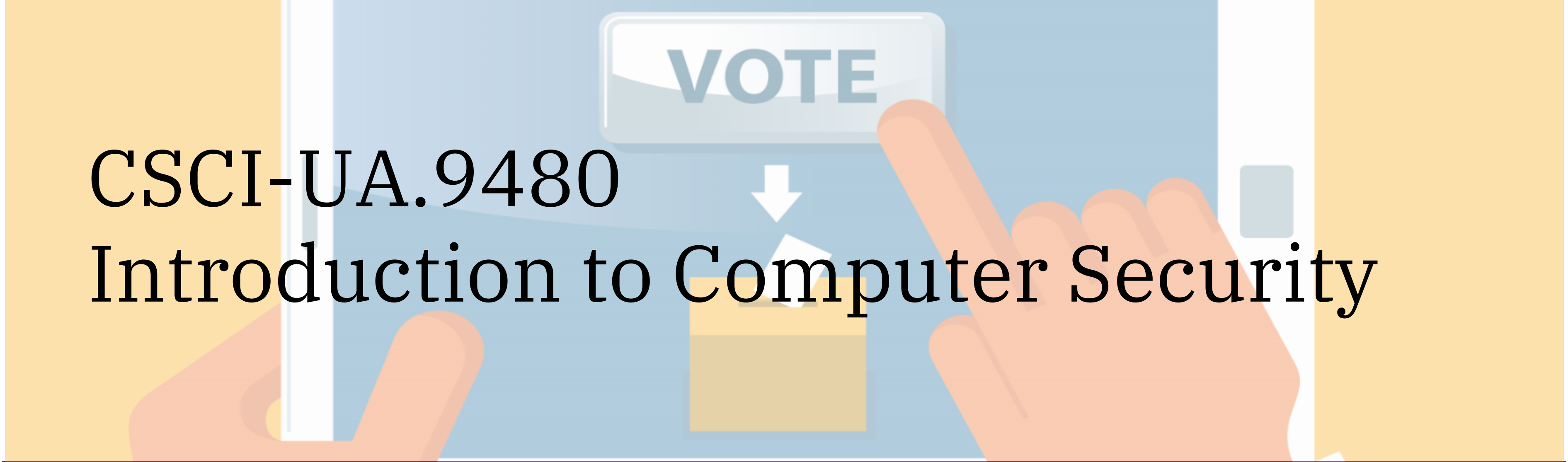


CSCI-UA.9480
Introduction to Computer Security

Session 1.8
E-Voting and Other Modern Uses of Cryptography

Prof. Nadim Kobeissi

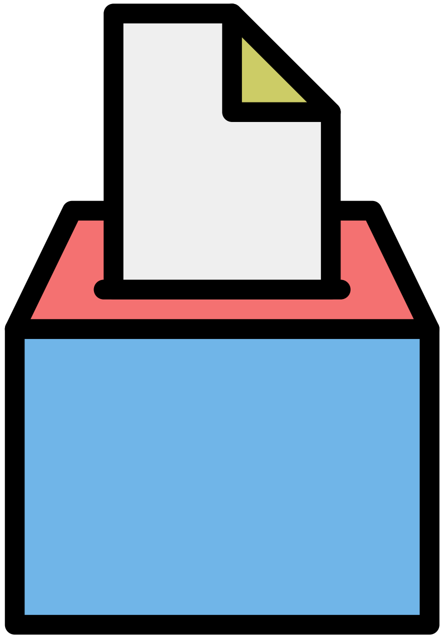
Electronic Voting

1.8a

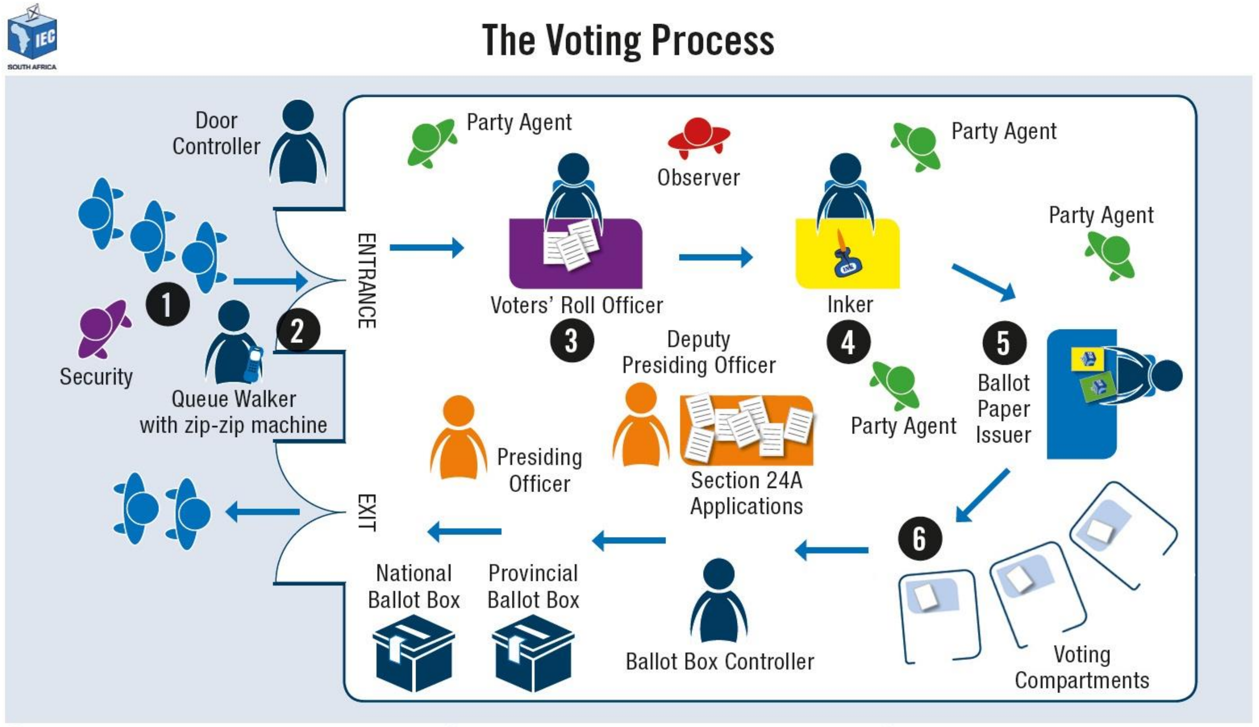
Properties of an traditional system.

