# Comment voter par Internet en toute sécurité ... ou pas ?

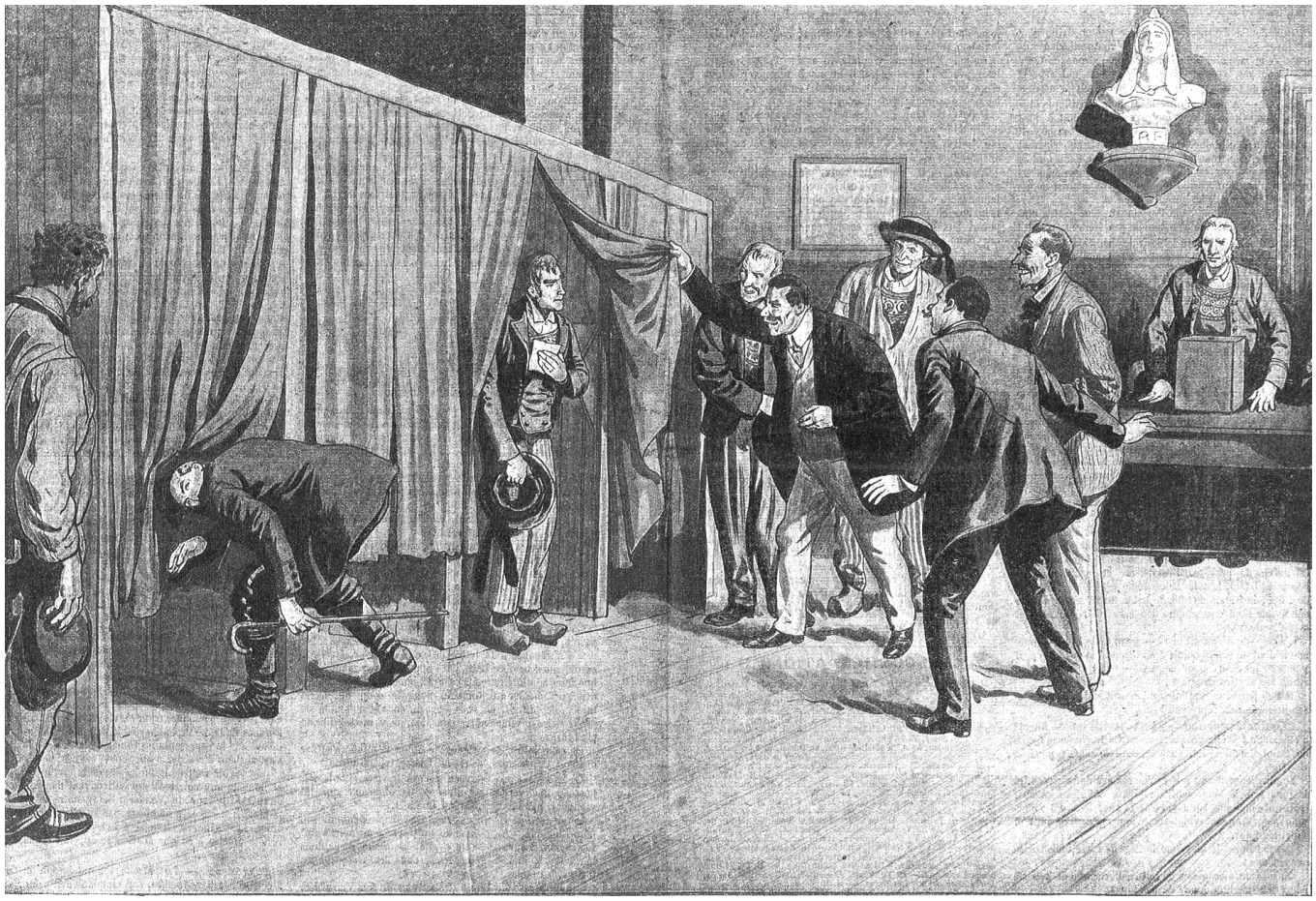
Steve Kremer

LORIA & Inria Nancy - Grand'Est

**Maths en mouvement:**
**le vote à la loupe**
11 juin 2022 – Paris

# The County Election, 1852 by George Caleb Bingham

# The need for privacy



*Premières expériences d'isoloir (appelé cabine d'isolement) aux élections municipales, en Bretagne. Caricature de Damblans, dans Le Pélerin, 23 novembre 1913.*

