E-Voting EPFL:
Authentication and Frontend

Etienne Bonvin

School of Computer and Communication Sciences
Decentralized and Distributed Systems lab

Semester project
Autumn 2017

Responsible
Prof. Bryan Ford
EPFL / DEDIS

Supervisor
Linus Gasser
EPFL / DEDIS
1 Introduction

2 Background

3 Implementation
   - Authentication server
   - Communication
   - Frontend

4 Limitations

5 Results

6 Conclusion
Introduction and challenges

Privacy
Authenticity
Reliability
Schnorr Signature
an efficient identification scheme
ElGamal Encryption System

asymmetric key encryption
Neff Shuffle
an insurance of privacy
Skipchains and Cothority

bringing reliability to the system
Authentication server
identify EPFL people
Authentication server
identify EPFL people
Communication

Frontend / Cothority

![Diagram showing communication flow with nodes labeled as voting.epfl.ch, Authentication server, and Conodes.](image)
socket.send('Login', 'LoginReply', loginRequest).then((data) => {
  if(data.admin){ // The user is a confirmed admin.
    showConnectedScreen();
    sessionToken = data.token;
    displayElections(data.elections);
  }else{ // The user is not an admin.
    $("#errDiv").append(
      paragraph("An admin account is required " +
        "to access this site.");
  }
}).catch((err) => {
  displayError('An error occurred during the login, "+|
    "please try again later.");
  console.log(err);
});
Communication

Frontend / Cothority

User

Login
LoginReply
Cast
CastReply
Aggregate
AggregateReply

Conodes

Master skipchain
Genesis
Election #1
Election #2

Skipchain #1
Genesis
Ballot #1

Skipchain #2
Genesis
Ballot #1
Ballot #2
Shuffled
Decrypted
Communication

Frontend / Cothority

Diagram showing communication flow between Admin and Conodes, including messages like Login, LoginReply, Open, OpenReply, Shuffle, ShuffleReply, Decrypt, DecryptReply, and various skipchain and election structures.
**Frontend**

communicate with the user

<table>
<thead>
<tr>
<th></th>
<th>User</th>
<th>Admin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vote in election</td>
<td>✔</td>
<td>✗</td>
</tr>
<tr>
<td>Create election</td>
<td>✗</td>
<td>✔ ✔</td>
</tr>
<tr>
<td>Manage election</td>
<td>✗</td>
<td>✔ ✔</td>
</tr>
<tr>
<td>See results</td>
<td>✔ ✔</td>
<td>✔ ✔</td>
</tr>
</tbody>
</table>
Limitations
weak links and future enhancements

- **Nodejs server**: lose the no trusted server idea.
- **Authentication server message**: vulnerability to repetition attacks.
- **Elections limited to scipers**
Results
what has been achieved

Your ballot's encryption pair:

b29c9c202d905c37c35cdc1ad6336d2e34a9778e388044c555cb5517eb1fff01
125cc07ab786b1f841651c541fbb53528241e11e8fa377dba78a1b79b4a05d0e
Results
what has been achieved

Your shuffled ballot’s encryption pair:
5954de2be853df67320621236b581bc3b4e2ade229976cc4c4f33927bf742989
97347646f61ee39315762b65a44b8a72ec23a8b6882cc9ca788188c7acbd1a86

<table>
<thead>
<tr>
<th>Alpha</th>
<th>Beta</th>
</tr>
</thead>
<tbody>
<tr>
<td>101d3e8b5b5a7eaf53f1136663357b07dc0be68b6b5fa4b28bf35905c048</td>
<td>346e12f5373e07fe125302589100bbd94ec9baa0219f14e913ee365049134117d79</td>
</tr>
<tr>
<td>e360c23972191t326386bce714e9cd1e020b32c7342c0ef05543d5025f06</td>
<td>cc626745223504d05aef0b57b7e79e3b9cd3d791431de9d714e75764032731</td>
</tr>
<tr>
<td>db03c1d238af7b7a146e38ab4d46ce5e90e89238356281040a2a309333665ee9</td>
<td>38a0197a934d1b9410fd0b66a4f869eeaa2b9e683077feaf2db1c4b2b2bf76</td>
</tr>
<tr>
<td>6b3b206946b55b1a8482c447d997e73680ef01fa78666e7b94bca9e12391e</td>
<td>6142ce539c62756049eb9180dc37e8c86b4cd005b9a61b0b0f0e3fae4a8d</td>
</tr>
<tr>
<td>5954de2be853df67320621236b581bce3b4e2ade229976cc4c4f339270f742989</td>
<td>97347646f61ee39315762b65a44b8a72ec23a8b6882cc9ca788188c7acbd1a86</td>
</tr>
</tbody>
</table>

Record ID: 19
Results
what has been achieved

<table>
<thead>
<tr>
<th>Place</th>
<th>Sciper</th>
<th>Votes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>456789</td>
<td>10</td>
</tr>
<tr>
<td>2</td>
<td>123789</td>
<td>7</td>
</tr>
<tr>
<td>3</td>
<td>123456</td>
<td>6</td>
</tr>
<tr>
<td>4</td>
<td>248635</td>
<td>5</td>
</tr>
</tbody>
</table>
Conclusion
and future work

- Acknowledgments
- Future work