Revisiting silent coercion

David Chaum
Richard T. Carback III
Mario Yaksetig

Jeremy Clark***
Mahdi Nejadgholi

Filip Zagórski

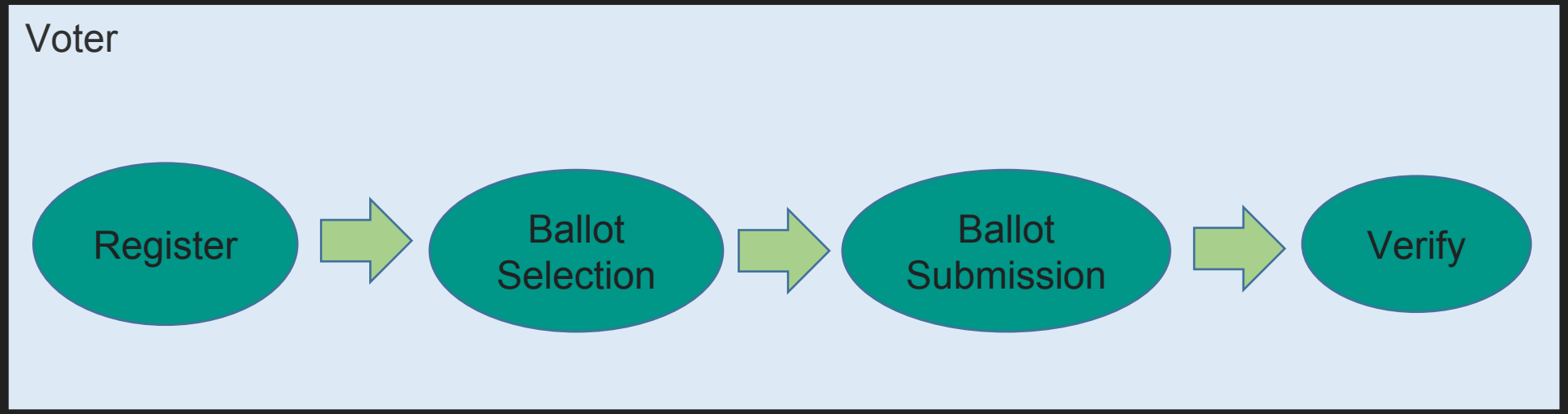
Alan Sherman
Chao Liu

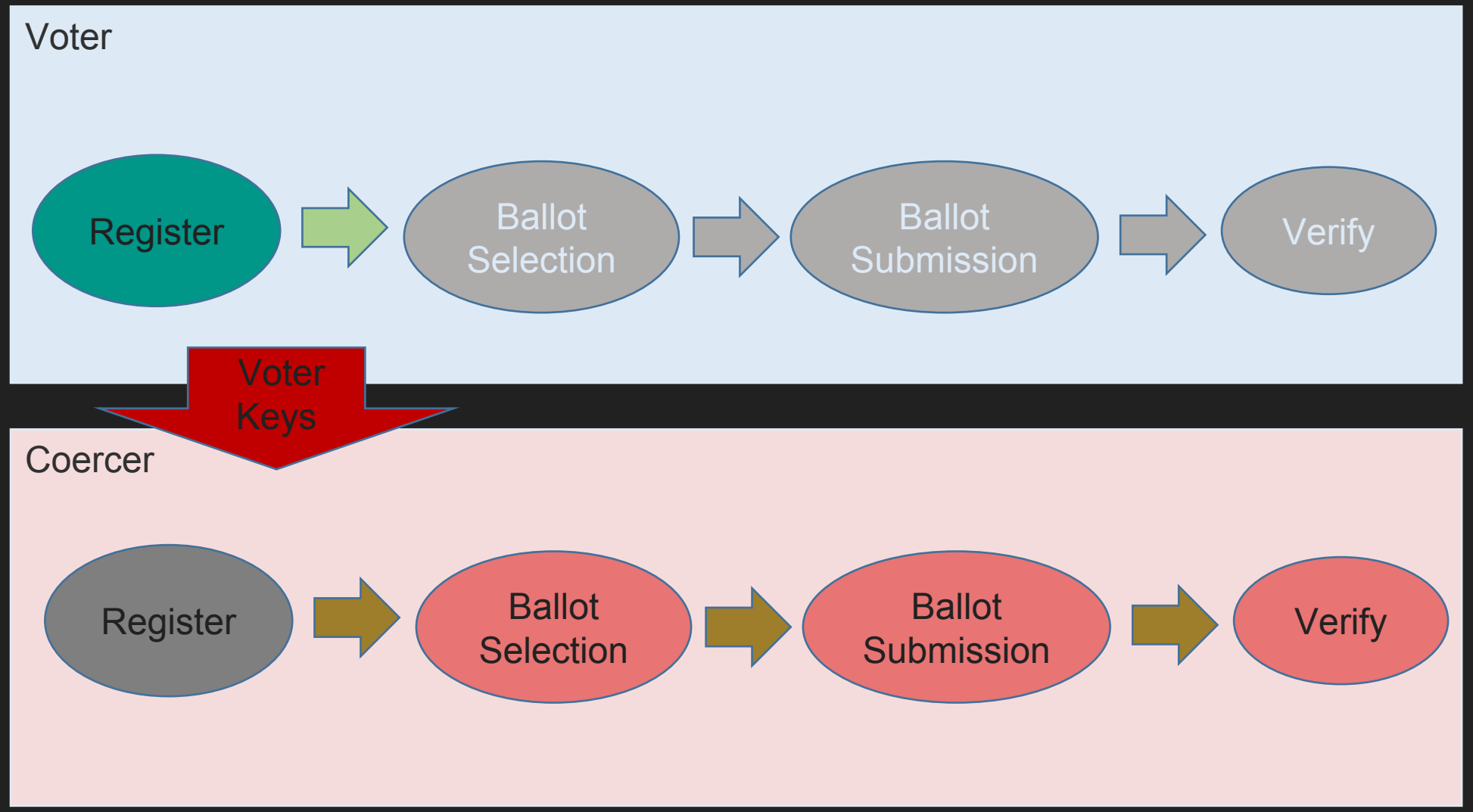
Zeyuan Yin
Bingsheng Zhang

Bart Preneel

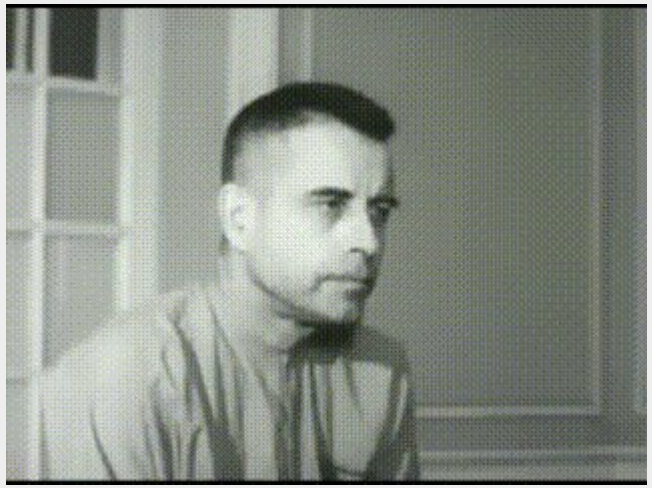
A worst case scenario

Suffragist Helena Hill looks out from her cell.
