

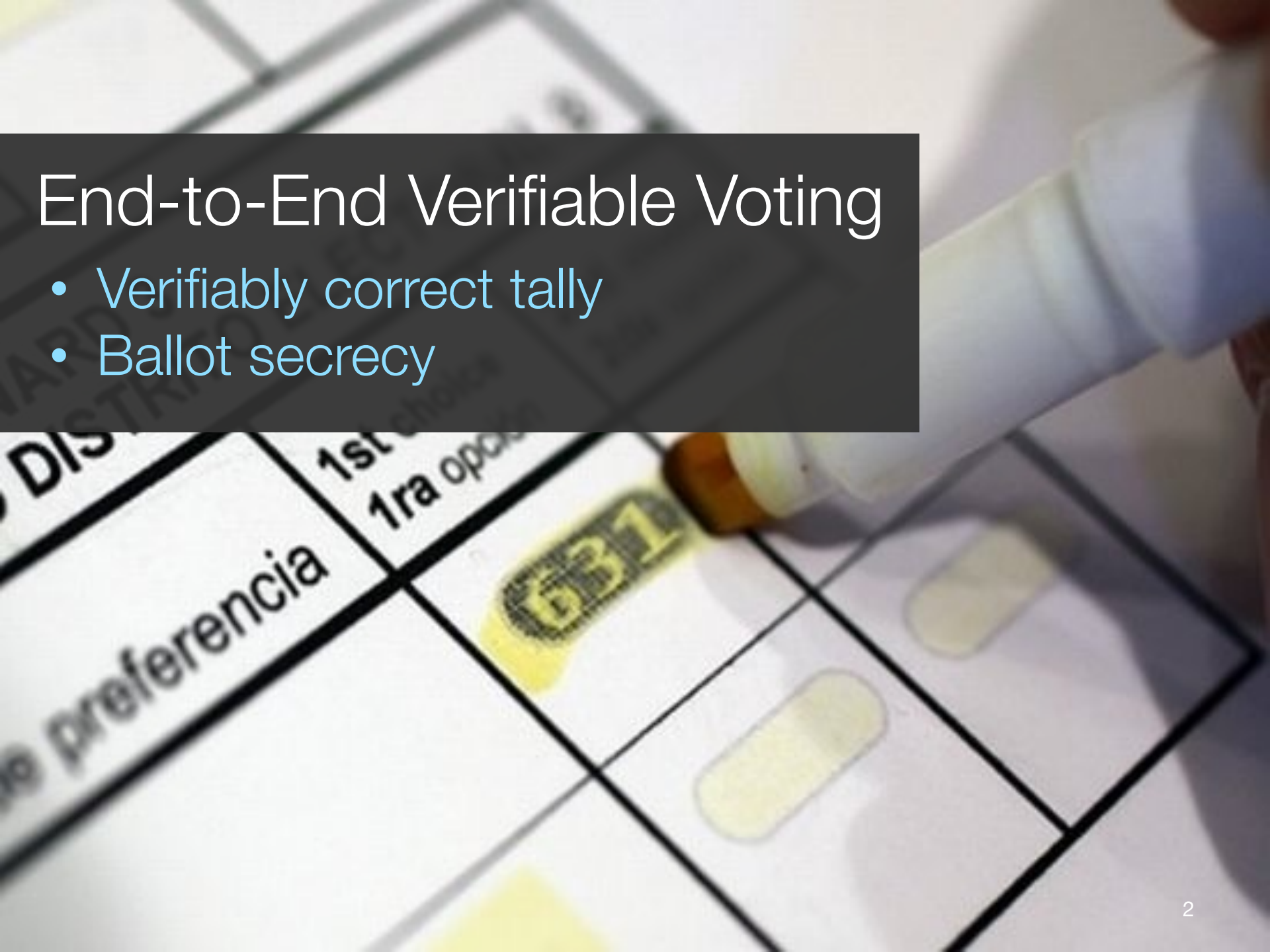
A photograph of the interior of Grand Central Terminal. The scene is filled with people walking through a grand, stone-walled space. In the foreground, a row of ticket vending machines is visible, with a sign above them that reads "TICKET VENDING MACHINES" and an arrow pointing left. The architecture is classical, with high ceilings and large windows. An American flag is visible on the right side of the image. The lighting is warm, highlighting the stone surfaces and the activity of the commuters.

