Electronic Voting and Receipt-freeness

Byoungcheon Lee[1,2], Colin Boyd[1], Ed Dawson[1]

[1]Information Security Research Centre, QUT

[2]Joongbu University, Korea

ARC Grant No: LX0346868

Contents

1. Introduction to electronic voting
   - Classification
   - Electoral systems
   - Security requirements
   - Approaches to electronic voting
2. Three main approaches
   - Blind signature based schemes
   - Homomorphic encryption based schemes
   - Mixnet based schemes

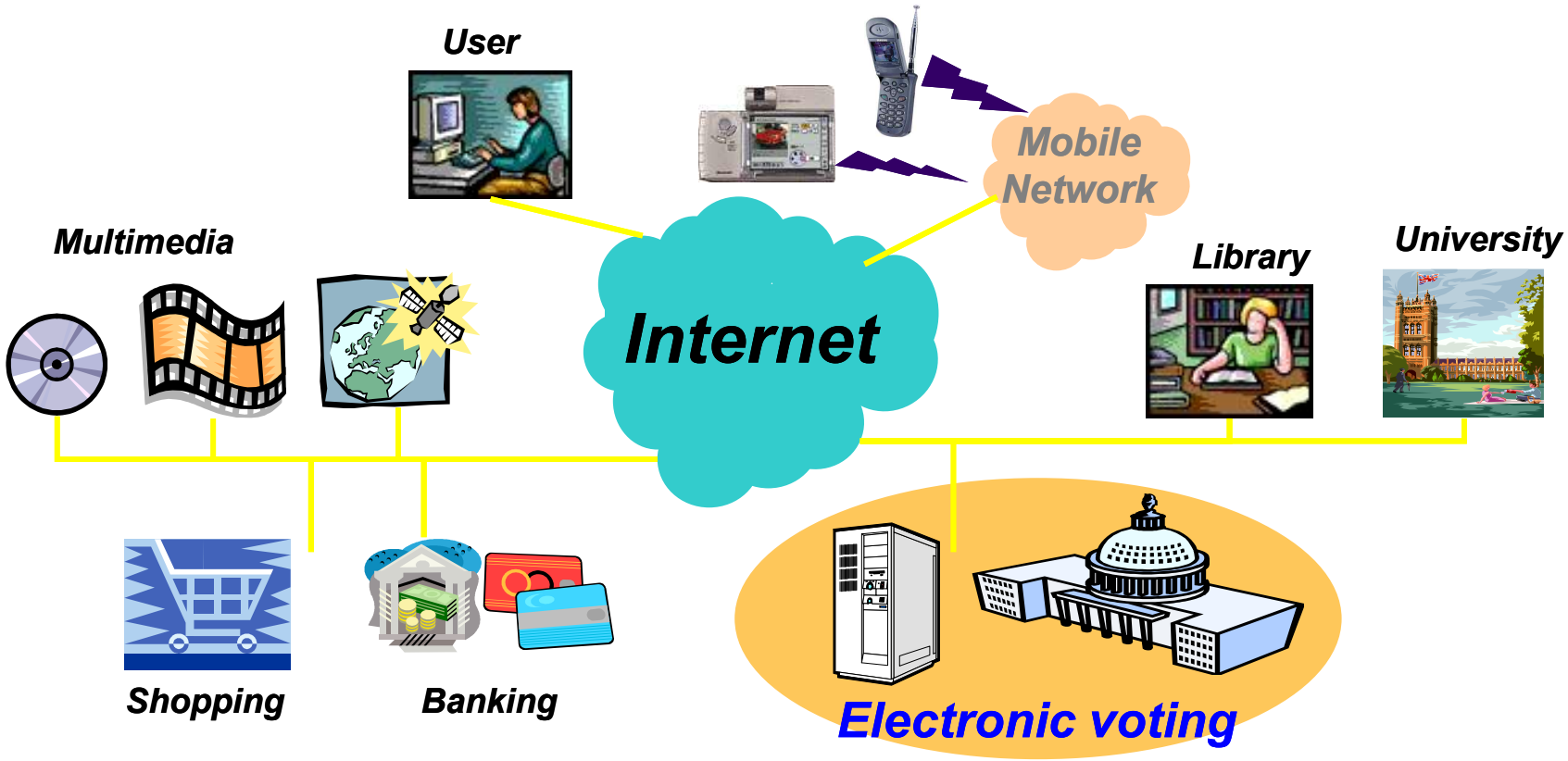
Contents

3. Receipt-free voting protocols
   - Receipt-freeness
   - Hirt-Sako scheme [HS00]
   - In Homomorphic encryption based voting [LK02]
   - In mixnet based voting [Lee et.al. 03]
4. Real world
   - Votopia – 2002 Worldcup voting project, ICU, Korea
   - VoteHere – Seattle based active voting company
5. Conclusion

1. Introduction to Electronic Voting

Electronic Voting

- Implement real world voting (election) by electronic means (using computer and network)



Why Electronic Voting?

- Advantages
  - Convenience for voters
  - Efficiency of management, counting
  - Provide alternative choice for voters rather than traditional paper-based voting
- Electronic voting can solve the problem of decreasing participation rate in voting
  - Younger generation prefers electronic means

Classification of e-voting

- **Computer voting** (kiosk, electronic voting booth)
  - Electronic voting using computer in voting booth
  - Convenient user interface
  - Efficient management and tally
  - But, just half way to electronic voting
- **Internet voting**
  - Electronic voting using computers connected to the Internet
  - Can participate in voting in any place over the Internet
  - Proceeding to mobile voting

Electoral Systems

1. Plurality systems (First-Past-The-Post)
   - Winner is who received the most votes regardless of majority requirement
   - UK, Canada, USA
   - Single non-transferable vote : Japan
   - Block vote, Limited vote : Britain
   - Approval voting : USA
2. Majoritorian systems
   - Winner is required to receive more than half
   - Second ballot
   - Preferential voting (Alternative voting) in Australia

Security Requirements

- Privacy (confidentiality)
- Prevention of double voting
- Universal verifiability (correctness)
- Fairness
- Robustness
- Receipt-freeness (prevent vote buying, coercion)

- Efficiency, Mobility, Convenience, Flexibility

Approaches to Electronic Voting

- Schemes using blind signature
  - [Cha88], [FOO92], [OMAFO99]
  - Efficient, but requires anonymous channel (frequently implemented using mixnet)
- Schemes using mixnet
  - [PIK93], [SK95], [Abe98], [HS00], [FS01], [Neff01]
  - Require huge computation for mixing
- Schemes using homomorphic encryption
  - [Ben87], [SK94], [CGS97], [LK00], [Hirt01], [MBC01], [BFPPS01], [LK02]
  - Huge proof size, restriction on message encoding
  - Many researches on receipt-freeness