From the collections of the Library of Congress (https://www.loc.gov/static/exhibitions/women-fight-for-the-vote/images/objects/ws0097_standard.jpg).


Voter
Register
Ballot Selection
Ballot Submission
Verify

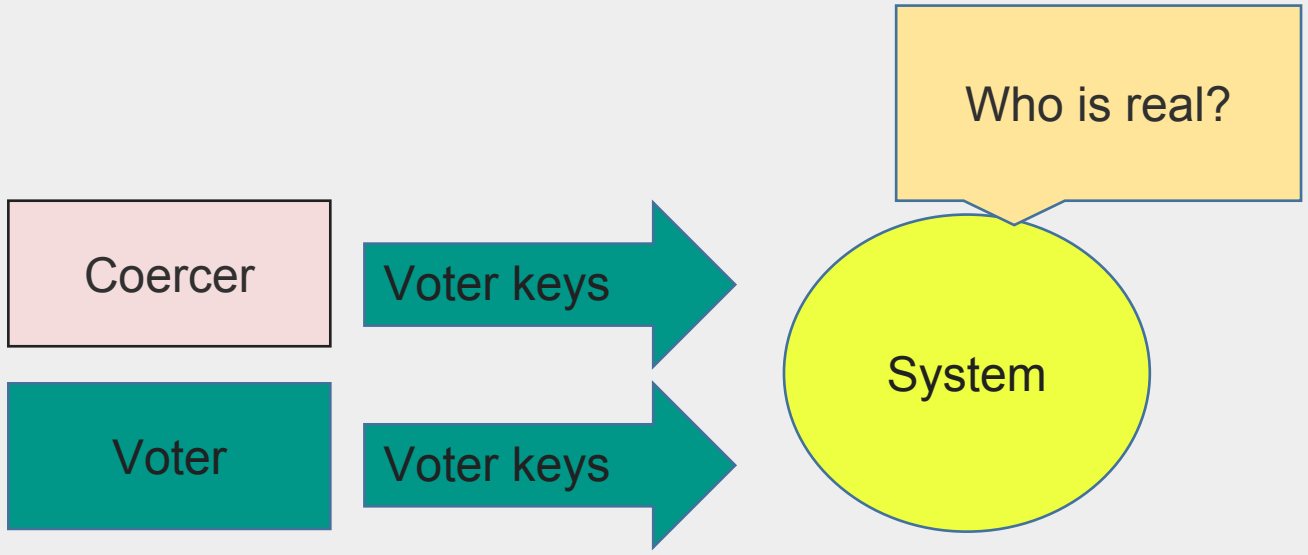

Voter
Register
Ballot Selection
Ballot Submission
Verify
Voter Keys
Coercer
Register
Ballot Selection
Ballot Submission
Verify

