IS&C

UNIVERSITÄT DES SAARLANDES

Automatic Verification of Remote Electronic Voting Protocols

Michael Backes, Cătălin Hriţcu, Matteo Maffei

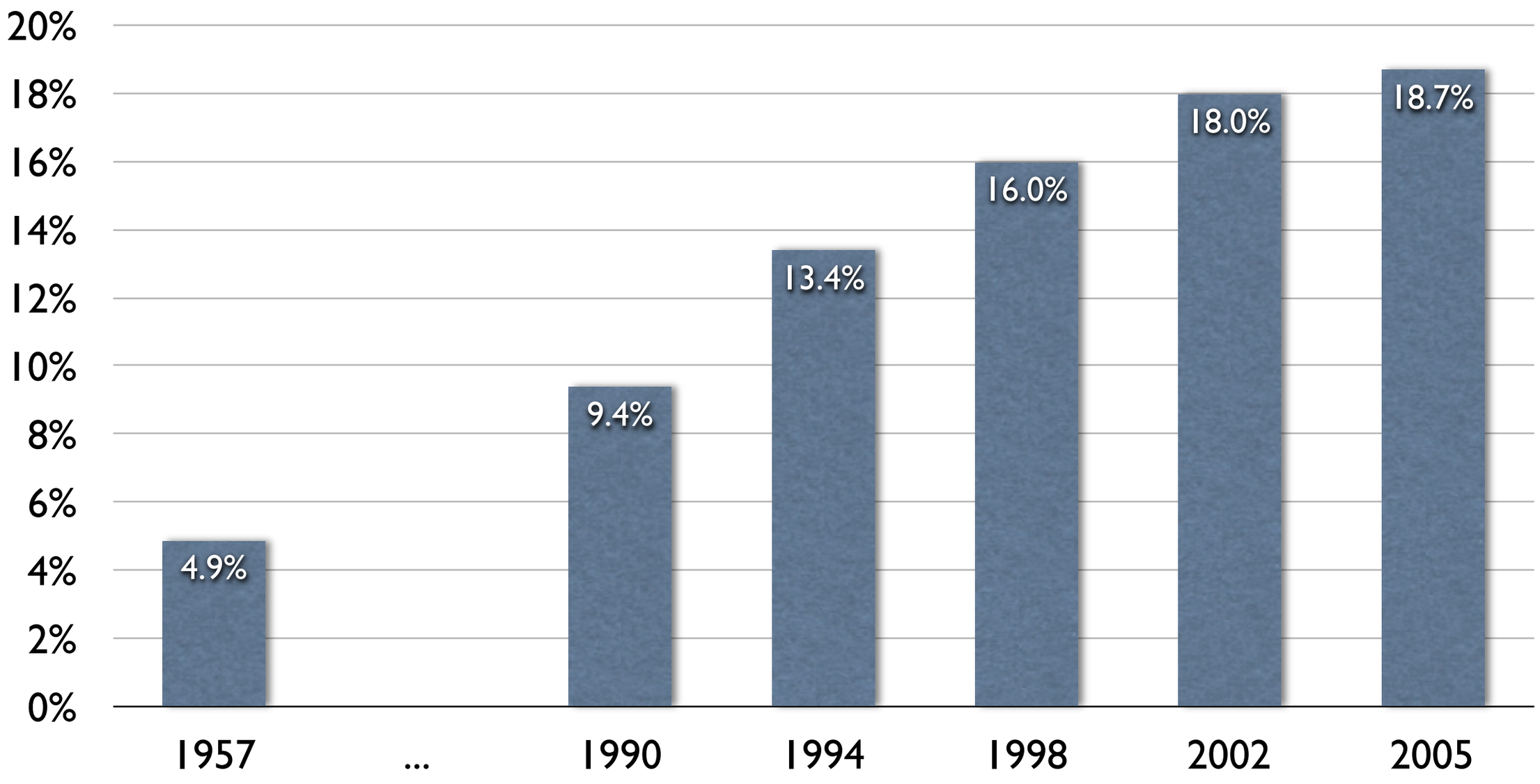
Information Security & Cryptography Group

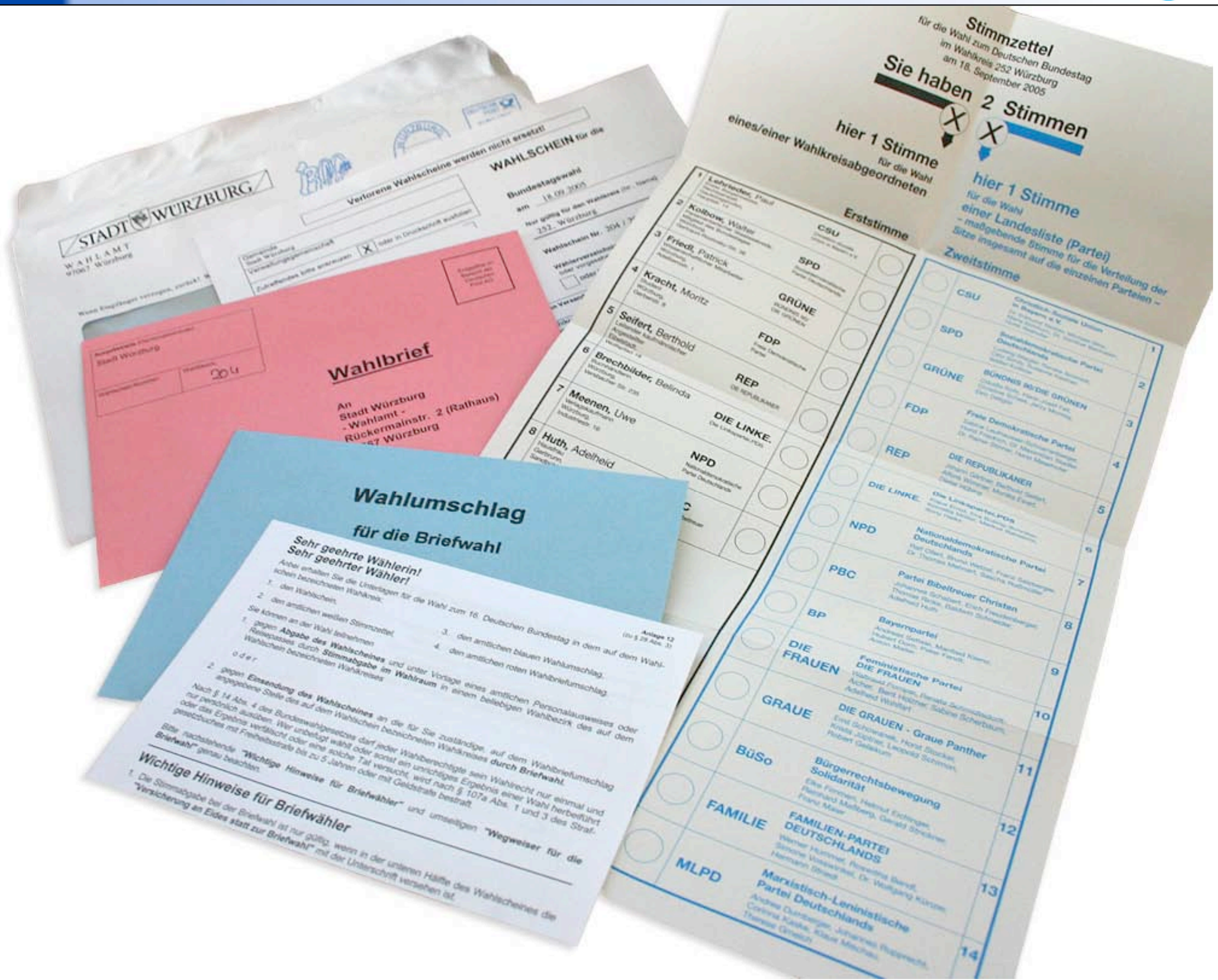
Colloquium of the GK and IMPRS, Saarbrücken, June 2008

The Big Picture

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**




STADT WÜRZBURG
WAHLAMT
97067 Würzburg
Verlorene Wahlscheine werden nicht ersetzt!
WAHLSCHEIN für die
Bundestagswahl
am 18.09.2005
Nur gültig für den Wahlkreis (Nr. Name)
252 - Würzburg
Wahlschein Nr. 304 / 3
Wahlbrief
An
Stadt Würzburg
- Wahlamt -
Rückermainstr. 2 (Rathaus)
97067 Würzburg
Wahlumschlag
für die Briefwahl
Sehr geehrte Wählerin!
Sehr geehrter Wähler!
Anlage 12
(zu § 29 Abs. 3)
Wichtige Hinweise für Briefwähler
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
Erststimme
Kolbow, Walter SPD
Friedl, Patrick
Kracht, Moritz GRÜNE
Seifert, Berthold FDP
Brechbilder, Belinda REP
Meenen, Uwe DIE LINKE.
Huth, Adelheid NPD
hier 1 Stimme
für die Wahl
einer Landesliste (Partei)
– maßgebende Stimme für die Verteilung der Sitze insgesamt auf die einzelnen Parteien –
Zweitstimme
CSU
SPD
GRÜNE
FDP
REP
DIE LINKE.
NPD
PBC
BP
DIE FRAUEN
GRAUE
BüSo
FAMILIE
MLPD

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)
  - better integrity, privacy, coercion-resistance, verifiability, trust is distributed, etc. ... all cryptographically enforced

Remote electronic voting

- Seems even cheaper and even more convenient
- Promises better security (than voting by post at least)
  - better integrity, privacy, coercion-resistance, verifiability, trust is distributed, etc. ... all cryptographically enforced

- Different security risks
  - Easier to launch large-scale attacks and erase evidence
  - Clients are the weakest link: e.g. remotely exploitable software flaws, viruses, Internet worms, trojans, lack of physical security, social engineering attacks, etc.
  - Network also vulnerable: e.g. voter demographic-based DDOS, cache poisoning DNS attacks, etc.

