Further protocols: Electronic voting

Requirements for electronic voting

- **Fairness:** no early results can be obtained which could influence the remaining voters.
- **Eligibility:** only legitimate voters can vote, and only once (**Democracy**).
- **Privacy:** the fact that a particular voted in a particular way is not revealed to anyone.
- **Individual verifiability:** a voter can verify that her vote was really counted.
- **Universal verifiability:** the published outcome really is the sum of all the votes.
- **Receipt-freeness:** a voter cannot prove that she voted in a certain way.

Stages of election procedures

- **Registration** – In the registration stage the authorities determine who is eligible to vote, maintain proper lists of the registered voters;
- **Validation** –when the election begins, administrators validate the credentials of those attempting to vote.
- **Collection** – At this stage the voted ballots are collected before the final stage of the tally;
- **Tallying** – At this stage the accumulated votes are counted, agreed upon and published.

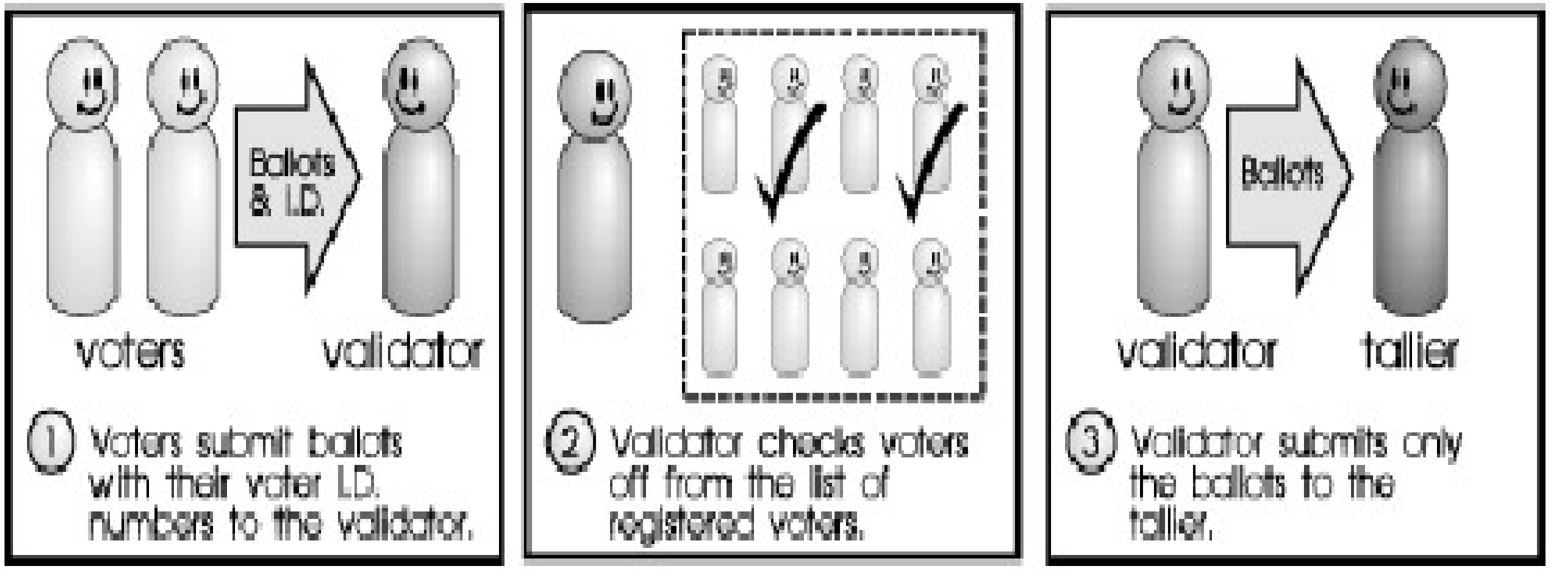
Participants (components) of e-vote systems

- **Voter:** Person who casts ballot.
- **Validator:** Person who authenticates the Voter.
- **Tallier:** Person who counts ballots and publishes
- results.

Simple voting protocol

- **Registration:** assign each eligible voter with a unique voter-id (VID).
- **Election:** the voter submits an electronic ballot (B) with the voter identification number attached to the "Validator".
- **Validation: t**he validator uses the identification number to check the voter off on a list of registered voters. Then the identification number is stripped off and the ballot is sent to an electronic "tallier".
- **Tallying:** The tallier records the votes and adds them to the election tally.

Simple voting protocol



Issues with the simple protocol

- Voters cannot be sure that the validator does not violate their privacy.

- There is no way to ensure that the
- validator does not alter ballots before sending them to the tallier;

- There is no way to ensure that the tallier accurately records the votes.

FOO protocol

- **Fujioka,Okamoto, and Ohta (1992):**
- Practical secret voting scheme based on blind signatures.
- **Notation:**
- **b** the ballot.
- **e,d** the voter’s private and public encryption/decryption keys.
- **k** a random blinding value.
- **ev,dv** the validator’s public and private encryption/decryption keys.

FOO protocol. Preparation and Verification

- **Voter's Preparation**
- A voter prepares a ballot **b**, encrypts it with a secret key **b^e=B**, and blinds it **($B*k^{ev}$).**
- The voter then **signs** the ballot **($B*k^{ev}$, id)** and sends it to the validator.
- **Verification:**
- The validator verifies that the signature belongs to a registered voter who has not yet voted.
- If the ballot is valid, the validator signs the ballot - **$(B*k^{ev})^{dv}$** - and returns it to the voter.