# Internet elections

**Political legally binding Internet elections** in Europe:

- parliamentary elections in **Switzerland** (several cantons)
- parliamentary election in **Estonia** (all eligible voters)
- municipal and county elections in **Norway** (selected municipalities, selected voter groups)
- parliamentary elections in in **France** ("expats")

But also **banned in Germany, Ireland, UK**

Even more **professional elections**

# E-voting

Essential **security properties** of (e-)voting:

- **Integrity** of the election
- **Secrecy** of the vote

# E-voting

Essential **security properties** of (e-)voting:

- **Integrity** of the election
- **Secrecy** of the vote

**Warning:**

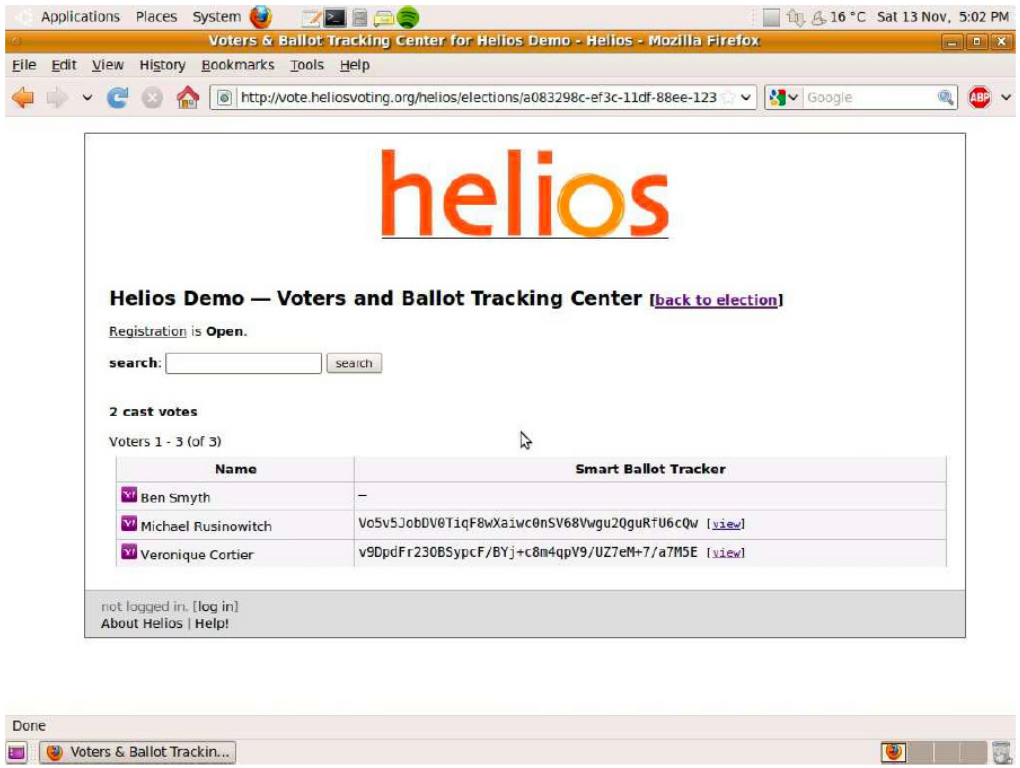
With Internet voting (like any remote voting) there is no private voting booth!

**Cryptographic protocols to the rescue?**

# The Helios e-voting protocol

Verifiable online elections via the Internet

http://heliosvoting.org/




Already in use:

- Election at Louvain University Princeton
- Election of the IACR board (major association in Cryptography)

Designed for low-coercion environments (not receipt-free).

# Crypto toolbox: public-key cryptography

Two keys:

- public encryption key
- private decryption key

# Crypto toolbox: public-key cryptography

Two keys:

- public encryption key
- private decryption key

Based on the notion of **one-way function**:

$f$ : easy to compute $\qquad$ $f^{-1}$ : hard to compute

# Crypto toolbox: public-key cryptography

Two keys:

- public encryption key
- private decryption key

Based on the notion of **one-way function**:

$$f: \text{ easy to compute} \qquad f^{-1}: \text{ hard to compute}$$

**Examples:**

- The discrete logarithm problem (ElGamal encryption)
  For a generator $g$ of a cyclic group: $f(a) = g^a$
- Factoring (RSA encryption)
  Given two (large) primes $p$ and $q$: $f(p, q) = p \times q$

