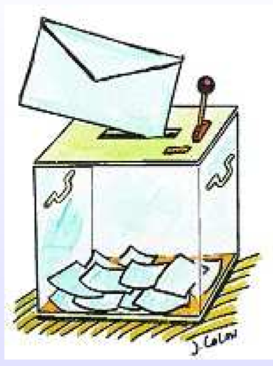


FORMAL ANALYSIS OF E-VOTING PROTOCOLS

AVOTÉ Project

France Telecom R&D - Loria - LSV - Verimag

http://www.lsv.ens-cachan.fr/Projects/anr-avote/

Elections are a cornerstone of modern democracies. In 2011, legally binding Internet voting was offered for parliamentary elections in Estonia and Switzerland, for municipal and county elections in Norway. In 2008, France changed its constitution to allow French expatriates to vote electronically.

Issues

Security properties.

Privacy: Secrecy of individual votes.

Coercion-resistance: A voter cannot prove to a coercer how he voted.

Individual and universal verifiability: Voters can check that their vote was counted. Anyone can check the accuracy of the tally.

Complex primitives.

Blind signatures: a server can sign without knowing the content

$$\mathsf{unblind}(\mathsf{sign}(\mathsf{blind}(m,s),sk),s) = \mathsf{sign}(m,sk)$$

Re-encryption: encryption can be re-randomized

$$\mathsf{reencrypt}(\mathsf{enc}(m,k,r),r') = \mathsf{enc}(m,k,f(r,r'))$$

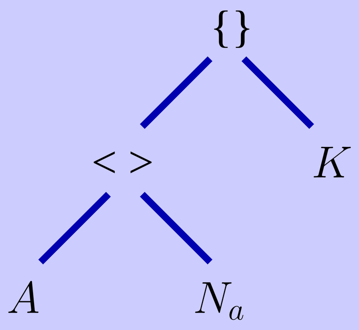
Homomorphic encryption: counting without decrypting ballots

$$\{v_1\}_{\mathsf{pk}(S)} * \{v_1\}_{\mathsf{pk}(S)} = \{v_1+v_2\}_{\mathsf{pk}(S)}$$

Accurracy of the models.

Symbolic models

- messages are represented by terms
- amenable to automation (decidability results, tools)



Computational models

- messages are bitstrings, adversaries are polynomial probabilistic Turing machines
- very accurate model

10101111101101
11110000110101
10111010101000

Results

Formalisation of security properties.

A voting system ensures **privacy** if an adversary cannot notice when two votes are swapped.

$$A(yes) \mid B(no) \approx A(no) \mid B(yes)$$

Receipt freeness and coercion-resistance can also be formally defined based on **process equivalences in the applied-pi calculus**.

Definitions for universal, individual, and eligibility verifiability.

Decidability results.

Static equivalence: families of convergent equational theories (including re-encryption, trapdoor commitment, . . .)

Equivalence of processes: families of convergent theories but no else branch; fixed standard signature with else branch

Soundness results.

Theorem: *security in symbolic models implies security in computational ones*

This result has been established in various contexts (static and active equivalences) and various primitives (symmetric encryption, bilinear pairing, hash functions, ...)

Automated proofs of generic constructions of encryption schemes.

Automatic tools.

