VAULT:

Verifiable Audits Using Limited Transparency

Josh Benaloh, Microsoft Research

Philip B. Stark, University of California, Berkeley

Vanessa Teague, University of Melbourne

Risk-Limiting Audits

- RLAs should be used in every contest of every election.
- This can be a heavy burden at scale.
- The most efficient RLAs are ballot-comparison audits.

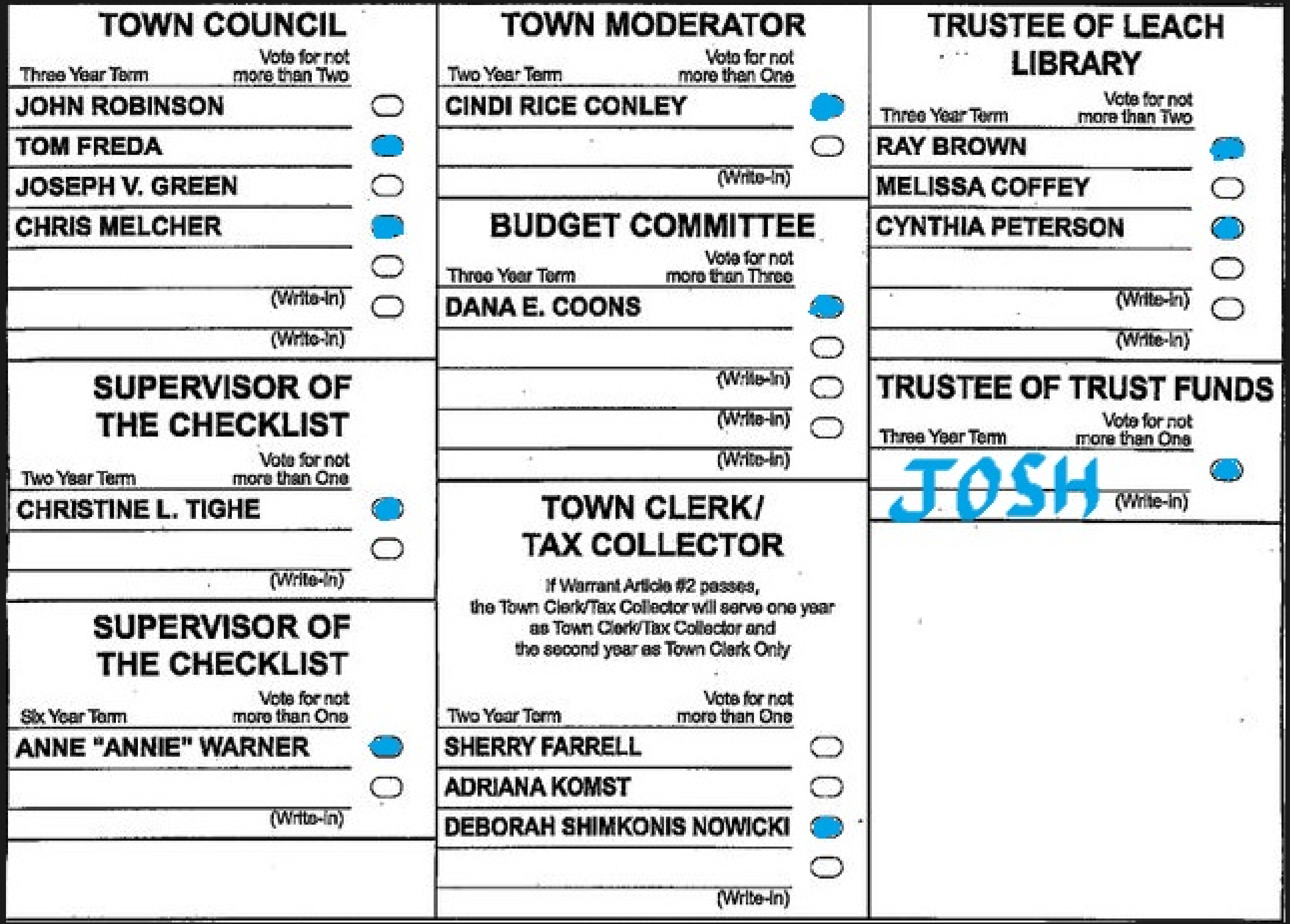
The Cast Vote Record Dilemma …

To publish – or not to publish

- If the CVRs are published, voter privacy is compromised (especially where complex ballots are used).
- If the CVRs are not published, why should the public believe the audit?

