VALG

e-valg 2011 - prosjektet

The Enemy Knows the System

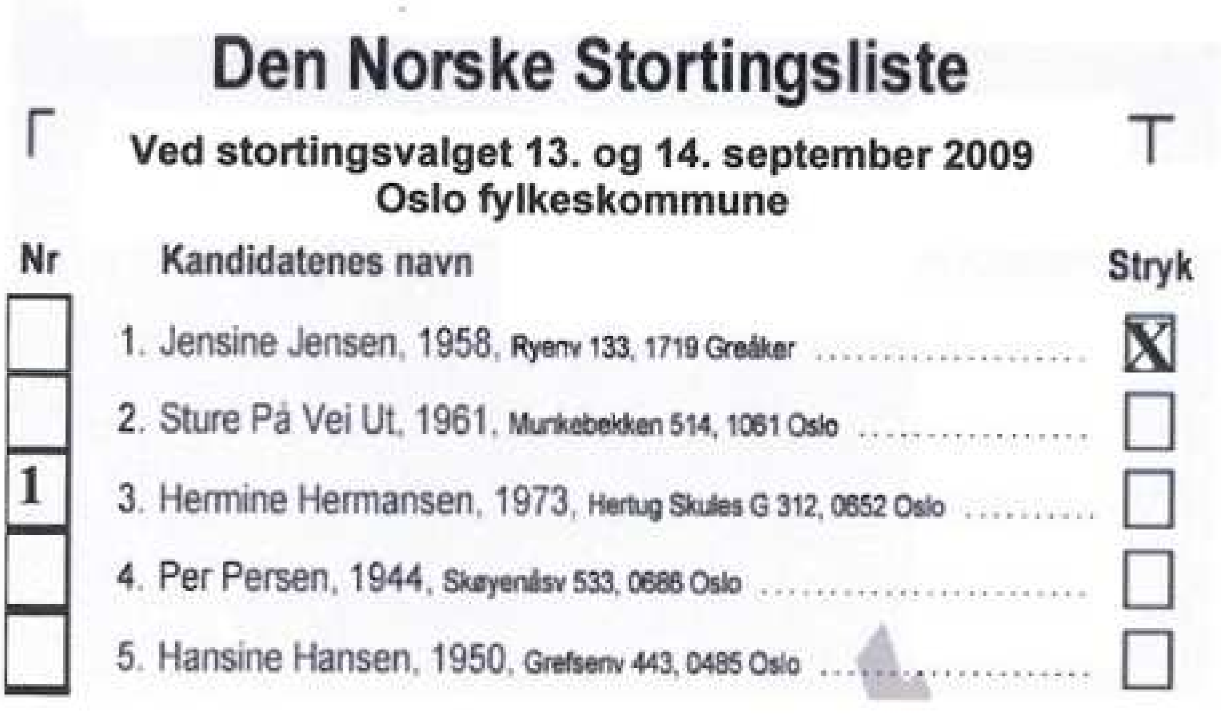
Open Source Remote Electronic Voting in Norway

Senior advisor Christian Bull
The Ministry of Local Government
and Regional Development

Background

- Norway is *tiny* in terms of population (3.300.000 voters)
  - Not so tiny in terms of wealth or geography
- A considerable (in Norwegian terms!) ex-pat population
- Bi-annual elections (parliamentary and local every four years, offset by two years)
- Infrequent, non-binding referenda
- Voters get to make changes to the ballot

The Norwegian Ballot



Den Norske Stortingsliste

Ved stortingsvalget 13. og 14. september 2009
Oslo fylkeskommune

Nr	Kandidatenes navn	Stryk
□	1. Jensine Jensen, 1958, Ryenv 133, 1719 Greåker	☒
□	2. Sture På Vei Ut, 1961, Munkebekken 514, 1061 Oslo	□
1	3. Hermine Hermansen, 1973, Hertug Skules G 312, 0652 Oslo	□
□	4. Per Persen, 1944, Skøyenåsv 533, 0686 Oslo	□
□	5. Hansine Hansen, 1950, Grefsenv 443, 0485 Oslo	□

A basic premise for e-voting

One basic and all important premise for all electronic voting is that the public trusts the government not to conspire against it.

