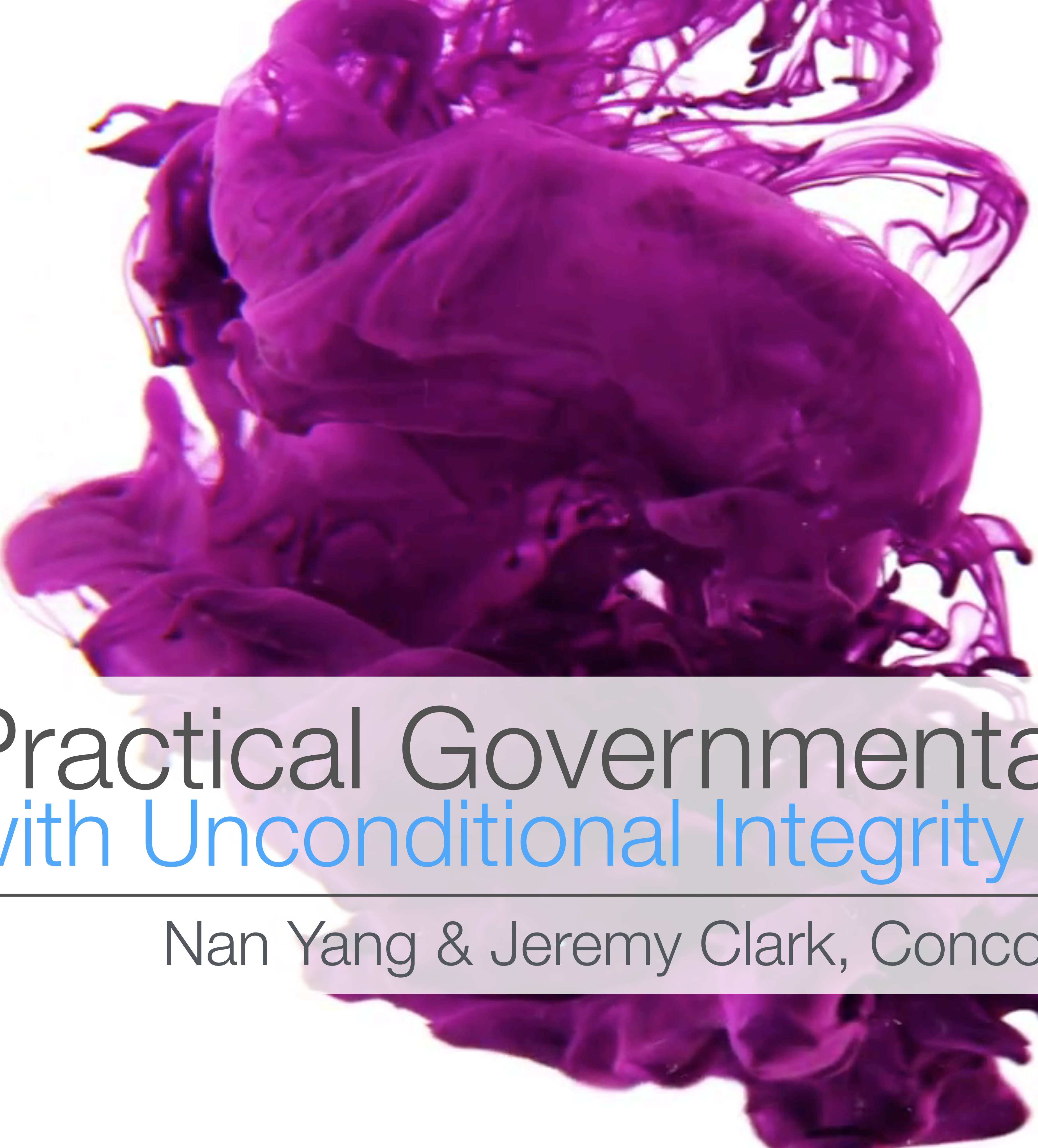
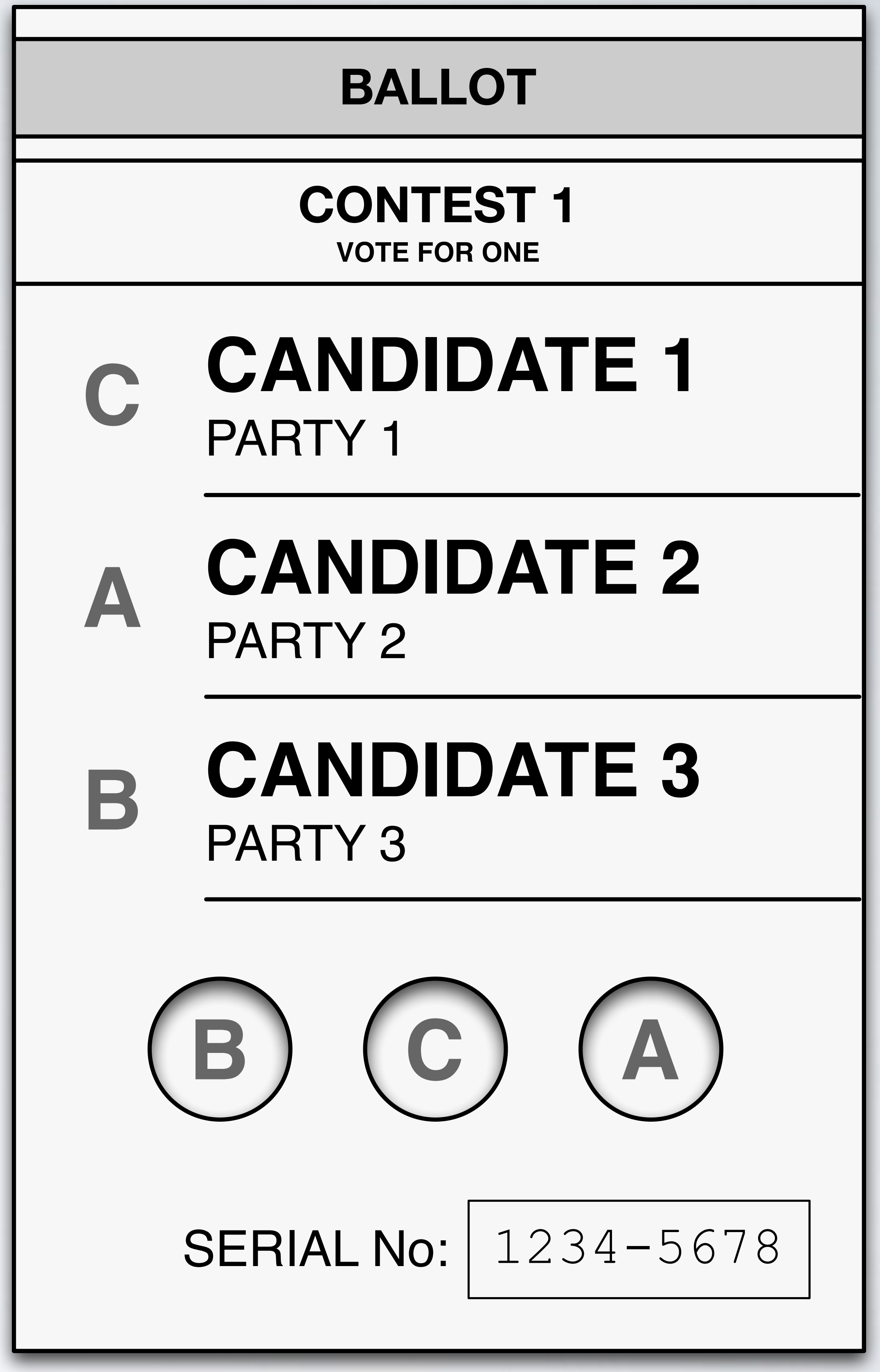


Practical Governmental Voting with Unconditional Integrity & Privacy

Nan Yang & Jeremy Clark, Concordia University

Punchscan
See your vote count.



BALLOT

CONTEST 1
VOTE FOR ONE

C CANDIDATE 1
PARTY 1

A CANDIDATE 2
PARTY 2

B CANDIDATE 3
PARTY 3

B C A

SERIAL No: 1234-5678

Unconditional Integrity

A corrupt EA cannot undetectably manipulate ballots

* Fully collude
* Learn all the secrets/keys
* Break all the cryptographic assumptions

Unconditional Integrity

A corrupt EA cannot undetectably manipulate ballots

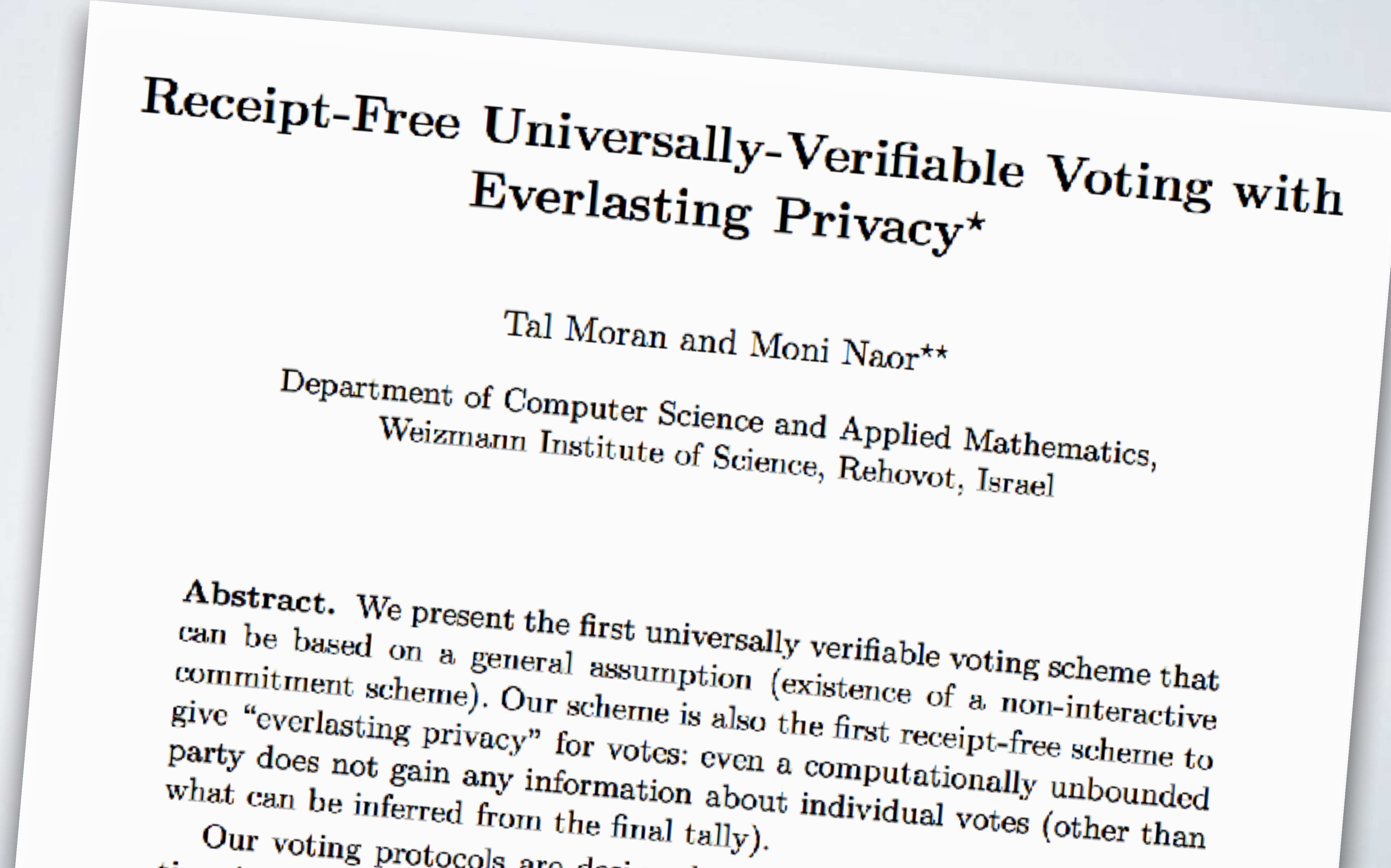
* Fully collude

* Learn all the secrets/keys

* Break all the cryptographic assumptions

Of course, ballot secrecy breaks completely

Everlasting Privacy



Receipt-Free Universally-Verifiable Voting with Everlasting Privacy*

Tal Moran and Moni Naor**

Department of Computer Science and Applied Mathematics,
Weizmann Institute of Science, Rehovot, Israel

Abstract. We present the first universally verifiable voting scheme that can be based on a general assumption (existence of a non-interactive commitment scheme). Our scheme is also the first receipt-free scheme to give "everlasting privacy" for votes: even a computationally unbounded party does not gain any information about individual votes (other than what can be inferred from the final tally).

Our voting protocols are

Everlasting Privacy

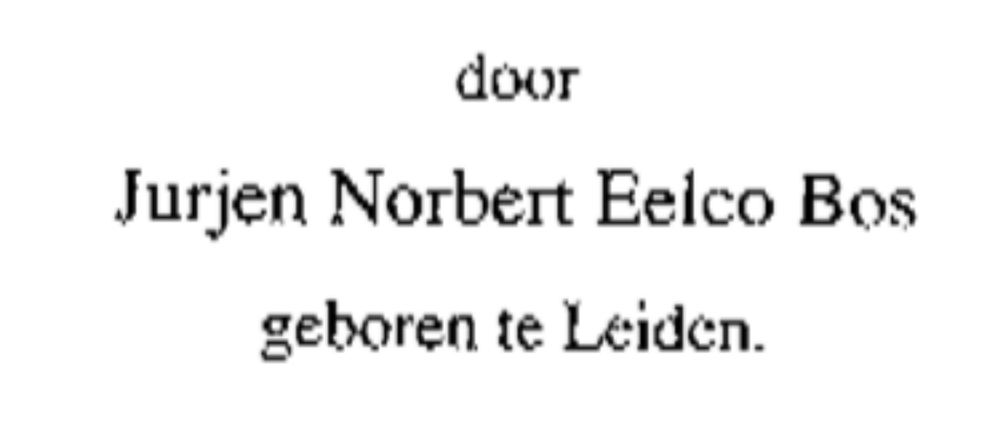
Ballot secrecy cannot be broken

* Break all the cryptographic assumptions

* (However collusion does break it)

And of course, integrity breaks completely

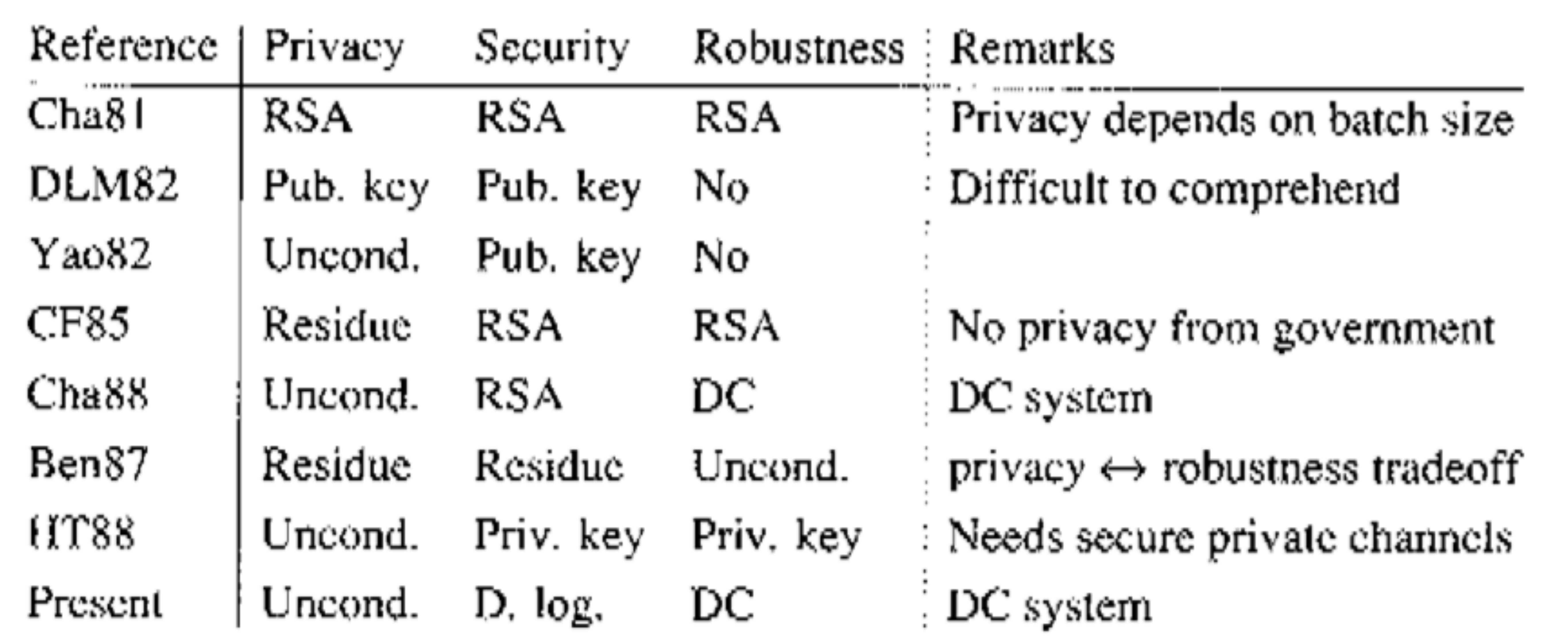
Integrity needs to last the lifetime of the election, while ballot secrecy should last centuries



door

Jurjen Norbert Eelco Bos

geboren te Leiden.



Reference	Privacy	Security	Robustness	Remarks
Cha81	RSA	RSA	RSA	Privacy depends on batch size
DLM82	Pub. key	Pub. key	No	Difficult to comprehend
Yao82	Uncond.	Pub. key	No	
CF85	Residue	RSA	RSA	No privacy from government
Cha88	Uncond.	RSA	DC	DC system
Ben87	Residue	Residue	Uncond.	privacy ↔ robustness tradeoff
HT88	Uncond.	Priv. key	Priv. key	Needs secure private channels
Present	Uncond.	D. log.	DC	DC system

Table 3: Comparison of voting schemes.