- **Availability:** Voters can actually vote.
- **Confidentiality:** votes remain secret.
- **Anonymity:** Votes are anonymous.
- **Integrity:** Votes cannot be tampered with.

- In addition, **separation of privilege** and the general **auditability** of al processes in the system as well as the system itself are paramount.



Traditional voting process.

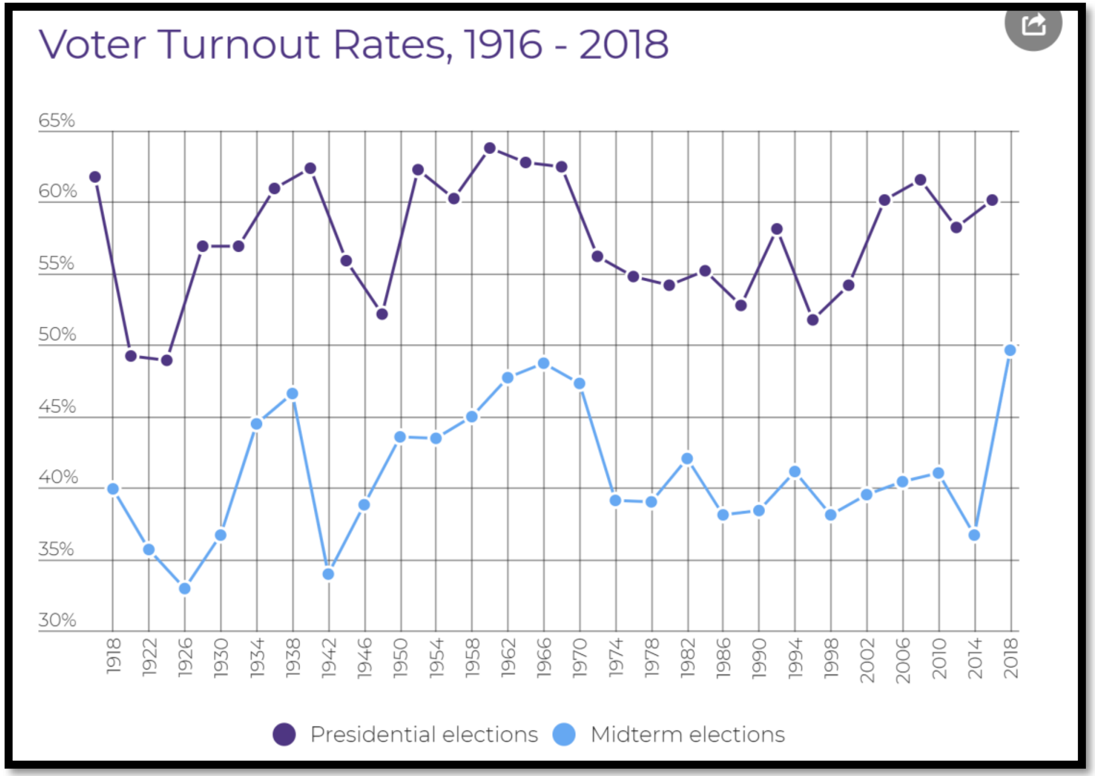


1. **In the queue:** An election official will check your ID to make sure you are registered.
2. **At the door:** An election official will scan your ID with the zip-zip machine.
3. **At the voters' roll table:** You will give your slip of paper to the voters' roll officer.
4. **At the inking table:** An election official will make a small mark on the nail of your left thumb with ink.
5. **At the ballot paper table:** You will be given up to two ballots.
6. **At the voting compartments:** Mark your ballot in secret.

Source: Electoral Commission of South Africa

So what’s the problem?

- Low turnout, as seen for example in the United States (source: fairvote.org)
- Expensive to organize.
- E-voting could allow for organizing more elections, delivering voting results more reliably…
- Widening access to voting?

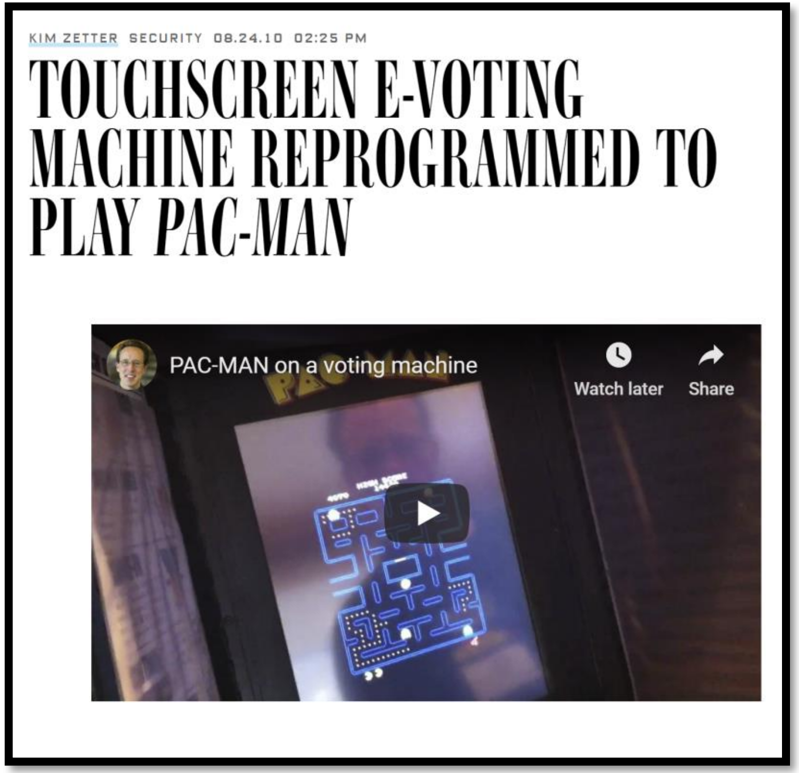


What about electronic voting machines?

