Civitas

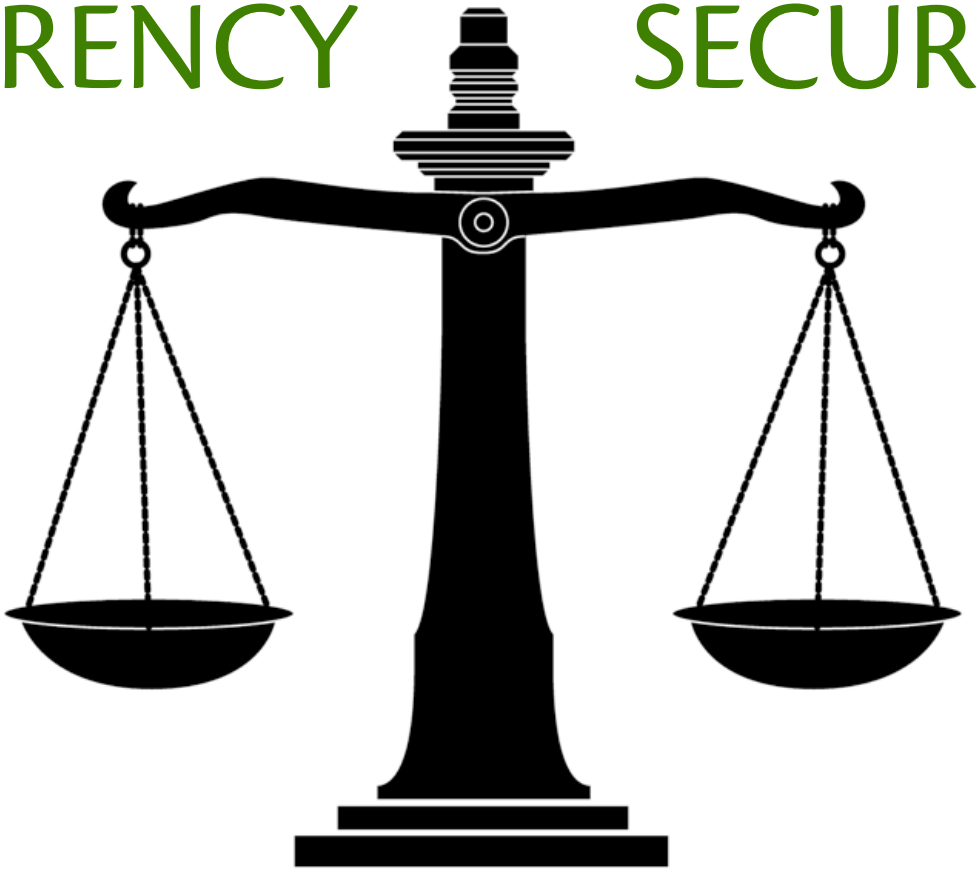
Security and Transparency for Remote Voting

Michael Clarkson
Cornell University

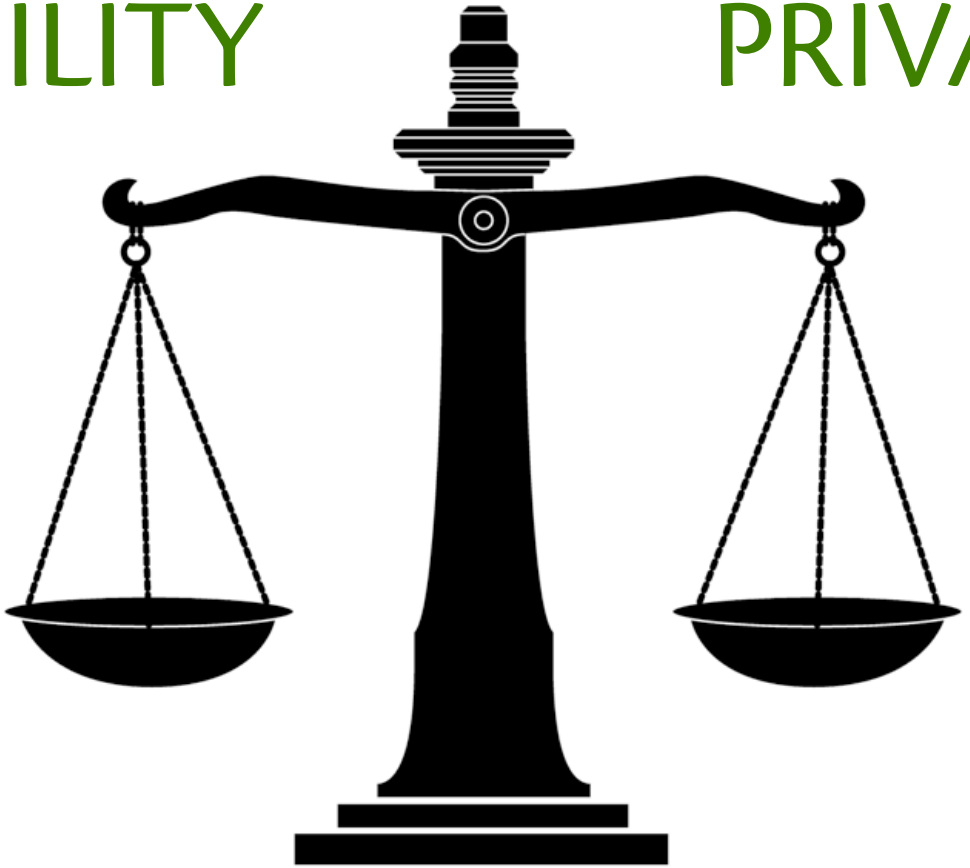
with Stephen Chong (Harvard) and Andrew Myers (Cornell)

