Coercion Resistant End-to-end Voting

Ryan W. Gardner   Sujata Garera   Aviel D. Rubin

ACCURATE

End-to-end Voting Schemes

```
┌─────────────────┐   encoded vote   ┌─────────────────────┐
│                 │  ──────────────▶ │                     │
│  Polling Place  │                  │ Public Bulletin Board│
│                 │                  │                     │
└─────────────────┘                  └─────────────────────┘
```

vote

receipt

receipt

verifies vote
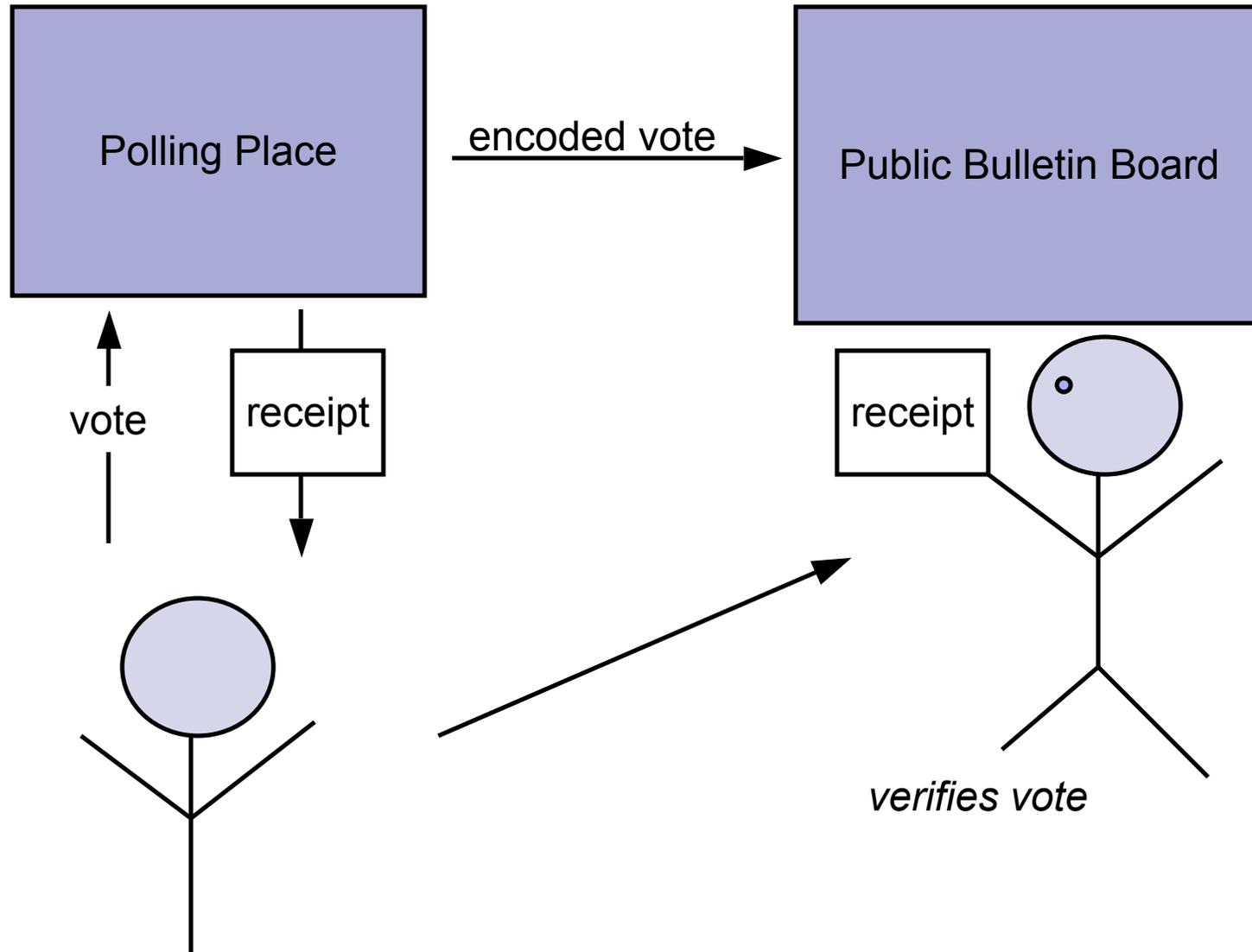
Motivation

- **End-to-end voting**
  - ☐ Integrity
    - ▪ Individual verifiability
    - ▪ Universal verifiability
  - ☐ Intended to provide guarantees regardless of software
- **Want to explore resistance of these schemes to attacks on privacy**
  - ☐ Civil right
  - ☐ Prevent coercion and vote selling

Vote Selling is Real

CNN.com technology > computing

Editions | myCNN | Video | Audio | Headline News Brief | Feedback

MAINPAGE
WORLD
U.S.
WEATHER
BUSINESS
SPORTS
TECHNOLOGY
computing
personal technology
SPACE
HEALTH
ENTERTAINMENT
POLITICS
LAW
CAREER
TRAVEL
FOOD
ARTS & STYLE
BOOKS
NATURE
IN-DEPTH
ANALYSIS
LOCAL

EDITIONS:

CNN.com Europe

Vote-selling Web site to be revived, possibly offshore

August 25, 2000
Web posted at: 3:05 p.m. EDT (1905 GMT)

By Richard Stenger
CNN.com Writer

(CNN) -- An Internet site designed to auction U.S. presidential votes could reopen days after New York authorities convinced its creator to shut it down, said a maverick Austrian businessman who bought the domain name.

Hans Bernhard said his holding company would operate voteauction.com outside the United States to circumvent federal and state laws that forbid purchasing and buying ballots.

"Our lawyers are evaluating the situation. The Web site should be up in the next 24 to 48 hours," Bernhard said Thursday. "We still have the option to go offshore if there are legal problems."

Vote Selling is Real

Our Contributions

- Consider privacy in the face of dishonest machines
- Identify example attack in a scheme by Benaloh [3,4]
  - Other attacks
    - Neff [10,11]
    - Benaloh and Tuinstra [14,15]
- Present a formal definition of coercion resistance geared toward end-to-end voting
- Present a new scheme that is coercion resistant under our definition
  - Extended from a scheme by Benaloh [3,4]
  - Minimal impact on the voter

Benaloh's Scheme [3,4]

Benaloh's Scheme

Anonymous
Voter

vote →

← encrypted vote

← "challenge?"

