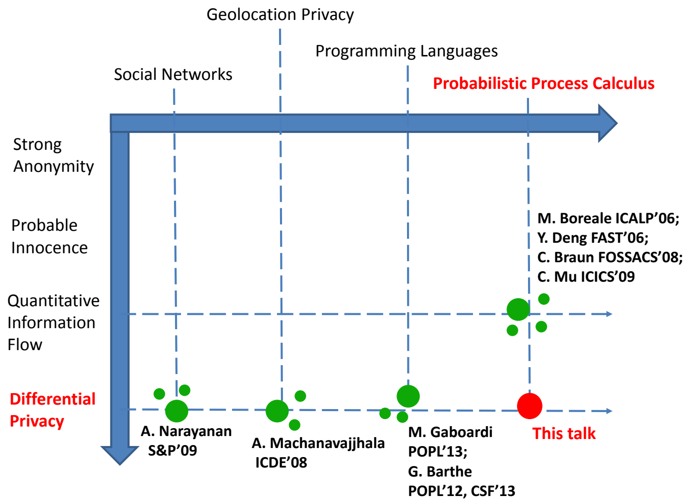
Metrics for Differential Privacy in Concurrent Systems

Lili Xu[1,3,4], Konstantinos Chatzikokolakis[2,3], Huimin Lin[4]

[1]INRIA [2]CNRS [3]Ecole Polytechnique, Paris, France
[4]Institute of Software, Chinese Academy of Sciences, Beijing, China

Berlin, Germany
June 5th, FORTE 2014

Background Sketch



How To Quantify the Amount of Privacy?

Definition (Standard Definition of Differential Privacy)

A query mechanism $\mathcal{A}$ is ϵ-differentially private if for any two adjacent databases u_1 and u_2, i.e. which differ only for one individual, and any property Z, the probability distributions of $\mathcal{A}(u_1), \mathcal{A}(u_2)$ differ on Z at most by e^ϵ, namely,

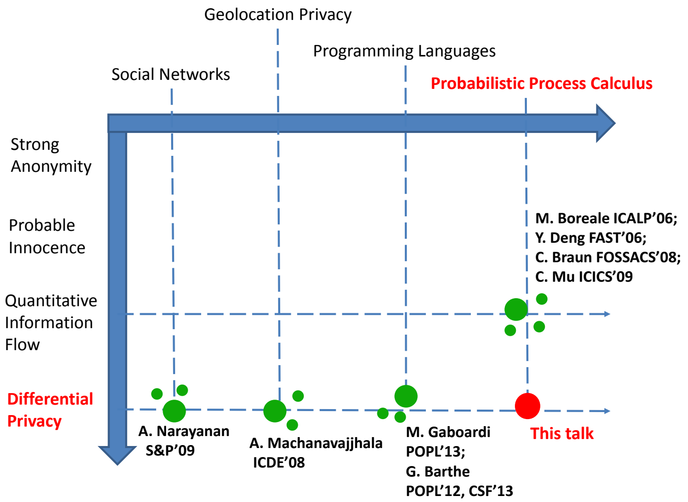
$$\Pr[\mathcal{A}(u_1) \in Z] \leq e^\epsilon \cdot \Pr[\mathcal{A}(u_2) \in Z].$$

The lower the value ϵ is, the better the privacy is protected.

Some Merits of Differential Privacy

- Strong notion of privacy.
- Independence from side knowledge.
- Robustness to attacks based on combining various sources of information.
- Looser restrictions between non-adjacent secrets.

Background Sketch



Outline

1. Introduction
   - Concurrent Systems
   - Differential Privacy
   - The Verification Framework
2. Two Pseudometrics
   - The Accumulative Bijection Pseudometric
   - The Amortised Bijection Pseudometric
   - Comparison
3. Non-expansive Process Operators
   - A Probabilistic Process calculus: CCS_p
4. An application to the Dining Cryptographers Protocol
   - The Dining Cryptographers Protocol

Motivation

- The model: Concurrent systems modeled as probabilistic automata.
- The measure of the level of privacy: Differential privacy

Motivation

- The model: Concurrent systems modeled as probabilistic automata.
- The measure of the level of privacy: Differential privacy

Goal:

