Electronic Voting

Prof. Clarkson

CS 2110 — Spring 2019

Announcements

- **A7 is due Friday night.** Download your submission and double check against pinned A7 note. BIG deduction if it doesn't compile. No late submission accepted because we have to grade and then develop tentative grades for you.

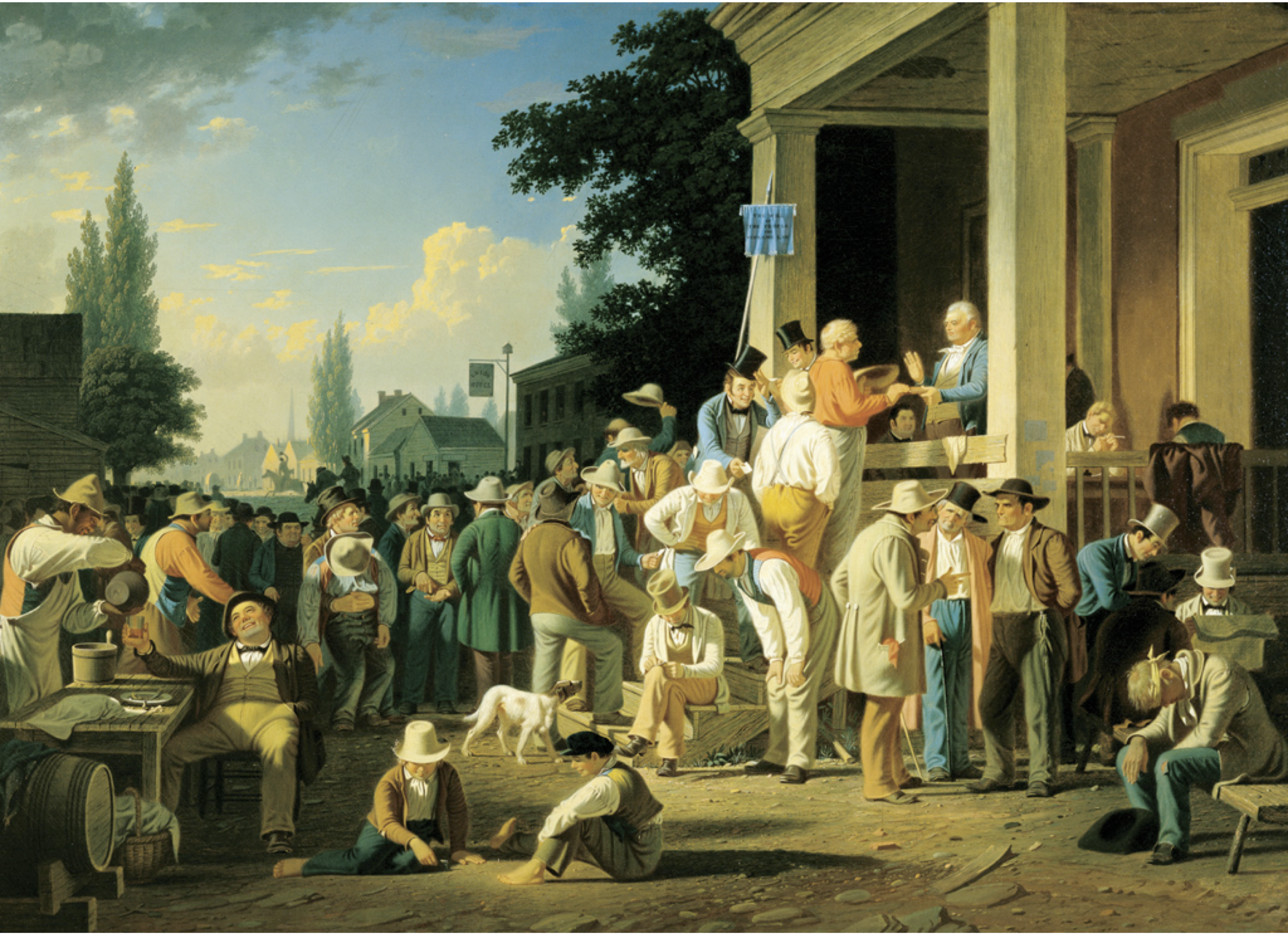
- **Course evaluations** small part of final grade; due Saturday midnight to be included in your tentative course grade.

- **Tentative course grades out as soon as we can.** Sunday evening at the earliest but could be later. Emailing/posting "when" or "how am I doing" isn't helpful.

