SAC "Summer" School

Can Crypto Enhance Democracy? Part I

Jeremy Clark, Concordia University

Agenda

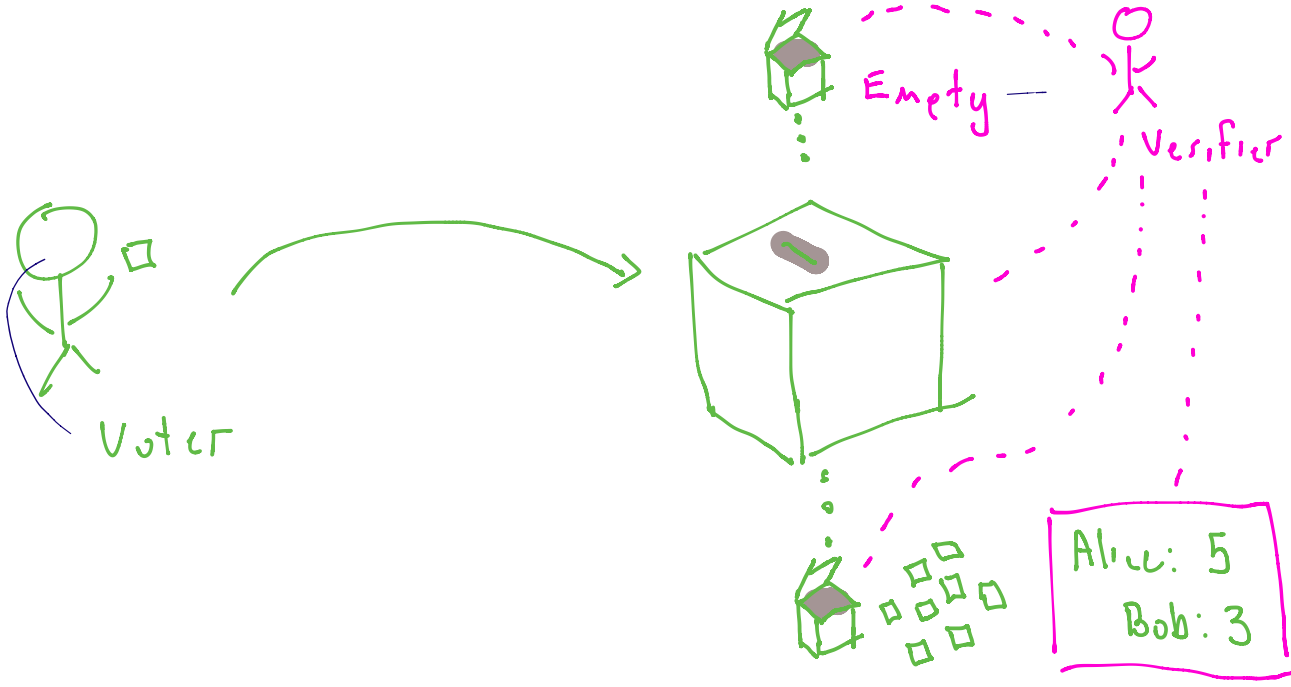
(1) Requirements

(2) CGS 1997 : basic backend

(3) Human Votable Ballots

(4) JCJ 2005 : Coercion resistance

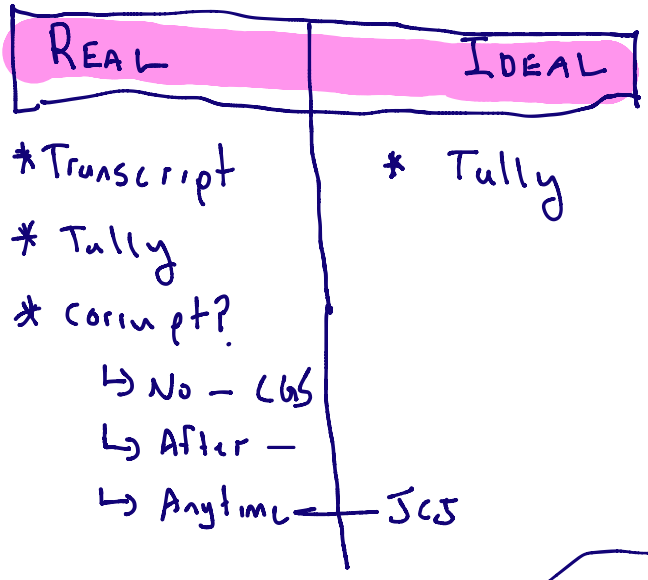
Requirements & Preliminaries

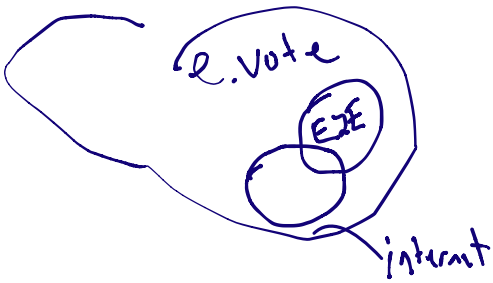


Requirements:

(1) Independently Verifiable
↳ integrity, soundness, etc. } fully correct

(2) Ballot secrecy
↳ receipt-free, coercion resistant, etc.
↳





Other requirements (situational)

* Dispute resolution
↳ accountability

* Independence
↳ simultaneity

* Fairness
↳ no 'running tally'

Uperio

* Robust, unconditional, submit-and-go