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*

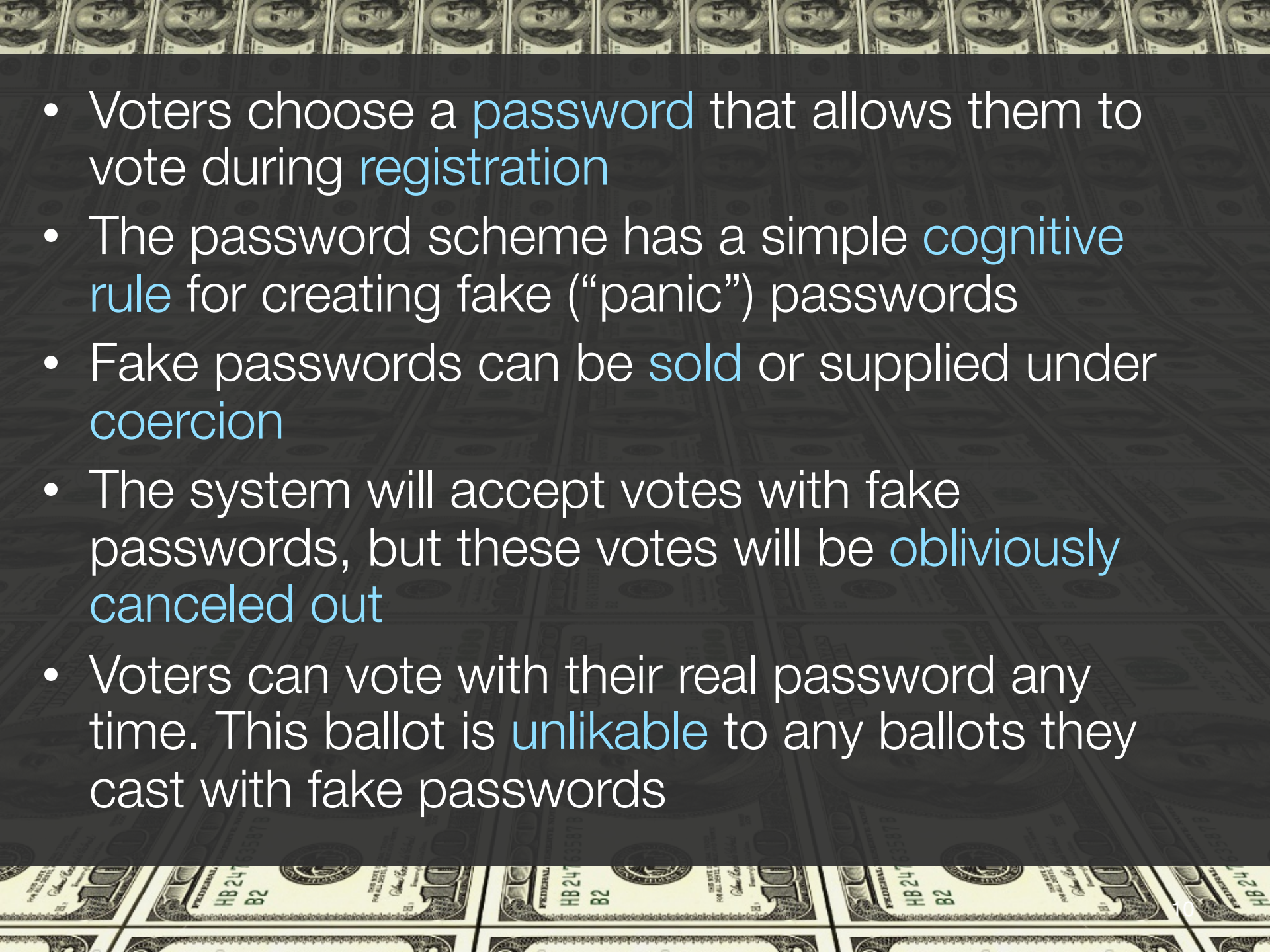
Denial of
Service Attacks

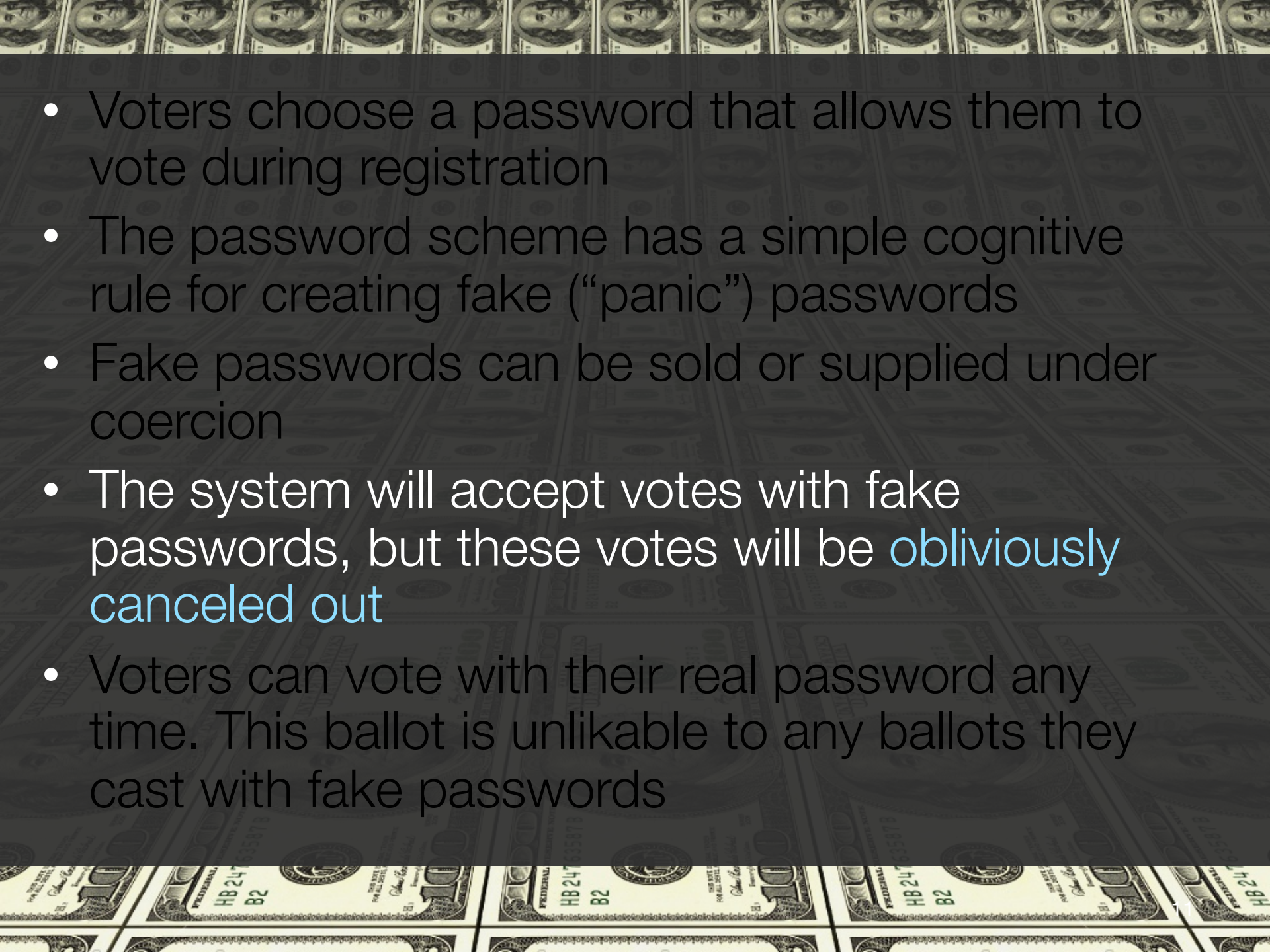
Application layer flooding



Coercion-Resistance

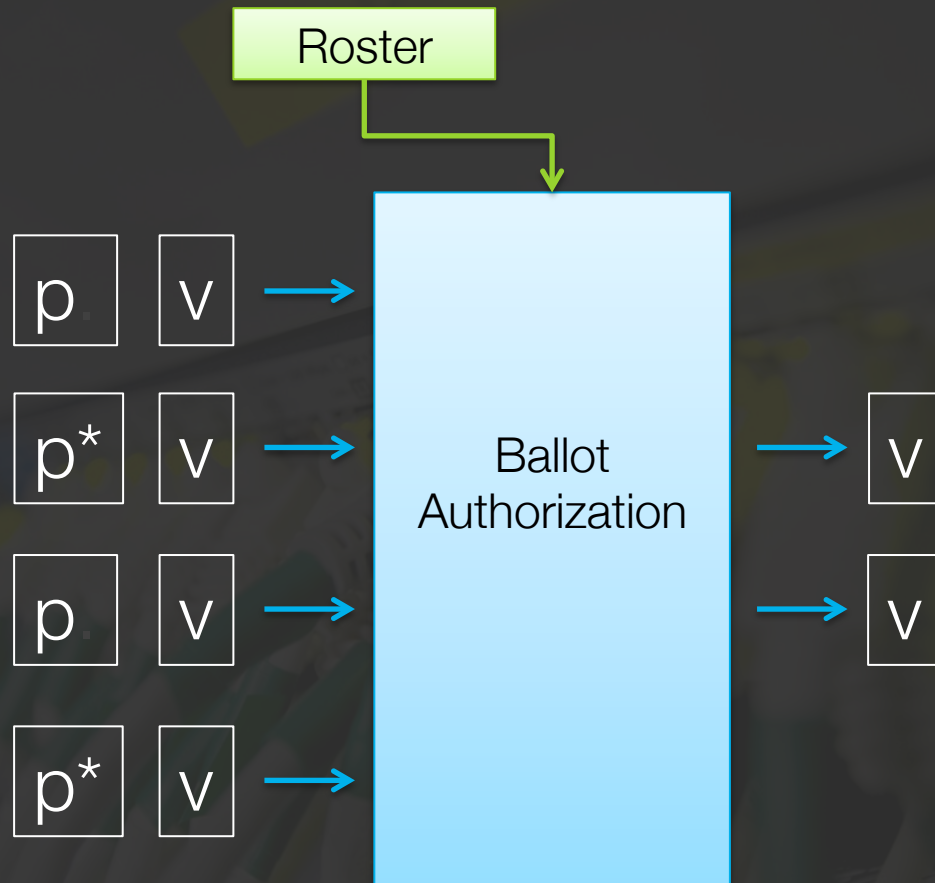
A voter can convince an adversary she voted for Alice while actually voting for Bob

