An introduction to electronic voting
Application to single transferable vote

Orange Labs

Jacques Traoré

21 June 2016

COST Action IC1205 Industry Day

Outline

- Context
- Problematic / Security issues
- Some challenges in Electronic Voting
- Introduction to public-key cryptography (short and non-technical)
- Recent breakthroughs in electronic voting
- Conclusion

1 Context

Definition

- E-election or e-referendum: a political election or referendum in which electronic means are used in one or more stages.

- E-voting: an e-election or e-referendum that involves the use of electronic means in at least the casting of the vote (entering the vote in the ballot box)
  - Recommendation of the Council of Europe: «Legal,Operational and Technical Standards for E-voting» , 30 September 2004

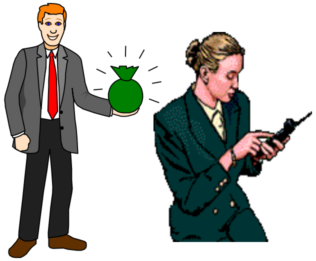
- The other phases (registration on the electoral roll, identification/authentication of elligible voters) can be done as in traditional paper-ballot elections or by using electronic means

Classification

- Supervised voting (off-line voting)
  - supervised physically by independent electoral authorities
  - voting machines located at polling stations (not connected)

- Hybrid Voting
  - supervised physically by election officials
  - Internet connected voting machines

- Remote voting (on-line voting)
  - unsupervised by election officials
  - (typically) through Internet using a personal computer or a mobile phone



Arguments (1)

- Reducing the overall cost to the electoral authorities of conducting an election or referendum
- Delivering voting results reliably and more quickly
- Increasing voter turnout by providing additional voting channels
- Increasing the number of elections

- Widening access to the voting process for voters with disabilities
- Bringing voting in line with new developments in society and increasing use of new technologies

Arguments (2)

- Handling different kind of voting methods (Single Transferable Vote, Condorcet, …)

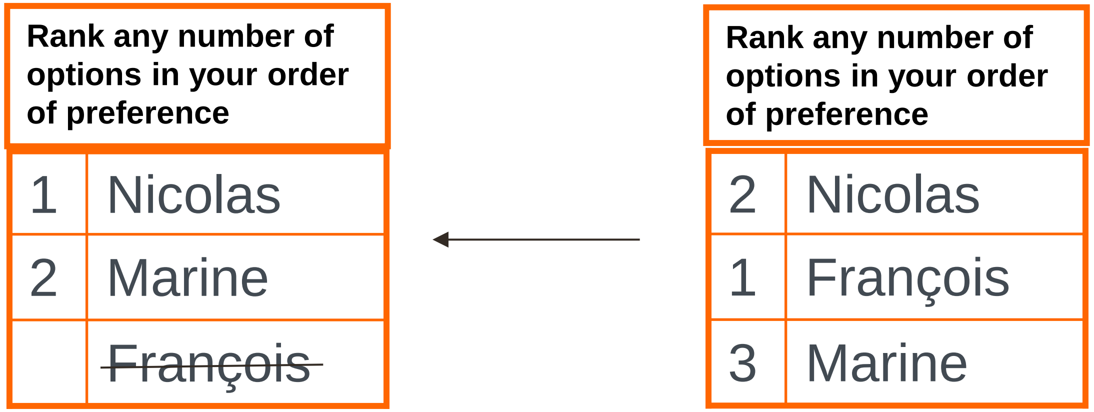
Rank any number of options in your order of preference

2	Nicolas
1	François
3	Marine

  - Manual counting would be cumbersome and prone to errors
  - Not a secure voting system: vulnerable to a so-called “Sicilian attack" (coercion attack)
  - STV used in several countries: Ireland, Scotland, Australia, etc.

Single Transferable Vote

- Take a blank ballot and rank the candidates in your order of preference



Rank any number of options in your order of preference	
1	Nicolas
2	Marine
	~~François~~

Rank any number of options in your order of preference	
2	Nicolas
1	François
3	Marine

- First round: only first choices are counted
- If a candidate obtains more votes (as first choice) than the quota he/she is elected
- otherwise, the candidate with the fewest votes (as first choice) is eliminated and the votes for this candidates are transferred to other candidates (the second choice becomes the first choice, the third becomes the second, etc.)
- Extra rounds until we obtain a winner

E-voting in France

- Supervised voting ☺
  - allowed for national elections since 1969 - decree n° 69-419 of 10 may 1969
  - used in 2005 (European Referendum) and in 2007 (presidential election)
- Hybrid voting 😐
  - might be allowed in the forthcoming years for national elections
- Remote voting ☹
  - similar to postal voting (forbidden since1975)
  - allowed, since 2003, for specific elections such as industrial tribunal elections

E-voting in other countries

- Supervised voting ☺
  - Belgium, Brazil, US,…
- Hybrid voting 😐
  - Italy : for a local election (Ladispoli)
- Internet voting ☹
  - Estonia: for major elections in 2005 (municipal), 2007 (parliamentary), 2009 (municipal) and 2011 (parliamentary) .
  - Korea: planned for presidential elections in the forthcoming years
  - Switzerland: test projects in several cantons (Aargau, Geneva, Neuchâtel and Zürich)
  - Norway: experiments in 2011 and 2013 for local and national elections

Current voting machines

Belgique - Election 2004 - http://www.poureva.be/ - (C) Kanar

- Several systems, only 3 have been approved in France:
  - iVotronic (ES&S – Datamatique)
  - Machine à voter v2.07 (Nedap – France Election)
  - Point & Vote (Indra Systemas)

- Objections
  - opaque systems (not open source)
  - similar to proxy voting (where a proxy form is given to a voting machine)
  - accuracy of the outcome of the election

- Several attacks have been reported
  - US: voting researchers converted a voting machine into a working PAC-MAN machine to show how easily its software could be modified
  - Arkansas : a candidate received no vote (although he voted for himself)
  - Belgium: number of votes **>>** number of registered voters

Security requirements (1)

- Eligibility
  - only legitimate voters can vote, and only once
- Ballot secrecy
  - No outside observer can determine for whom a voter voted
  - Perfect ballot secrecy = everlasting secrecy
- Receipt-freeness
  - A voter cannot prove *after the election* how she voted
  - prohibit proof of vote

- Coercion-resistance
  - no party should be able to force another party to vote in a certain way or abstain from voting

Security requirements (2)

- Individual verifiability
  - The voter can verify that his ballot has been cast /counted
- Universal verifiability
  - Any interested party can verify that the tally is correctly computed from votes that were cast by legitimate voters
- Fairness
  - No partial results are known before the election is closed

Het volk controleert de telling

Een functionaris van een Ugandees stembureau toont een stembiljet tijdens het tellen van de stemmen voor een nieuwe president. De huidige president Museveni wordt hoogstwaarschijnlijk herkozen. Verslag op pagina 5.