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

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

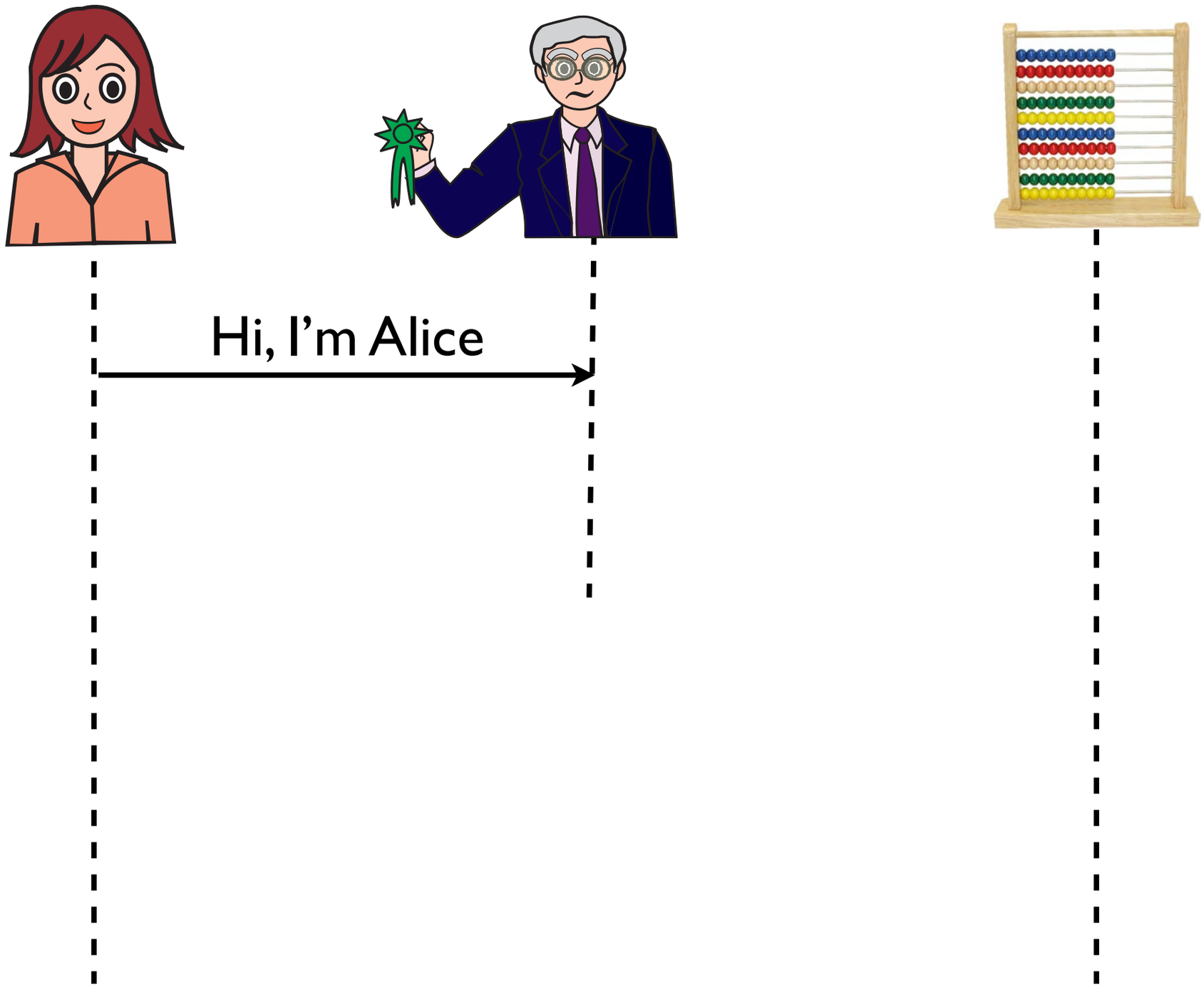
coercion-resistance

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

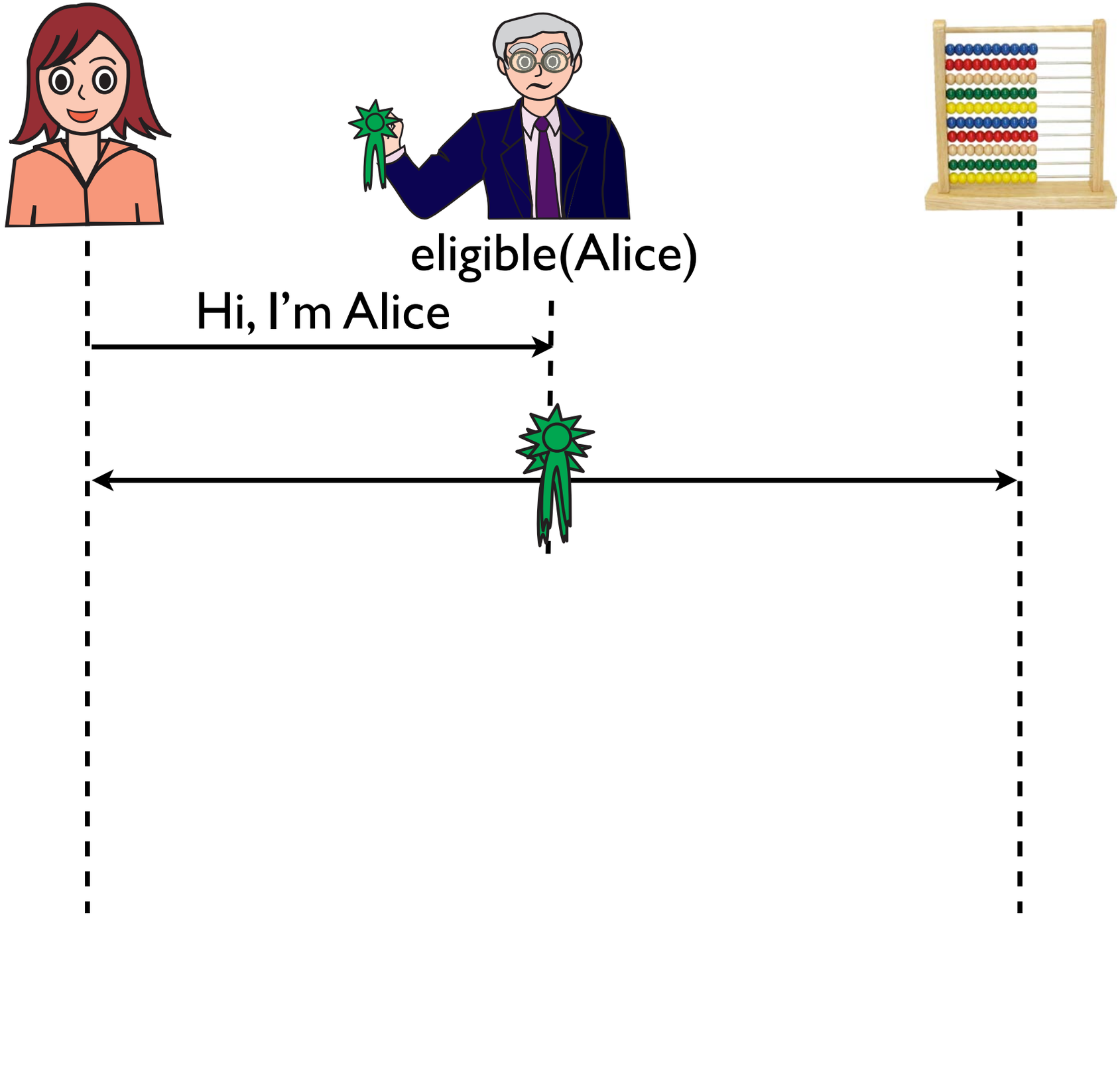
What we did

- 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)
- Proved that our coercion-resistance implies vote-privacy, immunity to forced-abstention attacks & receipt-freeness
- Automatically verified the security of the JCJ protocol

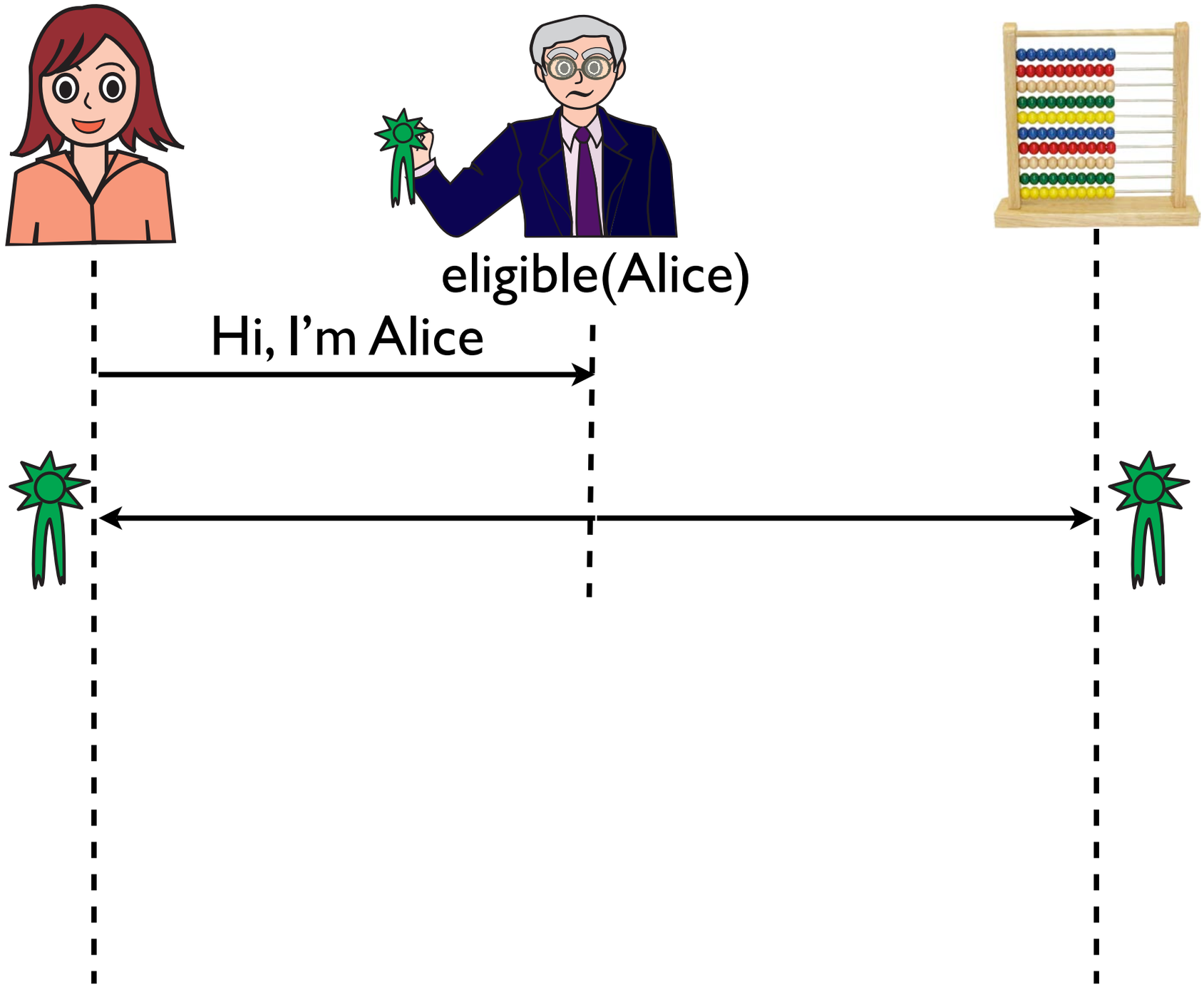
Soundness (eligibility, non-reusability, inalterability)



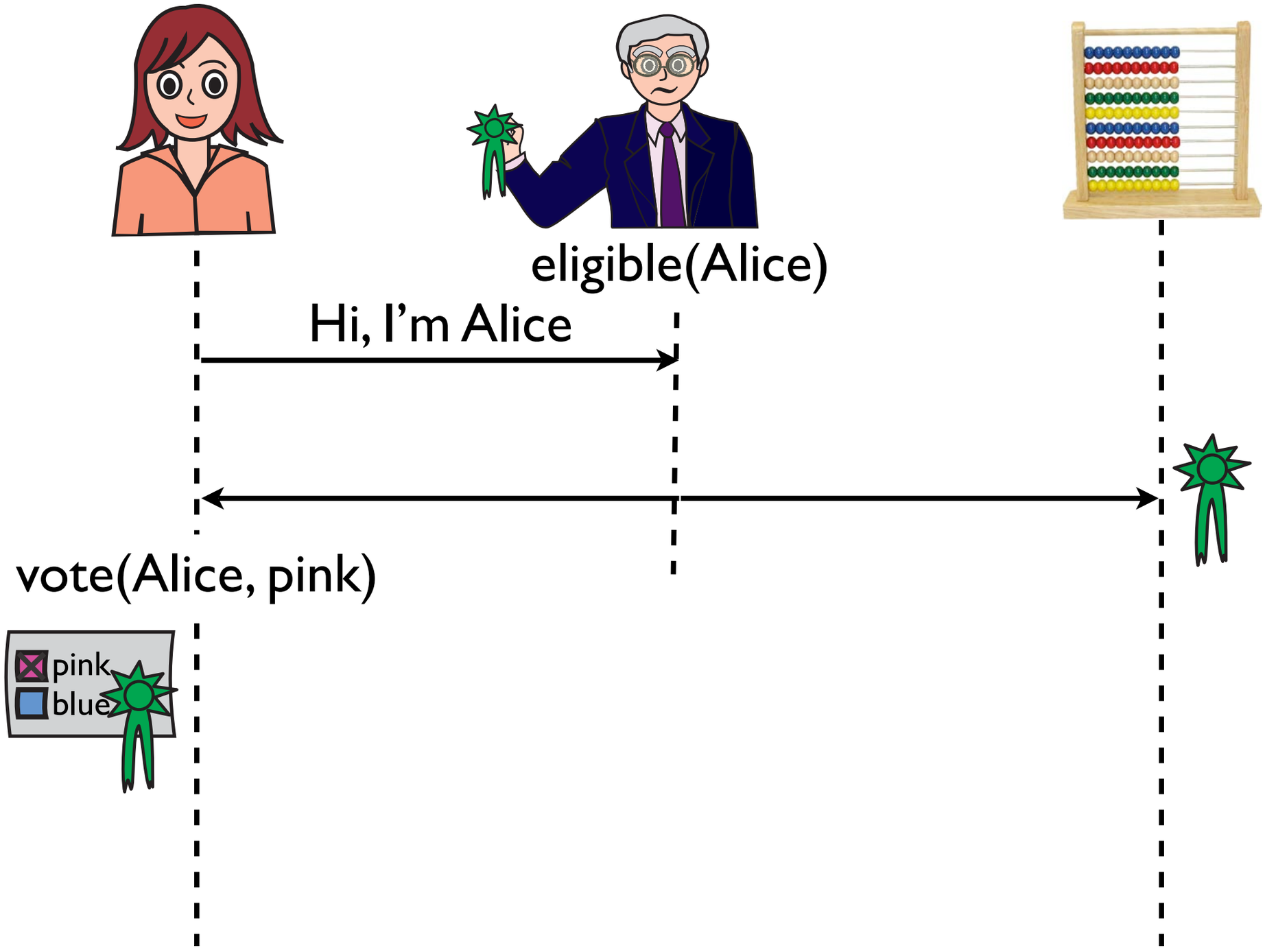
Soundness (eligibility, non-reusability, inalterability)