To verify differential privacy properties for concurrent systems

Outline

1. Introduction
   - Concurrent Systems
   - Differential Privacy
   - The Verification Framework
2. Two Pseudometrics
   - The Accumulative Bijection Pseudometric
   - The Amortised Bijection Pseudometric
   - Comparison
3. Non-expansive Process Operators
   - A Probabilistic Process calculus: CCS_p
4. An application to the Dining Cryptographers Protocol
   - The Dining Cryptographers Protocol

Our Model

A probabilistic automaton is a tuple $(S, \overline{s}, A, D)$

- S: a finite set of states;
- $\overline{s} \in S$: the start state;
- A: a finite set of action labels;
- $D \subseteq S \times A \times Disc(S)$: a transition relation. We also write $s \xrightarrow{a} \mu$.

Definition (Concurrent Systems with Secret Information)

Let U be a set of secrets. A concurrent system with secret information $\mathcal{A}$ is a mapping of secrets to probabilistic automata, where $\mathcal{A}(u), u \in U$ is the automaton modelling the behavior of the system when running on u.

How to Reason about Probabilistic Observations?

- A scheduler ζ resolves the non-determinism based on the history of a computation, inducing a probability measure over traces.

How to Reason about Probabilistic Observations?

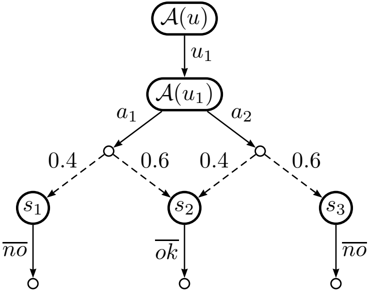
- A scheduler ζ resolves the non-determinism based on the history of a computation, inducing a probability measure over traces.

Probabilities of finite traces

Let α be the history up to the current state s. The probability of observing a finite trace $\vec{t}$ starting from α, denoted by $\Pr_\zeta[\alpha \rhd \vec{t}\,]$, is defined recursively as follows.

$$\Pr_\zeta[\alpha \rhd \vec{t}\,] = \begin{cases} 1 & \text{if } \vec{t} \text{ is empty,} \\ 0 & \text{if } \vec{t} = a^\frown\vec{t}', \zeta(\alpha) = s \xrightarrow{b} \mu \text{ and } b \neq a, \\ \sum_{s_i} \mu(s_i) \Pr_\zeta[\alpha a s_i \rhd \vec{t}'] & \text{if } \vec{t} = a^\frown\vec{t}' \text{ and } \zeta(\alpha) = s \xrightarrow{a} \mu. \end{cases}$$

An example: A PIN-Checking System



Example: The scheduler executes the a_1-branch.

$\Pr_\varsigma[\mathcal{A}(u_1) \triangleright a_1\overline{ok}\,]$	$=$	0.6	$\Pr_\varsigma[\mathcal{A}(u_2) \triangleright a_1\overline{ok}\,]$	$=$	0.4
$\Pr_\varsigma[\mathcal{A}(u_1) \triangleright a_1\overline{no}\,]$	$=$	0.4	$\Pr_\varsigma[\mathcal{A}(u_2) \triangleright a_1\overline{no}\,]$	$=$	0.6
$\Pr_\varsigma[\mathcal{A}(u_1) \triangleright a_2\overline{ok}\,]$	$=$	0	$\Pr_\varsigma[\mathcal{A}(u_2) \triangleright a_2\overline{ok}\,]$	$=$	0
$\Pr_\varsigma[\mathcal{A}(u_1) \triangleright a_2\overline{no}\,]$	$=$	0	$\Pr_\varsigma[\mathcal{A}(u_2) \triangleright a_2\overline{no}\,]$	$=$	0

Outline

1. Introduction
   - Concurrent Systems
   - Differential Privacy
   - The Verification Framework
2. Two Pseudometrics
   - The Accumulative Bijection Pseudometric
   - The Amortised Bijection Pseudometric
   - Comparison
3. Non-expansive Process Operators
   - A Probabilistic Process calculus: CCS_p
4. An application to the Dining Cryptographers Protocol
   - The Dining Cryptographers Protocol

Differential Privacy in the Context of Concurrent Systems

- The scheduler can easily break many security and privacy properties.
- We consider a restricted class of schedulers, called admissible schedulers.
  - make them unable to distinguish between secrets in the histories.

