Automatic Verification of Remote Electronic Voting Protocols

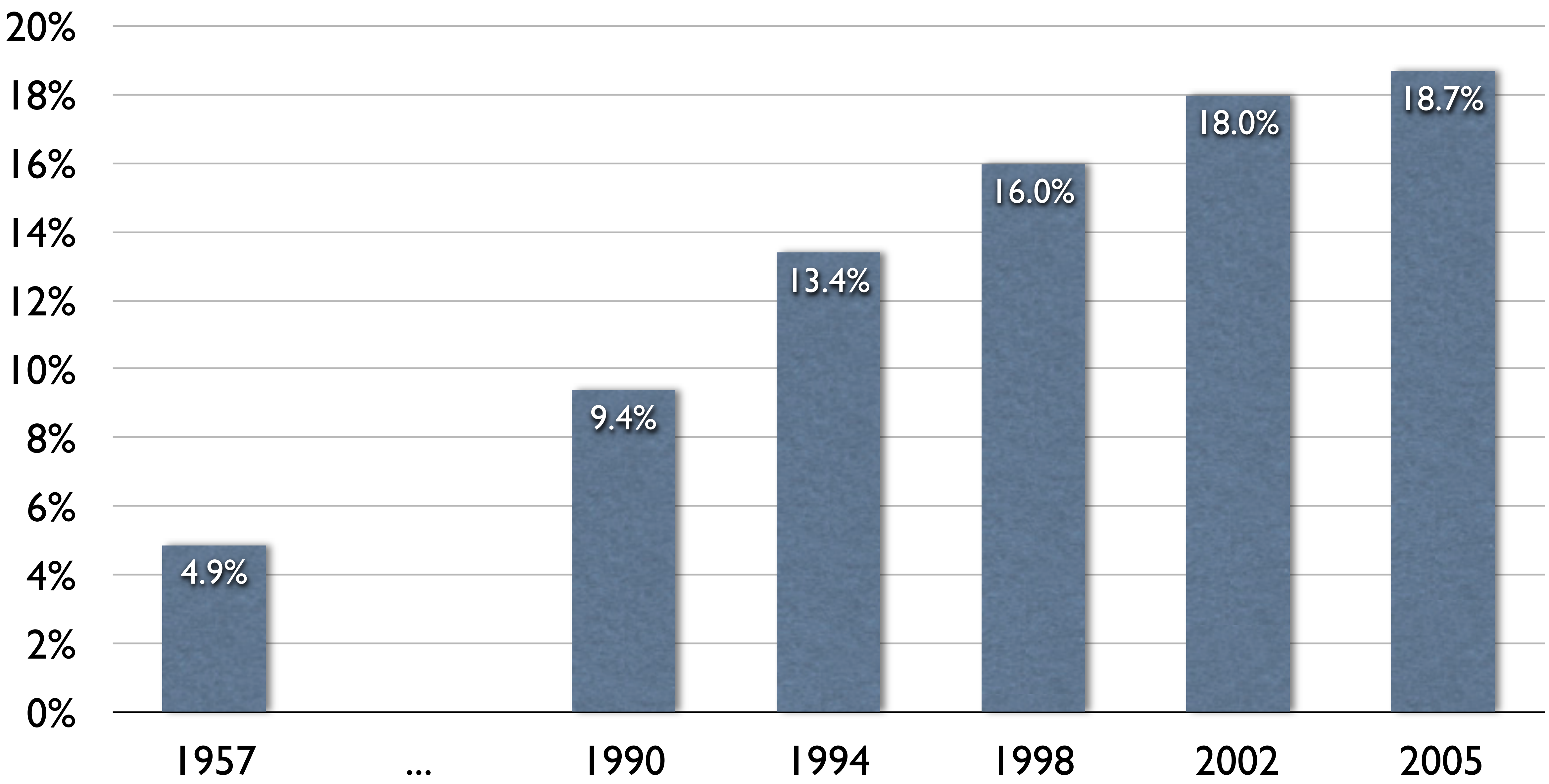
Cătălin Hrițcu

Saarland University, Saarbrücken, Germany

Joint work with: Michael Backes and Matteo Maffei

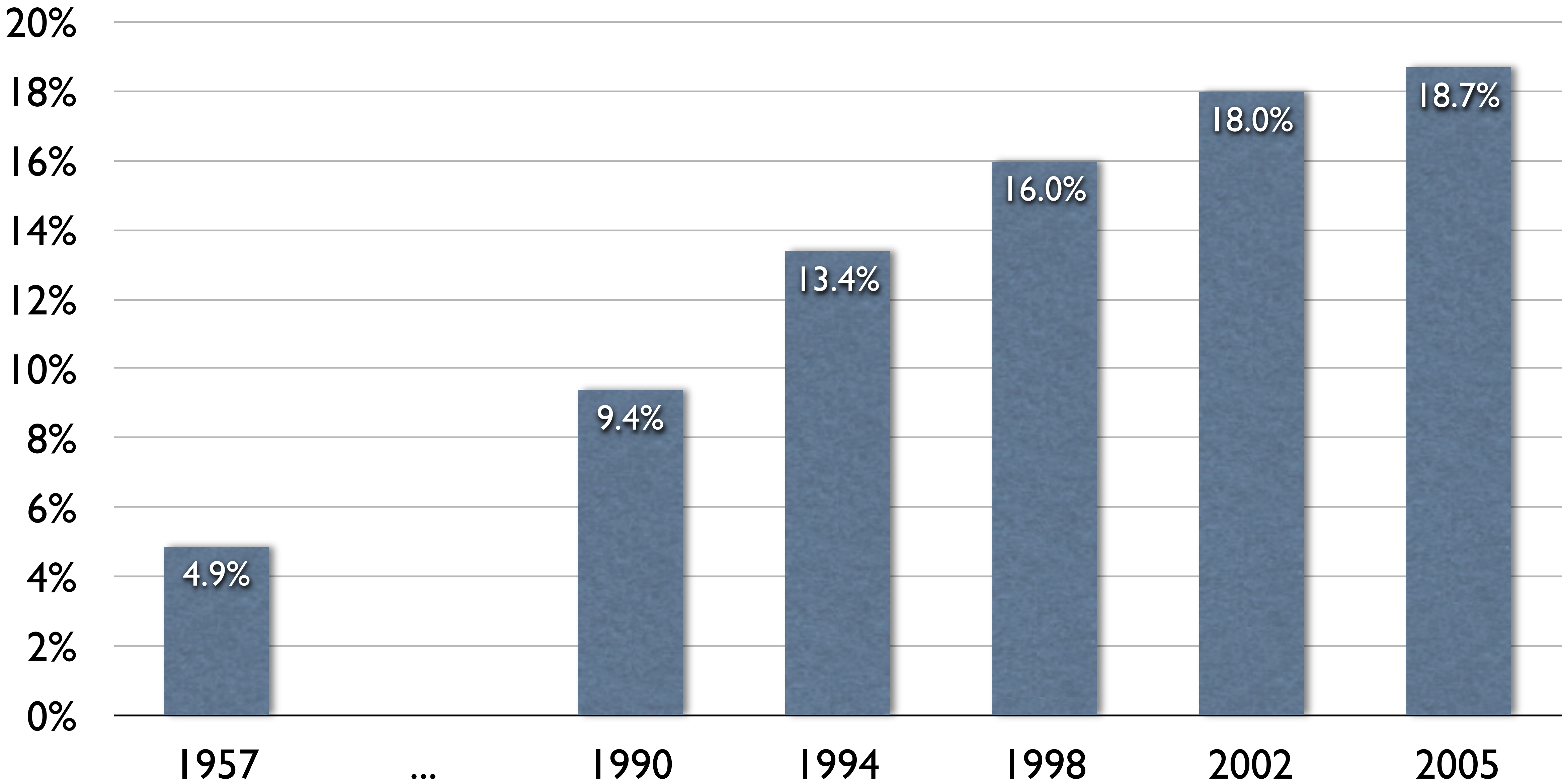
Did you know that ...

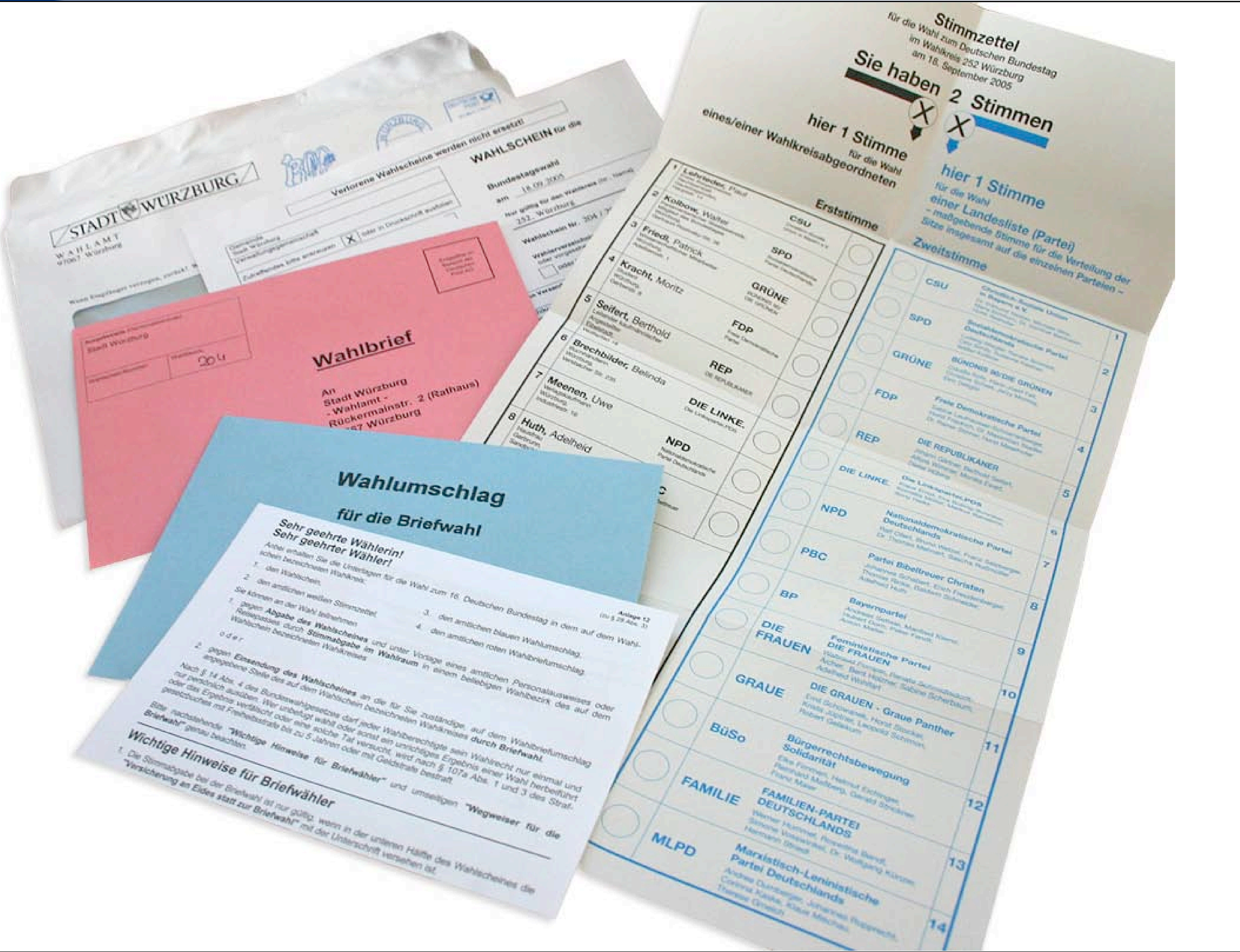
- ... in Germany, in the latest parliamentary elections **18.7%** of the votes were cast by post?



Did you know that ...

- ... in Germany, in the latest parliamentary elections **18.7%** of the votes were cast by post?
- this is a form of **remote voting**




Stimmzettel
für die Wahl zum Deutschen Bundestag
im Wahlkreis 252 Würzburg
am 18. September 2005
Sie haben 2 Stimmen
hier 1 Stimme
für die Wahl
eines/einer Wahlkreisabgeordneten
hier 1 Stimme
für die Wahl
einer Landesliste (Partei)
Erststimme
Zweitstimme
CSU
SPD
GRÜNE
FDP
REP
DIE LINKE.
NPD
PBC
BP
DIE FRAUEN
GRAUE
BüSo
FAMILIE
MLPD
STADT WÜRZBURG
WAHLSCHEIN für die
Bundestagswahl
Verlorene Wahlscheine werden nicht ersetzt!
Wahlbrief
An
Stadt Würzburg
- Wahlamt -
Rückermainstr. 2 (Rathaus)
Wahlumschlag
für die Briefwahl
Sehr geehrte Wählerin!
Sehr geehrter Wähler!
Wichtige Hinweise für Briefwähler

Remote voting (by post)

- More convenient than supervised voting
  - This should increase voter participation

Remote voting (by post)

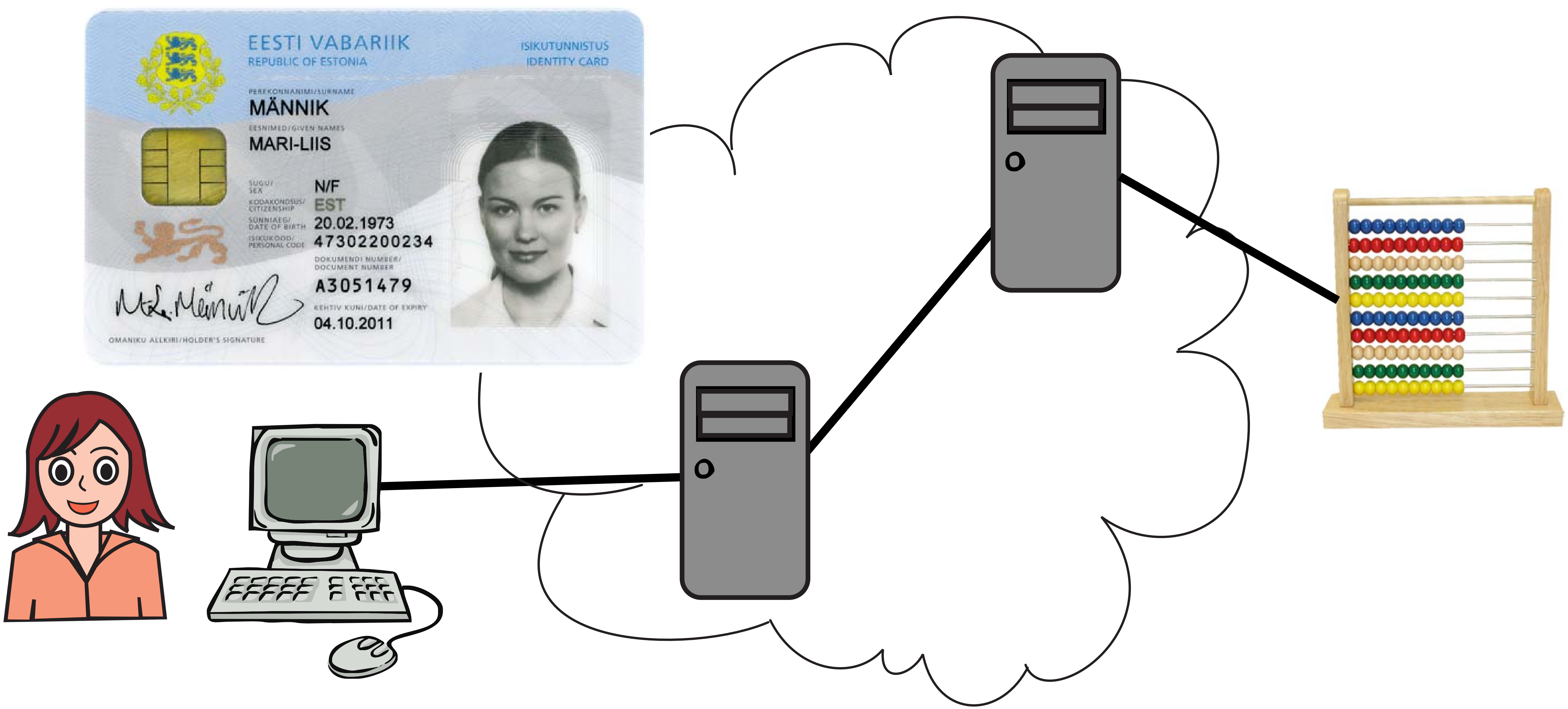
- More convenient than supervised voting
  - This should increase voter participation
- Voting by post raises many **security concerns**
  - An autograph signature does not authenticate the voter
  - An envelope does not guarantee secrecy or integrity
  - The post is not always a secure channel
  - Extremely easy to sell your vote
  - You can coerce voters to vote as you like

Remote voting (by post)

- More convenient than supervised voting
  - This should increase voter participation
- Voting by post raises many **security concerns**
  - An autograph signature does not authenticate the voter
  - An envelope does not guarantee secrecy or integrity
  - The post is not always a secure channel
  - Extremely easy to sell your vote
  - You can coerce voters to vote as you like
- Still, this has been used in Germany for 50+ years

