Bern University
of Applied Sciences

Verifiable Internet Elections in Switzerland

Rolf Haenni

March 22th, 2018

Outline

- Introduction
- E-Voting Research at BFH
- Swiss Context
- Verifiable Elections
- CHVote Voting Protocol in Geneva
- Conclusion

Introduction

It is enough that the people know there was an election. The people who cast the votes decide nothing, the people who count the votes decide everything.

Josef Stalin

If we are to bring computerization into our electoral processes, then we must do it in such a way as to [...] prevent concentration of power into the hands of the few who control the process.

Josh Benaloh, *Verifiable Secret-Ballot Elections*
PhD Thesis, Yale University, 1987

Bern University
of Applied Sciences

E-Voting Research at BFH

E-Voting Research Group

- Founded in 2007 by Eric Dubuis and Rolf Haenni
- Authors of >20 peer-reviewed research papers
- PC members of E-VOTE, VoteID, EVoteID, Voting, CeDEM conferences
- Conference chairs of VoteID'15 in Bern
- Swiss E-Voting Workshop 2009, 2010, 2012, 2014
- Supervision of multiple PhD theses

https://e-voting.bfh.ch

Research Projects

- FIDIS: Future of Identity in Information Society (2006–2009)
- SwissVote: Secure E-Voting in Switzerland (2009–2012)
- VIVO: Verifiable Internet Voting (2012–2015)
- UniVote: Secure E-Voting in Switzerland (2013–2017)
- UniBoard: Specification and Development of a Public Bulletin Board for Online Elections (2014–2017)
- CHVote: Cryptographic System Specification of the Geneva E-Voting System (since 2016)
- Verification Software for the Swiss Post E-Voting Solution (since 2017)

Swiss Context

Direct Democracy in Switzerland

- Up to four election days per year
  - Elections
  - Mandatory referendums
  - Optional referendums (>50k signatures)
  - Popular initiatives (>100k signatures)
- Four different political levels
  - Federal
  - Cantonal
  - Municipal
  - Pastoral
- Up to 10 different election topics per election day
- Voters are not necessarily eligible on all four levels, e.g. citizens living abroad can only vote on federal/cantonal level

E-Voting Tradition in Switzerland

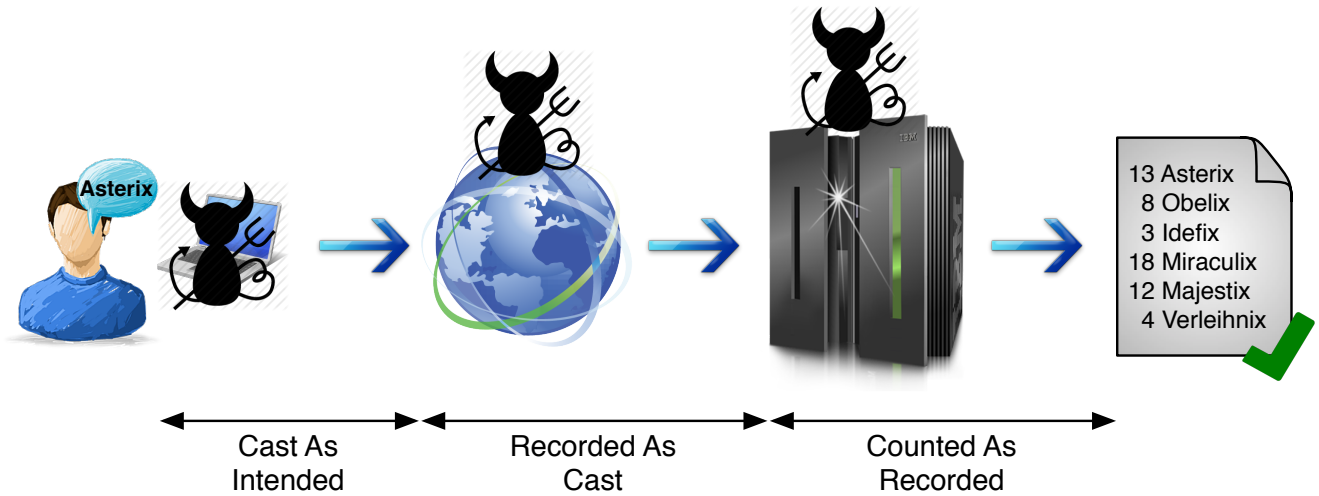
- Classical voting channels
  - Polling station
  - Landsgemeinde
  - Postal voting (since 1994, approx. 90%)
- Non-verifiable "blackbox" e-voting systems (1st generation)
  - Canton of Geneva (since 2003)
  - Canton of Zürich (Unisys, 2004–2015)
  - Canton of Neuchâtel (Scytl, 2005–2015)
- Collaborations with 10 other cantons (since 2009)
- Target audience: Swiss citizens living abroad

Landsgemeinde

Landsgemeinde Glarus, Switzerland (blick.ch)

Legal Ordinance on Electronic Voting

- Enhanced security requirements
  - End-to-end encryption
  - End-to-end verifiability (cast-as-intended, recorded-as-cast, counted-as-recorded)
  - Distribution of trust (shared decryption key, mix-net)
- Effective since December 2013

