QUT isi Information Security Institute

An Overview on Cryptographic Voting Systems

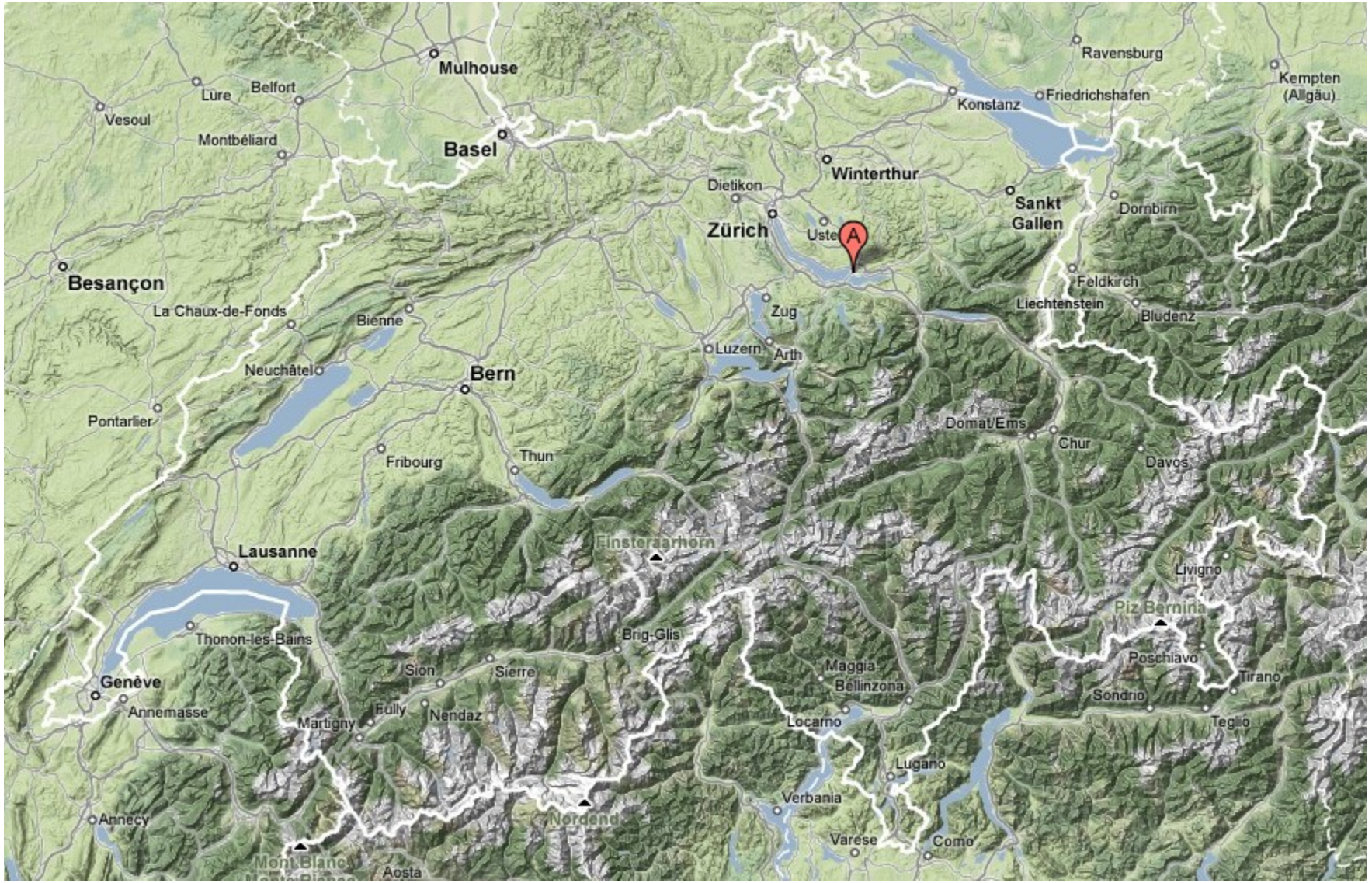
Prof. Andreas Steffen

University of Applied Sciences Rapperswil

andreas.steffen@hsr.ch

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

Where the heck is Rapperswil?



HSR - Hochschule für Technik Rapperswil

- University of Applied Sciences with about 1000 students
- Faculty of Information Technology (300-400 students)
- Bachelor Course (3 years), Master Course (+1.5 years)

Cryptographic Voting Systems

Summary of my talk:

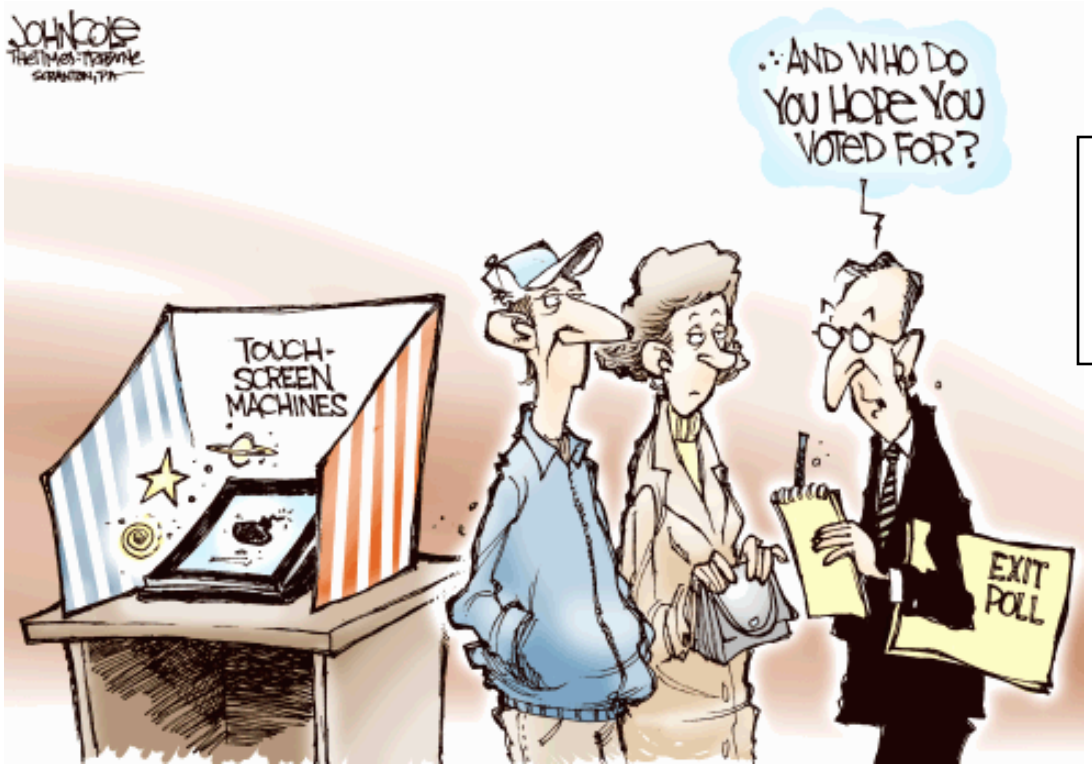
- Due to repeated failures and detected vulnerabilities in both electro-mechanical and electronic voting machines, voters have somehow lost faith that the outcome of a poll always represents the true will of the electorate.
- Manual counting of paper ballots is not really an option in the 21st century and is not free from tampering either.
- Modern cryptographic voting systems allow true end-to-end verification of the complete voting process by any individual voter, without sacrificing secrecy and privacy.