- Very popular across the world, actually.
- In France: iVotronic, “Machine à voter”, “Point & Vote”…

- Potential issues: systems not open source, issues of public confidence…

- Attacks reported: *“Alex Halderman and Ari Feldman replaced the voting software with Pac-Man. They did this in three afternoons, without breaking any tamper-evident seals. It would be easy to modify the software to steal votes, but that's been done before, and Pac-Man is more fun.”*

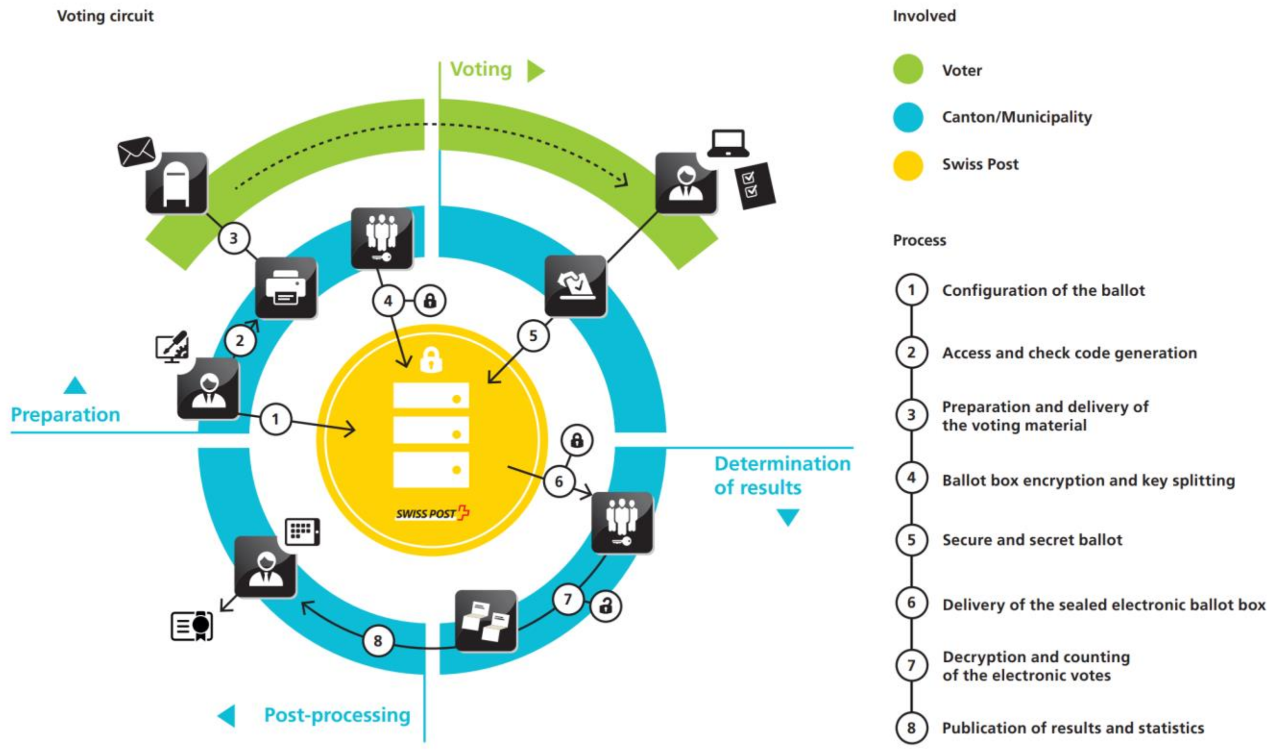

KIM ZETTER SECURITY 08.24.10 02:25 PM

TOUCHSCREEN E-VOTING MACHINE REPROGRAMMED TO PLAY *PAC-MAN*

Swiss Post's E-voting Solution.

- *"Cantons have* ***complete control*** *over the election process, which means that they can guarantee their sovereign jurisdiction at all times."*
- *"Cantons can organize their own elections and voting processes* ***very simply."***
- *"****Data protection*** *is guaranteed at all times:*
  - *List of all voters remains the sole property of the canton.*
  - *All data and servers located in Switzerland."*
- *"****Voting secrecy*** *is guaranteed at all times:*
  - *Based on a verifiable cryptographic protocol.*
  - *End-to-end encryption."*
- *"Guaranteed high level of* ***availability."***

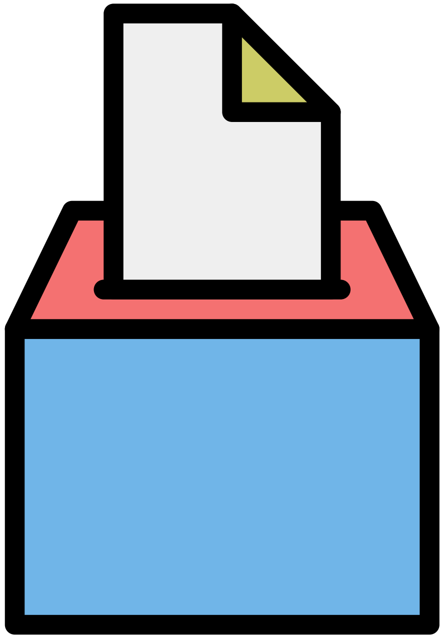
Swiss Post's E-voting solution.


Voting circuit
Voting
Preparation
Determination of results
Post-processing
SWISS POST
1
2
3
4
5
6
7
8
Involved
Voter
Canton/Municipality
Swiss Post
Process
1 Configuration of the ballot
2 Access and check code generation
3 Preparation and delivery of the voting material
4 Ballot box encryption and key splitting
5 Secure and secret ballot
6 Delivery of the sealed electronic ballot box
7 Decryption and counting of the electronic votes
8 Publication of results and statistics

Same security goals apply.