Unconditional
Integrity

Unconditional
Ballot Secrecy

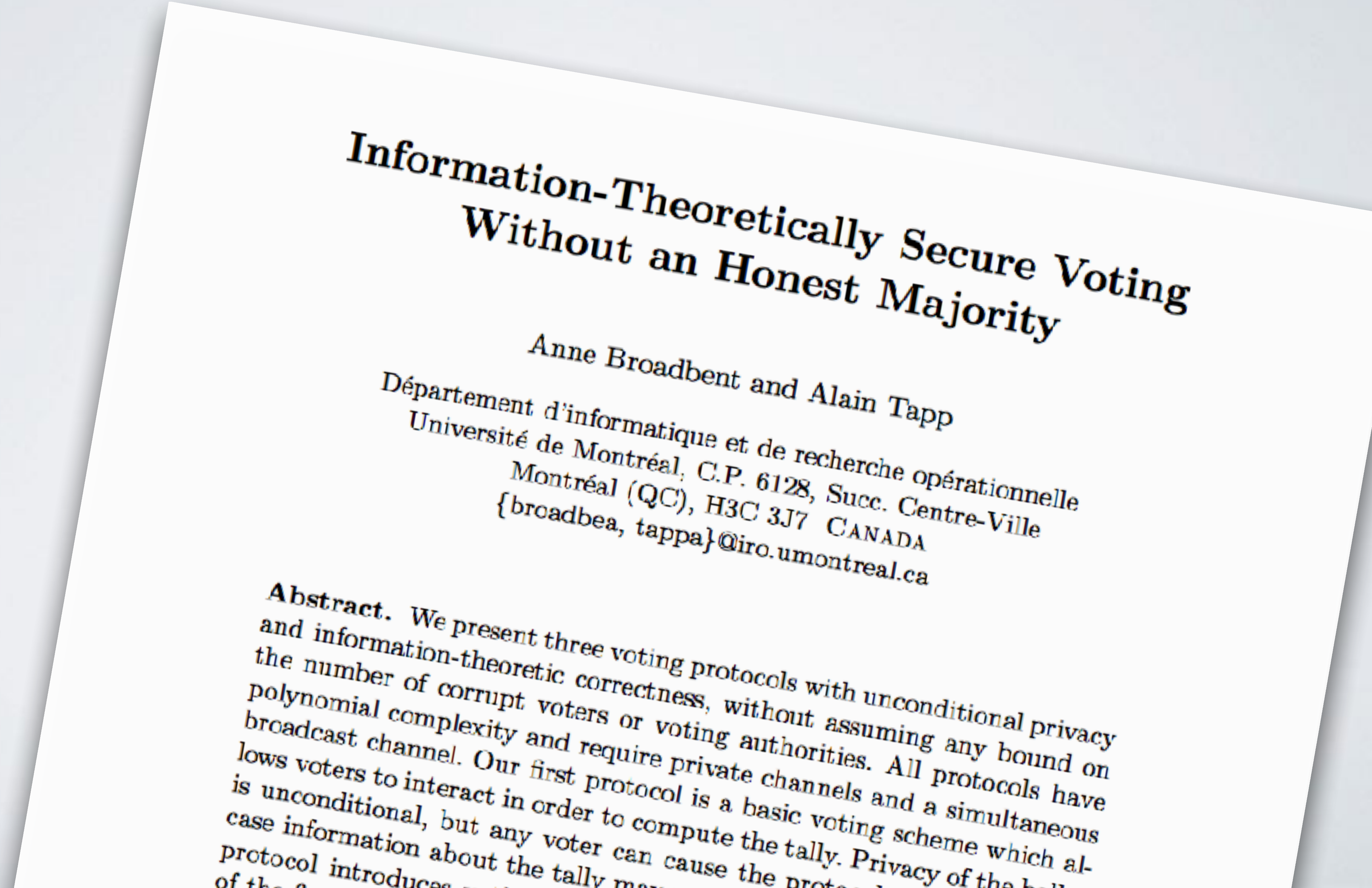
Unconditional Integrity

Punchscan
Scantegrity
Pret a Voter
Helios
JCJ/Civitas/Variants
STAR Voting

Unconditional Ballot Secrecy

Chaum 88
Kiayias-Yung
Moran-Naor
Demirel et al
Locher et al

You can have both



Information-Theoretically Secure Voting Without an Honest Majority

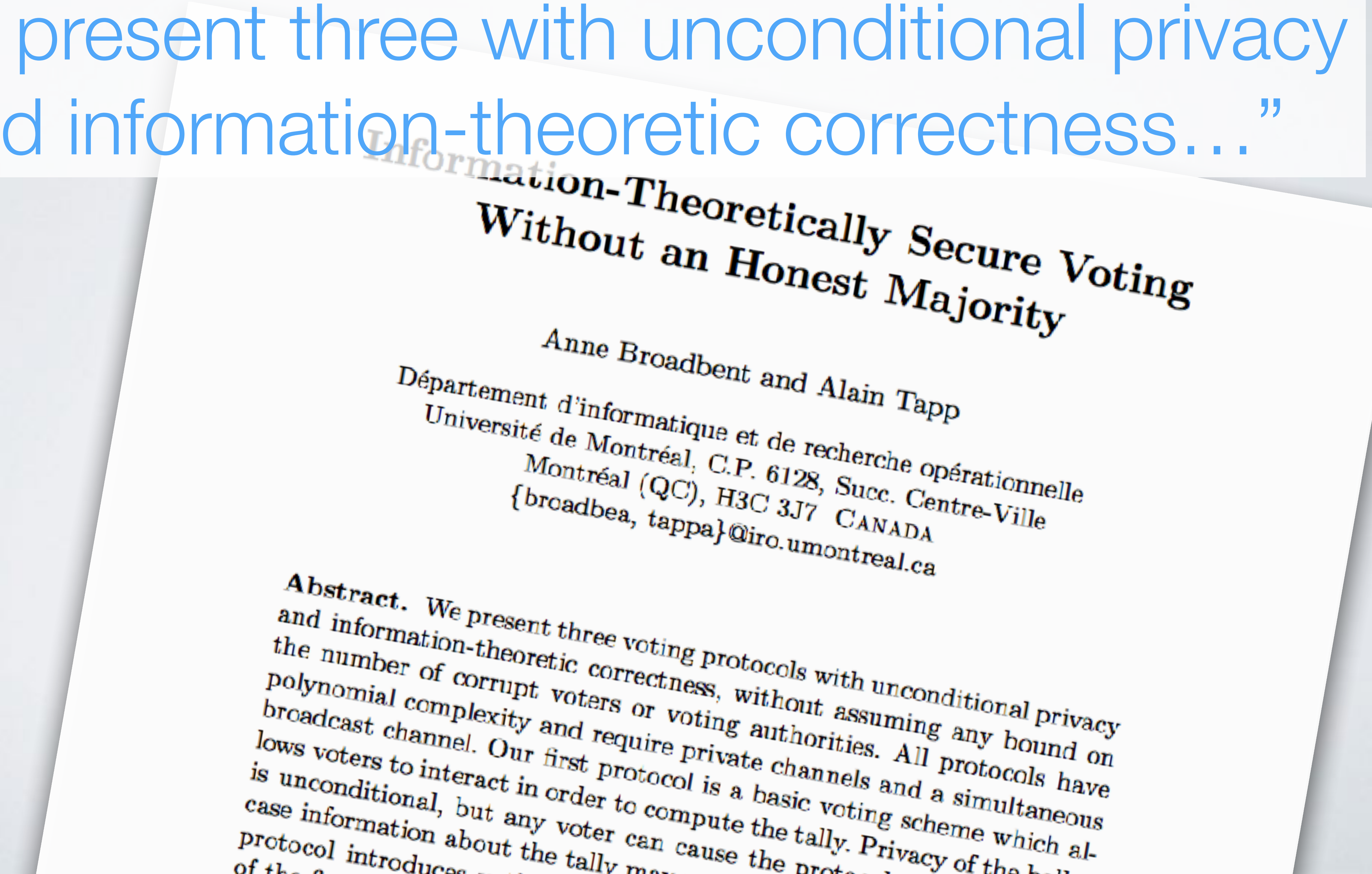
Anne Broadbent and Alain Tapp

Département d'informatique et de recherche opérationnelle
Université de Montréal, C.P. 6128, Succ. Centre-Ville
Montréal (QC), H3C 3J7 CANADA
{broadbea, tappa}@iro.umontreal.ca

Abstract. We present three voting protocols with unconditional privacy and information-theoretic correctness, without assuming any bound on the number of corrupt voters or voting authorities. All protocols have polynomial complexity and require private channels and a simultaneous broadcast channel. Our first protocol is a basic voting scheme which allows voters to interact in order to compute the tally. Privacy of the ball is unconditional, but any voter can cause the proto case information about the tally ma protocol introduc of th

You can have both

"We present three with unconditional privacy and information-theoretic correctness…"



Information-Theoretically Secure Voting Without an Honest Majority

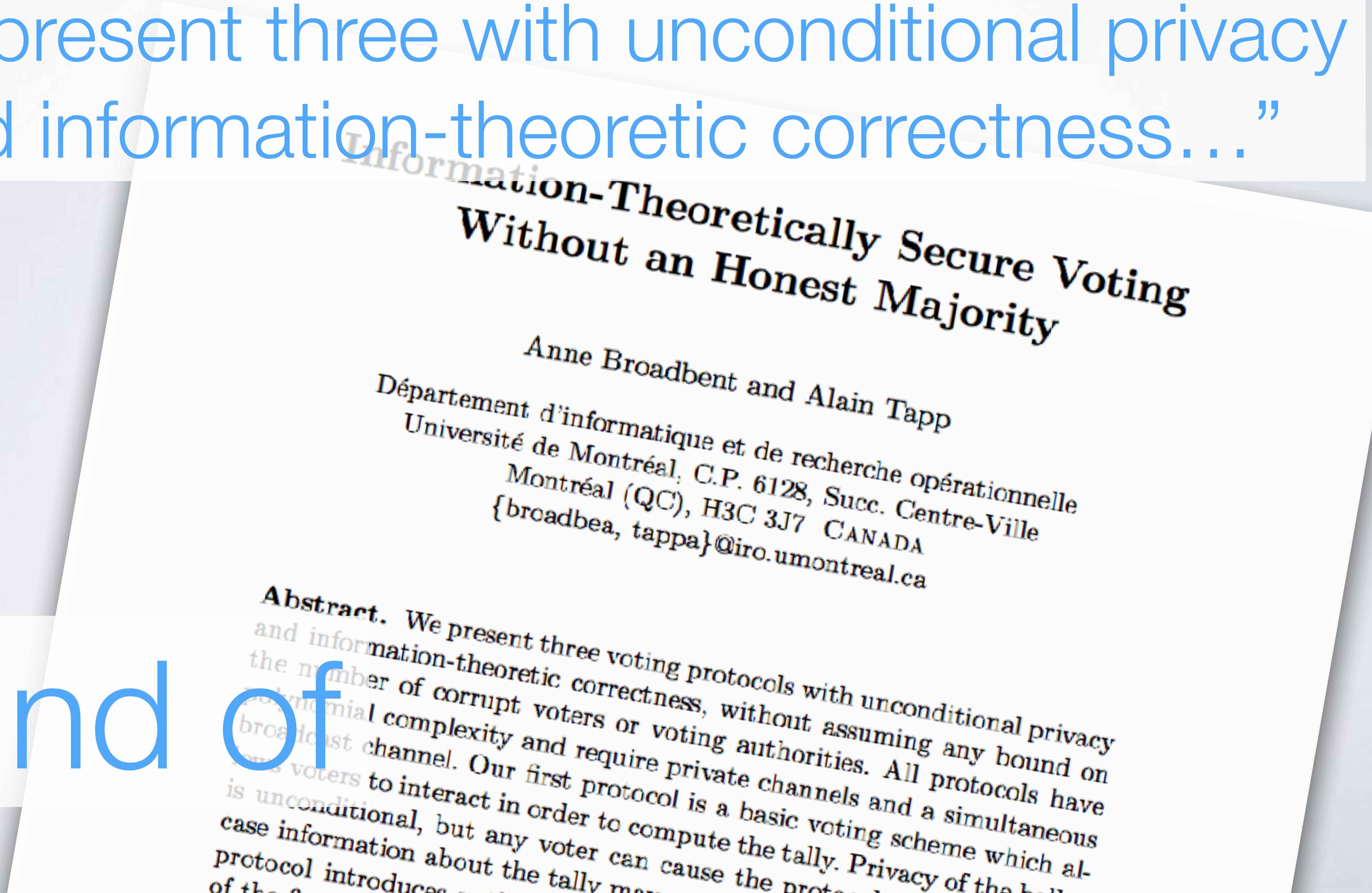
Anne Broadbent and Alain Tapp

Département d'informatique et de recherche opérationnelle
Université de Montréal, C.P. 6128, Succ. Centre-Ville
Montréal (QC), H3C 3J7 CANADA
{broadbea, tappa}@iro.umontreal.ca

Abstract. We present three voting protocols with unconditional privacy and information-theoretic correctness, without assuming any bound on the number of corrupt voters or voting authorities. All protocols have polynomial complexity and require private channels and a simultaneous broadcast channel. Our first protocol is a basic voting scheme which allows voters to interact in order to compute the tally. Privacy of the ball
is unconditional, but any voter can cause the proto
case information about the tally ma
protocol introduces
of th

You can have both*

"We present three with unconditional privacy and information-theoretic correctness…"



Information-Theoretically Secure Voting Without an Honest Majority

Anne Broadbent and Alain Tapp

Département d'informatique et de recherche opérationnelle
Université de Montréal, C.P. 6128, Succ. Centre-Ville
Montréal (QC), H3C 3J7 CANADA
{broadbea, tappa}@iro.umontreal.ca

Abstract. We present three voting protocols with unconditional privacy and information-theoretic correctness, without assuming any bound on the number of corrupt voters or voting authorities. All protocols have polynomial complexity and require private channels and a simultaneous broadcast channel. Our first protocol is a basic voting scheme which allows voters to interact in order to compute the tally. Privacy of the ballot is unconditional, but any voter can cause the proto
case information about the tally ma
protocol introduces
of th

*kind of

Info-Theoretic Secure

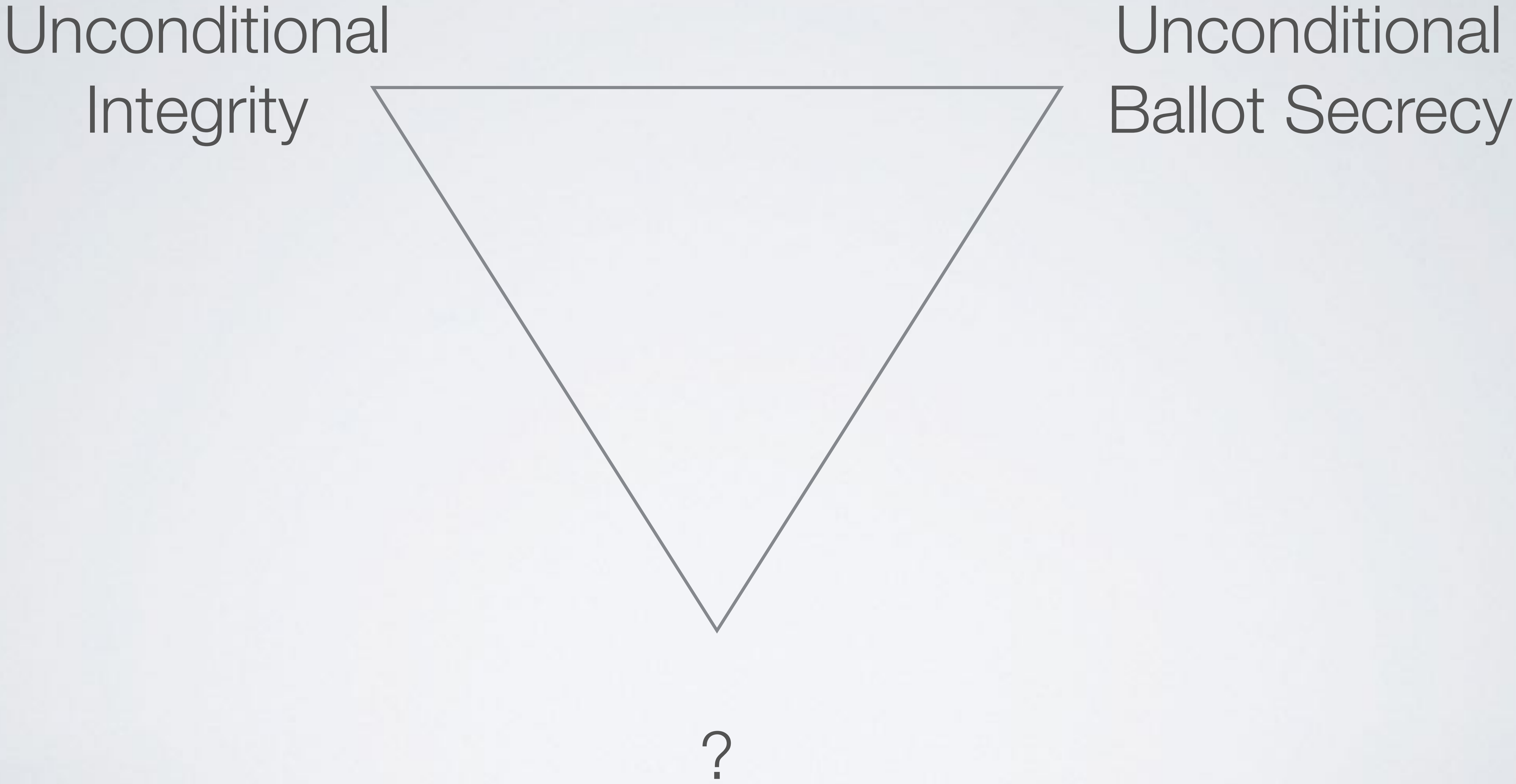
Unconditional Integrity & Everlasting Privacy

- Voters participate in tallying the result
- Essentially a big MPC with ballots as private inputs
- "Boardroom Voting" - lots of earlier papers

Governmental Elections

- Human voteable
- Vote-and-go

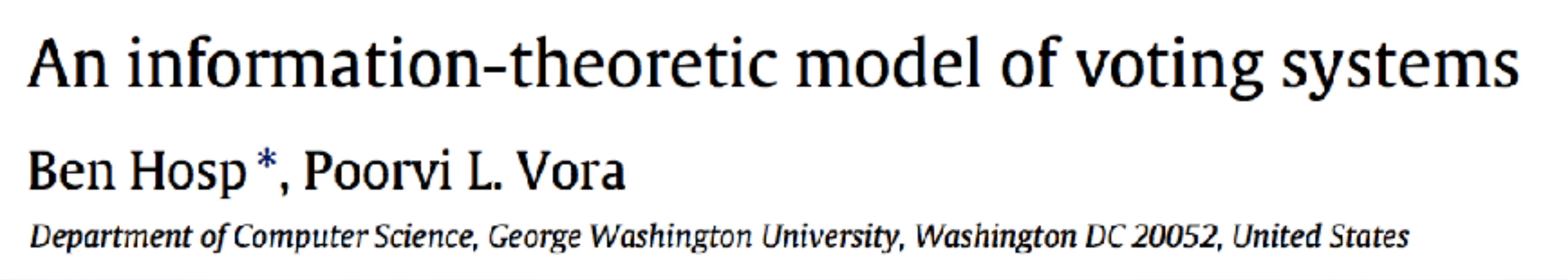
Can you have it all? Probably not, it is 2017 after-all



Unconditional Integrity

Unconditional Ballot Secrecy

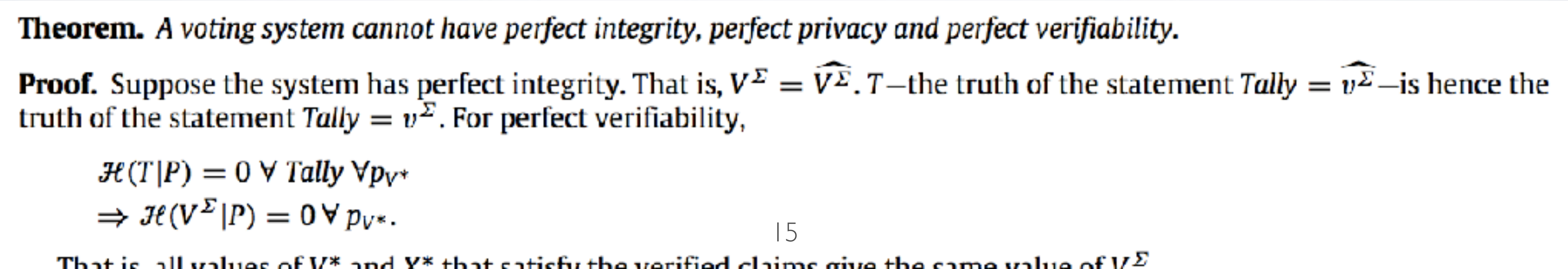
?



An information-theoretic model of voting systems

Ben Hosp *, Poorvi L. Vora

Department of Computer Science, George Washington University, Washington DC 20052, United States



Theorem. *A voting system cannot have perfect integrity, perfect privacy and perfect verifiability.*

Proof. Suppose the system has perfect integrity. That is, $V^{\Sigma} = \widehat{V^{\Sigma}}$. T—the truth of the statement $Tally = \widehat{v^{\Sigma}}$—is hence the truth of the statement $Tally = v^{\Sigma}$. For perfect verifiability,

$$\mathcal{H}(T|P) = 0 \ \forall \ Tally \ \forall p_{V^*}$$
$$\Rightarrow \mathcal{H}(V^{\Sigma}|P) = 0 \ \forall \ p_{V^*}.$$

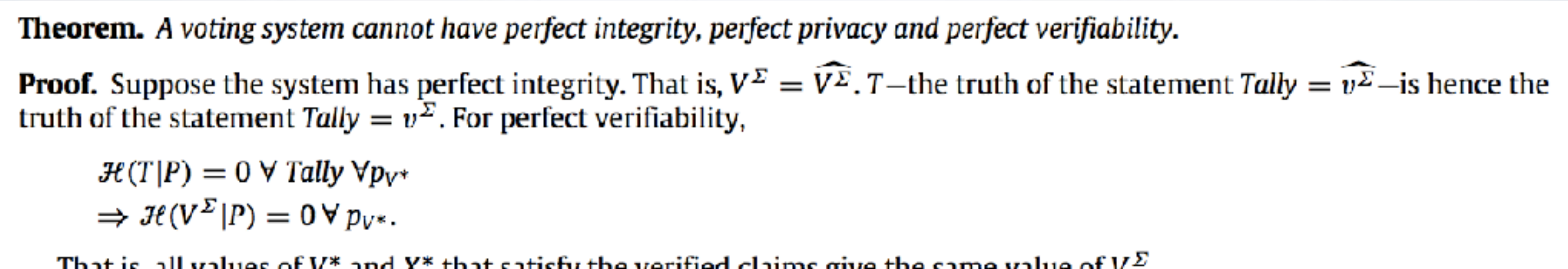
That is, all values of V^* and X^* that satisfy the verified claims give the same value of V^{Σ}

An information-theoretic model of voting systems

Ben Hosp *, Poorvi L. Vora

Department of Computer Science, George Washington University, Washington DC 20052, United States

Theorem. A voting system cannot have perfect integrity, perfect privacy and perfect verifiability.



