Bern University
of Applied Sciences

One E-Citizen, One E-Vote ?

Rolf Haenni

ISSS Security Talk, Zürich
November 26th, 2019

Outline

- Introduction
- Swiss E-Voting Experience
- Cryptographic Voting Protocols
- Cast-As-Intended Verifiability
- Conclusion

Introduction

Neue Zürcher Zeitung

Gegner wollen E-Voting mit einer Volksinitiative verbieten

Politiker, Juristen, IT-Experten und Hacker sehen die Demokratie in Gefahr, wenn die Schweiz elektronische Abstimmungen zulässt. Solche E-Wahlsysteme seien einfach zu manipulieren und die Gefahr von Wahlfälschungen gross.

E-Voting: Wie sicher sind die Schweizer Lösungen?

Wie sicher sind die Schweizer E-Voting-Systeme? Diese Frage beschäftigt nicht nur die Politik, sondern auch die IT-Security-Szene. So widmete sich auch ein Themenblock am diesjährigen SwissCyberStorm in Luzern der elektronischen Stimmabgabe.

Tages-Anzeiger

Front Zürich Schweiz International Wirtschaft Börse Sport Kultur Reisen Wissen Auto Blogs Panorama Mehr ▾

SonntagsZeitung // ePaper Leserangebote Leserreisen Leserbriefe Monatsquiz Abonnieren

E-Voting: Unsicheres System und Maulkorb für Kritiker

Befürworter elektronischer Abstimmungen wie FDP-Nationalrat Marcel Dobler wollen die Technologie auf Teufel komm raus durchboxen.

Bundesrat schiebt E-Voting auf die lange Bank

Bis 2019 sollen alle Auslandschweizer elektronisch wählen können, fordert der CVP-Ständerat Filippo Lombardi. Der Bundesrat hält dieses Ziel jedoch für «unrealistisch».

Blick

Ihre Meinung · Zürich 5° · Suche · Anmelden

Home News Sport Politik Wirtschaft People Leben Digital Auto Virtual Reality Video Services

SIE SIND HIER: HOME > NEWS > POLITIK > WAHL-SYSTEM: DESHALB KANN E-VOTING DAS STIMMGEHEIMNIS GEFÄHRDEN

Datenschützer kritisiert Digital-Wahl

Gefährdet E-Voting das Stimmgeheimnis?

Bereits 2019 sollen zwei Drittel der Kantone digital abstimmen können. Aber wie soll das funktionieren und gefährdet E-Voting möglicherweise das Stimmgeheimnis?

Tages-Anzeiger

Was, wenn der Tresorraum der Schweizer Demokratie geknackt wird?

Hernani Marques fasst es nicht: Im Cyber-Krieg setzt die Schweiz auf E-Voting? Jetzt will er demonstrativ hacken.

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.