FOTO JEAN-MARC BOUJU/AI

Some challenges in e-voting

- How to combine (perfect) *secrecy* and (universal) *verifiability* ? (Challenge A)

- How to detect misbehaving voting machines?

  (Challenge B)

  - “It's not the people who vote that count. It's the people who count the votes” (Joseph Stalin)
  - What you see is what you vote for

- How to combine *remote* voting and *coercion-free* voting ? (Challenge C)

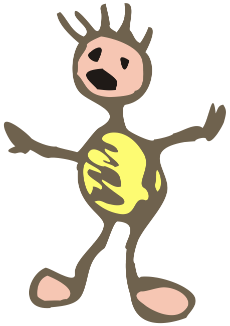
Challenge A

- How to combine (perfect) *secrecy* and (universal) *verifiability* ?
- Perfect = unconditional = everlasting
- *Easy* to solve if secrecy is not required to be perfect (e.g. use *homomorphic encryption*)
- *Impossible* to solve (in a practical environment) if secrecy is required to be perfect (Chevallier-Mames/Fouque/Pointcheval/Stern/Traoré*)

* On Some Incompatible Properties of Voting Schemes, Benoît Chevallier-Mames, Pierre-Alain Fouque, David Pointcheval, Julien Stern, Jacques Traoré, Towards Trustworthy Elections, Springer Verlag, 2010.

2 Cryptography

Definitions

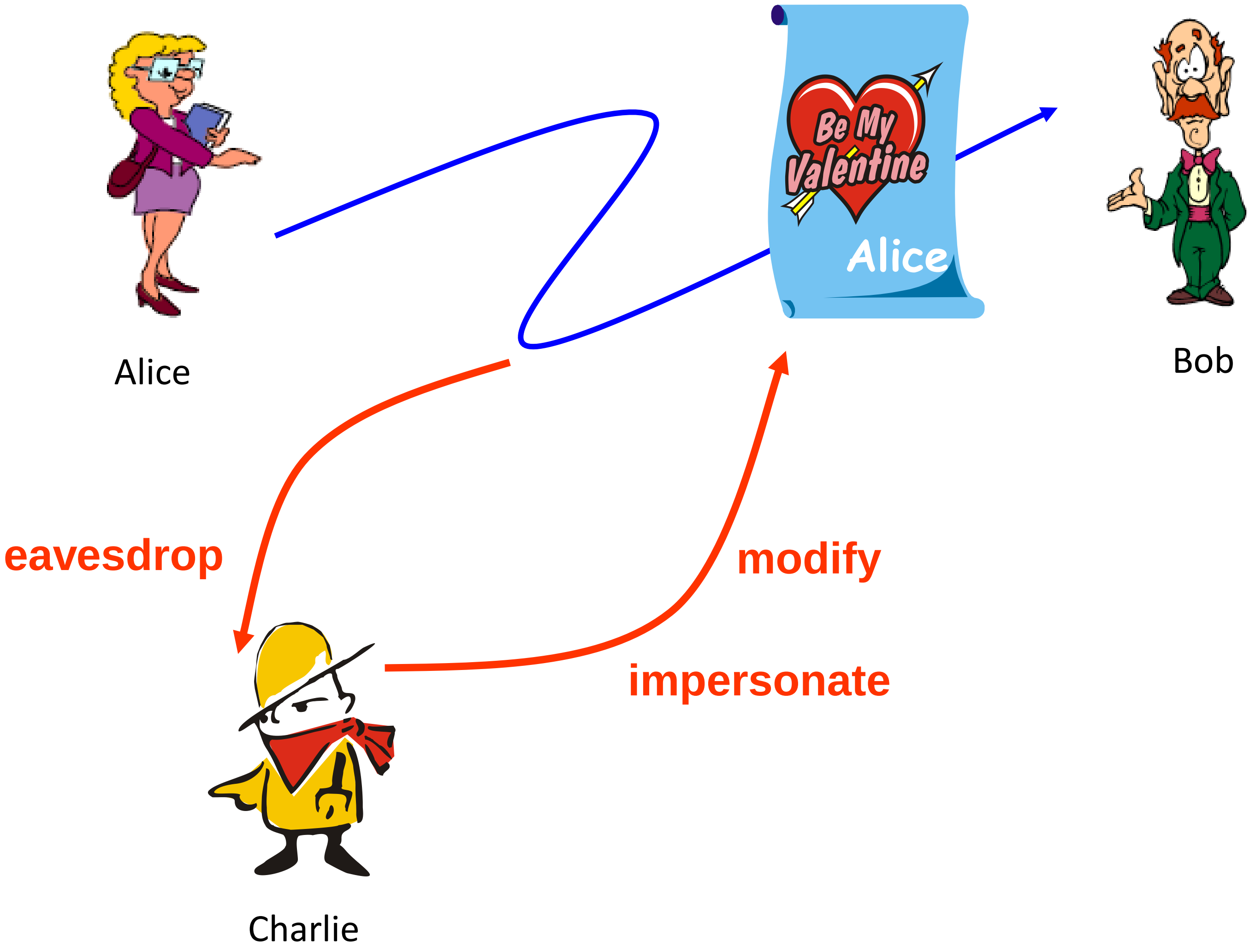


- crypto = κρυπτός = “hidden, secret”

- **cryptography** = **cryptology** = « science of secret » or « science of trust »

- Crossroads between art, science, research and industry, mathematics and computer science

