Electronic voting promises
- *convenient* way of recording and tallying votes
- *security* against fraud and manipulation
- *transparency* for voters and candidates

It could be used in a variety of kinds of elections
- small committees or on-line communities
- student elections, trade unions, local government
- full national elections

Governments worldwide are investing in e-voting

Electronic systems potentially allow large scale undetectable fraud
- In contrast, fraud in manual systems limited by requirement to generate or dispose of paper, which is quite hard to do undetectably in presence of TV cameras.

There are protocols which are capable of guaranteeing strong properties
- But few companies are marketing them, and few countries are interested in them for their government elections

Some desired properties of e-voting systems

- **1. Accuracy:** the declared outcome corresponds properly to the votes cast.
- **2. Eligibility:** only eligible voters can vote, and only once.
- **3. Fairness:** no early results; i.e. no voter can be influenced by votes already made.

Question: which of these properties does the current UK system provide?

Remark: difference between “assurance” and “cryptographic guarantee”

More desired properties

- **Transparency**
  - **4. Individual verifiability:** a voter can verify that her vote was counted.
  - **5. Universal verifiability:** a voter can verify that the published result is the tally of the votes cast.
Yet more desired properties

- **6. Privacy**
  - no-one can find out how Alice voted.

- **7. Receipt-freeness**
  - Alice doesn’t get a receipt (or any other by-product of the voting process); thus:
  - Alice cannot prove afterwards to a coercer how she voted
  - Thus, *receipt-freeness* is like *privacy*, but even with Alice’s cooperation

- **8. Coercion-resistance**
  - Alice cannot prove how she voted, even if interaction with the coercer is allowed during the voting process
  - Even stronger than *receipt-freeness*.

Coercion-resistance

- Alice interacts with the coercer (e.g. by mobile phone) during the election.

- The coercer can participate in Alice’s vote:
  - She can tell him messages she receives during the process (although he might not believe her)
  - He can instruct her on what messages to send back (although she might not obey).
  - He might have independent means of verifying her reports and her actions

Some “non-functional” requirements

- **9. Robustness:** Voters cannot disrupt the election. Faulty behaviour tolerated.

- **10. Vote-and-go:** Voters participate just once in an election.
US Presidential election 2000 and 2004 employed a variety of “direct recording electronic” (DRE) systems, the dominant supplier of which is Diebold.

- **Proprietary system**, not based on disciplined protocol. Numerous allegations of involvement of equipment supplier with a political party.
- “I voted party p1 and the system said `Thank you, we have recorded your vote for party p2.'” (Radio phone-ins, websites)
- None of our list of desired properties can be guaranteed in any meaningful way.

The current situation in the USA

- Diebold’s code was leaked on the internet.
- Academic computer security researchers Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach wrote a damning critique of it, showing lots of naive assumptions and security risks.
- “15 year old in garage could manufacture cards and sell them on the internet that would allow multiple votes” [Avi Rubin]

The current situation in Estonia

- Tiny former Soviet republic (pop. 1.4M) nicknamed "e-Stonia" because of its tech-savvy population
- Oct 2005 election allowed voters nationwide to cast ballots over the Internet.
- Fewer than 10,000 people (1% of registered voters) participated online.
- Officials hailed the experiment as a success. Said they had received no reports of flaws or hacking attempts. The system is based on Linux.
- Voters need a special ID card, a $24 device that reads the card, and a computer with Internet access. About 80 percent of Estonian voters have the ID cards, also used since 2002 for online access to bank accounts and tax records.
Estonia and coercion-resistance

- Estonian election system allows multiple online votes to be cast by the same person during the days of advance voting, with each subsequent vote cancelling out the previous one.

- The Estonian system still gives priority to paper ballots, so anyone who voted online can also go to a polling station on election day and vote in the traditional way, cancelling out the vote they cast online.

But critics claim no system better than manual voting

- "The benefits don't come anywhere near the risks," said Jason Kitcat, an online consultant and researcher at the University of Sussex in England. "It's a waste of money and a waste of government energy."

- He acknowledged that Estonia's system was the most secure to date but said no system was "good enough for a politically binding election."

Electronic voting protocols

- The systems used in the USA and other countries are based on proprietary code
  - Therefore, it is impossible to investigate the properties of those systems properly

- Some systematic protocols exist
  - The protocols can be systematically evaluated in terms of whether they satisfy properties.
  - Systems can be implemented that comply with the protocols.

[FujiokaOkamotoOhta1992]

"Check out the world's most high-tech cabinet room. This e-cabinet doesn't just look cool. It is cool – and it promotes efficiency and saves money, too." Newsweek, March 11, 2002
- Blind signatures
  - To guarantee privacy
- Commitment
  - To guarantee fairness
- Three phases
  - To avoid traffic analysis attacks

**Simplified [LBDKYY’03]**

- Uses re-encryption and designated verifier proofs.
- Re-encryption
  - Randomised encryption: \(\{m\}_K\) contains “random coins”
  - Re-encryption: change the random coin
    - E.g., in El Gamal, the ciphertext \((x,y)\) is changed to \((xg',yh')\).
- Designated verifier proofs
  - \(S\) can prove to \(A\) that, say, \(c\) is the encryption of \(m\), but \(A\) cannot use this proof to convince someone else.
  - Technically this is achieved by giving \(A\) the ability to simulate transcripts of the proof

**Cryptographic guarantees of**

- privacy (link between voter and vote kept secret)
- fairness (no early results)
  - even if the election officials are corrupt.

**does not satisfy**

- vote-and-go
- coercion resistance

---

**Simplified [LBDKYY’03]**

```
Alice

\[\text{Sign} \left( v_{\text{Coll}, \text{Alice}}^r \right) \]

\[\text{reencrypt} \]

\[\text{Sign} \left( v_{\text{Coll}, \text{Admin}}^{r_2} \right) \]

\[\text{DVP} \left[ v_{\text{Coll}, \text{Admin}}^{r_1} = v_{\text{Coll}, \text{Admin}}^{r_2} \right] \]

\[\text{Sign} \left( v_{\text{Coll}, \text{Admin}}^{r_1} \right) \]

Collector

Trusted smartcard
```
Simplified [LBDKYY’03]

- Cryptographic guarantees of
  - privacy (link between voter and vote kept secret)
  - fairness (no early results)
  - receipt-freeness (like coercion resistance, but assuming passive attacker)
    even if the election officials are corrupt.
- also satisfies
  - vote-and-go
- does not satisfy
  - coercion resistance

Where will it go from here?

- Stakes very high. Powerful players. American experience gives plenty of cause for concern. Estonian experience significantly better.
- Apparently no real effort at using strong protocols.
- Ron Rivest is leading a standards initiative in the USA. Might not result in anything, but ....
- David Chaum a passionate believer in citizen empowerment, and sells (or used to sell) voting systems through his company Votegrity.

[Chaum P.Ryan Schneider 2005]