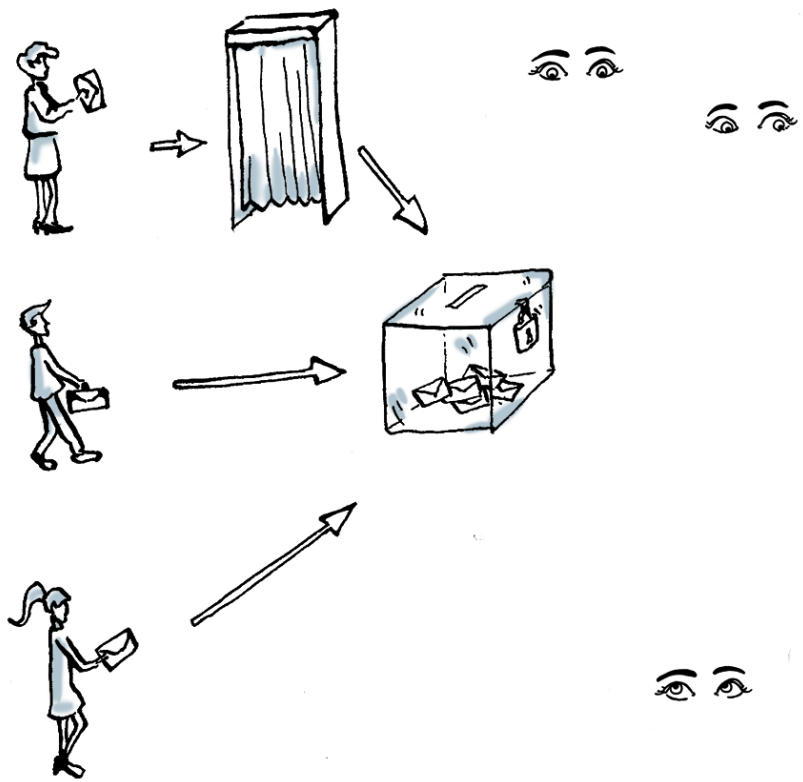


Stepwise Introduction

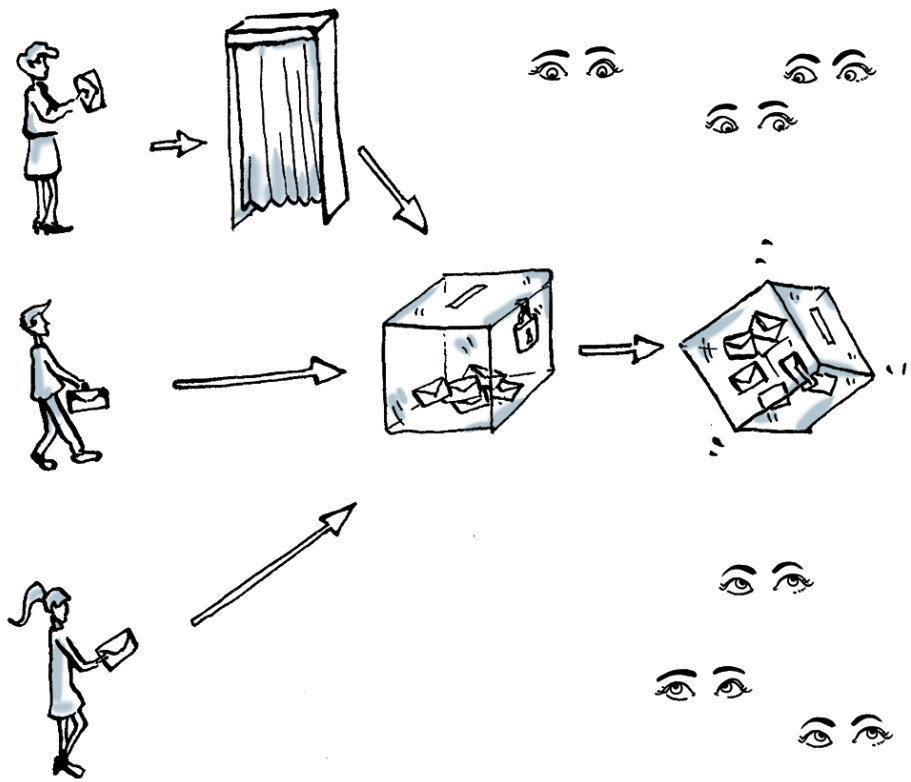
- Current systems
  - max. 10/30% of federal/cantonal electorate
- Two-step expansion
  - Step 1: max. 30/50% of federal/cantonal electorate
  - Step 2: 100% electorate
- There are two competing 2nd generation projects
- Swiss Post (Scytl):
  - Step 1 reached in 2017
  - Step 2 planned in 2019
- Canton of Geneva (CHVote)
  - Step 2 planned in 2019

