

Automatic Verification of Remote Electronic Voting Protocols

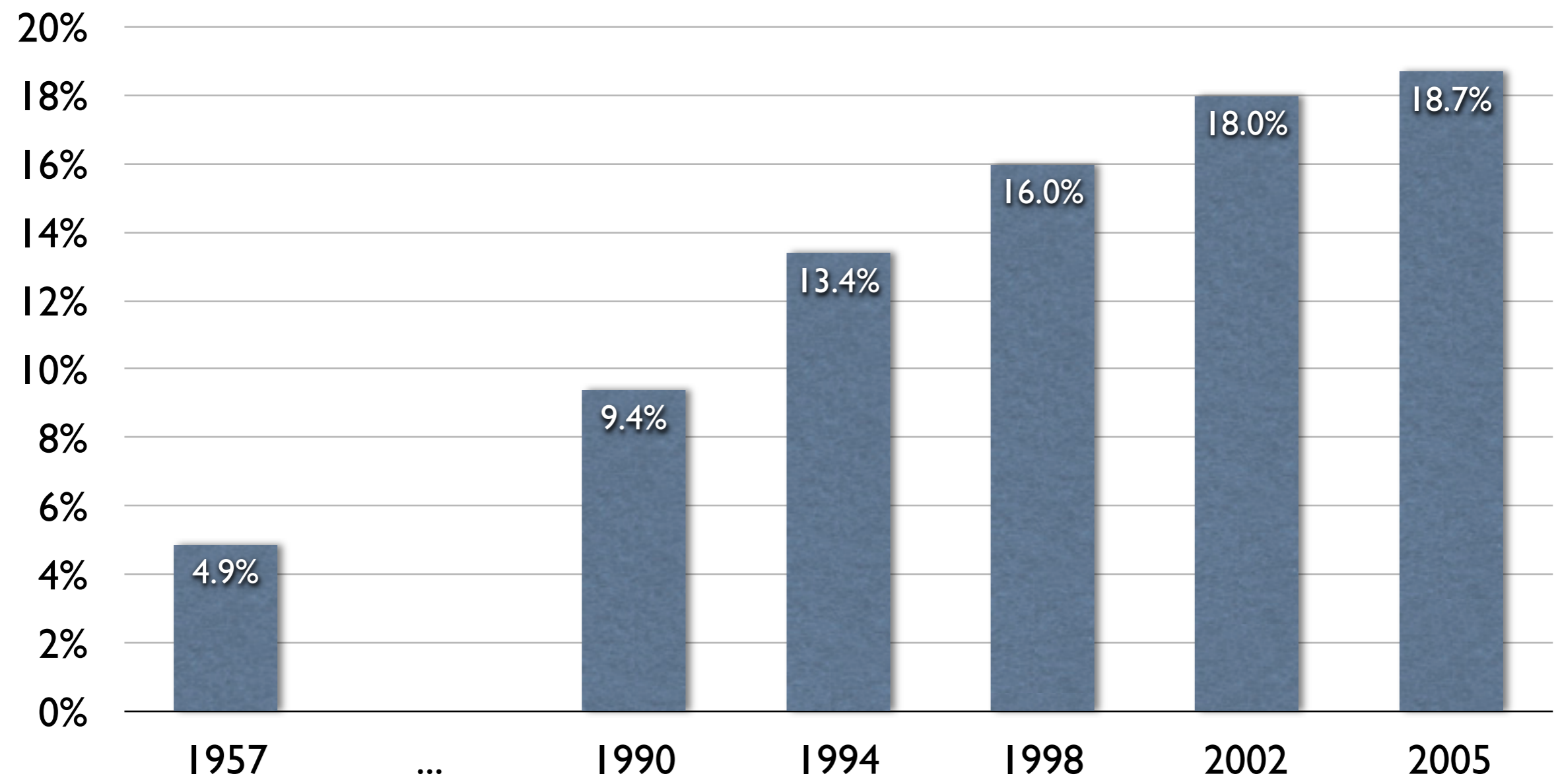
Cătălin Hrițcu

Saarland University, Saarbrücken, Germany

Joint work with: Michael Backes and Matteo Maffei

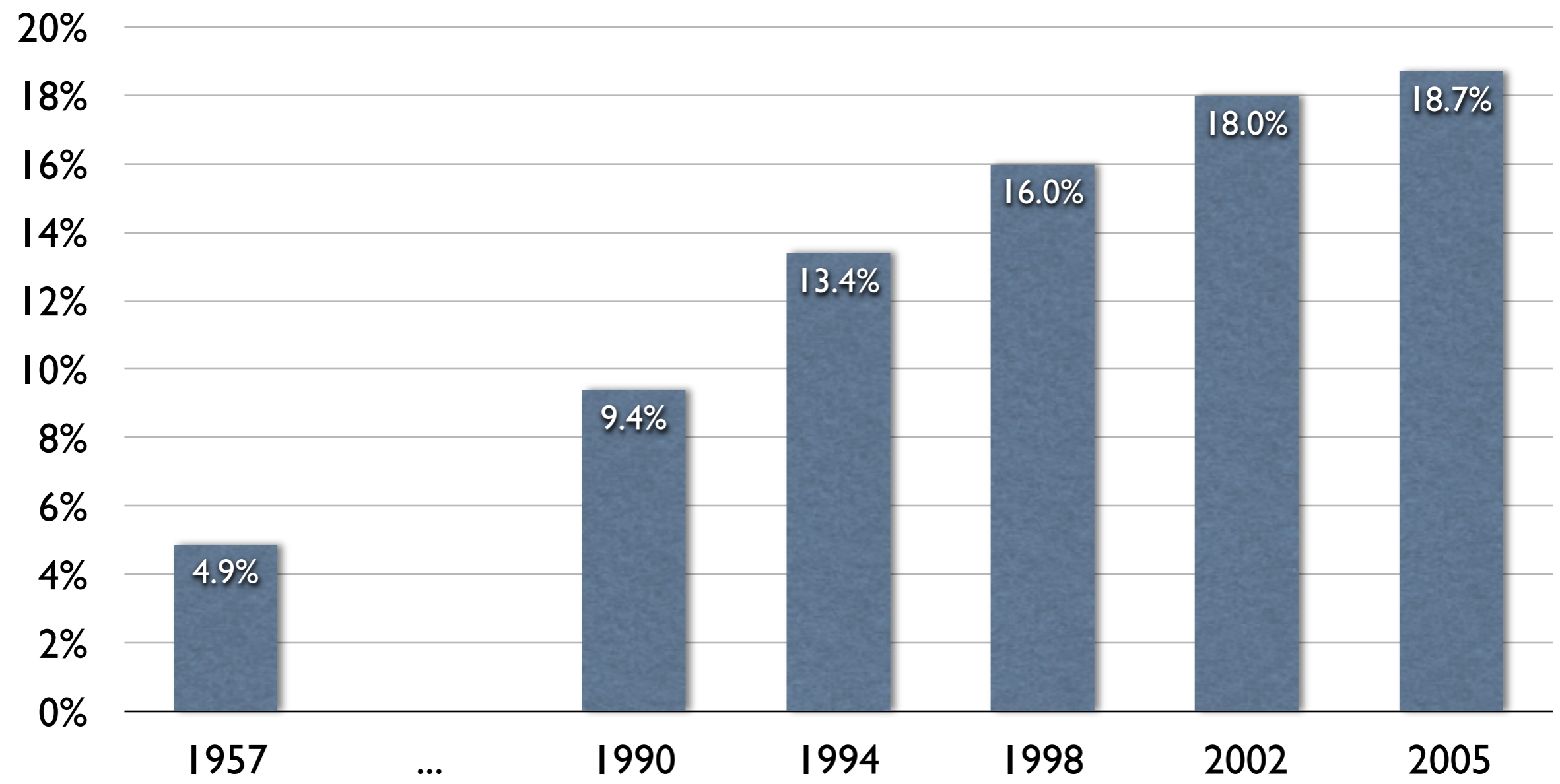
Did you know that ...

- ... 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**



STADT WÜRZBURG
WAHLAMT Würzburg

Verlorene Wahlscheine werden nicht ersetzt!

WAHLSCHHEIN für die Bundestagswahl am 18.09.2005

Nur gültig für den Wahlkreis (St. - Name) 252 - Würzburg

Wahlschein Nr. 30A / 30

Wahlerverschlüsselung: oder in Druckform ausfüllen

Zustimmendes bitte ankreuzen: oder in Druckform ausfüllen

Empfänger der Briefwahl (Name, Adresse, PLZ, Ort)

Wahlbrief

An Stadt Würzburg - Wahlamt - Rückermainstr. 2 (Rathaus) 97082 Würzburg

Wahlumschlag für die Briefwahl

Sehr geehrte Wählerin! Sehr geehrter Wähler!

Anbei erhalten Sie die Unterlagen für die Wahl zum 16. Deutschen Bundestag in dem auf dem Wahlumschlag bezeichneten Wahlkreis.

- den Wahlschein,
- den amtlichen weißen Stimmzettel,
- den amtlichen blauen Wahlumschlag,
- den amtlichen roten Wahlbriefumschlag.

Sie können an der Wahl teilnehmen

- gegen **Abgabe des Wahlscheines** und unter Vorlage eines amtlichen Personalausweises oder Reisepasses durch **Stimmabgabe im Wahlraum** in einem beliebigen Wahlbezirk des auf dem Wahlumschlag bezeichneten Wahlkreises
- gegen **Einreichung des Wahlscheines** an die für Sie zuständige, auf dem Wahlbriefumschlag angegebene Stelle des auf dem Wahlschein bezeichneten Wahlkreises durch **Briefwahl**.

Nach § 14 Abs. 4 des Bundeswahlgesetzes darf jeder Wahlberechtigte sein Wahlrecht nur einmal und nur persönlich ausüben. Wer unzulässig wählt oder sonst ein unrichtiges Ergebnis einer Wahl herbeiführt oder das Ergebnis verfälscht oder eine solche Tat versucht, wird nach § 107a Abs. 1 und 3 des Strafgesetzbuches mit Freiheitsstrafe bis zu 5 Jahren oder mit Geldstrafe bestraft.

Sie berücksichtigen **Wichtige Hinweise für Briefwähler** und umseitigen **Wegweiser für die Briefwahl**, genau beachten.

Wichtige Hinweise für Briefwähler

Die Stimmabgabe bei der Briefwahl ist nur gültig, wenn in der unteren Hälfte des Wahlscheines die **„Versicherung an Eides statt zur Briefwahl“** mit der Unterschrift versehen ist.

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) - maßgebende Stimme für die Verteilung der Sitze insgesamt auf die einzelnen Parteien -

Erststimme

1	Lehrbinder, Friedl	CSU	<input type="radio"/>
2	Kollbow, Walter	SPD	<input type="radio"/>
3	Friedl, Patrick	GRÜNE	<input type="radio"/>
4	Kracht, Moritz	FDP	<input type="radio"/>
5	Seifert, Berthold	REP	<input type="radio"/>
6	Brechbildner, Beinda	DIE LINKE	<input type="radio"/>
7	Meenen, Uwe	NPD	<input type="radio"/>
8	Huth, Adelheid	MLPD	<input type="radio"/>

Zweitstimme

1	CSU	Christlich-Sozialer Union in Bayern e.V.	<input type="radio"/>
2	SPD	Sozialdemokratische Partei Deutschlands	<input type="radio"/>
3	GRÜNE	BÜNDNIS 90/DIE GRÜNEN	<input type="radio"/>
4	FDP	Freie Demokratische Partei	<input type="radio"/>
5	REP	DIE REPUBLIKANER	<input type="radio"/>
6	DIE LINKE	DIE LINKE	<input type="radio"/>
7	NPD	Nationaldemokratische Partei Deutschlands	<input type="radio"/>
8	PBC	Partei Bibeltreuer Christen	<input type="radio"/>
9	BP	Bayerpartei	<input type="radio"/>
10	DIE FRAUEN	Feministische Partei DIE FRAUEN	<input type="radio"/>
11	GRAUE	DIE GRAUEN - Graue Panther	<input type="radio"/>
12	BüSo	Bürgerrechtsbewegung Solidarität	<input type="radio"/>
13	FAMILIE	FAMILIEN-PARTEI DEUTSCHLANDS	<input type="radio"/>
14	MLPD	Marxistisch-Leninistische Partei Deutschlands	<input type="radio"/>

Remote voting (by post)

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

Remote voting (by post)

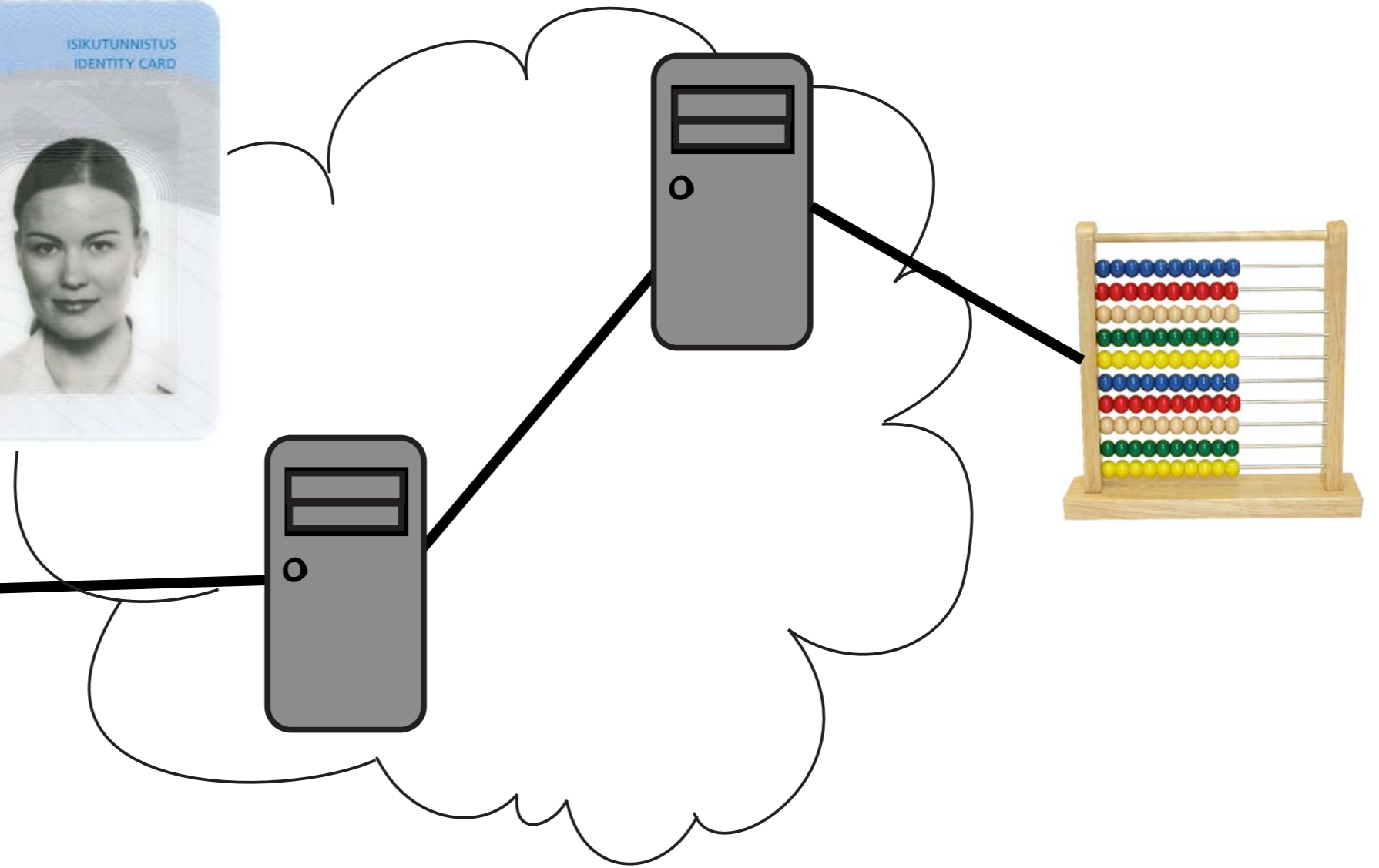
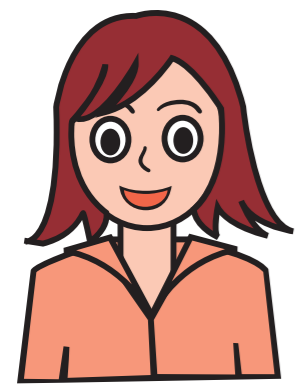
- More convenient than supervised voting
 - ▶ This should increase voter participation
- Voting by post raises many **security concerns**
 - ▶ An autograph signature does not authenticate the voter
 - ▶ An envelope does not guarantee secrecy or integrity
 - ▶ The post is not always a secure channel
 - ▶ 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