2. Three Main Approaches

2.1 Based on blind signature

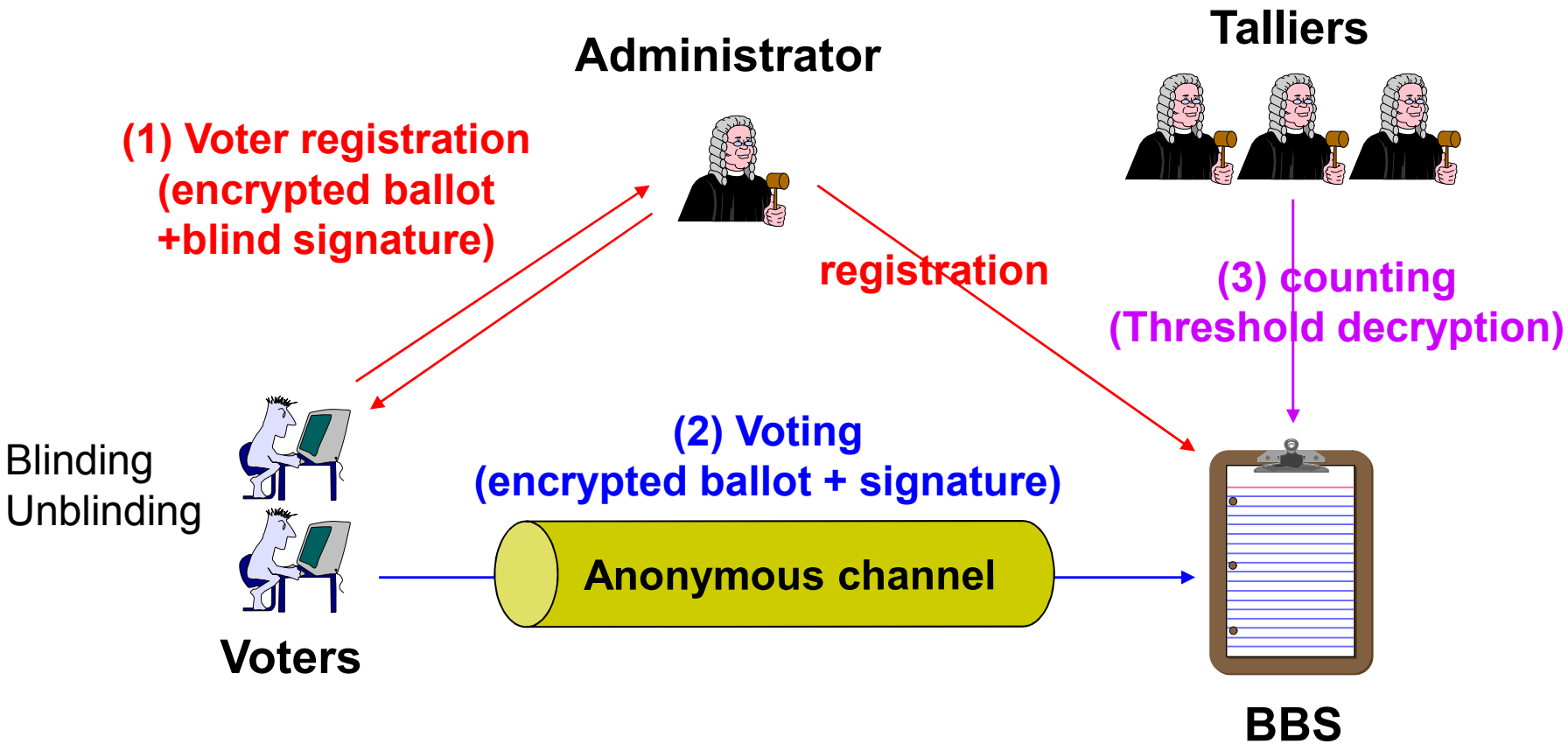
2.2 Based on homomorphic encryption

2.3 Based on mixnet

2.1 Based on Blind Signature

- Main idea
  - Administrator issues valid ballots using blind signature (User authentication and vote secrecy)
  - Use anonymous channel to hide the voter-vote relationship (mainly implemented with mixnet)
- Criticism
  - Hard to assume anonymous channel
  - If mixnet is used, blind signature is not necessary
  - User chosen randomness in blinding can work as a receipt

Overview


Administrator
Talliers
(1) Voter registration
(encrypted ballot
+blind signature)
registration
(3) counting
(Threshold decryption)
Blinding
Unblinding
(2) Voting
(encrypted ballot + signature)
Anonymous channel
Voters
BBS

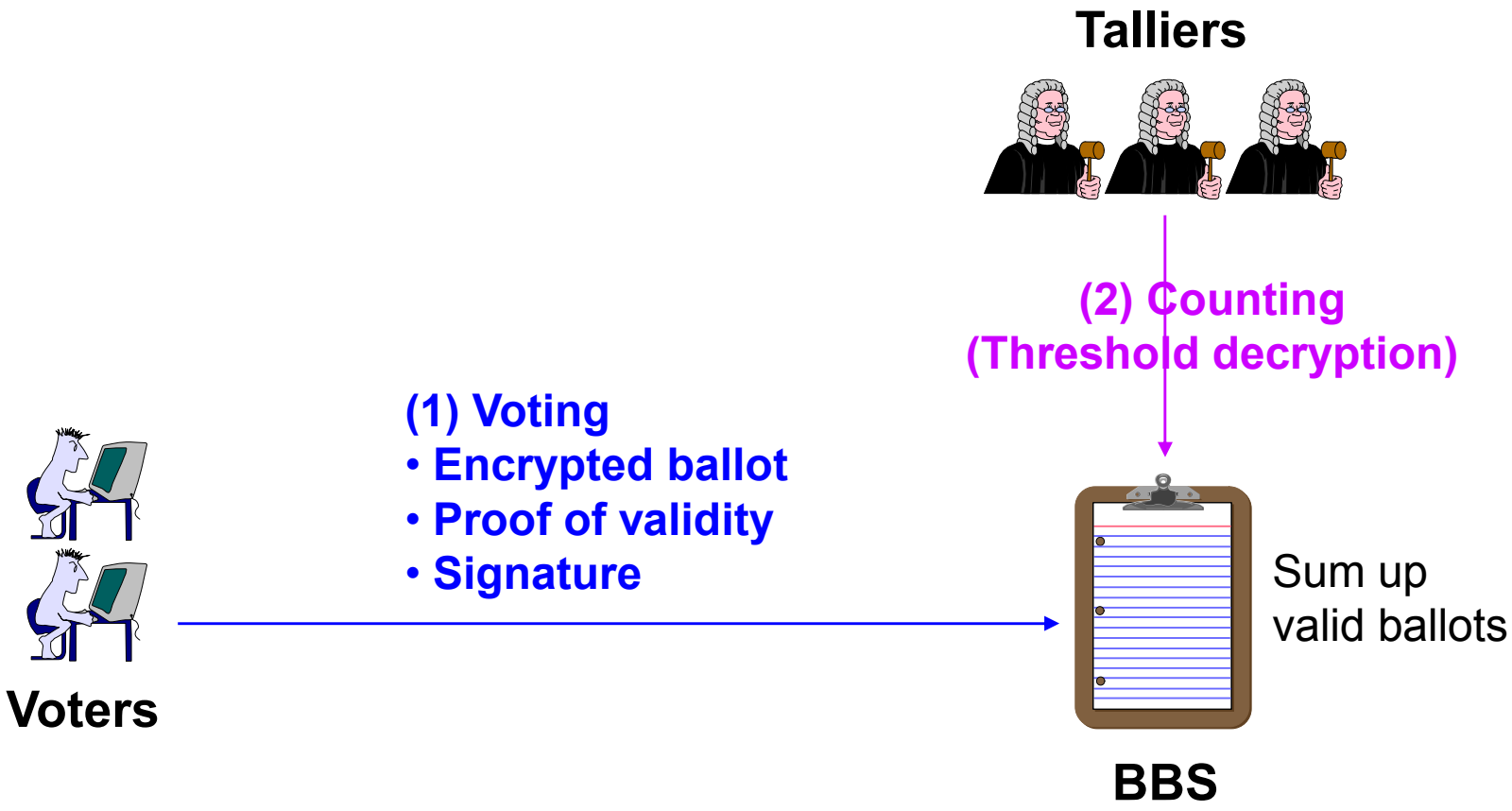
Many Implementation Examples

- Sensus
  - L.F. Cranor, Washington Univ. http://www.ccrc.wustl.edu/~lorracks/sensus
  - FOO92
  - Assumption : anonymous channel, key distribution
- EVOX
  - M.A. Herschberg, R.L. Rivest, MIT, http://theory.lcs.mit.edu/~cis/voting/voting.html
  - FOO92 + Anonymizer
  - Assumption : key distribution

2.2 Based on Homomorphic Encryption

- Main idea
  - Tally the summed ballots with a single threshold decryption using the homomorphic property of encryption (keep the privacy of ballots)
  - Each ballot should be valid (voter should provide the proof of validity of ballot)
  - Relatively easy to design receipt-free voting schemes
- Criticism
  - Message encoding is very restrictive
  - Large amount of ZK proofs, overload in computation and communication