Verifiable Elections

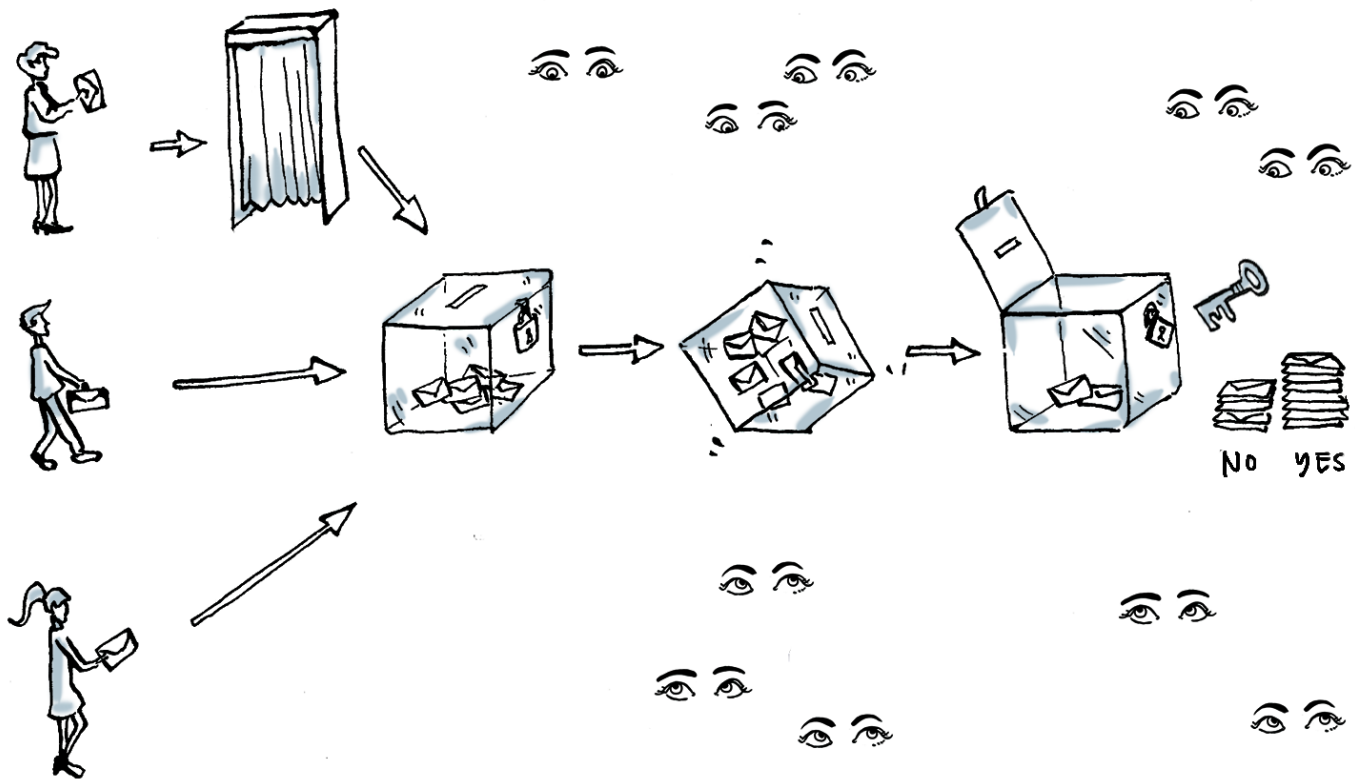
Traditional Paper-Based Voting



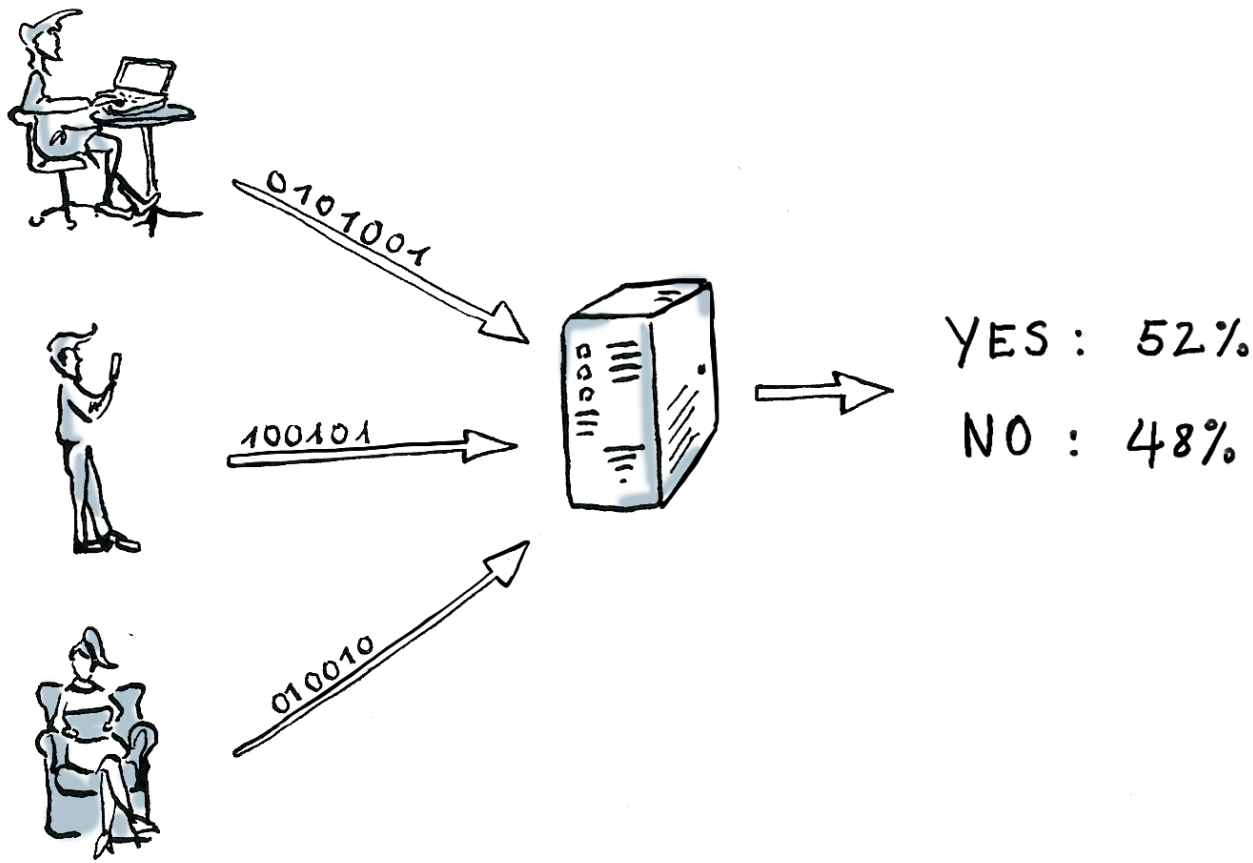
Traditional Paper-Based Voting



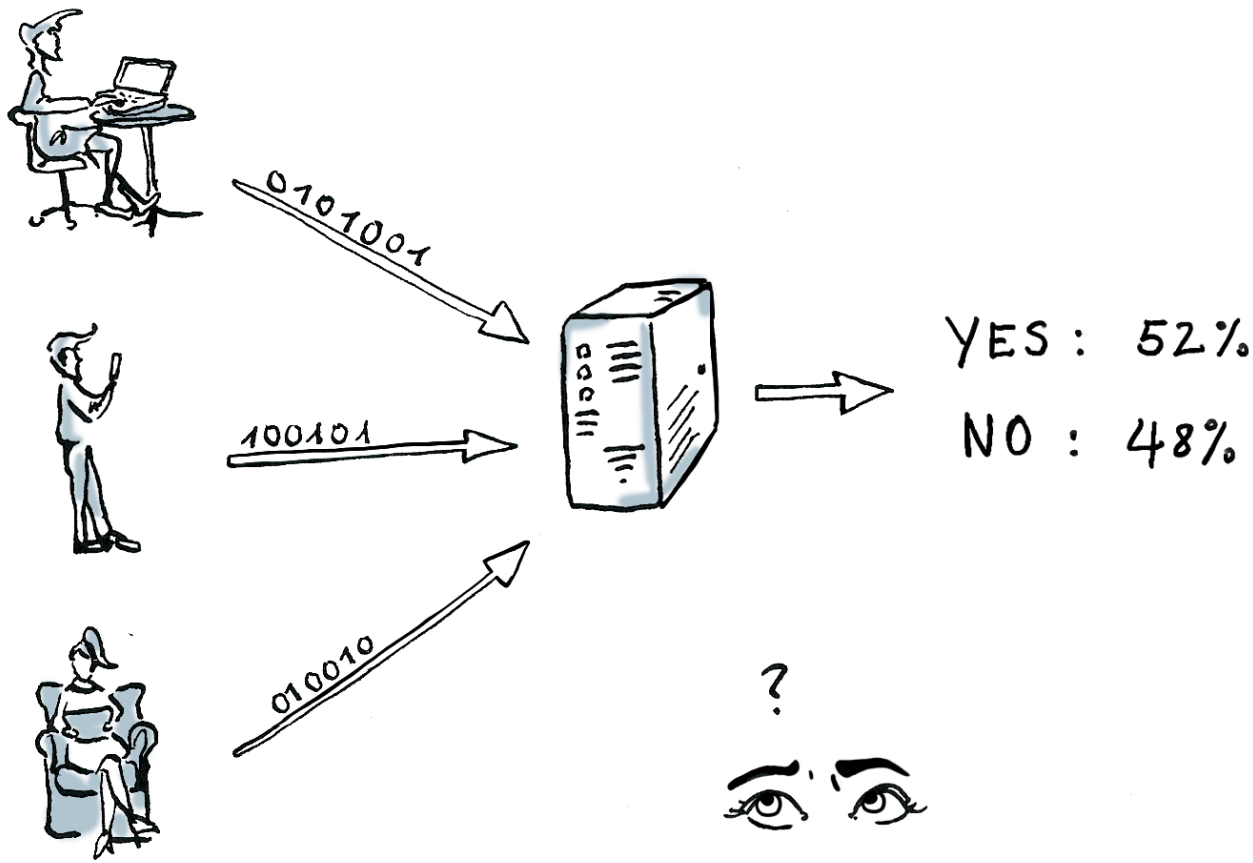
Traditional Paper-Based Voting



Remote Electronic Voting (Blackbox)



Remote Electronic Voting (Blackbox)



Verifiability

The introduction of verifiability is central to the new security requirements.

3rd Vote Electronique Report