Published Cast Vote Records

Coercion with write-ins



TOWN COUNCIL

Three Year Term — Vote for not more than Two

JOHN ROBINSON ○
TOM FREDA ●
JOSEPH V. GREEN ○
CHRIS MELCHER ●
(Write-In) ○
(Write-In) ○

SUPERVISOR OF THE CHECKLIST

Two Year Term — Vote for not more than One

CHRISTINE L. TIGHE ●
(Write-In) ○

SUPERVISOR OF THE CHECKLIST

Six Year Term — Vote for not more than One

ANNE "ANNIE" WARNER ●
(Write-In) ○

TOWN MODERATOR

Two Year Term — Vote for not more than One

CINDI RICE CONLEY ●
(Write-In) ○

BUDGET COMMITTEE

Three Year Term — Vote for not more than Three

DANA E. COONS ●
(Write-In) ○
(Write-In) ○
(Write-In) ○

TOWN CLERK/ TAX COLLECTOR

If Warrant Article #2 passes, the Town Clerk/Tax Collector will serve one year as Town Clerk/Tax Collector and the second year as Town Clerk Only

Two Year Term — Vote for not more than One

SHERRY FARRELL ○
ADRIANA KOMST ○
DEBORAH SHIMKONIS NOWICKI ●
(Write-In) ○

TRUSTEE OF LEACH LIBRARY

Three Year Term — Vote for not more than Two

RAY BROWN ●
MELISSA COFFEY ○
CYNTHIA PETERSON ●
(Write-In) ○
(Write-In) ○

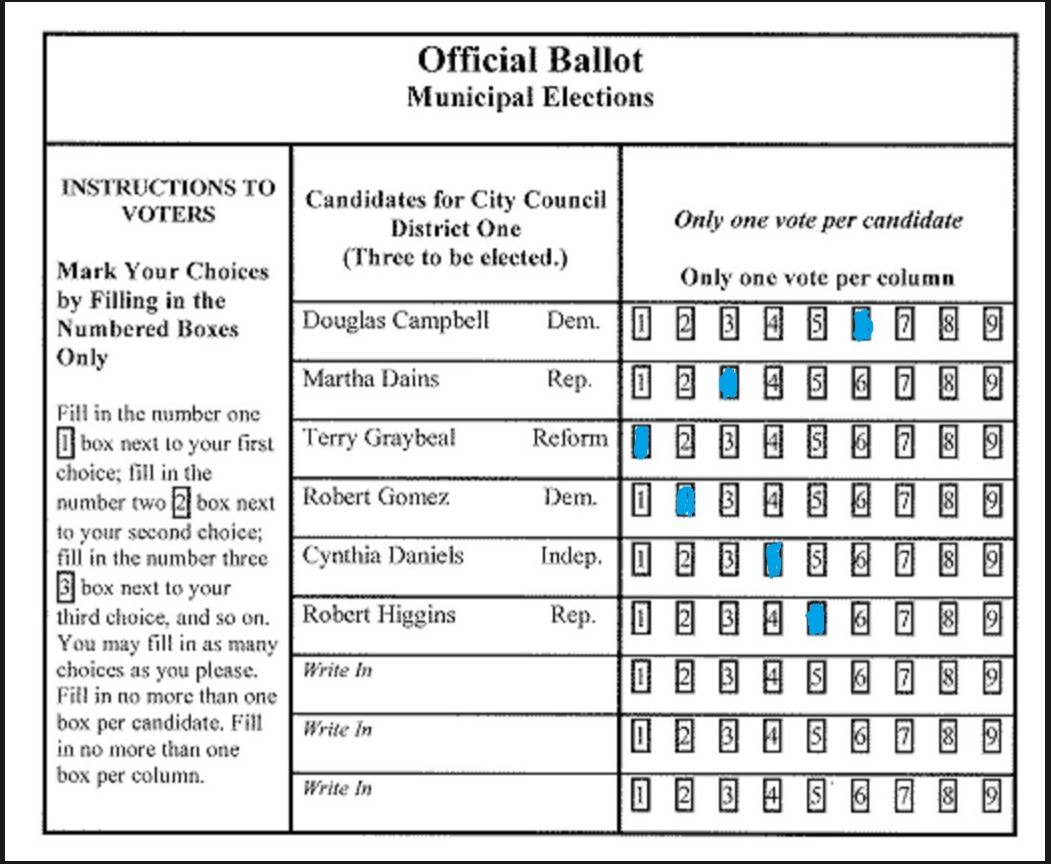
TRUSTEE OF TRUST FUNDS

Three Year Term — Vote for not more than One

JOSH (Write-In) ●

Published Cast Vote Records

Coercion with IRV



Official Ballot
Municipal Elections

INSTRUCTIONS TO VOTERS

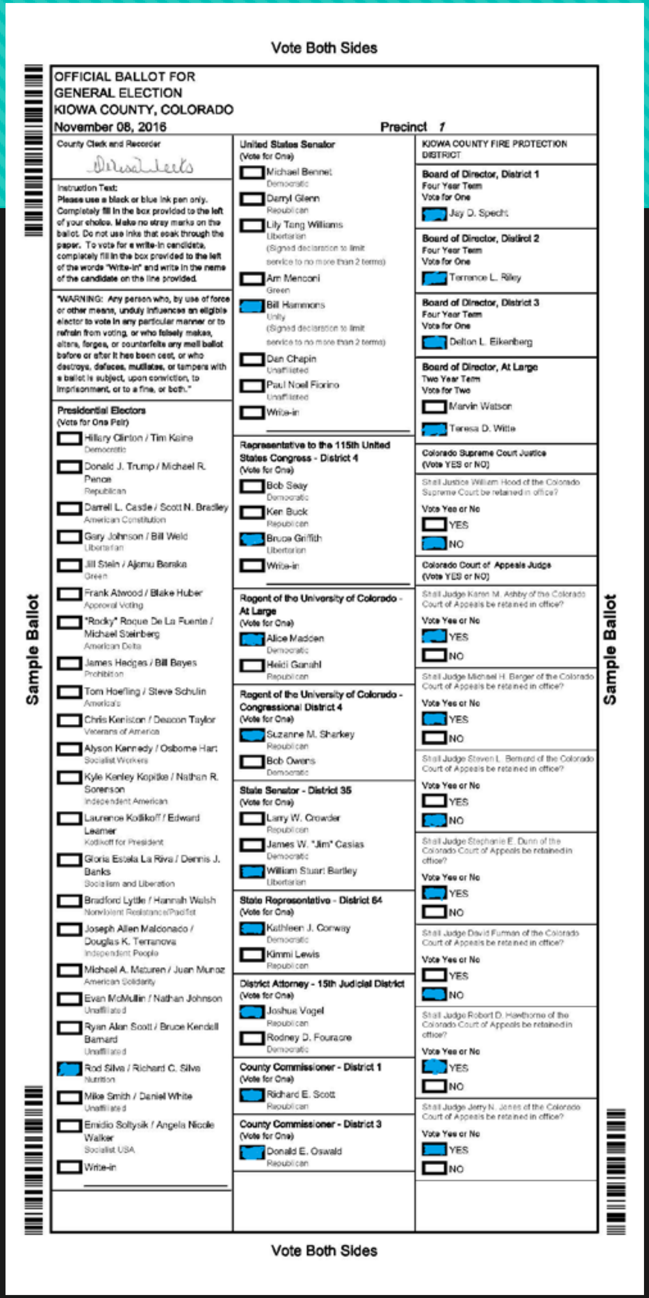
Mark Your Choices by Filling in the Numbered Boxes Only

Fill in the number one 1 box next to your first choice; fill in the number two 2 box next to your second choice; fill in the number three 3 box next to your third choice, and so on. You may fill in as many choices as you please. Fill in no more than one box per candidate. Fill in no more than one box per column.