# Behavior of Helios (simplified)

## Phase 1: voting


**Bulletin Board**

| | | |
|---|---|---|
| Alice | $\{v_A\}_{pk(E)}$ | $v_A = 0$ or $1$ |
| Bob | $\{v_B\}_{pk(E)}$ | $v_B = 0$ or $1$ |
| Chris | $\{v_C\}_{pk(E)}$ | $v_C = 0$ or $1$ |

# Behavior of Helios (simplified)

## Phase 1: voting


$\{v_D\}_{pk(E)} \longrightarrow$

**Bulletin Board**

| | | |
|---|---|---|
| Alice | $\{v_A\}_{pk(E)}$ | $v_A = 0$ or $1$ |
| Bob | $\{v_B\}_{pk(E)}$ | $v_B = 0$ or $1$ |
| Chris | $\{v_C\}_{pk(E)}$ | $v_C = 0$ or $1$ |

$pk(E)$: election public key

# Behavior of Helios (simplified)

## Phase 1: voting


| Bulletin Board | | |
|---|---|---|
| Alice | $\{v_A\}_{pk(E)}$ | $v_A = 0$ or $1$ |
| Bob | $\{v_B\}_{pk(E)}$ | $v_B = 0$ or $1$ |
| Chris | $\{v_C\}_{pk(E)}$ | $v_C = 0$ or $1$ |
| David | $\{v_D\}_{pk(E)}$ | $v_D = 0$ or $1$ |

$pk(E)$: election public key

# Behavior of Helios (simplified)

## Phase 1: voting


**Bulletin Board**

| | | |
|---|---|---|
| Alice | $\{v_A\}_{pk(E)}$ | $v_A = 0$ or $1$ |
| Bob | $\{v_B\}_{pk(E)}$ | $v_B = 0$ or $1$ |
| Chris | $\{v_C\}_{pk(E)}$ | $v_C = 0$ or $1$ |
| David | $\{v_D\}_{pk(E)}$ | $v_D = 0$ or $1$ |
| ... | ... | |

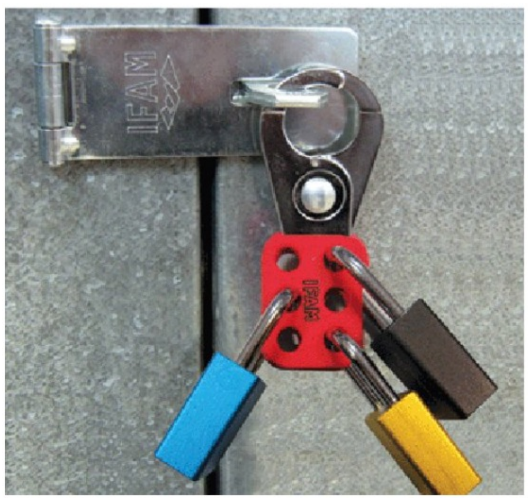
$pk(E)$: election public key

# Behavior of Helios (simplified)

## Phase 1: voting


| Bulletin Board | | |
|---|---|---|
| Alice | $\{v_A\}_{pk(E)}$ | $v_A = 0$ or $1$ |
| Bob | $\{v_B\}_{pk(E)}$ | $v_B = 0$ or $1$ |
| Chris | $\{v_C\}_{pk(E)}$ | $v_C = 0$ or $1$ |
| David | $\{v_D\}_{pk(E)}$ | $v_D = 0$ or $1$ |
| ... | ... | |

$pk(E)$: election public key; private key shared among trustees.




# Behavior of Helios (simplified)

## Phase 1: voting


| Bulletin Board | | |
|---|---|---|
| Alice | $\{v_A\}_{pk(E)}$ | $v_A = 0$ or $1$ |
| Bob | $\{v_B\}_{pk(E)}$ | $v_B = 0$ or $1$ |
| Chris | $\{v_C\}_{pk(E)}$ | $v_C = 0$ or $1$ |
| David | $\{v_D\}_{pk(E)}$ | $v_D = 0$ or $1$ |
| ... | ... | |

## Phase 2: Tallying using homomorphic encryption (El Gamal)

$$\prod_{i=1}^{n} \{v_i\}_{pk(E)} = \{\sum_{i=1}^{n} v_i\}_{pk(E)}$$

based on $g^a * g^b = g^{a+b}$

$\rightarrow$ Only the final result needs to be decrypted!