Swiss Federal Council, 2013

Individual Verifiability

Voters must be able to ascertain whether their vote has been manipulated or intercepted on the user platform or during transmission. [. . .] Voters must receive proof that the server system has registered the vote as it was entered by the voter on the user platform.

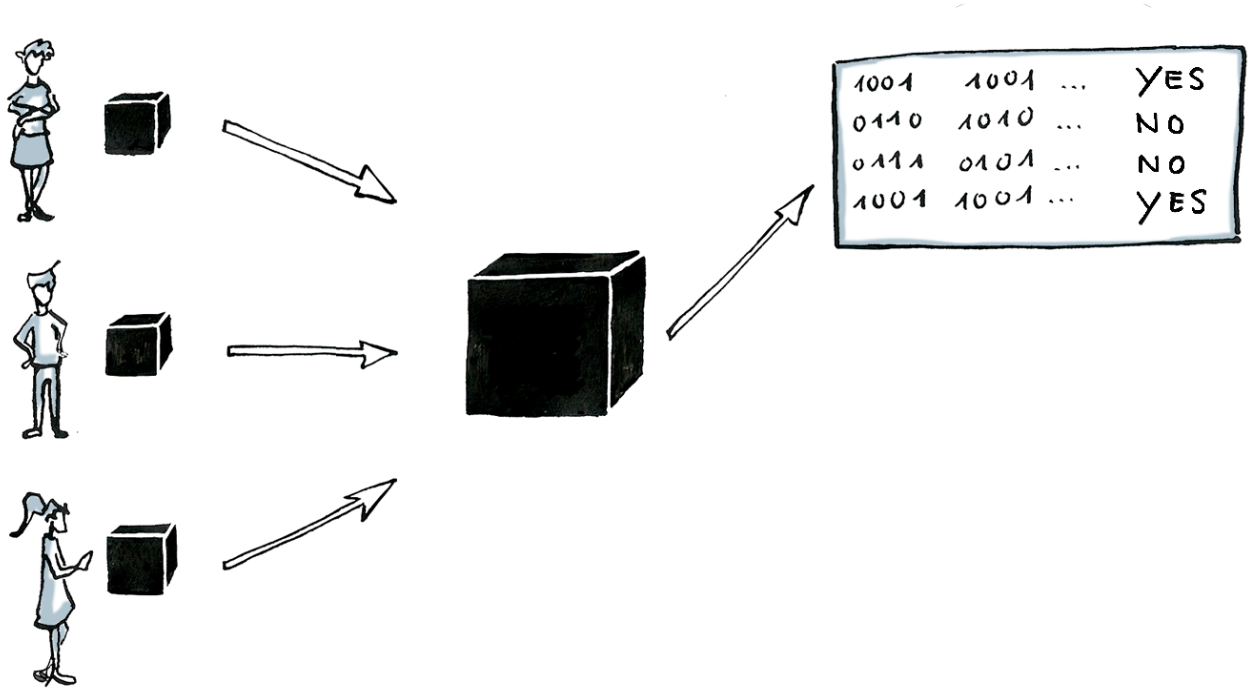
Federal Chancellery Ordinance on Electronic Voting
VEleS, Art.4, 2013

