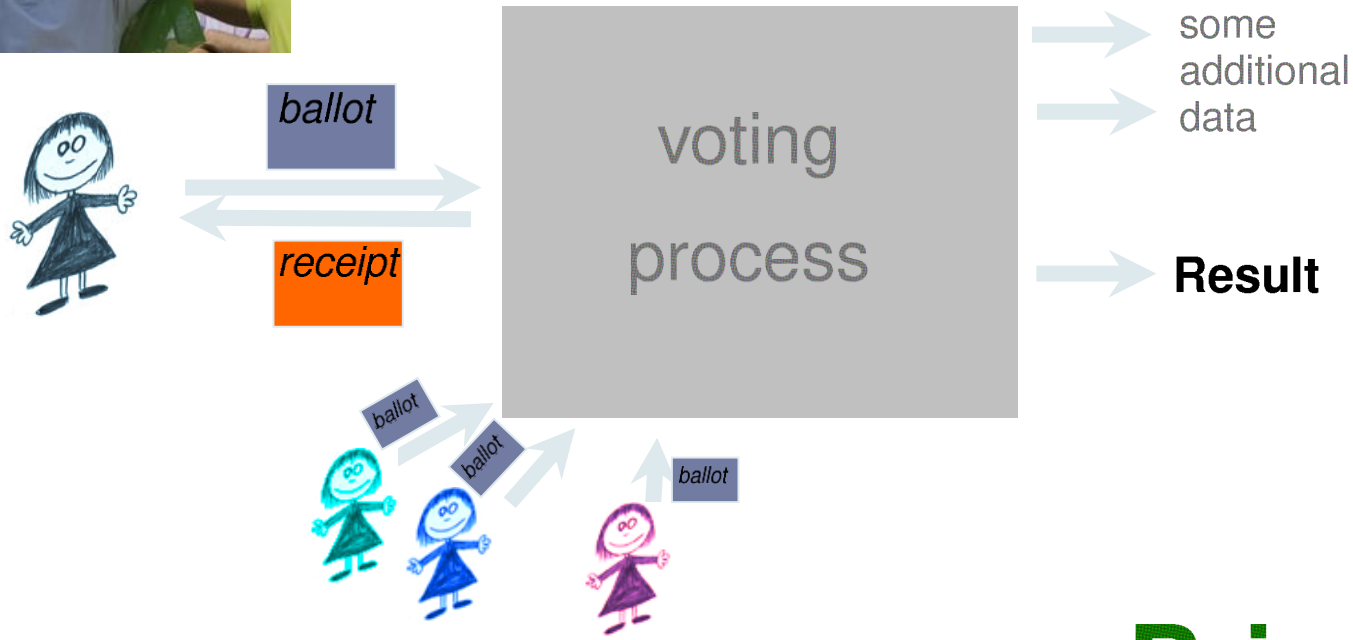
18733: Applied Cryptography

Electronic Voting

Anupam Datta
CMU
Spring 2017

Voting

Verifiability



Privacy

Voting

Verifiability

Coercion-resistance

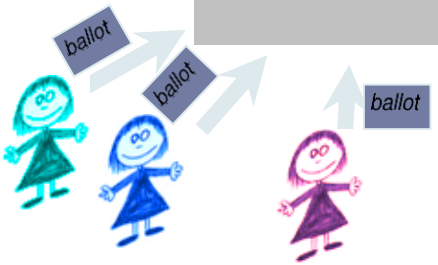
ballot

receipt

voting process

some additional data

Result



Privacy

Two variants of electronic voting

- Voting over the Internet
  - Example: Helios (used for IACR elections etc.)

    https://vote.heliosvoting.org/

"**Should we start using Helios for public-office elections? Maybe US President 2020?**

No, you should not. Online elections are appropriate when one does not expect a large attempt at defrauding or coercing voters…If you'd like to use a truly verifiable voting system for your public-office election, we recommend an in-person election"

Two variants of electronic voting

- Voting in person at polling stations
  - Examples: ThreeBallot, Scantegrity, Pret-a-Voter