Attacks



Alice

Bob

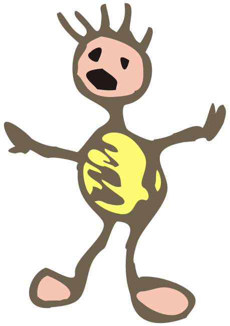
eavesdrop

modify

impersonate

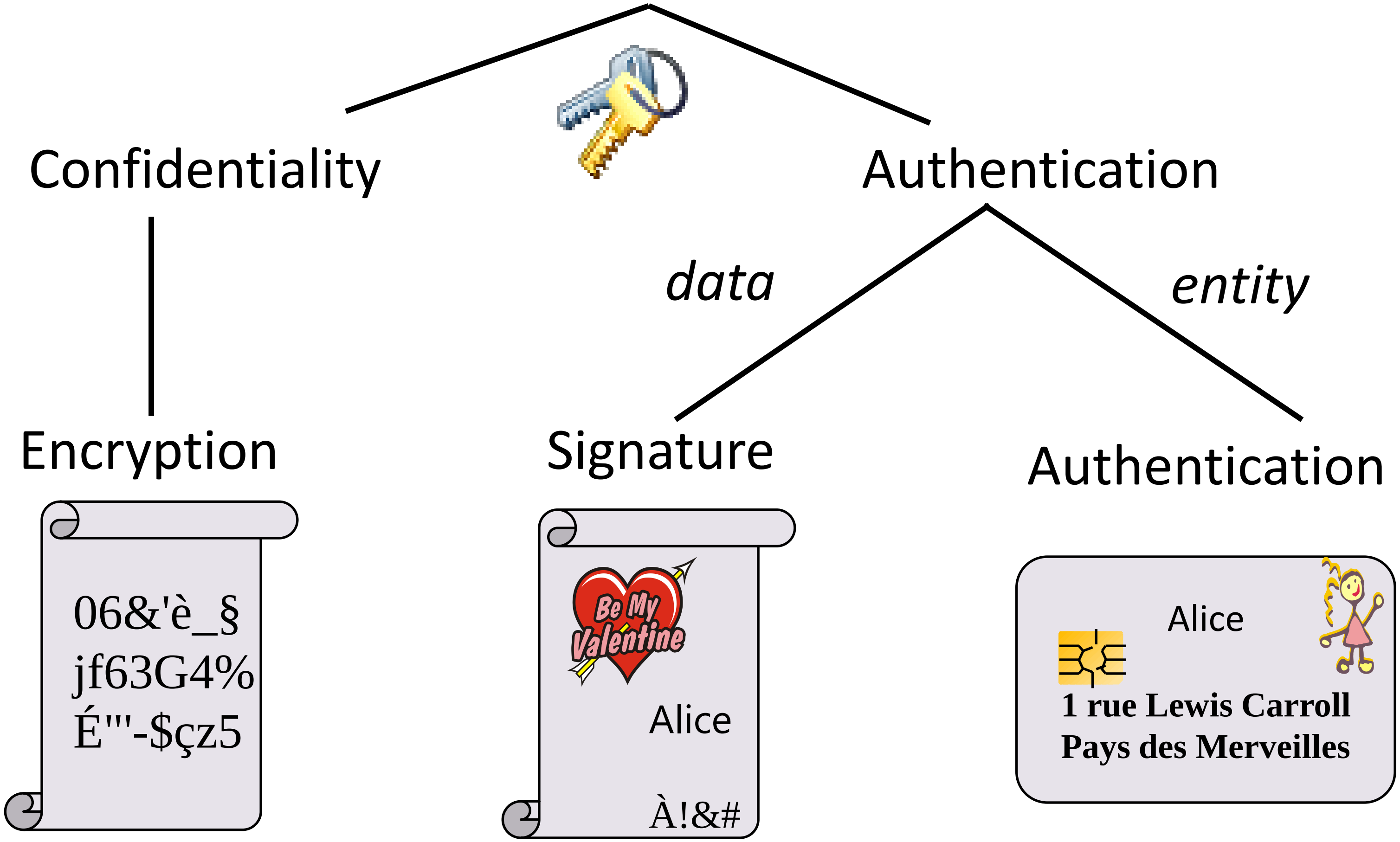
Charlie

Main goals of cryptography



- data confidentiality (privacy)
- data/entity authentication (it came from where it claims)
- data integrity (it has not been modified on the way)

Cryptography



Confidentiality

Authentication

data

entity

Encryption

06&'è_§
jf63G4%
É"'-$çz5

Signature

Alice

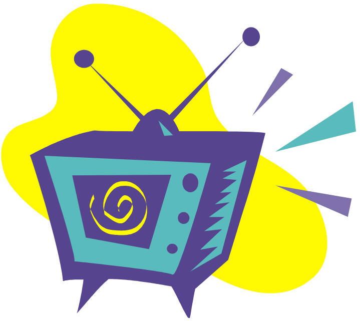
À!&#

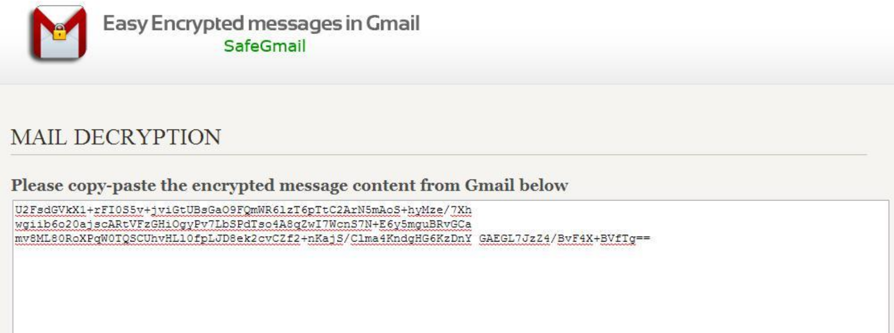
Authentication

Alice

1 rue Lewis Carroll
Pays des Merveilles

Cryptography is everywhere…





MAIL DECRYPTION

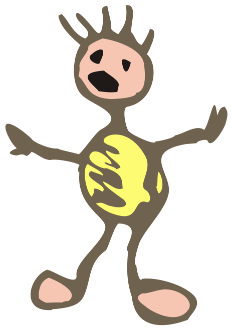
Please copy-paste the encrypted message content from Gmail below

```
U2FsdGVkX1+rFI0S5v+jviGtUBsGaO9FQmWR6lzT6pTtC2ArN5mAoS+hyMze/7Xh
wgiib6o20ajscARtVFzGHiOgyPv7LbSPdTso4A8qZwI7WcnS7N+E6y5mguBRvGCa
mv8ML80RoXPqW0TQSCUhvHL10fpLJD8ek2cvCZf2+nKajS/Clma4KndgHG6KzDnY GAEGL7JzZ4/BvF4X+BVfTg==
```