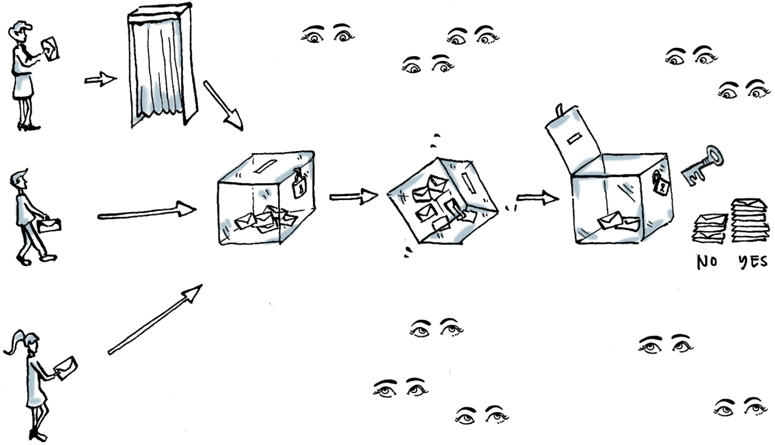
Josef Stalin

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

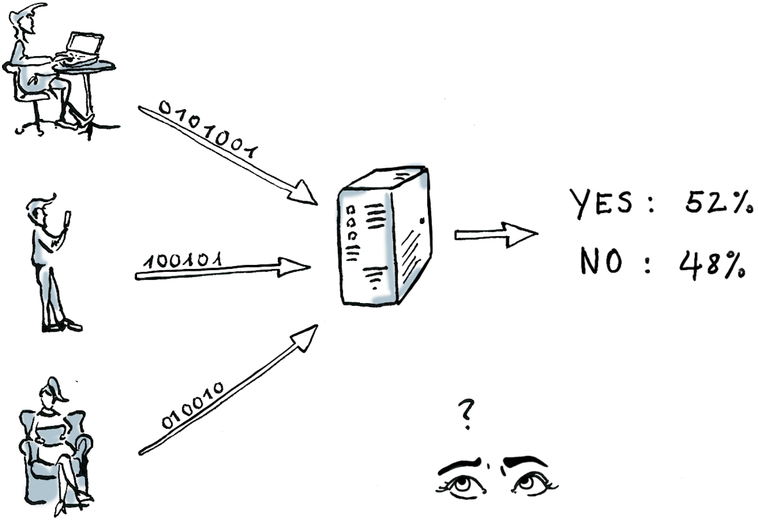
Josh Benaloh, *Verifiable Secret-Ballot Elections*
PhD Thesis, Yale University, 1987

Swiss E-Voting Experience

Traditional Paper-Based Voting



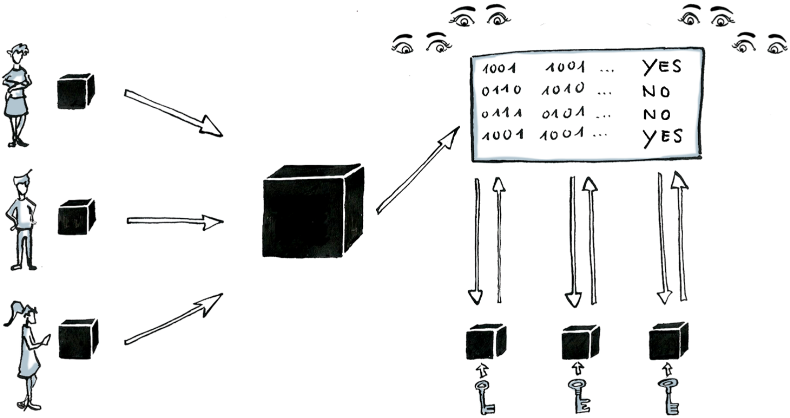
1st Generation Systems



1st Generation Systems

- Non-verifiable “blackbox” systems (1st generation)
  - Canton of Geneva (2003–2019)
  - Canton of Zürich (Unisys, 2004–2015)
  - Canton of Neuchâtel (Scytl, 2005–2015)
- Almost no security other than secured channels (TLS)
  - Fully trusted voting server
  - Fully trusted voting client
- Target audience: Swiss living abroad

2nd Generation Systems



2nd Generation Systems

- Legal Ordinance on Electronic Voting (VEleS)
  - Effective since December 2013
  - Enhanced security requirements (end-to-end encryption, end-to-end verifiability, distribution of trust, transparency)
- Relaunched project CHVote 2.0 (Geneva)
  - Collaboration with academia
  - Stopped in November 2018 for financial reasons
- New project by Swiss Post
  - Collaboration with Scytl (Barcelona, Spain)
  - Stopped in June 2019 by Federal Chancellery
- Target audience: All Swiss citizens

VEleS

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

3rd Vote Electronique Report
Swiss Federal Council, 2013

VEleS: 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.