- **Availability:** Voters can actually vote.
- **Confidentiality:** votes remain secret.
- **Anonymity:** Votes are anonymous.
- **Integrity:** Votes cannot be tampered with.

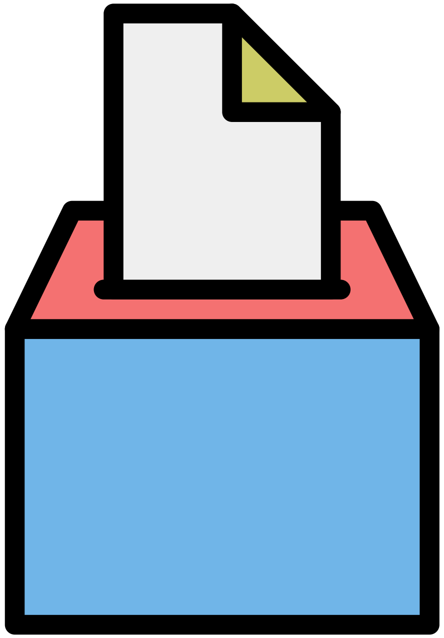
- In addition, **separation of privilege** and the general **auditability** of al processes in the system as well as the system itself are paramount.



Threat modeling for e-voting.

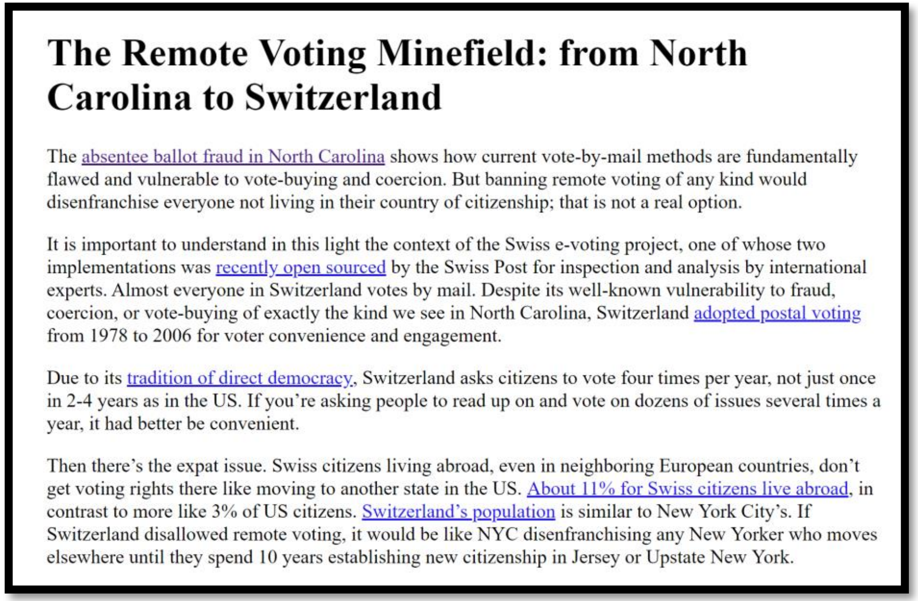
- Insider attack.
- Backdoored code.
- Flaws in code.
- Computer or server compromise.
- Denial of Service attacks.

- What about public confidence? Even a flawless election can result in a political crisis if the public doesn't believe in the legitimacy or credibility of the process.



So is e-voting even worth it?

- Debate has been ongoing but was recently reinvigorated by the Swiss Post public audit and penetration test initiative.
- Bryan Ford argues that it's worth it →
- *"International scrutiny of E-voting systems like Switzerland's is extremely important and welcome. But simplistically opposing all E-voting, on grounds of complexity or failure to solve problems like vote-buying that alternatives like postal voting have too, is counterproductive. The only way to solve critical open security challenges like vote-buying is to press forward and work to advance the state-of-the-art further, not retreat to a techno-luddist position that any voting method using paper is automatically more secure than any method using electrons."*



The Remote Voting Minefield: from North Carolina to Switzerland

The absentee ballot fraud in North Carolina shows how current vote-by-mail methods are fundamentally flawed and vulnerable to vote-buying and coercion. But banning remote voting of any kind would disenfranchise everyone not living in their country of citizenship; that is not a real option.

It is important to understand in this light the context of the Swiss e-voting project, one of whose two implementations was recently open sourced by the Swiss Post for inspection and analysis by international experts. Almost everyone in Switzerland votes by mail. Despite its well-known vulnerability to fraud, coercion, or vote-buying of exactly the kind we see in North Carolina, Switzerland adopted postal voting from 1978 to 2006 for voter convenience and engagement.

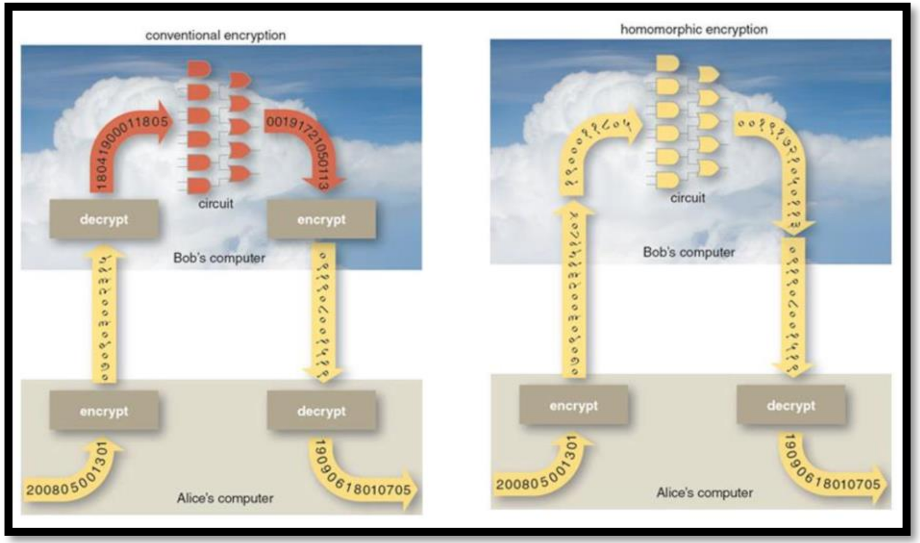
Due to its tradition of direct democracy, Switzerland asks citizens to vote four times per year, not just once in 2-4 years as in the US. If you're asking people to read up on and vote on dozens of issues several times a year, it had better be convenient.

