Chaum's Visual Crypto Scheme

Michael Schläpfer

Information Security Group
ETH Zurich

09 June 2010

Outline

1 Introduction

2 Protocol functioning

3 Security properties

4 Conclusions

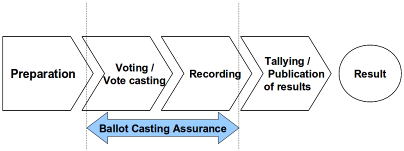
Goals

What do we want to achieve primarily:

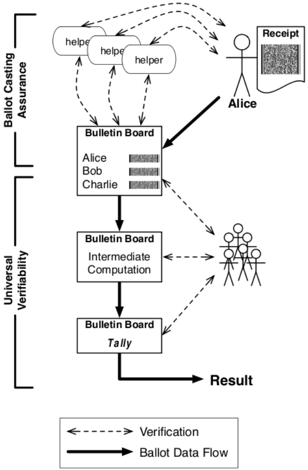
- Integrity
- Secrecy
- Receipt-freeness

Integrity

E2E verifiability



- Individually verifiable:
  - Cast as intended
  - Recorded as cast
- Universally verifiable: All other phases



Outline

1 Introduction

2 Protocol functioning

3 Security properties

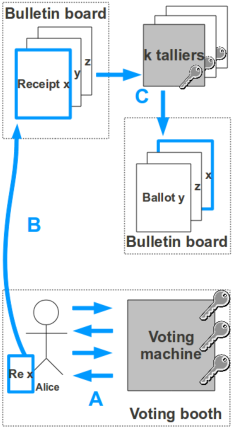
4 Conclusions

Overview

A Voter enters choice and gets two receipts for which she is able to verify the correctness of the encryption visually

B Voter chooses one receipt randomly. This receipt is published on a bulletin board

C Talliers decrypt and mix the encrypted receipts

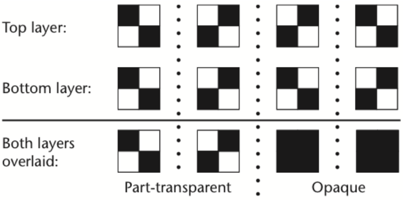


Key idea

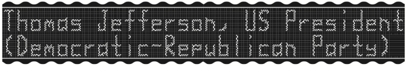
- Let  = 1 and  = 0
- Then we define a visual xor operation $\oplus_v$ such that:

$$
\begin{aligned}
1 \oplus_v 1 &= 0 \\
0 \oplus_v 0 &= 0 \\
1 \oplus_v 0 &= 1 \\
0 \oplus_v 1 &= 1
\end{aligned}
$$

- Represent voter's choice as matrix of parity cells (visual representation of a bit string)



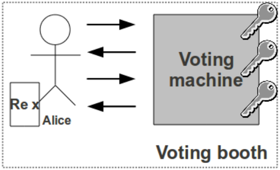
Parity cells. (Source: David Chaum)

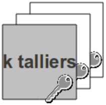


An example. (Source: David Chaum)

Protocol functioning

Preliminaries





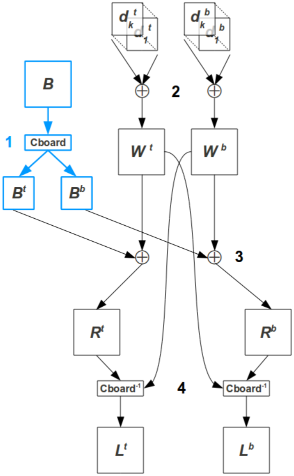
- Controlled voting booth used
- Voting machine holds three keys for:
  - Signing BSN (bottom)
  - Signing BSN (top)
  - Overall signing the entire receipt
- There exist two hash functions h and h', where h is public and h' (keyed) is only known to authority and official auditors (e.g. political parties)
- Every tallier holds a private key and the corresponding public key is public

