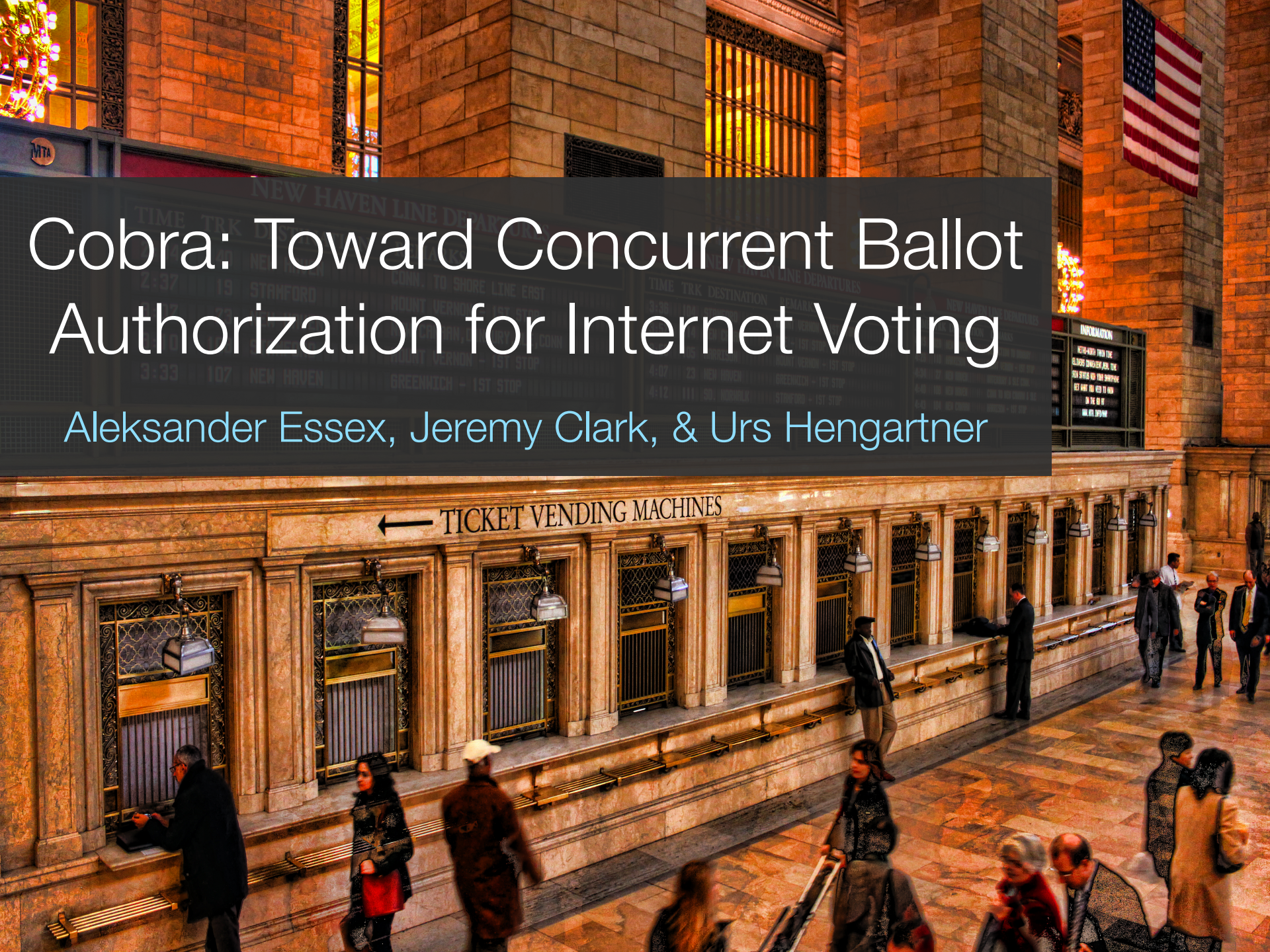
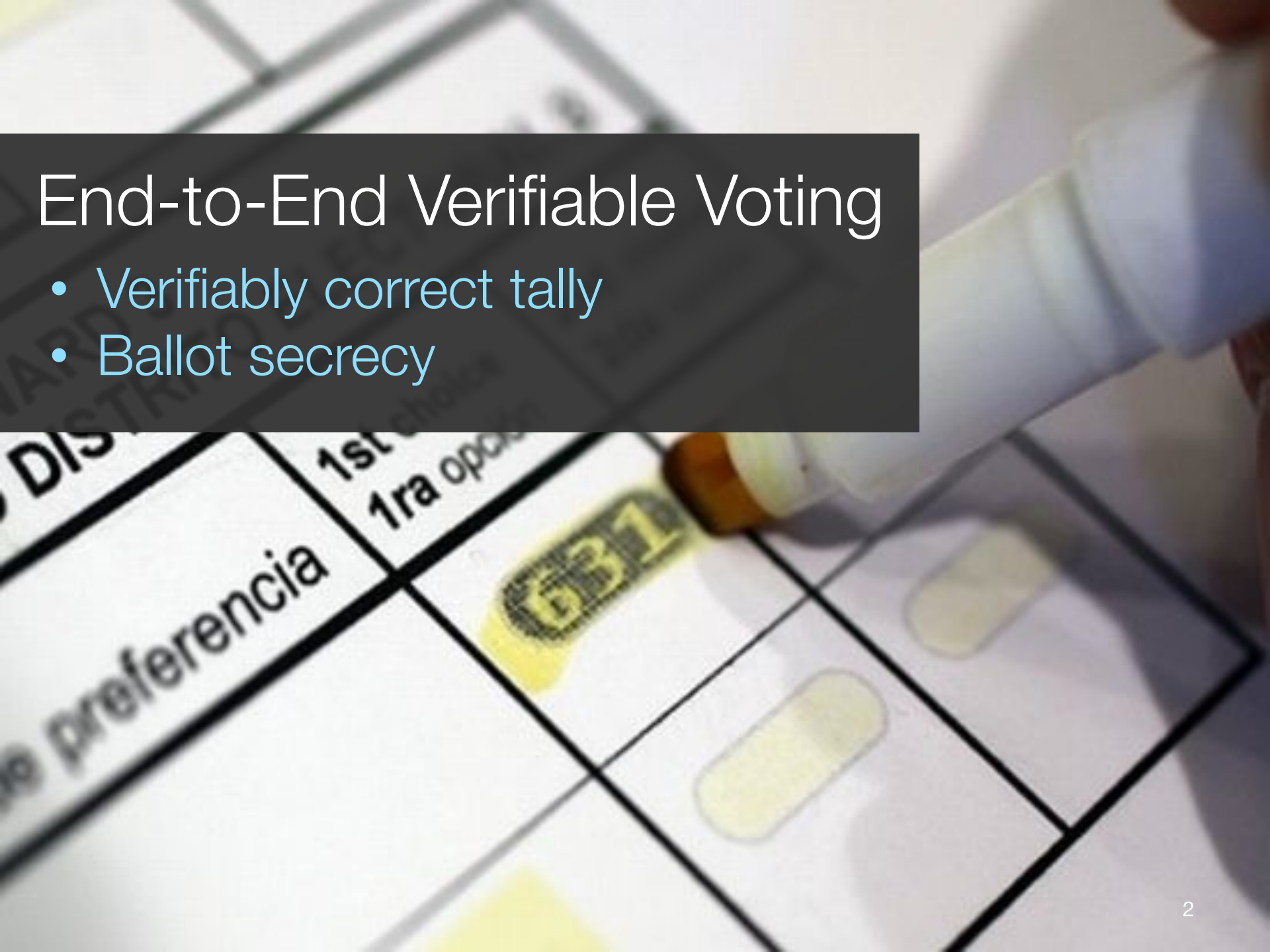
Cobra: Toward Concurrent Ballot Authorization for Internet Voting

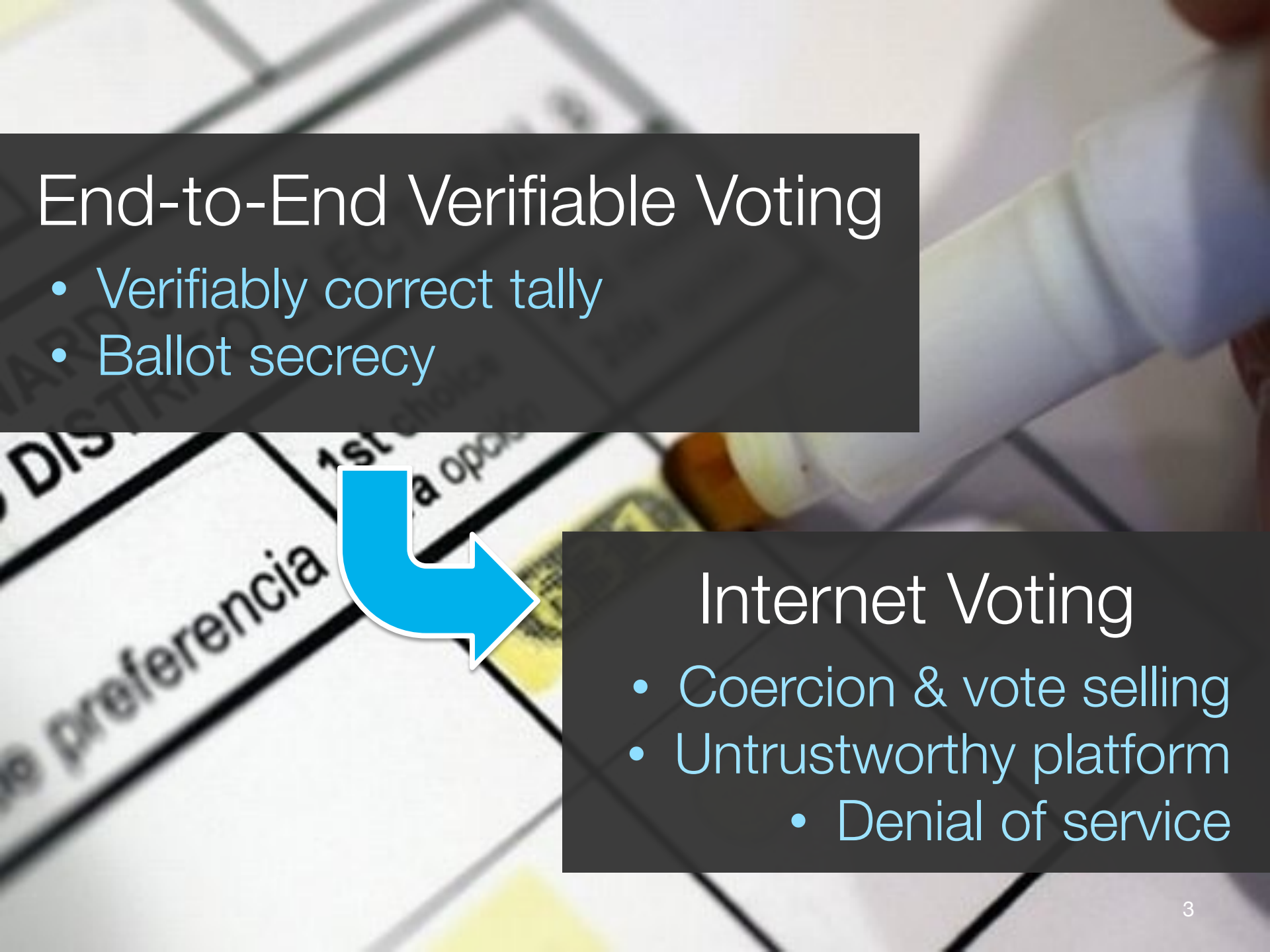
Aleksander Essex, Jeremy Clark, & Urs Hengartner