Swiss E-Voting Workshop
September 6, 2010

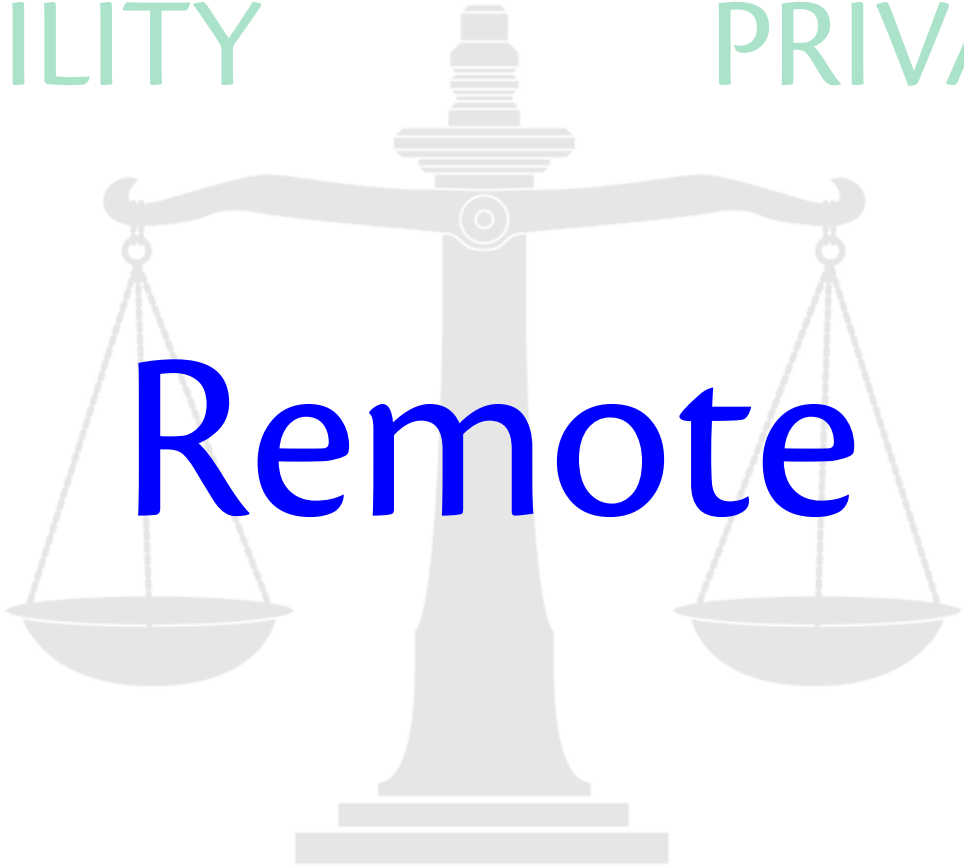
TRANSPARENCY SECURITY



VERIFIABILITY PRIVACY



VERIFIABILITY PRIVACY



Remote

KEY PRINCIPLE:

Mutual Distrust

VERIFIABILITY

Universal verifiability

Voter verifiability

UV: [Sako and Killian 1994, 1995]

VV: [Kremer, Ryan & Smyth 2010]