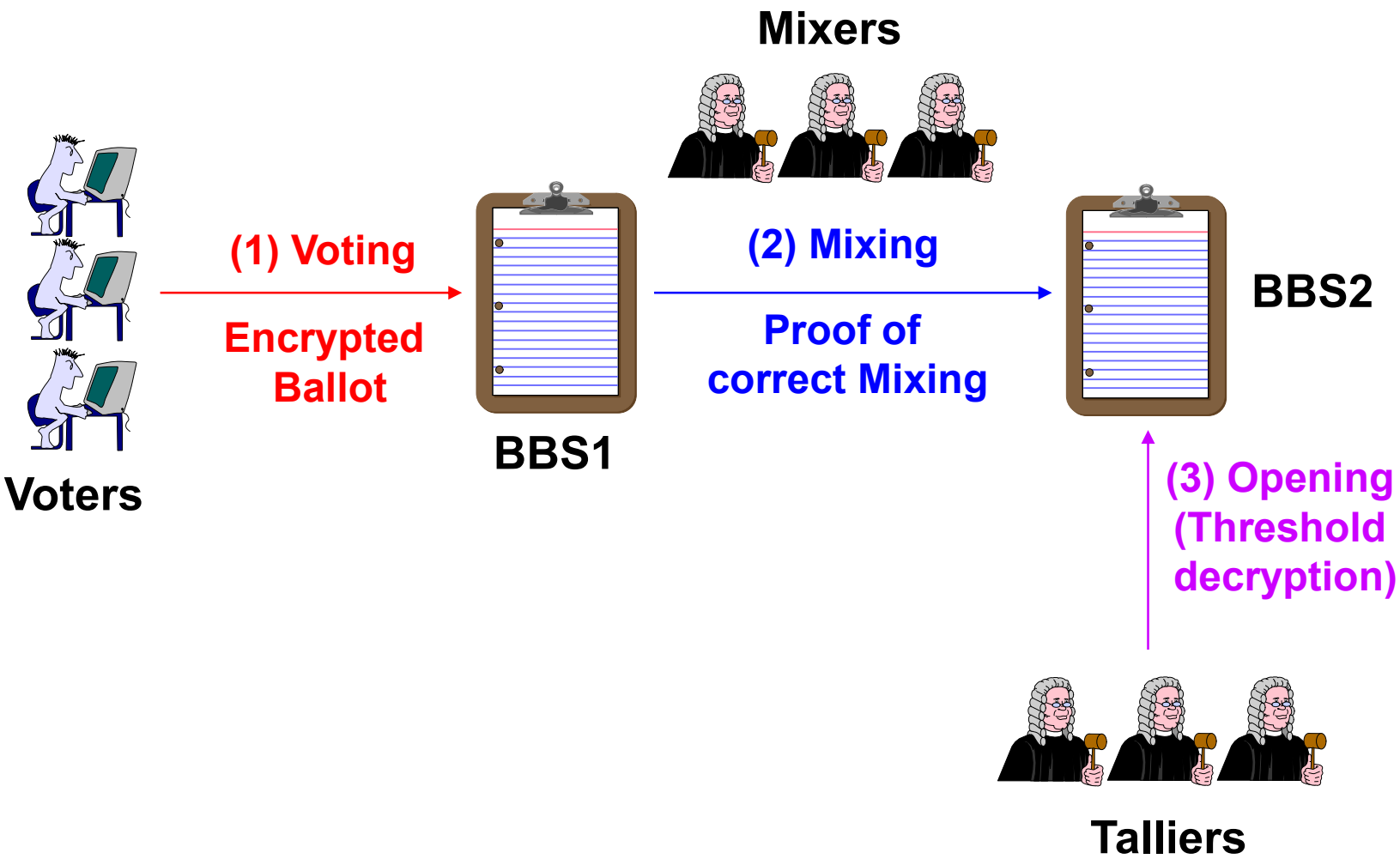
Overview


Talliers
(2) Counting
(Threshold decryption)
(1) Voting
• Encrypted ballot
• Proof of validity
• Signature
Voters
Sum up
valid ballots
BBS

2.3 Based on Mixnet

- Main idea
  - Voters take part in the voting in authentic way
  - Encrypted ballots are shuffled using mixnet (anonymity)
  - Multiple talliers open each ballot in a threshold manner (open only after mixing)
- Criticism
  - Large amount of computation for mixing

Overview


Mixers
(1) Voting
Encrypted Ballot
BBS1
(2) Mixing
Proof of correct Mixing
BBS2
Voters
(3) Opening (Threshold decryption)
Talliers

3. Receipt-free Voting Protocols

3.1 Receipt-freeness

3.2 In Hirt-Sako scheme [HS00]

3.3 In Homomorphic encryption based voting [LK02]

3.4 In mixnet based voting [Lee et.al. 03]

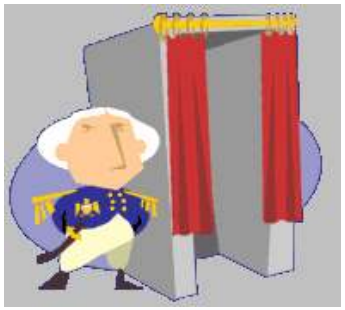
3.1 Receipt-freeness

- Receipt-freeness [BT94]
  - A unique security requirement of electronic voting
  - Voter should not be able to construct a receipt
  - Voter must keep his vote private
- Why is it important?
  - Vote buying is a common experience in real political voting (threat, solicitation)
- Previous works
  - Studies on receipt-freeness had been done mainly in homomorphic encryption based schemes

How to Achieve Receipt-freeness?

- Using some kind of randomization service
  - Voter has to lose his knowledge on randomness
  - Designated-verifier re-encryption proofs
- Channel assumption is used
  - One-way untappable channel from voter to authority [Oka97]
  - One-way untappable channel from authority to voter [SK95, HS00]
  - Two-way untappable channel between voter and authority (using voting booth) [BT94, LK00, Hirt01]
  - Internal channel [MBC01, LK02, Lee03]

