April 29, 2005 -- Lecture 39

22C:169 Computer Security

Douglas W. Jones

Department of Computer Science

Chaum's Voting Idea

Visual Cryptography

Idea

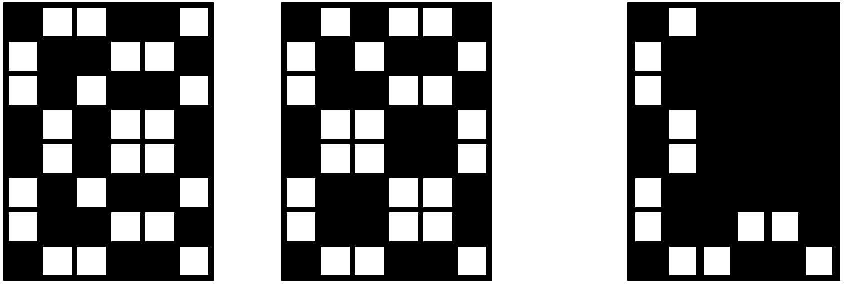
Two pixel values: ▞ and ▚

Use superposition as XOR operation,

So ▚ + ▚ = ▚, while ▚ + ▞ = █

Construct bitmap images:

Key + Cyphertext = Plaintext



Cyphertext + Key = Plaintext

Refinement:

Instead of a pseudorandom key

Use cyphertext!
Well encrypted cyphertext looks random.

Consequence:

Can encrypt the votes cast by a voter,
Use that as a key for visual crypto,
Use that to print two layers of ballot.

Voter's viewpoint:

Vote on electronic voting machine,
Display two-layer human readable ballot,
Separate layers into unreadable layers,
Give one layer to voter,
Drop other layer in ballot box.

Voter verification that ballot was not lost

Voting machine

Posts electronic image of voter's layer.
Voter can check that his layer is posted.
So voter knows his vote is in ballot box.

Brute-force recount is possible

Print electronic images
Superimpose with ballots found in box

But how do we count votes normally?

Mix nets:

Encrypt electronic votes on ballot as:

cyphertext = $E_{K1public}(E_{K2public}(votes))$

To decrypt ballots:

Shuffle ballots in ballot box
Decrypt using K2private
Shuffle ballots in ballot box
Decrypt using K1private

To increase voter privacy

increase number of keys and shuffles.
distribute keys to multiple custodians.
use public keys to encrypt.

To assure that mix-net is honest:

For each shuffle step:

- *Copy random sample of input ballots*
- *Decrypt them externally*
- *Check to see they are in result set*

Important

- *No peeking between shuffle and decrypt*

Advantages

- *Scheme offers end-to-end assurance?*
- *No trusted software?*

Questions about Chaum's Scheme

Who does it require us to trust?

Key custodians!

What if they conspire?

Ballot secrecy can be lost!
But only if voter discloses voted ballot.
Corrupt government could buy votes.

Remedy: Custodians should be diverse

Chairs of opposing parties,
Judge, Mayor, Sheriff

Legal barrier to Chaum's scheme

Typical US state law

- *Requires that it be impossible to attribute ballots to the voters who cast them.*

Chaum's scheme

- *Merely makes it difficult*
- *This would be legal under British law.*