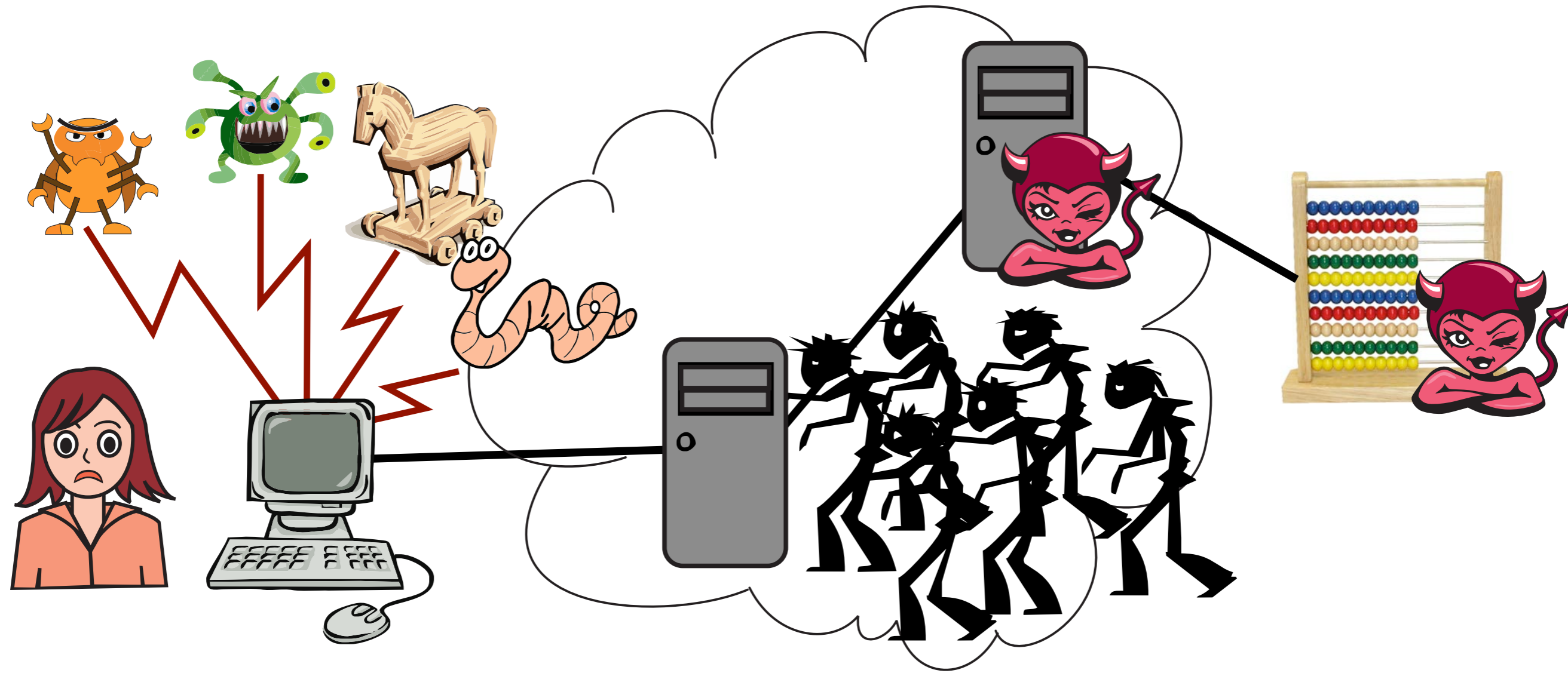
Remote electronic voting

- 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

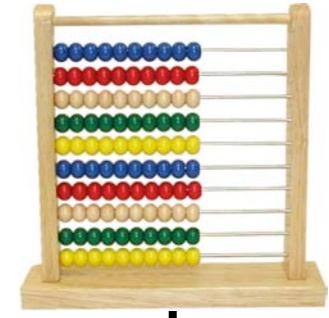
What we did

- 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

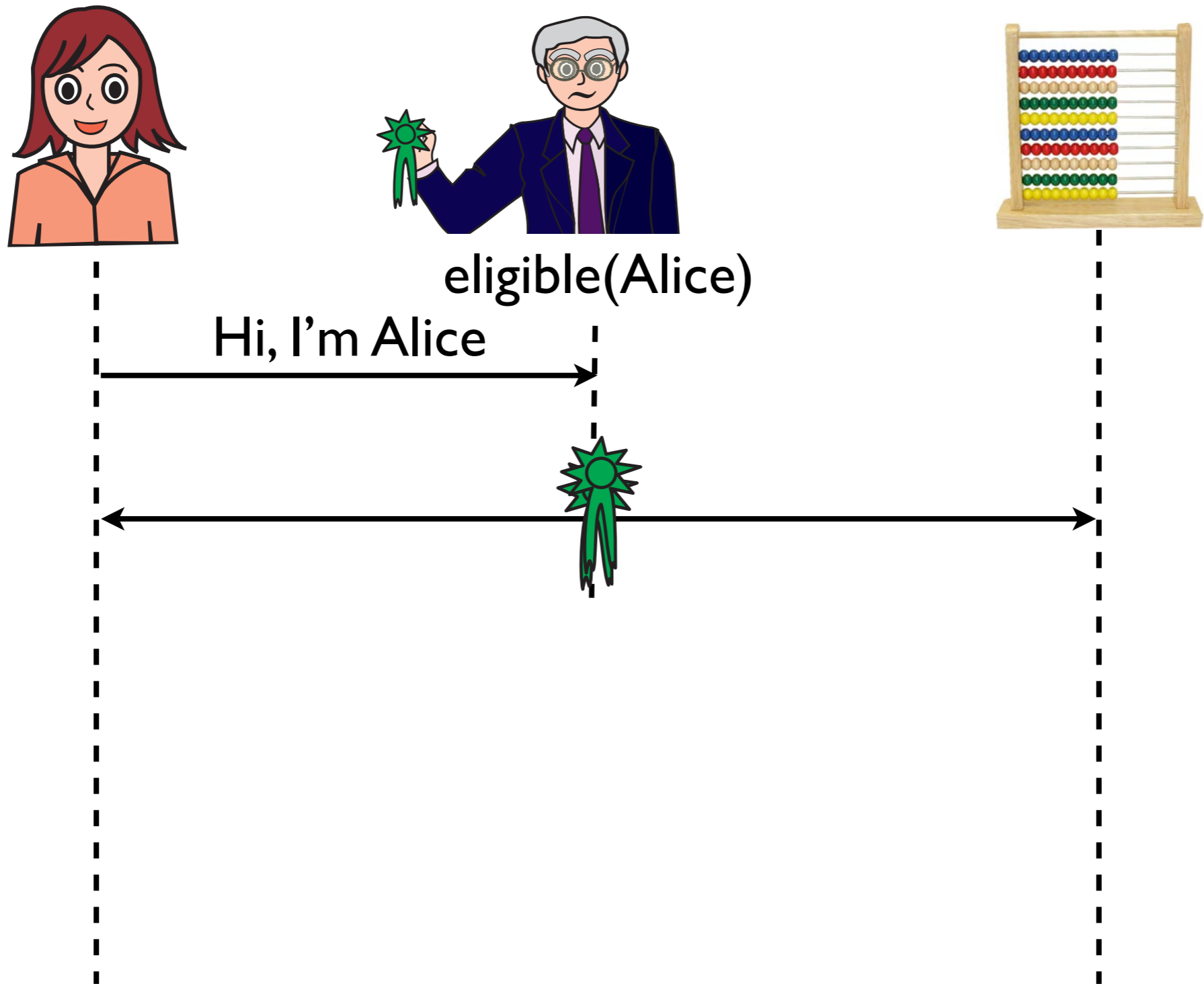


Soundness (eligibility, non-reusability, inalterability)

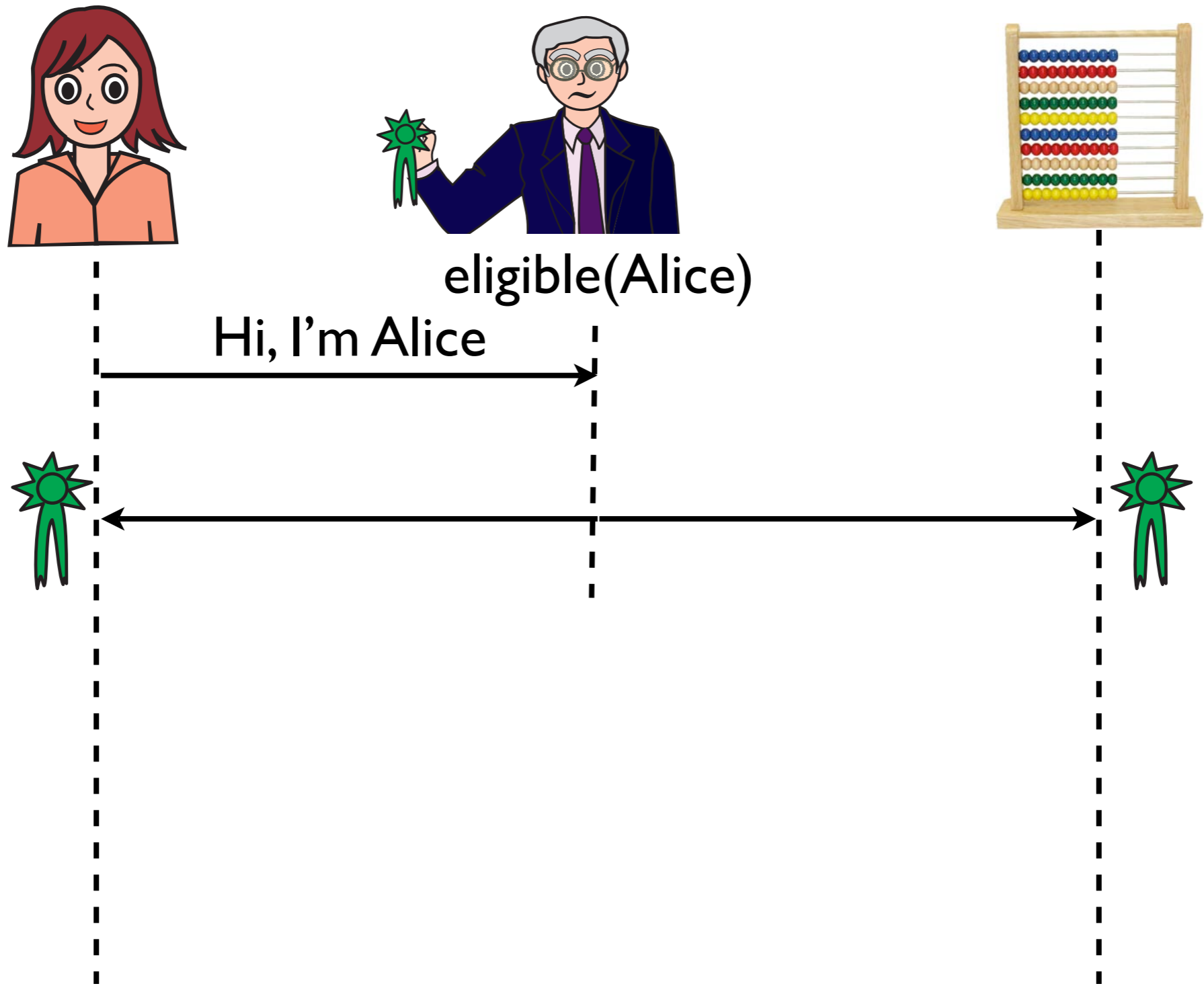


Hi, I'm Alice

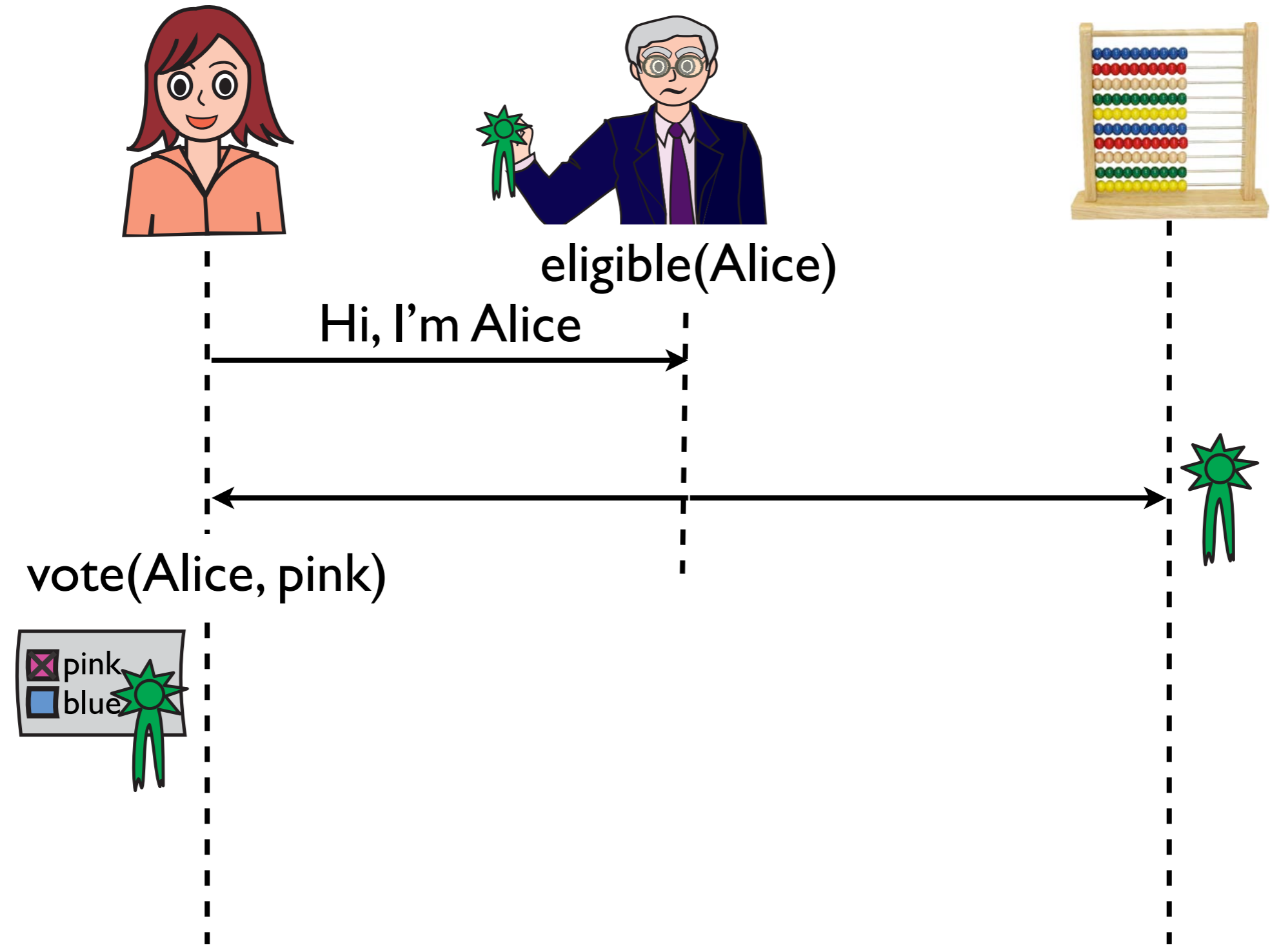
Soundness (eligibility, non-reusability, inalterability)



