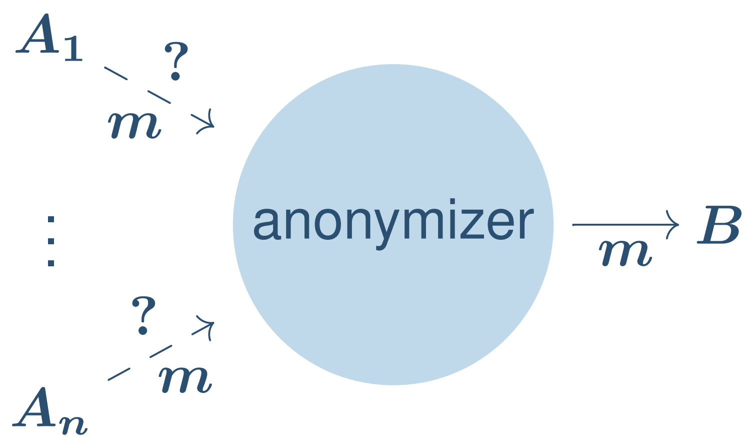
Given: B receives message (containing) m.

Weak ver.

Not sure if A sent m

$$\neg \Box_B \; A \textbf{ Sends } m$$

Anonymity set $\{A_1, \ldots, A_n\}$



Each A_i is suspected as sender

$$\begin{array}{ll} & \Diamond_B \; A_1 \textbf{ Sends } m \\ \wedge & \Diamond_B \; A_2 \textbf{ Sends } m \\ \wedge & \cdots \\ \wedge & \Diamond_B \; A_n \textbf{ Sends } m \end{array}$$

“Anonymity” expressed with epistemic logic

Unlinkability

Adversary is not sure if A sent something to B.

"Anonymity" expressed with epistemic logic

Unlinkability

Adversary is not sure if A sent something to B.

$$\neg\Box_{\mathsf{spy}}\ \exists m.\ (A\ \textbf{Sends}\ m \wedge B\ \textbf{Receives}\ m)$$

"Anonymity" expressed with epistemic logic

Plausible deniability

R can claim it is not aware of content m
"I relayed something, but don't know what it was!"

$$A \xrightarrow{((m))} R \xrightarrow{(m)} B$$

$$(m) = \{\!|m|\!\}_B$$
$$((m)) = \{\!|n_1, B, (m)|\!\}_R$$

"Anonymity" expressed with epistemic logic

Plausible deniability

R can claim it is not aware of content m

"I relayed something, but don't know what it was!"

$$A \xrightarrow{((m))} R \xrightarrow{(m)} B$$

$$(m) = \{\!|m|\!\}_B$$

$$((m)) = \{\!|n_1, B, (m)|\!\}_R$$

$$\forall m.\ \neg\Box_R(R \textbf{ Sends } m)$$

Semantics of epistemic operators

Possible world = a **run**, or **trace** of protocol

Two aspects of observational equivalence $\cong_A$:

- Not every event is observed by an agent
  (However we assume global eavesdropper as adversary)
- **Use of cryptographic operation**
  Encryptions/hashes makes messages look random junk!
  (Mauw, Verschuren, de Vink)

Semantics of epistemic operators

However, two random junks

$$\{\!|m|\!\}_A \quad \text{and} \quad \{\!|\{\!|m|\!\}_A|\!\}_B$$

should be related.

That is, mapping all undecryptable messages to single $\perp$ is not fine enough.

Our approach is finer than preceeding work, taking care of this point.

Reinterpretation of messages

Our approach is finer, using **reinterpretation**

We cheat adversary, by reinterpreting

message which looks junk for adversary   into   another message

in the way adversary cannot detect a lie.

Reinterpretation of messages

Our approach is finer, using **reinterpretation**

We cheat adversary, by reinterpreting

message which looks junk for adversary — into — another message

in the way adversary cannot detect a lie.

Definition U: a set of messages (e.g. **spy**'s possession)

Permutation π of messages is **reinterpretation under** U if:

$$\pi(p) = p \quad \text{for a primitive term } p$$

$$\pi(\{\!|m|\!\}_K) = \{\!|\pi(m)|\!\}_K \quad \text{if } \begin{cases} m, K \in U, \text{ or} \\ \{\!|m|\!\}_K, K^{-1} \in U \end{cases}$$

$$\pi(\mathbf{hash}(m)) = \mathbf{hash}(\pi(m)) \quad \text{if } m \in U$$

$$\pi(\langle m_1, m_2 \rangle) = \langle \pi(m_1), \pi(m_2) \rangle$$

In short, π preserves term structures available in U.