Direct Recording Electronic Voting Machines

- In the 2006 mid-term federal elections, one third of registered U.S. voters used Direct Recording Electronic (DRE) voting machines.
- In the 2008 federal elections, many states returned to paper ballots with optical scanning but six states used 100% DREs without a Voter-Verified Paper Audit Trail (VVPAT).

Diebold Elections System DRE voting machine with a VVPAT attachment.

Losing Trust in Electronic Voting Systems

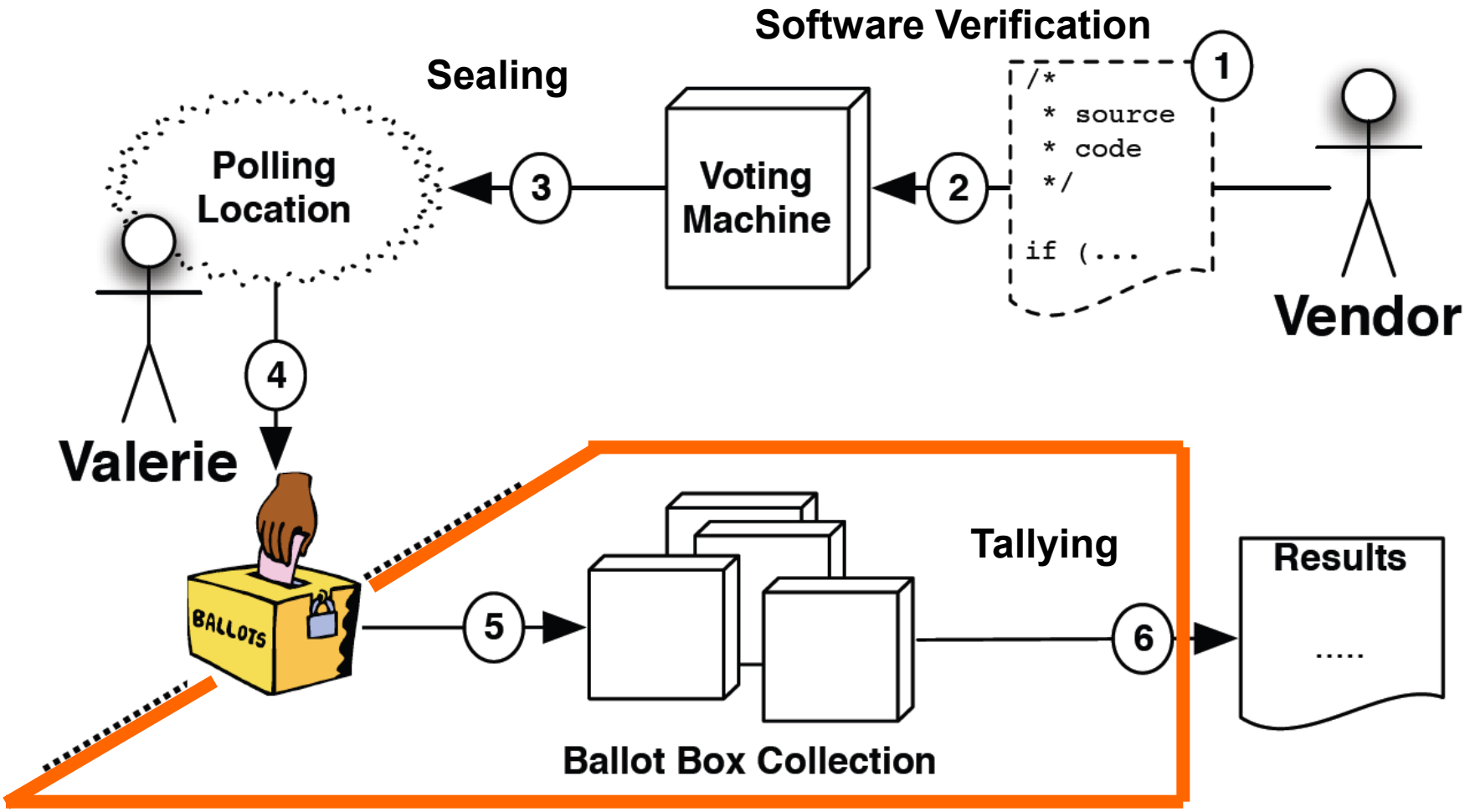


