Cryptographic Voting Protocols: Taking Elections out of the Black Box

Phong Le

Department of Mathematics
University of California, Irvine

Mathfest 2009

Problems with the current system

Necessity of vote reform:

- 2000 Bush/Gore Presidential race,
- 2008 Coleman/Franken Minnesota US Senate race,
- 2009 Ahmadinejad/Mousavi Iran Presidential Elections.

In each instance, the controversy erodes voter confidence and ultimately undermines the democratic system.

Public Voting

Public Voting

In public voting each voter announces their vote.

Advantages-

- A voter can easily verify that their vote is recorded correctly.
- The entire voting process is transparent.

Disadvantages-

- Vote selling.
- Voter coercion.

Paper Ballots

Paper Ballots

Each voter fills out a paper ballot which is collected in a central location.

Advantages-

- Voting is anonymous.
- Voting leaves a paper trial for recounting and verification purposes.

Disadvantages-

- Ballots can suffer from mechanical errors such as hanging chads.
- Ballots can be falsified, lost or unreadable.
- A trusted third party is required to count the votes.

Direct Record Electronic System (DRE)

DRE

Voters indicate their choices on a computer screen, which then records and tabulates their votes.

Advantages-

- Fast.
- Leaves a paper trail for recounts.
- No mechanical errors.

Disadvantages-

- Hackable.
- Possible manipulation by the DRE manufacturer or voting officials.

In this case, the trusted third party is the DRE.

Applying Cryptology

- Ideally we would like a voter to verify that the vote is cast appropriately and that the vote is accurately counted.
- In 2004 David Chaum proposed a method to accomplish this using cryptography.
- In his work, and the many protocols that followed, three concepts from cryptology are used:
  - public key cryptology,
  - zero-knowledge protocols,
  - mix nets.

Public Key Cryptology

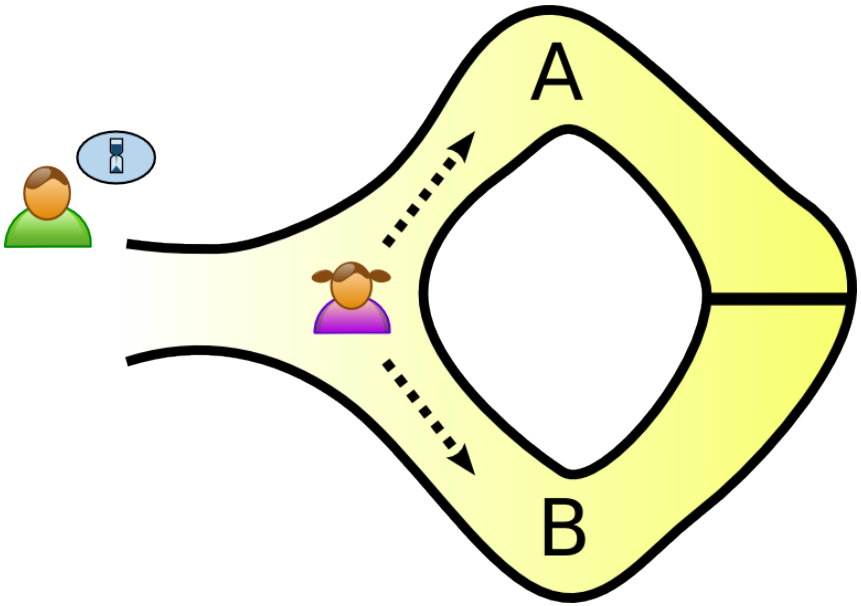
Key features of public key cryptology:

- The encryption algorithm, known as the public key, is publicly available.
- The decryption algorithm, known as the private key, is computationally difficult to determine from the encryption algorithm.
- The private key is held only by the receiver.

