THE CASE FOR NETWORKED REMOTE VOTING PRECINCTS

Daniel R. Sandler and Dan S. Wallach
Rice University

EVT '08
2008 USENIX/ACCURATE Electronic Voting Technology workshop | July 28, 2008

When I talk to my father about e-voting

he always asks the same question

“When will we be able to vote over the internet?”

This is a (mostly) reasonable question!

We can now do almost anything over the internet

remotely! *reliably!* *securely!*

(when was the last time you went in to a bank?)

the expectation exists:

“surely this must be possible”

“When will we be able to vote over the internet?”

“When will we be able to vote over the internet?”

The “right answer” from a security standpoint is

“When will we be able to vote over the internet?”

The “right answer” from a security standpoint is

NEVER

voting is special

unlike *entertainment* **&** *communication* **&** *banking*

a physical presence is absolutely essential

why?

EQUIPMENT

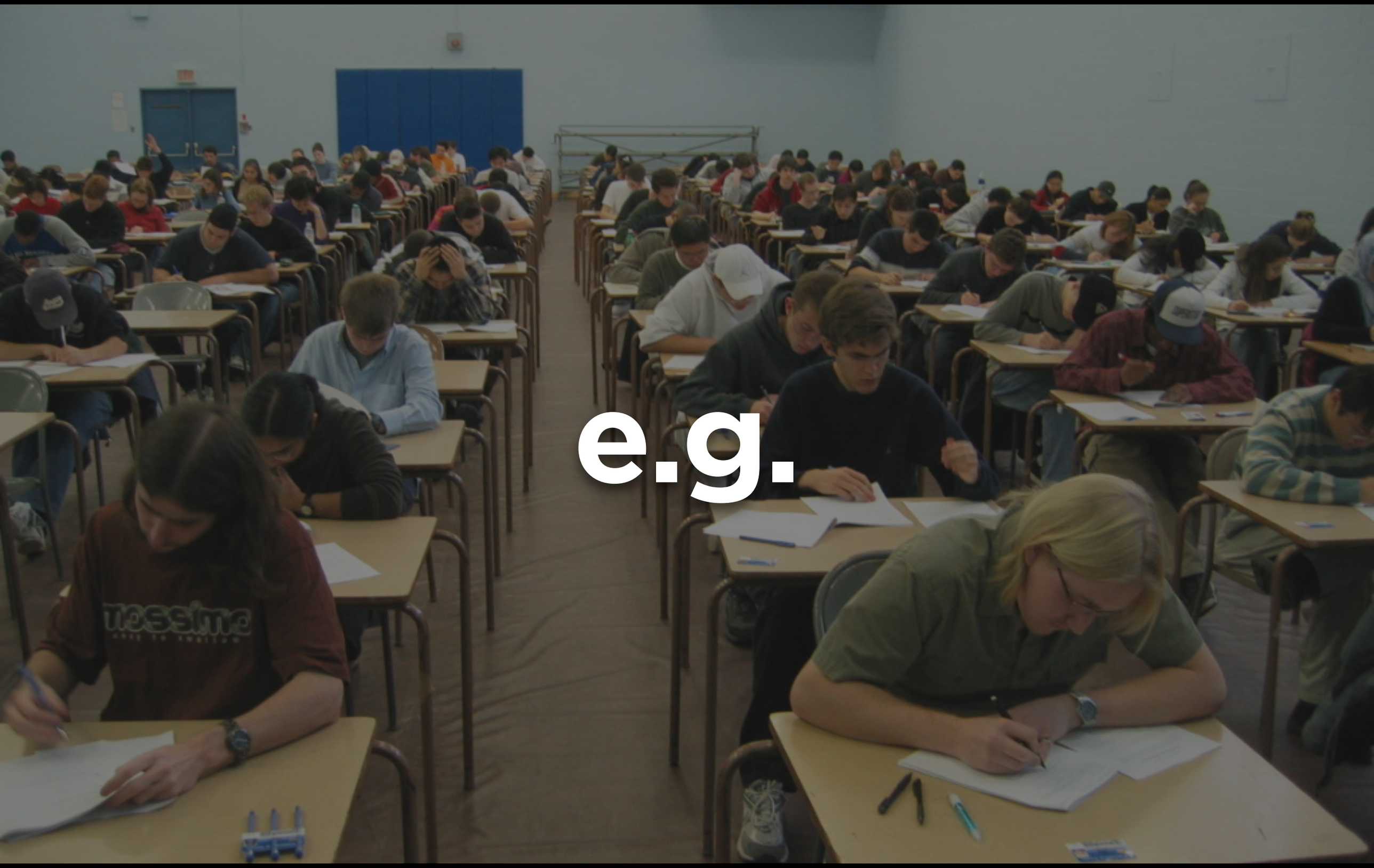
ENVIRONMENT

EQUIPMENT

the voting terminal must be trusted

the voter must be free of coercion

ENVIRONMENT



e.g.

voting at home may *never* be practical or secure

voting at home may *never* be practical or secure

remote voting may be both practical and secure

HOW?

we propose a solution inspired by

PROVISIONAL & **POSTAL** VOTING

but relying on e-voting technology

POSTAL VOTING

POSTAL VOTING

aka “vote-by-mail”

POSTAL VOTING

aka “vote-by-mail”

voters declare intent to vote by mail

POSTAL VOTING

aka “vote-by-mail”

voters declare intent to vote by mail

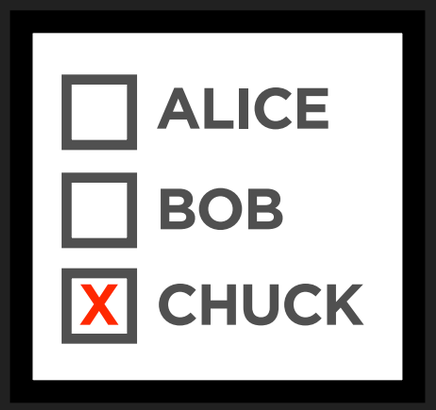
ballots are mailed in advance of the election

POSTAL VOTING

aka “vote-by-mail”

voters declare intent to vote by mail

ballots are mailed in advance of the election

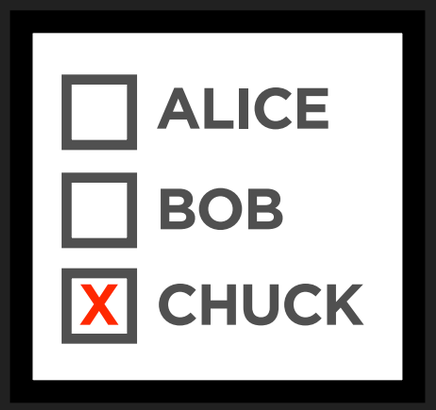


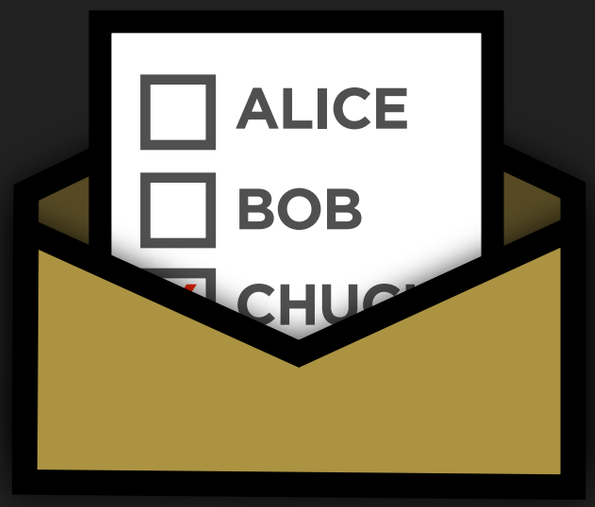
POSTAL VOTING

aka “vote-by-mail”