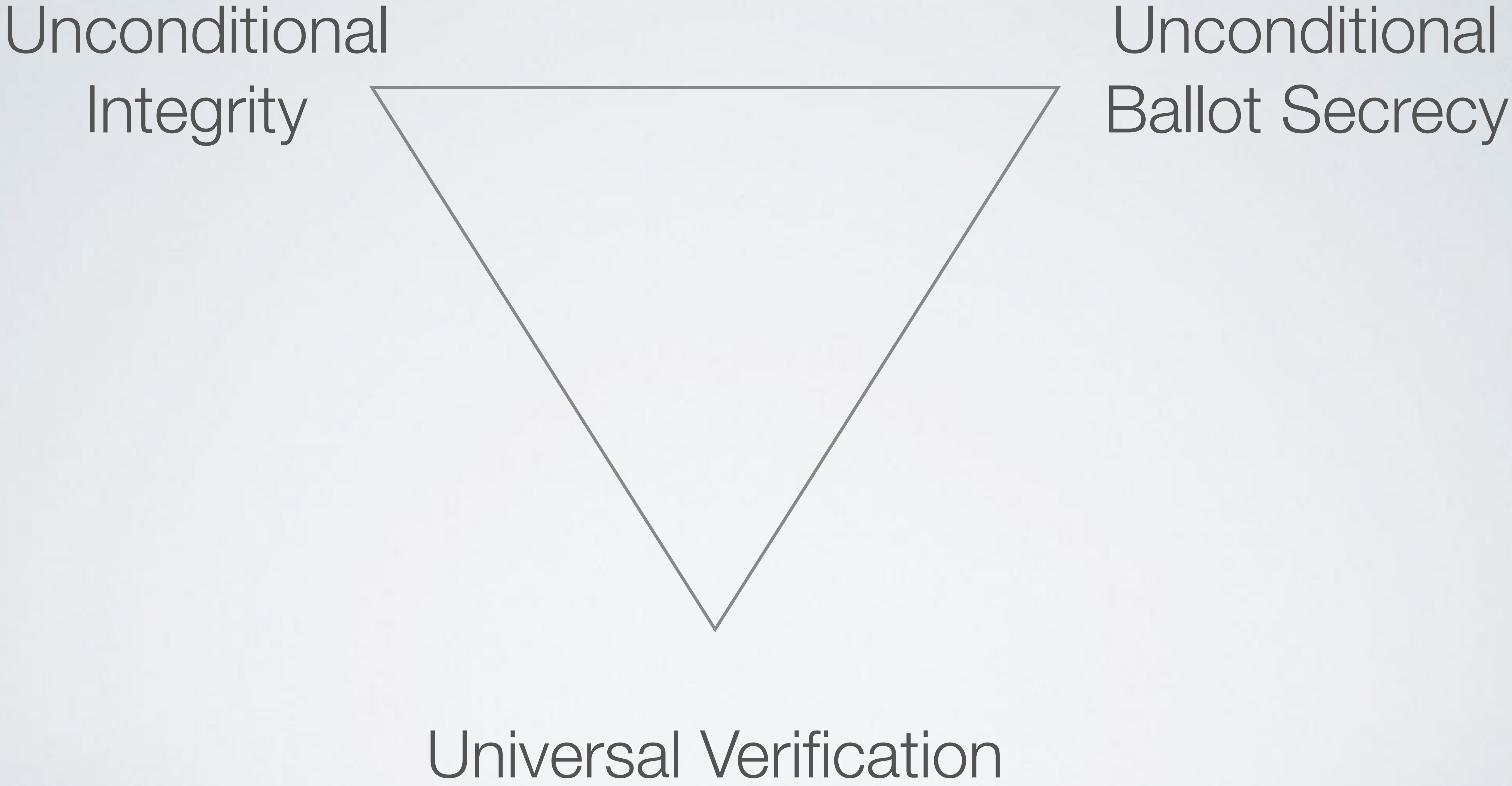
Theorem. *A voting system cannot have perfect integrity, perfect privacy and perfect verifiability.*

Proof. Suppose the system has perfect integrity. That is, $V^{\Sigma} = \widehat{V^{\Sigma}}$. T—the truth of the statement $Tally = \widehat{v^{\Sigma}}$—is hence the truth of the statement $Tally = v^{\Sigma}$. For perfect verifiability,

$$\mathcal{H}(T|P) = 0 \;\forall\; Tally\; \forall p_{V^*}$$
$$\Rightarrow \mathcal{H}(V^{\Sigma}|P) = 0 \;\forall\; p_{V^*}.$$

That is, all values of V^* and X^* that satisfy the verified claims give the same value of V^{Σ}

Hosp-Vora Triangle

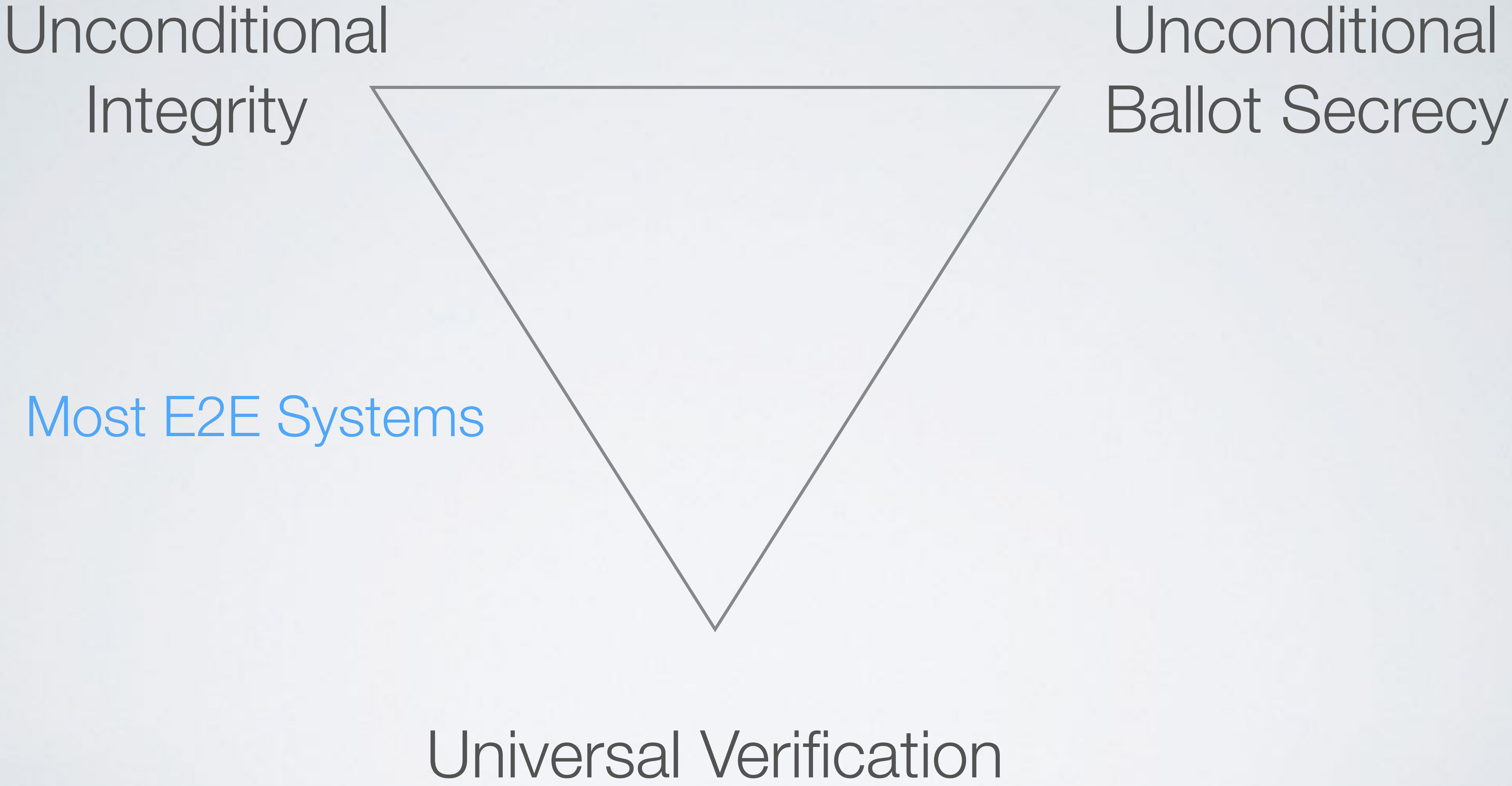


Unconditional Integrity

Unconditional Ballot Secrecy

Universal Verification

Hosp-Vora Triangle



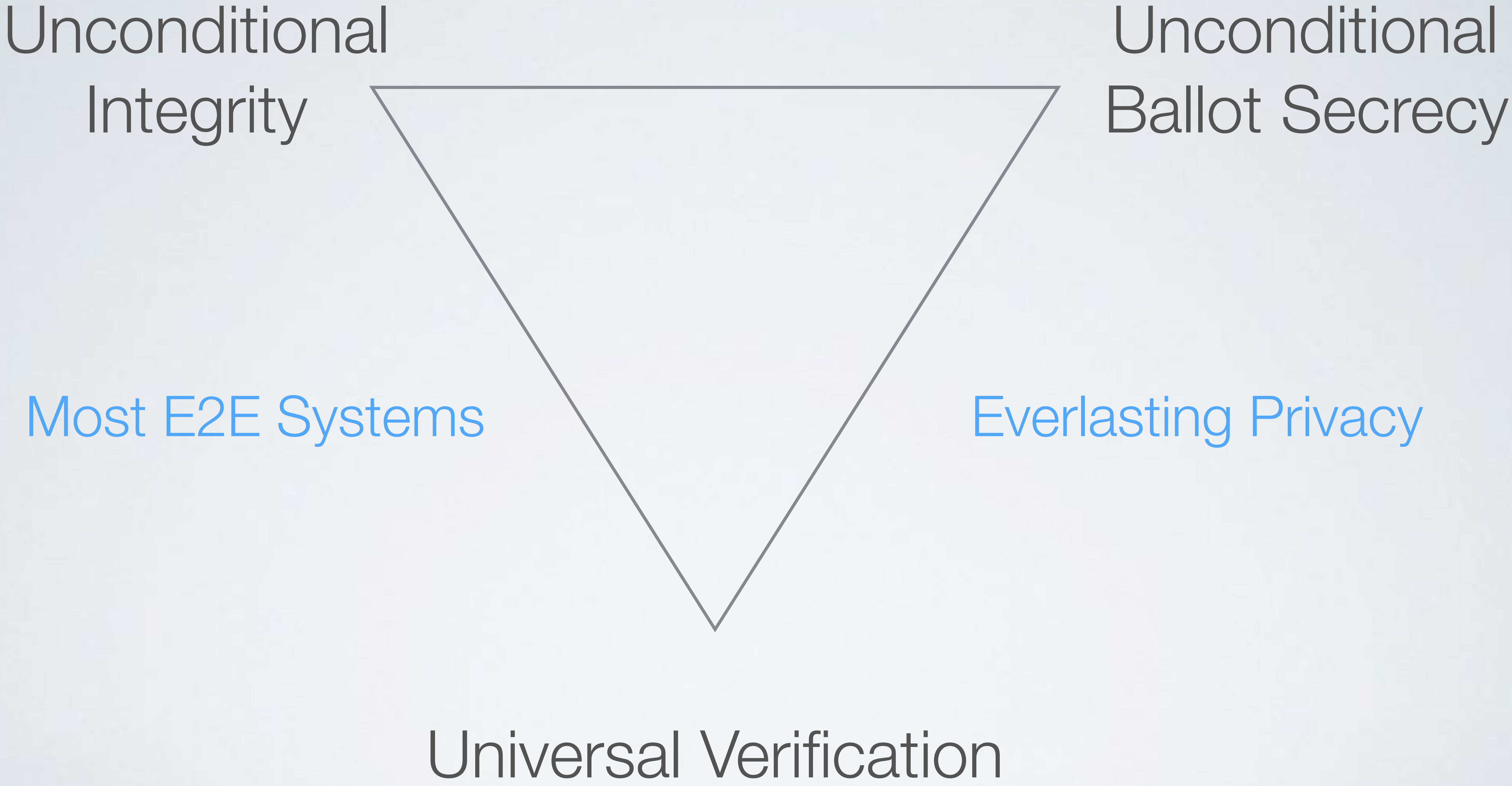
Unconditional Integrity

Unconditional Ballot Secrecy

Most E2E Systems

Universal Verification

Hosp-Vora Triangle



Unconditional Integrity

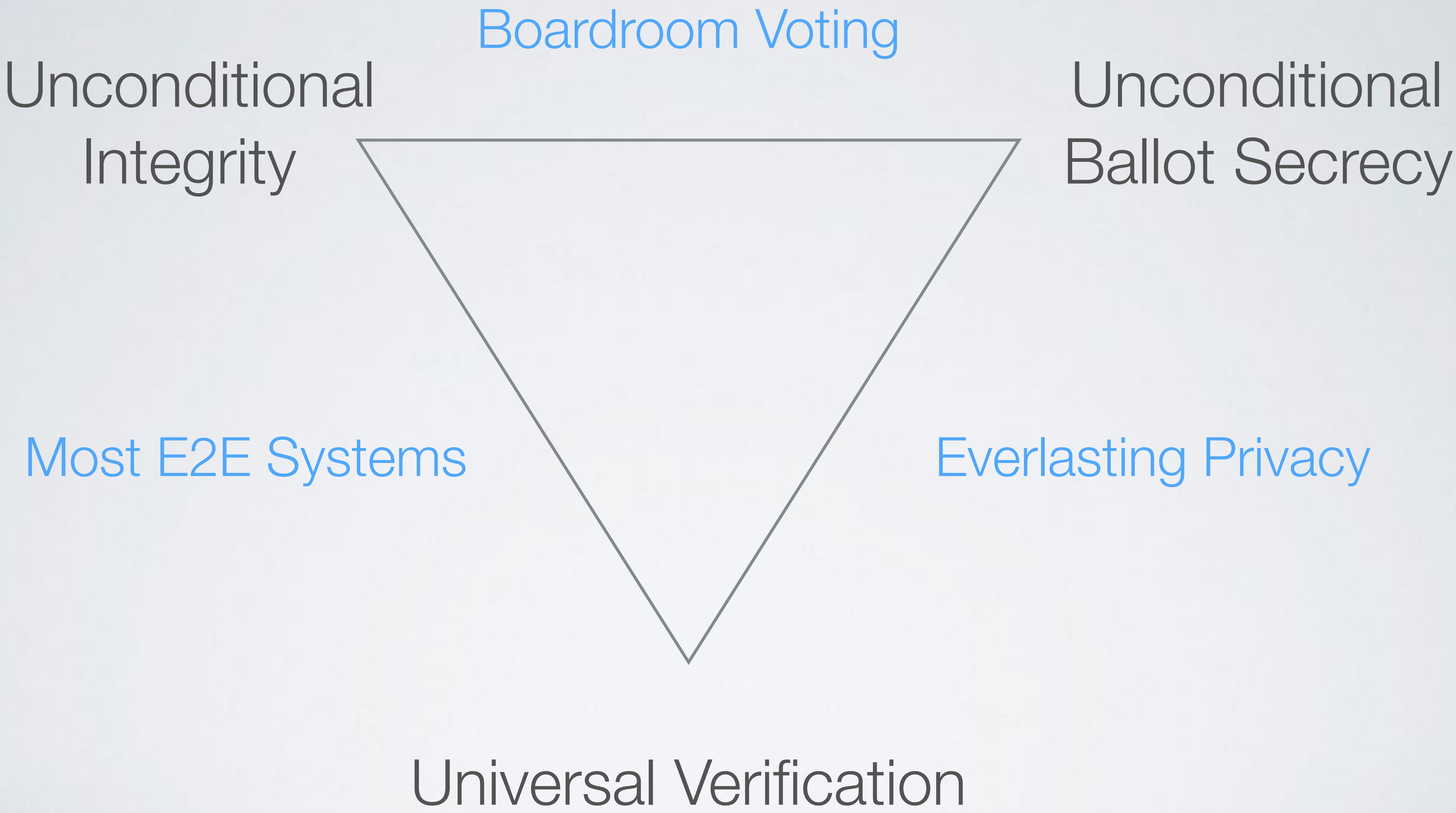
Unconditional Ballot Secrecy

Most E2E Systems

Everlasting Privacy

Universal Verification

Hosp-Vora Triangle



Boardroom Voting

Unconditional Integrity

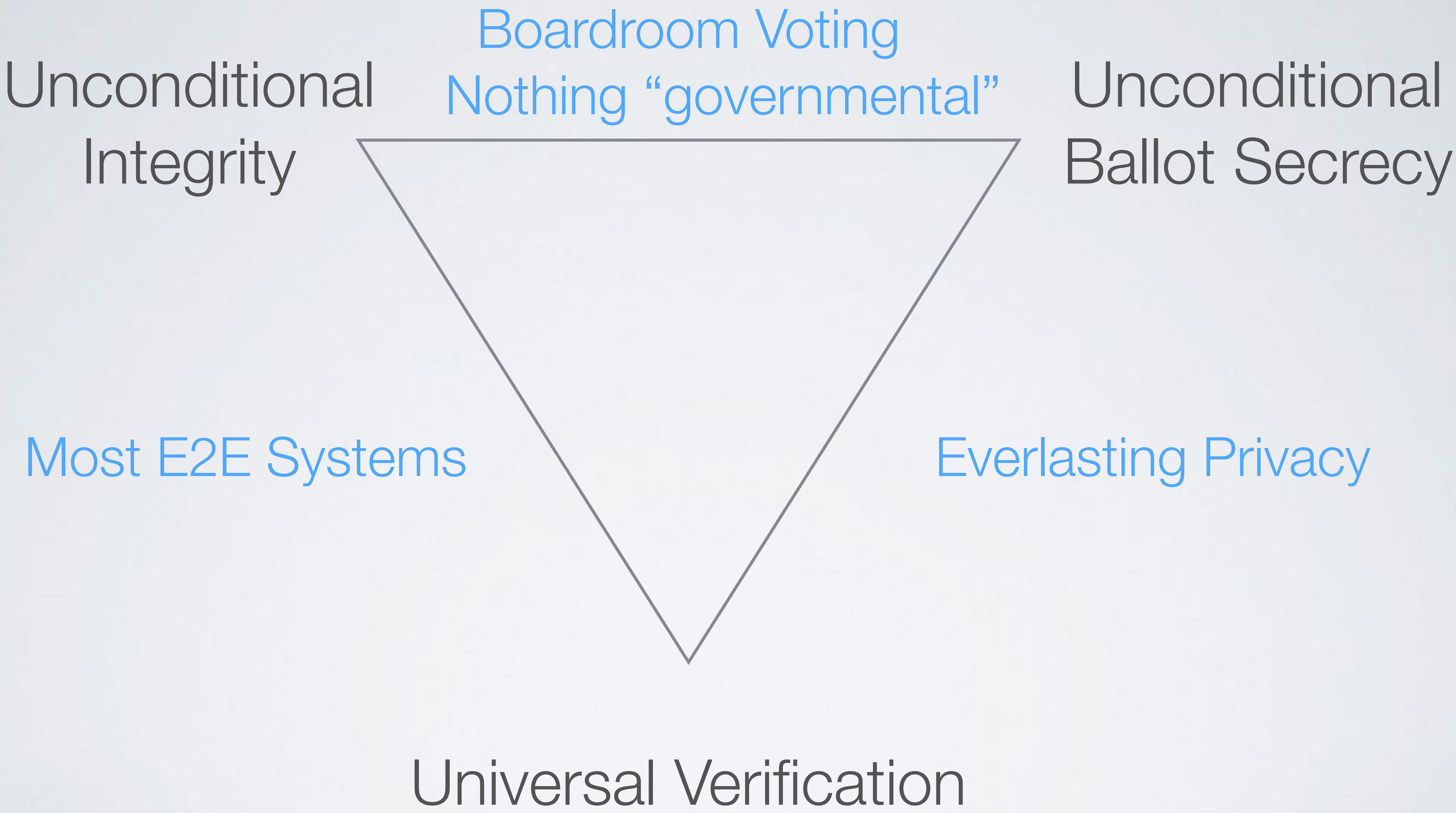
Unconditional Ballot Secrecy

Most E2E Systems

Everlasting Privacy

Universal Verification

Hosp-Vora Triangle



Boardroom Voting
Nothing “governmental”