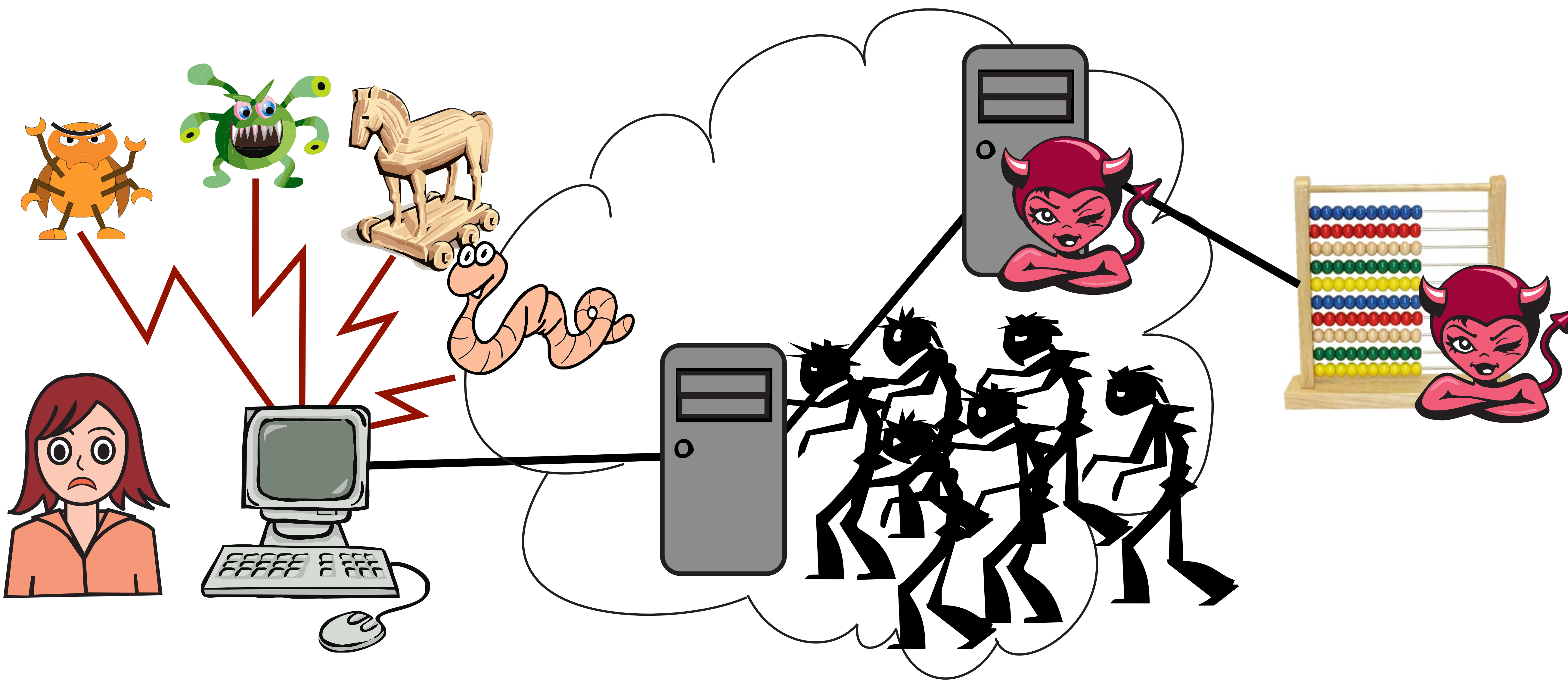
Remote electronic voting

- Seems even cheaper and even more convenient
- Promises better security (than voting by post at least)
  - the security properties can be cryptographically enforced



Remote electronic voting

- Seems even cheaper and even more convenient
- Promises better security (than voting by post at least)
    - the security properties can be cryptographically enforced



accuracy eligibility democracy fault tolerance

inalterability non-reusability robustness

completeness correctness scalability availability

fairness **desired properties**

vote-privacy

universal verifiability no forced-abstention attacks

individual verifiability receipt-freeness

coercion-resistance

accuracy

eligibility

democracy

fault tolerance

inalterability

non-reusability

robustness

completeness

correctness

scalability

availability

fairness

desired properties

vote-privacy

universal verifiability

no forced-abstention attacks

individual verifiability

receipt-freeness

coercion-resistance

- Careful formalization and automatic verification of these properties important before widespread adoption

eligibility

inalterability

non-reusability

vote-privacy

no forced-abstention attacks

receipt-freeness

coercion-resistance

- Careful formalization and automatic verification of these properties important before widespread adoption

soundness

eligibility

inalterability

non-reusability

vote-privacy

no forced-abstention attacks

receipt-freeness

coercion-resistance

- Careful formalization and automatic verification of these properties important before widespread adoption

soundness

eligibility

inalterability

non-reusability

privacy

vote-privacy

no forced-abstention attacks

receipt-freeness

coercion-resistance

- Careful formalization and automatic verification of these properties important before widespread adoption

What we did

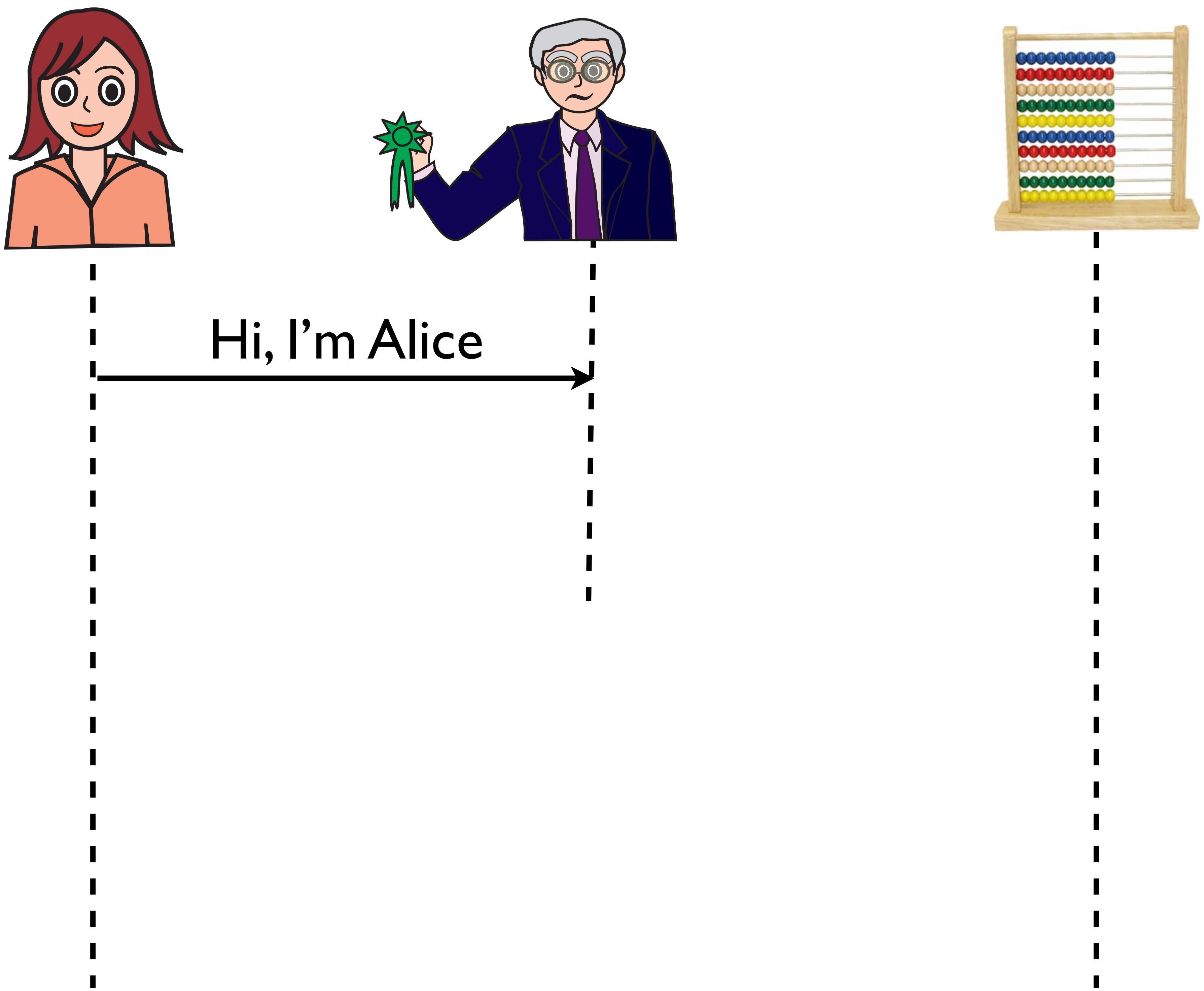
- General technique for modeling remote electronic voting protocols (in the applied pi-calculus) and automatically verifying their security
- New formal definitions of
  - soundness - trace property
  - coercion-resistance - observational equivalence
  - both definitions amenable to automation (e.g. ProVerif)
- Automatically verified the security of the JCJ protocol

What we did

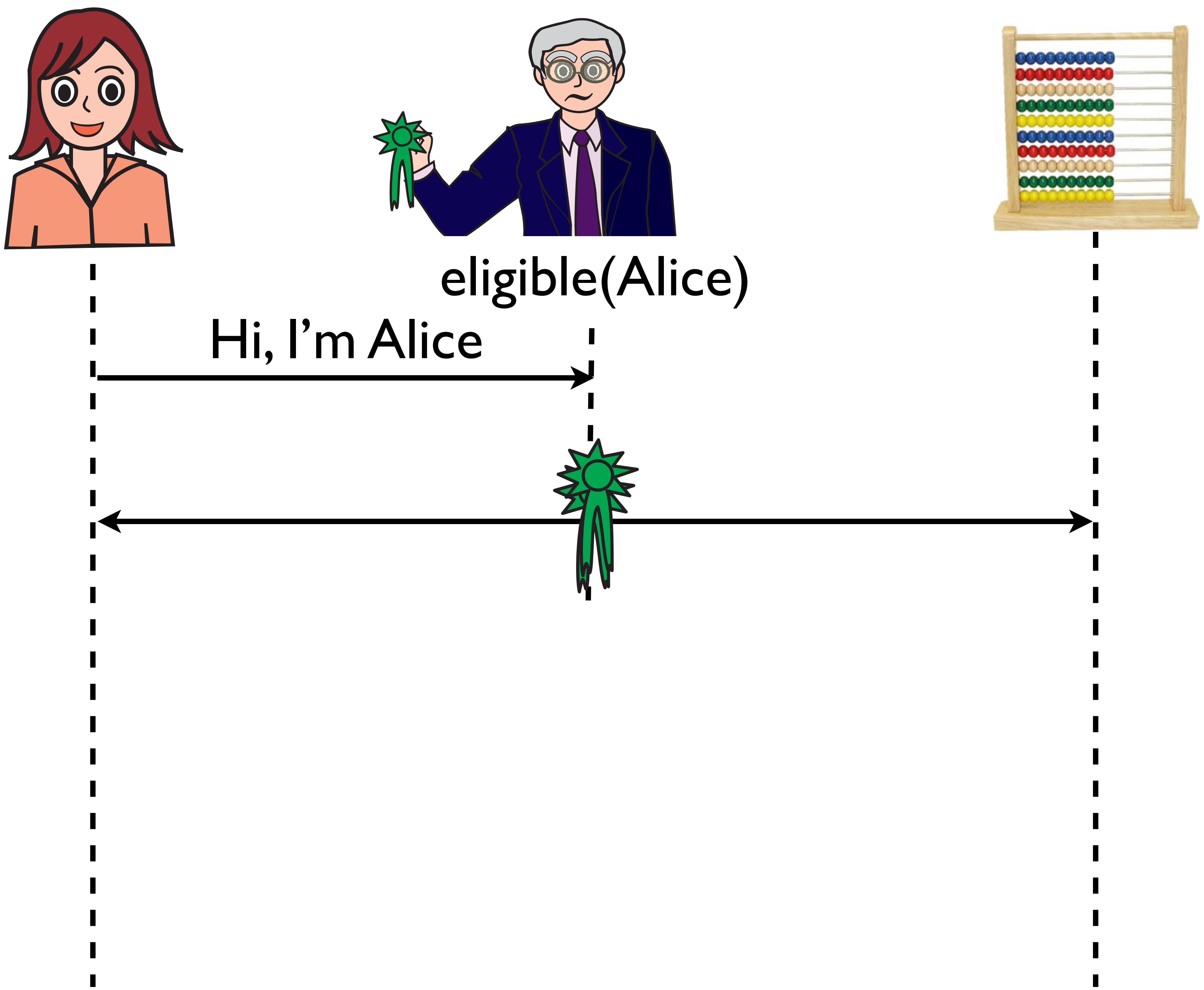
- General technique for modeling remote electronic voting protocols (in the applied pi-calculus) and automatically verifying their security
- New formal definitions of
  - soundness - trace property
  - coercion-resistance - observational equivalence
  - both definitions amenable to automation (e.g. ProVerif)
- Automatically verified the security of the JCJ protocol
- For all details see [Backes, Hrițcu & Maffei, CSF 2008]

The Big Picture

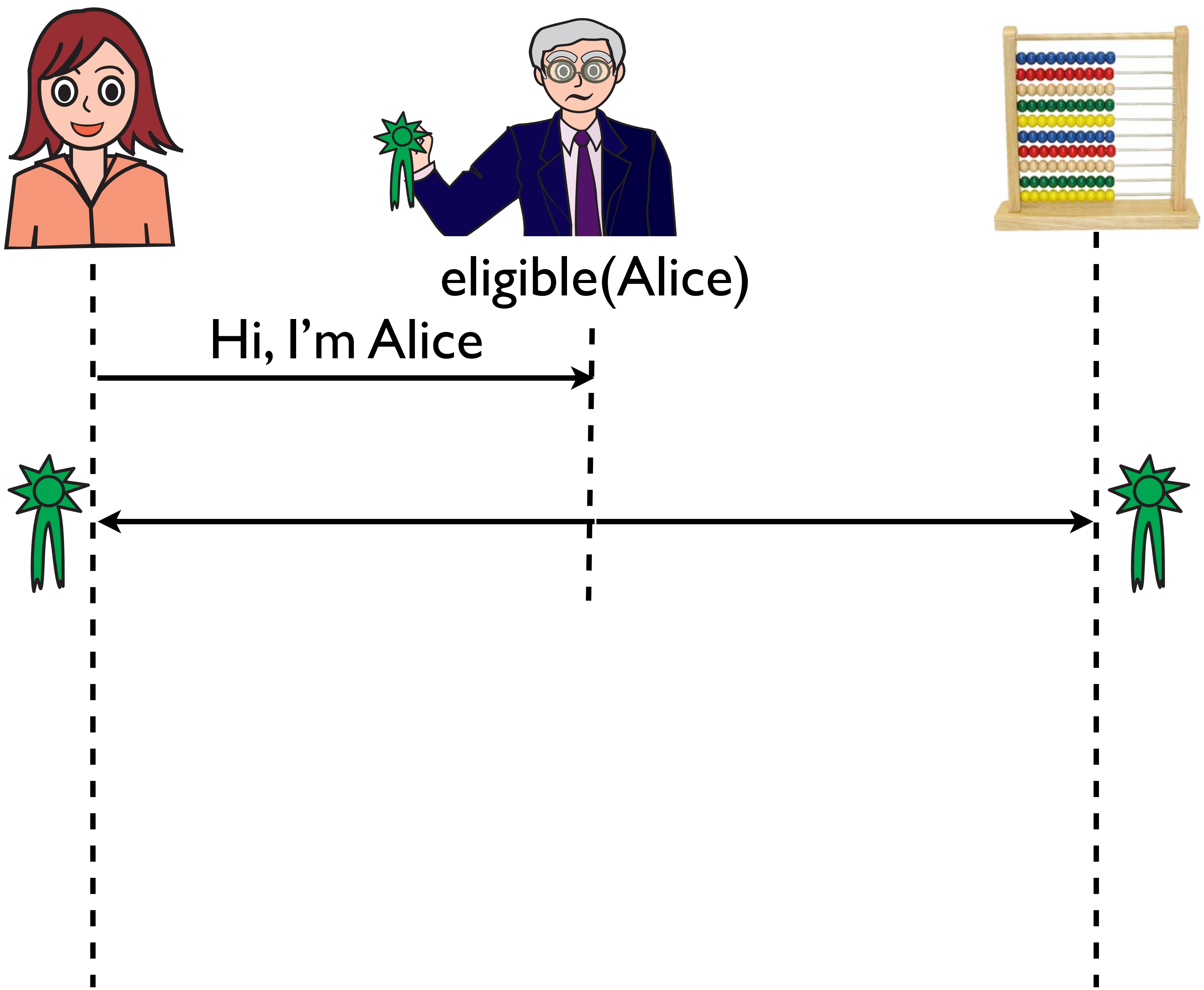
Soundness (eligibility, non-reusability, inalterability)