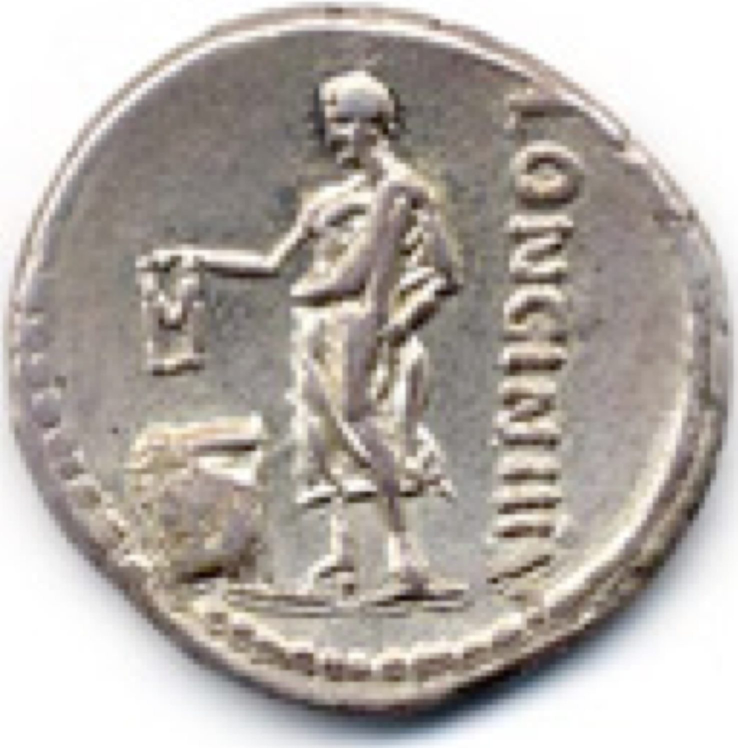
- CMS contains weights for all parts of the course. They add up to 93 because the course evaluations and A7 are not yet included. Weights are from syllabus:

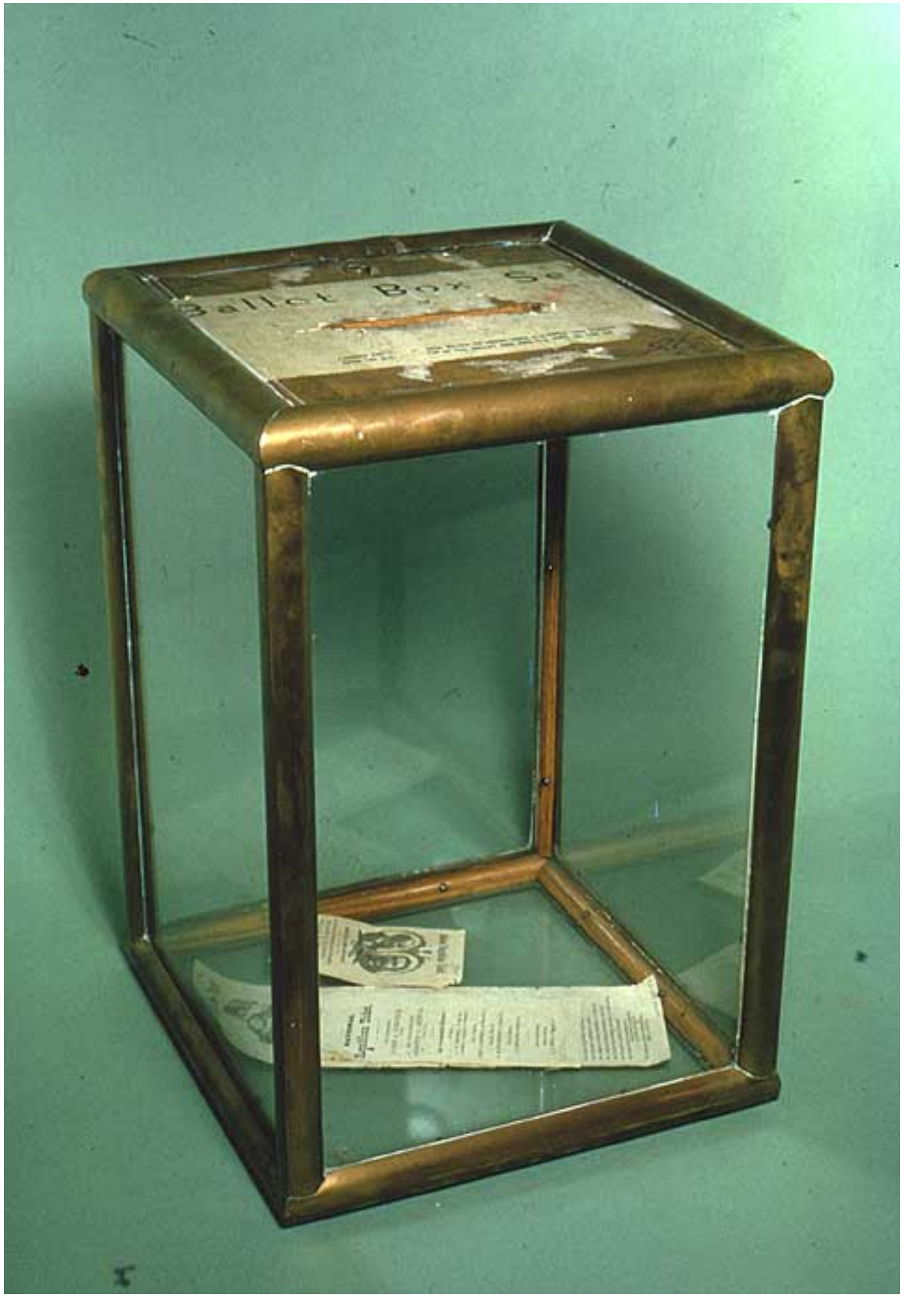
  http://www.cs.cornell.edu/courses/cs2110/2019sp/courseinfo.html#grading