Then there's the expat issue. Swiss citizens living abroad, even in neighboring European countries, don't get voting rights there like moving to another state in the US. About 11% for Swiss citizens live abroad, in contrast to more like 3% of US citizens. Switzerland's population is similar to New York City's. If Switzerland disallowed remote voting, it would be like NYC disenfranchising any New Yorker who moves elsewhere until they spend 10 years establishing new citizenship in Jersey or Upstate New York.

Computing on encrypted data.

- Homomorphic encryption allows computing on encrypted data without decrypting it.
- For example, Alice can add `E(K,1)` to `E(K,5)` without knowing *K*, and obtain `E(K,6)`.

$$\begin{tikzcd}
m_1 \arrow[d] & & m_2 \arrow[d] \\
E_{pk}(m_1) \arrow[dr] & & E_{pk}(m_2) \arrow[dl] \\
& \times \arrow[d] & \\
& E_{pk}(m_1 + m_2) &
\end{tikzcd}$$



Source: Orange Labs

Applications to e-voting: referendum case.

- "Yes vote" = 1 and "no vote" = 0,
- Each voter encrypts her vote using the tallier's public keys.
- The voting center computes an encryption of the sum of the votes thanks to the properties of the homomorphic encryption scheme.
- The tallier decrypts this ciphertext and obtain the outcome of the election.
- **No individual vote is revealed!**

$$\begin{tikzcd}
m_1 \arrow[d] & & m_2 \arrow[d] \\
E_{pk}(m_1) \arrow[dr] & & E_{pk}(m_2) \arrow[dl] \\
& \times \arrow[d] & \\
& E_{pk}(m_1 + m_2) &
\end{tikzcd}$$

Source: Orange Labs

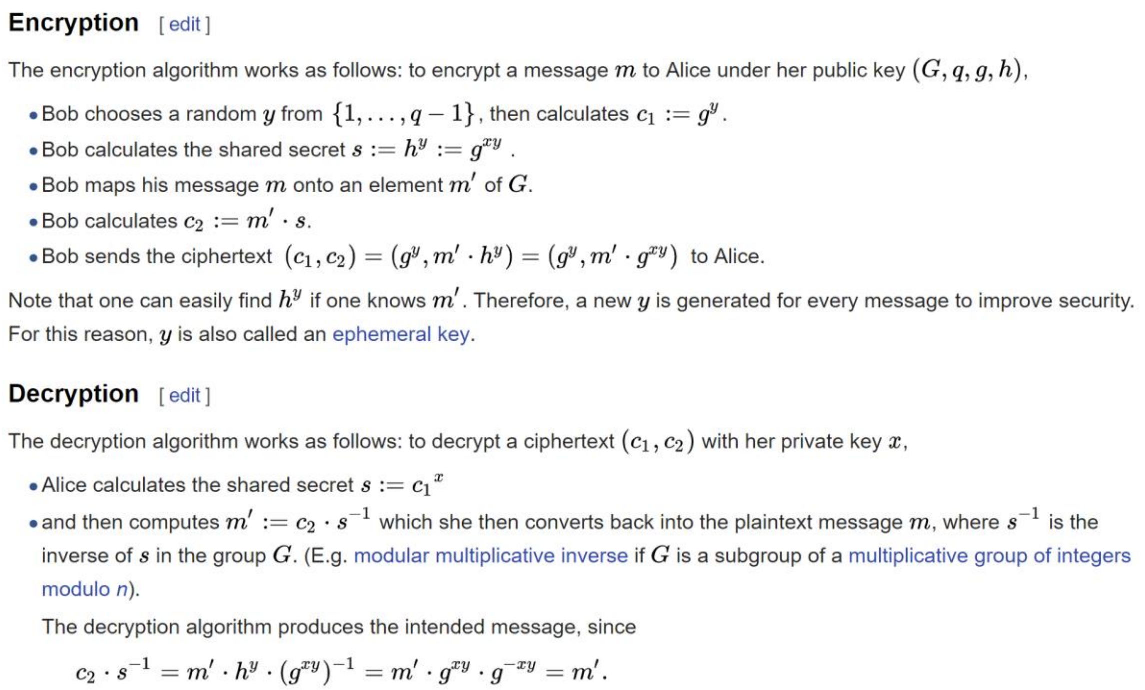
What about coercion, remote impersonation?

- To mislead a coercer, the voter sends invalid ballot(s) as long as he is coerced, and a valid ballot as soon as he is not coerced.
- It suffices that the voter finds a window-time during which he is not coerced.

$$\begin{tikzcd}
m_1 \arrow[d] & & m_2 \arrow[d] \\
E_{pk}(m_1) \arrow[dr] & & E_{pk}(m_2) \arrow[dl] \\
& \times \arrow[d] & \\
& E_{pk}(m_1 + m_2) &
\end{tikzcd}$$

Source: Orange Labs

ElGamal is partially homomorphic.



Encryption [edit]

The encryption algorithm works as follows: to encrypt a message m to Alice under her public key (G, q, g, h),

- Bob chooses a random y from $\{1, \ldots, q-1\}$, then calculates $c_1 := g^y$.
- Bob calculates the shared secret $s := h^y := g^{xy}$.
- Bob maps his message m onto an element m' of G.
- Bob calculates $c_2 := m' \cdot s$.
- Bob sends the ciphertext $(c_1, c_2) = (g^y, m' \cdot h^y) = (g^y, m' \cdot g^{xy})$ to Alice.

