Modelling Unlinkability

Stefan Köpsell
Technische Universität Dresden
<sk13@inf.tu-dresden.de>

Sandra Steinbrecher
Freie Universität Berlin
<steinbrecher@acm.org>

Talk at PET 2003, Dresden

Contents:

1. Metrics for anonymity
2. Linkability influences anonymity
3. Unlinkability within one set
4. Unlinkability between sets
5. Attacks on unlinkability
6. Future tasks

Defining Anonymity

'Anonymity is the state of being not identifiable within a set of subjects, the anonymity set.' (Köhntopp/Pfitzmann, 2001)

Real world scenarios: A subject's anonymity is related to an action.

Communication systems: Sender/receiver anonymity
Relationship anonymity

A human being's anonymity should be measured by

- Size of the respective anonymity set.
- Probability distribution on this anonymity set.

Approaches on measuring anonymity:

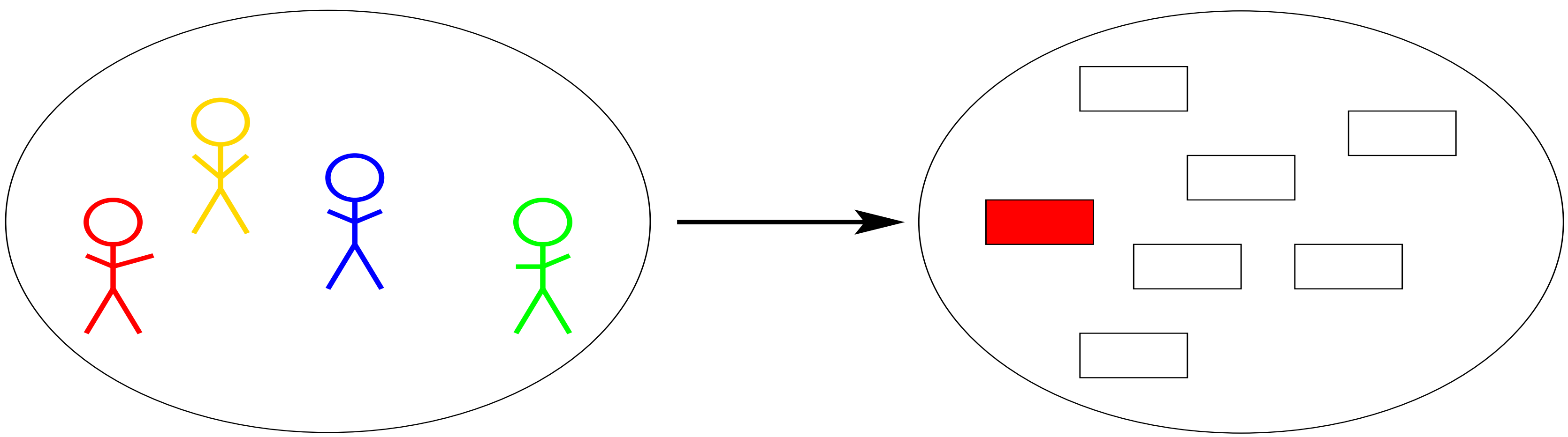
- 'Informal continuum' with 6 intermediate points from 'absolute privacy' to 'provably exposed':
  - proposed by Reiter/Rubin ,1998.
  - formalised as temporal probabilistic logic formulas by Shmatikov, 2002.

- Formal languages and logics:
  - Schneider/Sidiropoulos, 1996: Process algebraic formalisation in CSP.
  - Syverson/Stubblebine, 1999: Epistemic language based on group principals.
  - Hughes/Shmatikov, 2003: Function view.

- Information theoretic models:
  - Danezis/Serjantov, 2002. Diaz/Seys/Claessens/Preneel, 2002.

Anonymity in arbitrary scenarios

(Extension of Diaz et al. and Danezis/Serjantov, 2002)



$U = \{u_1, \ldots, u_n\}$
set of subjects
e.g., set of senders

$\{p_1, \ldots, p_i\}$
probability distribution

A_i
set of actions.
e.g., set of messages

Measuring anonymity in arbitrary scenarios

Attacker model: A priori: u_i executes a with probability $\frac{1}{n}$.

A posteriori: u_i executes a with probability $p_i \geq \frac{1}{n}$

It holds $\sum_{i=1}^{n} p_i = 1$.

Effective size of the anonymity probability distribution:

$$H(X) = -\sum_{i=1}^{n} p_i \log_2(p_i).$$

Information the attacker has learned: $(\max(H(X)) - H(X))$.