Definition (Differential Privacy in Our Setting)

A concurrent system $\mathcal{A}$ satisfies ϵ-*differential privacy* (DP) iff for any two adjacent secrets u, u', any finite trace $\vec{t}$ and any admissible scheduler ζ:

$$\Pr_{\zeta}[\mathcal{A}(u) \triangleright \vec{t}\,] \leq e^{\epsilon} \cdot \Pr_{\zeta}[\mathcal{A}(u') \triangleright \vec{t}\,]$$

The PIN-Checking System Revisited

Definition (Differential Privacy in Our Setting)

A concurrent system $\mathcal{A}$ satisfies ϵ-*differential privacy* (DP) iff for any two adjacent secrets u, u', any finite trace $\vec{t}$ and any admissible scheduler ζ:

$$\Pr_{\zeta}[\mathcal{A}(u) \triangleright \vec{t}\,] \leq e^{\epsilon} \cdot \Pr_{\zeta}[\mathcal{A}(u') \triangleright \vec{t}\,]$$

Example

$$\begin{array}{lcl}
\Pr_{\zeta}[\mathcal{A}(u_1) \triangleright a_1\overline{ok}\,] & = & 0.6 \\
\Pr_{\zeta}[\mathcal{A}(u_1) \triangleright a_1\overline{no}\,] & = & 0.4 \\
\Pr_{\zeta}[\mathcal{A}(u_1) \triangleright a_2\overline{ok}\,] & = & 0 \\
\Pr_{\zeta}[\mathcal{A}(u_1) \triangleright a_2\overline{no}\,] & = & 0
\end{array}
\qquad
\begin{array}{lcl}
\Pr_{\zeta}[\mathcal{A}(u_2) \triangleright a_1\overline{ok}\,] & = & 0.4 \\
\Pr_{\zeta}[\mathcal{A}(u_2) \triangleright a_1\overline{no}\,] & = & 0.6 \\
\Pr_{\zeta}[\mathcal{A}(u_2) \triangleright a_2\overline{ok}\,] & = & 0 \\
\Pr_{\zeta}[\mathcal{A}(u_2) \triangleright a_2\overline{no}\,] & = & 0
\end{array}$$

In this case, the level of differential privacy $\epsilon = \ln \frac{3}{2}$.

Outline

1. Introduction
   - Concurrent Systems
   - Differential Privacy
   - The Verification Framework
2. Two Pseudometrics
   - The Accumulative Bijection Pseudometric
   - The Amortised Bijection Pseudometric
   - Comparison
3. Non-expansive Process Operators
   - A Probabilistic Process calculus: CCS_p
4. An application to the Dining Cryptographers Protocol
   - The Dining Cryptographers Protocol

Neighboring processes have neighboring behaviors.

- For example: behavioural equivalences
  - $\mathcal{A}(u) \simeq \mathcal{A}(u') \Longrightarrow$ Secrecy [Abadi and Gordon, the Spi-calculus]

The property of differential privacy requires that the observations generated by two adjacent secrets are probabilistically close.

Neighboring processes have neighboring behaviors.

- For example: behavioural equivalences
  - $\mathcal{A}(u) \simeq \mathcal{A}(u') \Longrightarrow$ Secrecy [Abadi and Gordon, the Spi-calculus]

The property of differential privacy requires that the observations generated by two adjacent secrets are probabilistically close.

Verification Technique

- Behavioural approximation:Pseudometrics on processes.
- Find a pseudometric m on states of a concurrent system for two adjacent secrets u, u', such that:

$$m(\mathcal{A}(u), \mathcal{A}(u')) \leq \epsilon \Longrightarrow \mathcal{A}(u) \text{ and } \mathcal{A}(u') \text{ are } \epsilon\text{-differentially private.}$$

Outline

1. Introduction
   - Concurrent Systems
   - Differential Privacy
   - The Verification Framework
2. Two Pseudometrics
   - The Accumulative Bijection Pseudometric
   - The Amortised Bijection Pseudometric
   - Comparison
3. Non-expansive Process Operators
   - A Probabilistic Process calculus: CCS_p
4. An application to the Dining Cryptographers Protocol
   - The Dining Cryptographers Protocol

The Accumulative Bijection Pseudometric

It stems from the work of

- Michael C. Tschantz, Dilsun Kaynar, and Anupam Datta.
  Formal verification of differential privacy for interactive systems. ENTCS 2011.

