

(In)Security of e-voting



Pascal Lafourcade



FIC 2023, April 2023

E-voting a reality



The screenshot shows the top section of a Le Monde article. At the top left, there is a small icon and the text 'Consulter le journal'. The Le Monde logo is centered at the top. To the right, there are links for 'Se connecter' and 'S'abonner'. Below the logo is a navigation bar with categories: ACTUALITÉS, PRÉSIDENTIELLE 2022, ÉCONOMIE, VIDÉOS, DÉBATS, CULTURE, M LE MAG, SERVICES, and a search icon. The article title is 'Elections régionales 2021 : le vote électronique, remède à l'abstention?'. Below the title is a sub-header 'LES DÉCODEURS' and 'RÉGIONALES | DÉPARTEMENTALES'. The main text starts with 'Après un premier tour marqué par une abstention historique, des membres de la majorité ont appelé à moderniser les scrutins, pour voter plus facilement, et donc de mobiliser davantage les électeurs.' The author is 'Par Assma Maad et Clément Perruche'. At the bottom, it says 'Publié le 25 juin 2021 à 18h40 - Mis à jour le 26 juin 2021 à 10h42 - Lecture 7 min.' There are also social media sharing icons.

Consulter le journal

Le Monde

Se connecter S'abonner

ACTUALITÉS PRÉSIDENTIELLE 2022 ÉCONOMIE VIDÉOS DÉBATS CULTURE M LE MAG SERVICES

LES DÉCODEURS RÉGIONALES | DÉPARTEMENTALES

Elections régionales 2021 : le vote électronique, remède à l'abstention ?

Après un premier tour marqué par une abstention historique, des membres de la majorité ont appelé à moderniser les scrutins, pour voter plus facilement, et donc de mobiliser davantage les électeurs.

Par Assma Maad et Clément Perruche

Publié le 25 juin 2021 à 18h40 - Mis à jour le 26 juin 2021 à 10h42 - Lecture 7 min.

Hauts-De-Seine : Neuilly-Sur-Seine Met En Place Un Système De Vote Électronique

On **Juil 5, 2021**

Le vote électronique fera son retour en 2022



Après la découverte de failles en 2019, tous les projets de scrutin en ligne ont été suspendus. La Poste a cependant poursuivi l'aventure. Elle développe à Neuchâtel un système mieux sécurisé qu'elle soumettra à des hackers

Flaws in E-voting a reality

TECH > VIE NUMÉRIQUE

SUISSE: UNE FAILLE DE SÉCURITÉ "MAJEURE" DANS LE SYSTÈME DE VOTE EN LIGNE

Raphaël Grably Le 13/03/2019 à 11:10



NEWS

Flaw in NSW's iVote platform confirmed by researcher



By Rohan Pearce

Editor, Computerworld | NOV 14, 2019 6:08 AM PST

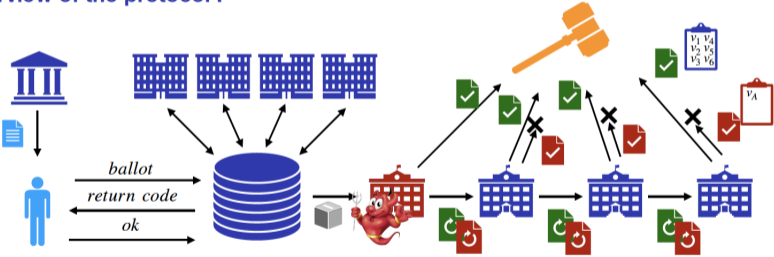
A security researcher has confirmed that the version of New South Wales' online voting platform, iVote, employed during the 2019 election contained a vulnerability that potentially allowed the creation of false decryption proofs for ballots.

Swiss Post Attack (Bug Bounty 40Keuros)

A privacy attack against Swiss-Post protocol

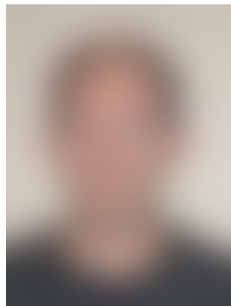


Overview of the protocol :



Cortier et al. RWC'22

Le Vote électronique



De Pierrick GAUDRY, Véronique CORTIER
256 pages, Odile Jacob 18/05/2022

Outline

Motivations

Formal Methods

e-voting

Some Attacks

- Sicilian

- Vote Copy

- Cryptographic Flaw

- Clash

- Machine Bugs

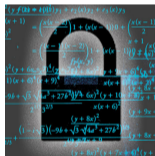
Conclusion

Cryptography



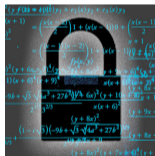
Cryptography

Primitives
RSA, Elgamal,
AES, DES, SHA-3...