Static equivalence

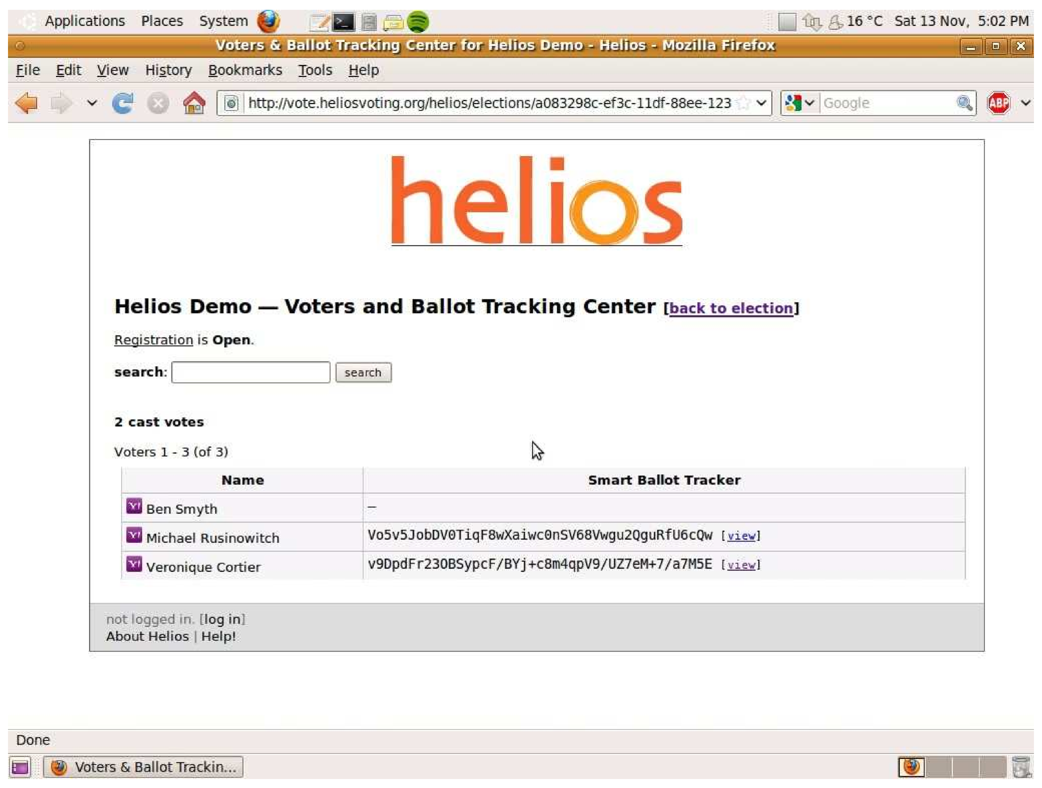
YAPA & KISS: families of subterm, equational theories (including blind signatures, trapdoor commitment, . . .)

Equivalence of processes

- ADECS: fixed theory (encryption, signatures and hash)
- AKISS: convergent theories, termination not guaranteed

Case studies.

Helios is an open-source web-based e-voting system, suitable for low-coercion environments. It has already been deployed in several important elections: the International Association of Cryptologic Research used Helios to elect its board members; University of Louvain adopted the system to elect the university president; Princeton University used Helios to elect the student vice president.



→ **Breach of privacy** (a voter was able to re-use a published ballot)
→ Proposition of a **fixed version**
→ **Formal proof** of privacy, individual and universal verifiability

We have also studied a **postal voting system** designed by a French company (Tagg Informatique) and used by the CNRS. The system was making use of barcodes to facilitate the tallying phase. We discovered that is was subject to major ballot stuffing. Our attack was confirmed by the CNRS election service and a new system has been designed by Tagg Informatique.

France Telecom (until Sept. 2008): Francis Klay (**local coordinator**), Jacques Traoré, Camille Vacher
LORIA : Mathilde Arnaud, Stefan Ciobaca, Véronique Cortier (**coordinator**), Mounira Kourjieh, Ben Smyth, Laurent Vigneron
LSV : Mathilde Arnaud, Gergei Bana, Sergiu Bursuc, Vincent Cheval, Stefan Ciobaca, Hubert Comon-Lundh, Stéphanie Delaune, Florent Jacquemard, Steve Kremer (**local coordinator**), Antoine Mercier, Camille Vacher
Verimag : Scott Cotton, Judicaël Courant, Cristian Ene, Florent Garnier, Pascal Lafourcade (**local coordinator**), Yassine Lakhnech, Jean-François Monin