PRIVACY

Coercion resistance

better than **receipt freeness**
or simple **anonymity**

RF: [Benaloh 1994]
CR: [Juels, Catalano & Jakobsson 2005]

ROBUSTNESS

Tally availability

Civitas Security Properties

Original system:

- Universal verifiability
- Coercion resistance

Ongoing projects:

- Voter verifiability
- Tally availability

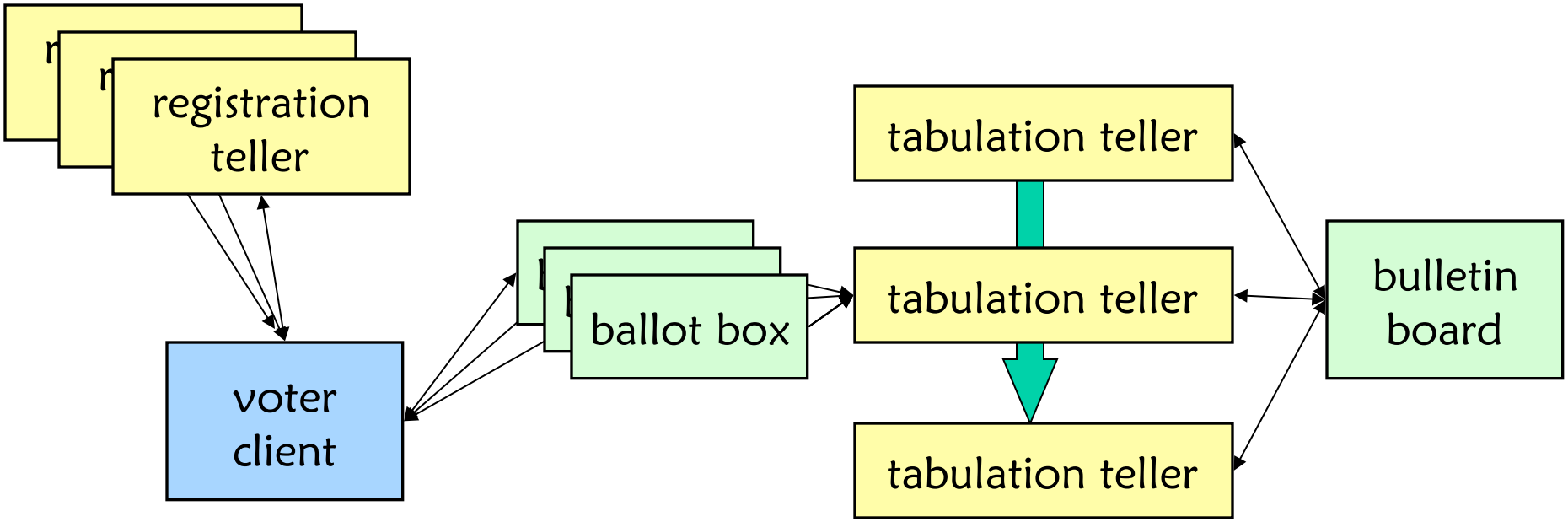
JCJ Voting Scheme

[Juels, Catalano & Jakobsson 2005]

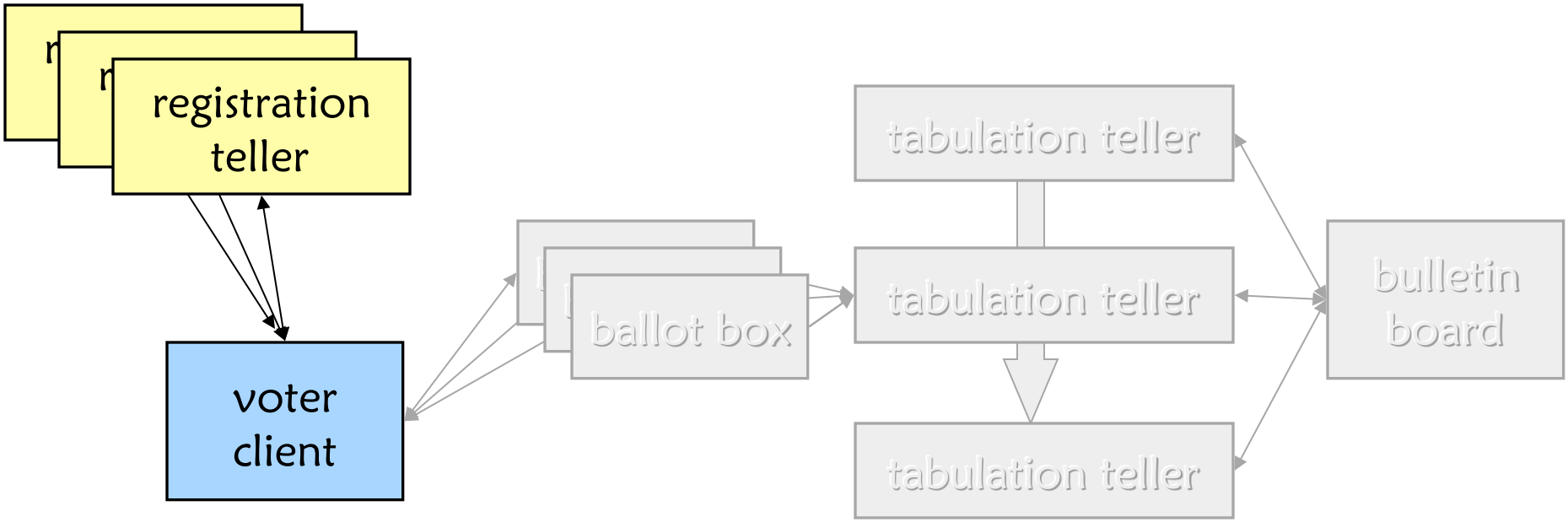
Proved universal verifiability
and coercion resistance