Candidates for City Council District One (Three to be elected.)		*Only one vote per candidate* Only one vote per column								
Douglas Campbell	Dem.	1	2	3	4	5	■	7	8	9
Martha Dains	Rep.	1	2	■	4	5	6	7	8	9
Terry Graybeal	Reform	■	2	3	4	5	6	7	8	9
Robert Gomez	Dem.	1	■	3	4	5	6	7	8	9
Cynthia Daniels	Indep.	1	2	3	■	5	6	7	8	9
Robert Higgins	Rep.	1	2	3	4	■	6	7	8	9
Write In		1	2	3	4	5	6	7	8	9
Write In		1	2	3	4	5	6	7	8	9
Write In		1	2	3	4	5	6	7	8	9

Published CVRs

Coercion with neither



Vote Both Sides

Sample Ballot

OFFICIAL BALLOT FOR
GENERAL ELECTION
KIOWA COUNTY, COLORADO
November 08, 2016

Precinct 1

County Clerk and Recorder

Delisa Weeks

Instruction Text:
Please use a black or blue ink pen only. Completely fill in the box provided to the left of your choice. Make no stray marks on the ballot. Do not use inks that soak through the paper. To vote for a write-in candidate, completely fill in the box provided to the left of the words "Write-in" and write in the name of the candidate on the line provided.

"WARNING: Any person who, by use of force or other means, unduly influences an eligible elector to vote in any particular manner or to refrain from voting, or who falsely makes, alters, forges, or counterfeits any mail ballot before or after it has been cast, or who destroys, defaces, mutilates, or tampers with a ballot is subject, upon conviction, to imprisonment, or to a fine, or both."

Presidential Electors
(Vote for One Pair)

- □ Hillary Clinton / Tim Kaine
  Democratic
- □ Donald J. Trump / Michael R. Pence
  Republican
- □ Darrell L. Castle / Scott N. Bradley
  American Constitution
- □ Gary Johnson / Bill Weld
  Libertarian
- □ Jill Stein / Ajamu Baraka
  Green
- □ Frank Atwood / Blake Huber
  Approval Voting
- □ "Rocky" Roque De La Fuente / Michael Steinberg
  American Delta
- □ James Hedges / Bill Bayes
  Prohibition
- □ Tom Hoefling / Steve Schulin
  America's
- □ Chris Keniston / Deacon Taylor
  Veterans of America
- □ Alyson Kennedy / Osborne Hart
  Socialist Workers
- □ Kyle Kenley Kopitke / Nathan R. Sorenson
  Independent American
- □ Laurence Kotlikoff / Edward Leamer
  Kotlikoff for President
- □ Gloria Estela La Riva / Dennis J. Banks
  Socialism and Liberation
- □ Bradford Lyttle / Hannah Walsh
  Nonviolent Resistance/Pacifist
- □ Joseph Allen Maldonado / Douglas K. Terranova
  Independent People
- □ Michael A. Maturen / Juan Munoz
  American Solidarity
- □ Evan McMullin / Nathan Johnson
  Unaffiliated
- □ Ryan Alan Scott / Bruce Kendall Barnard
  Unaffiliated
- ■ Rod Silva / Richard C. Silva
  Nutrition
- □ Mike Smith / Daniel White
  Unaffiliated
- □ Emidio Soltysik / Angela Nicole Walker
  Socialist USA
- □ Write-in

United States Senator
(Vote for One)

