



A Modular Voting Architecture ("Frogs")

Shuki Bruck

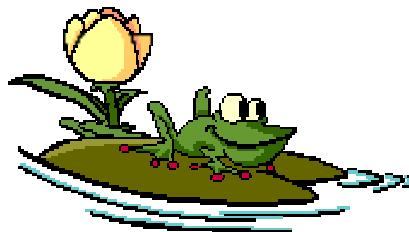
David Jefferson

Ronald L. Rivest

(CalTech)

(Compaq)

(MIT)



(WOTE, August 28, 2001)

Outline

- ◆ Moving from paper → electronic
- ◆ Voting with frogs
- ◆ Advantages of frogs
- ◆ Security
- ◆ Conclusions

What's next in voting?

- ◆ We propose a practical voting system for the near term (2004?) that
 - moves from paper to electronic
 - *emphasizes and standardizes a clean separation between "vote generation" and "vote casting" components* (for many good reasons).
 - uses digital signatures to witness "votes cast"

Where are we now? Op-scan

- ◆ Ballots are printed beforehand.
- ◆ On election day, voter:
 - Identifies himself
 - Receives ballot
 - Fills out ballot ("vote generation")
 - Casts ballot ("vote casting")
- ◆ Ballots scanned; results tabulated.
- ◆ Problems: UI , printing and storage costs, scanning accuracy, security.

Move from paper to electronic?

- ◆ Preserve “voting experience”
- ◆ Paper ballot → electronic “frog”
(term intended to be neutral as to technology)
- ◆ Frog might be “dumb” flash memory card (4K bytes) with “freeze” (lock) capability. (No software on frog to validate/certify!)



Voting with Frogs: (1) Sign-in

- ◆ Voter identifies himself to pollworker.
- ◆ Pollworker takes blank frog, and “initializes” it. (Election specification, ballot style written on frog.)
- ◆ Pollworker gives frog to voter.



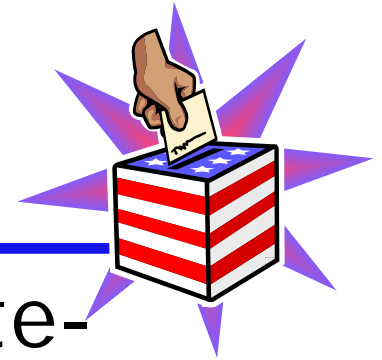
(2) Vote Generation



- ◆ Voter inserts frog into “vote generation” equipment.
- ◆ Vote generation equipment reads ballot style, provides superb UI for voter to indicate his selections.
- ◆ Voters selections are written onto frog in a standard format.
- ◆ Voter removes frog.



(3) Vote-casting



- ◆ Voter inserts his frog into vote-casting equipment.
- ◆ Voter sees frog contents displayed.
- ◆ If voter pushes "Cast" button:
 - Frog is digitally signed; same signing key(s) used for all votes.
 - Frog is frozen and deposited in frog bin.
 - Electronic copy(s) of vote → storage.
- ◆ Else frog is returned and voter goes back to (2) vote generation.

(4) Web posting/Tabulation

- ◆ Once election is over, election officials for each precinct post on Web, as separate, unmatched lists in random order:
 - Names of all voters who voted.
 - All cast ballots (with digital signatures)
- ◆ Everyone can verify signatures on ballots, and compute total.

Advantages of frogs

- ◆ Electronic: no “scanning errors”
- ◆ Frogs can be kept as “physical audit trail” after election.
- ◆ No printing costs: frogs can be purchased “blank” in bulk (20 cents?)
- ◆ Frogs can be stored compactly (size of business card?)
- ◆ Frog can be “frozen” when cast making it “read-only” (unmodifiable).

Advantages of frogs

- ◆ Frogs are *digital*: so they are compatible with cryptography (e.g. digital signatures).
- ◆ Frog is just a carrier for a digital representation of ballot; technology can evolve while keeping underlying data formats constant (our proposal is technology-neutral).

Standardized Frog Format

- ◆ This may be the most important part of our proposal:

*Standardize the format
of electronic ballots !!!*

- ◆ Standard data file format:
header + one line/race,
standard character set (UTF-8).
- ◆ This should be vigorously pursued,
independent of whether the rest of
our proposal is adopted.

