A Modular, Dual and Voter-Verifiable Electronic Voting System

Camilo Gómez N.
cjgomez@dcc.uchile.cl

Motivation

End-to-End (E2E) Verification:

- Cast as intended.
- Recorded as cast.
- Tallied as recorded.

Usability problems on electronic voting.

The system must give trust to the voter.

General Properties

Simplicity:

- Configuration.
- Implementation.

Use of cryptography.

VVPAT included

Description of the System

Modular, Dual and Voter-Verifiable.

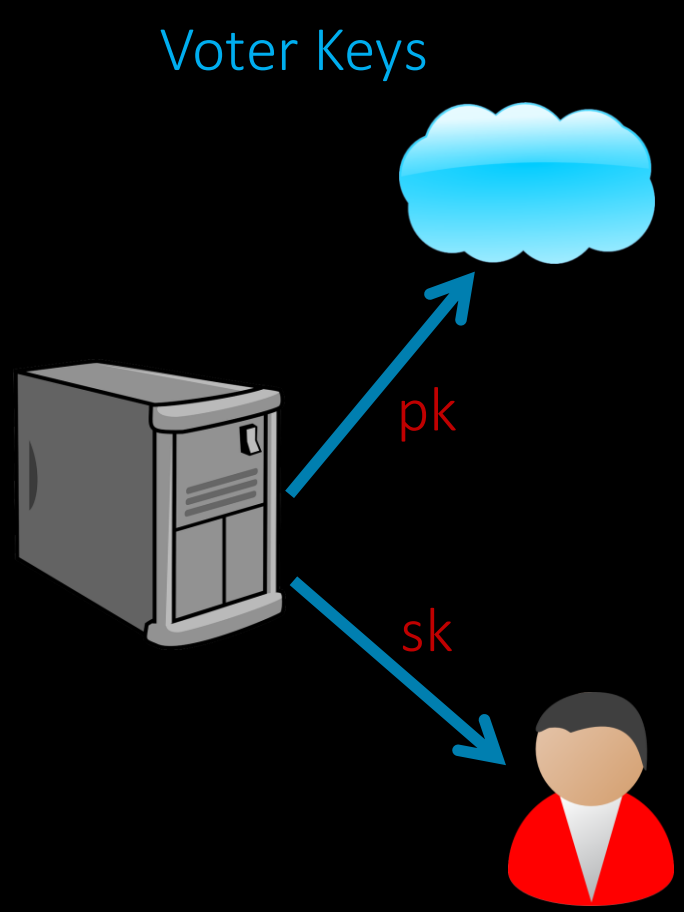
Parts of the System:

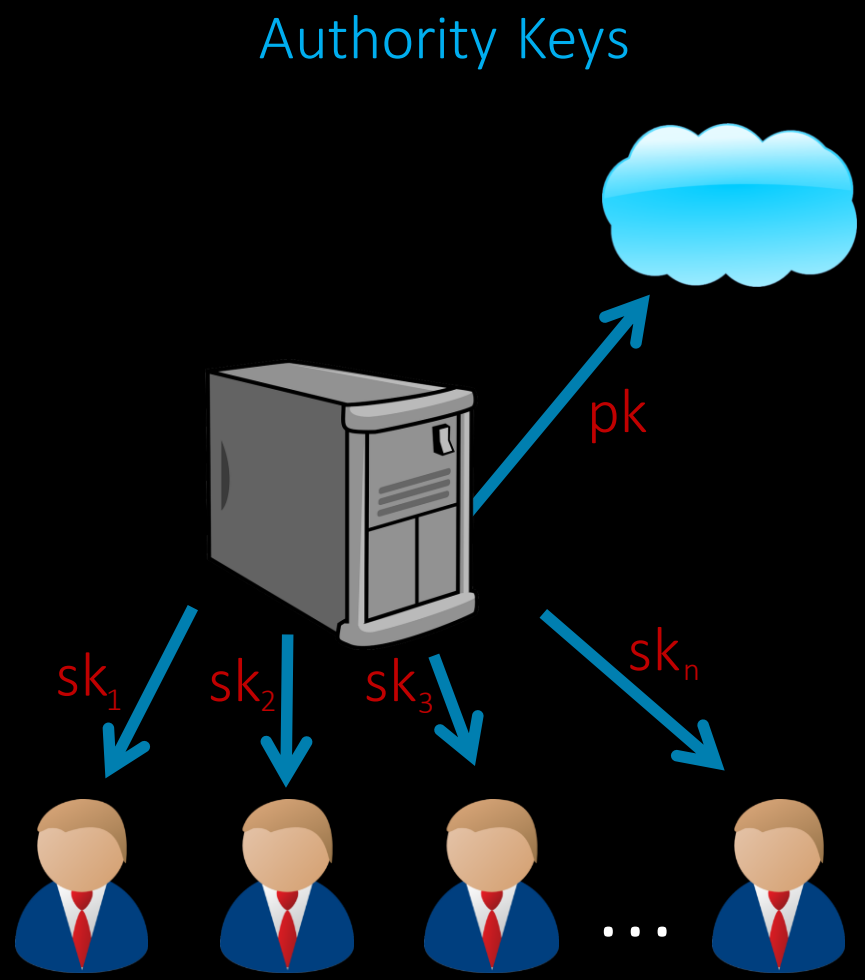
- Keys Generation (Authority and voters).
- Ballot Generation.
- Ballot Verification.