"yes/no" →

yes

← decryption of vote

*reveals randomness
used to encrypt*
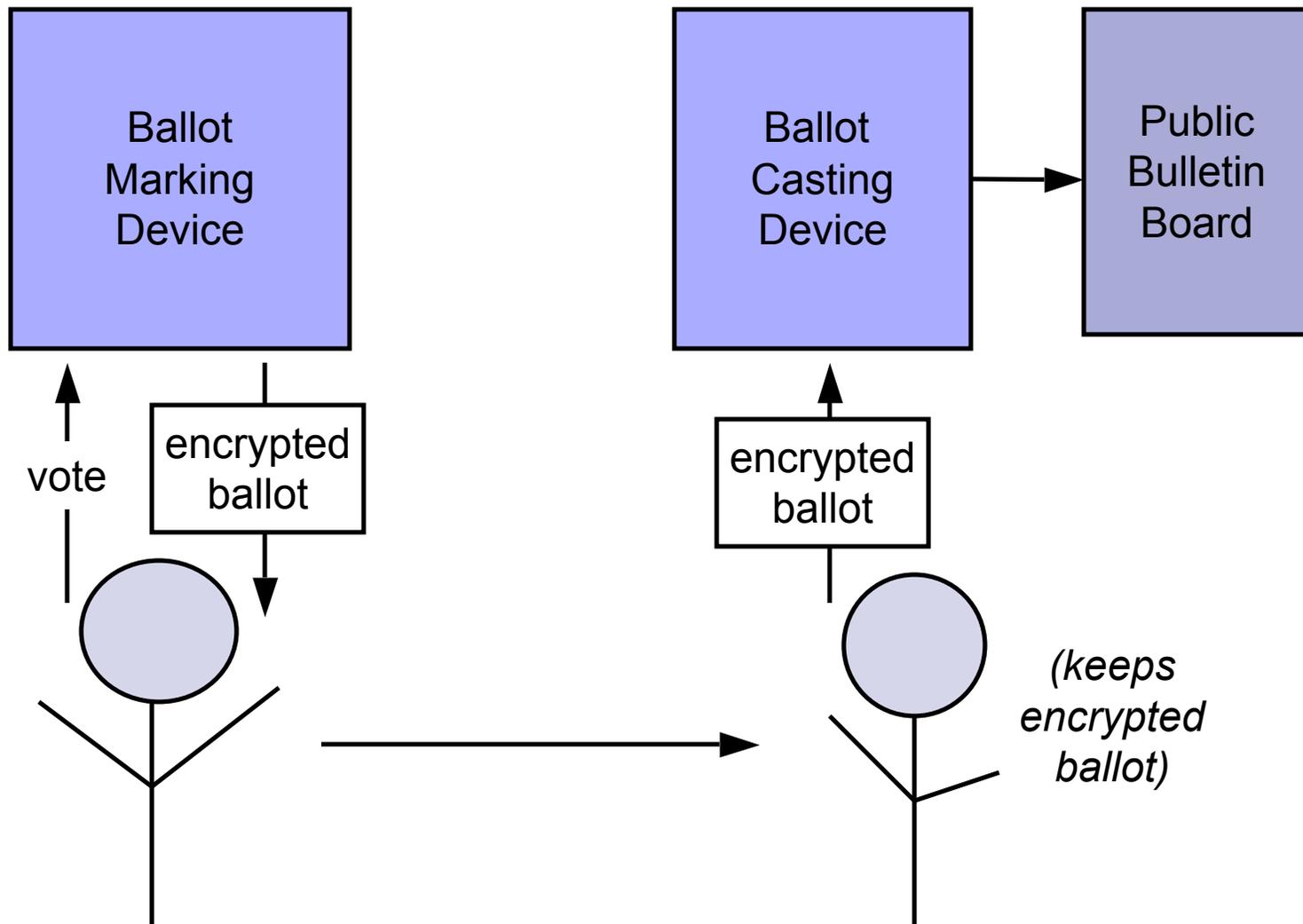
