Audit Thoughts

Ronald L. Rivest

MIT CSAIL

Audit Working Meeting

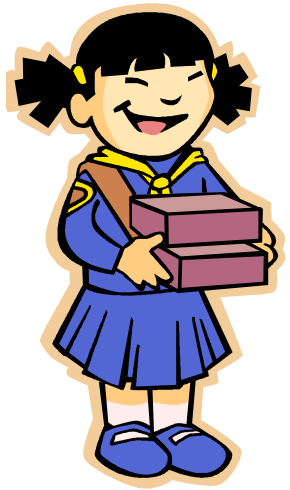
ASA, Alexandria, VA

October 24, 2009

CSAIL

Viewpoint on high-tech

- *We should think of a computer (or other forms of "high tech") as a very fast and well-trained four-year old child.*
- The child may be very helpful (she is fast, and well-trained!) but may not always do the right thing (she's only four!).
- For something as important as an election, a ``grown-up'' should always check her work.



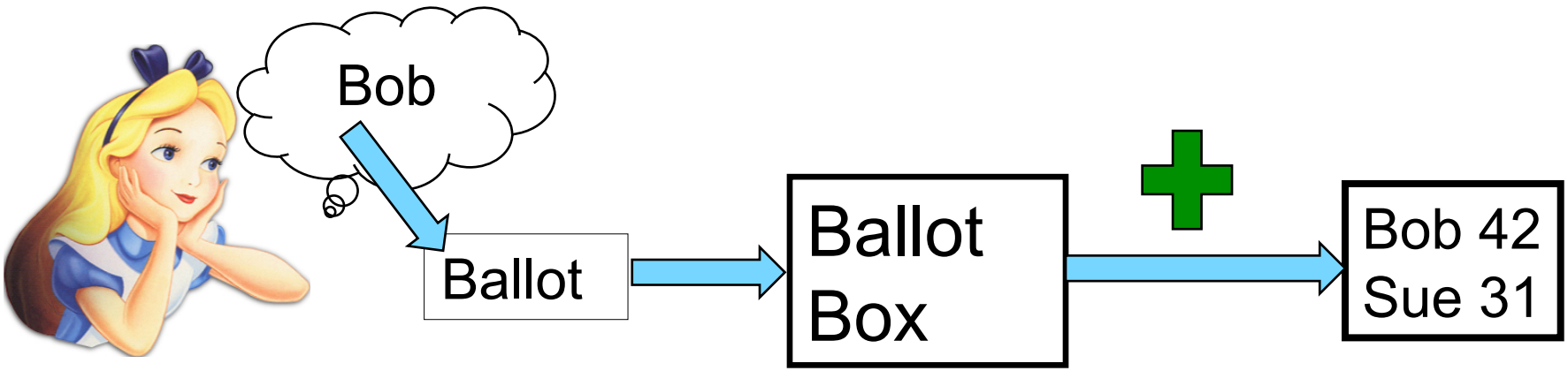
Audit Method Types

- Post-Election Manual Tally (PEMT)
  - Audit tallying by ``batches''
- Single-ballot methods (e.g. CHF'07)
  - Convert all ballots to electronic form first
  - Audit the conversion; then tally is easy (even IRV)
- End-to-End Voting Systems
  - Scantegrity II, Pret A Voter, …
  - Takoma Park election (Nov 2009)

Assume ``chain of custody'' is OK ??