Cryptography

Primitives
RSA, Elgamal,
AES, DES, SHA-3...



Protocols
Distributed
Programs

Security: Cryptography for a Property in an Hostile Environment



TOP SECRET



Cryptography



Primitives
RSA, Elgamal,
AES, DES, SHA-3...



Protocols
Distributed
Programs



Security: Cryptography for a Property in an Hostile Environment



TOP SECRET

Primitives
RSA, Elgamal,
AES, DES, SHA-3...



Cryptography Verification



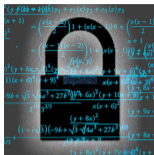
Protocols
Distributed
Programs



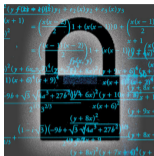
Why Verification is Useful !



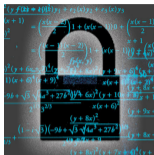
Formal Security Verification Team



Formal Security Verification Team



Formal Security Verification Team



Formal Security Verification Team



Outline

Motivations

Formal Methods

e-voting

Some Attacks

Sicilian

Vote Copy

Cryptographic Flaw

Clash

Machine Bugs

Conclusion

E-Voting vs Traditional Voting



Vote électronique



Vote traditionnel

- + Accessibility
- + Reducing the abstention rate
- + Automatic counting
- + Less organisation costs

Two e-voting (1/2)

Offline

- + Efficient and fast counting
- + Vote in any voting station
 - Trust the machines



Two e-voting (2/2)

Online

- + Vote at home
- + Easy process
- + Less costs
 - Possible influence



Voting Protocol Organisation

5 Phases

1. Registration
2. Validation
3. Vote
4. Counting
5. Verification

Register
to **VOTE**





Security Requirements



Eligibility



Fairness



Universal Verifiability

Individual Verifiability



Secure e-voting protocol



Correctness

Coercion-Resistance

Privacy

Robustness



Receipt-Freeness



Eligibility

Only the registered voters can vote



Prevent double voting

Robustness



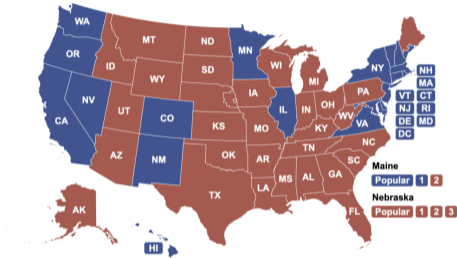
Tolerate a certain number of misbehaving voters

Correctness



Results should be correct

Fairness



No preliminary results

Individual Verifiability



Each voter can check whether his vote was counted correctly

Universal Verifiability



Anybody can verify that the announced result corresponds to the sum of all votes

Anonymity

Privacy: unlinkability between the voter and his vote



Receipt-Freeness: A voter cannot construct a receipt



Corecion-Resistance: A coercer cannot be sure the voter followed his instructions



Privacy implies Individual Verifiability

2018 Cortier et al.























A system without Individual Verifiability cannot achieve privacy !

Reduction Results: How many agents ?



- ▶ Security properties: **two** agents are sufficient.
2004 by Hubert Comon-Lundh, Véronique Cortier
- ▶ When Are **Three Voters** Enough for Privacy Properties?
2016 by Myrto Arapinis, Véronique Cortier, Steve Kremer

Security Trust Assumptions for Belenios

	 Voter	 Vote Client	 Registrar	 Voting Server	 Decryption Trustees	 Bulletin Board
 Vote Secrecy					 k out of n	
 Verifiability						

Outline

Motivations

Formal Methods

e-voting

Some Attacks

- Sicilian

- Vote Copy

- Cryptographic Flaw

- Clash

- Machine Bugs

Conclusion

Sicilian Attack

Arlette
François
Emanuel
Marine
Jean-Luc
Arnaud
Ségolène
Jacques
Georges
Charles
Jean-Marie
Valérie

With 12 candidates, > 479 millions possible combinations!

