Formal Verification of e-Auction protocols

Jannik Dreier, Pascal Lafourcade, Yassine Lakhnech

Université Grenoble 1, CNRS, VERIMAG
firstname.lastname@imag.fr

Principles of Security and Trust (POST) 2013, Rome

March 19, 2013

Plan

Plan

1. Introduction
2. Formal Definitions
   - Authentication
   - Fairness
   - Privacy
3. Case Studies
   - Curtis et al.
   - Brandt
4. Conclusion

e-Auctions

quicksales .com.au

Sotheby's

GUN BROKER.COM
The Bidding Starts Now

AutoBidsOnline.com
Don't Request a Quote, Set Your Price!

ricardo.ch

ebay

mercado Libre

hood.de

WineCommune Buy and Sell Fine Wine - Online!

Challenges in e-Auctions

- Competing parties: Bidders/Buyers, Seller, Auctioneer, ...
- Many possible (complex) mechanisms:
  - English
  - Dutch
  - Sealed Bid
  - First Price
  - Second Price
  - Bulk Goods
  - ...
- Here: Sealed Bid First Price auctions

e-Auctions: Security Requirements

Fairness

Verifiability

Non-Repudiation

Non-Cancellation

Security Requirements

Secrecy of Bidding Price

Receipt-Freeness

Coercion-Resistance

Anonymity of Bidders

Plan

The Applied π-Calculus [AF01]

We use the Applied π-Calculus to model protocols:

$P, Q, R :=$	processes
0	null process
$P \mid Q$	parallel composition
$!P$	replication
$\nu n.P$	name restriction ("new")
$\texttt{if } M = N \texttt{ then } P \texttt{ else } Q$	conditional
$\texttt{in}(u, x)$	message input
$\texttt{out}(u, x)$	message output
$\{^M/_x\}$	substitution

Events

To express our properties, we use the following events:

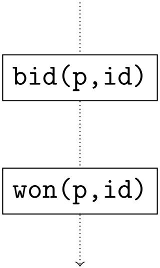
- `bid(p,id)`: a bidder `id` bids the price `p`
- `recBid(p,id)`: a bid at price `p` by bidder `id` is recorded by the auctioneer/bulletin board/etc.
- `won(p,id)`: a bidder `id` wins the auction at price `p`

Plan

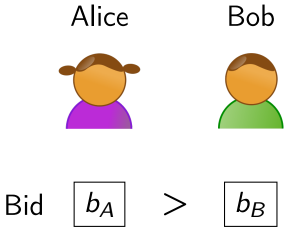
1. Introduction
2. Formal Definitions
   - Authentication
   - Fairness
   - Privacy
3. Case Studies
   - Curtis et al.
   - Brandt
4. Conclusion

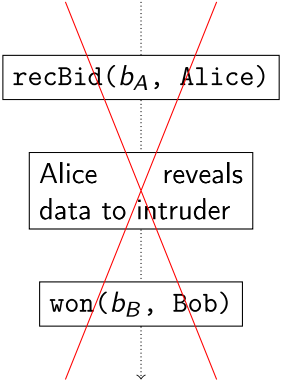
Non-Repudiation

On every trace:



Non-Cancellation





Plan

Strong Noninterference & Weak Noninterference

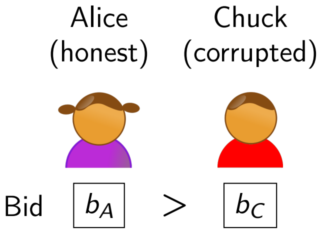
Definition (Strong Noninterference (SN))

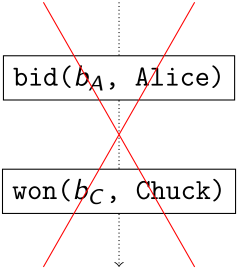
An auction protocol ensures *Strong Noninterference (SN)* if for any two auction processes AP_A and AP_B that halt at the end of the bidding phase (i.e. where we remove all code after the last `recBid` event) we have $AP_A \approx_l AP_B$.

Definition (Weak Noninterference (WN))

Like Strong Noninterference, but we consider only processes with the same bidders.

Highest Price Wins





Plan

Strong Bidding-Price Secrecy (SBPS) [DJP10]

Main idea: Observational equivalence between two situations.

