# Efficient Receipt-Free Ballot Casting Resistant to Covert Channels

Ben Adida
C. Andrew Neff

EVT / WOTE
August 11th, 2009
Montreal, Canada

Andy uses a voting machine to prepare a ballot.

Andy wants to verify that the machine properly encrypted the ballot.

# Neff's MarkPledge and Moran-Naor.

# Two Problems.

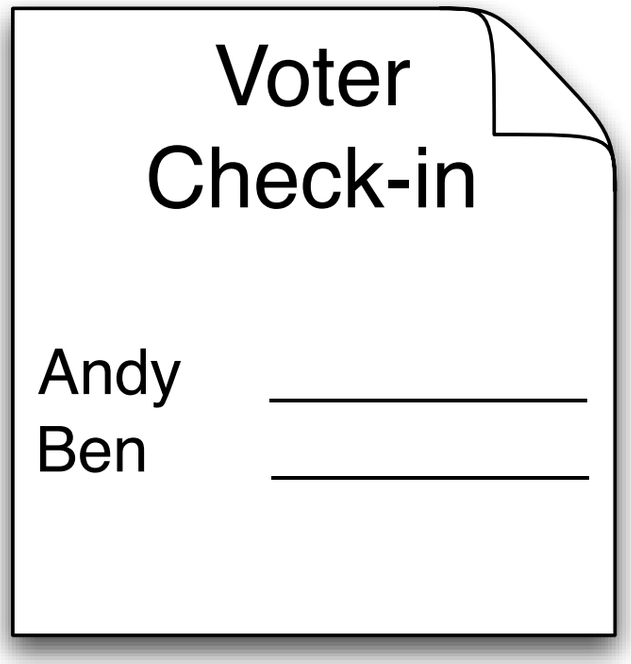
1) 2 ciphertexts per challenge bit (40-50)
2) machine can use ballot to leak plaintext.

# MarkPledge2

- efficient ballot encoding:
  2 ciphertexts for any challenge length
- covert-channel resistance:
  no leakage via the ballot.
- voting machine is significantly simplified.
  - ➡ simpler voting machine = less chance of errors.

# Voter Experience

# Voter Experience



# Voter Experience

Voter
Check-in

Andy VHTI

Ben

# Voter Experience

Voter
Check-in

Andy VHTI

Ben

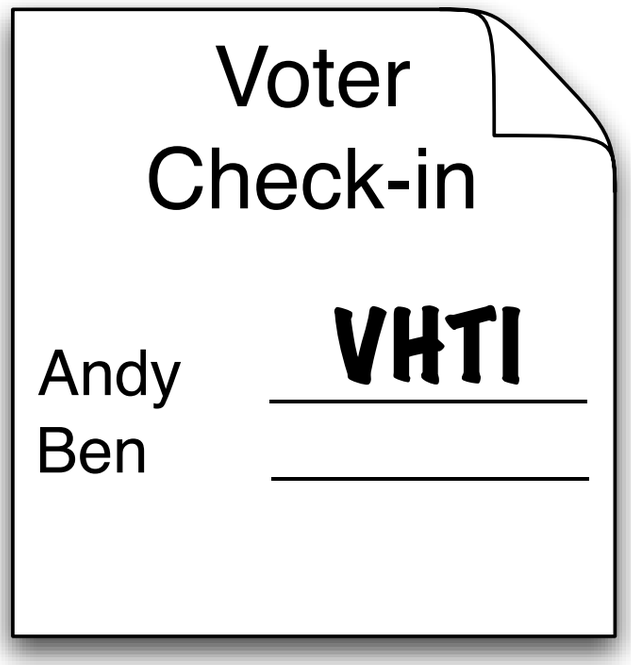
Hillary ☐

Barack ☐

John ☐

Bill ☐

# Voter Experience




# Voter Experience

Voter
Check-in

Andy VHTI

Ben

Hillary ☐

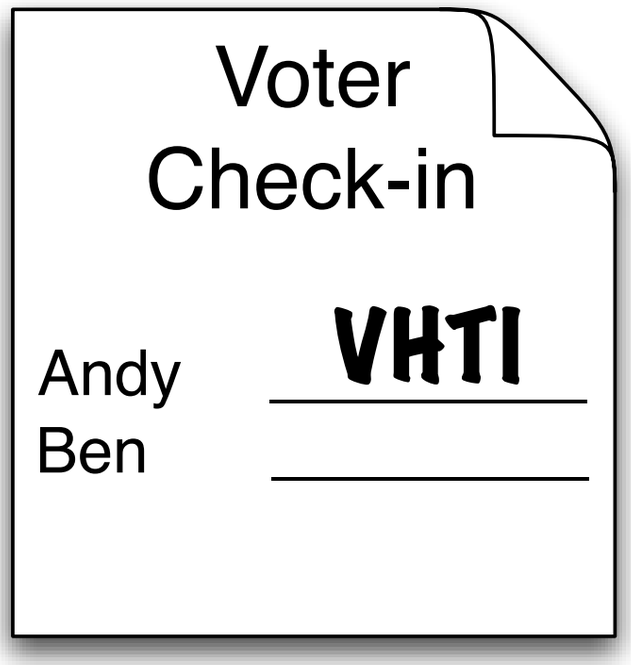
Barack ☑

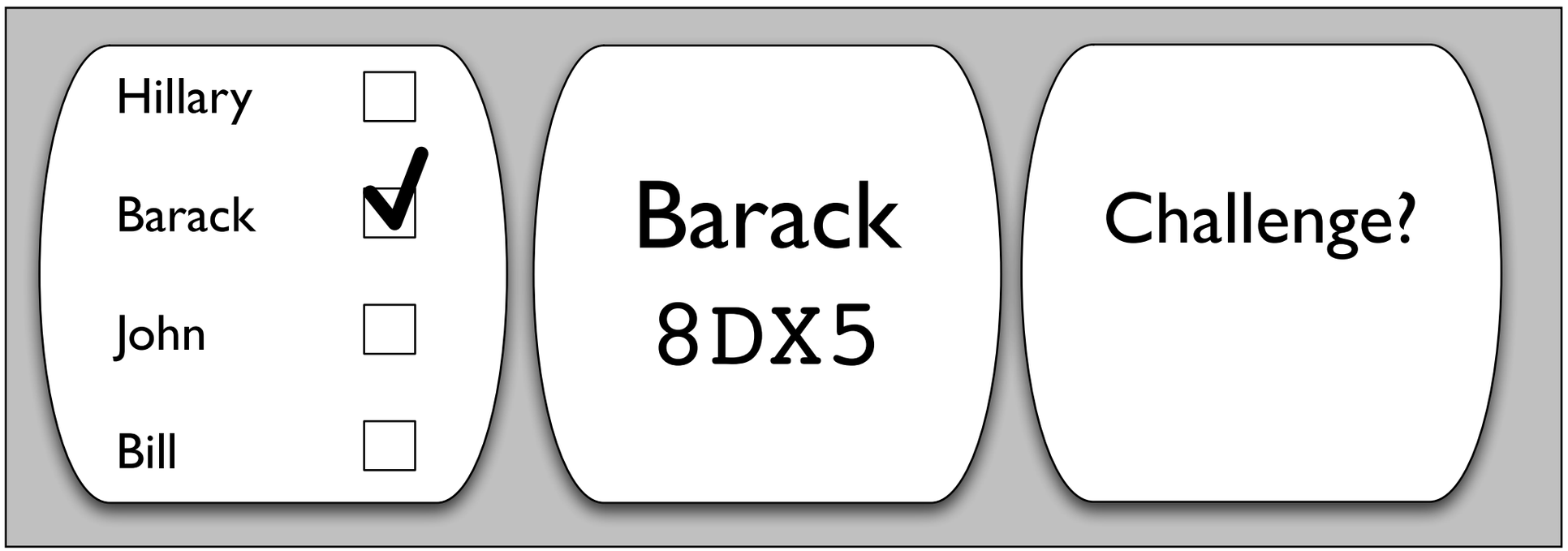
John ☐

Bill ☐

Barack
8DX5

# Voter Experience



# Voter Experience

Voter
Check-in

Andy VHTI

Ben

Hillary ☐

Barack ☑

John ☐

Bill ☐

Barack
8DX5

Challenge?
VHTI

# Voter Experience

Voter Check-in

Andy VHTI

Ben

Receipt

| | |
|---|---|
| Hillary | MCN3 |
| Barack | 8DX5 |
| John | I341 |
| Bill | LQ21 |

Challenge

VHTI

- [ ] Hillary
- [x] Barack
- [ ] John
- [ ] Bill

Barack

8DX5

Challenge?

