IS&C

UNIVERSITÄT DES SAARLANDES

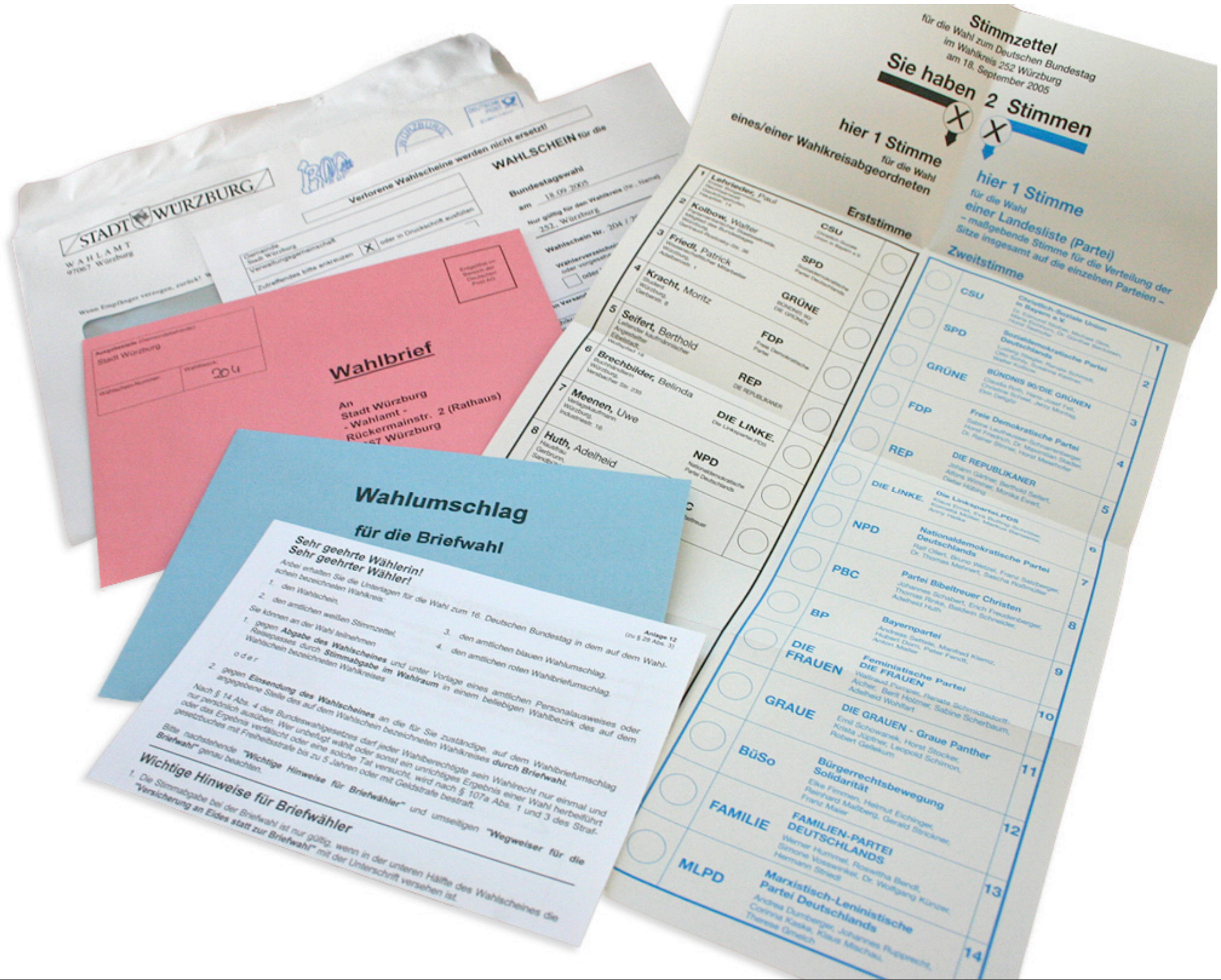
Automatic Verification of Remote Electronic Voting Protocols

Michael Backes, Cătălin Hriţcu, Matteo Maffei

Information Security & Cryptography Group

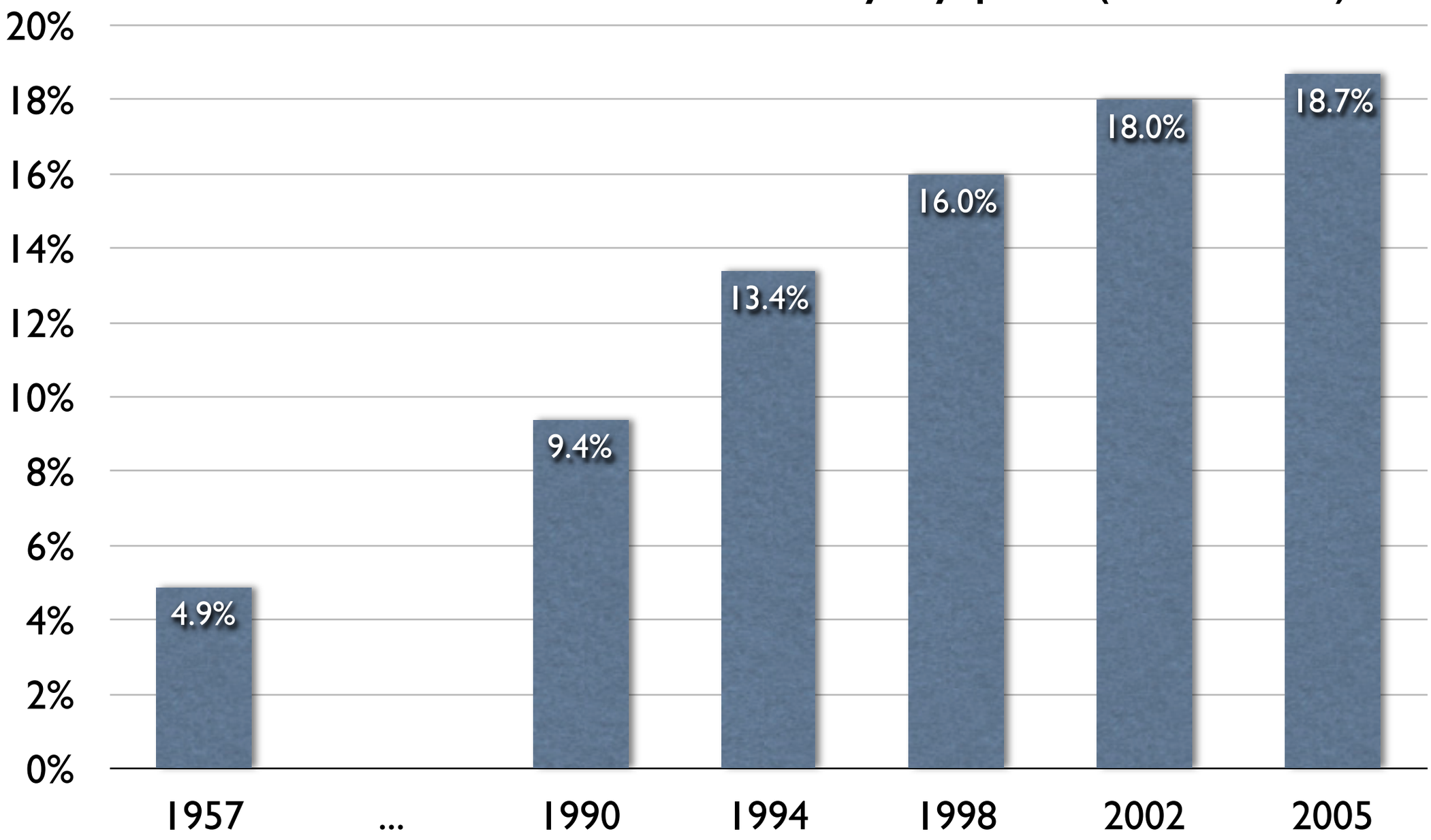
Max Planck Institute for Software Systems - Faculty Retreat, Berlin, March 2008

Remote voting is a reality!



Remote voting in Germany

- Did you know that ...
  - ... in the latest parliamentary elections **18.7%** of the votes were cast remotely by post (Briefwahl)?



Remote voting

Remote voting

- Cheaper and more convenient than supervised voting
  - This could increase voter participation

Remote voting

- Cheaper and more convenient than supervised voting
  - This could 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
  - Really easy to buy/sell votes
  - Not that hard to coerce someone to vote as you like

Remote voting

- Cheaper and more convenient than supervised voting
  - This could 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
  - Really easy to buy/sell votes
  - Not that hard to coerce someone to vote as you like
- Still, this has been used in Germany for 50+ years

Remote electronic voting

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.

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.
- Still, Internet voting might be just around the corner

Some of the desired properties

Correctness

- soundness
  - eligibility
  - non-reusability
  - inalterability
- completeness
- fairness

Privacy

- vote-privacy
- immunity to forced-abstention attacks
- receipt-freeness
- coercion-resistance

Verifiability

- universal
- individual

Robustness

- fault tolerance
- availability
- scalability

Some of the desired properties

Correctness

- soundness
  - eligibility
  - non-reusability
  - inalterability
- completeness
- fairness

Privacy

- vote-privacy
- immunity to forced-abstention attacks
- receipt-freeness
- coercion-resistance

Verifiability

- universal
- individual

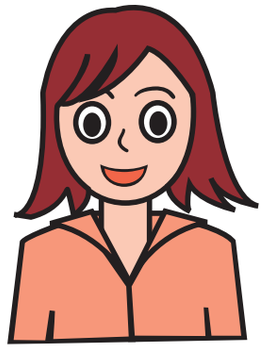
Robustness

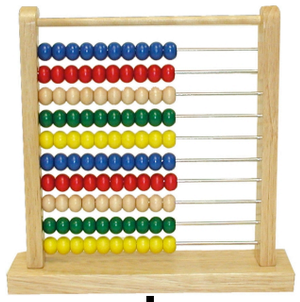
- fault tolerance
- availability
- scalability