Alice | Carol

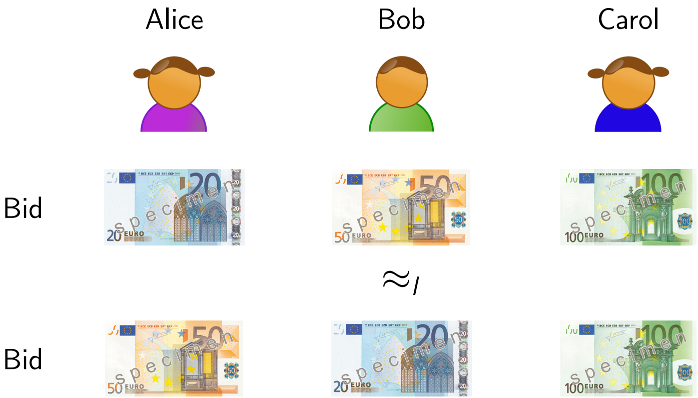

Bid


$\approx_l$

Bid

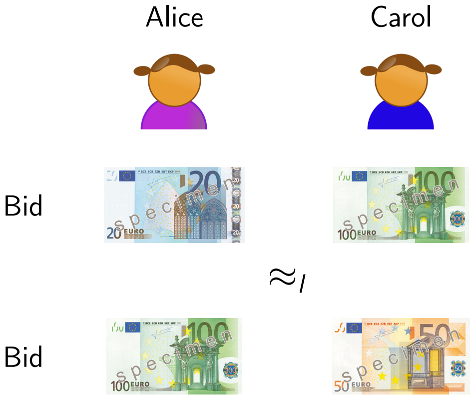

Bidding-Price Unlinkability (BPU)

The list of bids can be public, but must be unlinkable to the bidders.



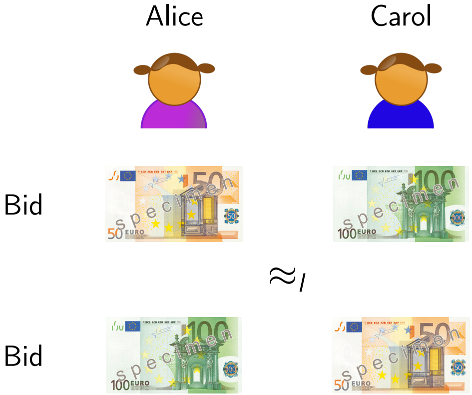
Strong Anonymity (SA)

The winner may stay anonymous.

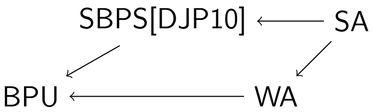


Weak Anonymity (WA)

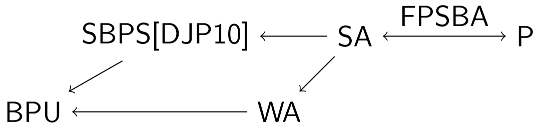
Unlinkability, but also for the winner.



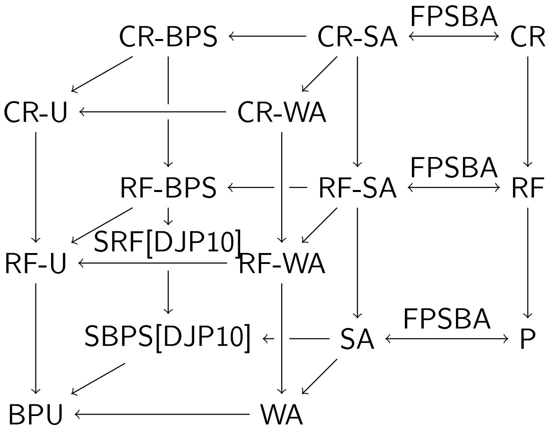
e-Auctions: Hierarchy of Privacy Notions



e-Auctions: Hierarchy of Privacy Notions



e-Auctions: Hierarchy of Privacy Notions



Plan

Plan

1. Introduction
2. Formal Definitions
   - Authentication
   - Fairness
   - Privacy
3. Case Studies
   - Curtis et al.
   - Brandt
4. Conclusion

Protocol by Curtis et al. [CPS07]: Registration

Main idea: a registration authority (RA) distributes pseudonyms, which are then used for bidding.

Bidder	Registration Authority

Protocol by Curtis et al. [CPS07]: Registration

Main idea: a registration authority (RA) distributes pseudonyms, which are then used for bidding.