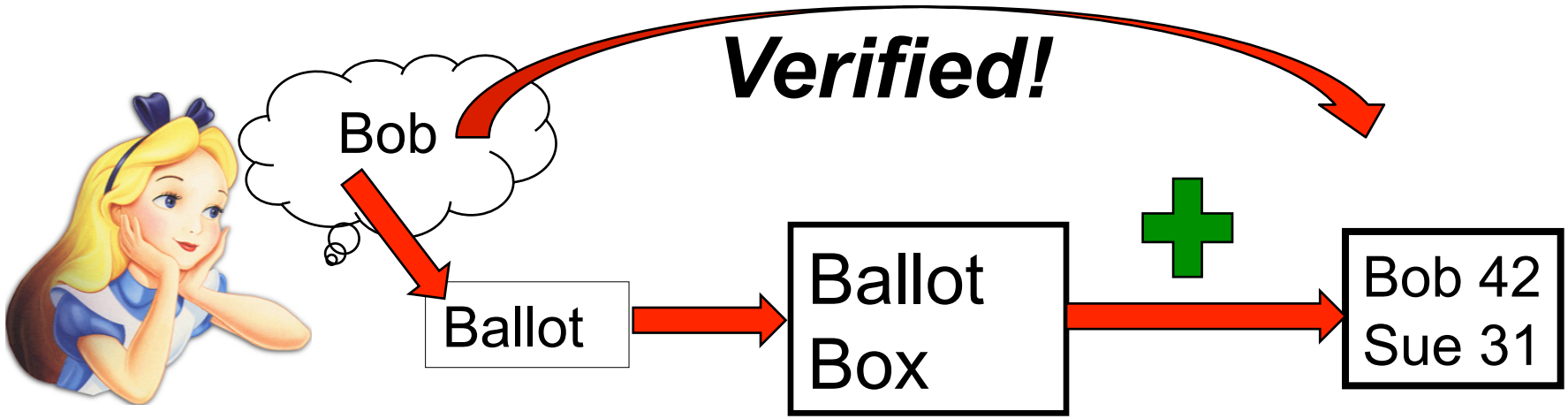
Voting Steps

- *recorded as intended*
- *cast (and collected) as recorded*
- *counted as cast*



End-to-End Voting Steps

- verifiably *recorded as intended* (by voter)
- verifiably *cast (and collected) as recorded* (“)
- verifiably *counted as cast* (by anyone)



PEMT considerations

- PEMT is also about tradeoffs between
  - Cost
  - Level of assurance provided
  - Simplicity / Understandability
- If you're already spending $6 / voter, spending another $0.10 on integrity/audit is ``low order'' (e.g. auditing 20% at $0.50/ballot)

PEMT considerations

- Precincts have variable sizes!
- A small amount of ``interpretation error'' is expected (e.g. people see voter intent differently than a scanner does)
- Late batches vs. fast start
- Staged audits vs. tight timescale
- Multiple, overlapping, contests

Detection vs. Correction

- Much initial work (e.g. APR) strove for high-probability *detection* of error sufficient to have changed outcome.
- Models tended to ignore interpretation error.
- APR and similar works also treated ``what to do'' (correction) lightly. E.g. assuming that full recount would be done if error was detected (which would then make them two-stage risk-limiting audits). See Stark for more discussion of turning detection → correction.

Margin-based audits

- Let M = reported margin of victory
- Want smaller audit when M is large
- Assume n batches
- Let u_i be upper bound on error in i-th batch
  U = sum_i u_i is their total
- Let e_i be actual error in i-th batch towards changing outcome (determinable by audit)
- Want to know if sum_i e_i >= M
- Many approaches (Saltman; SAFE; …)

PPEBWR [APR'07]

- Probability proportional to error bound, with replacement
- Pick batch i with probability proportional to u_i / U; do this t times (with replacement).
- Chance that precincts with error of total magnitude M is never picked is
  $<= (1 – M/U)^t$
- To get this chance < alpha (e.g. alpha = 0.05):
  $t > \ln(\text{alpha}) / \ln(1 – M/U)$

NEGEXP [APR'07]

- Batch i is picked *independently* with probability

$$p\_i = 1 - \text{alpha} \wedge (u_i / M)$$

- When total error is at least M , the chance of not detecting any errors in sampled batches is less than alpha .

PPEBWR and NEGEXP

- Require that you know margins to get started
- Both require more sophisticated sampling than simple random (uniform) sampling.
- Are not risk-limiting unless you do full recount when error detected (or embed them otherwise in an appropriate escalation procedure).