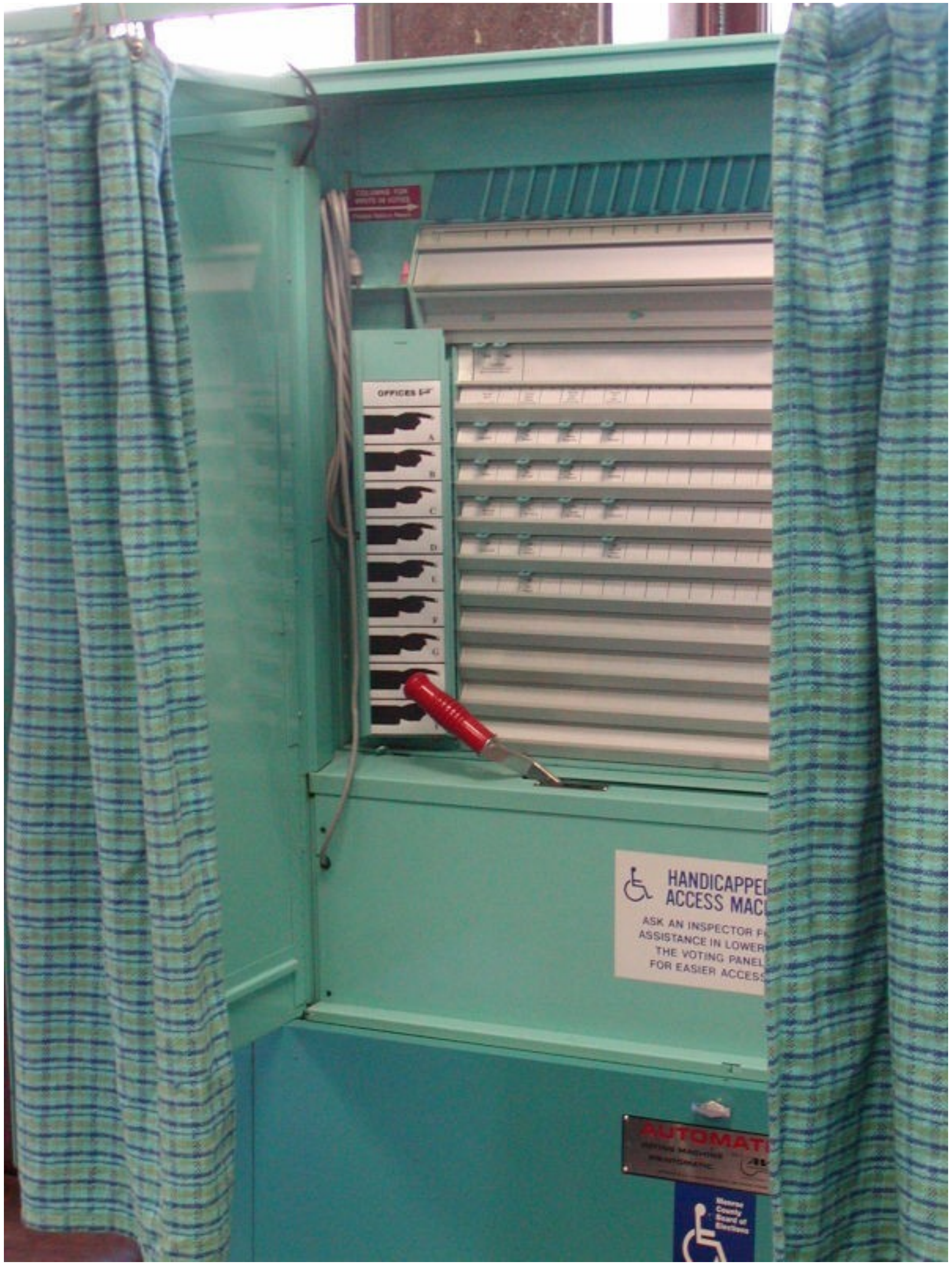
Piazza Poll

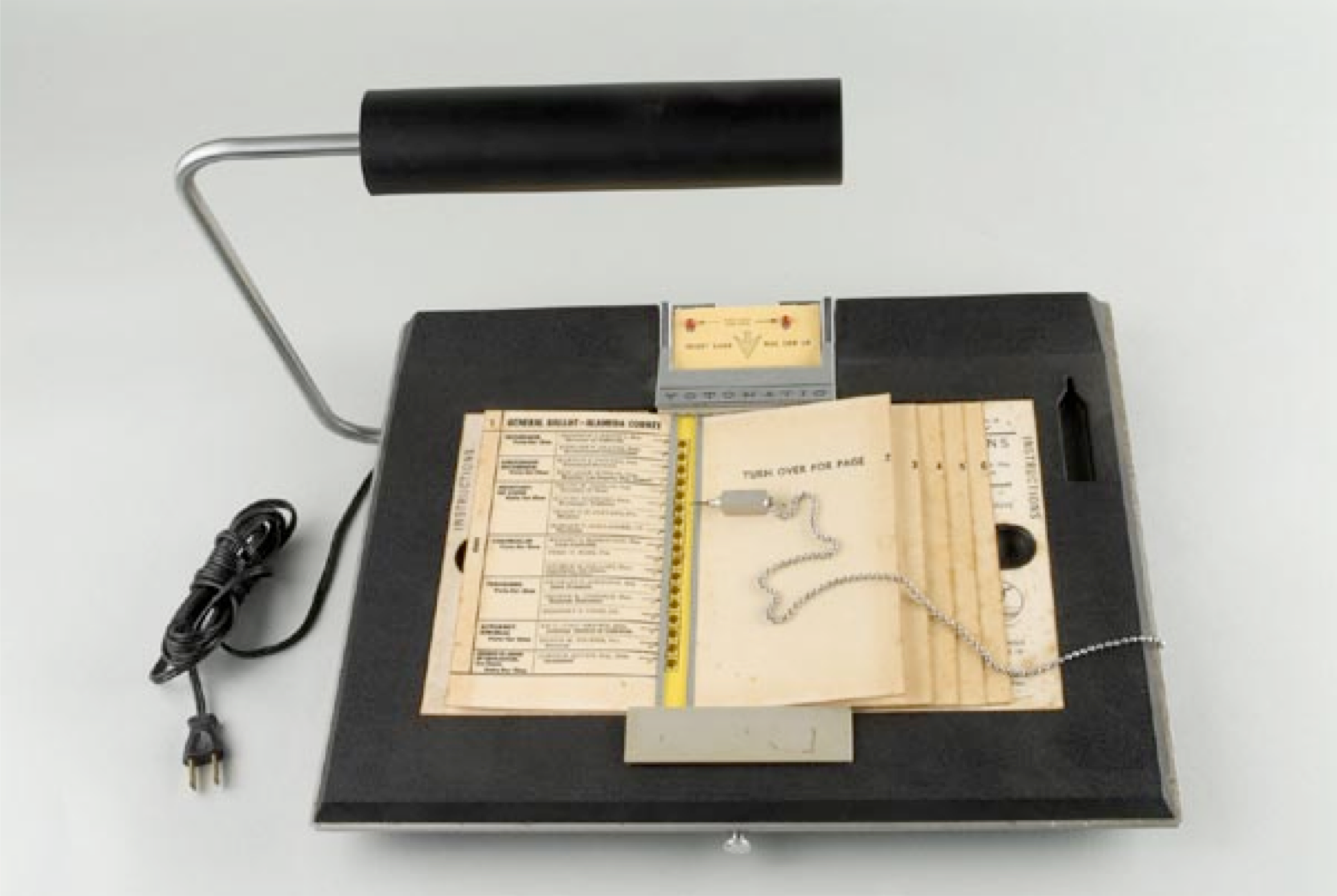


Secret Ballot


LONGINIIIV


Ballot Box Se


COLUMNS FOR
WRITE IN VOTES
