Votegral:
Towards Usable Coercion-Resistant Online Voting Systems

Louis-Henri Merino
DEDIS lab
Prof. Bryan Ford

PhD Defense

Sep 24, 2025

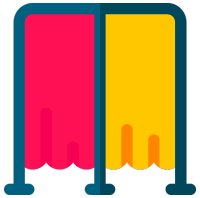
What are the Risks with Online Voting?

In-Person Voting

Software-Independent, Auditable Paper Record

Public Transparency

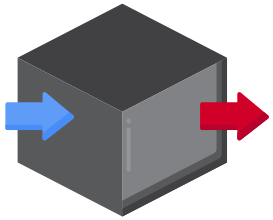
Online Voting



Ballot Secrecy

Online Voting Risks

Untrusted Devices



Opaque Counting

Coercion Attacks

Online voting naively does not offer the same voter protections as in-person voting.

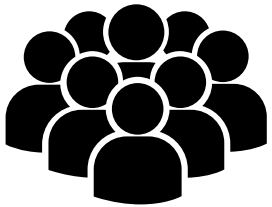
What are the Desired System Properties of an Online Voting System?

Universal Verifiability

Individual Verifiability

Ballot Secrecy

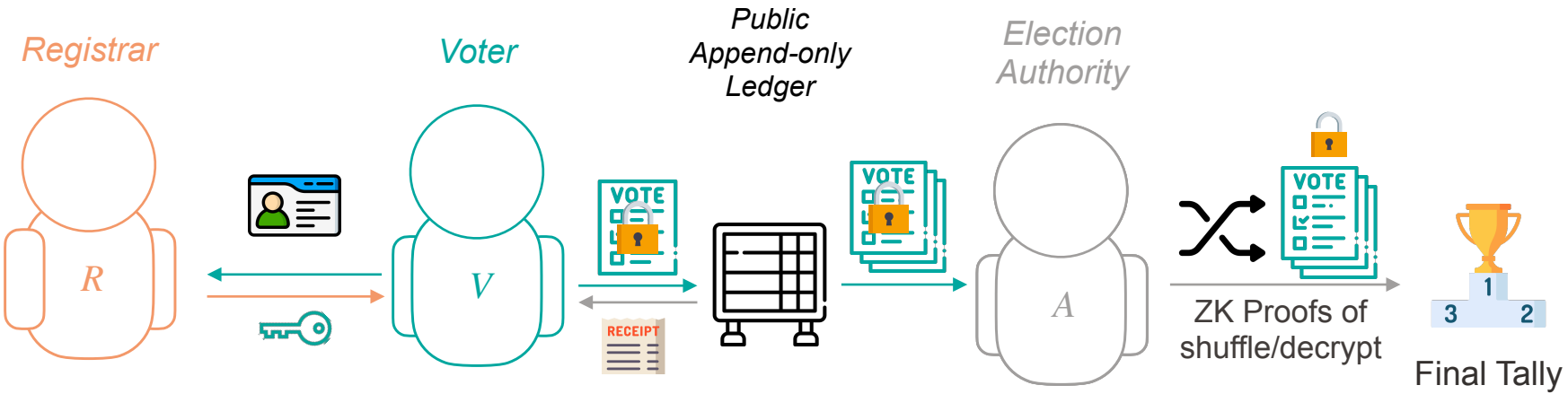
Coercion-resistance



Scalability and Availability

Usability

Modern Online Voting Systems:
End-to-end Verifiable Electronic Voting



System Properties:
End-to-End Verifiable Voting Systems

Universal Verifiability

Individual Verifiability

Ballot Secrecy

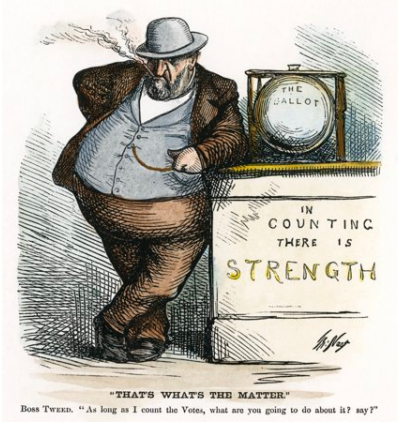
Coercion-resistance

Scalability and Availability

Usability

Why is Coercion Important?

Historical Events



William “Boss” Tweed
(NYC - 1860s)

Present Day Events

October 25, 2024 11:42 CET

By RFE/RL's Moldovan Service

Moldovan Police Accuse Pro-Russian Oligarch Of $39M Vote-Buying Scheme

Saving Democracy: Reducing Gang Influence on Political Elections in El Salvador

Eleno Castro & Randy Kotti

Advisor: Gautam Nair, Section Leader: Rema Hanna
John F. Kennedy School of Government, Harvard University
In fulfilment of the requirements for the Master in Public Administration in International Development