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

What we did

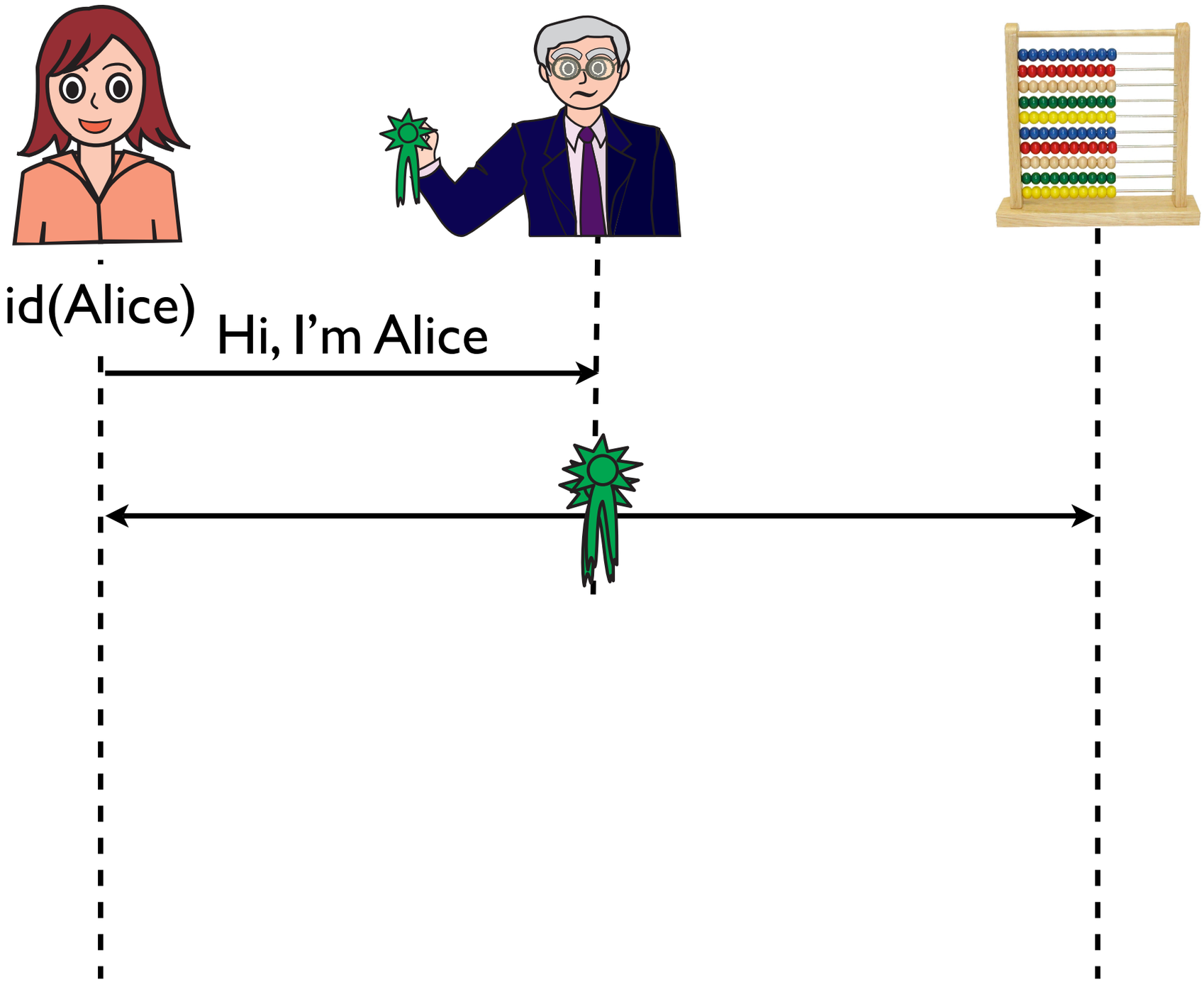
- General technique for
  - modeling remote electronic voting protocols (in the applied pi-calculus)
  - and automatically verifying their security
- New formal definitions of
  - soundness - trace property
  - coercion-resistance - observational equivalence
  - Both definitions amenable to automation in ProVerif
- Proved that our coercion-resistance implies vote-privacy, immunity to forced-abstention attacks & receipt-freeness
- Automatically verified the security of the JCJ protocol

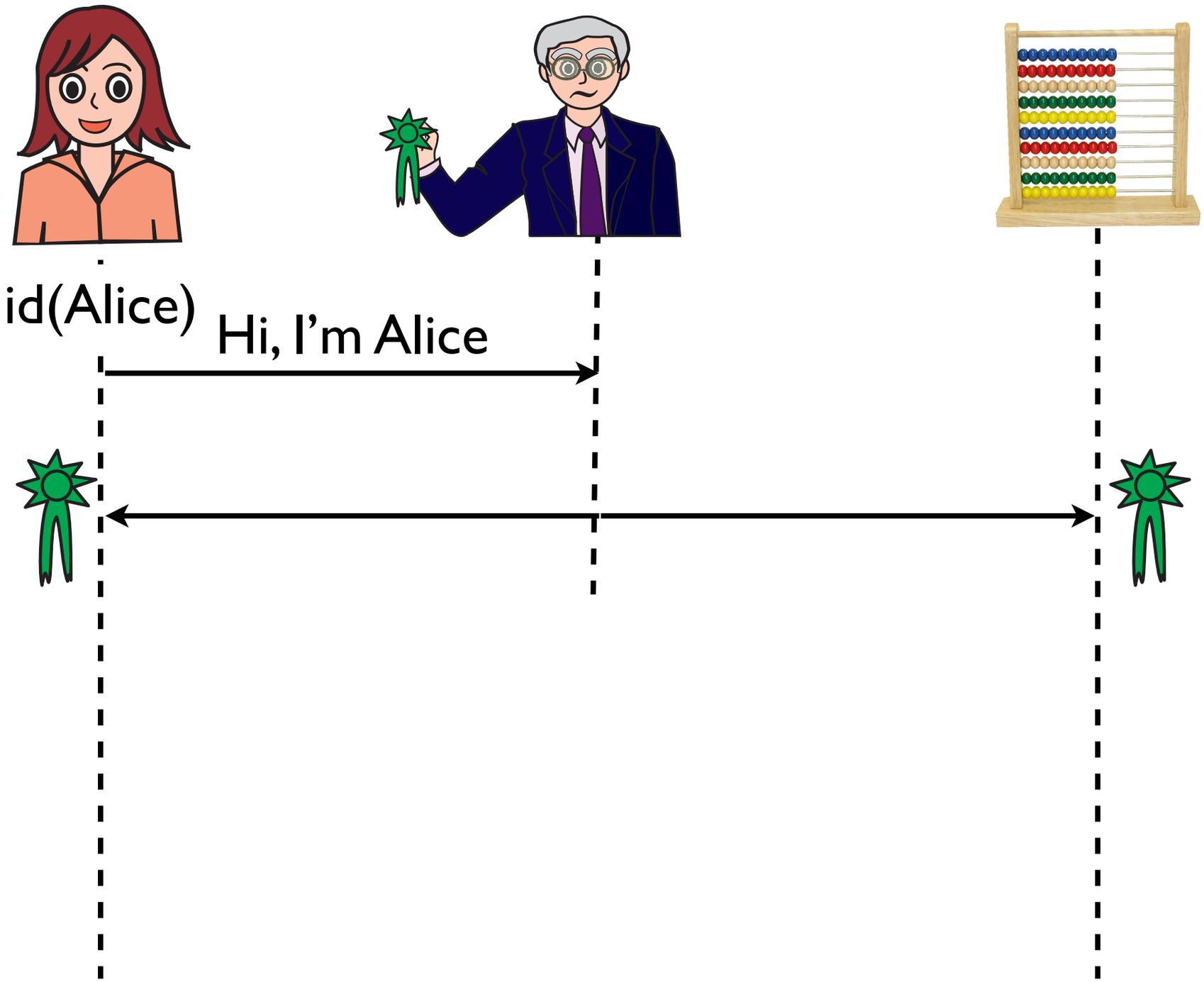


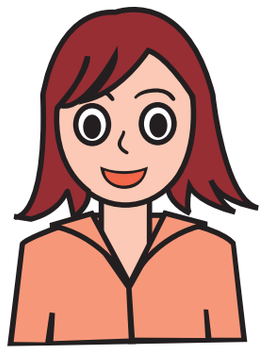


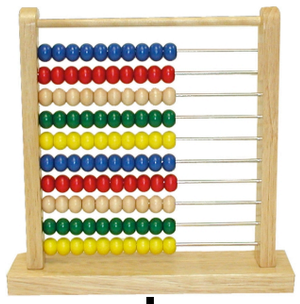
id(Alice)

Hi, I'm Alice


id(Alice)
Hi, I'm Alice

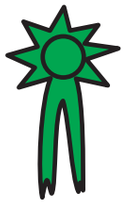

id(Alice)
Hi, I'm Alice



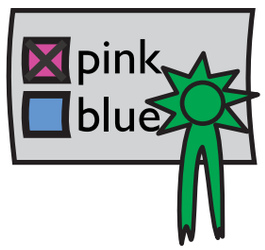


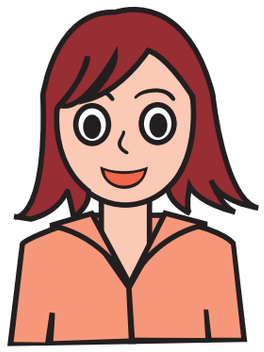
id(Alice)

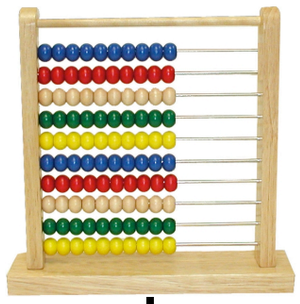
Hi, I'm Alice



vote(Alice, pink)

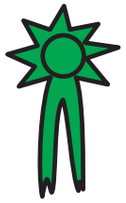




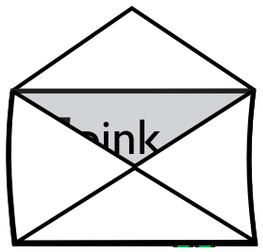


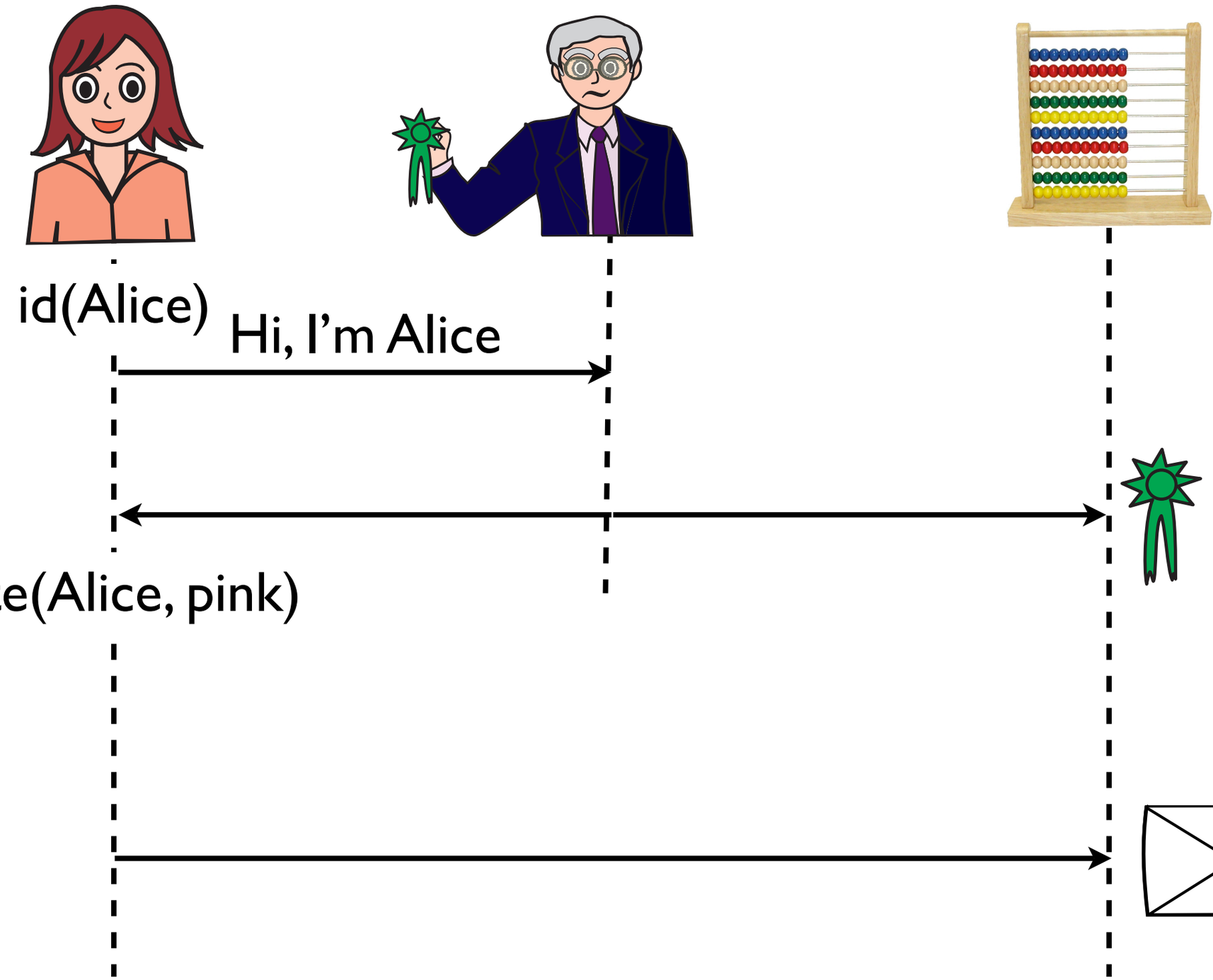
id(Alice)