Standardized Frog Format

```
Massachusetts, Middlesex County, Precinct 11  
Election Closes November 7, 2004 at 8pm EST  
Ballot: MA/Middlesex/1; English; No rotation  
Ballot Initialized by Election Official 10
```

You have chosen:

U.S. President: Mary Morris

U.S. Vice President: Alice Applebee

Middlesex Dog Catcher: Sam Smith (write-in)

Proposition 1 (Casino): FOR

Proposition 2 (Taxes): AGAINST

Proposition 3 (Swimming Pool): FOR

Proposition 4 (Road Work): NO VOTE

Standardized Frog Format

- ◆ Is both human and machine-readable.
- ◆ Provides a clean interface between vote-generation (frog-writing) and vote-casting (frog confirmation / freezing / depositing).
- ◆ Allows *different* manufacturers to build different vote-generation equipment (varying UI 's) compatible with *same* vote-casting equipment.

Security

- ◆ In near term, the only trustworthy equipment available to voter will be that provided by election officials. (PC's/handhelds/phones all vulnerable. Thus, no individual digital signatures, and no voting from home.)
- ◆ In effect, vote-casting equipment is "proxy" for voter in electronic voting scheme.

Security

- ◆ A secure system needs to be *simple*.
Very simple. Very very simple.
- ◆ A good user interface is *complex*.
Quite complex. Really very complex.
- ◆ It follows that the sophisticated user interface should be separated from the security-critical components.

What is *most* security-critical?

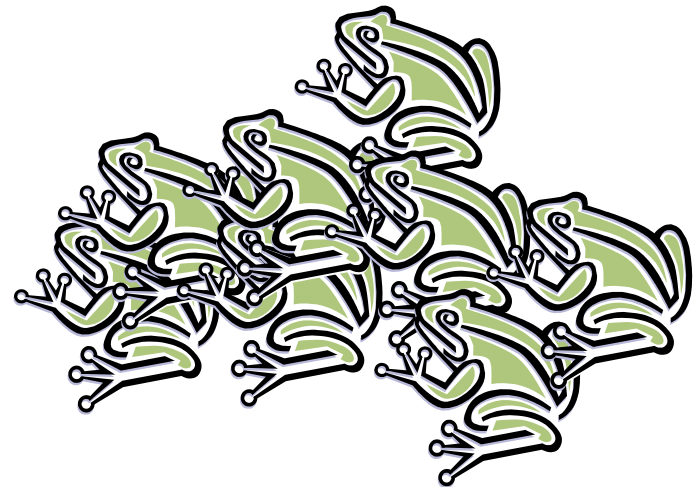
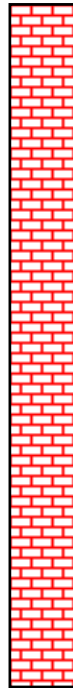
- ◆ *Vote-casting*, wherein voter
 - *Confirms* that his selection are recorded accurately,
 - *Officially casts* his recorded selections.
- ◆ This operation needs to be exceptionally trustworthy.
- ◆ With electronics, records are *indirect*; voter is much like a blind man voting with someone's assistance.

Vote-Casting: the critical instant

From "Bob's vote"



To "anonymous vote"



Vote-casting equipment should:

- ◆ Display *exactly and completely* whatever is in frog.
- ◆ Be *stateless* (no test/real modes!)
- ◆ For cast vote, *digitally sign* whatever is in frog, using one key (election official) or more (political parties too).
- ◆ Send copies of cast votes → storage units.
- ◆ Be *open source*.
- ◆ Be long-term purchase.

Vote-generation equipment:

- ◆ Is less security-critical.
- ◆ May have proprietary design/code.
- ◆ Has less stringent certification requirements, and so can evolve more quickly with technology.
- ◆ May be leased rather than purchased.

Notes:

- ◆ Anonymity up to precinct level; should be OK.
- ◆ Write-ins might be handled by “splitting” into write-in/non-write-in components to preserve privacy.
- ◆ Provisional ballots can be handled as usual. (Put aside in envelope.)
- ◆ Voter may prepare ballot at home and bring it to poll-site for final editing/casting.

Conclusion

We have presented a practical proposal for a modular architecture for near-term pollsite voting that can achieve a high degree of security while simultaneously enabling innovation.

(The End)