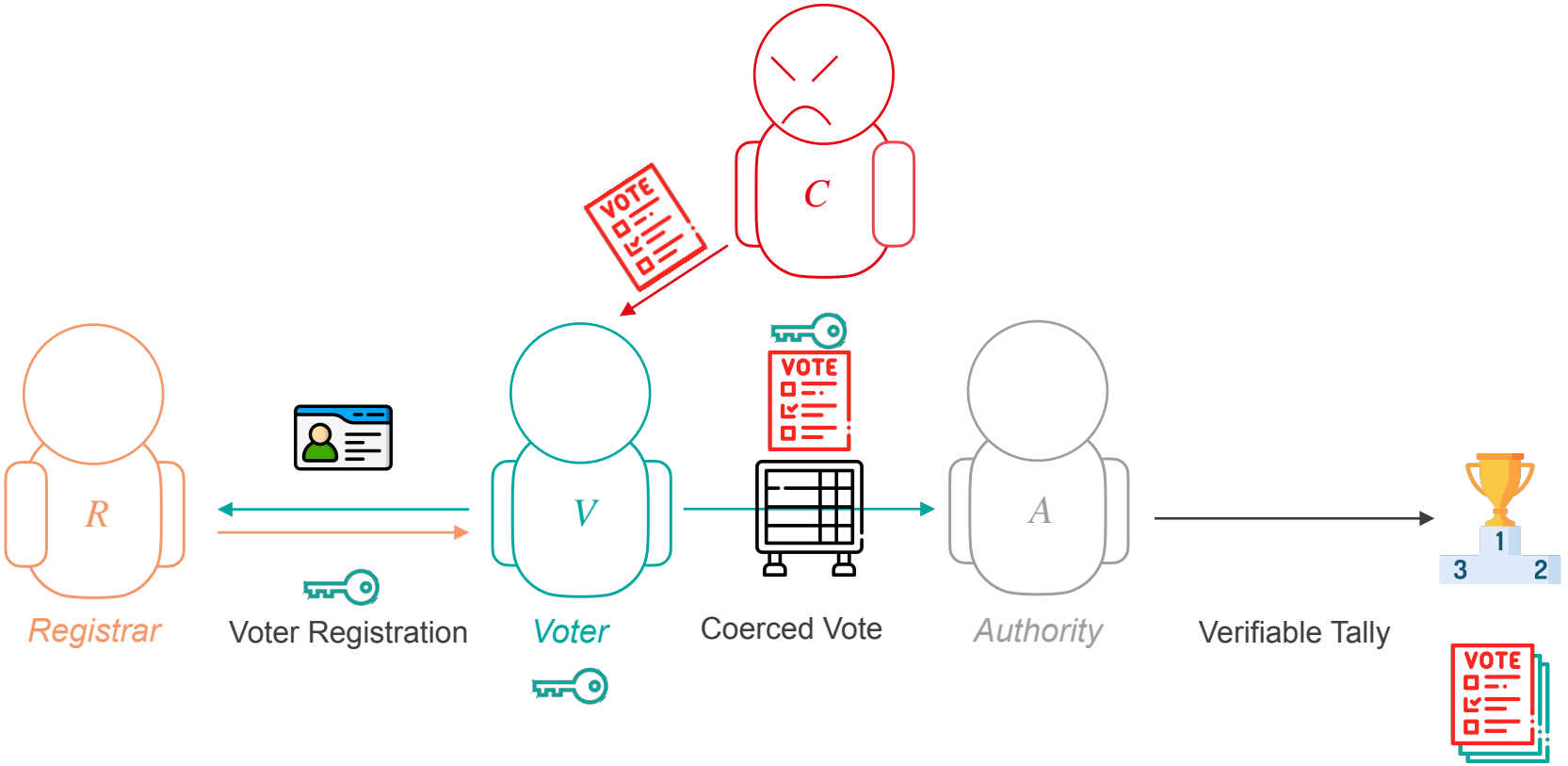
Sept. 27, 2022, 3:33 AM CEST / Source: Associated Press

By The Associated Press

RALEIGH, N.C. – Four people pleaded guilty on Monday to misdemeanors for their roles in absentee ballot fraud in rural North Carolina during the 2016 and 2018 elections. The convictions stemmed from an investigation that in part resulted in a do-over congressional election.

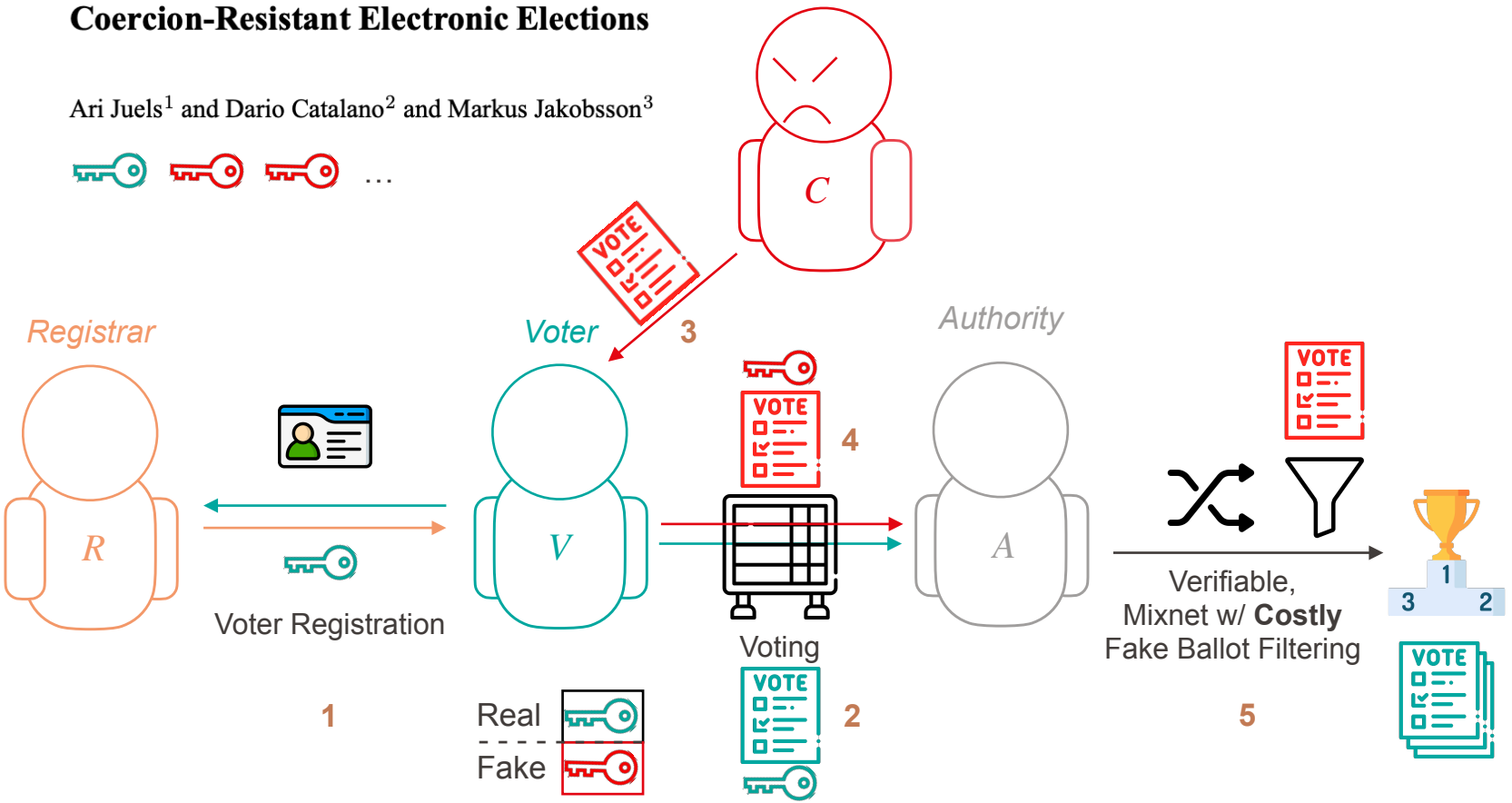
Coercion and voter intimidation remains a prevalent issue today

