Privacy-supporting cloud-based conference systems: protocol and verification

Myrto Arapinis, Sergiu Bursuc, Mark Ryan

School of Computer Science, University of Birmingham

Security of cloud computing

Does user have to trust the service provider?

- Confidentiality ⟵ main issue
- Integrity
- Availability

EasyChair: the little Facebook

Year	#confs
2002	2
2003	3
2004	7
2005	66
2006	276
2007	629
2008	1312
2009	2183
2010	3306
2011	>3690
2012	>161
2013	>5

EasyChair data about Mark Ryan, 2005-2011

Reviewed papers by A.Gordon (CSF'11), D.Ghica (FCS'11), G.Steel (ESORICS'10), M.Fisher (FM'10), P.Panagaden (LICS'09), and others. Recommended *reject* for all of them.

Had papers reviewed by S.Kremer (S&P'10), A.Martin (TRUST'09), M.Huth (POPL'08), J.Fiadeiro (CAV'09), etc. They all recommended *accept*.

EasyChair data about Mark Ryan, 2005-2011

Reviewed papers by A.Gordon (CSF'11), D.Ghica (FCS'11), G.Steel (ESORICS'10), M.Fisher (FM'10), P.Panagaden (LICS'09), and others. Recommended *reject* for all of them.

Had papers reviewed by S.Kremer (S&P'10), A.Martin (TRUST'09), M.Huth (POPL'08), J.Fiadeiro (CAV'09), etc. They all recommended *accept*.

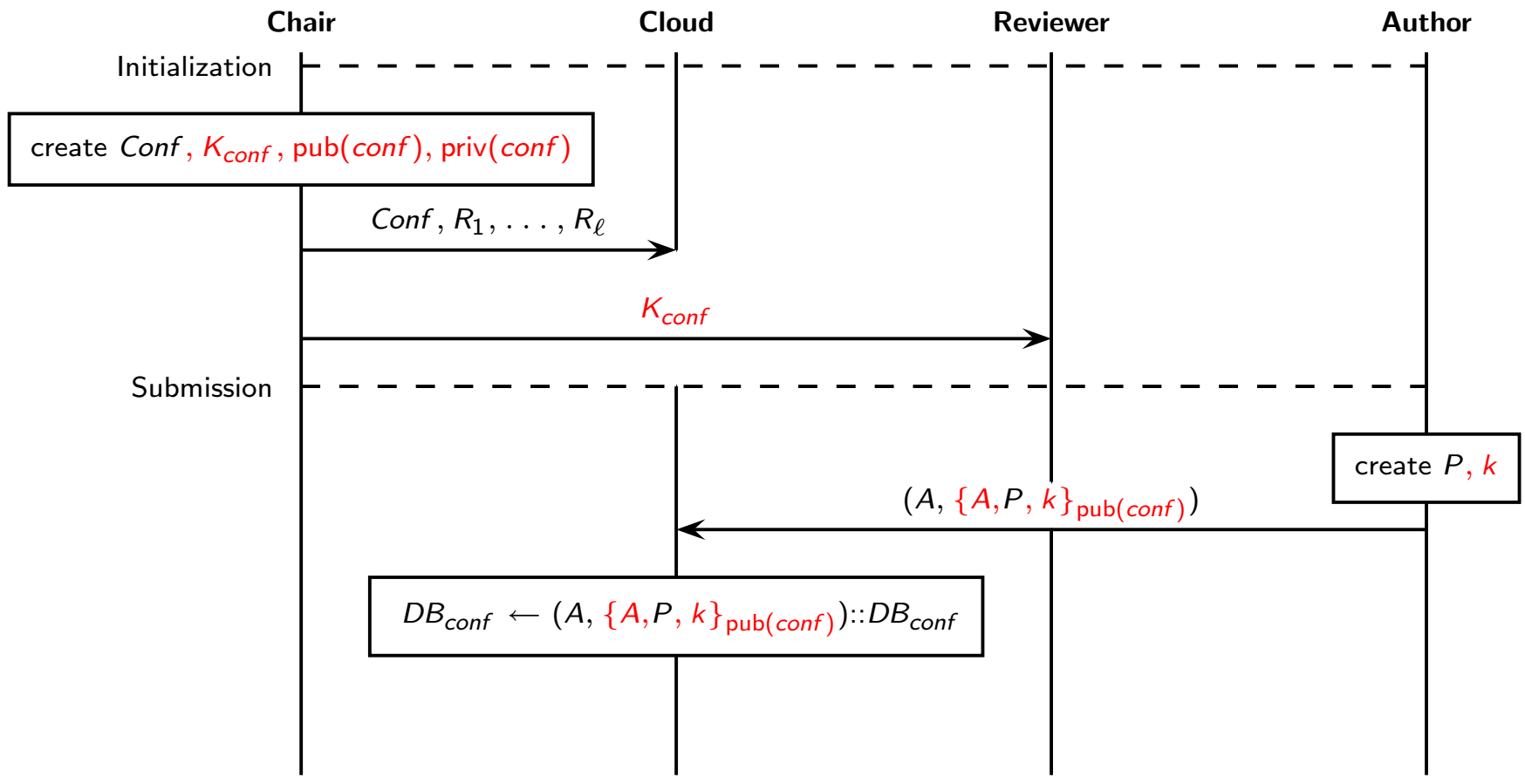
number of papers submitted	25
number of papers accepted	17
Acceptance rate	0.68
number of papers reviewed	107
number of times recommended accept	24
Recomendation agr. w. outcome	28%

