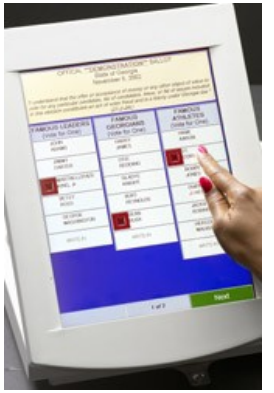
Some issues in verifying e-voting systems

Mark D. Ryan

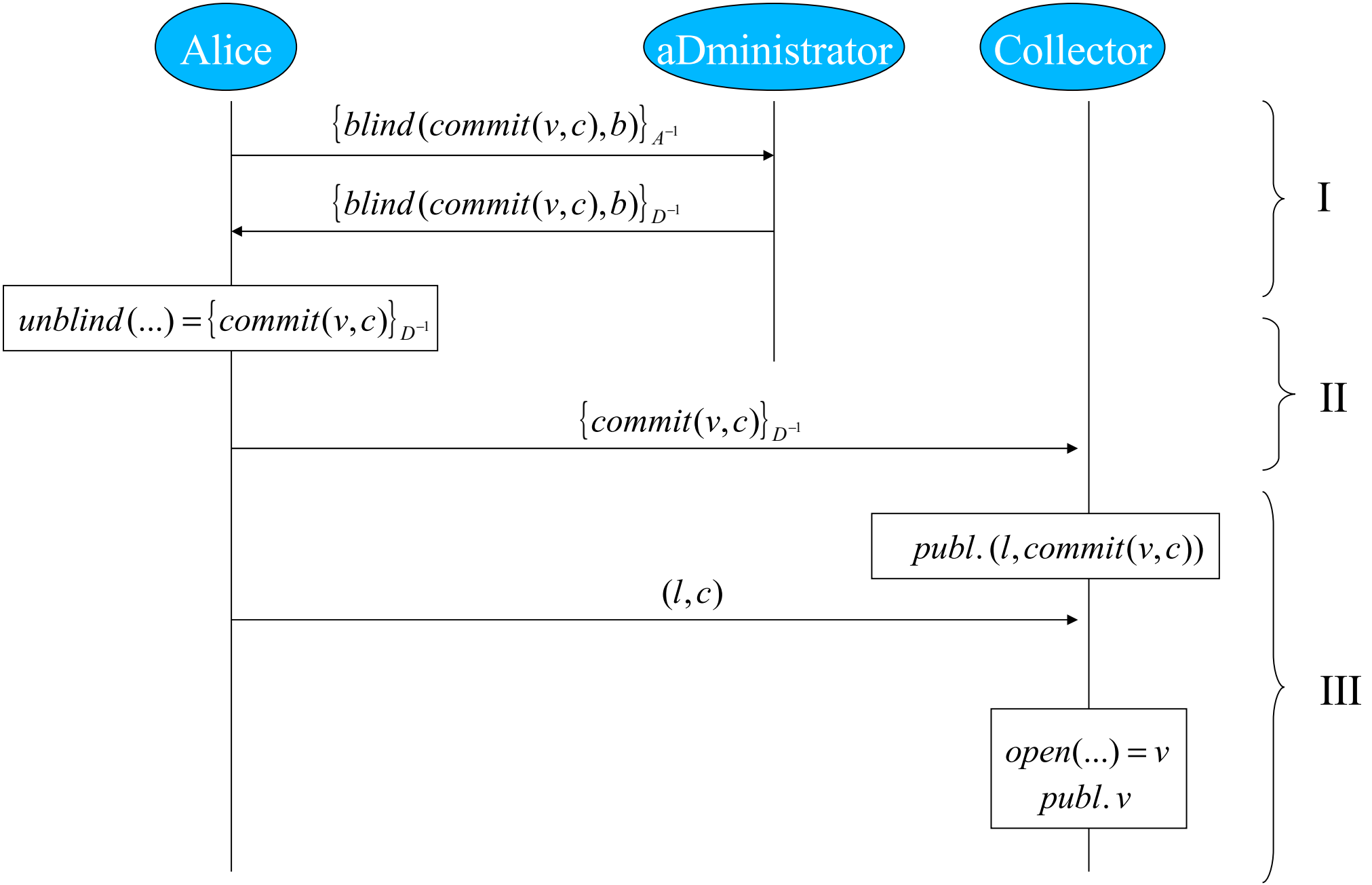
- **Present-day e-voting offers few security properties** [KohnoStubblefieldRubinWallach2004] **compared to what is desirable:**
  - *Eligibility:* only eligible voters can vote, and only once.
  - *Fairness:* no voter can be influenced by votes already made.
  - ***Indiv. verif.:*** a voter can verify that her vote was counted.
  - ***Universal verifiability:*** a voter can verify that the published result is the tally of the votes cast.
  - ***Privacy:*** no-one can find out how a voter voted.
  - ***Receipt-freeness:*** privacy, even if voter cooperates.
  - *Robustness:* Voters cannot disrupt the election. Faulty behaviour tolerated.
  - *Vote-and-go:* Voters participate in one session.