End-to-End Verifiable Voting

- Verifiably correct tally
- Ballot secrecy



End-to-End Verifiable Voting

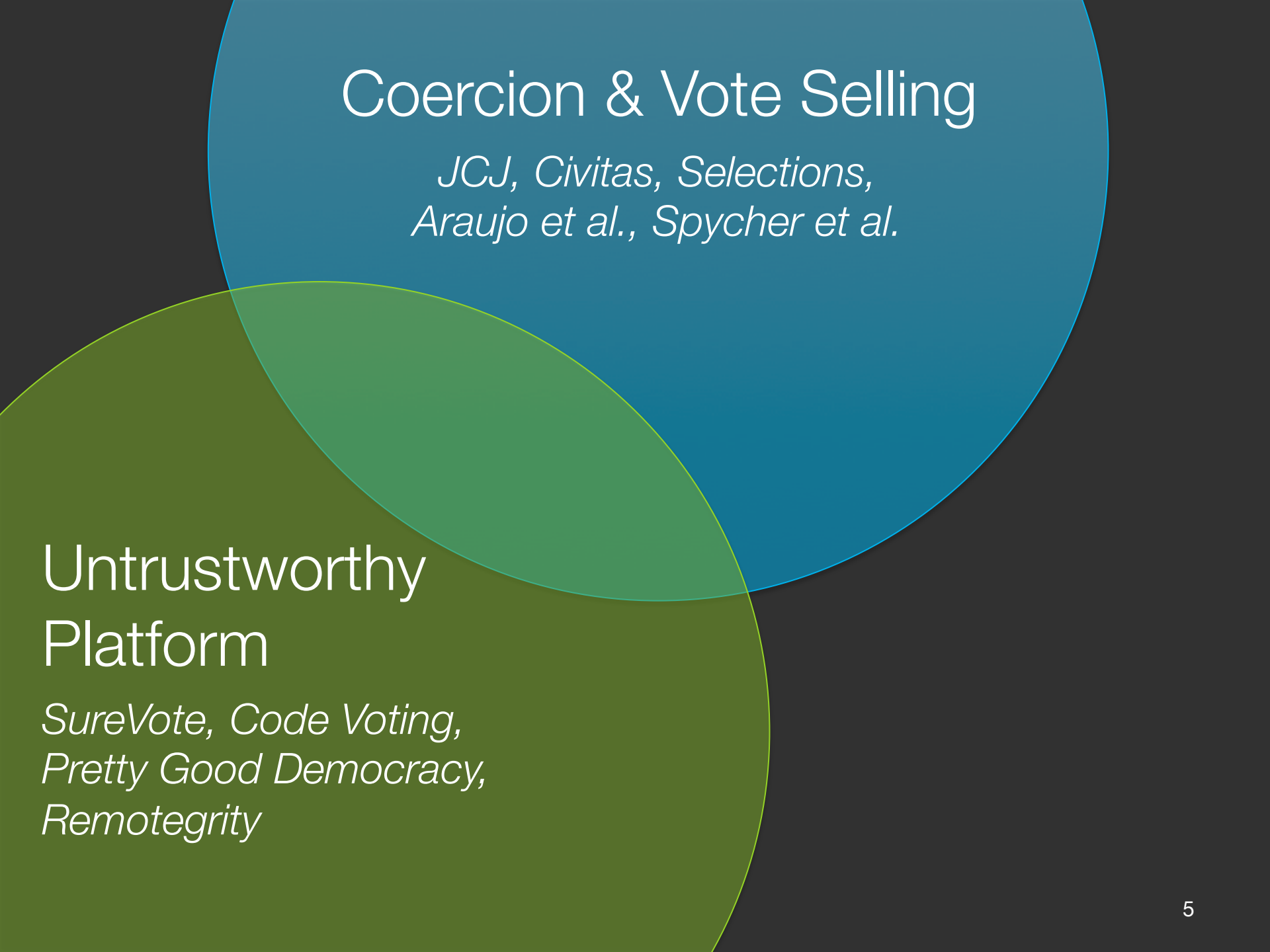
- Verifiably correct tally
- Ballot secrecy

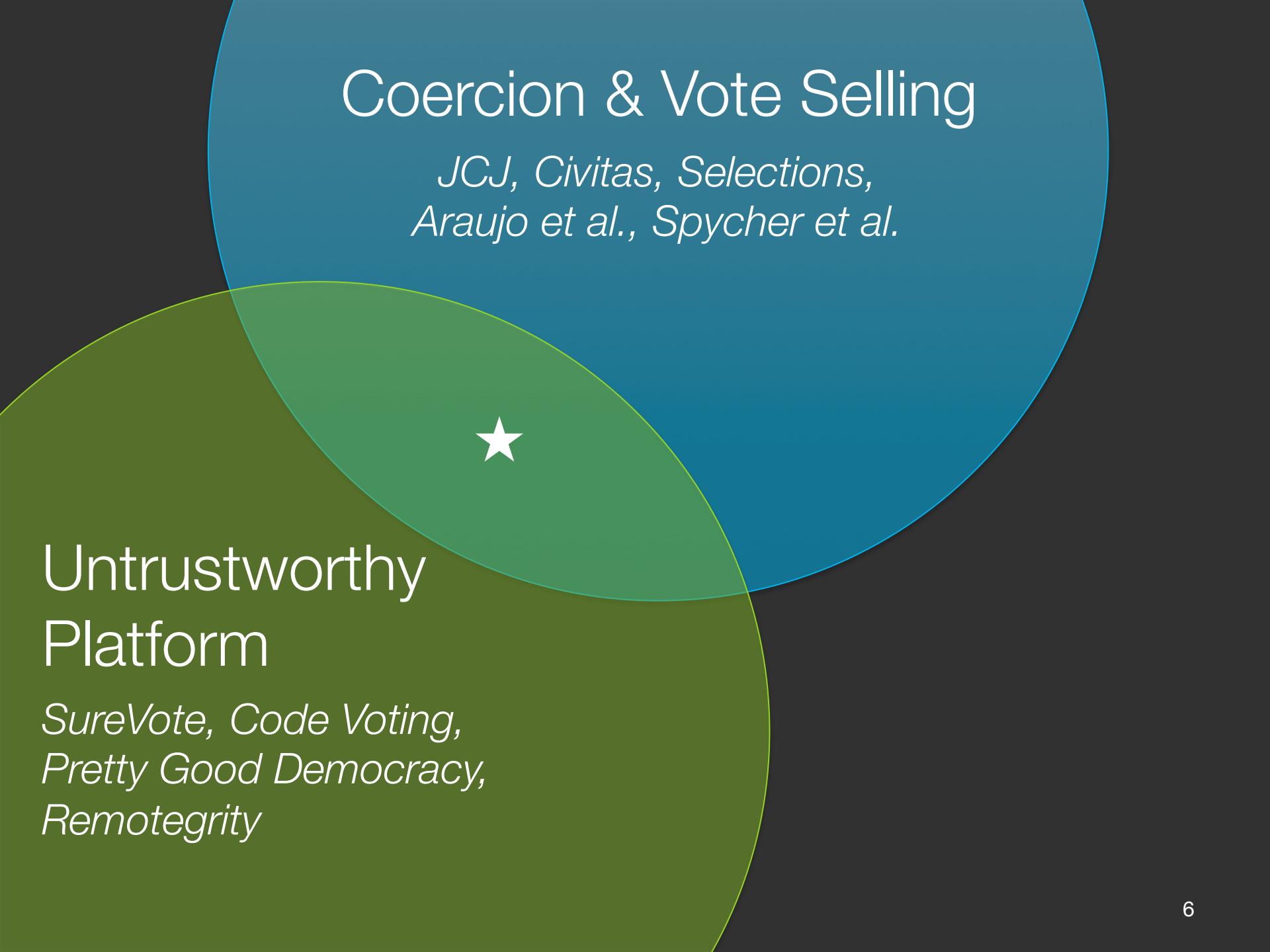
Internet Voting

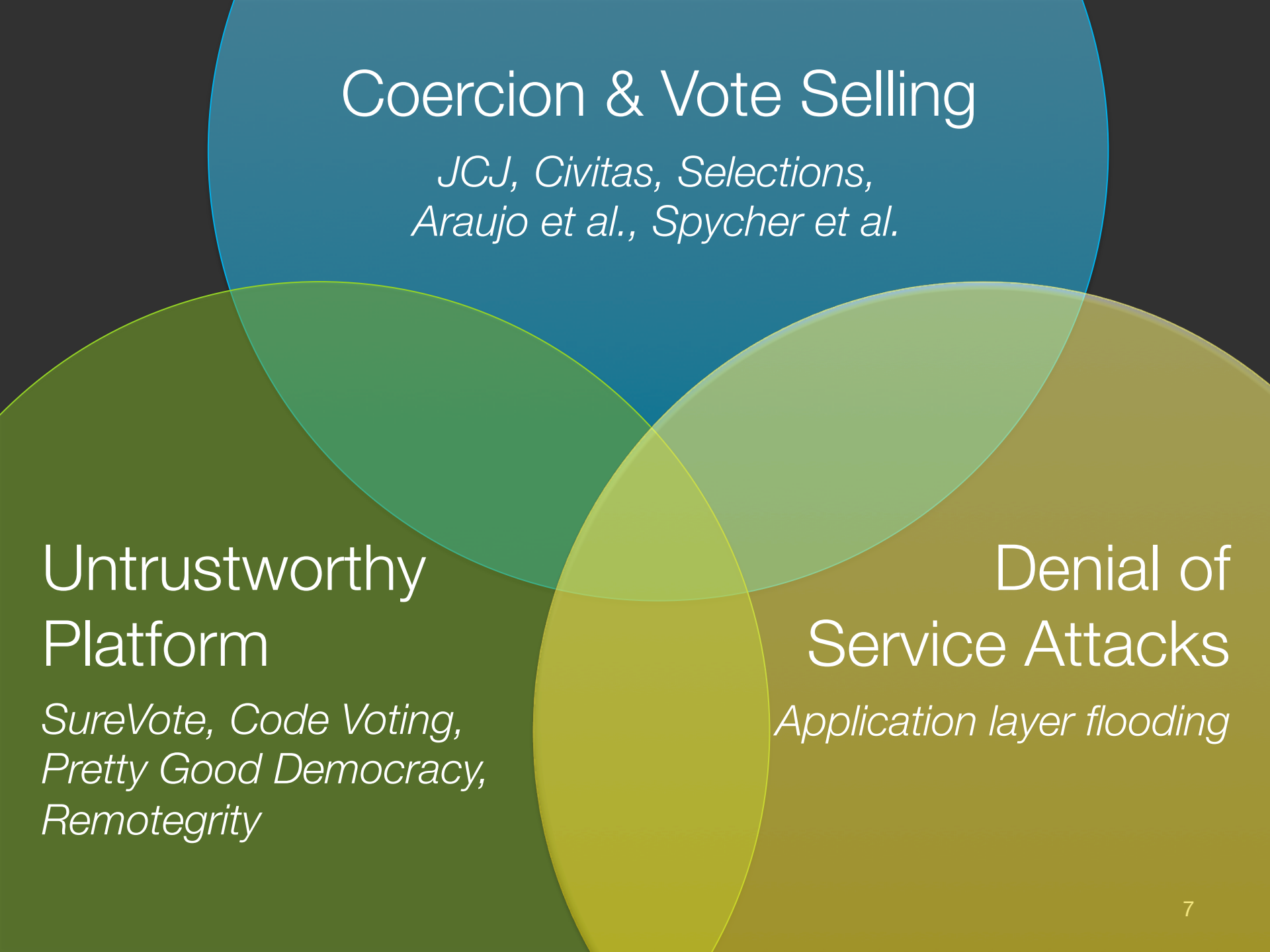
- Coercion & vote selling
- Untrustworthy platform
- Denial of service