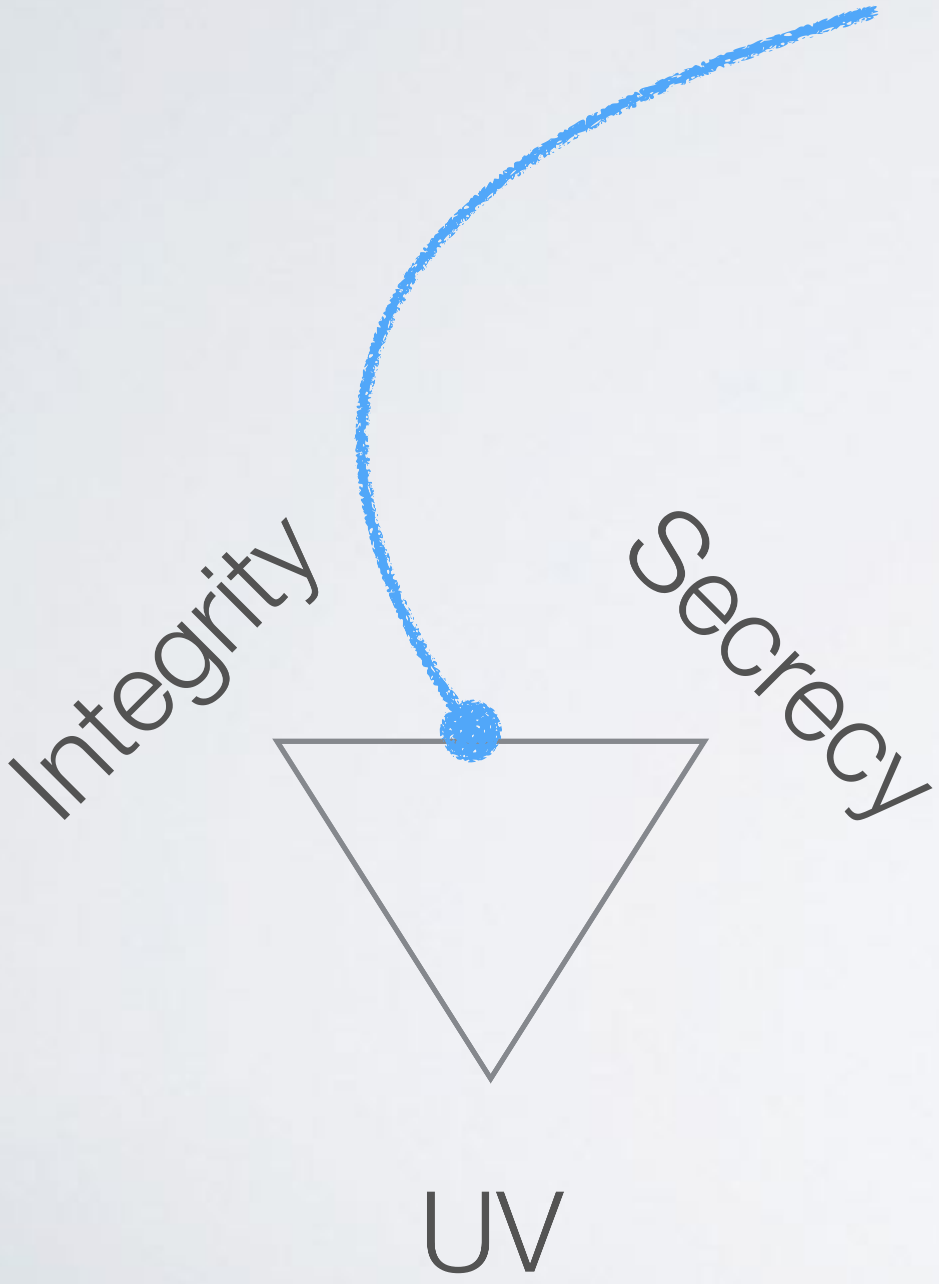
Unconditional
Integrity

Unconditional
Ballot Secrecy

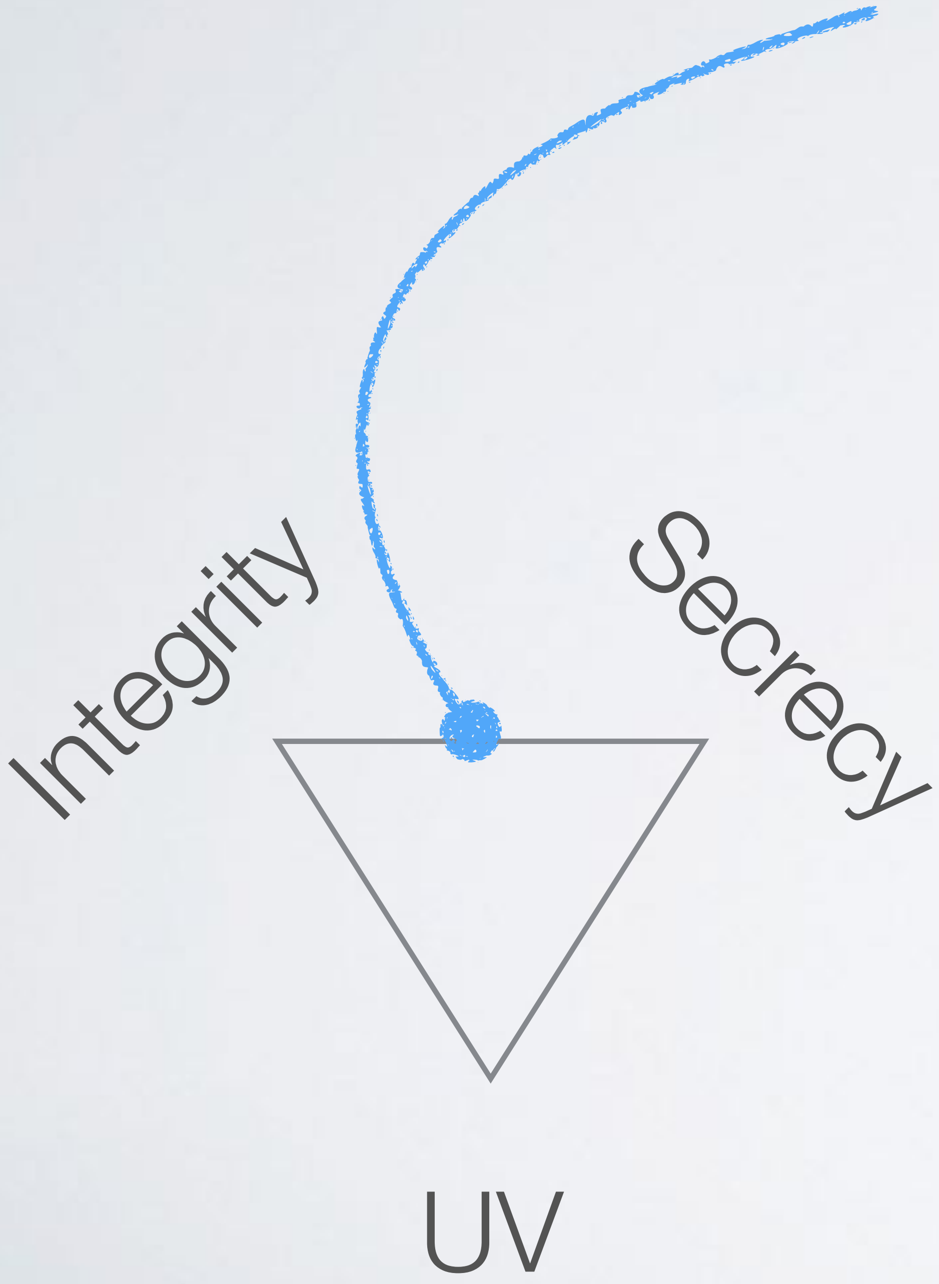
Most E2E Systems

Everlasting Privacy

Universal Verification


Integrity
Secrecy
UV

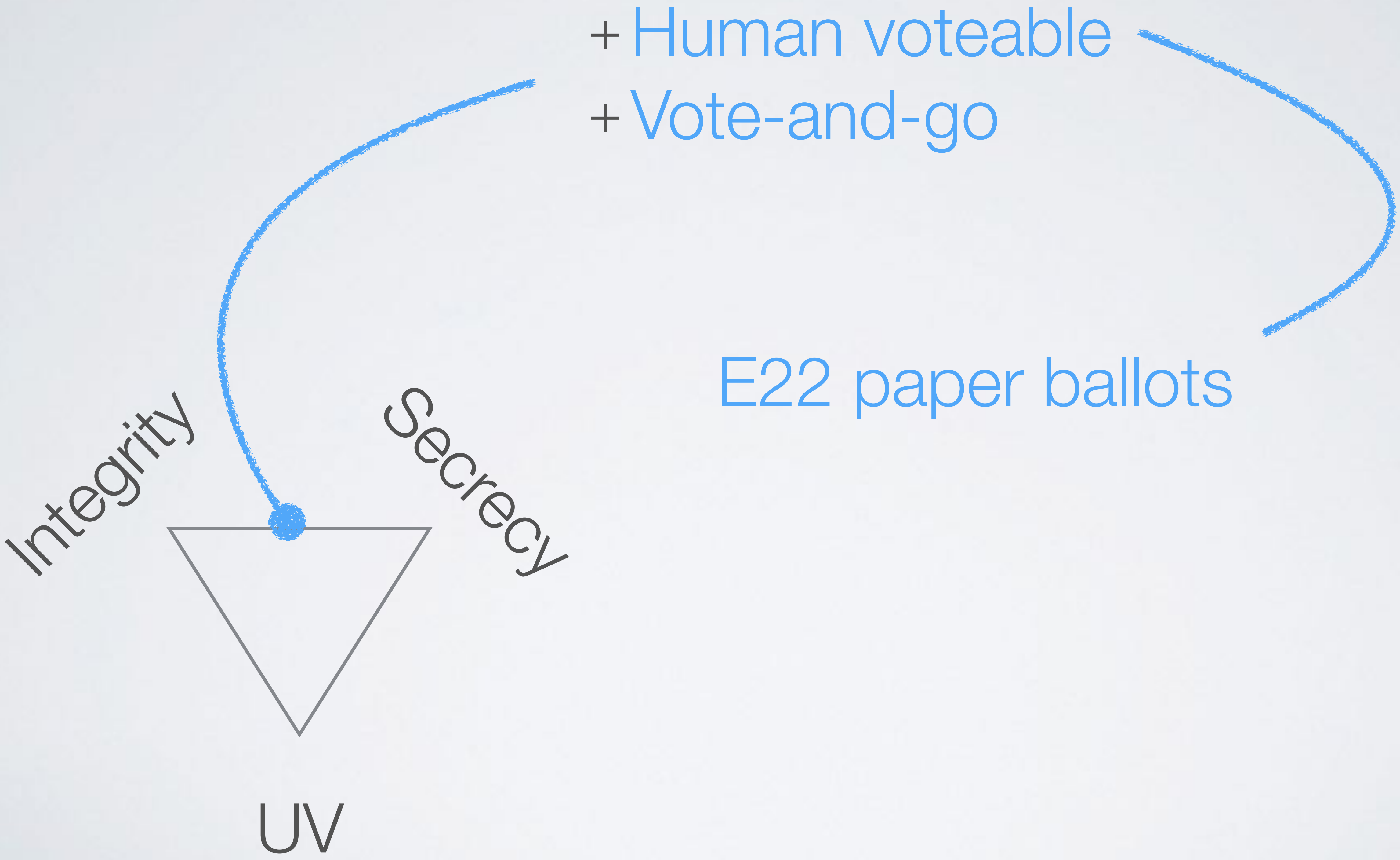
- Human voteable
- Vote-and-go



Integrity

Secrecy

UV



+ Human voteable

+ Vote-and-go

E22 paper ballots

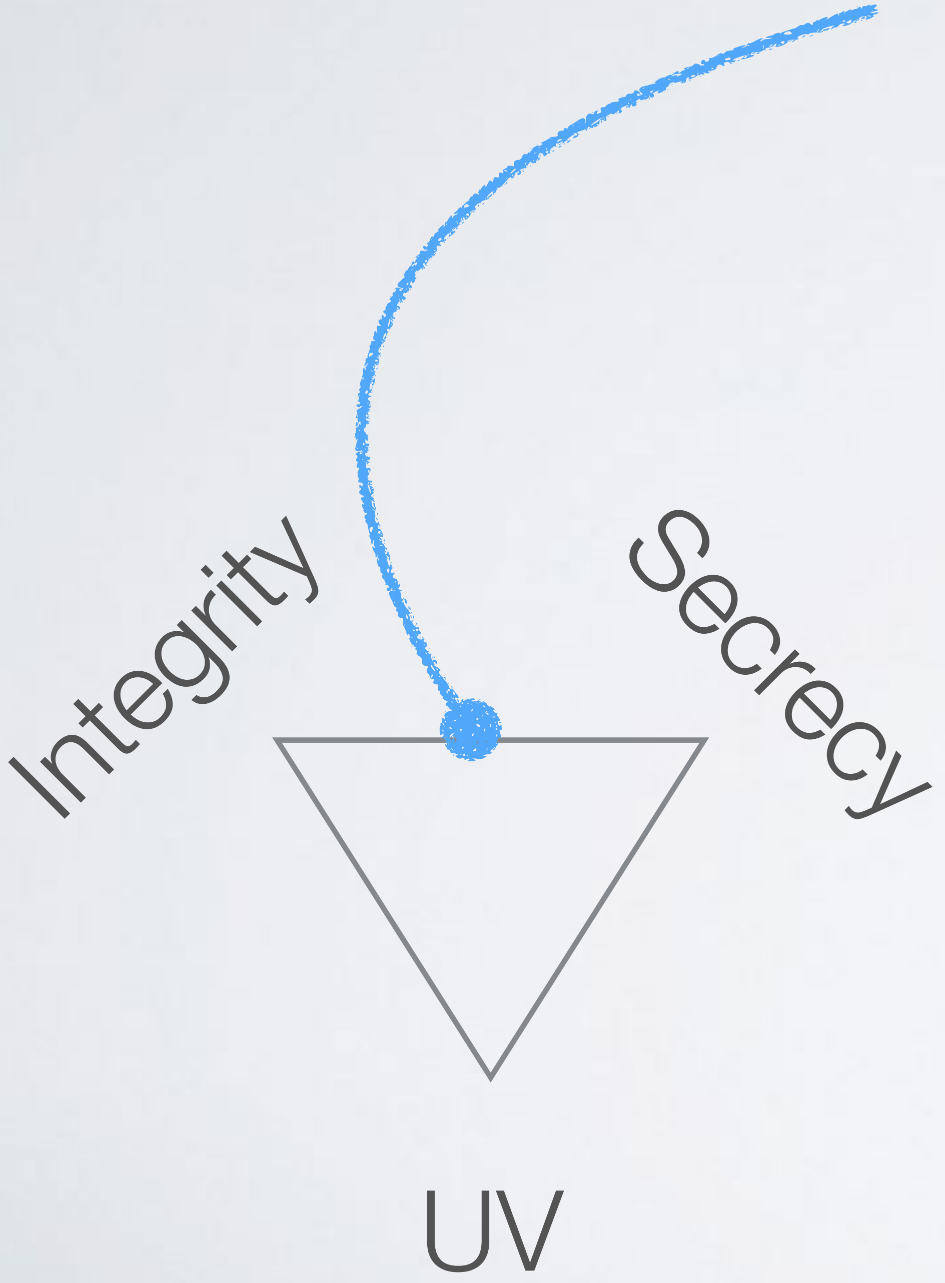
Integrity

Secrecy

UV

+ Human voteable

+ Vote-and-go



Integrity

Secrecy

UV

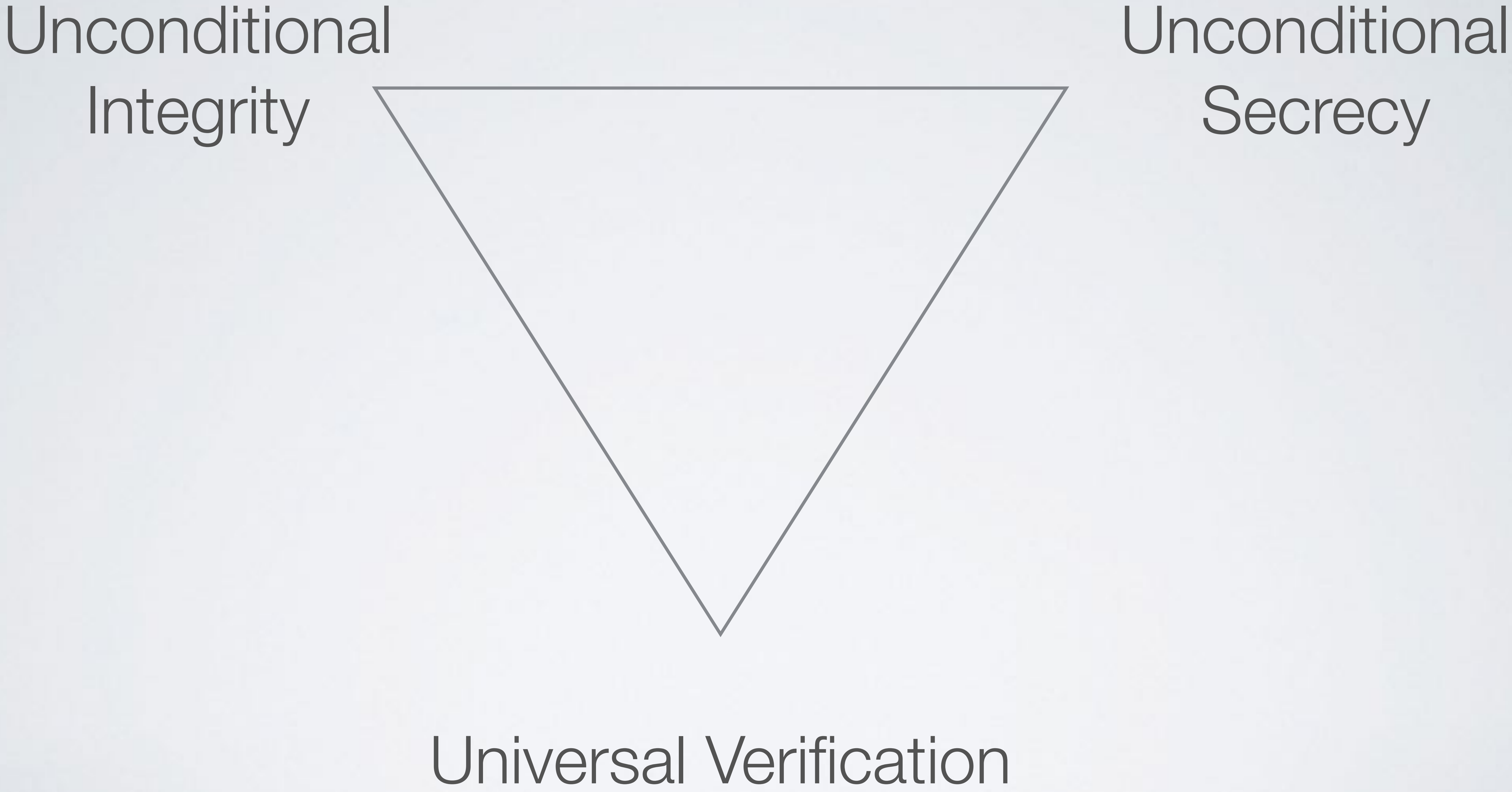
E22 paper ballots

Obfuscation of the vote:

* Commit / Encrypt

* ZKPs

Vote Obfuscation

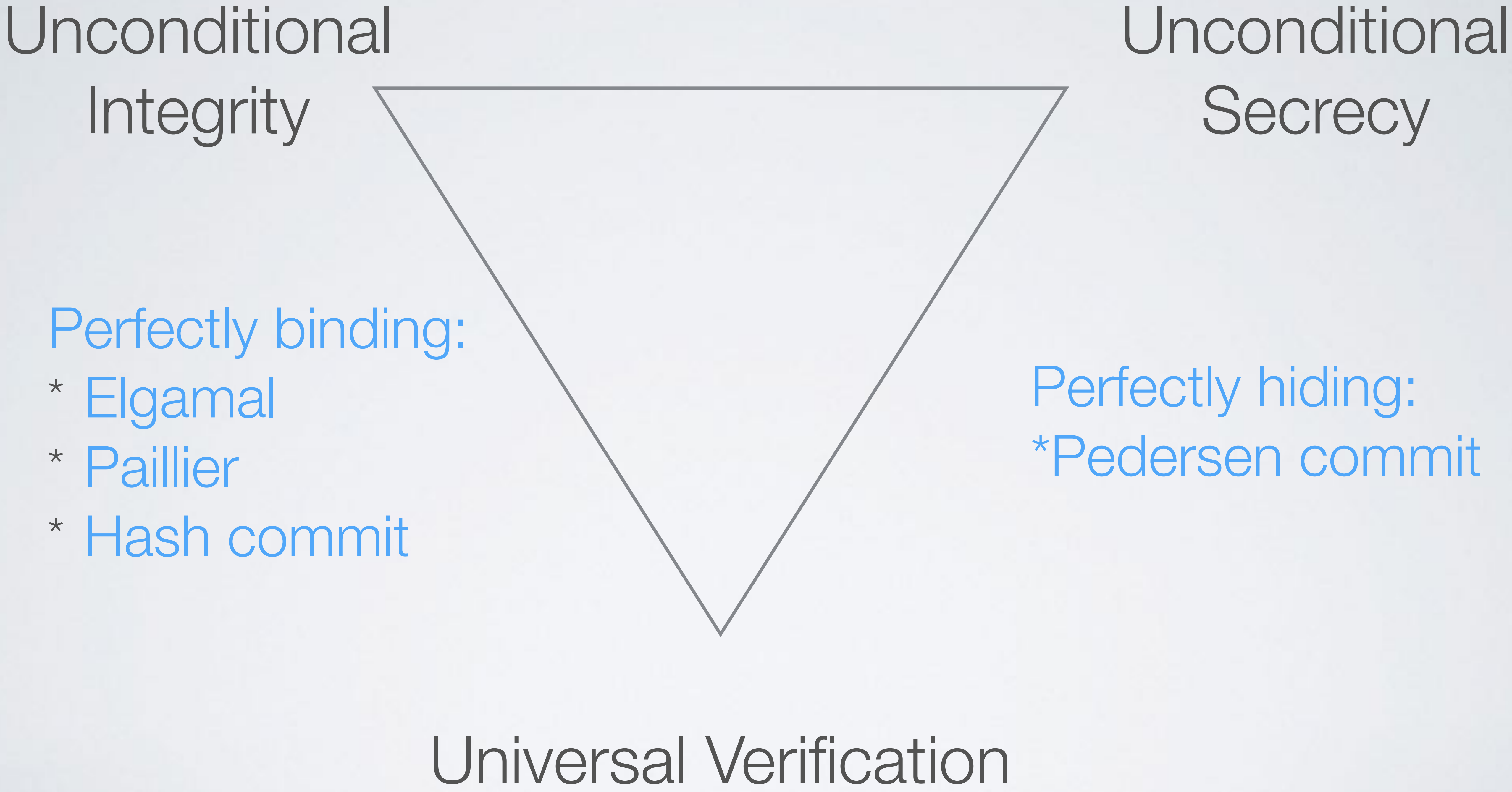


Unconditional Integrity

Unconditional Secrecy

Universal Verification

Vote Obfuscation



Unconditional Integrity

Unconditional Secrecy

Perfectly binding:

* Elgamal

* Paillier

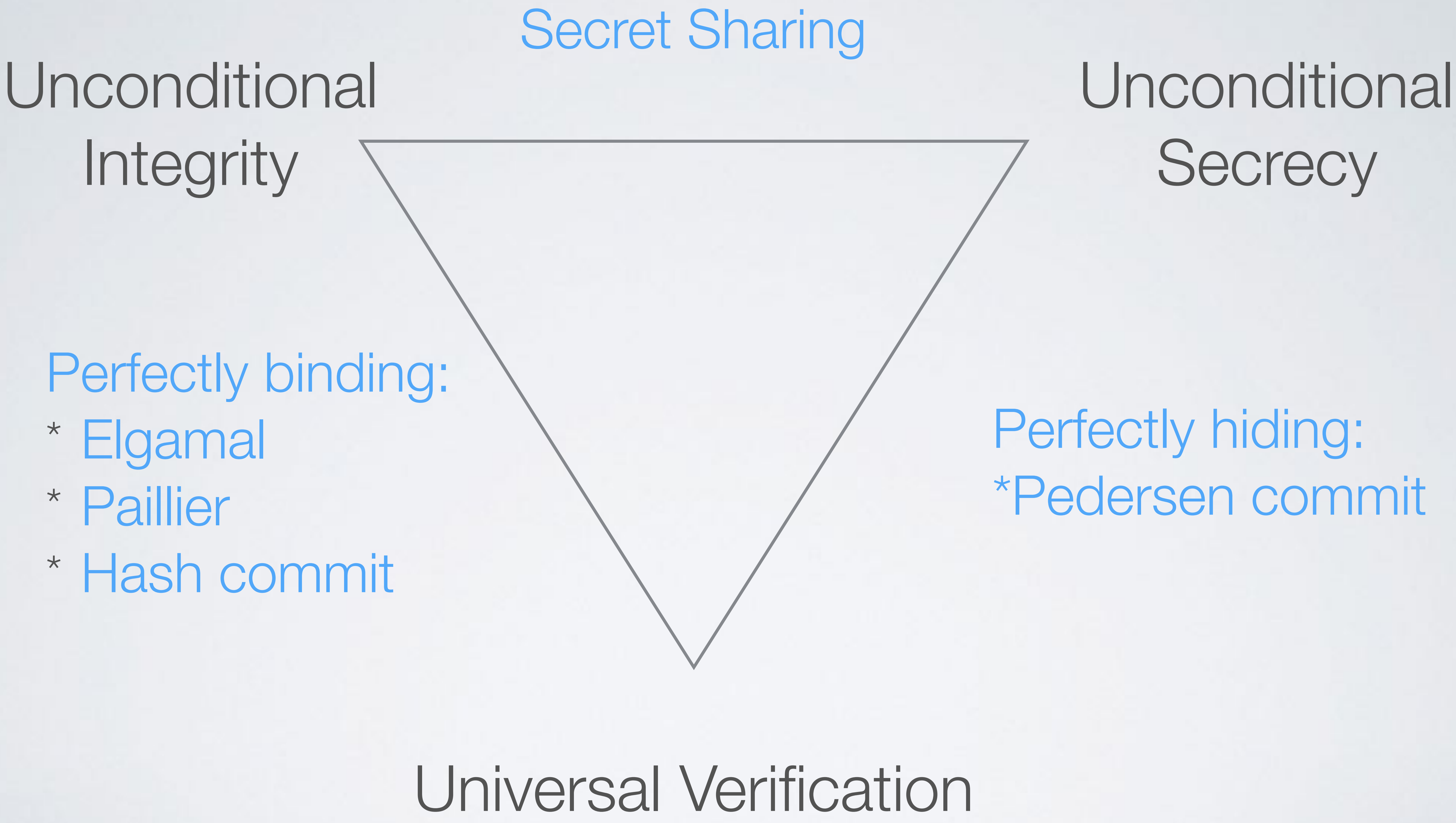
* Hash commit

Perfectly hiding:

*Pedersen commit

Universal Verification

Vote Obfuscation



Secret Sharing

Unconditional Integrity

Unconditional Secrecy

Perfectly binding:

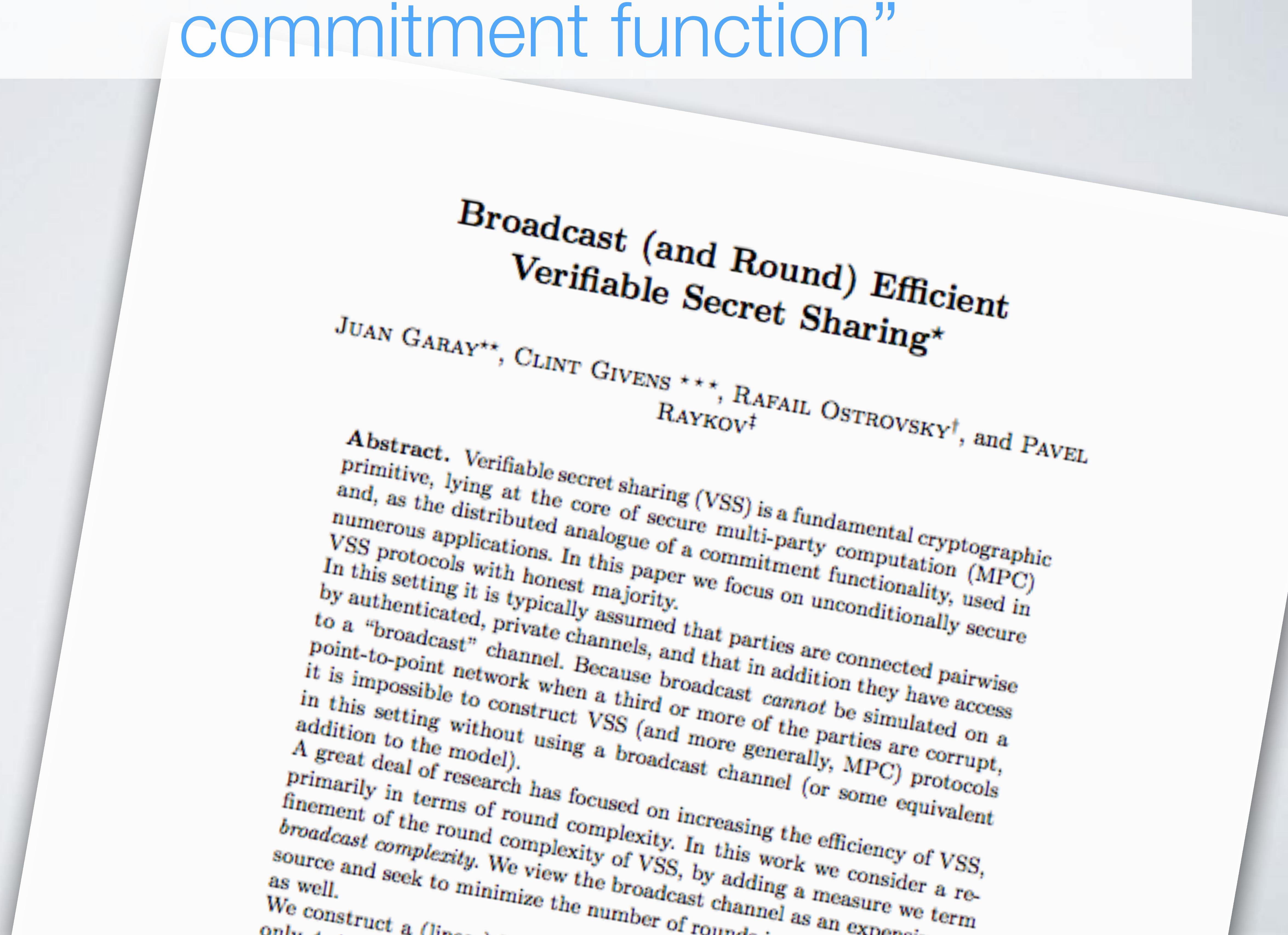
- Elgamal
- Paillier
- Hash commit

Perfectly hiding:

*Pedersen commit

Universal Verification

"VSS is… the distributed analogue of a commitment function"



Broadcast (and Round) Efficient Verifiable Secret Sharing[*]

Juan Garay[**], Clint Givens[***], Rafail Ostrovsky[†], and Pavel Raykov[‡]

Abstract. Verifiable secret sharing (VSS) is a fundamental cryptographic primitive, lying at the core of secure multi-party computation (MPC) and, as the distributed analogue of a commitment functionality, used in numerous applications. In this paper we focus on unconditionally secure VSS protocols with honest majority.

In this setting it is typically assumed that parties are connected pairwise by authenticated, private channels, and that in addition they have access to a "broadcast" channel. Because broadcast *cannot* be simulated on a point-to-point network when a third or more of the parties are corrupt, it is impossible to construct VSS (and more generally, MPC) protocols in this setting without using a broadcast channel (or some equivalent addition to the model).

A great deal of research has focused on increasing the efficiency of VSS, primarily in terms of round complexity. In this work we consider a refinement of the round complexity of VSS, by adding a measure we term *broadcast complexity*. We view the broadcast channel as an expensive resource and seek to minimize the number of rounds in which it is invoked as well.

We construct a

“VSS is… the distributed analogue of a commitment function”

Broadcast (and Round) Efficient Verifiable Secret Sharing*

Juan Garay, Clint Givens, and Pavel

Abstract. Verifiable secret sharing

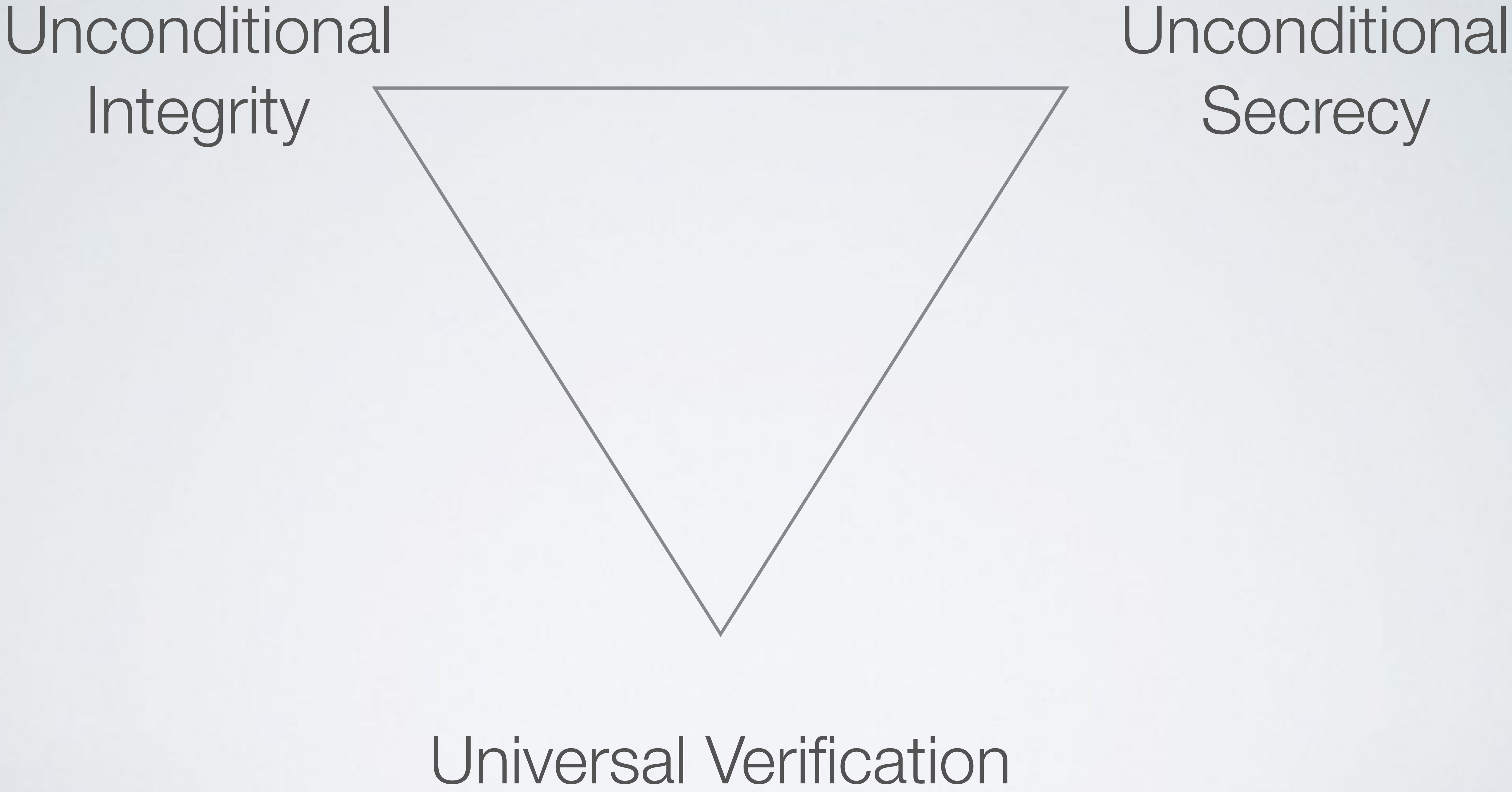
point-to-point" channel. Because broadcast *cannot* be simulated on a point-to-point network when a third or more of the parties are corrupt, it is impossible to construct VSS (and more generally, MPC) protocols in this setting without using a broadcast channel (or some equivalent addition to the model).

A great deal of research has focused on increasing the efficiency of VSS, primarily in terms of round complexity. In this work we consider a refinement of the round complexity of VSS, by adding a measure we term *broadcast complexity*. We view the broadcast channel as an expensive resource and seek to minimize the number of rounds in which it is invoked as well.

We construct a (linear)

Computationally it unconditionally secure (hiding and binding) however it requires an honest threshold of shareholders

Zero Knowledge

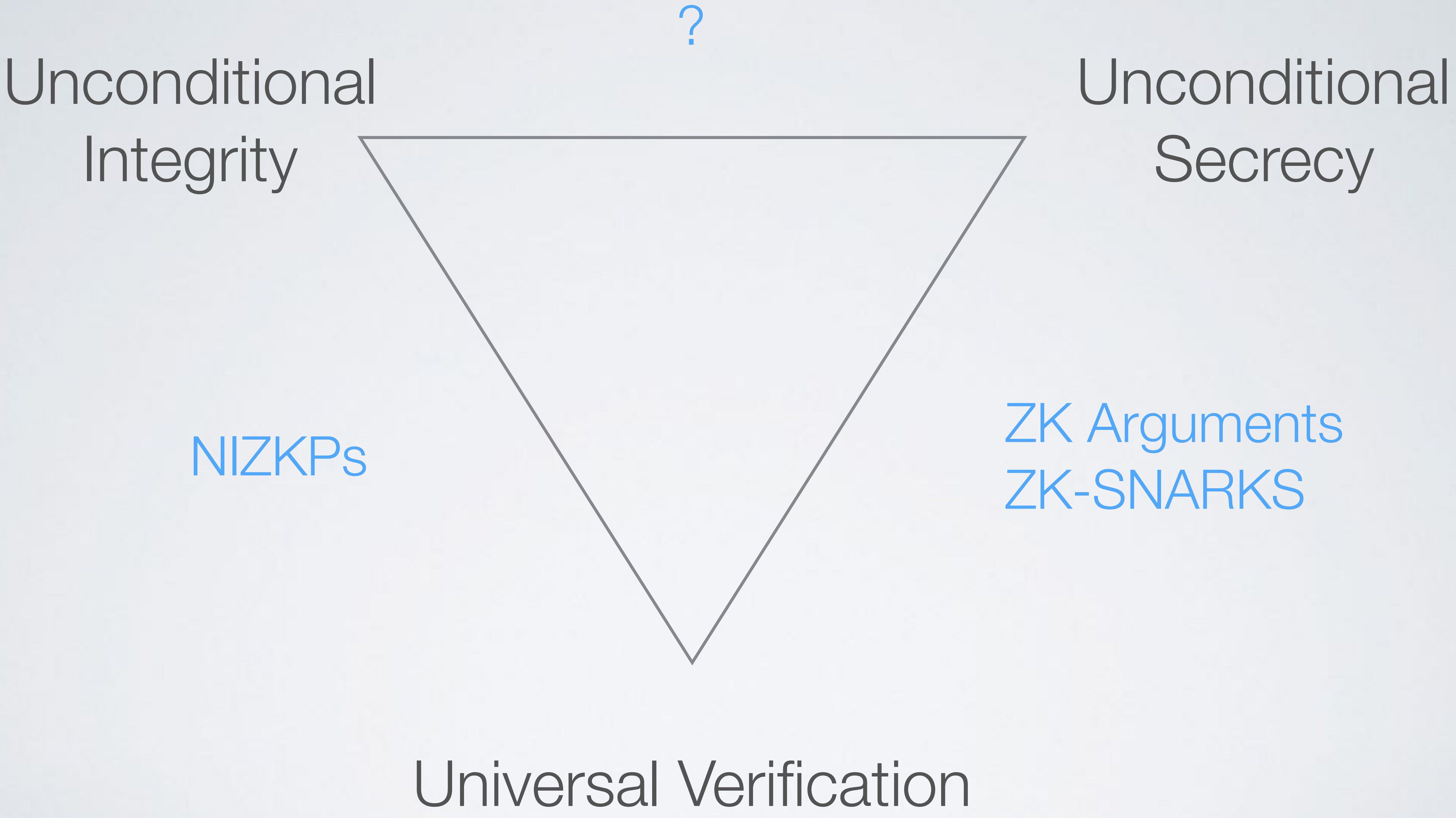


Unconditional Integrity

Unconditional Secrecy

Universal Verification

Zero Knowledge



?