} Inside voting booth

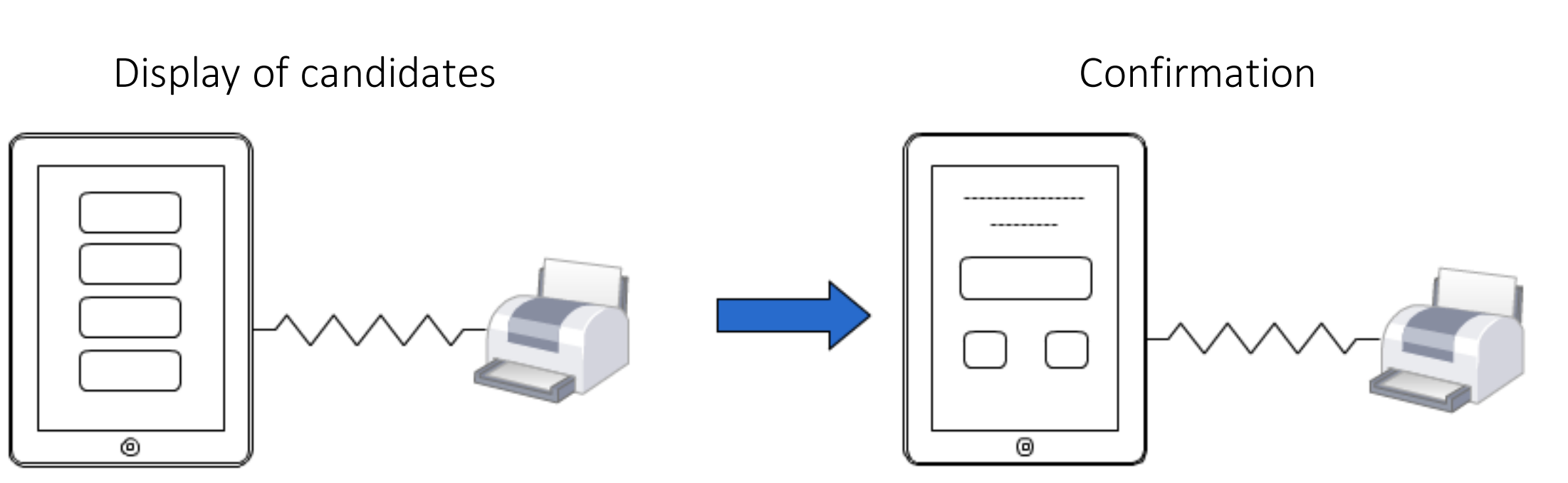
- Ballot Casting.
- Count of Votes.

