Coercion-Resistance and Receipt-Freeness in Electronic Voting

Stéphanie Delaune\textsuperscript{1,2}, Steve Kremer\textsuperscript{2} and Mark Ryan\textsuperscript{3}

\textsuperscript{1} LSV, ENS de Cachan, CNRS & INRIA, France
\textsuperscript{2} France Télécom R&D
\textsuperscript{3} School of Computer Science, University of Birmingham, UK
Electronic voting

Advantages:
- Convenient,
- Efficient facilities for tallying votes.

Drawbacks:
- Risk of large-scale and undetectable fraud,
- Such protocols are extremely error-prone.

"A 15-year-old in a garage could manufacture smart cards and sell them on the Internet that would allow for multiple votes"

Avi Rubin

Possible issue: formal methods
abstract analysis of the protocol against formally-stated properties
Expected properties

Privacy: the fact that a particular voted in a particular way is not revealed to anyone

Receipt-freeness: a voter cannot prove that she voted in a certain way (this is important to protect voters from coercion)

Coercion-resistance: same as receipt-freeness, but the coercer interacts with the voter during the protocol, e.g. by preparing messages
Summary

Observations:
- Definitions of security properties are often **insufficiently precise**
- **No clear distinction** between receipt-freeness and coercion-resistance

Goal:
Propose the first “formal methods” definitions of receipt-freeness and coercion-resistance

Results:
- **Formalisation** of receipt-freeness and coercion-resistance as some kind of observational equivalence in the applied pi-calculus,
- **Coercion-Resistance** $\Rightarrow$ **Receipt-Freeness** $\Rightarrow$ **Privacy**,
- Case study: protocol due to Lee et al. [Lee et al., 03]
Summary

Observations:
- Definitions of security properties are often insufficiently precise
- No clear distinction between receipt-freeness and coercion-resistance

Goal:
Propose the first “formal methods” definitions of receipt-freeness and coercion-resistance

Results:
- Formalisation of receipt-freeness and coercion-resistance as some kind of observational equivalence in the applied pi-calculus,
- Coercion-Resistance $\Rightarrow$ Receipt-Freeness $\Rightarrow$ Privacy,
- Case study: protocol due to Lee et al. [Lee et al., 03]
Outline of the talk

1. Introduction

2. Applied $\pi$-calculus

3. Formalisation of Privacy and Receipt-Freeness

4. Formalisation of Coercion-Resistance

5. Conclusion and Future Works
Outline of the talk

1. Introduction

2. Applied $\pi$-calculus

3. Formalisation of Privacy and Receipt-Freeness

4. Formalisation of Coercion-Resistance

5. Conclusion and Future Works
Motivation for using the applied $\pi$-calculus

Applied pi-calculus: [Abadi & Fournet, 01]

- basic programming language with constructs for concurrency and communication
  - based on the $\pi$-calculus [Milner et al., 92]
  - in some ways similar to the spi-calculus [Abadi & Gordon, 98]

Advantages:

- allows us to model less classical cryptographic primitives
- both reachability and equivalence-based specification of properties
- automated proofs using ProVerif tool [Blanchet]
- powerful proof techniques for hand proofs
- successfully used to analyze a variety of security protocols
Motivation for using the applied $\pi$-calculus

Applied pi-calculus: [Abadi & Fournet, 01]
basic programming language with constructs for concurrency and communication

- based on the $\pi$-calculus [Milner et al., 92]
- in some ways similar to the spi-calculus [Abadi & Gordon, 98]

Advantages:

- allows us to model less classical cryptographic primitives
- both reachability and equivalence-based specification of properties
- automated proofs using ProVerif tool [Blanchet]
- powerful proof techniques for hand proofs
- successfully used to analyze a variety of security protocols
The applied $\pi$-calculus on an example

Syntax:

- **Equational theory**: $\text{dec} (\text{enc}(x, y), y) = x$
- **Process**:

$$P = \nu s, k. (\text{out}(c_1, \text{enc}(s, k)) \mid \text{in}(c_1, y).\text{out}(c_2, \text{dec}(y, k))).$$

Semantics:

- **Operational semantics** $\rightarrow$:

$$P \rightarrow \nu s, k. \text{out}(c_2, s)$$

- **Operational labeled semantics** $\alpha$:

$$P \xrightarrow{\nu x_1.\text{out}(c_1, x_1)} \nu s, k. (\text{in}(c_1, y).\text{out}(c_2, \text{dec}(y, k))) \mid \{\text{enc}(s, k)/x_1\})$$

$$\xrightarrow{\text{in}(c_1, x_1)} \nu s, k. (\text{out}(c_2, s) \mid \{\text{enc}(s, k)/x_1\})$$

$$\ldots$$
The applied $\pi$-calculus on an example

Syntax:
- Equational theory: $\text{dec}(\text{enc}(x, y), y) = x$
- Process:

$$P = \nu s, k. (\text{out}(c_1, \text{enc}(s, k)) \mid \text{in}(c_1, y).\text{out}(c_2, \text{dec}(y, k))).$$

Semantics:
- Operational semantics $\rightarrow$:

$$P \rightarrow \nu s, k.\text{out}(c_2, s)$$

- Operational labeled semantics $\xrightarrow{\alpha}$:

$$P \xrightarrow{\nu x_1.\text{out}(c_1, x_1)} \nu s, k. (\text{in}(c_1, y).\text{out}(c_2, \text{dec}(y, k))) \mid \{\text{enc}(s, k)/x_1\})$$

$$\xrightarrow{\text{in}(c_1, x_1)} \nu s, k. (\text{out}(c_2, s) \mid \{\text{enc}(s, k)/x_1\})$$

...
Static equivalence on frames – passive attacker

Frame
A frame is a process of the form $\nu \tilde{n}.(\{M_1/x_1\} | \ldots | \{M_n/x_n\})$.

Example

$$P = \nu s, k. (\text{out}(c_2, s) | \{\text{enc}(s, k)/x_1\}) \quad \phi(P) = \nu s, k. \{\text{enc}(s, k)/x_1\}$$

Static equivalence on frames ($\approx_s$)

$\varphi \approx_s \psi$ when

- $\text{dom}(\varphi) = \text{dom}(\psi)$ (the frames coincide on unrestricted variables),
- for all terms $U, V$, $(U =_E V)\varphi$ iff $(U =_E V)\psi$
Static equivalence on frames – passive attacker

Frame
A frame is a process of the form \( \nu \hat{n}.(\{^{M_1}_x\} \mid \ldots \mid \{^{M_n}_x\}) \).

Example

\[
P = \nu s, k.(\text{out}(c_2, s) \mid \{\text{enc}(s, k)/x_1\}) \quad \phi(P) = \nu s, k.\{\text{enc}(s, k)/x_1\}
\]

Static equivalence on frames \((\approx_s)\)

\(\varphi \approx_s \psi\) when

- \(\text{dom}(\varphi) = \text{dom}(\psi)\) (the frames coincide on unrestricted variables),
- for all terms \(U, V\), \((U =_E V)\varphi\) iff \((U =_E V)\psi\)

Example 1: \(\nu k.(\{\text{enc}(a,k)/x\} \mid \{k/y\}) \not\approx_s \nu n.(\{\text{enc}(b,k)/x\} \mid \{k/y\})\)
Static equivalence on frames – passive attacker

Frame
A frame is a process of the form $\nu \tilde{n}.(\{M_1/x_1\} | \ldots | \{M_n/x_n\})$.

Example

$$P = \nu s, k. (\text{out}(c_2, s) | \{\text{enc}(s, k)/x_1\}) \quad \phi(P) = \nu s, k. \{\text{enc}(s, k)/x_1\}$$

Static equivalence on frames ($\approx_s$)

$\varphi \approx_s \psi$ when

- $\text{dom}(\varphi) = \text{dom}(\psi)$ (the frames coincide on unrestricted variables),
- for all terms $U, V$, $(U =_E V)\varphi$ iff $(U =_E V)\psi$

Example 2:

$$\nu k. \{\text{enc}(a, k)/x\} \approx_s \nu n. \{\text{enc}(b, k)/x\}$$
Labeled bisimulation on processes – active attacker

Labeled bisimulation \((\cong_\ell)\)

Labeled bisimilarity is the largest symmetric relation \(\mathcal{R}\) on closed extended processes, such that \(A \mathcal{R} B\) implies

1. \(\phi(A) \cong_s \phi(B)\),
2. if \(A \rightarrow A'\), then \(B \rightarrow^* B'\) and \(A' \mathcal{R} B'\) for some \(B'\),
3. if \(A \xrightarrow{\alpha} A'\), then \(B \rightarrow^* \xrightarrow{\alpha} \rightarrow^* B'\) and \(A' \mathcal{R} B'\) for some \(B'\).