Scantegrity was used in the 2011 Takoma Park Municipal election

http://scantegrity.org/

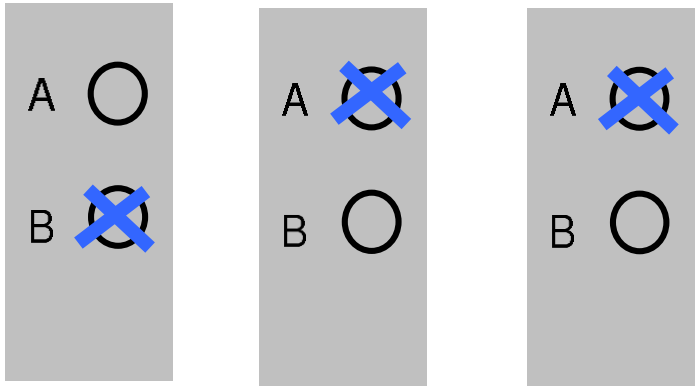
Outline

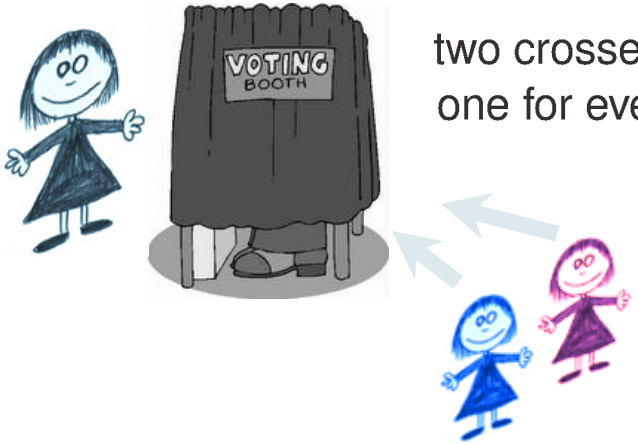
- The ThreeBallot Voting Scheme

- Privacy
- Verifiability
- Coercion-resistance

ThreeBallot

[Rivest, 2006]



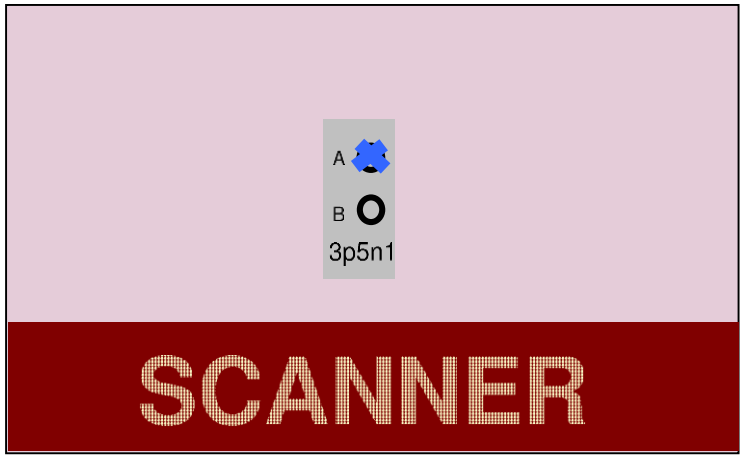


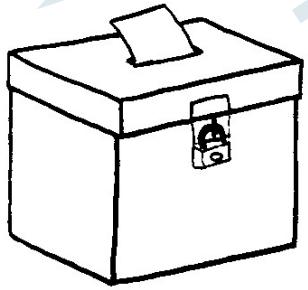
two crosses for her candidate
one for everybody else

checks well-formedness

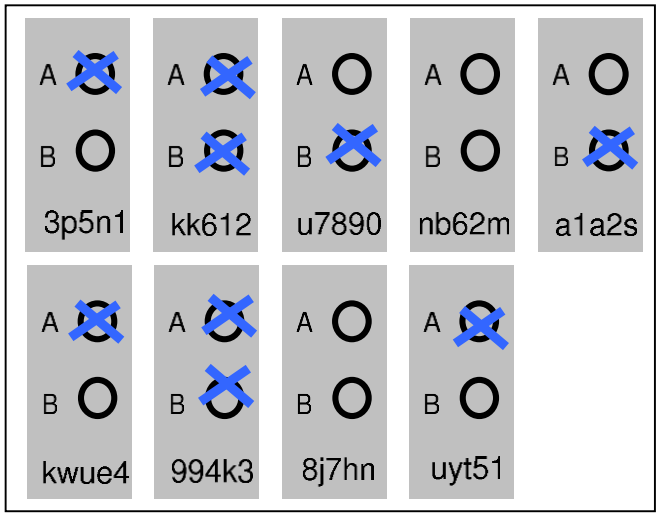
prints random serial numbers

Alice chooses receipt (simple ballot)