Civitas extends JCJ

Civitas Architecture



Registration

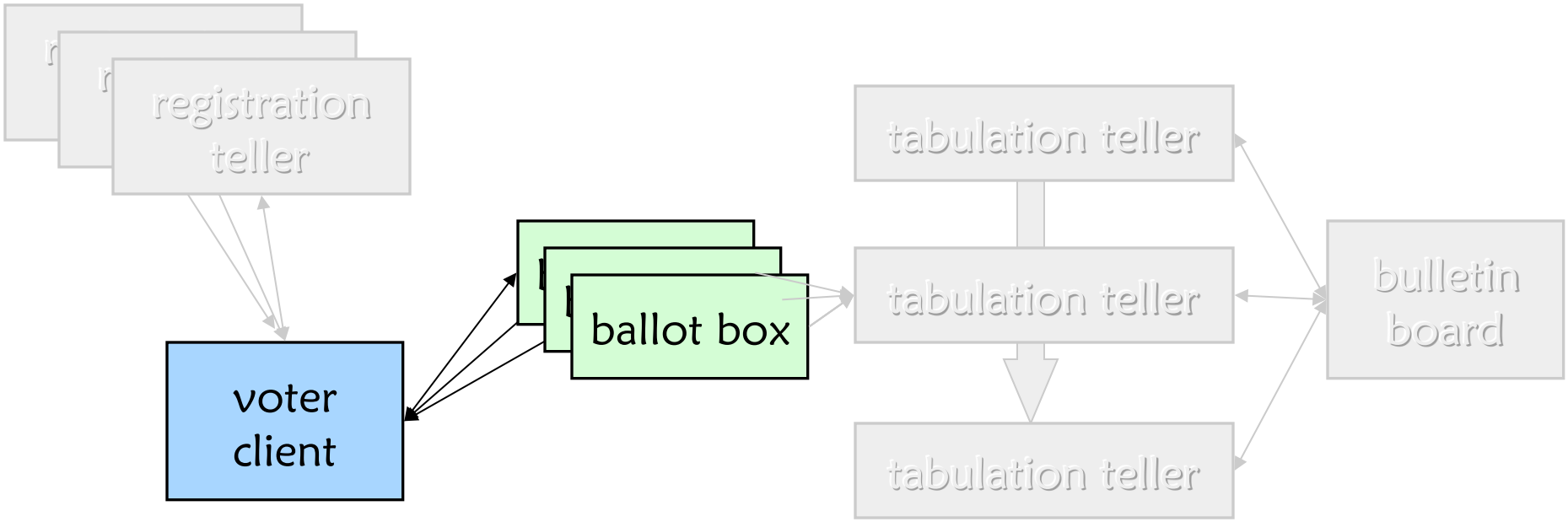


Voter retrieves *credential share* from each registration teller; combines to form *credential*

