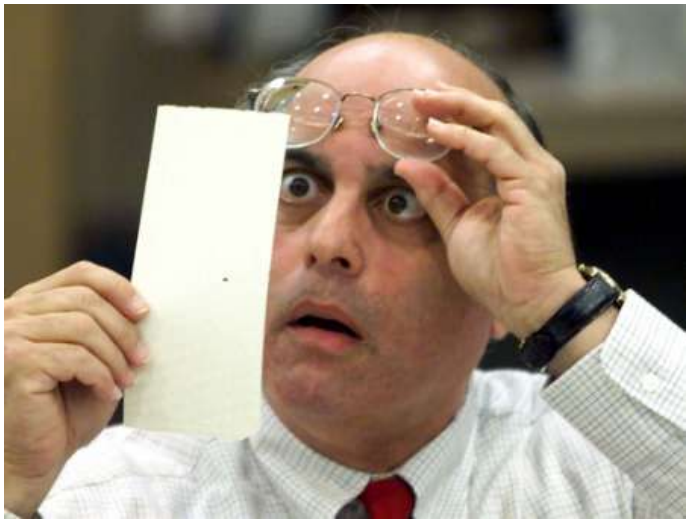
Auditability and Verifiability of Elections

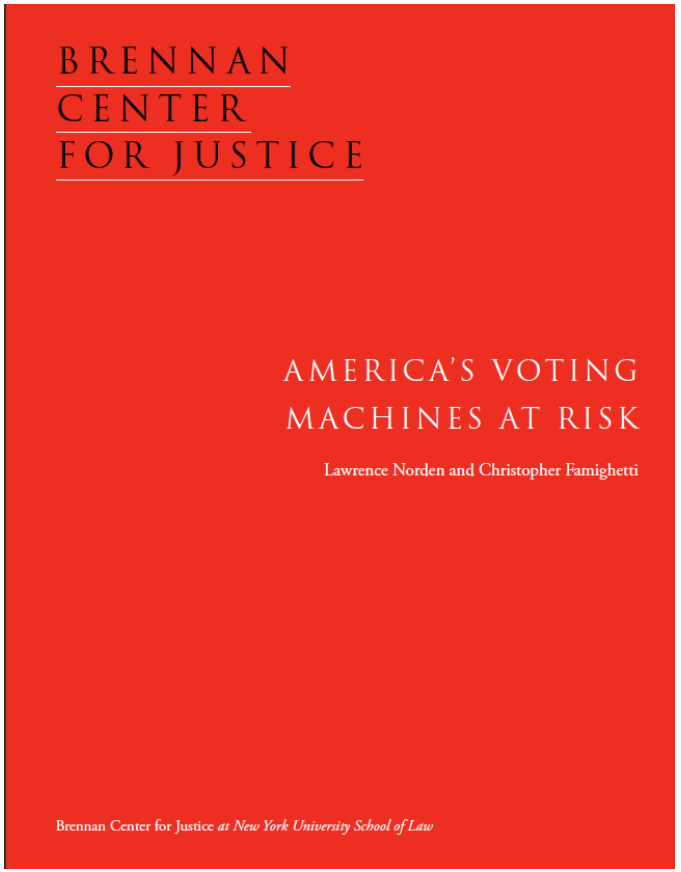
Ronald L. Rivest
MIT

UC Davis
December 1, 2016

Have we made progress since 2000?



Hanging chads (2000)



>>> Voting Machines at Risk (2015)

Nov. 2016 – Who Really Won?

Hillary or Donald ?

Evidence-Based Elections

An election should not only

find out who won,

but should also

provide convincing evidence

that the winner really won.

(Stark & Wagner 2012)

NO: "Trust me and my software"

YES: "Mistakes will be made. Find and fix them."

YES: "Trust but verify."

Outline

- Security Requirements
- Software Independence
- Auditing of Paper Ballots
- Cryptographic Voting Schemes (E2E)
- Remote (Internet?) Voting ???

