Belenios: a simple private and verifiable electronic voting system

Authors : Véronique Cortier, Pierrick Gaudry, Stéphane Glondu

CNRS, Inria, Univ. Lorraine, France

UNIVERSITÉ DE LORRAINE

Arnaud Labourel (AMU, CNRS, LIS)

Distributed team
ALGOrithms seminar

Online electronic voting systems

E(lectroning)-voting systems

E(lectroning)-voting system

Voting system that uses computers to take care of casting and counting ballots.

Two kinds of e-voting:

- **Machine-based:** the voter uses voting machines located at polling stations.
- **Online (the subject of this talk):** the voter submits via the Internet his or her vote electronically to the election authorities, from any location.

Online e-voting systems

Online e-voting systems are now used for important elections in several countries: Australia, Estonia, Switzerland, Russia, USA, France, ...

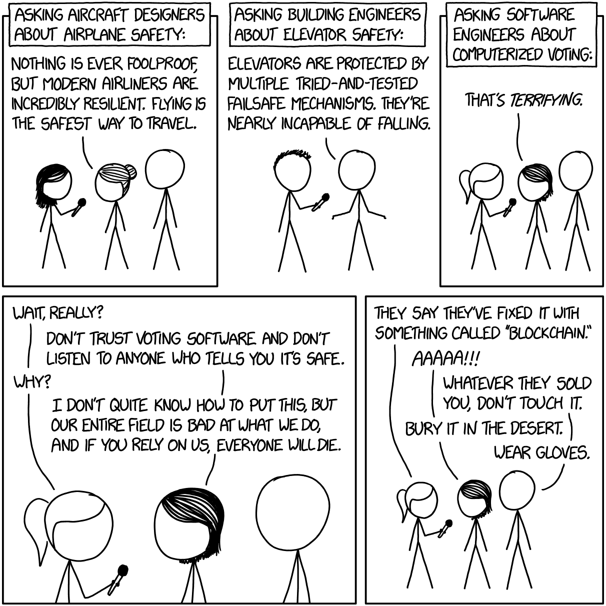
Pros

- Speed up the tallying of votes for complex elections
- Facilitate the participation and organization of elections

Cons

- Security experts have found security problems in most attempts at online e-voting systems
- Online e-voting systems are difficult to understand $\Rightarrow$ less trust from voters

XKCD (Randall Munroe): Voting software


ASKING AIRCRAFT DESIGNERS ABOUT AIRPLANE SAFETY:
NOTHING IS EVER FOOLPROOF, BUT MODERN AIRLINERS ARE INCREDIBLY RESILIENT. FLYING IS THE SAFEST WAY TO TRAVEL.
ASKING BUILDING ENGINEERS ABOUT ELEVATOR SAFETY:
ELEVATORS ARE PROTECTED BY MULTIPLE TRIED-AND-TESTED FAILSAFE MECHANISMS. THEY'RE NEARLY INCAPABLE OF FALLING.
ASKING SOFTWARE ENGINEERS ABOUT COMPUTERIZED VOTING:
THAT'S TERRIFYING.
WAIT, REALLY?
DON'T TRUST VOTING SOFTWARE AND DON'T LISTEN TO ANYONE WHO TELLS YOU IT'S SAFE.
WHY?
I DON'T QUITE KNOW HOW TO PUT THIS, BUT OUR ENTIRE FIELD IS BAD AT WHAT WE DO, AND IF YOU RELY ON US, EVERYONE WILL DIE.
THEY SAY THEY'VE FIXED IT WITH SOMETHING CALLED "BLOCKCHAIN."
AAAAA!!!
WHATEVER THEY SOLD YOU, DON'T TOUCH IT.
BURY IT IN THE DESERT.
WEAR GLOVES.

Online voting: not a perfect solution !

There are a lot of concerns for the use of online voting : coercion, trust, security, ...

- Online voting systems are not recommended by expert for high stake elections
- They can be used for other elections instead of remote postal voting

VÉRONIQUE CORTIER
PIERRICK GAUDRY

Préface de Gérard Berry

LE VOTE ÉLECTRONIQUE

Les défis du secret
et de la transparence

Odile Jacob

What is Belenios?

Belenios

What is Belenios?

An electronic voting protocol with:

- **Vote privacy**: no one (except the voter herself) should know the content of the vote
- **Full verifiability**: possibility to check that the votes are correctly counted

even against a compromised voting server.