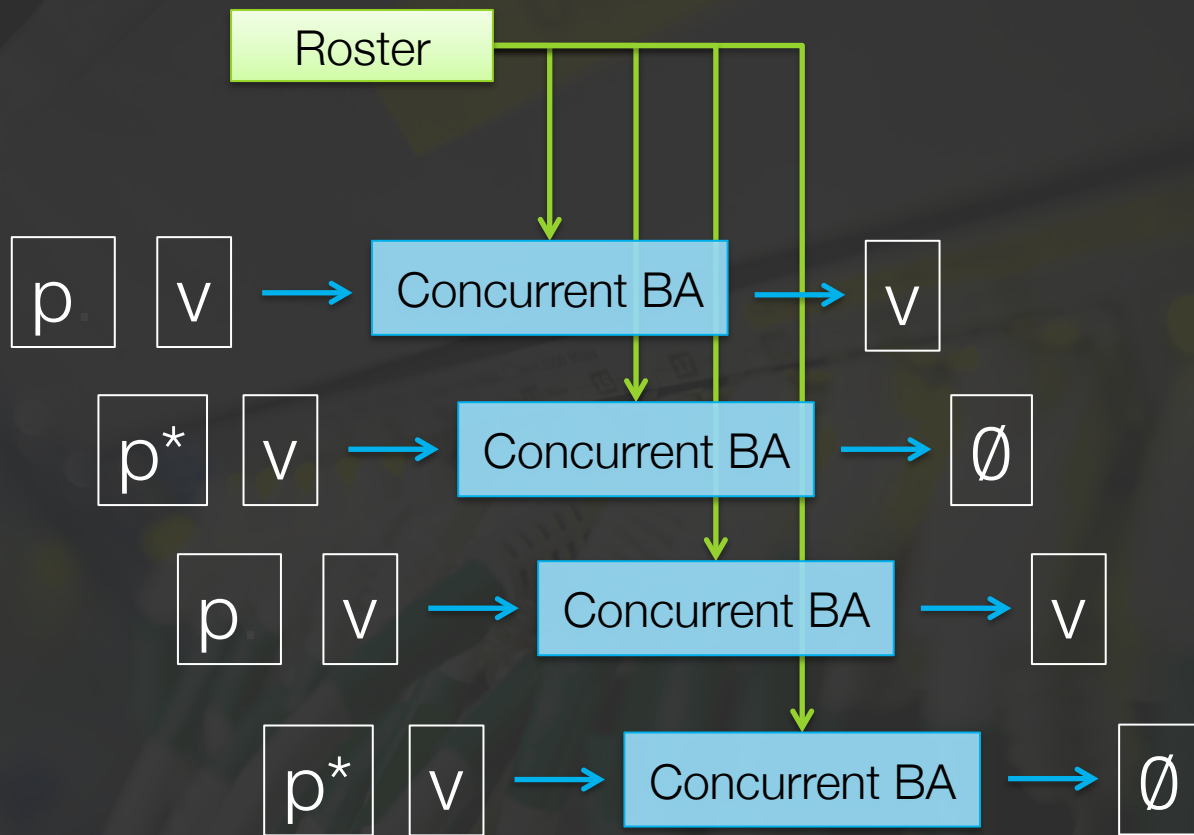
- 
- The background of the slide is a dark, textured surface with a repeating pattern of US dollar bills. The bills are oriented vertically, showing the portrait of George Washington on the left and the number '10' on the right. The text 'FEDERAL RESERVE NOTE' and 'HB 24 B2' is visible on the bills. The overall appearance is that of a stack of money.
- 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 **obviously canceled out**
 - Voters can vote with their real password any time. This ballot is **unlikable** to any ballots they cast with fake passwords

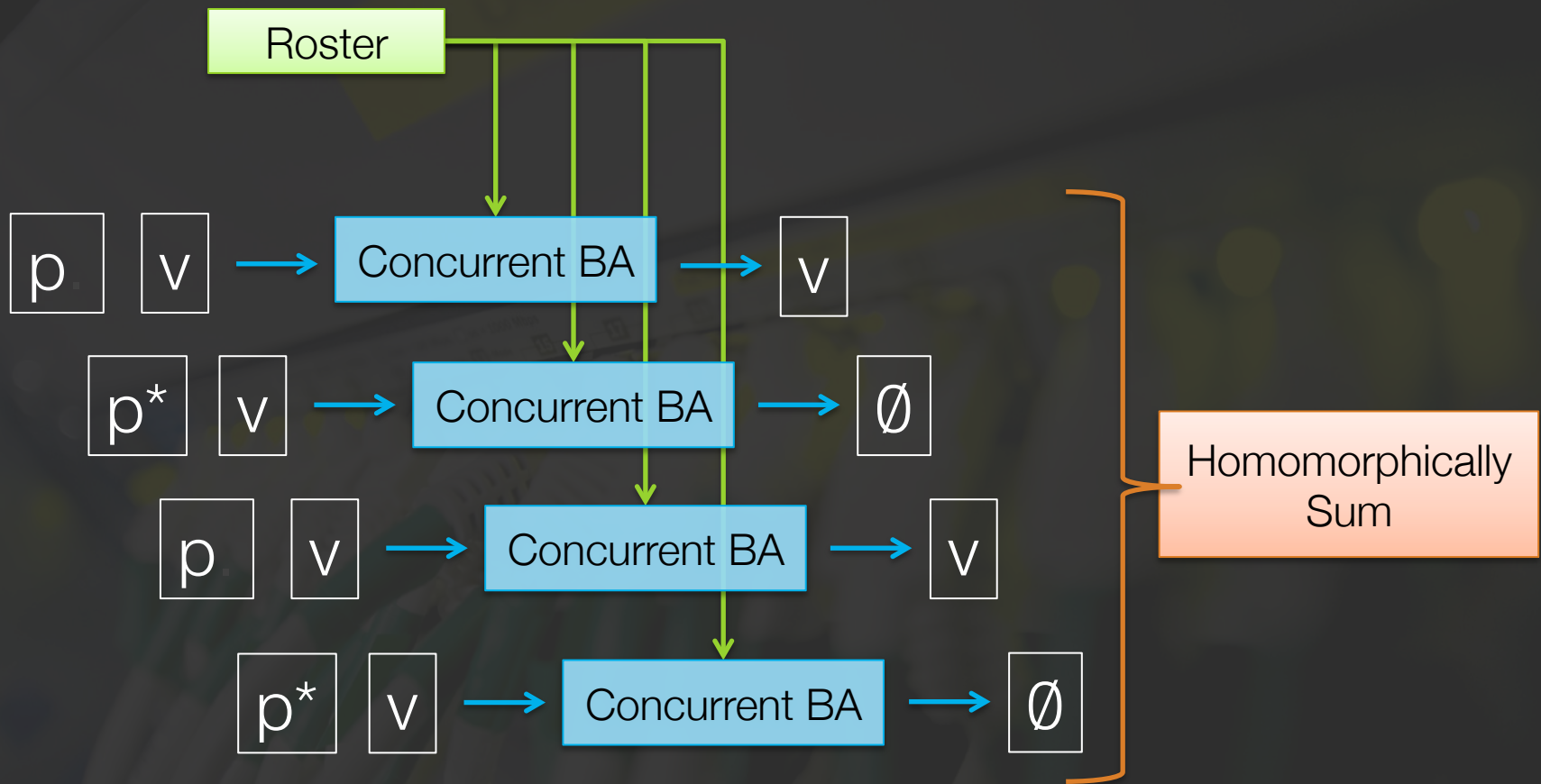
- 
- Voters choose a password that allows them to vote during registration
 - The password scheme has a simple cognitive rule for creating fake (“panic”) passwords
 - Fake passwords can be sold or supplied under coercion
 - The system will accept votes with fake passwords, but these votes will be **obviously 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