OFFICES
A
B
C
D
E
F
G
HANDICAPPE
ACCESS MAC
ASK AN INSPECTOR F
ASSISTANCE IN LOWER
THE VOTING PANEL
FOR EASIER ACCESS
AUTOMAT
Monroe
County
Board of
Elections


VOTOMATIC
GENERAL BALLOT - ALAMEDA COUNTY
INSTRUCTIONS
TURN OVER FOR PAGE
INSTRUCTIONS

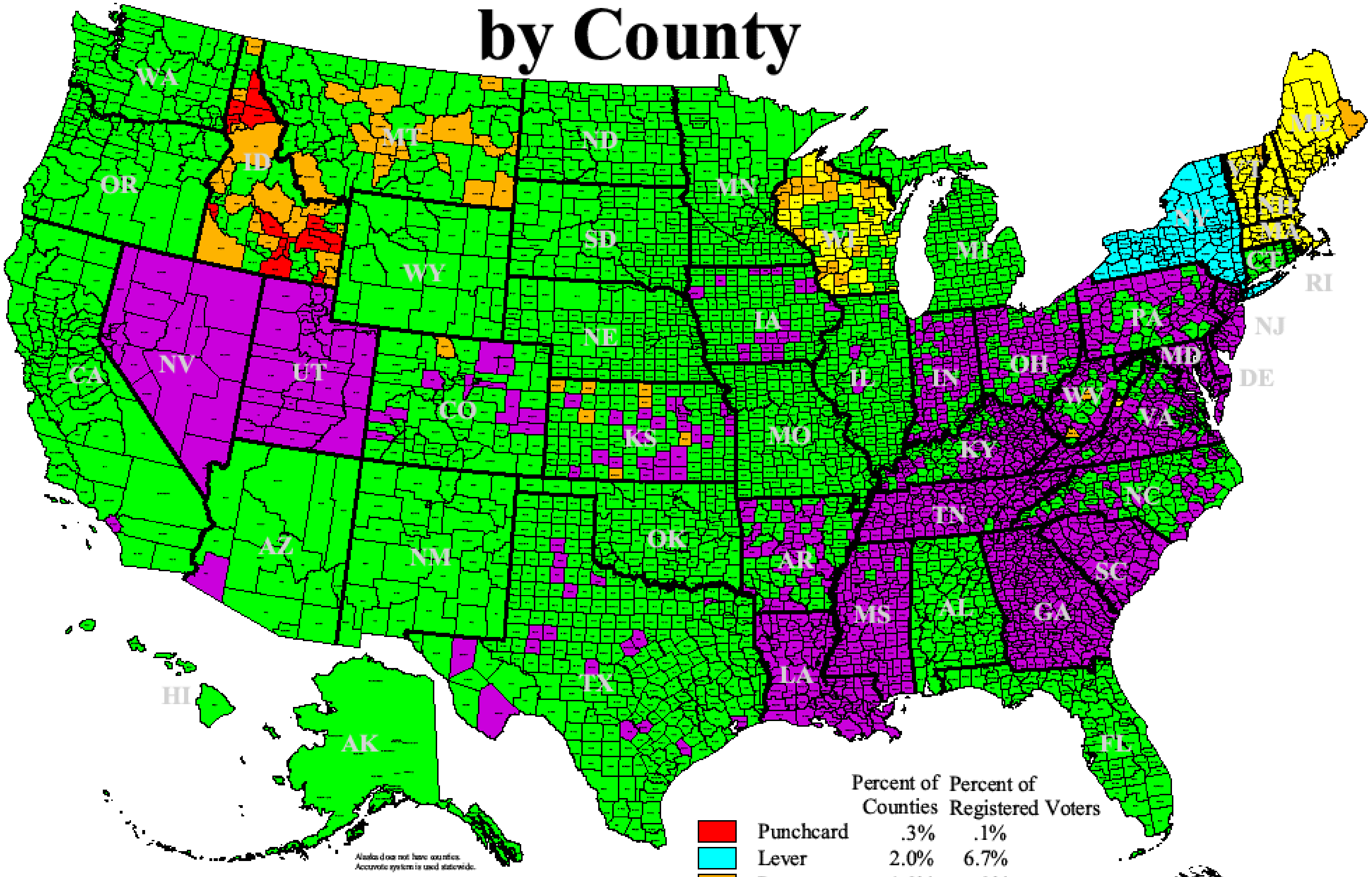
WB
WB
VOTE
BOTH
SIDES
— VOTE BOTH SIDES —