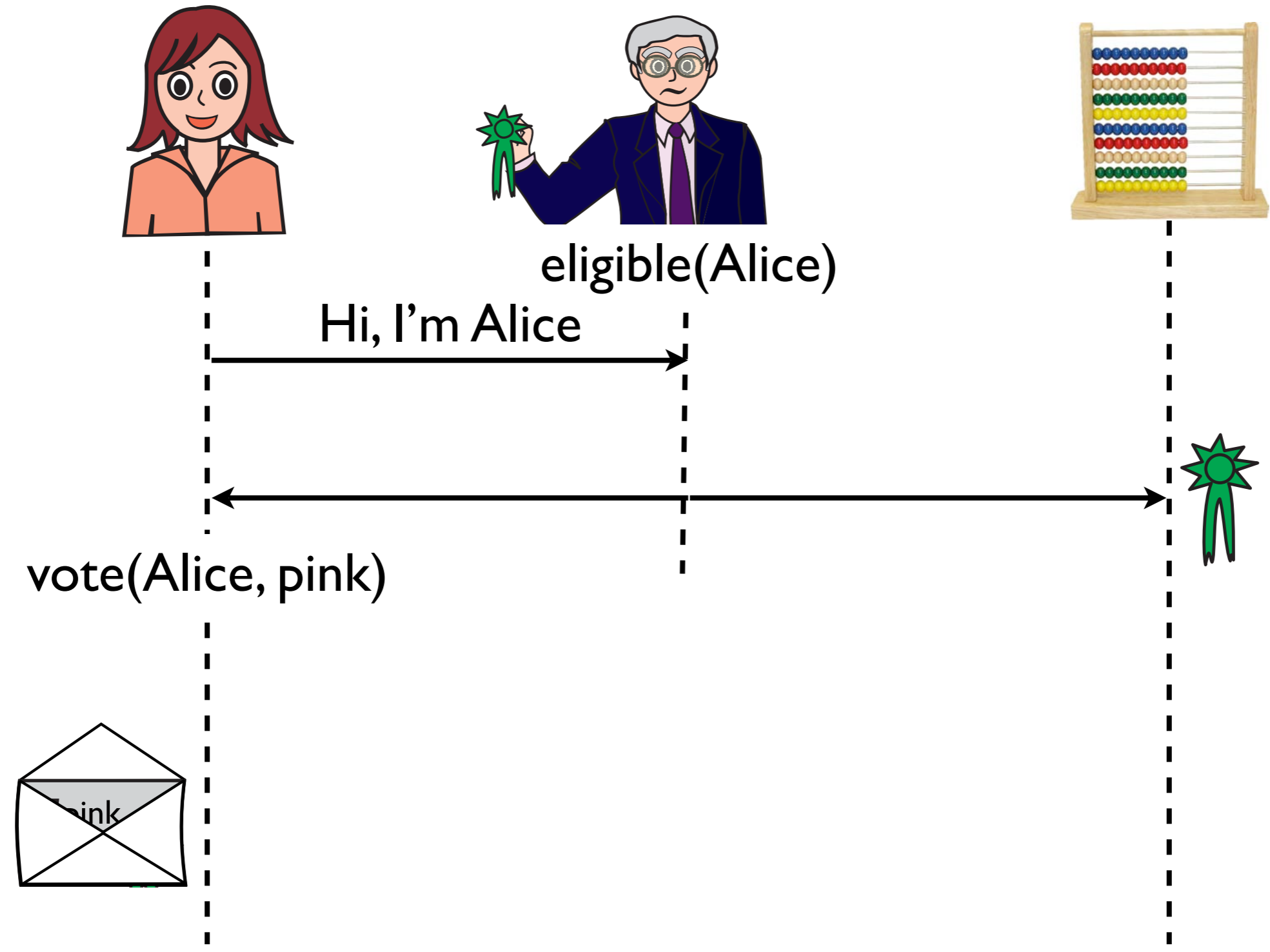
Soundness (eligibility, non-reusability, inalterability)



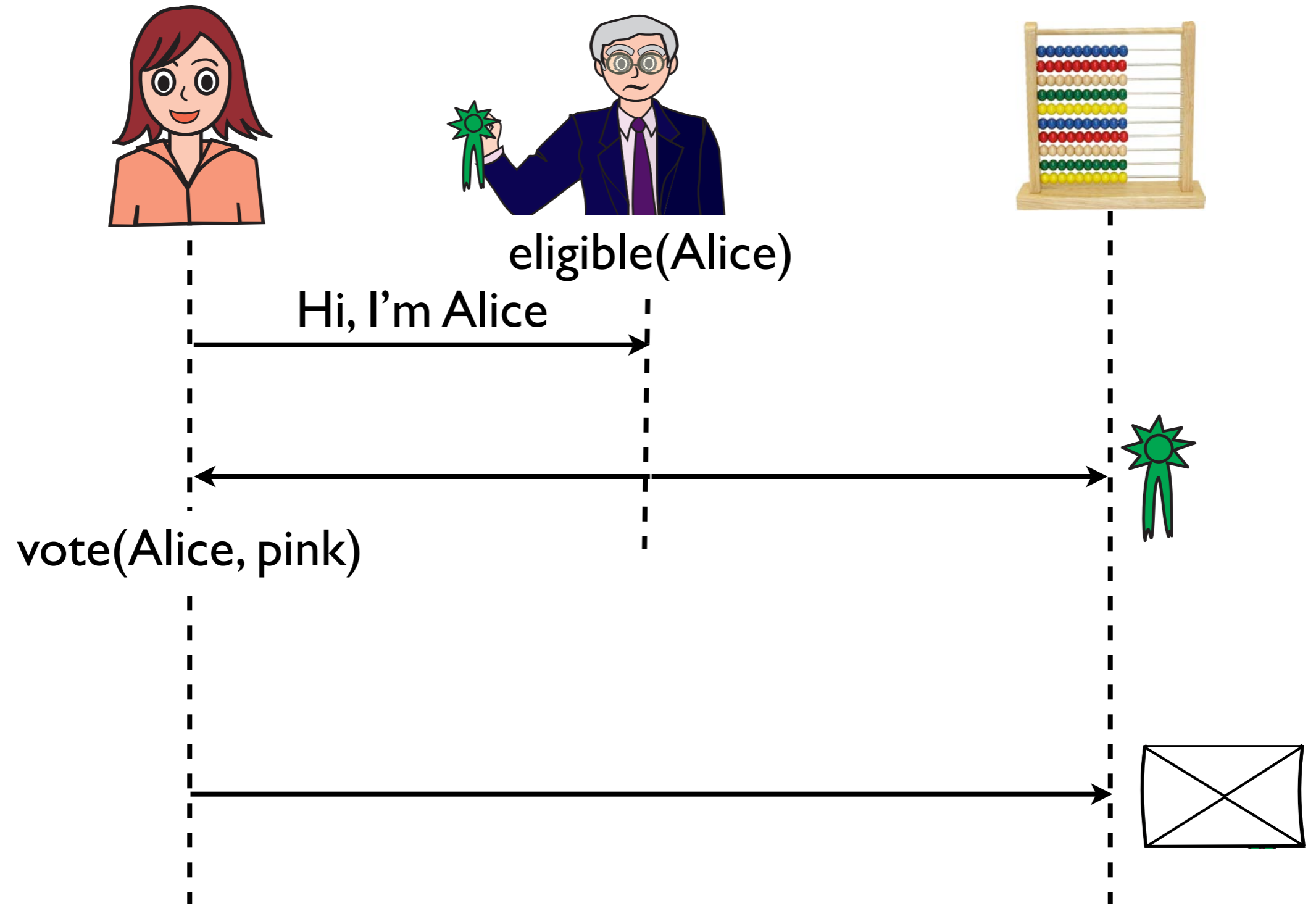
Soundness (eligibility, non-reusability, inalterability)



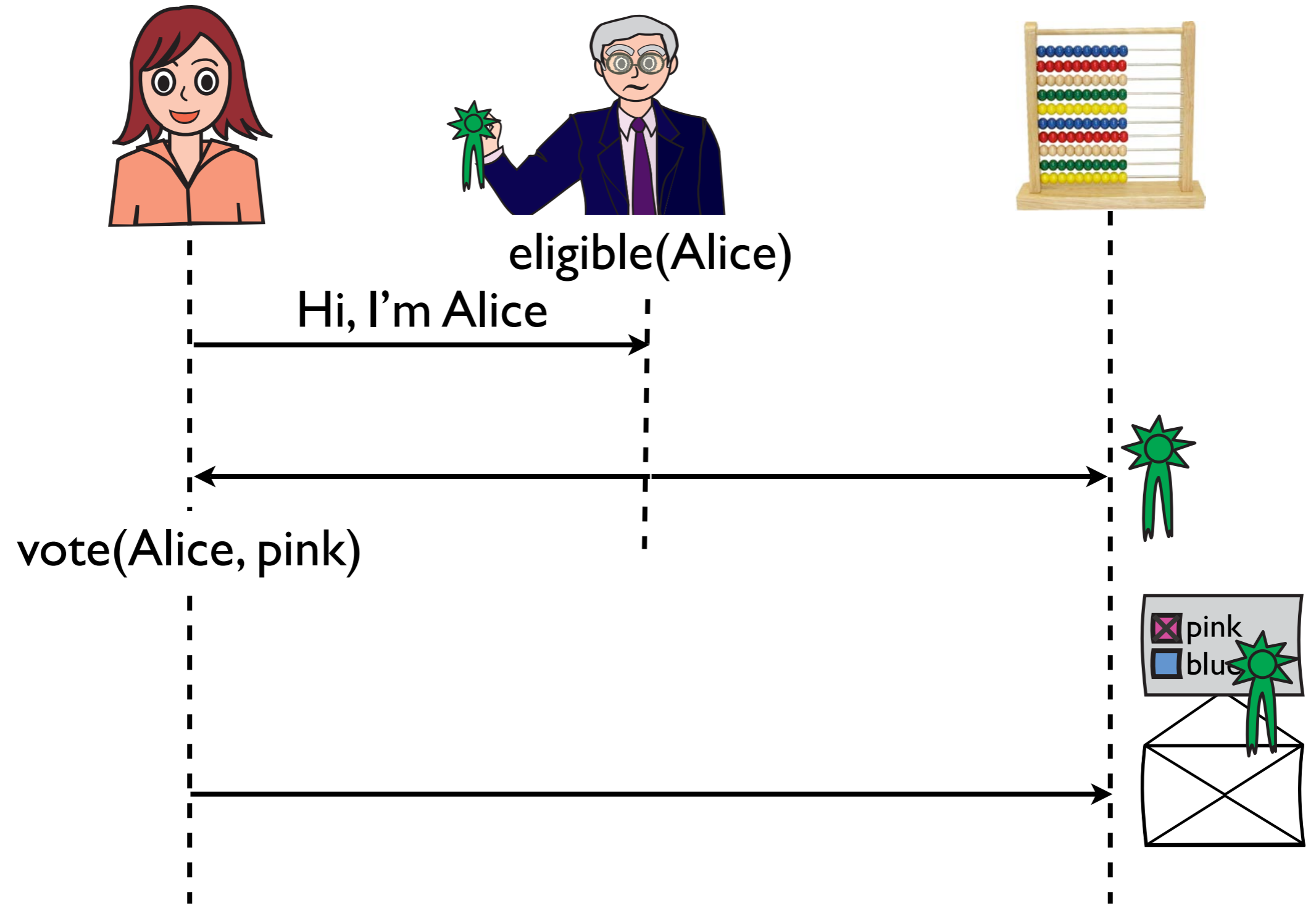
Soundness (eligibility, non-reusability, inalterability)



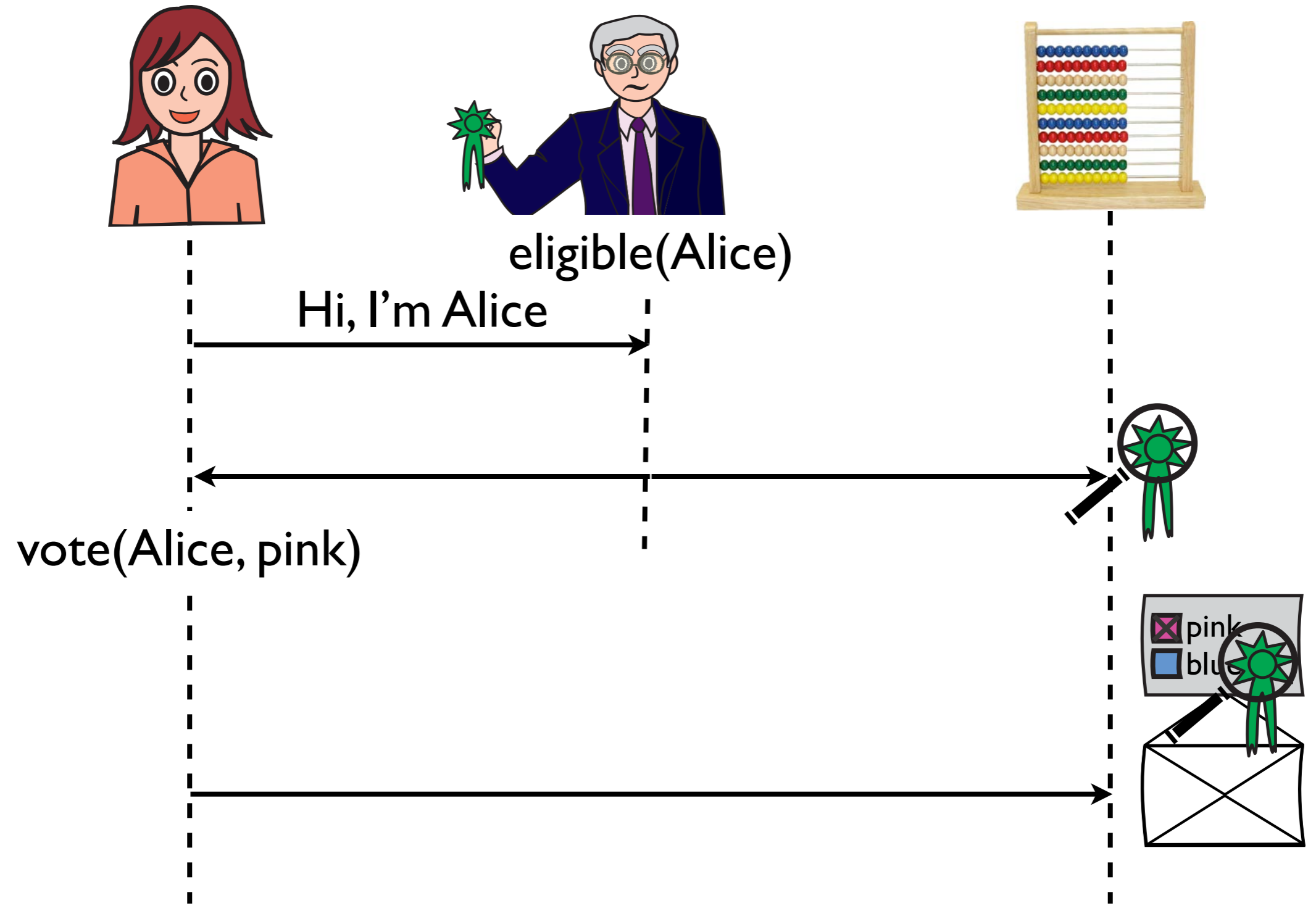
Soundness (eligibility, non-reusability, inalterability)