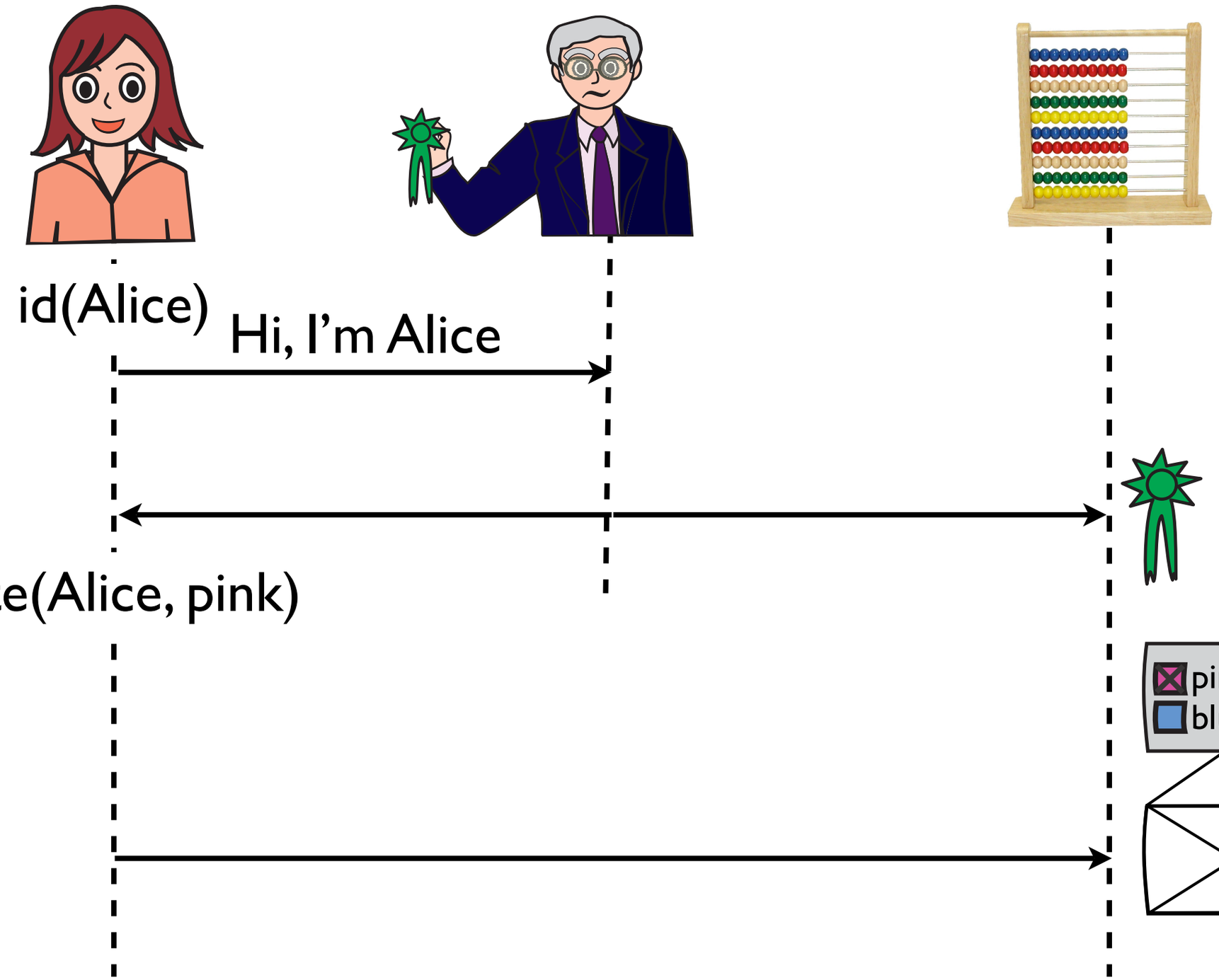
Hi, I'm Alice

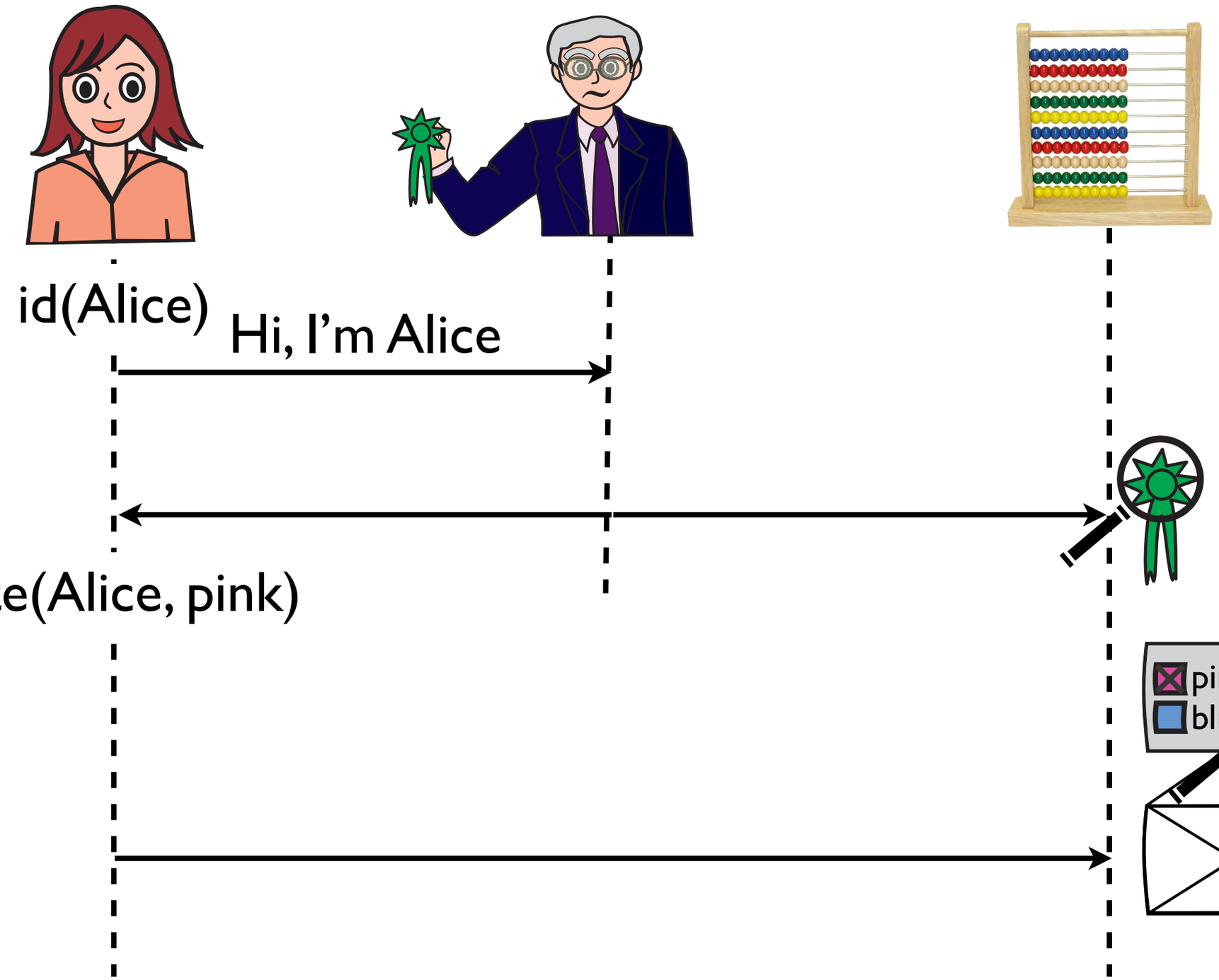


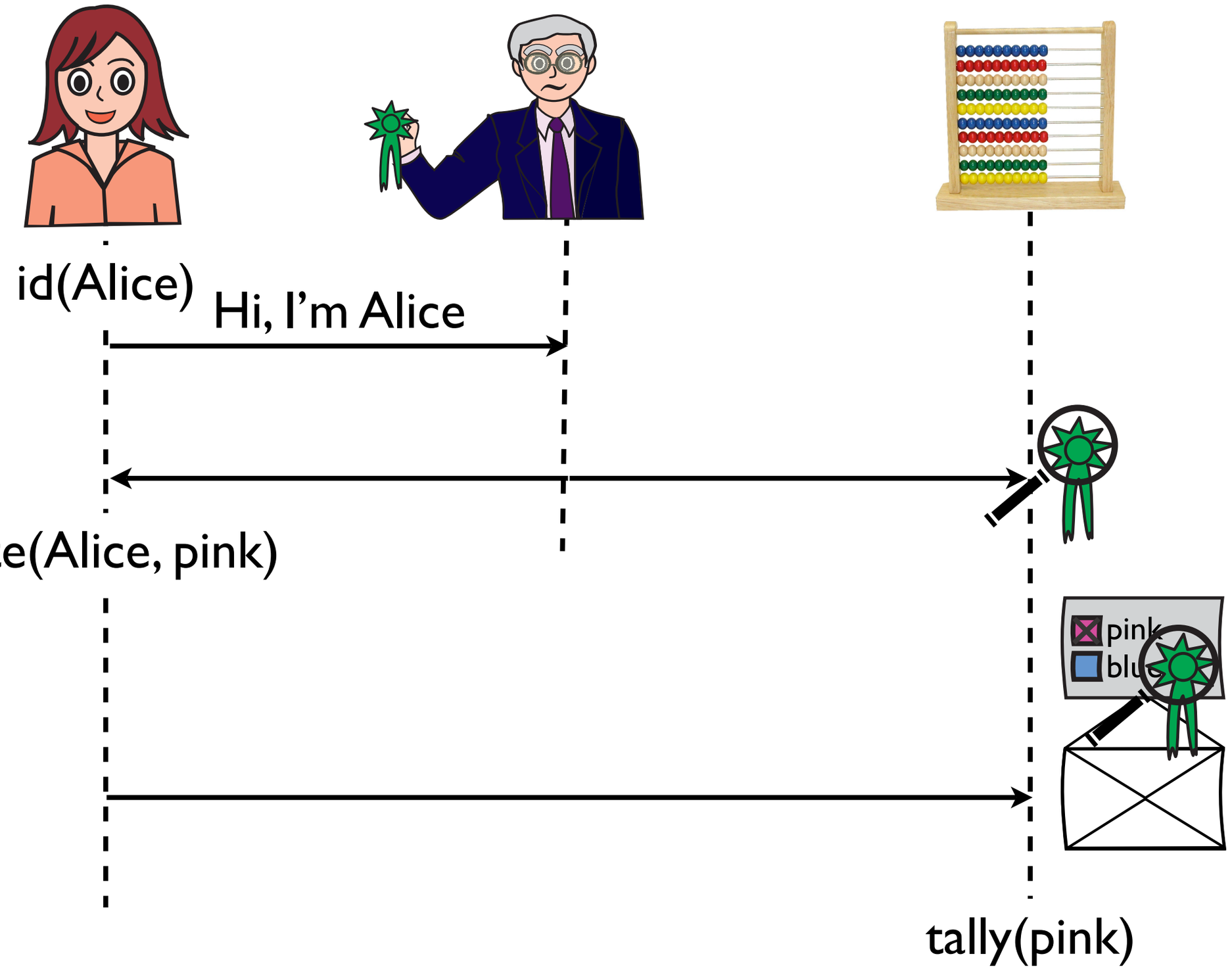
vote(Alice, pink)

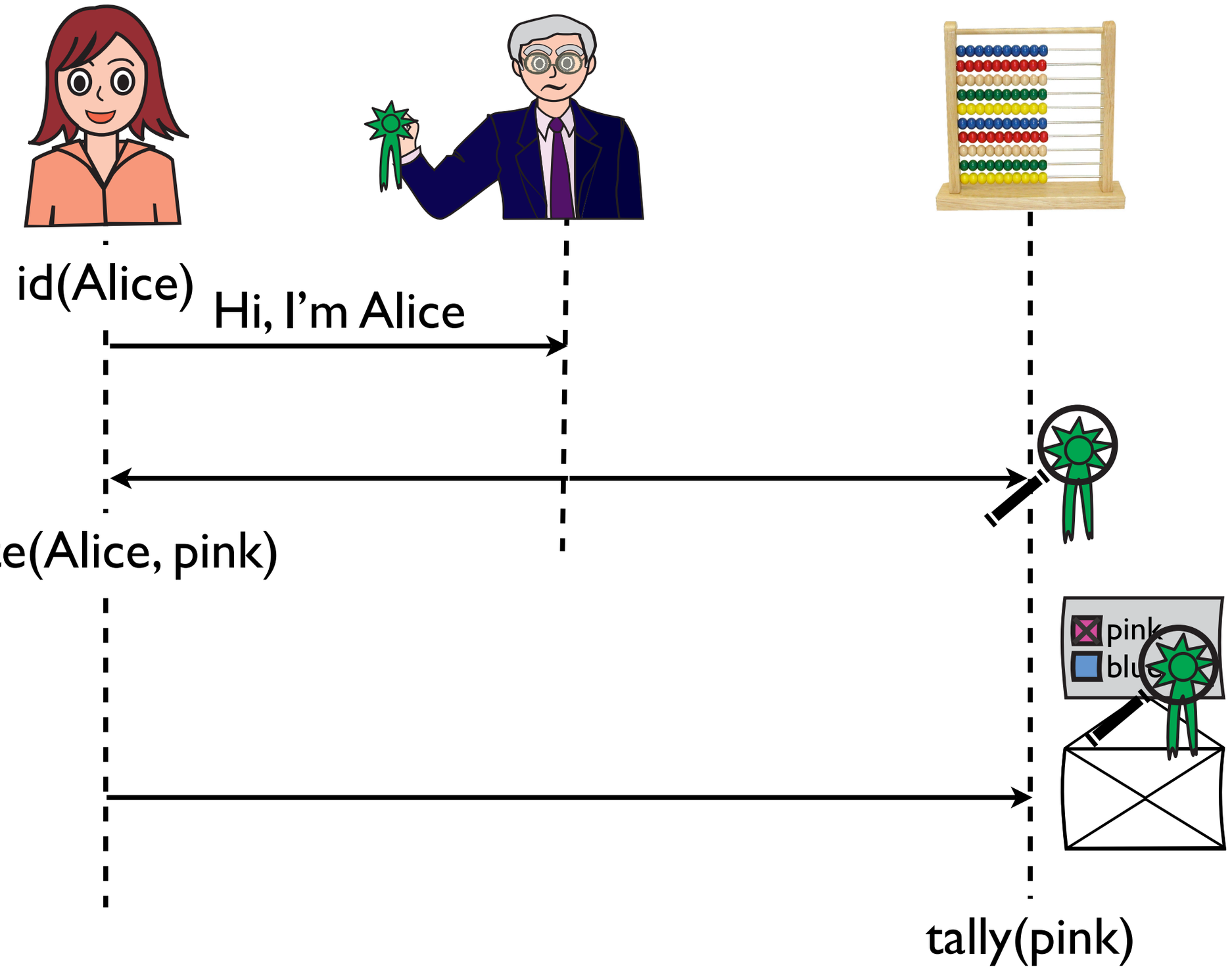



id(Alice)
Hi, I'm Alice