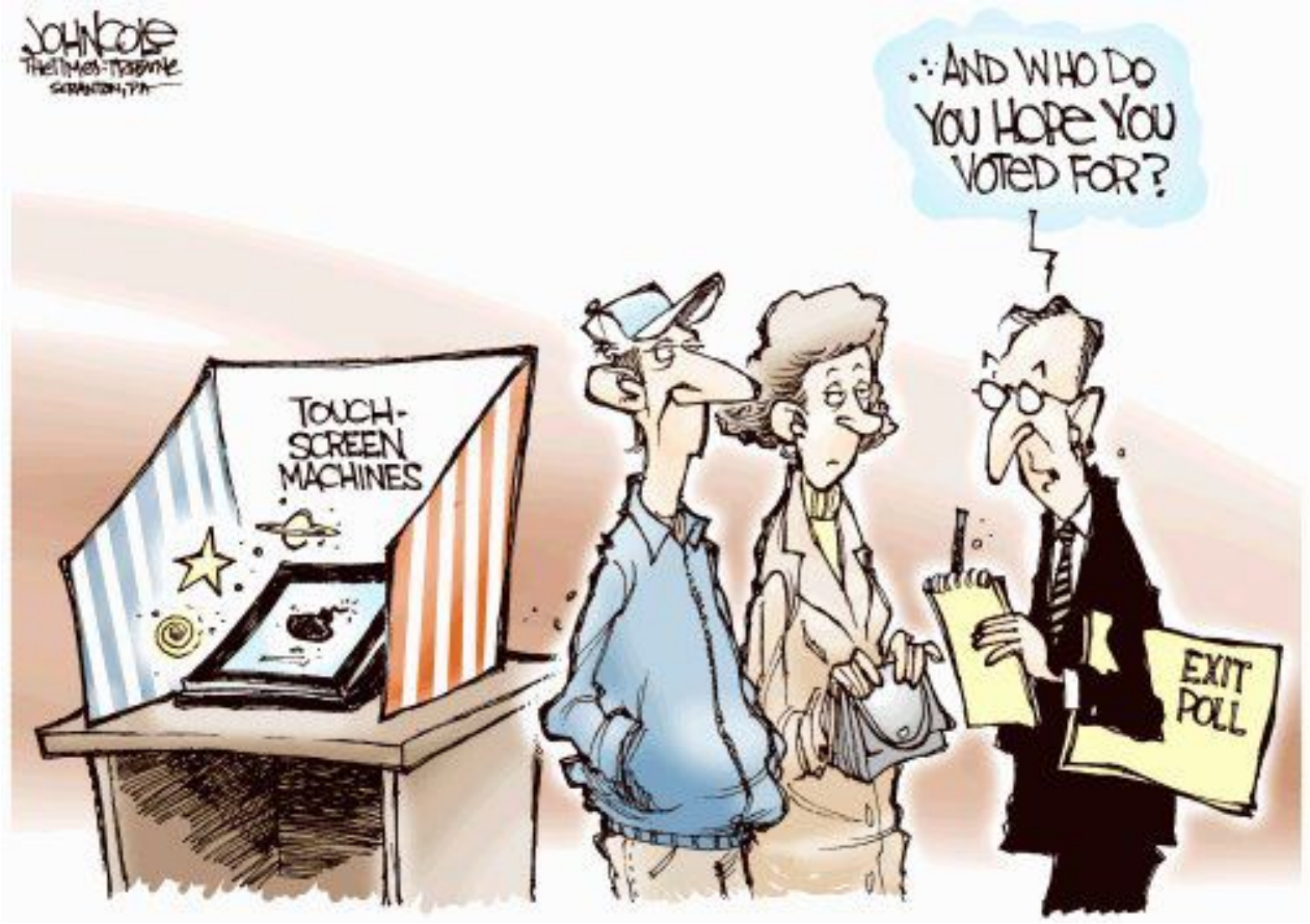
Security Requirements

Security Requirements

- Only eligible voters may vote, and each eligible voter votes at most once.
- Each cast vote is **secret**, even if voter wishes otherwise!
  -- No vote-selling!
  -- No receipt showing how you voted!
- Final outcome is **verifiably correct**.
- No ``trusted parties'' – **all are suspect**!
  Vendors, voters, election officials, candidates, spouses, other nation-states, …

Software Independence

(Rivest & Wack, 2006)



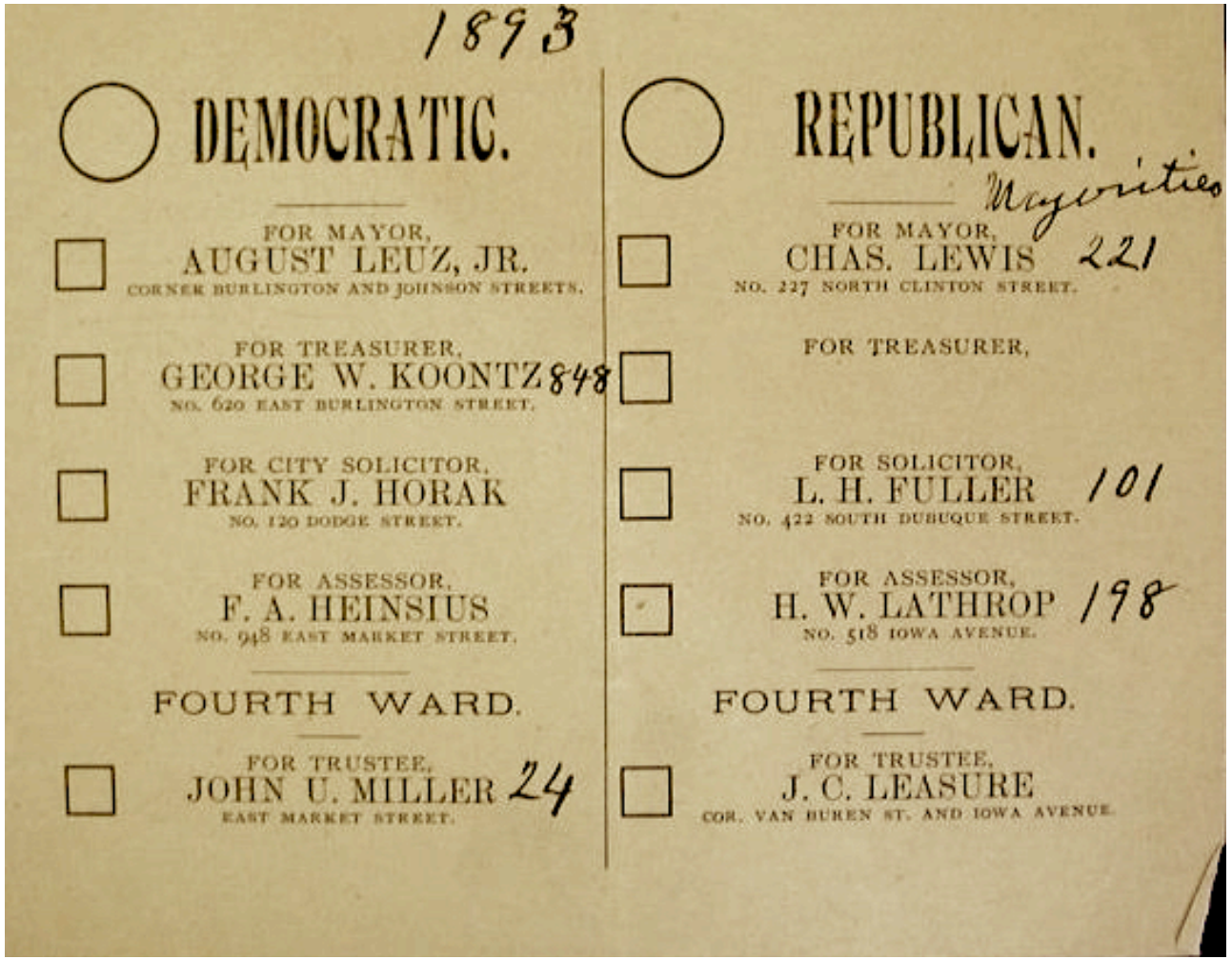
And Who Do You Hope You Voted For?