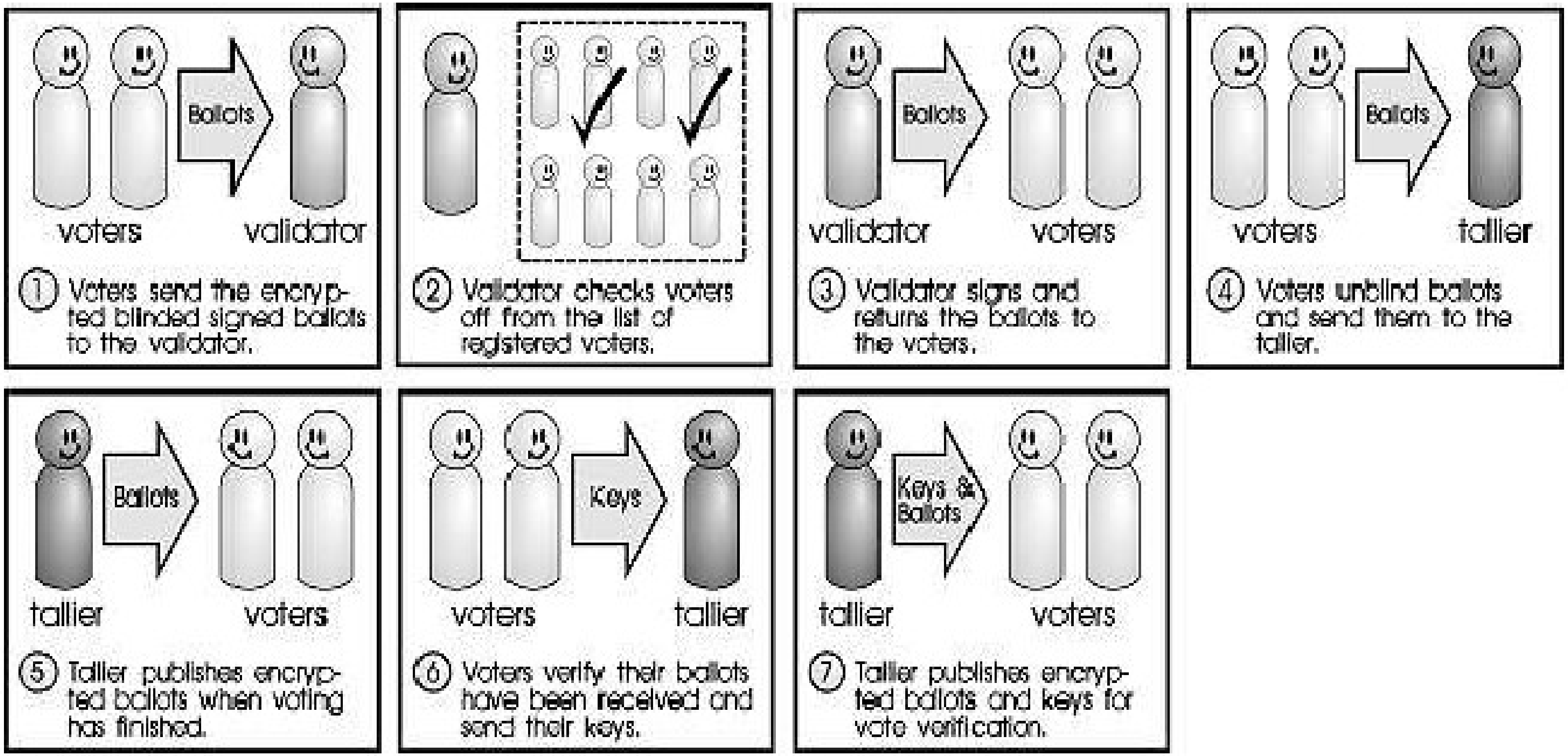
FOO protocol. Collection

- **Collection:**
- The voter removes the blinding encryption layer
- **$(B*k^{ev})^{dv}$ / k**, revealing an encrypted ballot signed by the validator **B^{dv}**.
- The voter then sends the resultant signed-encrypted-ballot **B^{dv}** to the tallier.
- The tallier checks the signature on the encrypted ballot. If the ballot is valid, the tallier places it on a list that is published after all voters vote.

FOO protocol. Final stages.

- **Tallying:**
- After the list has been published, voters verify that their ballots are on the list and send the tallier the decryption keys (ballots are still encrypted at that moment!)
- The tallier uses these keys to decrypt the ballots and add the votes to the election tally.
- **Verification:**
- After the election the tallier publishes the decryption keys along with the encrypted ballots so that voters may independently verify the election results **(B,b,d).**

FOO protocol



① Voters send the encrypted blinded signed ballots to the validator.

② Validator checks voters off from the list of registered voters.

③ Validator signs and returns the ballots to the voters.

④ Voters unblind ballots and send them to the tallier.

⑤ Tallier publishes encrypted ballots when voting has finished.

⑥ Voters verify their ballots have been received and send their keys.

⑦ Tallier publishes encrypted ballots and keys for vote verification.

Additional assumption

- For FOO to protect privacy one has to rely on the assumption that
-
- ***signed unblind ballots and their keys are sent to the tallier over an an anonymous channel***

Good properties of FOO

- **Privacy:** voters' anonymity from authorities is assured, even in the case when Validator and Tallier may cooperate;
- **Verifiability**: voters can verify ballots were counted correctly;
- **Flexibility**: FOO may be used for different formats of polls (simple "yes/no" format; multiple choice, etc).
-

Issues with FOO (and other protocols)

- The Validator can stuff the ballot box with abstaining votes;
- The protocol provides voters with the means to verify (and thus prove) their vote (no receipt-freeness) ;
- Anonymity allows voters to let someone else vote for them.
-
- *Although these problems may be remedied to some extent they still remain obstacles in large scale practical applications such as general elections*
- *Possible way forward: secure multi party computations for voting.*