E2E Voting Systems: Voter Under Coercion



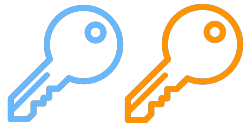
E2E verifies integrity of what was cast, not the freedom with which it was cast

Coercion-Resistant Online Voting

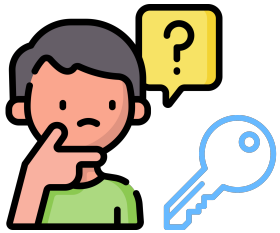


Fake credentials allow voters to appear compliant with the coercer's demands

Challenges



Coercion-Resistance (Credential Issuance):
How can the system deliver real and fake credentials to voters in a manner *only* the voter can identify their real credential from fake ones?



Individual Verifiability (Private Confirmation):
How can the system convince voters that their real credential casts ballots that count in elections?

Scalability:
How to make the filtering process efficient and robust?

Usability:
Can voters understand and use fake credentials?

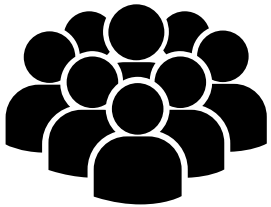
System Properties:
Coercion-Resistant E-Voting Systems

Universal Verifiability

Individual Verifiability

Ballot Secrecy

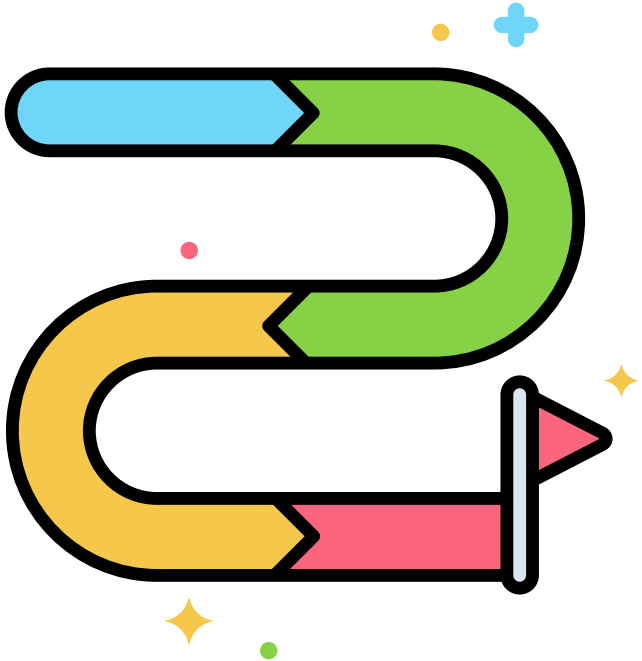
Coercion-resistance



Scalability and Availability

Usability

Roadmap



- Background
- **Contributions and Model**
- Votegral: TRIP
- Votegral: VLT
- Discussion

High-Level Contributions

Design Registration Process: TRIP
- Modeled after in-person voting
- Verifiable issuance of real cred.
- Fake credentials distinguishable only to the voter.

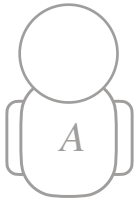
Conduct Usability Study on TRIP
- Understand fake credentials?
- Reliably distinguish real from fake?
- Detect malicious real cred. issuance?

Design Tallying Process: VLT
- Delegated voting when faced with extreme coercion
- Coercion Evidence

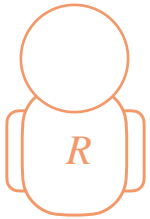
Merino, Louis-Henri, Alaleh Azhir, Haoqian Zhang, et al. “E-Vote Your Conscience: Perceptions of Coercion and Vote Buying, and the Usability of Fake Credentials in Online Voting.” *2024 IEEE Symposium on Security and Privacy (SP)*, May 2024, 3478–96.

Merino, Louis-Henri, Simone Colombo, Rene Reyes, et al. “TRIP: Coercion-Resistant Registration for E-Voting with Verifiability and Usability in Votegral.” *2025 Symposium on Operating Systems Principles (SOSP)*. October 2025.