- □ Michael Bennet
  Democratic
- □ Darryl Glenn
  Republican
- □ Lily Tang Williams
  Libertarian
  (Signed declaration to limit service to no more than 2 terms)
- □ Arn Menconi
  Green
- ■ Bill Hammons
  Unity
  (Signed declaration to limit service to no more than 2 terms)
- □ Dan Chapin
  Unaffiliated
- □ Paul Noel Fiorino
  Unaffiliated
- □ Write-in

Representative to the 115th United States Congress - District 4
(Vote for One)

- □ Bob Seay
  Democratic
- □ Ken Buck
  Republican
- ■ Bruce Griffith
  Libertarian
- □ Write-in

Regent of the University of Colorado - At Large
(Vote for One)

- ■ Alice Madden
  Democratic
- □ Heidi Ganahl
  Republican

Regent of the University of Colorado - Congressional District 4
(Vote for One)

- ■ Suzanne M. Sharkey
  Republican
- □ Bob Owens
  Democratic

State Senator - District 35
(Vote for One)

- □ Larry W. Crowder
  Republican
- □ James W. "Jim" Casias
  Democratic
- ■ William Stuart Bartley
  Libertarian

State Representative - District 64
(Vote for One)

- ■ Kathleen J. Conway
  Democratic
- □ Kimmi Lewis
  Republican

District Attorney - 15th Judicial District
(Vote for One)

- ■ Joshua Vogel
  Republican
- □ Rodney D. Fouracre
  Democratic

County Commissioner - District 1
(Vote for One)

- ■ Richard E. Scott
  Republican

County Commissioner - District 3
(Vote for One)

- ■ Donald E. Oswald
  Republican

KIOWA COUNTY FIRE PROTECTION DISTRICT

Board of Director, District 1
Four Year Term
Vote for One

- ■ Jay D. Specht

Board of Director, District 2
Four Year Term
Vote for One

- ■ Terrance L. Riley

Board of Director, District 3
Four Year Term
Vote for One

- ■ Delton L. Eikenberg

Board of Director, At Large
Two Year Term
Vote for Two

- □ Marvin Watson
- ■ Teresa D. Witte

Colorado Supreme Court Justice
(Vote YES or NO)

Shall Justice William Hood of the Colorado Supreme Court be retained in office?

Vote Yes or No

- □ YES
- ■ NO

Colorado Court of Appeals Judge
(Vote YES or NO)

Shall Judge Karen M. Ashby of the Colorado Court of Appeals be retained in office?

Vote Yes or No

- ■ YES
- □ NO

Shall Judge Michael H. Berger of the Colorado Court of Appeals be retained in office?

Vote Yes or No

- ■ YES
- □ NO

Shall Judge Steven L. Bernard of the Colorado Court of Appeals be retained in office?

Vote Yes or No

- □ YES
- ■ NO

Shall Judge Stephanie E. Dunn of the Colorado Court of Appeals be retained in office?

Vote Yes or No

- ■ YES
- □ NO

Shall Judge David Furman of the Colorado Court of Appeals be retained in office?

Vote Yes or No

- □ YES
- ■ NO

Shall Judge Robert D. Hawthorne of the Colorado Court of Appeals be retained in office?

Vote Yes or No

- ■ YES
- □ NO

Shall Judge Jerry N. Jones of the Colorado Court of Appeals be retained in office?

Vote Yes or No

- ■ YES
- □ NO

Sample Ballot

Vote Both Sides

Unpublished Cast Vote Records

- Selected ballots are compared to undisclosed CVRs.
- Why should someone who can’t see the CVR believe that it matches the physical ballot?
- Perhaps we can publish commitments to CVRs and then disclose the selected CVRs.

Published Commitments to CVRs

- Using commitments, we can enable public matching without publishing all CVRs and without compromising voter privacy.

- But why should the public believe that the committed CVRs match the announced tallies?