2006 - The Morning Call:
Voter smashes DRE in Allentown with metal cat

2006 - Princeton study on Diebold DRE:
Hack the vote? No problem

2006 - Dutch ES3B voting machines:
Hacked to play chess

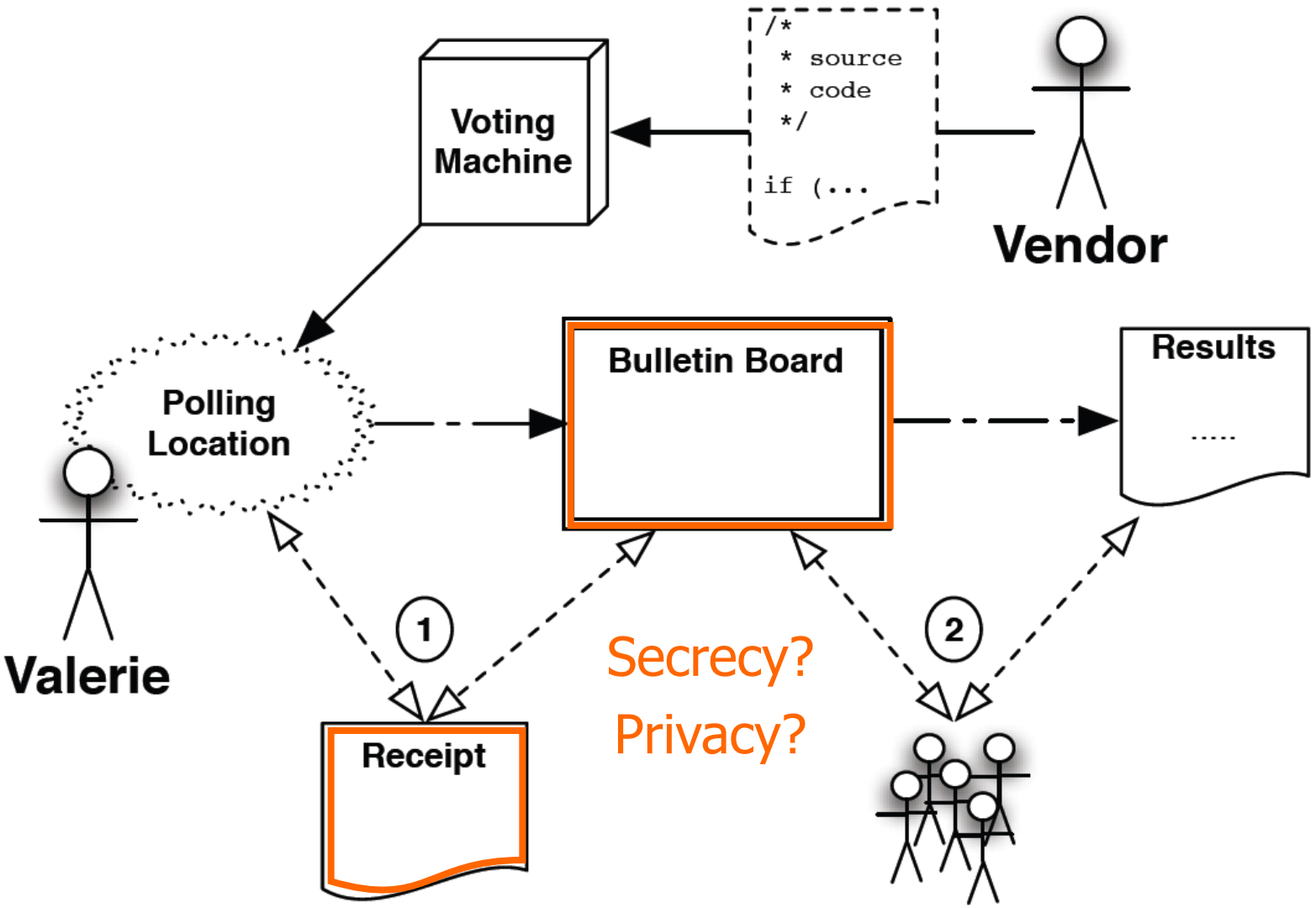
Traditional Chain-of-Custody Security



Verification by proxy only

Source: Ben Adida, Ph.D. Thesis 2006

Desirable: End-to-End Verification by Voter



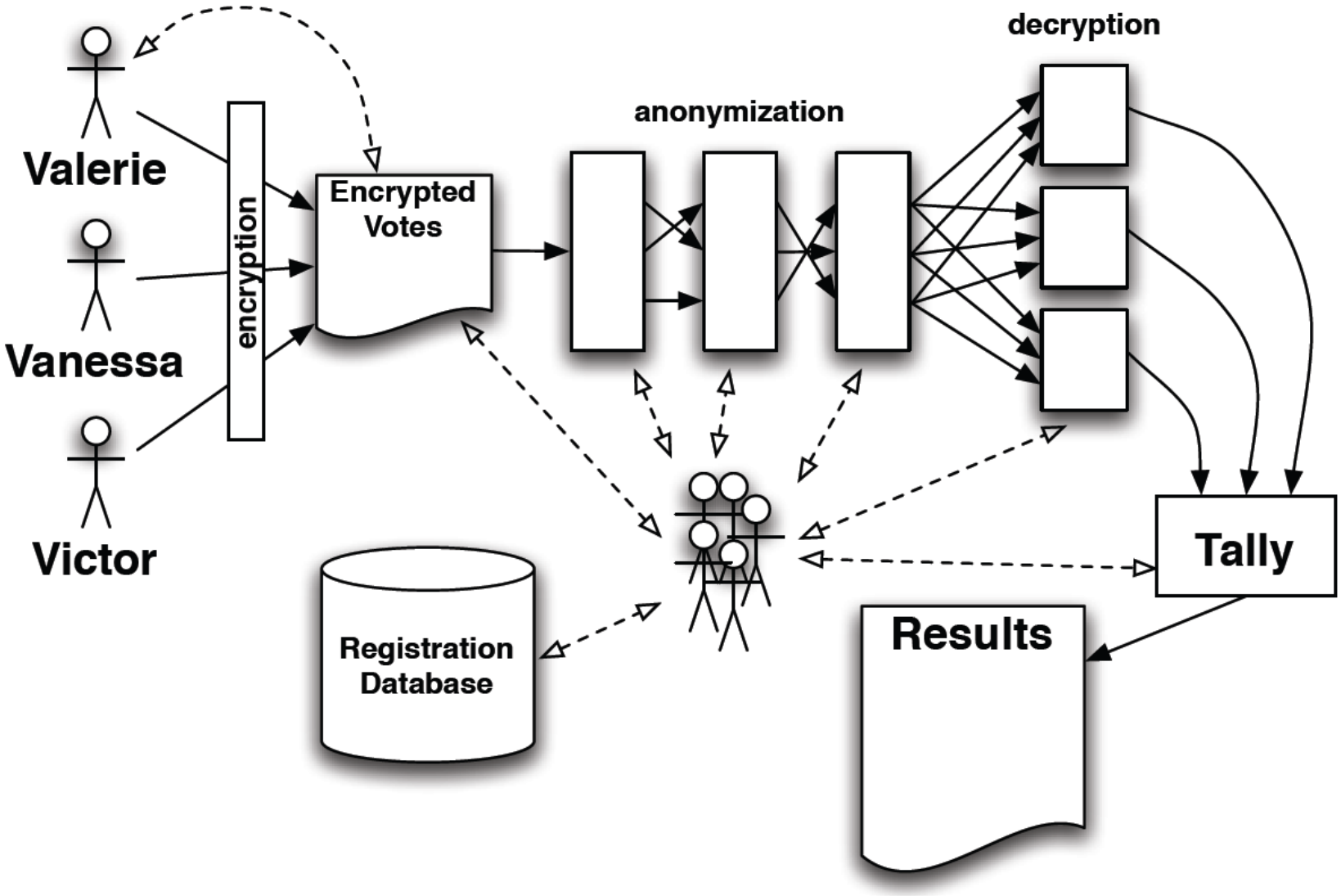
Source: Ben Adida, Ph.D. Thesis 2006

End-to-End Auditable Voting System (E2E)