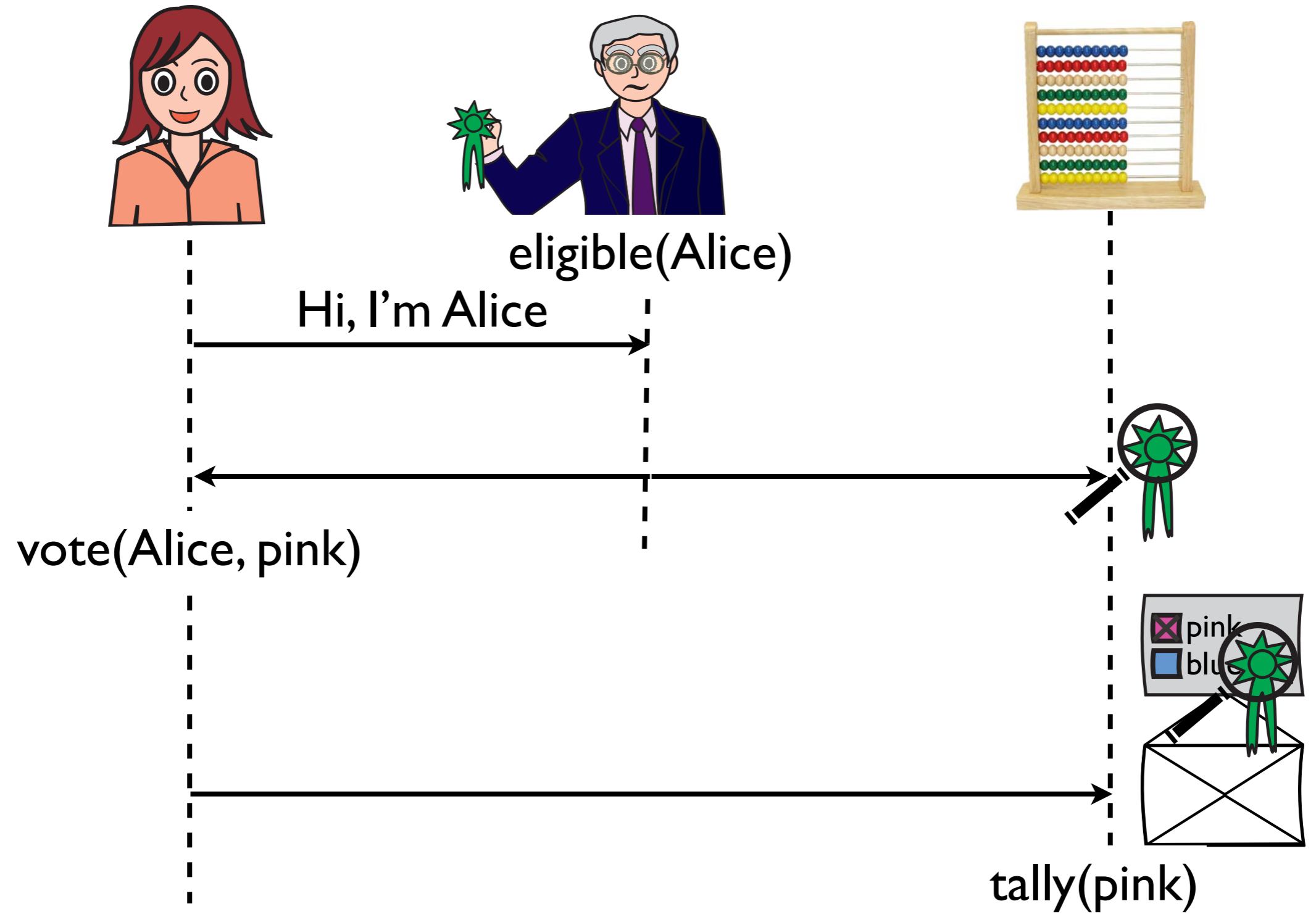
Soundness (eligibility, non-reusability, inalterability)



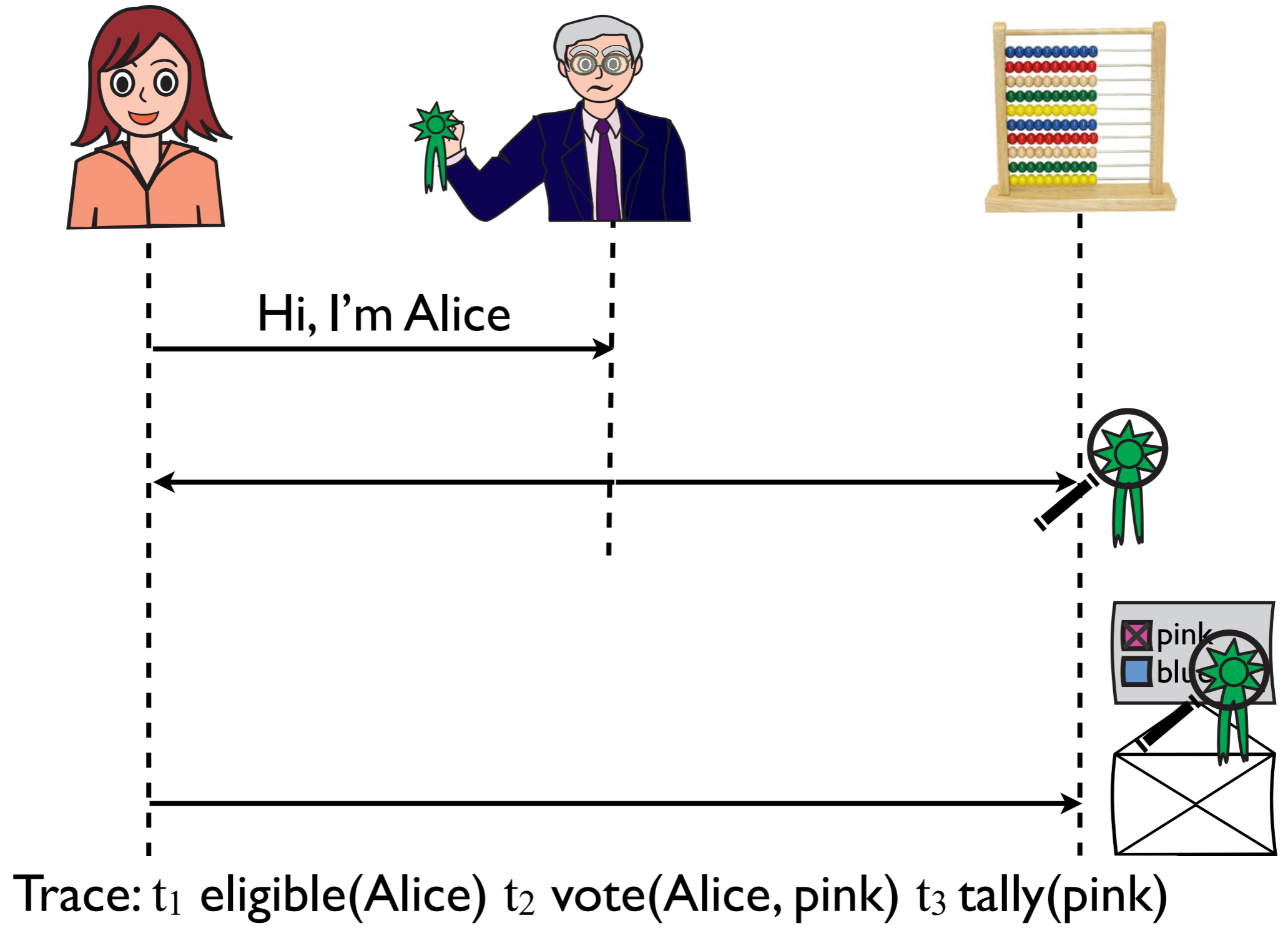
Soundness (eligibility, non-reusability, inalterability)



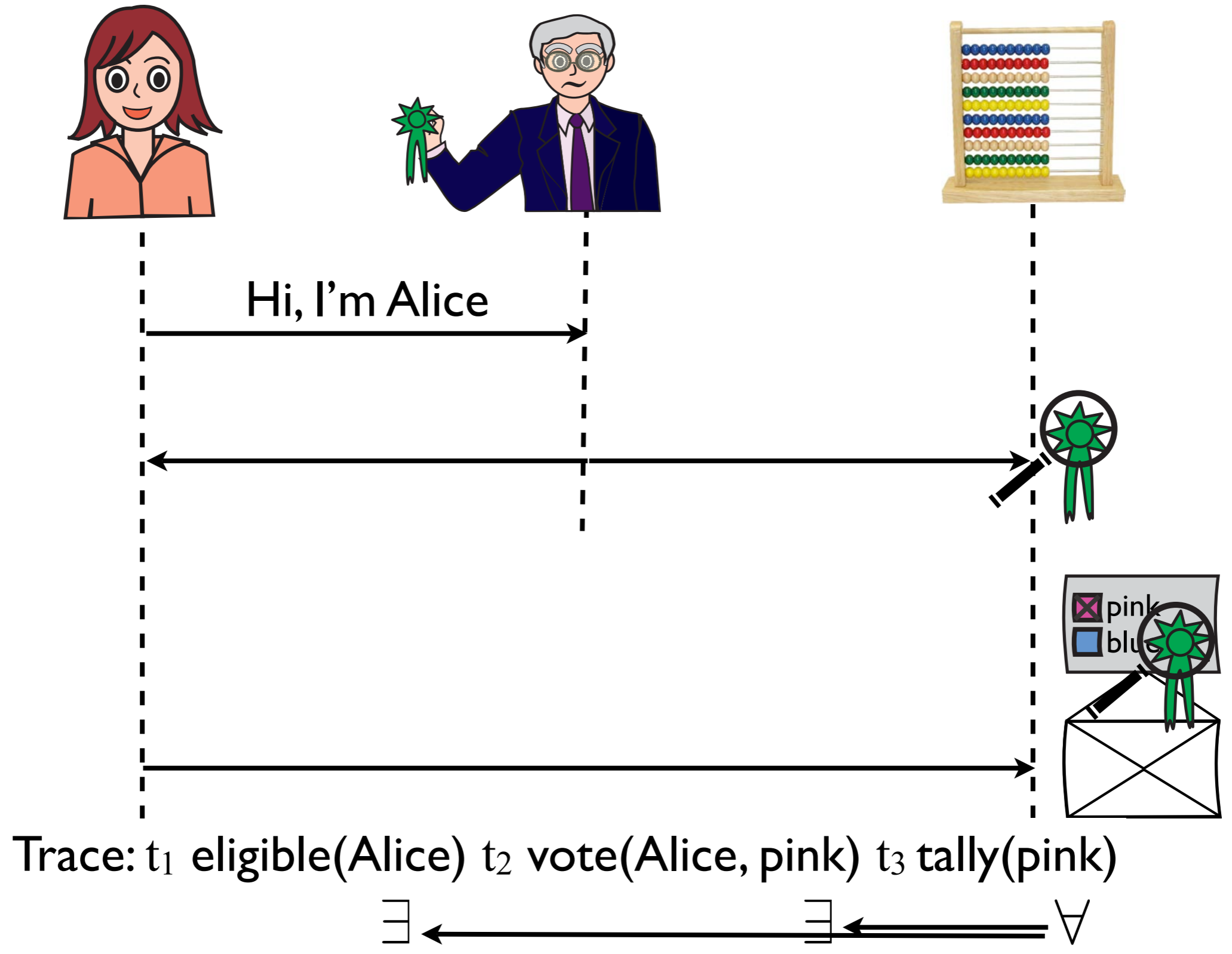
Soundness (eligibility, non-reusability, inalterability)



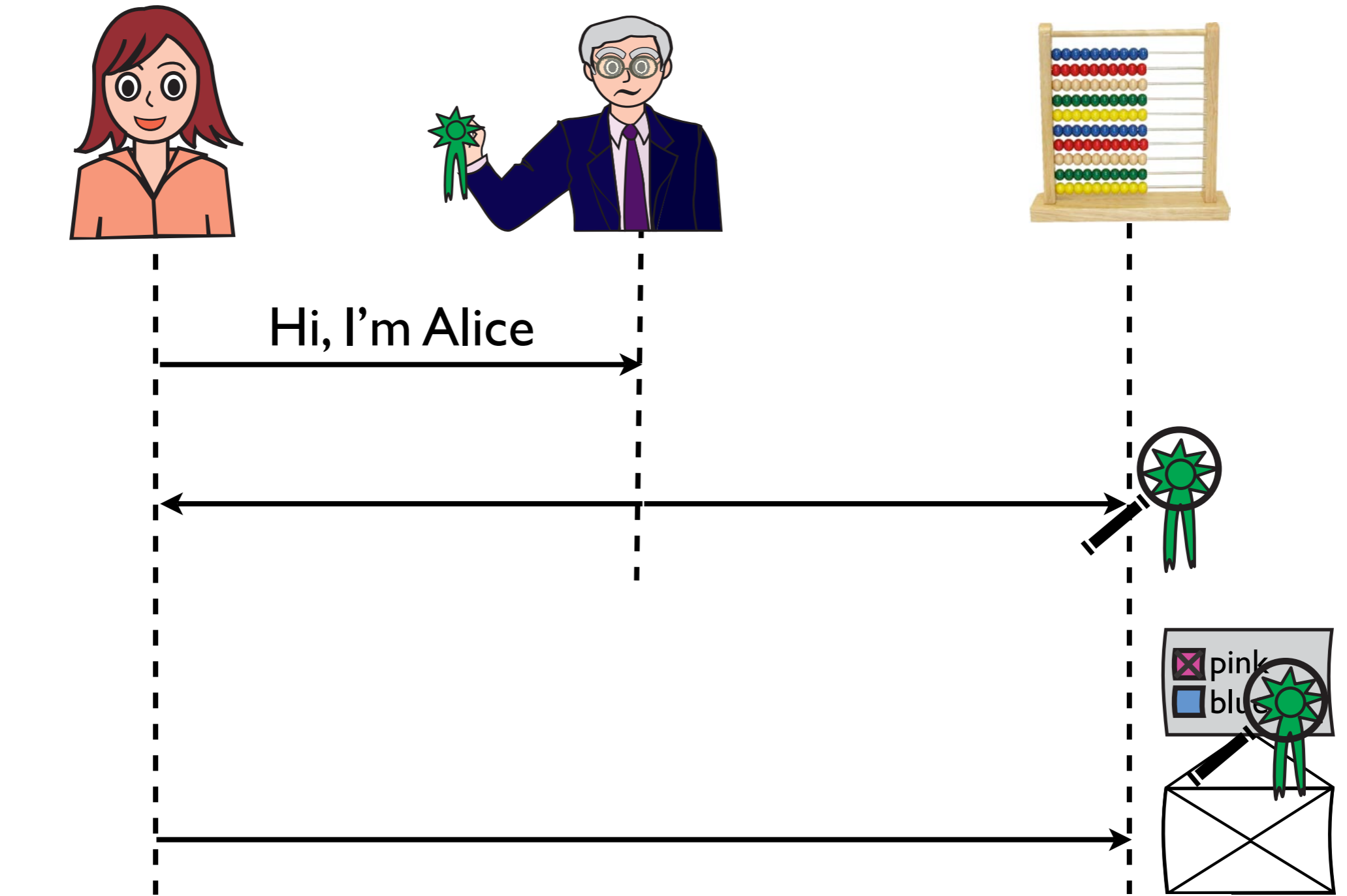
Soundness (eligibility, non-reusability, inalterability)



Soundness (eligibility, non-reusability, inalterability)



Soundness (eligibility, non-reusability, inalterability)



