Cast as Intended in voting protocols

Véronique Cortier, CNRS, Loria (Nancy, France)

Joint work with Alexandre Debant, Pierrick Gaudry, Stéphane Glondu, Anselme Goetschmann, Sophie Lemonnier

EVoteID, October 2023

What is a good voting system?

Confidentiality of the votes

Vote privacy

"No one should know how I voted"

Confidentiality of the votes

Vote privacy

"No one should know how I voted"

Better: Receipt-free / Coercion-resistant

"No one should know how I voted,
even if I am willing to tell my vote! "

- vote buying
- coercion

Confidentiality of the votes

Vote privacy

"No one should know how I voted"

Better: Receipt-free / Coercion-resistant

"No one should know how I voted,
even if I am willing to tell my vote! "

- vote buying
- coercion

Everlasting privacy: no one should know my vote, even when the cryptographic keys will be eventually broken.

Verifiability

Individual Verifiability: a voter can check that

- cast as intended: their ballot contains their intended vote
- recorded as cast: their ballot is in the ballot box.

Universal Verifiability: everyone can check that

- tallied as recorded: the result corresponds to the ballot box.
- eligibility: ballots have been casted by legitimate voters.

You should verify the election,
not the system.

Verifiability

Individual Verifiability: a voter can check that

- cast as intended: their ballot contains their intended vote
- recorded as cast: their ballot is in the ballot box.

Universal Verifiability: everyone can check that

- tallied as recorded: the result corresponds to the ballot box.
- eligibility: ballots have been casted by legitimate voters.

You should verify the election,
not the system.

Even better: accountability

- the system tells whom to blame
- eases dispute resolution

And many more properties

- Availability: servers available at any time
- Accessibility: easy to use, adapted to people with various issues
- ...

And many more properties

- Availability: servers available at any time
- Accessibility: easy to use, adapted to people with various issues
- ...

In this talk, focus on verifiability.

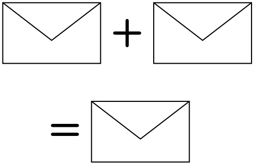
- cast ast intended
- recorded as cast
- tallied as recorded
- eligibilty verifiability

Tallied as recorded

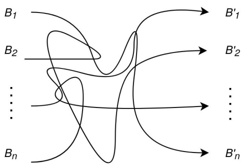
The result corresponds to the ballot box.

✓ Well studied academically, with two main techniques:

Homomorphic tally



Mixnet

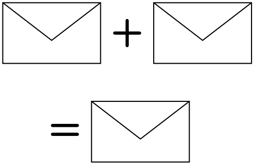


Tallied as recorded

The result corresponds to the ballot box.

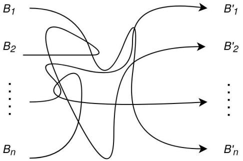
✓ Well studied academically, with two main techniques:

Homomorphic tally



In practice:

Mixnet



- ✓ Many deployed solutions use such techniques: Estonia, France, Switzerland, ...
- Many national evoting companies are still behind

Recorded as cast

✓ easy in theory: the voter simply checks that their ballot appear on the bulletin board

- Not so easy in practice

  - require a public bulletin board
  - voters do not check

Recorded as cast

✓ easy in theory: the voter simply checks that their ballot appear on the bulletin board

■ Not so easy in practice

- require a public bulletin board
- voters do not check

Alternative approaches

- delegation: voters send their ballot to a third party (eg French Legislative system, Polyas, ...)
- Swiss Post: the verification is embedded in the cast-as-intended mechanism, requires distributed servers
- Estonia: the ballot is sent (by the server) to another system component

Eligibility verifiability

✓academically: just sign but...

- require a PKI
- public voter list? everlasting privacy?

Eligibility verifiability

✓academically: just sign but...

- require a PKI
- public voter list? everlasting privacy?

In practice

- ✓ Estonia: voters sign with their id cards
  - ✓ strong and verifiable eligibility
  - ■ no public board
- ✗ login/password sent by mail, SMS $\rightarrow$ no eligibility verifiability
- ■ distributed trust between authorities, eg Belenios (OTP + asymmetric key credential)

Cast as intended (CaI)

- Few academic protocols

??? but yet a lot of systems in practice!

Cal in Australia

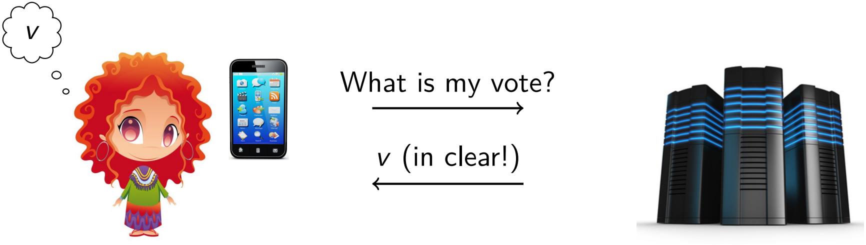
iVote system in the 2015 state election in New South Wales

What is my vote? $\longrightarrow$

v (in clear!) $\longleftarrow$

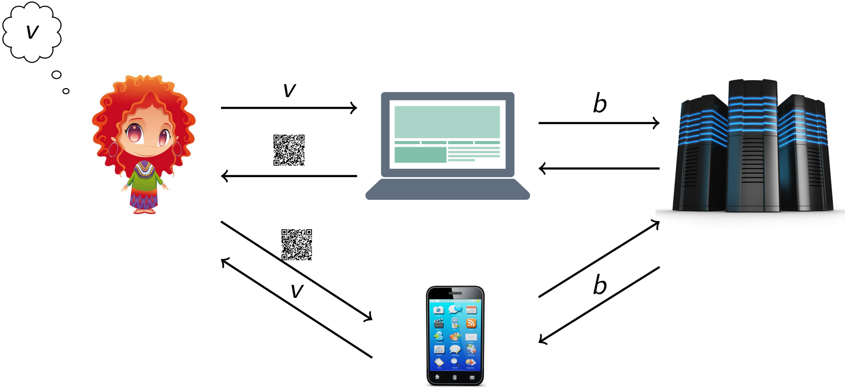
Cal in Australia

iVote system in the 2015 state election in New South Wales

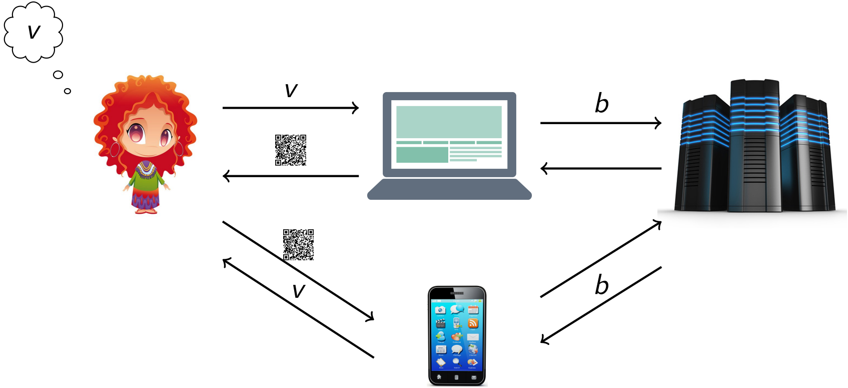


- ✓ simple
- ✓ cast-as-intended
- ✗ no vote privacy ⚠
- ✗ no cast-as-recorded

Cal in Estonia

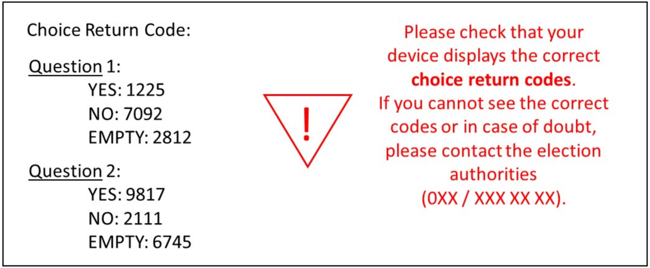


Cal in Estonia



- ✓ cast-as-intended
- some vote-buying threats (mitigated)
- proxy cast-as-recorded
- heavy infrastructure (two independent servers)

Cal in Switzerland



Choice Return Code:

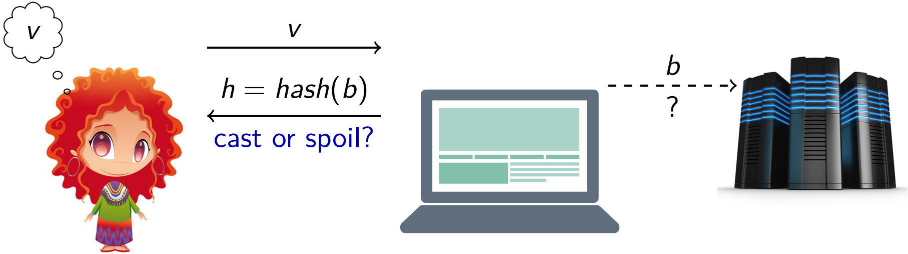
Question 1:
YES: 1225
NO: 7092
EMPTY: 2812