Observational equivalence

Definition

$r \cong_A r'$

$\overset{\text{def}}{\iff}$ $\exists \pi$, reinterpretation under A's possession, s.t.

$$\pi(r|_A) = r'|_A$$

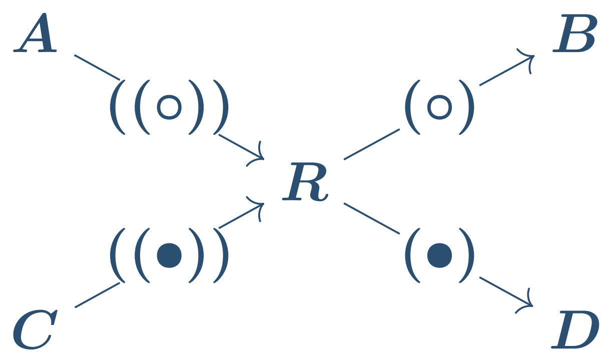
where $r|_A$: **A-visible part** of r

- For $A \neq$ **spy**, $r|_A$ consists of events where A is sender or receiver.
- $r|_{\textsf{spy}} = r$, i.e., **spy** is a global eavesdropper.

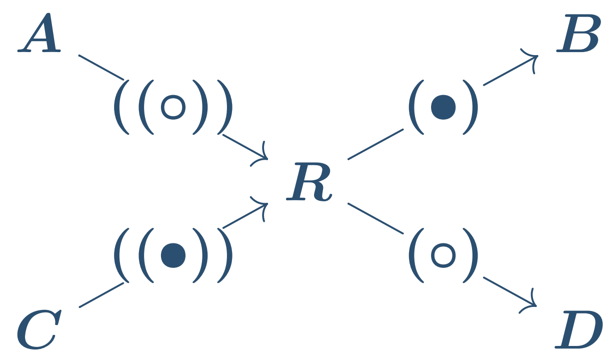
$\cong_A$ is in fact an equivalence relation.
Hence $\Box_A$ is S5-modality.