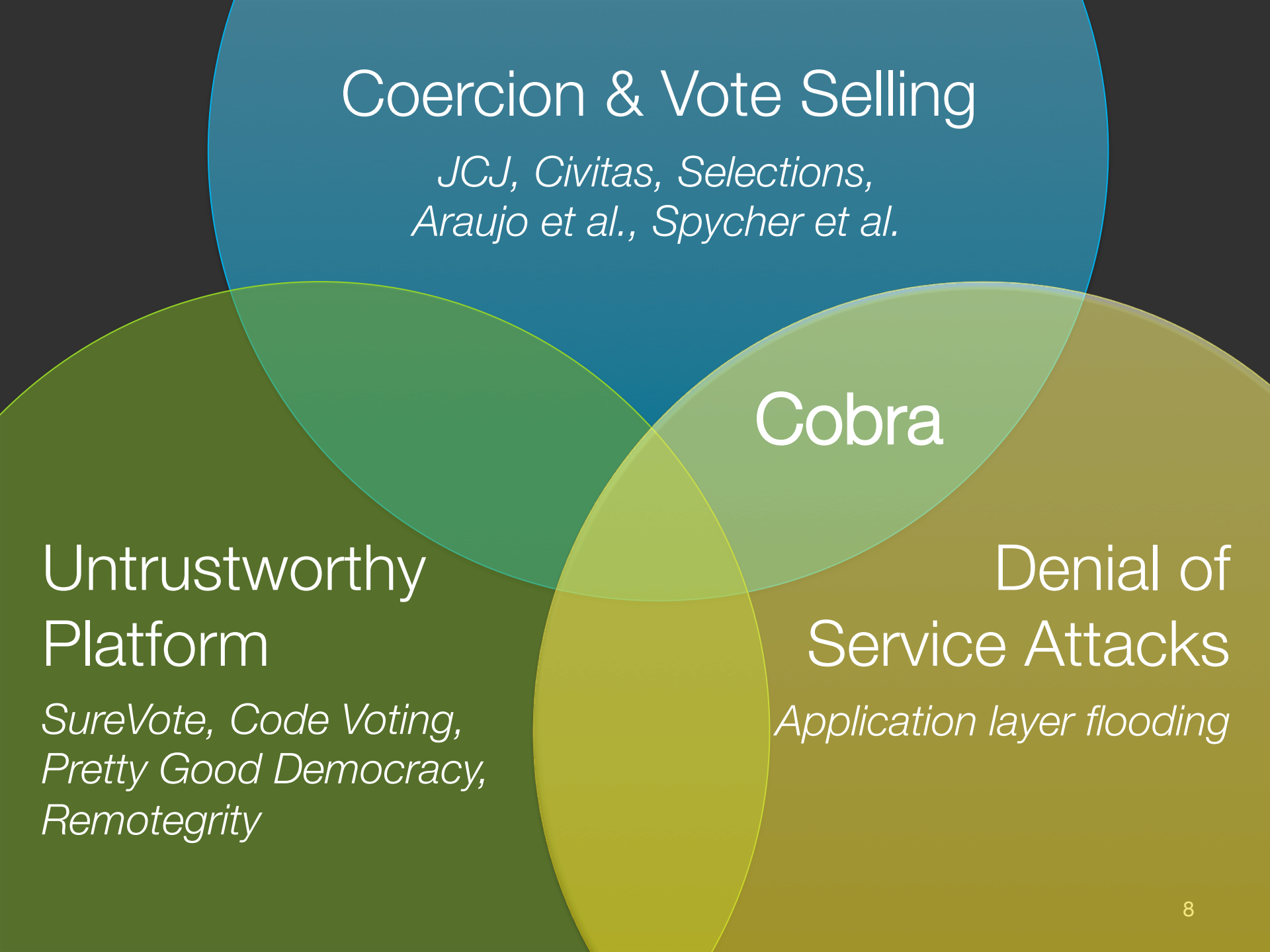
Coercion & Vote Selling

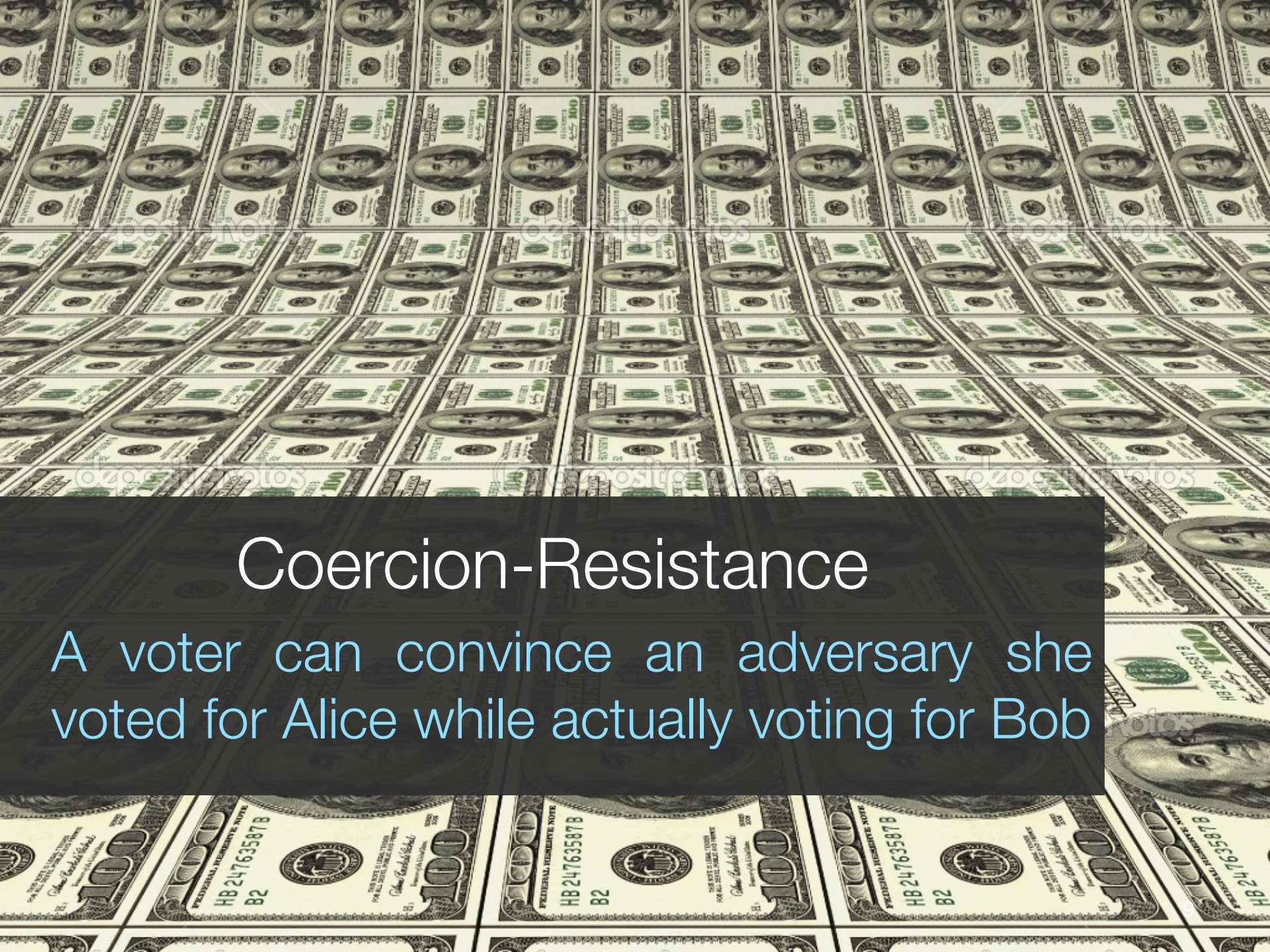
JCJ, Civitas, Selections,
Araujo et al., Spycher et al.