Universal Verifiability

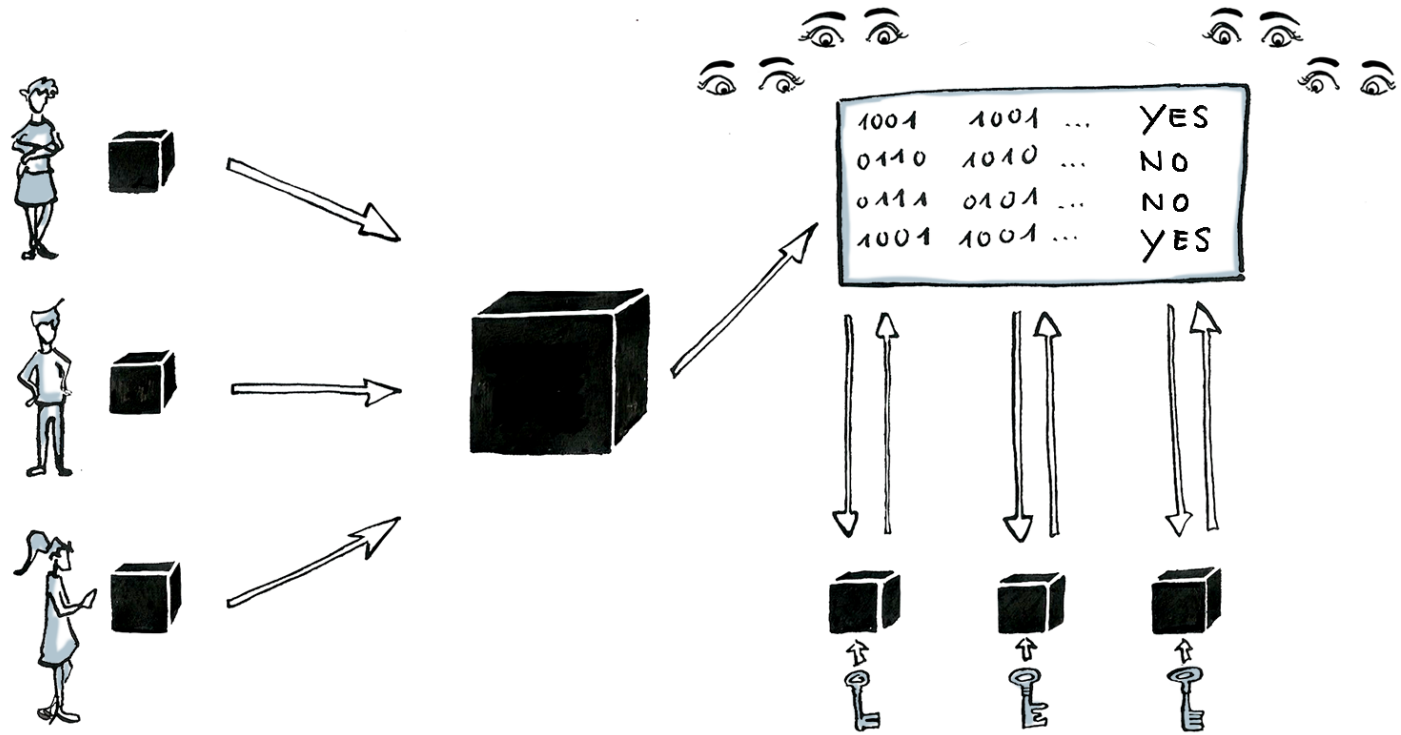
Auditors receive proof that the result has been ascertained correctly. They must evaluate the proof in a observable procedure. To do this, they must use technical aids that are independent of and isolated from the rest of the system.