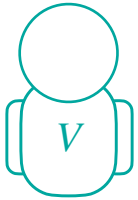
Actors



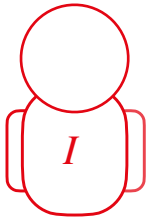
Authority (n members):
Tallies Ballots



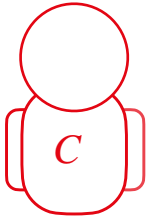
Registrar:
Issues voters their real and fake credentials



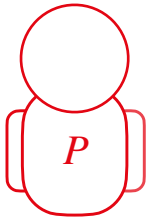
Voter:
Casts votes



Integrity:
Alter election outcome *undetected*



Coercer:
Force compliance of a target voter

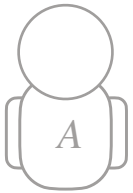


Privacy:
Learn an honest voter's vote

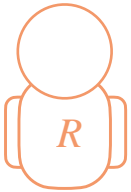
Threat Model

Can compromise

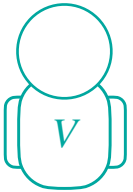
Trusted



Election Authority

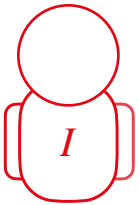


Registrar



Voters

Integrity

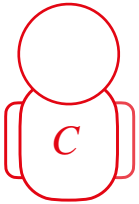


n_A

n_R

n_V

Coercer



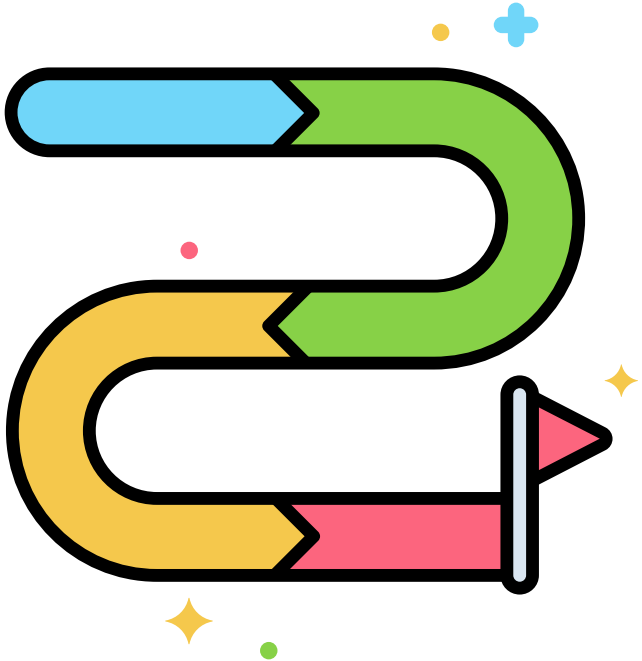
$n_A - 1$

$\varnothing$

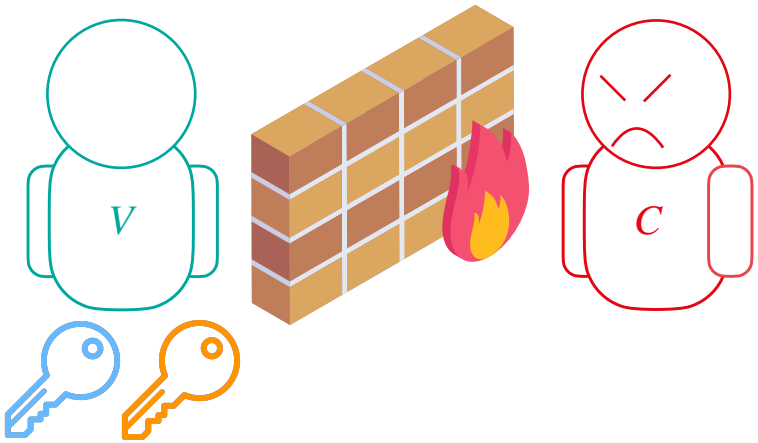
$C_S \subset V$

Modeled after E2E Voting Systems and after in-person voting

Roadmap



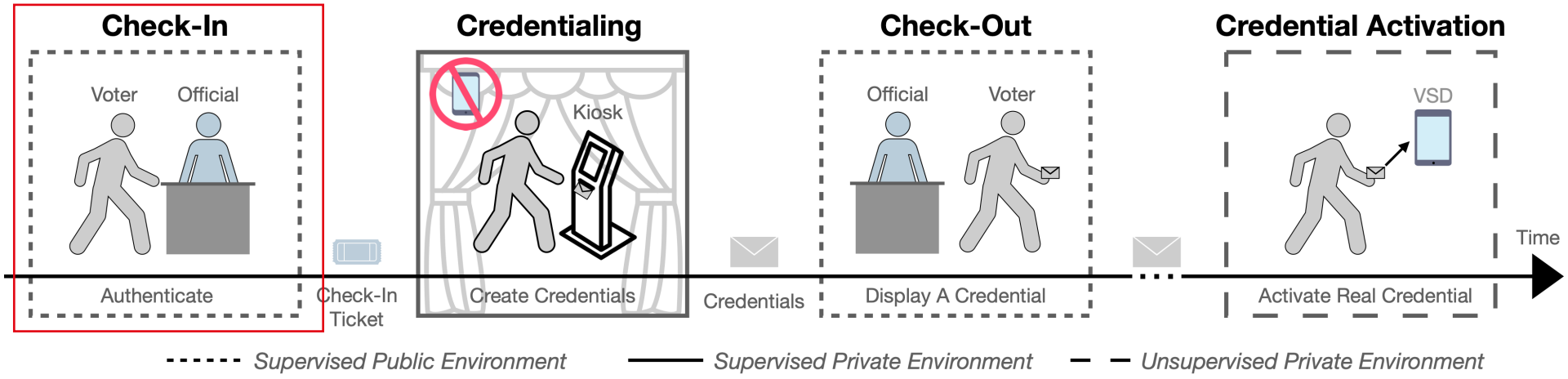
- Background
- Contributions and Model
- **Votegral: TRIP**
- Votegral: VLT
- Discussion