Theorem (Abadi & Fournet, 01)

\(A \cong_\ell B \iff\) no context can distinguish the two processes \(A\) and \(B\).
Voting protocols in the applied $\pi$-calculus

**Definition (Voting process)**

$$VP \equiv \nu \tilde{n}.(V \sigma_1 \mid \cdots \mid V \sigma_n \mid A_1 \mid \cdots \mid A_m)$$

- $V \sigma_i$: voter process and $\nu \in \text{dom}(\sigma_i)$ refers to the value of his vote
- $A_j$: election authority
- $\tilde{n}$: channel names

The outcome of the vote is made public, *i.e.* there exists $B$ such that

$$VP \xrightarrow{\ast \xrightarrow{\alpha} \ast} B$$

with $\phi(B) \equiv \varphi \mid \{^\nu \sigma_1/x_1, \ldots, ^\nu \sigma_n/x_n\}$ for some $\varphi$.

$\leftarrow S$ is a context which is as $VP$ but has a hole instead of two of the $V \sigma_i$
Outline of the talk

1. Introduction
2. Applied \( \pi \)-calculus
3. Formalisation of Privacy and Receipt-Freeness
4. Formalisation of Coercion-Resistance
5. Conclusion and Future Works
Formalisation of privacy

Classically modeled as observational equivalences between two slightly different processes $P_1$ and $P_2$, but
- changing the identity does not work, as identities are revealed
- changing the vote does not work, as the votes are revealed at the end

Solution: [Kremer & Ryan, 05]
$\rightarrow$ consider 2 honest voters and swap their votes

A voting protocol respects privacy if

$$S[V_A^{a/v} | V_B^{b/v}] \approx_\ell S[V_A^{b/v} | V_B^{a/v}].$$
Formalisation of privacy

Classically modeled as observational equivalences between two slightly different processes $P_1$ and $P_2$, but

- changing the identity does not work, as identities are revealed
- changing the vote does not work, as the votes are revealed at the end

Solution: [Kremer & Ryan, 05]

→ consider 2 honest voters and swap their votes

A voting protocol respects privacy if

$$S[V_A^{a/v} | V_B^{b/v}] \approx_{\ell} S[V_A^{b/v} | V_B^{a/v}].$$
Leaking secrets to the coercer

To model receipt-freeness we need to specify that a coerced voter cooperates with the coercer by leaking secrets on a channel \( ch \).

We denote by \( V^{ch} \) the process built from the process \( V \) as follows:

- \( 0^{ch} \equiv 0 \),
- \( (P \mid Q)^{ch} \equiv P^{ch} \mid Q^{ch} \),
- \( (\nu n. P)^{ch} \equiv \nu n. \text{out}(ch, n). P^{ch} \),
- \( (\text{in}(u, x). P)^{ch} \equiv \text{in}(u, x). \text{out}(ch, x). P^{ch} \),
- \( (\text{out}(u, M). P)^{ch} \equiv \text{out}(u, M). P^{ch} \),
- \( \ldots \)

We denote by \( V_{\text{out}(ch, \cdot)} \equiv \nu chc.( V \parallel \text{in}(chc, x) \). \)
Receipt-freeness

Definition (Receipt-freeness)

A voting protocol is receipt-free if there exists a process $V'$, satisfying

1. $V' \setminus \text{out}(\text{chg}, \cdot) \approx_l V_A\{a/v\}$,
2. $S[V_A\{c/v\}^{\text{chg}} \mid V_B\{a/v\}] \approx_l S[V' \mid V_B\{c/v\}]$.

Intuitively, there exists a process $V'$ which

- does vote $a$,
- leaks (possibly fake) secrets to the coancer,
- and makes the coancer believe he voted $c$. 
Some results

Let $VP$ be a voting protocol. We have formally shown that:

$$VP \text{ is receipt-free} \implies VP \text{ respects privacy}.$$  

Case study: Lee et al. protocol
We have proved receipt-freeness by

- exhibiting $V'$
- showing that $V' \setminus \text{out}(chc,\cdot) \approx_{\ell} V_A\{a/\nu\}$
- showing that $S[V_A\{c/\nu\}^\text{chc} \mid V_B\{a/\nu\}] \approx_{\ell} S[V' \mid V_B\{c/\nu\}]$
Outline of the talk

1. Introduction

2. Applied $\pi$-calculus

3. Formalisation of Privacy and Receipt-Freeness

4. Formalisation of Coercion-Resistance

5. Conclusion and Future Works
Interacting with the coercer

To model coercion-resistance, we need to model interaction between the coercer and the voter:

1. secrets are leaked to the coercer on a channel $c_1$, and
2. outputs are prepared by the coercer and given to the voter via $c_2$.