Ballot
Marking
Device
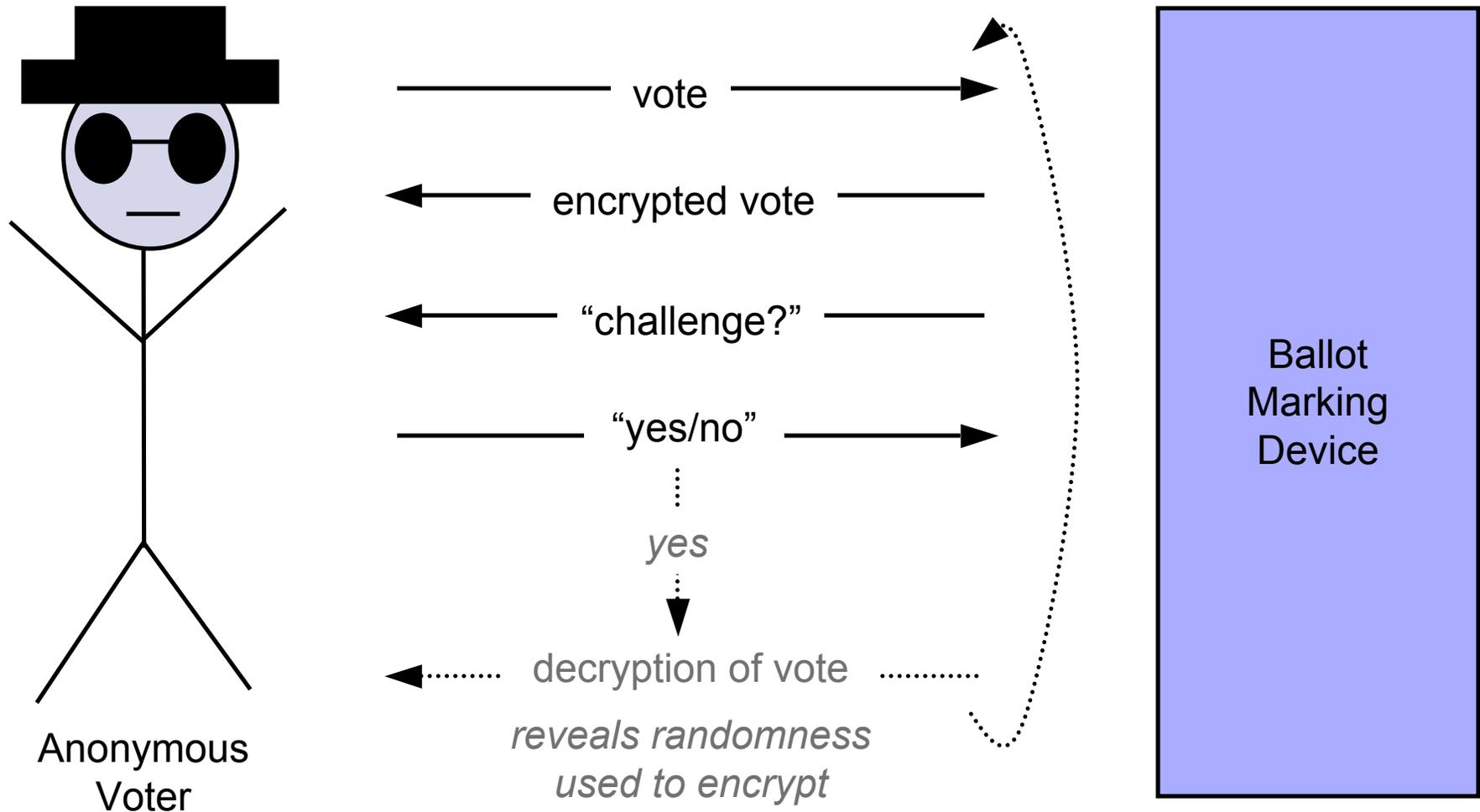
Compromising Privacy