voters declare intent to vote by mail

ballots are mailed in advance of the election



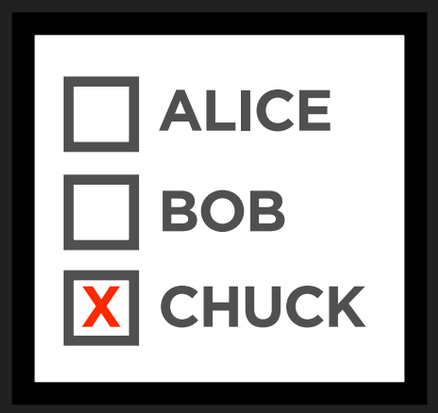


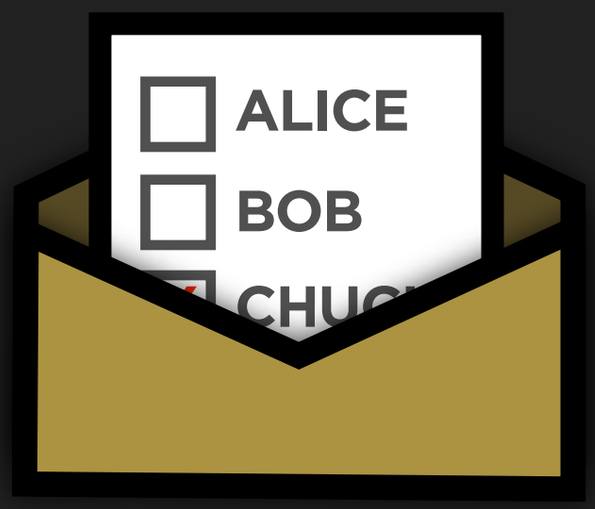
POSTAL VOTING

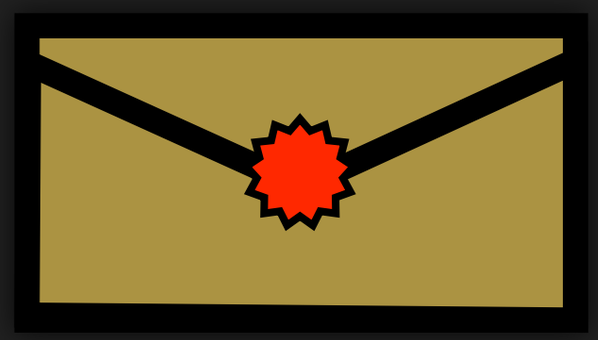
aka “vote-by-mail”