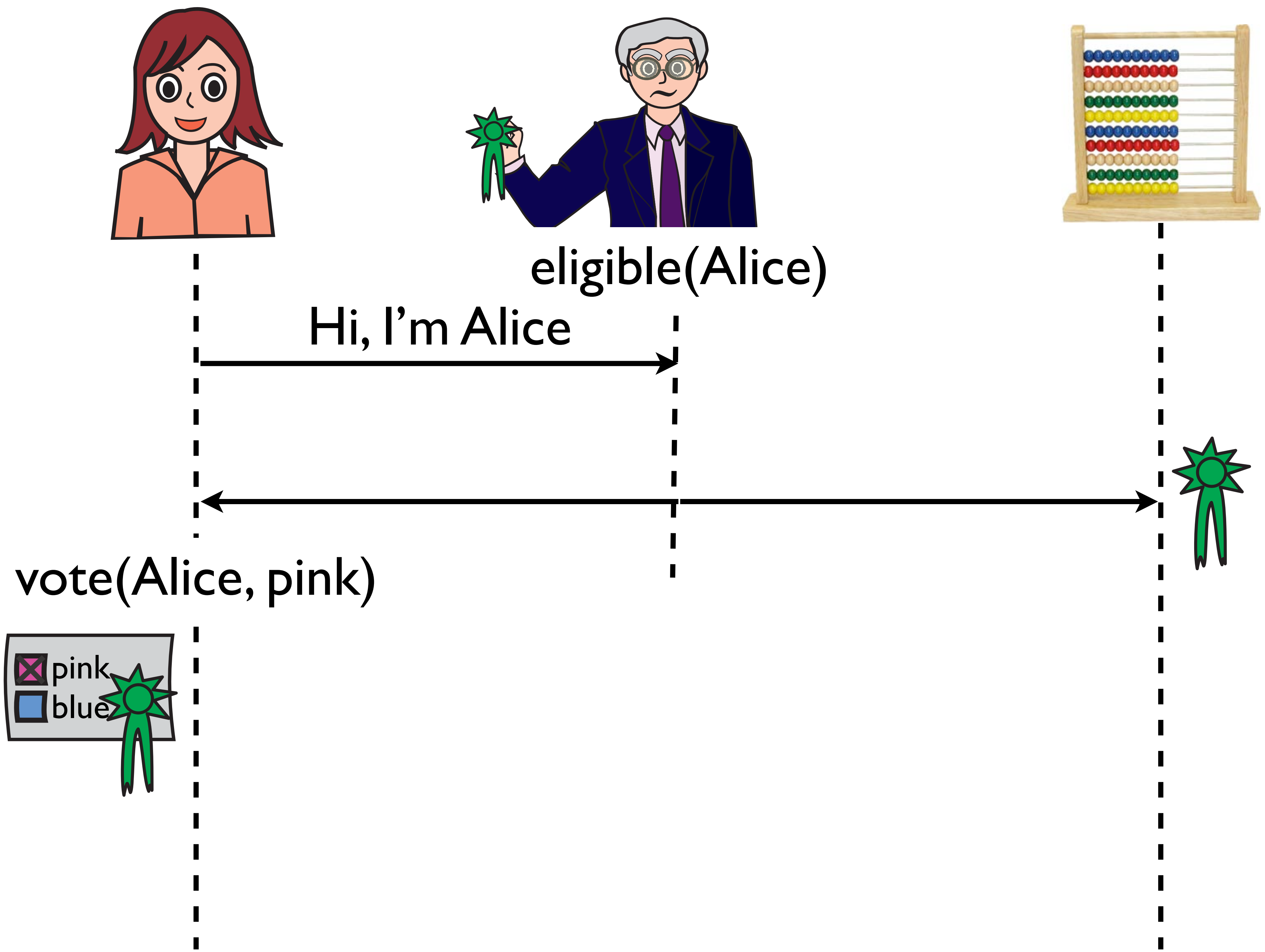
Soundness (eligibility, non-reusability, inalterability)



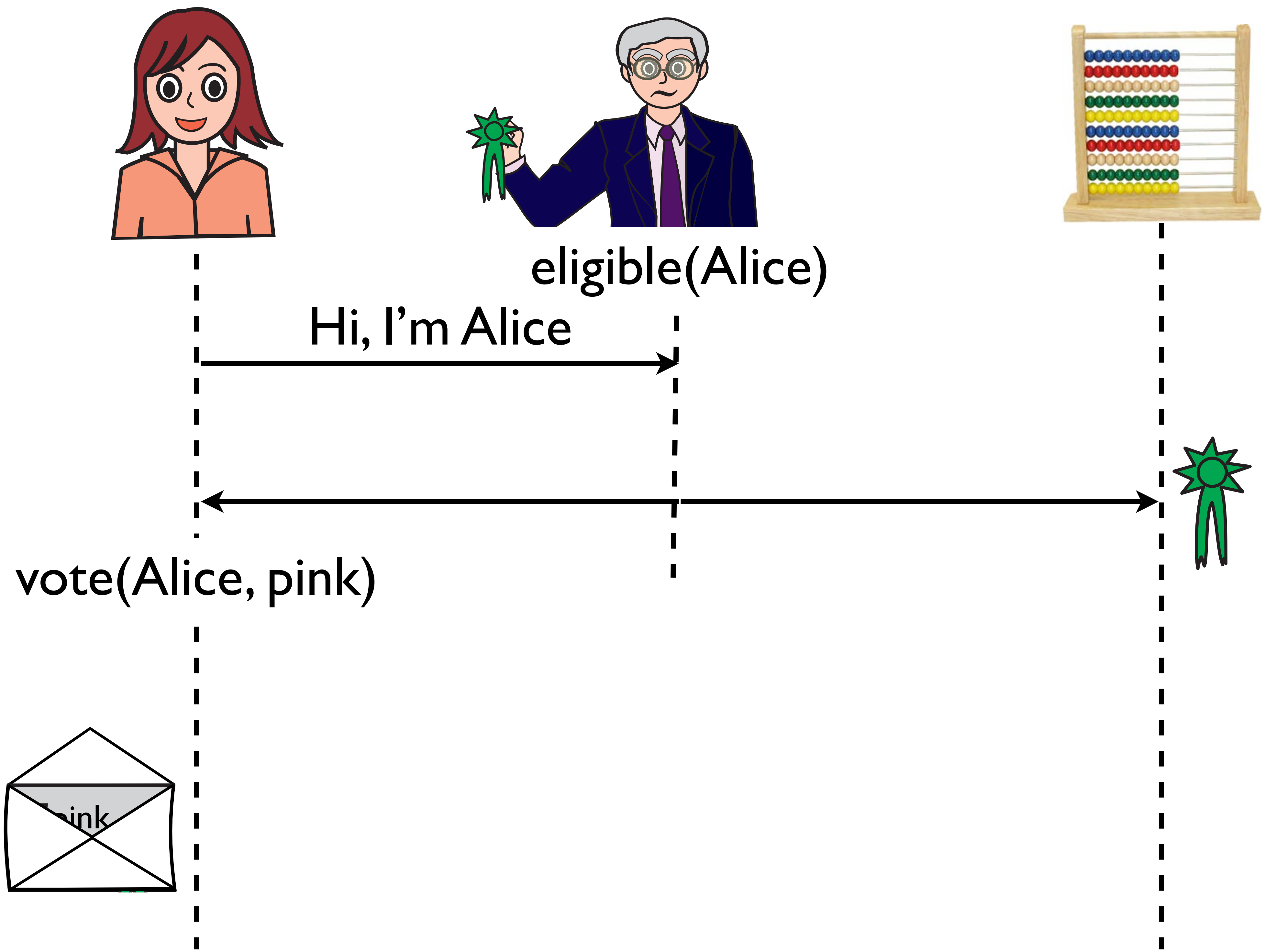
Soundness (eligibility, non-reusability, inalterability)



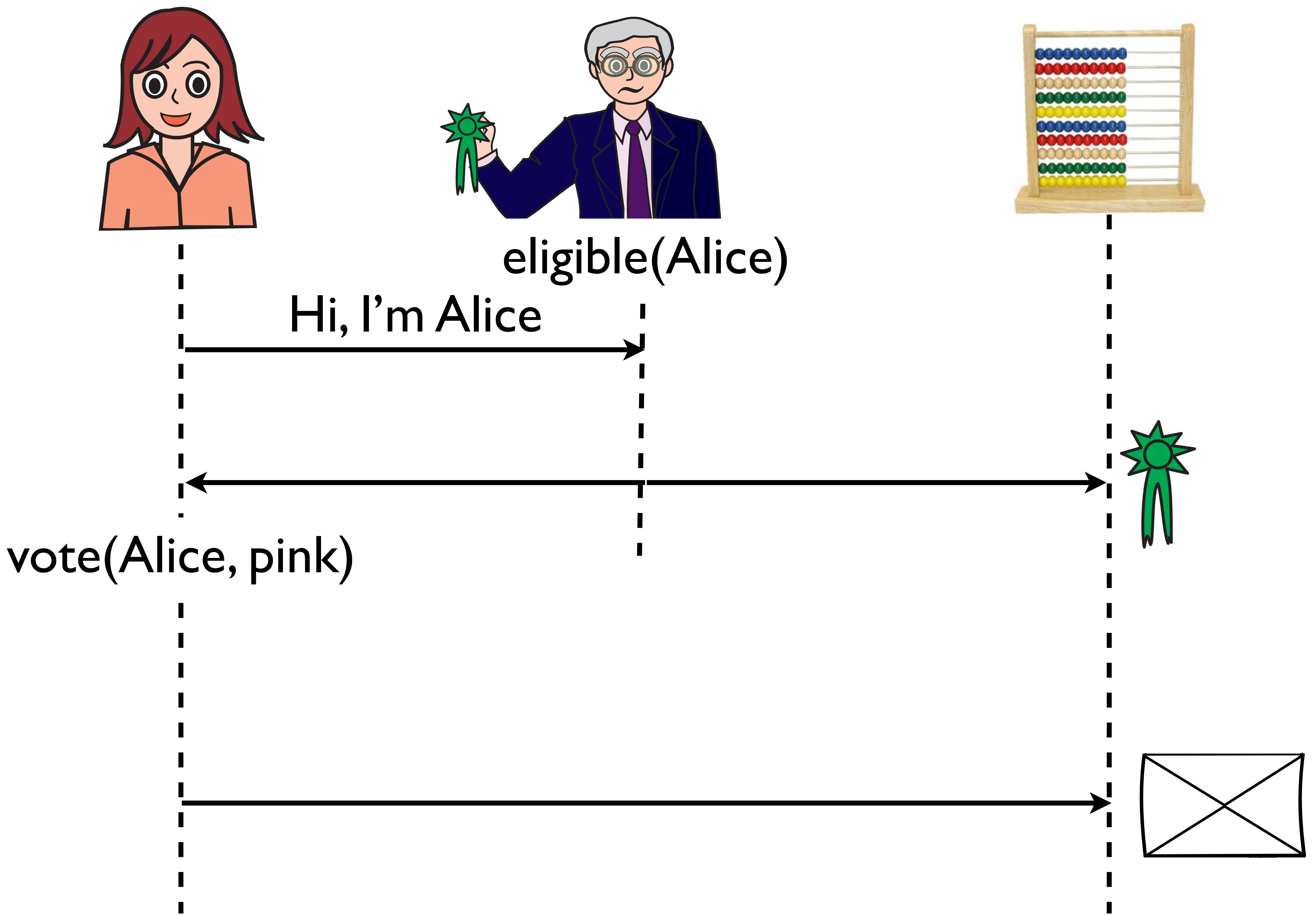
Soundness (eligibility, non-reusability, inalterability)



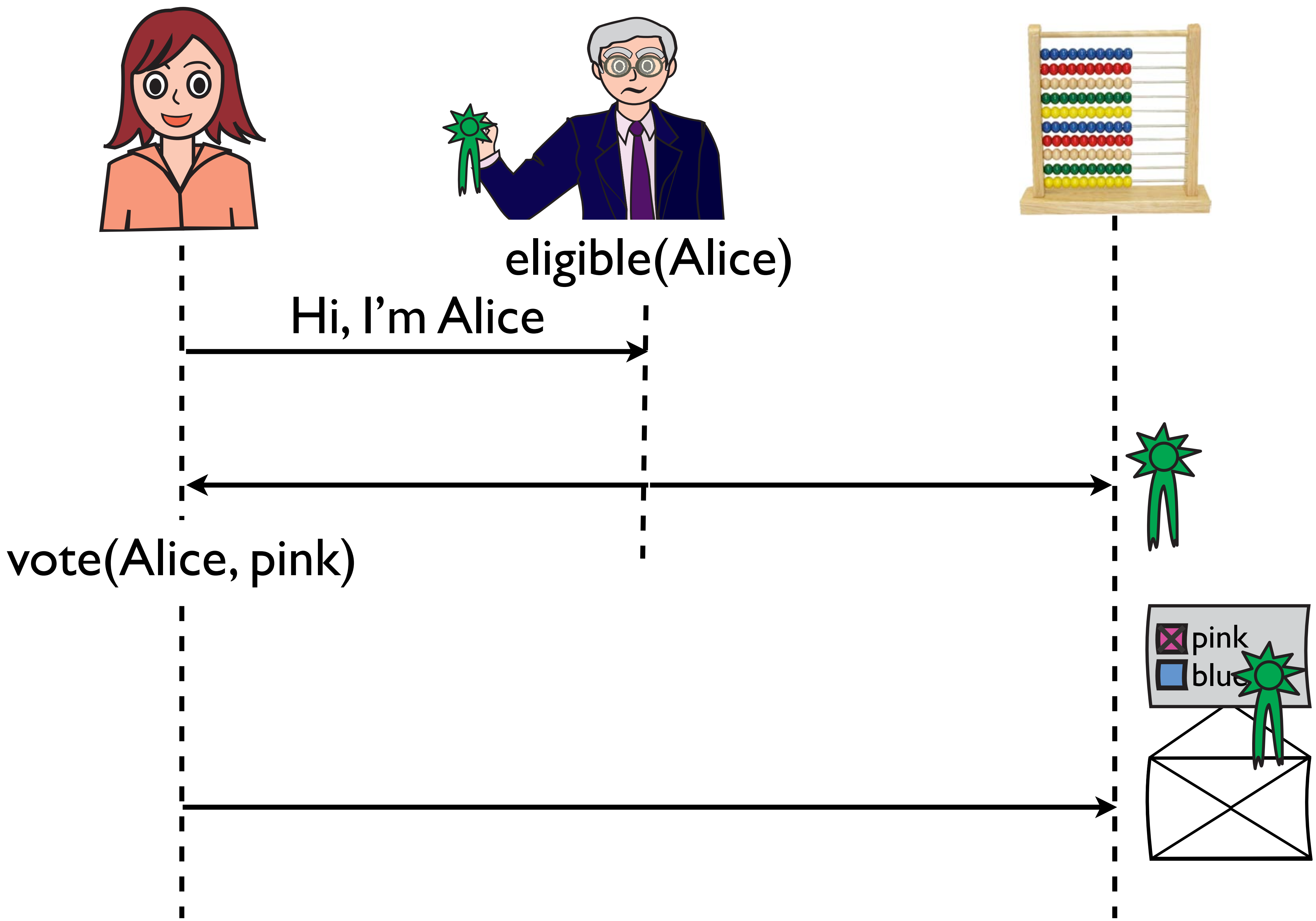
Soundness (eligibility, non-reusability, inalterability)



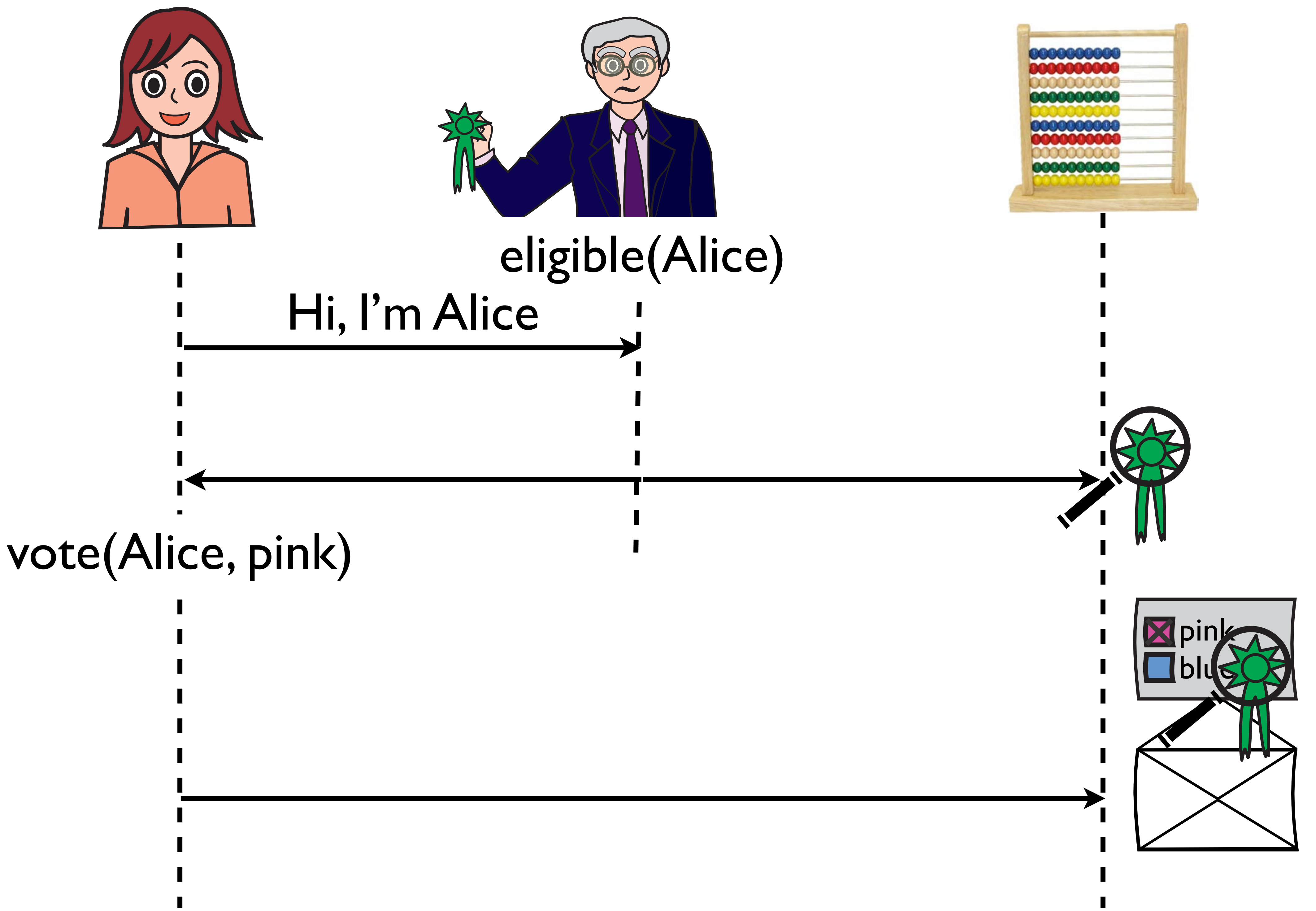
Soundness (eligibility, non-reusability, inalterability)