Degree of anonymity

Normalisation of the information:

$$d(U) \quad := \quad 1 - \frac{max(H(X)) - H(X)}{max(H(X))} = \frac{H(X)}{max(H(X))}.$$

Note the degree measures only the probability distribution not the size of the anonymity set!

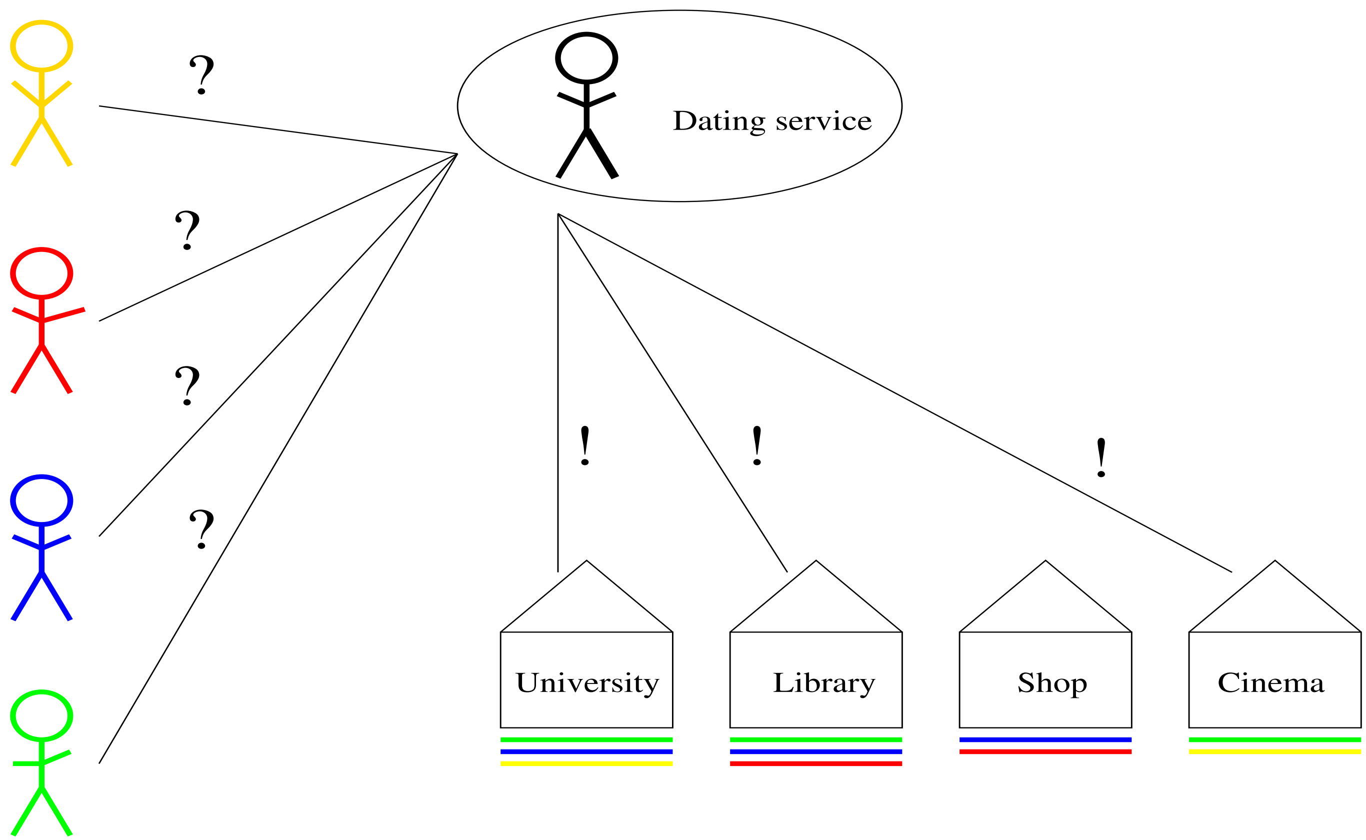
The degree's maximum/minimum is reached if

$$d(U) = 0 \qquad \Leftrightarrow \qquad \exists i \in \{1, \ldots, n\} : p_i = 1,$$

$$d(U) = 1 \qquad \Leftrightarrow \qquad \forall i \in \{1, \ldots, n\} : p_i = \frac{1}{n}.$$

How linkability endangers anonymity

Example: 'Social' attacks in a dating service (Clayton et al., 2001)



Notions of Unlinkability

Anonymity (regarding a specific action) usually restricted to users.