Software Independence

- Software is *not* to be trusted!
- A voting system is *software independent* if **an undetected error in the software can not cause an undetectable change in the election outcome**.
- *Strongly software-independent* if it is possible to correct any such outcome error
- Example: Paper ballots (with hand recount)

Paper Ballots

1893 – “Australian” Paper Ballot



1893

DEMOCRATIC.

FOR MAYOR,
AUGUST LEUZ, JR.
CORNER BURLINGTON AND JOHNSON STREETS.

FOR TREASURER,
GEORGE W. KOONTZ 848
NO. 620 EAST BURLINGTON STREET.

FOR CITY SOLICITOR,
FRANK J. HORAK
NO. 120 DODGE STREET.

FOR ASSESSOR,
F. A. HEINSIUS
NO. 948 EAST MARKET STREET.

FOURTH WARD.

FOR TRUSTEE,
JOHN U. MILLER 24
EAST MARKET STREET.

REPUBLICAN.

Majorities

FOR MAYOR,
CHAS. LEWIS 221
NO. 227 NORTH CLINTON STREET.

FOR TREASURER,

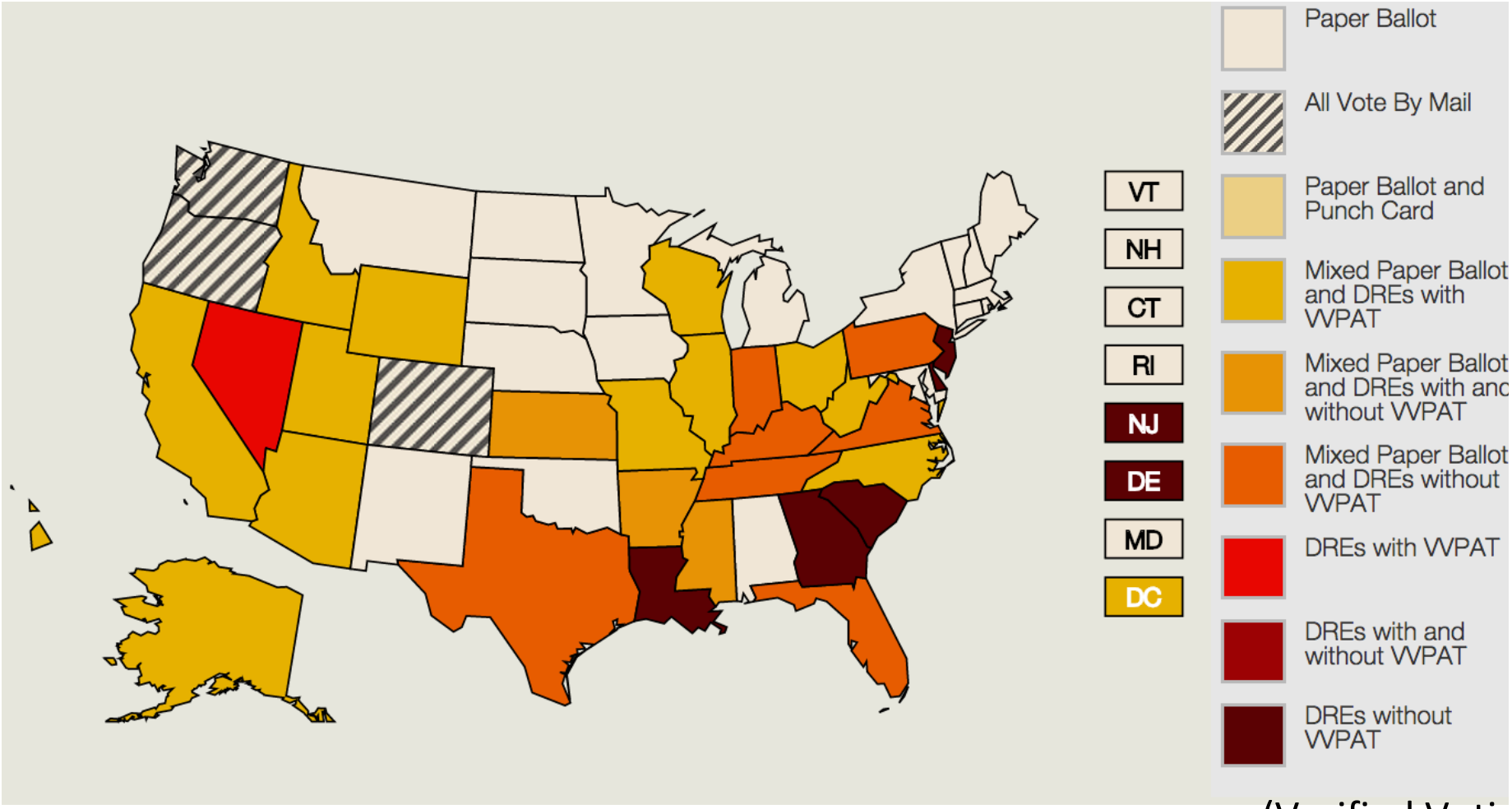
FOR SOLICITOR,
L. H. FULLER 101
NO. 422 SOUTH DUBUQUE STREET.