DIEBOLD
CLERK OF THE CIRCUIT COURT
Vote for One
Terry Bork
Republican
Democratic
Write in
Write in
BOARD OF EDUCATION
BOARD OF EDUCATION DISTRICT 1
Vote for One
Judy Docca
Michael Ibañez
Write in
BOARD OF EDUCATION
BOARD OF EDUCATION DISTRICT 3
Vote for One
SHERIFF
Vote for One
Republican
Philip

Florida 2000:
Bush v. Gore

“Flawless”

November 2008 Voting Equipment Usage by County



Alaska does not have counties.
Accuvote system is used statewide.

		Percent of Counties	Percent of Registered Voters
🟥	Punchcard	.3%	.1%
🟦	Lever	2.0%	6.7%
🟧	Paper	1.8%	.2%
🟩	Optical	58.9%	56.2%
🟪	Electronic	34.3%	32.6%
🟨	Mixed Systems	2.7%	4.2%

Equipment expected to be used in the November 2008 election as reported by state election officials and news media. The map shows equipment used at polling places, not necessarily absentee or disabled balloting.

Printed with information available as of 10/14/2008

Election Data Services
(202) 789-2004
6171 Emerywood Court
Manassas, VA 20112-3078
www.ElectionDataServices.com

Security FAIL

Analysis of an electronic voting system [Kohno et al. 2003, 2004]

- DRE trusts smartcards
- Hardcoded keys and initialization vectors
- Weak message integrity
- Cryptographically insecure random number generator
- ...

California top-to-bottom reviews [Bishop, Wagner, et al. 2007]

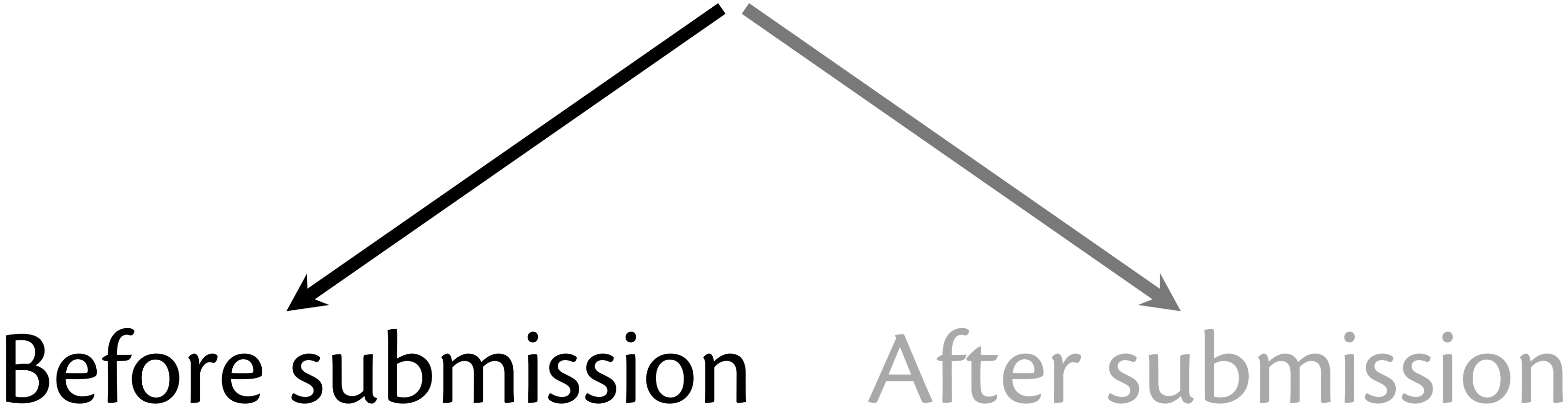
- *“Virtually every important software security mechanism is vulnerable to circumvention.”*
- *“An attacker could subvert a single polling place device…then reprogram every polling place device in the county.”*
- *“We could not find a single instance of correctly used cryptography that successfully accomplished the security purposes for which it was apparently intended.”*

Why is this so hard?

