

# 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>

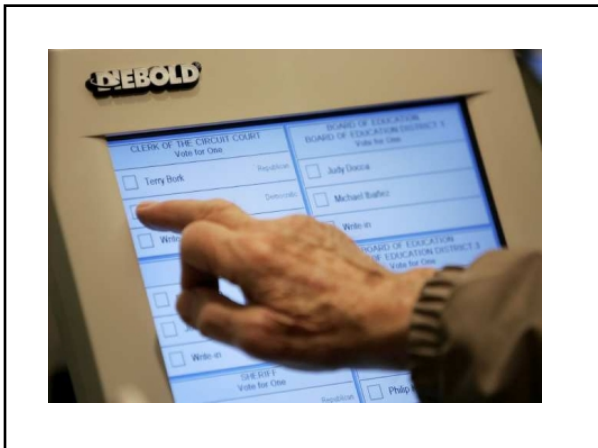
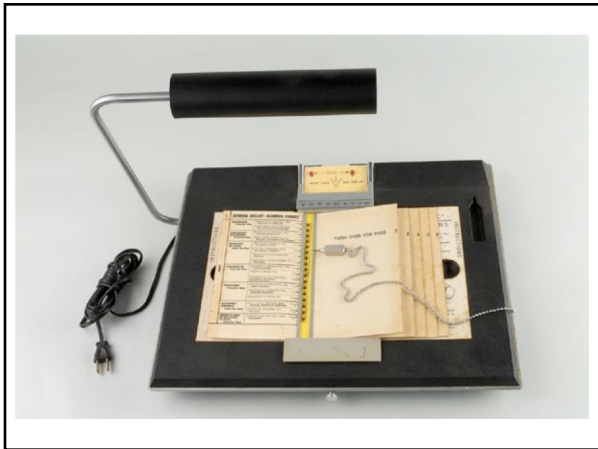
2

## Piazza Poll



## Secret Ballot

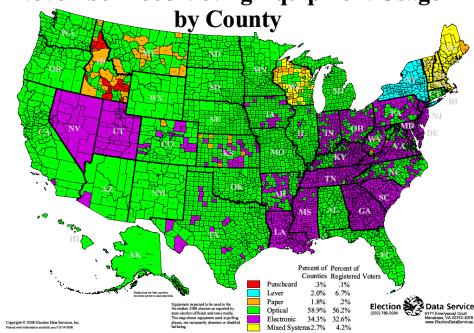




Florida 2000:  
**Bush** v. **Gore**

“Flawless”

November 2008 Voting Equipment Usage by County



14

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



19

# Achieving Confidentiality

## When is Vote Anonymized?

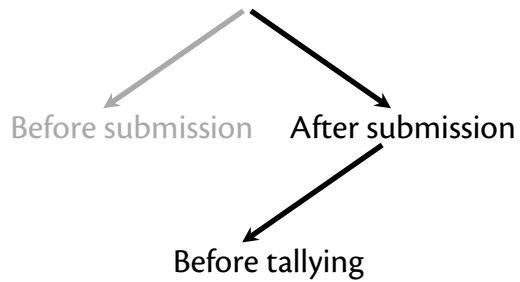


## Blind Signatures



[Chaum 1983]

## When is Vote Anonymized?

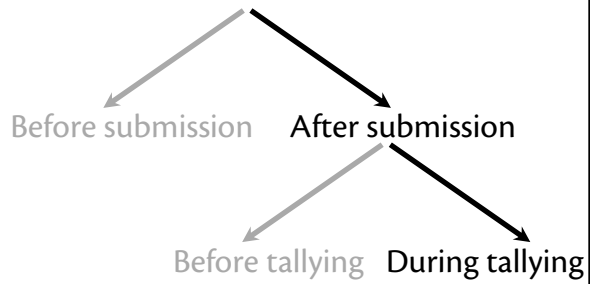


## Mix Networks

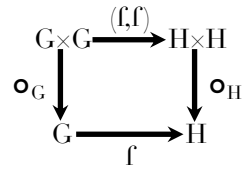


[Chaum 1981]

## When is Vote Anonymized?



## Homomorphic Encryption



[Rivest, Adleman, Dertouzos 1978]

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

## 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?