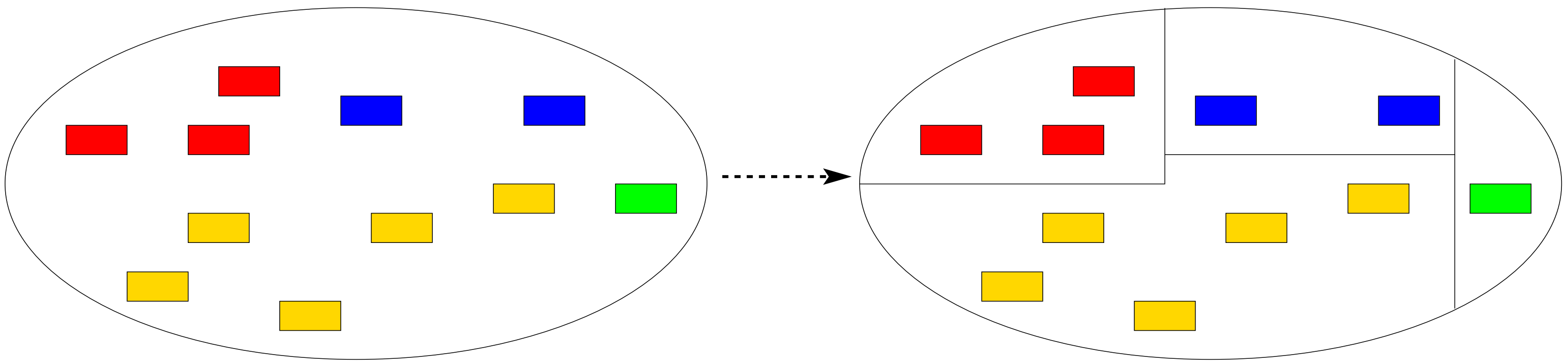
Unlinkability applicable to arbitrary items within a given system.

'Unlinkability of two or more items means that within this system, these items are no more and no less related than they are related concerning the a priori knowledge.' (Köhntopp/Pfitzmann, 2001)

Unlinkability in electronic payment systems is slightly less restrictive:

'The privacy requirement for the users is that payments made by users should not be linkable (informally, linkability means that the a posteriori probability of matching is nonneglibly greater than the a priori probability) to withdrawals, even when banks cooperate with all the shops.' (Brands 1993).

Unlinkability within one set



$A = \{a_1, \ldots, a_n\}$	$\sim_{r(A)}$	$A_1, \ldots, A_l$
set of items	equivalence relation	equivalence classes
e.g., set of messages	e.g., sent by same sender	e.g., sent by specific user

Items are related to each other. $\Leftrightarrow$ Items are in the same equivalence class.

Attacker model: A priori: A, but not $\sim_{r(A)}$.
A posteriori: something about $\sim_{r(A)}$.

Unlinkability of two items within one set

$P(a_i \sim_{r(A)} a_j)$ a posteriori probability that a_i and a_j are related.

$P(a_i \not\sim_{r(A)} a_j)$ a posteriori probability that a_i and a_j are not related.

$$P(a_i \sim_{r(A)} a_j) + P(a_i \not\sim_{r(A)} a_j) = 1 \quad \forall a_i, a_j \in A.$$

Degree of (i,j)-unlinkability:

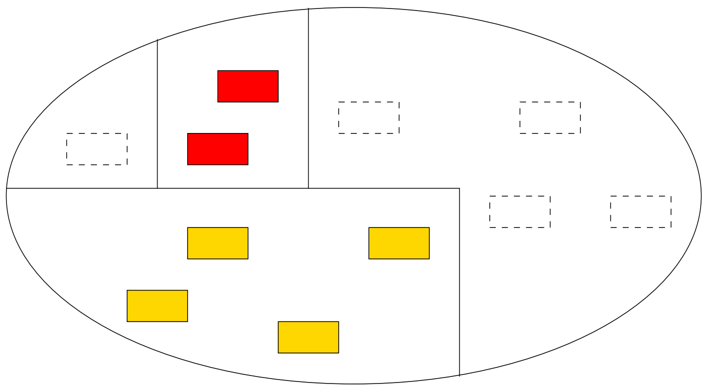
$$\begin{aligned} d(i,j) := H(i,j) \quad = \quad & -P(a_i \sim_{r(A)} a_j) \cdot \log_2(P(a_i \sim_{r(A)} a_j)) \\ & -P(a_i \not\sim_{r(A)} a_j) \cdot \log_2(P(a_i \not\sim_{r(A)} a_j)) \in [0,1]. \end{aligned}$$