Credentials

- Verifiable
- Unsalable
- Unforgeable
- Anonymous

Voting



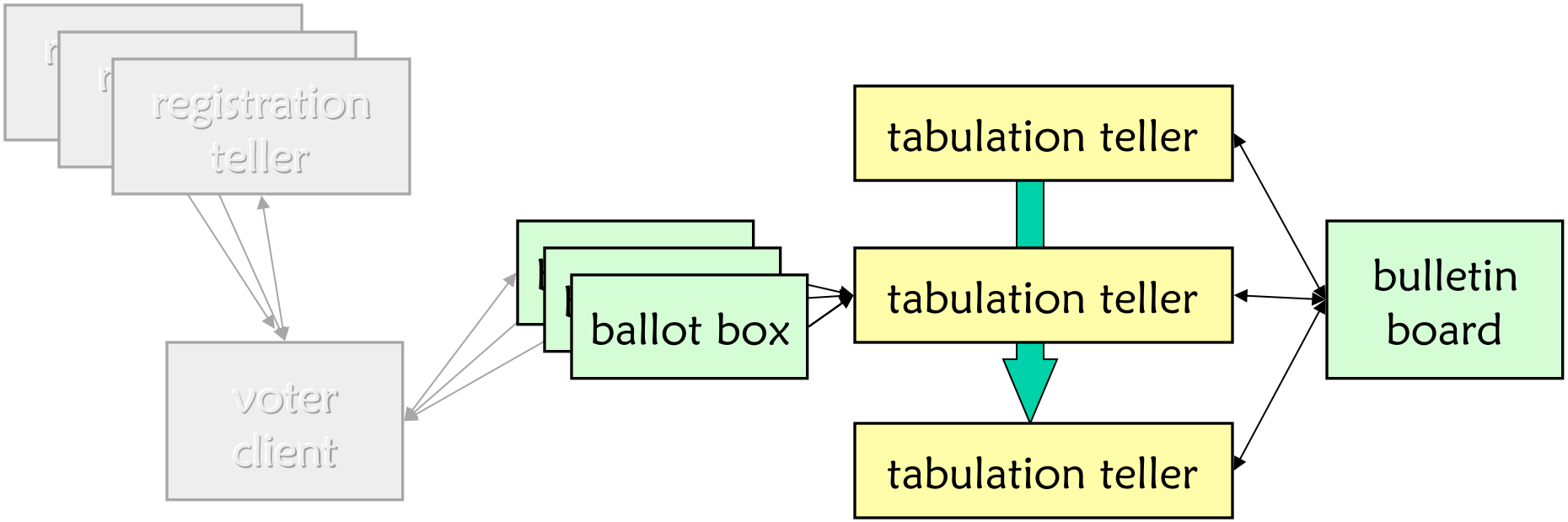
Voter submits copy of encrypted *choice* and credential to each ballot box

Resisting Coercion: Fake Credentials

Resisting Coercion

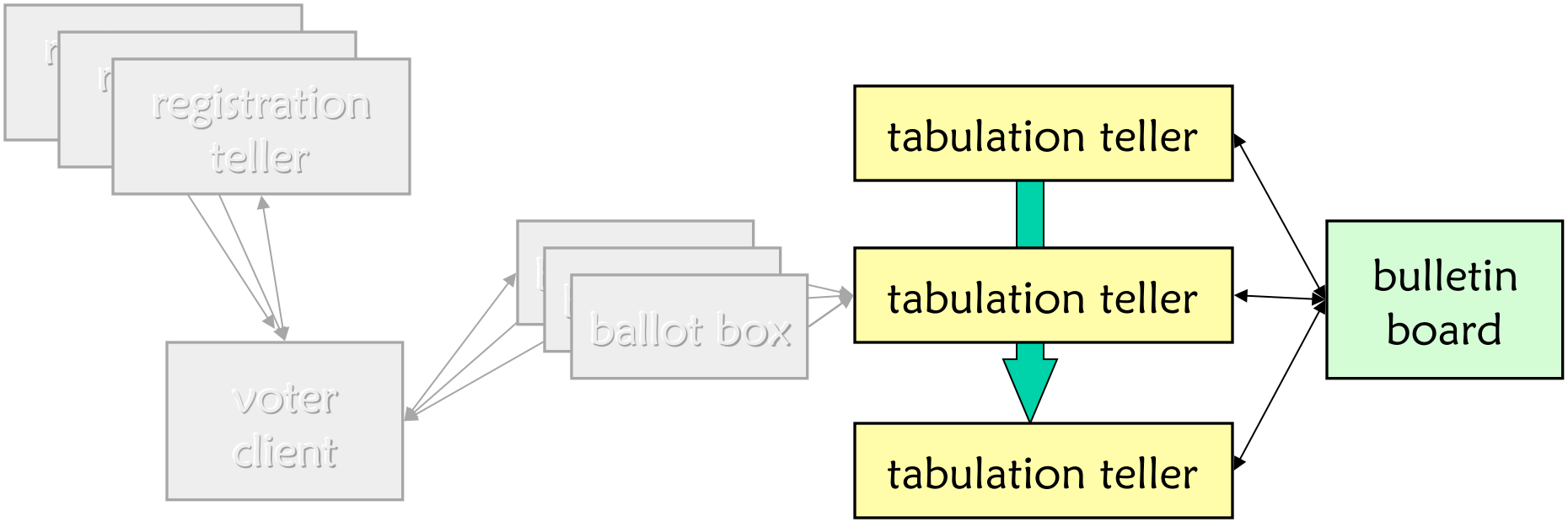
If the coercer demands that the voter…	**Then the voter…**
Submits a particular vote	Does so with a fake credential.
Sells or surrenders a credential	Supplies a fake credential.
Abstains	Supplies a fake credential to the adversary and votes with a real one.