Tamper Resistant Hardware

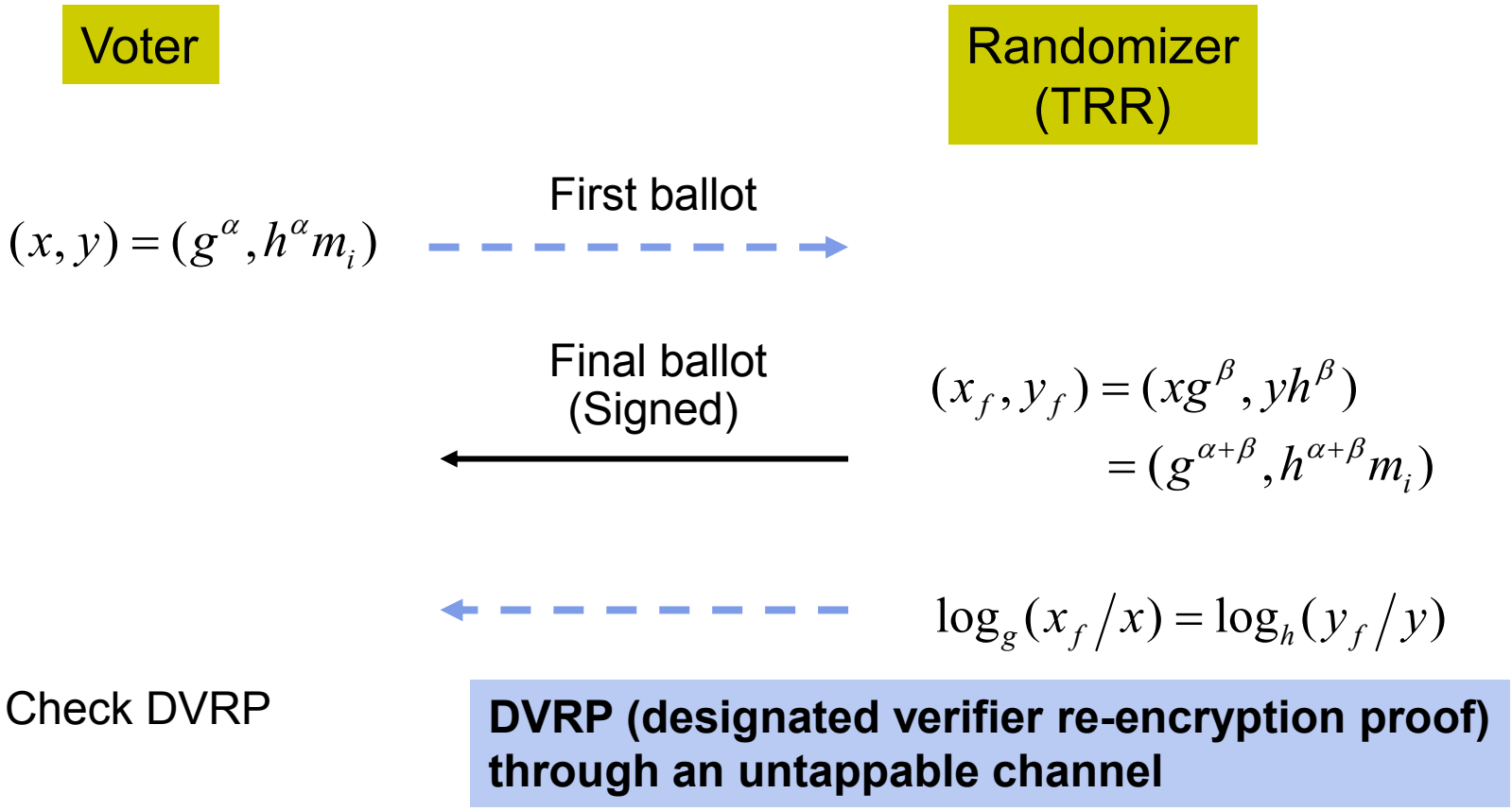


- Assumptions required for receipt-freeness
  - Third party randomizer (trusted)
  - Untappable channel (voting booth)

- Tamper resistant randomizer (TRR)
  - can replace the role of

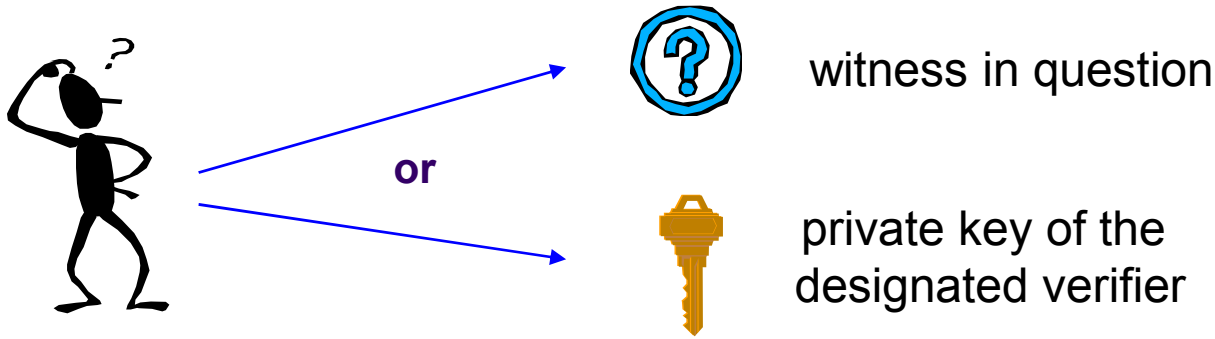
    "Third party randomizer + Untappable channel"
  - Ultimate place to store user's secret information

Re-encryption (Randomization)



Designated-verifier Re-encryption Proof

- Designated verifier proof
  - Prove the knowledge of either the witness in question or the private key of the designated verifier
  - Using the chameleon commitment scheme

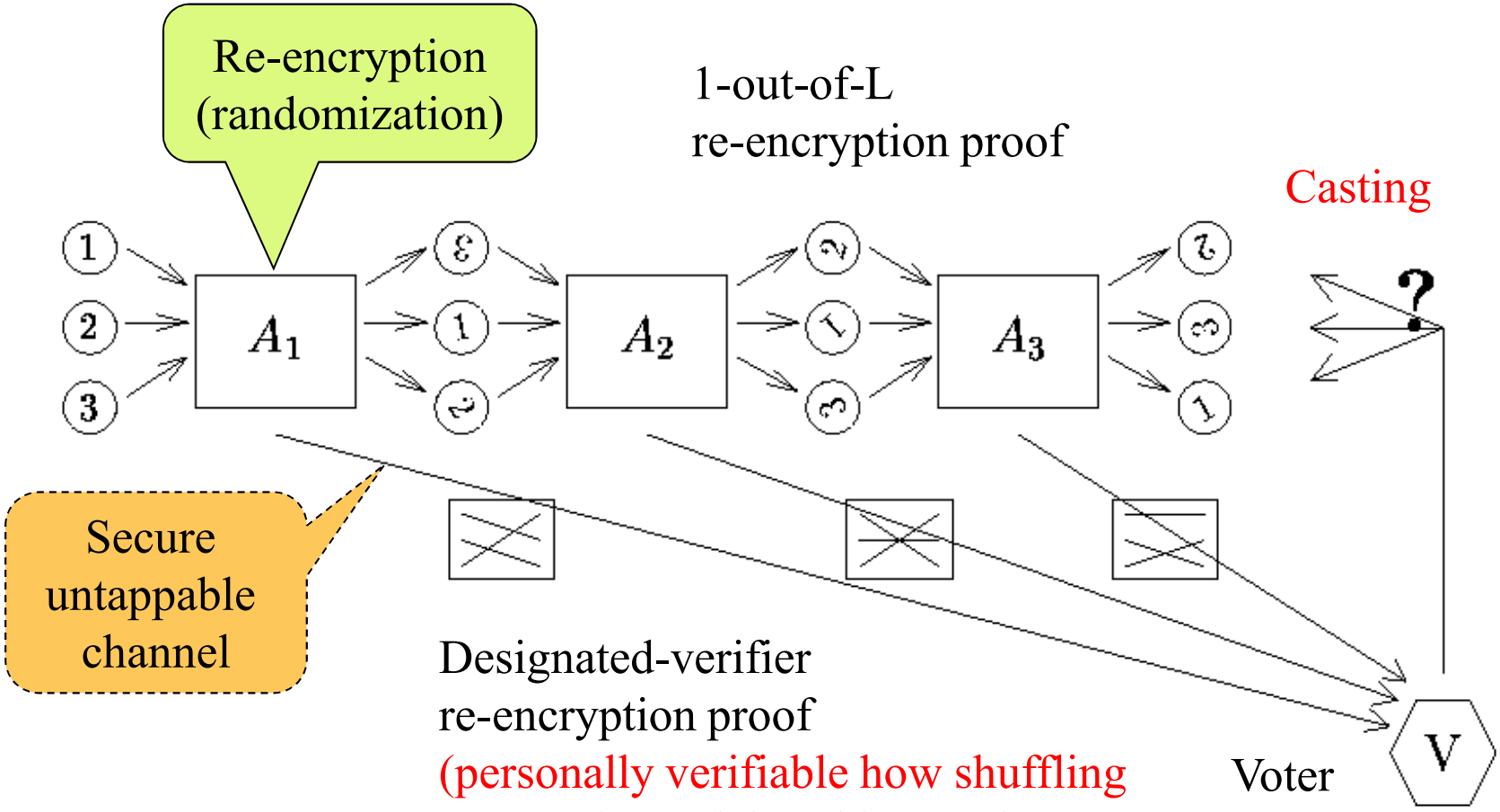


  - Convincing only the designated verifier
  - Completely useless when transferred to other parties, since the verifier can open the proof in any way he likes

3.2 Receipt-freeness in [HS00]

- Hirt and Sako, “Efficient receipt-free voting based on homomorphic encryption”, Eurocrypt2000
- Basic idea: “Mix-then-choose” approach
- Primitives
  - 1-out-of-L re-encryption proof : authority proves publicly that she shuffles the ballots correctly
  - Designated-verifier re-encryption proof : authority proves privately to voter that which encrypted ballot is which