$pk(E)$: election public key; private key shared among trustees.

# This is oversimplified!


| Bulletin Board | |
|---|---|
| Alice | $\{v_A\}_{pk(E)}$ |
| Bob | $\{v_B\}_{pk(E)}$ |
| Chris | $\{v_C\}_{pk(E)}$ |
| David | $\{v_D\}_{pk(E)}$ |
| ... | ... |

$v_A = 0$ or 1

$v_B = 0$ or 1

$v_C = 0$ or 1

**Result**: $\{v_A + v_B + v_C + v_D + \cdots\}_{pk(E)}$

# This is oversimplified!


| Bulletin Board | | |
|---|---|---|
| Alice | $\{v_A\}_{pk(E)}$ | $v_A = 0$ or $1$ |
| Bob | $\{v_B\}_{pk(E)}$ | $v_B = 0$ or $1$ |
| Chris | $\{v_C\}_{pk(E)}$ | $v_C = 0$ or $1$ |
| David | $\{v_D\}_{pk(E)}$ | $v_D = 100$ |
| ... | ... | |

**Result**: $\{v_A + v_B + v_C + 100 + \cdots\}_{pk(E)}$

A malicious voter can cheat!

# This is oversimplified!


| Bulletin Board | | |
|---|---|---|
| Alice | $\{v_A\}_{pk(E)}$ | $v_A = 0$ or $1$ |
| Bob | $\{v_B\}_{pk(E)}$ | $v_B = 0$ or $1$ |
| Chris | $\{v_C\}_{pk(E)}$ | $v_C = 0$ or $1$ |
| David | $\{v_D\}_{pk(E)}$ | ~~$v_D = 100$~~ |
| ... | ... | |

**Result**: $\{v_A + v_B + v_C + v_D + \cdots\}_{pk(E)}$

~~A malicious voter can cheat!~~

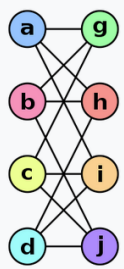
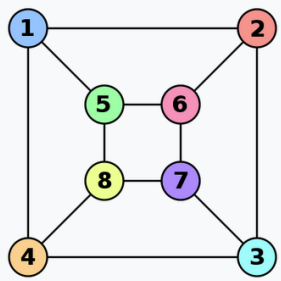
In Helios: use Zero Knowledge Proof

$$\{v_D\}_{pk(E)}, \text{ZKP}\{v_D = 0 \text{ or } 1\}$$

# Crypto toolbox: zero-knowledge proofs

**Goal**: provide the proof of the truth of a statement, without conveying any information except that the statement is indeed true

**Example:**

| Graph G | Graph H | An isomorphism between G and H |
|---|---|---|
|  |  | $f(a) = 1$<br>$f(b) = 6$<br>$f(c) = 8$<br>$f(d) = 3$<br>$f(g) = 5$<br>$f(h) = 2$<br>$f(i) = 4$<br>$f(j) = 7$ |





Deciding whether 2 graphs are isomorphic is computationally hard (NP-complete)

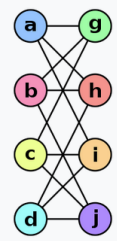
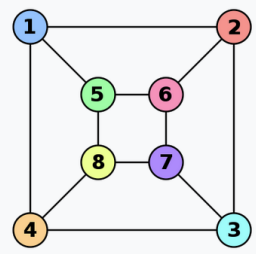
How can I prove that I know the isomorphism between G and H without revealing any information about the solution?

# Crypto toolbox: zero-knowledge proofs

**Goal**: Alice wants to prove to Bob that she knows the isomorphism $f$ (without revealing $f$)

**Example:**

1. Alice generates a random $f_1$ and computes $I = f_1(G)$. From $f$ and $f_1$ compute $f_2$ such that $f_2(H) = I$.
2. Alice sends $I$ to Bob.
3. Bob randomly chooses $i \in \{1, 2\}$ and sends $i$ to Alice.
4. Alice reveals $f_i$ and Bob checks $f_i(G) = H$

| Graph G | Graph H | An isomorphism between G and H |
|---|---|---|
|  |  | $f(a) = 1$<br>$f(b) = 6$<br>$f(c) = 8$<br>$f(d) = 3$<br>$f(g) = 5$<br>$f(h) = 2$<br>$f(i) = 4$<br>$f(j) = 7$ |



$$G \xrightarrow{f_1} I \xleftarrow{f_2} H$$

**Alice can cheat with probability $\frac{1}{2}$ by "guessing" the value of $i$.**

**Iterate $n$ times and reduce probability to $\frac{1}{2^n}$**

# Vote privacy in Helios?


| Bulletin Board | | |
|---|---|---|
| Alice | $\{v_A\}_{pk(S)}$ | $v_A = 0$ or $1$ |
| Bob | $\{v_B\}_{pk(S)}$ | $v_B = 0$ or $1$ |