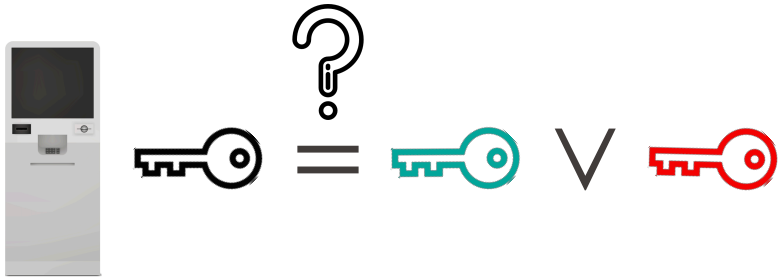


Credential Issuance:
How can the system deliver real and fake credentials to voters in a manner where *only* the voter can tell real from fake?

- **TRIP**
  - **Coercion-Resistance**
  - Individual Verifiability
  - Usability

Supervised In-Person Voter Registration

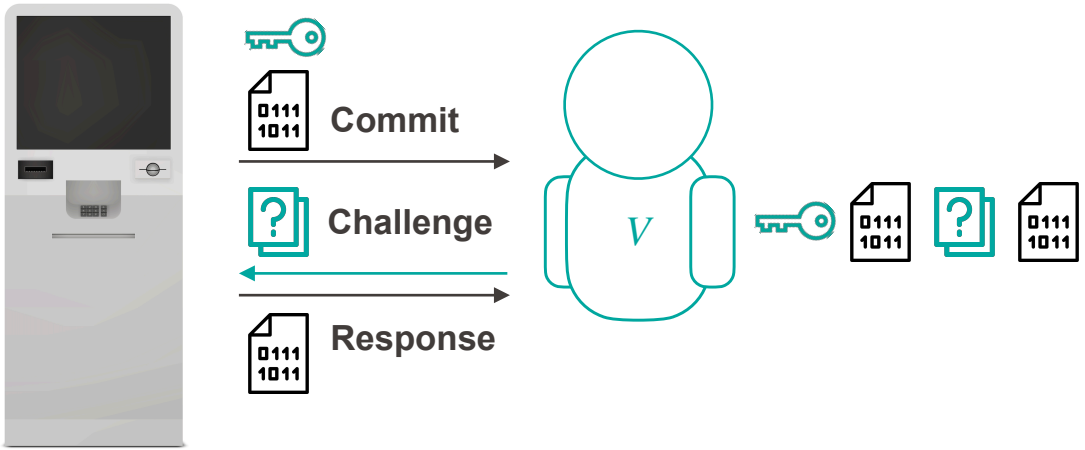




Individual Verifiability:
How can the system convince voters that their real credential casts ballots that count in elections?

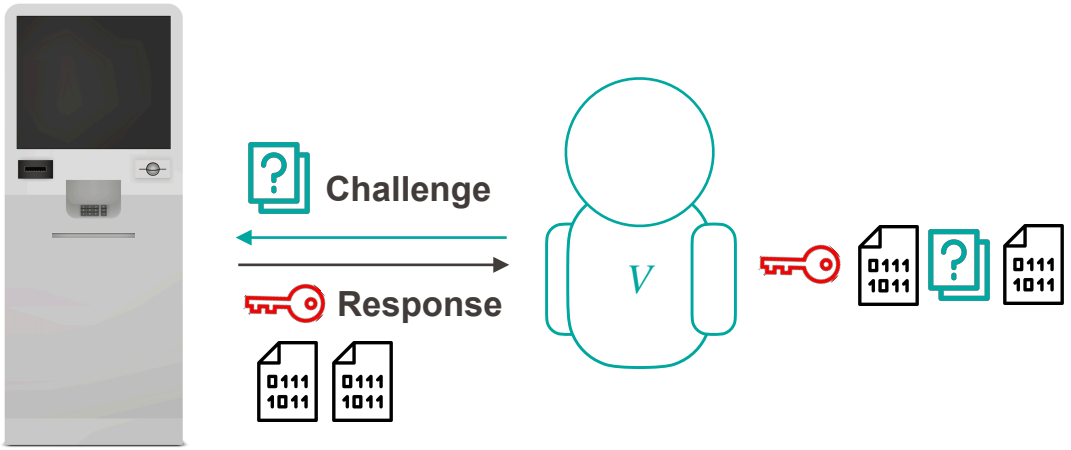
- **TRIP**
  - Coercion-Resistance
  - **Individual Verifiability**
  - Usability

Real Credential Issuance: Schnorr interactive zero-knowledge proof



- ✓ Kiosk forced to maintain integrity of the real credential
- ✗ Cannot create fake credentials using this process

Fake Credential Issuance:
Simulated Schnorr interactive zero-knowledge proof



- Voters can *visually* distinguish real and fake credentials (3 vs 2 steps)
- Real and fake credentials *indistinguishable* outside privacy booth

Usability:
- Comprehension of fake credentials
- The ability to distinguish real from fake when intending to cast their real credential.
- The ability to notice a misbehaving kiosk.

- **TRIP**
  - Coercion-Resistance
  - Individual Verifiability
  - **Usability**

QR Codes on Paper

Credential Issuance (Inside Booth)

Credential Activation (After In-Person Registration)

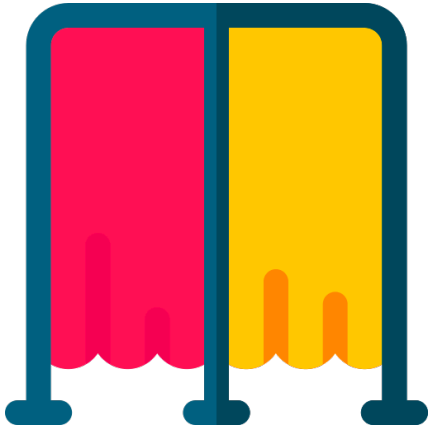
QR Codes on receipt paper

“Digitize” credential

- Resistant to Wear/Tear use
- Inexpensive (Paper)
- Freedom of device
- Visually verify IZKP order

- No Additional Voting Hardware
- Freedom of device choice
- Verify cryptographic IZKP transcript

How do we put together all these pieces?