We reformulate the notion of approximate similarity proposed in the above work in terms of a pseudometric, and exhibit its properties as a distance relation.

Definitions

We define an approximate bisimulation relation:

Definition (Accumulative Bisimulation)

A relation $\mathcal{R} \subseteq S \times S \times [0, \epsilon]$ is an ϵ-accumulative bisimulation iff for all $(s, t, c) \in \mathcal{R}$:

- $s \xrightarrow{a} \mu$ implies $t \xrightarrow{a} \nu$ with $\mu \mathcal{L}^D(\mathcal{R}, c)\nu$
- $t \xrightarrow{a} \nu$ implies $s \xrightarrow{a} \mu$ with $\mu \mathcal{L}^D(\mathcal{R}, c)\nu$

Definitions

First, lift a relation over states to a relation over distributions.

Definition (D-Approximate Lifting)

$$\mu \mathcal{L}^D(\mathcal{R}, c)\nu \quad \text{iff} \quad \exists \text{ bijection } \beta : supp(\mu) \to supp(\nu) \text{ such that}$$

$$\forall s \in supp(\mu) : (s, \beta(s), c + \sigma) \in \mathcal{R} \quad \text{where} \quad \sigma = \max_{s \in supp(\mu)} \left| \ln \frac{\mu(s)}{\nu(\beta(s))} \right|$$

We define an approximate bisimulation relation:

Definition (Accumulative Bisimulation)

A relation $\mathcal{R} \subseteq S \times S \times [0, \epsilon]$ is an ϵ-accumulative bisimulation iff for all $(s, t, c) \in \mathcal{R}$:

- $s \xrightarrow{a} \mu$ implies $t \xrightarrow{a} \nu$ with $\mu \mathcal{L}^D(\mathcal{R}, c)\nu$
- $t \xrightarrow{a} \nu$ implies $s \xrightarrow{a} \mu$ with $\mu \mathcal{L}^D(\mathcal{R}, c)\nu$

We can now define a pseudometric based on accumulative bisimulation as:

$$m^D(s,t) = \min\{\epsilon \mid (s,t,0) \in \mathcal{R} \text{ for some } \epsilon\text{-accumulative bisimulation } \mathcal{R}\}$$

Proposition

m^D is a pseudometric, that is:

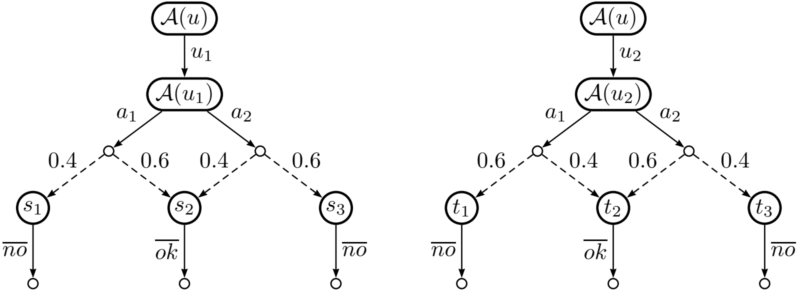
- *(reflexivity)* $m^D(s,s) = 0$
- *(symmetry)* $m^D(s_1,s_2) = m^D(s_2,s_1)$
- *(triangle inequality)* $m^D(s_1,s_3) \leq m^D(s_1,s_2) + m^D(s_2,s_3)$

Verification of differential privacy using m^D

Theorem

A concurrent system $\mathcal{A}$ is ϵ-differentially private if $m^D(\mathcal{A}(u), \mathcal{A}(u')) \leq \epsilon$ for any two adjacent secrets u and u'.