# Vote privacy in Helios?


$\{v_A\}_{pk(S)} \longrightarrow$

| Bulletin Board | | |
|---|---|---|
| Alice | $\{v_A\}_{pk(S)}$ | $v_A = 0$ or $1$ |
| Bob | $\{v_B\}_{pk(S)}$ | $v_B = 0$ or $1$ |
| Chris | $\{v_A\}_{pk(S)}$ | |

**Replay attack** break vote privacy:
Alice must have voted for the winner!

# From Helios to Belenios

Helios does not guarantee **Eligibility verifiability**

$\rightsquigarrow$ **ballot stuffing** possible by dishonest Bulletin Board

# From Helios to Belenios

Helios does not guarantee **Eligibility verifiability**

$\rightsquigarrow$ **ballot stuffing** possible by dishonest Bulletin Board


**Belenios**: variant of Helios

- introduce credential issuer
- public credentials allow to verify eligibility
- private credentials necessary to vote (unknown to Bulletin Board)

Developed in the LORIA lab at Nancy.

Supports different tally methods: $k$-out-of-$n$, Condorcet, Majority Judgment, ...

`https://www.belenios.org/`

# How do I know whether my voting system is secure?

# How do I know whether my voting system is secure?

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

**Chancellerie fédérale ChF**
Section des droits politiques

13 décembre 2013

**Exigences techniques et administratives applicables au vote électronique**

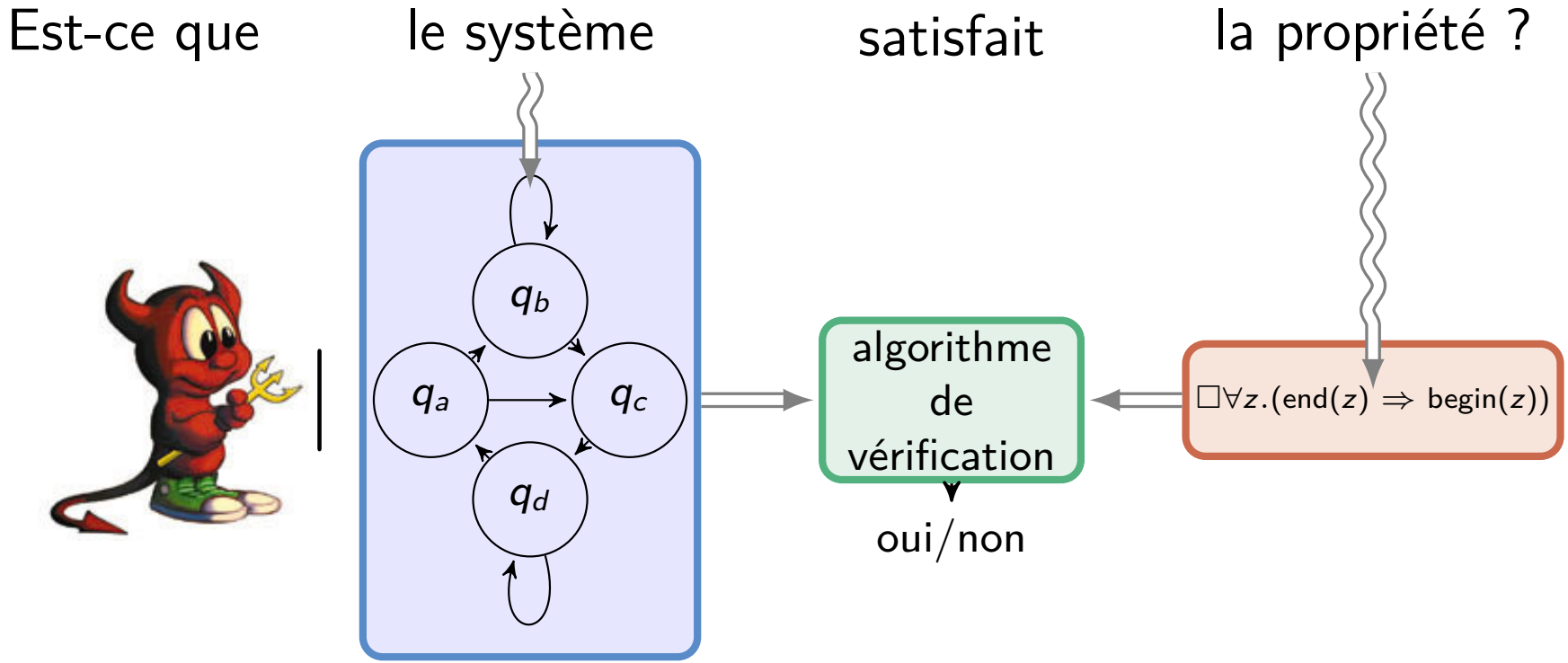
**Entrée en vigueur: 15 janvier 2014**

V. 1.0

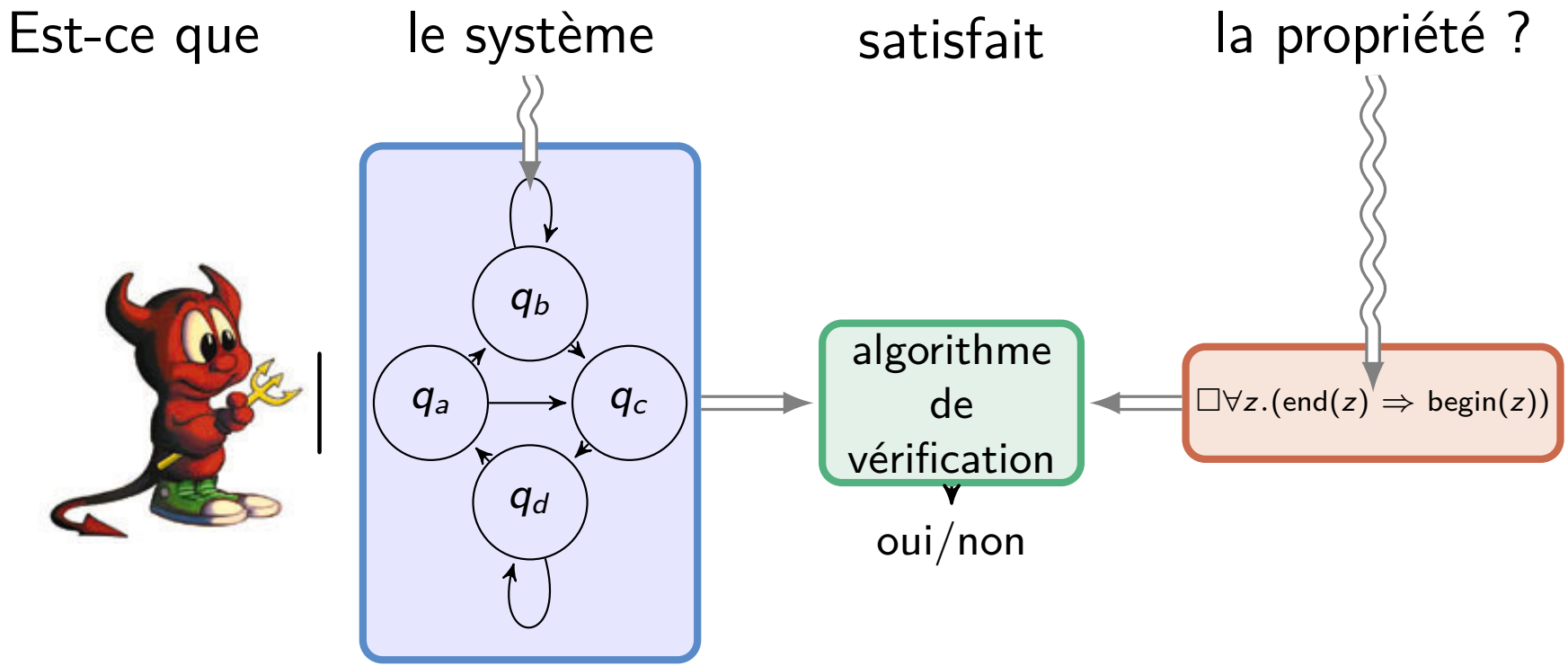
## 5.1. Contrôle du protocole cryptographique