Question 2:
YES: 9817
NO: 2111
EMPTY: 6745

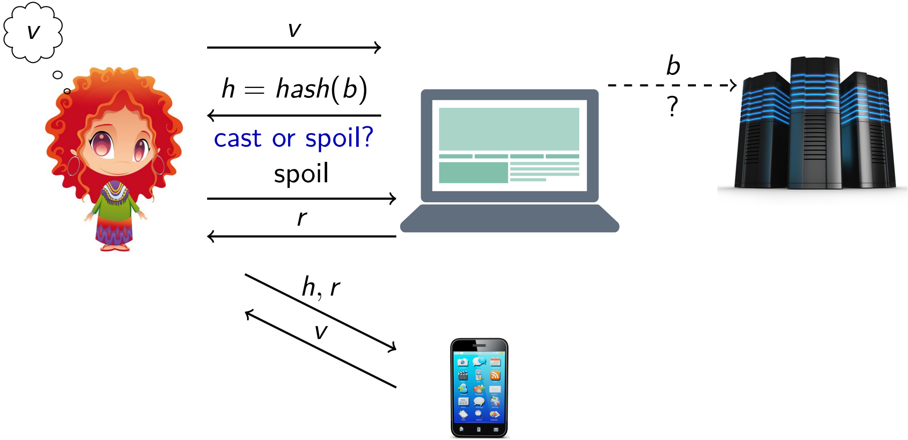
Please check that your device displays the correct **choice return codes**. If you cannot see the correct codes or in case of doubt, please contact the election authorities (0XX / XXX XX XX).

- ✓ cast-as-intended
- proxy cast-as-recorded
- heavy infrastructure (four independent servers)

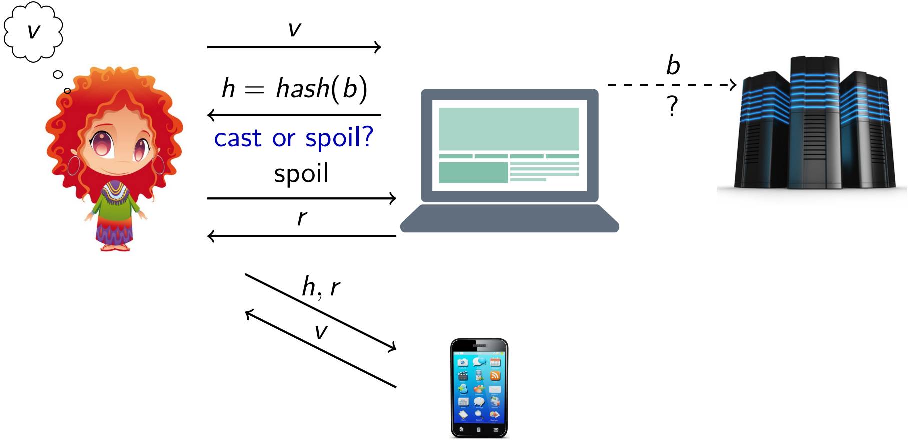
Benaloh's challenge: cast or spoil



Benaloh's challenge: cast or spoil



Benaloh's challenge: cast or spoil



- ✓ simple principle
- ✓ can be adapted to many systems
- ■ requires a second device

Helios Voting Booth

exit

Choice of the EVoteID nicest location

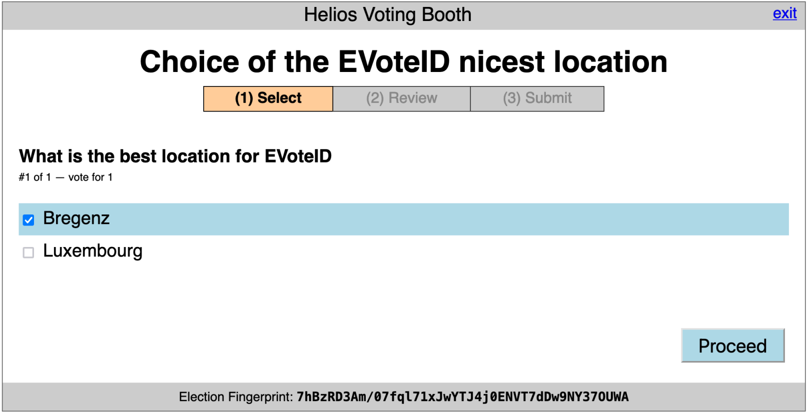
To vote, follow these steps:

1. **Select** your preferred options.
2. **Review** your choices, which are then encrypted.
3. **Submit** your encrypted ballot and authenticate to verify your eligibility.

Start

You can email for help.

Election Fingerprint: **7hBzRD3Am/07fql71xJwYTJ4j0ENVT7dDw9NY37OUWA**


Helios Voting Booth
exit
Choice of the EVoteID nicest location
(1) Select
(2) Review
(3) Submit
What is the best location for EVoteID
#1 of 1 — vote for 1
Bregenz
Luxembourg
Proceed
Election Fingerprint: 7hBzRD3Am/07fql71xJwYTJ4j0ENVT7dDw9NY37OUWA

Helios Voting Booth

exit

Choice of the EVoteID nicest location

(1) Select | **(2) Review** | (3) Submit

Review your Ballot

Question #1: What is the best location for EVoteID
✓ **Bregenz**
[change]

Your ballot tracker is **+JLW+ti+ERZLOjPQNeRIAFi7RD6ZHIakX9a6n6XFWno**.

Submit this Vote

Spoil & Audit [optional]

Election Fingerprint: **7hBzRD3Am/07fql71xJwYTJ4j0ENVT7dDw9NY37OUWA**

Helios Voting Booth exit

Choice of the EVoteID nicest location

(1) Select | **(2) Review** | (3) Submit

Review your Ballot

Question #1: What is the best location for EVoteID
✓ **Bregenz**
[change]

Your ballot tracker is **+JLW+ti+ERZLOjPQNeRIAFi7RD6ZHIakX9a6n6XFWno**.

Submit this Vote

Spoil & Audit [optional]

If you choose, you can spoil this ballot and reveal how your choices were encrypted. This is an optional auditing process.

You will then be guided to re-encrypt your choices for final casting.

Spoil & Audit

Election Fingerprint: **7hBzRD3Am/07fql71xJwYTJ4j0ENVT7dDw9NY37OUWA**

Helios Voting Booth exit

Choice of the EVoteID nicest location

(1) Select | **(2) Review** | (3) Submit

Review your Ballot

Question #1: What is the best location for EVoteID
✓ **Bregenz**
[change]

Your ballot tracker is **+JLW+ti+ERZLOjPQNeRIAFi7RD6ZHIakX9a6n6XFWno**.

Submit this Vote

Spoil & Audit [optional]

If you choose, you can spoil this ballot a
reveal how your choices were encrypted
is an optional auditing process.

You will then be guided to re-encrypt yo
choices for final casting.

Spoil & Audit

Vote privacy issue!

The voter is likely to use their true vote.

Election Fingerprint: **7hBzRD3Am/07fql71xJwYTJ4j0ENVT7dDw9NY37OUWA**

Benaloh: voter strategy

A voter should

1. decide at random if they will truly vote or audit
2. → if vote, then vote
   → if audit, decide at random then audit and go to step 1

- ✗ usability
- ■ which probabilities to use?
- ▶ is it truly cast-as-intended? (see e.g. Jamroga's talk)

Other Cal solutions

Select, Selene, Hyperion: votes appear in clear on the ballot box

- ✓ simple for the voters
- specific systems
- adversary caught to late
  $\rightarrow$ strong accountability needed

Other CaI solutions

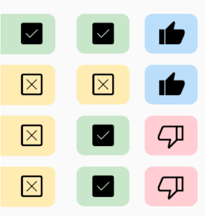
Select, Selene, Hyperion: votes appear in clear on the ballot box

- ✓ simple for the voters
- specific systems
- adversary caught to late
  $\rightarrow$ strong accountability needed

Two device solutions: Du-Vote, CAISED (this Friday!)

Our proposal: BeleniosCal

BELENIOS +



- based on Belenios
- could be adapted to other protocols
- no second device (except to read BB), no paper material
- on the fly detection
- one server

Voting protocol Belenios

- variant of Helios, designed by Ben Adida
- developed at Loria, teams Pesto and Caramba (P. Gaudry)
  Developer: Stéphane Glondu
- used in 2000+ elections, with a total of 100 000+ voters

`http://www.belenios.org/`

- confidentiality of the votes
- verifiability of the voting process
  → The ballot box is public at any time.
  → All the operations (tally, ...) can be checked by anyone.

How Belenios works (simplified)

Phase 1: vote

pkE

Ballot Box

Alice	$\{v_A\}_{\text{pkE}}$	$v_A = 0$ or 1
Bob	$\{v_B\}_{\text{pkE}}$	$v_B = 0$ or 1
Chris	$\{v_C\}_{\text{pkE}}$	$v_C = 0$ or 1

pkE: public key, the private keys are shared among the authorities.