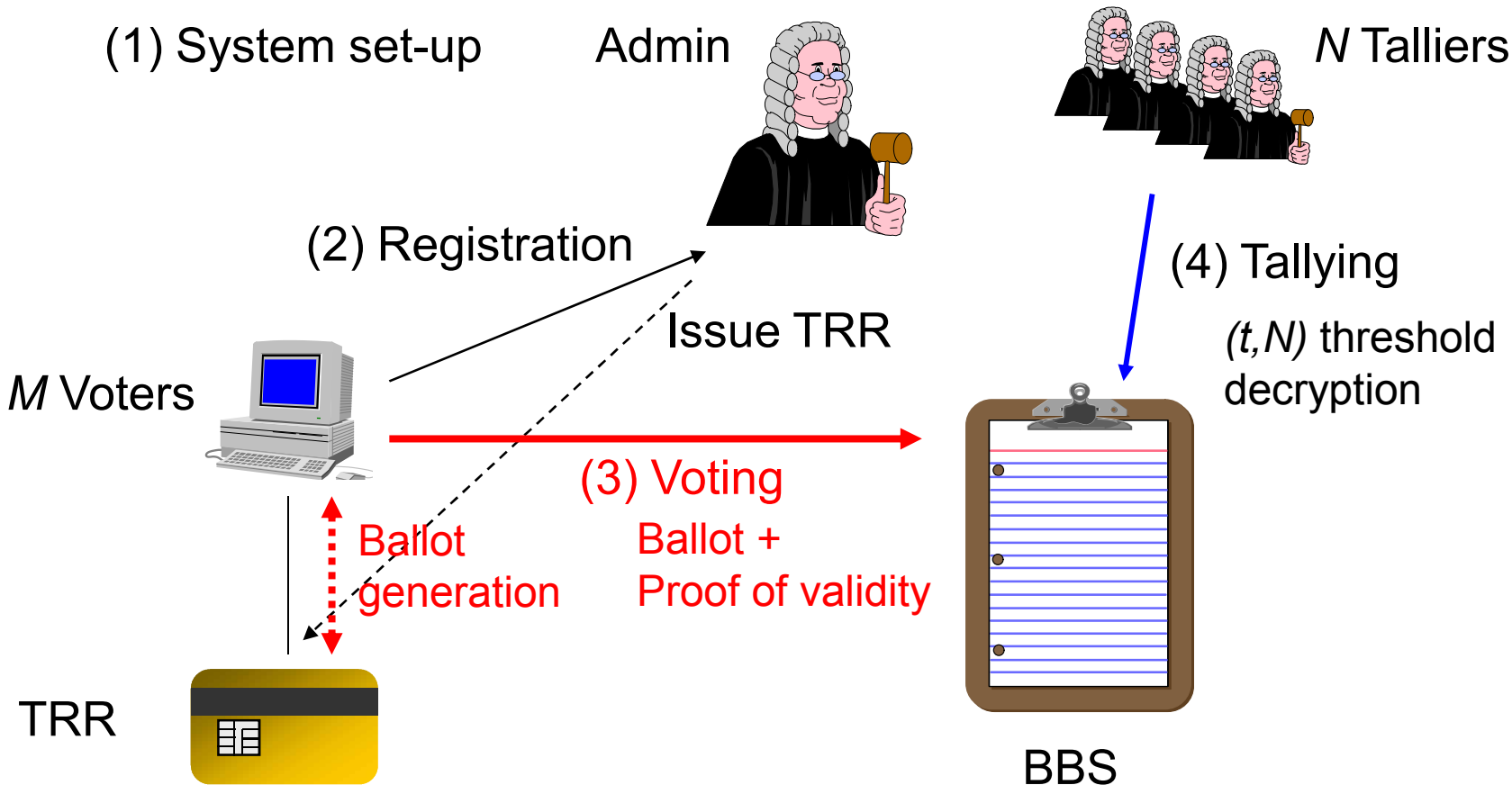
Receipt-freeness in [HS00]



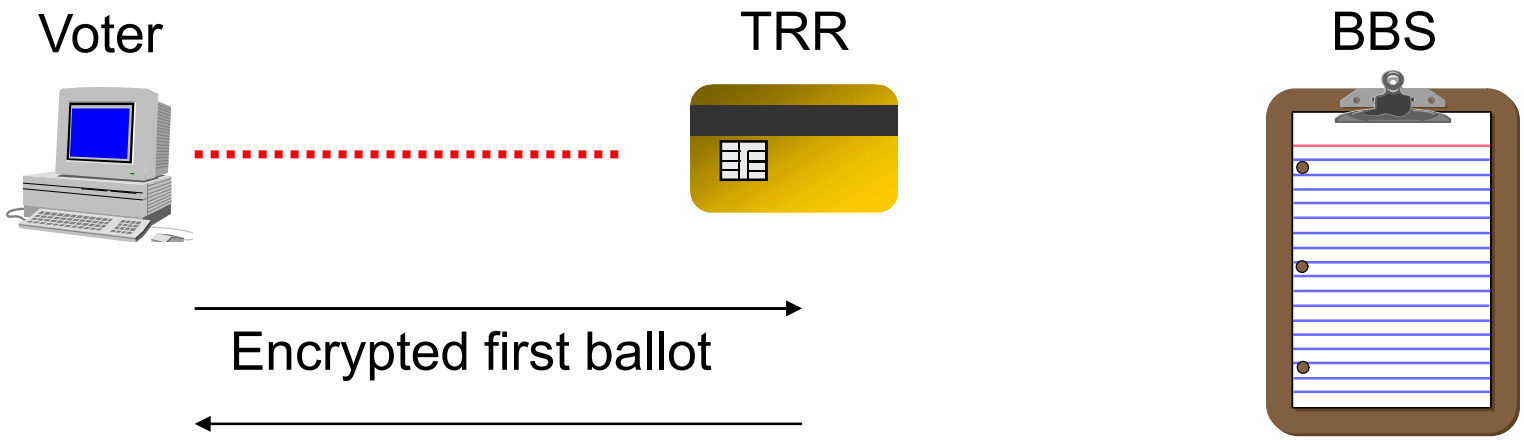
3.3 In Homomorphic Encryption Based Voting [LK02]

- Lee and Kim, “Receipt-free electronic voting scheme with a tamper-resistant randomizer”, ICISC2002
- Basic Idea: Improved K-out-of-L voting scheme using
  - Designated-verifier re-encryption proof (DVRP)
  - Divertible proof of validity
  - Divertible proof of difference
  - Replace untappable channel and a third party randomizer by a tamper-resistant randomizer (TRR)

Overview of Voting Protocol



Voting Stage



3.4 In Mixnet-based Voting

- Lee, Boyd, Dawson, et. al., “Providing receipt-freeness in mixnet-based voting protocols”, ICISC2003
- Incorporate receipt-freeness in mixnet-based electronic voting
  - Designated-verified re-encryption proof (DVRP)
  - Using a tamper resistant randomizer (TRR)
- Mixnet voting + Randomization by TRR
  - 1. Voting (Randomization by TRR)
  - 2. Mixing
  - 3. Tally