- Encrypted vote is $\mathsf{Enc}_k(v,r)$
- Attacks
  - □ Known "randomness"
    - Fix PRNG in the machine and use it to generate "randomness" in encrypted votes
  - □ Non-determinism in general
    - Say we guarantee that the "randomness" was chosen at random at some point
    - Machine can try encrypting repeatedly with new values
    - Allows for subliminal channels
      - □ Reveal votes

Coercion Resistance

V: voting input
C: receipt output
P: proof of correctness

For all ballot creators and PPT adversaries:

$$V=(v,s,*) \longrightarrow$$

$$\longleftarrow C$$

$$\longrightarrow (V, C, P) \longrightarrow$$

. . .

. . .

$$V_0=(v_0,s',*)$$
$$V_1=\text{GenInput}(v_1,s',V_0) \longrightarrow$$

$$\longrightarrow (V_b, C_b, P_b) \longrightarrow$$

$$\longleftarrow C_b$$

adversary

ballot marker

verifier

$$V=(v,s,*) \longrightarrow$$

$$\longrightarrow (V, C, P) \longrightarrow$$

$$\longleftarrow C$$

. . .

. . .

$$b' \longrightarrow$$
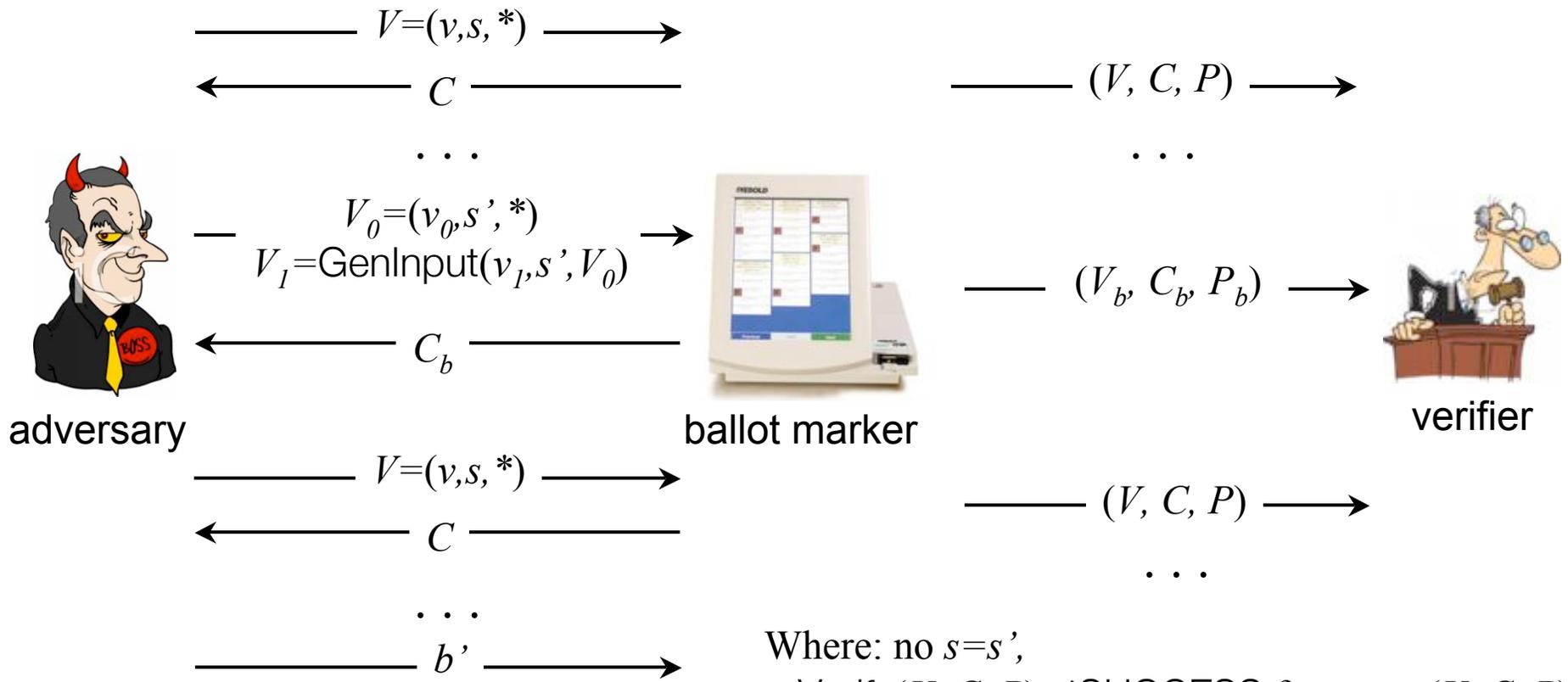
Where: no $s=s'$,
    Verify$(V, C, P) \neq$ SUCCESS for some (V, C, P)
    or $Pr(b'=b)<1/2 + \text{negl}(k)$