> 2,000,000 votes have been cast

helios
Trust the vote.

<https://vote.heliosvoting.org/>

Helios code is Open Source
Based on scientific papers
Use mixnet

By V. Cortier et al in 2010

Replaying a voter's ballot

- ▶ Alice votes A
- ▶ Bob votes B
- ▶ Charlie votes like Alice

This attack works on other protocols like Lee et al and Sako et al.



<https://www.belenios.org/>
Belenios code is Open Source

Russian Online Election



In 2019, Breaking the encryption scheme of the Moscow Internet voting system by P. Gaudry et al

- ▶ Elgamal key sizes are too small (CADO-NFS)
- ▶ Counting the number of votes cast for a candidate.



1994 Benaloh's Scheme

$$\text{enc}(a, pk_S) * \text{enc}(b, pk_S) = \text{enc}(a + b, pk_S)$$

Partial homomorphic are widely used in voting schemes

$$\prod \text{enc}(v_i, pk_S) = \text{enc}(\sum v_i, pk_S)$$



Original Benaloh's scheme is ambiguous

$$\text{dec}(\text{enc}(14, pk_S), sk_S) = 14 \pmod{15} \text{ or } 14 \pmod{5} = 4$$

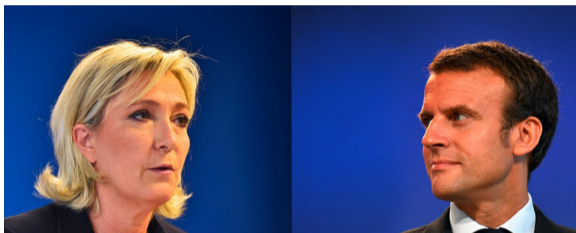
Revisited Benaloh's encryption [FLA'11]

- ▶ Drawing false parameters: 33%
- ▶ Proposition of corrected version
- ▶ Proof using Kristian Gjosteen result.



Impact

Example with 15 voters



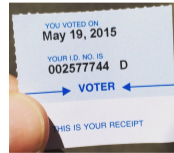
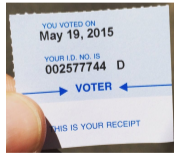
$\{0\}_{pk_S}$

$\{1\}_{pk_S}$

- ▶ $\prod enc(v_i, pk_S) = enc(\sum v_i, pk_S) = enc(14, pk_S)$
- ▶ Result can be either 14 or 4

Clash Attack on the verifiability of e-voting systems

By 2012 Kuesters et al.



Different voters with the same receipt
⇒ Authorities can manipulate the election without being detected

Attacks



- ▶ In 2007, Security Analysis of the Diebold AccuVote-TS Voting Machine
- ▶ In 2012, Attacking the Washington, D.C. Internet Voting System
- ▶ In 2017 Voting Machine Hacking Village by Matt Blaze et al.

Machines :

- ▶ AVS WinVote DRE
- ▶ Premier AccuVote TSx DRE
- ▶ ES&S iVotronic DRE
- ▶ PEB version 1.7c-PEB-S
- ▶ Sequoia AVC Edge DRE
- ▶ Diebold Express Poll 5000 electronic pollbook

With limited resources and information, they can be hacked.

Outline

Motivations

Formal Methods

e-voting

Some Attacks

- Sicilian

- Vote Copy

- Cryptographic Flaw

- Clash

- Machine Bugs

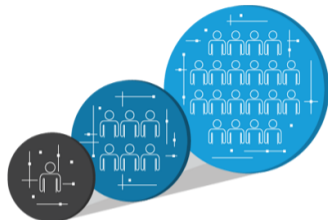
Conclusion

Summary



- ▶ Voting is important for democracy
- ▶ Protocols must be open
- ▶ Design of voting protocols is not easy
- ▶ Formal Verification can help
- ▶ Proving all properties together is difficult

Future Work



- ▶ Scalability
- ▶ Human aspect are not yet taken into account
- ▶ End-to-end verification
- ▶ All properties in one tool !

Thank you for your attention.