Crypto - toolbox

Homomorphic encryption

ZKPs

Ring signatures

Mix networks

anonymous credentials

MPC

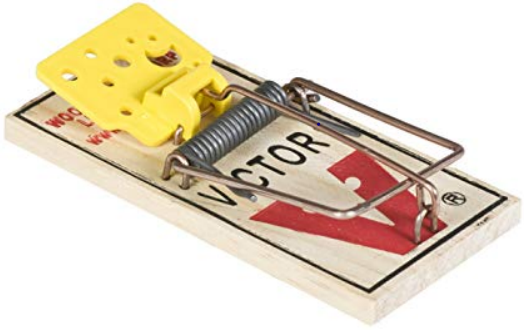
commitments

cut & choose

secret sharing

oblivious transfer

blind signatures

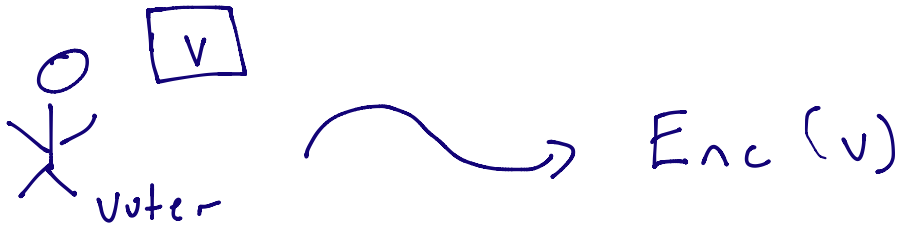


etc. etc.

↳ >200 papers proposing voting systems.

CGS - 1997

Cramer, Gennaro, Schoenmakers (Eurocrypt)



$Enc_{pk}(v, r) \rightarrow [v]$

↳ public key: EA ~> 3 out of 5

↳ [Distributed Key Generation (DKG)]

↳ Threshold decryption

↳ CPA secure

↳ Additively Homomorphic

$$[a] \cdot [b] = [a+b]$$

$$[a]^r = [a \cdot r]$$

~~$[a]^{[b]} = [a \cdot b]$~~

↳ Exponential Elgamal, Paillier, BGN.

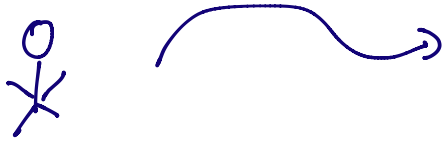
B.B.