Question

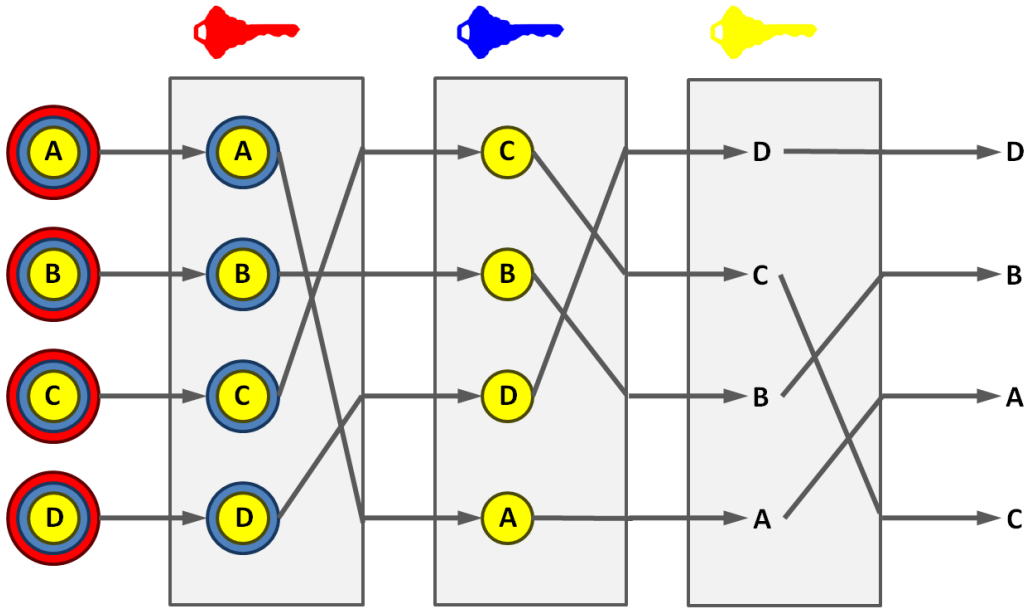
How might one use public key cryptography to make voting more secure?

Zero-Knowledge Protocols



- Peggy (in purple) claims she has uncovered a secret word to open a magic door in a cave.
- Vern (in green) says he will pay for the secret word but not until he's sure that she really knows it.
- Peggy needs to prove to Vern that she knows the secret word, without revealing what that word is.

Mix Nets



A chain of public keys (encryptions) are applied in layers to several messages sent by several different people.

Cryptology in Voting

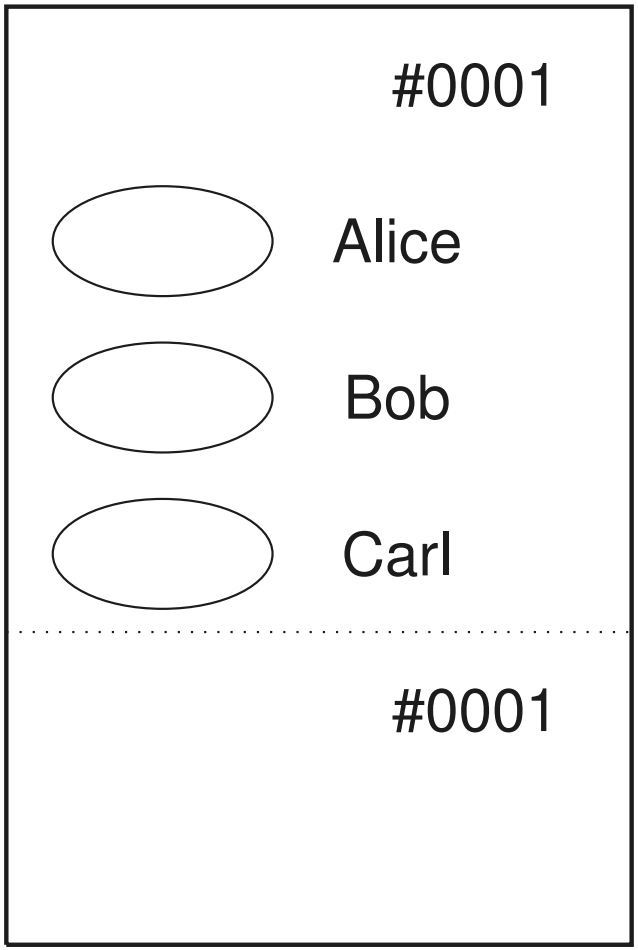
- Public key cryptology may be used to construct mix nets and possibly to encipher the candidate choice.
- Zero-knowledge protocols may be used to provide strong evidence that a tally of votes was made correctly.
- Mix nets may be used to make ballots untraceable.

Question

How can we combine these ideas to create a voting protocol?