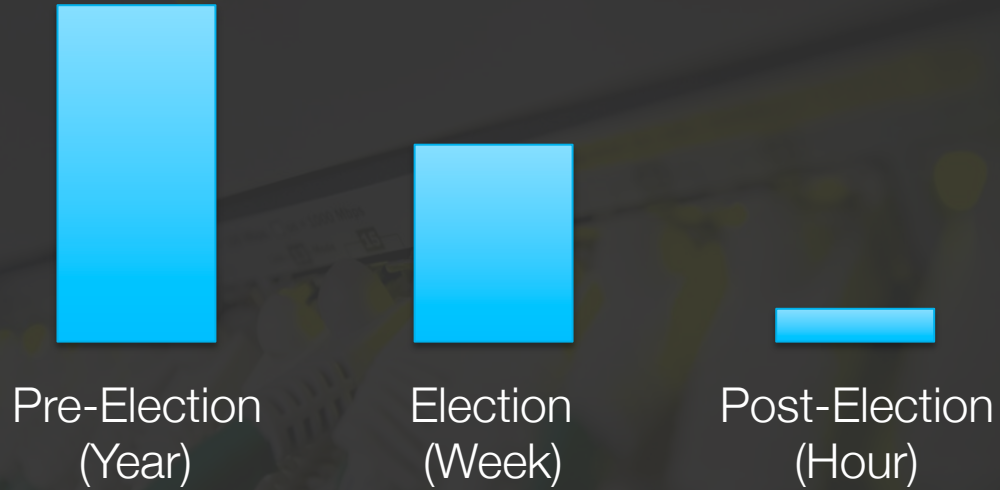


Pre-Election
(Year)

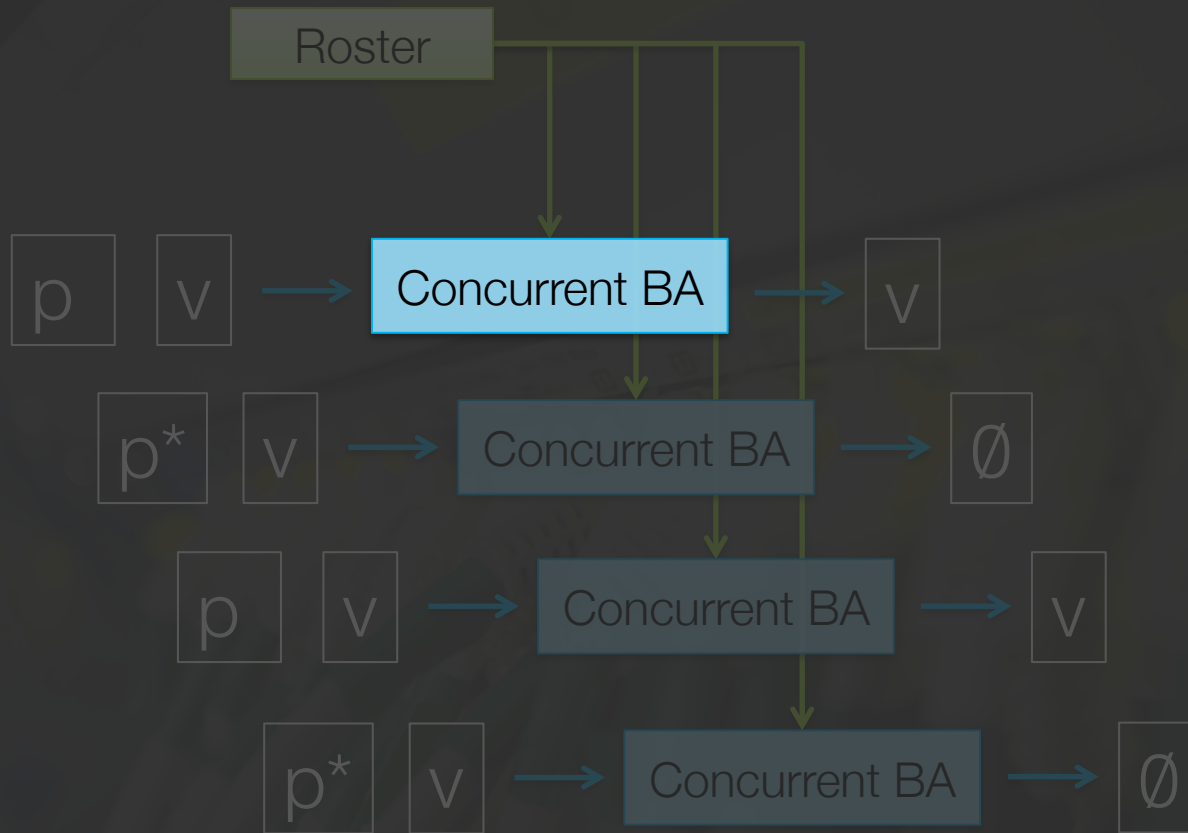
Election
(Week)

Post-Election
(Hour)

Work done by election authority



Work done by election authority



A close-up photograph of a heavily rusted mechanical assembly. The central focus is a large gear with several circular cutouts, showing significant orange-brown corrosion. A metal chain with rivets is visible, running across the top and right sides of the frame. The background is dark and textured, suggesting a complex machinery environment.