Bidder

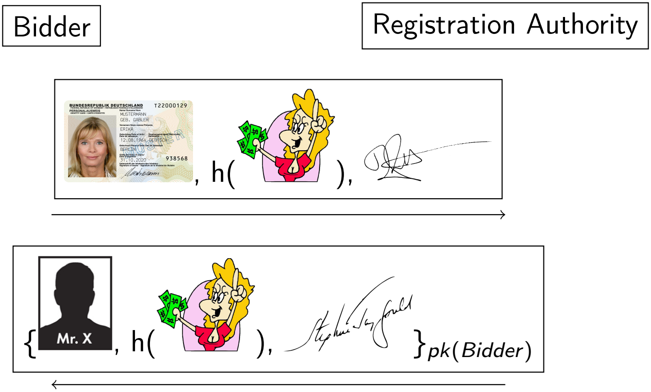
Registration Authority

, h(), 

→

Protocol by Curtis et al. [CPS07]: Registration

Main idea: a registration authority (RA) distributes pseudonyms, which are then used for bidding.

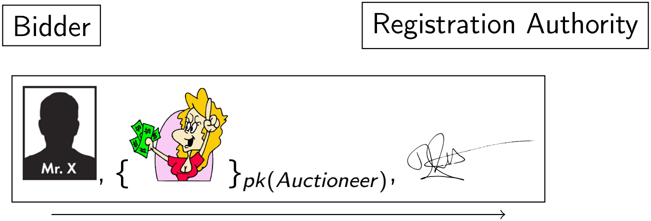


Bidding

The bidder uses his pseudonym to submit his bids.

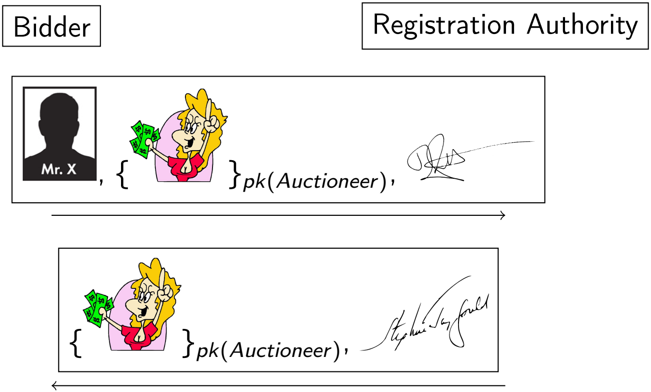
Bidding

The bidder uses his pseudonym to submit his bids.



Bidding

The bidder uses his pseudonym to submit his bids.



Bidding Cont'd

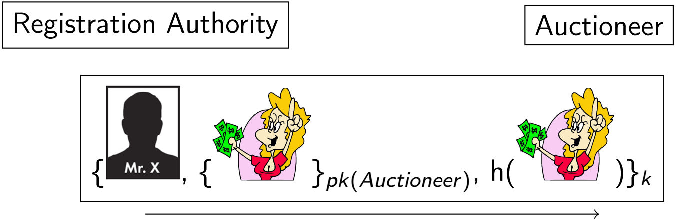
The Registration Authority forwards the bids to the auctioneer, encrypted using a symmetric key k, which is revealed at the end.

Registration Authority

Auctioneer

Bidding Cont'd

The Registration Authority forwards the bids to the auctioneer, encrypted using a symmetric key k, which is revealed at the end.



Bidding Cont'd

The Registration Authority forwards the bids to the auctioneer, encrypted using a symmetric key k, which is revealed at the end.

Registration Authority

Auctioneer

{ 

, {  $\}_{pk(Auctioneer)}$, h()$\}_k$

→

k, n

→

Completion

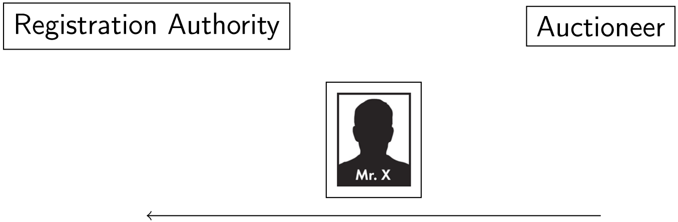
The auctioneer decrypts the bids using k and his secret key $sk(Auctioneer)$, and announces the winning pseudonym.