Protocol functioning

Encryption

1 Voter's choice represented as $m \times n$-matrix B

B is "checkerboarded" to bitstrings B^t and B^b of length $\frac{mn}{2}$

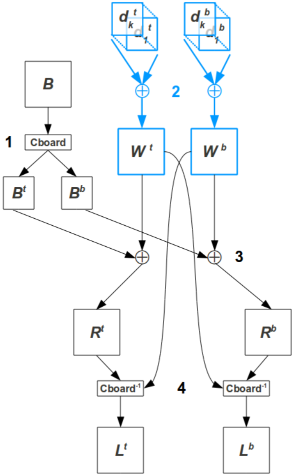


Protocol functioning

Encryption

2 $2k$ pseudo random hash values v_i^t and v_i^b of length $\frac{mn}{2}$ are generated from the signed *BSN (Ballot Sequence Number)* using h

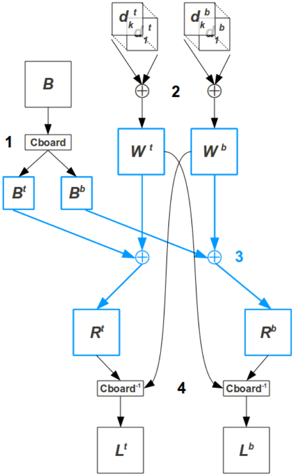
- $d_i^t = h'(v_i^t)$ and $d_i^b = h'(v_i^b)$
- $W^t := \bigoplus_{1 \leqslant i \leqslant k} d_i^t$ and
  $W^b := \bigoplus_{1 \leqslant i \leqslant k} d_i^b$
- In parallel, the *top doll* D^t and the *bottom doll* D^b are created for later decryption.
  $D^t := \{v_k^t, \{\cdots\{v_2^t, \{v_1^t\}_{pk_1}\}_{pk_2}\cdots\}_{pk_{k-1}}\}_{pk_k}$



Protocol functioning

Encryption

3. B^t and B^b are encrypted by bitwise xor-ing with the corresponding W:
   - $R^t := B^t \oplus W^t$
   - $R^b := B^b \oplus W^b$

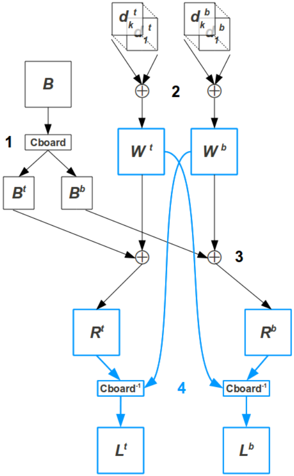


Protocol functioning

Encryption

4 Reverse "checkerboard" B^t with W^b and B^b with W^t to the *top layer* L^t and the *bottom layer* L^b

Represent the layers with visual parity cells

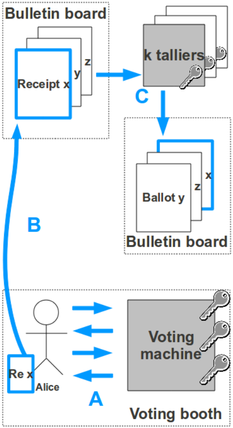


Overview

A Voter enters choice and gets two receipts for which she is able to verify the correctness of the encryption visually

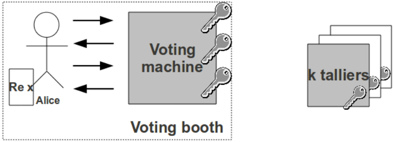
B Voter chooses one receipt randomly. This receipt is published on a bulletin board

C Talliers decrypt and mix the encrypted receipts



Protocol functioning

Vote casting



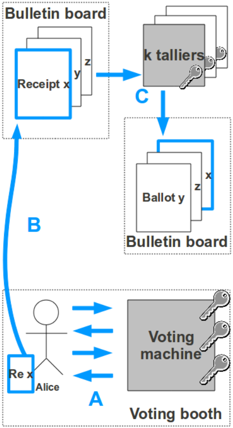
- Voter chooses layer randomly
- Voting machine signs BSN with the corresponding signing key
- Voting machine prints all this information on the chosen layer's receipt
- Voting machine signs with overall signing key:
  - Chosen layer L^x
  - BSN
  - Signed BSN
  - Dolls D^t and D^b
- Chosen receipt is scanned and published