1) Keys Generation

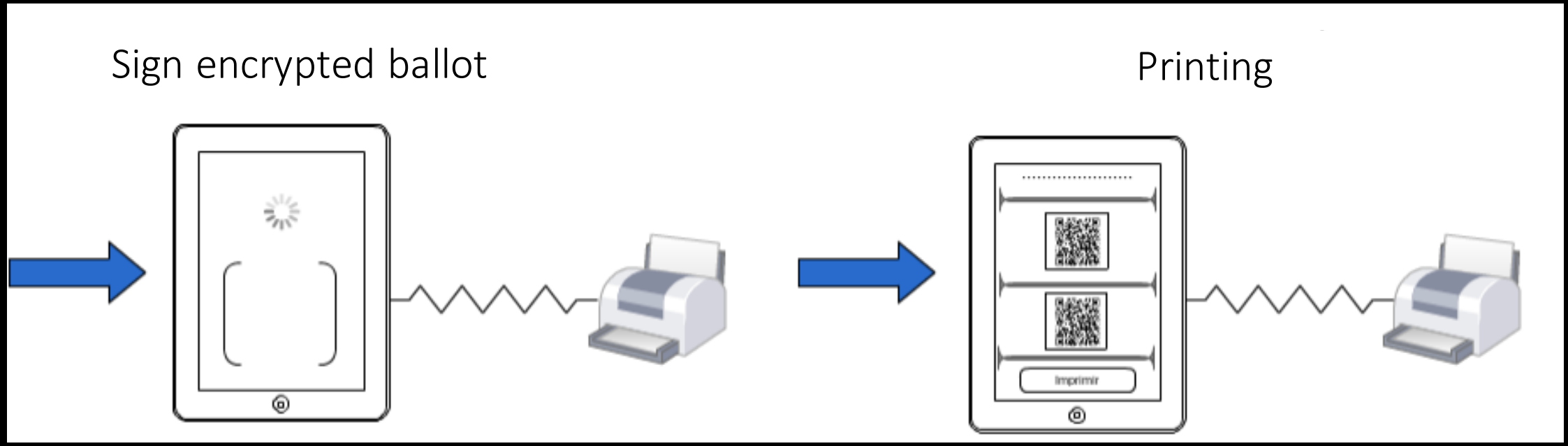




2) Ballot Generation



2) Ballot Generation



2) Ballot Generation

Generates ballot with three parts:

1.- Selection in plain text (VVPAT).

2.- Encryption of the selection + signature.

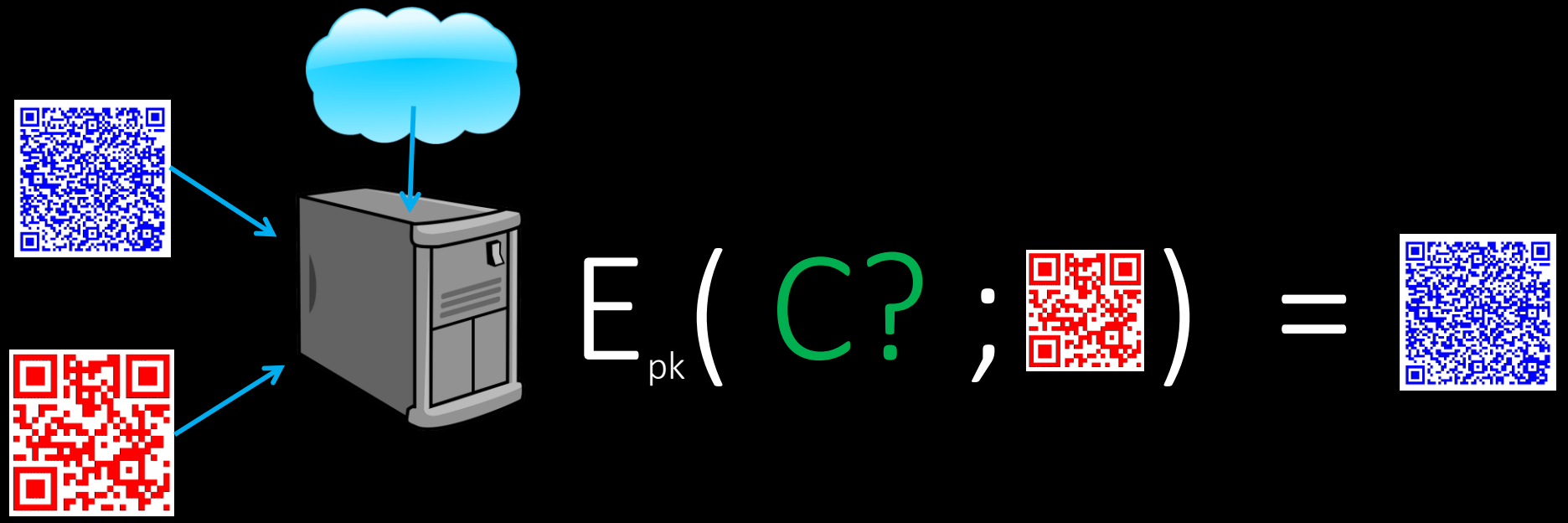
3.- Randomness used to encrypt.