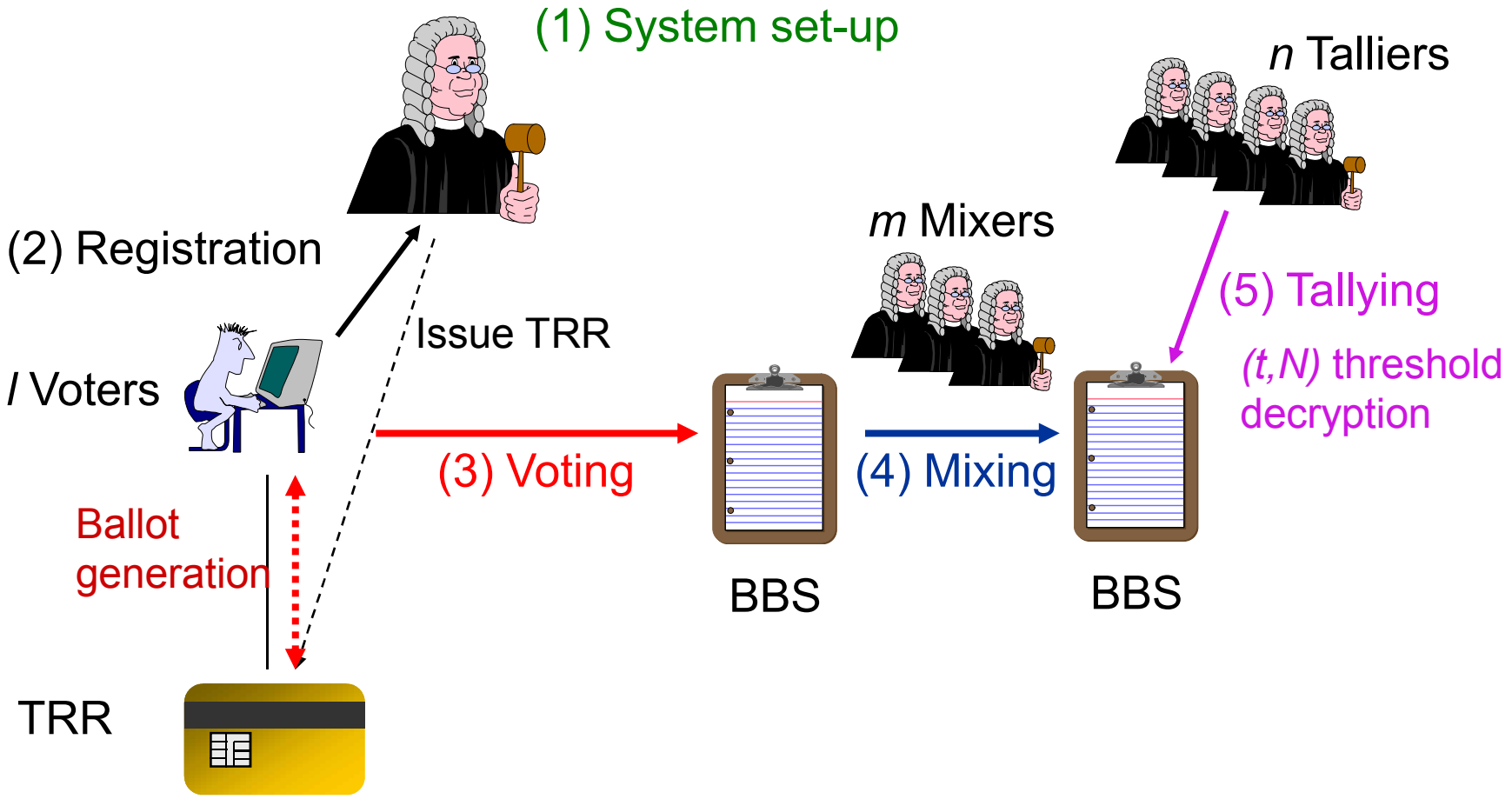
Mixnet Schemes

- Mixnet provides anonymity service

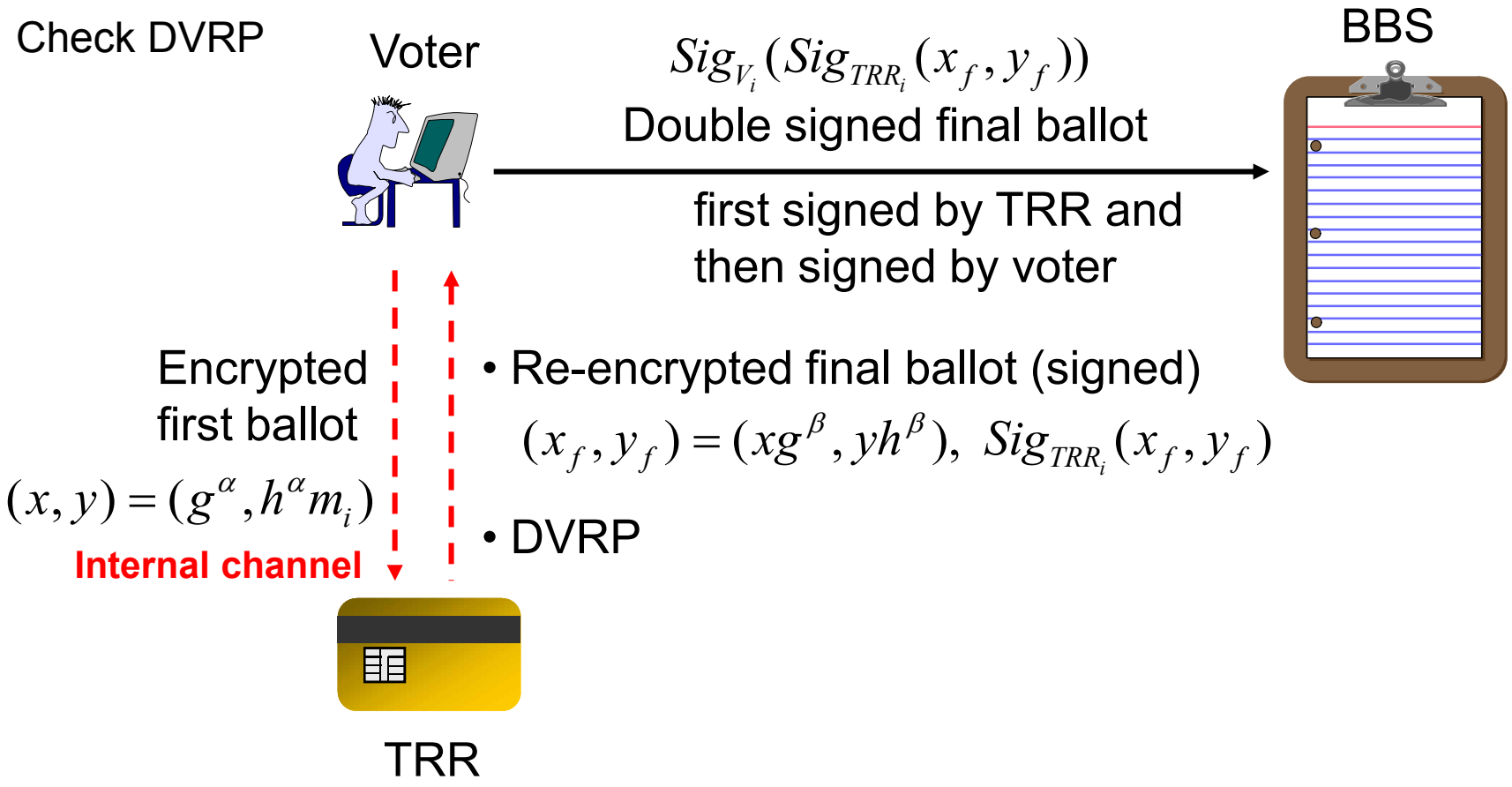
- Classification (based on mixing mechanism)
  - Decryption mixnet
  - Re-encryption mixnet
- Classification (based on correctness proof)
  - Verifiable mixnet: [Abe99], [FS01], [Nef01], [Gro03]
  - Optimistic mixnet: [Jak98], [Gol02]