VHTI

# Voter Experience

Voter Check-in

Andy VHTI

Ben

Receipt

| | |
|---|---|
| Hillary | MCN3 |
| Barack | 8DX5 |
| John | I341 |
| Bill | LQ21 |

Challenge

VHTI

Hillary ☐

Barack ☑

John ☐

Bill ☐

Barack

8DX5

Challenge?

VHTI

# Voter Experience

Voter Check-in

Andy VHTI

Ben

Receipt

| | |
|---|---|
| Hillary | MCN3 |
| Barack | 8DX5 |
| John | I341 |
| Bill | LQ21 |

Challenge

VHTI

Hillary ☐

Barack ☑

John ☐

Bill ☐

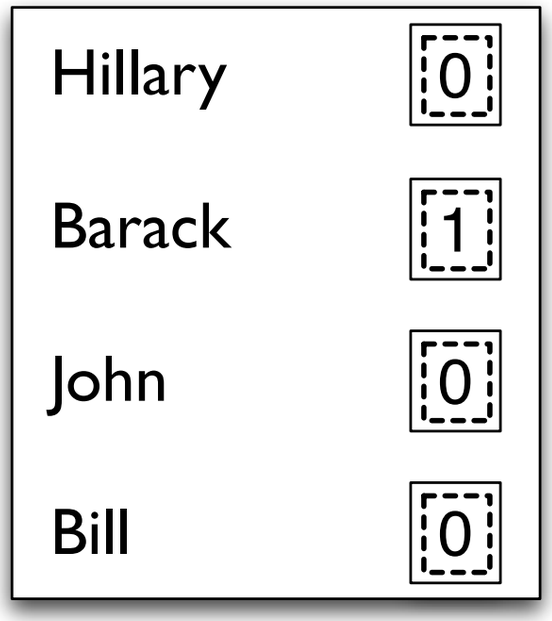
Barack

8DX5

Challenge?

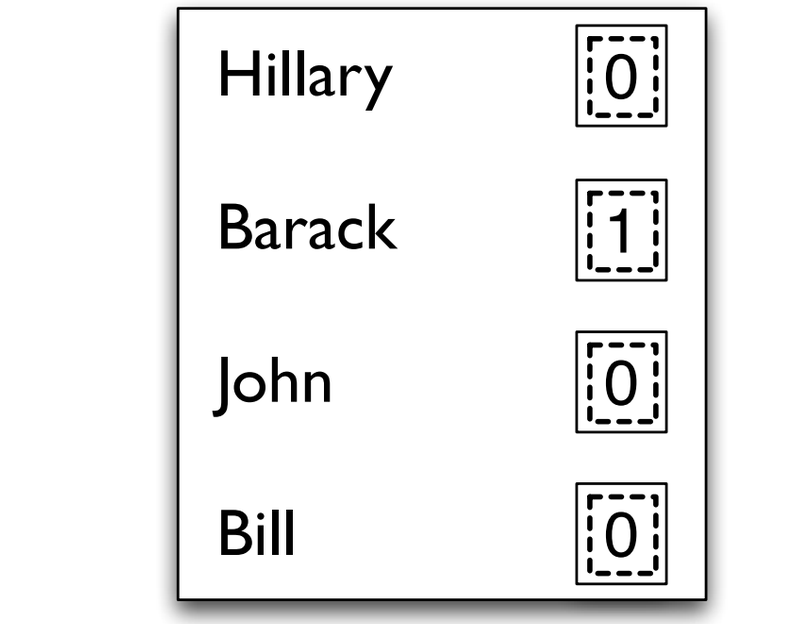
VHTI

# Special Bit Encryption




- Encrypt a 0 or 1 for each candidate
- Special proof protocol
  - ➡ for bit b=1
  - ➡ meaningful short strings as part of the commitment
  - ➡ short challenge strings for real and simulated proofs

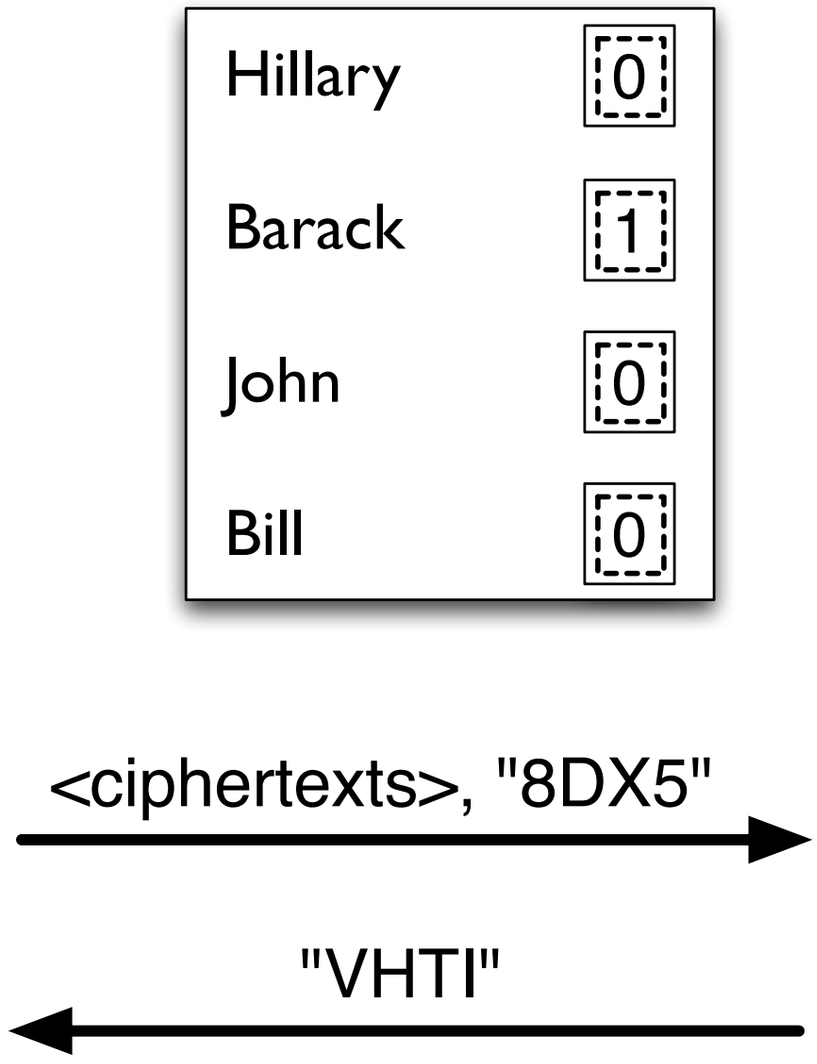
# Special Bit Encryption




<ciphertexts>, "8DX5"

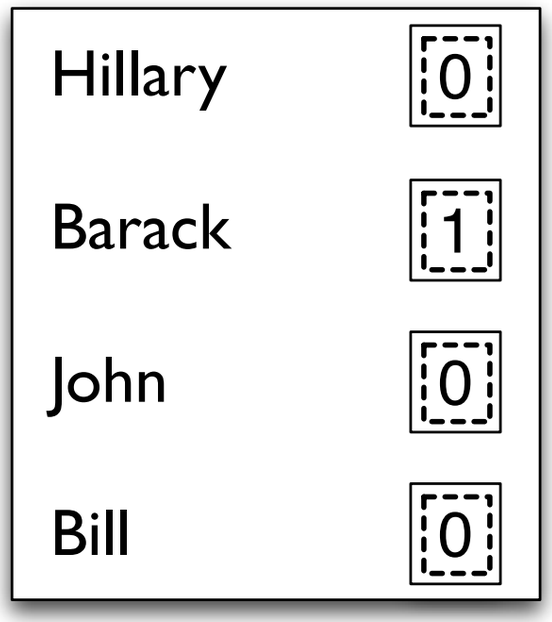
- Encrypt a 0 or 1 for each candidate
- Special proof protocol
  - ➡ for bit b=1
  - ➡ meaningful short strings as part of the commitment
  - ➡ short challenge strings for real and simulated proofs