That having been said, the system should not require that no conspiracy against it exists whithin the government!

The Challenges of Remote e-voting

- Auditability / transparency to the lay person
- The buying and selling of votes
- Coercion / family voting
- Home computer security
- Anonymity of the vote
- Attacks *scale,* and there are *externalities*

The Challenges of Remote e-voting

- Auditability / transparency to the lay person
- The buying and selling of votes
- Coercion / family voting
- Home computer security
- Anonymity of the vote
- Attacks *scale,* and there are *externalities*

Caveat:

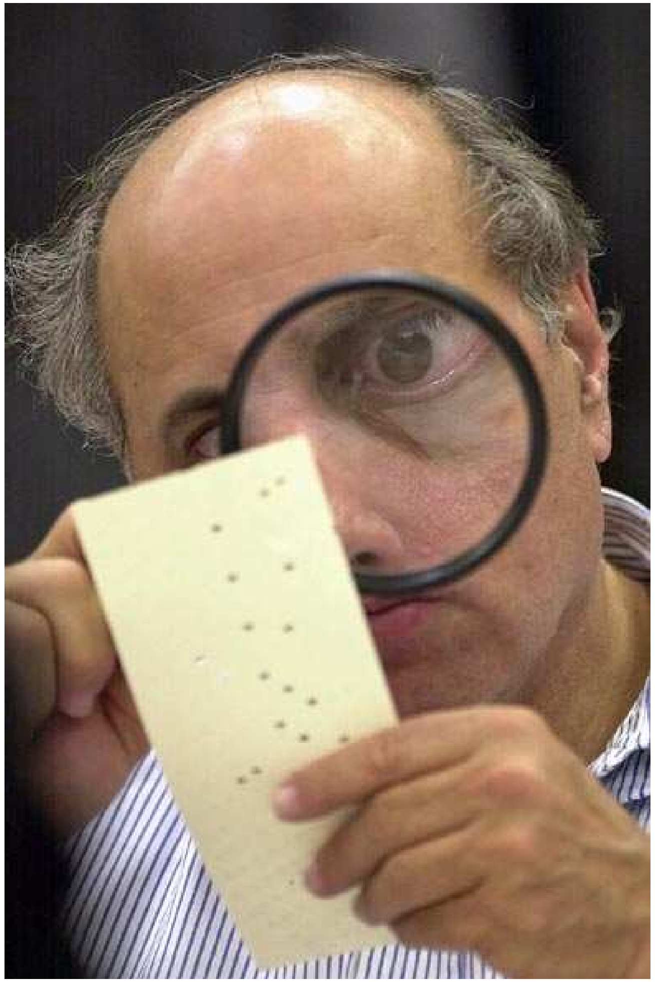
- The complete system with all its nooks and crannies can not be presented in 30 minutes.
- Also, IANAC - I’m leaving out *a lot* of detail.

The Challenges of Remote e-voting

- Auditability / transparency to the lay person
- The buying and selling of votes
- Coercion / family voting
- Home computer security
- Anonymity of the vote
- Attacks *scale,* and there are *externalities*