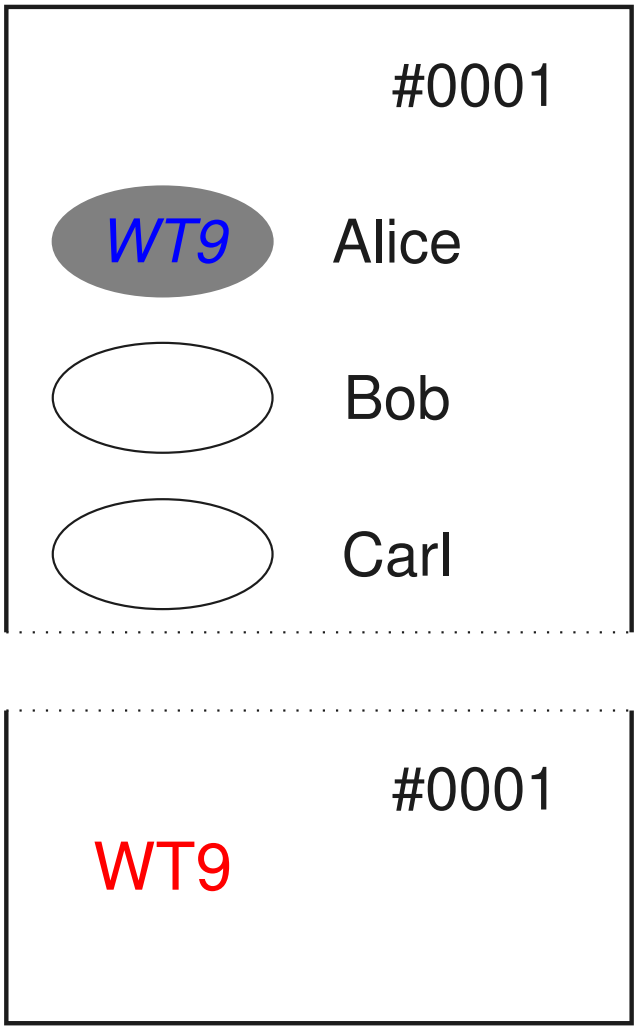
A Sample Protocol: Scantegrity II

First lets examine the voter experience:



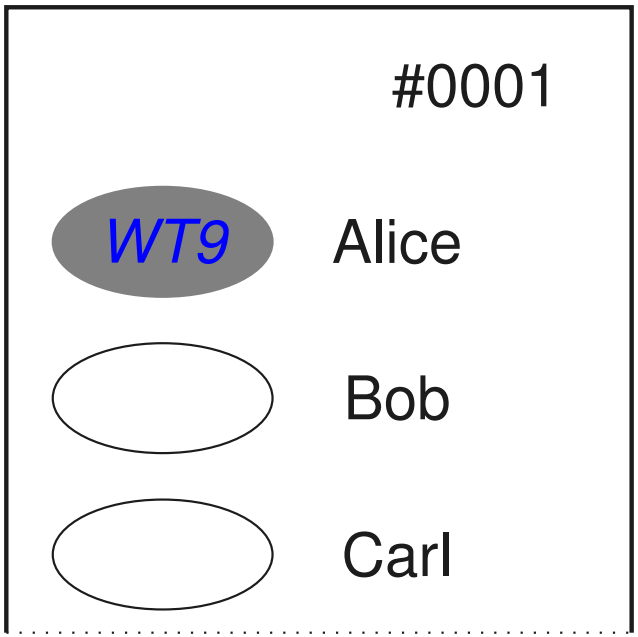
This is a blank ballot. The portion at the bottom is the receipt.

A Completed Ballot



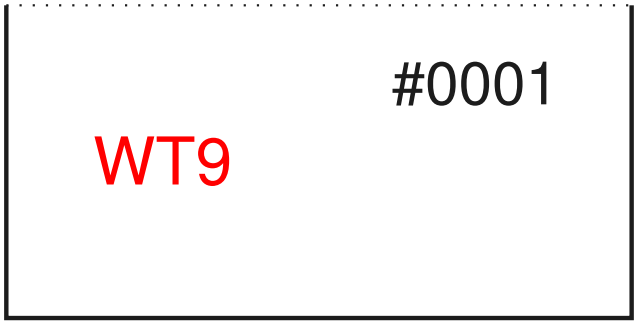
Using a special pen, the voter marks their selection and reveals a unique confirmation code. The voter can then separate the receipt and write down the confirmation code on the receipt.