The PIN-Checking System Revisited



Example

The following relation is a $\ln\frac{3}{2}$-accumulative bisimulation between $\mathcal{A}(u_1)$ and $\mathcal{A}(u_2)$.

$$\mathcal{R} = \{ (\mathcal{A}(u_1), \mathcal{A}(u_2), 0), \quad (s_1, t_1, \ln\tfrac{3}{2}) \quad (s_2, t_2, \ln\tfrac{3}{2}), \quad (s_3, t_3, \ln\tfrac{3}{2}) \}$$

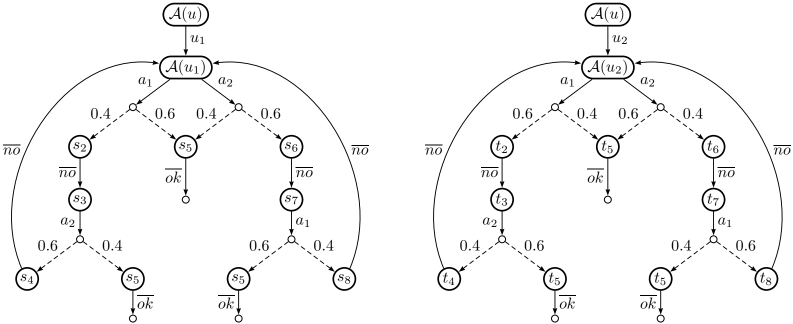
Thus $m^D(\mathcal{A}(u_1), \mathcal{A}(u_2)) = \ln\frac{3}{2}$, system $\mathcal{A}$ is $\ln\frac{3}{2}$-differentially private.

The Use of the Privacy Budget May Be a bit Wasteful?

m^D is useful for verifying differential privacy. However,

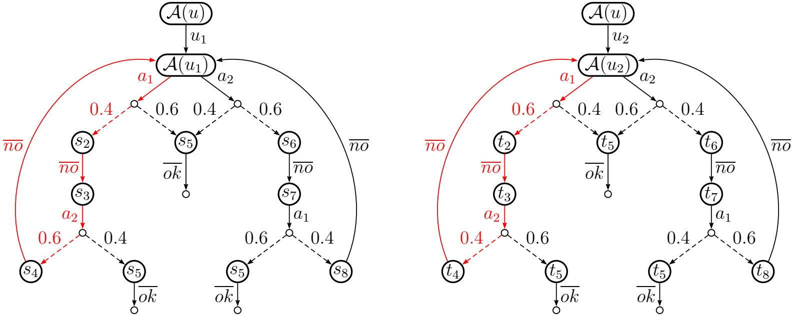
- the amount of leakage is only accumulated.
- the accumulation is the same for all branches, and equal to the worst branch.

The Use of the Privacy Budget May Be a bit Wasteful?



Consider the above example. m^D gives ∞ for the distance between $\mathcal{A}(u_1)$ and $\mathcal{A}(u_2)$.

The Use of the Privacy Budget May Be a bit Wasteful?



Assume that the scheduler executes the a_1-branch. The ratios of probabilities for $\mathcal{A}(u_1)$ and $\mathcal{A}(u_2)$ producing the same finite sequences:

$$(a_1\overline{no}\,a_2\overline{no})^* \quad : \quad = \left(\frac{0.4\times0.6}{0.6\times0.4}\right)^* = 1$$

$$(a_1\overline{no}\,a_2\overline{no})^* a_1\overline{ok} \quad : \quad = \frac{3}{2}$$

$$(a_1\overline{no}\,a_2\overline{no})^* a_1\overline{no}\,a_2\overline{ok} \quad : \quad = \frac{9}{4}$$

Outline

1. Introduction
   - Concurrent Systems
   - Differential Privacy
   - The Verification Framework
2. Two Pseudometrics
   - The Accumulative Bijection Pseudometric
   - The Amortised Bijection Pseudometric
   - Comparison
3. Non-expansive Process Operators
   - A Probabilistic Process calculus: CCS_p
4. An application to the Dining Cryptographers Protocol
   - The Dining Cryptographers Protocol

The Amortised Bijection Pseudometric

We employ amortised bisimulation relation from:

- Astrid Kiehn and S. Arun-Kumar.
  Amortised bisimulations. In *FORTE*, 2005.
- Gerald Lüttgen and Walter Vogler.
  Bisimulation on speed: A unified approach. *Theor. Comuput. Sci.*, 2006.

Intuition

The privacy budget in each simulation step may be either reduced due to a negative difference of probabilities, or increased due to a positive difference. Hence, the long-term budget might get amortised.