Unconditional Integrity

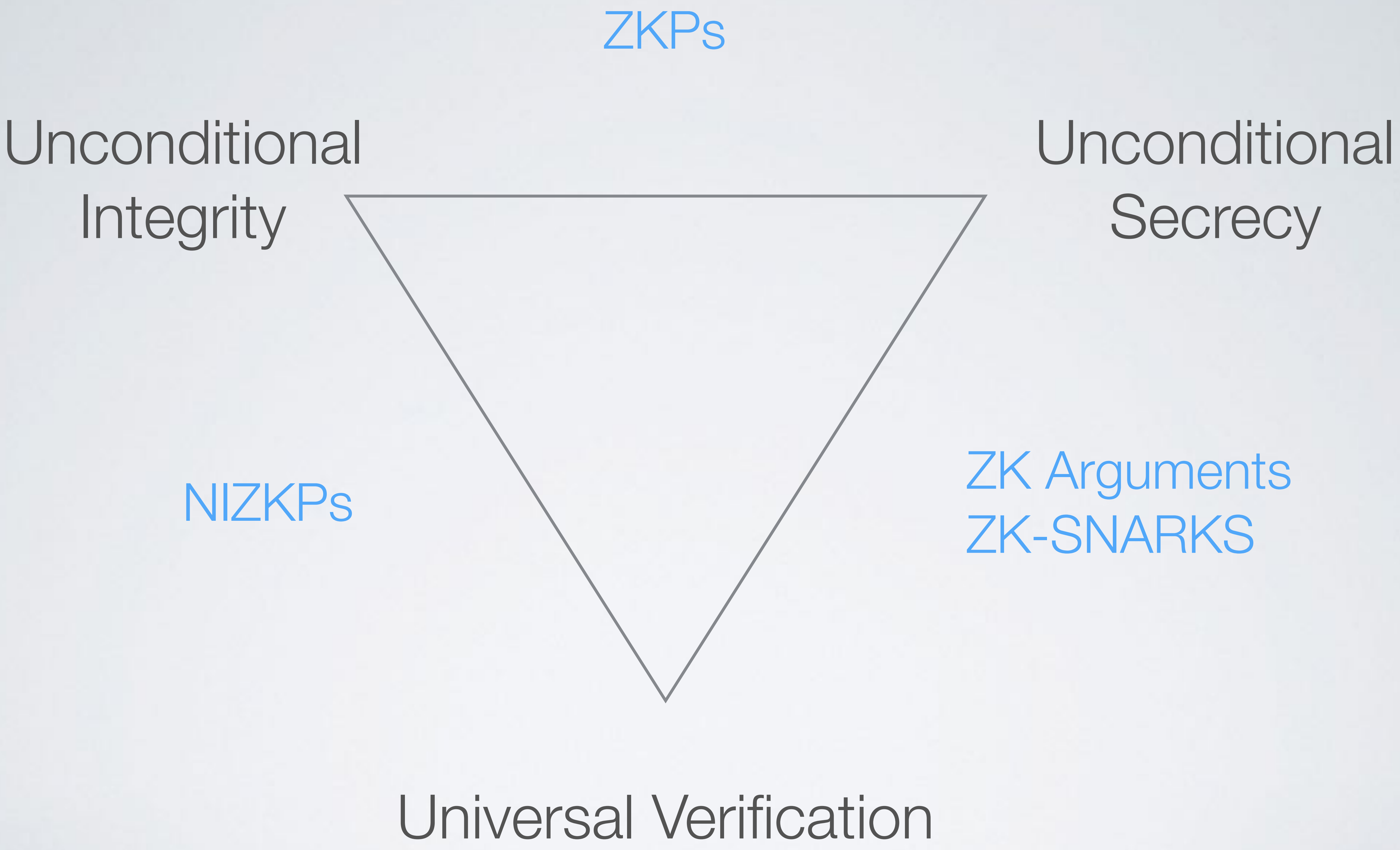
Unconditional Secrecy

NIZKPs

ZK Arguments
ZK-SNARKS

Universal Verification

Zero Knowledge



ZKPs

Unconditional Integrity

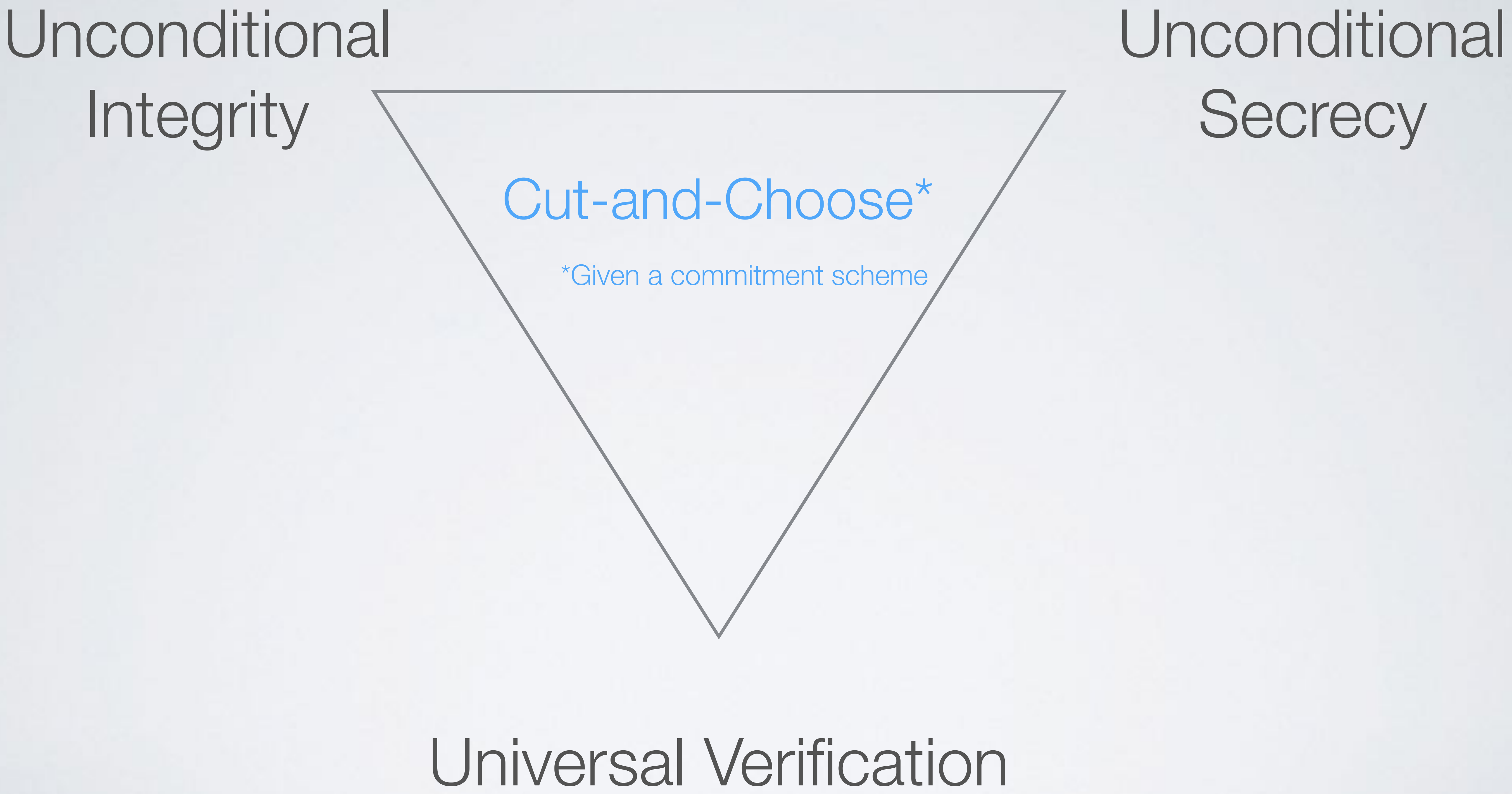
Unconditional Secrecy

NIZKPs

ZK Arguments
ZK-SNARKS

Universal Verification

Zero Knowledge



Unconditional Integrity

Unconditional Secrecy

Cut-and-Choose*

*Given a commitment scheme

Universal Verification

Wanted

Existing voting system:

* Only relies on commitments

* Uses cut-and-choose

* Human-votable paper (or untrusted DRE) ballots

* Voter not involved in tallying process

Wanted

Existing voting system:

* Only relies on commitments

* Uses cut-and-choose

* Human-votable paper (or untrusted DRE) ballots

* Voter not involved in tallying process

Possible!

* Punchscan

* Scantegrity

* Eperio (fast, easy, can do in a spreadsheet)

Wanted

Existing voting system:

* Only relies on commitments

* Uses cut-and-choose

* Human-votable paper (or untrusted DRE) ballots

* Voter not involved in tallying process

Possible!

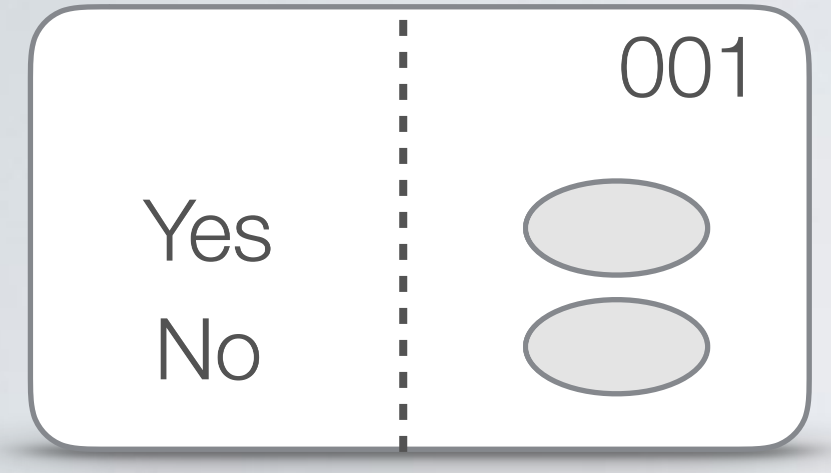
* Punchscan

* Scantegrity

* Eperio (fast, easy, can do in a spreadsheet)