- Designed by two researchers of CNRS and one engineer of Inria
- Open source code available since 2015
- Machine-checked proved with the Easycrypt tool

Other systems similar to Belenios

- **Helios**: the voting system from which Belenios is based without mechanisms to avoid ballot stuffing from a dishonest public board.
- **CHVote**: Swiss electronic voting systems with similar properties and using of the same cryptographic tools
- **Neuchâtel protocol**: another swiss voting protocol verified with ProVerif (automatic cryptographic protocol verifier)
- **Civitas**: only voting protocol with both verifiability and coercion resistance (voters can produce fake credentials and cannot prove their vote to other parties)
- ...

Vote privacy

Intuitively easy to understand but difficult to formally define
$\Rightarrow$ no well established consensus on a formal definition

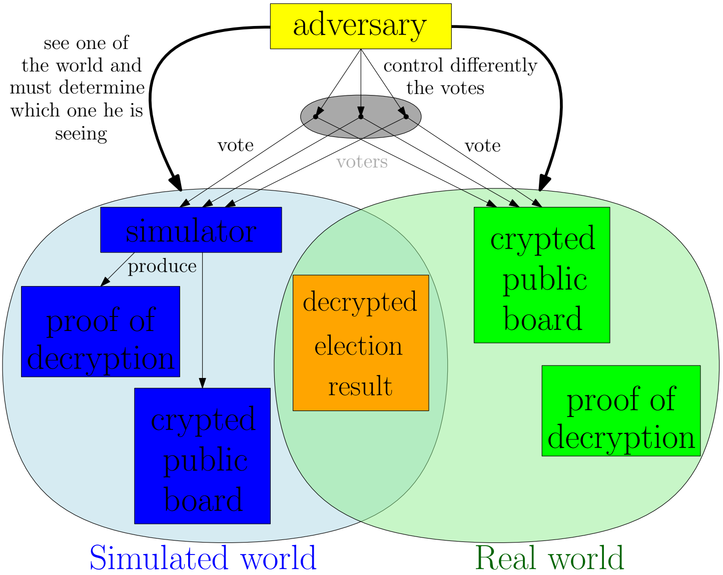
Definition used by the creators of Belenios

Privacy definition BPRIV

Game-based definition: any (limited) adversary is unable to distinguish between a real world and a simulated world by checking the public board

Public board: list of legitimate encrypted ballots that is available at any time of the election

BPRIV experiment



BPRIV experiment

- There are two worlds: a real one and a simulated one and the adversary is in one of them
- The adversary can:
  - control differently the votes of honest voters in both worlds
  - check the public board of the world he is in with all the encrypted ballots
    - either the real one
    - for a fake simulated one
  - cast any ballot in both worlds
- At the end of the election, the adversary gets the result of the election of the real world with a proof:
  - issued from the algorithm if he is in the real world
  - faked by a simulator s.t. it corresponds to the real result but with respect to the fake public board

BPRIV experiment

BPRIV privacy definition

If no polynomial-time adversary can guess with a non-negligible advantage in which world he is, then the scheme respects privacy.

Capture the fact that, besides the result of the election, no other data should leak information about the votes.

Verifiability

Often divided into three sub-properties:

- **individual verifiability:** a voter can check that her vote has been properly counted;
- **universal verifiability:** everyone can check that the result corresponds to the ballots on the public bulletin board;
- **eligibility verifiability:** everyone can check that ballots come from legitimate voters

Verifiability

The result of the vote must correspond to:

- all the votes of honest voters who have checked their votes;
- some votes from other honest voters;
- a number of valid votes smaller than the number of corrupted voters.

In Belenios, verifiability is guaranteed except if both the entity managing the credentials of voters and the server hosting the public board (list of ballots) are compromised.