vote(Alice, pink)

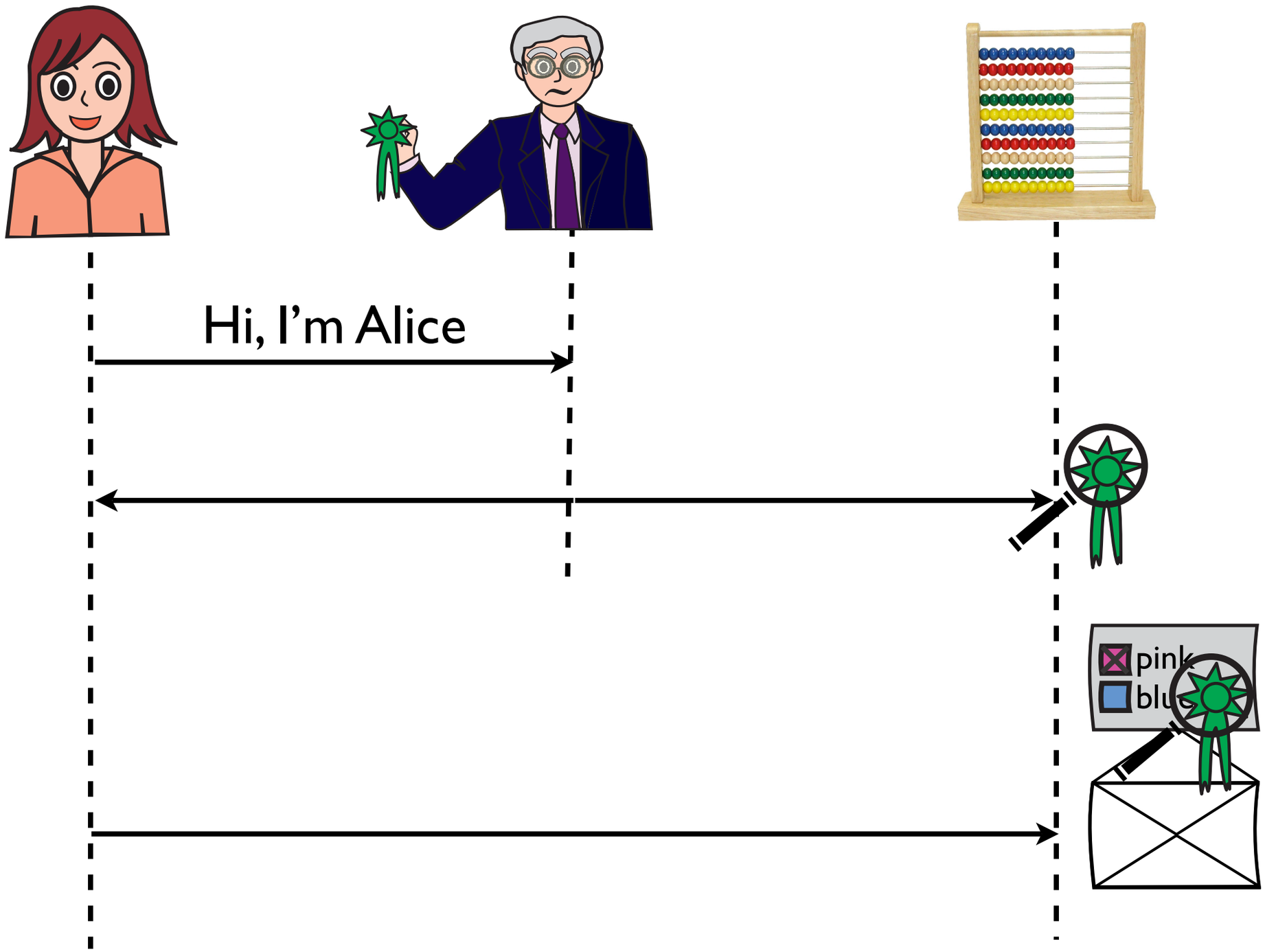

id(Alice)
Hi, I'm Alice
vote(Alice, pink)
pink
blue


id(Alice)
Hi, I'm Alice
vote(Alice, pink)
pink
blue


id(Alice)
Hi, I'm Alice
vote(Alice, pink)
pink
blue
tally(pink)