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



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

Vote-privacy



Voters

Alice

Bob

Charlie

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

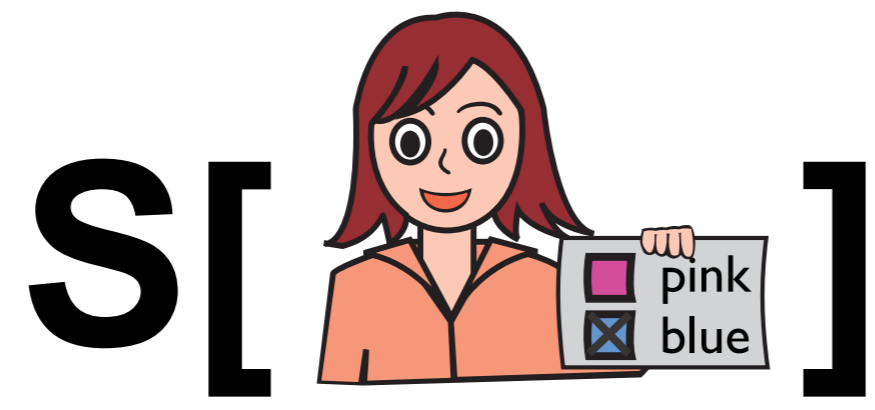
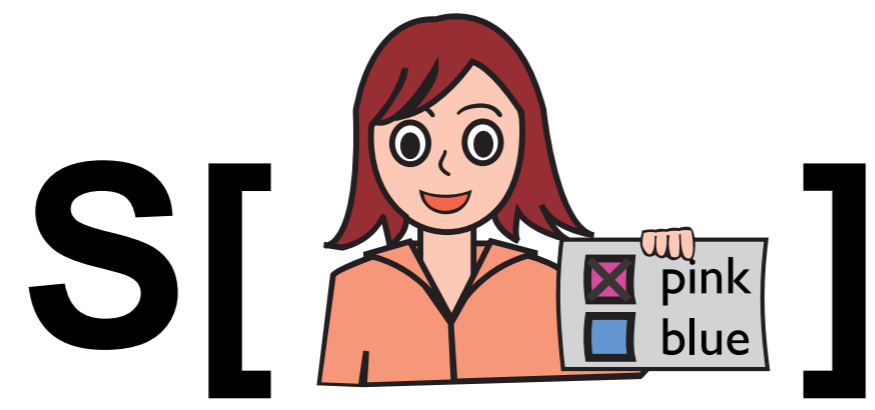
Voters
Alice
Bob
Charlie

Results
pink party |
blue party ||

~~**“Detailed” results**
Alice pink party
Bob blue party
Charlie blue party~~

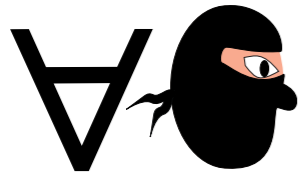
Definition of vote-privacy

[Delaune, Kremer & Ryan; CSF '06]



Definition of vote-privacy

[Delaune, Kremer & Ryan; CSF '06]

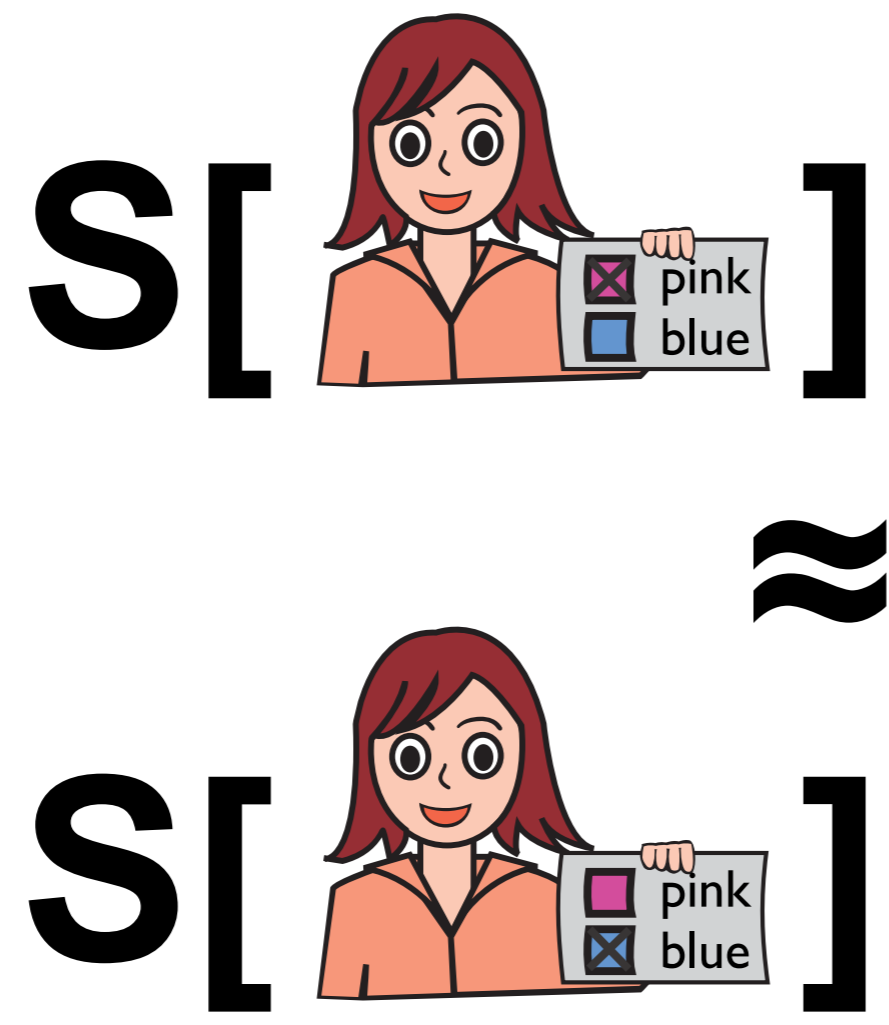


indistinguishable from



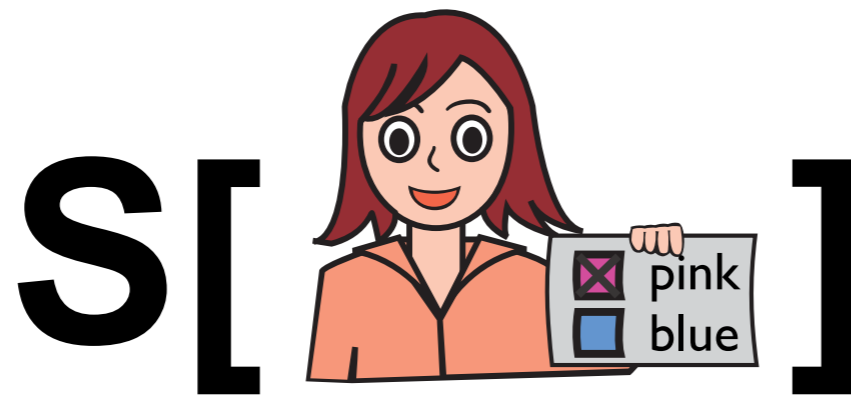
Definition of vote-privacy

[Delaune, Kremer & Ryan; CSF '06]

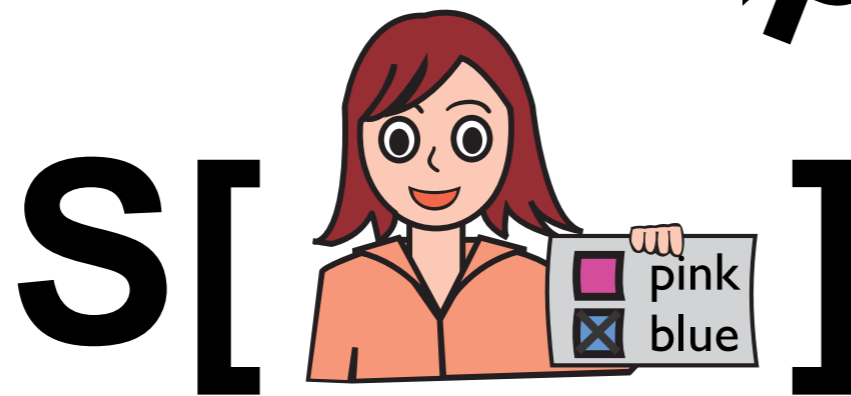


Definition of vote-privacy

[Delaune, Kremer & Ryan; CSF '06]

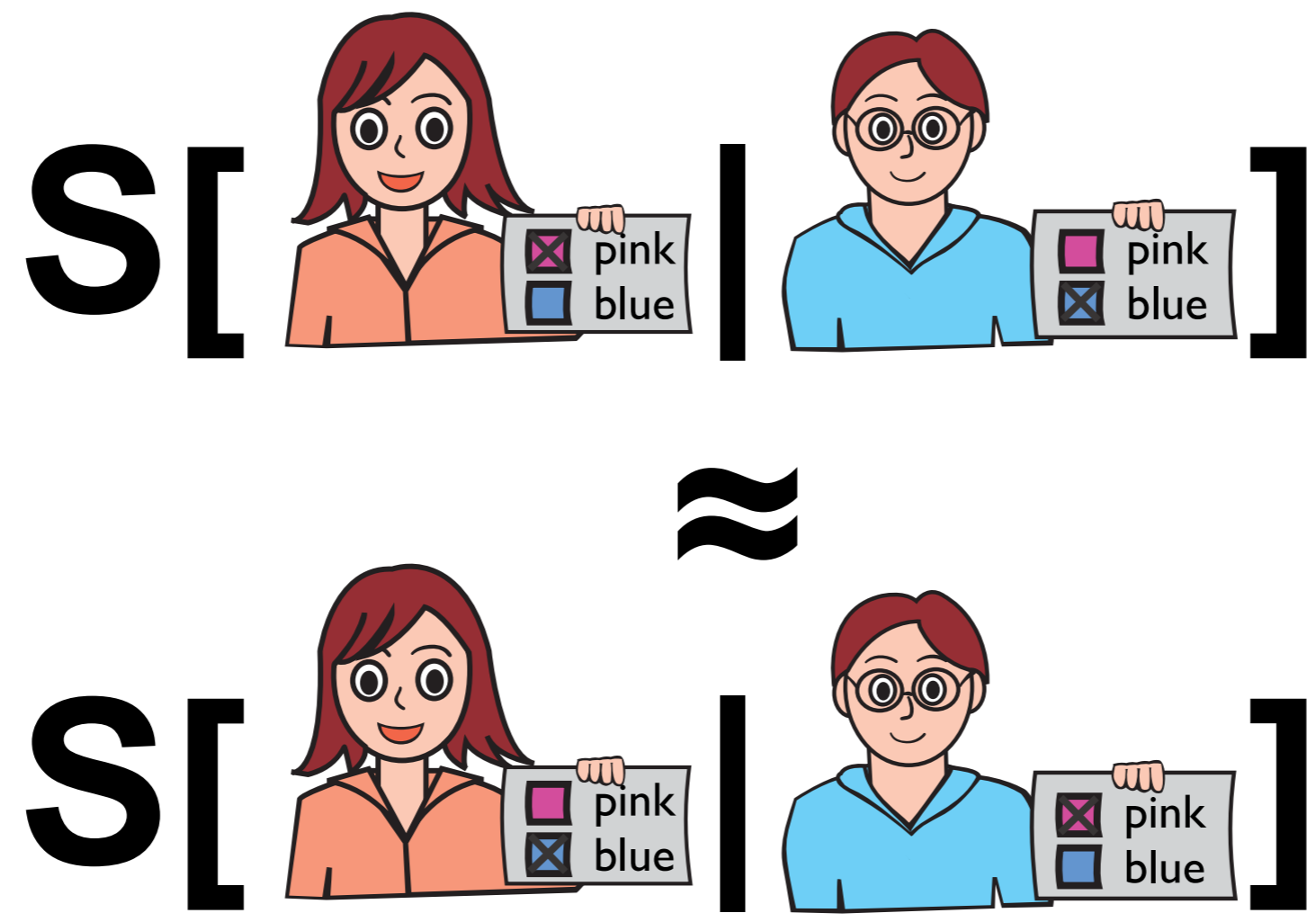


≠

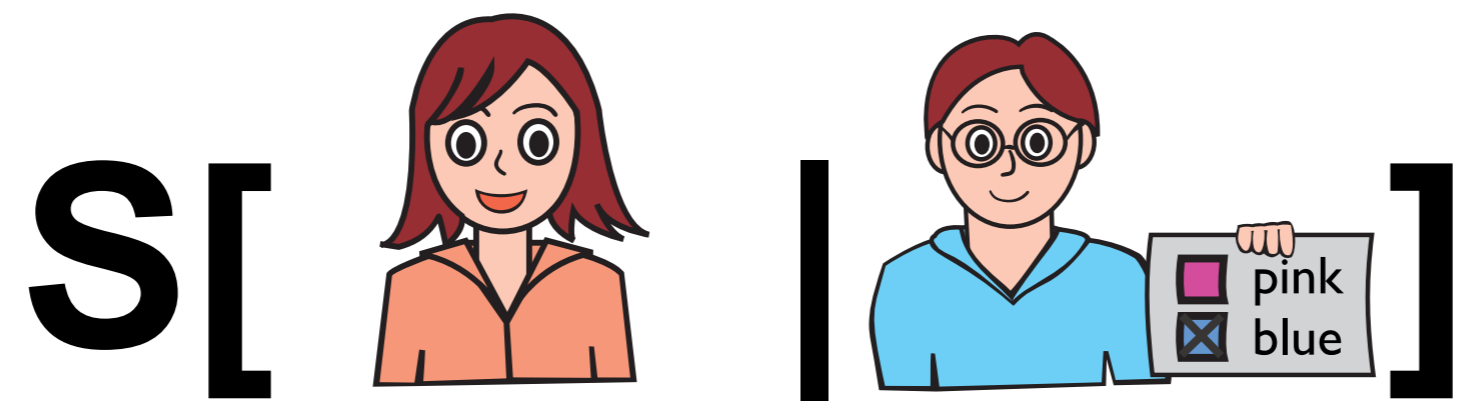


Definition of vote-privacy

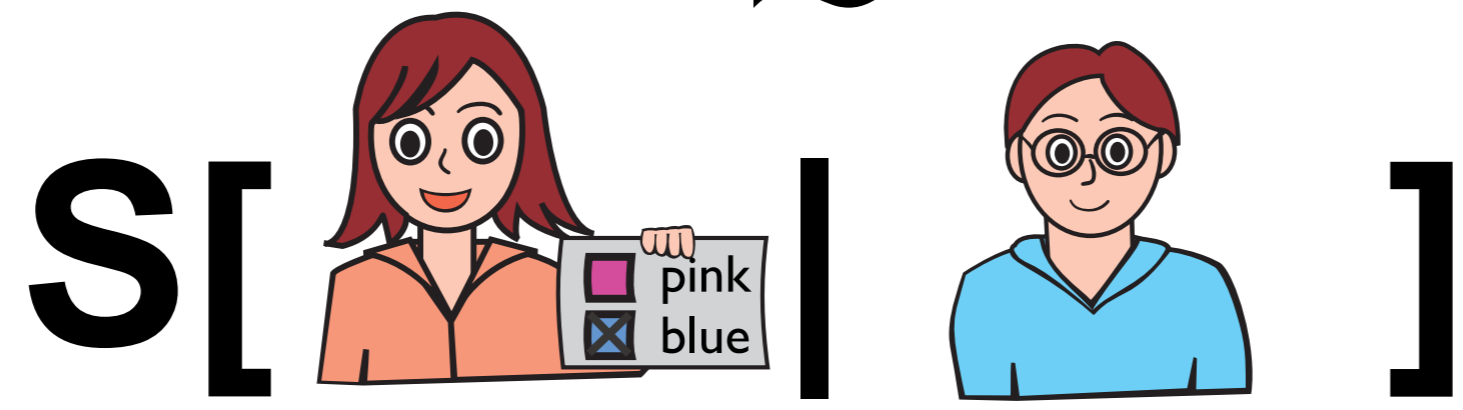
[Delaune, Kremer & Ryan; CSF '06]