Privacy Booth

Kiosk

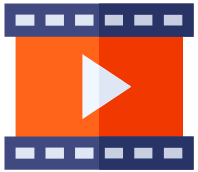
Interactive Zero-Knowledge Proofs

Real and Fake Credentials

QR Codes

User Study Design

- 150 participants
- Suburban Park in Boston, Massachusetts, U.S.A.



Instructional Video →  **Registration** →  **Vote** →  **Survey**

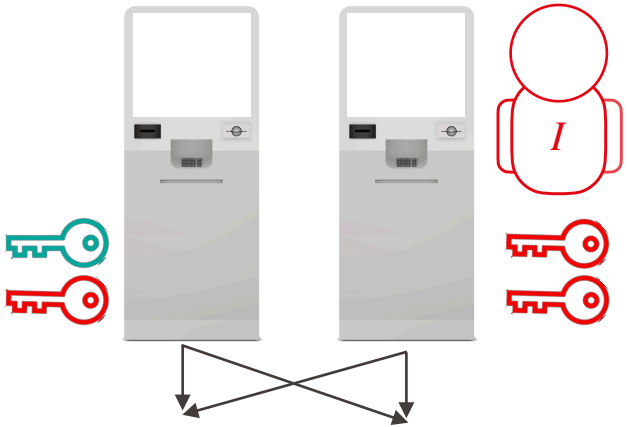
- Quizzes
- System Usability Scale
- User Experience Questionnaire
- System Trust Rating
- Coercion Occurrence

~30 min per participant

Control + Treatment Groups

Control Group

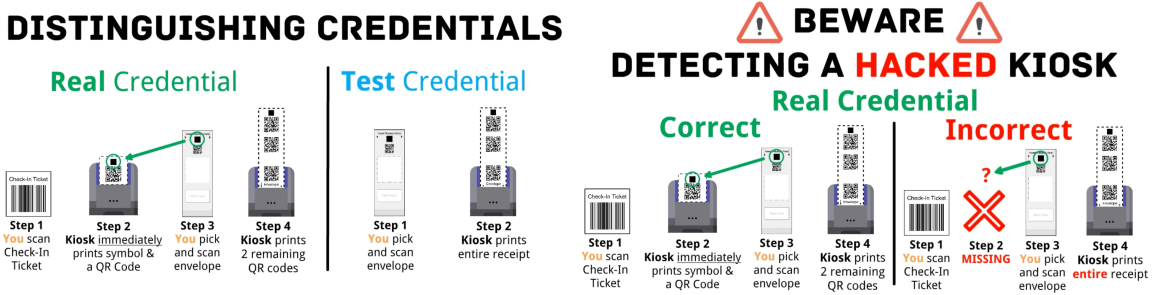
Video A (Real only)



Honest OR Malicious Kiosk

Video B (Real + Fake)

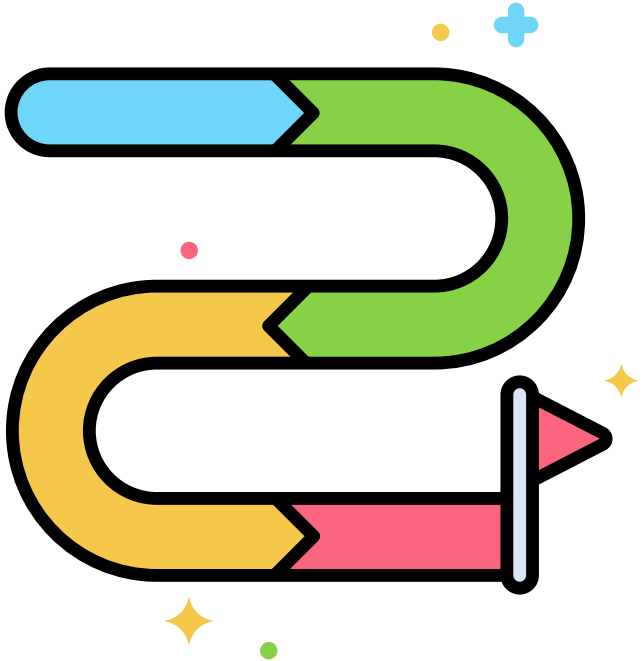
Video C (B + Security Priming)



User Study Results (Highlights)

- **Participants' Background**
  - Average/Median Age: 44 and 36.5.
  - 26% of participants reported experiencing, or know someone who has experienced coercion.
- **Usability**
  - 83% of participants created and activated their credentials & cast a real vote
  - With security priming, 47% of participants reported the malicious kiosk to facilitator; 10% without.
- **Fake Credentials**
  - 96% understood the use of fake credentials
  - 90% can distinguish their real and fake credential to cast a real vote
  - 53% said they would create fake credentials in the real world

Roadmap



- Background
- Contributions and Model
- Votegral: TRIP
- **Votegral: VLT**
- Discussion

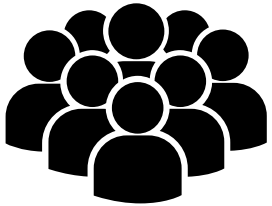
System Properties:
End-to-End Verifiable Voting Systems

Universal Verifiability

Individual Verifiability

Ballot Secrecy

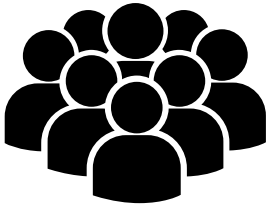
Coercion-resistance



Scalability and Availability

Usability

Challenges

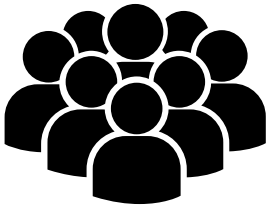


Scalability and Availability

How to tally votes efficiently and verifiably?