- Any voter can verify that his or her ballot is included unmodified in a collection of ballots.
- Any voter (and typically any independent party additionally) can verify, with high probability, that the collection of ballots produces the correct final tally.
- No voter can demonstrate how he or she voted to any third party (thus preventing vote-selling and coercion).

Source: Wikipedia

Solution: Cryptographic Voting Systems

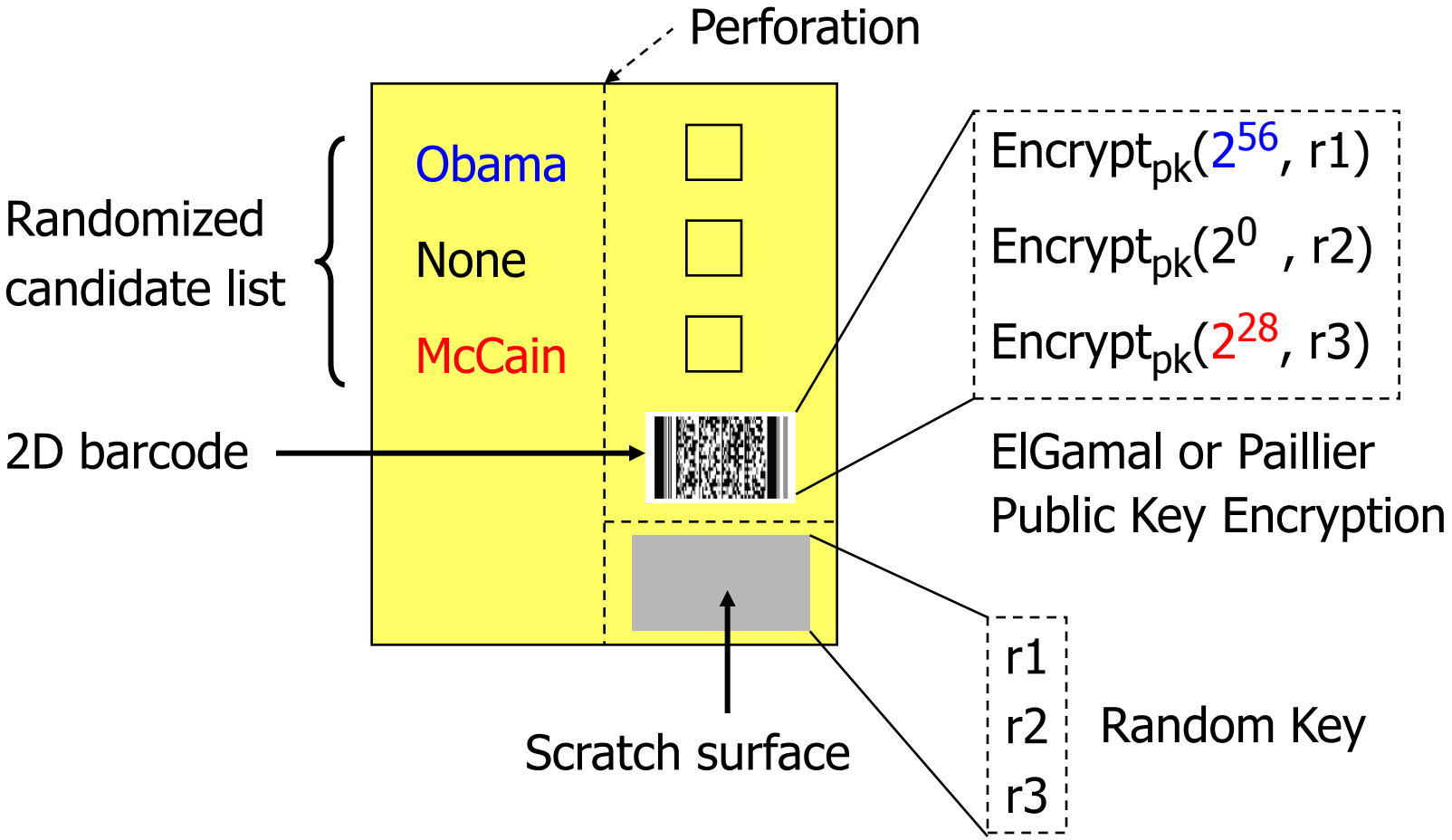


Source: Ben Adida, Ph.D. Thesis 2006

Proposed E2E Systems

- Punchscan by David Chaum.
- Prêt à Voter by Peter Ryan.
- Scratch & Vote by Ben Adida and Ron Rivest.
- ThreeBallot by Ron Rivest (paper-based without cryptography)
- Scantegrity II by David Chaum, Ron Rivest, Peter Ryan et al. (add-on to optical scan voting systems using Invisible Ink)