voters declare intent to vote by mail

ballots are mailed in advance of the election

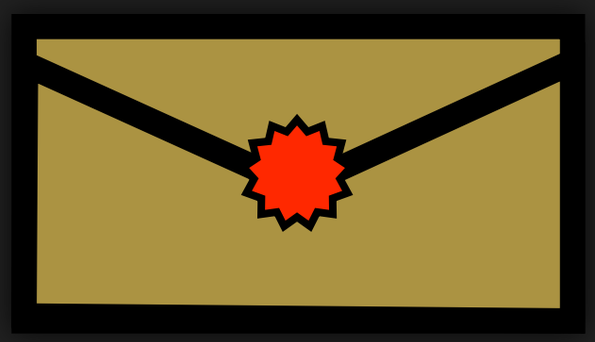






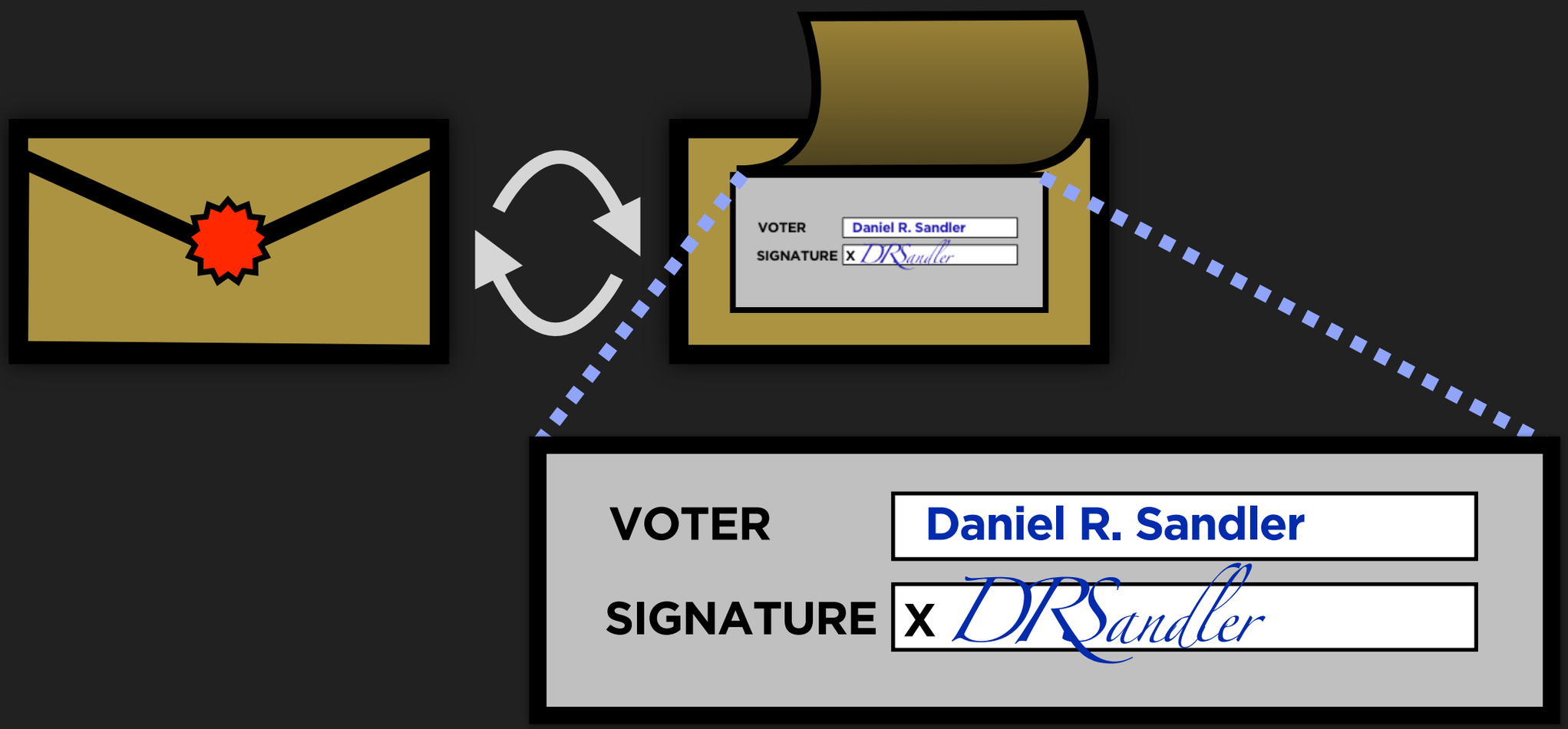
POSTAL VOTING

POSTAL VOTING

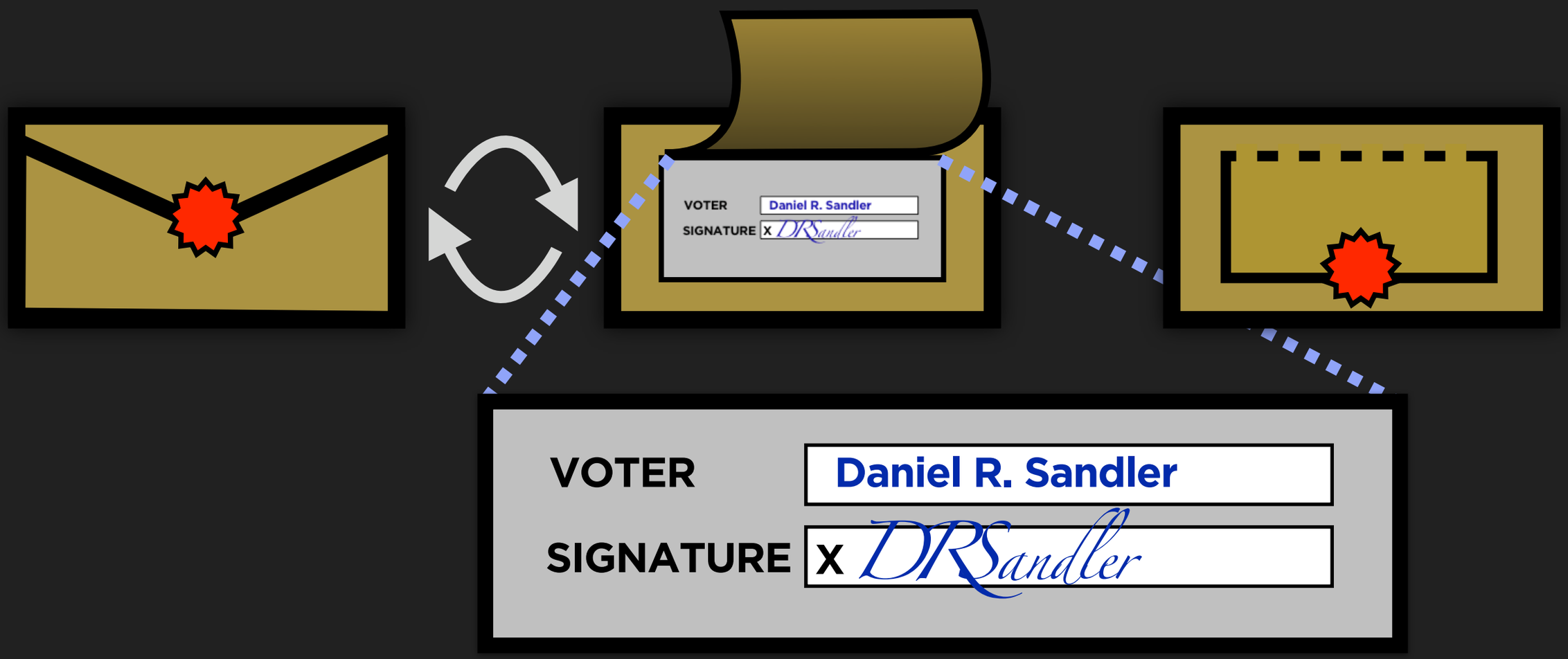


POSTAL VOTING

POSTAL VOTING



POSTAL VOTING



PROVISIONAL VOTING

Similar to postal voting, but in a polling place

Voter and pollworkers disagree about eligibility

Voter casts a ballot anyway

Ballot sealed in an opaque envelope w/ voter's identifying info & claim of eligibility

The double enclosure

Allows election officials to decide whether to count a vote before the vote is revealed

Our objectives

1. obviate voter's need to be at "home"
2. replace (unreliable, slow) postal channel with networked transmission

Ingredients

Electronic voting system

Remote polling place

Database of eligible remote voters

Voter identification

Provisional electronic ballots

One-way publishing medium

Electronic voting system, e.g.