Note that one can easily find h^y if one knows m'. Therefore, a new y is generated for every message to improve security. For this reason, y is also called an ephemeral key.

Decryption [edit]

The decryption algorithm works as follows: to decrypt a ciphertext (c_1, c_2) with her private key x,

- Alice calculates the shared secret $s := c_1{}^x$
- and then computes $m' := c_2 \cdot s^{-1}$ which she then converts back into the plaintext message m, where s^{-1} is the inverse of s in the group G. (E.g. modular multiplicative inverse if G is a subgroup of a multiplicative group of integers modulo *n*).

  The decryption algorithm produces the intended message, since

$$c_2 \cdot s^{-1} = m' \cdot h^y \cdot (g^{xy})^{-1} = m' \cdot g^{xy} \cdot g^{-xy} = m'.$$

Secret key: x
Public key: (G, q, g, h = g^x)

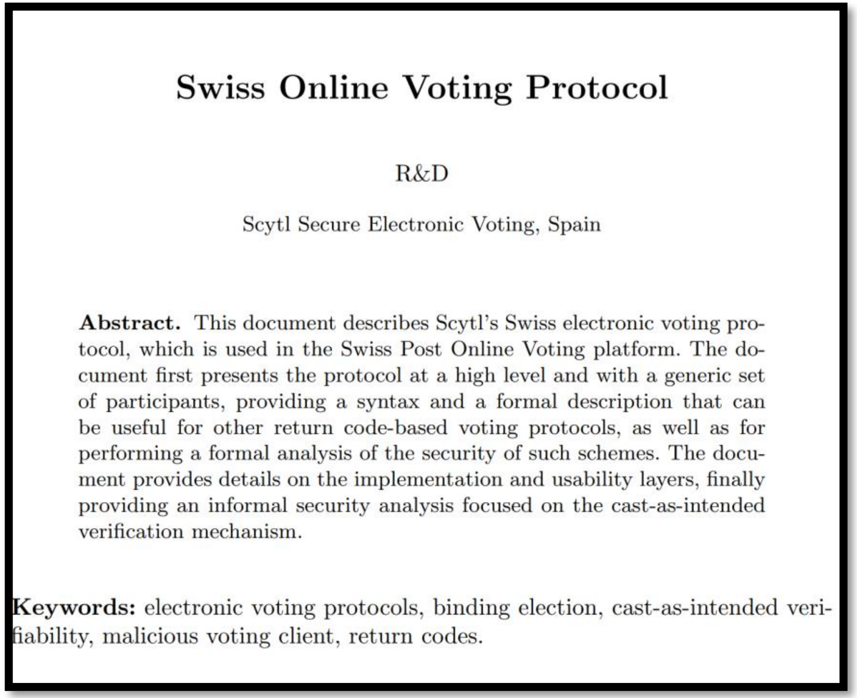
$$\boxed{\begin{aligned} &\mathcal{E}(m_1) \cdot \mathcal{E}(m_2) = (g^{r_1}, m_1 \cdot h^{r_1})(g^{r_2}, m_2 \cdot h^{r_2}) \\ &= (g^{r_1+r_2}, (m_1 \cdot m_2)h^{r_1+r_2}) = \mathcal{E}(m_1 \cdot m_2). \end{aligned}}$$

Source: Wikipedia

Looking at Swiss E-voting's cryptography.

- Uses ElGamal.
- Uses zero-knowledge proofs of knowledge (proving that you know *x* to a verifier without either party revealing anything about *x*).

- Read the whole thing here: https://www.post.ch/-/media/post/evoting/dokumente/swiss-post-online-voting-protocol.pdf