Scratch & Vote Ballot



Source: Ben Adida, Ph.D. Thesis 2006

Homomorphic Counters

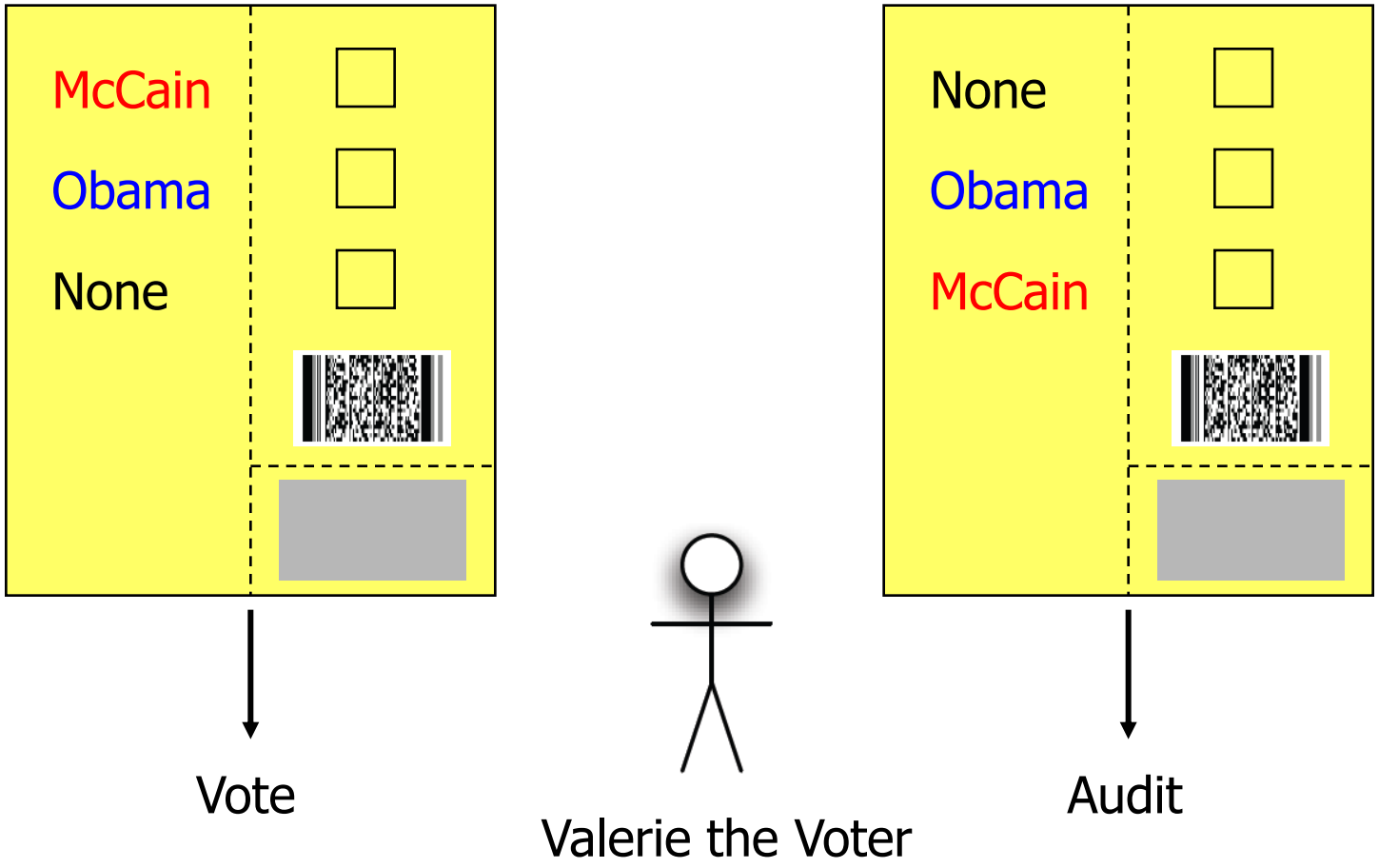
2^{56}	00...01	00...00	00...00	One vote for Obama
2^{28}	00...00	00...01	00...00	One vote for McCain
2^{0}	00...00	00...00	00...01	One vote for None
	Obama	McCain	None	
	00...10	00...01	00...00	Tallying Counter

Multiplication of all encrypted votes with Tallying Counter accumulates votes in the candidates‘ counters in encrypted form.

Total number of registered U.S. voters < 2^{28} (28 bits)
1024 bit Paillier Public Key Cryptosystem could handle 35 candidates