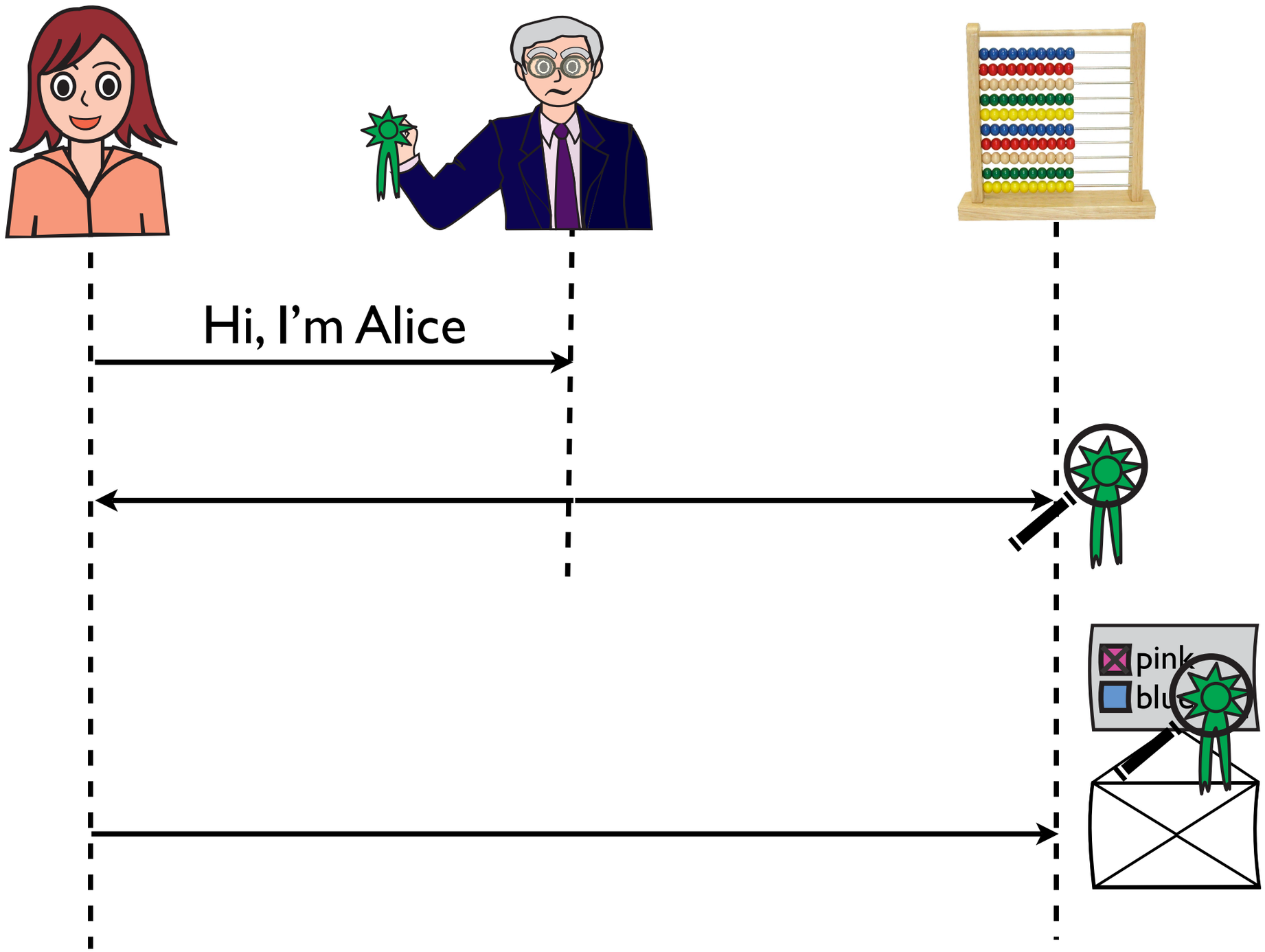


Soundness: eligibility, non-reusability, inalterability

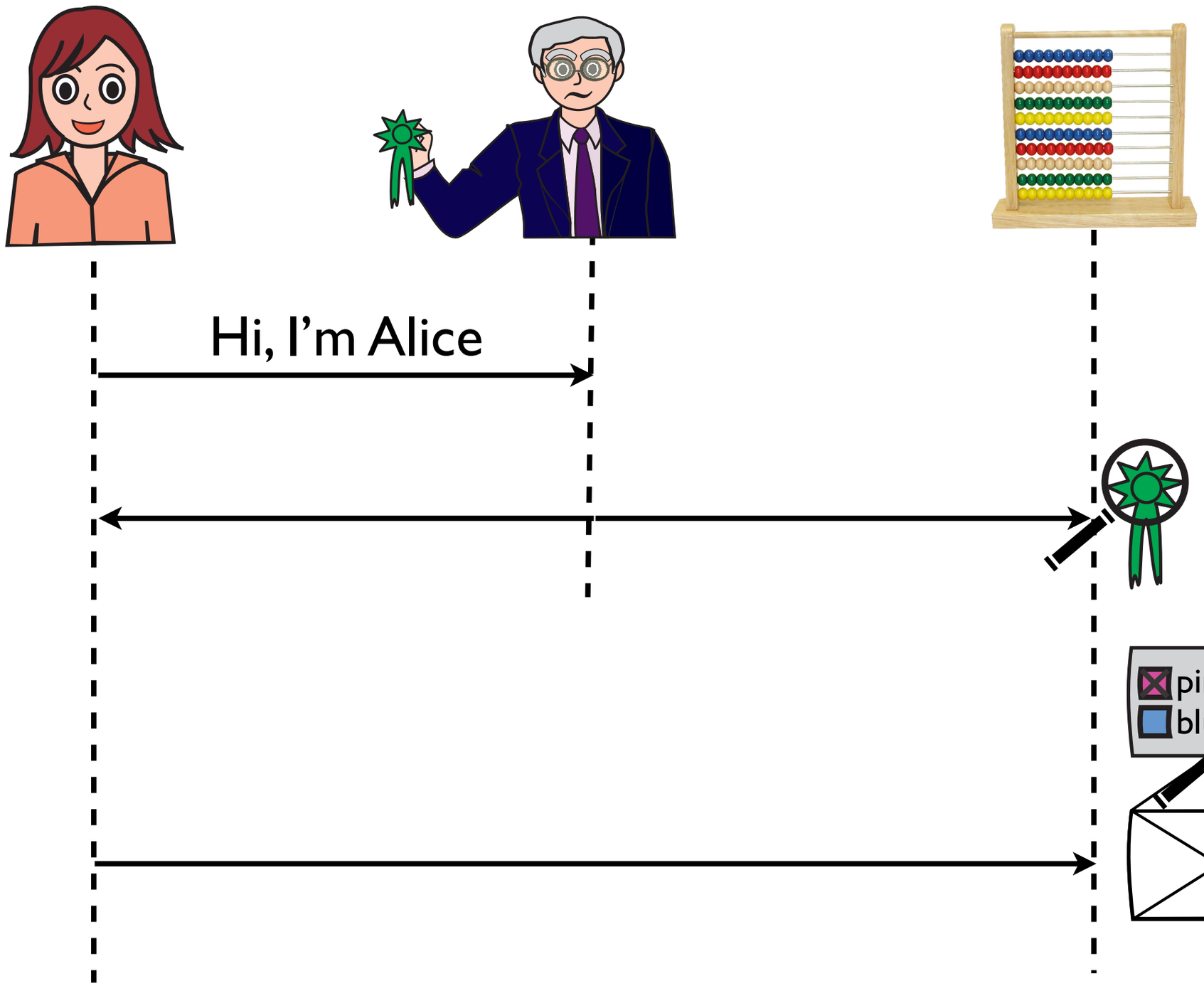


Trace: ... id(Alice) ... vote(Alice, pink) ... tally(pink)

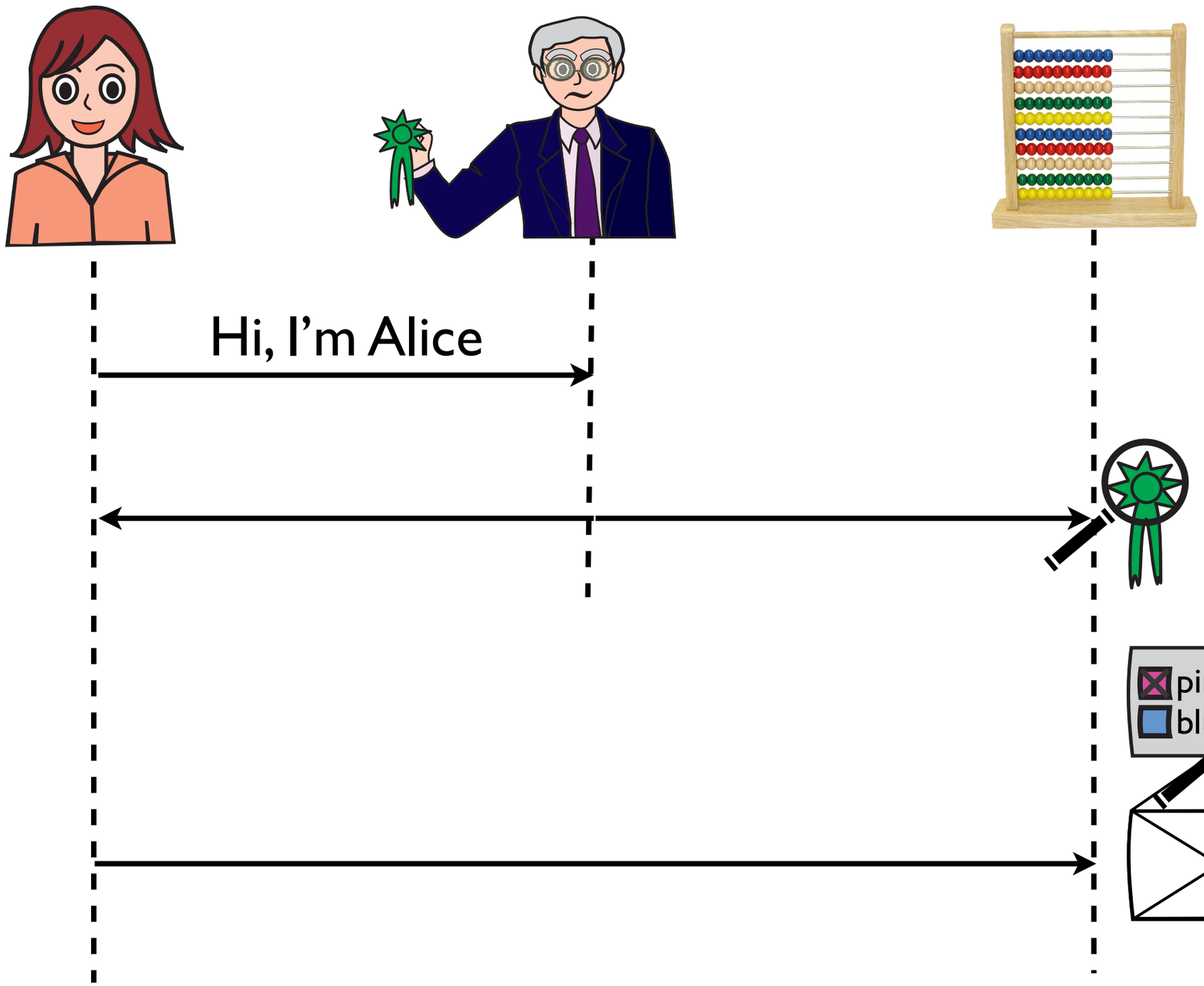
Soundness: eligibility, non-reusability, inalterability