Coercion & Vote Selling
JCJ, Civitas, Selections,
Araujo et al., Spycher et al.
Untrustworthy
Platform
SureVote, Code Voting,
Pretty Good Democracy,
Remotegrity


Coercion & Vote Selling
JCJ, Civitas, Selections,
Araujo et al., Spycher et al.
Untrustworthy
Platform
SureVote, Code Voting,
Pretty Good Democracy,
Remotegrity


Coercion & Vote Selling
JCJ, Civitas, Selections,
Araujo et al., Spycher et al.
Untrustworthy Platform
SureVote, Code Voting,
Pretty Good Democracy,
Remotegrity
Denial of Service Attacks
Application layer flooding


Coercion & Vote Selling
JCJ, Civitas, Selections,
Araujo et al., Spycher et al.
Cobra
Untrustworthy Platform
SureVote, Code Voting,
Pretty Good Democracy,
Remotegrity
Denial of Service Attacks
Application layer flooding

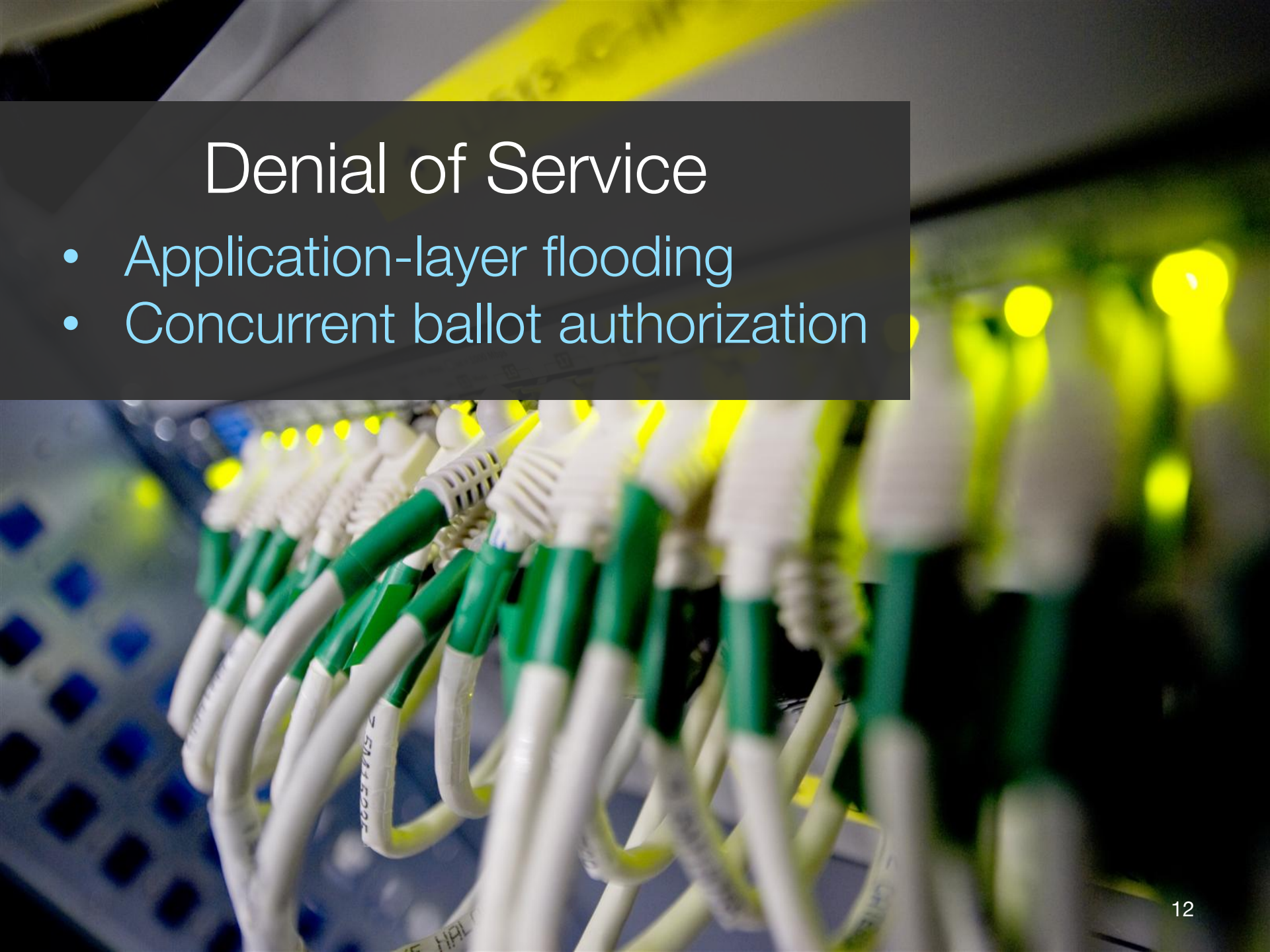


Coercion-Resistance

A voter can convince an adversary she voted for Alice while actually voting for Bob

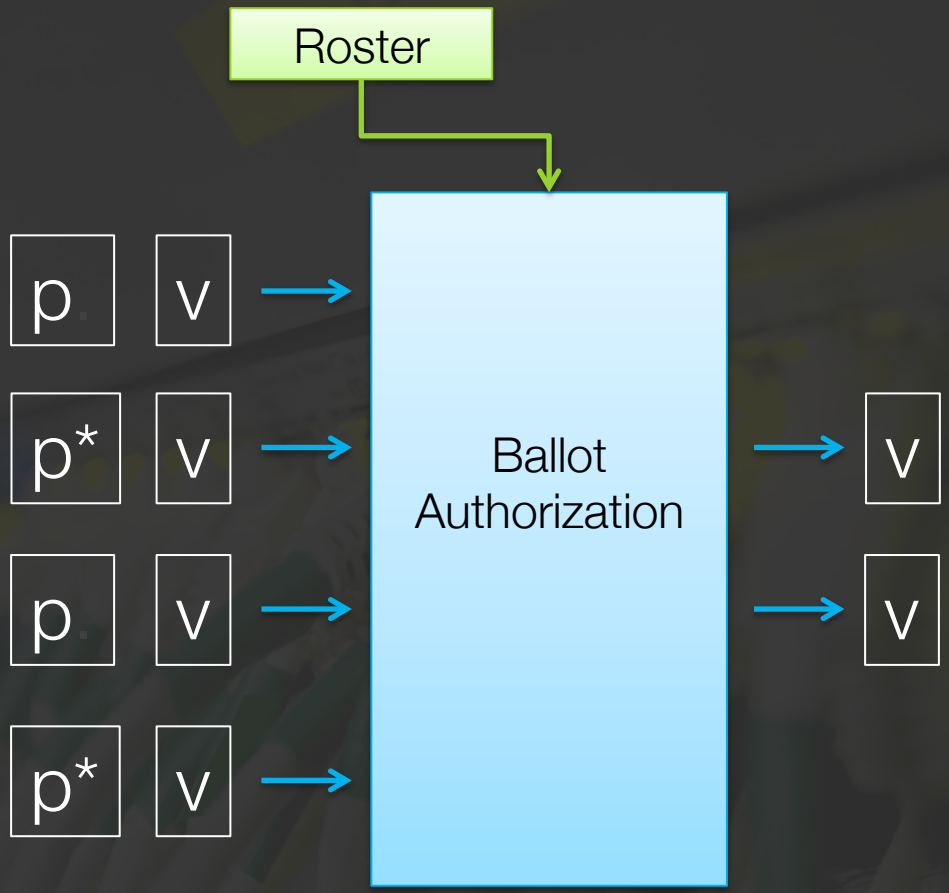
- Voters choose a password that allows them to vote during registration
- The password scheme has a simple cognitive rule for creating fake (“panic”) passwords
- Fake passwords can be sold or supplied under coercion
- The system will accept votes with fake passwords, but these votes will be obliviously canceled out
- Voters can vote with their real password any time. This ballot is unlikable to any ballots they cast with fake passwords

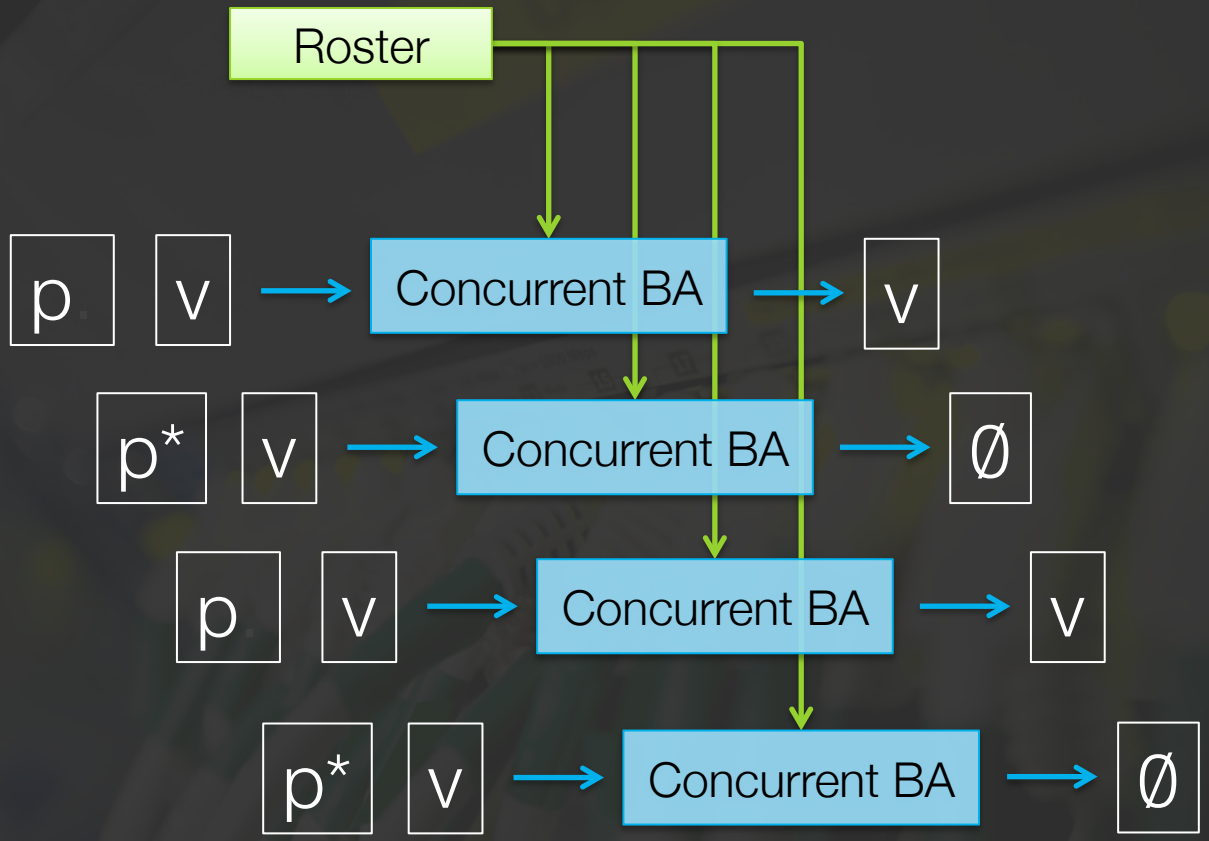
- Voters choose a password that allows them to vote during registration
- The password scheme has a simple cognitive rule for creating fake (“panic”) passwords
- Fake passwords can be sold or supplied under coercion
- The system will accept votes with fake passwords, but these votes will be obliviously canceled out
- Voters can vote with their real password any time. This ballot is unlikable to any ballots they cast with fake passwords