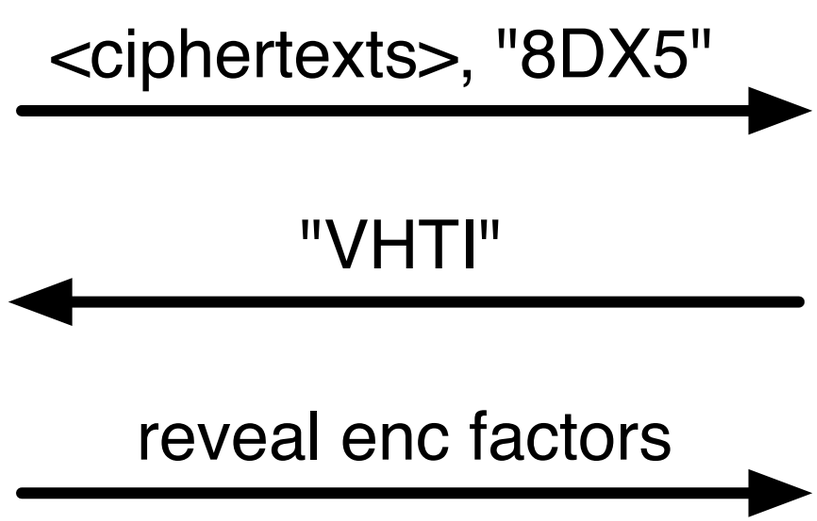
# Special Bit Encryption




- Encrypt a 0 or 1 for each candidate
- Special proof protocol
  - ➡ for bit b=1
  - ➡ meaningful short strings as part of the commitment
  - ➡ short challenge strings for real and simulated proofs

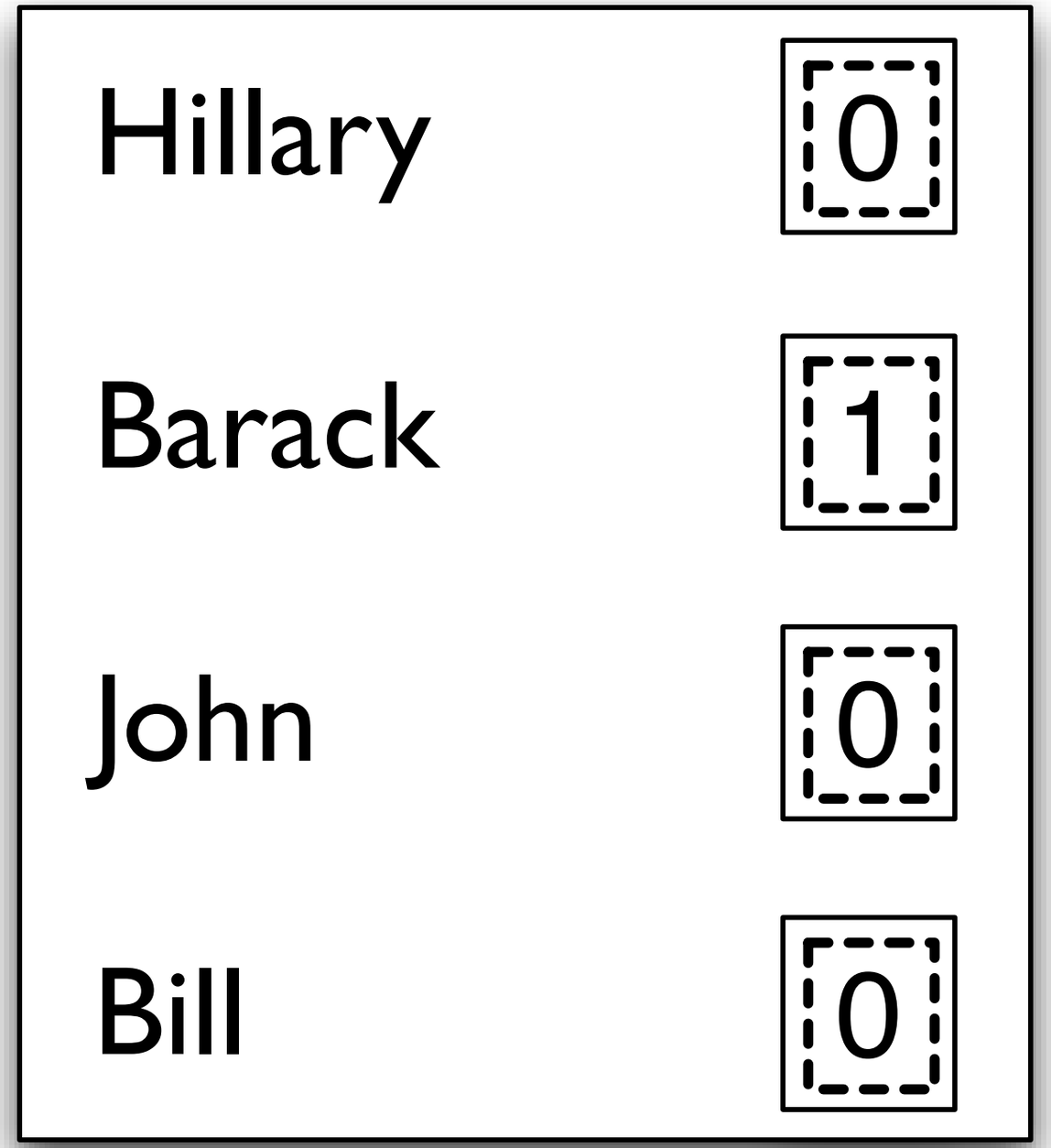
# Special Bit Encryption



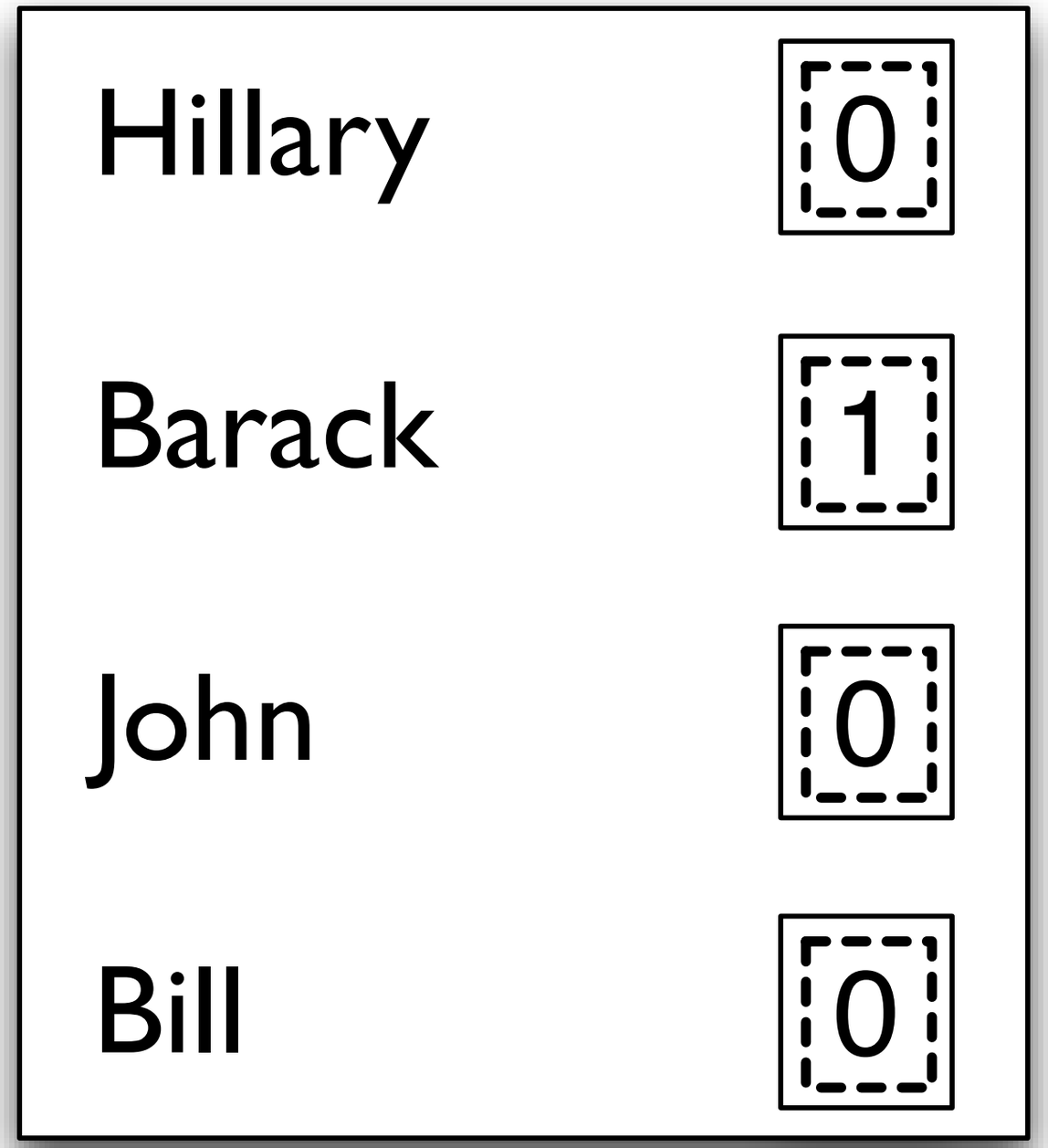




- Encrypt a 0 or 1 for each candidate
- Special proof protocol
  - ➡ for bit b=1
  - ➡ meaningful short strings as part of the commitment
  - ➡ short challenge strings for real and simulated proofs