Observational equivalence

actual run

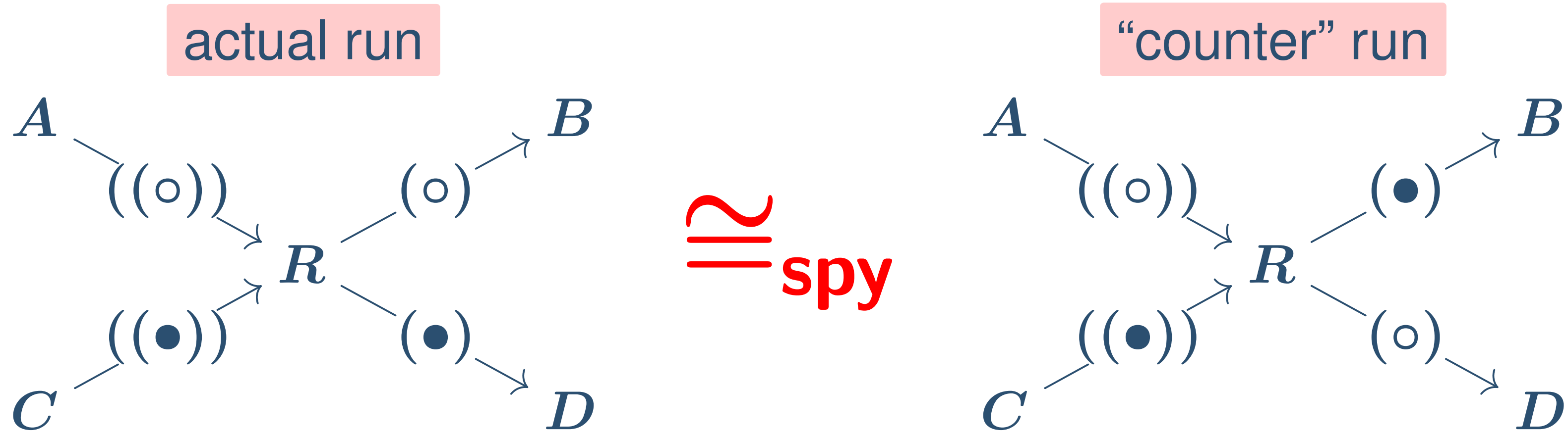


"counter" run



where $((\circ)) = \{\!|n, (\circ)|\!\}_R$ $\quad n$: random nonce

Observational equivalence

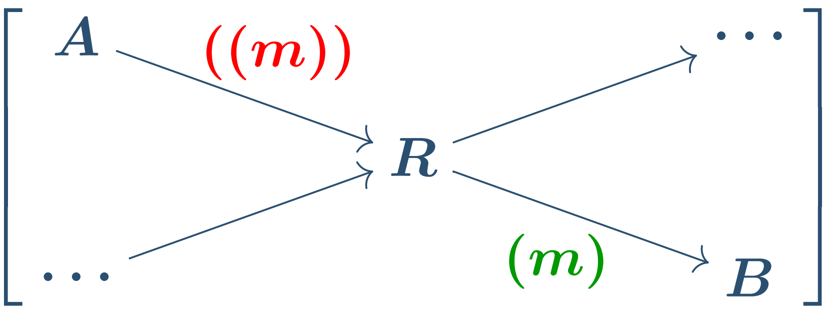


where $((\circ)) = \{\!|n, (\circ)|\!\}_R$ n : random nonce

Reinterpretation π:

$$((\circ)) \mapsto ((\circ)) \qquad ((\bullet)) \mapsto ((\bullet))$$
$$(\circ) \mapsto (\bullet) \qquad (\bullet) \mapsto (\circ)$$

Onion routing: unlinkability

$r =$ 

where

$(\!(m)\!) = \{\!|n, B, (m)|\!\}_R$

Theorem

$r \models \neg\Box_{\mathsf{spy}}\, \exists m.\, (A \textbf{ Sends } m \wedge B \textbf{ Receives } m)$

(A and B are unlinkable)

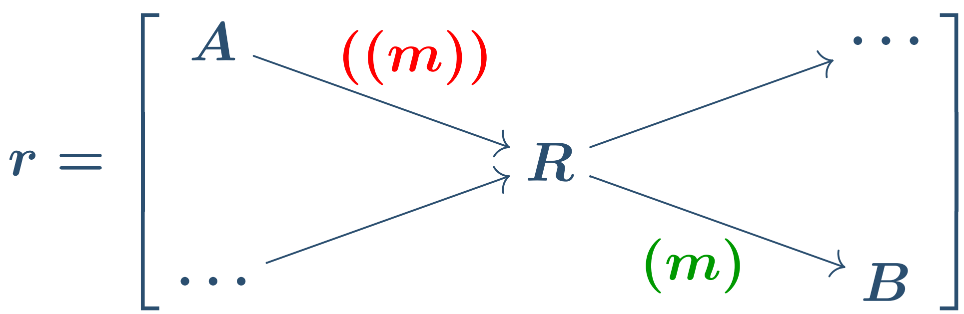
$\iff$

some $C \neq A$ sends $(\!(m')\!)$ to R, before R relays (m).

(there is enough padding)

Proof $[\Rightarrow]$ By contradiction. In $\forall r' \cong_{\mathsf{spy}} r$, π of (m) must result from π of $(\!(m)\!)$. Hence they have same core of onion.

Onion routing: plausible deniability



where

$$((m)) = \{\!|n, B, (m)|\!\}_R$$

Theorem For any m,

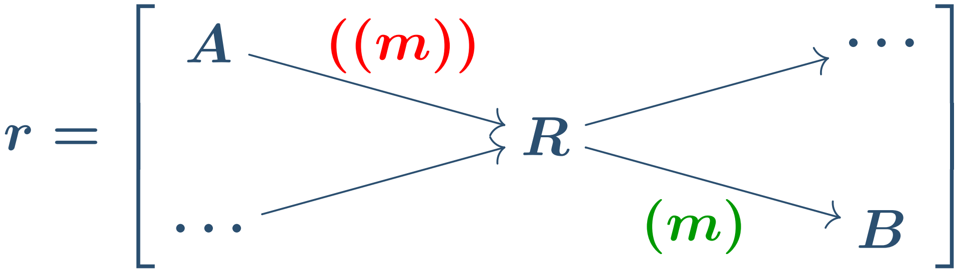
$$r \models \neg\Box_R(R \textbf{ Sends } m)$$