In Mixnet-based Voting

Overview



(3) Voting stage



4. Real World

4.1 Votopia

http://mvp.worldcup2002.or.kr/

4.2 VoteHere

http://www.votehere.com

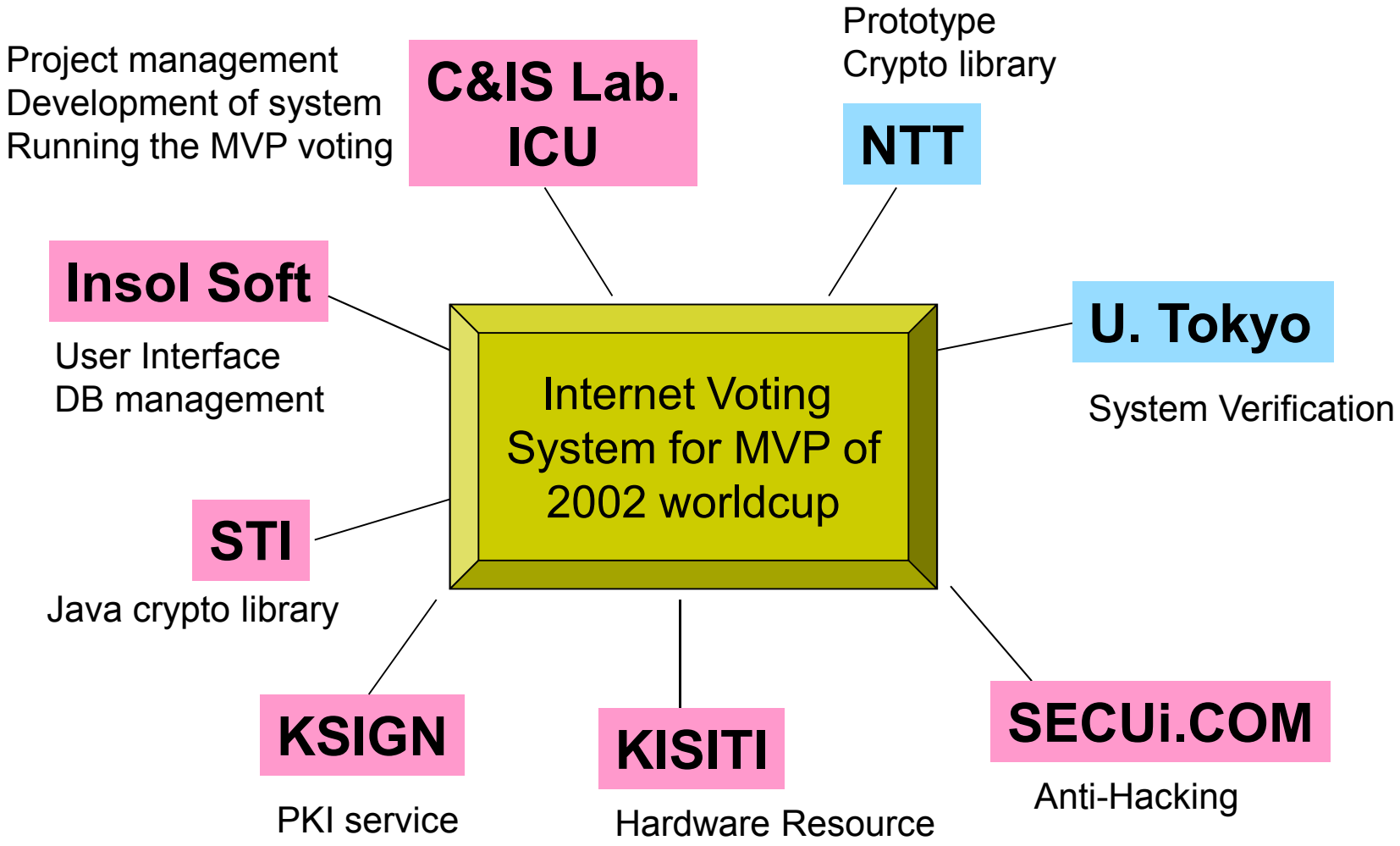
Activities in the Real World

- **International Projects**
  - Internet Voting Technology Alliance, http://www.ivta.org
  - EU CyberVote, http://www.eucybervote.org
  - Votopia, http://mvp.worldcup2002.or.kr/
- **Companies**
  - VoteHere.Net, http://www.votehere.net/
  - CyberVote.Com, http://www.cybervote.com/
  - SCYTL, http://www.scytl.com/
  - Campus-Vote, http://www.campus-vote.com/
  - Exnet, http://exnet.bizmag.co.kr
  - Hwajinsoft, http://www.hwajinsoft.co.kr

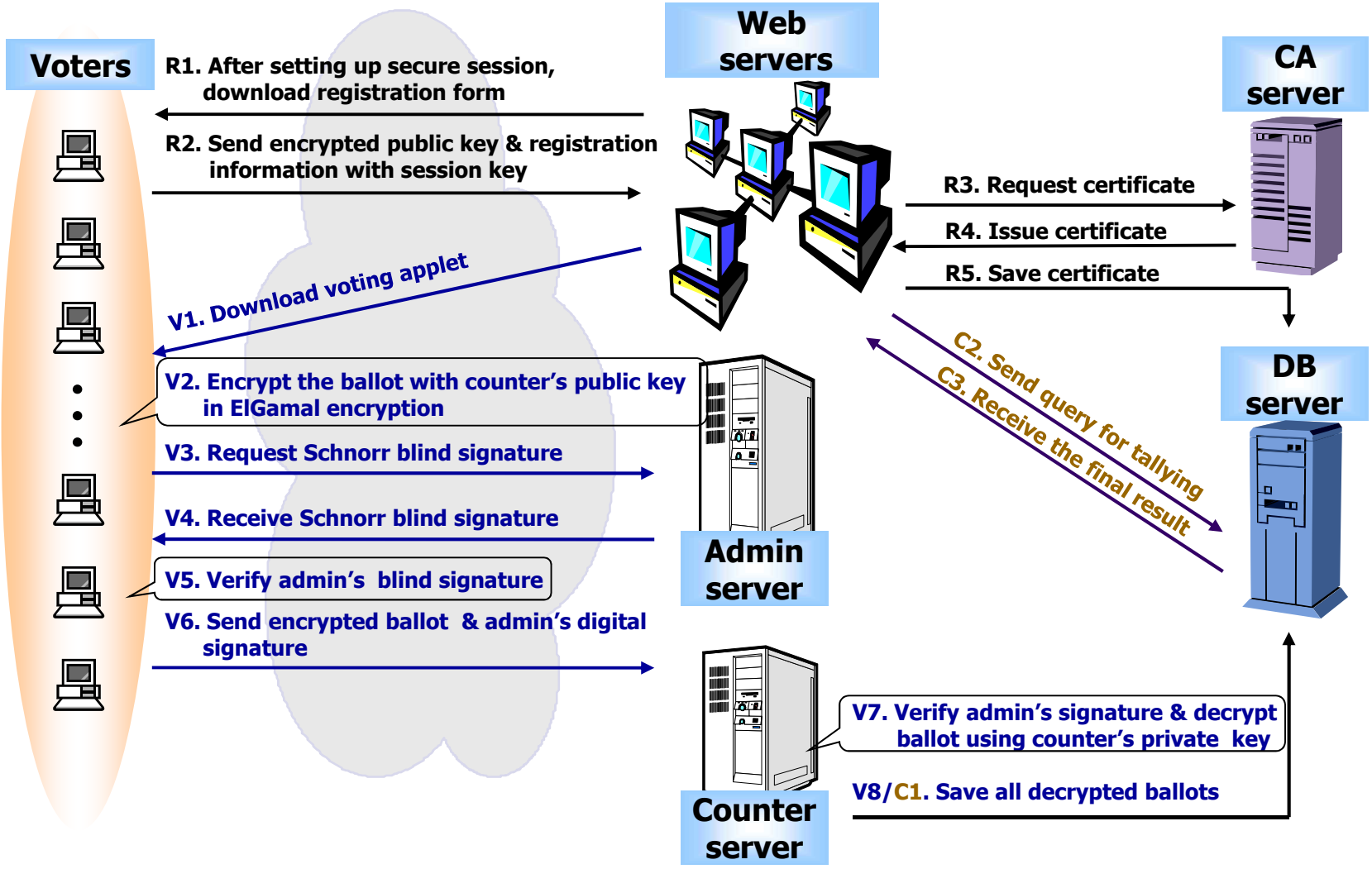
4.1 Votopia

- Developed by ICU (Korea) and NTT (Japan)
- Blind signature based Internet voting system
  - Anonymous channel by using mixnet
  - Using Internet web browser
  - Voting client is implemented by Java applet
  - PKI based voter authentication
- Served for the selection of MVPs in 2002 FIFA Worldcup Korea/Japan
  - http://mvp.worldcup2002.or.kr/