Yes : [1]
No : [0]

[1]

[0] -3

[0]



$[x]^2$, π

[1]

[0]

[1]

↳ $\pi[v_i] = [4]$ ~> 4 ~> {4: Yes, 3: No} (EA)

If: [V] encrypts 0 or 1

↳ given $c_1, c_2 = Enc_y(m, r)$

$= \langle g^r, g^m y^r \rangle$ ~ g^{sk}

↳ $\langle g, y, c_1, c_2/g^v \rangle$ y^0

↳ DDH tuple iff [V]

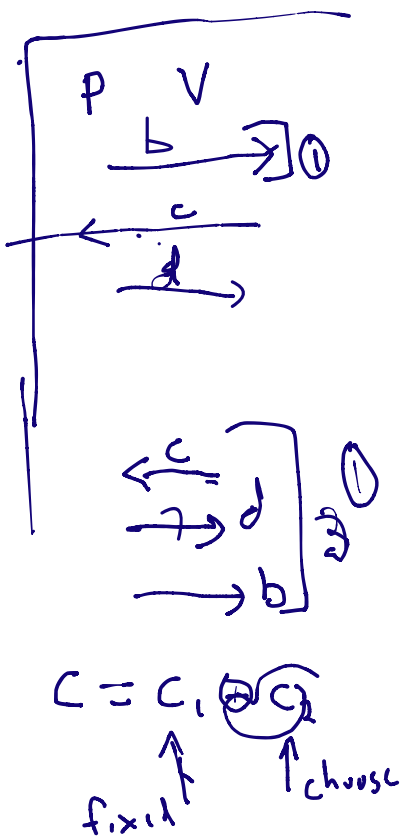
↳ $\langle g, y, c_1, c_2/g^0 \rangle$ or $\langle g, y, c_1, c_2/g^1 \rangle$

is DDH tuple.