# Voter Experience (II)



# Voter Experience (II)



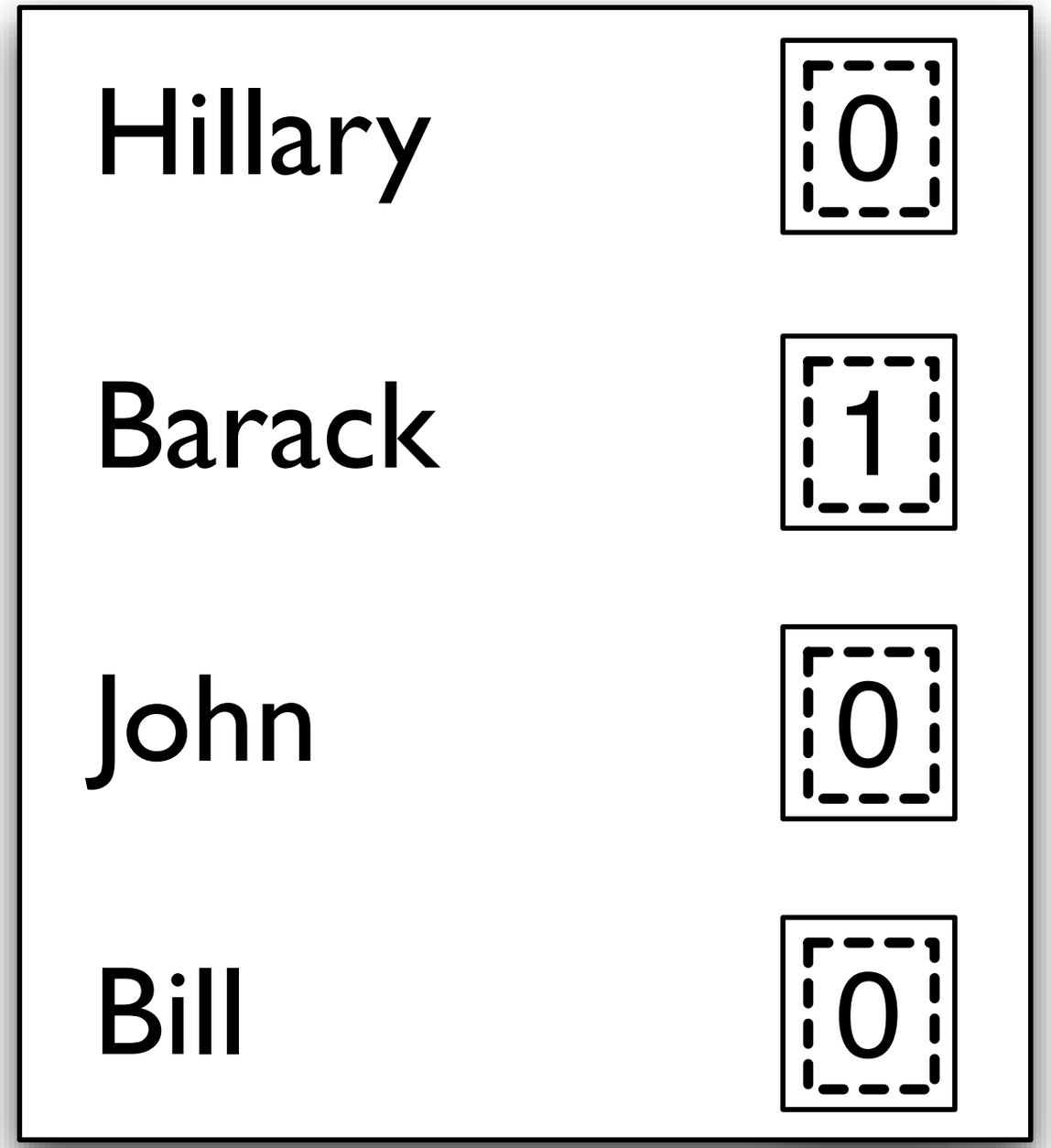

<ciphertexts>,

<ciphertexts>, "8DX5"