3) Ballot Verification

Simple algorithm.

Minimal hardware.

Counteract (possible) complexity of ballot generation.



4) Ballot Casting

The randomness (third part of the ballot) needs to be destroyed-> Prevent proof by the voter of how she voted.

Capture the encrypted ballot (second part), after verify the signature.

Upload the encrypted ballot to the bulletin-board.

Voter deposits the plain text (first part) folded to an urn.

Voter can take home the encrypted ballot, to verify his ballot was tallied.

5) Count of Votes

Homomorphic property of the encryption system (Paillier, for example).

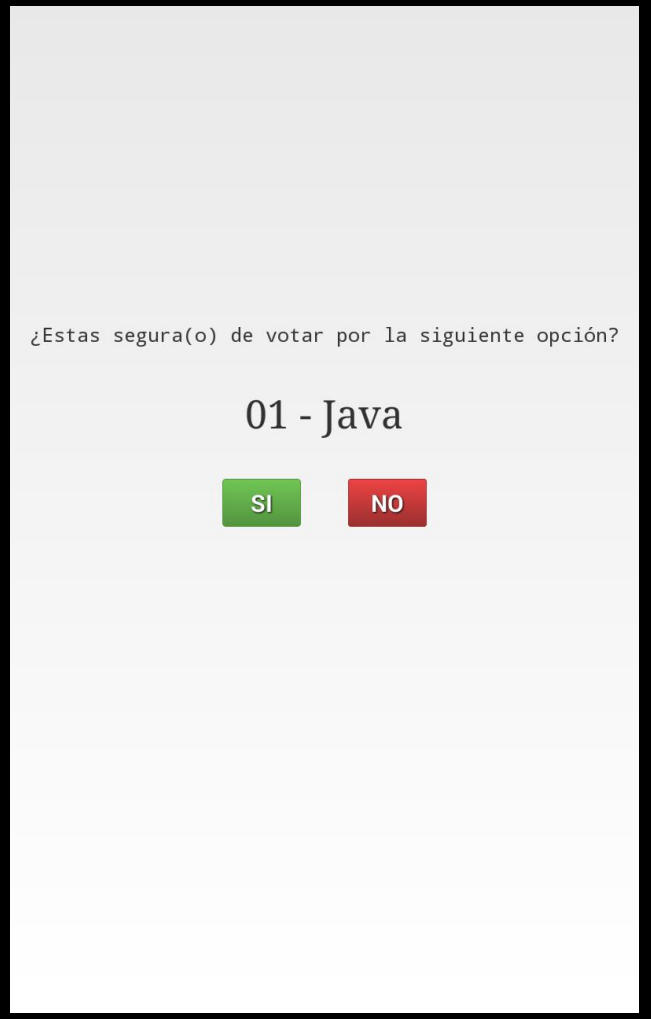
Ballots on the bulletin-board.

With Paillier, the bulletin-board calculates the multiplication of the votes, and this is given to each of the authorities.

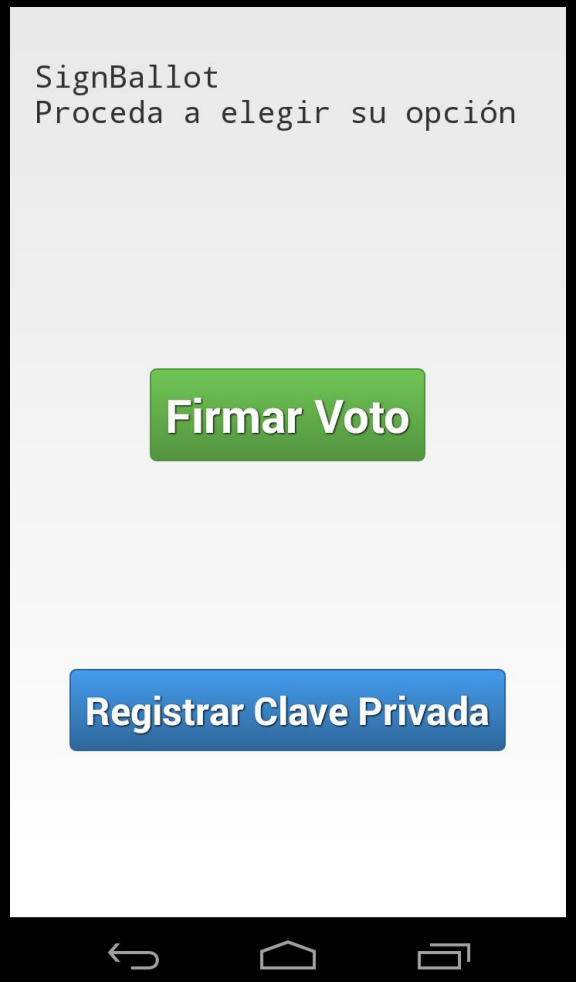
Each authority decrypts this value using his part of the private key (threshold) and uploads it to the bulletin-board.