Tabulation



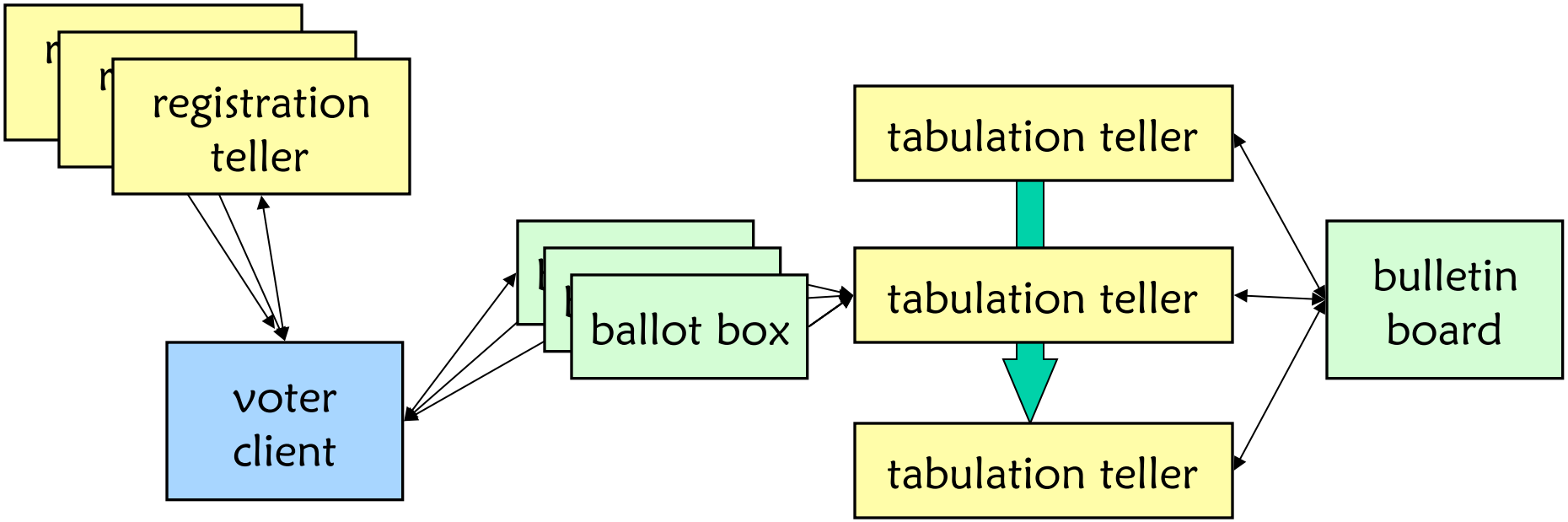
Tellers retrieve votes from ballot boxes

Tabulation



Tabulation tellers anonymize votes;
eliminate unauthorized (and fake) credentials;
decrypt remaining choices.