11

Coercion Resistance

- Intuitively
  - Adversary can interact with ballot marker as much as she wants
  - Adversary cannot distinguish between the output from a vote of her choice and any vote of the voter's choice
- No post-election communication between adversary and device
  - Mostly unavoidable [12]
  - Strictly stronger than previous models
  - Keeping privacy compromising information out of the public

High Level Description of Solution

- Root all entropy in a small number of keys
- Distribute among parties with conflicting interests
  - E.g. the political parties
  - Requires that one is honest
- Utilize inexpensive, trusted hardware
  - E.g. smart cards
- Allow users to verify pseudorandomness
- Based on the Dodis Yampolskiy verifiable random function [5]

Assumptions

- Group $\mathbb{G}$ of prime order p and $\mathbb{G}_1$ such that
  - Generator g
  - There is an admissible bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_1$
    - Bilinear: $e(g_1^x, g_2^y) = e(g_1, g_2)^{xy}$
    - Non-degenerate: $e(g, g) \neq 1$
    - Computable: There is an efficient (polynomial time) algorithm to compute e
  - q-decisional bilinear Diffie-Hellman inversion assumption (q-DBDHI) [5] holds
    - Can't distinguish $e(g,g)^{1/x}$ from random $\Gamma \in \mathbb{G}_1$ given $g, g^x, \ldots, g^{(x^q)}$

$\text{Enc}_{e,r} : \{0.1\}^* \to \{0.1\}^*$

Our Construction

- Initialization
  - Each of *n* political parties independently chooses a random $K_i \in \mathbb{Z}_p^*$ and writes it to a smart card *i*
  - Smart card from each party inserted into the ballot marking machine
  - Sets the public verification key to $\lambda_i = g^{K_i}$
  - $\lambda_1, \ldots, \lambda_n$ are posted to the public bulletin board

Ballot Marking

- Voter $\longrightarrow v \longrightarrow$ Machine
- Machine $\longrightarrow s \longrightarrow$ Smart card$_i$ for $i=1,\ldots,n$
- Smart card$_i - \pi_i = g^{1/(s+K_i)} \rightarrow$ Machine
- Machine computes $\mu = \prod_{i=1}^{n} \pi_i$ and pseudorandom value $r' = \varphi(e(g,\mu))$ (for hash φ)
- Machine computes $c = \mathsf{Enc}_{e,r'}(v)$
- Machine $\longrightarrow c \longrightarrow$ Receipt
- Machine asks **Voter** if she wishes to cast her created ballot

Option 1: Casting

☐ Voter indicates that she would like to cast this ballot

☐ Voter takes her Receipt with her encrypted vote c to the Casting Machine

☐ Receipt $\longrightarrow c, s \longrightarrow$ Bulletin Board

☐ Verify that c, s appear on the board

Option 2: Auditing

☐ Voter indicates that she would not like to cast this ballot

☐ Machine $\xrightarrow{\hspace{2cm} v \hspace{2cm}}$ Receipt

☐ Machine $\xrightarrow{s, v, c, \pi_1, \ldots, \pi_n}$ Bulletin Board

☐ Voter can check that v is correct and s, v, c appear on the Bulletin Board

☐ Any verifier including the voter can check that
$\text{Verify}(s, v, c, \pi_1, \ldots, \pi_n, \lambda_1, \ldots, \lambda_n)$ outputs SUCCESS where
$\text{Verify}(s, v, c, \pi_1, \ldots, \pi_n, \lambda_1, \ldots, \lambda_n)$

- Checks that $e(g^s \lambda_i, \pi_i) = e(g, g)$
- Computes $r' = \varphi\left(e\left(g, \prod_{i=1}^n \pi_i\right)\right)$ and $c'' = \text{Enc}_{e,r'}(v)$ and checks $c'' = c$

(For correct π_i, $\quad e(g^s \lambda_i, \pi_i) = e(g^s g^{K_i}, g^{1/(s+K_i)}) = e(g, g)$)