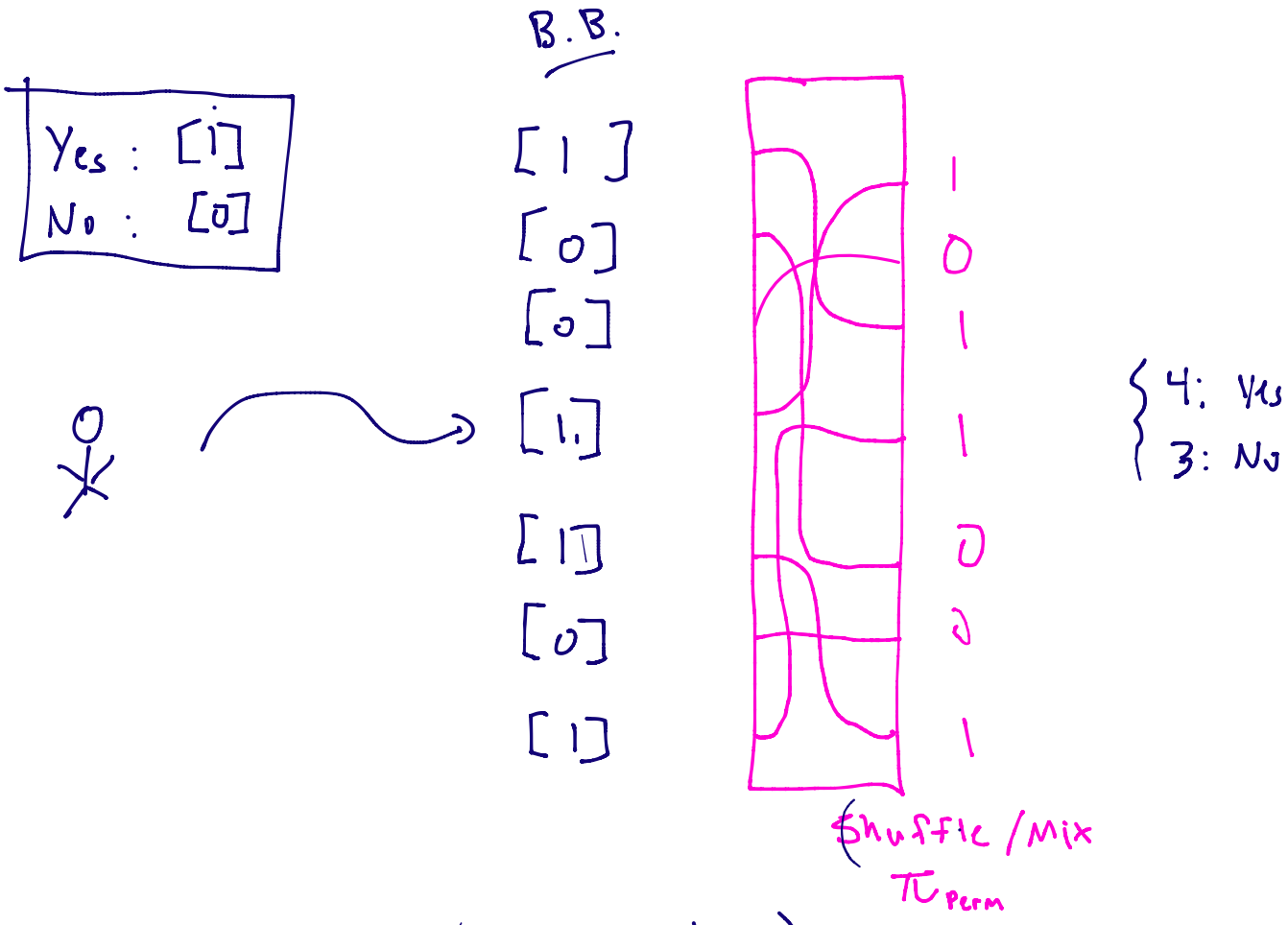
Multi-candidate (Hirt)

Alice	[0]	$\pi_{\{0,1\}}$
Bob	[0]	$\pi_{\{0,1\}}$
Carol	[1]	$\pi_{\{0,1\}}$
David	[0]	$\pi_{\{0,1\}}$

↳ Σ_1 → $[1]_{\pi_{\{0,1\}}}$



Alternative → Mixing [PIK93*, Chu81, SK95]