Extreme Coercion

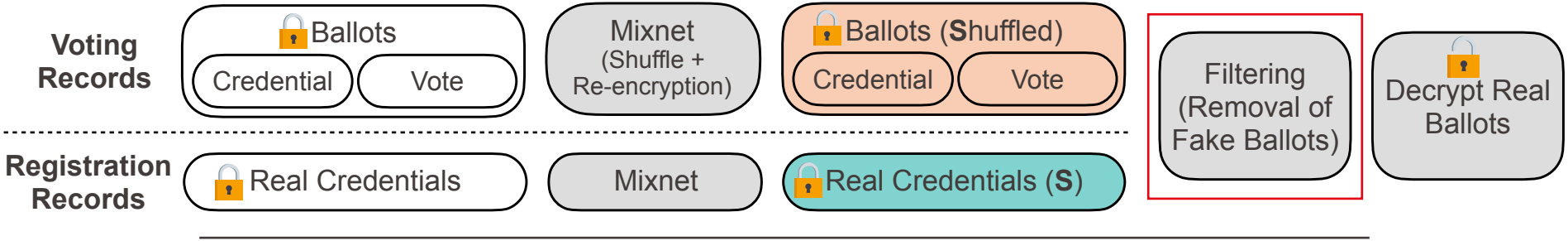
How to safely let voters cast a vote even when faced with all-seeing coercer post-registration?



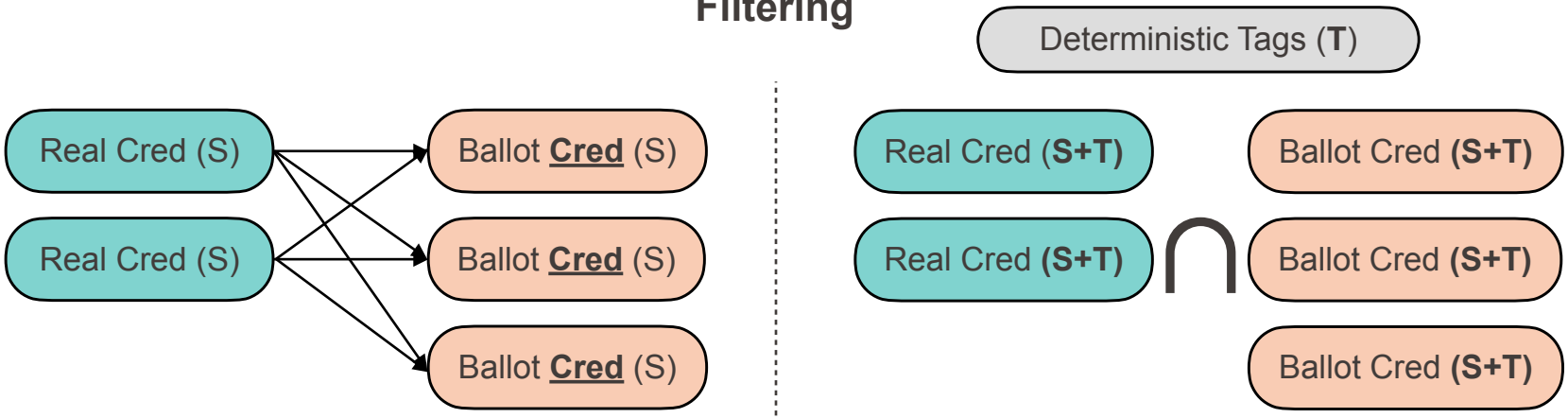
How to tally votes efficiently and verifiably?

- **VLT**
  - **Scalability**
  - Extreme Coercion

Tallying: Addressing Scalability



Filtering



Privacy Equivalence Tests (PETs)
(Jakobsson and Juels)

Deterministic Tags
(Smith, Weber)

Tagging Vulnerability

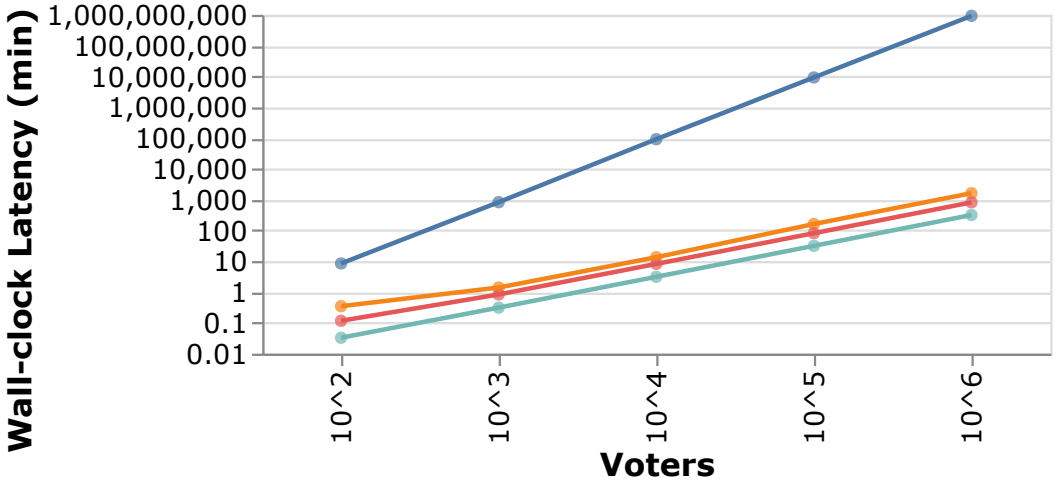
- **Intended Leakage: Plaintext Equality**
  - $T = \mathrm{Tag}(\sigma) = \sigma^s$
- **Compliance Test** (due to homomorphism):
  - **Coercer casts vote** with credential σ_c and **demands voter to vote** with $\sigma_v = \sigma_c^{\alpha}$.
  - After mix + tagging, the set of tags $\mathscr{T}$ contains $T = \mathrm{Tag}(\sigma_c)$ and $T' = \mathrm{Tag}(\sigma_v)$.
  - Coercer declares compliance iff $\exists\, T, T' \in \mathscr{T}$ such that $T' = T^{\alpha}$.