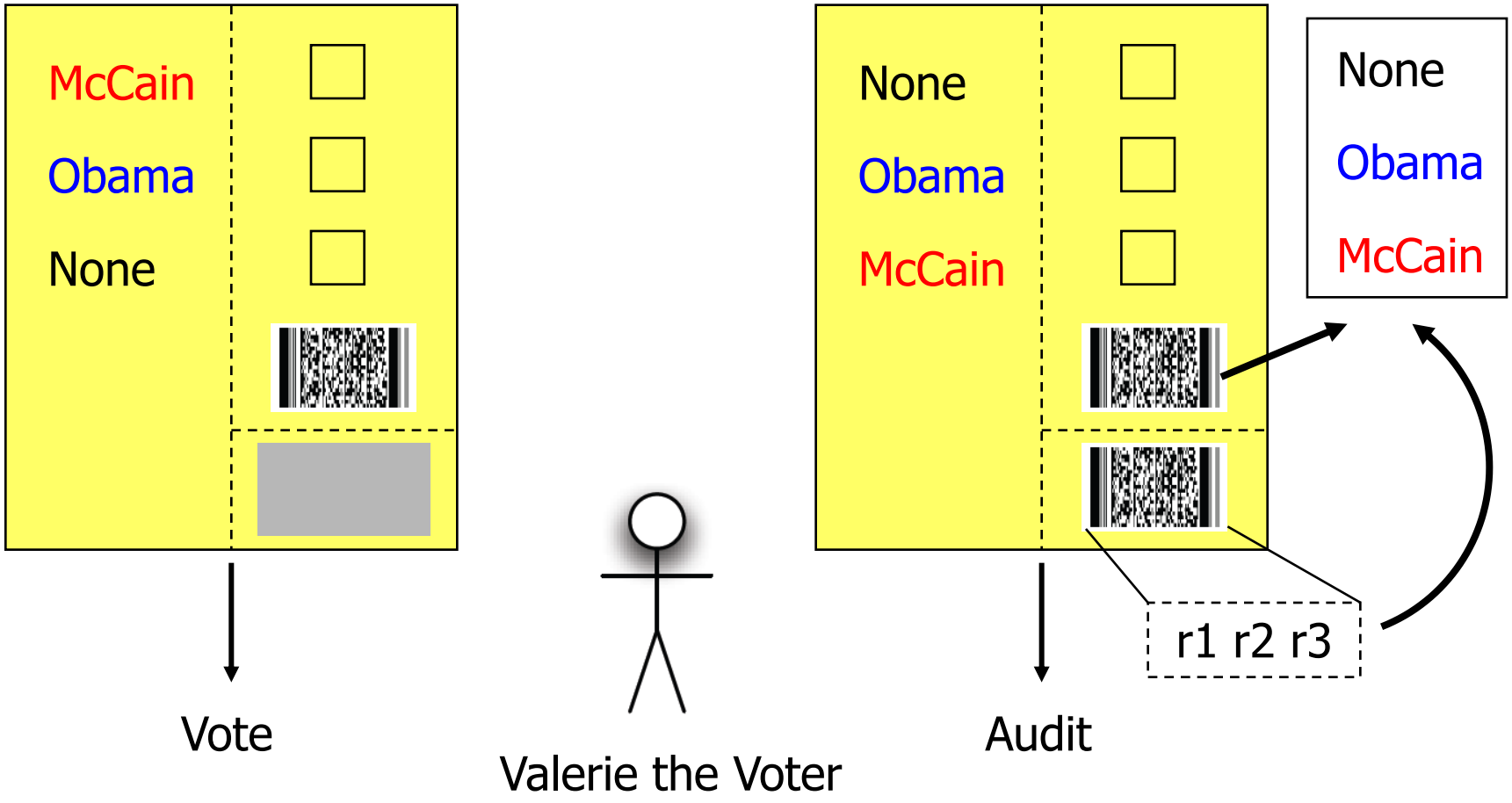
Source: Ben Adida, Ph.D. Thesis 2006

Pre-Voting Verification I



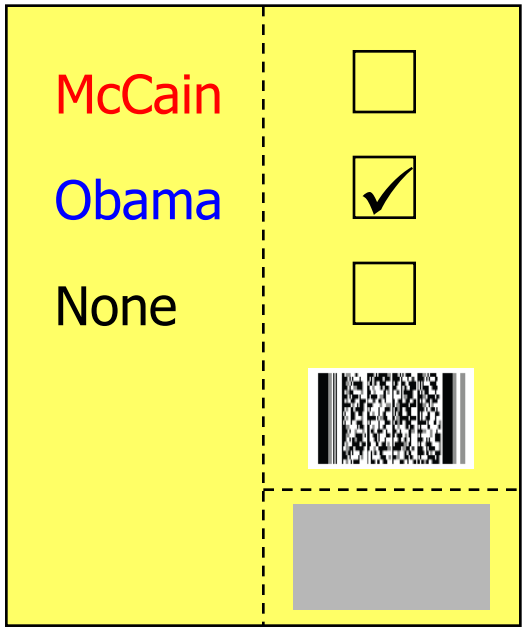
Source: Ben Adida, Ph.D. Thesis 2006

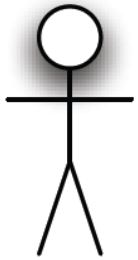
Pre-Voting Verification II



Source: Ben Adida, Ph.D. Thesis 2006

Casting the Ballot I

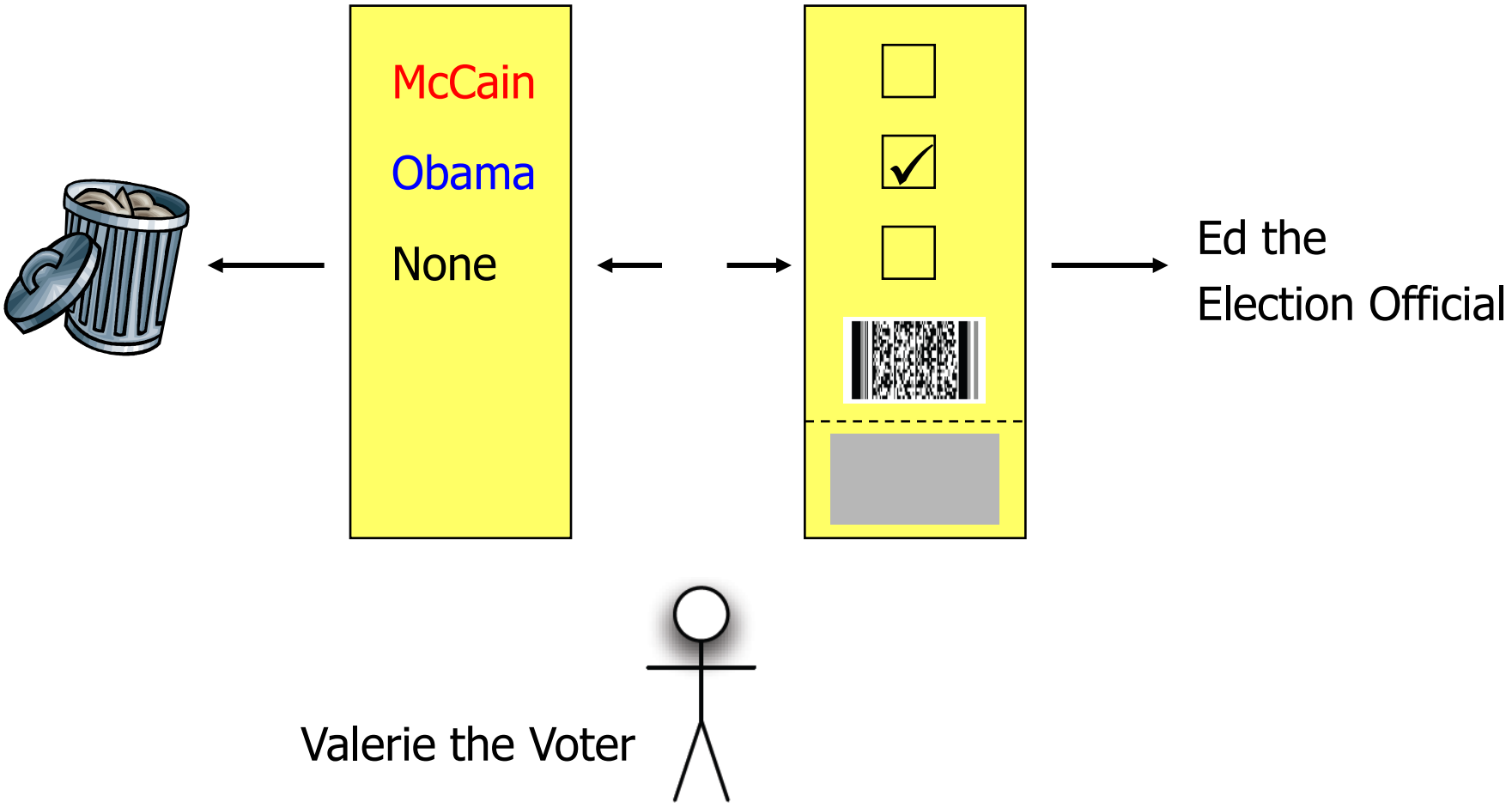




Valerie the Voter

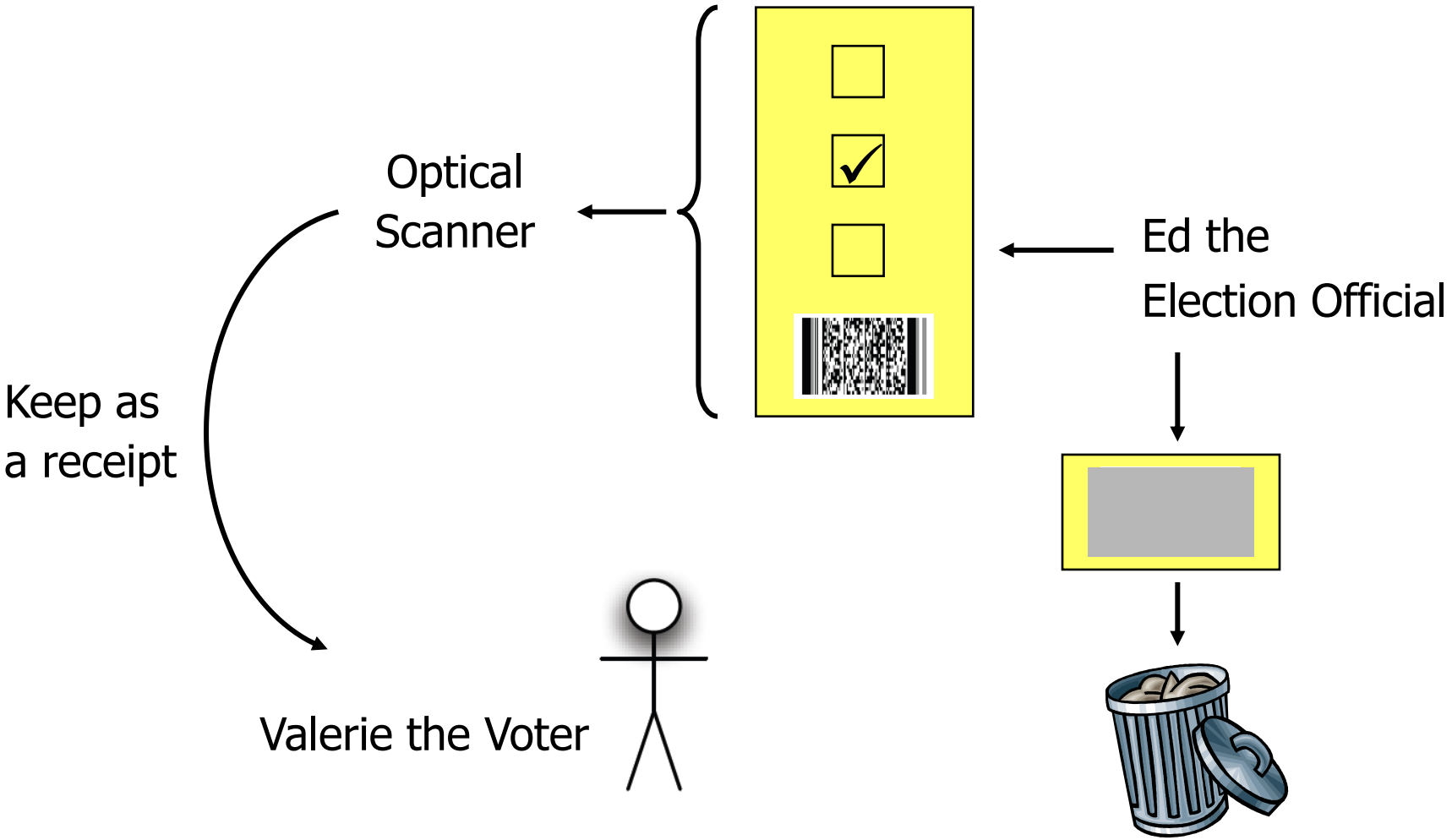