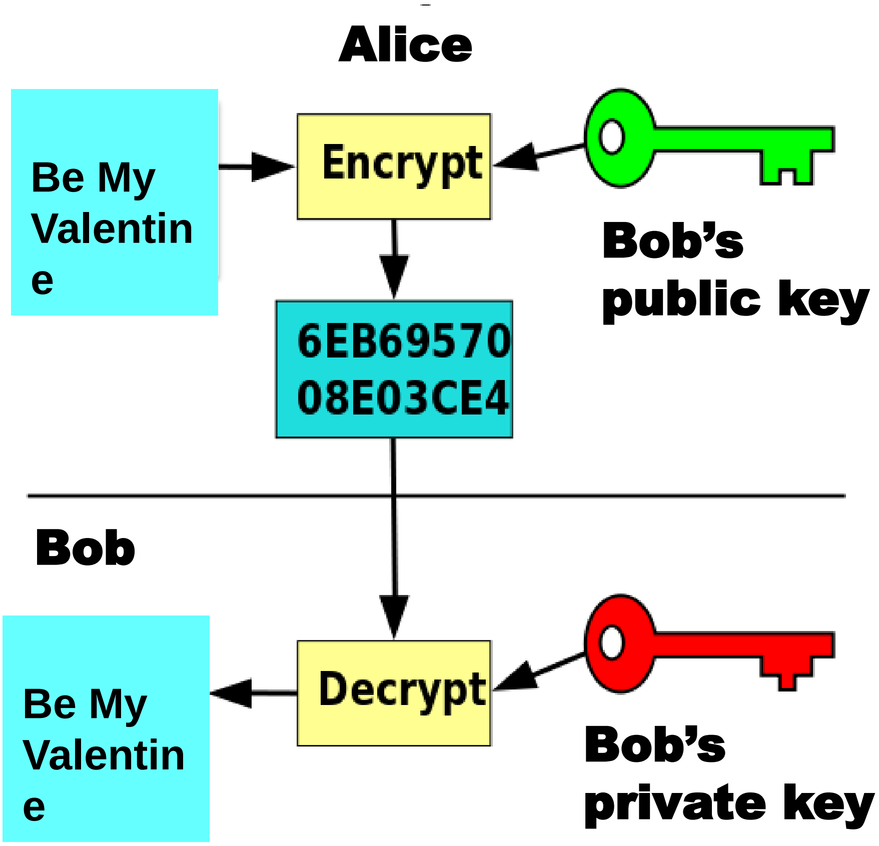
Show My Mail

3 Public-Key Cryptography

Principle



- **asymmetric** cryptography = **public-key** cryptography (discovered – officially – in 1976)



Alice

Be My Valentine

Encrypt

Bob's public key

6EB69570 08E03CE4

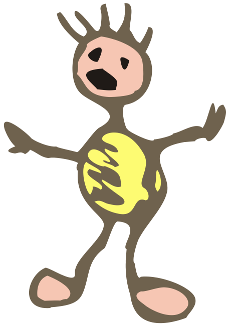
Bob

Be My Valentine

Decrypt

Bob's private key

How does it works?



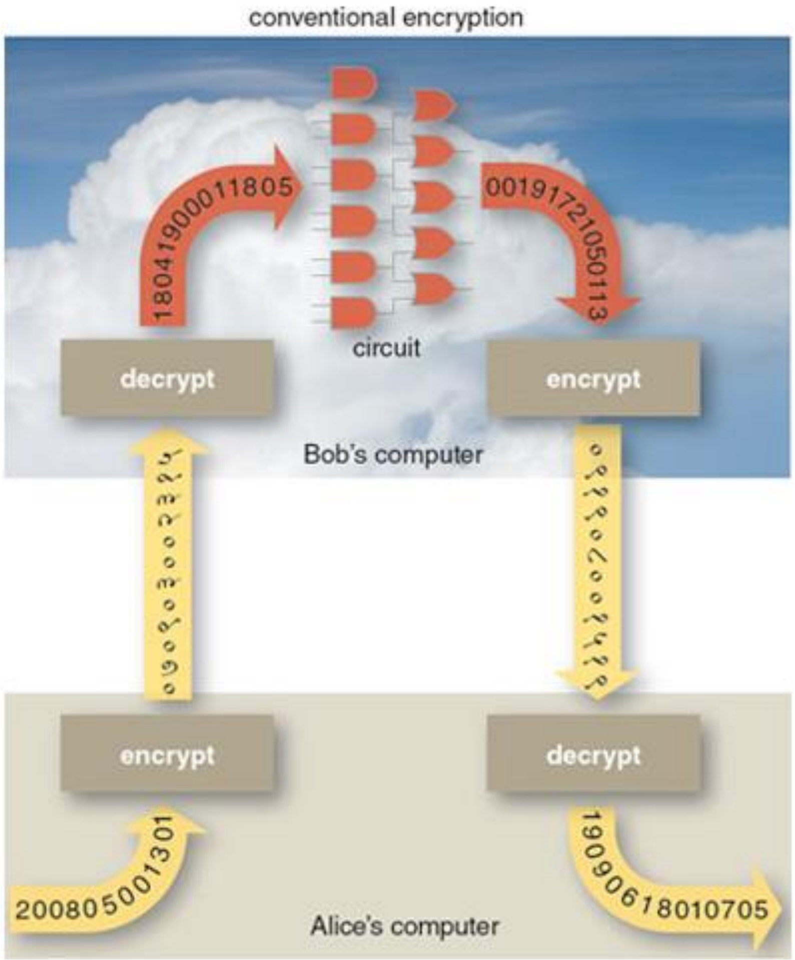
- Asymmetric cryptography exists because "asymmetric" problems exist