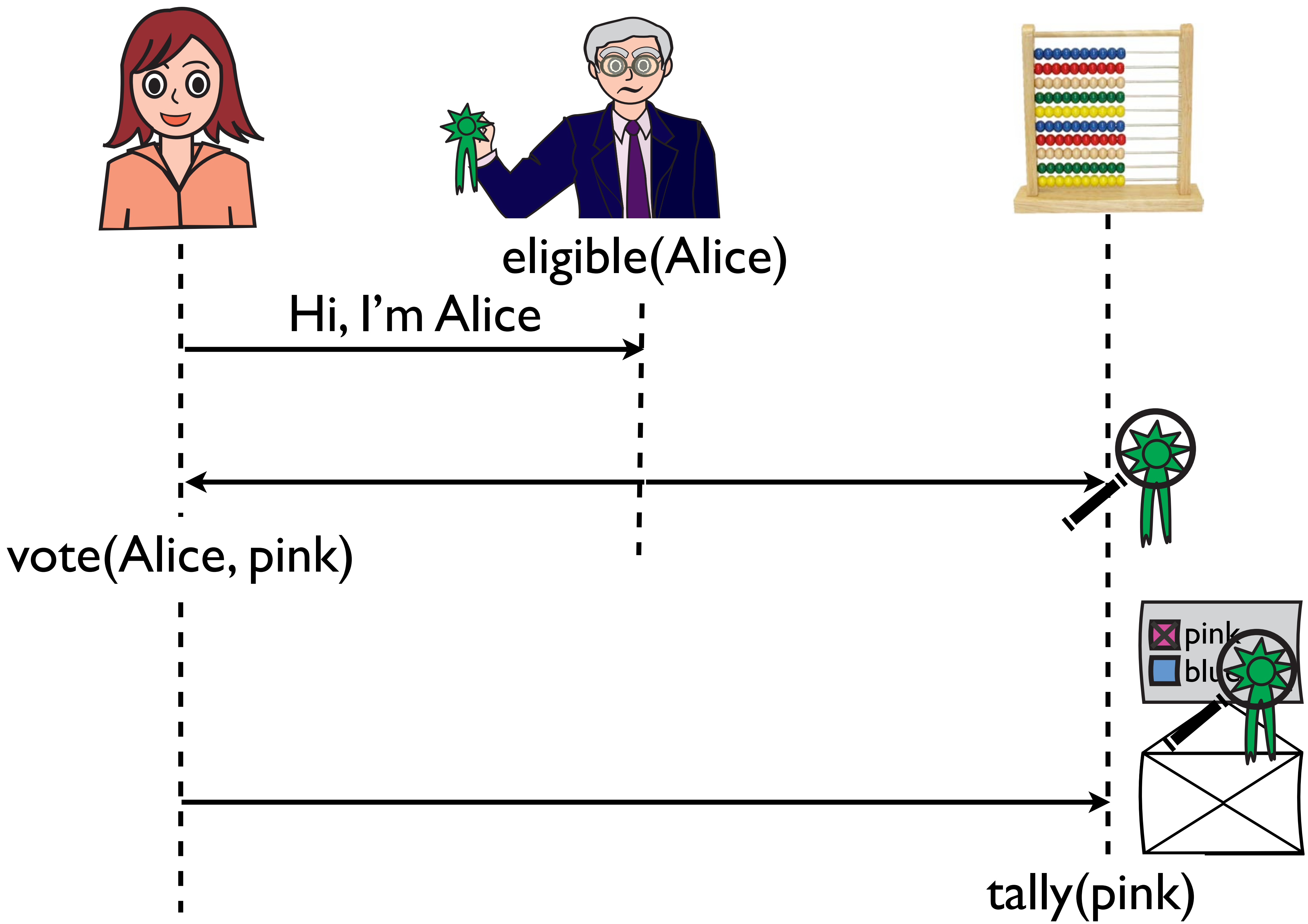
Soundness (eligibility, non-reusability, inalterability)



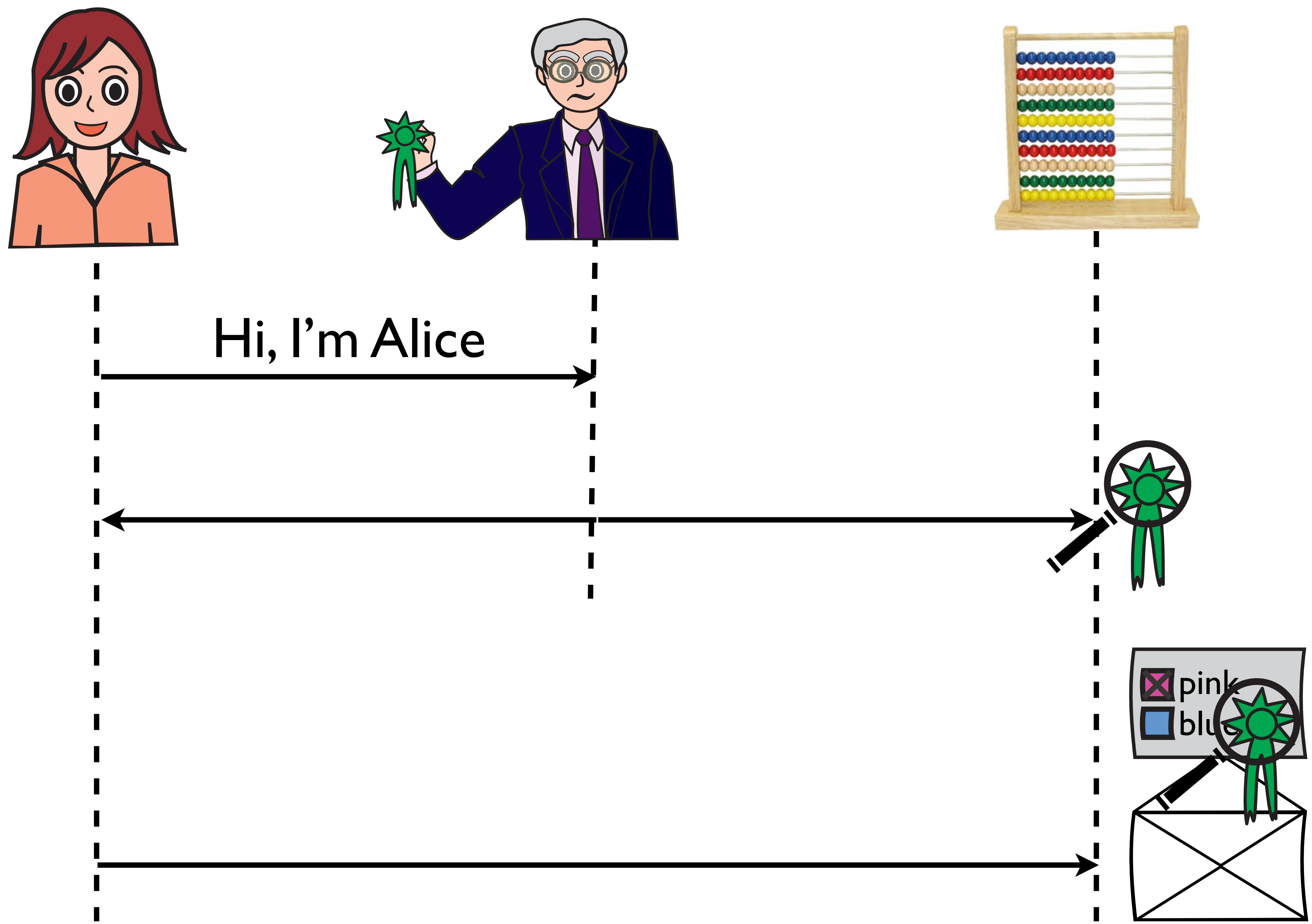
Soundness (eligibility, non-reusability, inalterability)



Soundness (eligibility, non-reusability, inalterability)

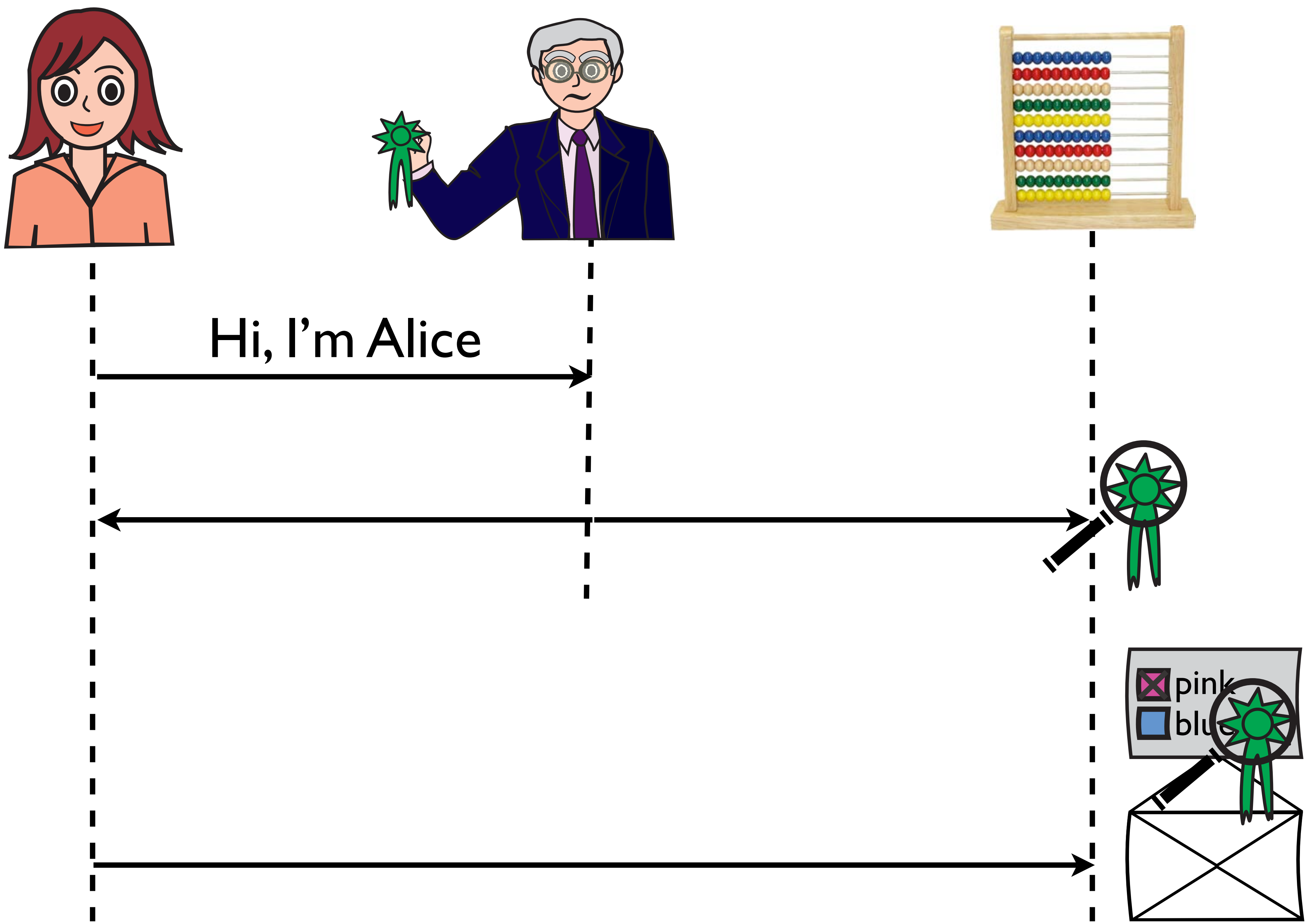


Soundness (eligibility, non-reusability, inalterability)



Trace: t_1 eligible(Alice) t_2 vote(Alice, pink) t_3 tally(pink)

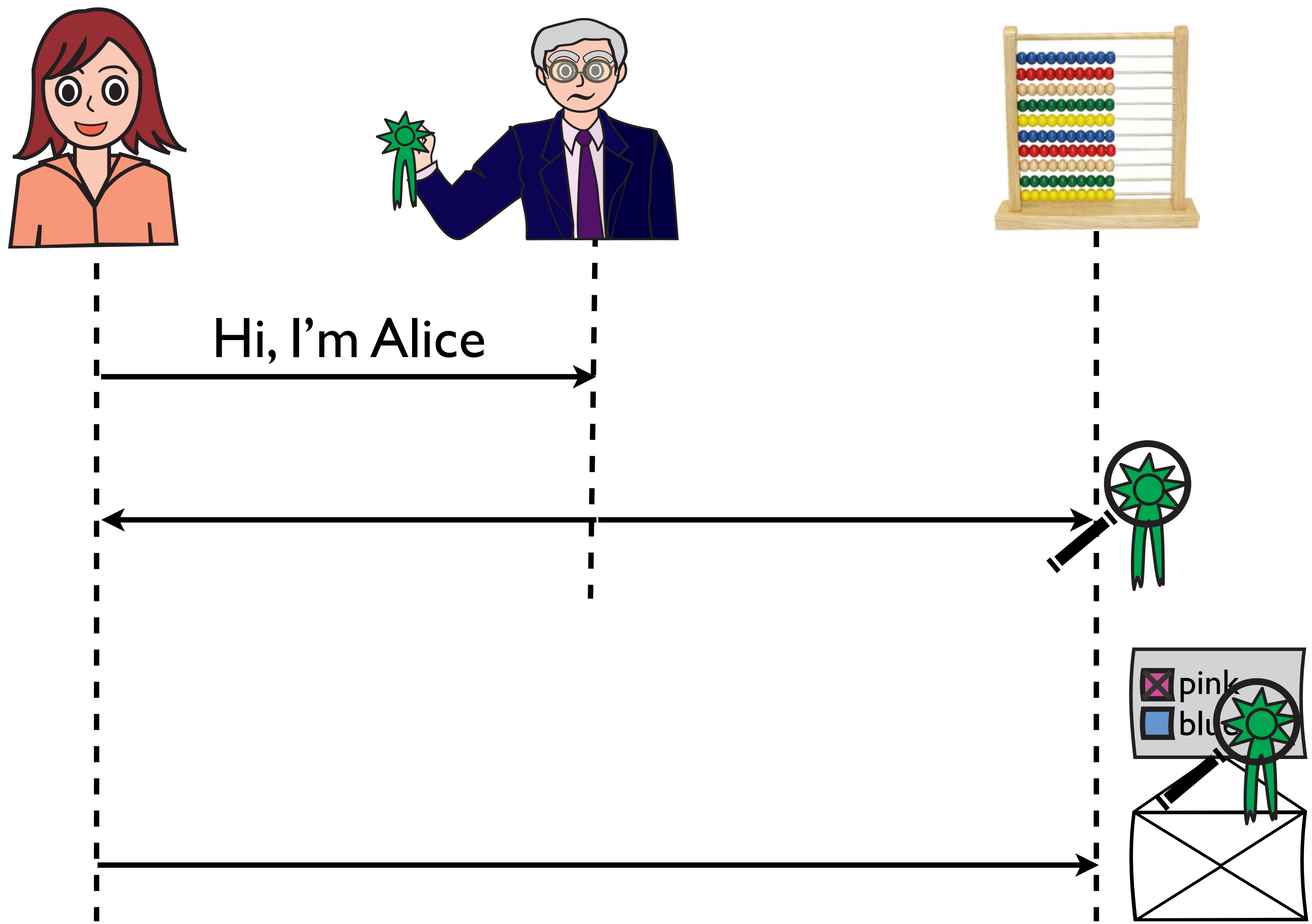
Soundness (eligibility, non-reusability, inalterability)



Trace: t_1 eligible(Alice) t_2 vote(Alice, pink) t_3 tally(pink)

$\exists \longleftarrow \exists \Longleftarrow \forall$

Soundness (eligibility, non-reusability, inalterability)

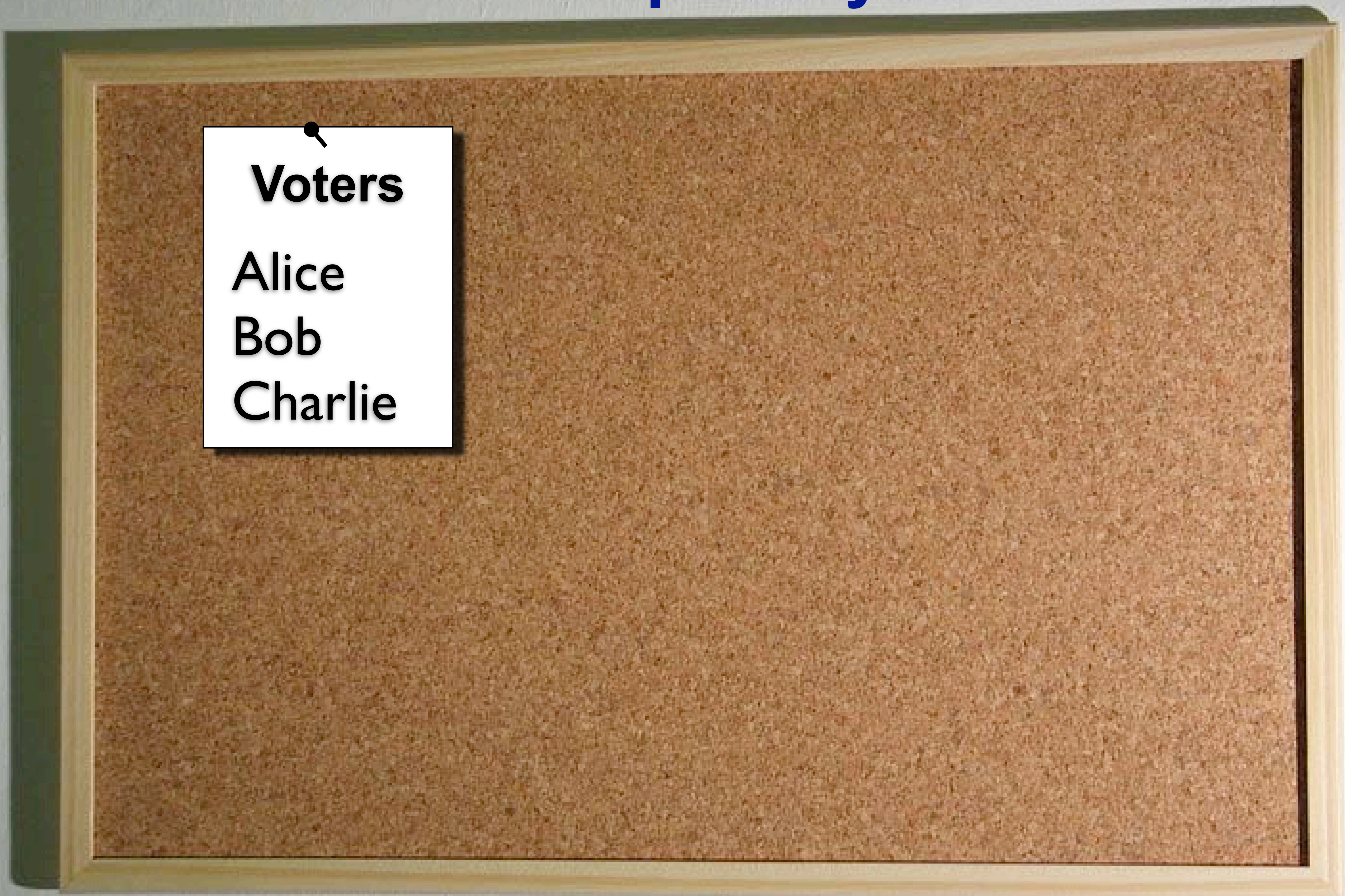


Trace: t_1 eligible(Alice) t_2 vote(Alice, pink) t_3 tally(pink)