Top Portion



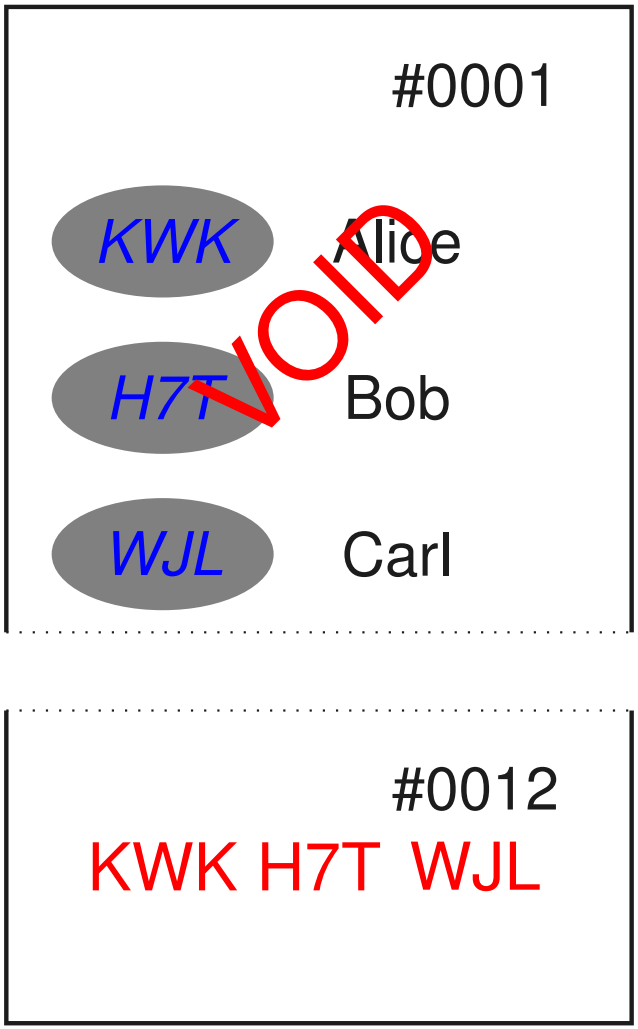
The top of the ballot is run through an optical scanner and a tally is made. The ballot ID and the confirmation code are also recorded.

The Receipt and Verification



The voter can use their receipt to check online whether the confirmation code was recorded correctly. Note that the voter can only verify that the vote was recorded correctly, not reveal what choice was made.

Ballot Audit



A voter may also audit an additional ballot for integrity. The additional ballot is marked void and all the confirmation codes are revealed. This helps ensure that the ballots are created correctly. These ballots are also scanned and can be checked online.

Ballot Creation

Voting officials first generate a ballot table. Randomly generated unique confirmation codes are created and associated to each ballot and candidate.

Ballot Key			
Ballot ID	Alice	Bob	Carl
0001	WT9	7LH	JNC
0002	KMT	TC3	J3K
0003	CH7	3TW	9JH
0004	WJL	KWK	H7T
0005	M39	LTM	HNN

Ballot Shuffling

The confirmation codes of each row are permuted. This is our first mix in our mix net.

Ballot Key			
Ballot ID	Alice	Bob	Carl
0001	WT9	7LH	JNC
0002	KMT	TC3	J3K
0003	CH7	3TW	9JH
0004	WJL	KWK	H7T
0005	M39	LTM	HNN

$\longrightarrow$

Table Q			
Ballot ID			
0001	7LH	WT9	JNC
0002	J3K	TC3	KMT
0003	9JH	CH7	3TW
0004	KWK	H7T	WJL
0005	M39	HNN	LTM

After mixing the columns do not correspond to the different candidates anymore.

The Commitments

Another table is created that permutes the ballot IDs and reveals which confirmation code is assigned to which candidate. This is called the table of commitments. It is our second mix.

Table Q			
Ballot ID			
0001	7LH	WT9	JNC
0002	J3K	TC3	KMT
0003	9JH	CH7	3TW
0004	KWK	H7T	WJL
0005	M39	HNN	LTM

+

Commitment Table		
Flag	Q-Pointer	S-Pointer
	(0005, 1)	(2, 1)
	(0003, 3)	(4, 2)
	(0002, 1)	(4, 3)
	(0001, 3)	(3, 3)
	(0001, 2)	(4, 1)
	(0005, 3)	(3, 2)
	(0004, 2)	(5, 3)
	(0003, 1)	(2, 3)
	(0004, 3)	(3, 1)
	(0002, 3)	(1, 1)
	(0001, 1)	(2, 2)
	(0002, 2)	(5, 2)
	(0004, 1)	(1, 2)
	(0003, 2)	(5, 1)
	(0005, 2)	(1, 3)

=

Table S: Tally		
Alice	Bob	Carl
KMT	KWK	HNN
M39	7LH	9JH
WJL	LTM	JNC
WT9	3TW	J3K
CH7	TC3	H7T

Private Information

Ballot Key			
Ballot ID	Alice	Bob	Carl
0001	WT9	7LH	JNC
0002	KMT	TC3	J3K
0003	CH7	3TW	9JH
0004	WJL	KWK	H7T
0005	M39	LTM	HNN