FOR ASSESSOR,
H. W. LATHROP 198
NO. 518 IOWA AVENUE.

FOURTH WARD.

FOR TRUSTEE,
J. C. LEASURE
COR. VAN BUREN ST. AND IOWA AVENUE.

What is used now?



(Verified Voting)

DRE = Direct Recording by Electronics

VVPAT = Voter Verified Paper Audit Trail

Election Process (paper ballots)

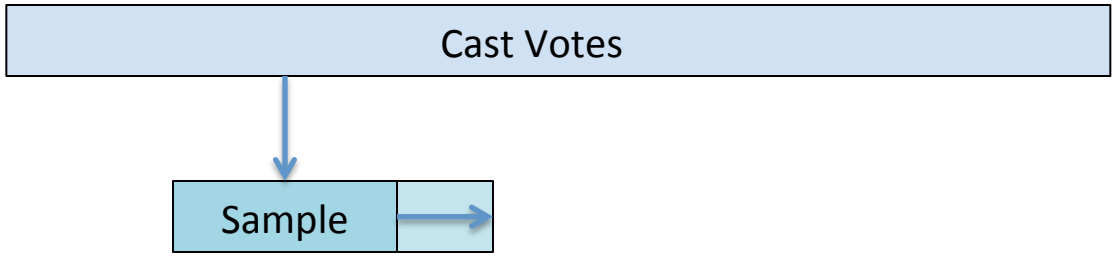
- Print ballots; setup
- Vote
- Initial count (by scanners);
  initial ("reported") outcome
- Statistical audit (by hand) of paper ballots to confirm/disprove reported outcome

Auditing of Paper Ballots

Two auditing paradigms

- *Ballot-polling audits*:
  All you have are the cast paper ballots.
  (Like ``exit poll'' of ballots…)
- *Comparison audits*:
  Uses both paper and electronic records
  ("cast vote records'' – CVRs)
  Paper ballot given an ID when scanned;
  CVR has same ID.
  Audit compares paper ballot to its CVR.

General audit structure



1. Draw an initial random sample of ballots.
2. Interpret them by hand.
3. Stop if reported outcome is now confirmed to desired confidence level.
4. If all ballots have now been examined, you have done a full recount, and are done. Otherwise increase sample size; return to 2.

Bravo audit [LSY12]

- Ballot-polling audit
- ***Risk-limiting audit****: provides guarantee that chance of accepting incorrect outcome is at most given risk limit (e.g. $\alpha = 0.05$).*
- Uses reported margin-of-victory as input (e.g. accumulate product of A/2 or B/2 where A, B are *reported* fractions of votes for Alice, Bob.
- Can needlessly do a full recount if reported margin-of-victory is wrong…

DiffSum audit [*R*15]

- No dependence on reported margin-of-victory.
- For two-candidate race, stops when

  $$(a - b)^2 > (a + b) \bullet log_{10}(n)$$

  where a, b = number of votes for Alice, Bob

  n = total number of votes cast
- Risk limit α determined *empirically;* forthcoming work gives way to make this approach work with rigorous bounds.

Other social choice functions

Social choice functions

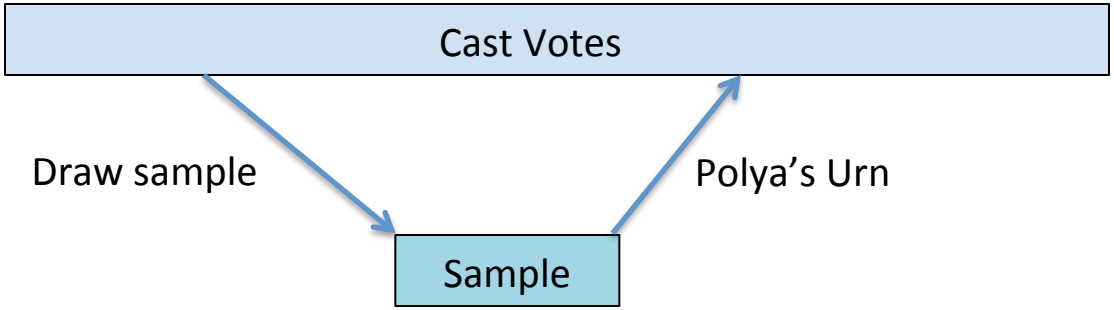
- Not all elections are *plurality*
- Some elections are *ranked-choice:*
  ballot gives voter's preferences:
  $$A > C > D > B$$
- A specified ``social choice function'' maps collections of ballots to outcomes.
- Example: IRV (Instant Runoff Voting) – Keep eliminating candidate with fewest first-choice votes until some candidate has a majority of first-choice votes. (San Francisco uses IRV.)