Registration Authority

Auctioneer

Completion

The auctioneer decrypts the bids using k and his secret key $sk(Auctioneer)$, and announces the winning pseudonym.



Analysis

Formal analysis using ProVerif [Bla01]:

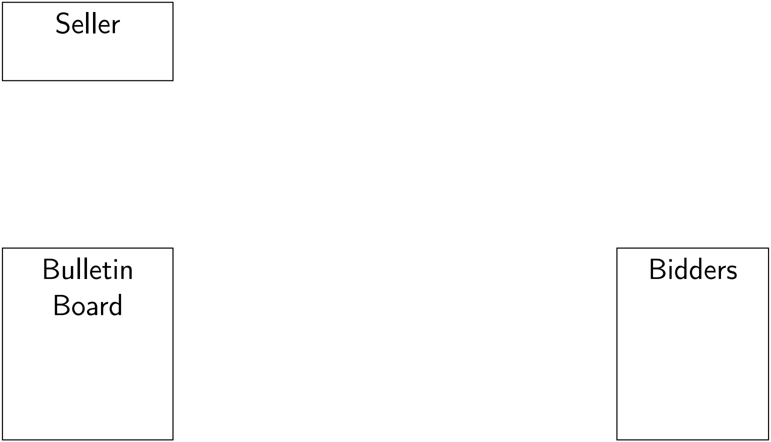
- **Non-Repudiation:** ✗ attack, the messages from the RA to the auctioneer are not authenticated - anybody can impersonate the RA
- **Non-Cancellation:** ✗ same attack
- **Highest Price Wins:** ✗ same attack
- **Weak Noninterference:** (✓) OK if first message (hash of bid) is encrypted.
- **Privacy:** (✓) Weak Anonymity if first message is encrypted and synchronization is added

Plan

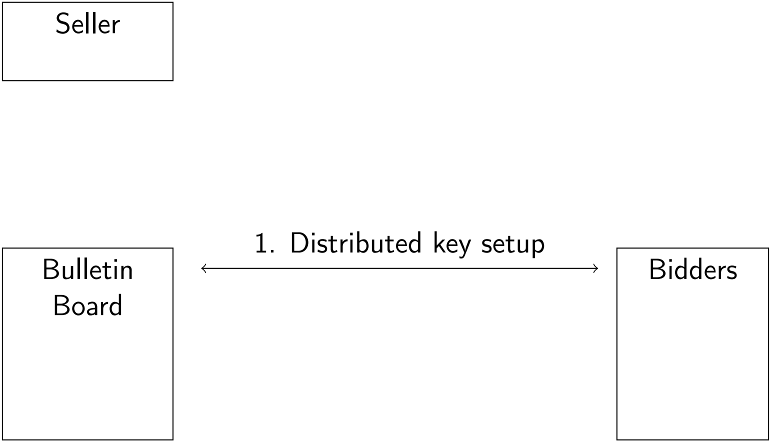
"How to obtain full privacy in auctions" by Brandt [Bra06]

- Completely distributed protocol (no authorities)
- Distributed homomorphic ElGamal encryption
- Function $f_{ij} = 1$ if bidder i won at price j, $f_{ij} \neq 1$ otherwise.