The minimum/maximum is reached if

$$d(i,j) = 0 \quad \Leftrightarrow \quad (P(a_i \sim_{r(A)} a_j) = 1 \quad \vee \quad P(a_i \sim_{r(A)} a_j) = 0)$$

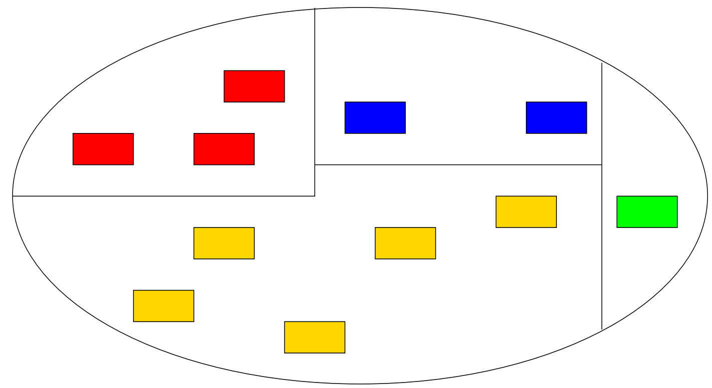
$$d(i,j) = 1 \quad \Leftrightarrow \quad P(a_i \sim_{r(A)} a_j) = P(a_i \not\sim_{r(A)} a_j) = \frac{1}{2}.$$

Linkability of $k > 2$ items within one set



$\{a_{i_1}, \ldots, a_{i_k}\} \subseteq A$

$\sim_{r(\{a_{i_1}, \ldots, a_{i_k}\})}$



$A = \{a_1, \ldots, a_n\}$

$\sim_{r(A)}$

Probability that the distribution of the elements $a_{i_1}, \ldots, a_{i_k}$ on equivalence classes in $\{a_{i_1}, \ldots, a_{i_k}\}$ is the same as in A:

$$P\left(\left(\sim_{r(A)} |_{\{a_{i_1}, \ldots, a_{i_k}\}}\right) = \left(\sim_{r(A)}\right) \right).$$

I_k index set enumerating equivalence relations on $\{a_{i_1}, \ldots, a_{i_k}\}$:

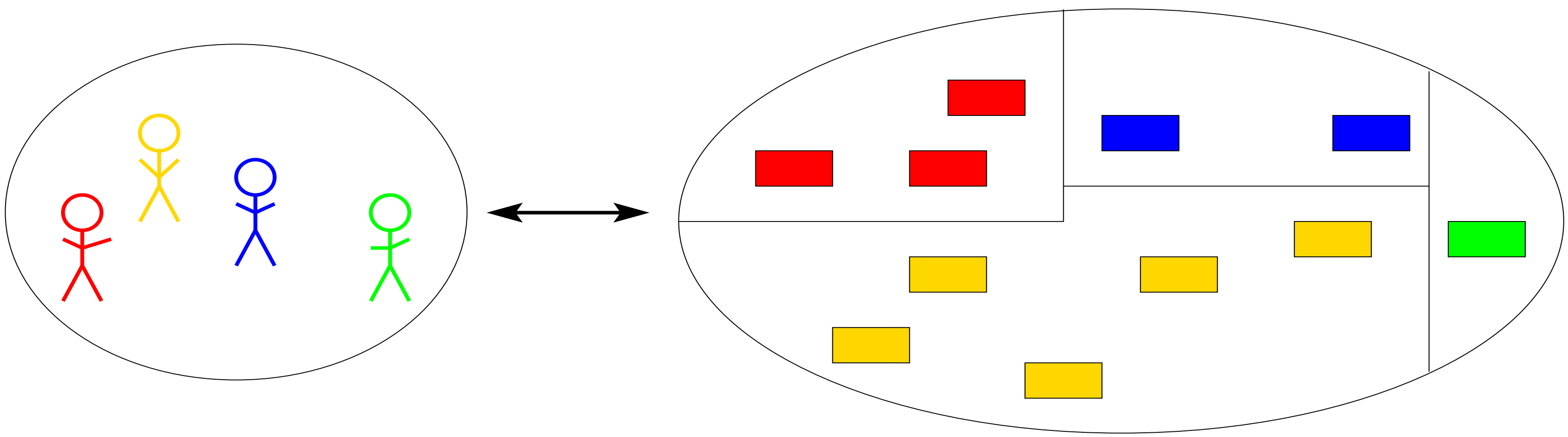
$$\sum_{j \in I_k} P\left((\sim_{r_j(A)} |_{\{a_{i_1},\ldots,a_{i_k}\}}) = (\sim_{r(A)}) \right) = 1.$$