Federal Chancellery Ordinance on Electronic Voting
VEleS, Art.5, 2013

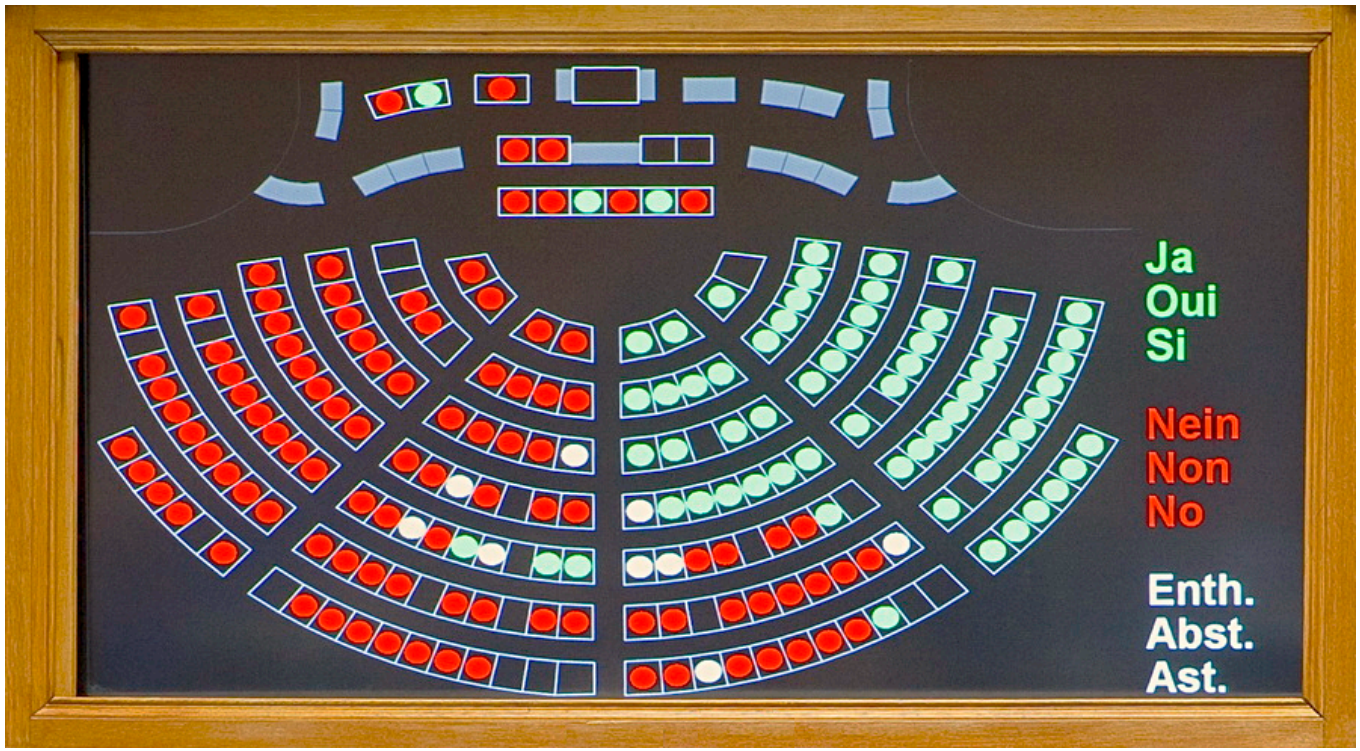
Verifiable Remote Electronic Voting



Verifiable Remote Electronic Voting



Bulletin Board

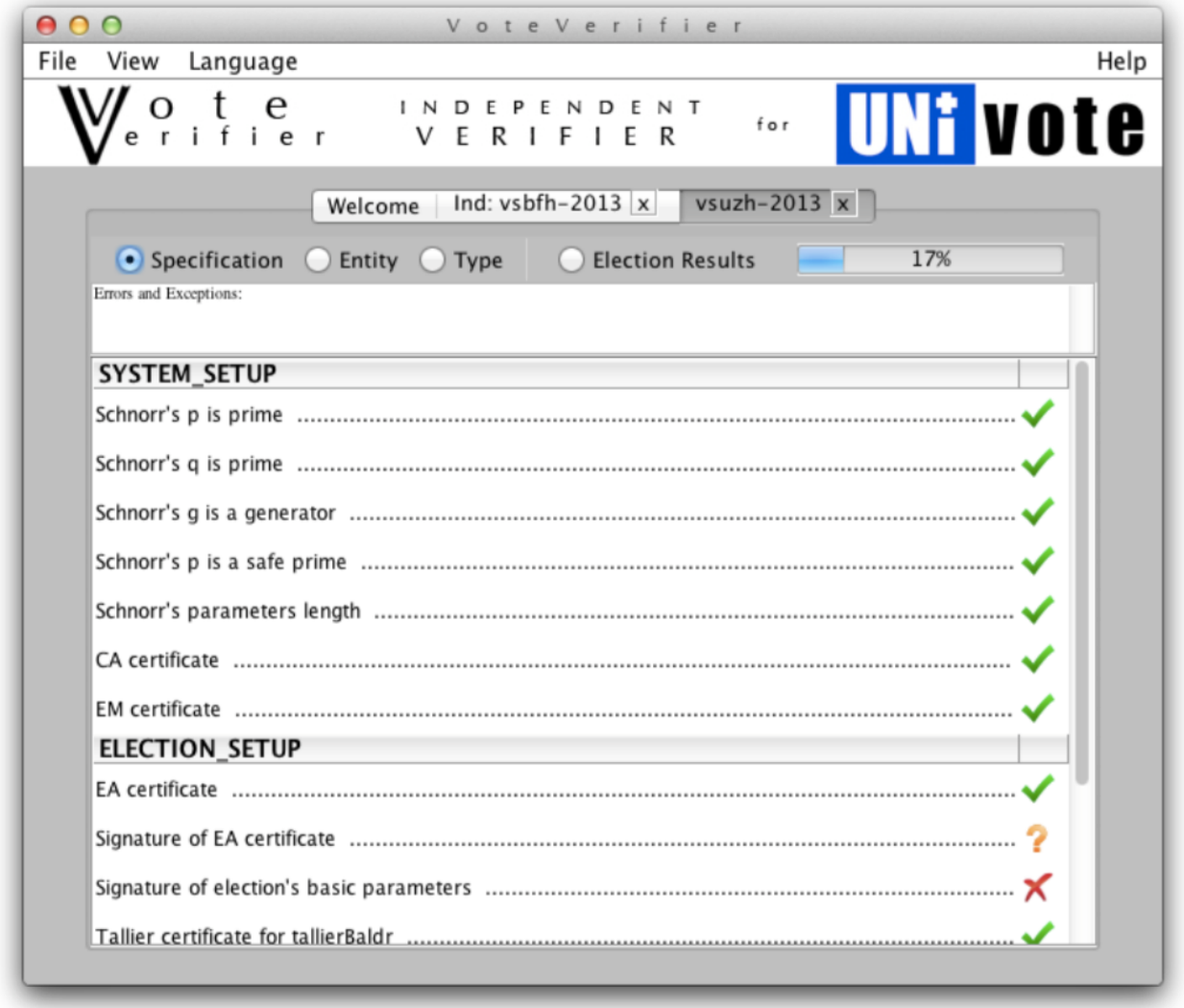


Voting panel, Swiss National Council, Bern, Switzerland (srf.ch)