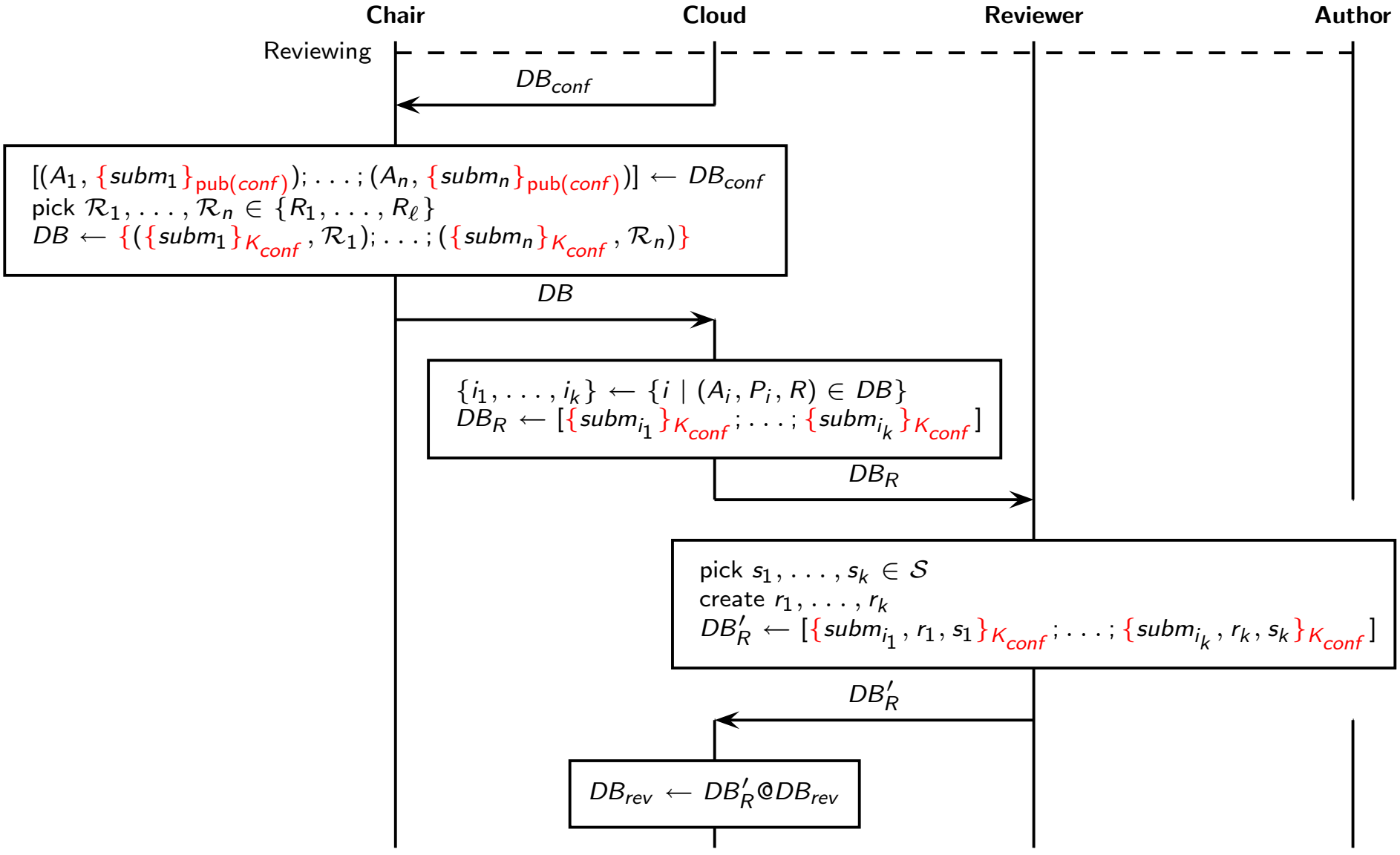
EasyChair data about Mark Ryan, 2005-2011