Immunity to forced-abstention

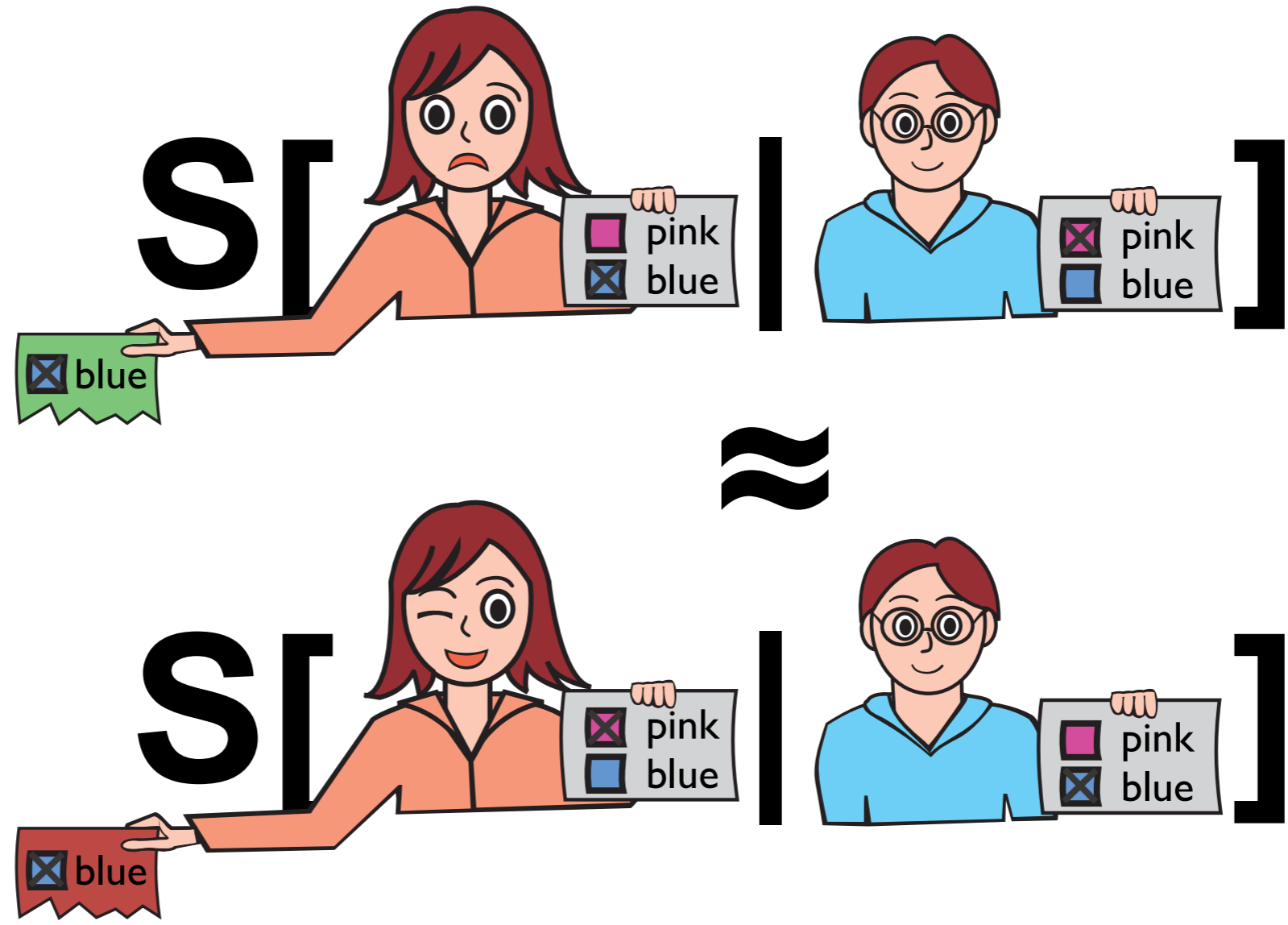
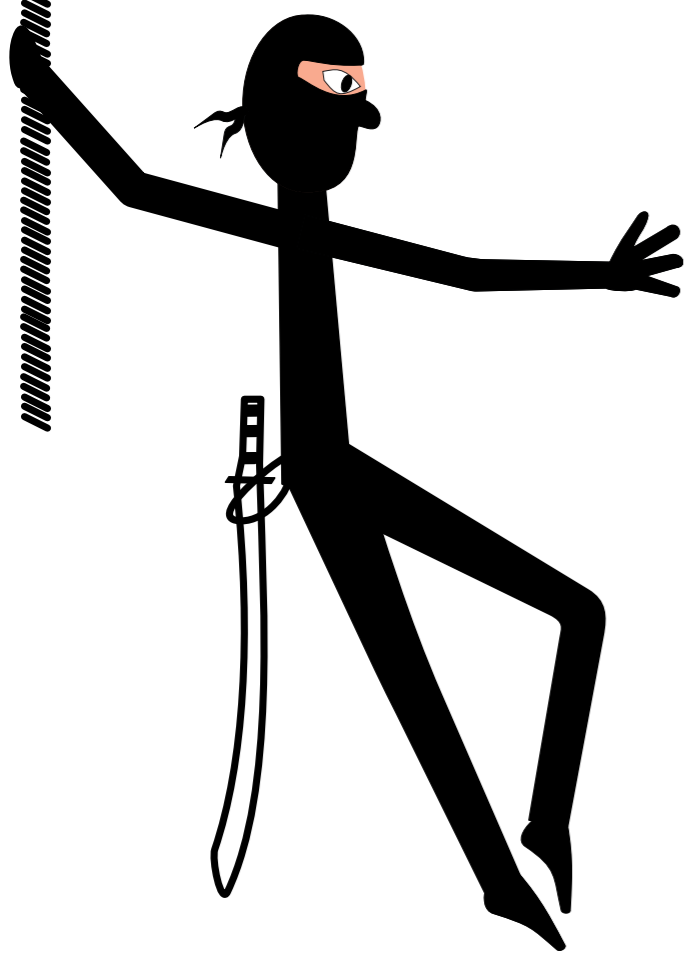


\approx



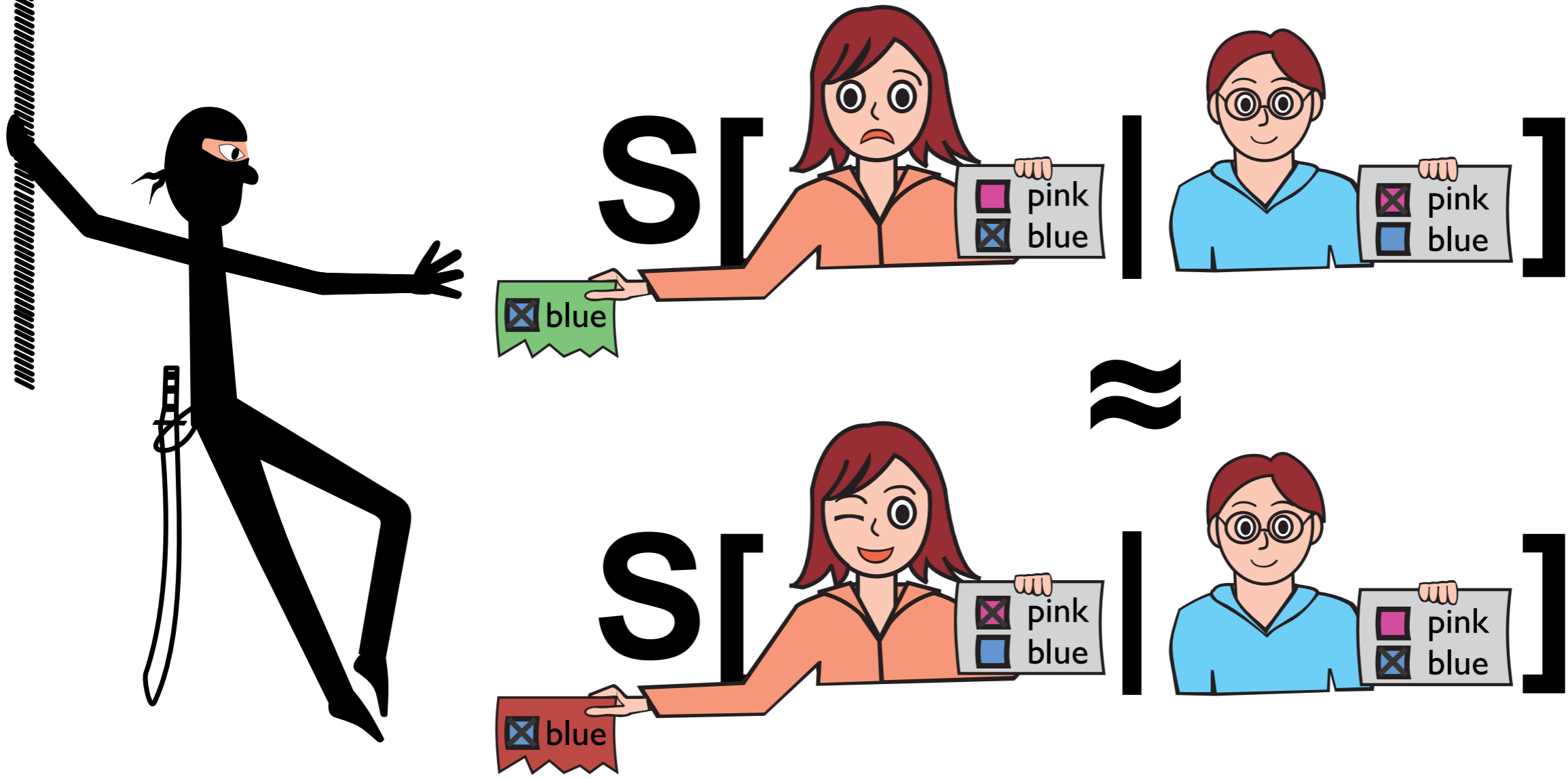
Receipt-freeness

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



Receipt-freeness

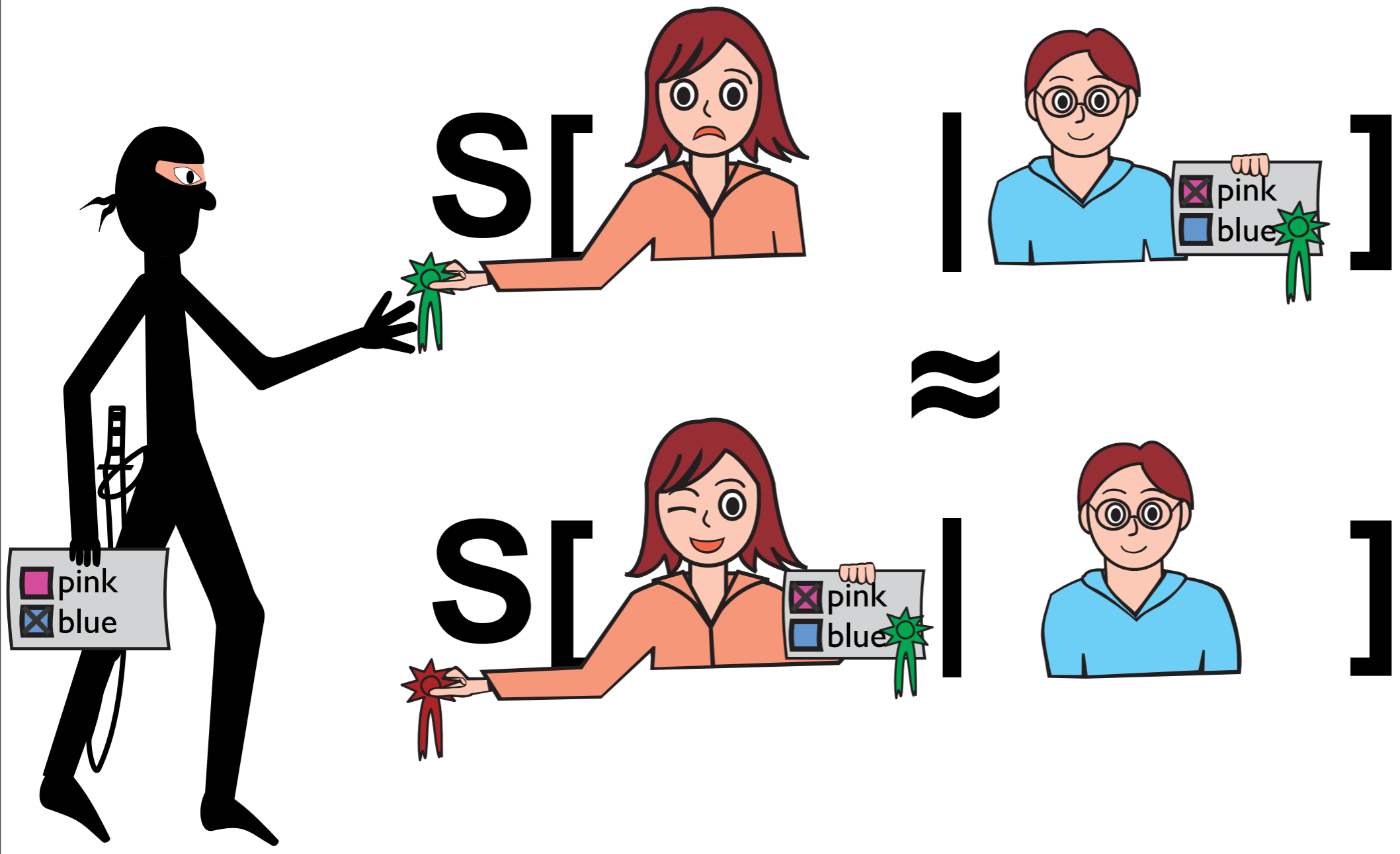
- Cryptographic setting [Benaloh & Tuinstra; STOC '94]