Black-box audits

- "Black-box audits" only need to
  - draw random samples
  - derive variant samples of a random sample
  - apply the social choice function in a "black-box" manner to some samples, to determine the winners of those samples.
- *Black-box audits thus apply to any voting system (any social choice function) !*
- Three examples: Bayesian, Bootstrap, and *T*-pile audits.

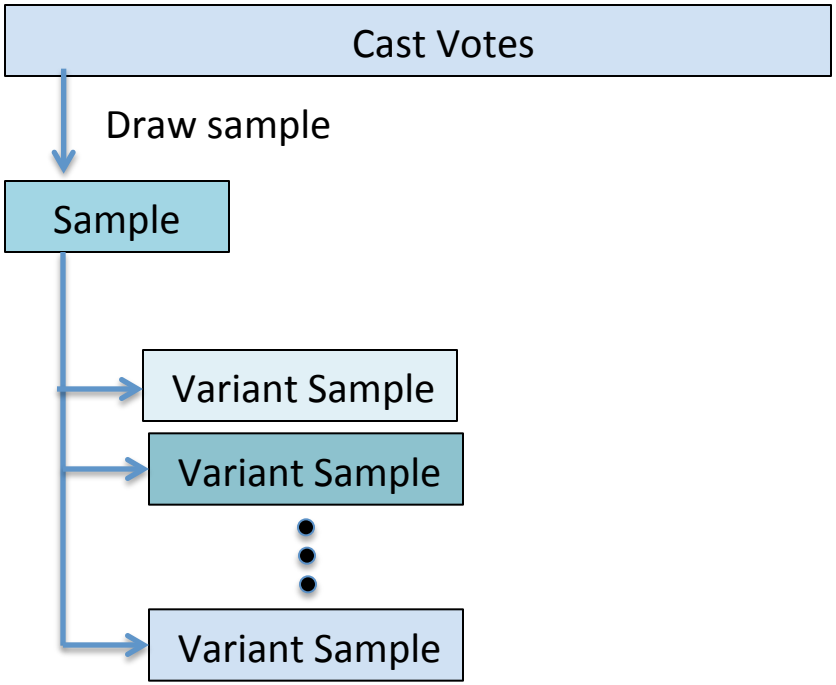
Bayesian audit [*RS*12]

- ``Inverse'' of sampling is Polya's Urn:



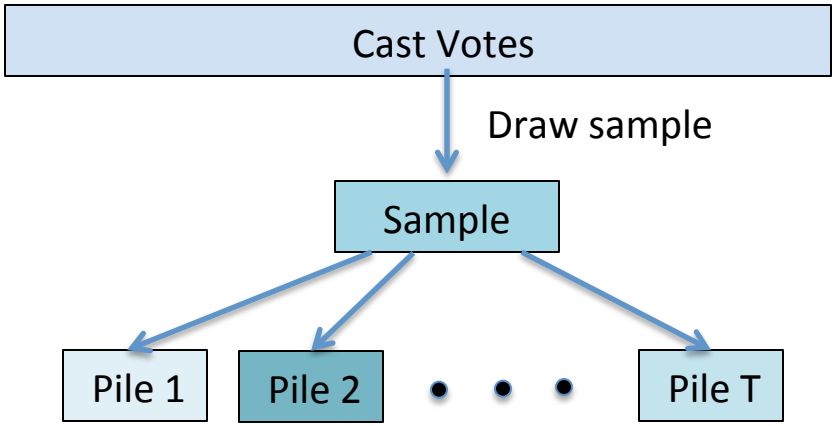
- Place sample in urn. Draw one ballot out at random, put two copies back. Rinse and repeat.
- This samples Bayesian posterior distribution for collection of cast votes.
- Can thus measure "Probability that reported outcome is correct" given sample. Stop if $> 1 - \alpha$.

Bootstrap audit [*RS*15]



- Create from given sample T (e.g. 100) "variant samples" (e.g. by subsampling with replacement)
- Stop audit if sample and all variants have same outcome as reported outcome.

T-pile audit



- "Deal" sample in round-robin manner into *T* (e.g. T=7) disjoint piles.
- Stop audit if sample and all piles have same outcome as reported outcome.
- Provably risk-limiting under reasonable assumption that most likely sample outcome is correct one.
- But not as efficient as general bootstrap audit…

Comparison Audits

- More efficient (1/margin-of-victory) since you are estimating error rate in CVRs (near 0) rather than vote shares of candidates (near ½)
- Typical audit may only need to audit a few dozens of ballots
- Bayesian audit can do comparison audits
- Other methods: SOBA [BJLLS11]

End-to-end Verifiable Voting

End-to-End Verifiable Voting

- Provides "end-to-end" integrity; votes are
  - "**cast as intended**" (*verified by voter)*
  - "**collected as cast**" (*verified by voter or proxy)*
  - "**counted as collected**" (*verified by anyone)*
- Paper ballots have only *first* property; once ballot is cast, integrity depends on "chain of custody" of ballots.
- End-to-end systems provide software independence, verifiable chain of custody, and verifiable tally.