Civitas Architecture



Universal verifiability:
Tellers post *zero-knowledge proofs* during tabulation

Coercion resistance:
Voters can undetectably fake credentials

Protocols

- El Gamal; distributed [Brandt]; non-malleable [Schnorr and Jakobsson]
- Proof of knowledge of discrete log [Schnorr]
- Proof of equality of discrete logarithms [Chaum & Pederson]
- Authentication and key establishment [Needham-Schroeder-Lowe]
- Designated-verifier reencryption proof [Hirt & Sako]
- 1-out-of-L reencryption proof [Hirt & Sako]
- Signature of knowledge of discrete logarithms [Camenisch & Stadler]
- Reencryption mix network with randomized partial checking [Jakobsson, Juels & Rivest]
- Plaintext equivalence test [Jakobsson & Juels]

Civitas Implementation

Component	**LoC**
Tabulation teller	5,700
Registration teller	1,300
Bulletin board, ballot box	900
Voter client	800
Other (incl. common code)	4,700
Low-level crypto and I/O (Java and C)	8,000
Total LoC	**21,400**

Trust Assumptions

Civitas Trust Assumptions

1. "Cryptography works."
2. The adversary cannot masquerade as a voter during registration.
3. Voters trust their voting client.
4. At least one of each type of authority is honest.
5. The channels from the voter to the ballot boxes are anonymous.
6. Each voter has an untappable channel to a trusted registration teller.

Civitas Trust Assumptions

1. "Cryptography works."
2. The adversary cannot masquerade as a vote
3. Voters trust their voting client.

Universal verifiability
Coercion resistance

---

4. At least one of each type of authority is ho

Coercion resistance

5. The channels from the voter to the ballot boxes are anonymous.
6. Each voter has an untappable channel to a trusted registration teller.

Civitas Trust Assumptions

1. "Cryptography works."
2. The adversary cannot masquerade as a voter during registration.
3. Voters trust their voting client. UV + CR

---

4. At least one of each type of authority is honest. CR
5. The channels from the voter to the ballot boxes are anonymous.
6. Each voter has an untappable channel to a trusted registration teller.

Civitas Trust Assumptions

1. "Cryptography works."
2. The adversary cannot masquerade as a voter during registration.
3. Voters trust their voting client. UV + CR

---

4. At least one of each type of authority is honest. CR
5. The channels from the voter to the ballot boxes are anonymous.
6. Each voter has an untappable channel to a trusted registration teller.

Civitas Trust Assumptions

1. "Cryptography works."
2. The adversary cannot masquerade as a voter during registration.
3. Voters trust their voting client. UV + CR

---

4. At least one of each type of authority is honest. CR
5. The channels from the voter to the ballot boxes are anonymous.
6. Each voter has an untappable channel to a trusted registration teller.

Registration

In person.

In advance.

Con: System not fully remote

Pro: Credential can be used in many elections

Civitas Trust Assumptions

1. "Cryptography works."
2. The adversary cannot masquerade as a voter during registration.
3. Voters trust their voting client. UV + CR

---

4. At least one of each type of authority is honest. CR
5. The channels from the voter to the ballot boxes are anonymous.
6. Each voter has an untappable channel to a trusted registration teller.

Eliminating Trust in Voter Client

UV: Use *challenges*, like in Helios

CR: Open problem

Civitas Trust Assumptions

1. "Cryptography works."
2. The adversary cannot masquerade as a voter during registration.
3. Voters trust their voting client. UV + CR

---

4. At least one of each type of authority is honest. CR
5. The channels from the voter to the ballot boxes are anonymous.
6. Each voter has an untappable channel to a trusted registration teller.

Civitas Trust Assumptions

1. "Cryptography works."
2. The adversary cannot masquerade as a voter during registration.
3. Voters trust their voting client. UV + CR

---

4. At least one of each type of authority is honest. CR
5. The channels from the voter to the ballot boxes are anonymous.
6. Each voter has an untappable channel to a trusted registration teller.

Civitas Trust Assumptions

1. "Cryptography works."
2. The adversary cannot masquerade as a voter during registration.
3. Voters trust their voting client. UV + CR

---

4. At least one of each type of authority is honest. CR
5. The channels from the voter to the ballot boxes are anonymous.
6. Each voter has an untappable channel to a trusted registration teller.

Untappable Channel

Minimal known assumption
for receipt freeness and coercion resistance

Eliminate? Open problem.

(Eliminate trusted registration teller? Also open.)