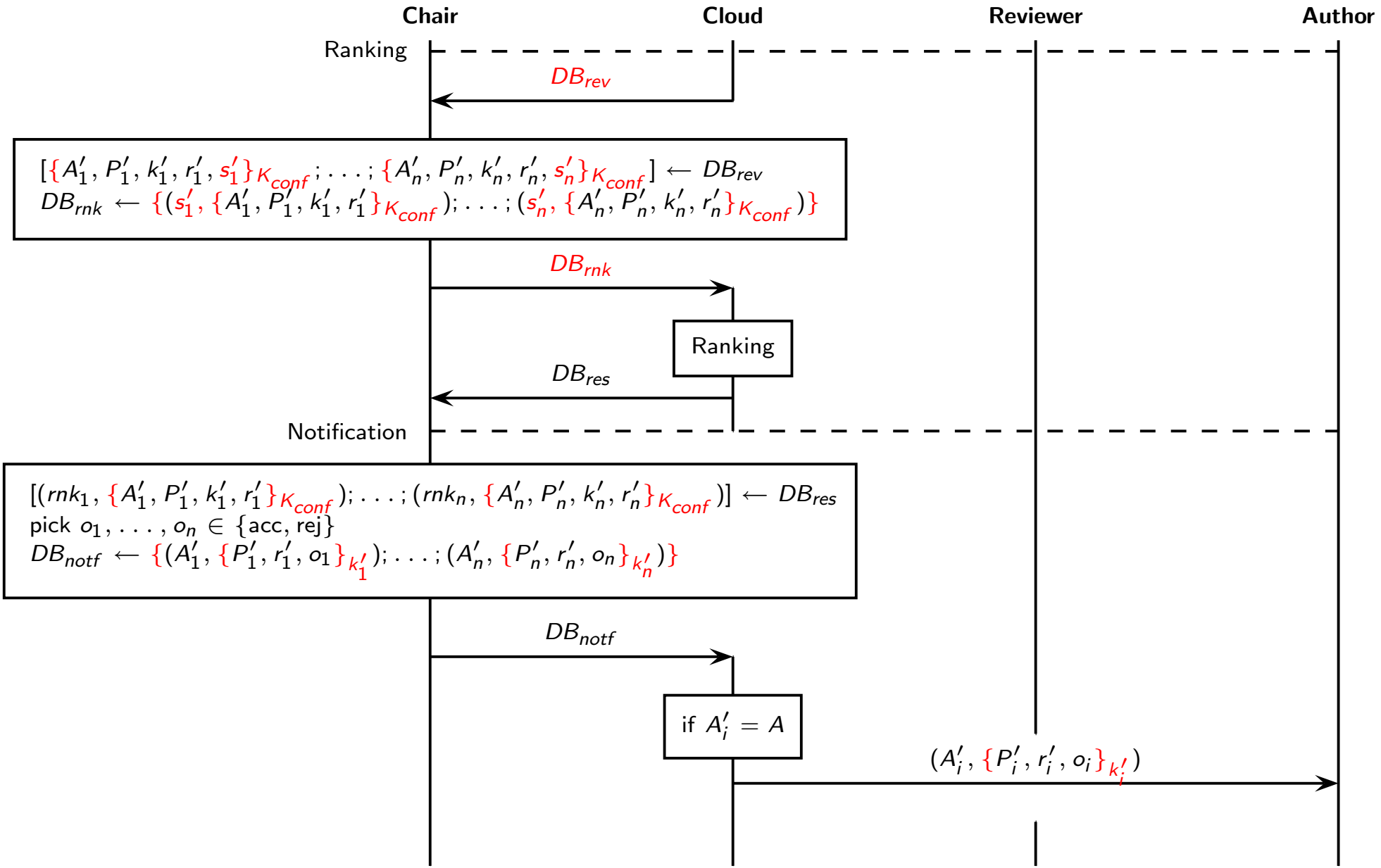
Reviewed papers by A.Gordon (CSF'11), D.Ghica (FCS'11), G.Steel (ESORICS'10), M.Fisher (FM'10), P.Panagaden (LICS'09), and others. Recommended *reject* for all of them.