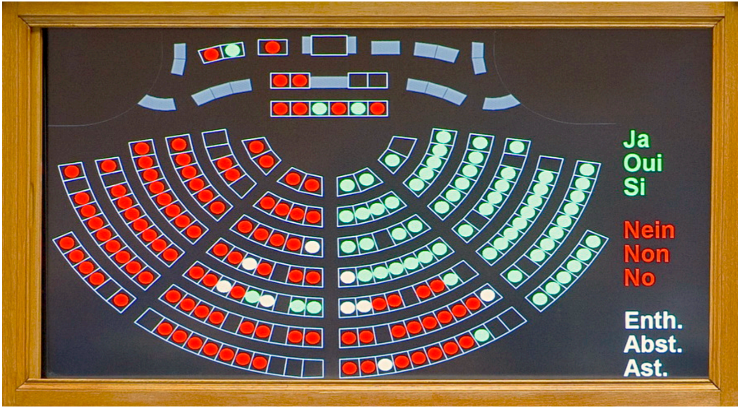
Federal Chancellery Ordinance on Electronic Voting
VEleS, Art.4, 2013

VEleS: 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

Bulletin Board



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

Cryptographic Voting Protocols

Cryptographic Voting Protocol

- A *cryptographic voting protocol* tries to solve the following multi-party-computation problem:
  - Parties $V_1, \ldots, V_n$ with private inputs $v_i \in \{0, 1\}$
  - Common output $s = f(v_1, \ldots, v_n) = \sum_{i=1}^{n} v_i$
- Formal security definition based on ideal/real-model paradigm
  - Fairness: Parties select their private inputs independently
  - Correctness: The protocol outputs the correct value s
  - Privacy: Nobody learns anything more than s
- General MPC protocols are not efficient enough for real-world elections (when n is large)

Cryptographic Voting Protocol

- 30 years of academic research focused on designing specialized cryptographic voting protocols
  - Voters $V_1, \ldots, V_n$
  - Election administrator AD
  - Independent authorities EA_j (of which some are honest)
  - Bulletin board BB
- Attack Model: Any coalition of parties may try to attack the protocol (except too many authorities together)
- Solution: The cryptographic voting protocol outputs a proof that the announced result is correct (= no attack took place)

Approach 1: Homomorphic Tallying

- Public-key encryption scheme
  - Key generation: $(pk, sk) \leftarrow KeyGen()$
  - Encryption: $e \leftarrow Enc_{pk}(m)$
  - Decryption $m \leftarrow Dec_{sk}(e)$

- Additively homomorphic encryption scheme:

$$Enc_{pk}(m_1) * Enc_{pk}(m_2) = Enc_{pk}(m_1 + m_2),$$

  and therefore:

$$\prod_{i=1}^{n} Enc_{pk}(m_i) = Enc_{pk}(\sum_{i=1}^{n} m_i)$$

- Examples: Exponential ElGamal, Paillier

Approach 1: Homomorphic Tallying

- Step 1: Every participating voter ...
  - selects $v_i \in \{0, 1\}$
  - computes $e_i = Enc_{pk}(v_i)$
  - submits e_i to bulletin board
- Step 2: The authority ...
  - retrieves $e_1, \ldots, e_n$ from bulletin board
  - computes $e = \prod_{i=1}^{n} e_i$
  - decrypts e into $s = Dec_{sk}(e)$ using sk
  - publishes s on the bulletin board
- Bulletin board contents at the end of protocol:

$e_1, \ldots, e_n$
s

Non-Interactive Cryptographic Proofs

- Attack 1: Dishonest voters selects invalid $v_i \notin \{0, 1\}$
- Attack 2: Dishonest authority publishes incorrect $s \neq Dec_{sk}(e)$
- These attacks can be prevented by publishing *non-interactive zero-knowledge proofs* (NIZKP) along with e_i and s

$$\pi_{e_i} = NIZKP\,[(r) : e_i = Enc_{pk}(0, r) \vee e_i = Enc_{pk}(1, r)]$$
$$\pi_s = NIZKP\,[(sk) : s = Dec_{sk}(e) \wedge pk = publicKey(sk)]$$

- Bulletin board contents at the end of protocol:

$(e_1, \pi_{e_1}), \ldots, (e_n, \pi_{e_n})$
s, pk, π_s

Threshold Decryption

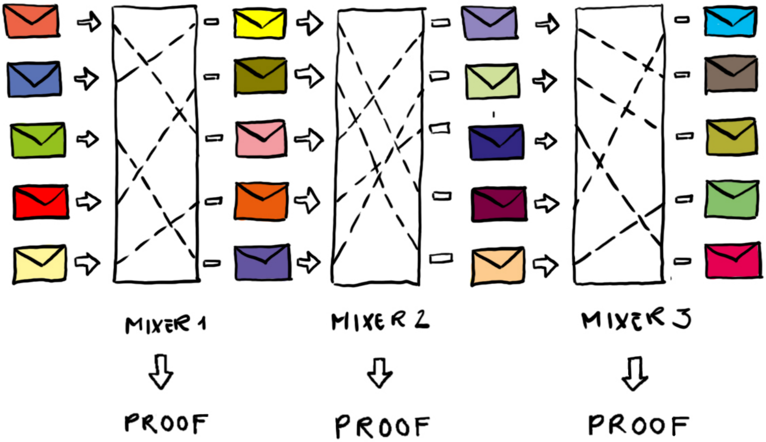
- Attack 3: Dishonest authority decrypts e_i individually
- This attack can be prevented by sharing the private key among multiple authorities,
$$(sk_1, \dots, sk_k) = Share(sk, t),$$
where $0 \leq t \leq k$ denotes the *sharing threshold*
- To decrypt e, at least t authorities compute $s_j = Dec_{sk_j}(e)$ and publish s_j along with π_{s_j}
- The election result s follows deterministically from $s_1, \dots, s_t$
- Bulletin board contents at the end of protocol:

$(e_1, \pi_{e_1}), \dots, (e_n, \pi_{e_n})$
$(s_1, pk_1, \pi_{s_1}), \dots, (s_t, pk_t, \pi_{s_t})$

Approach 2: Re-Encryption Mixnet

- A homomorphic encryption $e = Enc_{pk}(m)$ can be *re-encrypted*:
  $$e' = ReEnc_{pk}(e) = e * Enc_{pk}(0) = Enc_{pk}(m)$$
- A *cryptographic shuffle* transforms a list $E = (e_1, \ldots, e_n)$ of encryptions into $E' = (e'_1, \ldots, e'_n)$ such that $e'_j = ReEnc_{pk}(e_i)$ for every $j = \psi(i)$
- The correctness of the shuffle needs to be proven:
  $$\pi_{\psi} = NIZKP\left[(\psi) : e_j = ReEnc_{pk}(e_i),\ \forall j = \psi(i)\right]$$
- A series of cryptographic shuffles forms a *re-encryption mixnet*

Approach 2: Re-Encryption Mixnet



Approach 2: Re-Encryption Mixnet

- Bulletin board contents at the end of protocol:

$$E = (e_1, \ldots, e_n) = E_0$$
$$E' = (e'_1, \ldots, e'_n) = E_t$$
$$(E_0, E_1, \pi_{\psi_1}), (E_1, E_2, \pi_{\psi_2}), \ldots, (E_{t-1}, E_t, \pi_{\psi_t})$$
$$(s_1, pk_1, \pi_{s_1}), \ldots, (s_t, pk_t, \pi_{s_t})$$

- Re-encryption mixnets are more flexible and efficient than homomorphic tallying

Cast-As-Intended Verifiability

Cast-as-Intended Verification

- <u>Attack 4</u>: Dishonest voting computer encrypts $v' \neq v$
- This attack can be detected, if a personalized code sheet with different verification codes for each voting option is generated for every voter

Code Sheet Nr.291

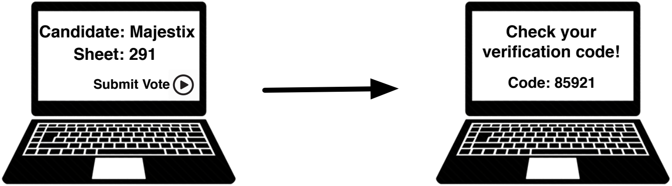
Candidates	Codes
Asterix	74494
Obelix	84443
Idefix	91123
Miraculix	63382
Majestix	85921
Verleihnix	79174