Global ideas behind Belenios

Separate the responsibilities between different entities :

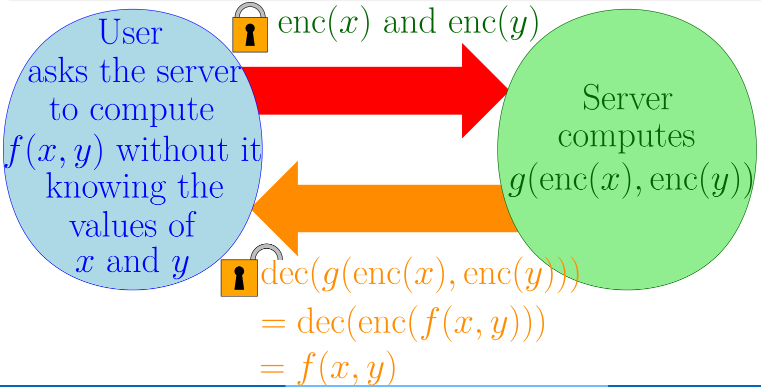
1. **Registrar**: generates credential for voters.
2. **Voting server**: maintains available for all the list of encrypted ballots (public board), accepts ballot after checking that it is valid.
3. **Decryption trustees**: collectively detain the private key of the election ($t + 1$ trustees are needed to decrypt the result of the election).

Global ideas behind Belenios

Partially homomorphic encryption

enc is a partially homomorphic encryption scheme if there are two functions *f* and *g* such that :

$$\forall x, y, g(\mathrm{enc}(x), \mathrm{enc}(y)) = \mathrm{enc}(f(x, y))$$



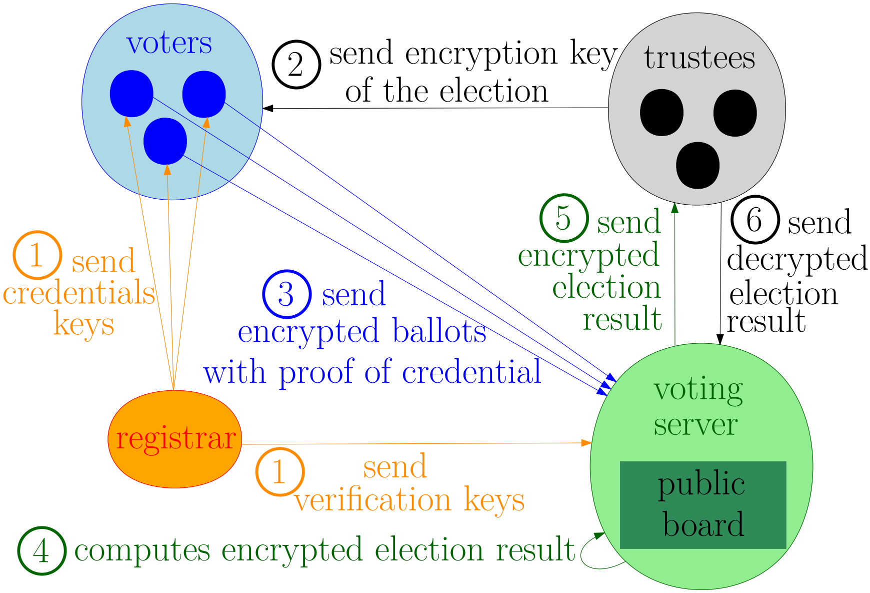
User asks the server to compute $f(x, y)$ without it knowing the values of x and y

$\mathrm{enc}(x)$ and $\mathrm{enc}(y)$

Server computes $g(\mathrm{enc}(x), \mathrm{enc}(y))$

$\mathrm{dec}(g(\mathrm{enc}(x), \mathrm{enc}(y)))$
$= \mathrm{dec}(\mathrm{enc}(f(x, y)))$
$= f(x, y)$

Global ideas behind Belenios



voters

trustees

2 send encryption key of the election

1 send credentials keys

3 send encrypted ballots with proof of credential

5 send encrypted election result

6 send decrypted election result

registrar

1 send verification keys

voting server

public board

4 computes encrypted election result

Cryptographic tools used by Belenios

- Partially homomorphic ElGamal encryption scheme
  used to encrypt the votes
- Cryptographic hash function
  used for signatures and ZKP
- Non-interactive Zero-Knowledge Proofs (ZPK) used
  - by voters to prove validity of votes and avoid ballot stuffing
  - by trustees to prove the correct decryption of the election result
- Schnorr signature scheme
  used to sign the ballot
- Pedersen's threshold secret sharing scheme
  used by trustees s.t. no single authority has the private key of the election

Partial conclusion

Partial conclusion

We have seen :

- the electronic voting system Belenios
- the global ideas behind it

Next week, we will see :

- the cryptographic tools used by Belenios
- more details on how Belenios works and how it is implemented