Tallying and Verification

☐ Voters check that no s appears on the bulletin board more than once

☐ Encrypted votes are secretly shuffled and decrypted with corresponding proofs of correctness

Preserving Uniqueness of *s*

- Require parties to program smartcards to only respond to strictly increasing values of *s*
  - Minimal requirements on smartcard
  - Voting machines can check before sending large values to the cards to prevent accidental DoS

Practical Considerations

- Impact on voters
  - Typical voter can simply cast vote and leave
  - Small percentage of voters need to audit ballots and check that s, v, c appear on the bulletin board correctly
  - Small percentage of voters need to check that their cast c appears on the bulletin board
  - One person needs to verify all the proofs and cryptographic operations
- Effectiveness
  - Example from Neff's analysis [13]
  - Suppose there were an election with
    - 100,000 voters
    - A machine attempted to dishonestly encrypt 500 ballots
    - If 1% of the created ballots were randomly audited, the cheating would be detected with greater than 99% probability

Summary

- Privacy is important

- Can increase privacy in end-to-end voting schemes without significantly increasing the impact on the voter

Future Work

- Human understanding
- Stronger model
  - Prevent a machine from potentially storing votes
- Removing the voter further
  - Use the smart cards to provide "challenges" to the machine
  - Use machine commitments as part of the seed (i.e. serial numbers)
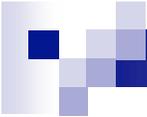
References

- [1] B. Adida and R. L. Rivest. Scratch and vote. In WPES '06: Workshop on Privacy in the Electronic Society, 2006.
- [2] M. Bellare and P. Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In CCS '93: ACM Conference on Computer and Communications Security, 1993.
- [3] J. Benaloh. Simple verifiable elections. In EVT '06:USENIX/ACCURATE Electronic Voting Technology Work- shop, 2006.
- [4] J. Benaloh. Ballot casting assurance via voter-initiated poll station auditing. In EVT '07:USENIX/ACCURATE Electronic Voting Technology Workshop, 2007.
- [5] Y. Dodis and A. Yampolskiy. A verifiable random function with short proofs and keys. In PKC '05: Workshop on Theory and Practice of Public Key Cryptography, 2005.
- [6] D. Chaum. Secret-ballot receipts: True voter-verifiable elections. IEEE Security and Privacy, 2(1):38-47, 2004.
- [7] R. Canetti, O. Goldreich, and S. Halevi. The random oracle methodology, revisited (preliminary version). In STOC '98: ACM Symposium on the Theory of Computing, 1998.
- [8] I. O. for Standardization. ISO/IEC 7816-8 standard, 2004.
- [9] P. Golle, M. Jakobsson, A. Juels, and P. F. Syverson. Universal re-encryption for mixnets. In Topics in Cryptology - CT-RSA ΙO4: Cryptographers' Track at RSA, 2004.
- [10] C. Karlof, N. Sastry, and D. Wagner. Cryptographic voting protocols: A systems perspective. In USENIX Security Symposium, 2005.
- [11] A. Neff. Practical high certainty intent verification for encrypted votes, 2004. Available at http://www.votehere.com/vhti/documentation.
- [12] B. Riva and A. Ta-Shma. Bare handed electronic voting with pre-processing. In EVT '07:USENIX/ACCURATE Electronic Voting Technology Work- shop, 2007.
- [13] A. Neff. Election confidence: A comparison of methodologies and their relative effectiveness at achieving it, 2003. Available at http://www.votehere.com.
- [14] J. Benaloh and D. Tuinstra. Receipt-free secret-ballot elections (extended abstract). In STOC '94: ACM Symposium on Theory of Computing, 1994.
- [15] M. Hirt and K. Sako. Efficient receipt-free voting based on homomorphic encryption. In EUROCRYPT '00: Advances in Cryptology, 2006.