The fine print

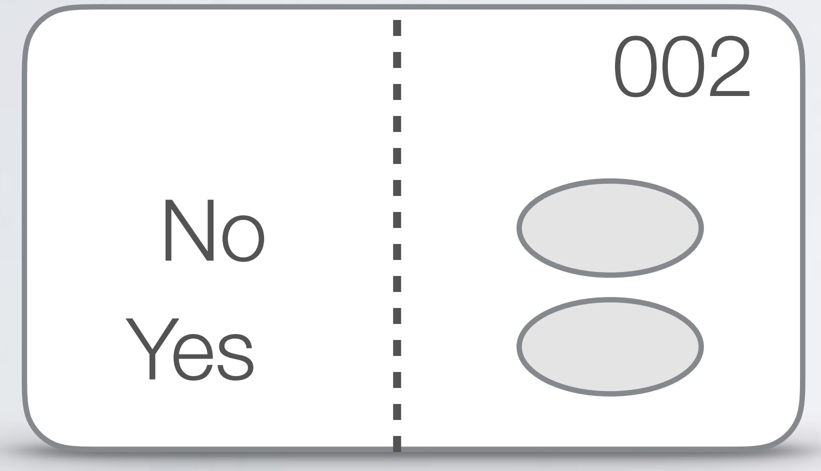
* Black box assumption



001

Yes ○

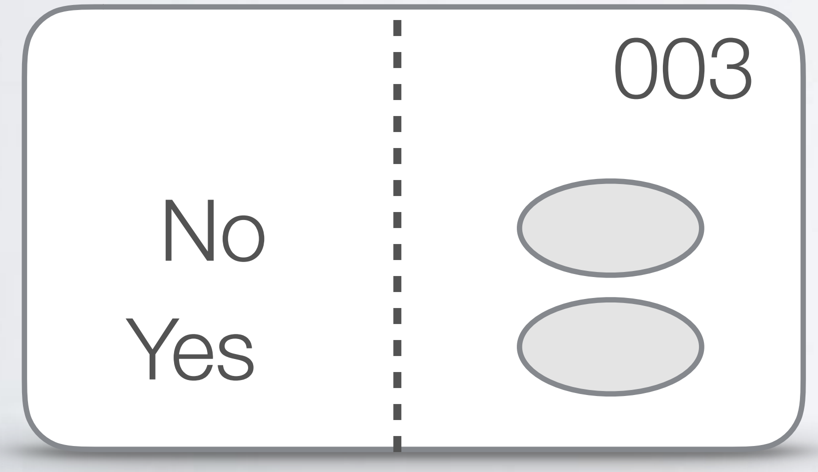
No ○



002

No ○

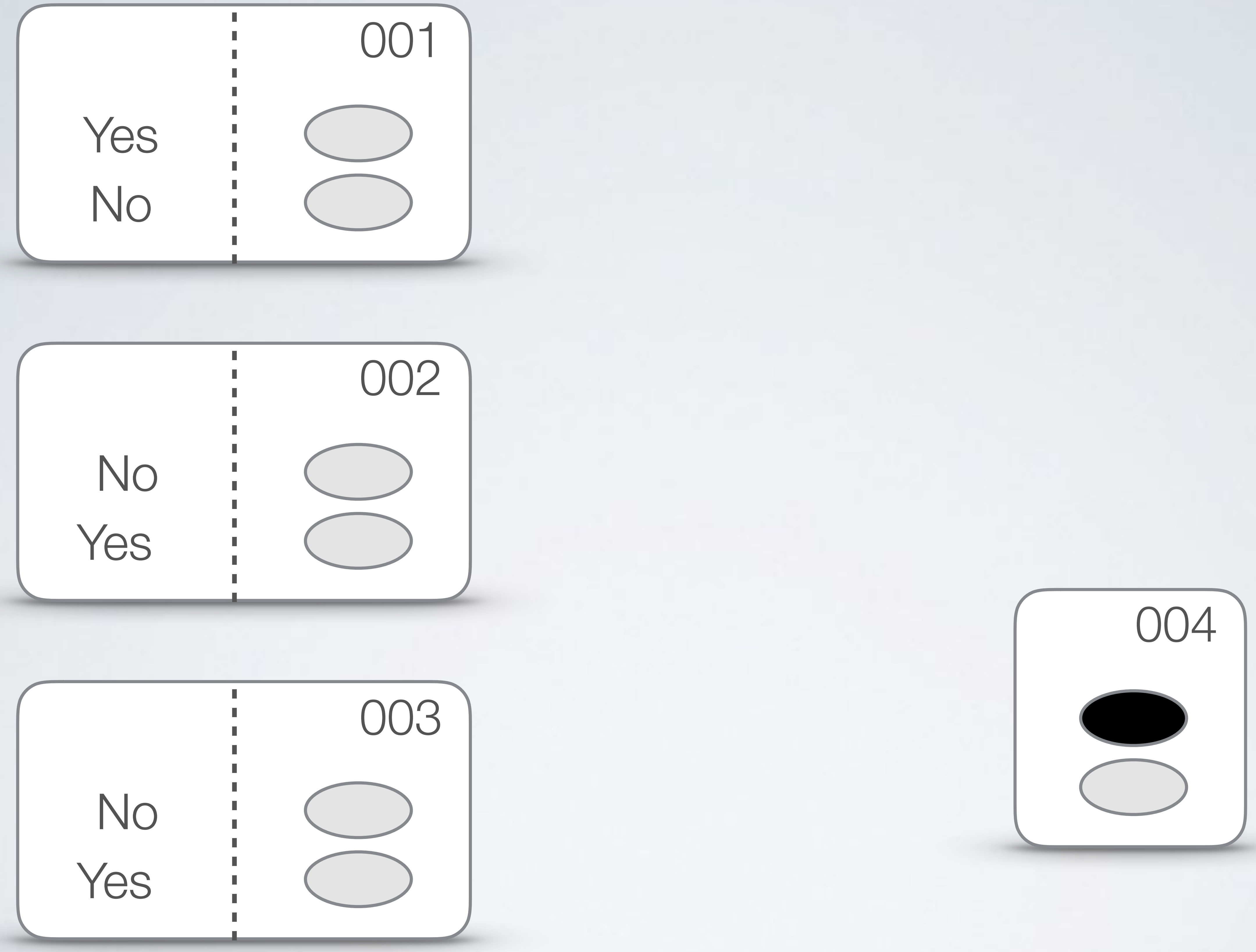
Yes ○



003

No ○

Yes ○



001

Yes ○

No ○

002

No ○

Yes ○

003

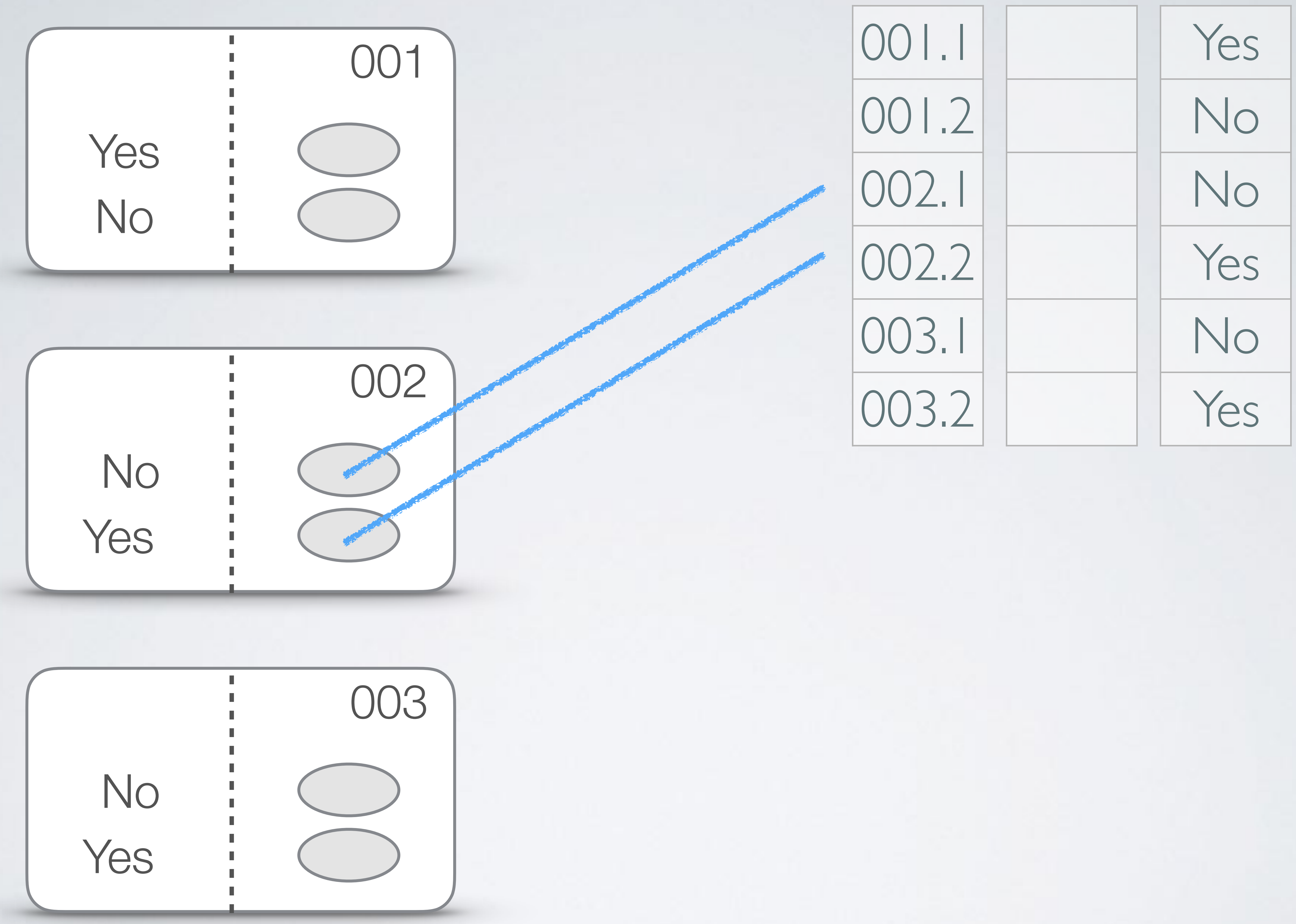
No ○

Yes ○

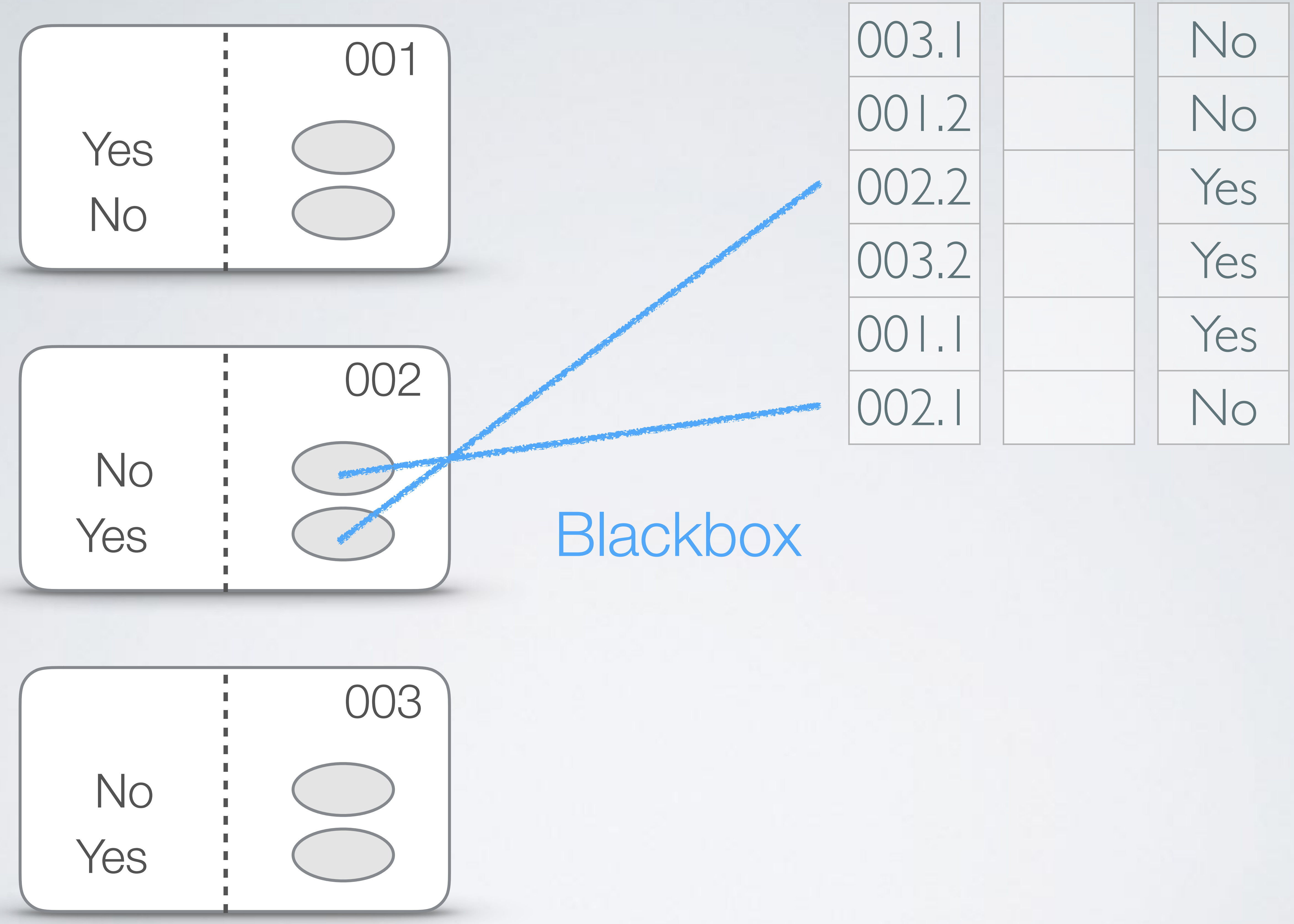
004

●

○



001.1		Yes
001.2		No
002.1		No
002.2		Yes
003.1		No
003.2		Yes



003.1		No
001.2		No
002.2		Yes
003.2		Yes
001.1		Yes
002.1		No

001

Yes ○
No ○

002

No ○
Yes ○

003

No ○
Yes ○

003.1		No
001.2		No
002.2		Yes
003.2		Yes
001.1		Yes
002.1		No

002.2		Yes
002.1		No
001.2		No
003.2		Yes
001.1		Yes
003.1		No

001

Yes ○
No ○

002

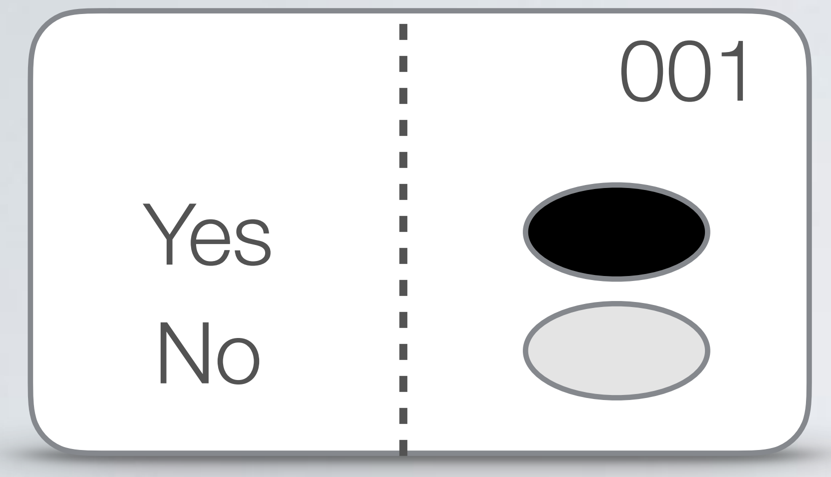
No ○
Yes ○

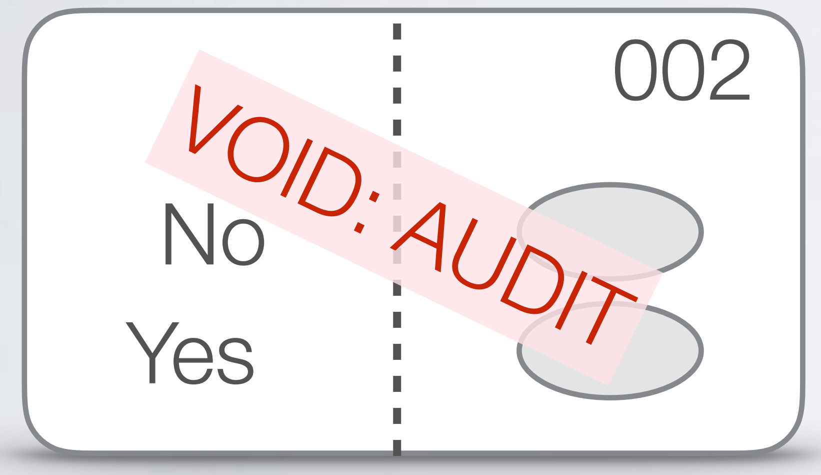
003

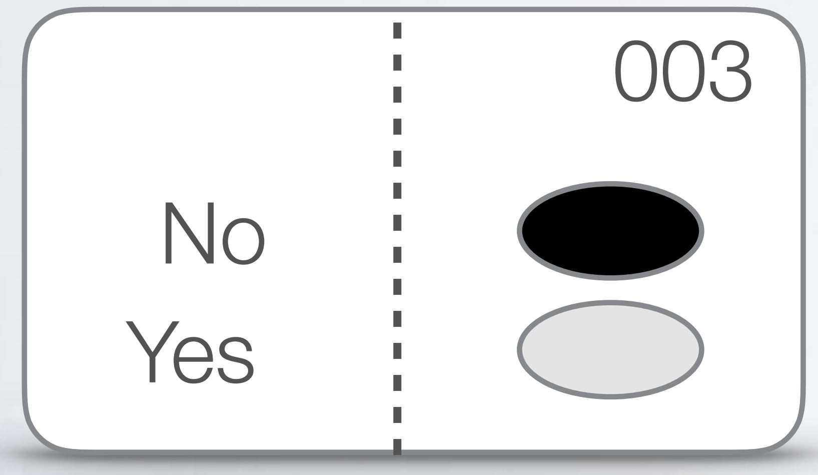
No ○
Yes ○

003.1		No
001.2		No
002.2		Yes
003.2		Yes
001.1		Yes
002.1		No

002.2		Yes
002.1		No
001.2		No
003.2		Yes
001.1		Yes
003.1		No

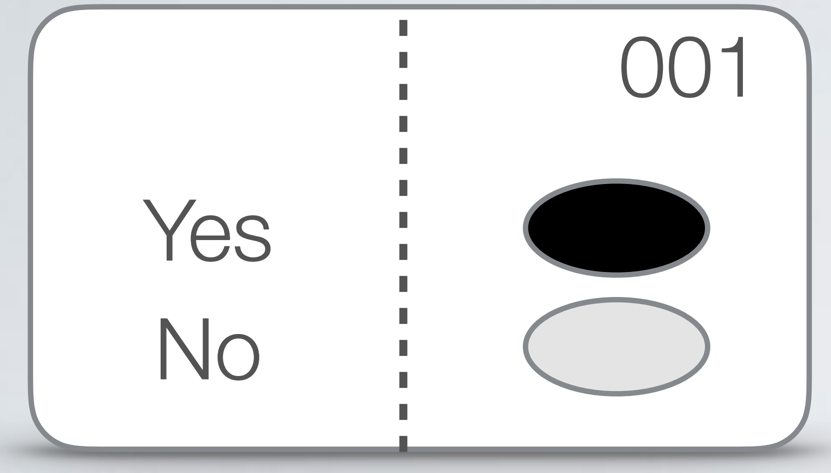






003.1		No
001.2		No
002.2		Yes
003.2		Yes
001.1		Yes
002.1		No

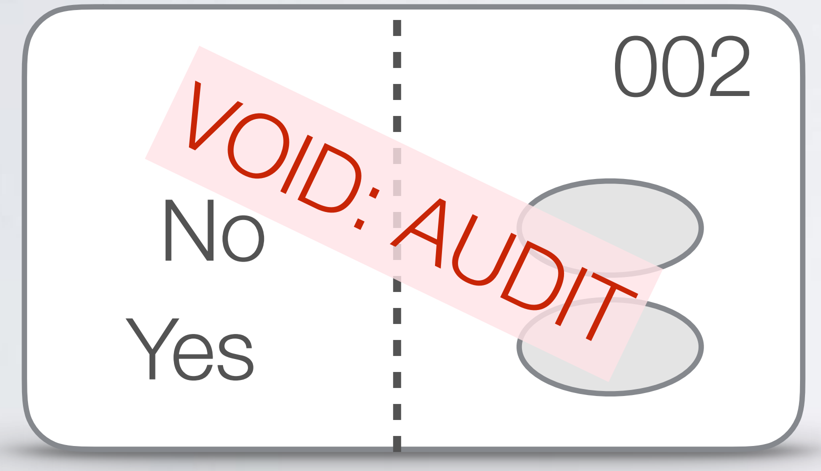
002.2		Yes
002.1		No
001.2		No
003.2		Yes
001.1		Yes
003.1		No



001

Yes ●

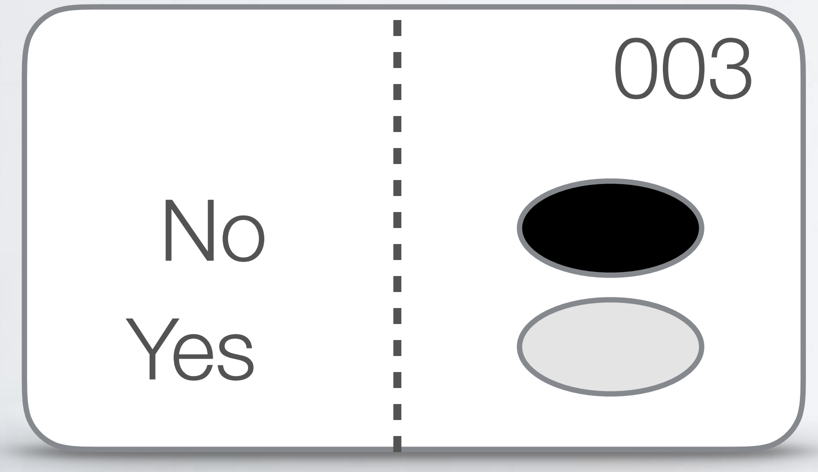
No ○



002

No ○

Yes ○



003

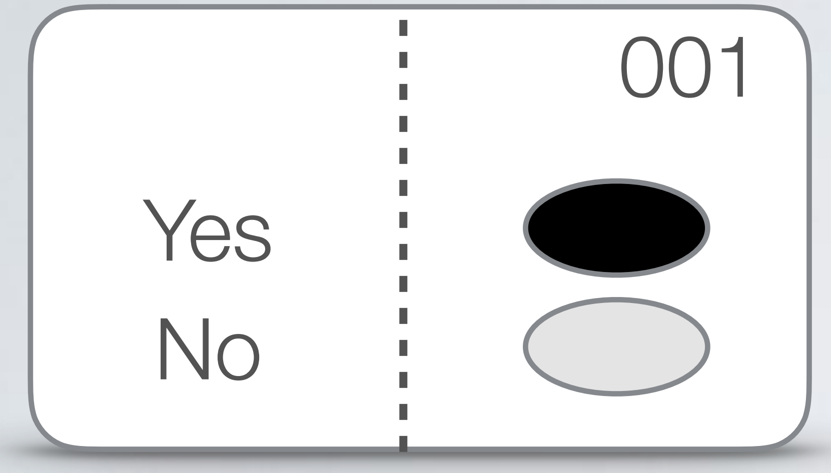
No ●

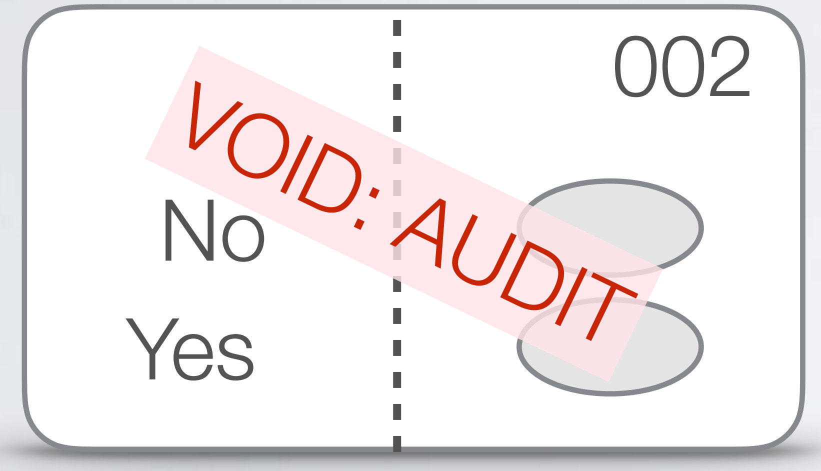
Yes ○

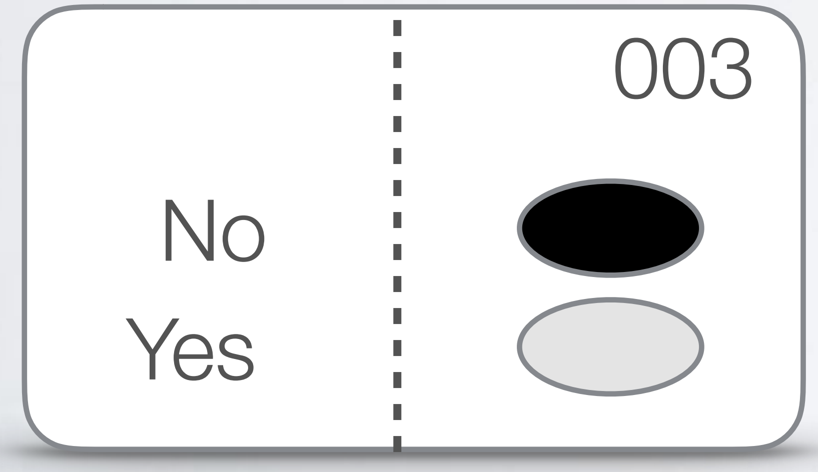
003.1	✓	No
001.2		No
002.2		Yes
003.2		Yes
001.1	✓	Yes
002.1		No

002.2		Yes
002.1		No
001.2		No
003.2		Yes
001.1	✓	Yes
003.1	✓	No

001
Yes
No
VOID: AUD
No
Yes
No
Yes
003.1
✓
No
001.2
No
002.2
Yes
2
Yes
✓
Yes
No
Yes
No
No
2
Yes
001.1
✓
Yes
003.1
✓
No

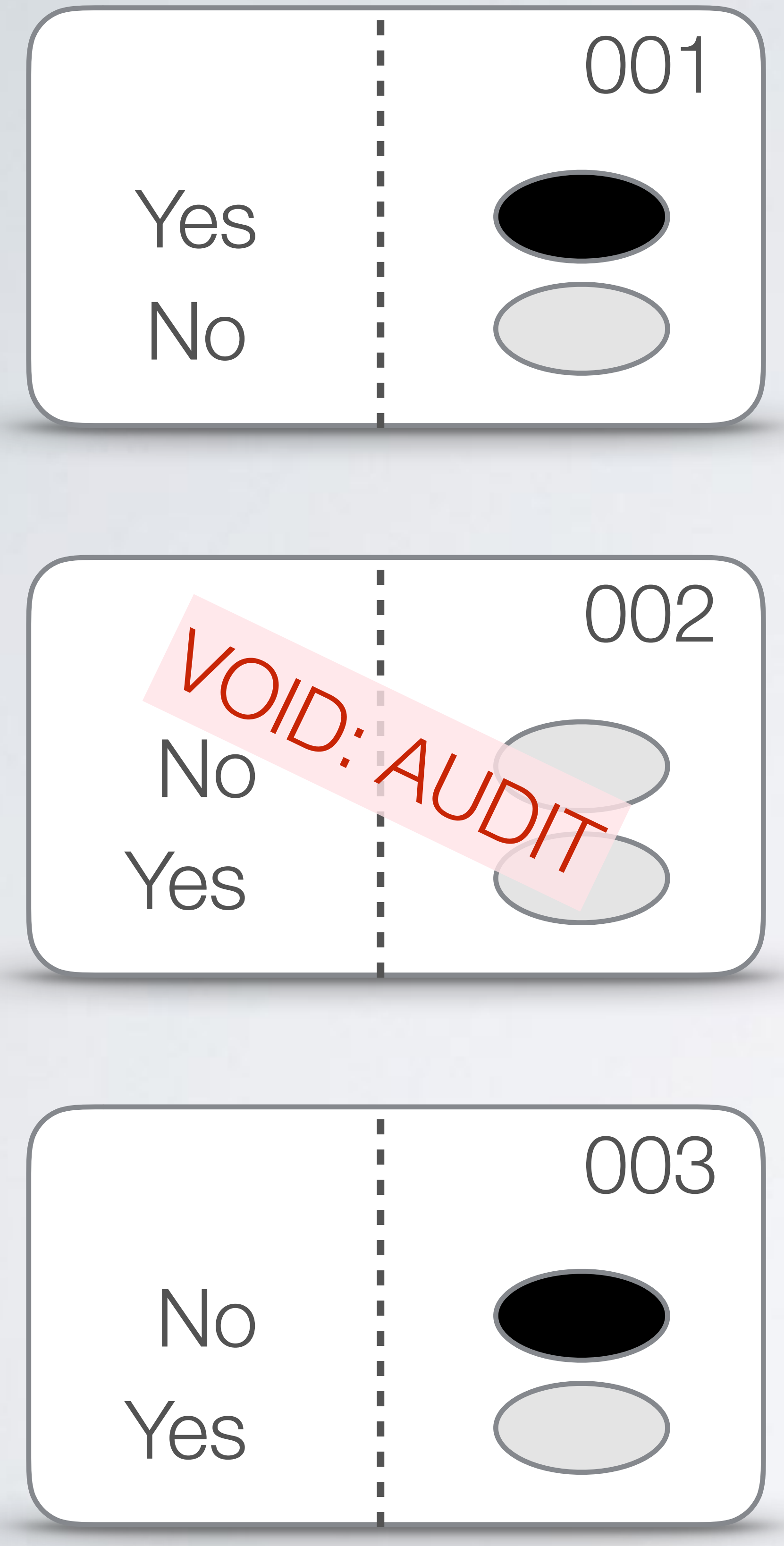






003.1	✓	No
001.2		No
002.2		Yes
003.2		Yes
001.1	✓	Yes
002.1		No

002.2		Yes
002.1		No
001.2		No
003.2		Yes
001.1	✓	Yes
003.1	✓	No



001

Yes ●

No ○

002

VOID: AUDIT

No ○

Yes ○

003

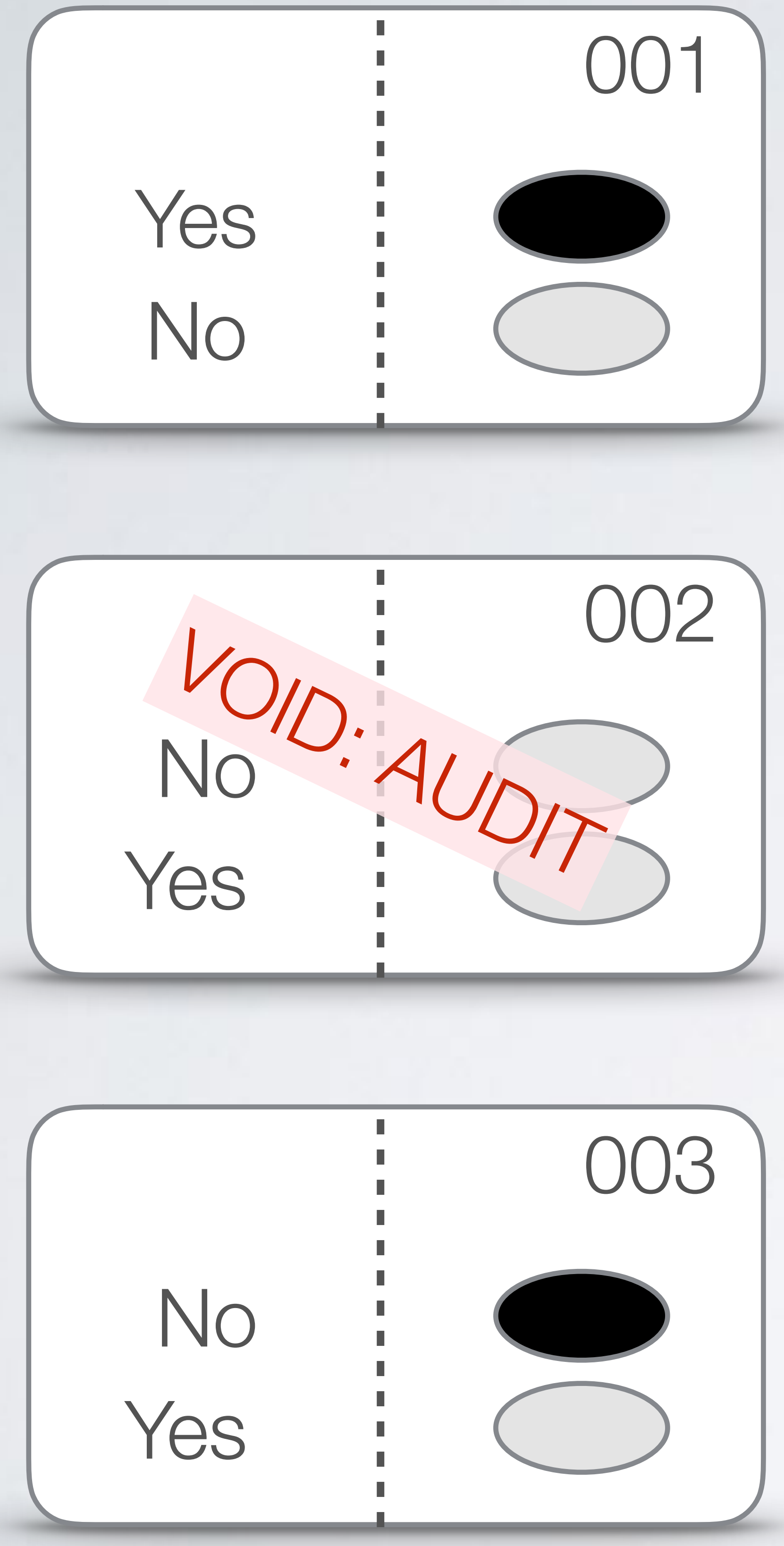
No ●

Yes ○

Honest Quorum

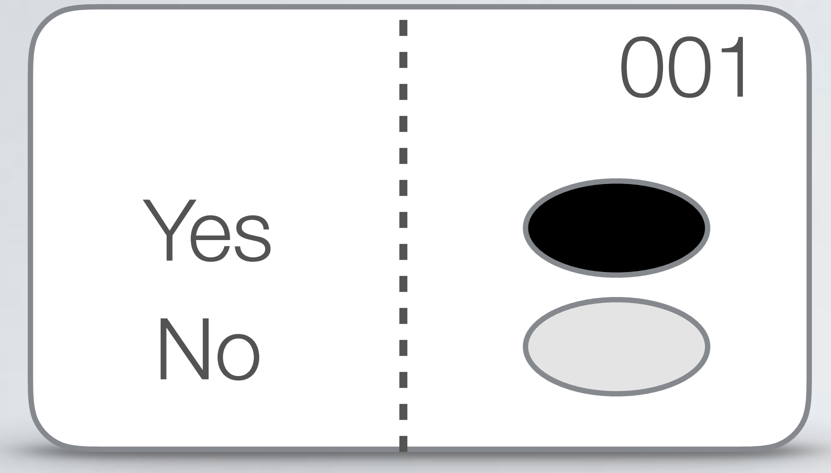
003.1	✓	No
001.2		No
002.2		Yes
003.2		Yes
001.1	✓	Yes
002.1		No