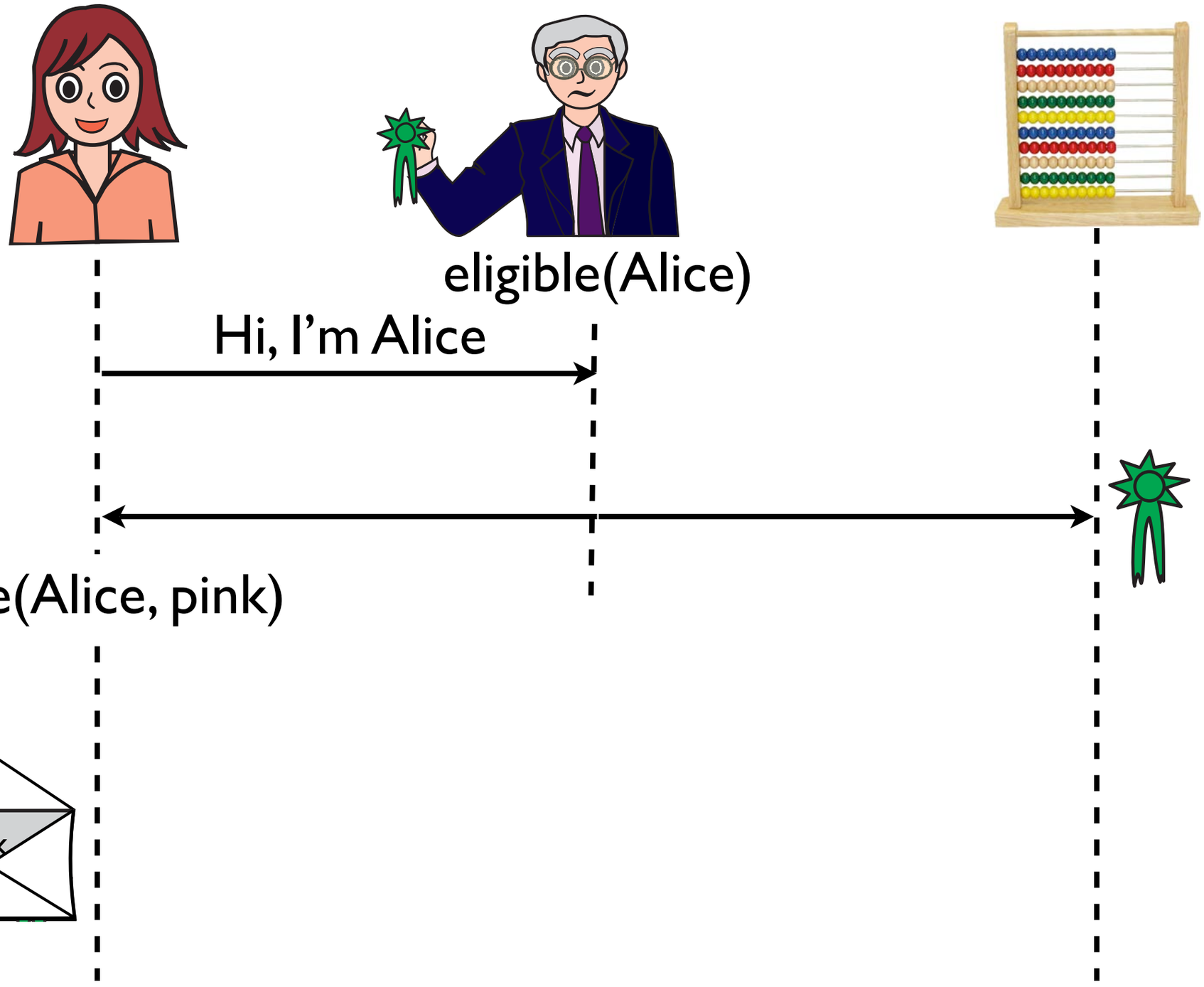
Soundness (eligibility, non-reusability, inalterability)



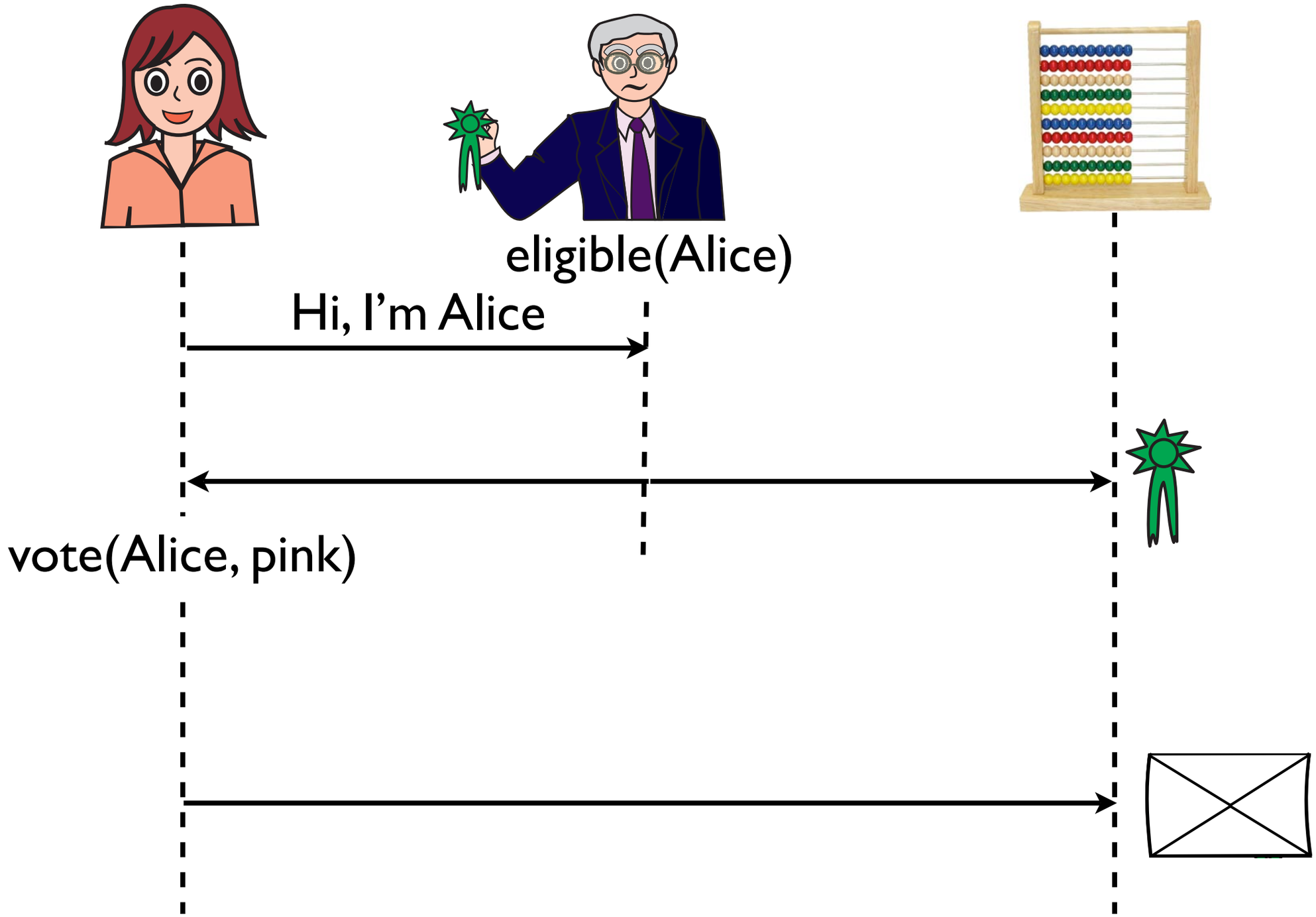
Soundness (eligibility, non-reusability, inalterability)



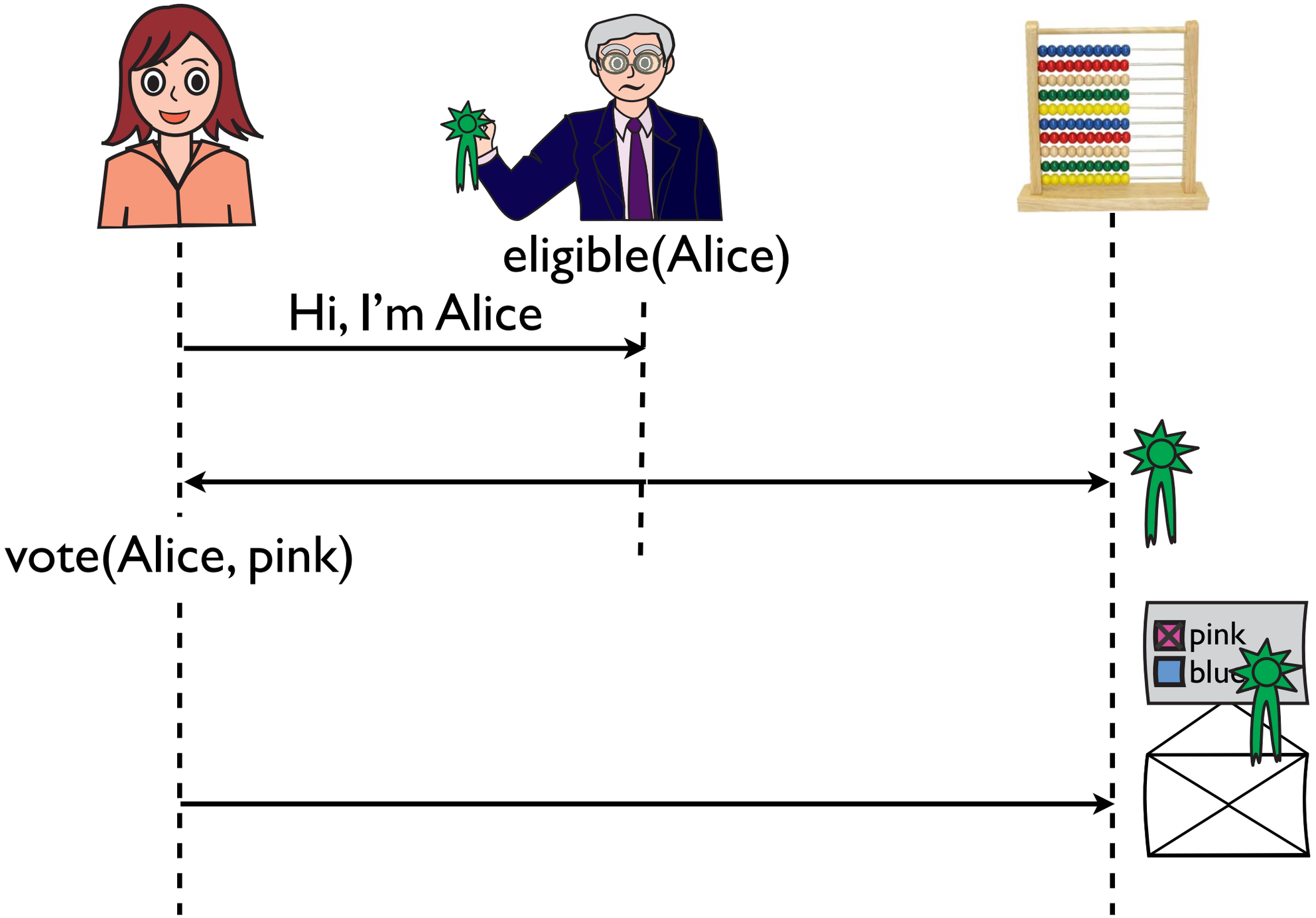
Soundness (eligibility, non-reusability, inalterability)