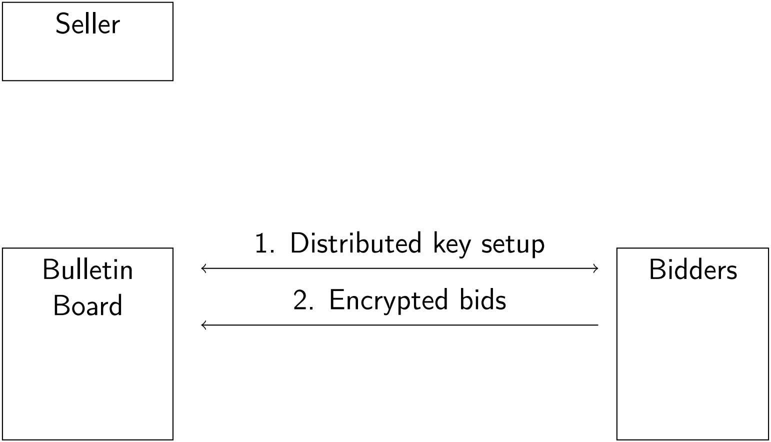
Protocol execution



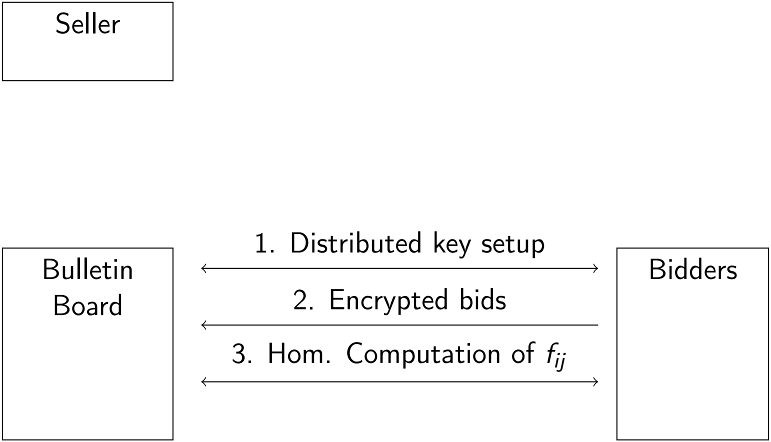
Protocol execution



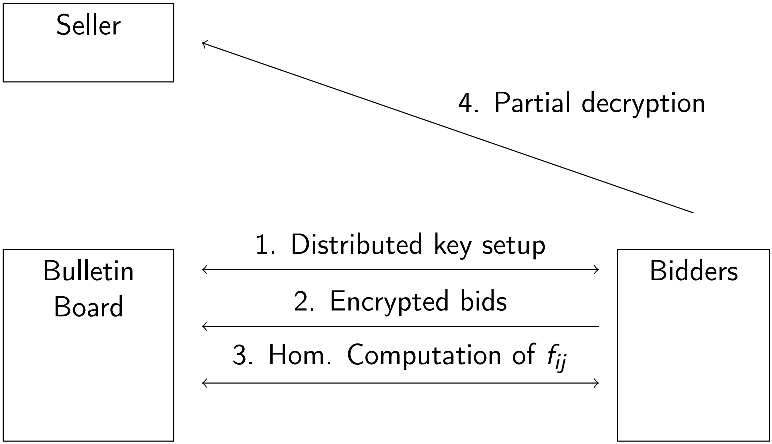
Protocol execution



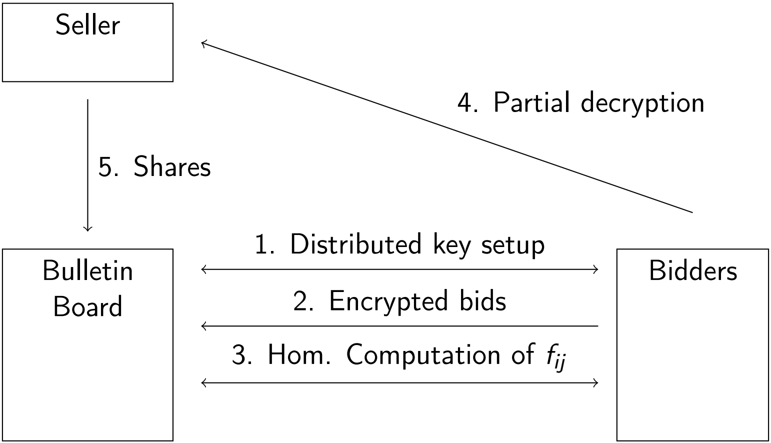
Protocol execution



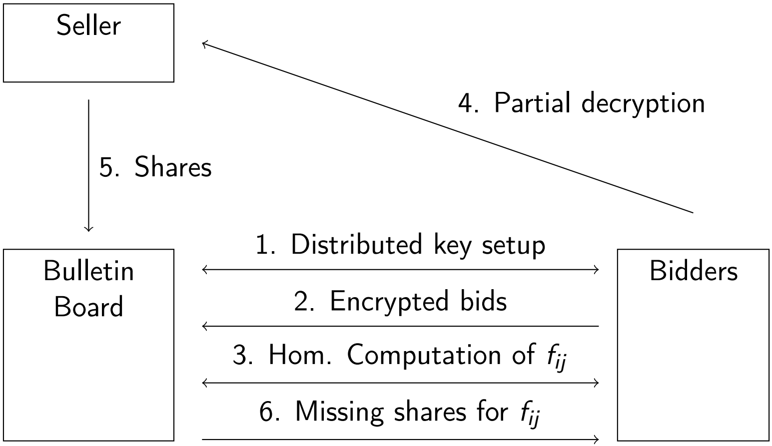
Protocol execution



Protocol execution



Protocol execution



Analysis

Automatic analysis using ProVerif:

- **Non-Repudiation, Non-Cancellation:** ✗ attack, lack of authentication
- **Weak Noninterference:** ✓ OK
- **Highest Price Wins:** ✗ attack, an intruder can impersonate all bidders, hence controlling winner and winning price
- **Privacy:** ✗ attack

Attack on Privacy

Exploit lack of authentication:

- Target one bidder
- Impersonate all other bidders
- Resubmit the targeted bidder's bid as their bids
- Impersonate the seller
- Obtain winning price=targeted bidder's bid

Plan

Conclusion

- Much work on e-Auction protocols, but not on formal analysis
- Developed a framework formalizing Non-Repudiation, Non-Cancellation, Fairness (Strong and Weak Noninterference, Highest Price Wins) and different notions of Privacy
- Suitable for automatic analysis using ProVerif
- Two case studies:
  - Protocol by Curtis et al.: attacks on Non-Repudiation, Non-Cancellation, Fairness and Privacy due to lack of authentication and synchronization
  - Protocol by Brandt: attacks on Privacy, Highest Price Wins, Non-Repudiation and Non-Cancellation
- Future work: fix problems and prove a protocol secure

Thank you for your attention!

Questions?

jannik.dreier@imag.fr

M. Abadi and C. Fournet.
Mobile values, new names, and secure communication.
In *Proc. 28th Symposium on Principles of Programming Languages*, POPL '01, pages 104–115, New York, 2001. ACM.

M. Abe and K. Suzuki.
Receipt-free sealed-bid auction.
In *Proc. 5th Conference on Information Security*, volume 2433 of *LNCS*, pages 191–199. Springer, 2002.

B. Blanchet.
An Efficient Cryptographic Protocol Verifier Based on Prolog Rules.
In *Proc. 14th Computer Security Foundations Workshop (CSFW-14)*, pages 82–96, Cape Breton, Nova Scotia, Canada, June 2001. IEEE Computer Society.

F. Brandt.

How to obtain full privacy in auctions.
International Journal of Information Security, 5:201–216, 2006.

B. Curtis, J. Pieprzyk, and J. Seruga.
An efficient eAuction protocol.
In *Proc. 7th Conference on Availability, Reliability and Security (ARES'07)*, pages 417–421. IEEE Computer Society, 2007.

Jannik Dreier, Hugo Jonker, and Pascal Lafourcade.
Defining verifiability in e-auction protocols.
In *8th ACM Symposium on Information, Computer and Communications Security (ASIACCS)*, 2013.

Naipeng Dong, Hugo L. Jonker, and Jun Pang.
Analysis of a receipt-free auction protocol in the applied pi calculus.

In Pierpaolo Degano, Sandro Etalle, and Joshua D. Guttman, editors, *Formal Aspects in Security and Trust*, volume 6561 of *LNCS*, pages 223–238. Springer, 2010.

N. Dong, H. L. Jonker, and J. Pang.
Analysis of a receipt-free auction protocol in the applied pi calculus.
In *Proc. 7th Workshop on Formal Aspects in Security and Trust (FAST'10)*, volume 6561 of *LNCS*, pages 223–238. Springer-Verlag, 2011.

Stéphanie Delaune, Steve Kremer, and Mark Ryan.
Verifying privacy-type properties of electronic voting protocols.
Journal of Computer Security, 17:435–487, December 2009.

J. Dreier, P. Lafourcade, and Y. Lakhnech.
A formal taxonomy of privacy in voting protocols.

In *Proc. 1st IEEE International Workshop on Security and Forensics in Communication Systems (ICC'12 WS - SFCS)*, 2012.

Jannik Dreier, Pascal Lafourcade, and Yassine Lakhnech.
Defining privacy for weighted votes, single and multi-voter coercion.
In Sara Foresti, Moti Yung, and Fabio Martinelli, editors, *Computer Security - ESORICS 2012 - 17th European Symposium on Research in Computer Security, Pisa, Italy, September 10-12, 2012. Proceedings*, volume 7459 of *LNCS*, pages 451–468. Springer, 2012.