Proof R doesn't possess private-key of B, hence for $\forall m'$, $\exists \pi$: reinterpretation under R, which gives

$$\text{(actual run)} \quad \cong_R \quad A \xrightarrow{((m'))} R \xrightarrow{(m')} B$$

Flawed onion routing 1: forgotten nonces

We forget nonces beneath skin of onion.



where $((m)) = \{\!|B, (m)|\!\}_R$

Theorem Unlinkability fails, i.e.

$$r \models \Box_{\mathsf{spy}}\ \exists m.\ (A\ \textbf{Sends}\ m \wedge B\ \textbf{Receives}\ m)$$

Proof Any reinterpretation π must be like

$$(m) \mapsto m_1 \qquad\qquad ((m)) \mapsto \{\!|B, m_1|\!\}_R$$

since **spy** possesses public-key of R.

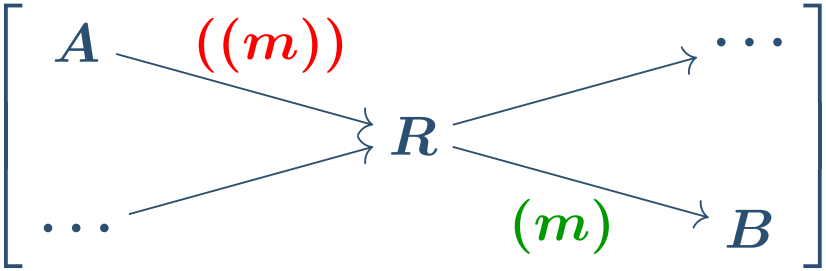
Hence any $r' \cong_{\mathsf{spy}} r$ is like $A \xrightarrow{\{\!|B, m_1|\!\}_R} R \xrightarrow{m_1} B$,

therefore $r' \models \exists m.\ (A\ \textbf{Sends}\ m \wedge B\ \textbf{Receives}\ m)$.

Flawed OR 2: private-key compromised

Private-key of R possessed by **spy**.

$r =$



where $(\!(m)\!) = \{\!|n, B, (m)|\!\}_R$

Theorem Unlinkability fails, i.e.

$$r \models \Box_{\mathsf{spy}}\, \exists m.\, (A \textbf{ Sends } m \wedge B \textbf{ Receives } m)$$

Proof Any reinterpretation π must be like

$$(m) \mapsto m_1 \qquad (\!(m)\!) \mapsto \{\!|n, B, m_1|\!\}_R$$

Hence any $r' \cong_{\mathsf{spy}} r$ is like

$$A \xrightarrow{\{\!|n, B, m_1|\!\}_R} R \xrightarrow{\;m_1\;} B$$, therefore

$r' \models \exists m.\, (A \textbf{ Sends } m \wedge B \textbf{ Receives } m)$.

Other examples

- Can detect even more subtle (artificial) flaw in Onion Routing: see full paper
- Crowds, for sender anonymity
- Internet voting protocol RIES
  In real use in the Netherlands (ongoing analysis)

Conclusion

- **Anonymity** is important, hard to define, hard to verify
- Competing notions are straightforwardly expressed with **epistemic** language
- First to consider use of **cryptographic operations** in semantics of epistemic logic
- Finer treatment of cryptographic operations using **reinterpretation**
- Able to **uniformly** verify/falsify wide variety of anonymizing systems

Future work

- Justification of reinterpretation (cf. Abadi, Rogaway)
- Tool support
- Quantitative analysis

Conclusion

- **Anonymity** is important, hard to define, hard to verify
- Competing notions are straightforwardly expressed with **epistemic** language
- First to consider use of **cryptographic operations** in semantics of epistemic logic
- Finer treatment of cryptographic operations using **reinterpretation**
- Able to **uniformly** verify/falsify wide variety of anonymizing systems

Future work

- Justification of reinterpretation (cf. Abadi, Rogaway)
- Tool support
- Quantitative analysis

Thank you for your attention!

Contact: **Ichiro Hasuo** **www.sos.cs.ru.nl** **ichiro@cs.ru.nl**