You can always send a signal



Admiral Jeremiah Andrew Denton Jr. spelling TORTURE in morse code with his eyes while a prisoner in vietnam

Fundamental Limitation



Answer: Sabotage (Nullification)

Nullification front end

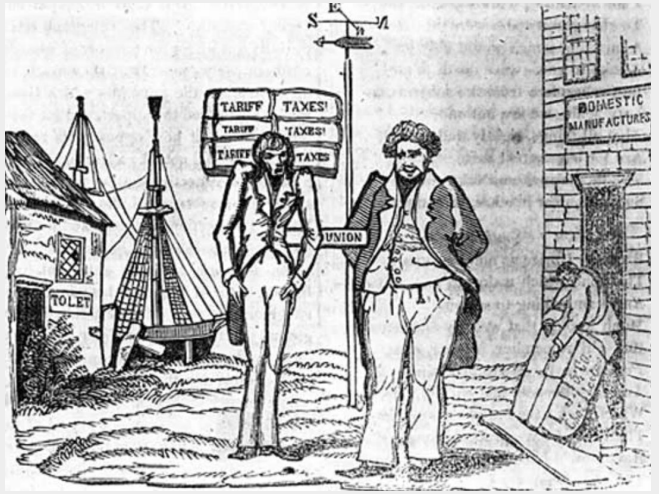
- A voter is eligible because they know a secret key
- The voter can see how they voted from bulletin board
- Voter can add a flag to their ballot for filtering after it is anonymized

We can wrap (overlay) any existing system that can support the above

Nullification front end

- A voter is eligible because they know a secret key
- **The voter can see how they voted from bulletin board**
- Voter can add a flag to their ballot for filtering after it is anonymized

What!?



Nullification Crisis, in U.S. history, confrontation between the state of South Carolina and the federal government in 1832–33 over the former's attempt to declare null and void within the state the federal Tariffs of 1828 and 1832. https://www.britannica.com/topic/Nullification-Crisis#/media/1/1808989/113277

Overview

- Voters sign ballot with a “yes” or “no” key and anonymously submit encrypted ballot to bulletin board
- EA decrypts and computes provisional tally
  - If “yes” signature present, “no” key can nullify
  - If “no” signature present, “yes” key can nullify

Specific to VoteXX, see paper for how it works for JCJ and Selections

- Nullifier (hedgehog) provides ZK proof with vector indicating which ballot to nullify, it proves knowledge of nullification key. EA then does final tally by computing nullification under encryption

Hedgehogs

- Semi-trusted, not required
- Can only vote “one-way”
  - If nullifying a “yes”, only given keys for “no”
  - If nullifying a “no, only given keys for “yes”
- Voters can do it, but hedgehogs are dedicated monitors

Prickly, hard to threaten (wikipedia.org)

Vote Flipping?

- Useful for “spousal coercion” scenarios
- Devolves into randomization of the vote which is roughly the same as nullification

https://x.com/TheDailyShow/status/796055685511446528

There is a lot more to do...

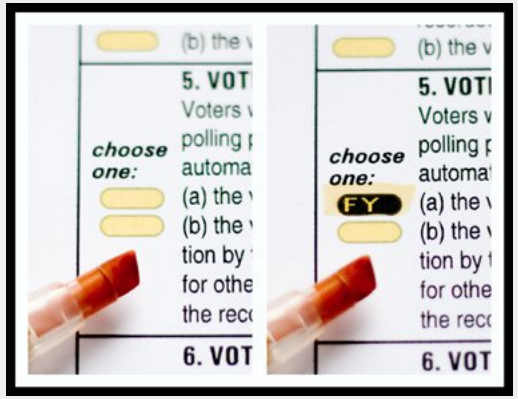
- This is a technique with a lot of optionality
  - Combining with other techniques should create powerful systems
- Add Inalienable authentication, malware protection, other techniques
- Overlay approach allows composability with panic passwords, re-voting, etc
- The paper has more discussion and details

Thank you

I'm inter/multi-disciplinary, ask me anything!

Richard T. Carback III
rick@carback.us
https://carback.us/rick

DRAPER
DRAPER LAB



UMBC

XX.NETWORK

Analysis of well-annotated next-generation sequencing data reveals increasing cases of SARS-CoV-2 reinfection with Omicron [PDF] nature.com

…, M Rubsamen, L Blankenberg, RT **Carback** III… - Communications …, 2023 - nature.com

SARS-CoV-2 has extensively mutated creating variants of concern (VOC) resulting in global infection surges. The Omicron VOC reinfects individuals exposed to earlier variants of SARS…

☆ Save 99 Cite Cited by 13 Related articles All 8 versions

quip

My Current Project: Quantum Computing
https://quip.network/