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

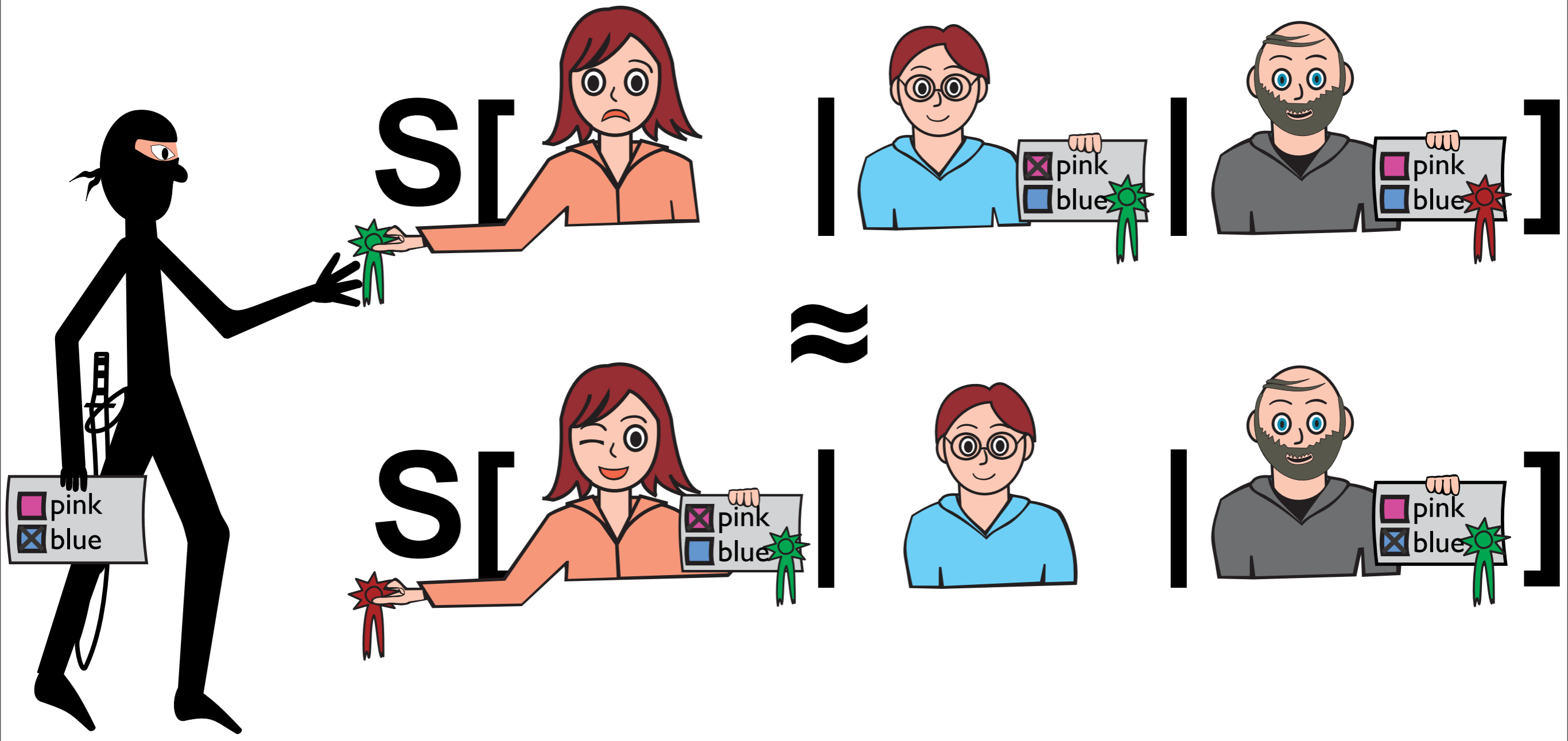
Coercion-resistance

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



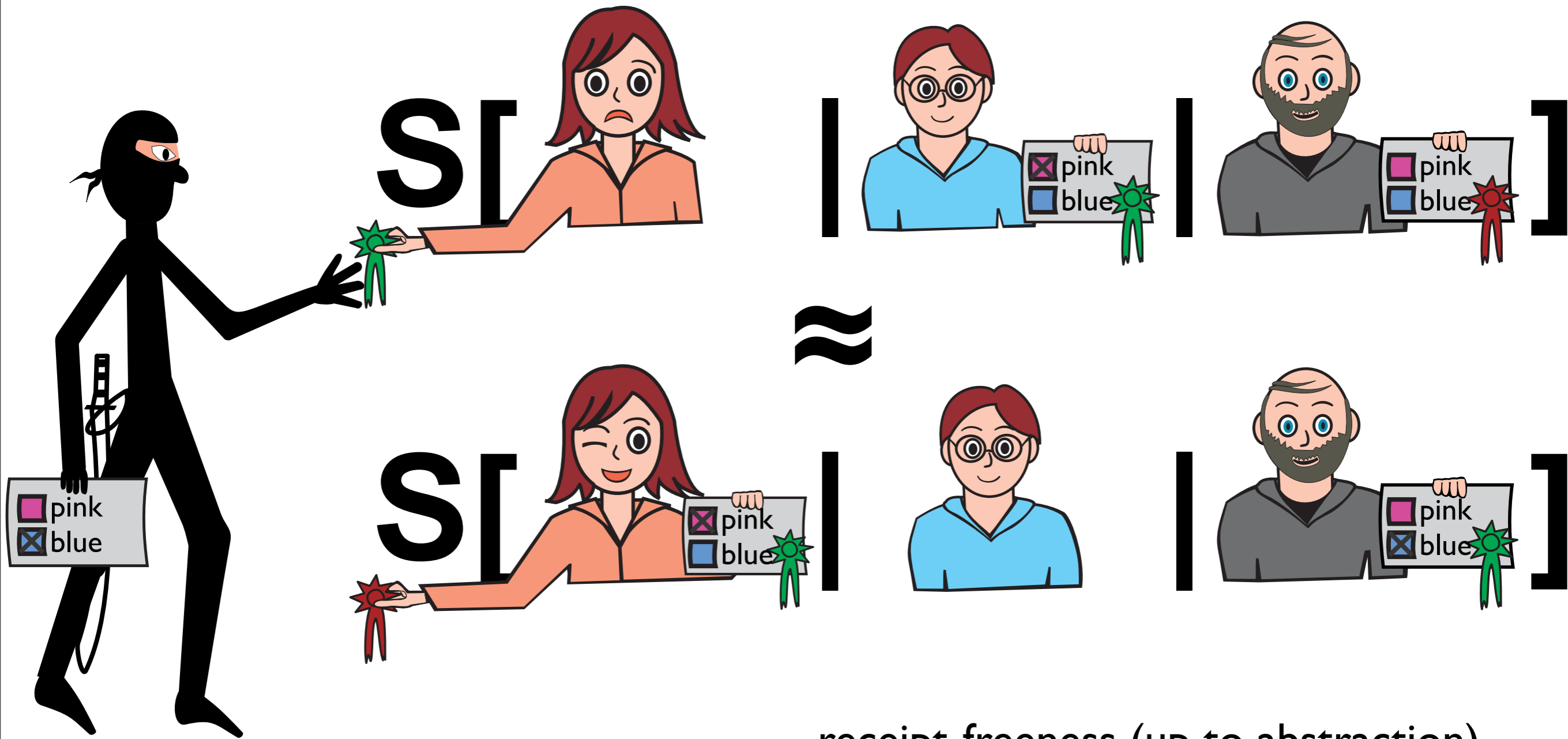
Coercion-resistance

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



Coercion-resistance

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



⇒ receipt-freeness (up to abstraction)

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

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]

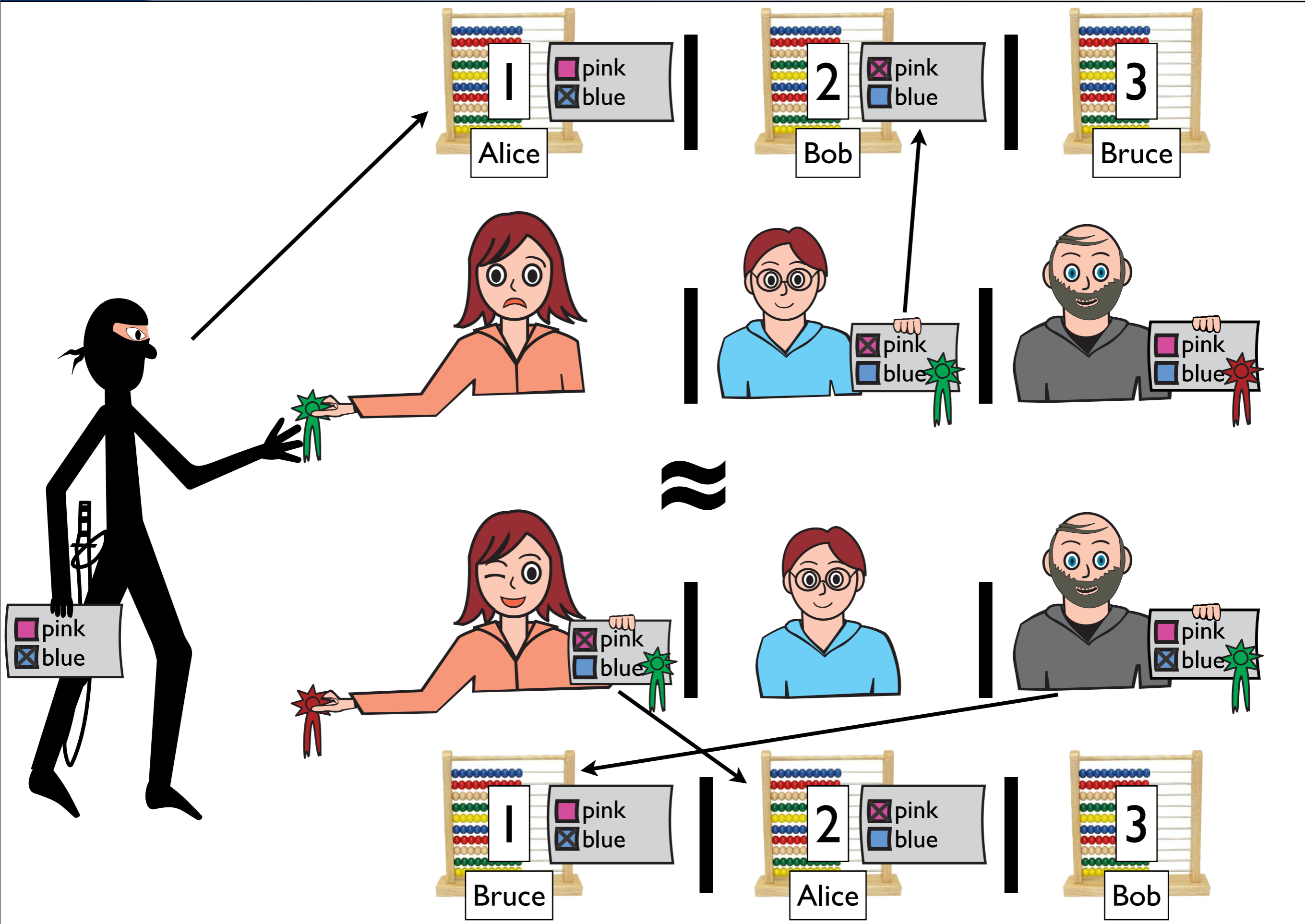
Current and Future work

- 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]