VoteBox

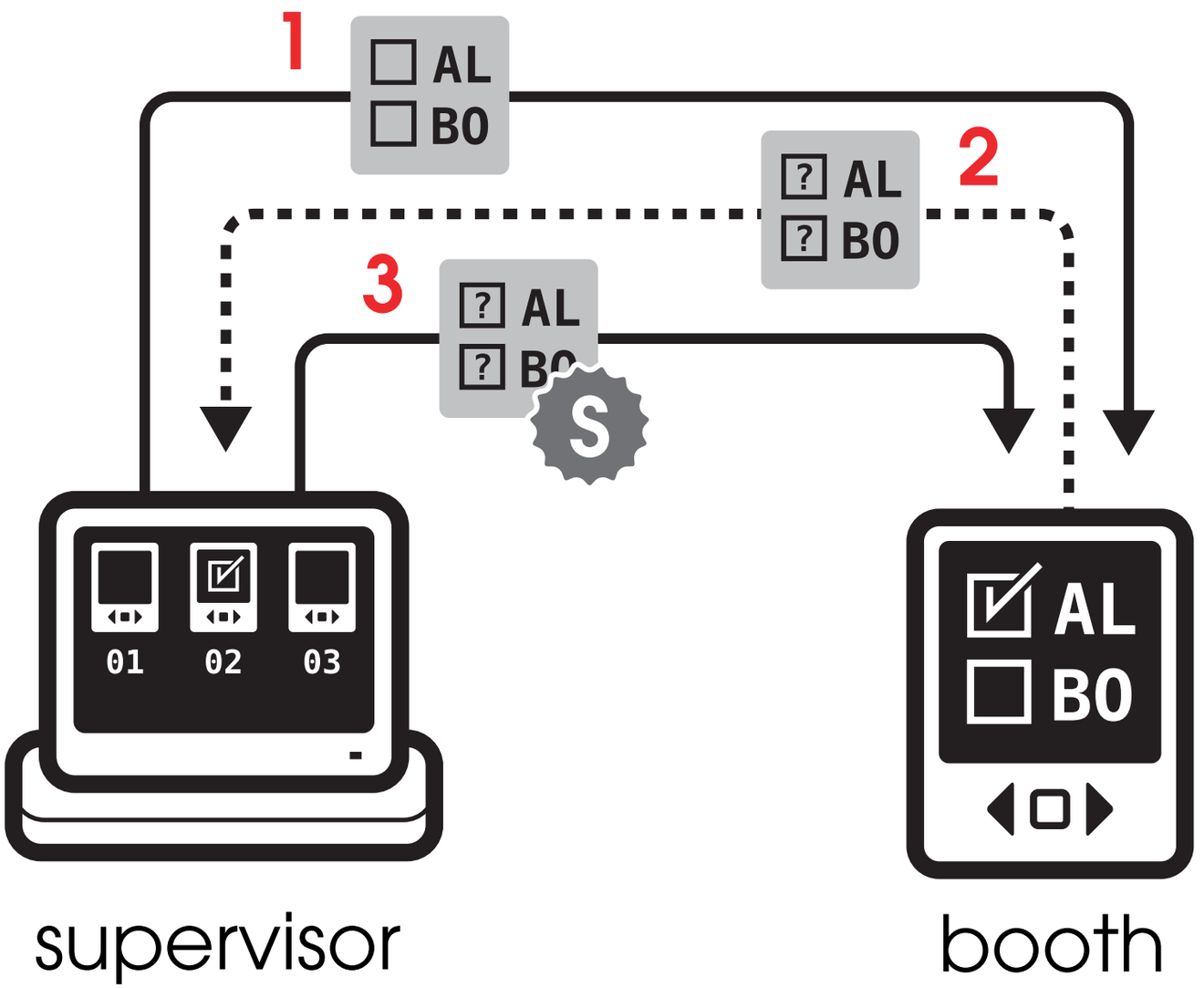
[see Sandler et al, USENIX Security '08]

voting machines are on a private network

all cast ballots are broadcast & logged by each VoteBox "booth" machine

to defend against loss & tampering

a "supervisor" machine manages the polling place



1 vote authorization (blank ballot)
2 cast ballot (encrypted)
3 vote confirmation (signed)

VoteBox tabulation

Encrypted ballots can be posted in public

Even in real time over the Internet.