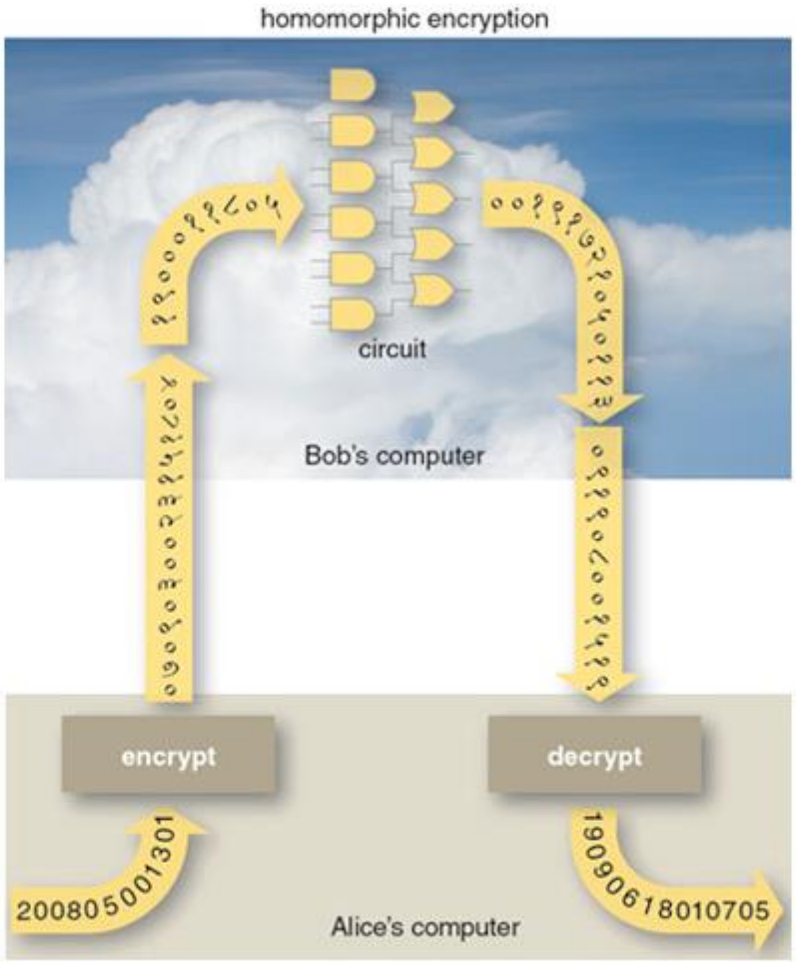
- Example (integer factorization) :
  - it is easy to compute the product of two large (prime) integers, however…
  - … it is hard, given only the product, to find its factorization (retrieve the two prime integers)

100 895 598 169 = ………….. × ……………… ?

4 Computing on Encrypted Data

What is homomorphic encryption?





Homomorphic Encryption in Practice

- Application to e-voting

$$\begin{tikzcd}
m_1 \arrow[d] & & m_2 \arrow[d] \\
E_{pk}(m_1) \arrow[dr] & & E_{pk}(m_2) \arrow[dl] \\
& \times \arrow[d] & \\
& E_{pk}(m_1 + m_2) &
\end{tikzcd}$$

- In e-voting, we use probabilistic encryption functions:
  - if you encrypt twice the same plaintext, you will obtain two different ciphertexts
  - roughly, to encrypt a message *m*, pick a random value *r* and compute $E_{PK}(m, r)$

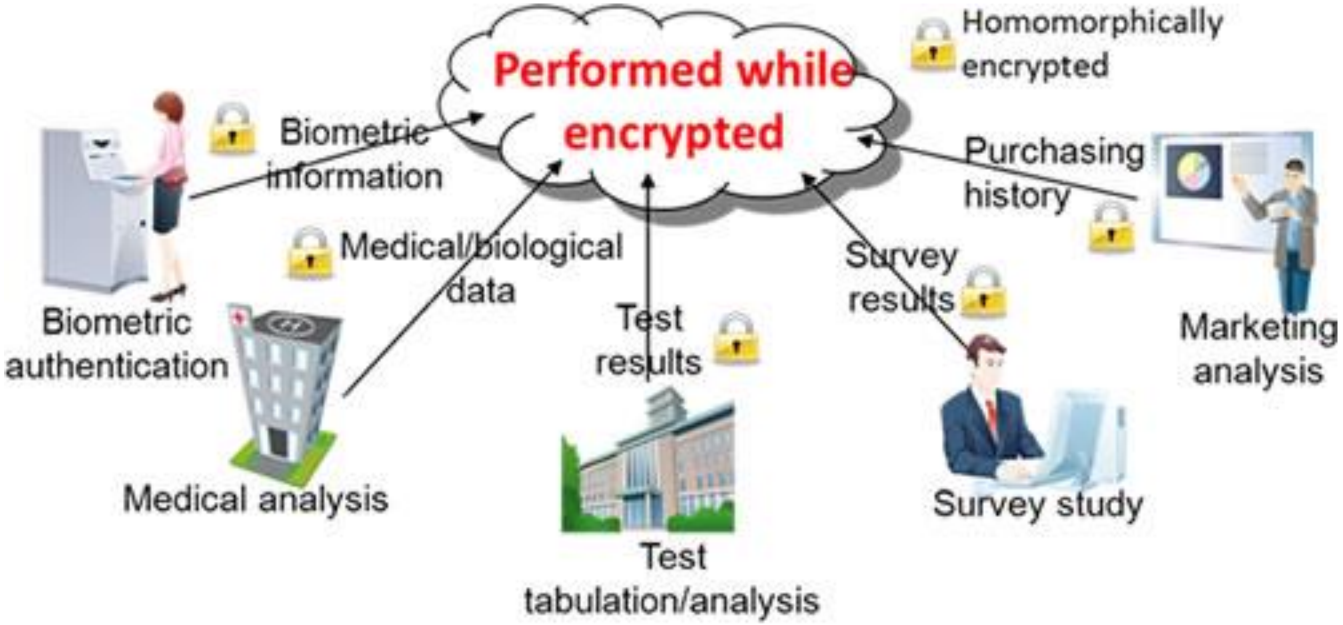
Real-life applications of Homomorphic Encryption

- Secret-ballot internet voting
- Supported computation: addition
- The decryption key is shared among the talliers:

- **Referendum case**: “yes” = 1 and “no” = 0,
  - Each voter encrypts her vote using the talliers’ public keys.
  - The voting center computes an encryption of the sum of the votes thanks to the properties of the homomorphic encryption scheme.
  - The talliers decrypt this ciphertext and obtain the outcome of the election.
  - No individual vote is revealed!