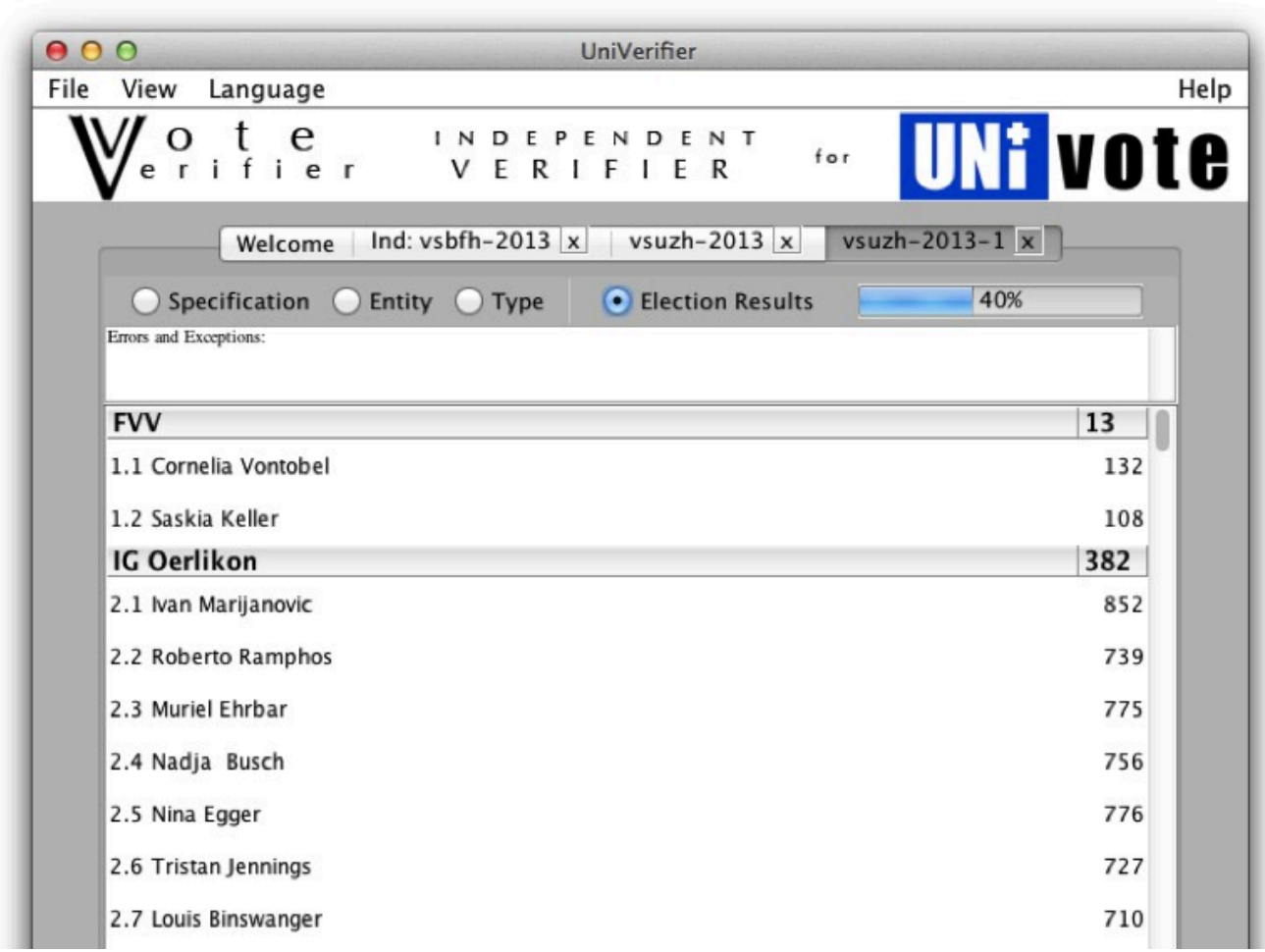
Bulletin Board

List of eligible voters, Erbil, Iraq (nzz.ch)

Verification Software



Verification Software



Bern University
of Applied Sciences

CHVote Voting Protocol in Geneva

Desirable Security Properties

- Privacy
  - Vote secrecy (everlasting?)
  - Participation secrecy
  - Receipt-freeness
- Correctness
  - Votes from ineligible voters are not counted
  - Eligible voters can vote at most once
  - All valid from eligible voters votes are counted
- E2E Verifiability
  - Individual (cast-as-intended, recorded-as-cast)
  - Universal (counted-as-recorded)
- Fairness: nobody learns partial election results during election
- Coercion-Resistance

CHVote Project in Geneva

- Project goals
  - New implementation from scratch
  - Reach second expansion stage in one step (100% electorate)
  - Developed, hosted, operated entirely by the State of Geneva
- Strategy
  - Collaboration with academia
  - State-of-the-art technologies
  - Maximal transparency
  - High-quality open documentation
  - Open-source license (Affero GPL)
  - Invitation to public code reviewing

https://eprint.iacr.org/2017/325.pdf

Cast-as-Intended Verification

- Prior to an election, a code sheet with different verification codes for each voting option is generated for every voter
- Code sheets are sent to voters by postal mail

Code Sheet Nr.291

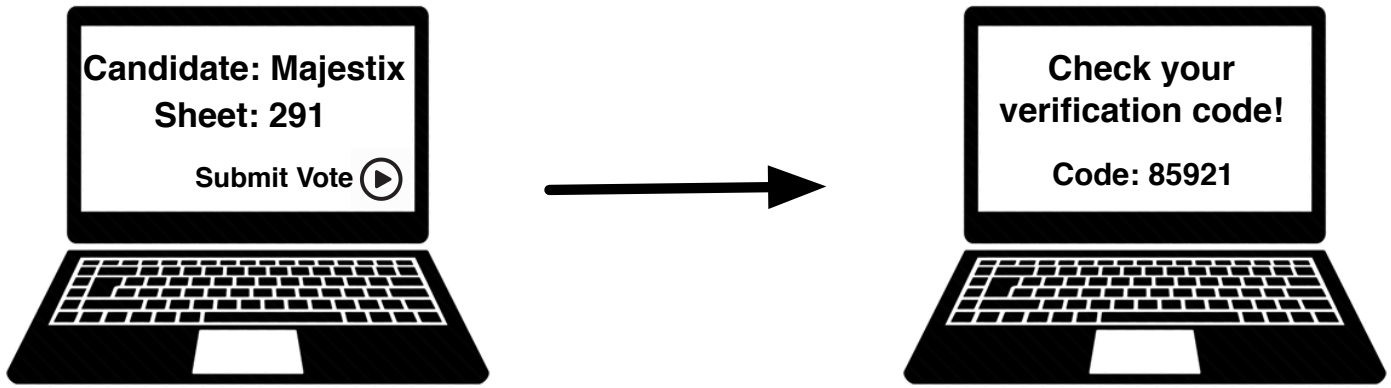
Candidates	Codes
Asterix	74494
Obelix	84443
Idefix	91123
Miraculix	63382
Majestix	85921
Verleihnix	79174

Code Sheet Nr.321

Candidates	Codes
Asterix	21344
Obelix	29173
Idefix	91123
Miraculix	72282
Majestix	18194
Verleihnix	53382