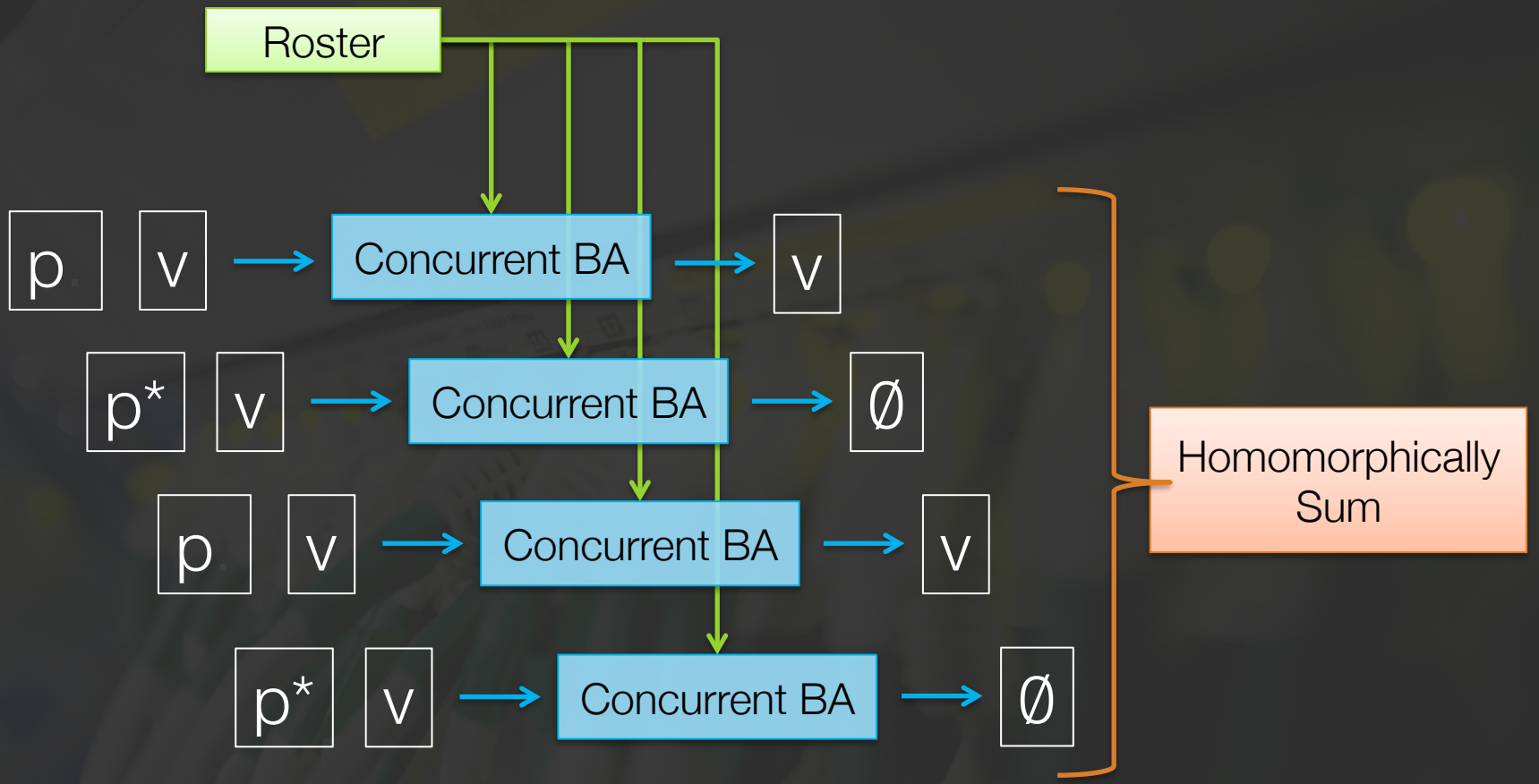


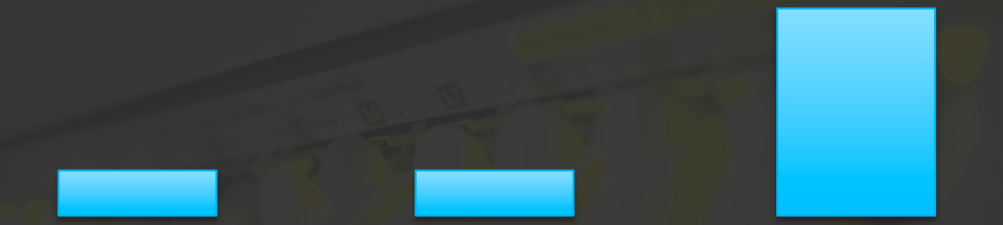
Denial of Service

- Application-layer flooding
- Concurrent ballot authorization

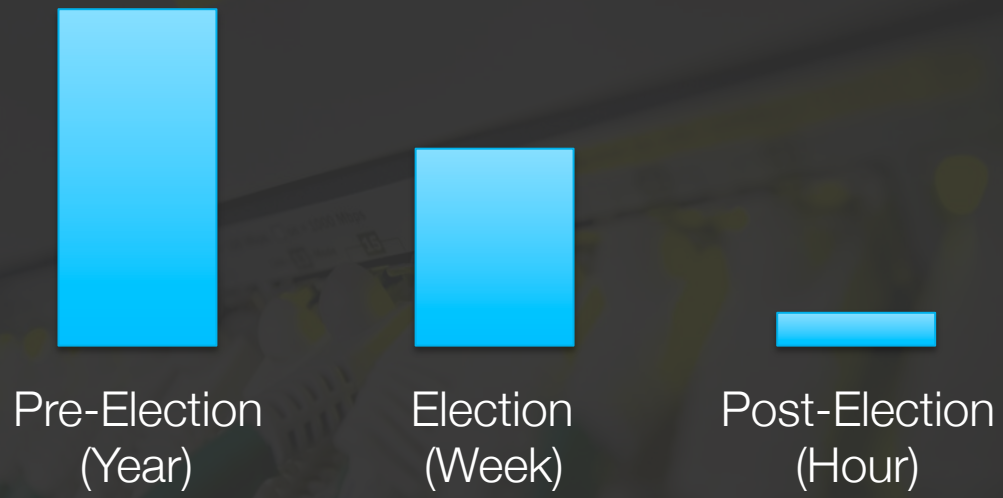

Roster
p
v
p*
v
p
v
p*
v
Ballot Authorization
v
v


Roster
p
v
Concurrent BA
v
p*
v
Concurrent BA
Ø
p
v
Concurrent BA
v
p*
v
Concurrent BA
Ø

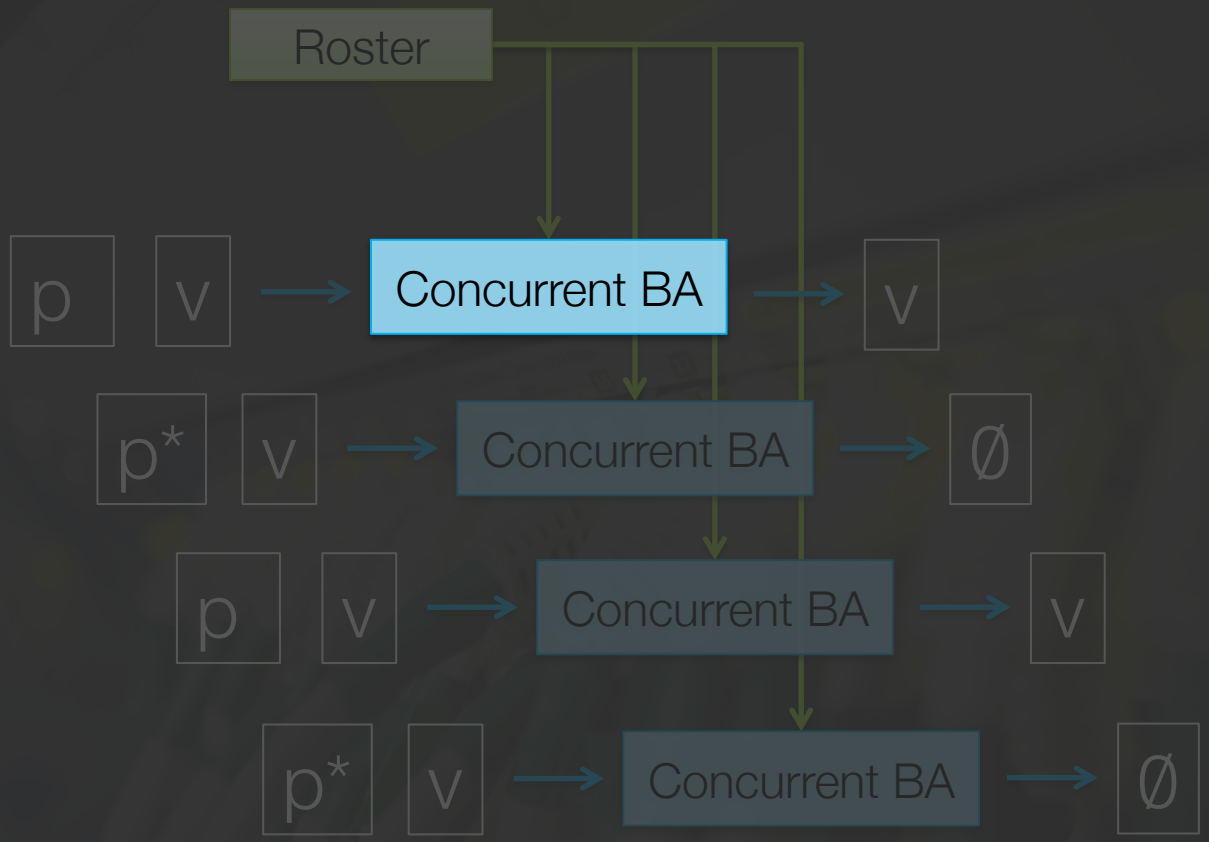

Roster
p
v
Concurrent BA
v
p*
v
Concurrent BA
Ø
p
v
Concurrent BA
v
p*
v
Concurrent BA
Ø
Homomorphically Sum



Work done by election authority



Work done by election authority


Roster
p
v
Concurrent BA
v
p*
v
Concurrent BA
Ø
p
v
Concurrent BA
v
p*
v
Concurrent BA
Ø

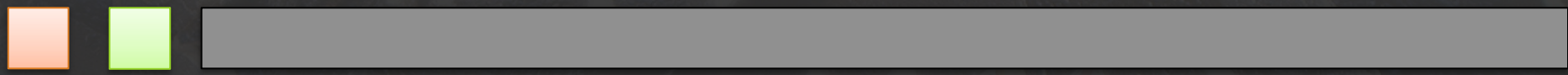
Fundamental Mechanism

- Private Set Membership

Is encrypted password [*p*] on the roster?

[0] [1]

Is encrypted password [*p*] on the roster?