Public Bulletin Board (PBB)

Public Bulletin Board:

<Election>

System PK parameters

Voter/Vote pairs:

"Abe_Smith", $E(vote_{Abe\_Smith})$

"Ben_Jones", $E(vote_{Ben\_Jones})$

…

Reported winner

Proof of correctness

</Election>

- E2E systems have "*public bulletin board*" posting election information (including encryptions of ballots).
- PBB posts "evidence" that reported winner is correct.

Ballots are encrypted

- Voter given copy of her encrypted ballot as "receipt"
- How can she verify that encryption was done correctly?
  Was vote "verifiably cast as intended?"
  - Answer: voter can arbitrarily decide either to cast encrypted vote, or to audit encryption by asking for decryption parameters. (Benaloh)

Voter can confirm chain of custody

- Voter names and receipts posted on PBB
- Voter checks “collected as cast” by verifying that her name/receipt is posted on PBB
- If it is missing, she can credibly complain if her receipt is ``authentic'' (e.g. hard to forge).
- Enough credible complaints ➔ Re-run election!

Anyone can verify tally

- System publishes final tally (reported outcome) and NIZK proof that reported outcome is correct.
- Decrypting individual ballots not necessary with *homomorphic tallying*:

  $$E(v1)\,E(v2) = E(v1+v2)$$

  Product of ciphertexts is ciphertext for sum. Only product of all votes needs to be decrypted.
- Another common approach based on *mixnets.*

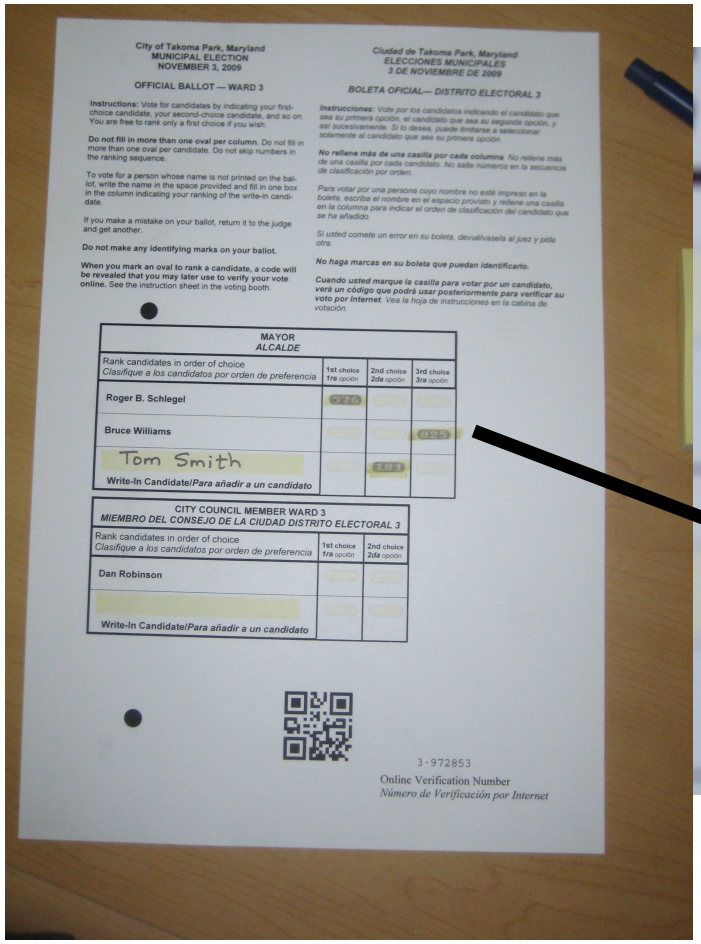
E2E deployments in real elections

- Scantegrity
  (Chaum; Takoma Park, MD; 2009 & 2011)
- Wombat
  (Rosen; 3 elections in Israel; 2011 & 2012)
- Prêt à Voter
  (Ryan; New South Wales, Australia; 2014)
- StarVote (Austin, Texas)
  (DeBeauvoir; in progress…)

Hybrid paper + electronic

- Some systems (like Scantegrity, Wombat, and StarVote) have *both* a paper ballot AND an electronic E2E subsystem.
- Can audit paper ballots as usual.
- Can audit electronic records on PBB as usual for E2E system. (That is, voter can verify her vote is there, and anyone can verify tally.)

Scantegrity confirmation codes


City of Takoma Park, Maryland
MUNICIPAL ELECTION
NOVEMBER 3, 2009

OFFICIAL BALLOT — WARD 3

Instructions: Vote for candidates by indicating your first-choice candidate, your second-choice candidate, and so on. You are free to rank only a first choice if you wish.

Do not fill in more than one oval per column. Do not fill in more than one oval per candidate. Do not skip numbers in the ranking sequence.

To vote for a person whose name is not printed on the ballot, write the name in the space provided and fill in one box in the column indicating your ranking of the write-in candidate.

If you make a mistake on your ballot, return it to the judge and get another.

Do not make any identifying marks on your ballot.

When you mark an oval to rank a candidate, a code will be revealed that you may later use to verify your vote online. See the instruction sheet in the voting booth.