Definitions

We define amortised bisimulation:

Definition (Amortised bisimulation)

A relation $\mathcal{R} \subseteq S \times S \times [-\epsilon, \epsilon]$ is an ϵ-amortised bisimulation iff for all $(s, t, c) \in \mathcal{R}$:

- $s \xrightarrow{a} \mu$ implies $t \xrightarrow{a} \nu$ with $\mu \mathcal{L}^A(\mathcal{R}, c)\nu$
- $t \xrightarrow{a} \nu$ implies $s \xrightarrow{a} \mu$ with $\mu \mathcal{L}^A(\mathcal{R}, c)\nu$

Definitions

First, define the corresponding lifting:

Definition (A-Approximate Lifting)

$$\mu \mathcal{L}^A(\mathcal{R}, c)\nu \quad \text{iff} \quad \exists \text{ bijection } \beta : supp(\mu) \to supp(\nu) \text{ such that}$$

$$\forall s \in supp(\mu) : (s, \beta(s), c + \ln \frac{\mu(s)}{\nu(\beta(s))}) \in \mathcal{R}$$

We define amortised bisimulation:

Definition (Amortised bisimulation)

A relation $\mathcal{R} \subseteq S \times S \times [-\epsilon, \epsilon]$ is an ϵ-amortised bisimulation iff for all $(s, t, c) \in \mathcal{R}$:

- $s \xrightarrow{a} \mu$ implies $t \xrightarrow{a} \nu$ with $\mu \mathcal{L}^A(\mathcal{R}, c)\nu$
- $t \xrightarrow{a} \nu$ implies $s \xrightarrow{a} \mu$ with $\mu \mathcal{L}^A(\mathcal{R}, c)\nu$

Verification of differential privacy using m^A

Similarly to the previous section, we can finally define a pseudometric on states as:

$$m^A(s,t) = \min\{\epsilon \mid (s,t,0) \in \mathcal{R} \text{ for some } \epsilon\text{-amortised bisimulation } \mathcal{R}\}$$

Proposition

m^A is a pseudometric.

Verification of differential privacy using m^A

Similarly to the previous section, we can finally define a pseudometric on states as:

$$m^A(s,t) = \min\{\epsilon \mid (s,t,0) \in \mathcal{R} \text{ for some } \epsilon\text{-amortised bisimulation } \mathcal{R}\}$$

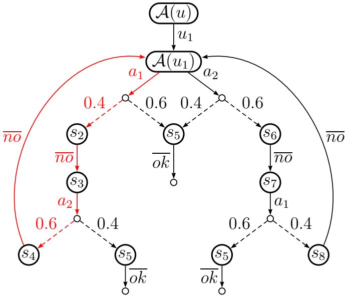
Proposition

m^A is a pseudometric.

Theorem

A concurrent system $\mathcal{A}$ is ϵ-differentially private if $m^A(\mathcal{A}(u), \mathcal{A}(u')) \leq \epsilon$ for any two adjacent secrets u and u'.

Indeed, a Thriftier Use of the Privacy Leakage Budget



The following relation is an amortised bisimulation between $\mathcal{A}(u_1)$ and $\mathcal{A}(u_2)$.

$$\begin{aligned}\mathcal{R} \;=\{\; & (\mathcal{A}(u_1),\mathcal{A}(u_2),0),\ (s_2,t_2,\ln\tfrac{2}{3}),\ (s_5,t_5,\ln\tfrac{3}{2}),\ (s_3,t_3,\ln\tfrac{2}{3}),\\ & (s_4,t_4,0),\ (s_5,t_5,\ln\tfrac{4}{9}),\ (s_6,t_6,\ln\tfrac{3}{2}),\ (s_5,t_5,\ln\tfrac{2}{3}),\\ & (s_7,t_7,\ln\tfrac{3}{2}),\ (s_8,t_8,0),\ (s_5,t_5,\ln\tfrac{9}{4})\,\}\end{aligned}$$

Thus $m^A(\mathcal{A}(u_1),\mathcal{A}(u_2)) = \ln\frac{9}{4}$, system $\mathcal{A}$ is $\ln\frac{9}{4}$-differentially private.