Soundness: eligibility, non-reusability, inalterability



Soundness: eligibility, non-reusability, inalterability



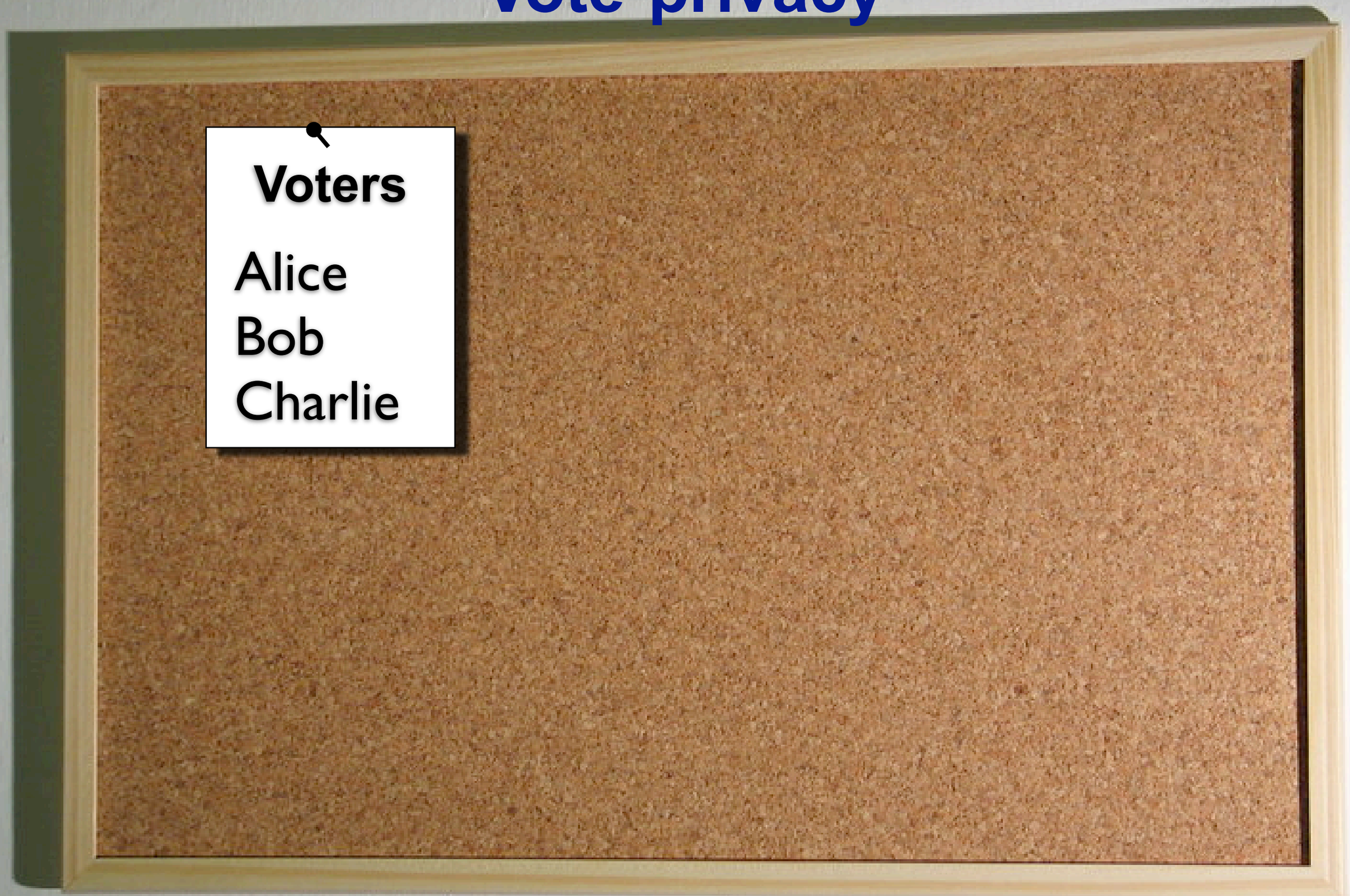
Trace: ... id(Alice) ... vote(Alice, pink) ... tally(pink)

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

$\forall \rightarrow \exists^{\leq 1}$

Soundness: eligibility, non-reusability, inalterability

Vote-privacy



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

Vote-privacy

Voters

Alice
Bob
Charlie

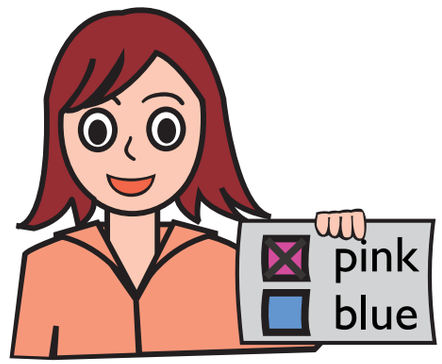
Results

pink party |
blue party ||

~~**Detailed results**~~

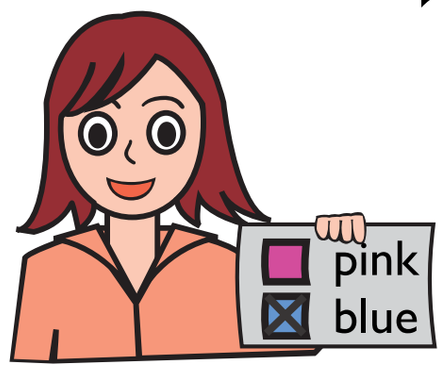
~~Alice ..... pink party~~
~~Bob ..... blue party~~
~~Charlie ..... blue party~~

Definition of vote-privacy

$S[$ 

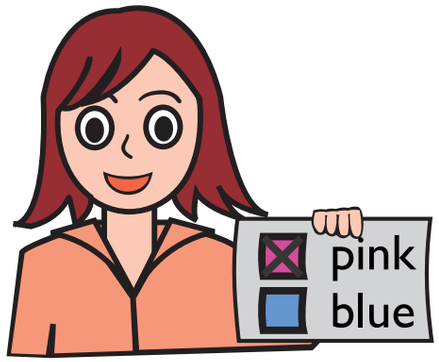
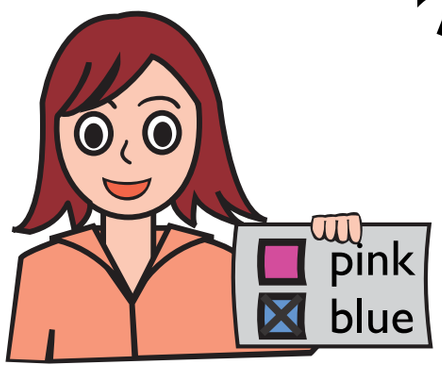
$]$

$\approx$

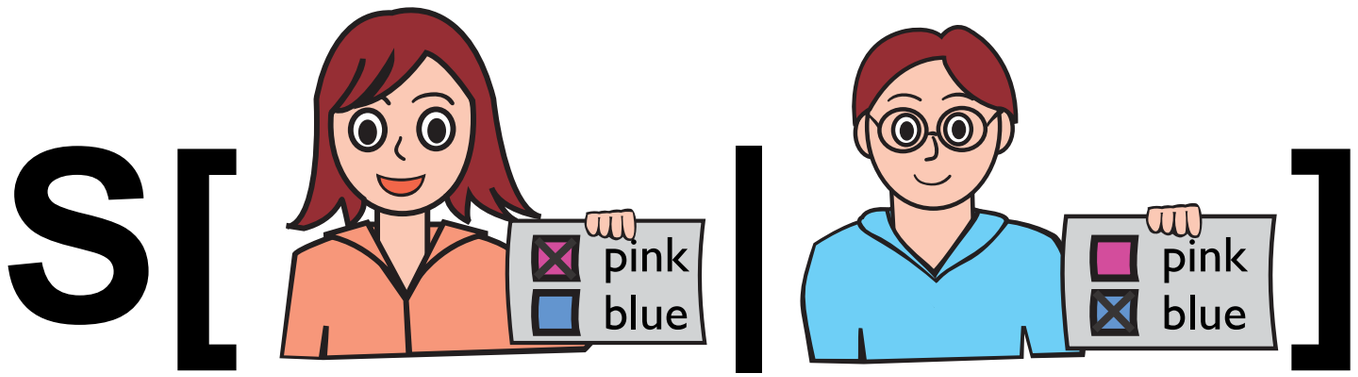
$S[$ 

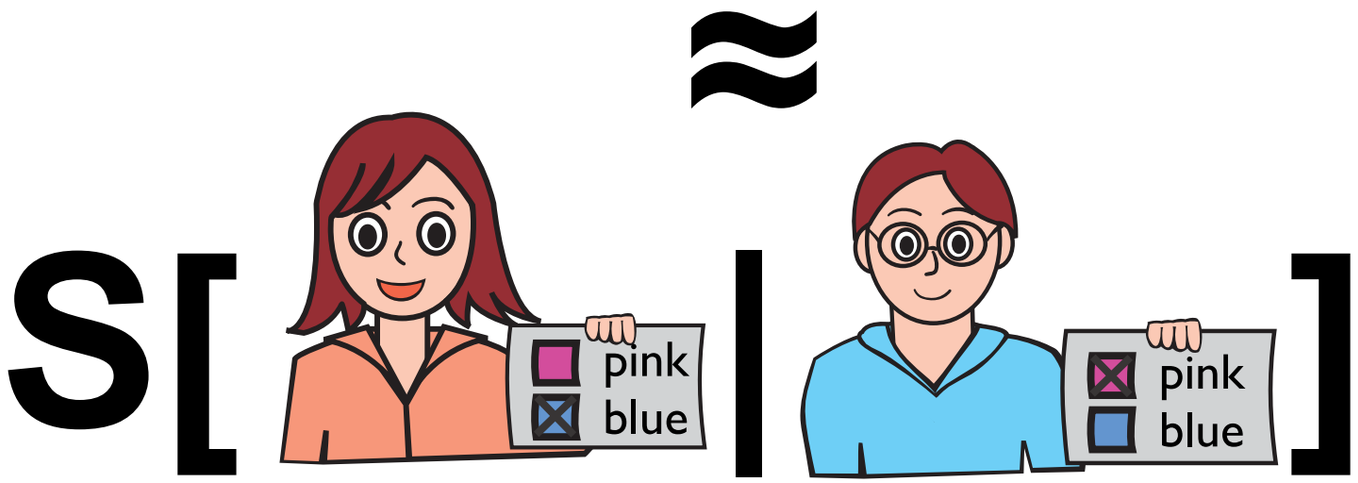
$]$

Definition of vote-privacy

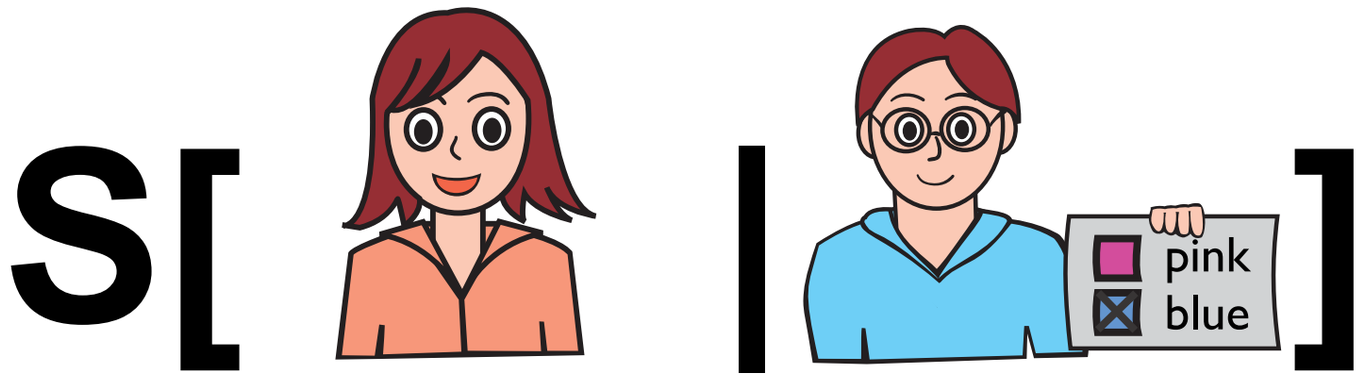
$$S[\ \text{  }\ ] \neq S[\ \text{  }\ ]$$