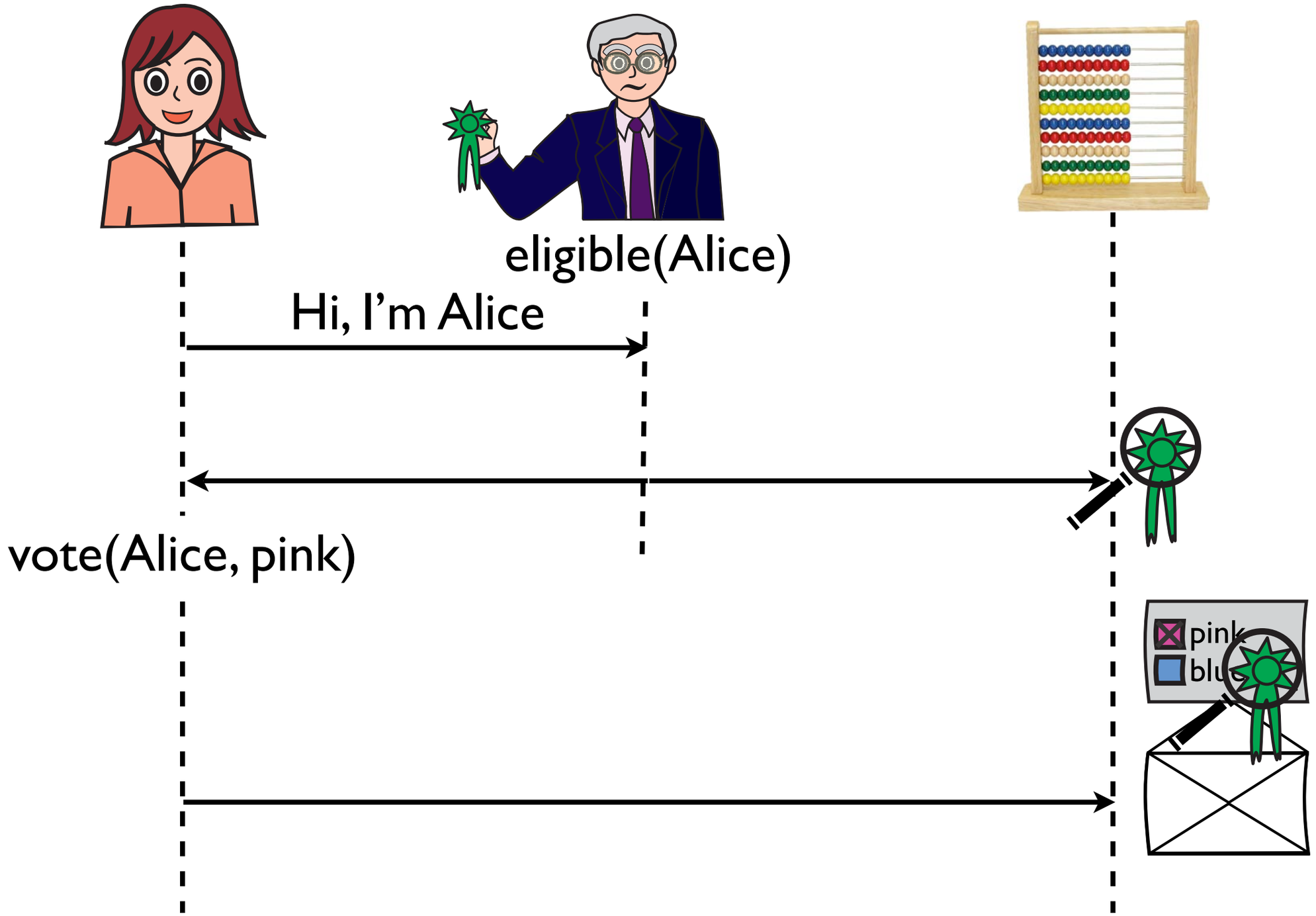
Soundness (eligibility, non-reusability, inalterability)



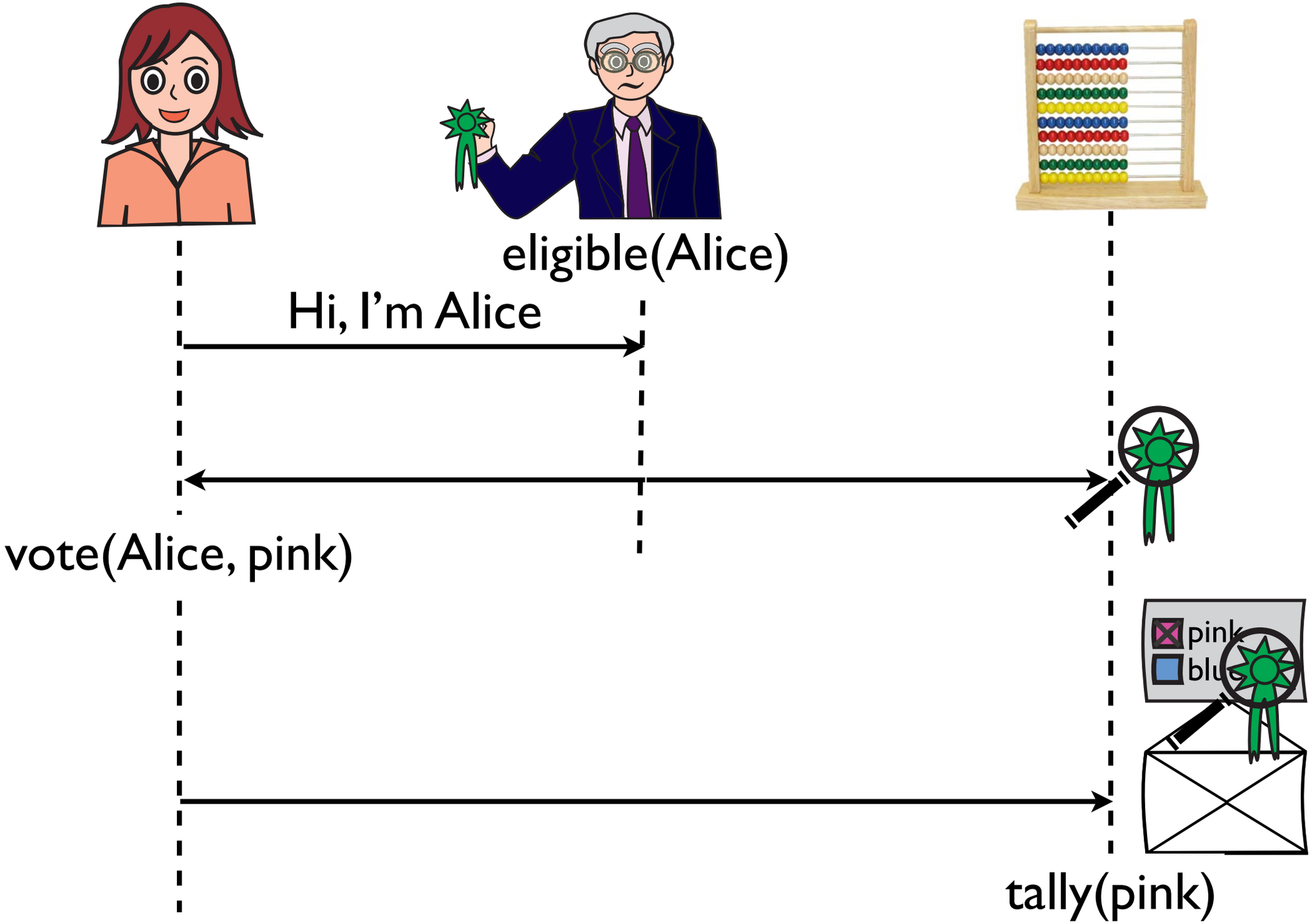
Soundness (eligibility, non-reusability, inalterability)



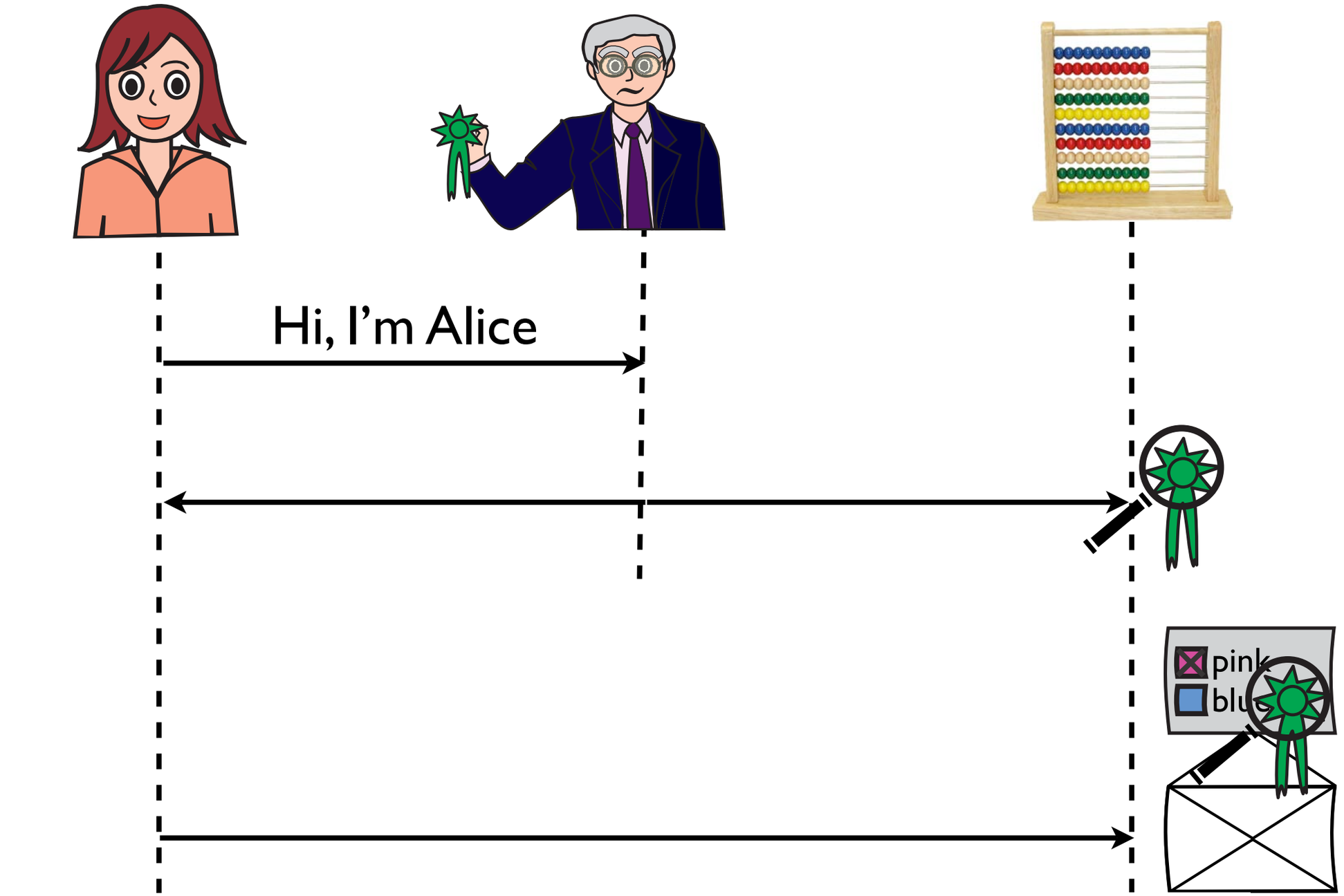
Soundness (eligibility, non-reusability, inalterability)



Soundness (eligibility, non-reusability, inalterability)