Fundamental Mechanism

- Private Set Membership

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



[0] [1]

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

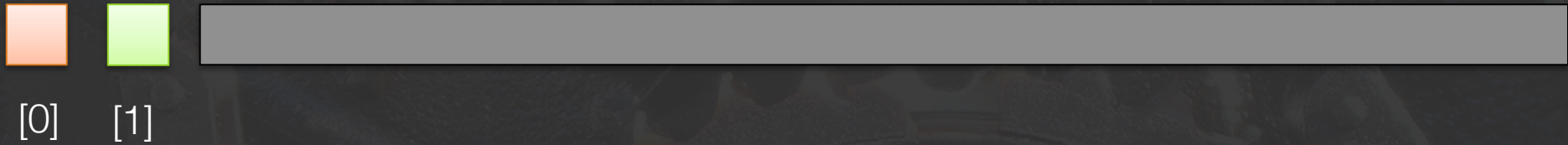


[0] [1]

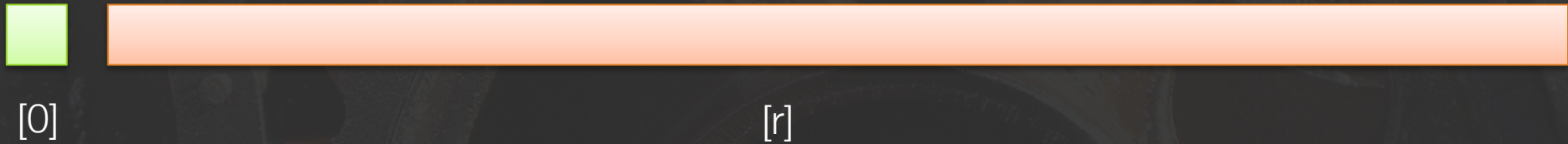
No: $[0] \times [v] = [0]$

Yes: $[1] \times [v] = [v]$

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

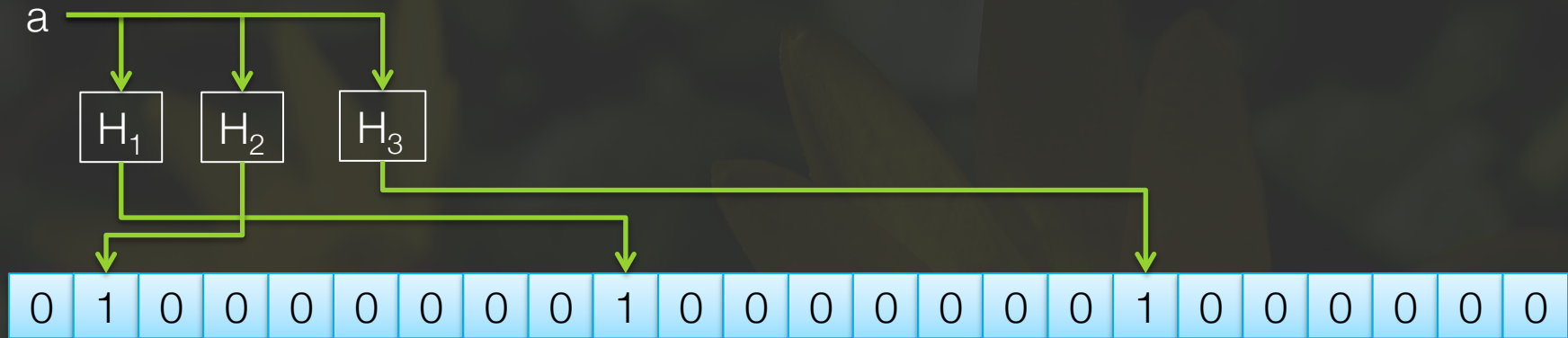


Plaintext equality tests & polynomials:

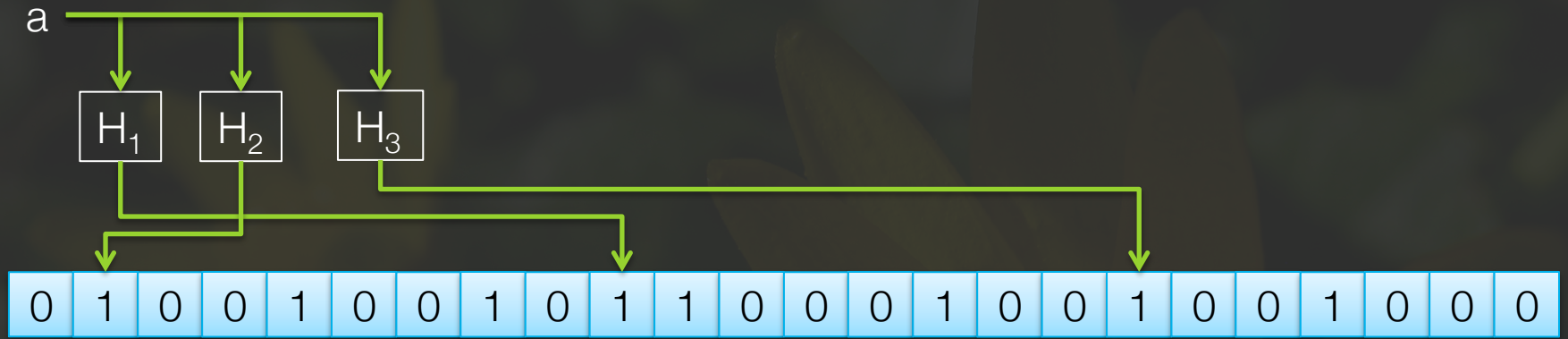


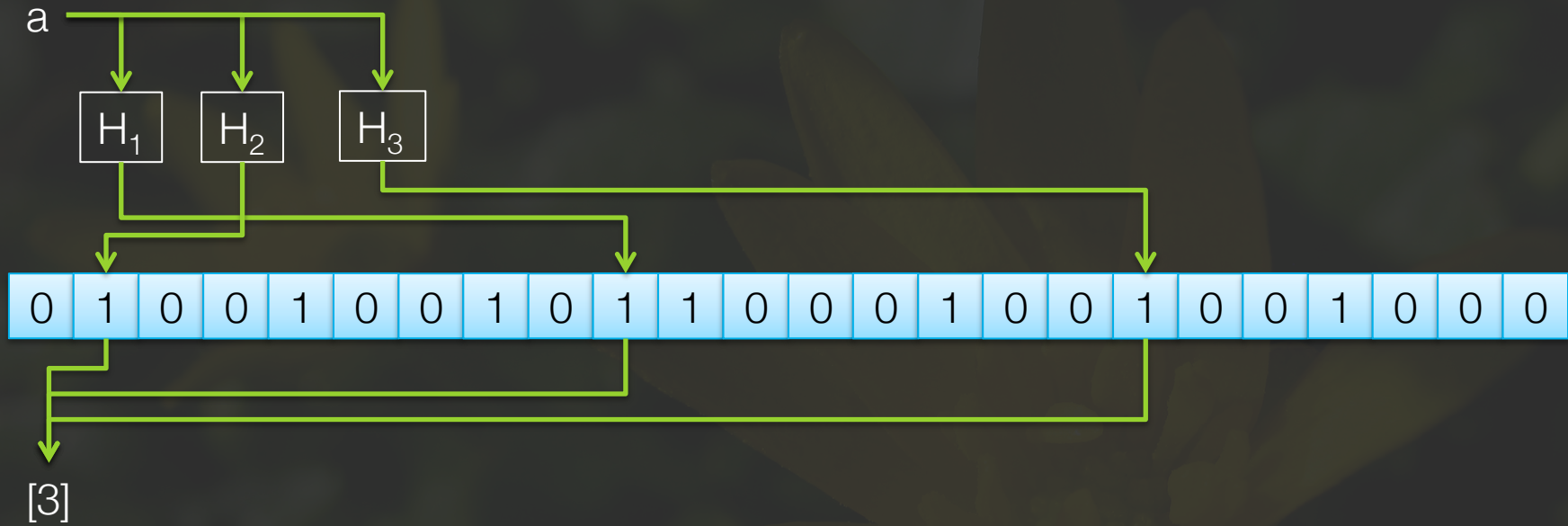


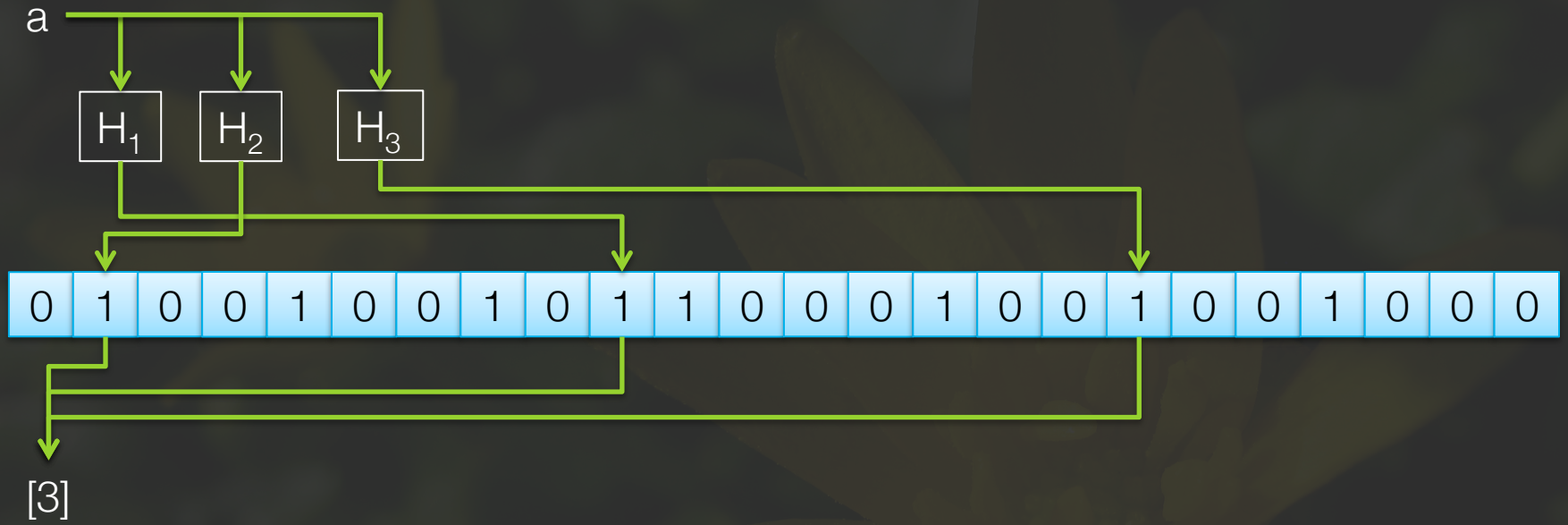
Encrypted Bloom Filters



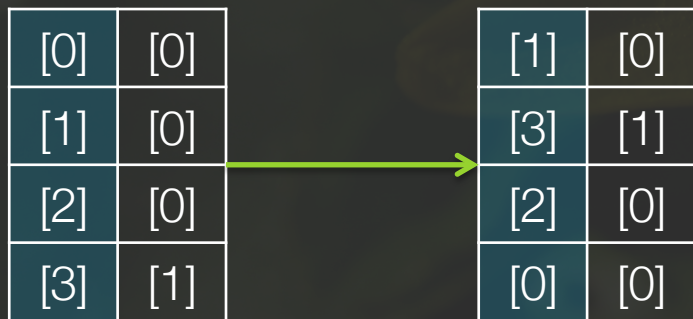
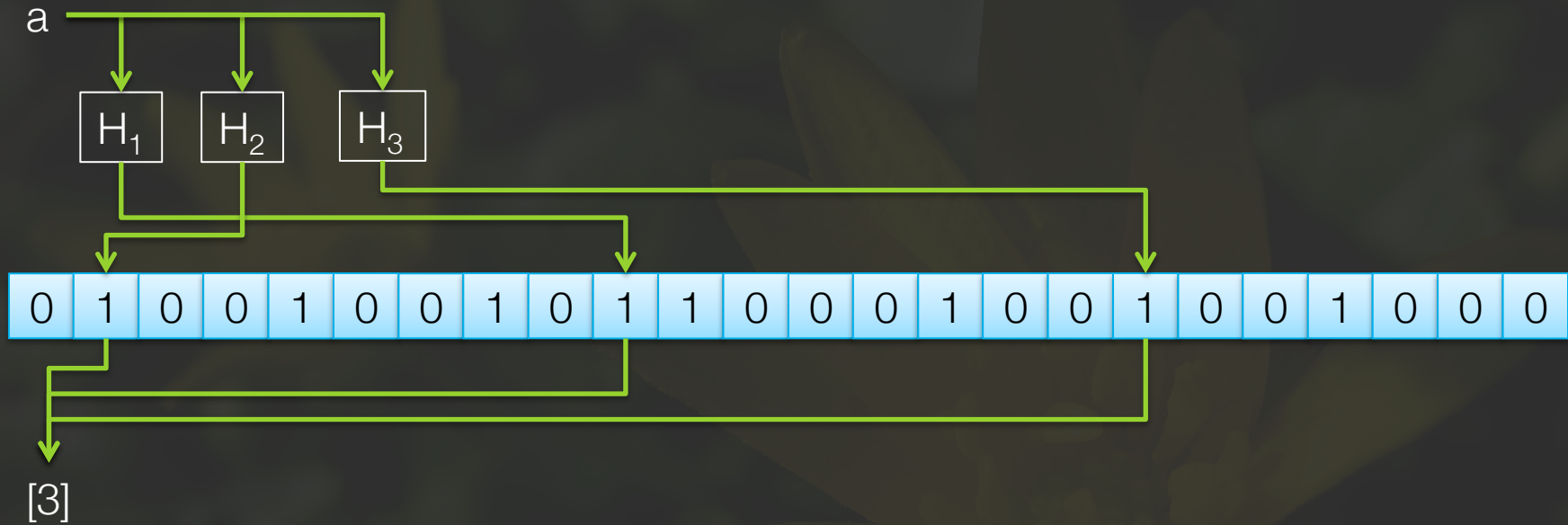
0 1 0 0 1 0 0 1 0 1 1 0 0 0 1 0 0 1 0 0 1 0 0 0