Table Q			
Ballot ID			
0001	7LH	WT9	JNC
0002	J3K	TC3	KMT
0003	9JH	CH7	3TW
0004	KWK	H7T	WJL
0005	M39	HNN	LTM

Commitments		
Flag	Q-Pointer	S-Pointer
	(0005, 1)	(2, 1)
	(0003, 3)	(4, 2)
	(0002, 1)	(4, 3)
	(0001, 3)	(3, 3)
	(0001, 2)	(4, 1)
	(0005, 3)	(3, 2)
	(0004, 2)	(5, 3)
	(0003, 1)	(2, 3)
	(0004, 3)	(3, 1)
	(0002, 3)	(1, 1)
	(0001, 1)	(2, 2)
	(0002, 2)	(5, 2)
	(0004, 1)	(1, 2)
	(0003, 2)	(5, 1)
	(0005, 2)	(1, 3)

Table S: Tally		
Alice	Bob	Carl
KMT	KWK	HNN
M39	7LH	9JH
WJL	LTM	JNC
WT9	3TW	J3K
CH7	TC3	H7T

Post-election Recount

First the ballot box is opened up and the confirmation codes are filled in. Audited ballots are also entered.

Table Q			
Ballot ID			
0001			
0002			
0003			
0004			
0005			

Commitments		
Flag	Q-Pointer	S-Pointer

Table S: Tally		
Alice	Bob	Carl

Post-election Recount

First the ballot box is opened up and the confirmation codes are filled in. Audited ballots are also entered.

Table Q			
Ballot ID			
0001		WT9	
0002	J3K		
0003		CH7	
0004	KWK	H7T	WJL
0005			LTM

Commitments		
Flag	Q-Pointer	S-Pointer

Table S: Tally		
Alice	Bob	Carl

Post-election Recount

The ballot officials also flag the corresponding entries in the tally table based on the hidden table of commitments.

Table Q			
Ballot ID			
0001		WT9	
0002	J3K		
0003		CH7	
0004	KWK	H7T	WJL
0005			LTM

Commitments		
Flag	Q-Pointer	S-Pointer

Table S: Tally		
Alice	Bob	Carl
	✓	
✓		✓
✓		

Post-election Recount

At this point the hidden table of commitments prevents the public from tallying the votes correctly. It also prevents the public from tracing a ballot.

Table Q			
Ballot ID			
0001		WT9	
0002	J3K		
0003		CH7	
0004	KWK	H7T	WJL
0005			LTM

Commitments		
Flag	Q-Pointer	S-Pointer

Table S: Tally		
Alice	Bob	Carl
	✓	
✓		✓
✓		

Post-election Recount

Next the flags in the table of commitments are raised corresponding to the associated commitments. Also, either the Q-pointer or the S-pointer of each row is randomly chosen to be revealed.

Table Q			
Ballot ID			
0001		WT9	
0002	J3K		
0003		CH7	
0004	KWK	H7T	WJL
0005			LTM

Commitments		
Flag	Q-Pointer	S-Pointer
		(2, 1)
	(0003, 3)	
✓		(4, 3)
		(3, 3)
✓	(0001, 2)	
✓	(0005, 3)	
	(0004, 2)	(5, 3)
		(2, 3)
	(0004, 3)	(3, 1)
	(0002, 3)	
	(0001, 1)	
	(0002, 2)	
	(0004, 1)	(1, 2)
✓		(5, 1)
	(0005, 2)	

Table S: Tally		
Alice	Bob	Carl
	✓	
✓		✓
✓		

Post-election Recount

If one entry in the table of commitments was modified, there would be a 50% that it would be revealed.

Table Q			
Ballot ID			
0001		WT9	
0002	J3K		
0003		CH7	
0004	KWK	H7T	WJL
0005			LTM

Commitments		
Flag	Q-Pointer	S-Pointer
		(2, 1)
	(0003, 3)	
✓		(4, 3)
		(3, 3)
✓	(0001, 2)	
✓	(0005, 3)	
	(0004, 2)	(5, 3)
		(2, 3)
	(0004, 3)	(3, 1)
	(0002, 3)	
	(0001, 1)	
	(0002, 2)	
	(0004, 1)	(1, 2)
✓		(5, 1)
	(0005, 2)	

Table S: Tally		
Alice	Bob	Carl
	✓	
✓		✓
✓		

Commitments

This half-open table of commitments combines part of the mix net and zero-knowledge proof protocols.

Flag	Q-Pointer	S-Pointer
		(2, 1)
	(0003, 3)	
✓		(4, 3)
		(3, 3)
✓	(0001, 2)	
✓	(0005, 3)	
	(0004, 2)	(5, 3)
		(2, 3)
	(0004, 3)	(3, 1)
	(0002, 3)	
	(0001, 1)	
	(0002, 2)	
	(0004, 1)	(1, 2)
✓		(5, 1)
	(0005, 2)	

Go and Vote!