How Belenios works (simplified)

Phase 1: vote

$id, \{v\}^r_{\mathrm{pkE}}$ →

pkE

Ballot Box

Alice	$\{v_A\}_{\mathrm{pkE}}$	$v_A = 0$ or 1
Bob	$\{v_B\}_{\mathrm{pkE}}$	$v_B = 0$ or 1
Chris	$\{v_C\}_{\mathrm{pkE}}$	$v_C = 0$ or 1

pkE: public key, the private keys are shared among the authorities.

How Belenios works (simplified)

Phase 1: vote

pkE

Ballot Box		
Alice	$\{v_A\}_{\text{pkE}}$	$v_A = 0$ or 1
Bob	$\{v_B\}_{\text{pkE}}$	$v_B = 0$ or 1
Chris	$\{v_C\}_{\text{pkE}}$	$v_C = 0$ or 1
David	$\{v_D\}_{\text{pkE}}$	$v_D = 0$ or 1

pkE: public key, the private keys are shared among the authorities.

How Belenios works (simplified)

Phase 1: vote

pkE

Ballot Box		
Alice	$\{v_A\}_{\text{pkE}}$	$v_A = 0$ or 1
Bob	$\{v_B\}_{\text{pkE}}$	$v_B = 0$ or 1
Chris	$\{v_C\}_{\text{pkE}}$	$v_C = 0$ or 1
David	$\{v_D\}_{\text{pkE}}$	$v_D = 0$ or 1
...	...	

Phase 2: Tally - homomorphic encryption (El Gamal)

$$\{v_1\}_{\text{pkE}} \times \cdots \times \{v_n\}_{\text{pkE}} = \{v_1 + \cdots + v_n\}_{\text{pkE}} \quad \text{since } g^a \times g^b = g^{a+b}$$

$\rightarrow$ Only the final result needs to be decrypted! And proved.

pkE: public key, the private keys are shared among the authorities.

Eligibility

$id, \{v\}^r_{\mathsf{pkE}}$ →

pkE

Ballot box

Alice	$\{v_A\}_{\mathsf{pkE}}$
Bob	$\{v_B\}_{\mathsf{pkE}}$
Chris	$\{v_C\}_{\mathsf{pkE}}$
...	...
...	

Eligibility

$id, \{v\}^r_{pkE}$ →

pkE

Ballot box	
Alice	$\{v_A\}_{pkE}$
Bob	$\{v_B\}_{pkE}$
Chris	$\{v_C\}_{pkE}$
...	$\{1\}_{pkE}$
...	$\{1\}_{pkE}$

The ballot box could add ballots!

Eligibility

$id, \{v\}^r_{pkE}$ →

$\mathsf{pkE}\quad \mathsf{vk}(cred_3), \mathsf{vk}(cred_1), \mathsf{vk}(cred_2), \ldots$

Ballot box

Alice	$\{v_A\}_{pkE}$
Bob	$\{v_B\}_{pkE}$
Chris	$\{v_C\}_{pkE}$
...	
...	

~~The ballot box could add ballots!~~

1. During the setup phase, a Registrar generates private signing keys, one for each voter

Eligibility

$id, \{v\}^r_{\mathrm{pkE}}$ →

pkE $\mathrm{vk}(cred_3), \mathrm{vk}(cred_1), \mathrm{vk}(cred_2), \ldots$

Ballot box

Alice	$[\{v_A\}_{\mathrm{pkE}}]_{\mathrm{sk}(cred_1)}$
Bob	$[\{v_B\}_{\mathrm{pkE}}]_{\mathrm{sk}(cred_2)}$
Chris	$[\{v_C\}_{\mathrm{pkE}}]_{\mathrm{sk}(cred_3)}$
...	
...	

~~The ballot box could add ballots!~~

1. During the setup phase, a Registrar generates private signing keys, one for each voter
2. The voters sign their ballot with a “credential” they have received (a credential = a right to vote)

BeleniosCal's principle

Alice' vote

$$bal = \{v\}_{\mathsf{pkE}}^{r_v},$$

BeleniosCal's principle

first control ciphertext

$bal = \{v\}^{r_v}_{\mathsf{pkE}}, \quad \{a\}^{r_a}_{\mathsf{pkE}},$

BeleniosCal's principle

second control ciphertext

$$bal = \{v\}^{r_v}_{\mathsf{pkE}},\ \ \{a\}^{r_a}_{\mathsf{pkE}},\ \ \{b\}^{r_b}_{\mathsf{pkE}},$$

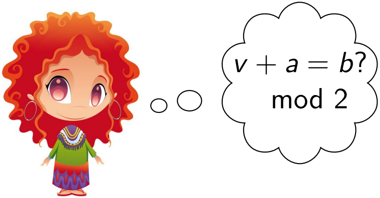
BeleniosCal's principle

proof that binds
the three ciphertexts

$$bal = \{v\}^{r_v}_{\mathsf{pkE}},\ \ \{a\}^{r_a}_{\mathsf{pkE}},\ \ \{b\}^{r_b}_{\mathsf{pkE}},\qquad ZKP(v + a = b \mod 2)$$

BeleniosCal's principle

$$bal = \{v\}_{\mathrm{pkE}}^{r_v}, \quad \{a\}_{\mathrm{pkE}}^{r_a}, \quad \{b\}_{\mathrm{pkE}}^{r_b}, \qquad ZKP(v + a = b \mod 2)$$



BeleniosCal's principle

$$bal = \{v\}^{r_v}_{\mathsf{pkE}}, \boxed{\{a\}^{r_a}_{\mathsf{pkE}},} \{b\}^{r_b}_{\mathsf{pkE}}, \qquad ZKP(v + a = b \mod 2)$$

Pick one of the two control ciphertexts at random

BeleniosCal's principle

$$bal = \{v\}^{r_v}_{\mathsf{pkE}}, \quad \{a\}^{r_a}_{\mathsf{pkE}}, \quad \boxed{\{b\}^{r_b}_{\mathsf{pkE}};} \qquad ZKP(v + a = b \mod 2)$$

Pick one of the two control ciphertexts at random

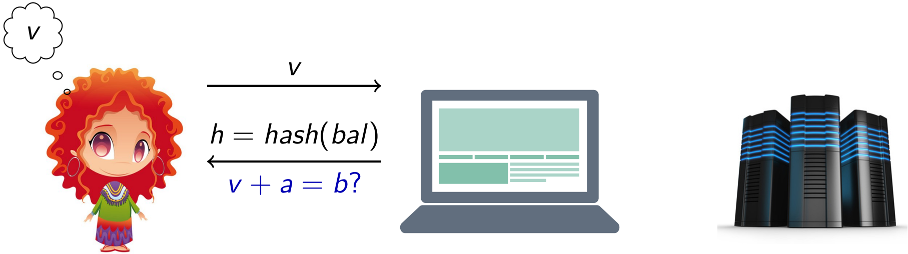
BeleniosCal's principle

$$bal = \{v\}^{r_v}_{\text{pkE}},\ \{a\}^{r_a}_{\text{pkE}},\ \{b\}^{r_b}_{\text{pkE}};\quad ZKP(v + a = b \mod 2)$$

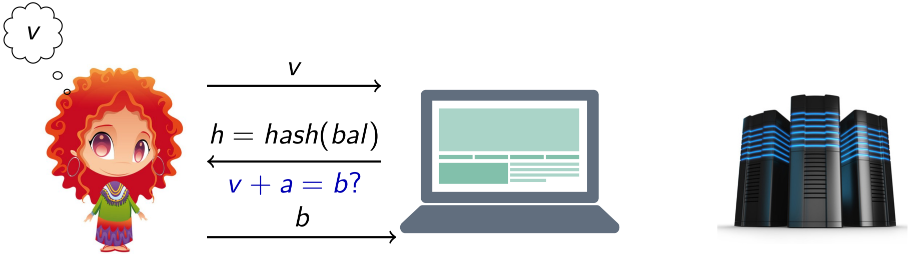
Pick one of the two control ciphertexts at random