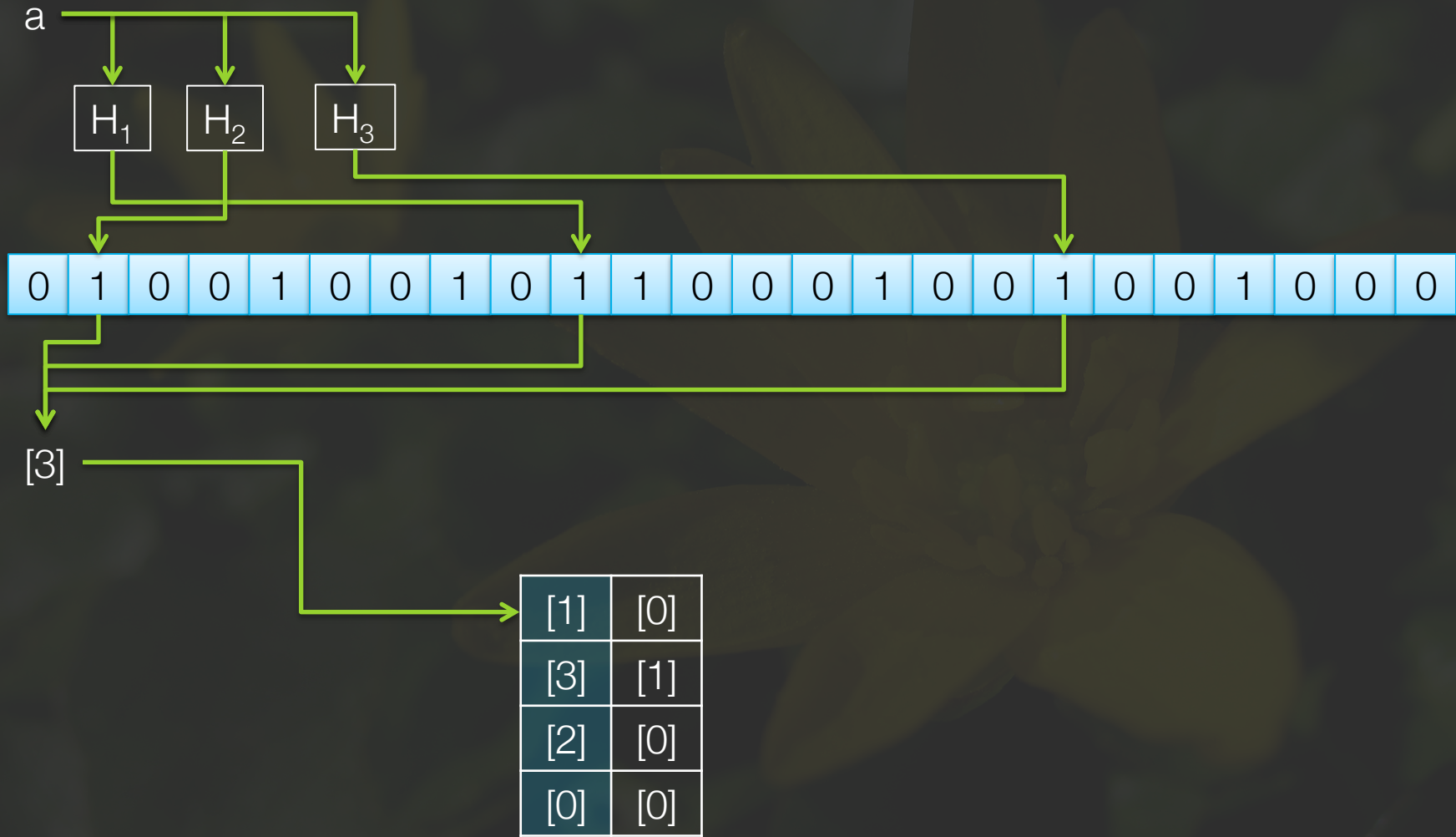


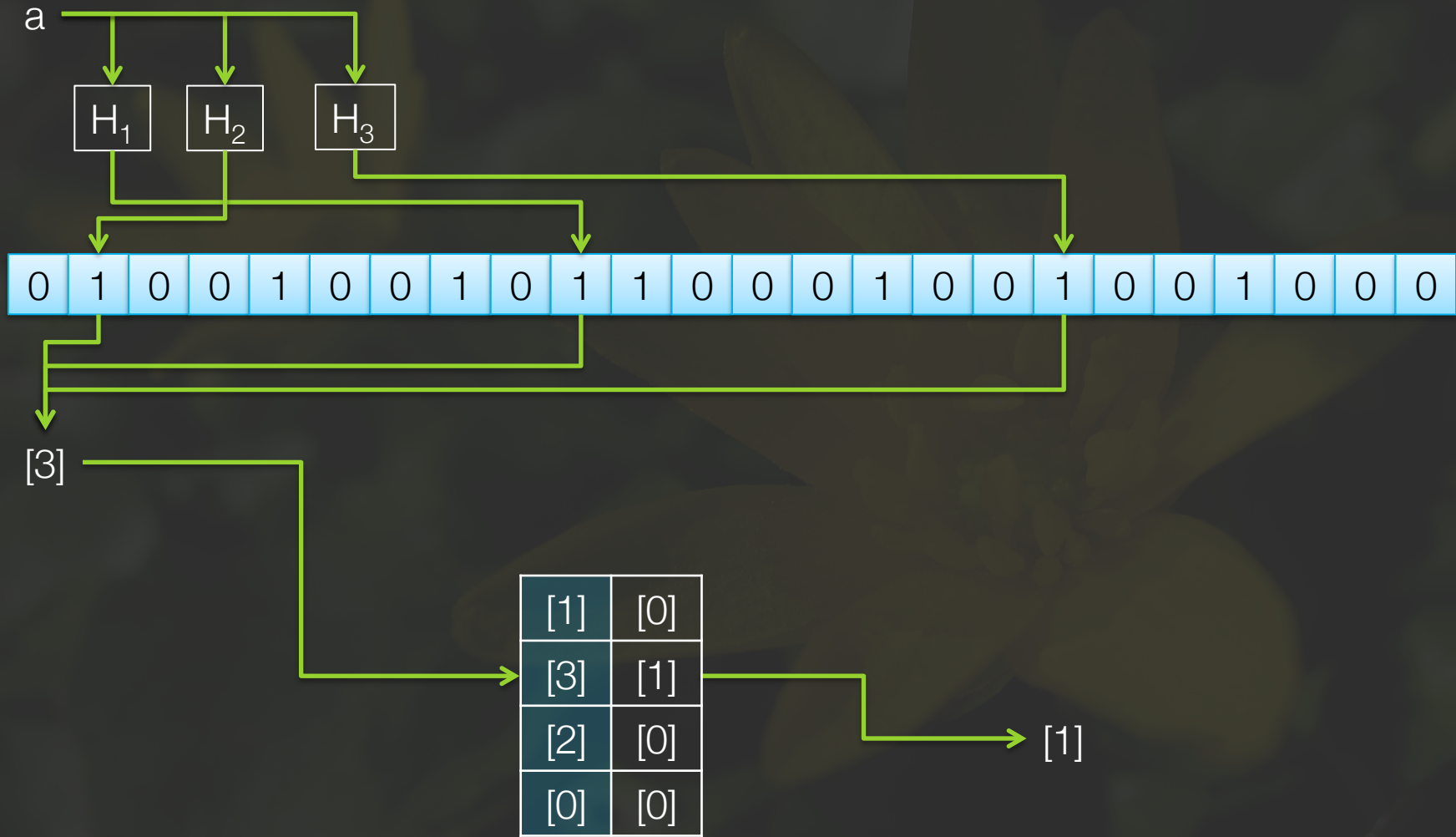




[0]	[0]
[1]	[0]
[2]	[0]
[3]	[1]