It holds $|I_k| = 2^{k-1}$ and $\max(H(i_1, \ldots, i_k)) = k - 1$

Degree of $(i_1, \ldots, i_k)$-unlinkability:

$$\begin{aligned} d(i_1, \ldots, i_k) &:= \frac{H(i_1, \ldots, i_k)}{k-1} \\ &= -\sum_{j \in I_k} \frac{1}{k-1} \left[P\left((\sim_{r_j(A)} |_{\{a_{i_1},\ldots,a_{i_k}\}}) = (\sim_{r(A)}) \right) \right. \\ &\qquad \left. \cdot \log_2 \left(P\left((\sim_{r_j(A)} |_{\{a_{i_1},\ldots,a_{i_k}\}}) = (\sim_{r(A)}) \right) \right) \right] \in [0, 1]. \end{aligned}$$

Unlinkability between sets



$U = \{u_1, \ldots, u_n\}$ e.g., set of users

relation $\sim_{r(U,A)}$ a user sent a message

$A = \{a_1, \ldots, a_k\}$ e.g., set of actions

Through $\sim_{r(U,A)}$ an equivalence relation $\sim_{r(A)}$ on A is defined as 'is related to the same item in U'.

Attacker model	A priori: A and U, but not $\sim_{r(U,A)}$ and $\sim_{r(A)}$
.	A posteriori: something about $\sim_{r(U,A)}$ and $\sim_{r(A)}$.

$P(u_i \sim_{r(U,A)} a_j)$	a posteriori probability that u_i and a_j are related.
$P(u_i \not\sim_{r(U,A)} a_j)$	a posteriori probability that u_i and a_j are not related.

It holds

$$P(u_i \sim_{r(U,A)} a_j) + P(u_i \not\sim_{r(U,A)} a_j) = 1 \quad \forall u_i \in U, a_j \in A.$$

Degree of (u_i, a_j)-unlinkability:

$$\begin{aligned} d(u_i, a_j) &= H(u_i, a_j) \\ &= -P(a_i \sim_{r(A)} a_j) \cdot \log_2(P(a_i \sim_{r(A)} a_j)) \\ &\quad -P(a_i \not\sim_{r(A)} a_j) \cdot \log_2(P(a_i \not\sim_{r(A)} a_j)) \in [0, 1]. \end{aligned}$$

Attacks on Unlinkability

1. **Existential break:** There exist any two items which unlinkability decreases.

2. **Selective break:** The attacker chooses the items which unlinkability should decreases.
   (a) Chosen subset of items
   (b) Chosen Item

In contrast to authentication or encryption systems existential breaks cannot be neglected!

Structure of the linkability relation

Attacker's knowledge about the structure of the relation $\sim_{r(A)}$ on the given set A of items influence his probability distribution of unlinkability:

A priori:	A	e.g., set of messages
A posteriori:	sizes of $A_1, \ldots, A_l$	e.g., number of messages from one sender

Impact on the a posteriori probabilities in an existential break:
$a_{i_1}, \ldots, a_{i_t} \in_R A$ lie in the same equivalence class with probability

$$P(a_{i_1} \sim_{r(A)} \ldots \sim_{r(A)} a_{i_t}) = \frac{\sum_{v=1}^{l} \binom{|A_v|}{t}}{\binom{n}{t}} \text{ with } \binom{n}{t} = 0 \text{ for } n < t.$$

Theorem 1. *It is impossible that all pairs of items a_{i_1} and a_{i_2} chosen arbitrarily from A with $|A| > 1$ have degree of unlinkability $d(i_1, i_2) = 1$.*

Future tasks

- Constructing sup-optimal equivalence classes: Which distribution is best for given parameters?
- Analysing linkable interests of users and the impact of this linkability on their anonymity: How can a better anonymity set be constructed?
- Combining different linkability relations on sets (e.g., different communication layers).
- Examples on the application layer: How often should pseudonyms be used depending on the sets and linkability relations?