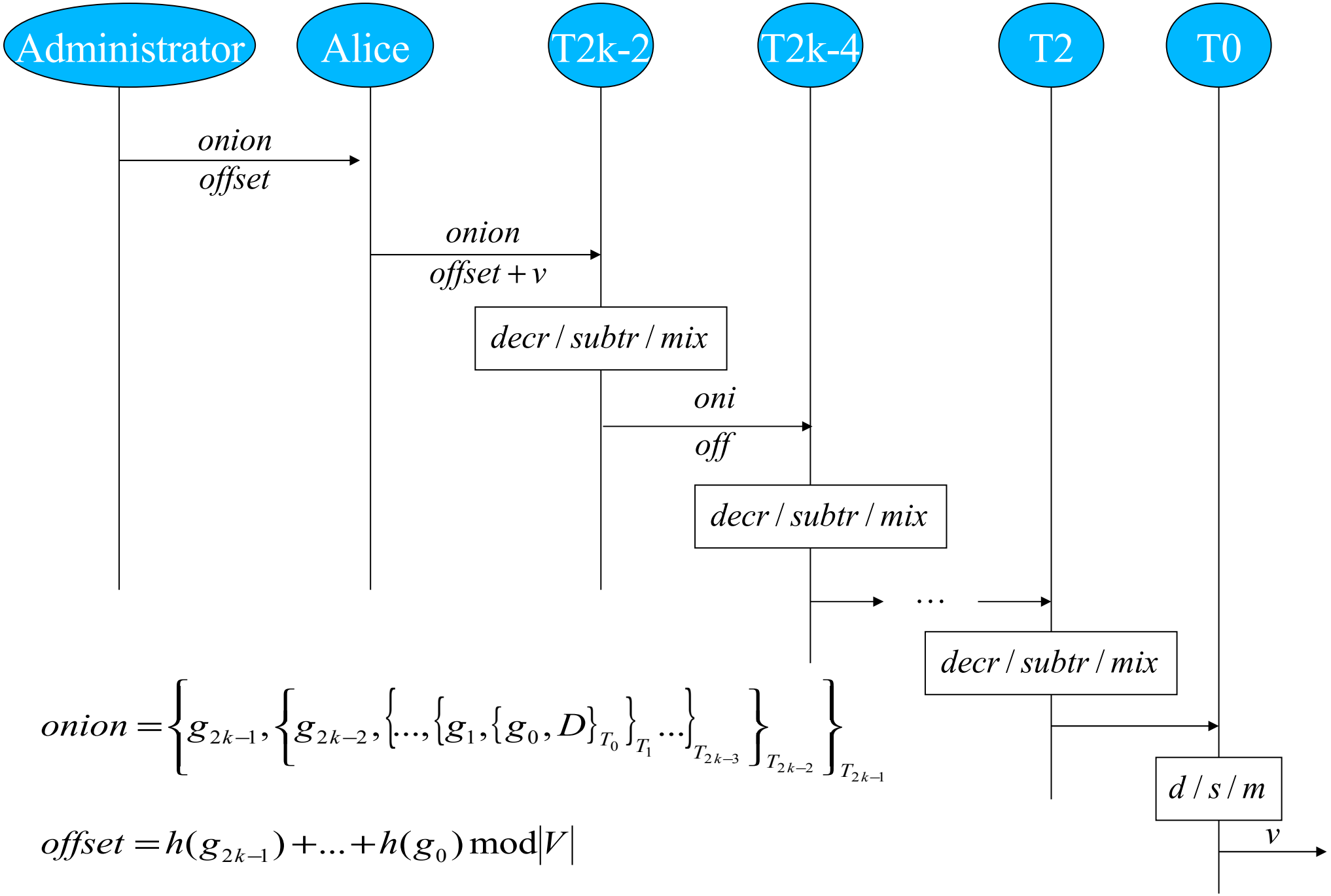
Some protocols

- *Classify according to how they obtain privacy*
  - *Anonymous channels and mixing the votes*
    - Look possible to model DY-style, since generally possible to abstract the crypto.
    - E.g. [FujiokaOkamotoOhta1992]; some properties verified [KremerRyan2005]
    - E.g. [Chaum P.Ryan Schneider 2005]
  - *Homomorphic encryption*
    - Look hard to model, since generally dependent on crypto details; not easy to abstract
      Hard to model *designated-verifier proofs*
    - E.g. [HirtSako 2000]

[FujiokaOkamotoOhta1992]



[Chaum P.Ryan Schneider 2005]



$$onion = \left\{ g_{2k-1}, \left\{ g_{2k-2}, \left\{ \ldots, \left\{ g_1, \left\{ g_0, D \right\}_{T_0} \right\}_{T_1} \ldots \right\}_{T_{2k-3}} \right\}_{T_{2k-2}} \right\}_{T_{2k-1}}$$

$$offset = h(g_{2k-1}) + \ldots + h(g_0) \bmod |V|$$

- **Some systems, and supposed properties**

Property	*FOO'92*	*HS'00*	*CRS'05*
Privacy	Blind signatures + phases	Homomorphic crypto	Anonymising mix
Receipt-freeness	X	Designated-verifier proofs	Receipt useless as proof
Indiv.verif.	Published list	X (I think!)	X, but *high assurance*
Vote&go	No	Yes	Yes

Issues in modelling the protocols

- *Applied-pi and Proverif*
- *[FOO92]*
  - Blind signatures
- *[CRS05]*
  - Modulo arithmetic
  - Choice of teller sequence
- *[HS00]*
  - Designated-verifier re-encryption proofs
  - 1-out-of-L re-encryption proofs

Should we have e-voting?

- *Experience in USA*
  - Proprietary system, not based on disciplined protocol, allegations of involvement of equipment supplier with a political party
  - “I voted party p1 and the system said `Thank you, we have recorded your vote for party p2.’ ” (Radio phone-ins, websites)
  - “15 year old in garage could manufacture cards and sell them on the internet that would allow multiple votes” [Avi Rubin]
- *Electronic systems potentially allow large scale undetectable fraud*
  - In contrast, fraud in manual systems limited by requirement to generate or dispose of paper, which is quite hard to do undetectably in presence of TV cameras.
- *Protocol complexity an obstacle to public confidence*
  - Public confidence is the most important ppty of an election system.