checks that $bal, (\_, b)$ appears on the ballot box

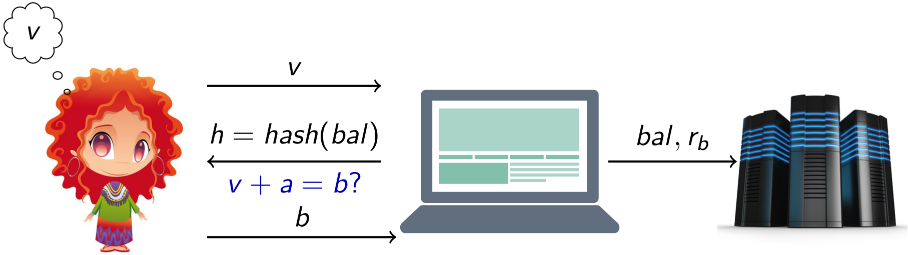
BeleniosCal's principle - continued



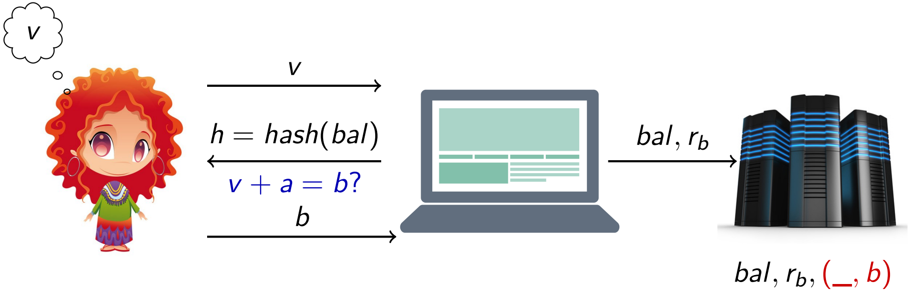
BeleniosCal's principle - continued



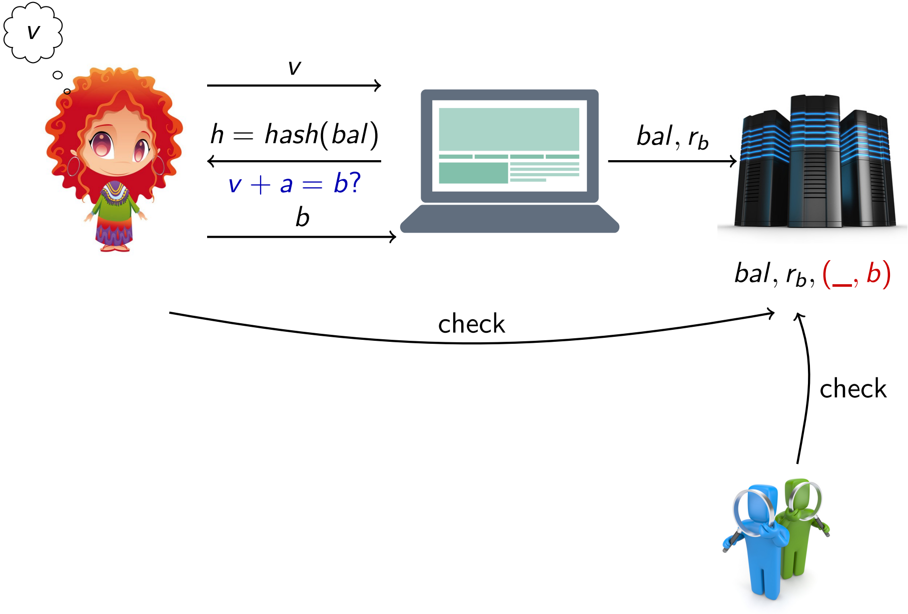
BeleniosCal's principle - continued



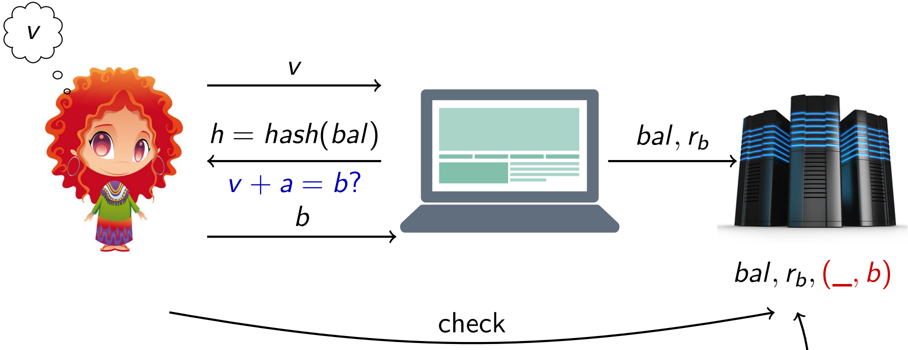
BeleniosCal's principle - continued



BeleniosCal's principle - continued

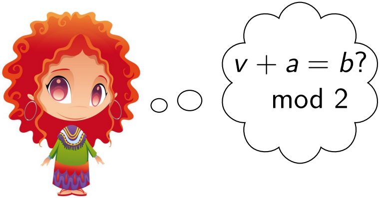


BeleniosCal's principle - continued

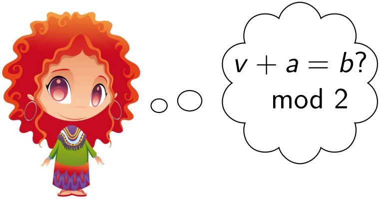


- ✓ no second device
- ✓ no paper material
- ✓ the audited ballot is cast
- ■ Alice needs to check the bulletin board
- ✗ Alice needs to compute modulo 2!

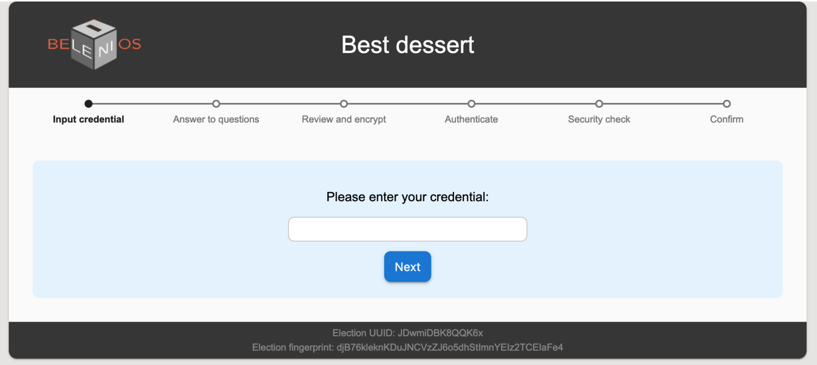
Can voters compute modulo 2 ?!?

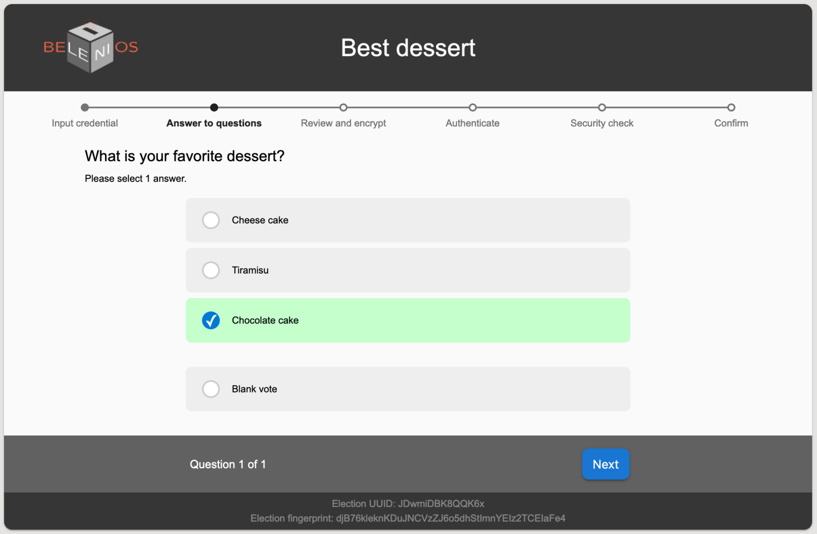


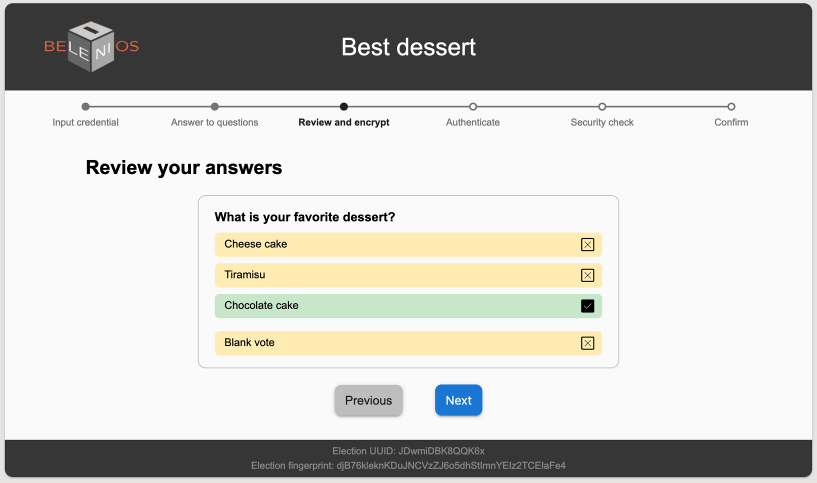
Can voters compute modulo 2 ?!?