- Homomorphic Encryption can also be used to securely handle STV

Other Applications



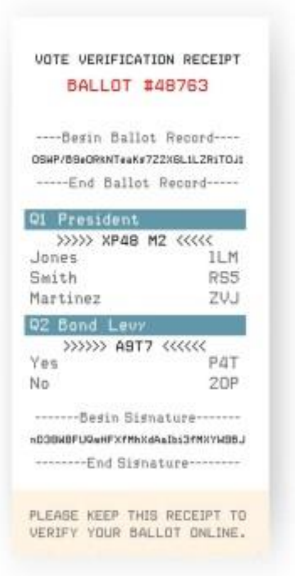
5 Challenge B

Challenge B: How to detect misbehaving voting machines

End-to-End verifiability: a voter can verify that

- cast-as-intended: her choice was not modified by the voting machine
- recorded-as-cast: her ballot was received the way she cast it
- tallied as recorded: her ballot count as received

Voting machine with untrusted software



```
VOTE VERIFICATION RECEIPT
BALLOT #48763

----Begin Ballot Record----
OSWP/B9eORkNTeaKs7Z2XGL1LZRiTOJ!
-----End Ballot Record-----

Q1 President
  >>>>> XP48 M2 <<<<<
Jones                  1LM
Smith                  RS5
Martinez               ZVJ
Q2 Bond Levy
  >>>>>> A9T7 <<<<<<
Yes                    P4T
No                     2DP

-------Begin Signature-------
nD3BWBFUQwHFXfMhKdAaIbi3fMXYWBBJ
--------End Signature--------

PLEASE KEEP THIS RECEIPT TO
VERIFY YOUR BALLOT ONLINE.
```

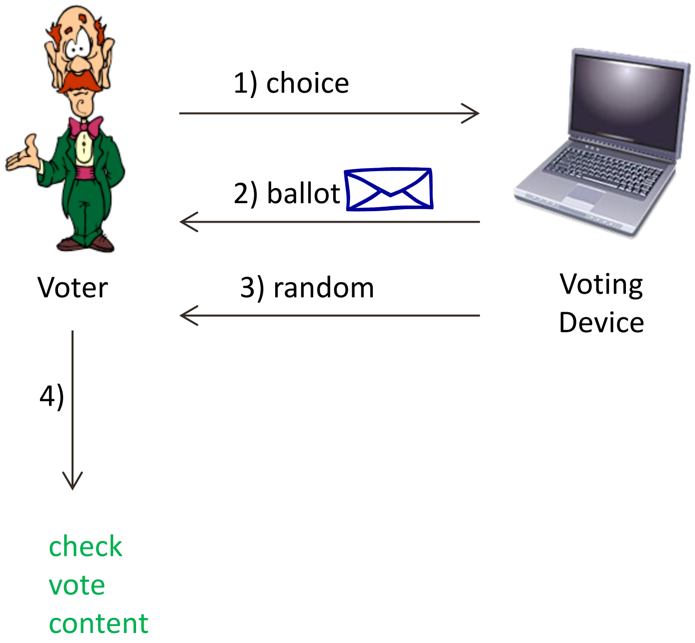
Vote Verification ticket

Cast as Intended in Helios

Challenge or cast ?

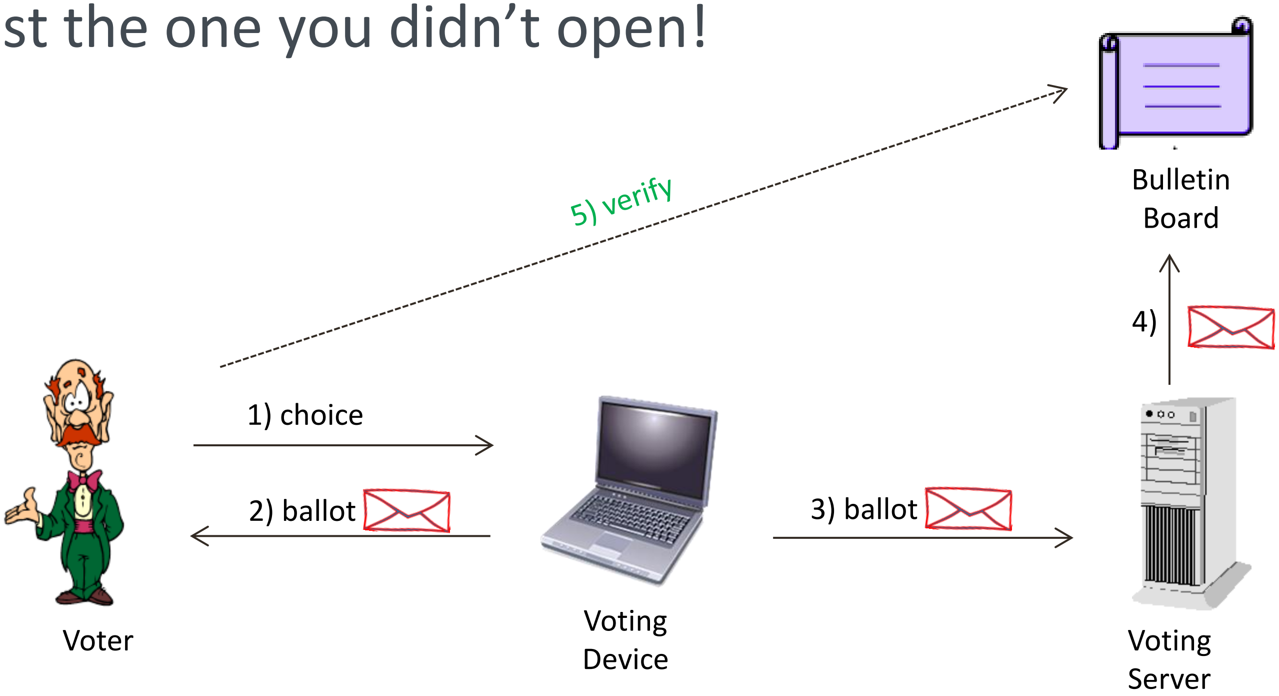
- Don’t trust your PC to encrypt the right thing!
- Ask your PC to produce lots of (different) encrypted votes
  - It doesn’t know which one you’re going to use
- Print them and send them to other devices
- Ask your PC to ‘open’ all but one of them
  - *i.e.* to tell you the randomness *r* it used for encrypting the ballot
  - Get the other devices to check the encryption was right
    - They just recompute $\mathrm{Enc}_{PK}(\mathrm{choice}, r)$

Challenge your voting device



Cast as Intended in Helios (2)

- Cast the one you didn't open!