Outline

1. Introduction
   - Concurrent Systems
   - Differential Privacy
   - The Verification Framework
2. Two Pseudometrics
   - The Accumulative Bijection Pseudometric
   - The Amortised Bijection Pseudometric
   - Comparison
3. Non-expansive Process Operators
   - A Probabilistic Process calculus: CCS_p
4. An application to the Dining Cryptographers Protocol
   - The Dining Cryptographers Protocol

Comparison of the Two Pseudometrics

The latter pseudometric is more liberal than the former one. Define $m_1 \preceq m_2$: $\forall s, t : m_1(s, t) \geq m_2(s, t)$.

Proposition

- $m^D \preceq m^A$

Relations with probabilistic bisimilarity $\sim$

Moreover, [Desharnais:2002:LICS] has proposed a criterion on pseudometrics *m* for probabilistic processes.

Criterion

- $m(s,t) = 0 \Leftrightarrow s \sim t$

where the corresponding lifting operation $\mu_1 \mathcal{L}(\mathcal{R}) \mu_2$ with respect to $s \sim t$ is: for all equivalence class $E \in S/\sim, \mu_1(E) = \mu_2(E)$.

We investigate their relation with bisimilarity $\sim$.

Proposition

The following hold:

- $m^D(s,t) = 0 \Rightarrow s \sim t$
- $m^A(s,t) = 0 \Rightarrow s \sim t$

Outline

1. Introduction
   - Concurrent Systems
   - Differential Privacy
   - The Verification Framework
2. Two Pseudometrics
   - The Accumulative Bijection Pseudometric
   - The Amortised Bijection Pseudometric
   - Comparison
3. Non-expansive Process Operators
   - A Probabilistic Process calculus: CCS_p
4. An application to the Dining Cryptographers Protocol
   - The Dining Cryptographers Protocol

A Probabilistic Process calculus: CCS_p

The syntax of CCS_p

$$\alpha ::= a \mid \bar{a} \mid \tau \qquad \text{prefixes}$$

$$P, Q ::= \alpha.P \mid P \,|\, Q \mid P + Q \mid \bigoplus_{i \in 1..n} p_i P_i \mid (\nu a)P \mid \mathbf{0} \qquad \text{processes}$$

A Probabilistic Process calculus: CCS_p

The syntax of CCS_p

$$\begin{array}{lcll} \alpha & ::= & a \mid \bar{a} \mid \tau & \text{prefixes} \\ P, Q & ::= & \alpha.P \mid P \,|\, Q \mid P + Q \mid \bigoplus_{i \in 1..n} p_i P_i \mid (\nu a)P \mid \mathbf{0} & \text{processes} \end{array}$$

The semantics of CCS_p

$$\text{ACT} \quad \frac{}{\alpha.P \xrightarrow{\alpha} \delta(P)} \qquad \text{PROB} \quad \frac{}{\bigoplus_{i \in I} p_i P_i \xrightarrow{\tau} \sum_i p_i P_i}$$

$$\text{SUM1} \quad \frac{P \xrightarrow{\alpha} \mu}{P + Q \xrightarrow{\alpha} \mu} \qquad \text{PAR1} \quad \frac{P \xrightarrow{\alpha} \mu}{P \,|\, Q \xrightarrow{\alpha} \mu \,|\, Q}$$

$$\text{COM} \quad \frac{P \xrightarrow{a} \delta(P') \quad Q \xrightarrow{\bar{a}} \delta(Q')}{P \,|\, Q \xrightarrow{\tau} \delta(P' \,|\, Q')} \qquad \text{RES} \quad \frac{P \xrightarrow{\alpha} \mu \qquad \alpha \neq a, \bar{a}}{(\nu a)P \xrightarrow{\alpha} (\nu a)\mu}$$

Non-expansive Process operators

Proposition

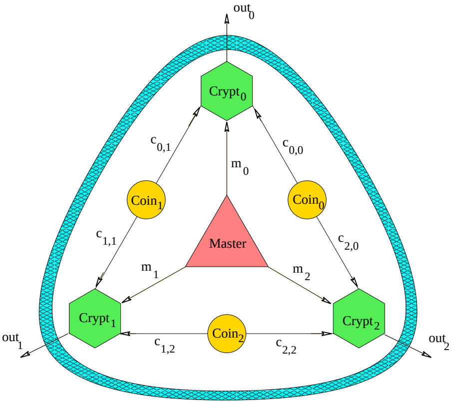
If $m(P,Q) \leq \epsilon$, *where* $m \in \{m^D, m^A\}$, *then*

- $m(a.P, a.Q) \leq \epsilon$
- $m(pR \oplus (1-p)P, pR \oplus (1-p)Q) \leq \epsilon$
- $m(R+P, R+Q) \leq \epsilon$
- $m((\nu a)P, (\nu a)Q) \leq \epsilon$
- $m(R \mid P, R \mid Q) \leq \epsilon$.