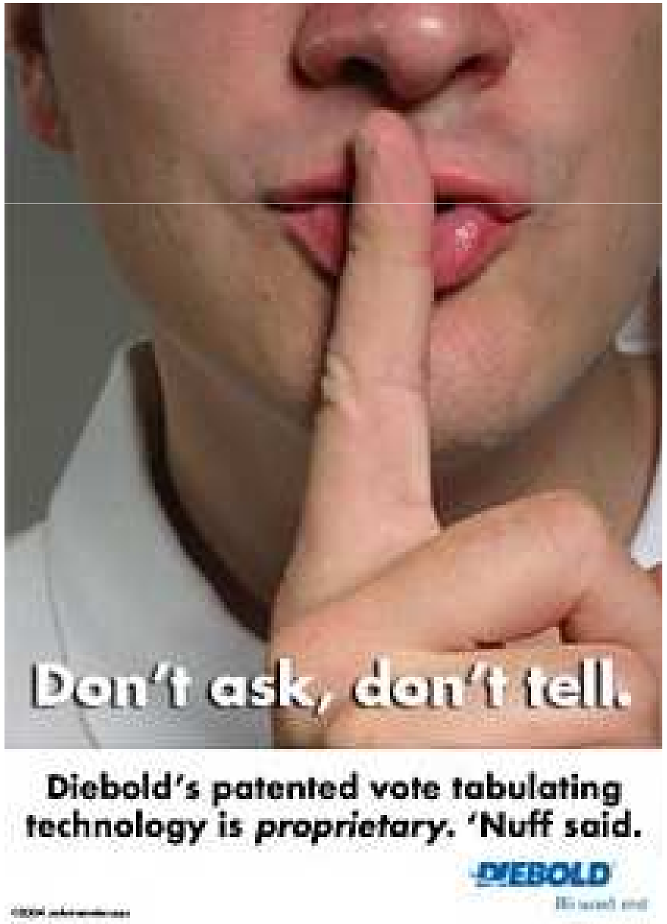
Transparent e-voting?

- Complete openness and transparecy in all aspects of the project
- Available source code
  - Unfourtunately cryptography is really, really hard
- Cryptographic proofs of correctness
  - Even the voter gets one
  - The good thing about crypto is that it's all just maths
- Immutable logging of all system events



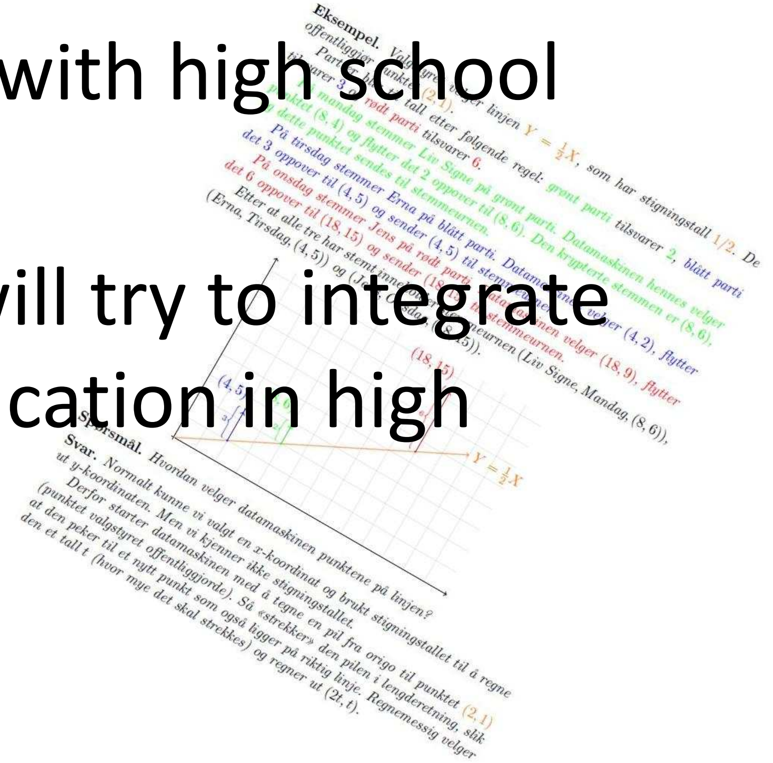
Transparent e-voting?

- Obviously open source won’t make the system understandable to ”everyone”
- …and extensive use of esoteric cryptography makes things worse…
- ..but at least the lay person can choose which expert to trust.
- Besides, paper voting really isn’t that transparent either!