M. Harkavy, J. D. Tygar, and H. Kikuchi.
Electronic auctions with private bids.
In *Proc. 3rd USENIX Workshop on Electronic Commerce*. Usenix, 1998.

B. Księżopolski and P. Lafourcade.
Attack and revision of electronic auction protocol using ofmc.
Annales UMCS Informatica 2007, pages 171–183, 2007.

R. Küsters, T. Truderung, and A. Vogt.
Accountability: definition and relationship to verifiability.
In *Proc. 17th Conference on Computer and Communications Security (CCS'10)*, CCS '10, pages 526–535. ACM, 2010.

G. Lowe.
A hierarchy of authentication specifications.
In *Computer Security Foundations Workshop, 1997. Proceedings., 10th*, pages 31 –43, jun 1997.

Frank Stajano and Ross J. Anderson.
The cocaine auction protocol: On the power of anonymous broadcast.

In Andreas Pfitzmann, editor, *Information Hiding*, volume 1768 of *LNCS*, pages 434–447. Springer, 1999.

K. Sako.
An auction protocol which hides bids of losers.
In Hideki Imai and Yuliang Zheng, editors, *Proc. 3rd Workshop on Practice and Theory in Public Key Cryptosystems (PKC 2000)*, volume 1751 of *LNCS*, pages 422–432. Springer, 2000.

Ben Smyth and Veronique Cortier.
Attacking and fixing helios: An analysis of ballot secrecy.
In *Proceedings of the 24th IEEE Computer Security Foundations Symposium (CSF'11)*, pages 297–311. IEEE, 2011.

Srividhya Subramanian.
Design and verification of a secure electronic auction protocol.

In *Proceedings of the The 17th IEEE Symposium on Reliable Distributed Systems*, SRDS '98, pages 204–, Washington, DC, USA, 1998. IEEE Computer Society.

e-Auctions: Related Work

- Plenty of protocols,
  e.g. [Bra06, CPS07, Sak00, AS02, SA99, HTK98] . . .
- Some properties known from different contexts, e.g. voting [DKR09, DLL12b, DLL12a, SC11, Low97] . . .
- Yet not much work on formalizing these properties for auctions:
  - Subramanian [Sub98]: design and verification using BAN-logic
  - B. Księżopolski and P. Lafourcade [KL07]: Authentication attack using OFMC
  - Dong, Jonker and Pang [DJP11]: Receipt-Freeness
  - Küsters et al. [KTV10]: Accountability
  - Dreier et al. [DJL13]: Verifiability

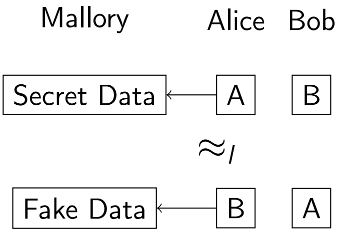
Receipt-Freeness (RF)

Again: Observational equivalence between two situations, but Alice tries to create a receipt or a fake.

Mallory	Alice	Bob
	A	B
$\approx_l$		
	B	A

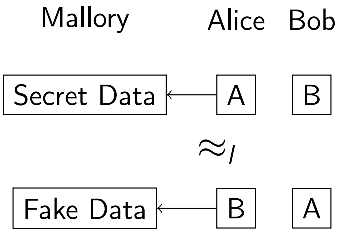
Receipt-Freeness (RF)

Again: Observational equivalence between two situations, but Alice tries to create a receipt or a fake.



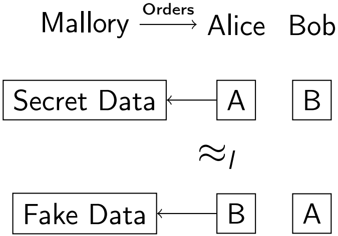
Coercion-Resistance (CR)

Observational equivalence between two situations, but Alice is under control by Mallory or only pretends to be so.



Coercion-Resistance (CR)

Observational equivalence between two situations, but Alice is under control by Mallory or only pretends to be so.