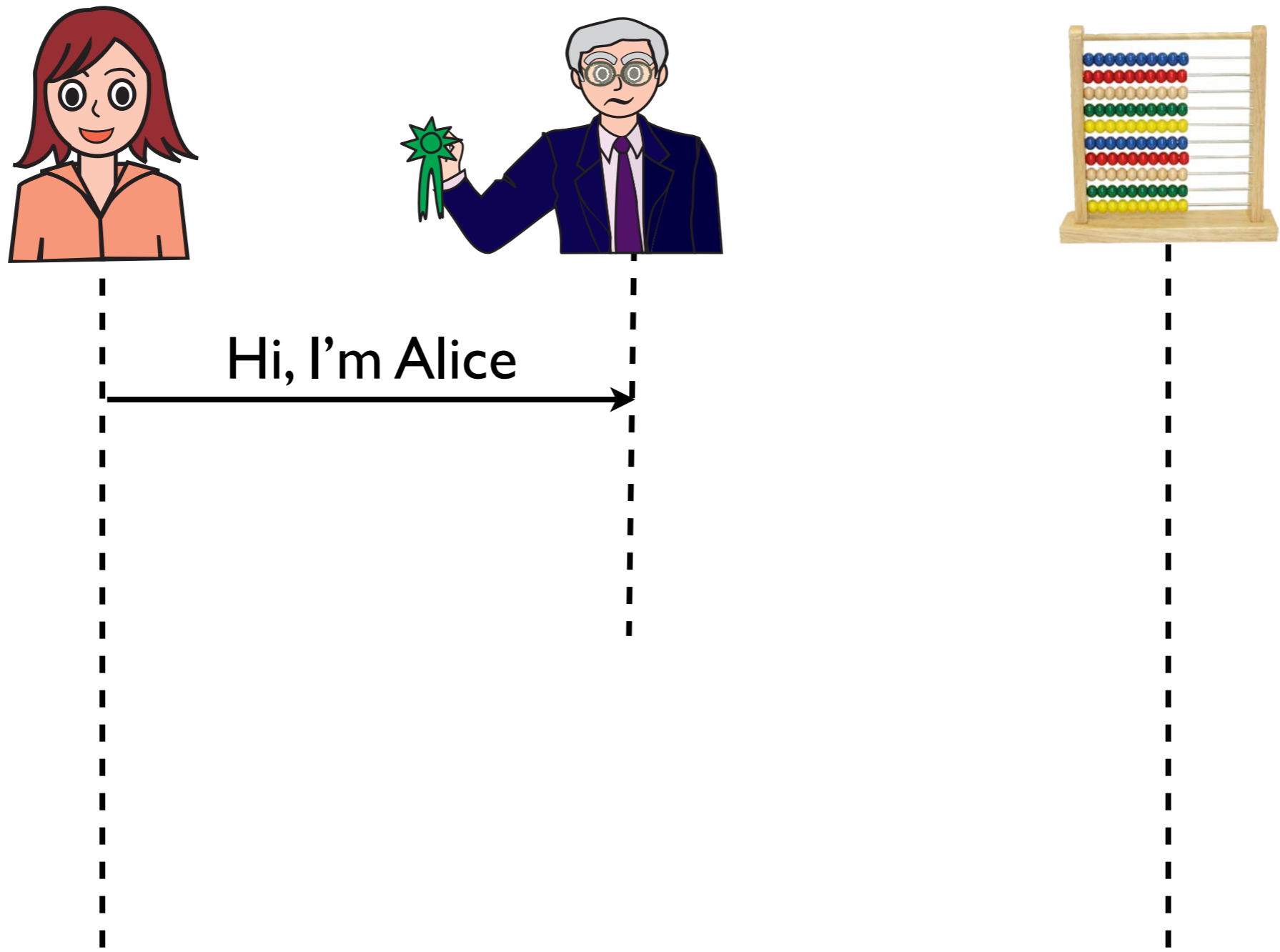
Current and Future work

- 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

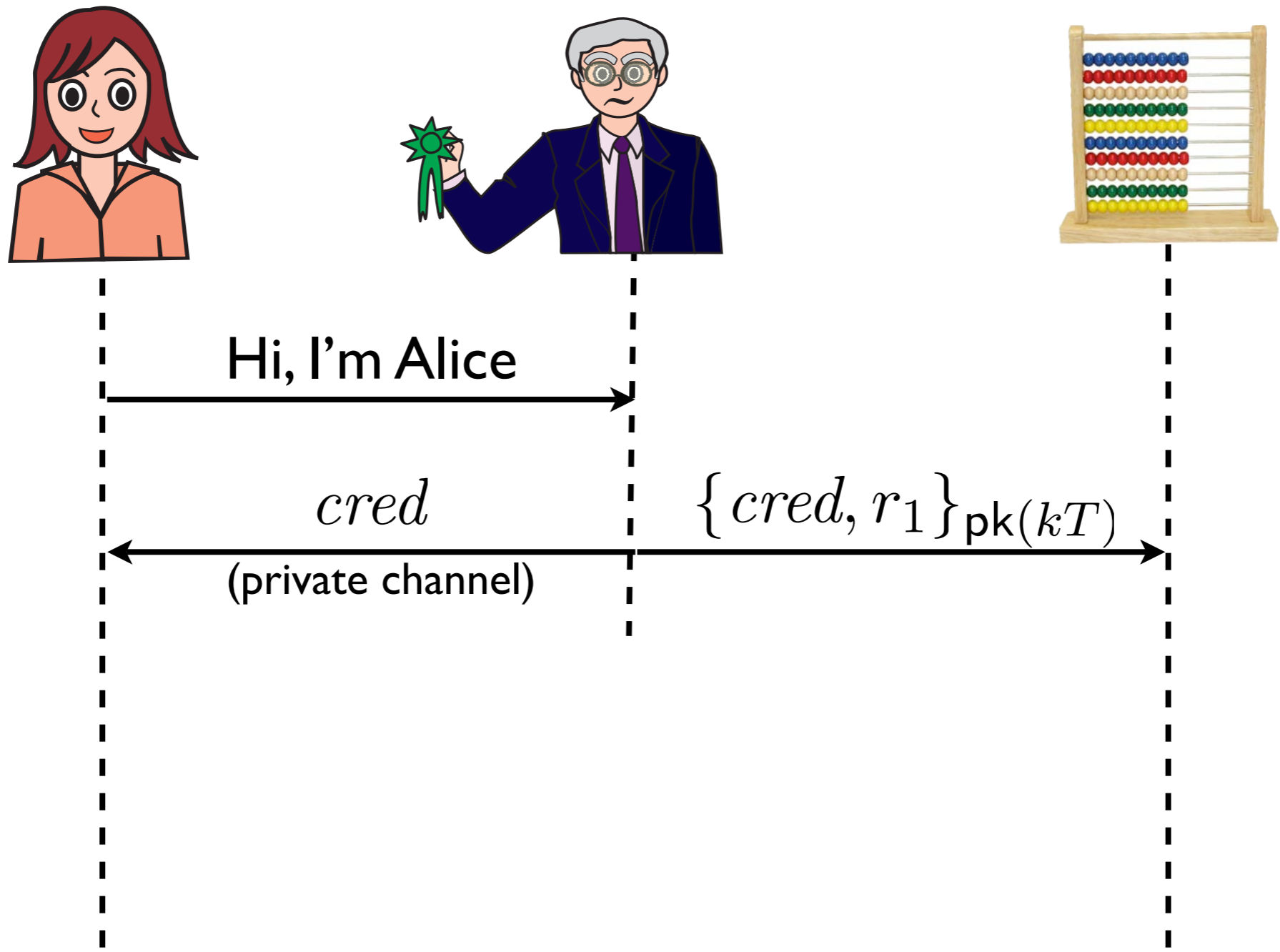
Backup slides



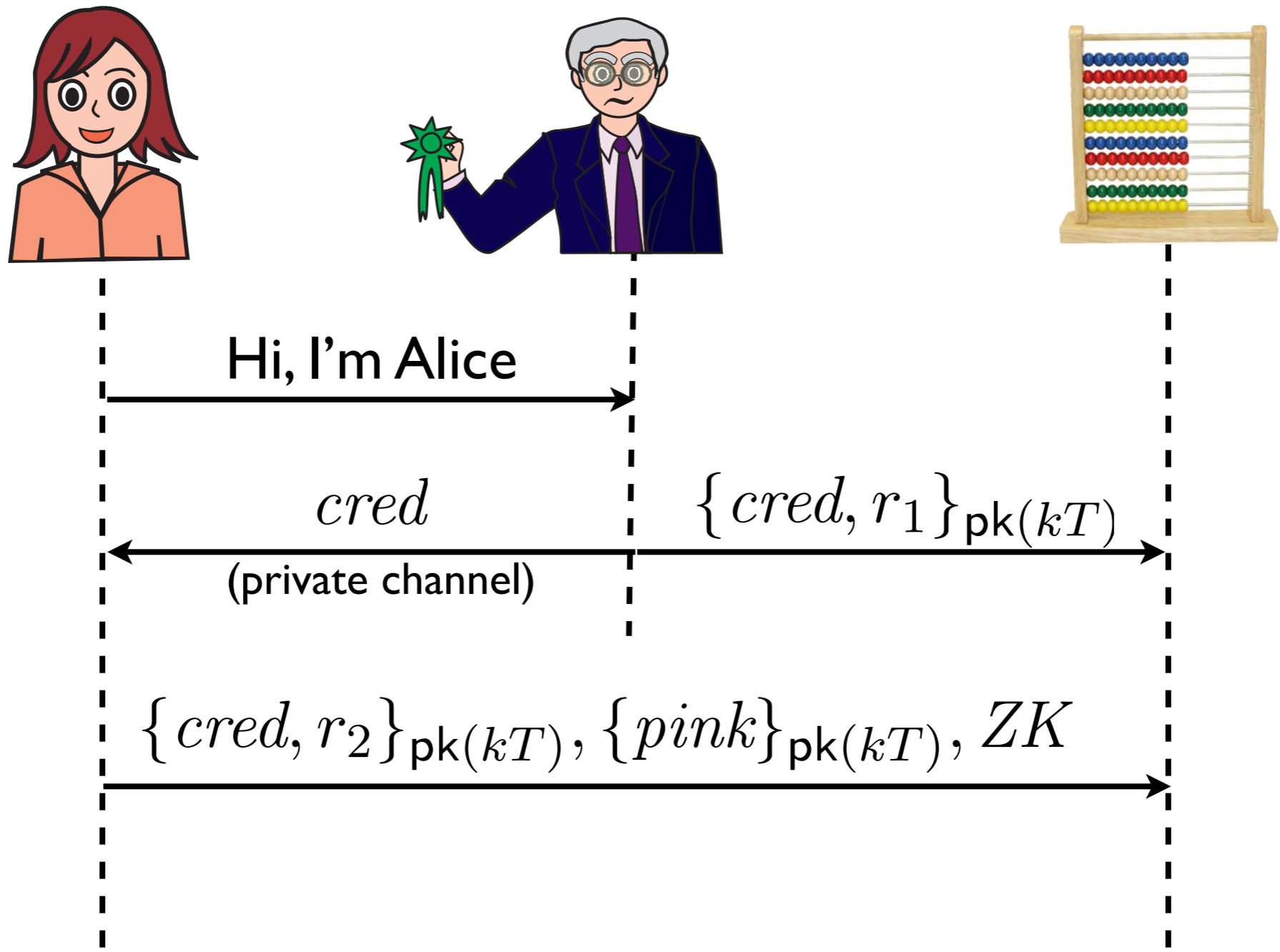
Simplified JCJ protocol



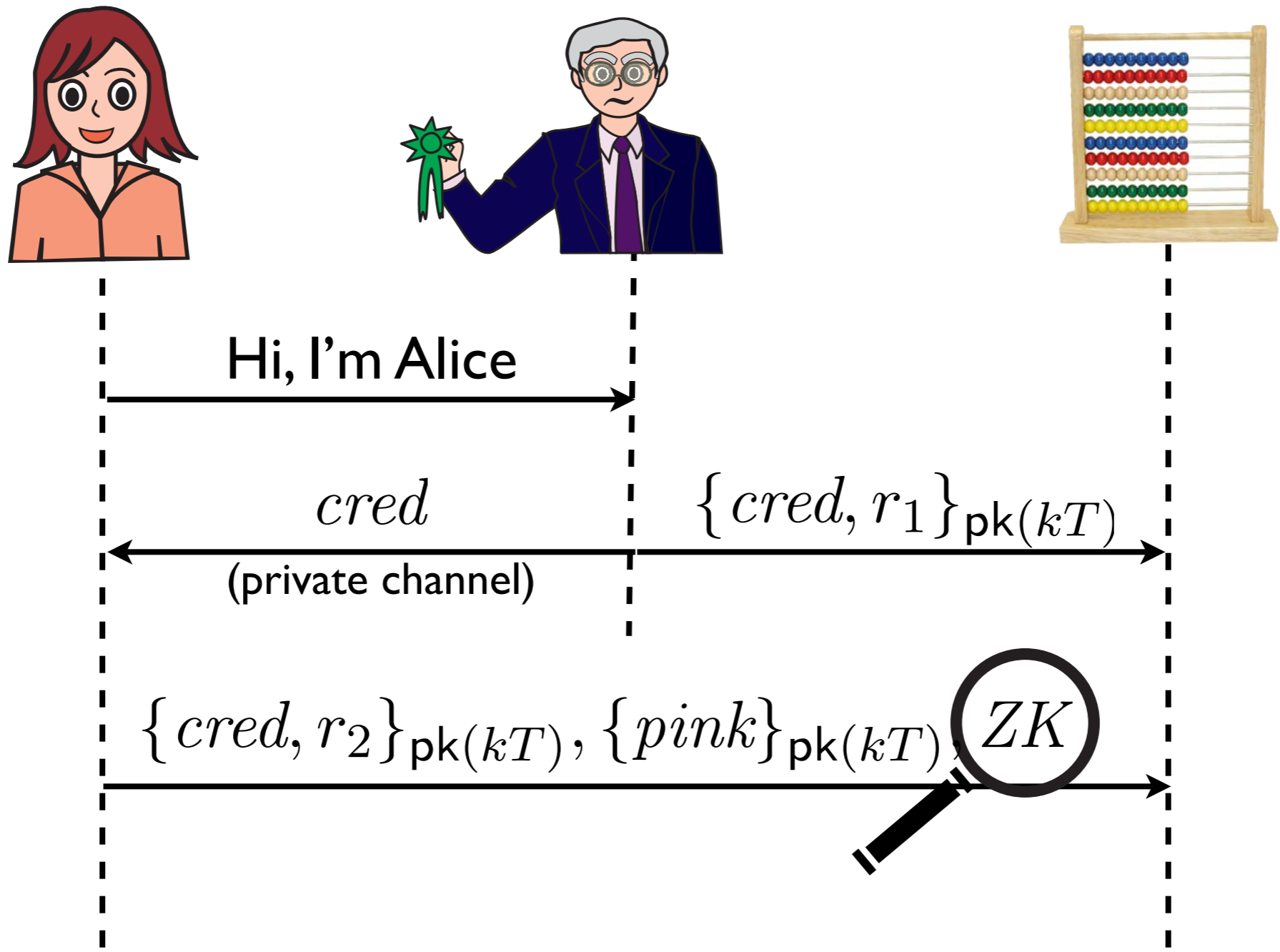
Simplified JCJ protocol



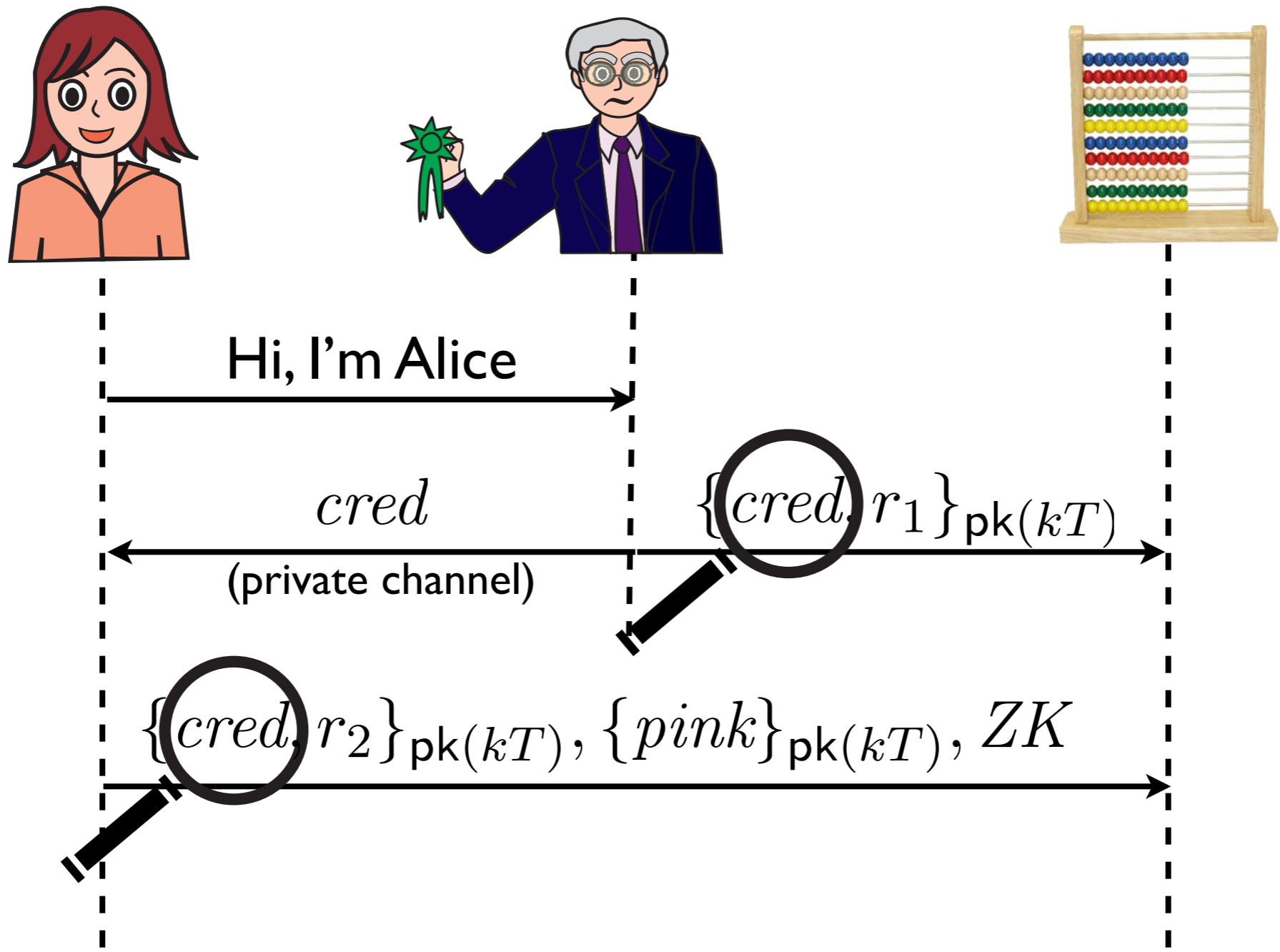
Simplified JCJ protocol



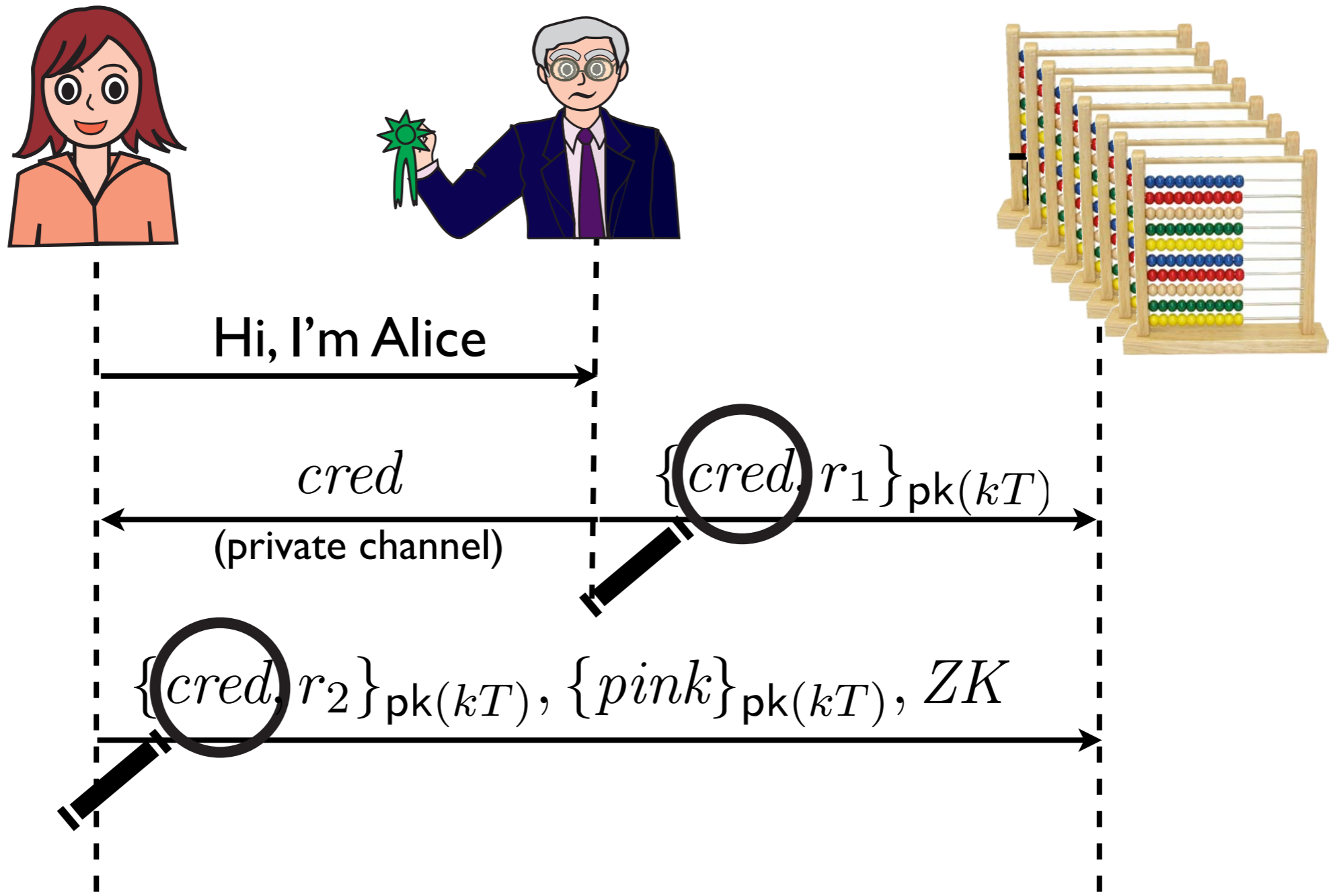
Simplified JCJ protocol



Simplified JCJ protocol



Simplified JCJ protocol



Simplified JCJ protocol