Bulletin Board



result

Informal Discussion

- Correctness
  - Count total no. of marks for a candidate: $2x + (n-x) = x + n$ where x = no. of votes for a candidate and n = total no. of voters = (no. of single ballots on bulletin board)/3

- Properties
  - Verifiability
    - Voter checks single ballot receipt appears on bulletin board
  - Privacy
    - Single ballot receipt does not reveal who a voter voted for
  - Coercion-Resistance
    - Single ballot receipt does not reveal who a voter voted for

Outline

- The ThreeBallot Voting Scheme

- Privacy
- Verifiability
- Coercion-resistance

Privacy

δ-Privacy

$\forall$ *candidates A, B*

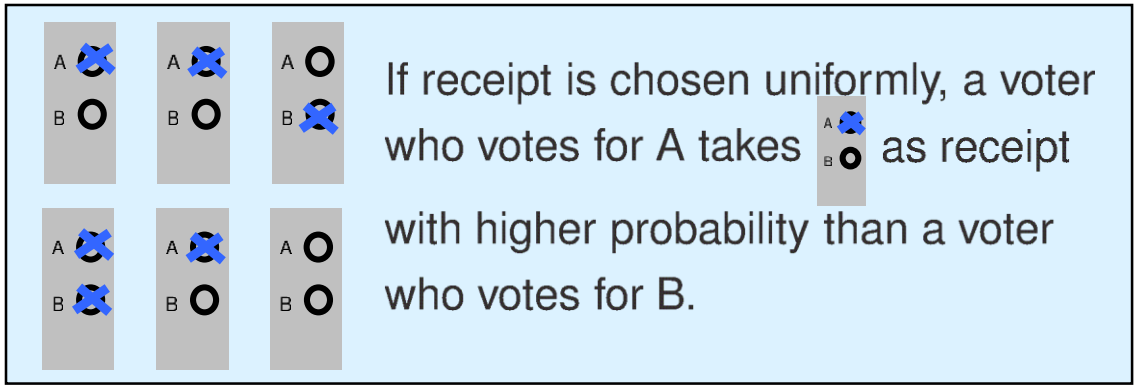
The observer cannot distinguish whether Alice votes for A or B but with probability δ.

Assumptions:

- Voting machine (scanner) is honest
- Bulletin board and voters may be dishonest
- Observer may have access to receipts of voters

- Challenge:
  - Defining and computing δ

ThreeBallot's Privacy (Intuition)



- A voter's receipt leaks information about which candidate (s)he voted for

- Idea: Observer O guesses that a voter V voted for candidate A when view is v if

$$\Pr[O \text{ observes view } v \mid V \text{ voted for } A] > \Pr[O \text{ observes view } v \mid V \text{ voted for } B]$$