CONFIDENTIALITY INTEGRITY

Achieving Confidentiality

When is Vote Anonymized?



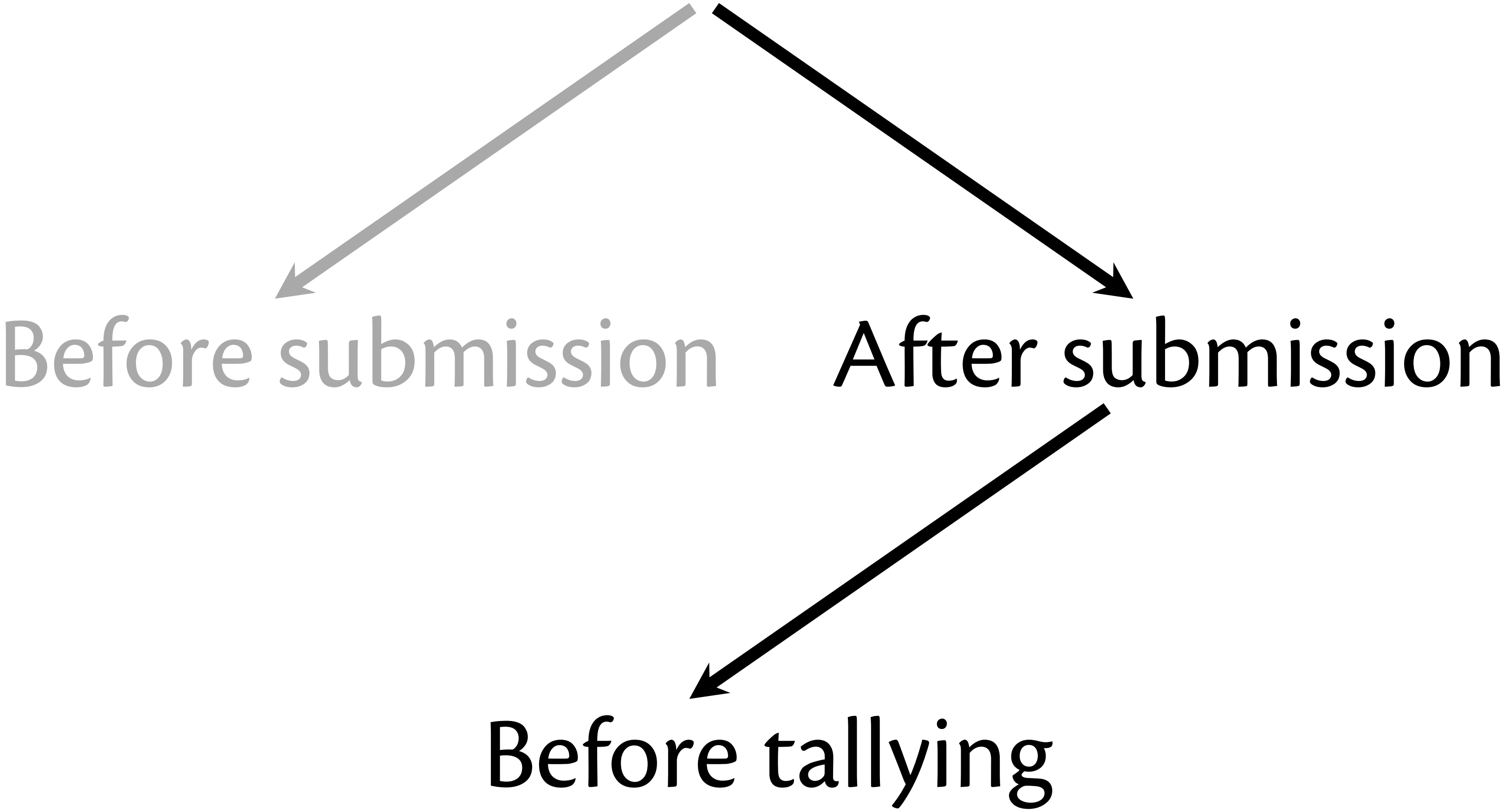
Before submission

After submission

Blind Signatures

[Chaum 1983]

When is Vote Anonymized?