Source: Ben Adida, Ph.D. Thesis 2006

Casting the Ballot II



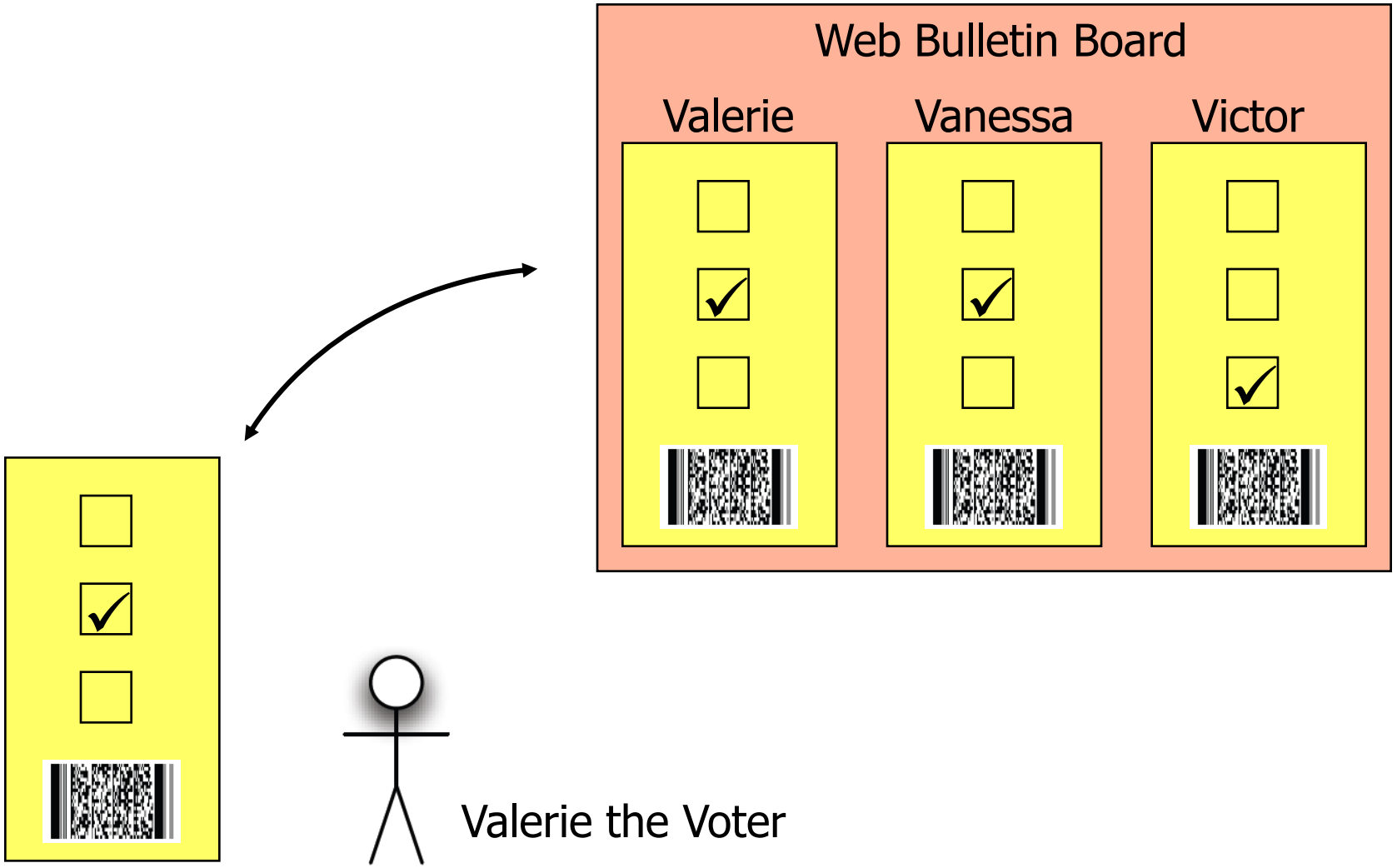
Source: Ben Adida, Ph.D. Thesis 2006

Casting the Ballot III



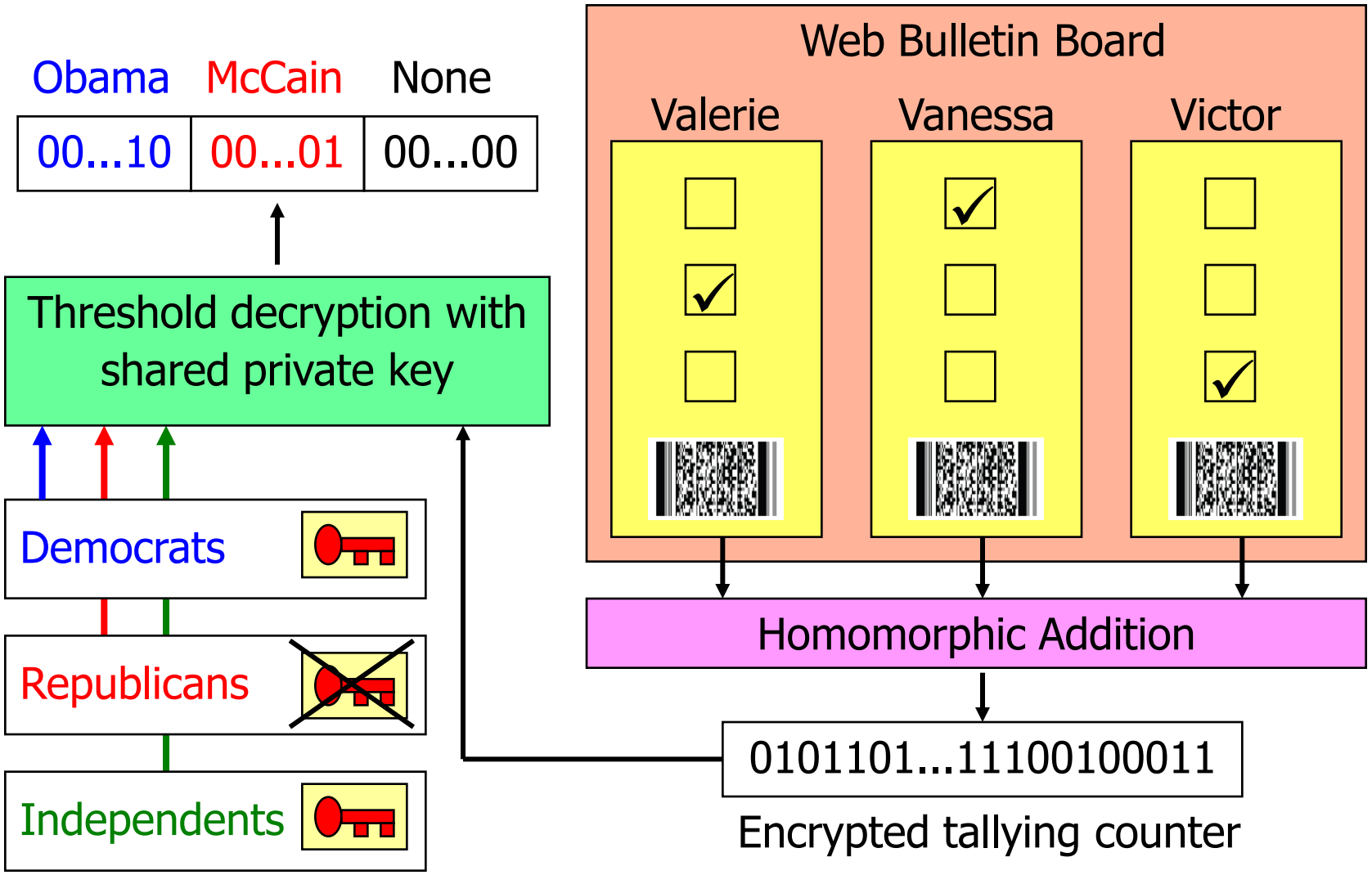
Source: Ben Adida, Ph.D. Thesis 2006

Post-Voting Verification



Source: Ben Adida, Ph.D. Thesis 2006

Tally and Decryption of Final Result



Source: Ben Adida, Ph.D. Thesis 2006

Conclusion

- Modern Cryptographic Voting Systems allow true end-to-end verification of the whole voting process by anyone while maintaining a very high level of secrecy.

- Due to the advanced mathematical principles they are based on, Cryptographic Voting Systems are not easy to understand and are therefore not readily accepted by authorities and the electorate.

- But let‘s give Cryptographic Voting Systems a chance!
  They can give democracy a new meaning in the 21st century!