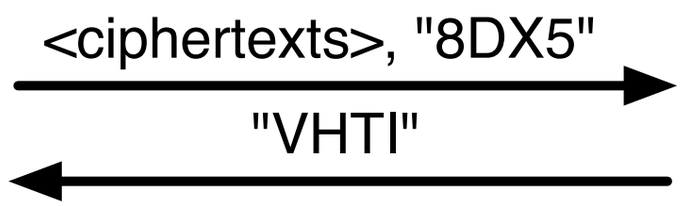
<ciphertexts>,

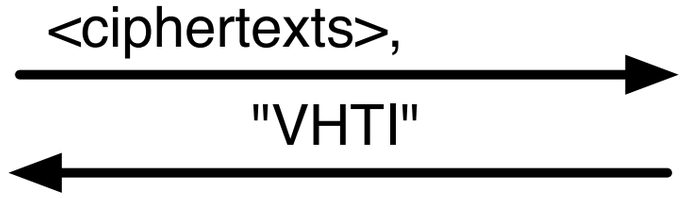
<ciphertexts>,

# Voter Experience (II)

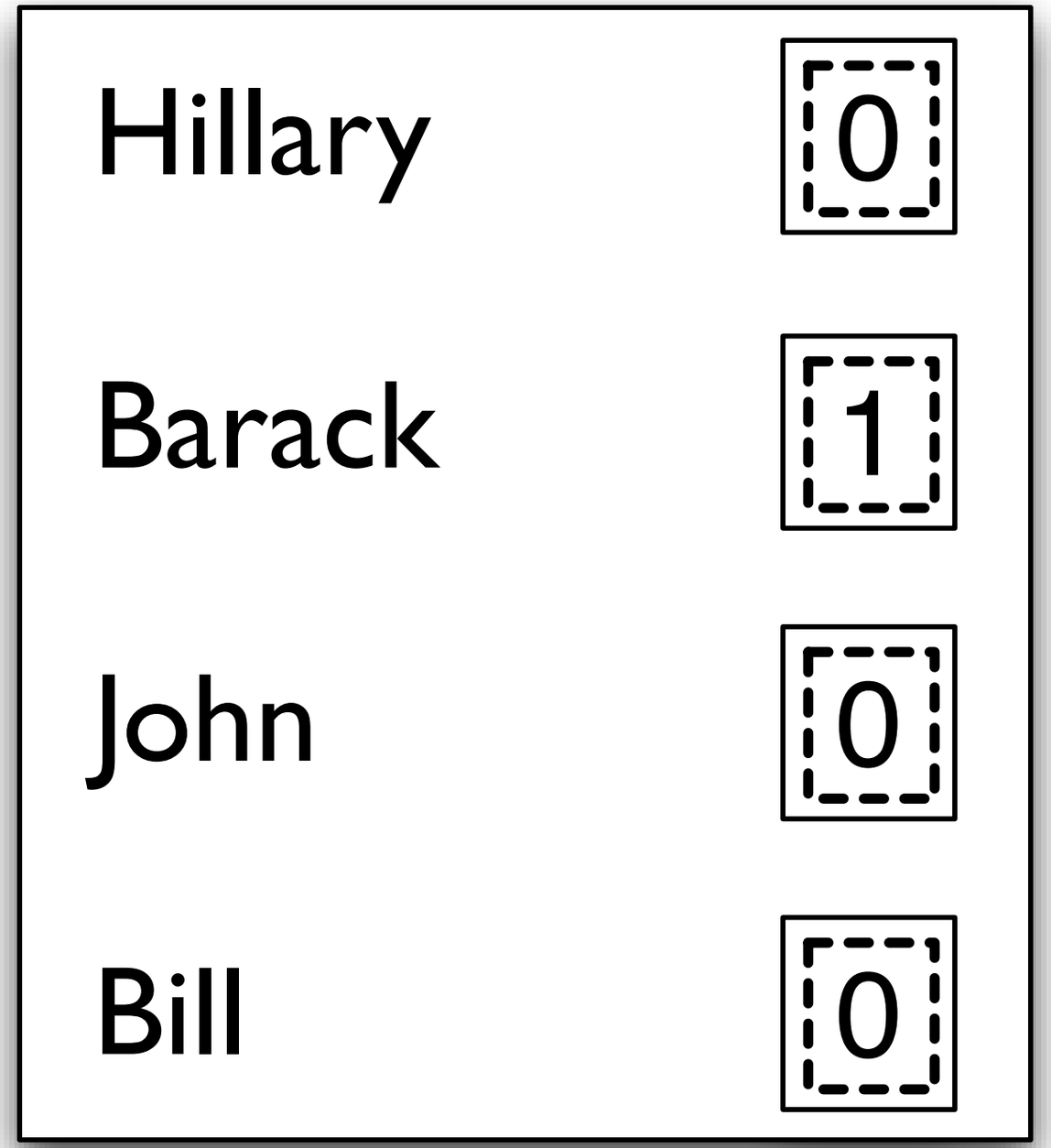


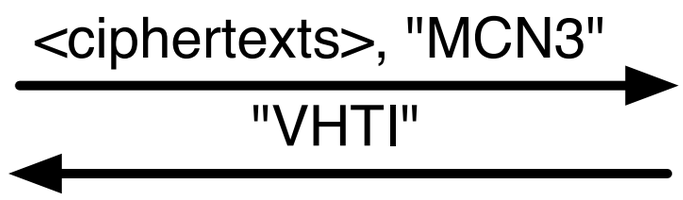


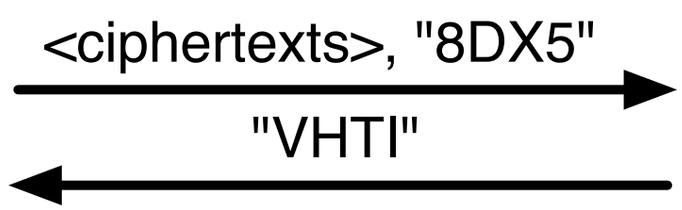


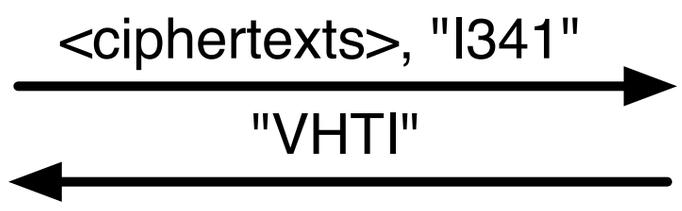