Had papers reviewed by S.Kremer (S&P'10), A.Martin (TRUST'09), M.Huth (POPL'08), J.Fiadeiro (CAV'09), etc. They all recommended *accept*.

number of papers submitted	25
number of papers accepted	17
Acceptance rate	0.68
number of papers reviewed	107
number of times recommended accept	24
Recomendation agr. w. outcome	28%
Probability CSF 2012 re-invites him	0.2
Prob. will win ACM Turing award	$2^{-11.2}$


Chair
Cloud
Reviewer
Author
Initialization
create $Conf$, K_{conf}, pub($conf$), priv($conf$)
$Conf, R_1, \ldots, R_\ell$
K_{conf}
Submission
create P, k
$(A, \{A, P, k\}_{\text{pub}(conf)})$
$DB_{conf} \leftarrow (A, \{A, P, k\}_{\text{pub}(conf)})::DB_{conf}$


Chair
Cloud
Reviewer
Author
Reviewing
DB_{conf}
$[(A_1, \{subm_1\}_{pub(conf)}); \ldots; (A_n, \{subm_n\}_{pub(conf)})] \leftarrow DB_{conf}$
pick $\mathcal{R}_1, \ldots, \mathcal{R}_n \in \{R_1, \ldots, R_\ell\}$
$DB \leftarrow \{(\{subm_1\}_{K_{conf}}, \mathcal{R}_1); \ldots; (\{subm_n\}_{K_{conf}}, \mathcal{R}_n)\}$
DB
$\{i_1, \ldots, i_k\} \leftarrow \{i \mid (A_i, P_i, R) \in DB\}$
$DB_R \leftarrow [\{subm_{i_1}\}_{K_{conf}}; \ldots; \{subm_{i_k}\}_{K_{conf}}]$
DB_R
pick $s_1, \ldots, s_k \in \mathcal{S}$
create $r_1, \ldots, r_k$
$DB'_R \leftarrow [\{subm_{i_1}, r_1, s_1\}_{K_{conf}}; \ldots; \{subm_{i_k}, r_k, s_k\}_{K_{conf}}]$
DB'_R
$DB_{rev} \leftarrow DB'_R @ DB_{rev}$


Chair
Cloud
Reviewer
Author
Ranking
DB_{rev}
$[\{A'_1, P'_1, k'_1, r'_1, s'_1\}_{K_{conf}}; \ldots; \{A'_n, P'_n, k'_n, r'_n, s'_n\}_{K_{conf}}] \leftarrow DB_{rev}$
$DB_{rnk} \leftarrow \{(s'_1, \{A'_1, P'_1, k'_1, r'_1\}_{K_{conf}}); \ldots; (s'_n, \{A'_n, P'_n, k'_n, r'_n\}_{K_{conf}})\}$
DB_{rnk}
Ranking
DB_{res}
Notification
$[(rnk_1, \{A'_1, P'_1, k'_1, r'_1\}_{K_{conf}}); \ldots; (rnk_n, \{A'_n, P'_n, k'_n, r'_n\}_{K_{conf}})] \leftarrow DB_{res}$
pick $o_1, \ldots, o_n \in \{\text{acc}, \text{rej}\}$
$DB_{notf} \leftarrow \{(A'_1, \{P'_1, r'_1, o_1\}_{k'_1}); \ldots; (A'_n, \{P'_n, r'_n, o_n\}_{k'_n})\}$
DB_{notf}
if $A'_i = A$
$(A'_i, \{P'_i, r'_i, o_i\}_{k'_i})$

Formal verification

Formal model

Term algebra $\mathcal{T}(\Sigma, \mathcal{N} \cup \mathcal{X})$

$$
\begin{array}{rcl}
\mathcal{X} & = & x, y, z, \ldots \\
\mathcal{N} & = & a, b, c, k_1, k_2, \ldots \\
\Sigma & = & \{\mathsf{senc}(\_,\_,\_), \mathsf{sdec}(\_,\_), \mathsf{pub}(\_), \mathsf{aenc}(\_,\_,\_), \mathsf{adec}(\_,\_), \\
 & & \langle \_,\_ \rangle, \mathsf{proj}_1(\_), \mathsf{proj}_2(\_)\}
\end{array}
$$

Process calculus ProVerif [Blanchet'2001]

$$
\begin{array}{rcl}
P, Q, R & ::= & 0 \\
 & & P \mid Q \\
 & & !P \\
 & & \mathrm{new}\ n; P \\
 & & \mathrm{let}\ M = D\ \mathrm{in}\ P\ \mathrm{else}\ Q \\
 & & \mathrm{in}(c, M); P \\
 & & \mathrm{out}(c, M); P
\end{array}
$$