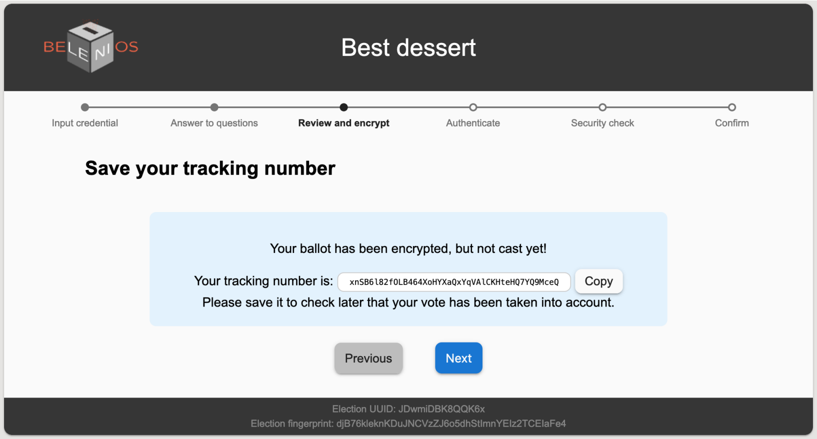


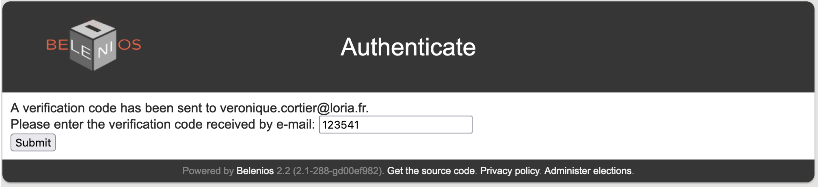
Let see how we propose to implement it.

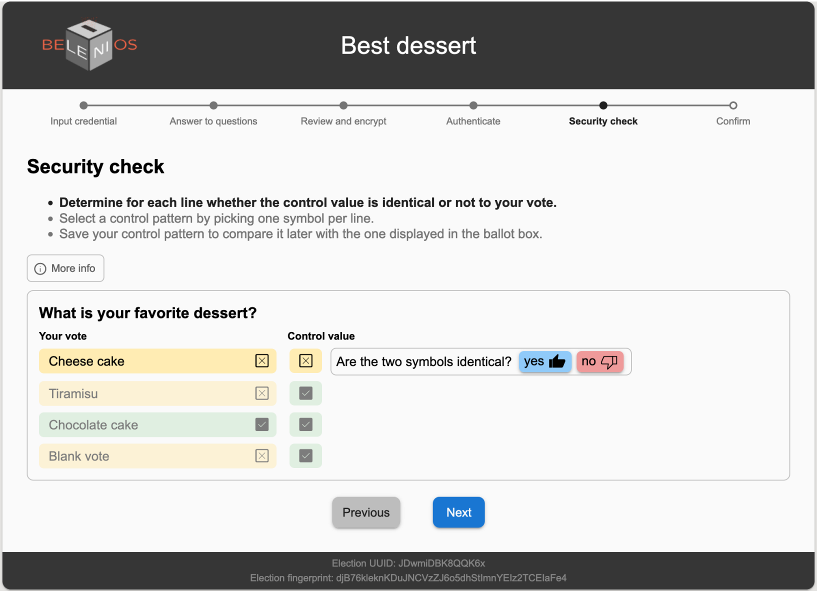

Best dessert
Input credential
Answer to questions
Review and encrypt
Authenticate
Security check
Confirm
Please enter your credential:
Next
Election UUID: JDwmiDBK8QQK6x
Election fingerprint: djB76kleknKDuJNCVzZJ6o5dhStImnYEIz2TCEIaFe4

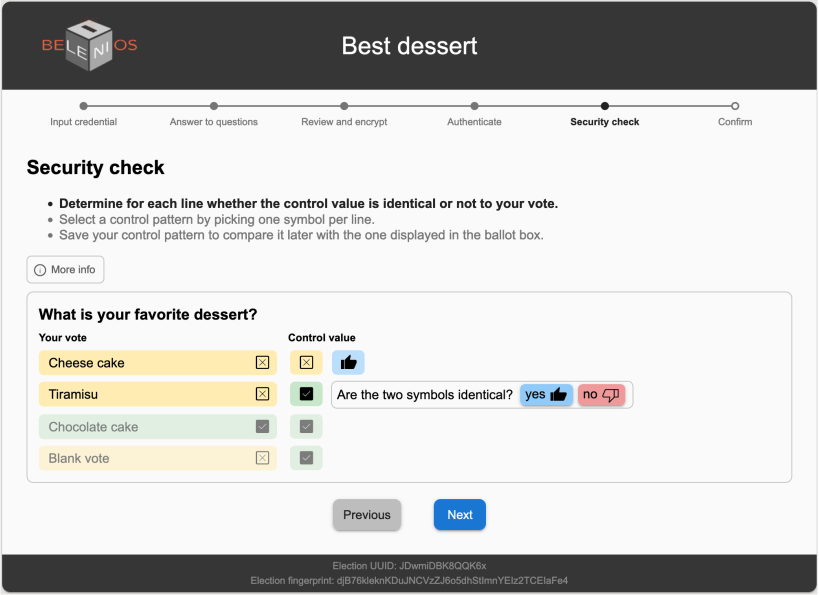

BELENIOS
Best dessert
Input credential
Answer to questions
Review and encrypt
Authenticate
Security check
Confirm
What is your favorite dessert?
Please select 1 answer.
Cheese cake
Tiramisu
Chocolate cake
Blank vote
Question 1 of 1
Next
Election UUID: JDwmiDBK8QQK6x
Election fingerprint: djB76kleknKDuJNCVzZJ6o5dhStlmnYEIz2TCEIaFe4

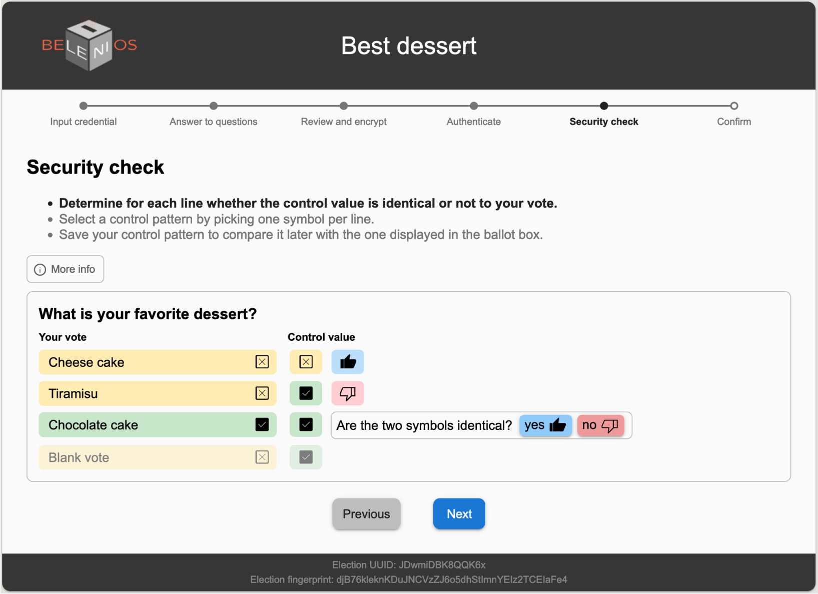

BELENIOS
Best dessert
Input credential
Answer to questions
Review and encrypt
Authenticate
Security check
Confirm
Review your answers
What is your favorite dessert?
Cheese cake
Tiramisu
Chocolate cake
Blank vote
Previous
Next
Election UUID: JDwmiDBK8QQK6x
Election fingerprint: djB76kleknKDuJNCVzZJ6o5dhStlmnYElz2TCElaFe4

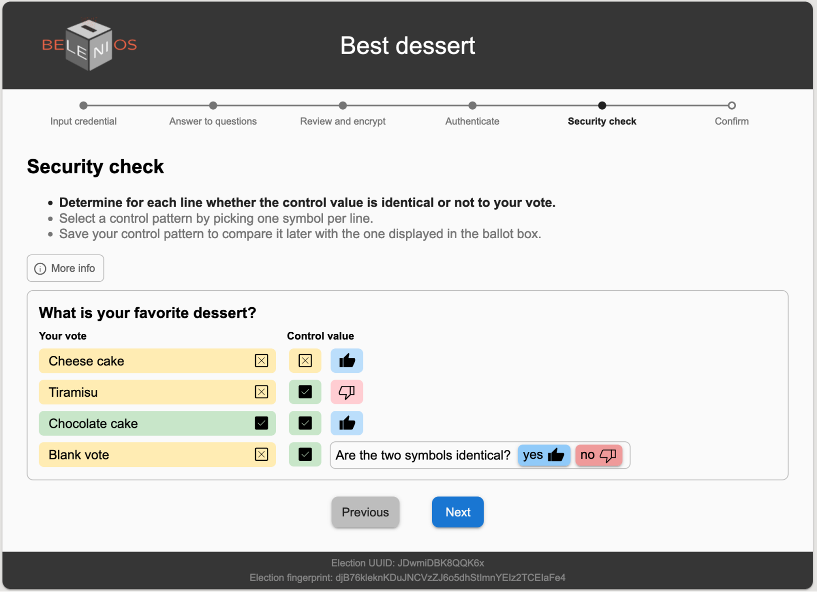

Best dessert
Input credential
Answer to questions
Review and encrypt
Authenticate
Security check
Confirm
Save your tracking number
Your ballot has been encrypted, but not cast yet!
Your tracking number is: xnSB6l82fOLB464XoHYXaQxYqVAlCKHteHQ7YQ9MceQ
Copy
Please save it to check later that your vote has been taken into account.
Previous
Next
Election UUID: JDwmiDBK8QQK6x
Election fingerprint: djB76kleknKDuJNCVzZJ6o5dhStlmnYElz2TCElaFe4