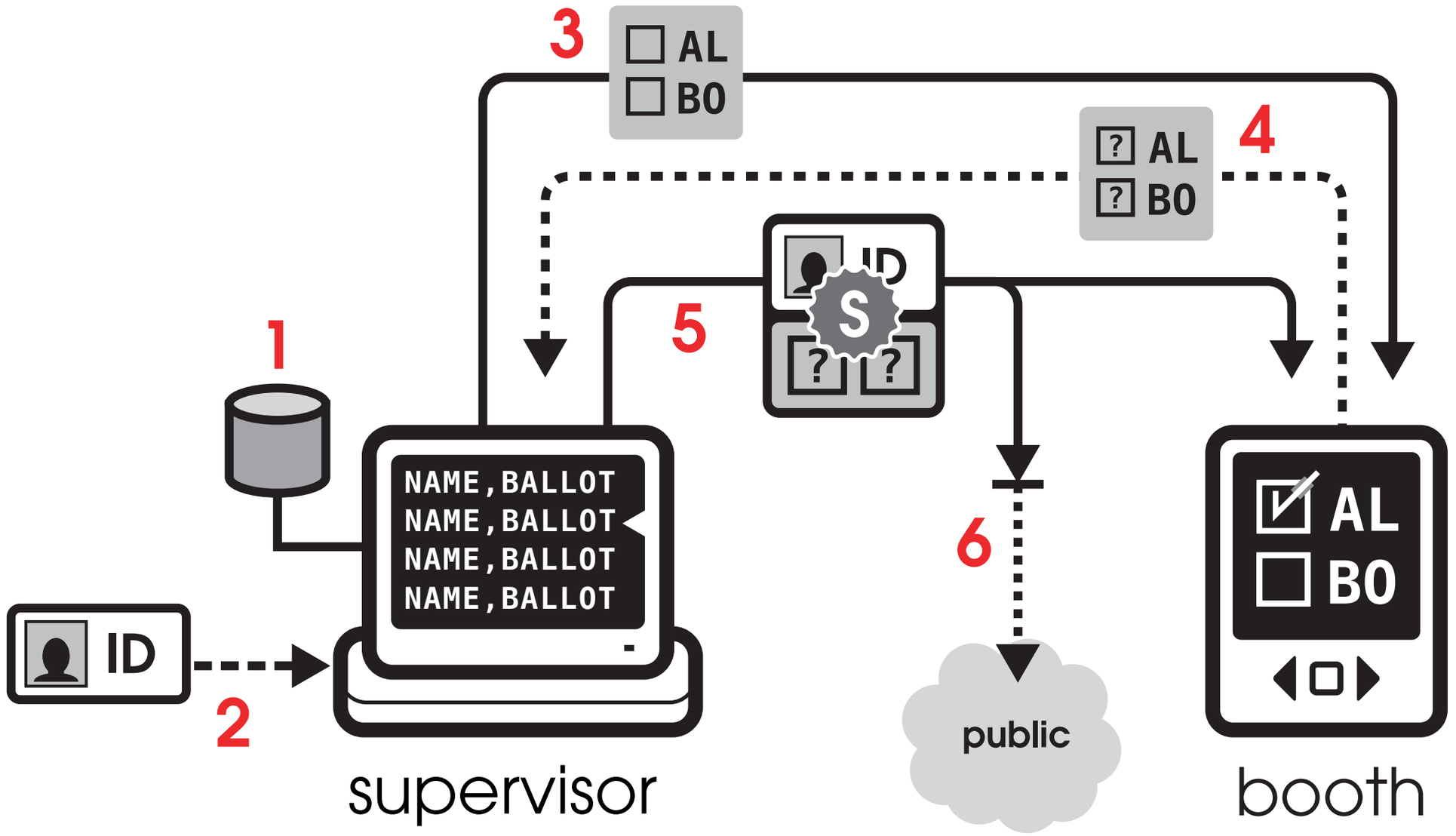
Benaloh challenges (EVT ’07)

Challenge machines to prove accuracy.

Threshold cryptography to decrypt totals

Anyone can verify the decryption.

Applicable to mixnets, homomorphic crypto, etc.



1 database: voter→ballot
2 voter identification
3 authorization (blank ballot)