SOBA

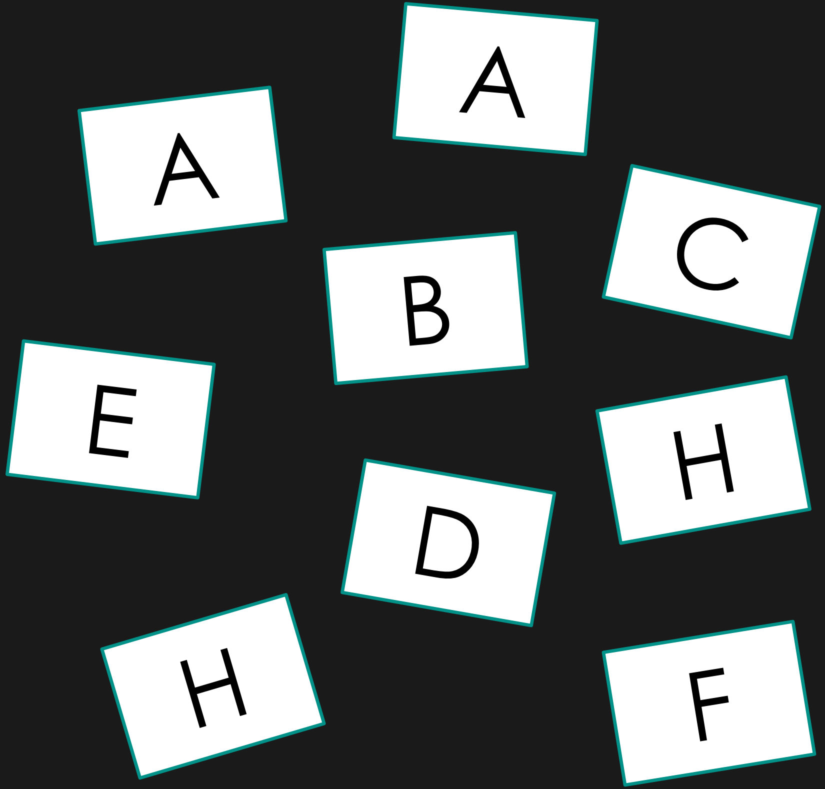
- Secrecy-Preserving Observable Ballot-Level Audits (2011) – Benaloh, Jones, Lazarus, Lindeman, and Stark.
- CVRs are split into individual contests.
- A web of interlocking commitments is formed.