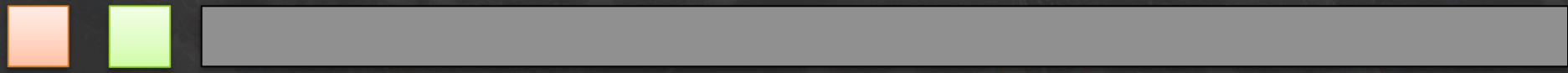


[0] [1]

No: [0] x [v] = [0]

Yes: [1] x [v] = [v]

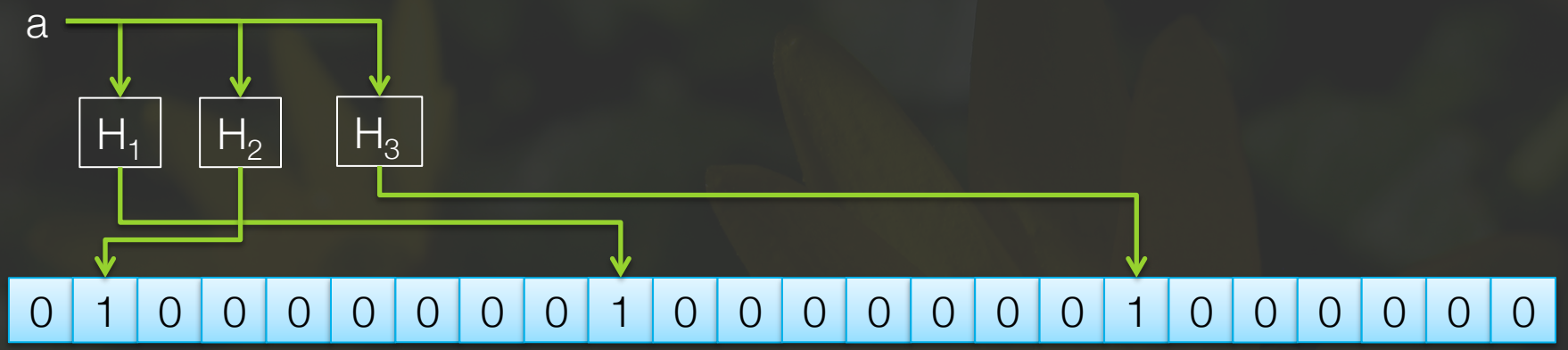
Is encrypted password [*p*] on the roster?



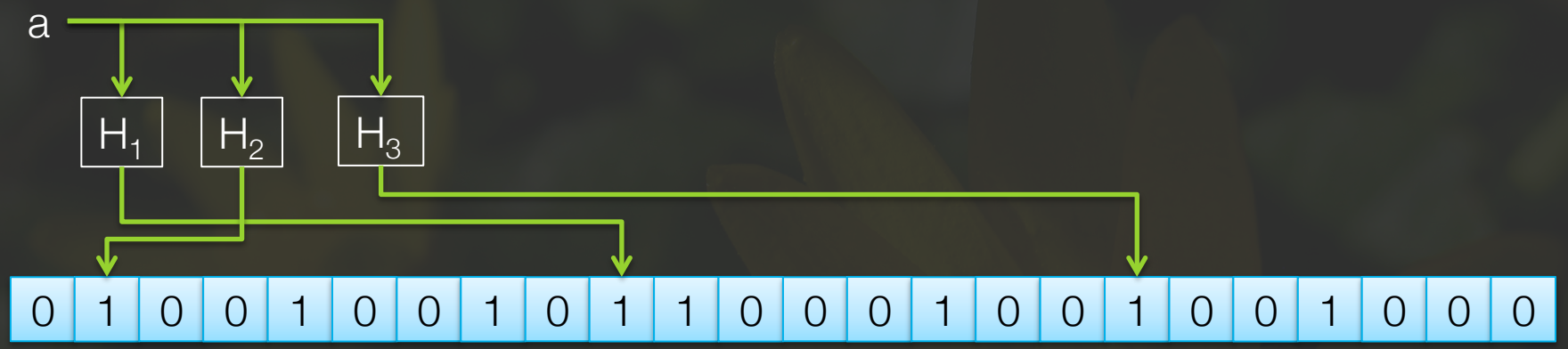
Plaintext equality tests & polynomials:

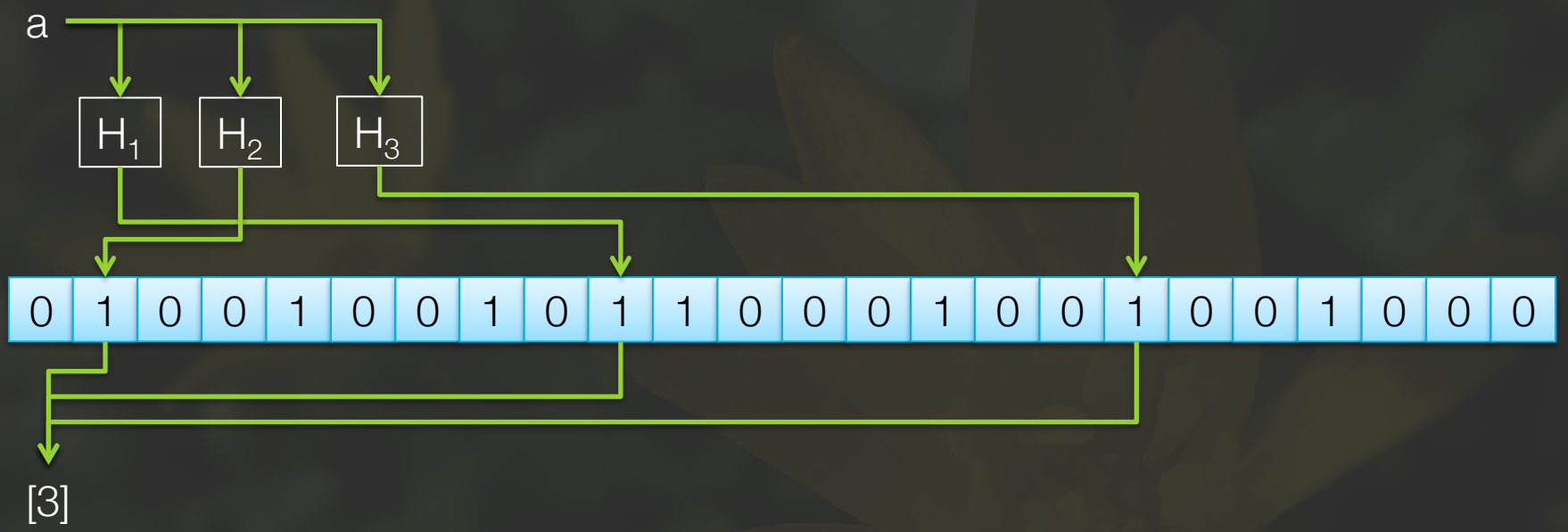
Encrypted Bloom Filters

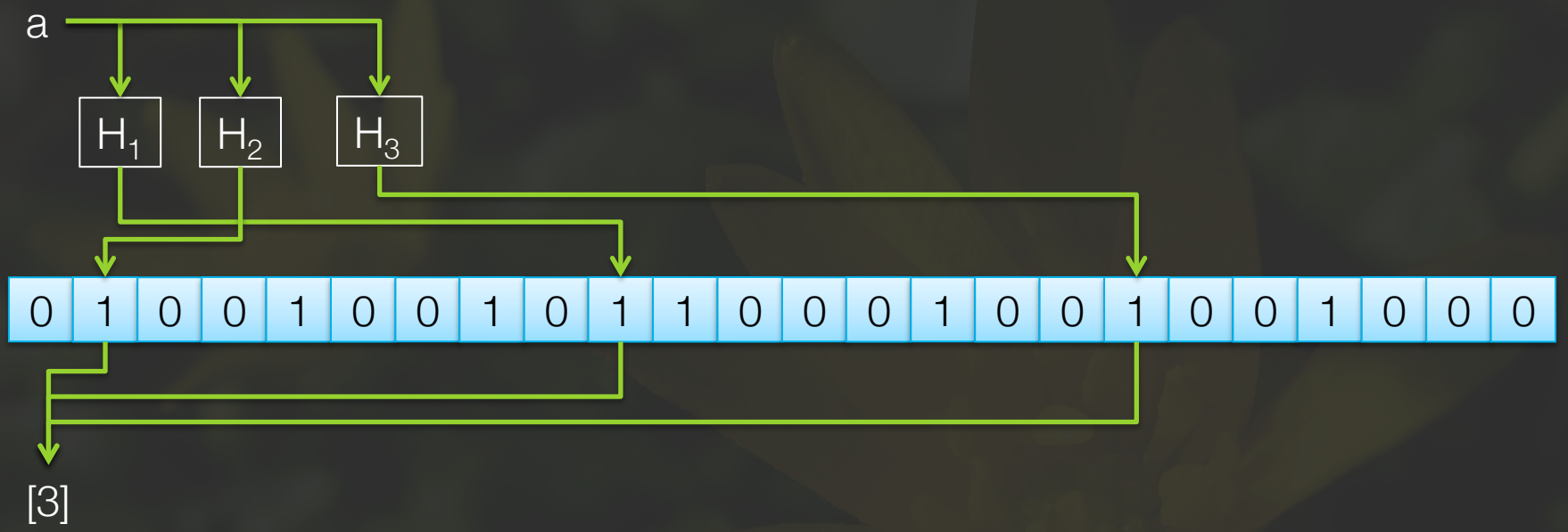

0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0


a
H_1
H_2
H_3
0 1 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 1 0 0 0 0 0 0

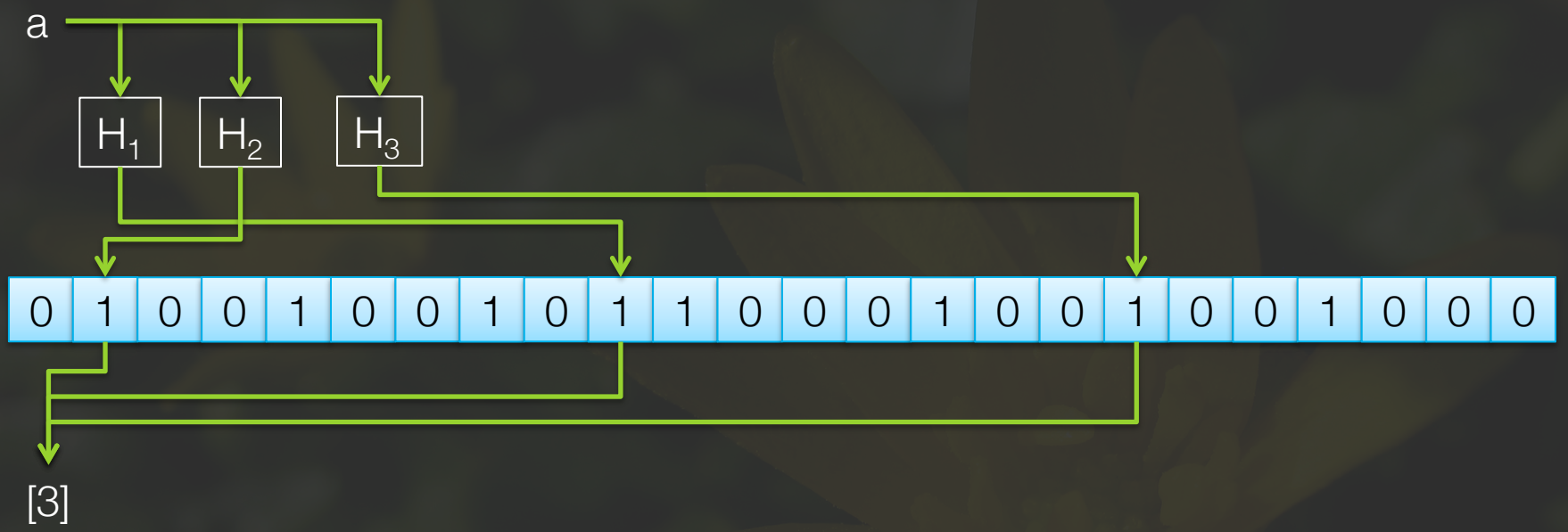

0 1 0 0 1 0 0 1 0 1 1 0 0 0 1 0 0 1 0 0 1 0 0 0


a
H_1
H_2
H_3
0 1 0 0 1 0 0 1 0 1 1 0 0 0 1 0 0 1 0 0 1 0 0 0


a
H_1
H_2
H_3
0 1 0 0 1 0 0 1 0 1 1 0 0 0 1 0 0 1 0 0 1 0 0 0
[3]