Overview

A Voter enters choice and gets two receipts for which she is able to verify the correctness of the encryption visually

B Voter chooses one receipt randomly. This receipt is published on a bulletin board

C Talliers decrypt and mix the encrypted receipts

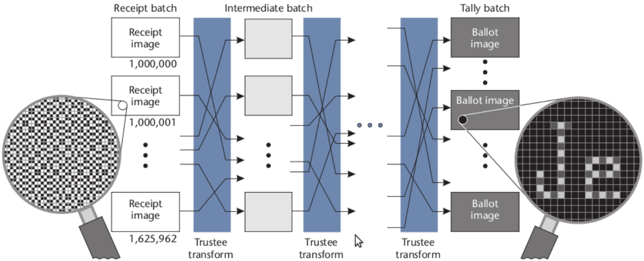


Protocol functioning

Tallying

Remember:

- $D := \{v_k, \{\cdots\{v_2, \{v_1\}_{pk_1}\}_{pk_2}\cdots\}_{pk_{k-1}}\}_{pk_k}$
- h' known to authority (talliers) and $W := \bigoplus_{1 \leqslant i \leqslant k} h'(v_i)$



Outline

1 Introduction

2 Protocol functioning

3 Security properties

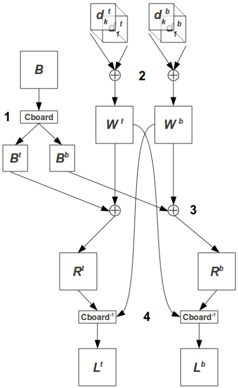
4 Conclusions

Security properties

Integrity

Voter is able to:

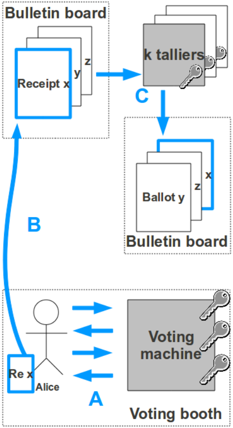
- Check the correctness of all the signatures printed on receipt
- Generate the k hash values v_i^x from the signed BSN
- Check the correctness of the doll D^x printed on his layer by sequentially encrypting hash values v_i^x with the public keys of the respective tallier i
- Check that the published receipt indeed corresponds to his receipt
- The tallying phase can be made universally verifiable



Security properties

Secrecy

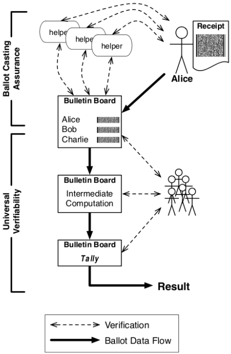
- Chaum claims “secure even if all used voting machines are corrupt”
- Agree on integrity
- Don’t agree on secrecy!
- Possible solution is to “pre-encrypt” voters choice



Security properties

Receipt-freeness

- Voter gets receipt for individual verification
- Receipt cannot be used to prove choice against third parties
- Receipt can be used to complain in case of failure (This property is often left out in considerations!)



Outline

1 Introduction

2 Protocol functioning

3 Security properties

4 Conclusions

Adaption to Internet voting

- Voter needs an accurate printer that can print on transparent foils
- Voter needs a scanner
- Complicated procedure for home use
- User is in possession of the entire receipt (both layers!)

Conclusion:

Not applicable for Internet voting!

Further readings

- D. Chaum. Secret-ballot receipts: True voter-verifiable elections. IEEE Security & Privacy Magazine, Citeseer, 2004.http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.123.7870&rep=rep1&type=pdf
- J. Bryans and P. Ryan. A dependability analysis of the Chaum digital voting scheme. University of Newcastle upon Tyne Technical Report Series CS-TR-809, 2003.http://www.cs.ncl.ac.uk/research/pubs/trs/papers/809.pdf