Civitas Trust Assumptions

1. "Cryptography works."
2. The adversary cannot masquerade as a voter during registration.
3. Voters trust their voting client. UV + CR

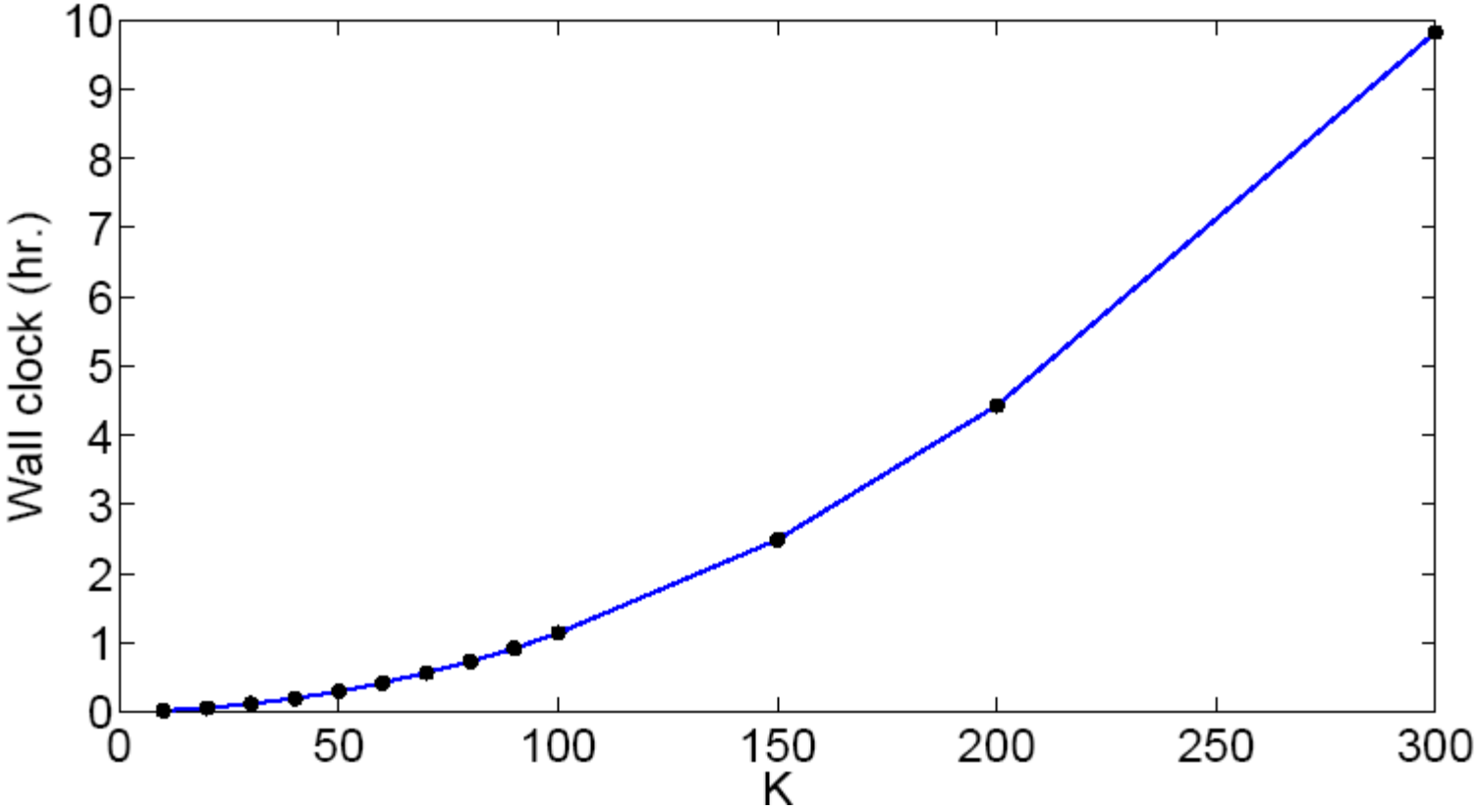
---

4. At least one of each type of authority is honest. CR
5. The channels from the voter to the ballot boxes are anonymous.
6. Each voter has an untappable channel to a trusted registration teller.

Trusted procedures?

Time to Tally

Tabulation Time vs. Precinct Size



voters in precinct = K, # tab. tellers = 4,
security strength ≥ 112 bits [NIST 2011–2030]

Summary

Can achieve strong security and transparency:

- Remote voting
- Universal verifiability
- Coercion resistance

Security is not free:

- Stronger registration (untappable channel)
- Cryptography (computationally expensive)

Assurance

Security proofs (JCJ)

Secure implementation (Jif)

Ranked Voting Methods

Open Research Problems

- Coercion-resistant voter client?
- Eliminate untappable channel in registration?
- Credential management?
- Application-level denial of service?

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

(google “civitas voting”)

Civitas

Security and Transparency for Remote Voting

Michael Clarkson
Cornell University

with Stephen Chong (Harvard) and Andrew Myers (Cornell)

Swiss E-Voting Workshop
September 6, 2010