Participants in the Project



Overall Configuration



4.2 VoteHere.net

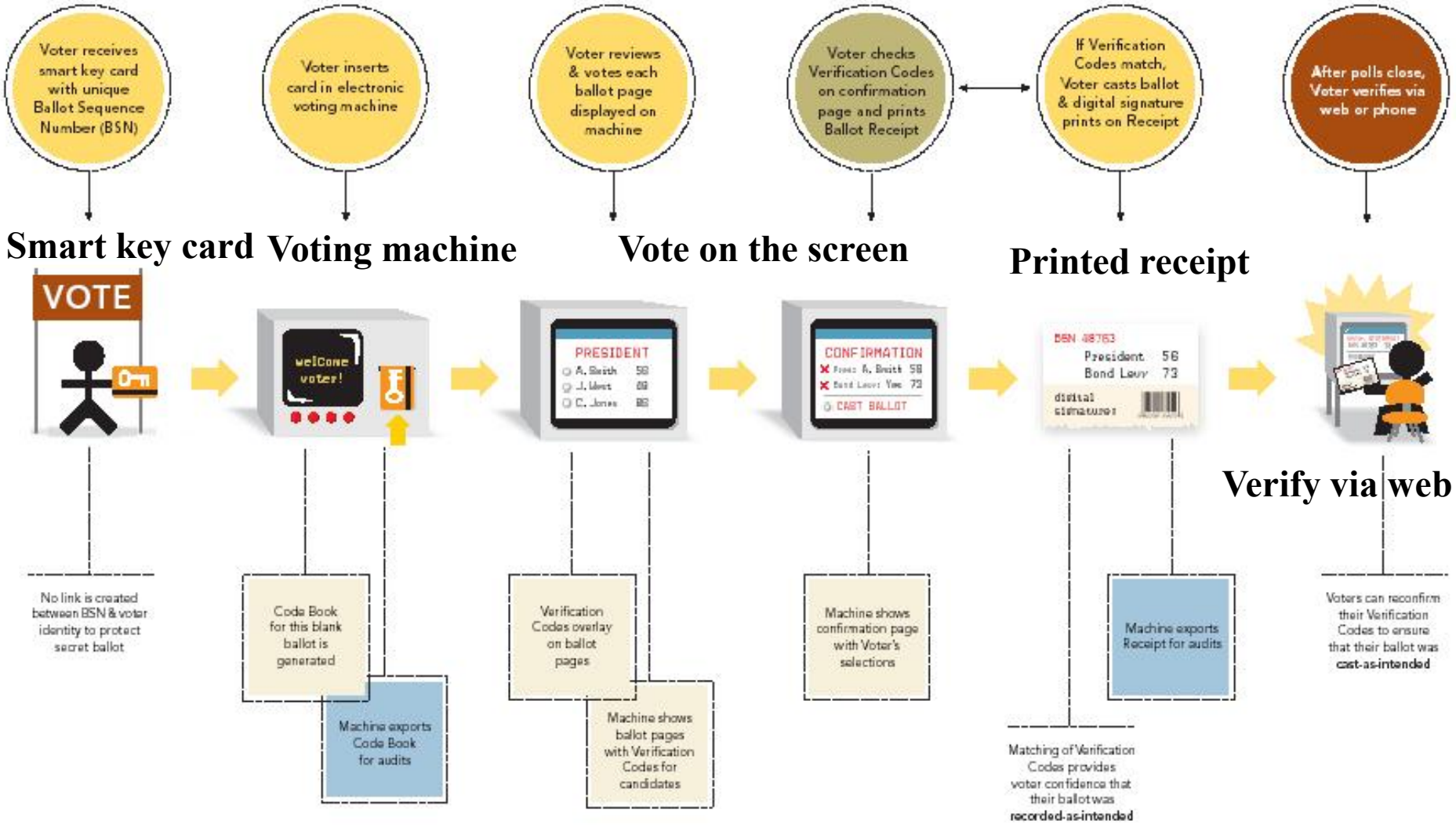
- Seattle based active voting company
  - http://www.votehere.net

- Many voting trials
  - Alaska Republican Party vote in January 2000
  - e-voting pilots for California, Arizona, Washington, and Alaska
  - Swindon, UK, the first e-voting public sector vote in the world, over 4,000 voters participated, May 2002

Technologies

- Homomorphic encryption based techniques
  - Voter receives smart key card with unique ballot sequence number
  - Use electronic voting machine (voting booth)
  - Give a digital signature printed receipt to voters
  - Heavily depend on trusted parties and machines (must believe verification code)
- Shuffling technology, A. Neff [ACM CCS 2001]
  - Verifiable permutation using iterated logarithmic multiplication proof

Voting Stages



5. Conclusion

5.1 Korean activities

5.2 Australian activities

Korean Activities

- Korea is a strong IT-based country
  - Broadband Internet connection to more than 70% homes
  - 30 million mobile users among 47 million population
  - More than 10 million Certificate users (Internet banking)
- e-government provides many services currently
  - http://www.egov.go.kr/
- E-voting activities
  - Public forums, seminars
  - E-voting for presidential candidate election in Democratic party, 2002
  - Some political parties are using Internet voting

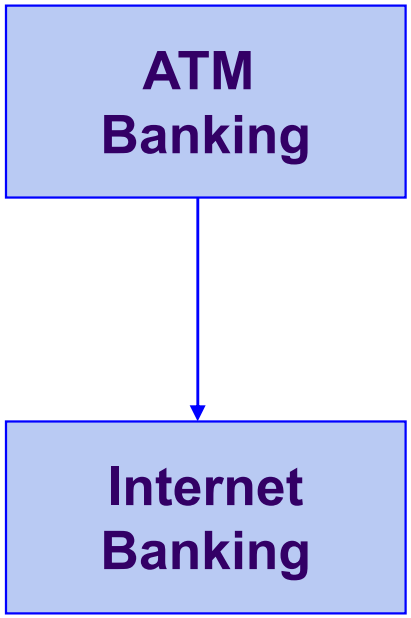
Australian Activities

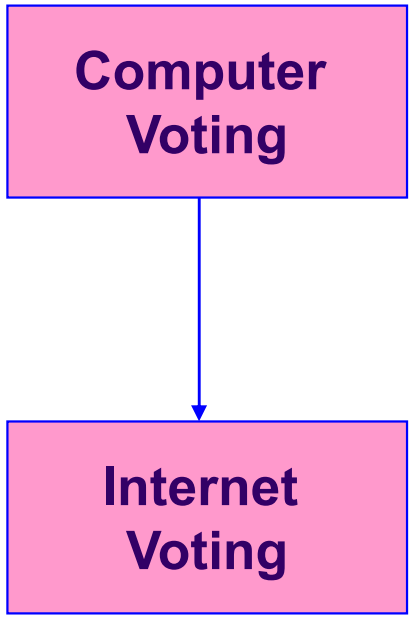
- Organizations
  - Electoral Council of Australia (ECA)
  - Australian Election Commission (AEC)
  - ACT Electoral Commission
- Electronic voting trial in October 2001
  - Australian Capital Territory (ACT) Electoral Commission
  - http://www.elections.act.gov.au

Comparison

- **Computer voting**
  - A secure environment, but not convenient
  - Many trials in many countries: USA, UK, Australia, Korea, etc…
  - Using just network security mechanism (?) – IPSec, SSL
  - Suitable for serious political elections
- **Internet voting**
  - More easy to participate in
  - Have to use secure electronic voting protocols
  - Authentication, Vote buying, Coercion issues
  - Suitable for non-serious elections

Internet Banking vs. Internet Voting





Secure environment

Public communication channel

Personal purpose
Non-serious(?)

Public purpose
Serious (political)
Non-serious (non-political)

Further Works

- Everlasting goal in research
  - Designing voting schemes with more security, efficiency, and additional features
- How to provide Australian preferential voting?
  - Probably using mixnet voting approach
  - Using real cryptographic protocols
- How to make it work in the real world?
  - More public activities – forum, workshop, standardization
  - Supported by the government
  - Good start with non-serious uses

Q & A