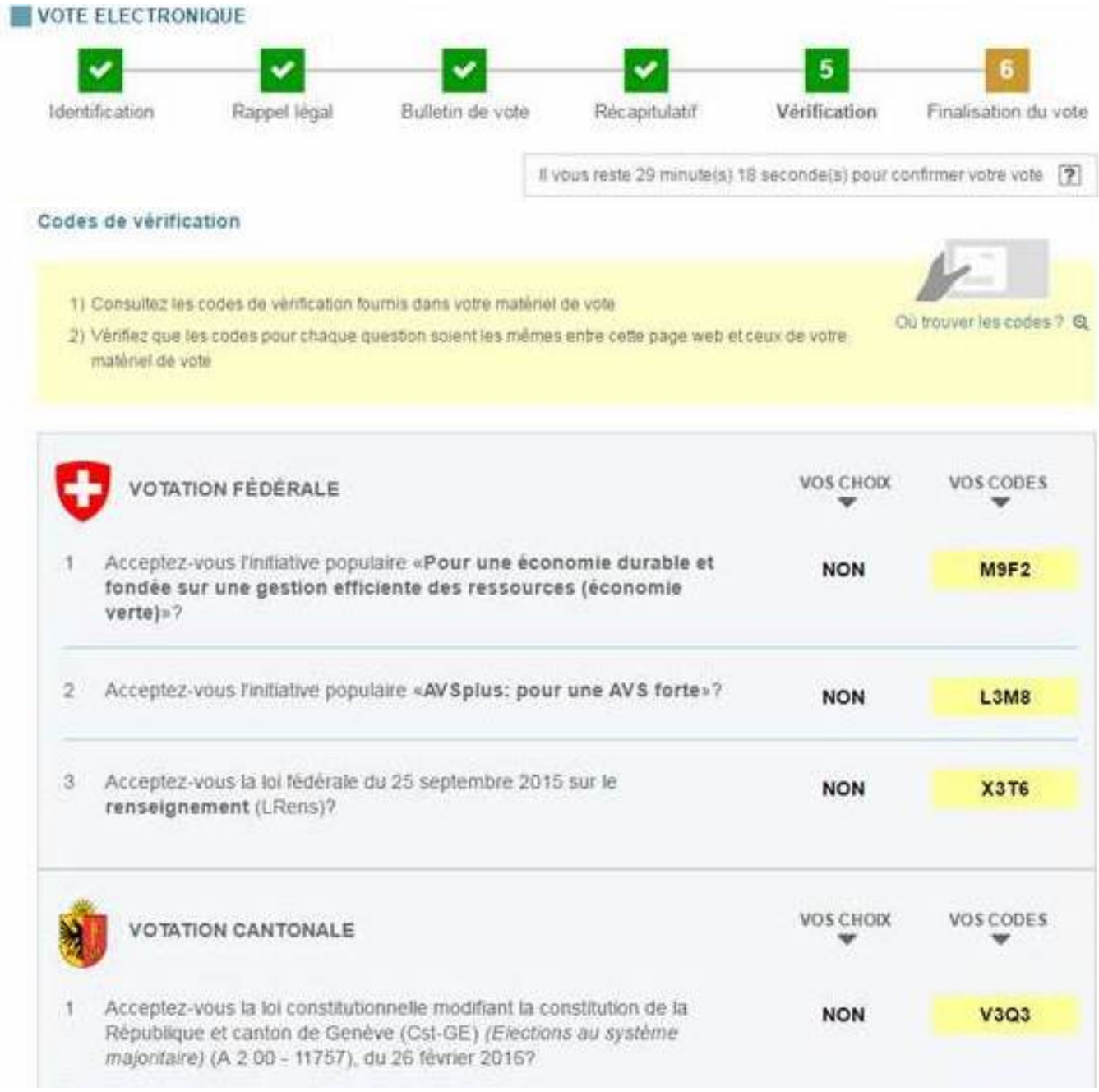
Cast-as-Intended Verification

- After submitting a vote, corresponding verification codes are displayed



- Matching codes imply that the vote has been cast as intended
- Otherwise, voters are instructed to vote by postal mail

Liste de codes pour la carte n° 5874-8863-1400-8743			
Votation fédérale			
Question 1 Acceptez-vous l'arrêté fédéral du 20 juin 2013 portant règlement du financement et de l'aménagement de l'infrastructure ferroviaire (Contre-projet direct à l'initiative populaire "Pour les transports publics", qui a été retirée) ?	Oui A2B4	Non J5B9	Blanc Z8H5
Question 2 Acceptez-vous l'initiative populaire "Financer l'avortement est une affaire privée - Alléger l'assurance-maladie en radiant les coûts de l'interruption de grossesse de l'assurance de base" ?	Oui P8H3	Non X2A7	Blanc Q3L7
Votation cantonale			
Question 1 Acceptez-vous l'initiative 143 «Pour une véritable politique d'accueil de la Petite enfance» ?	Oui U6T4	Non P3D6	Blanc S6C2
Question 2 Acceptez-vous la loi constitutionnelle modifiant la constitution de la République et canton de Genève (Contreprojet à l'IN 143) (A 2 00 – 10895), du 15 décembre 2011 ?	Oui N4F2	Non M2A3	Blanc Q9L5
Question 3 **Question subsidiaire**: Si l'initiative (IN 143 «Pour une véritable politique d'accueil de la Petite enfance») et le contreprojet sont acceptés, lequel des deux a-t-il votre préférence ? Initiative 143 ? Contreprojet ?	IN K9W9	CP T3S6	Blanc Y2V4


VOTE ELECTRONIQUE
Identification
Rappel légal
Bulletin de vote
Récapitulatif
5
Vérification
6
Finalisation du vote
Il vous reste 29 minute(s) 18 seconde(s) pour confirmer votre vote
Codes de vérification
1) Consultez les codes de vérification fournis dans votre matériel de vote
2) Vérifiez que les codes pour chaque question soient les mêmes entre cette page web et ceux de votre matériel de vote
Où trouver les codes ?
VOTATION FÉDÉRALE
VOS CHOIX
VOS CODES
1 Acceptez-vous l'initiative populaire «Pour une économie durable et fondée sur une gestion efficiente des ressources (économie verte)»? NON M9F2
2 Acceptez-vous l'initiative populaire «AVSplus: pour une AVS forte»? NON L3M8
3 Acceptez-vous la loi fédérale du 25 septembre 2015 sur le renseignement (LRens)? NON X3T6
VOTATION CANTONALE
VOS CHOIX
VOS CODES
1 Acceptez-vous la loi constitutionnelle modifiant la constitution de la République et canton de Genève (Cst-GE) (Elections au système majoritaire) (A 2 00 - 11757), du 26 février 2016? NON V3Q3

Conclusion

Conclusion

- Verifiability is central to making e-voting secure
- Various cryptographic protocols exist in scientific literature to achieve major security properties
- The process of introducing e-voting in Switzerland is slow, but on the right track (legal ordinance VEleS)
- Challenges and open problems
  - Complexity of cryptographic protocols
  - Cryptography in web browser (JavaScript)
  - Vote secrecy on insecure platform
  - Vote buying and coercion
  - Everlasting privacy
  - Usability and "voter education"