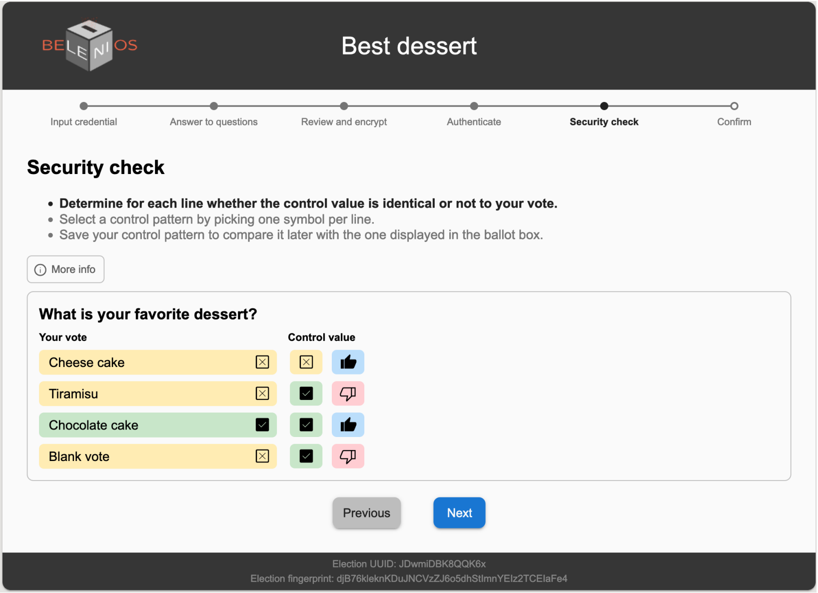

BELENIOS
Authenticate
A verification code has been sent to veronique.cortier@loria.fr.
Please enter the verification code received by e-mail: 123541
Submit
Powered by Belenios 2.2 (2.1-288-gd00ef982). Get the source code. Privacy policy. Administer elections.

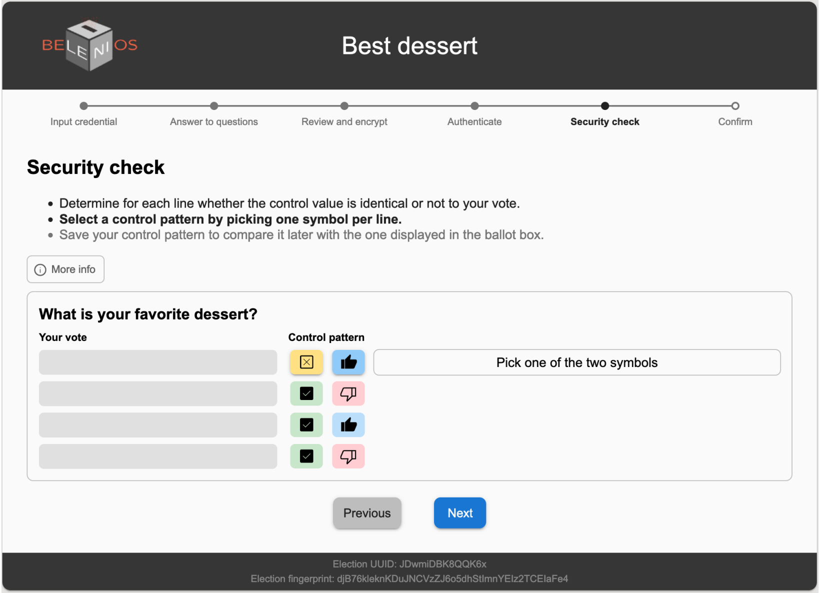

BELENIOS
Best dessert
Input credential
Answer to questions
Review and encrypt
Authenticate
Security check
Confirm
Security check
Determine for each line whether the control value is identical or not to your vote.
Select a control pattern by picking one symbol per line.
Save your control pattern to compare it later with the one displayed in the ballot box.
More info
What is your favorite dessert?
Your vote
Control value
Cheese cake
Are the two symbols identical?
yes
no
Tiramisu
Chocolate cake
Blank vote
Previous
Next
Election UUID: JDwmiDBK8QQK6x
Election fingerprint: djB76kleknKDuJNCVzZJ6o5dhStlmnYElz2TCElaFe4

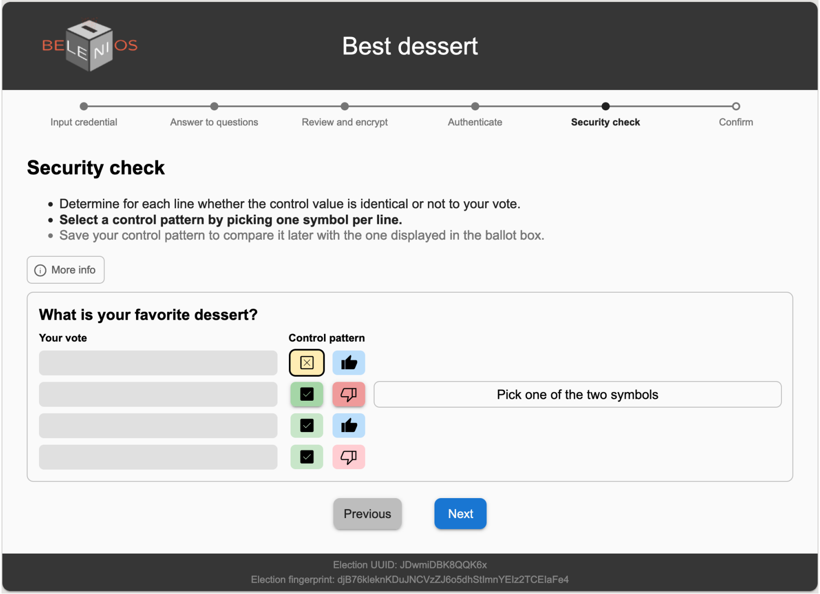

BELENIOS
Best dessert
Input credential
Answer to questions
Review and encrypt
Authenticate
Security check
Confirm
Security check
Determine for each line whether the control value is identical or not to your vote.
Select a control pattern by picking one symbol per line.
Save your control pattern to compare it later with the one displayed in the ballot box.
More info
What is your favorite dessert?
Your vote
Control value
Cheese cake
Tiramisu
Are the two symbols identical?
yes
no
Chocolate cake
Blank vote
Previous
Next
Election UUID: JDwmiDBK8QQK6x
Election fingerprint: djB76kleknKDuJNCVzZJ6o5dhStlmnYElz2TCElaFe4

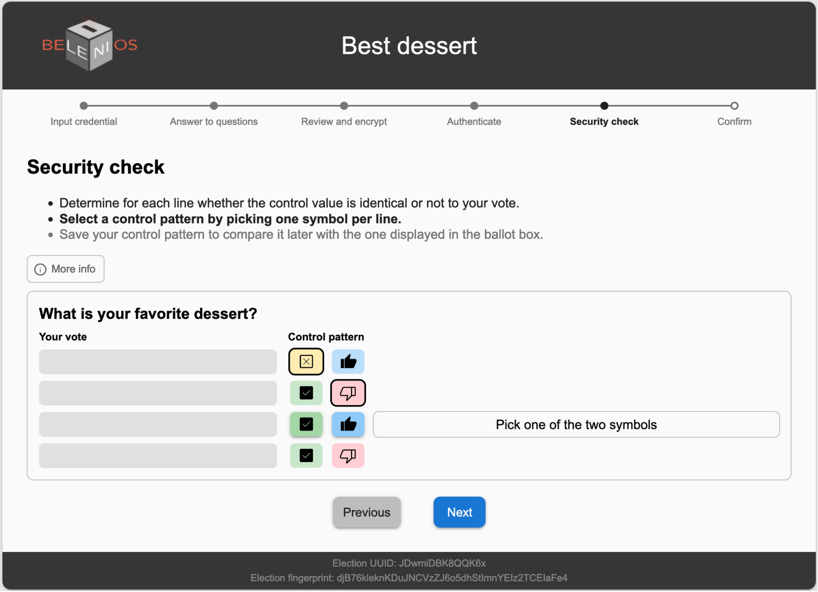

BELENIOS
Best dessert
Input credential
Answer to questions
Review and encrypt
Authenticate
Security check
Confirm
Security check
Determine for each line whether the control value is identical or not to your vote.
Select a control pattern by picking one symbol per line.
Save your control pattern to compare it later with the one displayed in the ballot box.
More info
What is your favorite dessert?
Your vote
Control value
Cheese cake
Tiramisu
Chocolate cake
Blank vote
Are the two symbols identical?
yes
no
Previous
Next
Election UUID: JDwmiDBK8QQK6x
Election fingerprint: djB76kleknKDuJNCVzZJ6o5dhStlmnYElz2TCElaFe4