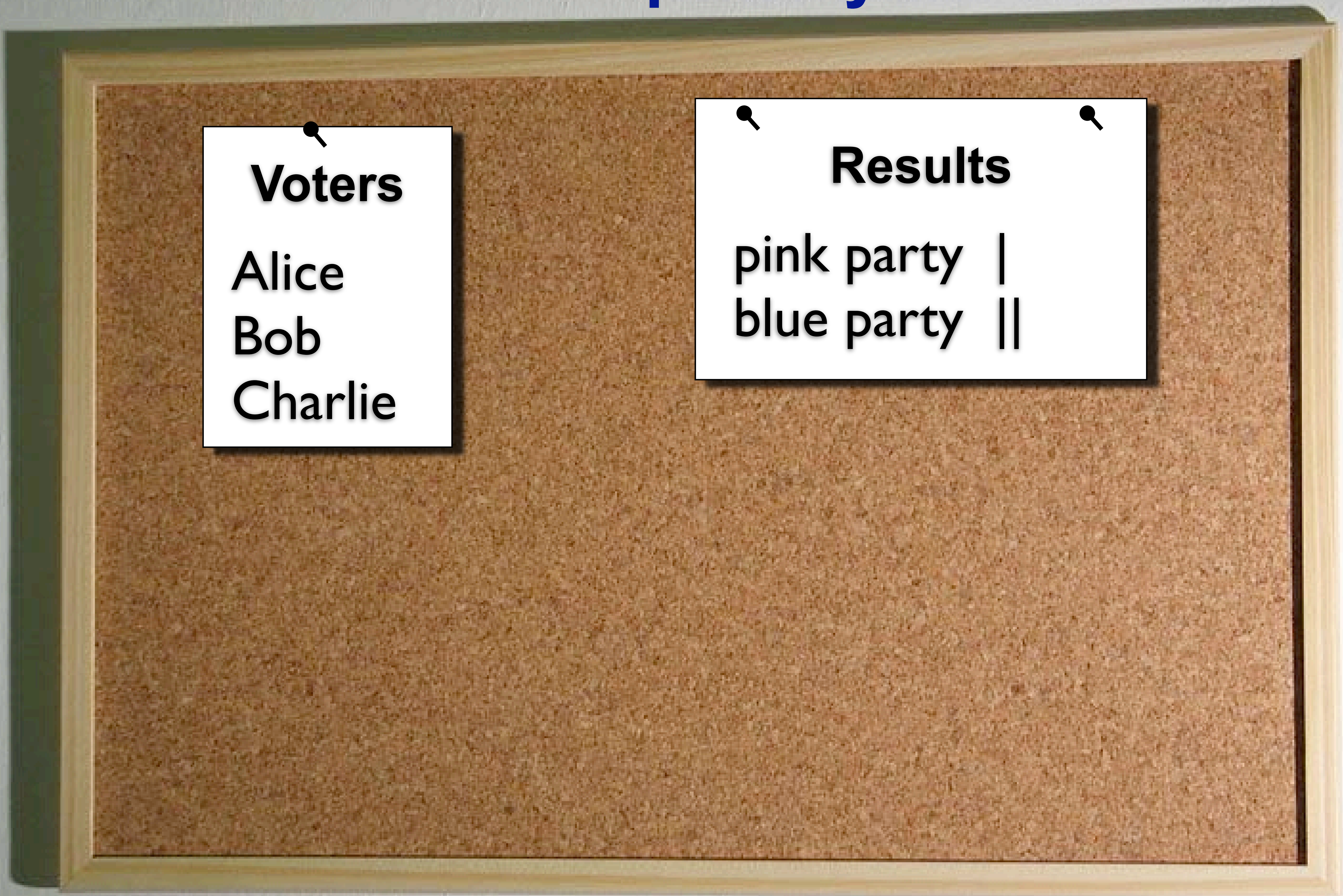
$\exists \longleftarrow \exists \Longleftarrow \forall$

and the trace t_1 t_2 t_3 is also sound (injective matching)

Vote-privacy



Vote-privacy



Vote-privacy

Voters

Alice
Bob
Charlie

Results

pink party |
blue party ||

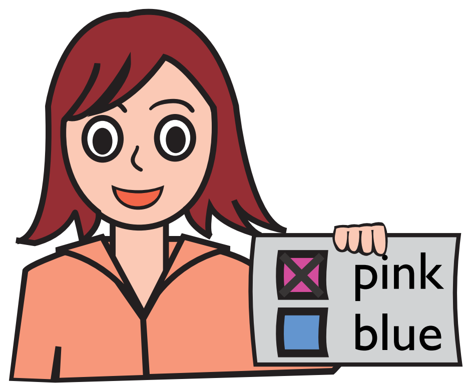
"Detailed" results

Alice .... pink party
Bob .... blue party
Charlie .... blue party

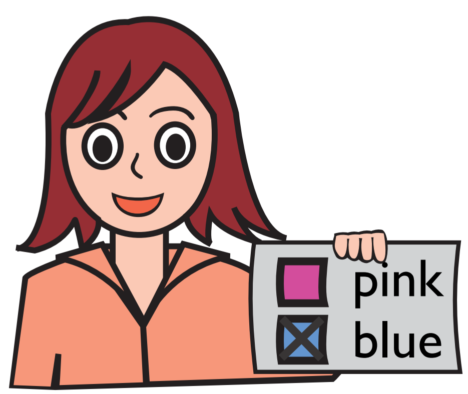
Vote-privacy

Definition of vote-privacy

[Delaune, Kremer & Ryan; CSF '06]

S[

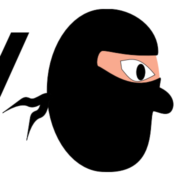
]

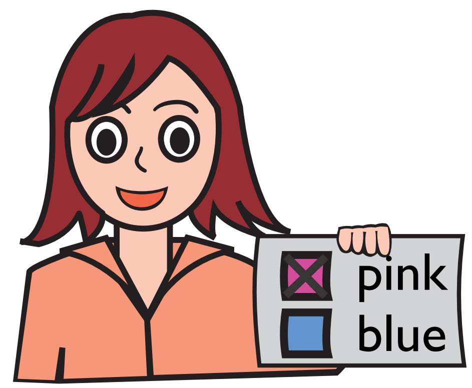
S[

]

Definition of vote-privacy

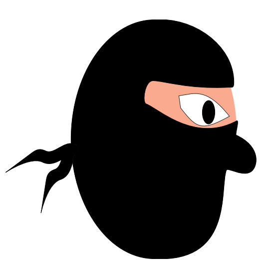
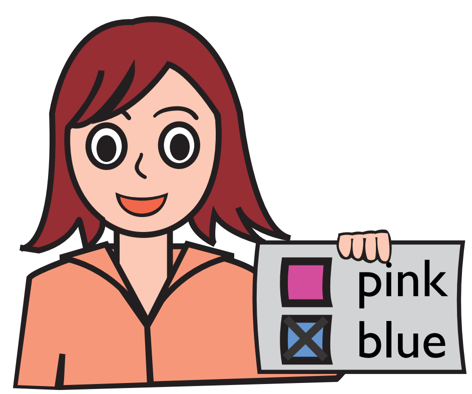
[Delaune, Kremer & Ryan; CSF ’06]

∀ 

 [S[

]]

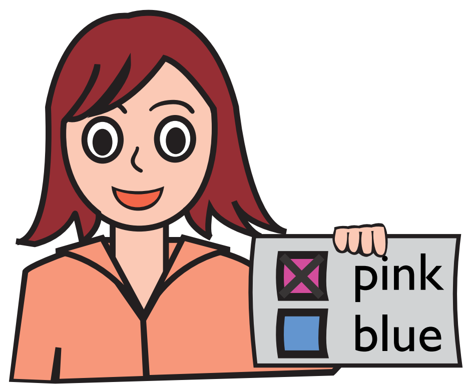
indistinguishable from

 [S[

]]

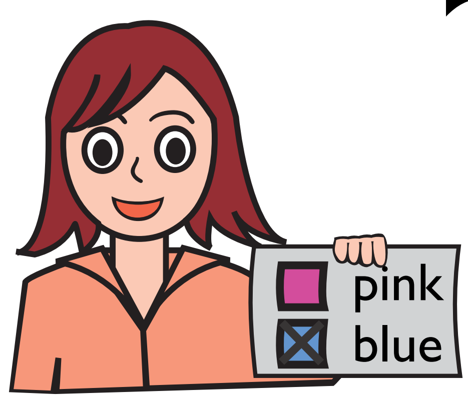
Definition of vote-privacy

[Delaune, Kremer & Ryan; CSF '06]

S[

]

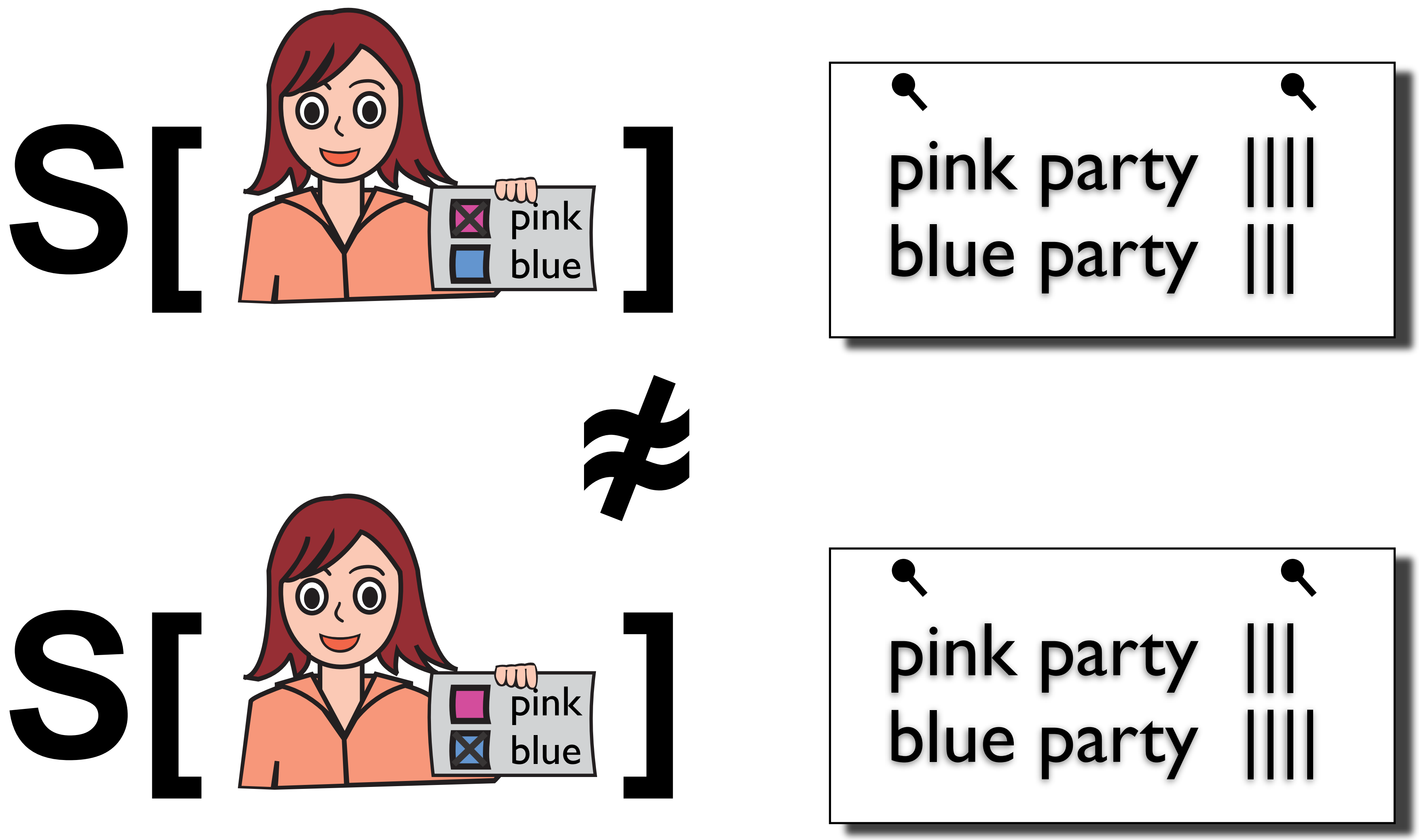
≈

S[

]

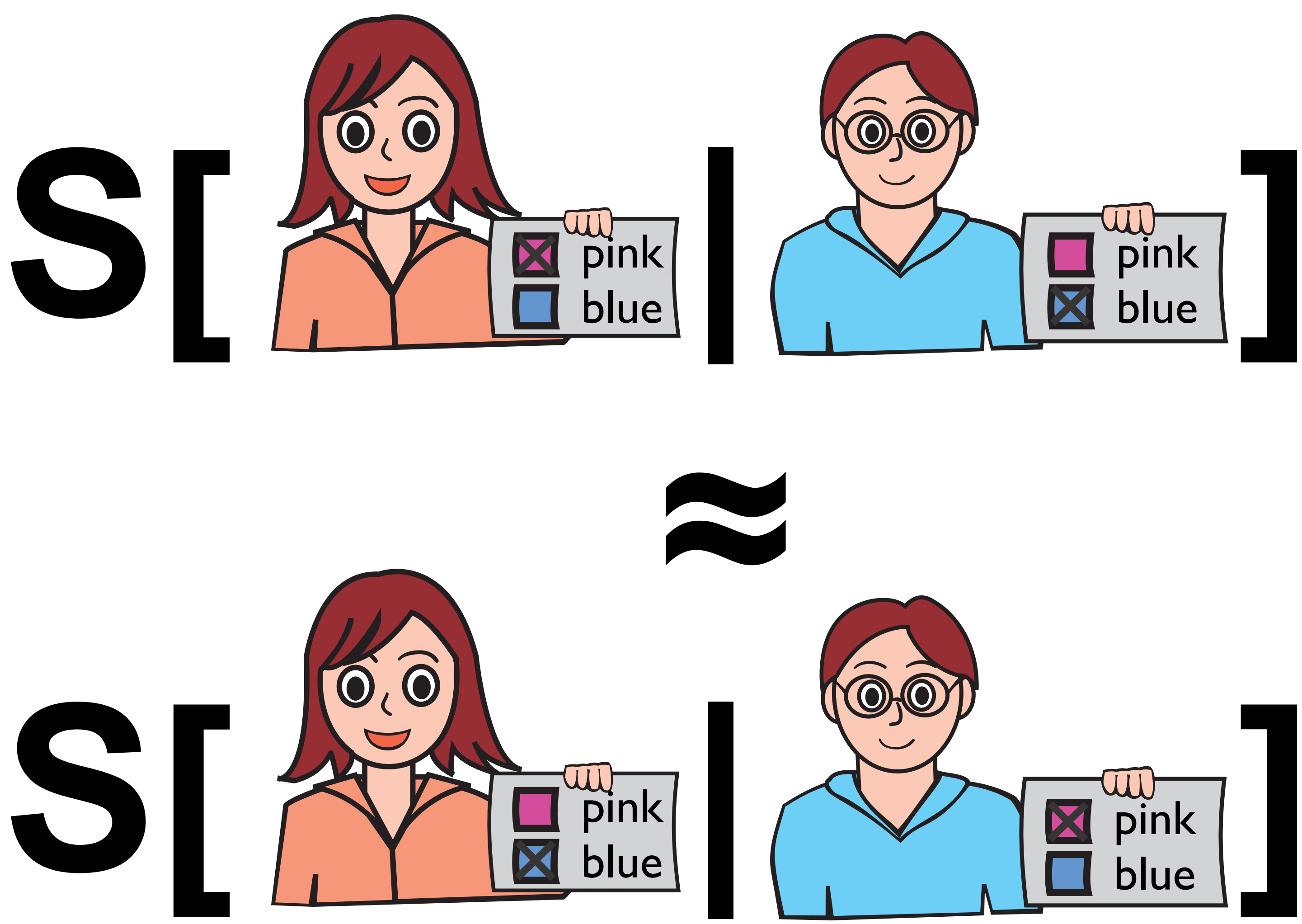
Definition of vote-privacy

[Delaune, Kremer & Ryan; CSF ’06]

