

The Pi-Vote eVoting System

How the Pirate Party Switzerland uses ADDER

Denis Simonet, Stefan Thöni

Pirate Party Switzerland

May 24, 2012

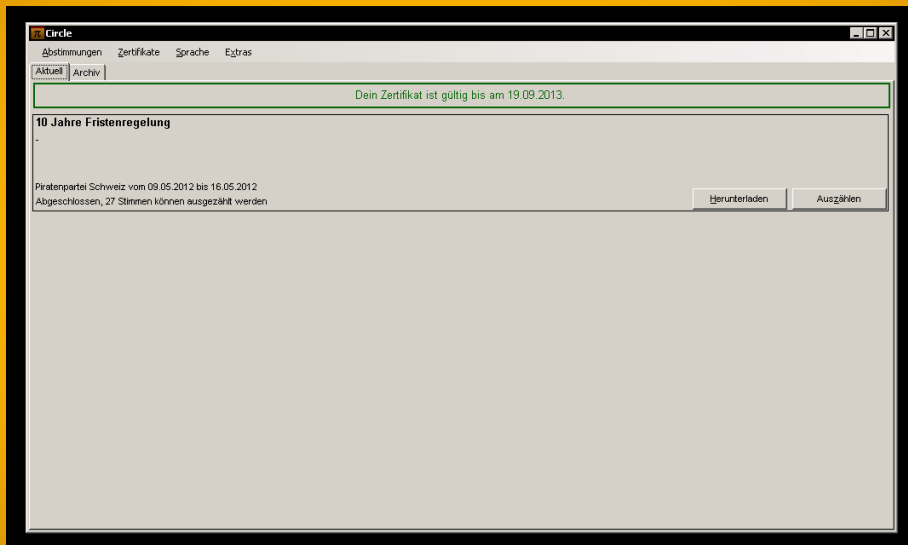


pirateparty
www.pirateparty.ch

Part I

**Why does the Pirate Party Switzerland
use eVoting?**

About Pi-Vote



The screenshot shows a web browser window titled "Circle". The navigation menu includes "Abstimmungen", "Zertifikate", "Sprache", and "Extras". The "Aktuell" tab is selected, and a message states "Dein Zertifikat ist gültig bis am 19.09.2013." Below this, the section "10 Jahre Fristenregelung" is displayed with a minus sign. A text block indicates "Piratenpartei Schweiz vom 09.05.2012 bis 16.05.2012" and "Abgeschlossen, 27 Stimmen können ausgezählt werden". Two buttons, "Herunterladen" and "Auszählen", are located at the bottom right of the content area.



Part II

**How Pi-Vote works and what Problems
remain**

Assumptions

We assume...

- Decisional Diffie-Hellman assumption is true;
- Integer factorization is hard;
- SHA-2 is sufficiently close to a random oracle;
- Random number generators in PCs/OS are good.



Secrecy

How is secrecy achieved?

- Homomorphic encryption of ballots
- 4 out of 5 sharing of the secret



Secrecy

How is secrecy achieved?

- Homomorphic encryption of ballots
- 4 out of 5 sharing of the secret

Potential problems

- Possibility of decryption exists and could be forced e.g. by law
- Parts of secret may be lost or given away later



Secrecy

How is secrecy achieved?

- Homomorphic encryption of ballots
- 4 out of 5 sharing of the secret

Potential problems

- Possibility of decryption exists and could be forced e.g. by law
- Parts of secret may be lost or given away later

Real problems

- Authorities can be unreliable!



Correctness

How is the correctness of ballots ensured?

- Zero knowledge proofs with Fiat-Shamir heuristic



Correctness

How is the correctness of ballots ensured?

- Zero knowledge proofs with Fiat-Shamir heuristic

Real problems

- Proofs take many CPU cycles to verify



Authorization

How is voting authorized?

- RSA signatures
- Certificates



Authorization

How is voting authorized?

- RSA signatures
- Certificates

Potential problems

- Compromised CA
- Only achieves pseudonymity



Authentication

How are members authenticated?

- Paper form
- 3 signatures from elected notaries



Authentication

How are members authenticated?

- Paper form
- 3 signatures from elected notaries

Potential problems

- Forged signatures
- Bribery and threat



Authentication

How are members authenticated?

- Paper form
- 3 signatures from elected notaries

Potential problems

- Forged signatures
- Bribery and threat

Real problems

- Not easy enough to use



Tallying

How to guarantee re-tallying at any time?

- Votes and partial decryptions are published and can be downloaded any time



Tallying

How to guarantee re-tallying at any time?

- Votes and partial decryptions are published and can be downloaded any time

Potential problems

- Breaking software changes



Receipt-freeness

Is Pi-Vote receipt-free?

- No
- Not a requirement



Receipt-freeness

Is Pi-Vote receipt-free?

- No
- Not a requirement

Possible solution

- Ballot re-randomization



Manipulated software

How to make sure the software is not manipulated?

- Transparency, Open Source



Manipulated software

How to make sure the software is not manipulated?

- Transparency, Open Source

Not good enough...

- No one ever publicly checked the software security!
- Most users simply download from our page



Denial of service

Internal attacker

- Delete the database
- Shut down the server



Denial of service

Internal attacker

- Delete the database
- Shut down the server

External attacker

- Overload the server



Denial of service

Internal attacker

- Delete the database
- Shut down the server

External attacker

- Overload the server

Impossible to solve...

- Hard to mitigate
- Mostly a case for courts



User acceptance

How do we achieve good user acceptance?

- Open and transparent processes
- Democratic voting on procedures



User acceptance

How do we achieve good user acceptance?

- Open and transparent processes
- Democratic voting on procedures

Real problems

- Users don't understand what's going on but most don't care either
- Multi-platform support and installation are trouble magnets
- Documentation is insufficient
- User interface is never satisfactory



Future plans

Process changes

- Accept identification by Swiss Post and Communal Administration
- Accept SuisseID



Future plans

Process changes

- Accept identification by Swiss Post and Communal Administration
- Accept SuisseID

Technical changes

- Additional Java client
- Android client
- Hardware certificates



Thank you for your attention.



pirateparty
www.pirateparty.ch