Don’t ask, don’t tell.
Diebold’s patented vote tabulating technology is *proprietary*. ‘Nuff said.
DIEBOLD

Communicating the crypto protocol

- The cryptographer behind it is working on a conceptual description which should be understandable for anyone with high school maths
- Amongst other things, we will try to integrate the protocol into maths education in high school.



Eksempel. Valgstyret velger linjen $Y = \frac{1}{2}X$, som har stigningstall 1/2. De offentliggjør punktet (2,1).

Partier blir til tall etter følgende regel: grønt parti tilsvarer 2, blått parti tilsvarer 3 og rødt parti tilsvarer 6.

På mandag stemmer Liv Signe på grønt parti. Datamaskinen hennes velger punktet (8,4) og flytter det 2 oppover til (8,6). Den krypterte stemmen er (8,6). Og dette punktet sendes til stemmeurnen.

På tirsdag stemmer Erna på blått parti. Datamaskinen velger (4,2), flytter det 3 oppover til (4,5) og sender (4,5) til stemmeurnen.

På onsdag stemmer Jens på rødt parti. Datamaskinen velger (18,9), flytter det 6 oppover til (18,15) og sender (18,15) til stemmeurnen.

Etter at alle tre har stemt inneholder stemmeurnen (Liv Signe, Mandag, (8,6)), (Erna, Tirsdag, (4,5)) og (Jens, Onsdag, (18,15)).

Spørsmål. Hvordan velger datamaskinen punktene på linjen?

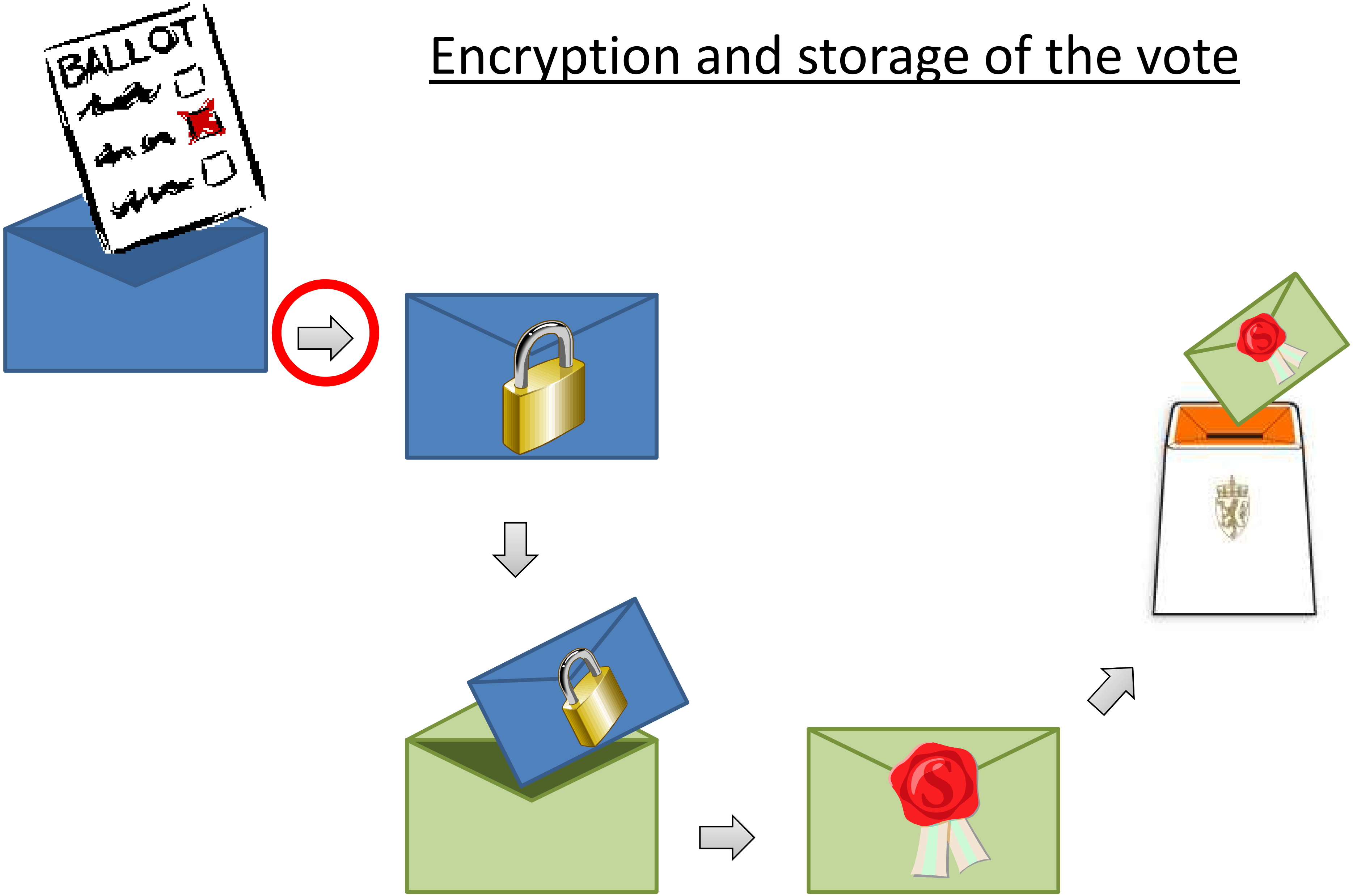
Svar. Normalt kunne vi valgt en x-koordinat og brukt stigningstallet til å regne ut y-koordinaten. Men vi kjenner ikke stigningstallet.