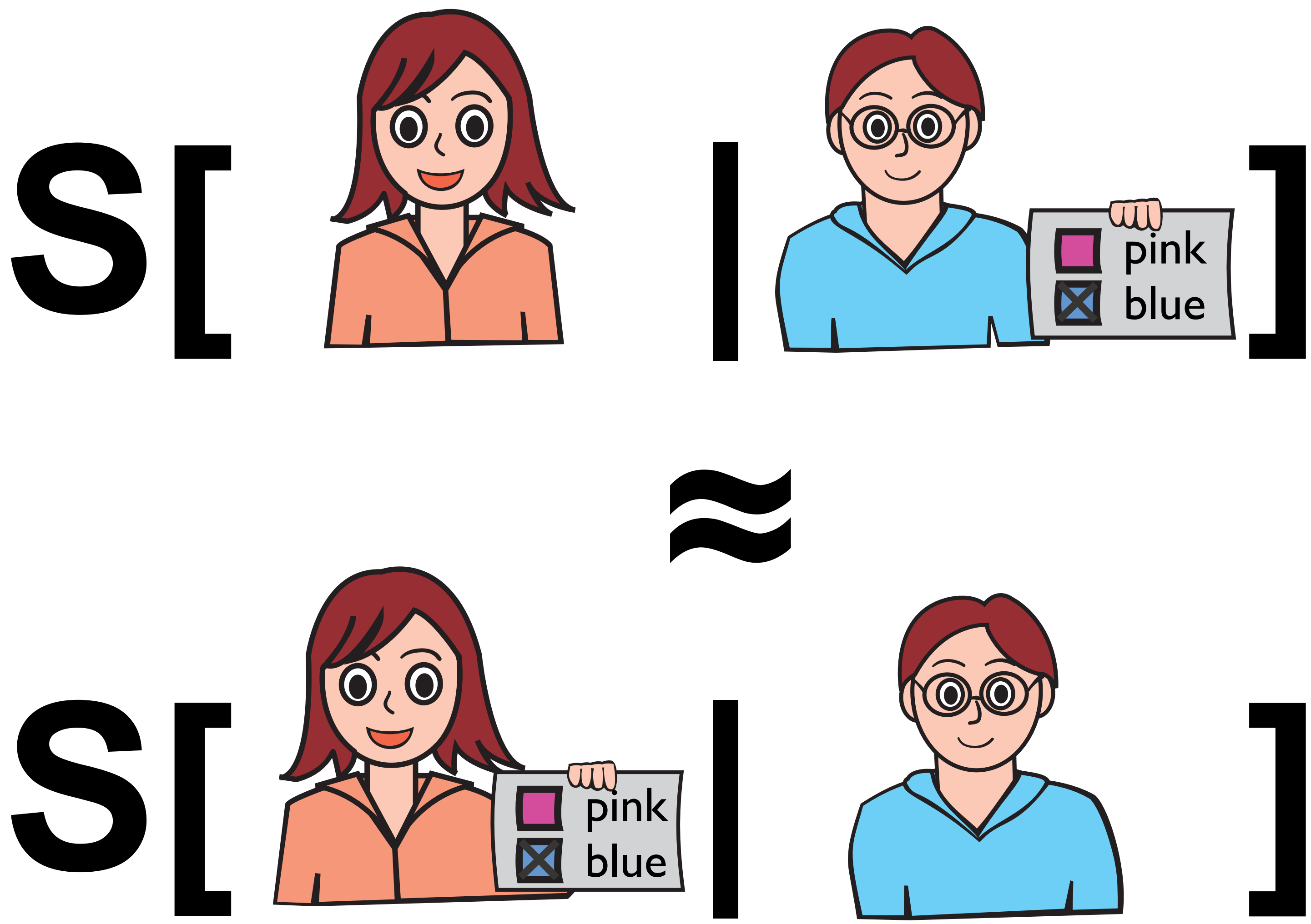


Definition of vote-privacy

[Delaune, Kremer & Ryan; CSF '06]

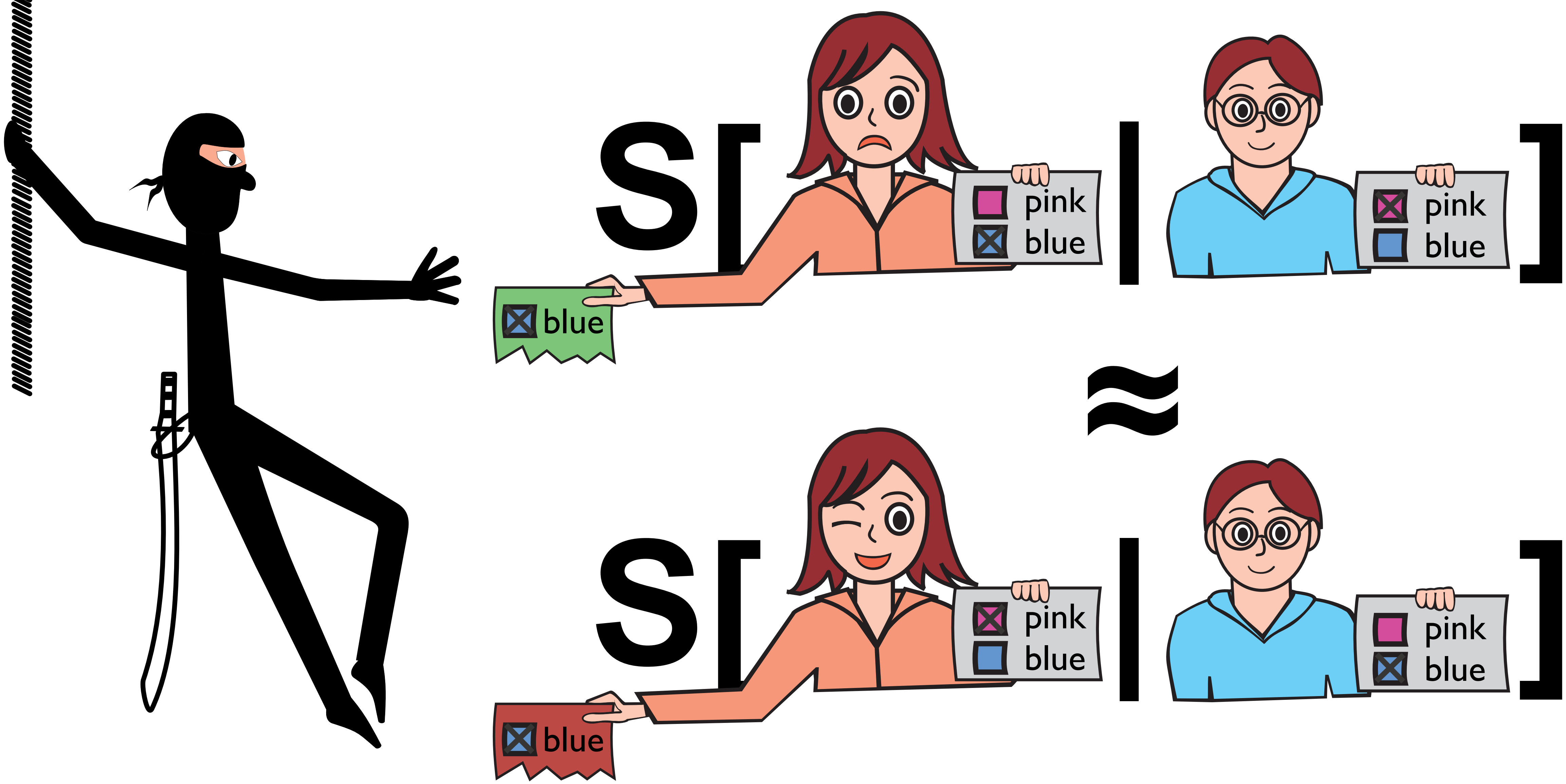


Immunity to forced-abstention



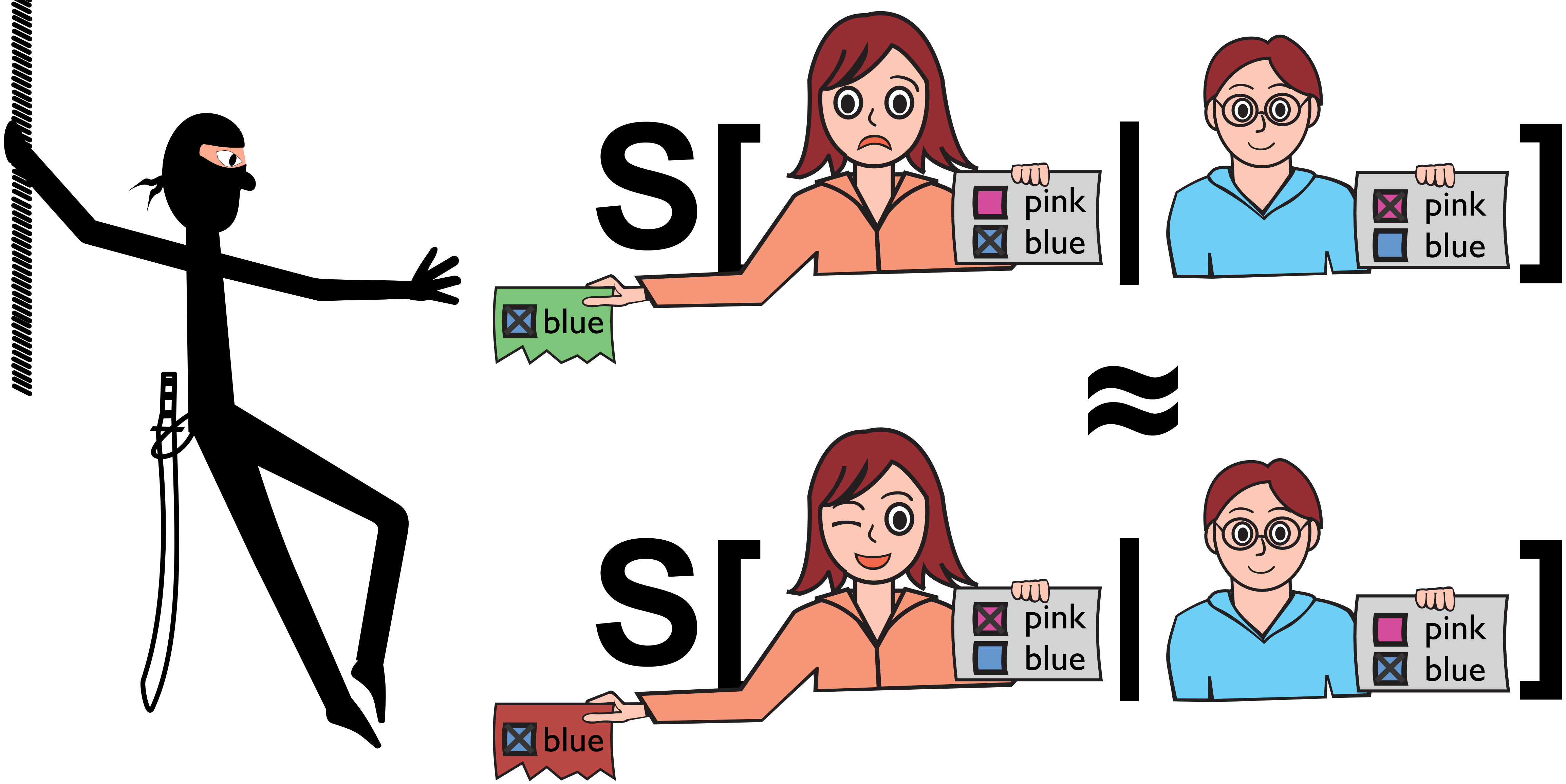
Receipt-freeness

- Cryptographic setting [Benaloh & Tuinstra; STOC '94]



Receipt-freeness

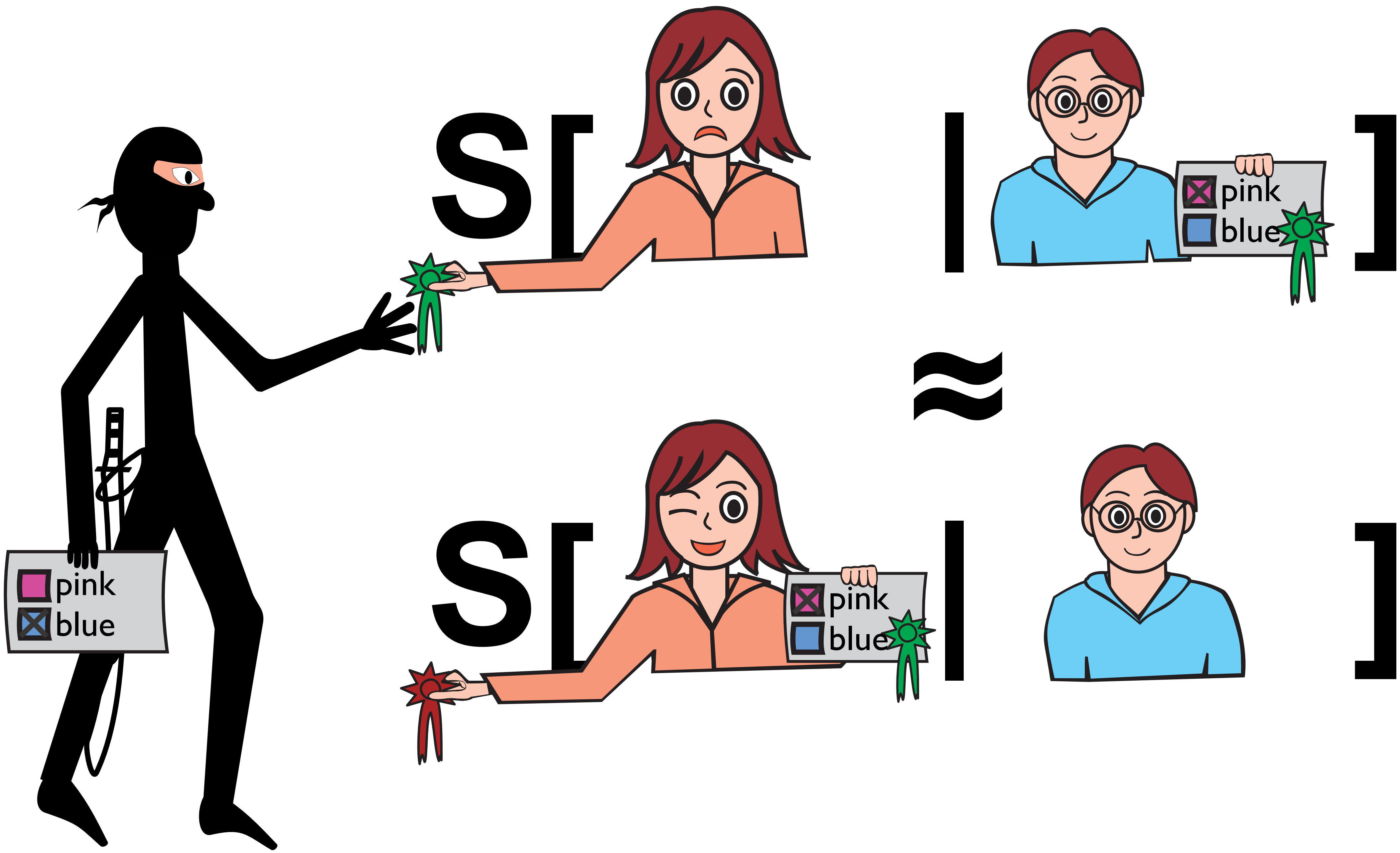
- Cryptographic setting [Benaloh & Tuinstra; STOC '94]



- We adapted definition by [Delaune, Kremer & Ryan; CSF '06] to **remote voting**

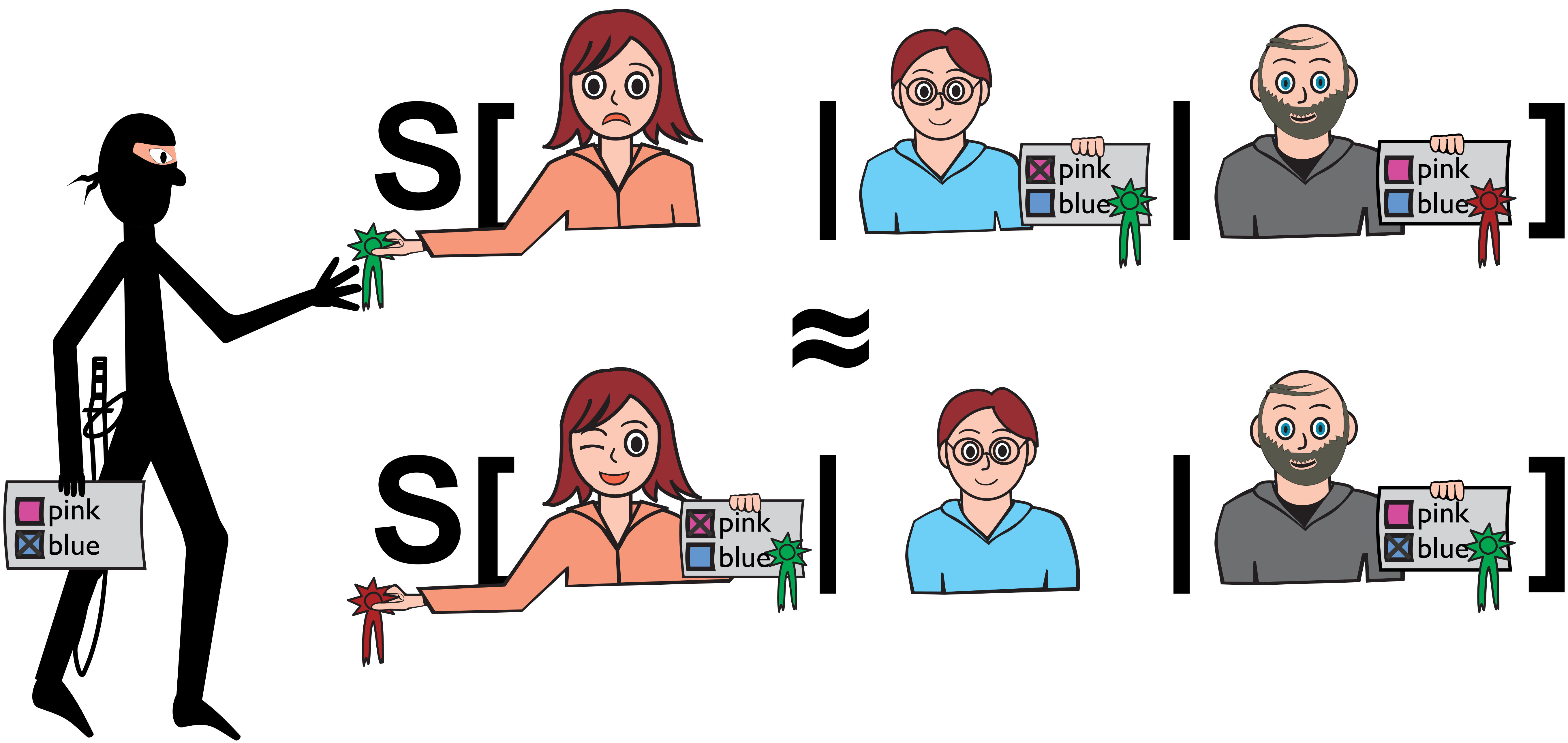
Coercion-resistance

- Cryptographic setting [Juels, Catalano & Jakobsson; WPES 2005]