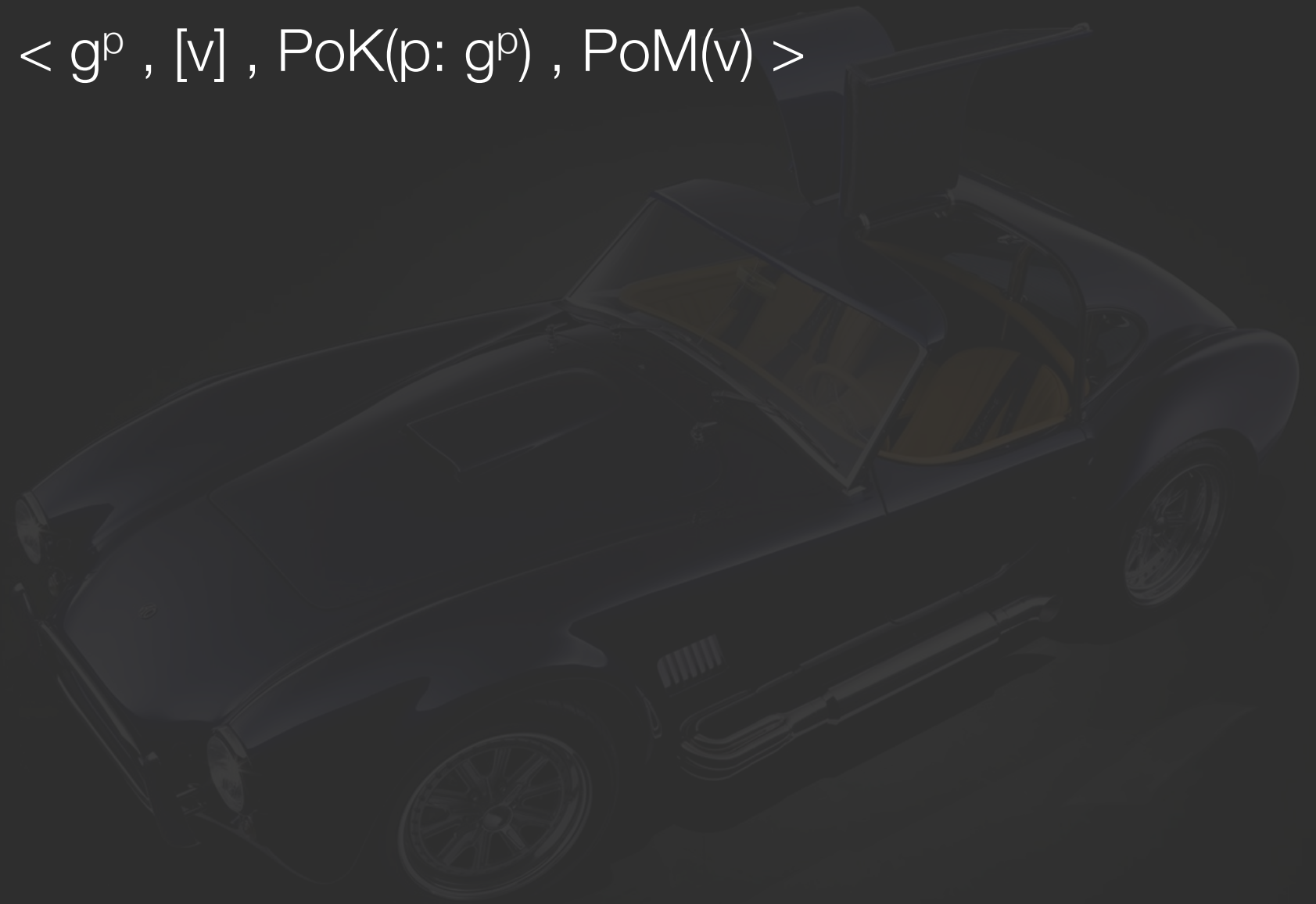




Cobra

- 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**

$\langle g^p, [v], \text{PoK}(p: g^p), \text{PoM}(v) \rangle$



$\langle g^p, [v], \text{PoK}(p: g^p), \text{PoM}(v) \rangle$

Check Proofs

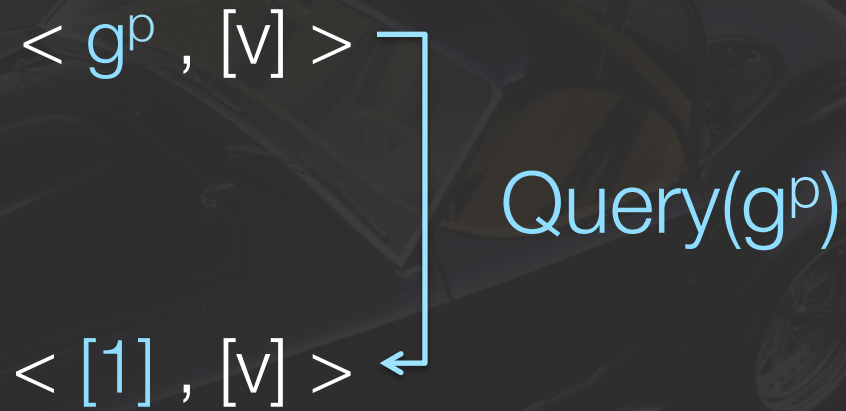
$\langle g^p, [v] \rangle$

$\langle g^p, [v], \text{PoK}(p: g^p), \text{PoM}(v) \rangle$

$\langle g^p, [v] \rangle$

Duplicate
Check

$\langle g^p, [v], \text{PoK}(p: g^p), \text{PoM}(v) \rangle$



$\langle g^p, [v], \text{PoK}(p: g^p), \text{PoM}(v) \rangle$

$\langle g^p, [v] \rangle$

$\langle [1], [v] \rangle$

$\langle [v] \rangle$

Mix & Match:

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

$\langle g^{p^*}, [v], \text{PoK}(p: g^p), \text{PoM}(v) \rangle$

$\langle g^{p^*}, [v] \rangle$

$\langle [0], [v] \rangle$

$\langle [0] \rangle$

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

NEW HAVEN LINE DEPARTURES		NEW HAVEN LINE DEPARTURES		INFORMATION
REMARKS	TIME TRK DESTINATION	REMARKS	REMARKS	INFORMATION
MOUNT VERNON - 1ST STOP	4:15 1102N NEW HAVEN	CONNECTION TO MOUNTAIN	NEW YORK FROM THE	PLEASE CHECK FOR THE
RYE - 1ST STOP	4:25 1110D GREENWICH	NEW HAVEN - 1ST STOP	NEW YORK FROM THE	NEW YORK FROM THE
MOUNT VERNON - 1ST STOP	4:30 1127 NEW HAVEN	GREENWICH & 1ST STOP	NEW YORK FROM THE	NEW YORK FROM THE
GREENWICH - 1ST STOP	4:40 1108 NEW HAVEN	CONNECTION TO NEW HAVEN & 1ST STOP	NEW YORK FROM THE	NEW YORK FROM THE
STAMFORD - 1ST STOP	4:45 1104 NEW HAVEN	GREENWICH - 1ST STOP	NEW YORK FROM THE	NEW YORK FROM THE

← TICKET VENDING MACHINES