Ciudad de Takoma Park, Maryland
ELECCIONES MUNICIPALES
3 DE NOVIEMBRE DE 2009

BOLETA OFICIAL— DISTRITO ELECTORAL 3

Instrucciones: Vote por los candidatos indicando el candidato que sea su primera opción, el candidato que sea su segunda opción, y así sucesivamente. Si lo desea, puede limitarse a seleccionar solamente al candidato que sea su primera opción.

No rellene más de una casilla por cada columna. No rellene más de una casilla por cada candidato. No salte números en la secuencia de clasificación por orden.

Para votar por una persona cuyo nombre no esté impreso en la boleta, escriba el nombre en el espacio provisto y rellene una casilla en la columna para indicar el orden de clasificación del candidato que se ha añadido.

Si usted comete un error en su boleta, devuélvasela al juez y pida otra.

No haga marcas en su boleta que puedan identificarlo.

Cuando usted marque la casilla para votar por un candidato, verá un código que podrá usar posteriormente para verificar su voto por Internet. Vea la hoja de instrucciones en la cabina de votación.

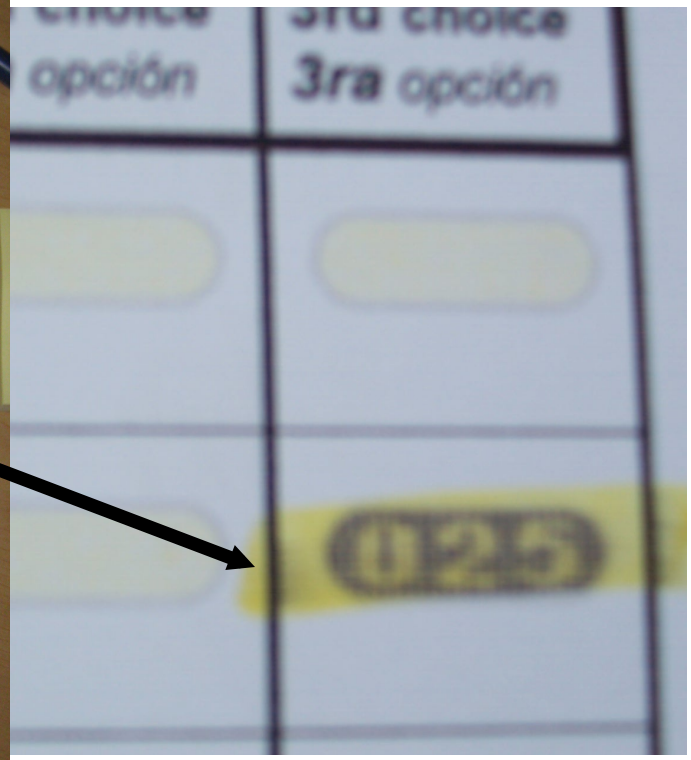
MAYOR
ALCALDE

Rank candidates in order of choice *Clasifique a los candidatos por orden de preferencia*	1st choice *1ra opción*	2nd choice *2da opción*	3rd choice *3ra opción*
Roger B. Schlegel	276		
Bruce Williams			025
Tom Smith		181	
Write-In Candidate/*Para añadir a un candidato*			

CITY COUNCIL MEMBER WARD 3
MIEMBRO DEL CONSEJO DE LA CIUDAD DISTRITO ELECTORAL 3

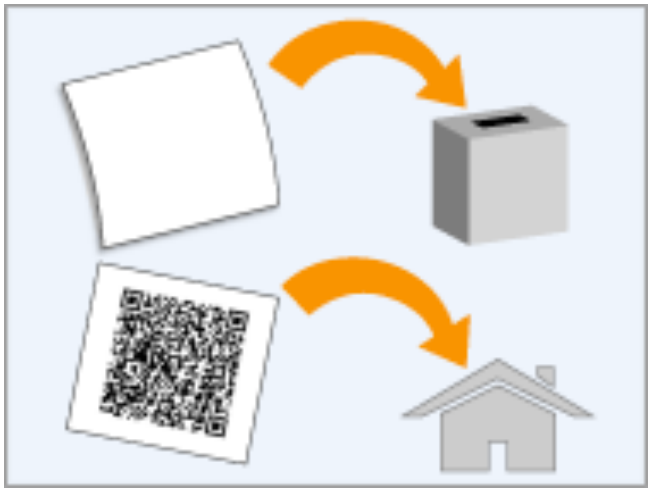
Rank candidates in order of choice *Clasifique a los candidatos por orden de preferencia*	1st choice *1ra opción*	2nd choice *2da opción*
Dan Robinson		
Write-In Candidate/*Para añadir a un candidato*		