Swiss Online Voting Protocol

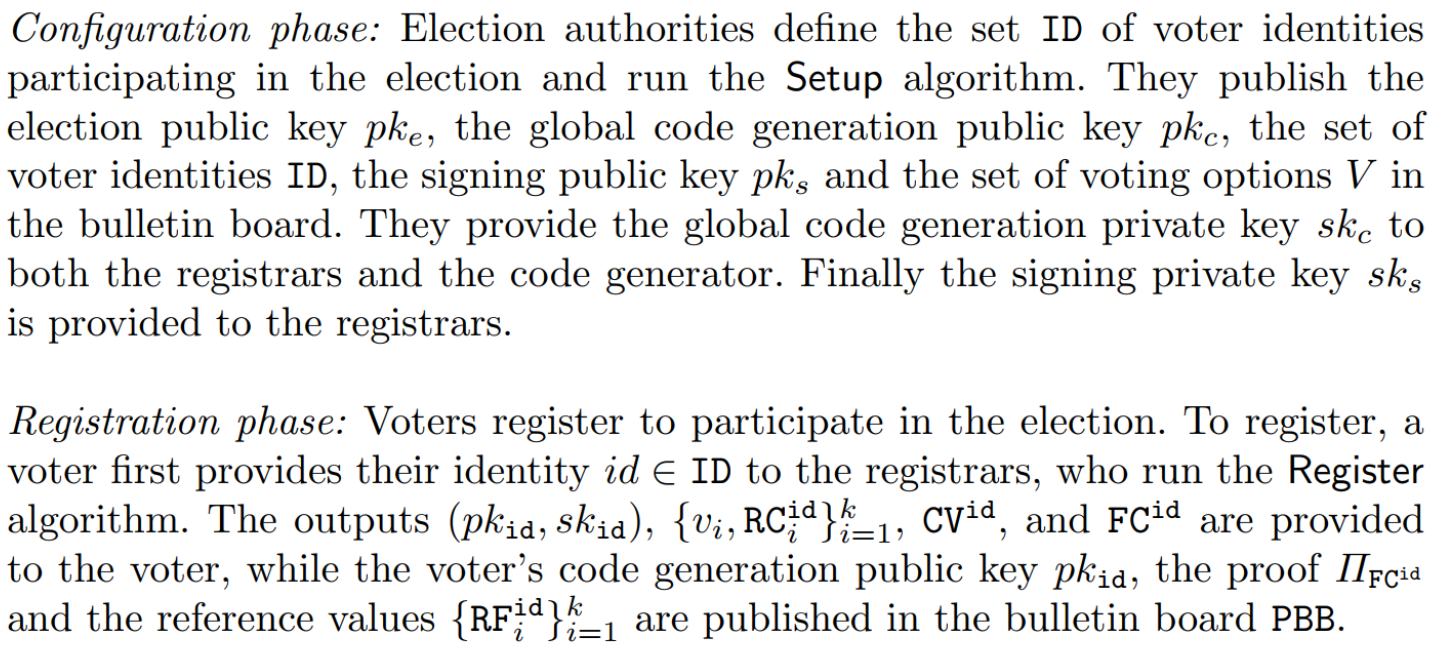
R&D

Scytl Secure Electronic Voting, Spain

Abstract. This document describes Scytl's Swiss electronic voting protocol, which is used in the Swiss Post Online Voting platform. The document first presents the protocol at a high level and with a generic set of participants, providing a syntax and a formal description that can be useful for other return code-based voting protocols, as well as for performing a formal analysis of the security of such schemes. The document provides details on the implementation and usability layers, finally providing an informal security analysis focused on the cast-as-intended verification mechanism.

Keywords: electronic voting protocols, binding election, cast-as-intended verifiability, malicious voting client, return codes.

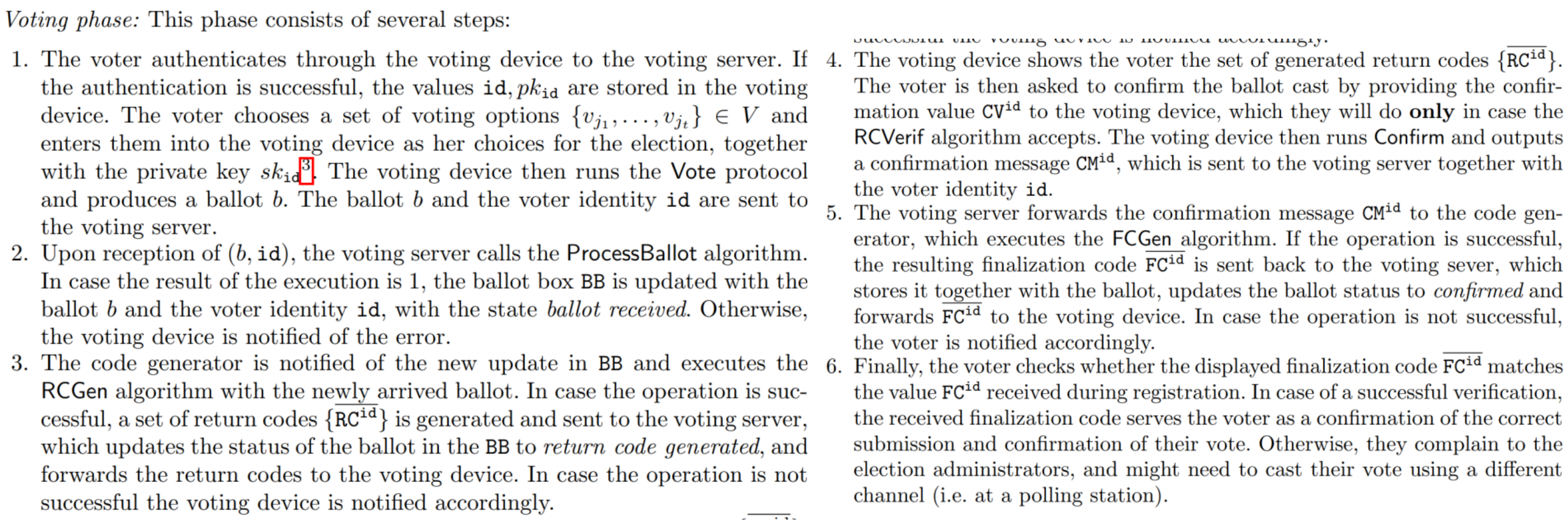
Swiss E-voting protocol workflow.



Configuration phase: Election authorities define the set $\texttt{ID}$ of voter identities participating in the election and run the Setup algorithm. They publish the election public key pk_e, the global code generation public key pk_c, the set of voter identities $\texttt{ID}$, the signing public key pk_s and the set of voting options V in the bulletin board. They provide the global code generation private key sk_c to both the registrars and the code generator. Finally the signing private key sk_s is provided to the registrars.

Registration phase: Voters register to participate in the election. To register, a voter first provides their identity $id \in \texttt{ID}$ to the registrars, who run the $\mathsf{Register}$ algorithm. The outputs $(pk_{\texttt{id}}, sk_{\texttt{id}})$, $\{v_i, \texttt{RC}_i^{\texttt{id}}\}_{i=1}^{k}$, $\texttt{CV}^{\texttt{id}}$, and $\texttt{FC}^{\texttt{id}}$ are provided to the voter, while the voter's code generation public key $pk_{\texttt{id}}$, the proof $\Pi_{\texttt{FC}^{\texttt{id}}}$ and the reference values $\{\texttt{RF}_i^{\texttt{id}}\}_{i=1}^{k}$ are published in the bulletin board $\texttt{PBB}$.

Swiss E-voting protocol workflow.