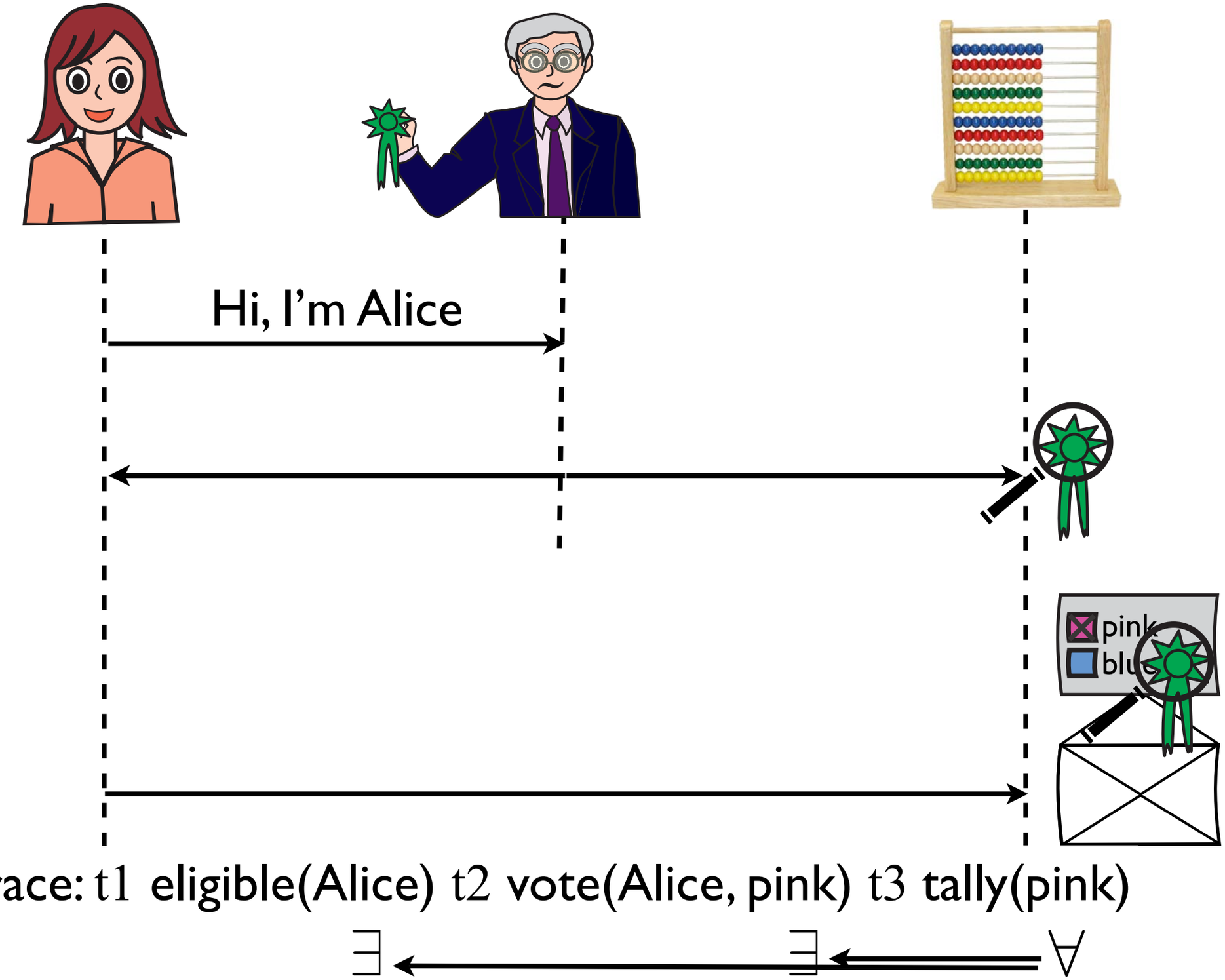


Soundness (eligibility, non-reusability, inalterability)

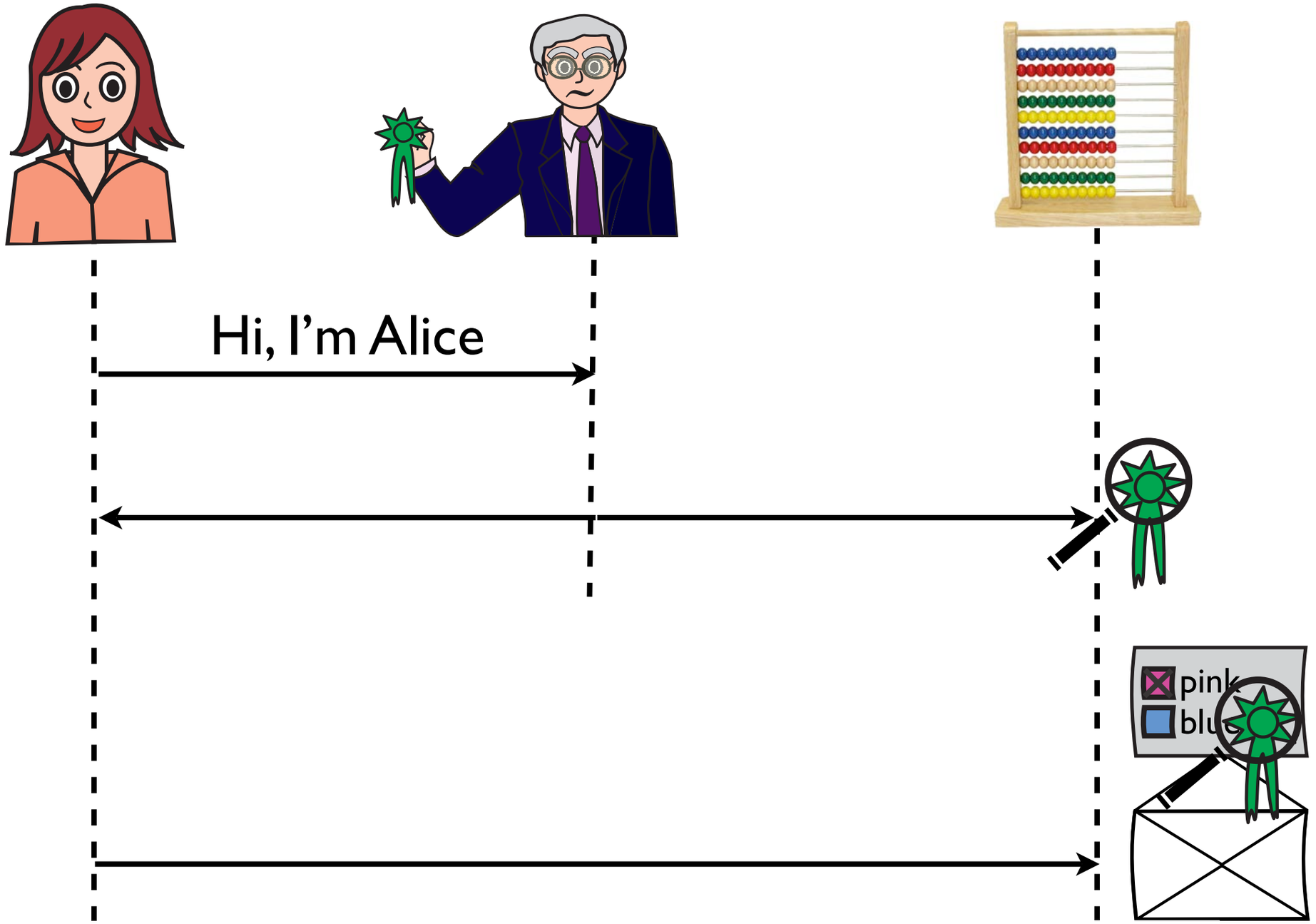


Trace: t1 eligible(Alice) t2 vote(Alice, pink) t3 tally(pink)

Soundness (eligibility, non-reusability, inalterability)



Soundness (eligibility, non-reusability, inalterability)



Trace: t1 eligible(Alice) t2 vote(Alice, pink) t3 tally(pink)

$\exists \quad \exists \quad \forall$

and the trace t1 t2 t3 is also sound (injective matching)

Vote-privacy

Voters

Alice
Bob
Charlie

Results

pink party |
blue party ||

Vote-privacy

Voters

Alice
Bob
Charlie

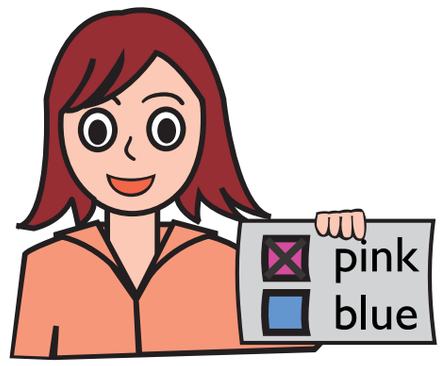
Results

pink party |
blue party ||

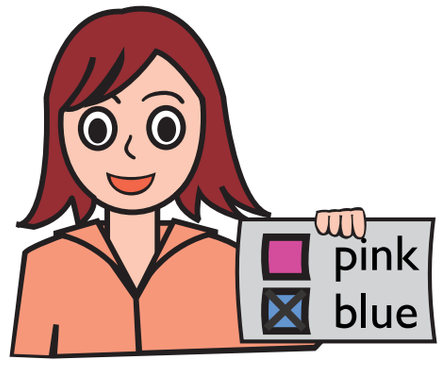
~~**"Detailed" results**~~

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

Definition of vote-privacy

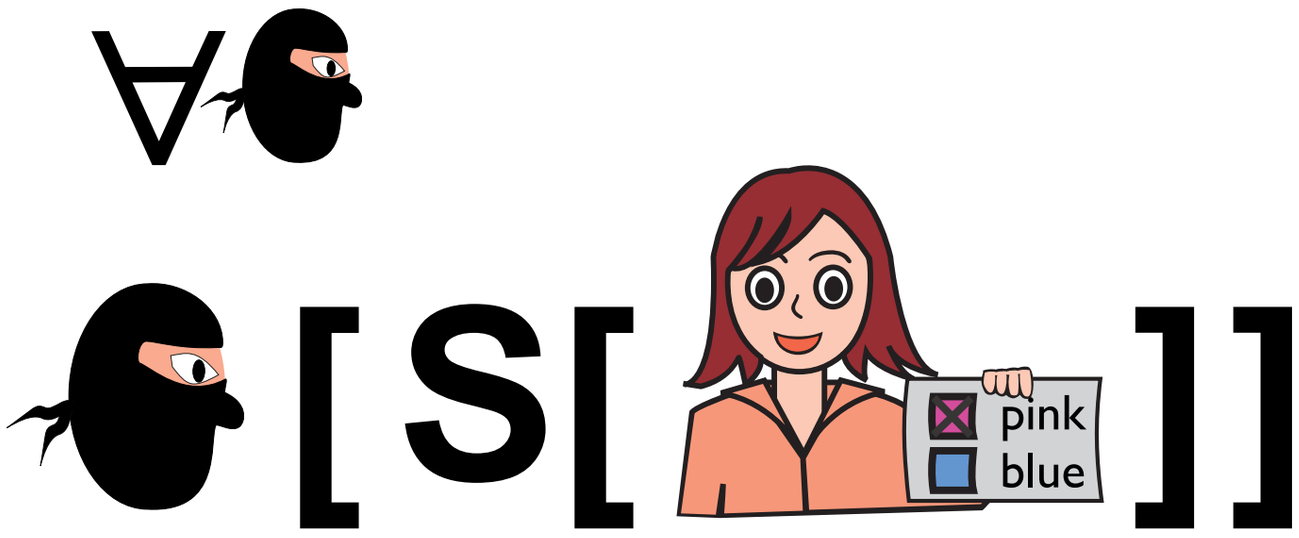
S[

]