Outline

- The ThreeBallot Voting Scheme

- Privacy
- Verifiability
- Coercion-resistance

Individual and Universal Verifiability

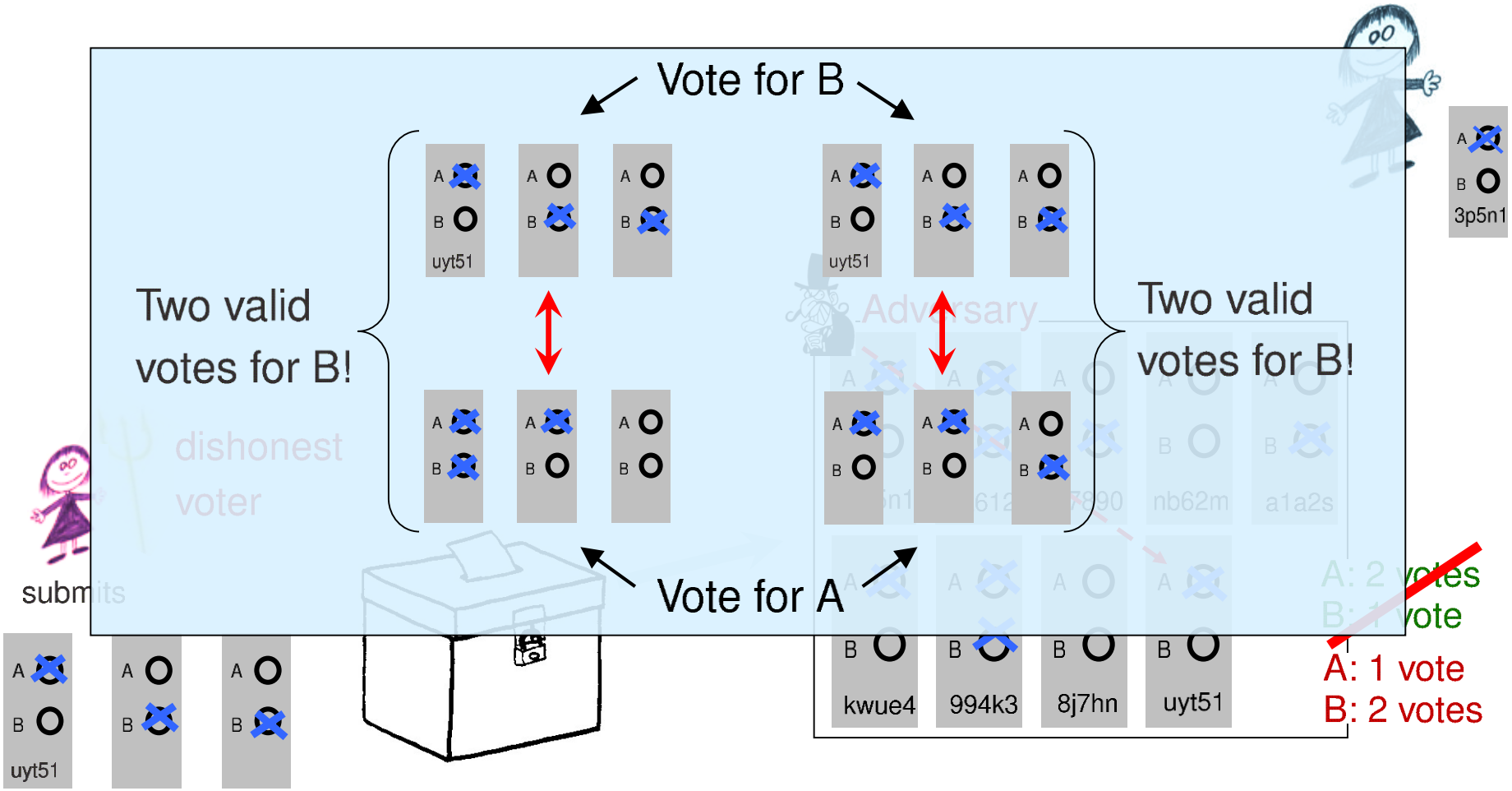
Individual verifiability:

A voter can make sure (with reasonable probability) that her ballots are published on the bulletin board.

Universal verifiability:

From the bulletin board, everybody can compute the result.

ThreeBallot: Verifiability



- The bulletin board remains consistent if there is a vote for A.
- Honest voters cannot detect any manipulation.
- Still, the result is not correct.

Verifiability

Individual verifiability

+

Universal verifiability

$\not\Rightarrow$

(global) verifiability

Global Verifiability

e.g. a voter
or a judge

In a voting protocol, the result is guaranteed by B and δ-verifiable by a if

set of authorities
e.g. machine, bulletin board,...

1) If the result is not correct, a does not accept,

2) If all members in B are honest, then a accepts.

Outline

- The ThreeBallot Voting Scheme

- Verifiability
- Privacy
- Coercion-resistance

Privacy

δ-Privacy

$\forall$ *candidates A, B*

The observer cannot distinguish whether Alice votes for A or B but with probability δ.

Coercion-Resistance

δ- Coercion-Resistance (informal)

arbitrary instructions for the coerced voter

For instance:

- not to vote
- to vote for C
- to cast a ballot formed in a certain way

certain goal

For instance:

- to vote for candidate C'

$\forall$ *coercion strategy* $v \in V$

$\exists$ *counter-strategy* $v' \in V$

1) If Alice runs v' she achieves her goal.
2) The coercer cannot distinguish, whether she runs v or v' but with probability δ.

Privacy vs. Coercion-Resistance

Two **general** observations (illustrated by ThreeBallot):

1) Privacy can be worse than coercion-resistance!

2) Improving privacy of a protocol might worsen coercion-resistance!

Privacy vs. Coercion-Resistance

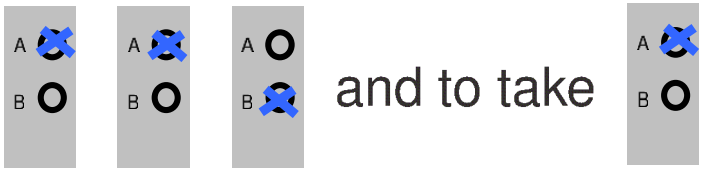
Illustrative (artificial) example:

An honest voter who wants to vote for A is supposed to submit either

and to take

as receipt

or



and to take

as receipt.