Operational semantics

Term rewriting

$$\begin{array}{rcl} \mathsf{sdec}(x, \mathsf{senc}(x, y, z)) & \rightarrow & z \\ \mathsf{adec}(x, \mathsf{aenc}(\mathsf{pub}(x), y, z)) & \rightarrow & z \end{array} \qquad \begin{array}{rcl} \mathsf{proj}_1(\langle x, y \rangle) & \rightarrow & x \\ \mathsf{proj}_2(\langle x, y \rangle) & \rightarrow & y \end{array}$$

Process reduction

$$\mathrm{out}(c, M).P \mid \mathrm{in}(c, x).Q \rightarrow P \mid Q\{^{M}/_{x}\}$$
$$\mathrm{let}\ M = D\ \mathrm{in}\ P\ \mathrm{else}\ Q \rightarrow P\sigma,\ \text{if } D \Downarrow N\ \&\ \sigma = \mu(M, N)$$
$$\mathrm{let}\ M = D\ \mathrm{in}\ P\ \mathrm{else}\ Q \rightarrow Q,\ \text{otherwise}$$

Observational equivalence

Observation $P \Downarrow c$:

$$\exists C[\_]\exists Q, \exists M. \qquad P \rightarrow^* C[\mathrm{out}(c, M).Q]$$

Largest equivalence relation s.t. $P \sim Q$ implies

$$\begin{array}{lrcl} 1. & P \Downarrow c & \Longrightarrow & Q \Downarrow c \\ 2. & P \rightarrow^* P' & \Longrightarrow & \exists Q'.\ Q \rightarrow^* Q' \ \&\ P' \sim Q' \\ 3. & \forall C[\_]. & & C[P] \sim C[Q] \end{array}$$

Secrecy in conference systems

$$\text{Papers:} \quad P_{\text{conf}} \rightsquigarrow P^{\mathbf{P}}_{\text{conf}}[\_]$$

$$\text{Reviews:} \quad P_{\text{conf}} \rightsquigarrow P^{\mathbf{R}}_{\text{conf}}[\_]$$

- Secrecy of papers: $P^{\mathbf{P}}_{\text{conf}}[\text{pap}] \sim P^{\mathbf{P}}_{\text{conf}}[\text{pap'}]$
- Secrecy of reviews: $P^{\mathbf{R}}_{\text{conf}}[\text{rev}] \sim P^{\mathbf{R}}_{\text{conf}}[\text{rev'}]$

Unlinkability in conference systems

Author-Score:

$$P^{\mathbf{AS}}_{\mathsf{conf}}(\mathsf{a}, \mathsf{one}) | P^{\mathbf{AS}}_{\mathsf{conf}}(\mathsf{b}, \mathsf{two}) \sim P^{\mathbf{AS}}_{\mathsf{conf}}(\mathsf{a}, \mathsf{two}) | P^{\mathbf{AS}}_{\mathsf{conf}}(\mathsf{b}, \mathsf{one})$$

Reviewer-Score:

$$P^{\mathbf{RS}}_{\mathsf{conf}}(\mathsf{ra}, \mathsf{one}) | P^{\mathbf{RS}}_{\mathsf{conf}}(\mathsf{rb}, \mathsf{two}) \sim P^{\mathbf{RS}}_{\mathsf{conf}}(\mathsf{ra}, \mathsf{two}) | P^{\mathbf{RS}}_{\mathsf{conf}}(\mathsf{rb}, \mathsf{one})$$

Author-Reviewer:

$$P^{\mathbf{AR}}_{\mathsf{conf}}(\mathsf{a}, \mathsf{ra}) | P^{\mathbf{AR}}_{\mathsf{conf}}(\mathsf{b}, \mathsf{rb}) \sim P^{\mathbf{AR}}_{\mathsf{conf}}(\mathsf{a}, \mathsf{rb}) | P^{\mathbf{AR}}_{\mathsf{conf}}(\mathsf{b}, \mathsf{ra})$$

Conclusions

"ToughChair"

- C does not know p and r
- C knows A, R, and s, but
  - does not know the link $A \longleftrightarrow s$
  - does not know the link $R \longleftrightarrow s$
  - does not know the link $A \longleftrightarrow R$

Formalising the properties, and verifying them.
Implementation by Matt Roberts and Joshua Phillips

`toughchair.markryan.eu`

The future

- A more systematic way to formalise the properties
- More cloud computing examples