Definition (Equivalence in a Frame)

Two terms M and N are equal in the frame ϕ, written $(M = N)\phi$, if and only if $\phi \equiv \nu\tilde{n}.\sigma$, $M\sigma = N\sigma$, and $\{\tilde{n}\} \cap (fn(M) \cup fn(N)) = \emptyset$ for some names $\tilde{n}$ and some substitution σ.

Definition (Static Equivalence ($\approx_s$))

Two closed frames ϕ and ψ are statically equivalent, written $\phi \approx_s \psi$, when dom(ϕ) =dom(ψ) and when for all terms M and N $(M = N)\phi$ if and only if $(M = N)\psi$. Two extended processes A and B are statically equivalent ($A \approx_s B$) if their frames are statically equivalent.

Definition (Labelled Bisimilarity ($\approx_l$))

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

1. $A \approx_s B$,
2. if $A \to A'$, then $B \to B'$ and $A' \mathcal{R} B'$ for some B',
3. if $A \xrightarrow{\alpha} A'$ and $fv(\alpha) \subseteq \text{dom}(A)$ and $bn(\alpha) \cap fn(B) = \emptyset$, then $B \to^* \xrightarrow{\alpha} \to^* B'$ and $A' \mathcal{R} B'$ for some B'.

Definition (Process P^{ch} [DKR09])

Let P be a process and ch be a channel. We define P^{ch} as follows:

- $0^{ch} \triangleq 0$,
- $(P|Q)^{ch} \triangleq P^{ch}|Q^{ch}$,
- $(\nu n.P)^{ch} \triangleq \nu n.\mathtt{out}(ch, n).P^{ch}$ when n is a name of base type,
- $(\nu n.P)^{ch} \triangleq \nu n.P^{ch}$ otherwise,
- $(\mathtt{in}(u, x).P)^{ch} \triangleq \mathtt{in}(u, x).\mathtt{out}(ch, x).P^{ch}$ when x is a variable of base type,
- $(\mathtt{in}(u, x).P)^{ch} \triangleq \mathtt{in}(u, x).P^{ch}$ otherwise,
- $(\mathtt{out}(u, M).P)^{ch} \triangleq \mathtt{out}(u, M).P^{ch}$,
- $(!P)^{ch} \triangleq !P^{ch}$,
- $(\mathtt{if}\ M = N\ \mathtt{then}\ P\ \mathtt{else}\ Q)^{ch} \triangleq \mathtt{if}\ M = N\ \mathtt{then}\ P^{ch}\ \mathtt{else}\ Q^{ch}$.

Definition (Process P^{c_1,c_2} [DKR09])

Let P be a process, c_1, c_2 channels. We define P^{c_1,c_2} as follows:

- $0^{c_1,c_2} \triangleq 0$,
- $(P|Q)^{c_1,c_2} \triangleq P^{c_1,c_2}|Q^{c_1,c_2}$,
- $(\nu n.P)^{c_1,c_2} \triangleq \nu n.\mathtt{out}(c_1, n).P^{c_1,c_2}$ if n is a name of base type,
- $(\nu n.P)^{c_1,c_2} \triangleq \nu n.P^{c_1,c_2}$ otherwise,
- $(\mathtt{in}(u, x).P)^{c_1,c_2} \triangleq \mathtt{in}(u, x).\mathtt{out}(c_1, x).P^{c_1,c_2}$ if x is a variable of base type & x is a fresh variable,
- $(\mathtt{in}(u, x).P)^{c_1,c_2} \triangleq \mathtt{in}(u, x).P^{c_1,c_2}$ otherwise,
- $(\mathtt{out}(u, M).P)^{c_1,c_2} \triangleq \mathtt{in}(c_2, x).\mathtt{out}(u, x).P^{c_1,c_2}$,
- $(!P)^{c_1,c_2} \triangleq !P^{c_1,c_2}$,
- $(\mathtt{if}\ M = N\ \mathtt{then}\ P\ \mathtt{else}\ Q)^{c_1,c_2} \triangleq \mathtt{in}(c_2, x).\mathtt{if}\ x = \mathrm{true}$ $\mathtt{then}\ P^{c_1,c_2}\ \mathtt{else}\ Q^{c_1,c_2}$ where x is a fresh variable and true is a constant

Definition (Process $A^{\backslash out(ch,\cdot)}$ [DKR09])

Let A be an extended process. We define the process $A^{\backslash out(ch,\cdot)}$ as $\nu ch.(A|!\text{in}(ch,x))$.