Cast as intended in Norway

EVOTE 2012

July 2012

Jordi Puiggali
VP R&D
Jordi.puiggali@scytl.com
- Introduction
- Proposal
- Remarks
Introduction
Norwegian Ministry started eValg2011 project in August 2008: remote electronic voting at municipal elections in 2011

One of the main security requirements: zero trust on voting client

Scytl proposed a cast-as-intended verifiable solution based on using return codes generated by making operations over the encrypted vote

Norwegian implemented solution is a variation of the Scytl’s proposal focused on making the solution more usable.

This proposal was modified to meet specific usability and performance requirements proposed during the eValg 2011 project [1]

<table>
<thead>
<tr>
<th>Parti</th>
<th>Returkode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disney Party</td>
<td>186479</td>
</tr>
<tr>
<td>Marvel Party</td>
<td>657294</td>
</tr>
<tr>
<td>Kandidat</td>
<td></td>
</tr>
<tr>
<td>Donald Duck, f. 1934, Disneyland</td>
<td>453782</td>
</tr>
<tr>
<td>Peter Pan, f. 1904, Disneyland</td>
<td>083128</td>
</tr>
<tr>
<td>Mickey Mouse, f. 1928, Disneyland</td>
<td>537287</td>
</tr>
<tr>
<td>Minnie Mouse, f. 1928, Disneyland</td>
<td>975659</td>
</tr>
<tr>
<td>Aurora Princess, f. 1959, Disneyland</td>
<td>736181</td>
</tr>
</tbody>
</table>
Proposal
Voting Process

1. Voter casts encrypted vote via Voting Card.
2. Encrypted vote transmitted through Internet to Vote Collector Server (VCS).
3. VCS processes vote and generates operated encrypted vote.
4. VCS sends receipt to Voter.
5. Voter receives receipt and confirms vote.

CardID: 4545 2321 6742
Candidates
Candidate 1 1092
Candidate 2 3417
Candidate 3 8417

You selected: 3417

3417 is sent to SMS gateway.
3. Return Code Generator (RCG) receives return code.
4. VCS sends operated encrypted vote receipt to Voter.
5. Voter receives receipt and confirms vote.

Scytl
Innovating Democracy
Proposal

Original Protocol

Step 1
Two vote encryptions + ZKP plaintext equivalence

Step 2
Return Code vote operation + ZKP plaintext equivalence

Step 3
Return Code vote operation + formatting

Step 4
Counting

Vote Encryption

VCS

RCG

BB

ZKP

Vote Encryption

Return Code

Voter
Proposal

Norwegian Protocol

Single vote encryption

Step 1

Pre-calculations over encrypted vote + ZKP

Step 2

Second pre-calculations over VCS ones + formatting

Step 3

Vote Encryption

VC

VCS

BB

RCG

RC

Voter

Step 4

Counting

Single vote encryption

Pre-calculations over encrypted vote + ZKP

Second pre-calculations over VCS ones + formatting

Vote Encryption

VC

VCS

BB

RCG

RC

Voter

Step 4

Counting
- **Norwegian**
  - Reduction of the cryptographic operations, since only requires a single encryption in the voter terminal
  - More usable for voters, since does not require to introduce any special code for generating a second encryption of the vote

- **Original**
  - It is more robust against collusion of actors, since VCS and RCG keys do not rely on the Election key used for decrypting the votes
  - Requires less resources in the server side, since some parts of the cryptographic operations done to obtain the return codes are implemented in the voting terminal
Participants of the voting process: voter V, voting client VC, voting server VCS, validation server RCG.

Asymmetric encryption: ElGamal.

- Election parameters:
  - \( p \) is a safe prime (\( p=2q+1 \) where \( q \) is also prime).
  - \( g \) is a generator of \( G_q \), a \( q \)-order subgroup of \( Z_p^* \).

- Key pairs:
  - Election: private key \( x_e \), public key \( h_e \).
  - VCS: private key \( x_{vcs} \), public key \( h_{vcs} \).
  - RCG: private key \( x_{rcg} \), public key \( h_{rcg} \).