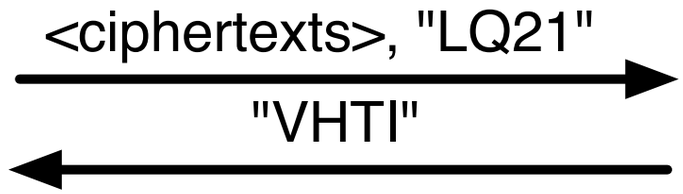

# Voter Experience (II)



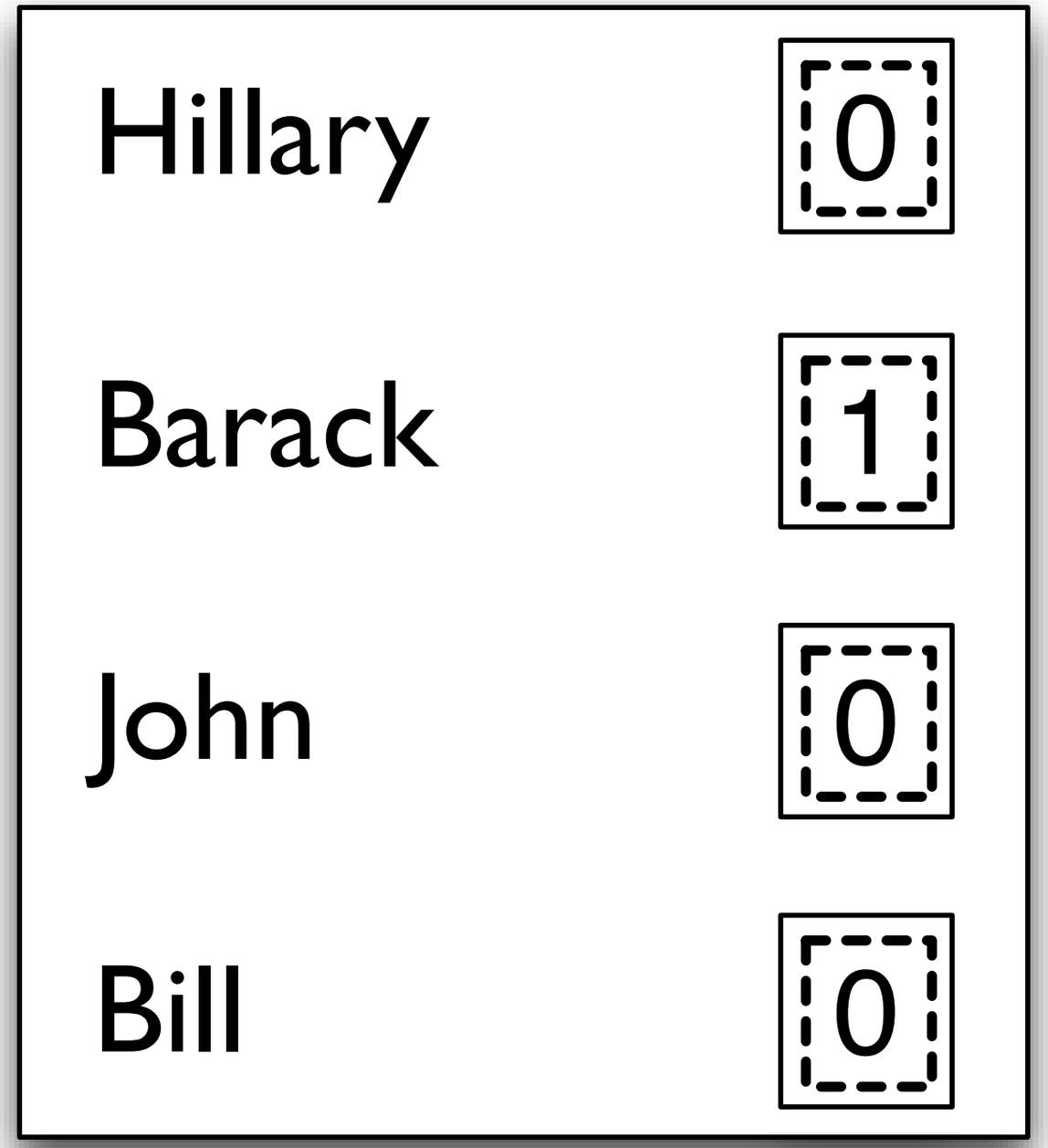



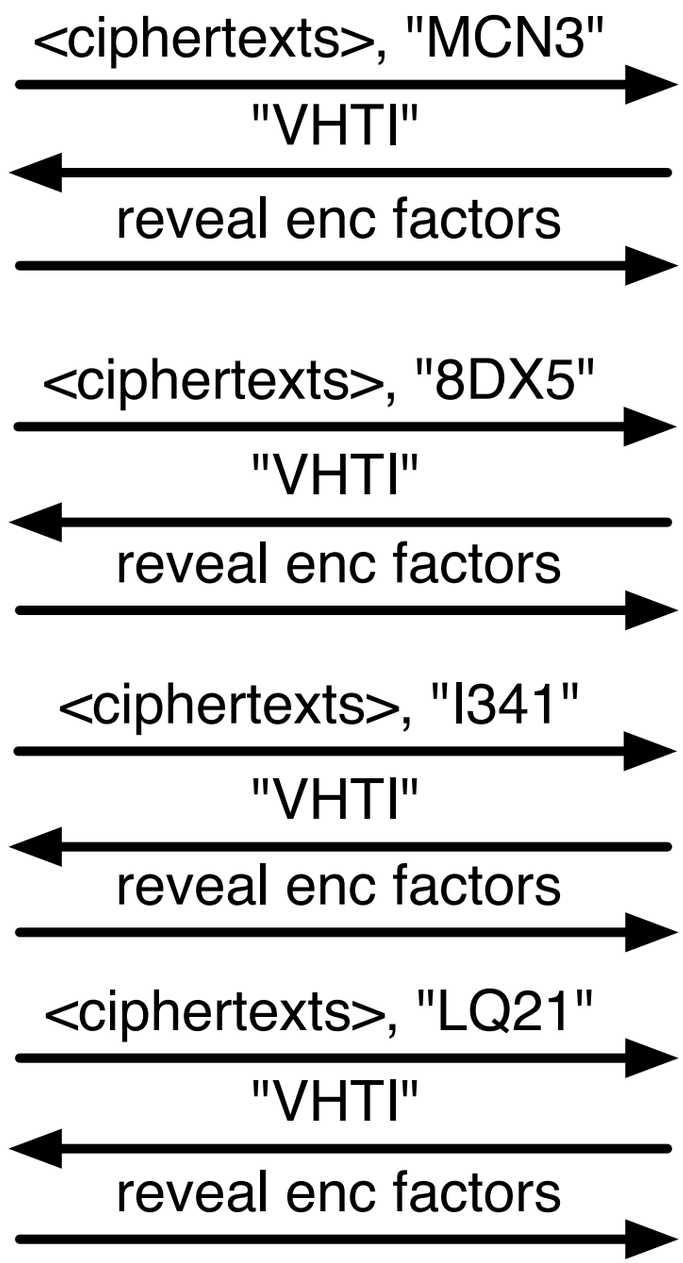



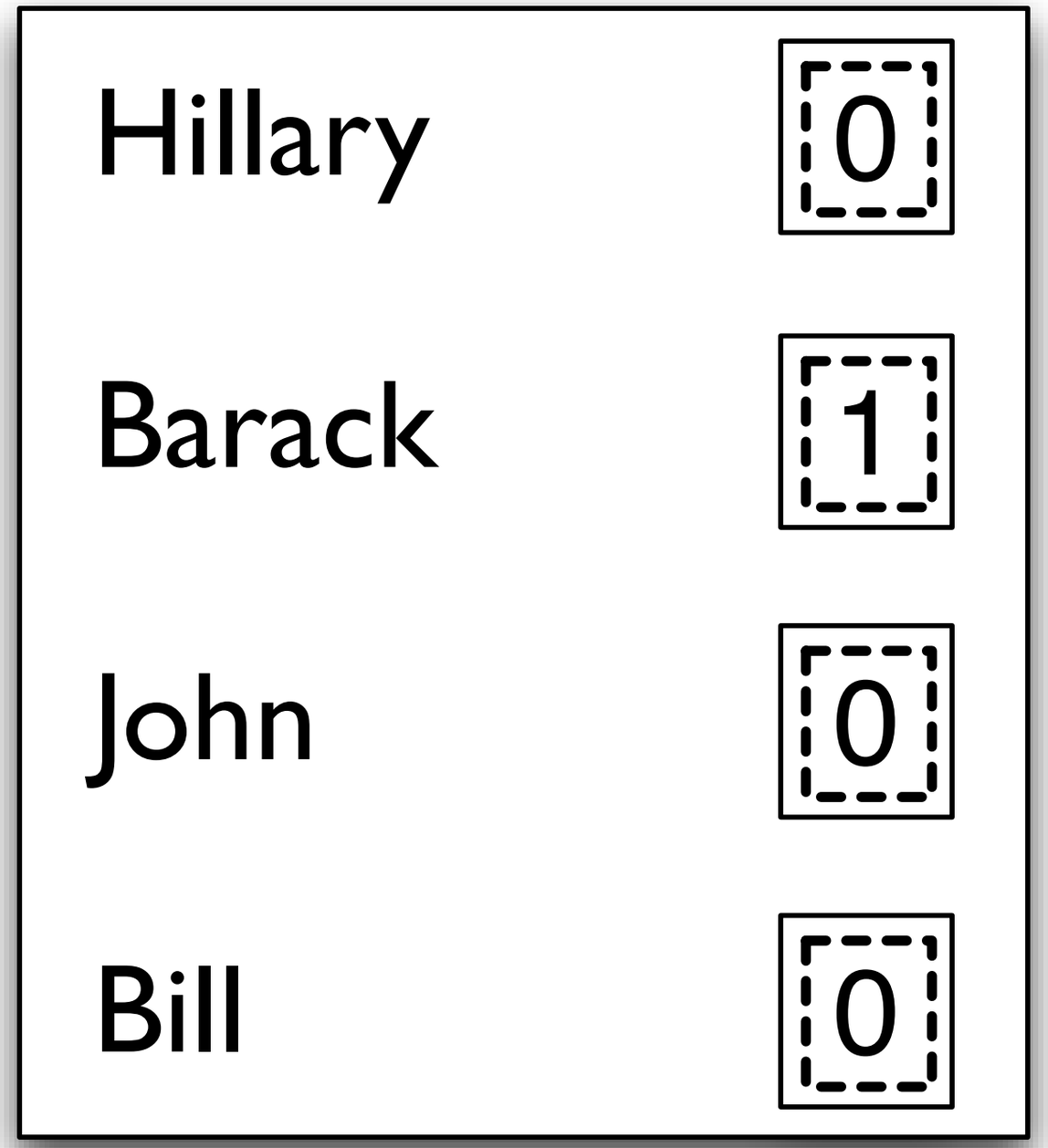



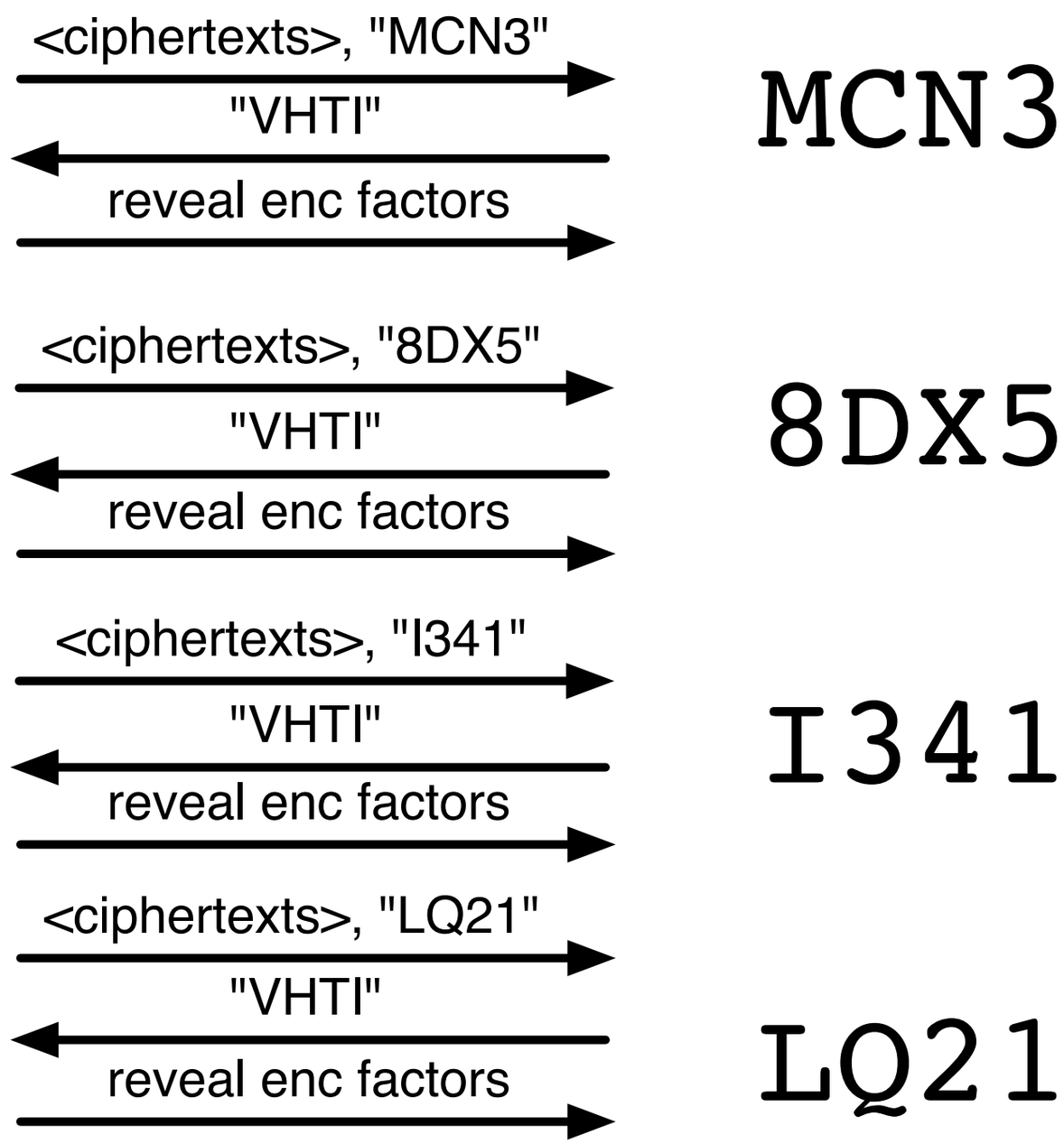
# Voter Experience (II)