SOBA

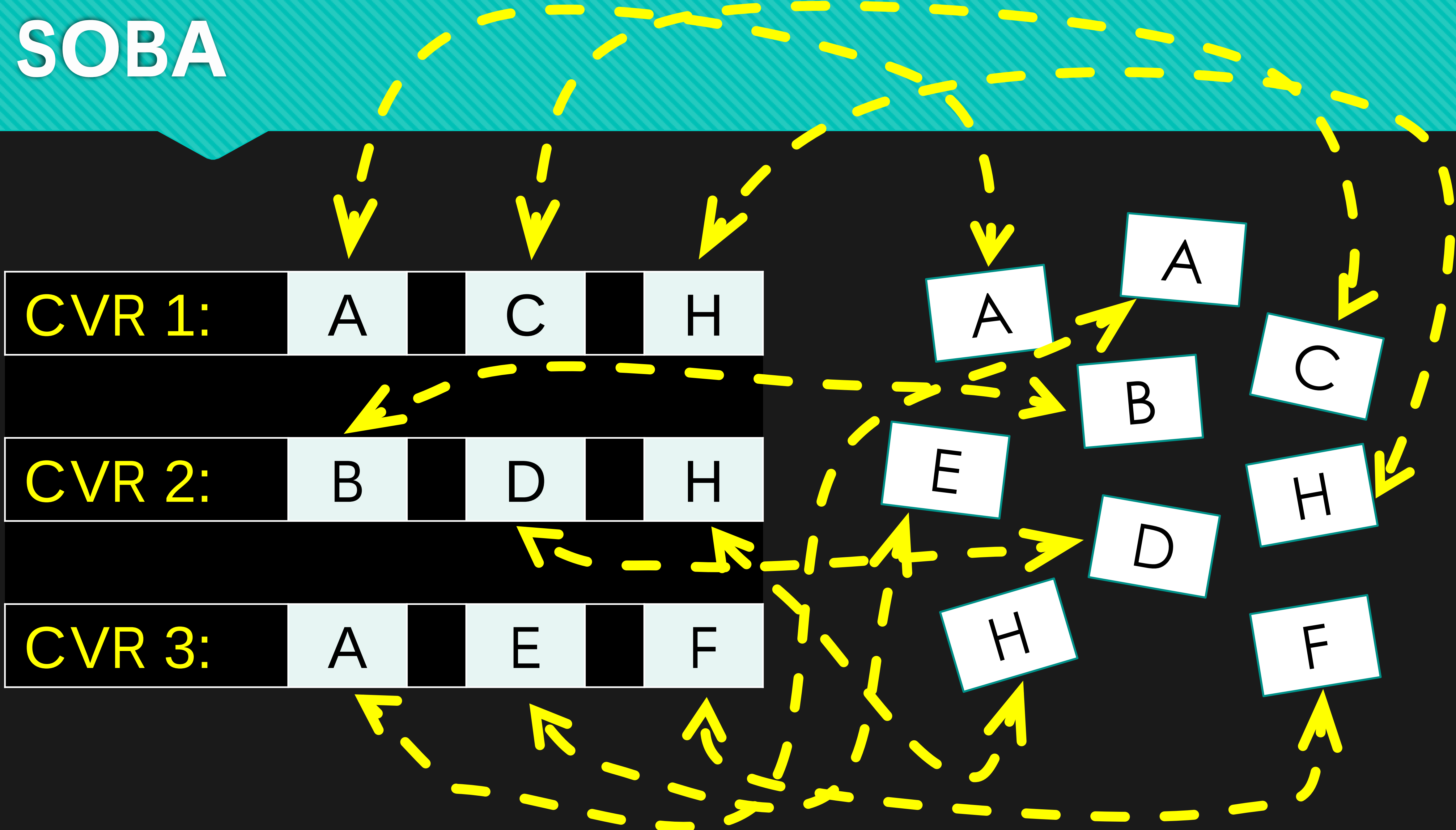
CVR 1:	A		C		H
CVR 2:	B		D		H
CVR 3:	A		E		F

SOBA

CVR 1:	A	C	H
CVR 2:	B	D	H
CVR 3:	A	E	F



SOBA



CVR 1:	A	C	H
CVR 2:	B	D	H
CVR 3:	A	E	F

The Gap

We need a clear, compelling, and well-understood method to

- Commit to CVRs,
- Allow them to be selectively opened, and
- Demonstrate that the committed CVRs match the announced tallies.

End-to-End (E2E) Verifiability

Techniques from E2E-verifiability allow CVRs to be

- encrypted (usually with a key shared by a set of election trustees),
- selectively decrypted (by a quorum of trustees), and
- tallied (without individually decrypting CVRs).

Privacy-Enhanced RLAs

What does a privacy-enhanced ballot-comparison audit look like in practice?

The steps match those of an ordinary ballot-comparison audit with two additions.

1. Encrypted CVRs are published and proven to match the announced tallies.
2. CVRs selected for auditing are decrypted.

How are Selected CVRs decrypted?

Many options are available.

- Assemble trustees to decrypt after the audit.
- Have trustees decrypt during audit.
- Enable a single administrator to decrypt CVRs during the audit.
- Use a hybrid system.

Hybrid System (Marc Rosen)

- Published CVRs are strongly encrypted with a joint public key shared by election trustees.
- Each ballot’s encryption nonce is itself encrypted with an administrative key and that encryption is printed directly onto the ballot.

IRV and Other Voting Rules

We can also handle IRV and related systems both for privacy-enhanced audits and for E2E-verifiability.

Assertions about the contents of each ballot are encrypted and collectively shown to match the election results.

Read the paper for details. ☺

Questions???