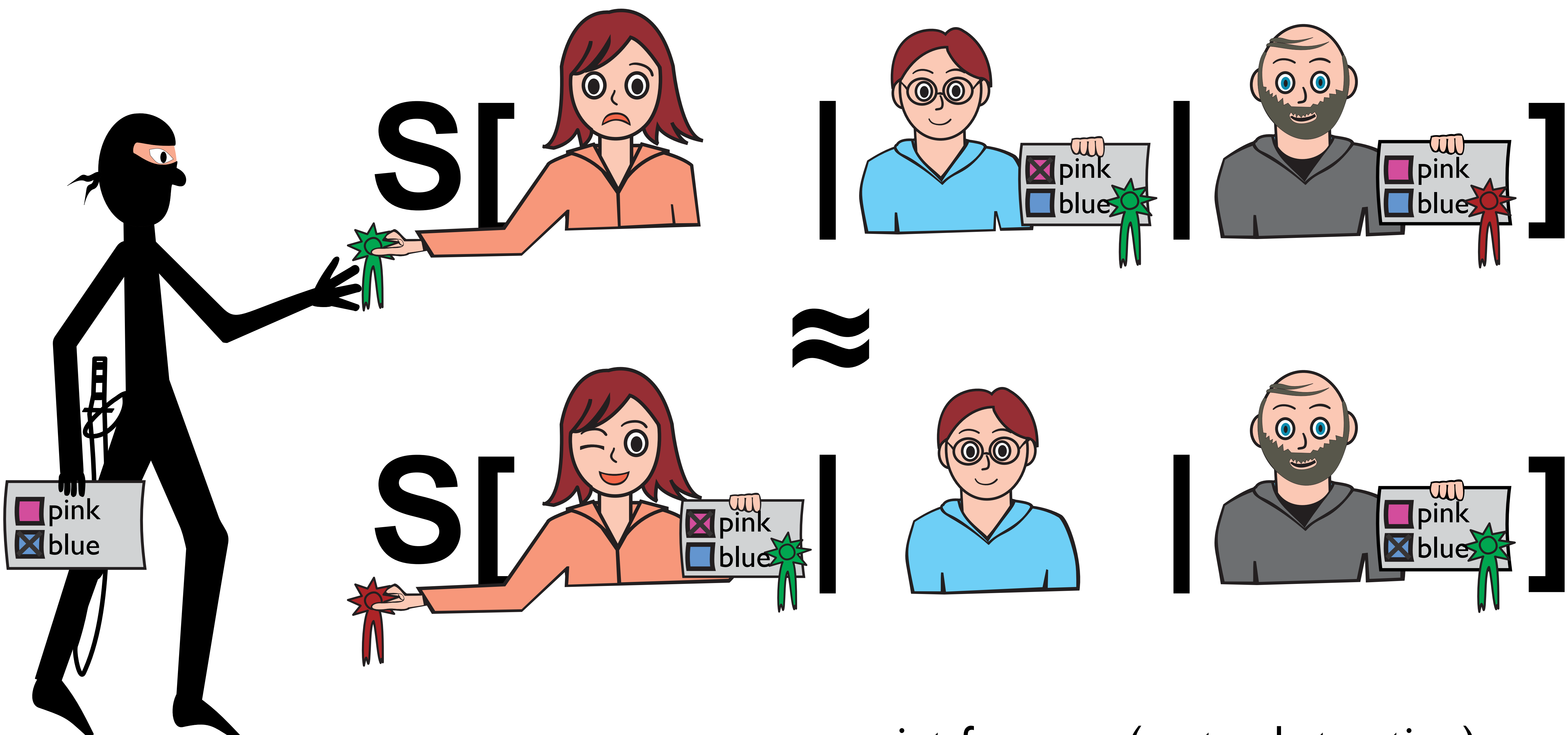
Coercion-resistance

- Cryptographic setting [Juels, Catalano & Jakobsson; WPES 2005]



Coercion-resistance

- Cryptographic setting [Juels, Catalano & Jakobsson; WPES 2005]



- Proved: coercion-resistance ⇒ no forced-abstention ⇒ vote-privacy

  ⇗ receipt-freeness (up to abstraction)

Definitions of coercion-resistance

	JCJ-WPES'05	DKR-CSF'06	DKR-TR'08	current
setting	remote voting	supervised voting	supervised voting	remote voting
automation	no (crypto)	no (adaptive simulation)	no ($\forall C.\ P \approx Q$)	yes ($\approx$)
vote-privacy	yes	yes	yes	yes
no simulation attacks	yes	n/a	n/a	yes
no forced-abstention	yes	no	no	yes
no randomization attacks (?)	yes (claimed not proved)	no	no	no
receipt-freeness	yes	yes	yes	yes (up to abstraction)

Analysis of JCJ

- first coercion-resistant protocol for remote voting [Juels, Catalano & Jakobsson; WPES '05]
- forms the basis of many recent protocols (e.g. Civitas [Clarkson, Chong & Myers; S&P '08])
- Analysis performed with ProVerif [Blanchet et. al.]
  - automatic protocol analyzer using Horn-clause resolution
  - we use our symbolic abstraction of zero-knowledge [Backes, Maffei & Unruh; S&P '08]
  - analyzing observational equivalence required (re)writing the specification in the shape of a biprocess
  - verification of JCJ succeeds, which yields security guarantees for unbounded number of voters, sessions, etc.

Current and Future work

- Currently analyzing a model of Civitas

Current and Future work

- Currently analyzing a model of Civitas
- Defining and analyzing other properties
  - Individual verifiability (trace property)
  - Immunity to randomization attacks (privacy property)

Current and Future work

- Currently analyzing a model of Civitas
- Defining and analyzing other properties
  - Individual verifiability (trace property)
  - Immunity to randomization attacks (privacy property)
- Using type systems for trace properties
  - e.g. type system for ZK [CCS '08] [Fournet et. al., CSF '07]

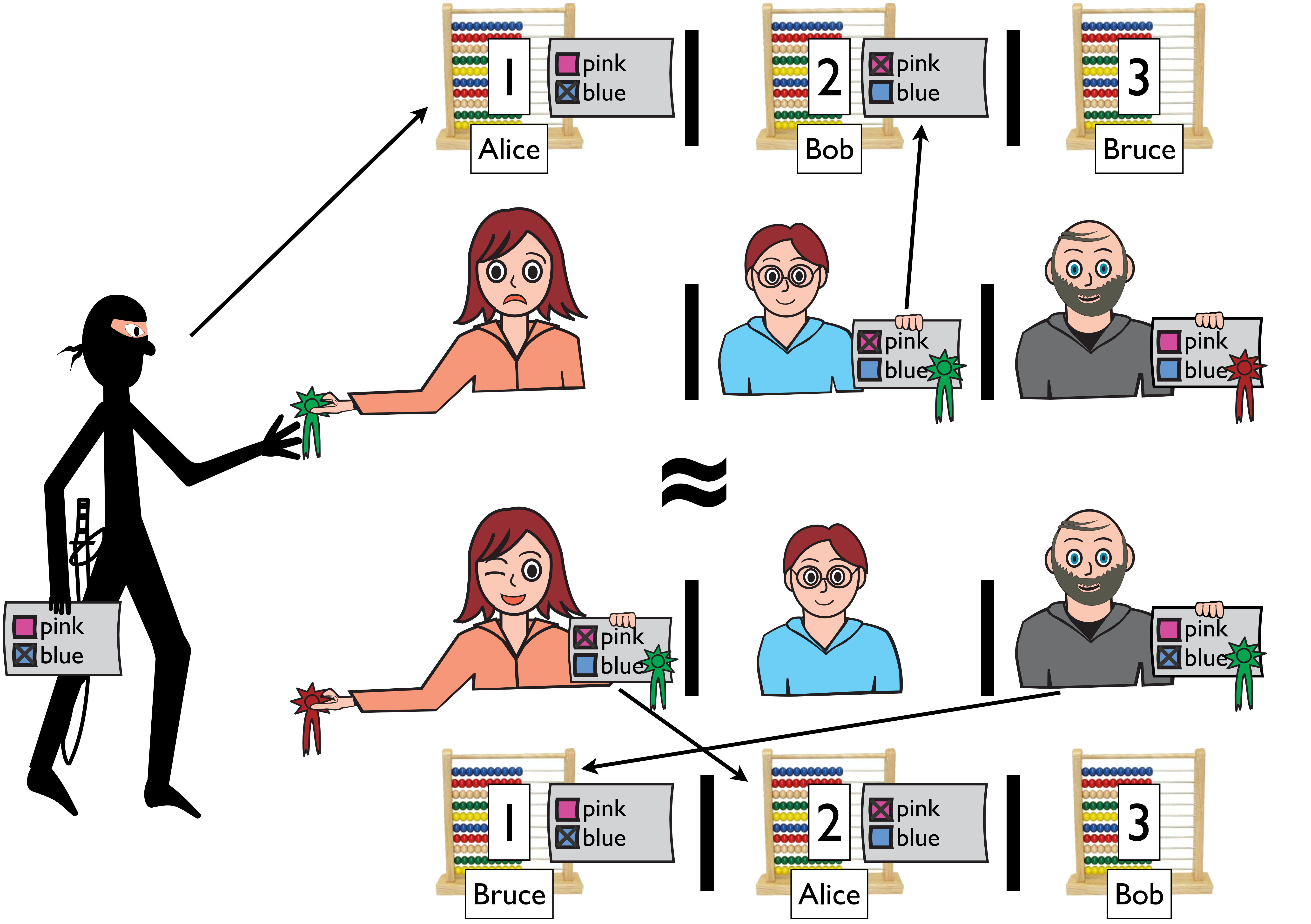
Current and Future work

- Currently analyzing a model of Civitas
- Defining and analyzing other properties
  - Individual verifiability (trace property)
  - Immunity to randomization attacks (privacy property)
- Using type systems for trace properties
  - e.g. type system for ZK [CCS '08] [Fournet et. al., CSF '07]
- Different techniques for observational equivalence
  - for instance using symbolic bisimulation [DKR, SecCo '07]

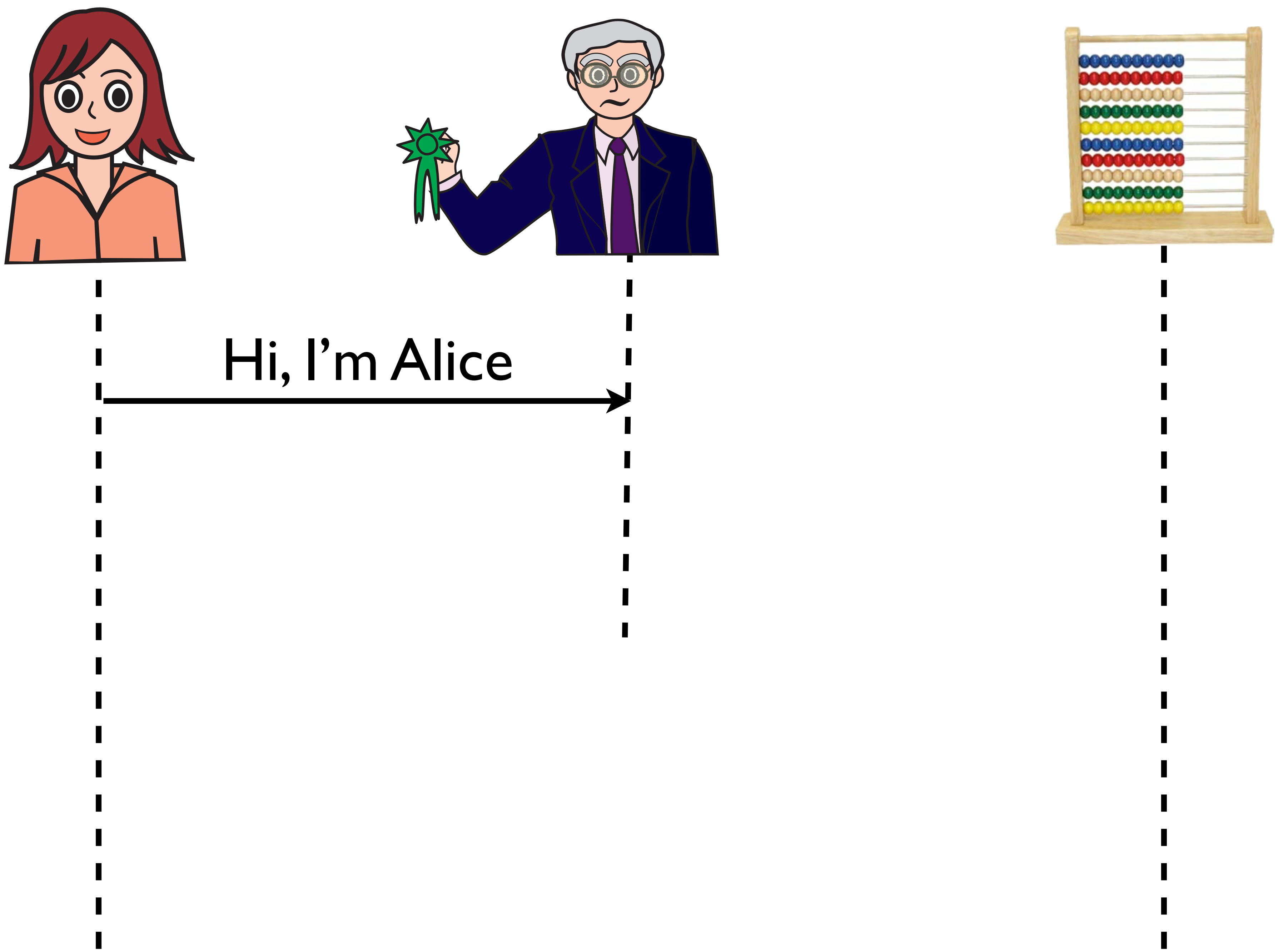
Current and Future work

- Currently analyzing a model of Civitas
- Defining and analyzing other properties
  - Individual verifiability (trace property)
  - Immunity to randomization attacks (privacy property)
- Using type systems for trace properties
  - e.g. type system for ZK [CCS ’08] [Fournet et. al., CSF ’07]
- Different techniques for observational equivalence
  - for instance using symbolic bisimulation [DKR, SecCo ’07]
- More accurate protocol models
  - The ultimate goal is to analyze implementations