Definition of vote-privacy

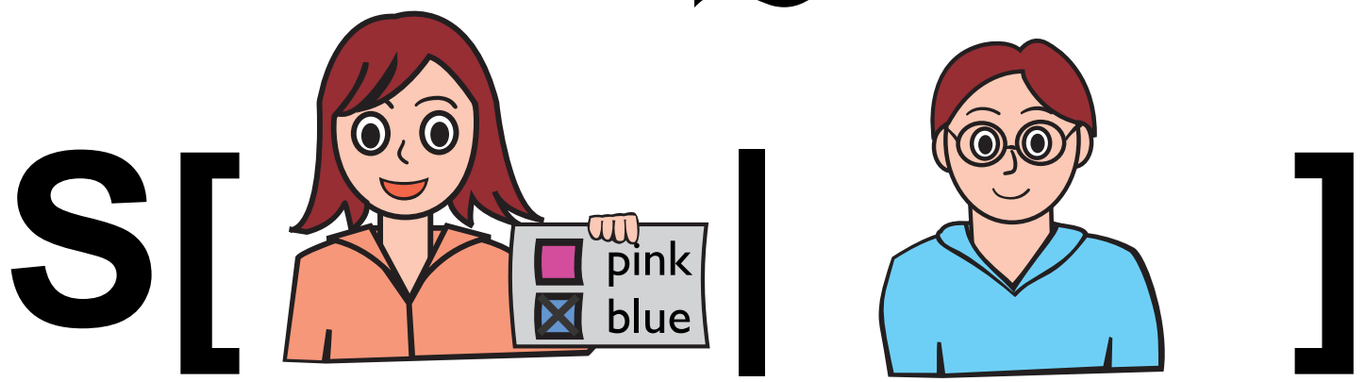




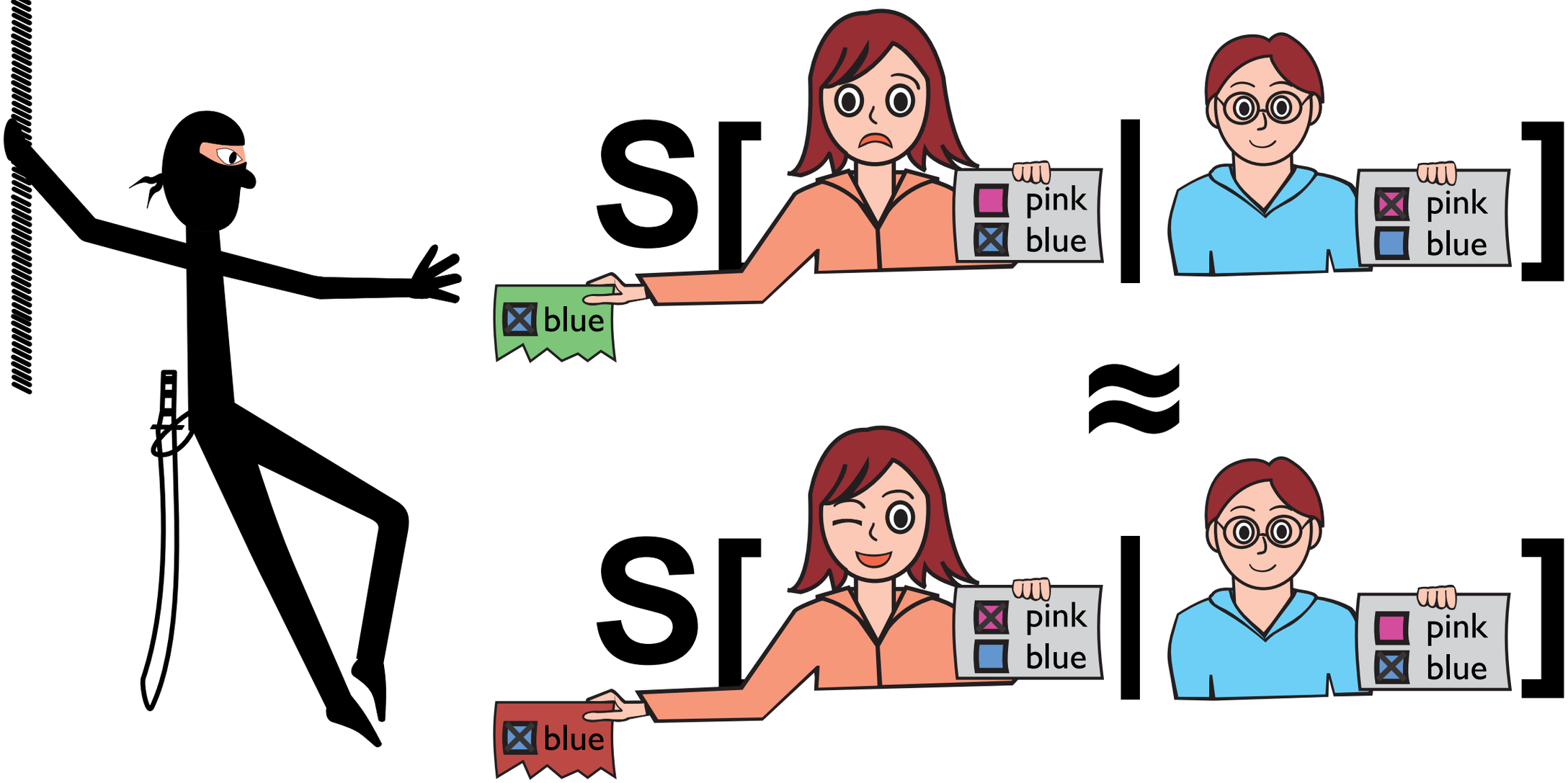
Immunity to forced-abstention



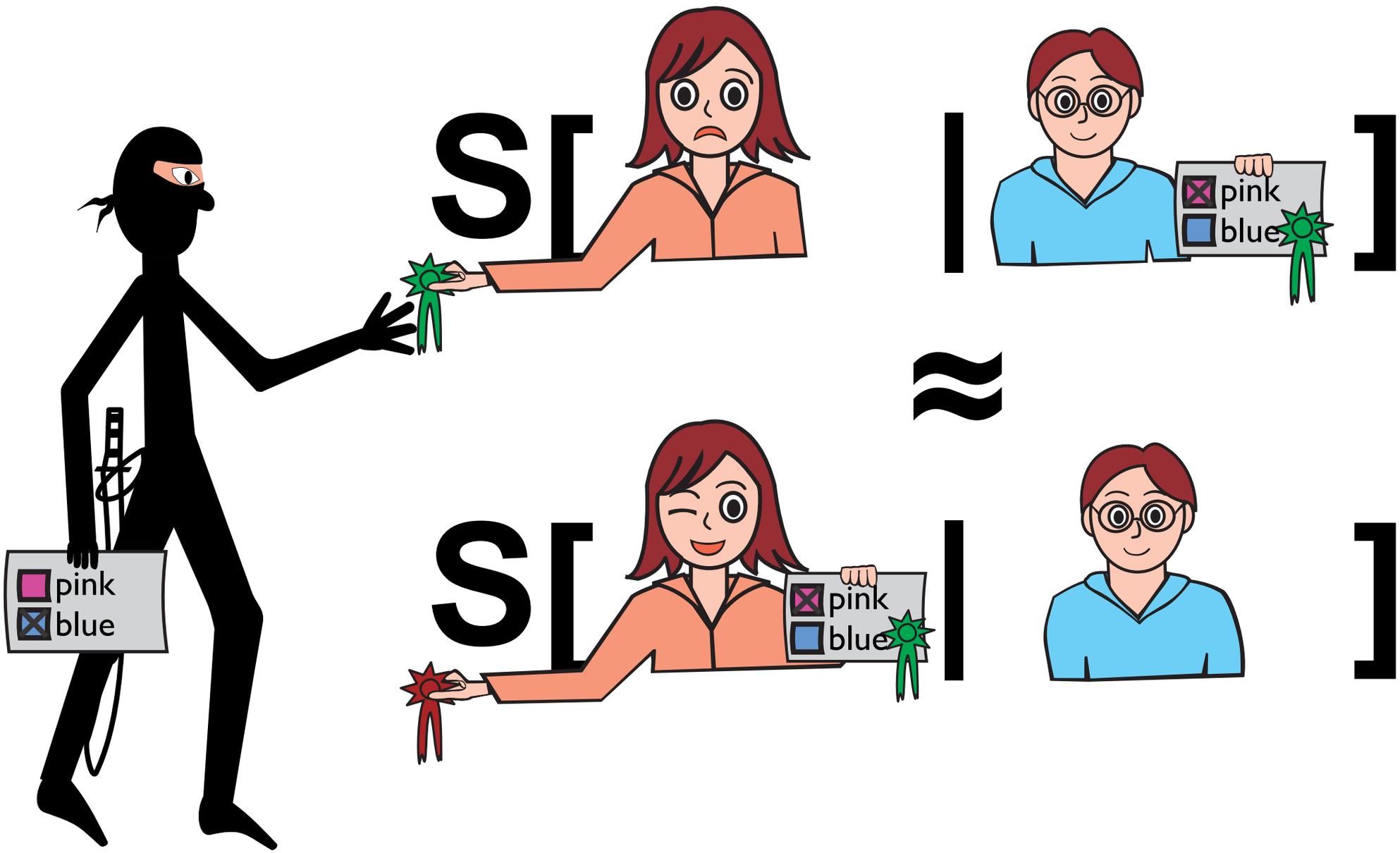
≈



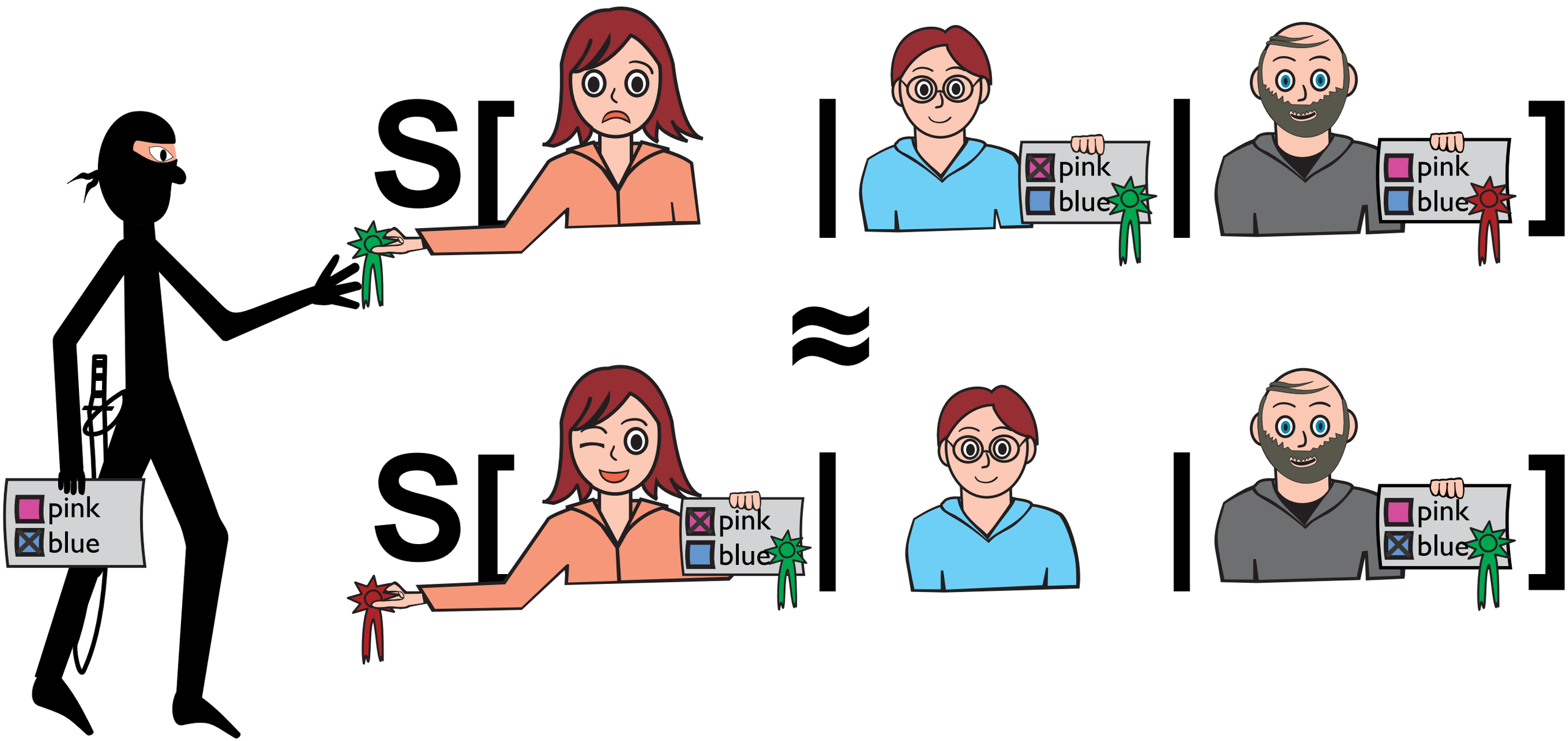
Receipt-freeness



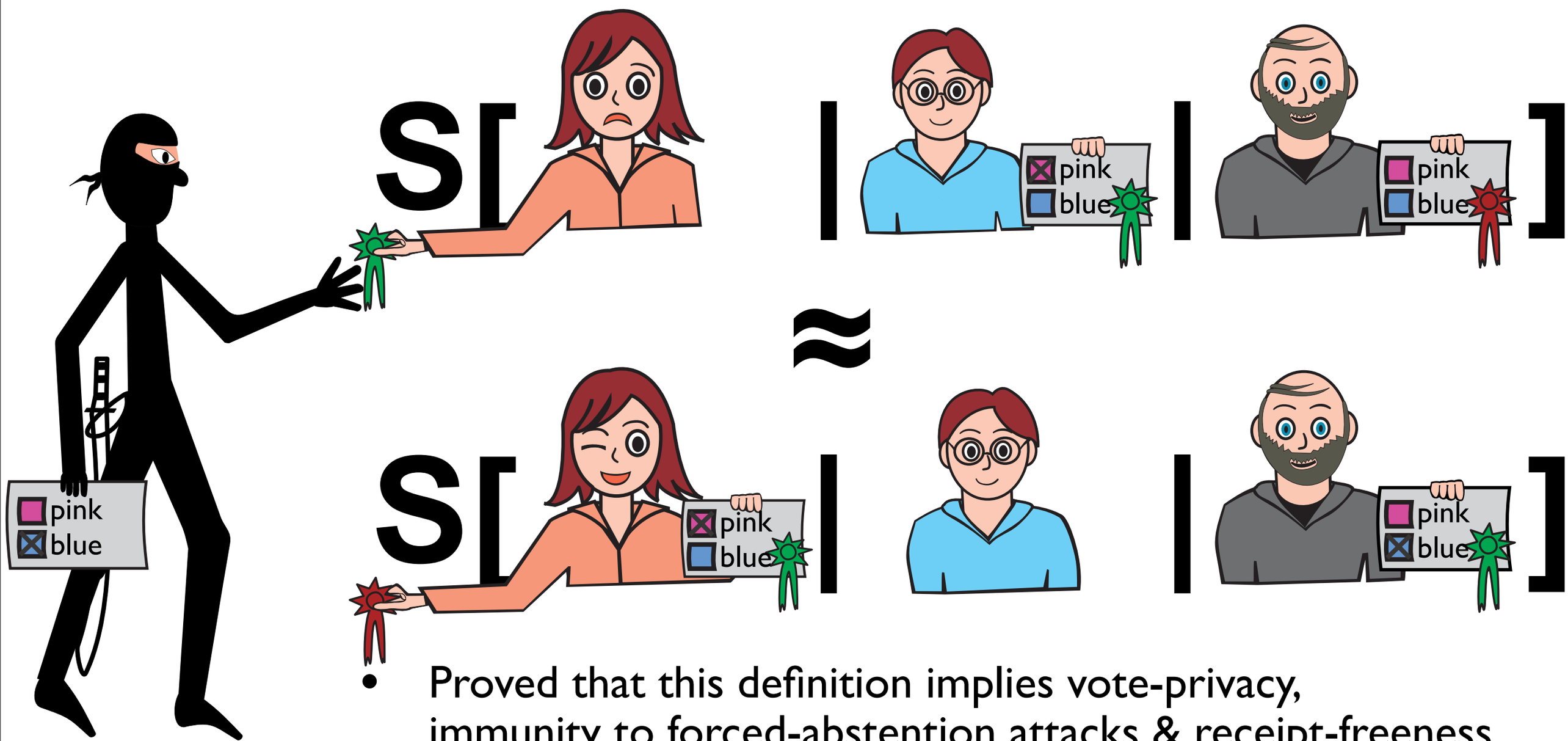
Coercion-resistance



Coercion-resistance

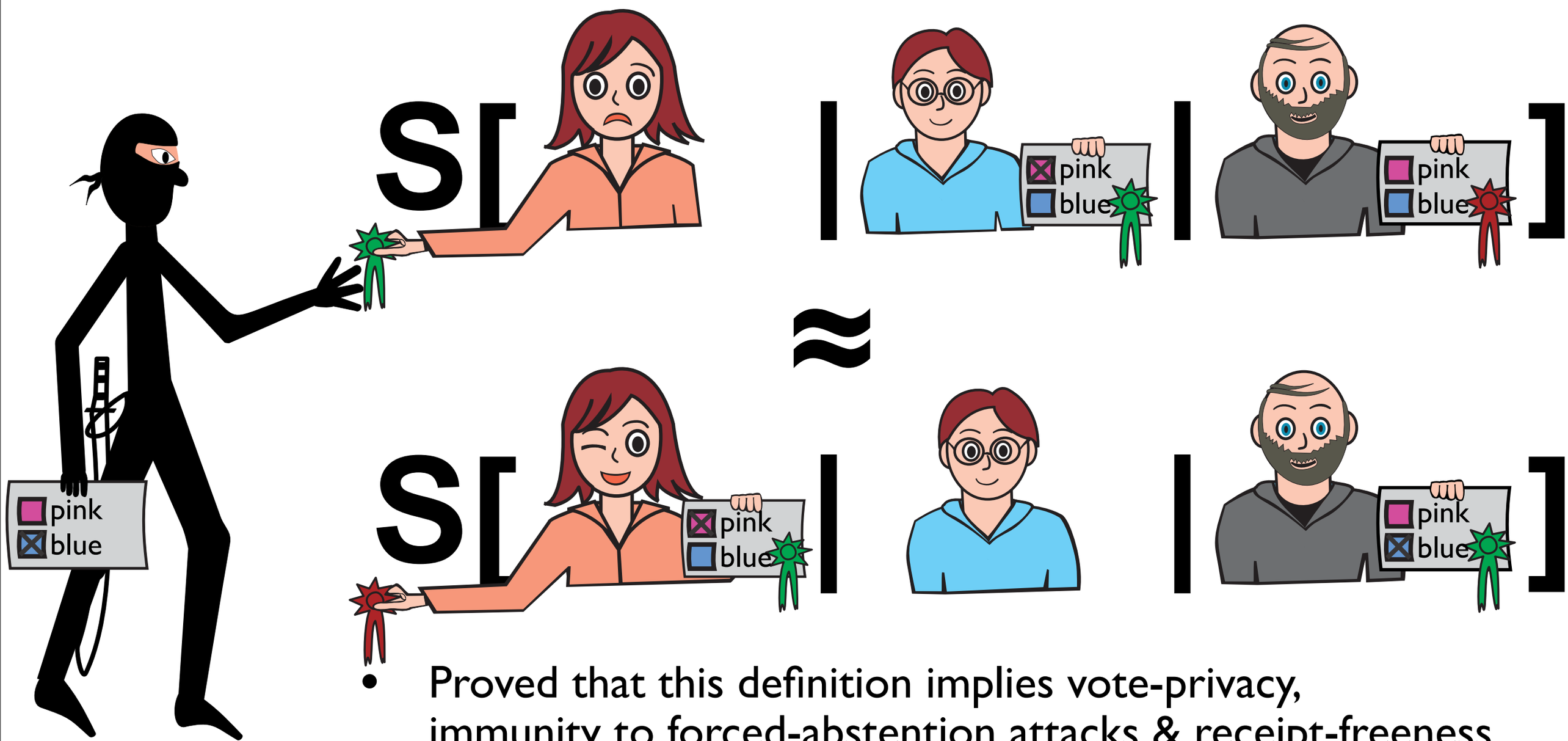


Coercion-resistance



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

Coercion-resistance



- Proved that this definition implies vote-privacy, immunity to forced-abstention attacks & receipt-freeness
- Used it to automatically analyze important protocol (JCJ)

Future work

- Analyze more protocols
  - Started with Civitas - variant of JCJ (has implementation)
- Better techniques for observational equivalence
  - for instance using symbolic bisimulation
- Analyzing other properties (in the same setting)
  - Immunity to randomization attacks (also privacy property)
  - Individual and universal verifiability
- More concrete protocol models
  - The ultimate goal would be to analyze implementations