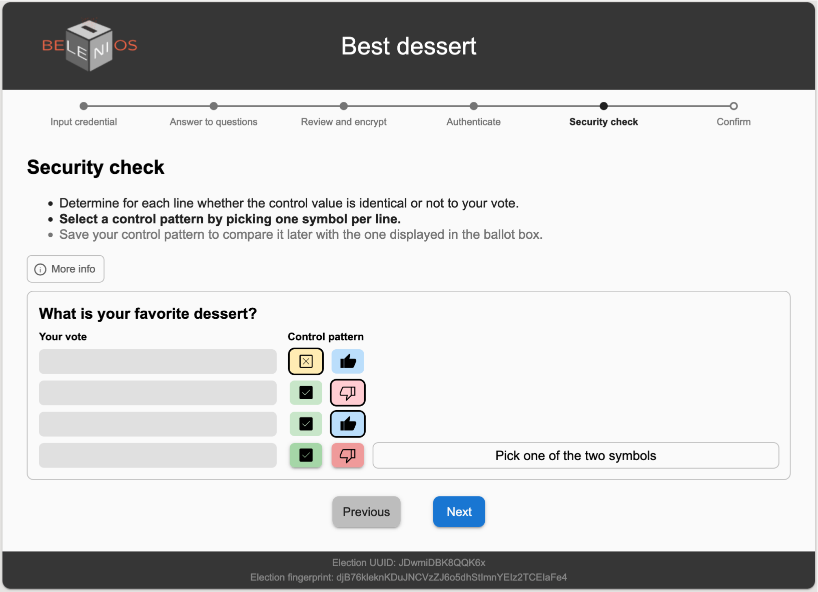

BELENIOS
Best dessert
Input credential
Answer to questions
Review and encrypt
Authenticate
Security check
Confirm
Security check
Determine for each line whether the control value is identical or not to your vote.
Select a control pattern by picking one symbol per line.
Save your control pattern to compare it later with the one displayed in the ballot box.
More info
What is your favorite dessert?
Your vote
Control value
Cheese cake
Tiramisu
Chocolate cake
Blank vote
Are the two symbols identical?
yes
no
Previous
Next
Election UUID: JDwmiDBK8QQK6x
Election fingerprint: djB76kleknKDuJNCVzZJ6o5dhStlmnYElz2TCElaFe4

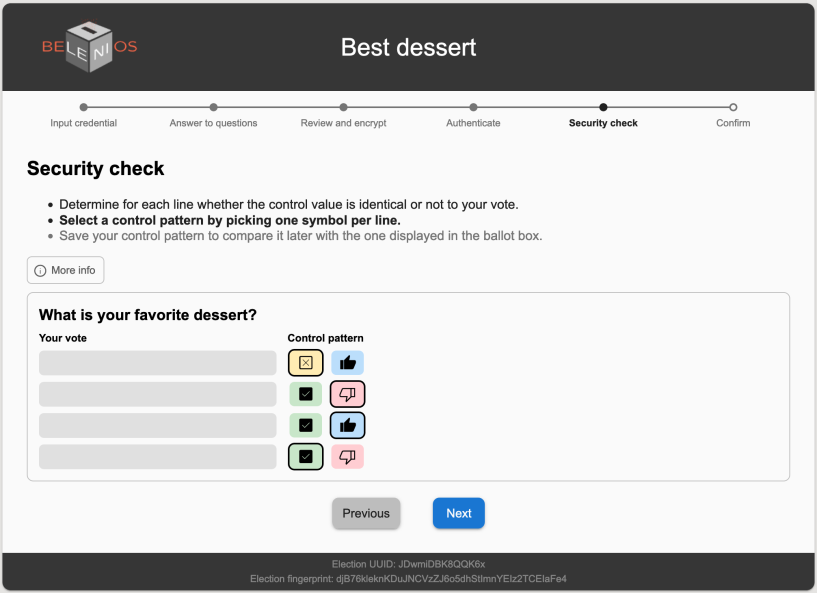

BELENIOS
Best dessert
Input credential
Answer to questions
Review and encrypt
Authenticate
Security check
Confirm
Security check
Determine for each line whether the control value is identical or not to your vote.
Select a control pattern by picking one symbol per line.
Save your control pattern to compare it later with the one displayed in the ballot box.
More info
What is your favorite dessert?
Your vote
Control value
Cheese cake
Tiramisu
Chocolate cake
Blank vote
Previous
Next
Election UUID: JDwmiDBK8QQK6x
Election fingerprint: djB76kleknKDuJNCVzZJ6o5dhStlmnYElz2TCElaFe4

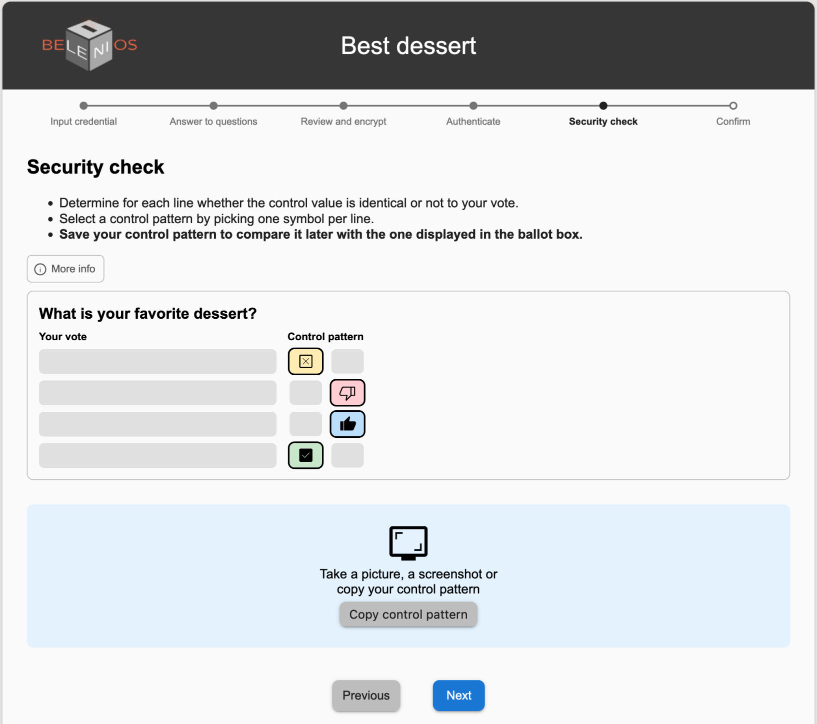

BELENIOS
Best dessert
Input credential
Answer to questions
Review and encrypt
Authenticate
Security check
Confirm
Security check
Determine for each line whether the control value is identical or not to your vote.
Select a control pattern by picking one symbol per line.
Save your control pattern to compare it later with the one displayed in the ballot box.
More info
What is your favorite dessert?
Your vote
Control pattern
Pick one of the two symbols
Previous
Next
Election UUID: JDwmiDBK8QQK6x
Election fingerprint: djB76kleknKDuJNCVzZJ6o5dhStlmnYElz2TCElaFe4


Best dessert
Input credential
Answer to questions
Review and encrypt
Authenticate
Security check
Confirm
Security check
Determine for each line whether the control value is identical or not to your vote.
Select a control pattern by picking one symbol per line.
Save your control pattern to compare it later with the one displayed in the ballot box.
More info
What is your favorite dessert?
Your vote
Control pattern
Pick one of the two symbols
Previous
Next
Election UUID: JDwmiDBK8QQK6x
Election fingerprint: djB76kleknKDuJNCVzZJ6o5dhStlmnYElz2TCElaFe4


BELENIOS
Best dessert
Input credential
Answer to questions
Review and encrypt
Authenticate
Security check
Confirm
Security check
Determine for each line whether the control value is identical or not to your vote.
Select a control pattern by picking one symbol per line.
Save your control pattern to compare it later with the one displayed in the ballot box.
More info
What is your favorite dessert?
Your vote
Control pattern
Pick one of the two symbols
Previous
Next
Election UUID: JDwmiDBK8QQK6x
Election fingerprint: djB76kleknKDuJNCVzZJ6o5dhStlmnYElz2TCElaFe4