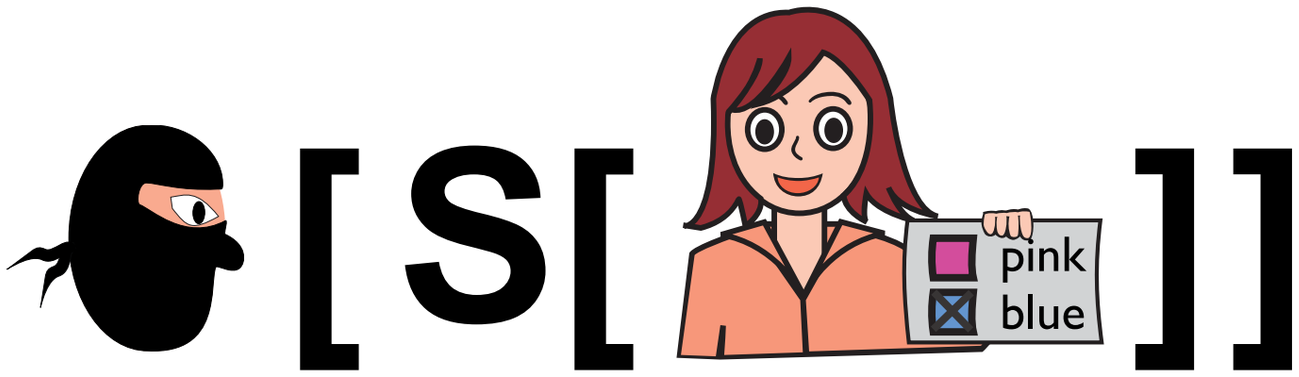
S[

]