002.2		Yes
002.1		No
001.2		No
003.2		Yes
001.1	✓	Yes
003.1	✓	No



003.1	✓	No
001.2		No
002.2		Yes
003.2		Yes
001.1	✓	Yes
002.1		No

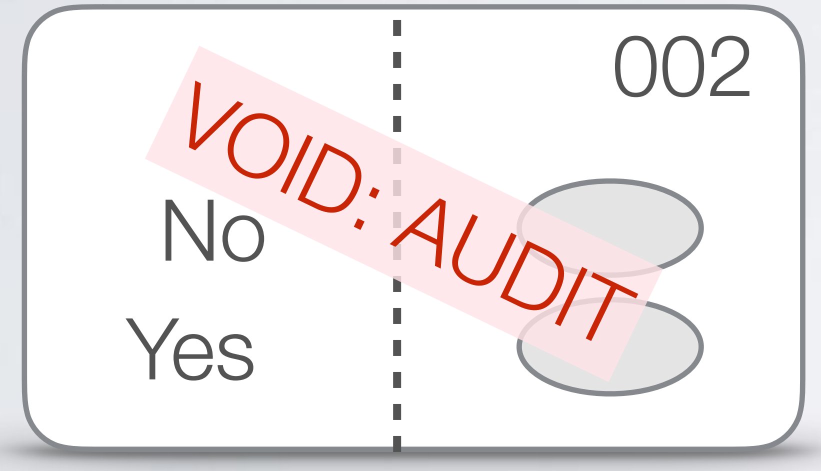
002.2		Yes
002.1		No
001.2		No
003.2		Yes
001.1	✓	Yes
003.1	✓	No



001

Yes ●

No ○

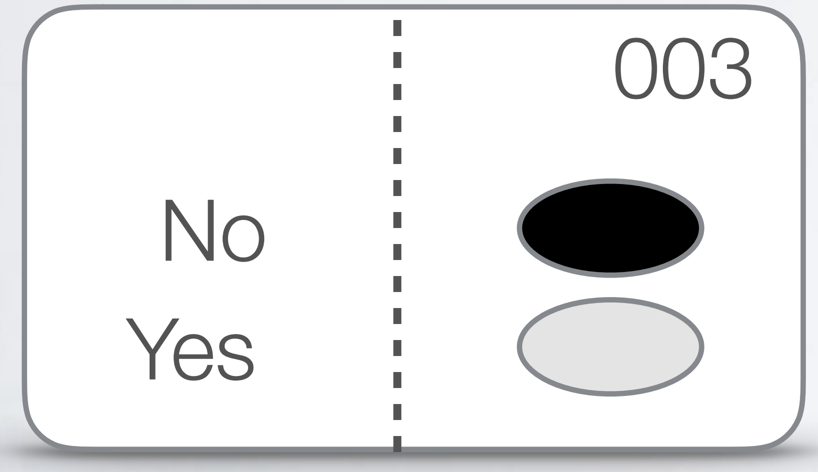


002

VOID: AUDIT

No ○

Yes ○



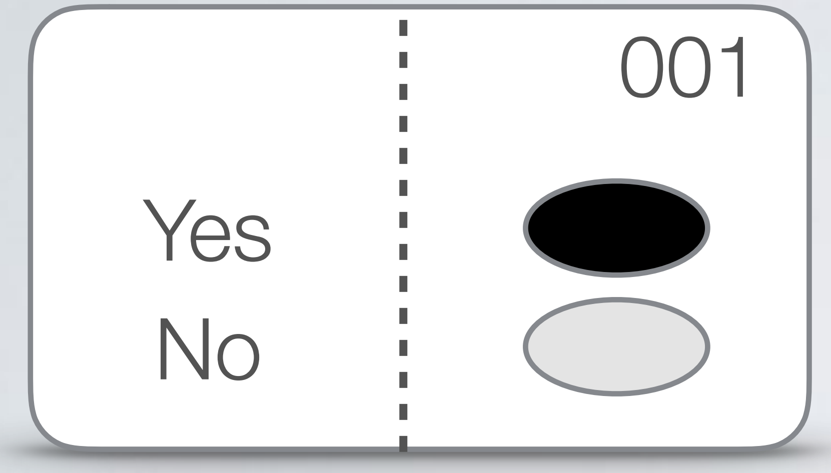
003

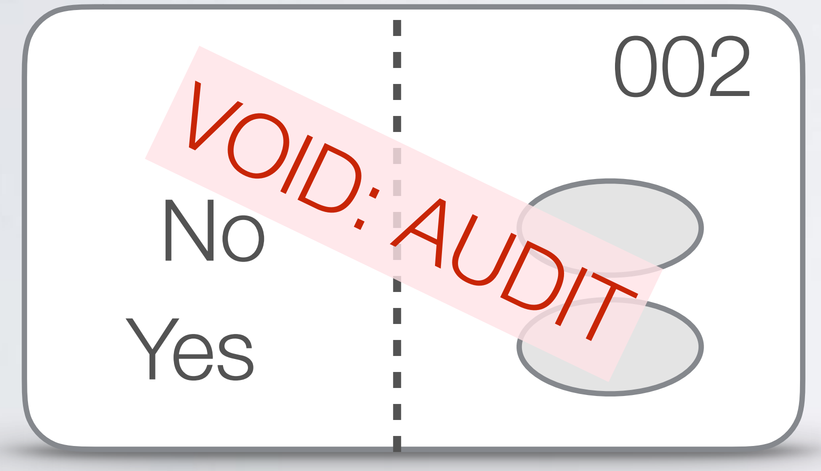
No ●

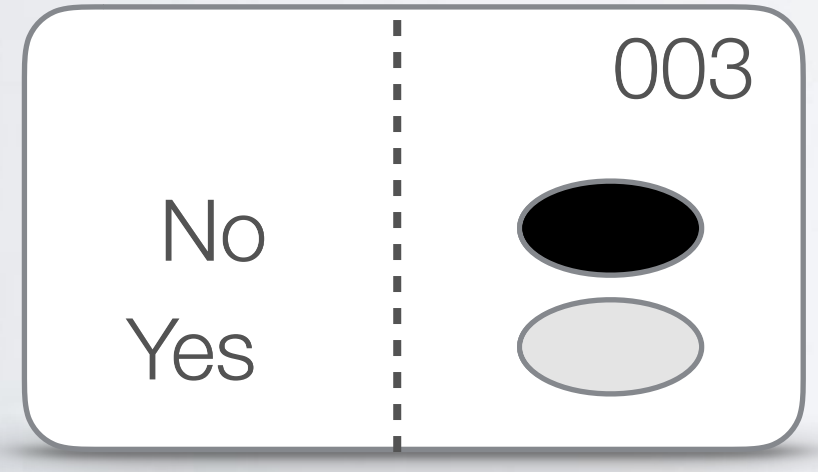
Yes ○

003.1	✓	No
001.2		No
002.2	|←→|	Yes
003.2		Yes
001.1	✓	Yes
002.1	|←→|	No

002.2	|←→|	Yes
002.1	|←→|	No
001.2		No
003.2		Yes
001.1	✓	Yes
003.1	✓	No



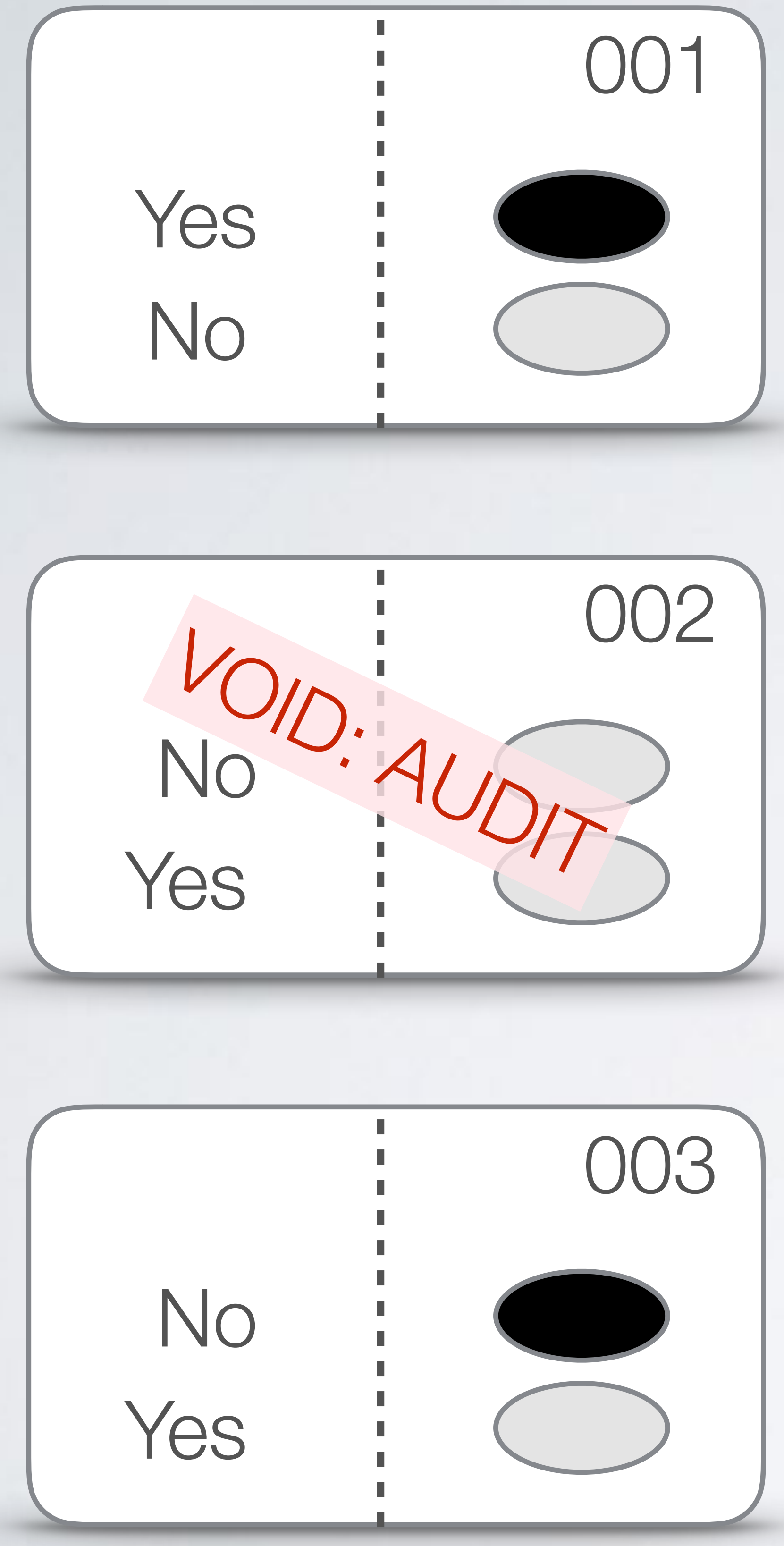




Corrupt

003.1	✓	No
001.2		No
002.2	⇤ ⇥	Yes
003.2		Yes
001.1	✓	Yes
002.1	⇤ ⇥	No

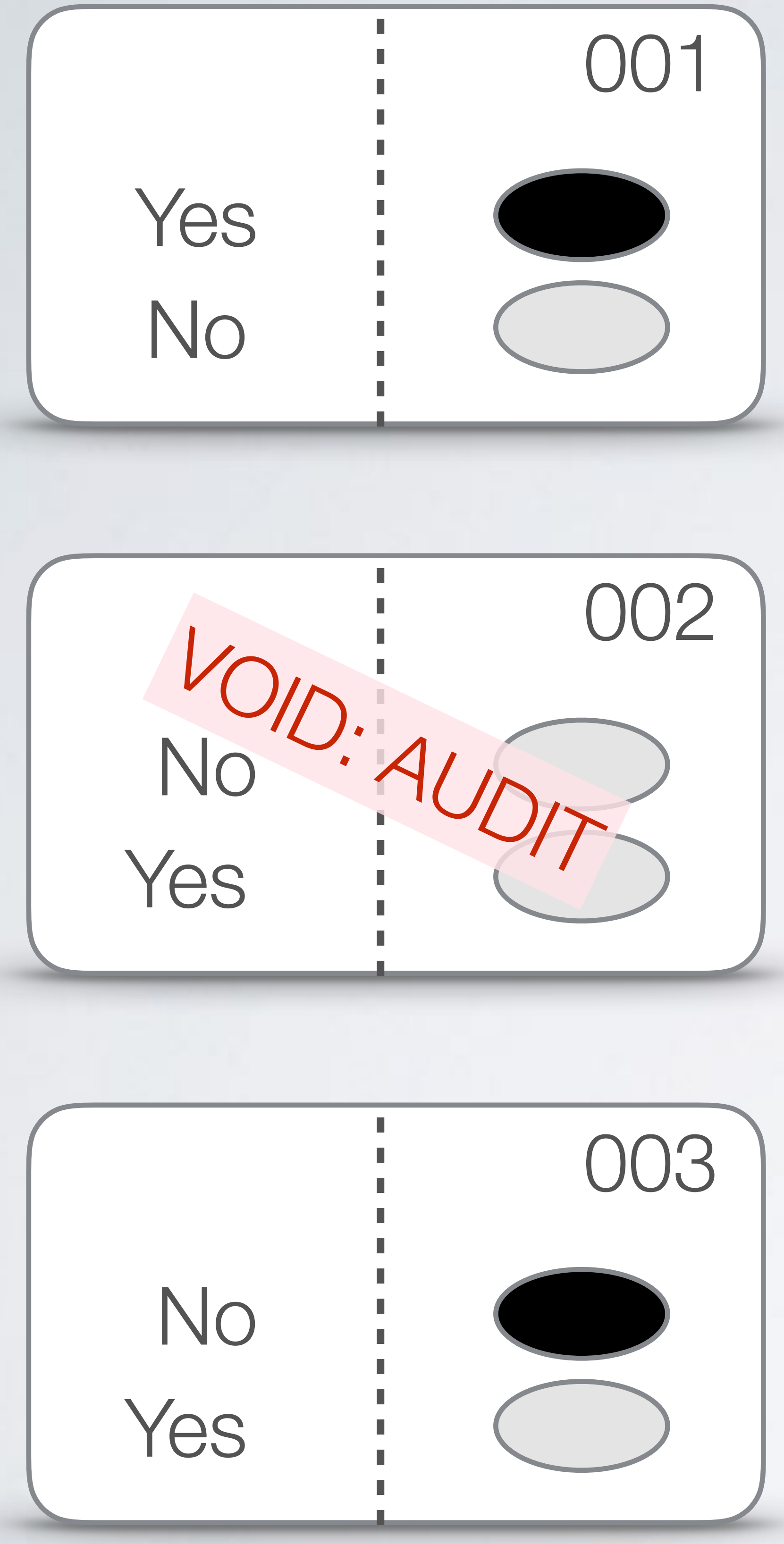
002.2	⇤ ⇥	Yes
002.1	⇤ ⇥	No
001.2		No
003.2		Yes
001.1	✓	Yes
003.1	✓	No



Corrupt

003.1	✓	No
001.2		No
002.2	⇤⇥	Yes
003.2		Yes
001.1	✓	Yes
002.1	⇤⇥	No

002.2	⇤⇥	Yes
002.1	⇤⇥	No
001.2		No
003.2		Yes
001.1	✓	Yes
003.1	✓	No

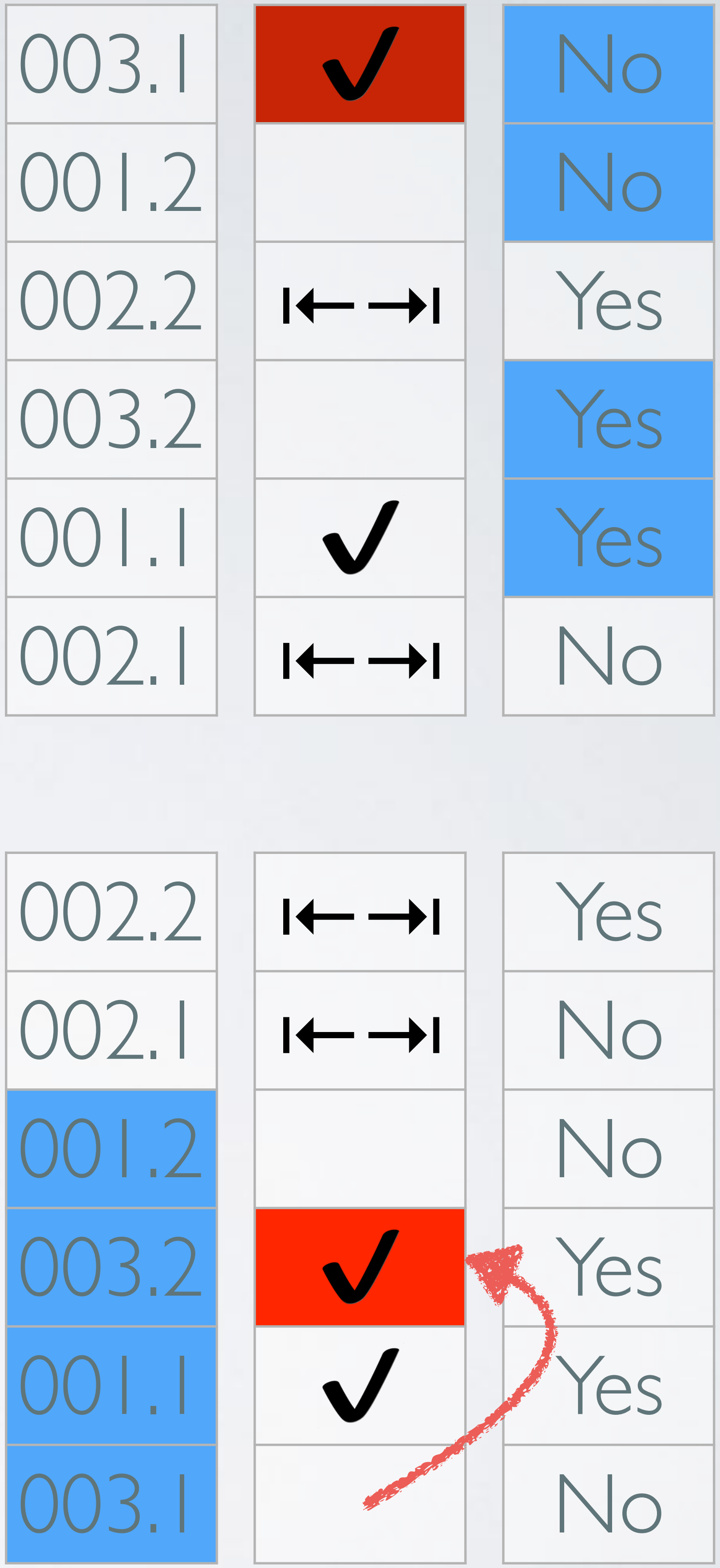


Corrupt

003.1	✓	No
001.2		No
002.2	⇤⇥	Yes
003.2		Yes
001.1	✓	Yes
002.1	⇤⇥	No

002.2	⇤⇥	Yes
002.1	⇤⇥	No
001.2		No
003.2	✓	Yes
001.1	✓	Yes
003.1		No

Pr[Detect]
= 1-2^t
= 99.9999% (t=20)



003.1	✓	No
001.2		No
002.2	⇤ ⇥	Yes
003.2		Yes
001.1	✓	Yes
002.1	⇤ ⇥	No

002.2	⇤ ⇥	Yes
002.1	⇤ ⇥	No
001.2		No
003.2	✓	Yes
001.1	✓	Yes
003.1		No

Universal Verification

Should we care?

- No: we already make collusion assumptions about election officials, so why not about verification?
- No: breaking integrity is zero-sum for the parties, but breaking privacy might not be
- Yes: auditing should be open to all, even non-voters
- Yes: the trustworthiness of auditing should not rely on whether I trust a preselected set of entities or not

Questions?

@PulpSpy http://vaddr.space