Before submission

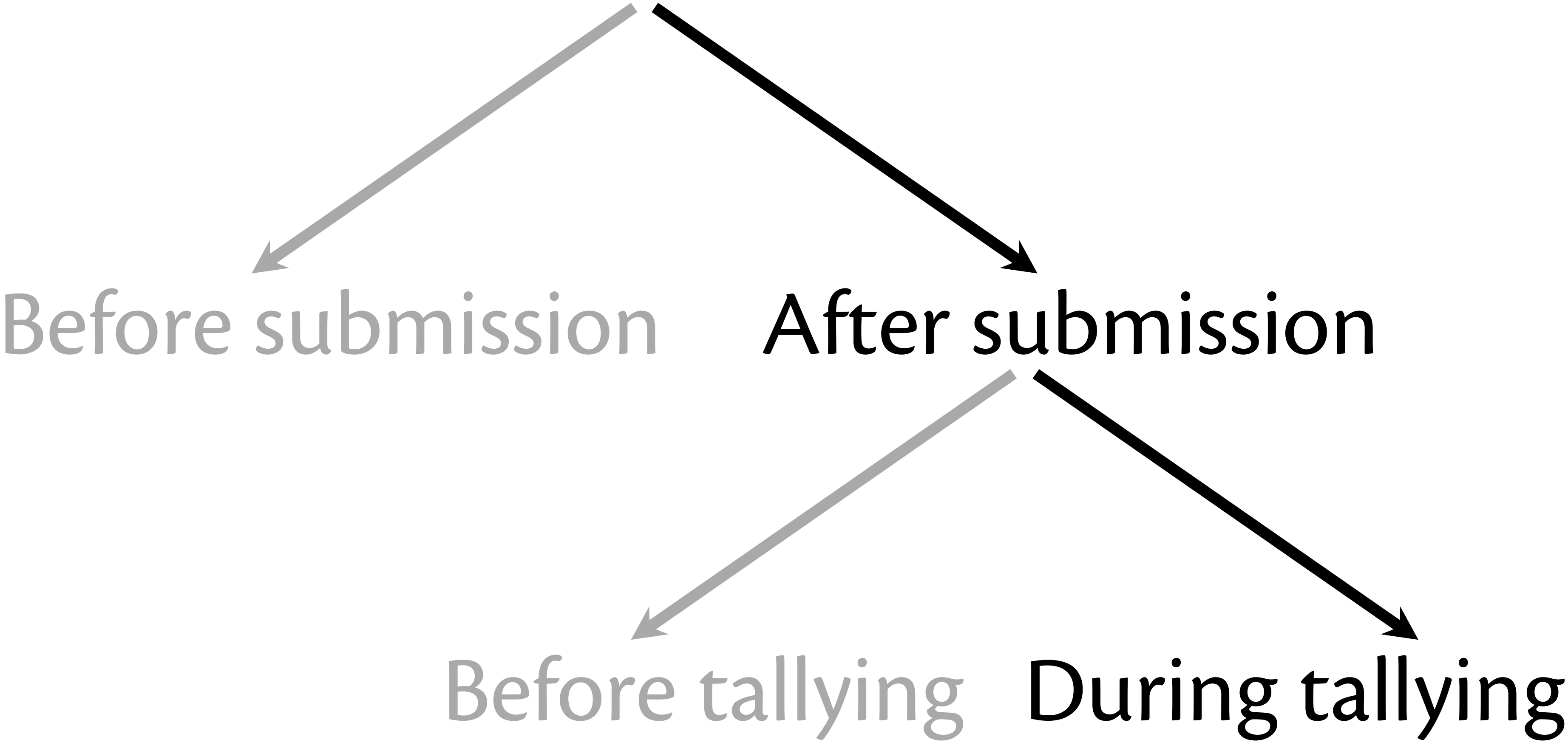
After submission

Before tallying

Mix Networks

[Chaum 1981]

When is Vote Anonymized?



Before submission

After submission

Before tallying

During tallying

Homomorphic Encryption

$$\begin{tikzcd}
G \times G \arrow[r, "(f,f)"] \arrow[d, "\circ_G"'] & H \times H \arrow[d, "\circ_H"] \\
G \arrow[r, "f"'] & H
\end{tikzcd}$$

[Rivest, Adleman, Dertouzos 1978]

$$\mathrm{enc}(v) \times \mathrm{enc}(v') = \mathrm{enc}(v+v')$$

Civitas

http://www.cs.cornell.edu/projects/civitas/

[Clarkson, Chong & Myers 2008]
based on [Juels, Catalano & Jakobsson 2005]

Implementation: 21k LoC in Java and Jif

11 years later

What can you do?