Analogously if she wants to vote for B.

- Level of privacy quite bad ($\geq \frac{1}{2}$), as the vote is revealed with probability $\frac{1}{2}$.
- Level of coercion-resistance is much better, as in the counter-strategy of the coerced voter the ballots might be filled out in a more clever way, e.g., in a way that never reveal the vote.
  Although the coercer learns approx. half of the votes of the honest voters, the coerced voter is hidden in the remaining half of the voters, which results in a quite small δ (depending of course on the number of voters).

Privacy vs. Coercion-Resistance

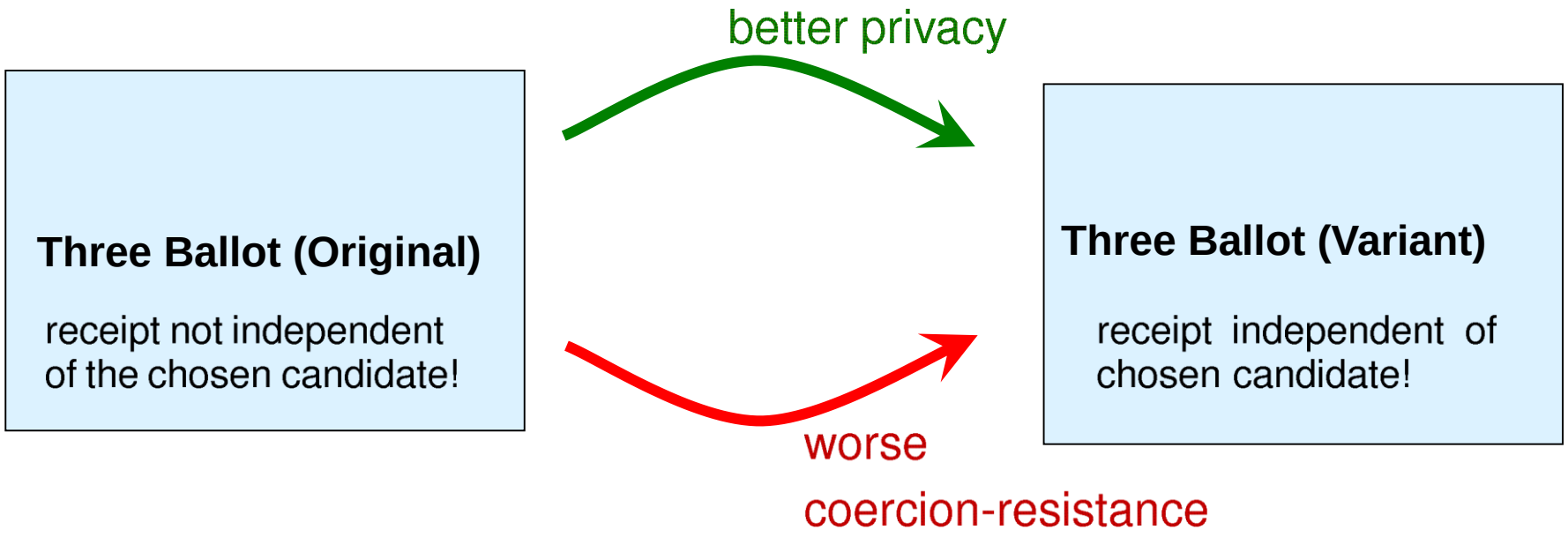
Two **general** observations (illustrated by ThreeBallot):

1) Privacy can be worse than coercion-resistance!

2) Improving privacy of a protocol might worsen coercion-resistance!

Privacy vs. Coercion-Resistance

2) Improving privacy of a protocol might worsen coercion-resistance!



ThreeBallot Variant

Receipt has marks for both candidates

- Ideal for privacy: receipt leaks no information about vote
- No coercion-resistance: If coerced voter asked to submit $\begin{pmatrix} o & x & o \\ \underline{x} & x & o \end{pmatrix}$ and he submits $\begin{pmatrix} o & x & x \\ \underline{x} & o & o \end{pmatrix}$; deviation can be detected by counting ballots of type $\begin{matrix} o \\ o \end{matrix}$ in the bulletin board

Acknowledgement

- Thanks to Ralf Kuesters for providing a number of slides used in this lecture.