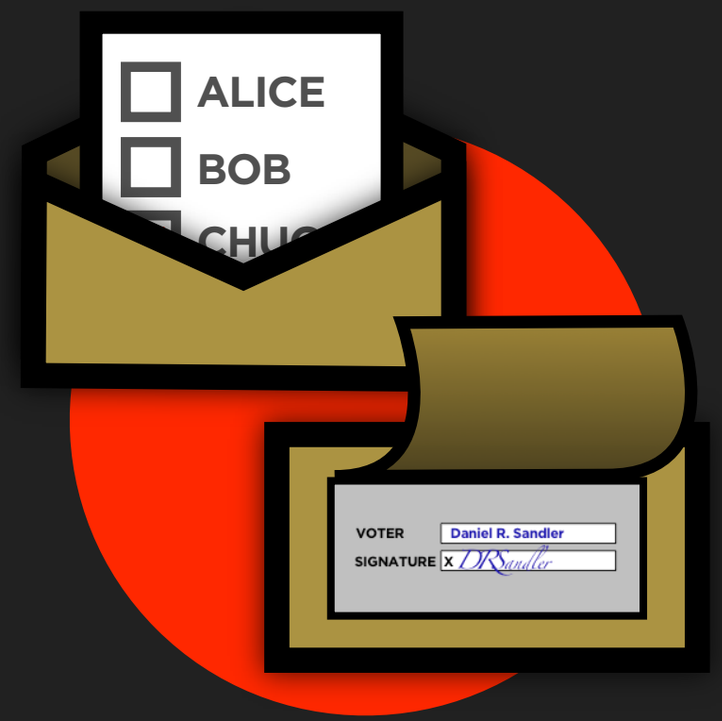
4 cast ballot (encrypted)
5 signed envelope: id + ballot
6 ballot forwarded to precinct


ID
S
?
?


ID
S
?
?

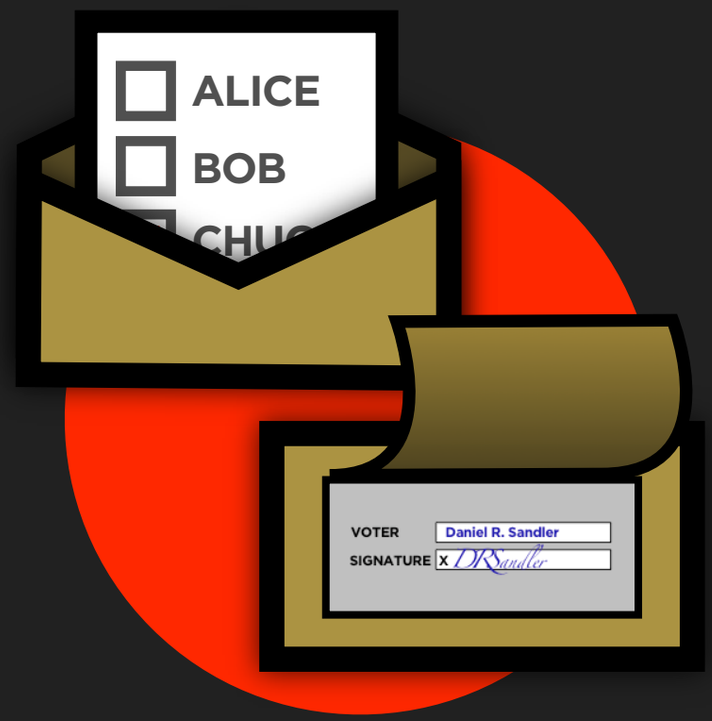

ID
S
?
?

=


ALICE
BOB
VOTER
Daniel R. Sandler
SIGNATURE
X


ID
S
?
?

>


ALICE
BOB
VOTER
Daniel R. Sandler
SIGNATURE
x DRSandler

Benefits of the networked remote polling place

Fast

Ballot types from home precinct

Cast ballots back to home precinct

Robust

Post and networks both lossy

…*but networks can retransmit*

More secure

Choices cannot be observed while in transit

Crypto protects vote secrecy (even from officials)

RELATED WORK

Industrial

US Military: SERVE (2004)

Democrats Abroad

Estonian election (2007)

Commercial systems: “unofficial” results by modem

Research systems

Fujioka, Okamoto, Ohta [FOO 93] blind-signature systems: Sensus [Craner & Cytron 97], EVOX [Herschberg 97], …

Civitas [Clarkson et al 08], Helios [Adida 08]

CONCLUSION

Remote e-voting works

a remote polling place is essential

coercion-resistance; trustworthy equipment

we use the provisional/postal voting model

replace the post with a network

replace opaque envelopes with encryption

replace sealed envelopes with digital sigs

a natural extension to existing research & industrial e-voting approaches

More on VoteBox

Presentation on Friday

www.cs.rice.edu/~dsandler/pub/sandler08votebox.pdf

Summer project: open source release coming soon