Restrict Valid Ballots

Preventing Board Flooding Attacks in Coercion-Resistant Electronic Voting Schemes

Reto Koenig[1,2], Rolf Haenni[1], and Stephan Fischli[1]

- Synergy between Koenig, Haenni and Fischli's work & TRIP's finite set of credentials.
  - Restrict the set of valid ballots to those cast with registrar-issued *real and fake* credentials to avoid compliance test
  - Use TRIP as the concrete voter registration process



- **1 million voters**
  - Civitas: 1,768 years
  - Swiss Post: 27 hours
  - **Votegral: 14 hours**
  - VoteAgain: 5 hours

- https://github.com/dedis/votegral

How to safely let voters cast a vote even when faced with all-seeing coercer post-registration?

- **VLT**
  - Scalability
  - **Extreme Coercion**

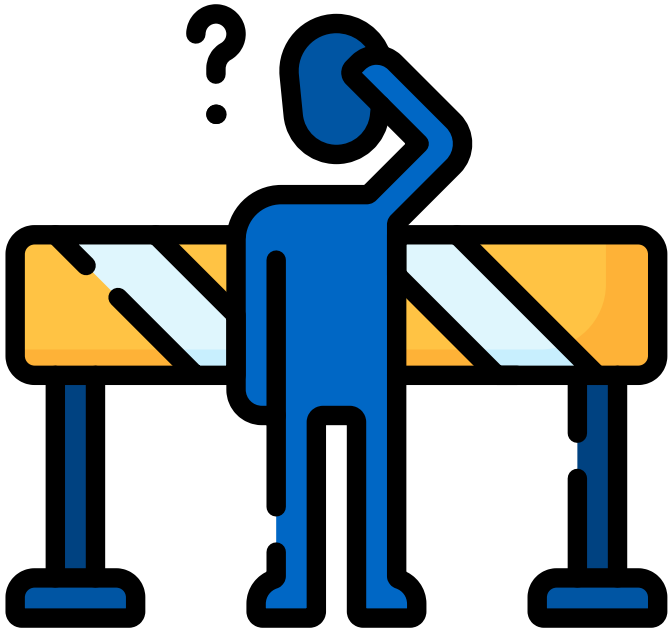
Extreme Coercion: Standing Votes

Registration

Voters delegate their vote to a political party, leaving the booth with only fake credentials

- The final tally reveals the multiplicities $M[P]$ for each political party P.
  - $M[P]$ values are public, auditable signals that M voters (aggregate) felt unsafe to keep a real credential—without identifying any voter.
  - Counts are “evidence,” not proof—some voters may delegate for convenience.

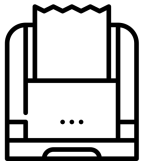
Roadmap



- Background
- Contributions and Model
- Votegral: TRIP
- Votegral: VLT
- **Discussion**

Votegral Limitations

- Side Channel Attacks (Registration Booth)



Printer Noise

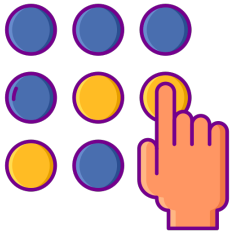
Timing Attacks

Electromagnetism

- Voter's device is trusted for coercion: can we weaken this assumption by concealing the real credential on a device?
- No individual verifiability for delegated votes since voters cannot sneak out information outside the booth.
- Lack of post-quantum security: Scheme based on DL

User Study Limitations

- Did not replicate an official registration environment
- Did not study voters actually under coercion
- Did not study long-term storage, use of credentials on voter's device.



PINs?

Passwords?

Images?

Conclusion

- Core blocker for online voting: coercion.
- Fake credentials help, but only if registration is safe from coercion and verifiable.
- **Votegral:** a practical path to coercion-resistant e-voting
  - In-person, paper-based registration (*TRIP*) + linear-time tally w/ standing votes (*VLT*).
  - *Coercion-resistance*: one real + indistinguishable fakes; standing votes for extreme cases.
  - *Individual verifiability*: voter-visible commit→challenge→response
  - *Scalable and robust*: constrain ballots to issued credentials
  - *Usability*: 150-person study (83% end-to-end success; 96% understood fake credentials)

Special Thank You

- Advisor
  - Prof. Bryan Ford (EPFL)
- Co-Authors
  - Jeff R. Allen (EPFL)
  - Alaleh Azhir (Harvard, MIT)
  - Simone Colombo (King's College London)
  - Vero Estrada-Galiñanes (EPFL)
  - Shailesh Mishra (EPFL)
  - Mohammad Amin Raeisi (Yale)
  - Rene Reyes (Boston University)
  - Bernhard Tellenbach (Armasuisse)
  - Pasindu Tennage (EPFL)
  - Haoqian Zhang (EPFL)
- Committee Members
  - Prof. Thomas Bourgeat
  - Prof. Dave Levin
  - Dr. Oliver Spycher
  - Prof. Clément Pit-Claudel

Questions