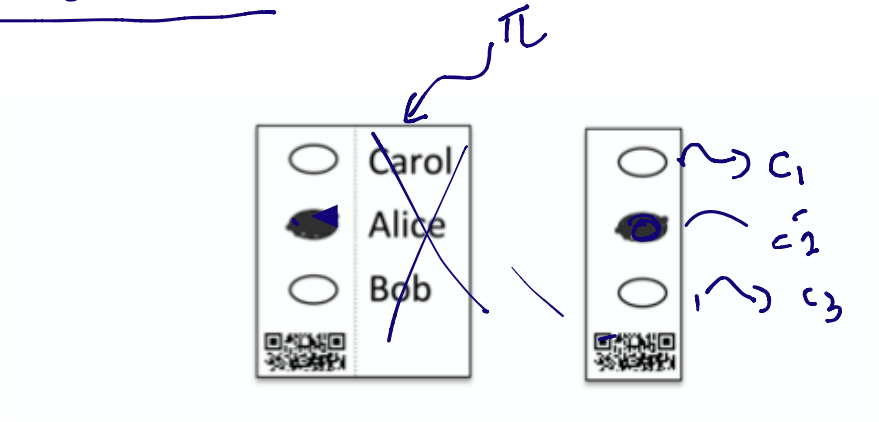


* Any candidate (even write-in)
* No voter ZKP

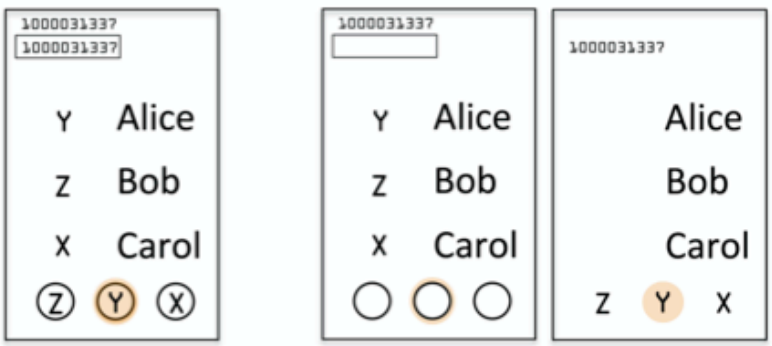
Summary

* Integrity
* Basic secrecy
  ↳ randomizers

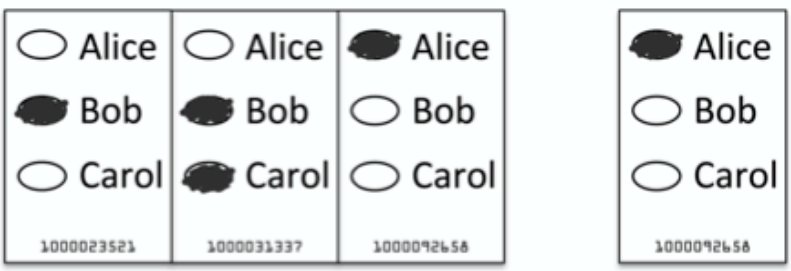
Human Votable



(a) Prêt à Voter



(b) Punchscan



(c) ThreeBallot

cast as intended

1337: TkG

π counted as cast

(d) Scantegrity : overlay, dispute

Scantegrity → Different Backend → TEE + commitments
(c.f. Eperio)
↳ Slides.

Internet Voting

Same requirements
+ untrusted platform
+ coercion resistance ← JCJ
+ DoS

JCJ05

Juels, Catalano, Jacobsson [WPES]
↳ Civitas

Principle: Voters have a "real" credential to vote. They can also make up a fake credential.
↳ Backend removes fakes w/o knowing what they are or who they are from

Voter Roster

Voter A $[\sigma_a]$ ← threshold

Voter B $[\sigma_b]$ → unstoppable channel → σ_b , π_b

Voter C $[\sigma_c]$

↳ $[\sigma_b]$ encrypts σ_b

or

I know Voter B's private key

↳ $\langle \tilde{\sigma}_b , \tilde{\pi}_b \rangle$

,

Votes

$[\text{Alice}]$, $[\tilde{\sigma}_b]$, π_{pok}

$[\text{Bob}]$, $[\sigma_b]$, π_{pok}

$[\text{Alice}]$, $[\sigma_a]$, π_{pok}

Votes shuffled

Roster shuffled

$[\sigma_b]$	$[\sigma_a]$	$[\sigma_c]$
F	T	F
T	F	F
F	F	F

$[\text{Alice}], [\sigma_a]$

$[\text{Bob}], [\sigma_b]$

$[\text{Alice}], [\tilde{\sigma}_b]$

Plaintext Equality Test

Alice : 1

Bob : 1

Given $[a]$ and $[b]$, $a \stackrel{?}{=} b$

↳ threshold decrypt

↳ learn nothing else

$$[a-b] = \begin{cases} [0] & \text{iff } a=b \\ [\Delta] & \text{iff } a \neq b \end{cases}$$

$$[?]^r = \begin{cases} [0 \cdot r] = [0] \\ [\Delta \cdot r] = [r] \end{cases}$$

Decrypt

Follow-up:

Make it linear [Selections, ABBT06]

↓ ↳ Alg. MACs

Panic passwords