BELENIOS
Best dessert
Input credential
Answer to questions
Review and encrypt
Authenticate
Security check
Confirm
Security check
• Determine for each line whether the control value is identical or not to your vote.
• Select a control pattern by picking one symbol per line.
• Save your control pattern to compare it later with the one displayed in the ballot box.
More info
What is your favorite dessert?
Your vote
Control pattern
Pick one of the two symbols
Previous
Next
Election UUID: JDwmiDBK8QQK6x
Election fingerprint: djB76kleknKDuJNCVzZJ6o5dhStlmnYElz2TCElaFe4


BELENIOS
Best dessert
Input credential
Answer to questions
Review and encrypt
Authenticate
Security check
Confirm
Security check
Determine for each line whether the control value is identical or not to your vote.
Select a control pattern by picking one symbol per line.
Save your control pattern to compare it later with the one displayed in the ballot box.
More info
What is your favorite dessert?
Your vote
Control pattern
Previous
Next
Election UUID: JDwmiDBK8QQK6x
Election fingerprint: djB76kleknKDuJNCVzZJ6o5dhStlmnYElz2TCElaFe4


BELENIOS
Best dessert
Input credential
Answer to questions
Review and encrypt
Authenticate
Security check
Confirm
Security check
Determine for each line whether the control value is identical or not to your vote.
Select a control pattern by picking one symbol per line.
Save your control pattern to compare it later with the one displayed in the ballot box.
More info
What is your favorite dessert?
Your vote
Control pattern
Take a picture, a screenshot or
copy your control pattern
Copy control pattern
Previous
Next

BELENIOS

Best dessert

Input credential — Answer to questions — Review and encrypt — Authenticate — Security check — **Confirm**

Thank you for voting!

Next steps

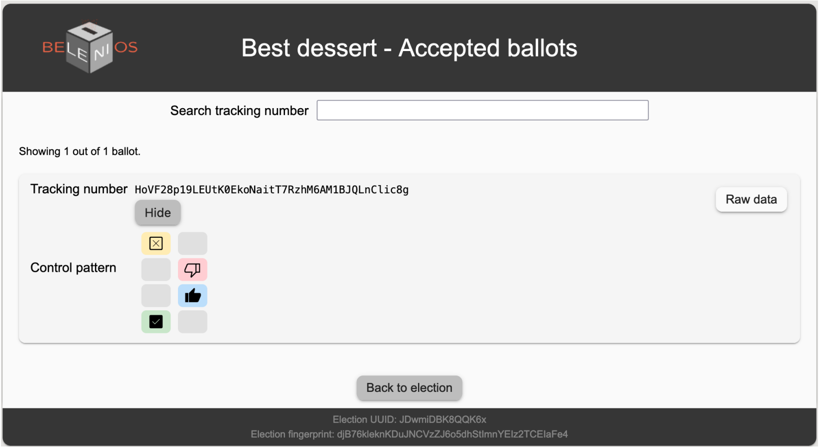
- Follow the link in your confirmation email
- Verify your control pattern
- If your ballot is missing or the control pattern does not match, contact the administrator: cortier

About your ballot

Voter	veronique.cortier@loria.fr
Tracking number	`HoVF28p19LEUtK0EkoNaitT7RzhM6AM1BJQLnClic8g`
Status	accepted
Revote	yes
Email sent	yes

Go back to election

Powered by Belenios 2.2 (2.1-300-g5e3113f8). Get the source code. Privacy policy. Administer this election. Advanced booth.


BELENIOS
Best dessert - Accepted ballots
Search tracking number
Showing 1 out of 1 ballot.
Tracking number HoVF28p19LEUtK0EkoNaitT7RzhM6AM1BJQLnClic8g
Hide
Raw data
Control pattern
Back to election
Election UUID: JDwmiDBK8QQK6x
Election fingerprint: djB76kleknKDuJNCVzZJ6o5dhStlmnYElz2TCElaFe4

How to analyse BeleniosCaI ?

Formal analysis of e-voting systems

Why a formal analysis of an e-voting system?

Formal analysis of e-voting systems

Why a formal analysis of an e-voting system?

$\longrightarrow$ Because formal methods can find attacks before implementations
$\longrightarrow$ Now a current practice for many protocols (TLS, 5G, ...)

Formal analysis of e-voting systems

Why a formal analysis of an e-voting system?

$\longrightarrow$ Because formal methods can find attacks before implementations
$\longrightarrow$ Now a current practice for many protocols (TLS, 5G, ...)

$\rightarrow$ Legal requirements in Switzerland to provide **symbolic and cryptographic proofs** of e-voting protocols.

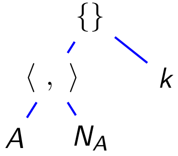
2.14 Proofs of compliance with the cryptographic protocol requirements

2.14.1 A symbolic and a cryptographic proof of compliance must demonstrate that the cryptographic protocol meets the requirements in Numbers 2.1–2.12.

2.14.2 The proofs of compliance must directly refer to the protocol description that forms the basis for system development.

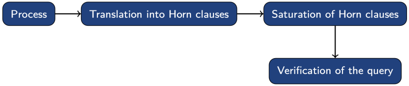
2.14.3 The proofs of compliance relating to basic cryptographic components may be provided according to generally accepted security assumptions and constructions (e.g. «random oracle model», «decisional Diffie-Hellman assumption», «Fiat-Shamir heuristic»).

Two main models for security

	Formal approach	Computational approach
Messages		0101000101110101 1101010110101010 0011101011101101 bitstrings
Encryption	terms	algorithm
Adversary	idealized	any polynomial algorithm
Guarantees	some attacks missed	stronger
Proof	often automatic	mostly by hand difficult for complex protocols

Good tools in practice for formal / symbolic models

ProVerif



- fully automatic
- axioms, lemmas, and restrictions [S&P'22]
- framework for verifiability [CSF'23]
- many voting protocols
  - Swiss Chancellery requirements: Swiss Post, CHVote
  - Helios, Belenios, ...

Tamarin

- semi automatic
- exclusive or
- voting protocols (Belenios, Selene, ...)

Two major issues for analyzing BeleniosCal

1. Addition modulo 2

$$\begin{aligned} 0+0 &= 0 \\ 0+1 &= 1 \\ 1+0 &= 1 \\ 1+1 &= 0 \end{aligned}$$

$\rightarrow$ state explosion
$\rightarrow$ non termination

Two major issues for analyzing BeleniosCaI

1. Addition modulo 2

$$\begin{aligned} 0 + 0 &= 0 \\ 0 + 1 &= 1 \\ 1 + 0 &= 1 \\ 1 + 1 &= 0 \end{aligned}$$

   $\rightarrow$ state explosion

   $\rightarrow$ non termination

2. Probabilistic model
   - Alice checks either a or b at random
   - Intuition: An attacker may modify k votes without been detected with proba $(\frac{1}{2})^k$.

Model for addition modulo - trace properties

Follows the approach introduced in CCS'22

Trace properties (verifiability)

Introduction of two predicates $\texttt{isSum}(x, a, b)$ and $\texttt{isNotSum}(x, a, b)$

$$\begin{array}{llll} \texttt{isSum}(x, a, b), & \texttt{isSum}(x, a, b') & \Rightarrow & b = b' \\ \texttt{isSum}(x, a, b), & \texttt{isNotSum}(x, a, b') & \Rightarrow & b \neq b' \end{array}$$

- sound over-approximation
- another arithmetic operator could be used

Model for addition modulo - equivalence properties

Vote secrecy

$$Alice(0) \mid Bob(1) \approx Alice(1) \mid Bob(0)$$

- over-approximation would be unsound

  $\rightarrow$ Exactly the same tuples (x, a, b) are created on the left and on the right.

  $$\texttt{(Lemma)} \quad \texttt{isSum}(x, a, b) \in fst(tr_b) \Leftrightarrow \texttt{isSum}(x, a, b) \in snd(tr_b)$$

  $\rightarrow$ allow to conclude by hand

Model for addition modulo - equivalence properties

Vote secrecy

$$Alice(0) \mid Bob(1) \approx Alice(1) \mid Bob(0)$$

- over-approximation would be unsound

  → Exactly the same tuples (x, a, b) are created on the left and on the right.

  $$\text{(Lemma)} \quad \mathtt{isSum}(x, a, b) \in fst(tr_b) \Leftrightarrow \mathtt{isSum}(x, a, b) \in snd(tr_b)$$

  → allow to conclude by hand

- privacy relies on the following property:
  for all x_1, x_2, a_1, a_2, there exist b_1, b_2, b_3, b_4 such that

  $$x_1 = a_1 + b_1 = a_2 + b_2$$
  $$x_2 = a_2 + b_3 = a_1 + b_4$$

  → Encoded in the privacy ProVerif query

Model for probabilities

- to be done! for a real model with probabilities
- for the moment, for verifiability,
  the model assumes that Alice asks for opening both ciphertexts.

To conclude

Many challenges remain! (which is fun 😀)

Strong demand for Cast as Intended

- many systems are currently proposed
- usability (two devices? computation in the head?)
- trust assumptions?
- vote secrecy

Better formal verification

- decision procedures for larger equational theory classes
- further improve tools
- account for probabilities