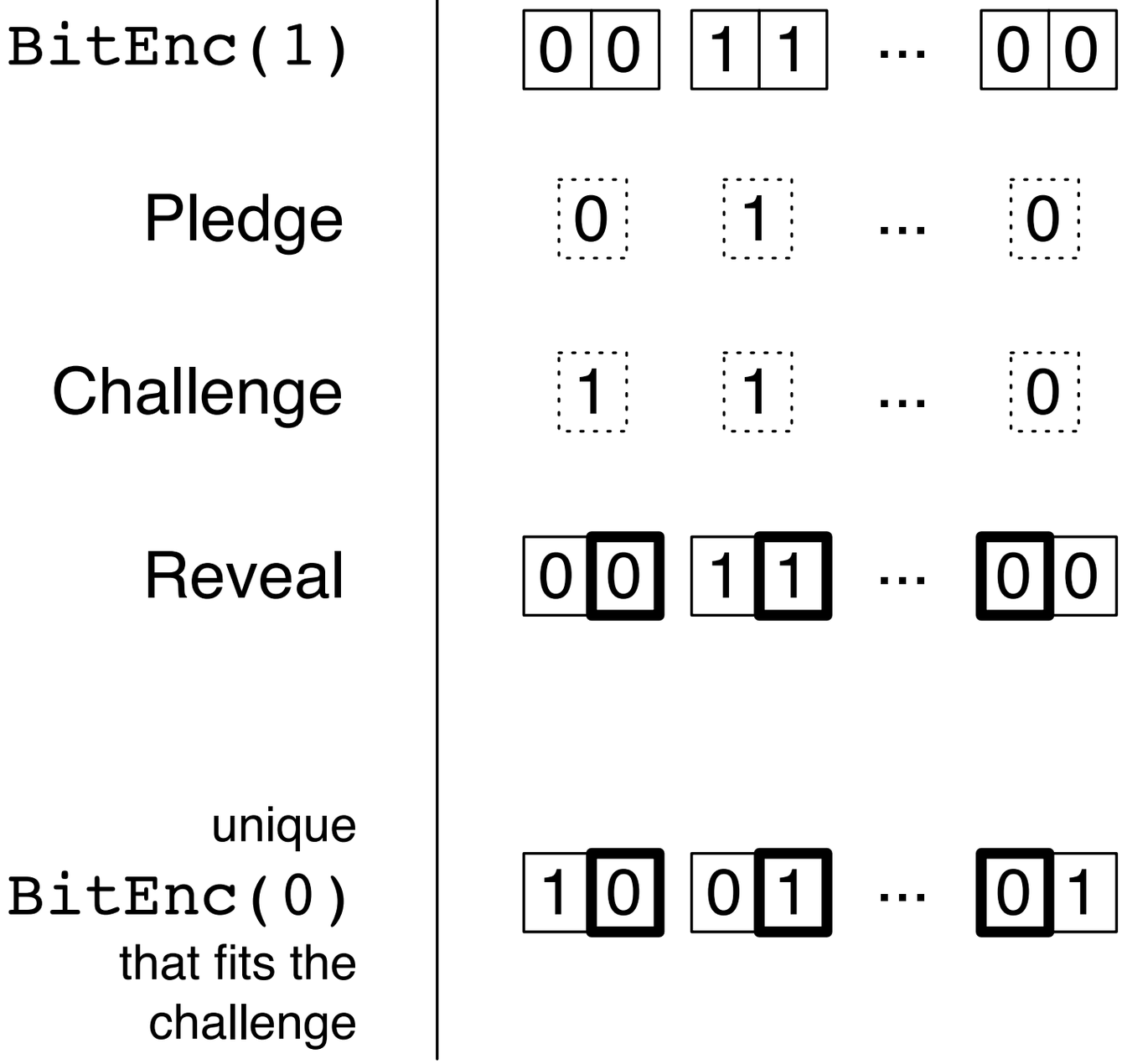



# Voter Experience (II)

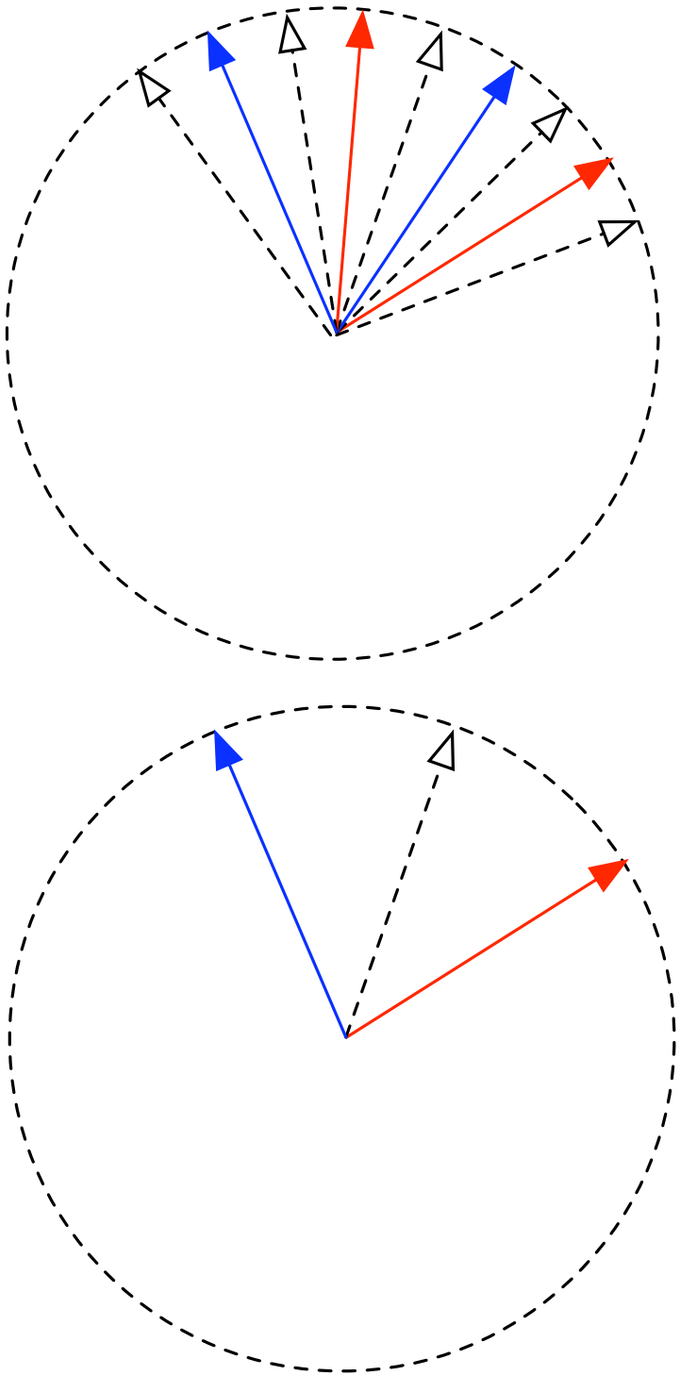


# MarkPledge & Moran-Naor

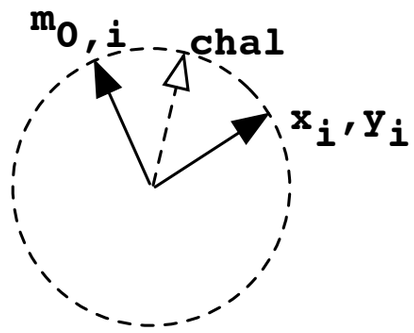


# Markpledge 2



- different bit encryption
- $(\alpha, \beta) \in Z_q^2$, with $\alpha^2 + \beta^2 = 1$
  - ➡ isomorphic to $SO(2, q)$
  - ➡ operation is rotation (matrix mult.)
- Designate 1-, 0-, and T-vectors
  - ➡ any pair of a 1-vector and 0-vector bisected by a test vector
  - ➡ dot-product with test vector.