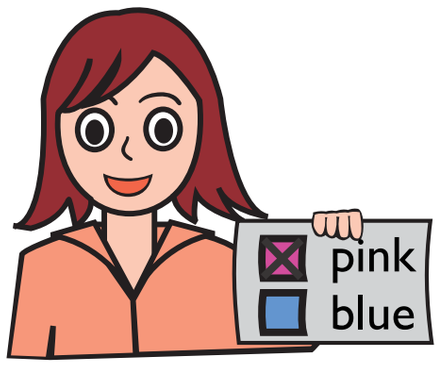
Definition of vote-privacy



indistinguishable from

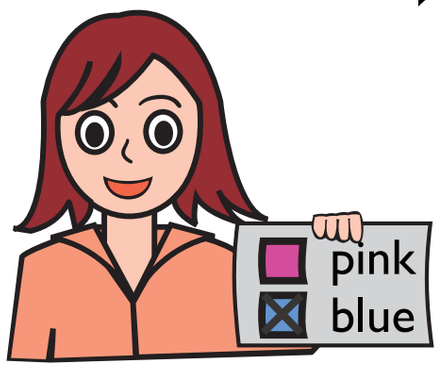


Definition of vote-privacy

$$S\left[\ \right.$$ 

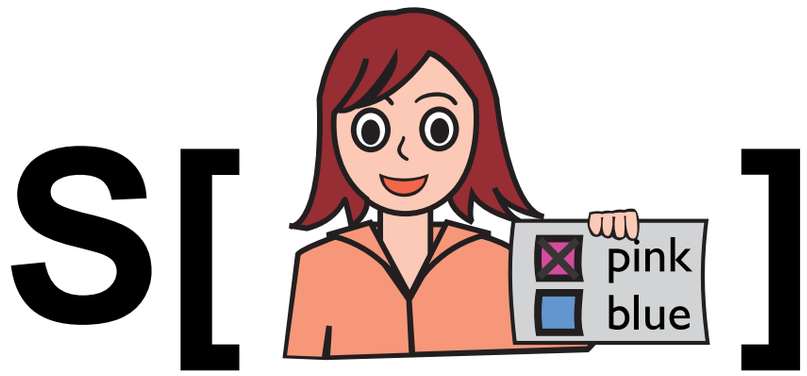
$$\left.\ \right]$$

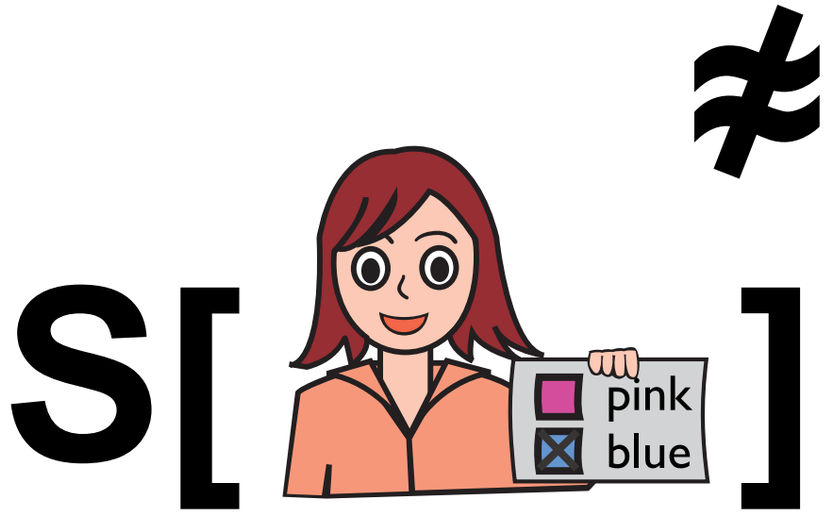
$$\approx$$

$$S\left[\ \right.$$ 

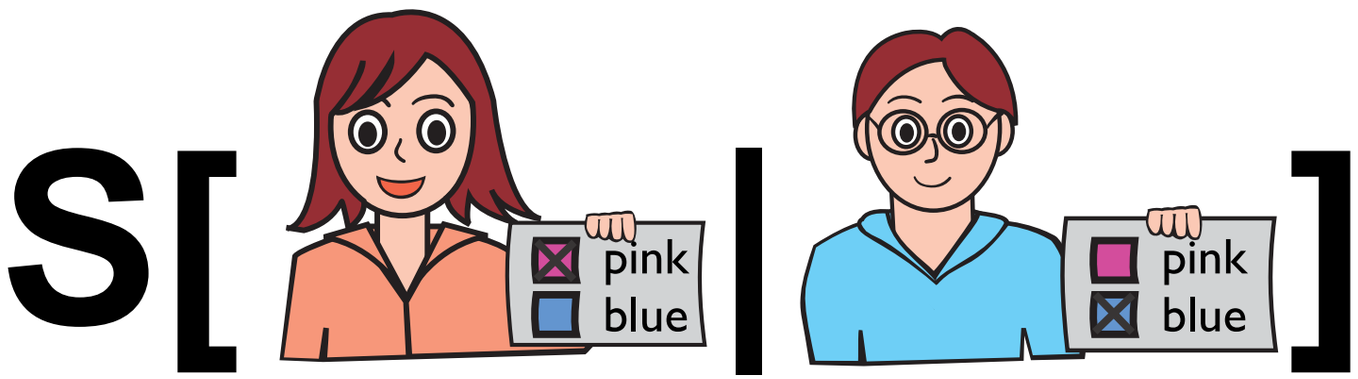
$$\left.\ \right]$$

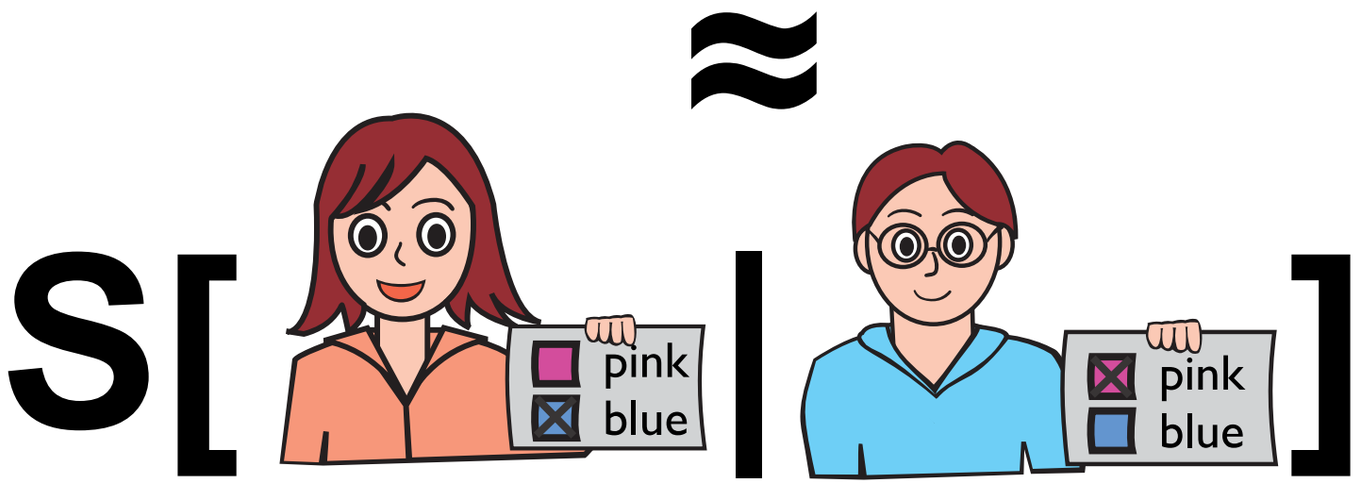
Definition of vote-privacy



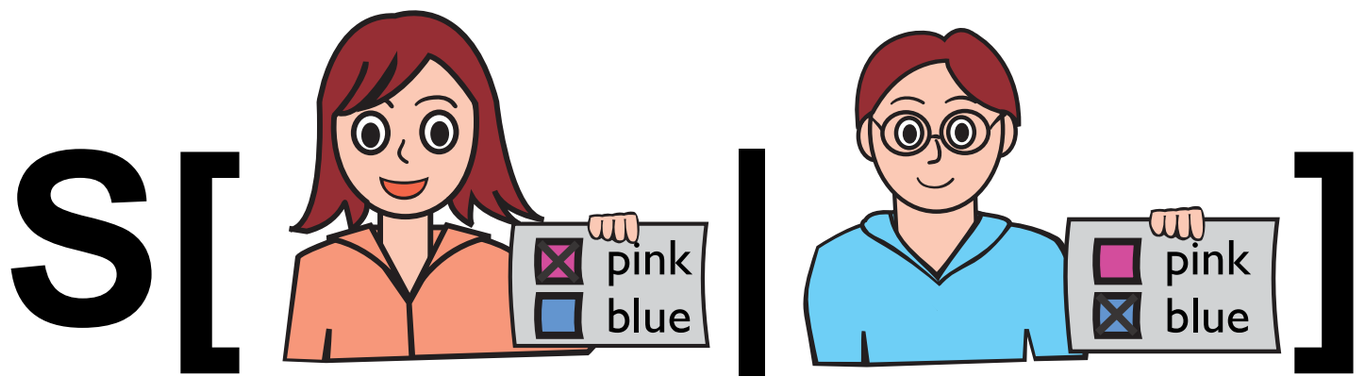


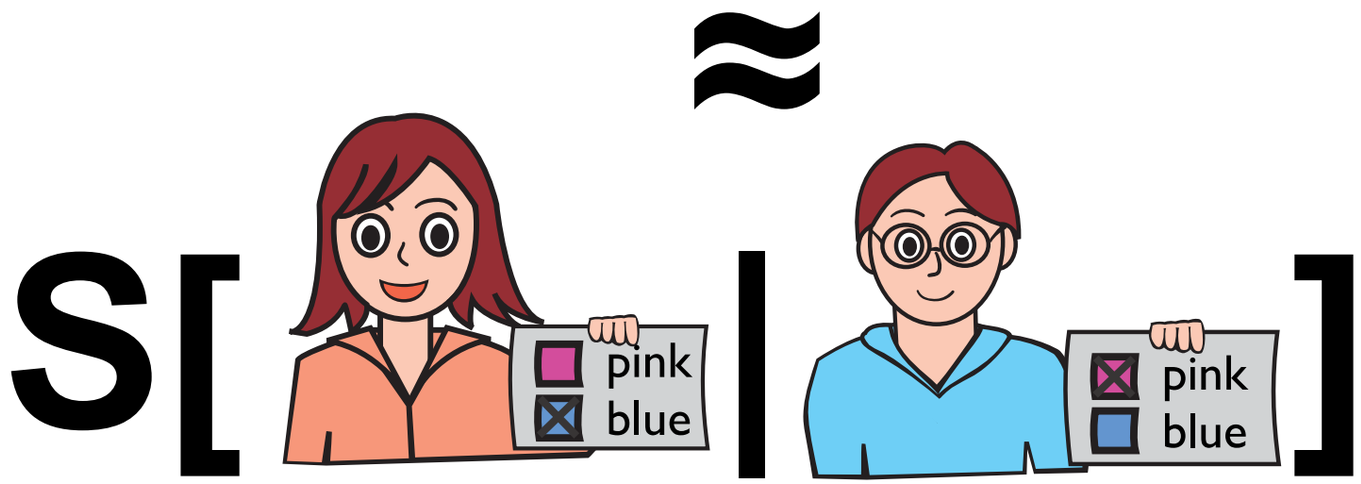
Definition of vote-privacy





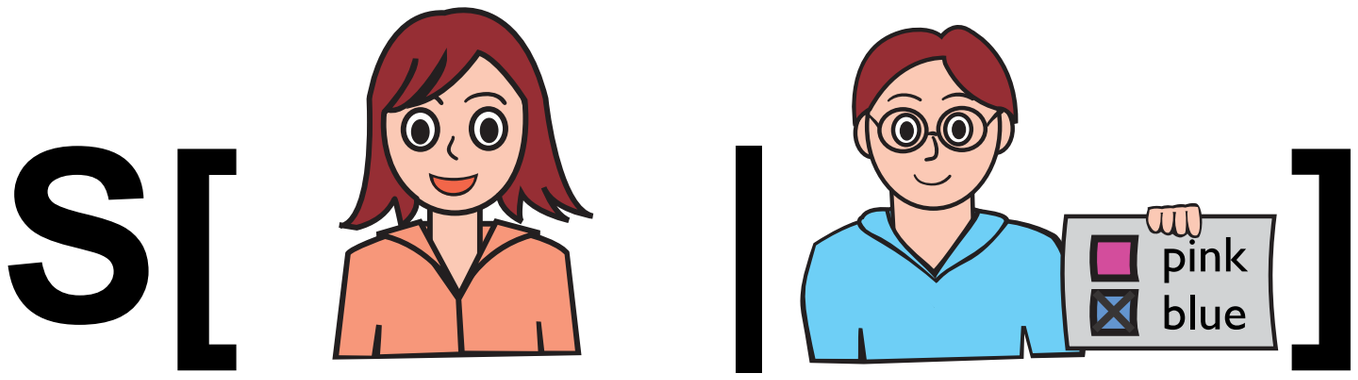
Definition of vote-privacy

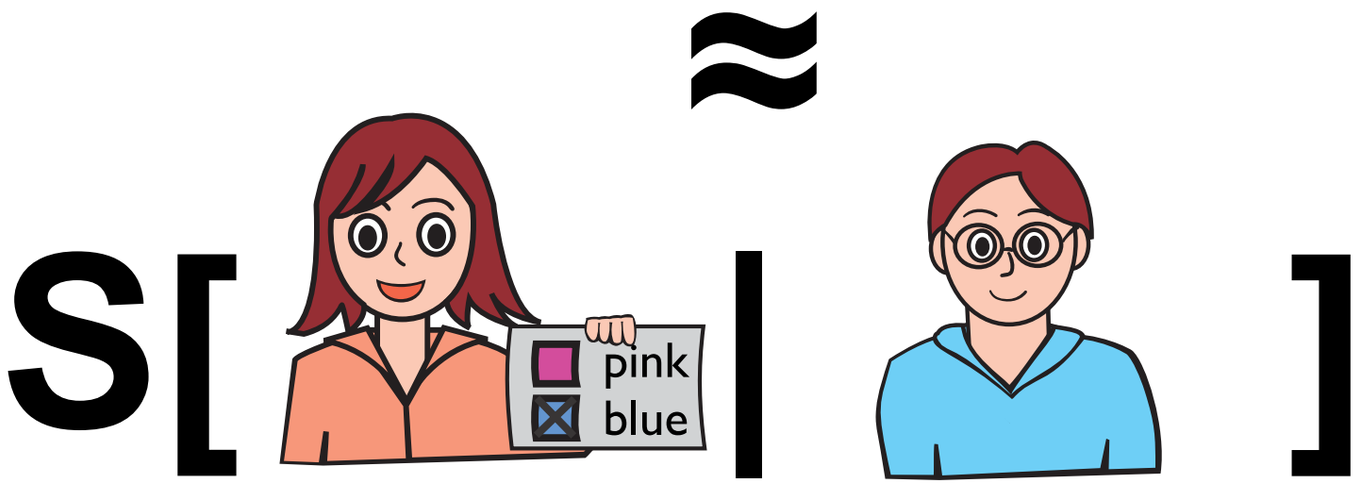




- [Delaune, Kremer & Ryan; CSF '06]

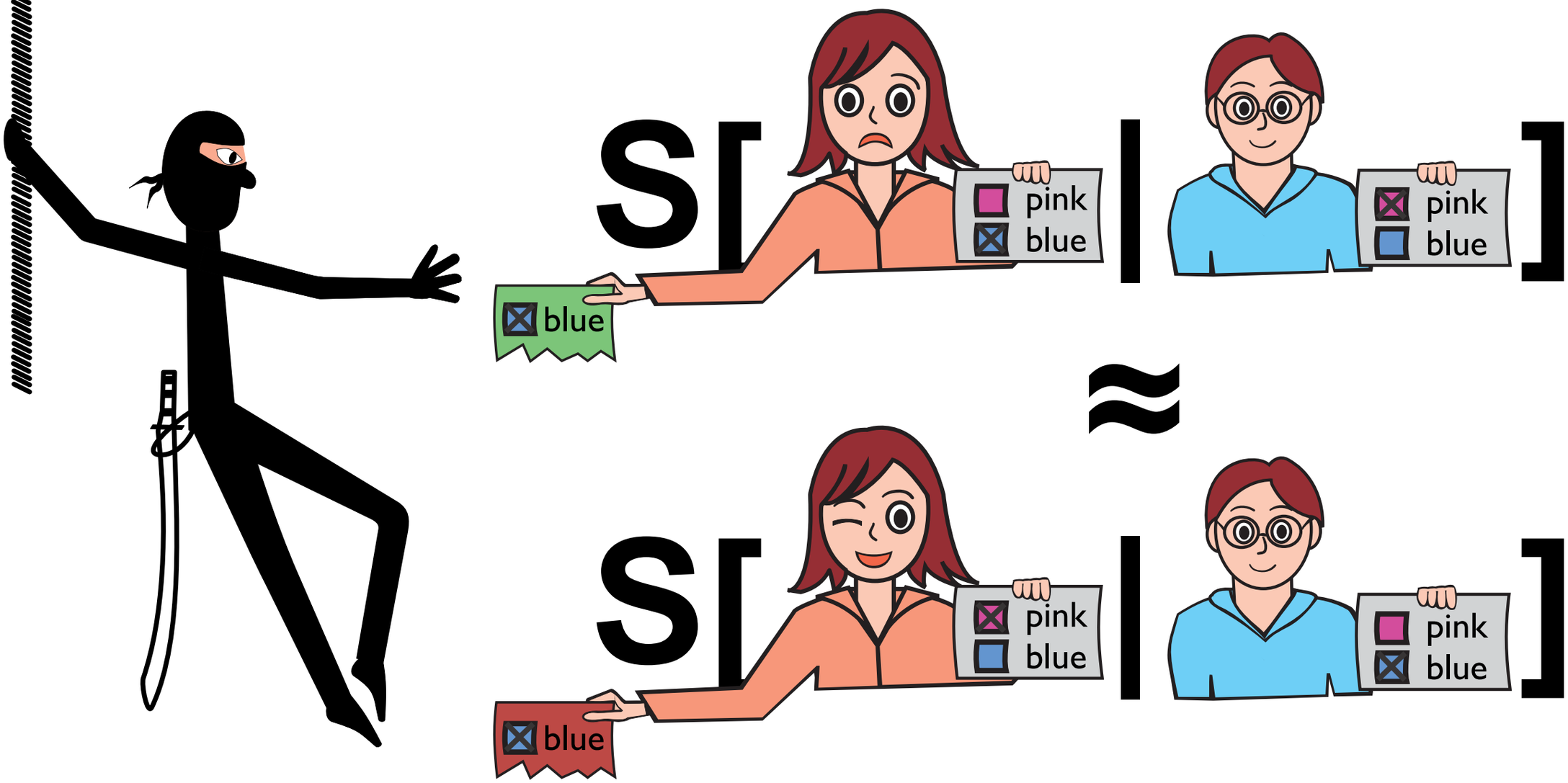
Immunity to forced-abstention





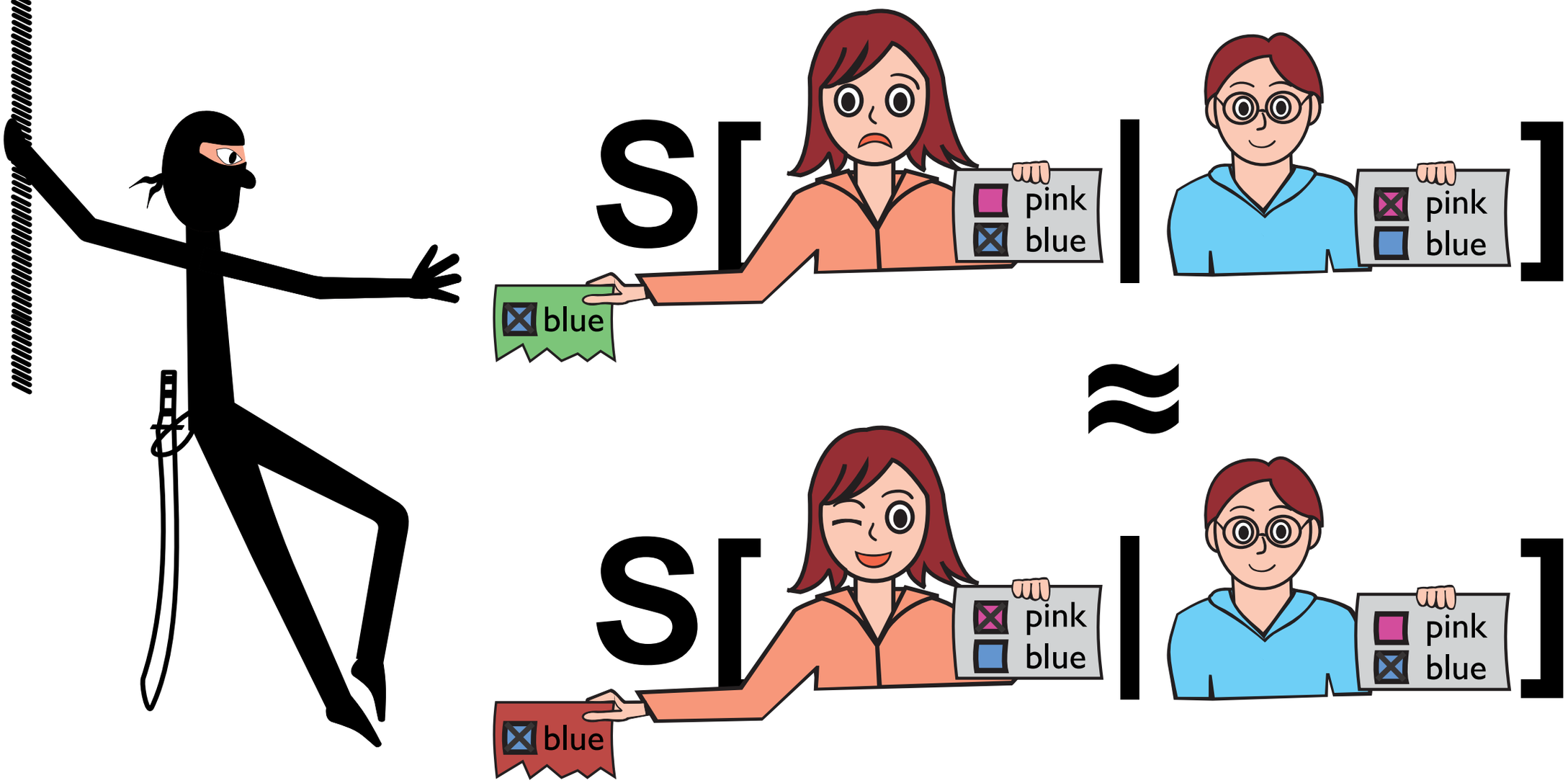
Receipt-freeness

- [Benaloh & Tuinstra; STOC '94]