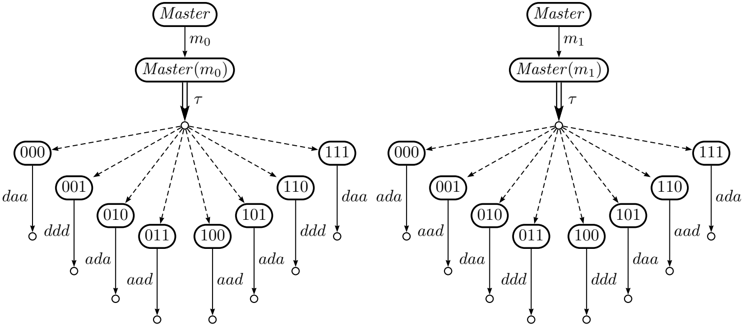
Outline

1. Introduction
   - Concurrent Systems
   - Differential Privacy
   - The Verification Framework
2. Two Pseudometrics
   - The Accumulative Bijection Pseudometric
   - The Amortised Bijection Pseudometric
   - Comparison
3. Non-expansive Process Operators
   - A Probabilistic Process calculus: CCS_p
4. An application to the Dining Cryptographers Protocol
   - The Dining Cryptographers Protocol

The Dining Cryptographers Protocol



The Probabilistic Automata of the Dining Cryptographers



(g) *Master* (m_0) (h) *Master* (m_1)

Let $b_0b_1b_2$ and $c_0c_1c_2$ represent two inner states of *Master* (m_0) and *Master* (m_1) respectively. There exists a bijection function f between them:

$$c_0c_1c_2 = f(b_0b_1b_2) = b_0(b_1 \oplus 1)b_2$$

$\{(Master(m_0), Master(m_1), 0)\} \cup \{\, (b_0b_1b_2, f(b_0b_1b_2), |\ln \frac{p}{1-p}|) \mid b_0, b_1, b_2 \in \{0,1\}\,\}$ forms a $|\ln \frac{p}{1-p}|$-accumulative bisimulation relation.
Thus $m^D(Master(m_0), Master(m_1)) \leq |\ln \frac{p}{1-p}|$.

Proposition

A DCP with three cryptographers and with probability-p biased coins is $|\ln \frac{p}{1-p}|$-differentially private.

$\{(Master(m_0), Master(m_1), 0)\} \cup \{\, (b_0b_1b_2, f(b_0b_1b_2), |\ln \frac{p}{1-p}|) \mid b_0, b_1, b_2 \in \{0,1\}\,\}$ forms a $|\ln \frac{p}{1-p}|$-accumulative bisimulation relation.

Thus $m^D(Master(m_0), Master(m_1)) \leq |\ln \frac{p}{1-p}|$.

Proposition

A DCP with three cryptographers and with probability-p biased coins is $|\ln \frac{p}{1-p}|$-differentially private.

Proposition (An extension to n fully connected cryptographers)

A DCP with n fully connected cryptographers and with probability-p biased coins is $|\ln \frac{p}{1-p}|$-differentially private.

Summary

We have investigated two pseudometrics on states:

- The first pseudometric is a reformulation of the notion proposed by Tschantz et al.
- The second one is designed such that the total privacy leakage bound gets amortised, thus more liberal than the first one.
- The closer processes are in the pseudometrics, the higher level of differential privacy they can preserve.
- Relations with bisimilarity; Nonexpansiveness study w.r.t. process combinators; An application to DCP.

- Outlook
  - To investigate a new pseudometric, adapted from the metric à la Kantorovich proposed by [Desharnais:2002:LICS], to fully characterise bisimilarity, and release the bijection requirement.

Thank you for your attention!

Questions?