Derfor starter datamaskinen med å tegne en pil fra origo til punktet (2,1) (punktet valgstyret offentliggjorde). Så «strekker» den pilen i lengderetning, slik at den peker til et nytt punkt som også ligger på riktig linje. Regnemessig velger den et tall t (hvor mye det skal strekkes) og regner ut $(2t, t)$.

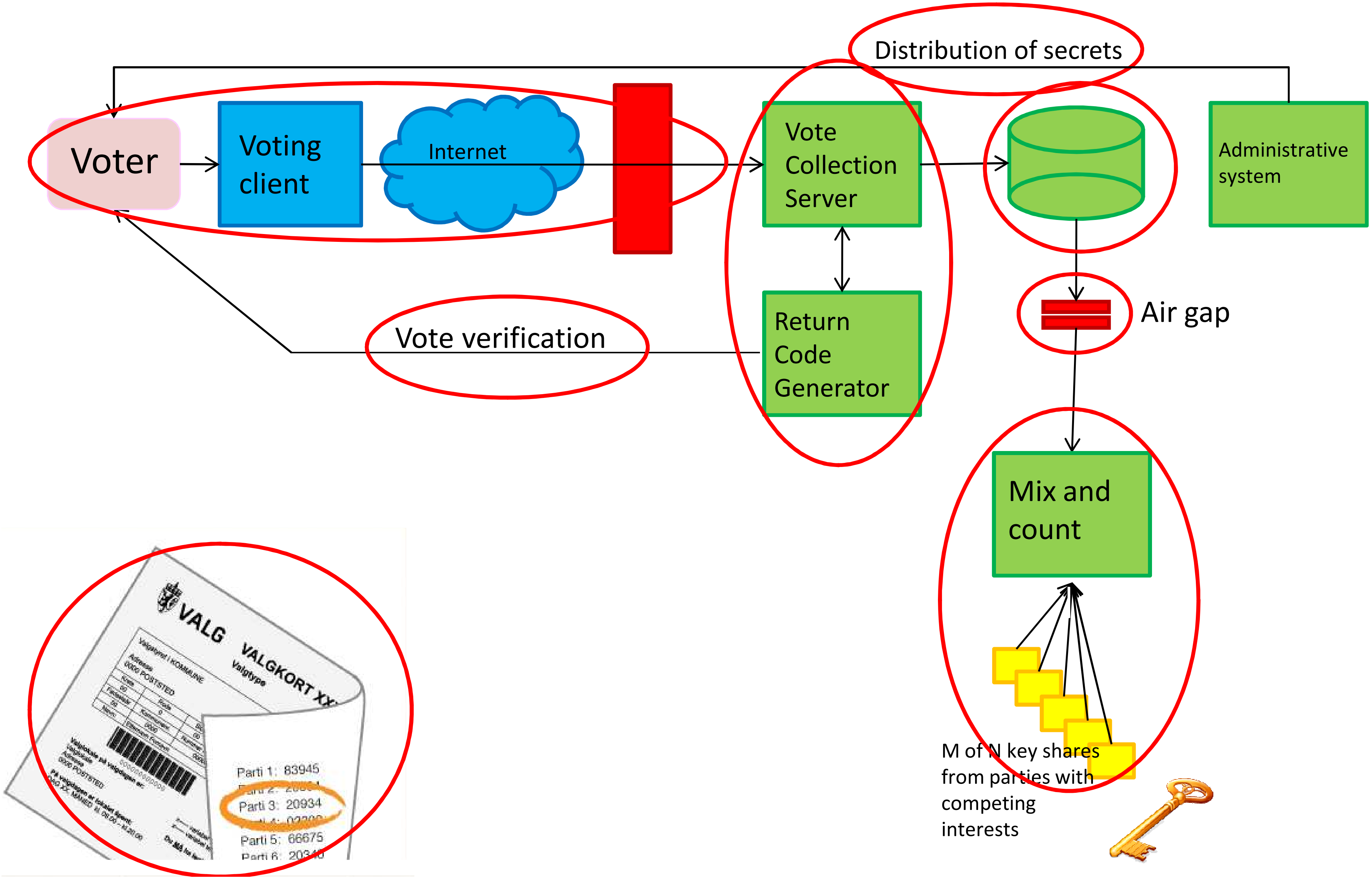
The Challenges of Remote e-voting

- Auditability / transparency to the lay person
- The buying and selling of votes
- Coercion / family voting
- **Home computer security**
- **Anonymity of the vote**
- Attacks *scale,* and there are *externalities*