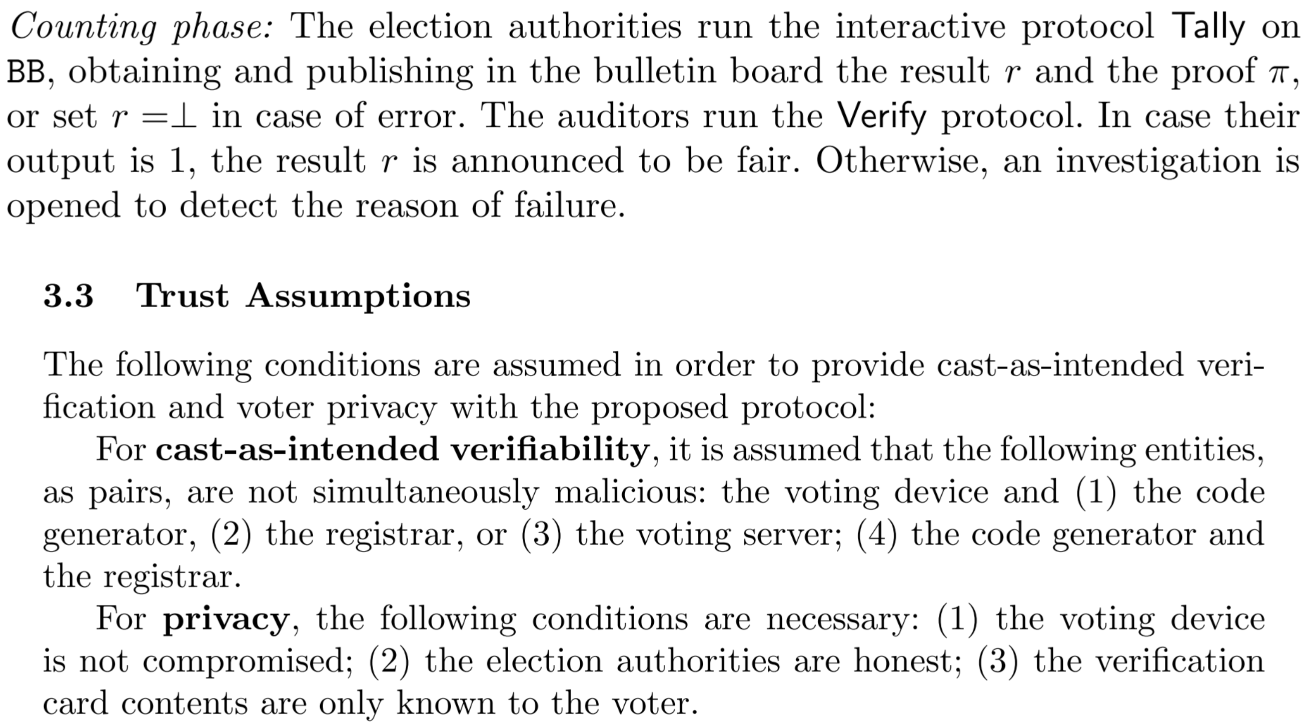
Voting phase: This phase consists of several steps:

1. The voter authenticates through the voting device to the voting server. If the authentication is successful, the values $\mathtt{id}, pk_{\mathtt{id}}$ are stored in the voting device. The voter chooses a set of voting options $\{v_{j_1}, \ldots, v_{j_t}\} \in V$ and enters them into the voting device as her choices for the election, together with the private key $sk_{\mathtt{id}}$[3]. The voting device then runs the Vote protocol and produces a ballot b. The ballot b and the voter identity $\mathtt{id}$ are sent to the voting server.
2. Upon reception of $(b, \mathtt{id})$, the voting server calls the ProcessBallot algorithm. In case the result of the execution is 1, the ballot box BB is updated with the ballot b and the voter identity $\mathtt{id}$, with the state *ballot received*. Otherwise, the voting device is notified of the error.
3. The code generator is notified of the new update in BB and executes the RCGen algorithm with the newly arrived ballot. In case the operation is successful, a set of return codes $\{\overline{\mathtt{RC}}^{\mathtt{id}}\}$ is generated and sent to the voting server, which updates the status of the ballot in the BB to *return code generated*, and forwards the return codes to the voting device. In case the operation is not successful the voting device is notified accordingly.

successful the voting device is notified accordingly.

4. The voting device shows the voter the set of generated return codes $\{\overline{\mathtt{RC}}^{\mathtt{id}}\}$. The voter is then asked to confirm the ballot cast by providing the confirmation value $\mathtt{CV}^{\mathtt{id}}$ to the voting device, which they will do **only** in case the RCVerif algorithm accepts. The voting device then runs Confirm and outputs a confirmation message $\mathtt{CM}^{\mathtt{id}}$, which is sent to the voting server together with the voter identity $\mathtt{id}$.
5. The voting server forwards the confirmation message $\mathtt{CM}^{\mathtt{id}}$ to the code generator, which executes the FCGen algorithm. If the operation is successful, the resulting finalization code $\overline{\mathtt{FC}}^{\mathtt{id}}$ is sent back to the voting sever, which stores it together with the ballot, updates the ballot status to *confirmed* and forwards $\overline{\mathtt{FC}}^{\mathtt{id}}$ to the voting device. In case the operation is not successful, the voter is notified accordingly.
6. Finally, the voter checks whether the displayed finalization code $\overline{\mathtt{FC}}^{\mathtt{id}}$ matches the value $\mathtt{FC}^{\mathtt{id}}$ received during registration. In case of a successful verification, the received finalization code serves the voter as a confirmation of the correct submission and confirmation of their vote. Otherwise, they complain to the election administrators, and might need to cast their vote using a different channel (i.e. at a polling station).

Swiss E-voting protocol workflow.



Counting phase: The election authorities run the interactive protocol Tally on BB, obtaining and publishing in the bulletin board the result r and the proof π, or set $r = \perp$ in case of error. The auditors run the Verify protocol. In case their output is 1, the result r is announced to be fair. Otherwise, an investigation is opened to detect the reason of failure.

3.3 Trust Assumptions

The following conditions are assumed in order to provide cast-as-intended verification and voter privacy with the proposed protocol:

For **cast-as-intended verifiability**, it is assumed that the following entities, as pairs, are not simultaneously malicious: the voting device and (1) the code generator, (2) the registrar, or (3) the voting server; (4) the code generator and the registrar.

For **privacy**, the following conditions are necessary: (1) the voting device is not compromised; (2) the election authorities are honest; (3) the verification card contents are only known to the voter.

Next time: Networking Basics, TCP, IP and DNS

The first session in Part 2 of our course: Network Security.

2.1