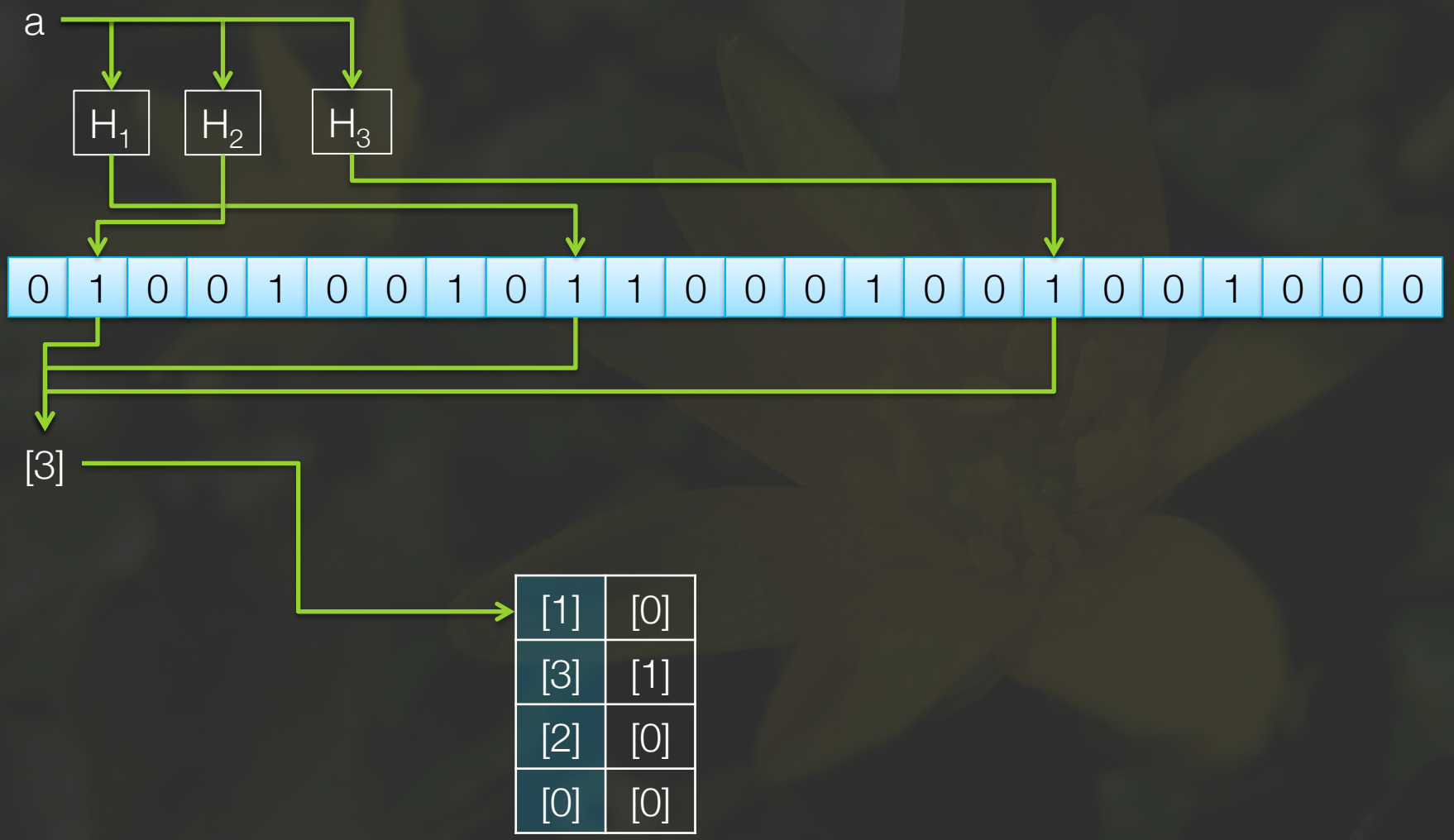


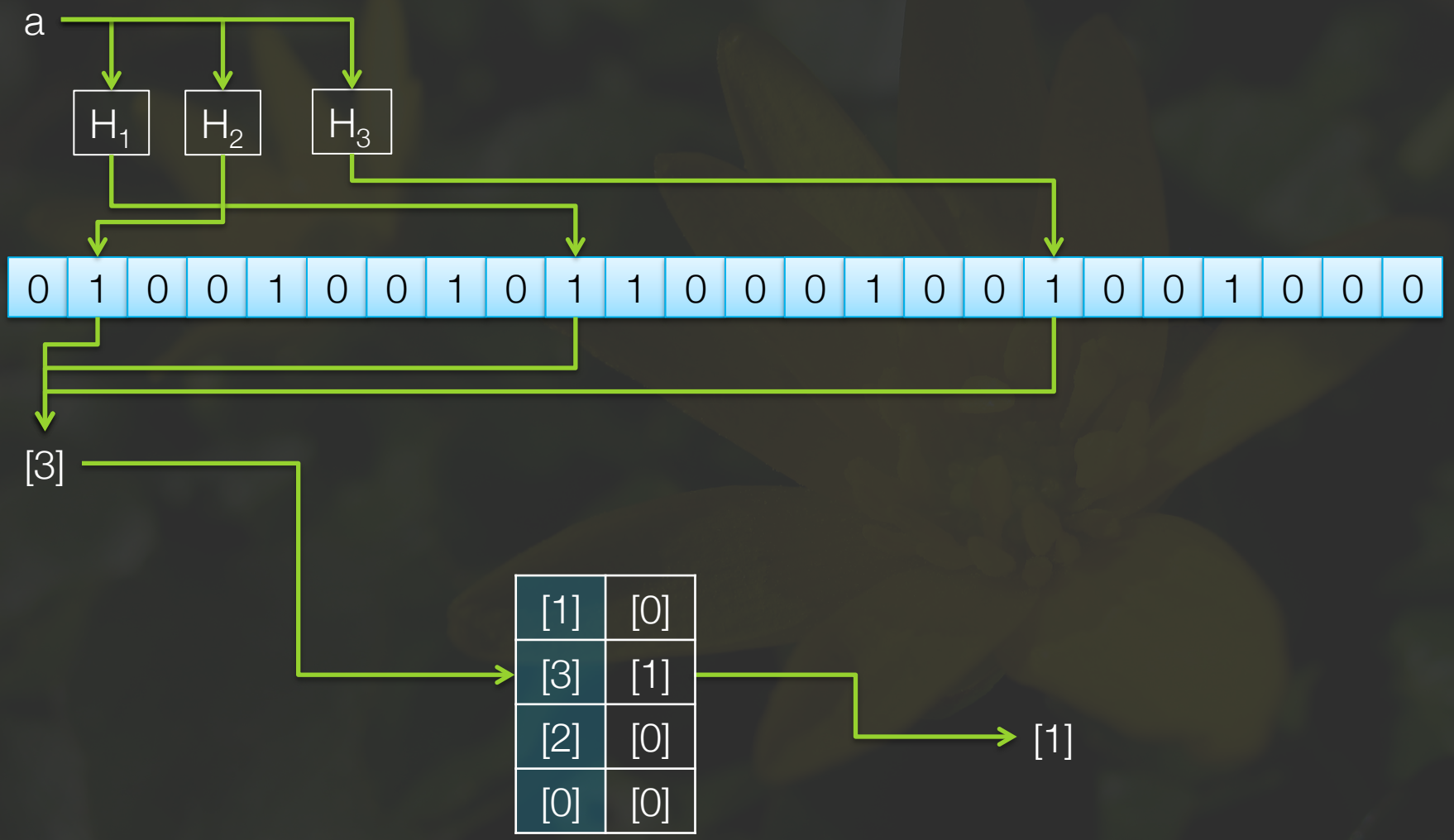
[0]	[0]
[1]	[0]
[2]	[0]
[3]	[1]



[0]	[0]
[1]	[0]
[2]	[0]
[3]	[1]

[1]	[0]
[3]	[1]
[2]	[0]
[0]	[0]


a
H_1
H_2
H_3
0 1 0 0 1 0 0 1 0 1 1 0 0 0 1 0 0 1 0 0 1 0 0 0
[3]
[1] [0]
[3] [1]
[2] [0]
[0] [0]


a
H_1
H_2
H_3
0 1 0 0 1 0 0 1 0 1 1 0 0 0 1 0 0 1 0 0 1 0 0 0
[3]
[1] [0]
[3] [1]
[2] [0]
[0] [0]
[1]