- Each voter can verify that his/her vote is:
  - cast as he/she intended
  - properly included in the count
- Used by the IACR in their board elections
- Usability issues: voters need to understand it to get it right

6 Challenge C

Challenge C

- How to combine *on-line* and *coercion-free* voting ? (Araujo-Foule-Traoré)*

- Basic ingredients
  - A ballot may be valid or not
  - A coercer cannot decide if a ballot is valid or not
  - A voter can vote more than once

- Basic idea
  - To mislead a coercer, the voter sends invalid ballot(s) as long as he is coerced, and a valid ballot as soon as he is not coerced
  - It suffices that the voter finds a window-time during which he is not coerced

* A Practical and Secure Coercion-Resistant Scheme for Internet Voting, Roberto Araujo, Sébastien Foule, Jacques Traoré, Towards Trustworthy Elections, Springer Verlag, 2010.

Conclusion

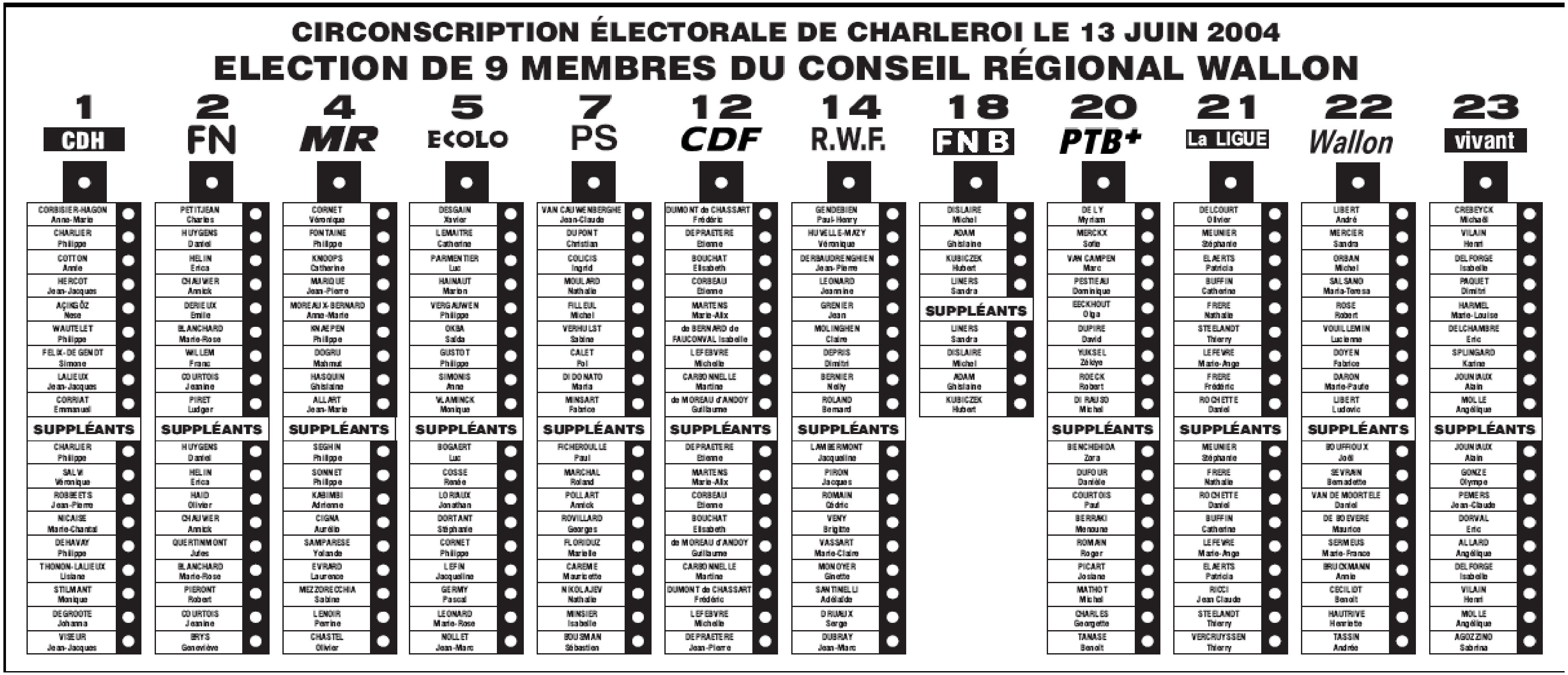
- E-voting is a true reality in several countries
  - Brazil, Estonia, United States, etc.
  - also in France (presidential election in 2007)

- Commercial e-voting solutions offer very poor security guarantees

- In spite of the impossibility result, there is some hope that a convenient (secure/practical) voting system exists one day, even for remote voting.