We denote by $V^{c_1,c_2}$ the process built from $V$ as follows:

- $0^{c_1,c_2} \equiv 0$,
- $(P \mid Q)^{c_1,c_2} \equiv P^{c_1,c_2} \mid Q^{c_1,c_2}$,
- $(\nu n.P)^{c_1,c_2} \equiv \nu n.\text{out}(c_1,n).P^{c_1,c_2}$,
- $(\text{in}(u,x).P)^{c_1,c_2} \equiv \text{in}(u,x).\text{out}(c_1,x).P^{c_1,c_2}$,
- $(\text{out}(u,M).P)^{c_1,c_2} \equiv \text{in}(c_2,x).\text{out}(u,x).P^{c_1,c_2}$ (x is a fresh variable),
- ...
Coercion-resistance (1)

First approximation:

\( VP \) is **coercion-resistant** if there exists a process \( V' \) such that

\[
S[V_A\{c / v\}^{c_1,c_2} \mid V_B\{a / v\}] \approx_{\ell} S[V' \mid V_B\{c / v\}].
\]

Problem:

- the coercer could oblige \( V_A\{c / v\}^{c_1,c_2} \) to vote \( c' \neq c \),
- the process \( V_B\{c / v\} \) would not counterbalance the outcome

Solution:

\( \rightarrow \) a new relation we have called adaptive simulation \( (A \preceq_a B) \)
Coercion-resistance (1)

First approximation:

$VP$ is coercion-resistant if there exists a process $V'$ such that

$$S[V_A\{c/v\}^{c_1,c_2} \mid V_B\{a/v\}] \approx_\ell S[V' \mid V_B\{c/v\}].$$

Problem:

- the coercer could oblige $V_A\{c/v\}^{c_1,c_2}$ to vote $c' \neq c$,
- the process $V_B\{c/v\}$ would not counterbalance the outcome

Solution:

$\rightarrow$ a new relation we have called adaptive simulation $(A \preceq_a B)$
Definition (Coercion-resistance)

A voting protocol is coercion-resistant if there exists a process $V'$ and an evaluation context $C$ satisfying

- $S[V_A\{c/v\}^{c_1,c_2} \mid V_B\{a/v\}] \preceq_a S[V' \mid V_B\{x/v\}]$,
- $\nu c_1, c_2. C[V_A\{c/v\}^{c_1,c_2}] \approx_\ell V_A\{c/v\}^{chc}$,
- $\nu c_1, c_2. C[V']^{out(chc,\cdot)} \approx_\ell V_A\{a/v\}$,

where $x$ is a fresh free variable.

Intuitively,

- $V_B\{x/v\}$ can adapt his vote and counter-balance the outcome,
- we require that when we apply a context $C$ (the coercer requesting $V_A\{c/v\}^{c_1,c_2}$ to vote $c$) the process $V'$ in the same context $C$ votes $a$. 
Some results

Let $VP$ be a voting protocol. We have formally shown that:

$VP$ is coercion-resistant $\implies$ $VP$ respects receipt-free.

→ reflects the intuition but the proof is technical

Case study: Lee et al. protocol

Coercion-resistance depends on implementation details:

- encryption with integrity check
  → fault attack: the protocol is not coercion-resistant

- encryption without integrity check
  → the protocol is coercion-resistant
Conclusion and Future Works

Conclusion:
- first **formal definitions** of receipt-freeness and coercion-resistance
- coercion-resistance $\Rightarrow$ receipt-freeness $\Rightarrow$ privacy,
- a case study giving interesting insights

Future Works:
- decision **procedure** for observational equivalence for processes without replication
- other properties based on *not being able to prove*
- individual/universal verifiability
Conclusion and Future Works

Conclusion:
- first **formal definitions** of receipt-freeness and coercion-resistance
- coercion-resistance $\Rightarrow$ receipt-freeness $\Rightarrow$ privacy,
- a case study giving interesting insights

Future Works:
- decision **procedure** for observational equivalence for processes without replication
- **other properties** based on *not being able to prove*
- individual/universal verifiability