Symmetric keys

- VCS: AES secret key \( K_{vcs} \).
- VCS: voter secret parameter \( s = AES_{K_{vcs}} (voterID') \).
- RCG: SHA2-HMAC secret key \( K_{rcg} \).

Relationship

\[
x_{rcg} - x_{vcs} \equiv x_e \pmod{p}.
\]
Proposal

Vote Casting details

**Step 1**

VC

Vote Encryption

**Step 2**

VCS

Vote Re-encryption

**Step 3**

RCG

Vote Decryption

\[ v_{opt_i} = (a_i, b_i) = (g^{r_i}, v_i \cdot h_e^{r_i}) \]

\[ ZKP(a_i, b_i) \]

\[ s = AES_{K_{vcs}}(\text{voterID}') \]

\[ v_{opt_i}' = (a_i', b_i') = (a_i^s, b_i^s) \]

\[ b_i'' = b_i' \cdot a_i^{x_{vcs}} \]

\[ v_{opt_i}'' = (a_i', b_i', b_i'') \]

\[ ZKP(a_i, b_i, a_i', b_i', b_i'') \]

\[ b_i'' \cdot a_i^{v_i^{x_{rcg}}} = \]

\[ b_i^s \cdot a_i^{s \cdot x_{vcs}} \cdot a_i^{s \cdot (-x_{rcg})} = \]

\[ (b_i \cdot a_i^{x_e})^s = v_i^s \]

\{Party/Cand\}Code_i = \]

\[ \text{HMAC}( v_i^s \| \text{voterID}, K_{rcg} ) \]
Proposal

Voting Card generation

Step 1

VCS’

Candidate re-encryption

\( v_i' = v_i^s \mod p \)

\( \text{rand}_i = \text{rand}() \)

\( (v_i, \text{rand}_i) \)

\( (v_i', \text{rand}_i) \)

Step 2

RCG’

Return code

\( (v_i', \text{rand}_i) \)

\( (\text{Code}_i, \text{voterID}_j) \)

\( (v_i', \text{Code}_i) \)

Step 3

Printing

\( \text{voterID}_i = \text{rand}() \)

\( \text{Code}_i = \text{HMAC}(v_i' \| \text{voterID}_i, K_{rcg}) \)

\( (\text{Code}_i, \text{voterID}_j) \)

\( (v_i', \text{Code}_i) \)

\( (v_i, \text{rand}_i) \)

\( (\text{Code}_i, \text{voterID}_j) \)

\( (v_i', \text{Code}_i) \)

\( (\text{voterID}_j, v_i', \text{Code}_i) \)
Assigning individual codes to parties and candidates generates a large voting card (e.g., 25 parties with 10 candidates generate 250 Return Codes)

- Implemented solution: position codes (reduction to 35 Return Codes)

- Side effects
  - Requires a database that translates the codes obtained RCG to candidate to position codes:
    \[(\text{Code}_i, \text{PositionCode}_j)\]
  - Database registers must be encrypted to preserve Return Codes privacy
    \[(H(\text{Code}_i), AES(\text{PositionCode}_j, \text{Code}_i))\]
  - Allows verification of correct vote contents preserving vote secrecy
  - Vulnerable to candidate shifting attacks but only in the same party
    - The majority of the voters (about 98%) not affected since they only select parties
Proposal

SMS message constraints

- Limited message size (160 chars)
  - Return codes limited to 4 digits
  - Position codes discarded and substituted by the number of selections made in the party

- Side effects
  - Requires a database that translates the 4 digit codes to codes obtained by RCG. This is not an issue since this was already required
  - Vulnerable to candidate shifting attacks (same arguments as before)
Final remarks

- Usability influenced several aspects of the Norwegian schema
  - Original protocol modified to reduce the number of operations in the voting terminals
  - Voting cards are linked to voters to prevent the introduction of any VoterID
  - Return codes use limited to parties to make voting cards smaller as well as SMS messages

- Decisions were evaluated considering the security risks
  - Risks were accepted considering the probability and therefore impact