Selene e-voting protocol: in your hand and in the booth
(E-Vote-ID 2017 - PhD Colloquium)

Marie-Laure Zollinger

Université du Luxembourg

October 24, 2017
Table of contents

1 Selene
   • Set-up phase
   • Voting protocol

2 A mobile application
   • Introduction
   • Development
   • Future research

3 In the booth
   • Goal
   • Adaptation
   • Next step
Election set-up

Selene is an e-voting protocol that notifies voters with a tracking number after the tally has been published.

Participants:

- Voters: public and secret keys,
- Election Authority: election public key,
- Bulletin Board: encrypted tracking numbers, voters public keys, commitments,
- Tellers: election secret keys, transcription of tracking numbers with voters keys
Trackers transcription

- Election authority key $PK$
- Voters key $PK_i$
- El-Gamal Encryption: $\{t_{\pi(i)}\}_{PK_i} = (\alpha, \beta)$ where $\beta$ is the commitment
Protocol

1. A voter casts an encrypted vote.
Protocol

1. A voter **casts an encrypted vote.**

2. The Tellers perform parallel mix and decryption of trackers and votes to **extract the pairs (tracker, vote).**
Protocol

1. A voter casts an encrypted vote.
2. The Tellers perform parallel mix and decryption of trackers and votes to extract the pairs (tracker, vote).
3. The Tellers notify the voters with the term $\alpha$. The voter can calculate the decryption of their tracking number and verify her vote.
Goals

- Provide an adaptable mockup for Selene to test user experience
- Improve trust and confidence, by showing a good level of security
- Test usability of the app
- Work on the acceptance of the scheme

This project focuses on the verifiability aspect of Selene.
⇒ Cryptography aspects kept hidden

An implementation of Selene’s security mechanisms has been done by Vincenzo Iovino in C language, and can be used as a library.
Design - Sequence diagram

- Selene e-voting protocol: in your hand and in the booth

Marie-Laure Zollinger
Administration

Administration page

Notify
To disable the checking function, click on the button below.

Disable

Candidates
- Stark
- Targaryen

Fill the form to set 2 new candidates. By setting two new candidates, you will erase the bulletin board.

C
R

Tally
A tally has already been generated. Check the bulletin board.
To define a new random bulletin board, click on "Generate". You can define a number of votes (default 100).

Generate

App Content
Here you can change the content of the application.

Welcome message: Welcome to Selene. From this app, you can cast a vote and check

Vote validation message: Your vote has been recorded. Find it on the bulletin board.

Voters
Fill the form to add a new eligible voter.

Add
Application
Application

Selene e-voting protocol: in your hand and in the booth

Selene
A mobile application
In the booth

Introduction
Development
Future research

Application
Application

Selene

A mobile application
In the booth

Introduction
Development
Future research

Application

Selene Demo

Welcome to Selene. From this app, you can cast a vote and check that it has been correctly recorded.

VOTE

CHECK BULLETIN BOARD
Application

Selene Demo

Welcome to Selene. From this app, you can cast a vote and check that it has been correctly recorded.

- VOTE
- CHECK BULLETIN BOARD

Please choose your candidate.

- Stark
- Targaryen

AUTHENTICATE
Web bulletin board

We display here a set of votes. From your Selene app, you can know which one is yours.
The election result is: Targaryen with 2 votes, Stark with 7 votes.
The winner is: Stark

<table>
<thead>
<tr>
<th>Tracking number</th>
<th>Vote</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Stark</td>
</tr>
<tr>
<td>2</td>
<td>Stark</td>
</tr>
<tr>
<td>3</td>
<td>Stark</td>
</tr>
<tr>
<td>4</td>
<td>Stark</td>
</tr>
<tr>
<td>5</td>
<td>Targaryen</td>
</tr>
<tr>
<td>6</td>
<td>Stark</td>
</tr>
<tr>
<td>7</td>
<td>Stark</td>
</tr>
<tr>
<td>8</td>
<td>Stark</td>
</tr>
<tr>
<td>9</td>
<td>Targaryen</td>
</tr>
</tbody>
</table>
Ideas

**Short term**
- Preparation phase: **focus groups**
- Improve the administration part
  - → **store data** for a better data analysis
  - → Bring more **adaptable elements** to configure the app

**Long term**
- Use **Vincenzo’s library** that implements Selene’s mechanisms
  - → keys distribution, encryptions, decryptions, commitments
- Design a secure architecture for the bulletin board
  - → accessibility
  - → data storage
  - → communication protocol
Selene in the booth

Goal

- Adapt Selene to in-booth voting scheme: from an individual voting process to a shared and public site

- Advantage: better coercion resistance

- Inconvenient: introduction of new issues
  - How do we authenticate a voter to use her keys?
  - How to notify the tracking number?
  - How do we design the ballot?
Workflow

1. **ID card** → **VSD** → **Scanner** → **Ballot box**
2. **ID** → **Vote** → **WBB**
3. **Commitment** → **Teller 1 → Teller t**
4. **(α, β) → TN**
Workflow

1. **ID card**

2. **VSD**

3. **Ballot box**

   - **Paper ballot**
     - Candidate A
     - Candidate B
     - Candidate C

4. **Scanner**

5. **WBB**

   - TN
   - Commitment
   - Vote
Workflow

1. User presents ID card to a VSD device.
2. VSD prints a paper ballot.
3. User puts the paper ballot into the ballot box.
4. Teller 1 verifies the ID of the user.
5. Teller 1 digitally signs the ballot.
6. Teller 1 returns the signed ballot to the user.
7. User seals the ballot and presents it to the WBB.
8. WBB verifies the user's ID and the ballot's signature.
9. WBB counts the votes and sends the result to the TN.
10. TN collects the results and updates the official record.
Work in progress...

- ID card
  ⇒ Content definition: certificates, PIN codes, etc.

- Notification of the tracking number
  ⇒ Verification application for mobile?
  ⇒ Email/text message with tracker?

- Dispute resolution
  ⇒ **Ballot proof**: receipt to prove that a voter cast a ballot but cannot be used for verifiability purpose
  ⇒ Paper audit trail: RLA with comparison algorithm