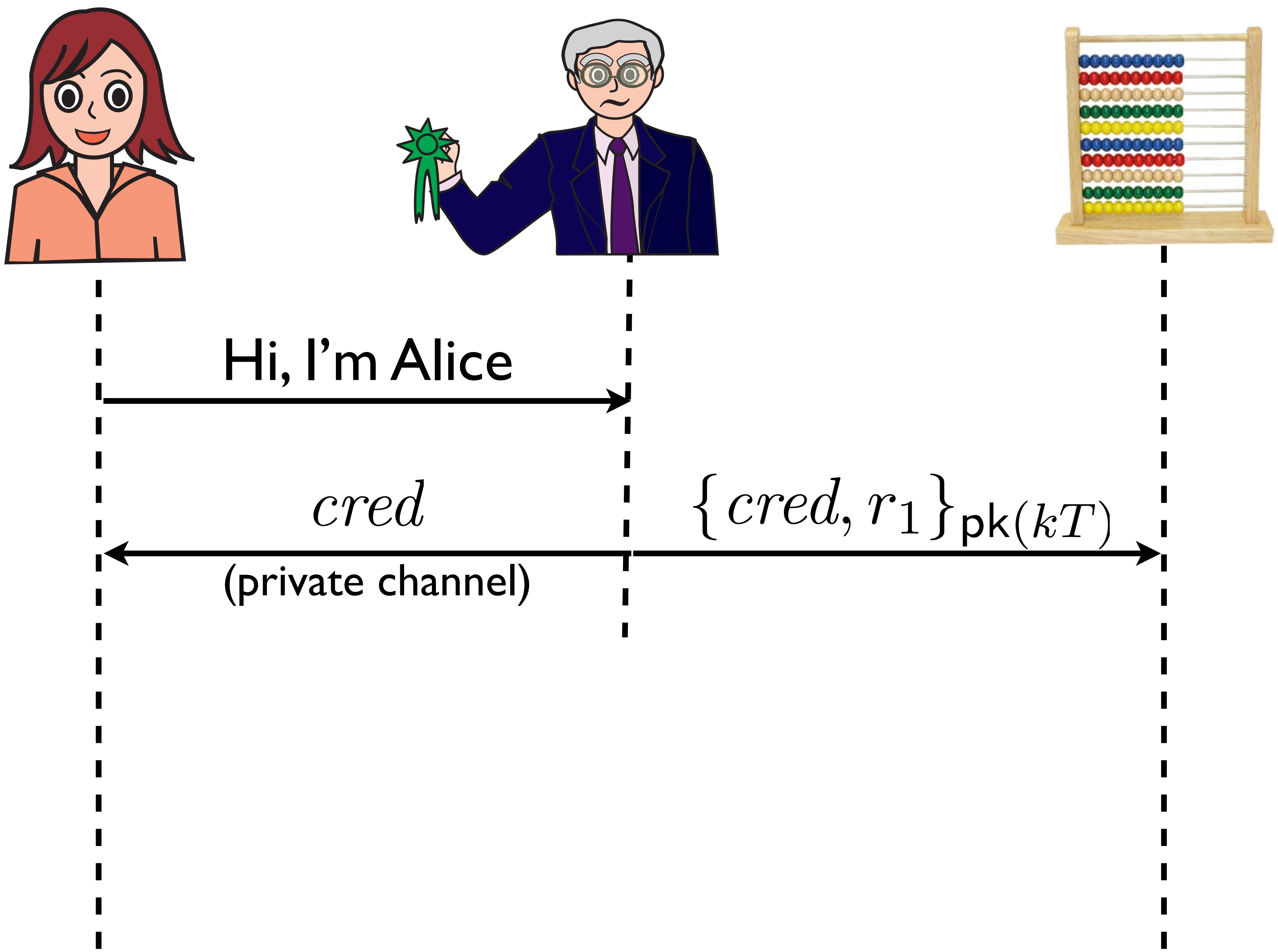
Backup slides


1
pink
blue
Alice
2
pink
blue
Bob
3
Bruce
pink
blue
pink
blue
pink
blue
≈
pink
blue
pink
blue
pink
blue
1
pink
blue
Bruce
2
pink
blue
Alice
3
Bob

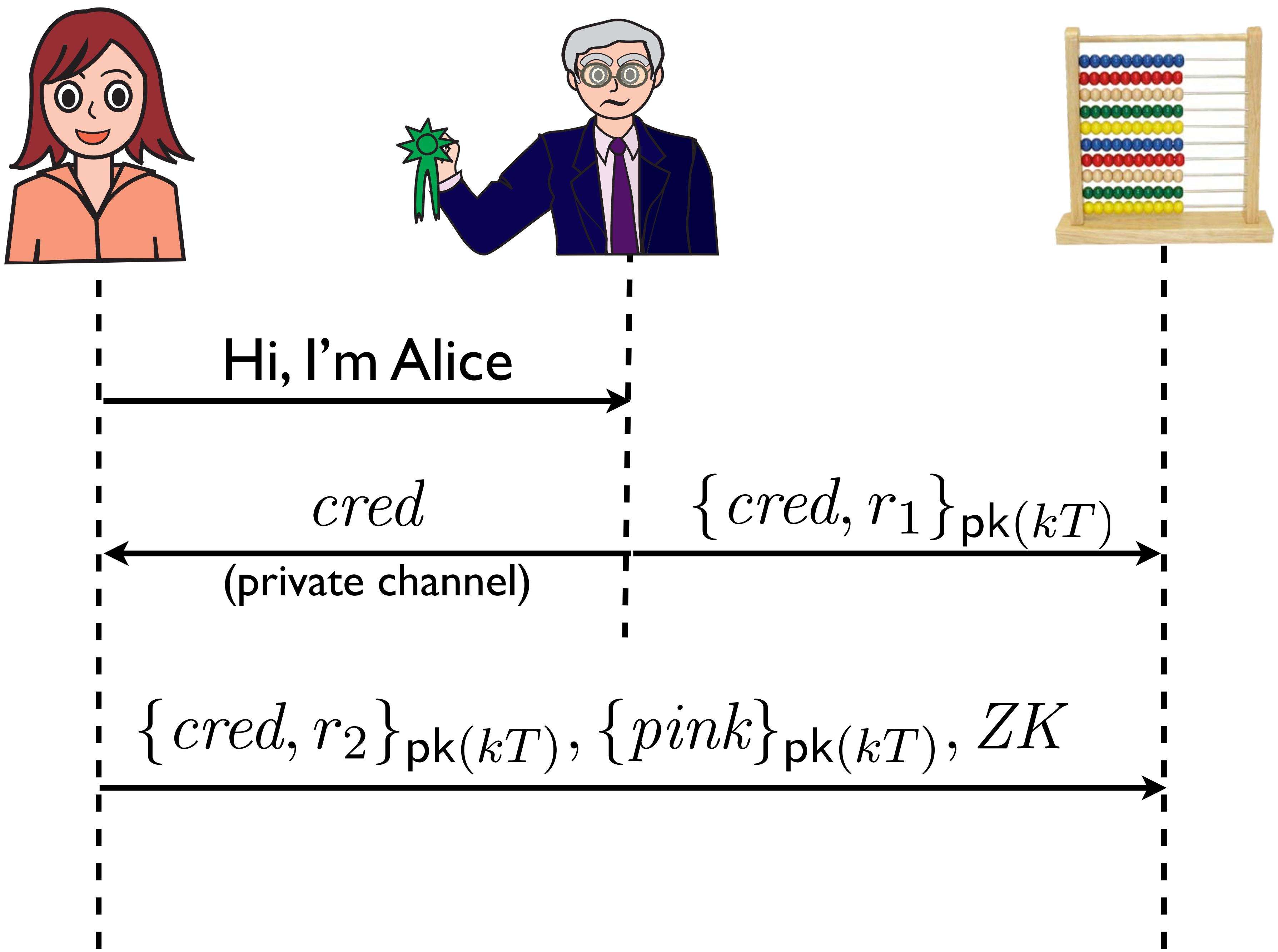
Simplified JCJ protocol



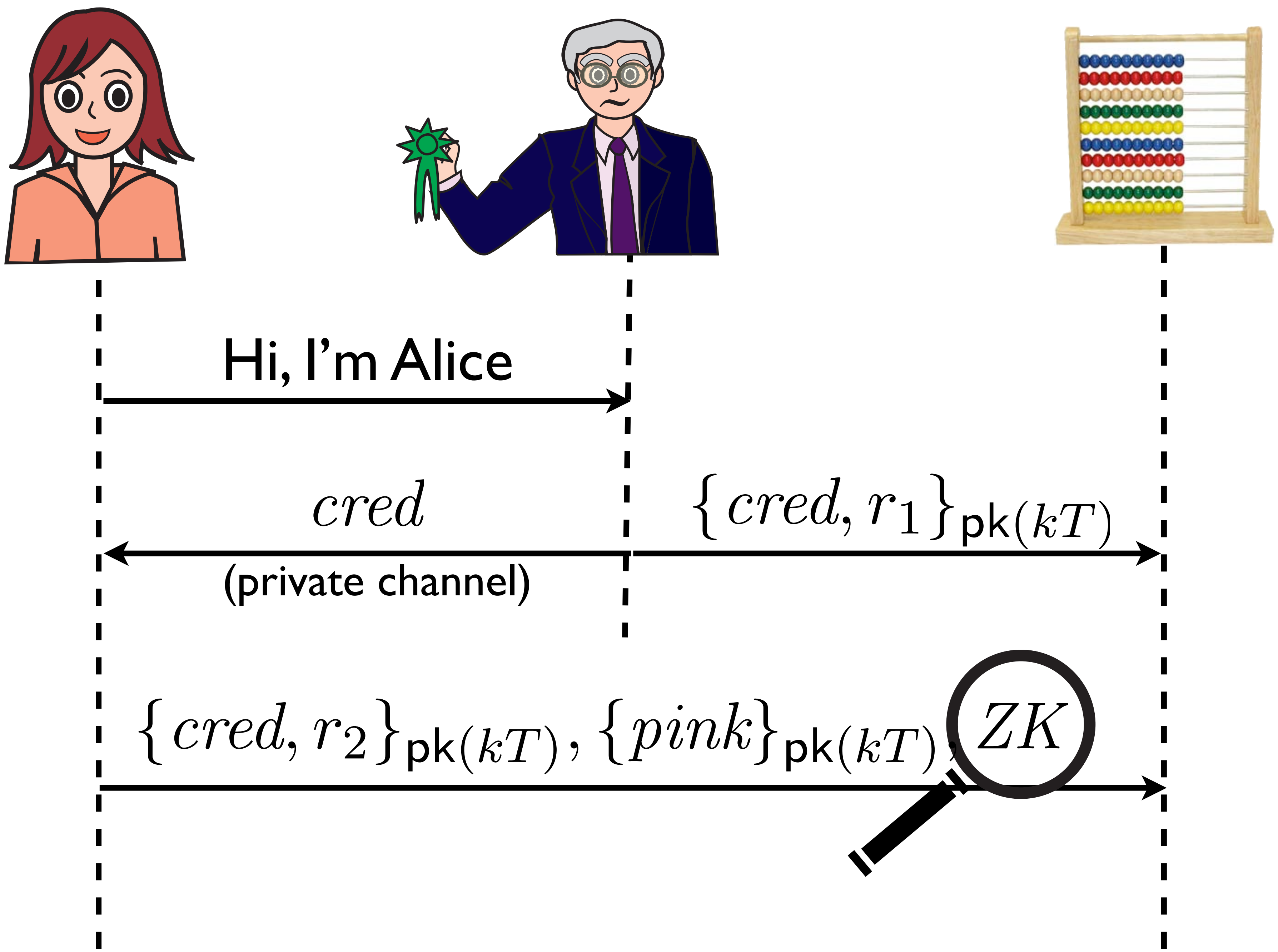
Simplified JCJ protocol



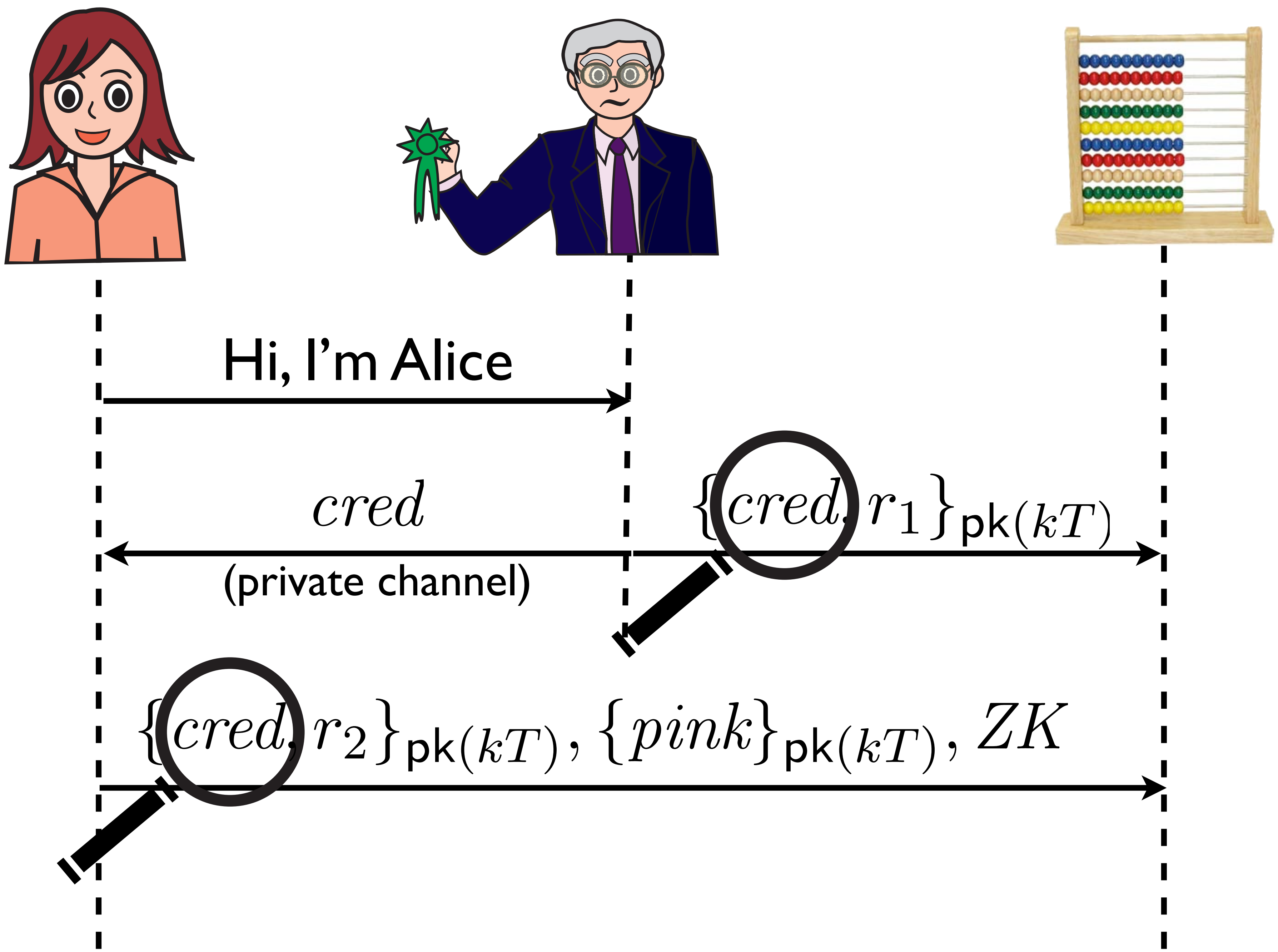
Simplified JCJ protocol



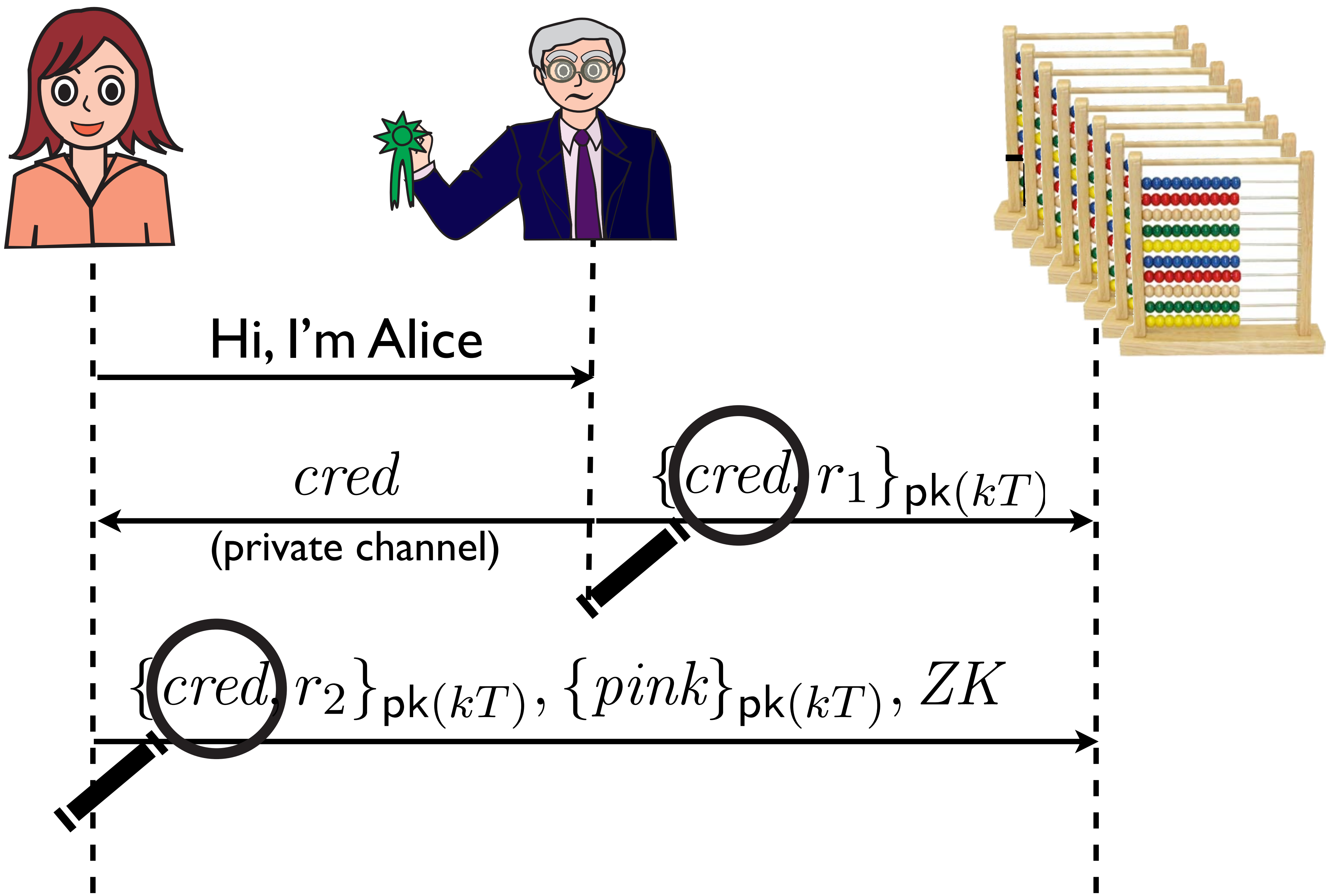
Simplified JCJ protocol



Simplified JCJ protocol



Simplified JCJ protocol



Simplified JCJ protocol