Finally, the bulletin-board combines the values given by the authorities and displays the result ofthe election.

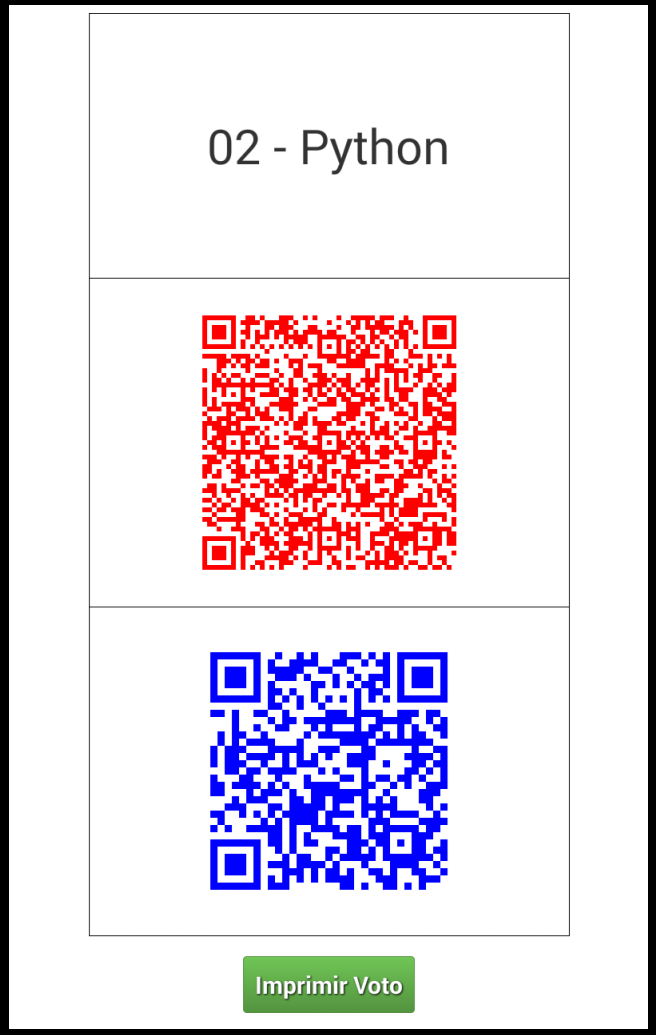
Implementation (Ballot Generation)



Implementation (Ballot Signing)



Implementation (Ballot Generation)



Implementation (Ballot Verification)

Hardware used:

- Raspberry Pi B+: Minimal hardware to run the application.
- 2D Code-Reader.

Improve usability for the voter.

Implementation (At the moment)

Application for the election administrator, to configurate all the aspects of the election, in a simple way.

Application for the authorities, to save the private key, and decrypt the value given by the bulletin-board, and upload it.

Interface of the bulletin-board, to have an easy access to check if the ballot will be tallied, and navigate through all the public information.

Future work

Formalize the security of the system (threat model, power of the adversaries, capability of the voters, etc.)

Improve usability of the system.

Rigorous analysis of the libraries used.

Specify the protocol for handling different situations (wrong signature, encryption fails systematically, etc.)

A Modular, Dual and Voter-Verifiable Electronic Voting System

Camilo Gómez N.
cjgomez@dcc.uchile.cl
@milogomez_
Github.com/CamiloG