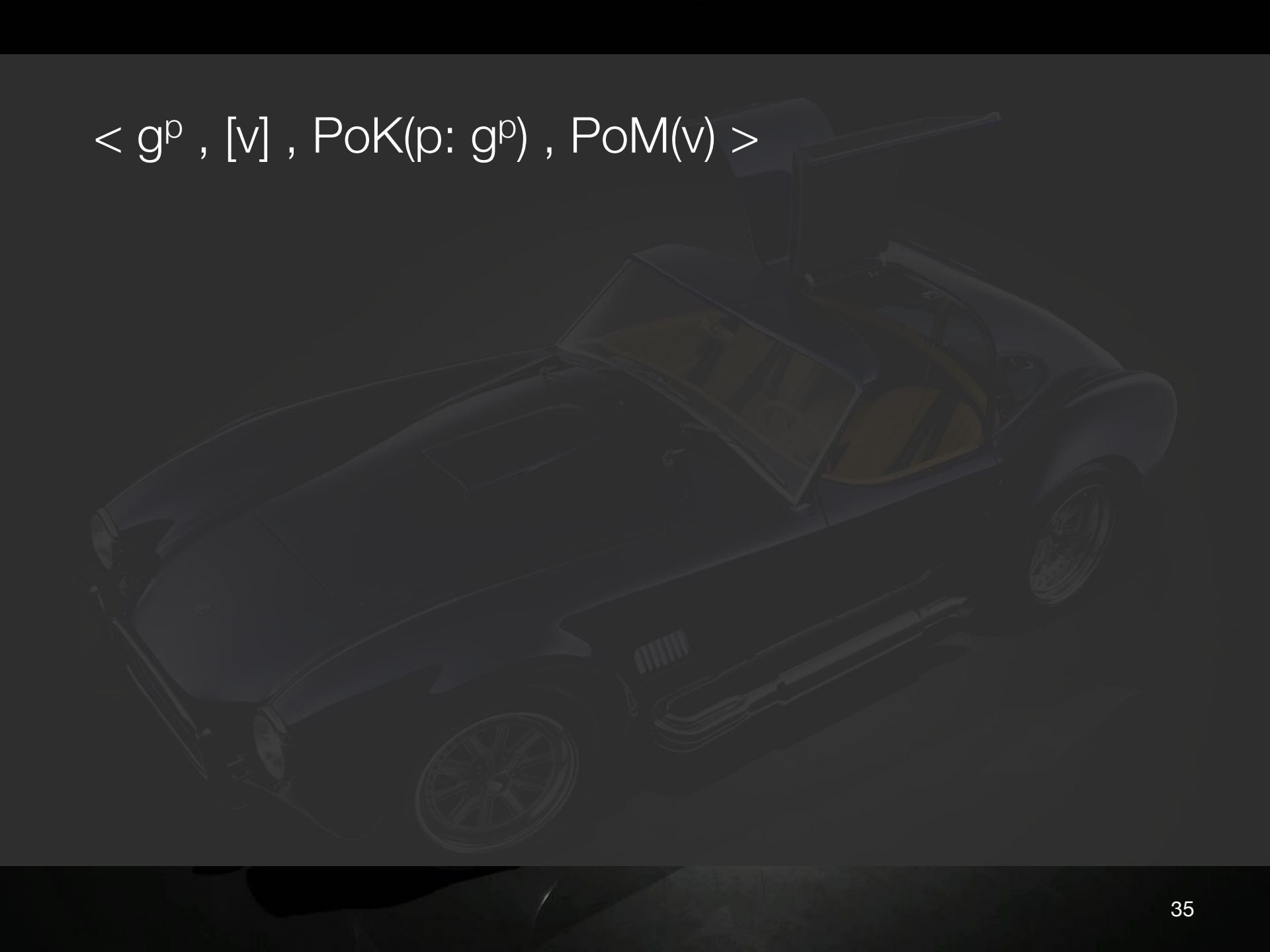

Cobra

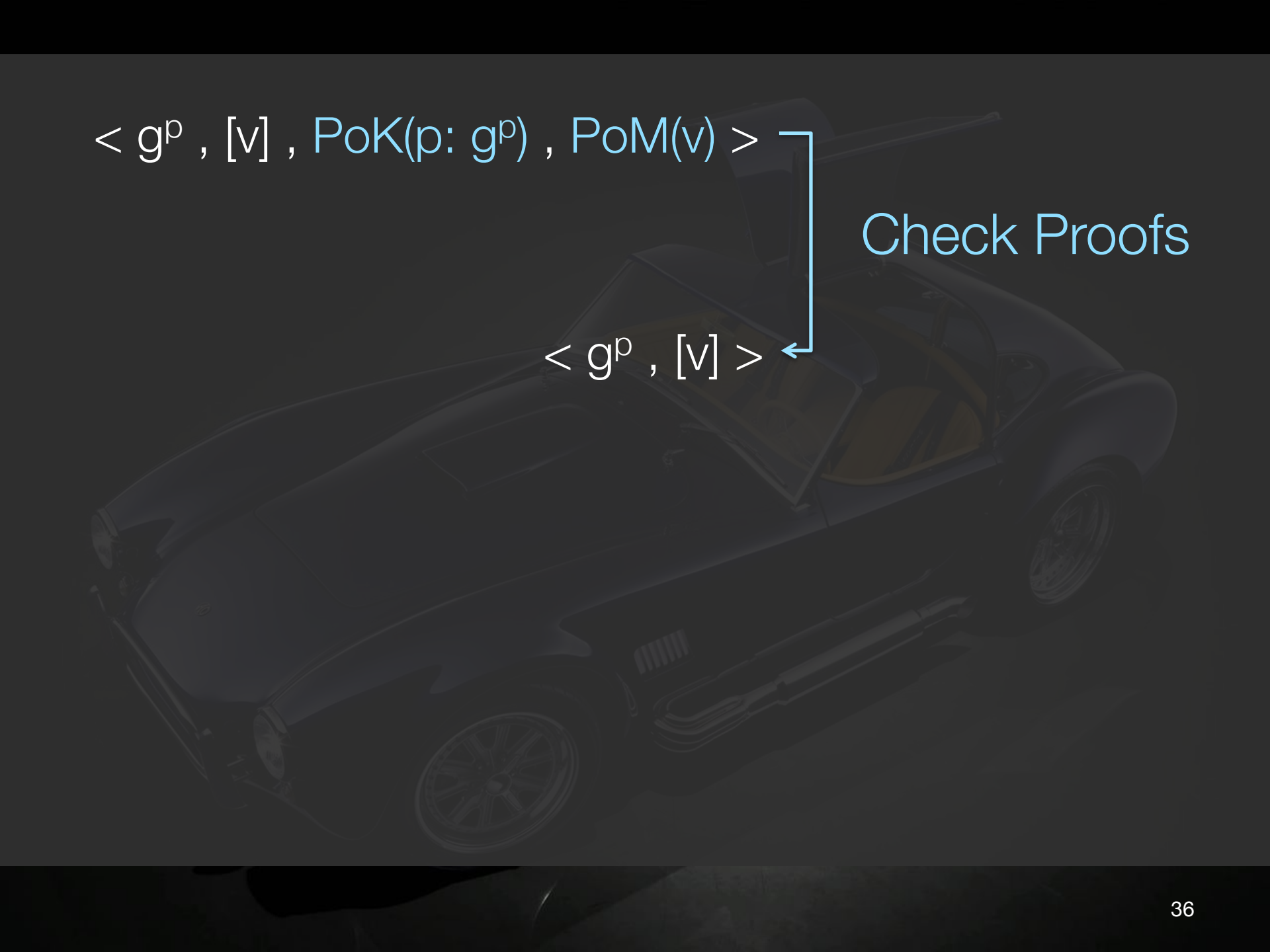
- Voters' (obfuscated) passwords are added to an encrypted Bloom filter during registration

- See paper for details

- Properties:
  - Registrar does not see obfuscated password
  - Publicly verifiable proof that each voter added only a single entry
  - Coercion-resistant

$< g^p , [v] , PoK(p: g^p) , PoM(v) >$

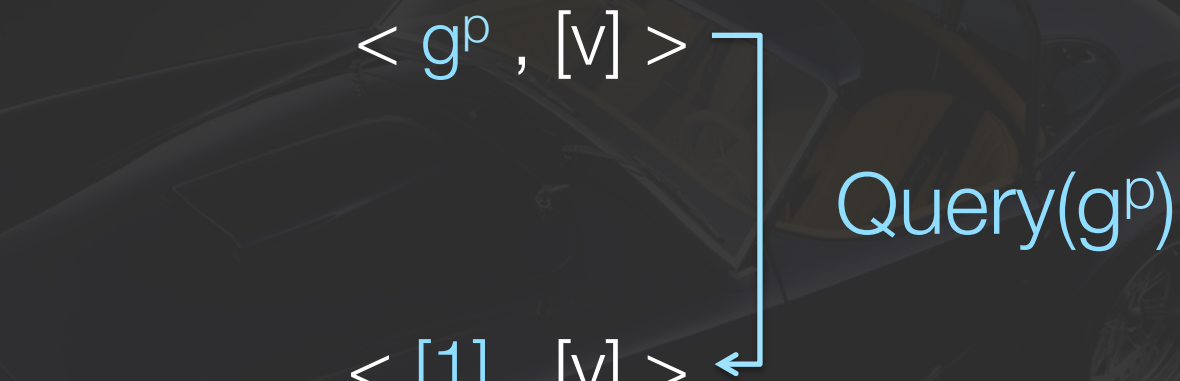



< g^p , [v] , PoK(p: g^p) , PoM(v) >
Check Proofs
< g^p , [v] >

$< g^p , [v] , PoK(p: g^p) , PoM(v) >$

$< g^p , [v] >$ ← Duplicate Check

$< g^p , [v] , PoK(p: g^p) , PoM(v) >$



$< g^p , [v] , PoK(p: g^p) , PoM(v) >$

$< g^p , [v] >$

$< [1] , [v] >$

$< [v] >$

Mix & Match:

[0]	[0]
[1]	[v]

$< g^{p^*} , [v] , PoK(p: g^p) , PoM(v) >$

$< g^{p^*} , [v] >$

$< [0] , [v] >$

$< [0] >$

Mix & Match:

[0]	[0]
[1]	[v]

See paper for more:

- Registration: setting up the Bloom filter (*expensive!*); setting false positive rate
- Optimizations: using BGN to eliminate steps
- Security analysis: eligibility verification, integrity, coercion-resistance
- A blueprint that might be useful for concurrent ballot authorization other ways

Performance

	JCJ/Civitas	ARRTY	Selections	SHKS	Cobra
Registration *(Before Election)*					
Voter	11	9	39	11	55,680,006
Registrar	8	10	20	8	37,120,006
Casting *(During Election)*					
Submit Ballot	42	42	42	42	42
Submit Credential	3	13	202	3	2
Processing *(During Election)*					
Check Ballots	240,000	240,000	240,000	240,000	240,000
Ballot Authorization	0	0	2,000,000	0	10,790,000
Processing & Tallying *(After Election)*					
Ballot Authorization	3,000,960,000	4,080,000	2,010,000	100,710,000	0
Tally Ballots	45	45	45	45	45

Table 1: Performance comparison in number of modular exponentiations for a moderately-sized election scenario: 5 candidates, 10,000 registered voters, 20,000 submitted ballots, and 3 trustees.

Concluding Remarks

- DOS on internet voting is a reality
- Common properties of coercion-resistance systems (anonymous ballot submission, intensive post-tally processing) make protocol-level DOS a threat
- We have shown in principle ballots can be authorized concurrently (and incidentally post the fastest tally with Cobra)
- Future work: speed-up registration


Questions?
@AleksEssex
@PulpSpy
@uhengart
TICKET VENDING MACHINES