7 Annex

Preferential Voting



CIRCONSCRIPTION ÉLECTORALE DE CHARLEROI LE 13 JUIN 2004

ELECTION DE 9 MEMBRES DU CONSEIL RÉGIONAL WALLON

1	2	4	5	7	12	14	18	20	21	22	23
CDH	FN	MR	ECOLO	PS	CDF	R.W.F.	FNB	PTB+	La LIGUE	Wallon	vivant
●	●	●	●	●	●	●	●	●	●	●	●
CORBISIER-HAGON Anne-Marie ○	PETITJEAN Charles ○	CORNET Véronique ○	DESGAIN Xavier ○	VAN CAUWENBERGHE Jean-Claude ○	DUMONT de CHASSART Frédéric ○	GENDEBIEN Paul-Henry ○	DISLAIRE Michel ○	DELY Myriam ○	DELCOURT Olivier ○	LIBERT André ○	CREBEYCK Michaël ○
CHARLIER Philippe ○	HUYGENS Daniel ○	FONTAINE Philippe ○	LEMAITRE Catherine ○	DUPONT Christian ○	DEPRAETERE Etienne ○	HUVELLE-MAZY Véronique ○	ADAM Ghislaine ○	MERCKX Sofie ○	MEUNIER Stéphanie ○	MERCIER Sandra ○	VILAIN Henri ○
COTTON Annie ○	HELIN Erica ○	KNOOPS Catherine ○	PARMENTIER Luc ○	COLICIS Ingrid ○	BOUCHAT Elisabeth ○	DERBAUDRENGHIEN Jean-Pierre ○	KUBICZEK Hubert ○	VAN CAMPEN Marc ○	ELAERTS Patricia ○	ORBAN Michel ○	DELFORGE Isabelle ○
HERCOT Jean-Jacques ○	CHAUWIER Annick ○	MARIQUE Jean-Pierre ○	HAINAUT Marion ○	MOULARD Nathalie ○	CORBEAU Etienne ○	LEONARD Jeannine ○	LINERS Sandra ○	PESTIEAU Dominique ○	BUFFIN Catherine ○	SALSANO Maria-Teresa ○	PAQUET Dimitri ○
AÇIKGÖZ Nese ○	DERIEUX Emile ○	MOREAUX-BERNARD Anne-Marie ○	VERGAUWEN Philippe ○	FILLEUL Michel ○	MARTENS Marie-Alix ○	GRENIER Jean ○	SUPPLÉANTS	EECKHOUT Olga ○	FRERE Nathalie ○	ROSE Robert ○	HARMEL Marie-Louise ○
WAUTELET Philippe ○	BLANCHARD Marie-Rose ○	KNAEPEN Philippe ○	OKBA Saïda ○	VERHULST Sabine ○	de BERNARD de FAUCONVAL Isabelle ○	MOLINGHEN Claire ○	LINERS Sandra ○	DUPIRE David ○	STEELANDT Thierry ○	VOUILLEMIN Lucienne ○	DELCHAMBRE Eric ○
FELIX-DE GENDT Simone ○	WILLEM Franc ○	DOGRU Mahmut ○	GUSTOT Philippe ○	CALET Pol ○	LEFEBVRE Michelle ○	DEPRIS Dimitri ○	DISLAIRE Michel ○	YUKSEL Zökiye ○	LEFEVRE Marie-Ange ○	DOYEN Fabrice ○	SPLINGARD Karine ○
LALIEUX Jean-Jacques ○	COURTOIS Jeanine ○	HASQUIN Ghislaine ○	SIMONIS Anne ○	DI DONATO Maria ○	CARBONNELLE Martine ○	BERNIER Nelly ○	ADAM Ghislaine ○	ROECK Robert ○	FRERE Frédéric ○	DARON Marie-Paule ○	JOUNIAUX Alain ○
CORRIAT Emmanuel ○	PIRET Ludger ○	ALLART Jean-Marie ○	VLAMINCK Monique ○	MINSART Fabrice ○	de MOREAU d'ANDOY Guillaume ○	ROLAND Bernard ○	KUBICZEK Hubert ○	DI RAUSO Michel ○	ROCHETTE Daniel ○	LIBERT Ludovic ○	MOLLE Angélique ○
SUPPLÉANTS	SUPPLÉANTS	SUPPLÉANTS	SUPPLÉANTS	SUPPLÉANTS	SUPPLÉANTS	SUPPLÉANTS		SUPPLÉANTS	SUPPLÉANTS	SUPPLÉANTS	SUPPLÉANTS
CHARLIER Philippe ○	HUYGENS Daniel ○	SEGHIN Philippe ○	BOGAERT Luc ○	FICHEROULLE Paul ○	DEPRAETERE Etienne ○	LAMBERMONT Jacqueline ○		BENCHEHIDA Zora ○	MEUNIER Stéphanie ○	BOUFFIOUX Joël ○	JOUNIAUX Alain ○
SALVI Véronique ○	HELIN Erica ○	SONNET Philippe ○	COSSE Renée ○	MARCHAL Roland ○	MARTENS Marie-Alix ○	PIRON Jacques ○		DUFOUR Danièle ○	FRERE Nathalie ○	SEVRAIN Bernadette ○	GONZE Olympe ○
ROBBEETS Jean-Pierre ○	HAID Olivier ○	KABIMBI Adrienne ○	LORIAUX Jonathan ○	POLLART Annick ○	CORBEAU Etienne ○	ROMAIN Cédric ○		COURTOIS Paul ○	ROCHETTE Daniel ○	VAN DE MOORTELE Daniel ○	PEMERS Jean-Claude ○
NICAISE Marie-Chantal ○	CHAUWIER Annick ○	CIGNA Aurélio ○	DORTANT Stéphanie ○	ROVILLARD Georges ○	BOUCHAT Elisabeth ○	VENY Brigitte ○		BERRAKI Menoune ○	BUFFIN Catherine ○	DE BOEVERE Maurice ○	DORVAL Eric ○
DEHAVAY Philippe ○	QUERTINMONT Jules ○	SAMPARESE Yolande ○	CORNET Philippe ○	FLORIDUZ Marielle ○	de MOREAU d'ANDOY Guillaume ○	VASSART Marie-Claire ○		ROMAIN Roger ○	LEFEVRE Marie-Ange ○	SERMEUS Marie-France ○	ALLARD Angélique ○
THONON-LALIEUX Lisiane ○	BLANCHARD Marie-Rose ○	EVRARD Laurence ○	LEFIN Jacqueline ○	CAREME Mauricette ○	CARBONNELLE Martine ○	MONOYER Ginette ○		PICART Josiane ○	ELAERTS Patricia ○	BRUCKMANN Annie ○	DELFORGE Isabelle ○
STILMANT Monique ○	PIERONT Robert ○	MEZZORECCHIA Sabine ○	GERMY Pascal ○	NIKOLAJEV Nathalie ○	DUMONT de CHASSART Frédéric ○	SANTINELLI Adélaïde ○		MATHOT Michel ○	RICCI Jean Claude ○	CECILIOT Benoît ○	VILAIN Henri ○
DEGROOTE Johanna ○	COURTOIS Jeanine ○	LENOIR Perrine ○	LEONARD Marie-Rose ○	MINSIER Isabelle ○	LEFEBVRE Michelle ○	DRUAUX Serge ○		CHARLES Georgette ○	STEELANDT Thierry ○	HAUTRIVE Henriette ○	MOLLE Angélique ○
VISEUR Jean-Jacques ○	BRYS Geneviève ○	CHASTEL Olivier ○	NOLLET Jean-Marc ○	BOUSMAN Sébastien ○	DEPRAETERE Jean-Pierre ○	DUBRAY Jean-Marc ○		TANASE Benoît ○	VERCRUYSSEN Thierry ○	TASSIN Andrée ○	AGOZZINO Sabrina ○

Sicilian Attack

2	Olivier
10	Nicolas
9	Ségolène
8	François
11	José
1	Dominique
3	Marie-George
4	Arlette
12	Frédéric
5	Pat Hibulaire
6	Al Cap
7	Aldo

With 12 candidates, there are more than 479 millions possible combinations!

Integer factorization

100 895 598 169 = 898 423 × 112 303

Number of digits	Time with 100 million of PC
200	5,6 days
300	228 years
450	17 million of years
600	610 000 million of years

Trapdoor function

$$\begin{tikzcd} f : x \arrow[r, bend left, "\text{easy}"] & y \arrow[l, bend left, "\text{difficult (unless...)}"] \end{tikzcd}$$