3-972853
Online Verification Number
Número de Verificación por Internet



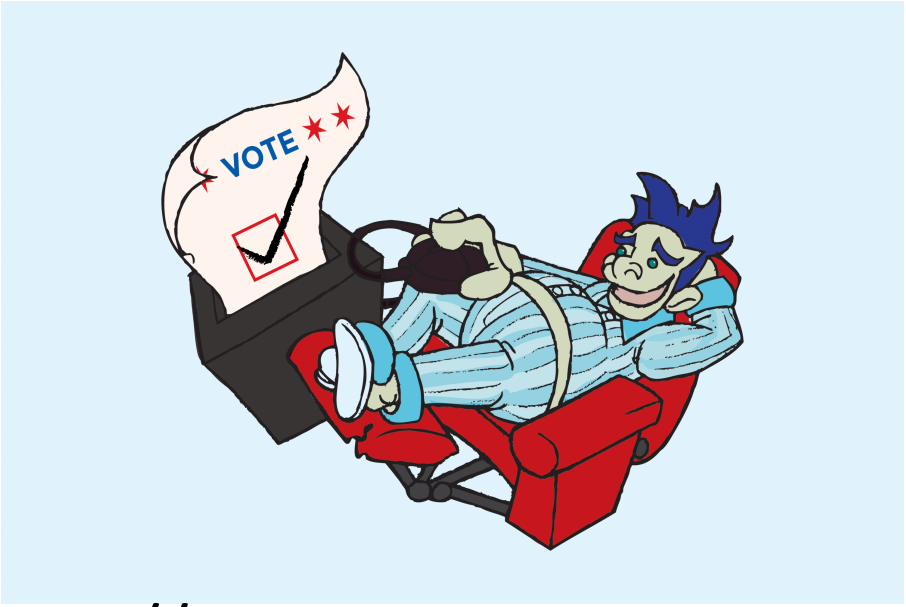
Invisible codes solves “receipt authenticity” problem: voter only gets codes for candidates she voted for.

Wombat voting

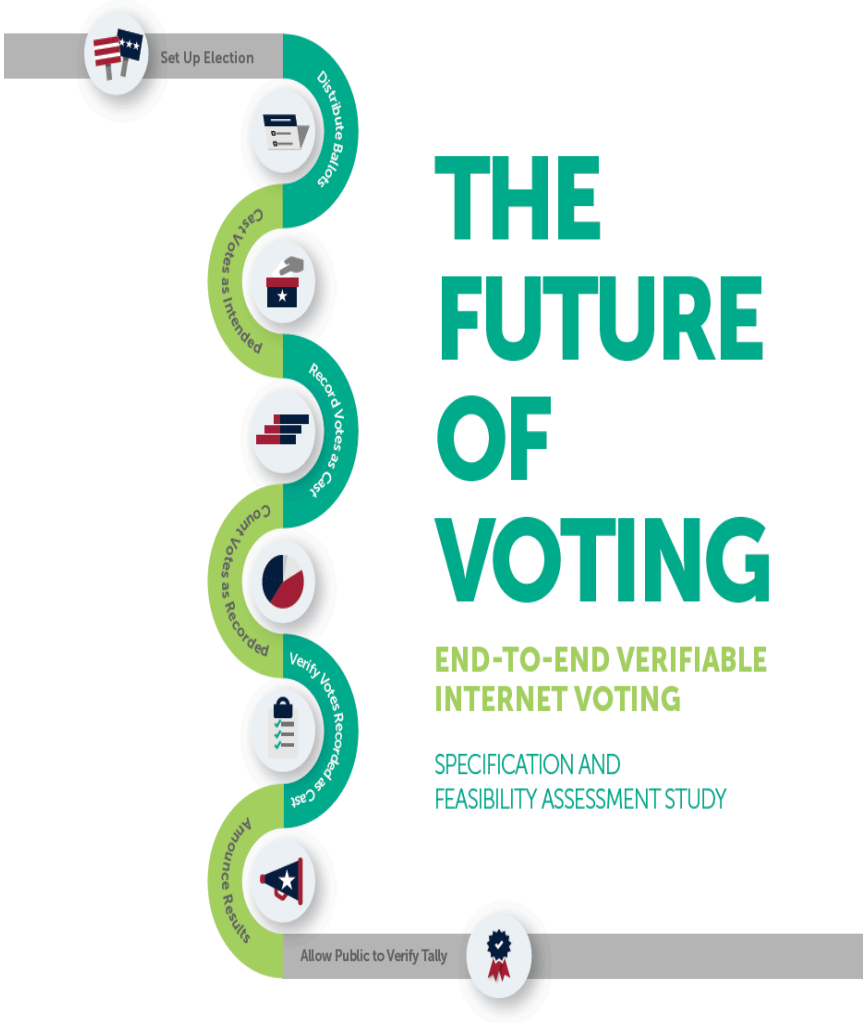


- Printed ballot has plaintext choice and QR code equivalent.
- Voter casts paper ballot into ballot box and has QR code scanned for PBB.
- Takes QR code receipt home to look up on PBB.

When can I vote on the Internet? (or on my phone?)



http://voteinyourpajamas.org/



- U.S. Vote Foundation 2015 Report on Internet Voting:
  - E2E *necessary* for IV
  - But: E2E should first be well-established and understood for in-person voting, and
  - E2E *not sufficient* for IV: many problems remain:
    - Malware
    - DDOS attacks
    - Authentication
    - MITM attacks
    - Zero-day attacks on servers
    - Coercion & vote-selling
    - …

Helios Voting (Adida)

- Prototype E2E internet voting system
  https://vote.heliosvoting.org/
- Uses homomorphic tallying
- Used by some professional societies…
- No protection against malware, DDOS, coercion, etc…
- *Not* suitable for real political elections!

Challenges / Open Problems

- Proofs of risk-limiting character for Bootstrap audits
- Develop theory for precinct-level audits
- Better E2E dispute resolution
- Good multi-channel remote voting methods (mail + phone?)
- Better ways to explain audits to non-technical folks (statistics; crypto; assumptions…)

Conclusions

- Election integrity remains a hard problem and a good research area.
- Internet voting is (or should be) a long ways off (20 years?)
- End-to-end verifiable voting methods (especially hybrid methods with paper ballots) are the way to go.

The End

Thanks for your attention!