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



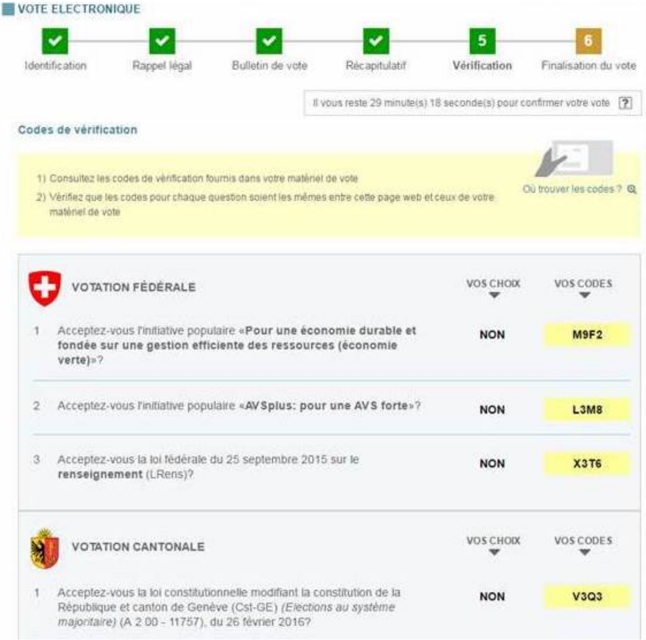
- Matching codes imply that the vote has been cast as intended
- Otherwise, voters are instructed to vote by postal mail

Cast-as-Intended Verification

- Detectable malware attacks (or software bugs)
  - Manipulated votes ✓
  - Suppressed votes ✓
  - Manipulated verification codes ✓
  - Suppressed verification codes ✓

- Unsolved malware attacks
  - Secrecy of vote ✗
  - Social engineering attack: "Please enter verification code" ✗

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

Oblivious Transfer

- Security properties of transmitting verification codes
  - The voting server does not learn the voter's selections
  - The voting client does not learn codes different from the voter's selections
- In cryptography, this is called an oblivious transfer (OT) problem between a sender and a receiver
  - The sender has n messages $\mathbf{m} = (m_1, \ldots, m_n)$, $m_i \in \{0,1\}^\ell$
  - The receiver selects k indices $\mathbf{s} = (s_1, \ldots, s_k)$, $s_i \in \{1, \ldots, n\}$
  - Executing the protocol reveals $\mathbf{m}_\mathbf{s} = (m_{s_1}, \ldots, m_{s_k})$ to the receiver

Properties of OT protocols

- Receiver privacy: the sender learns nothing about $\mathbf{s}$
- Sender privacy: the receiver learns nothing more than $\mathbf{m}_\mathbf{s}$

OT-Protocol by Chu and Tzeng

Receiver

selects $\mathbf{s} = (s_1, \ldots, s_k)$

for $j = 1, \ldots, k$

– pick random $r_j \in_R \mathbb{Z}_q$

– compute $a_j = \Gamma(s_j) \cdot g^{r_j}$

Sender

knows $\mathbf{m} = (m_1, \ldots, m_n)$

$\xrightarrow{\mathbf{a}=(a_1,\ldots,a_k)}$

pick random $r \in_R \mathbb{Z}_q$

for $j = 1, \ldots, k$

– compute $b_j = a_j^r$

for $i = 1, \ldots, n$

– compute $k_i = H(\Gamma(i)^r)$

– compute $c_i = m_i \oplus k_i$

compute $d = g^r$

$\xleftarrow{\mathbf{b}=(b_1,\ldots,b_k),\ \mathbf{c}=(c_1,\ldots,c_n),\ d}$

for $j = 1, \ldots, k$

– compute $k_j = H(b_j \cdot d^{-r_j})$

– compute $m_{s_j} = c_{s_j} \oplus k_j$

Conclusion

CHVote Protocol Specification

- Publicly available at https://eprint.iacr.org/2017/325
  - Version 1.0 published on April 20, 2017
  - Version 3.0 (to be released very soon)
- Self-contained and comprehensive document (∼200 pages)
  - Description of election use cases
  - Mathematical and cryptographic background
  - Details of encoding and hashing algorithms
  - Adversary and trust assumptions
  - Cryptographic and election parameters
  - Recommendations for group sizes, key lengths, code lengths
- About 80 pseudo-code algorithms

Conclusion

- Verifiability is central to making e-voting secure
- Many cryptographic protocols exist in scientific literature, e.g. based on homomorphic tallying or re-encryption mixnets
- 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"