Receipt-freeness

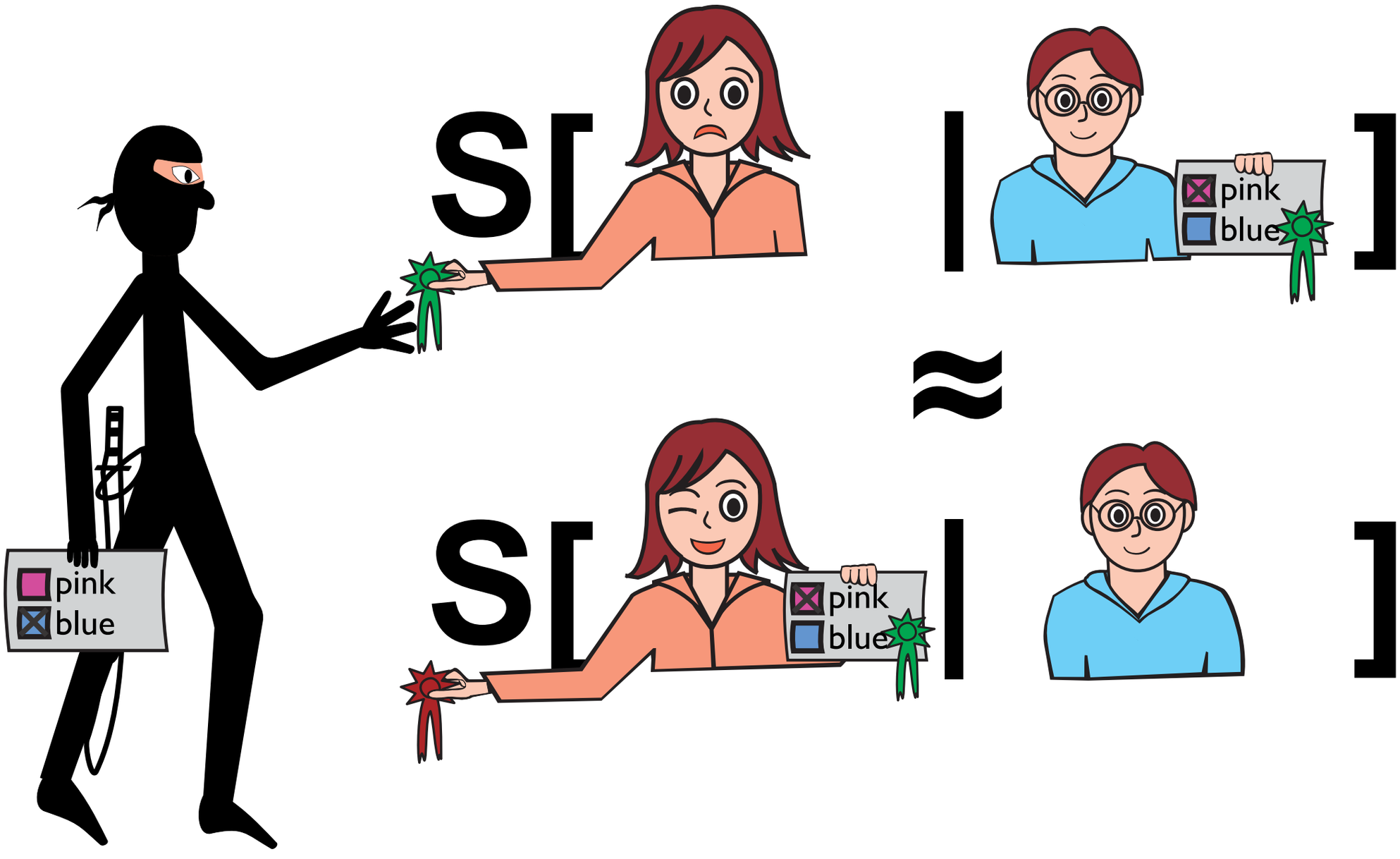
- [Benaloh & Tuinstra; STOC '94]



- [Delaune, Kremer & Ryan; CSF '06]

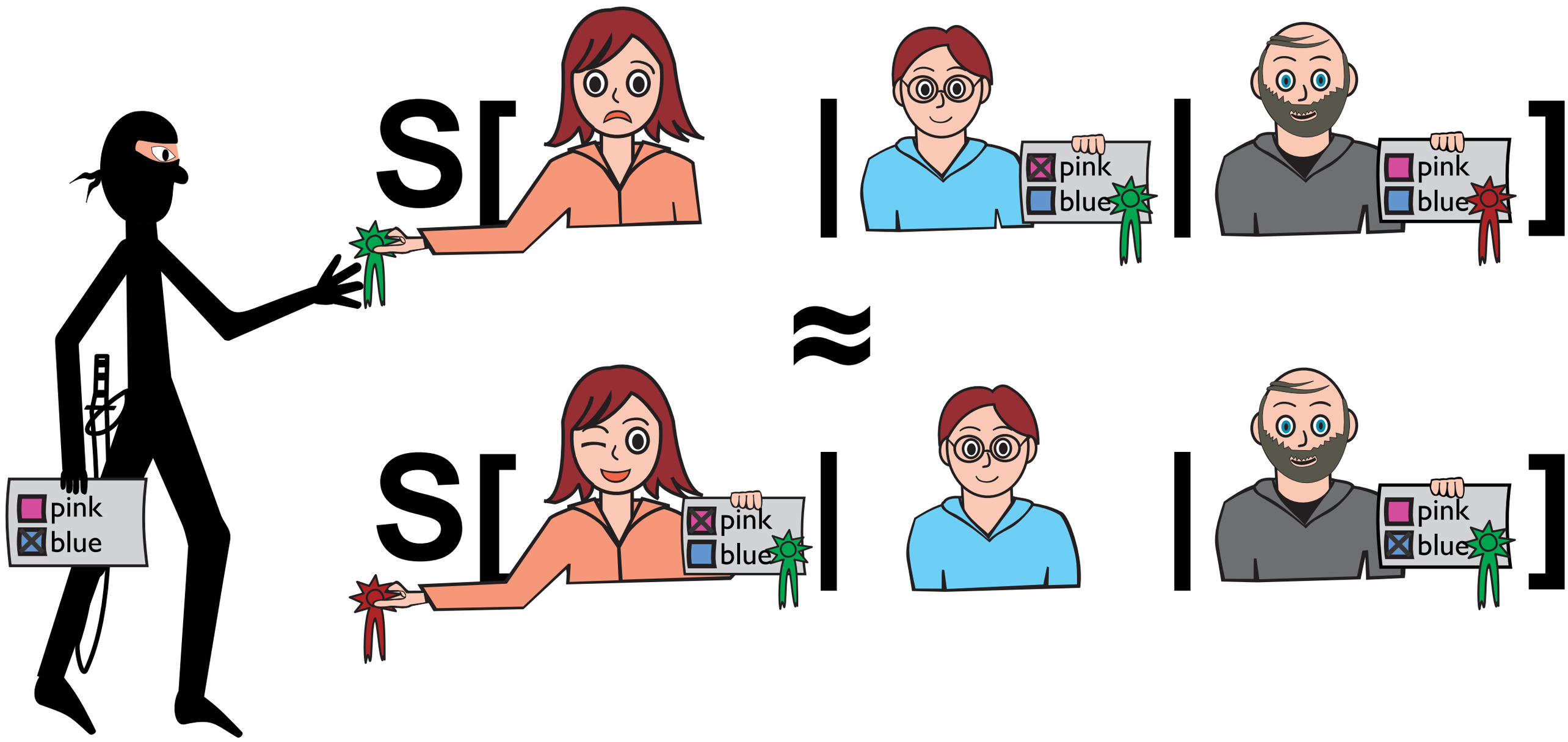
Coercion-resistance

- [Juels, Catalano & Jakobsson; WPES 2005]



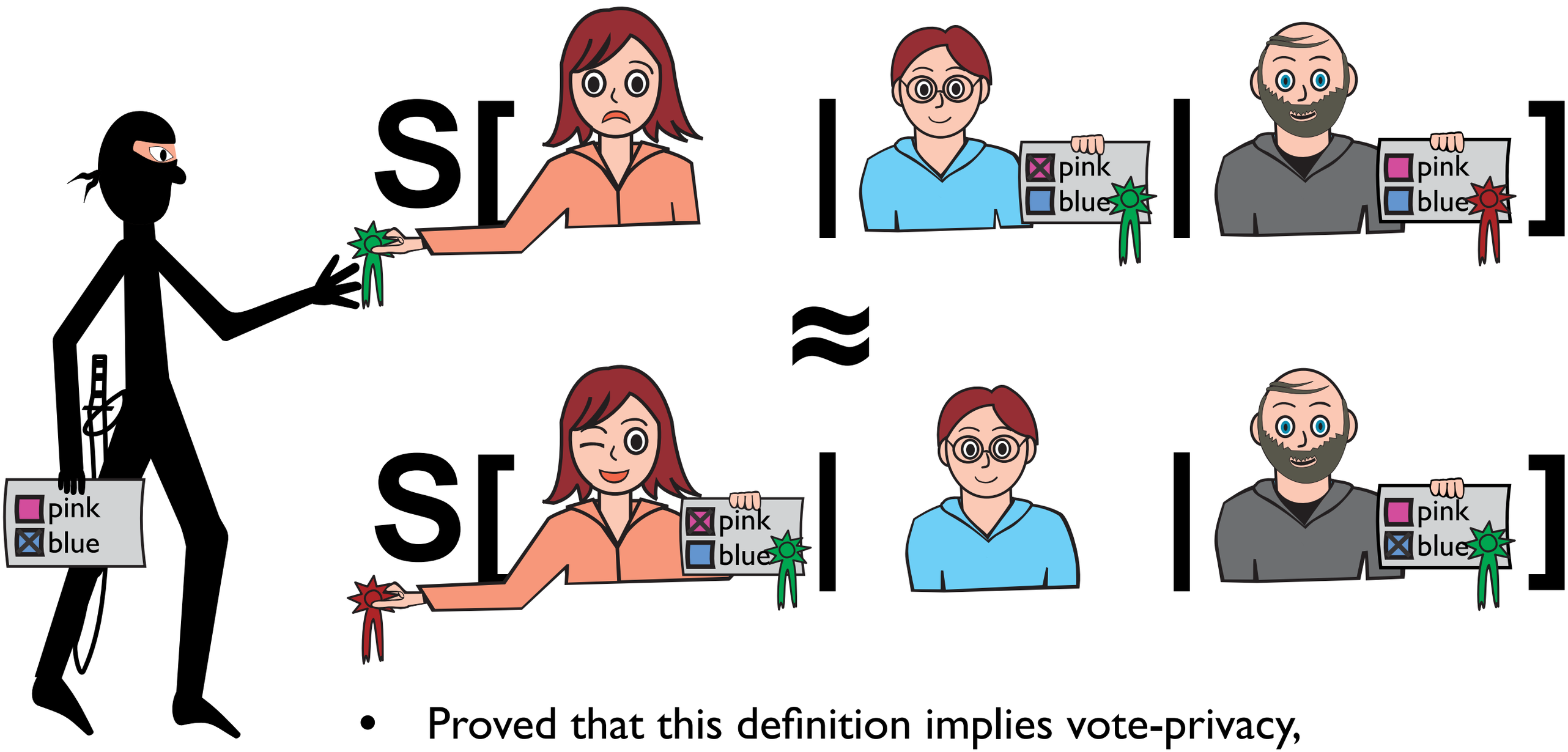
Coercion-resistance

- [Juels, Catalano & Jakobsson; WPES 2005]



Coercion-resistance

- [Juels, Catalano & Jakobsson; WPES 2005]



- Proved that this definition implies vote-privacy, immunity to forced-abstention attacks & receipt-freeness

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 (observational equivalence)
no simulation attacks	yes	n/a	n/a	yes
no forced-abstention	yes	no	no	yes
no randomization attacks (?)	yes	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)
- Analysis performed with ProVerif
  - automatic protocol analyzer using Horn-clause resolution
  - we use our abstraction of zero-knowledge [S&P 2008]
  - 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.

Future work

- Analyzing Civitas (variant of JCJ with implementation)
- Other properties
  - Individual verifiability (trace property)
  - Immunity to randomization attacks (privacy property)
- Different techniques for trace properties
  - type systems - e.g. our type system for ZK [WITS '08]
- Different techniques for observational equivalence
  - for instance using symbolic bisimulation [DKR, SecCo '07]
- More accurate protocol models
  - The ultimate goal is to analyze implementations