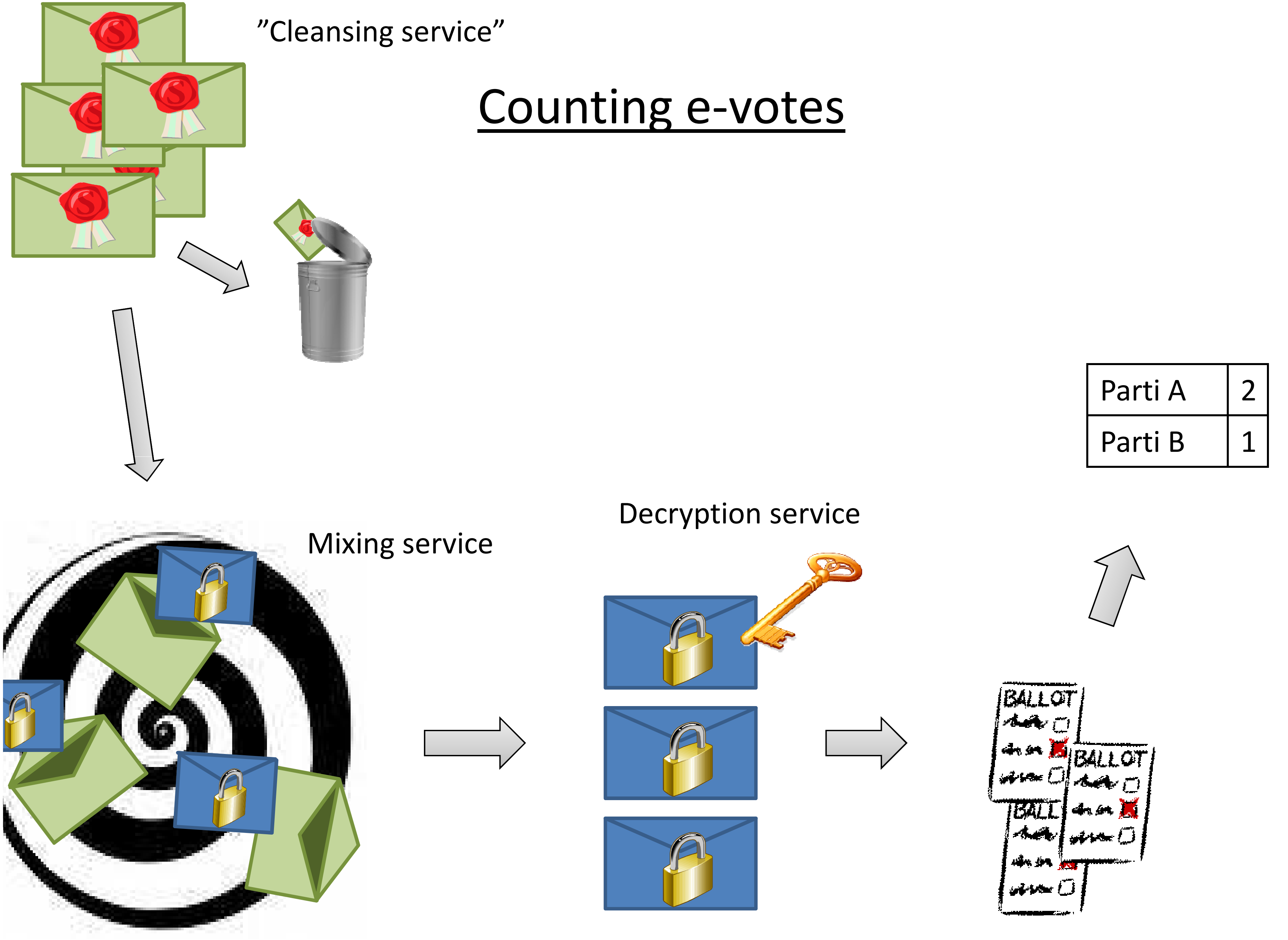
Encryption and storage of the vote



Conceptual model



Counting e-votes



”Cleansing service”

Mixing service

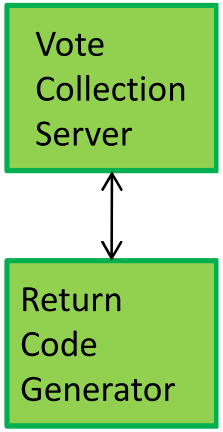
Decryption service

Parti A	2
Parti B	1

Particular challenges of the protocol

- The pre-election sharing of secrets is cumbersome and vulnerable
- Secure channels perhaps not truly secure?
- It will be tricky to decide when to ”pull the plug”
- Key management is key.

The interplay between VCS and RCG



- As previously noted, the VCS and RCG each possess a cryptographic key (K_{VCS} and K_{RCG})
- Thes keys share a relationship:
  - $K_{VCS} + K_{RCG} = K_{EB}$
  - In theory, someone in possession of both K_{VCS} and K_{RCG} key could be able to compromise the private key!
  - While this can certainly be made very tricky with conventional means, we always want to maximize the required conspiracy

The interplay between VCS and RCG

- The two keys are separated logically, geographically and organizationally
  - Logically (obviously) in the VCS and RCG
  - Geographically by 600km as the crow flies (or about 1000km by car) in different data centres
  - Organizationally in two different authorities undrer two different ministries
- The RCG watches the VCS, the public the RCG
  - The VCS *must* send all votes to the RCG, and the RCG *must* generate receipts for all votes

In conclusion – what we believe we’ve achieved

- A fully open source (or ”source available” if you must…) system
- Voter verifiability in remote e-voting
- Near independence of client side (in)security
- Excellent auditability and verifiability
  - Can be improved upon by an N-version architecture

- For more information, see evalg.dep.no
    - Most notably, for the protocol description