| | |
|---|---|
| 5.1.1 | Critères de contrôle: le protocole doit être conforme à l'objectif de sécurité et aux hypothèses de confiance figurant dans le modèle abstrait décrit au ch. 4. Pour cela, il doit exister une preuve cryptographique et une preuve symbolique. En ce qui concerne les composants cryptographiques fondamentaux, les preuves peuvent être apportées sur la base des hypothèses de sécurité généralement admises (par exemple « random oracle model », « decisional Diffie-Hellman assumption » et « Fiat-Shamir heuristic »). Le protocole doit se fonder si possible sur des protocoles éprouvés. |

# Symbolic protocol verification



# Symbolic protocol verification

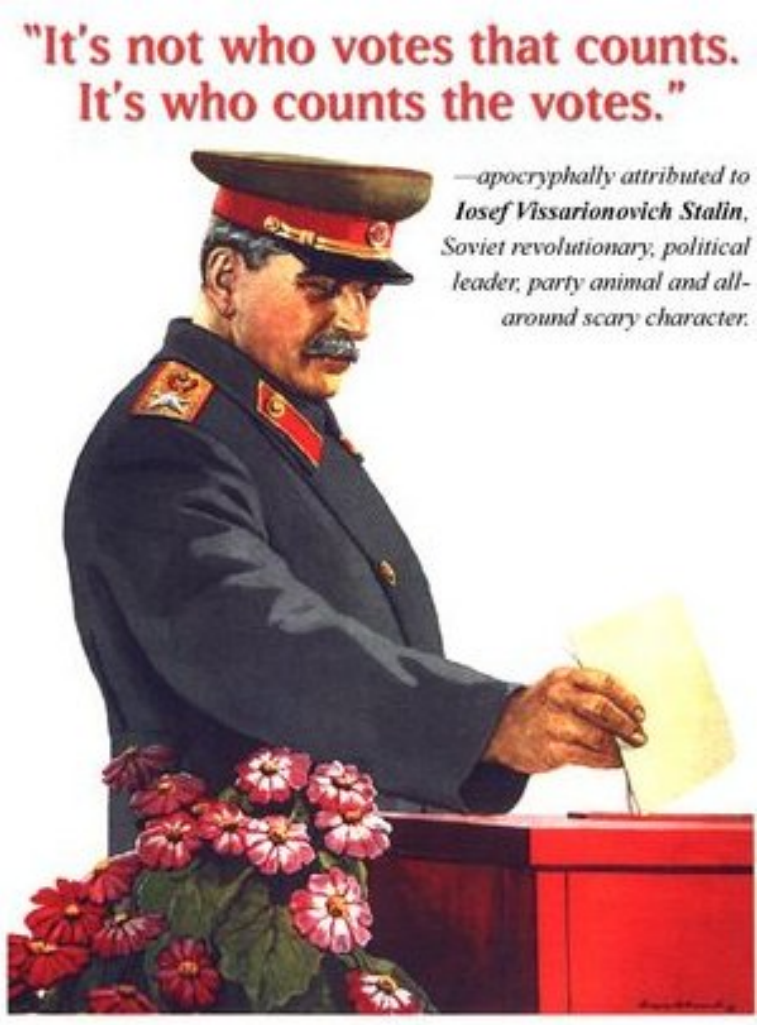



**Difficultés** : attaquant arbitraire contrôlant entièrement le réseau

**Techniques** : déduction automatique, logique du premier ordre, model-checking, théorie de la concurrence, ...

# Conclusion

- Voting through the Internet is a form of **remote voting**
- **Distribution of credentials** (login/password) is a sensitive procedure (above all if no existing infrastructure)
- Good **privacy** and **verifiability** guarantees if client is trusted
  $\rightsquigarrow$ **malware resistance** an active research topic
- **Receipt-freeness** / **coercion-resistance** can be achieved but solutions are generally complicated
- **In cryptography we trust?**
  $\rightsquigarrow$ complicated procedures – need to **trust experts**


"It's not who votes that counts.
It's who counts the votes."
—apocryphally attributed to
Iosef Vissarionovich Stalin,
Soviet revolutionary, political
leader, party animal and all-
around scary character.

# Questions?