Escalation of Sample Size

- PPEBWR fairly straightforward: you are effectively just increasing t and continuing the drawing process.
- For NEGEXP: Easier to think of this as decreasing alpha ; so p_i's are increasing. (Imagine having a random x_i for batch i ; where x_i is in [0,1]. Batch i is audited iff

  $$x_i <= p_i$$

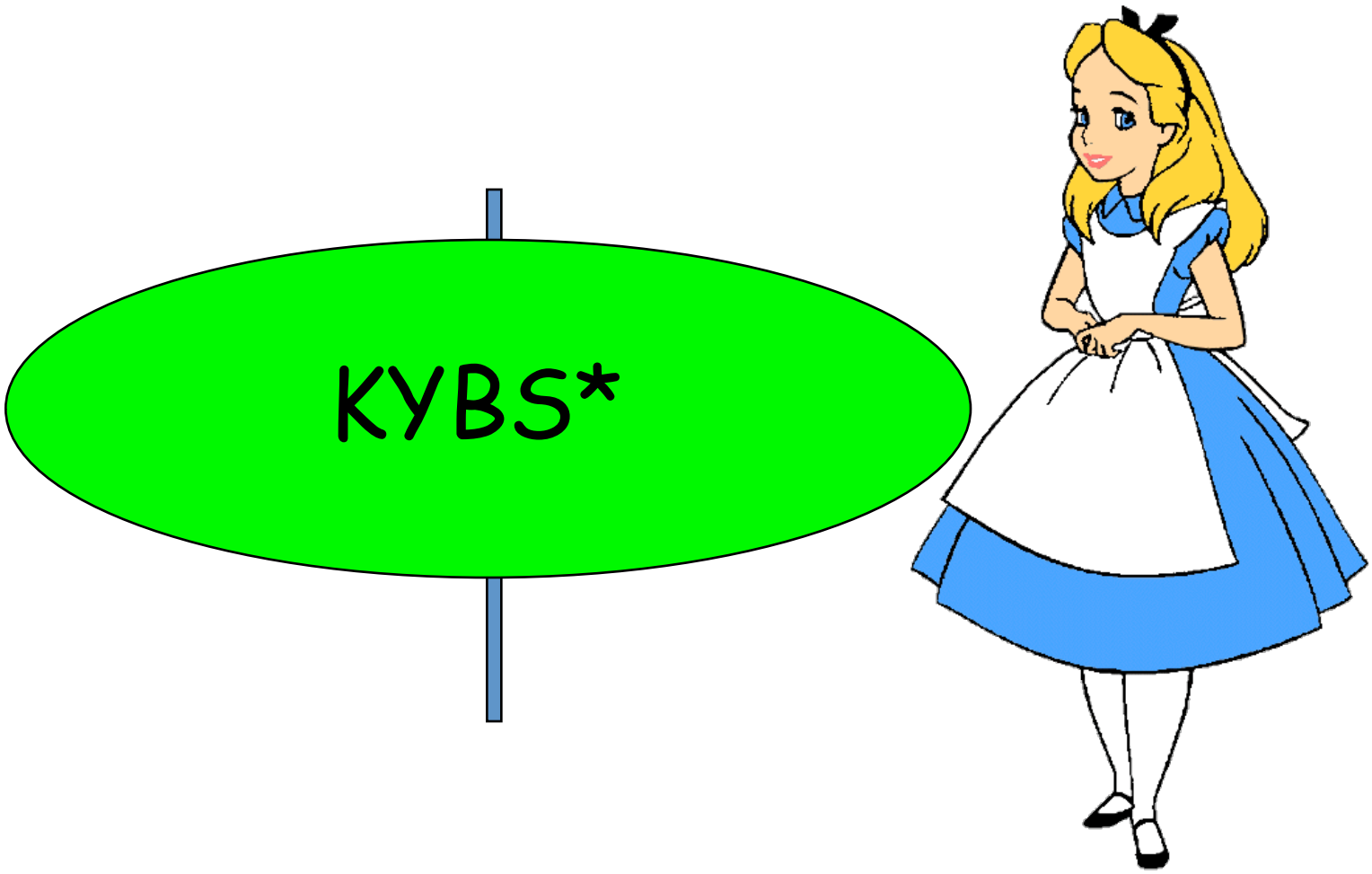
  Increasing p_i's will cause more to be audited, in a nice telescoping way.)

Combining multiple races

- Assume that there are ``economies'' – hard part is fetching ballots, easy to audit multiple races once you have ballots… (Is this true??)
- With NEGEXP, each race gives probability of audit for a batch: p'_i , p''_i , p'''_i, ...
- We can then audit batch with probability

  p_i = max(p'_i, p''_i, p'''_i, …)

  and satisfy auditing conditions for all races simultaneously…



* Keep Your Batches Small!

The End