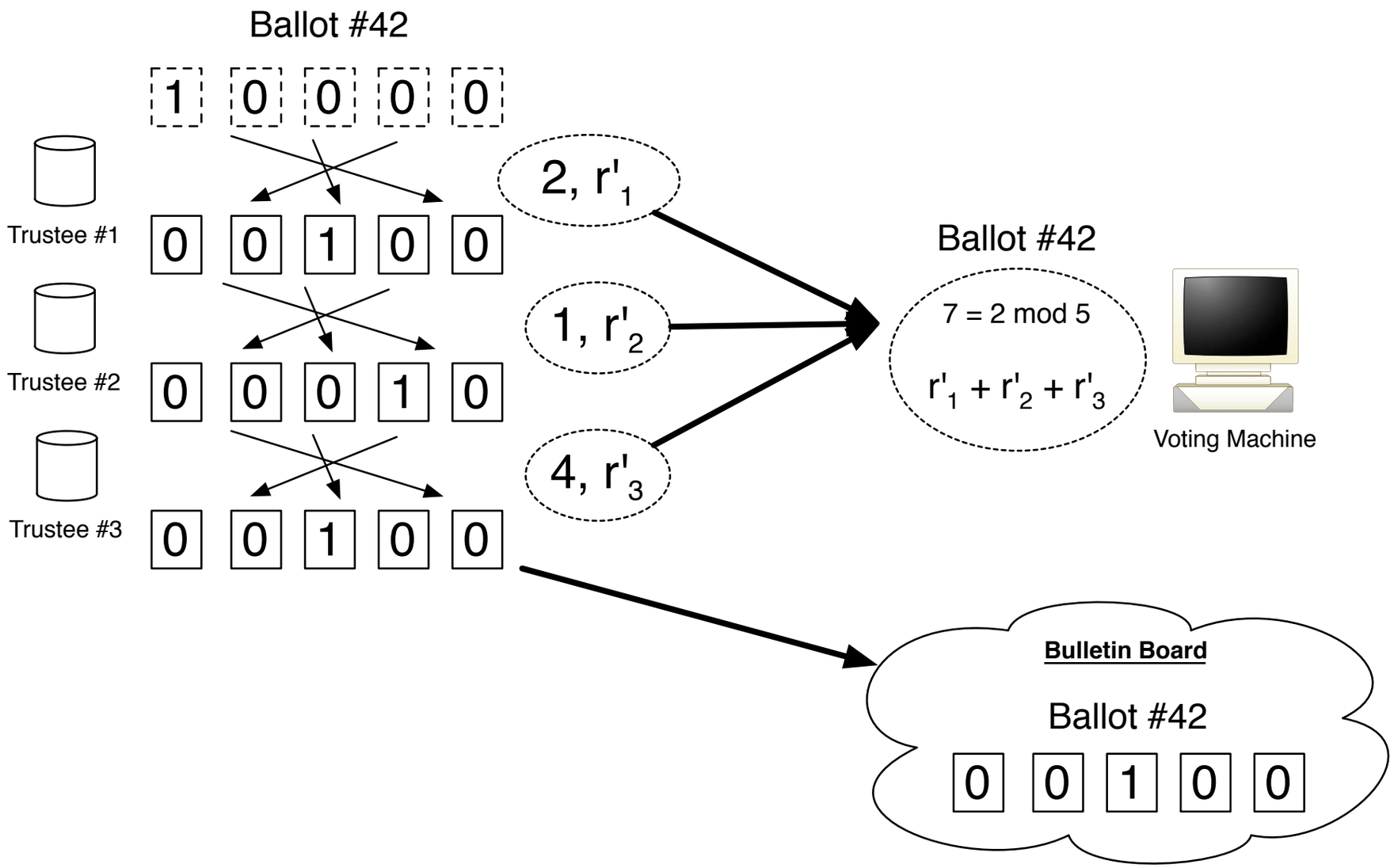
# Same pattern emerges

| | MarkPledge | MarkPledge2 |
|---|---|---|
| `BitEnc(1)` | 0 0 \| 1 1 \| … \| 0 0 | $x_i$ $y_i$ |
| Pledge | 0 1 … 0 | i |
| Challenge | 1 1 … 0 | $x_C, y_C$ |
| Reveal | 0 0 \| 1 1 \| … \| 0 0 | $x_C x_i + y_C y_i$ |
| unique `BitEnc(0)` that fits the challenge | 1 0 \| 0 1 \| … \| 0 1 |  |

# Covert Channel

- Raised by Karloff, Sastry & Wagner
- If the voting machine chooses the random factor, it can embed info
- Can we make the voting machine fully deterministic given a voter ID and a selection in a given race?

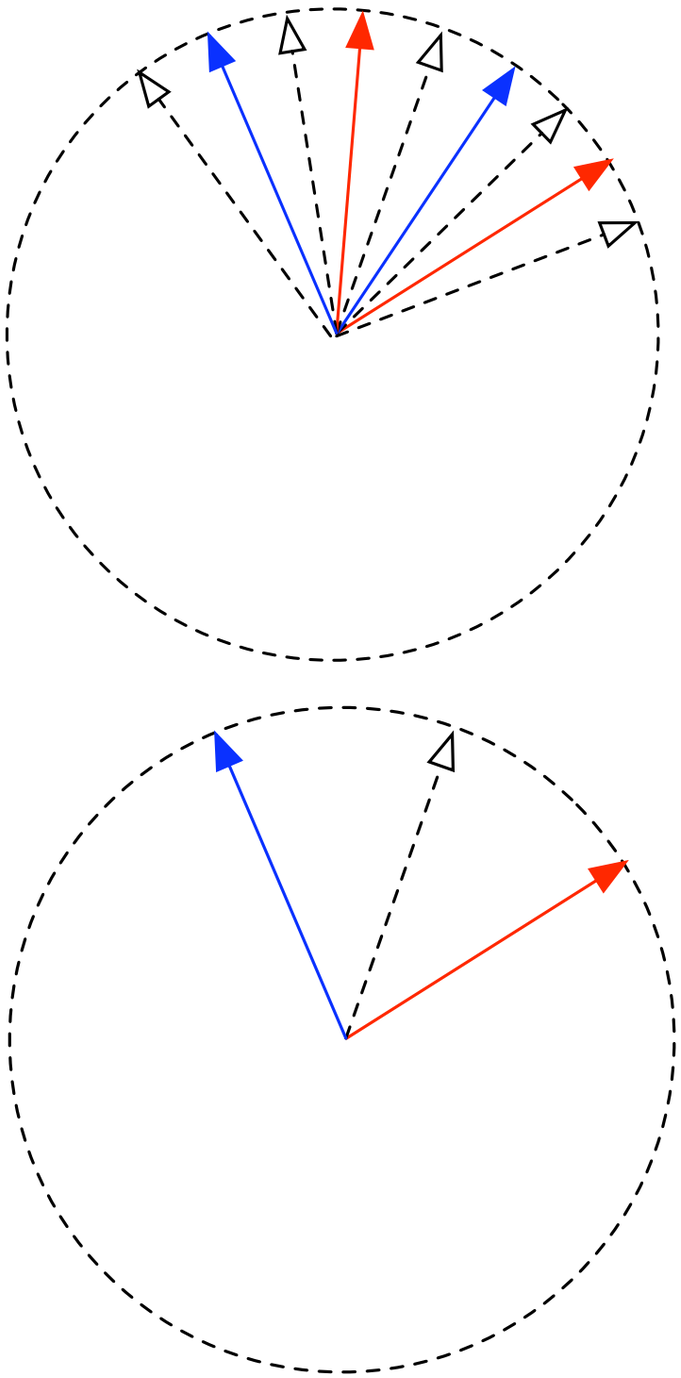
# Covert Channel




- Pre-generate ciphertexts with trustees
- Rotate them on voter selection

# Why is this receipt-free?

- What can the coercer ask the voter to do that affects the ballot / receipt?
- Only the challenge, which is selected before the voter enters the booth.
- All proofs will look the same, whether real or simulated.



# Questions?