# Cryptologic History Symposium

## A French Story…

LETTRES
SORBONNE
UNIVERSITÉ

# Storytelling …

01
**Jean-Louis Desvignes**
Presentation of ARCSI and its representatives

02
**Philippe Guillot**
From 16th to 19th century

03
**Agathe Couderc**
From 1912 to the 1920s

04
**Jean-Louis Desvignes**
From C-36 to
CP8 Smart Card

05
**Jean-Jacques Quisquater**
From Smart Cards to today
1967-2022

LETTRES
SORBONNE
UNIVERSITÉ

01

# Presentation of ARCSI and its Representatives

Jean-Louis Desvignes

https://www.arcsi.fr/

https://www.linkedin.com/groups/12503142/

https://twitter.com/arcsi_fr

LETTRES
SORBONNE
UNIVERSITÉ

# Presentation of ARCSI

- Created in 1928, the "Association des Réservistes du Chiffre et de la Sécurité de l'Information" (A.R.C.S.I.) has for mission to deepen and disseminate the historical knowledge of the field and to ensure its perenniality

LETTRES
SORBONNE
UNIVERSITÉ

# Our Activities

- 350 members: 3 Americans, 4 Belgians, 2 Spanish, 1 Canadian, 2 Lux…
- High quality daily electronic exchanges
- An annual newsletter
- An annual colloquium
- Visits
- Videoconferences (one per month)
- Exhibitions (local and national)
- A dream : “A museum of the secret”

# Our Team

- **Philippe Guillot**: engineer, historian, retired researcher at Paris 8 University
- **Agathe Couderc**: PhD student at Sorbonne University in France
- **Jean-Louis Desvignes**: retired general of the French Army
- **Jean-Jacques Quisquater**: world-renowned cryptologist

LETTRES
SORBONNE
UNIVERSITÉ

02

# From 16th to 19th Century

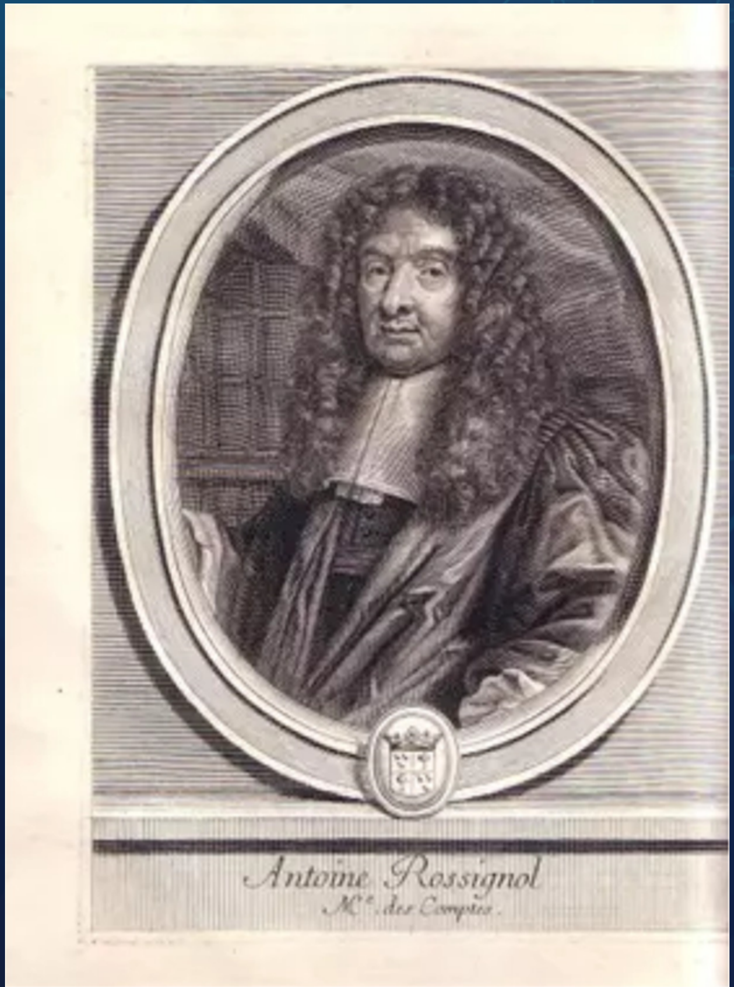
Philippe Guillot

# François Vieta (1540-1603)

# Infallible Rule

- Among three consecutive letters, there is always one or more of the five vowels A, E, I, O or U

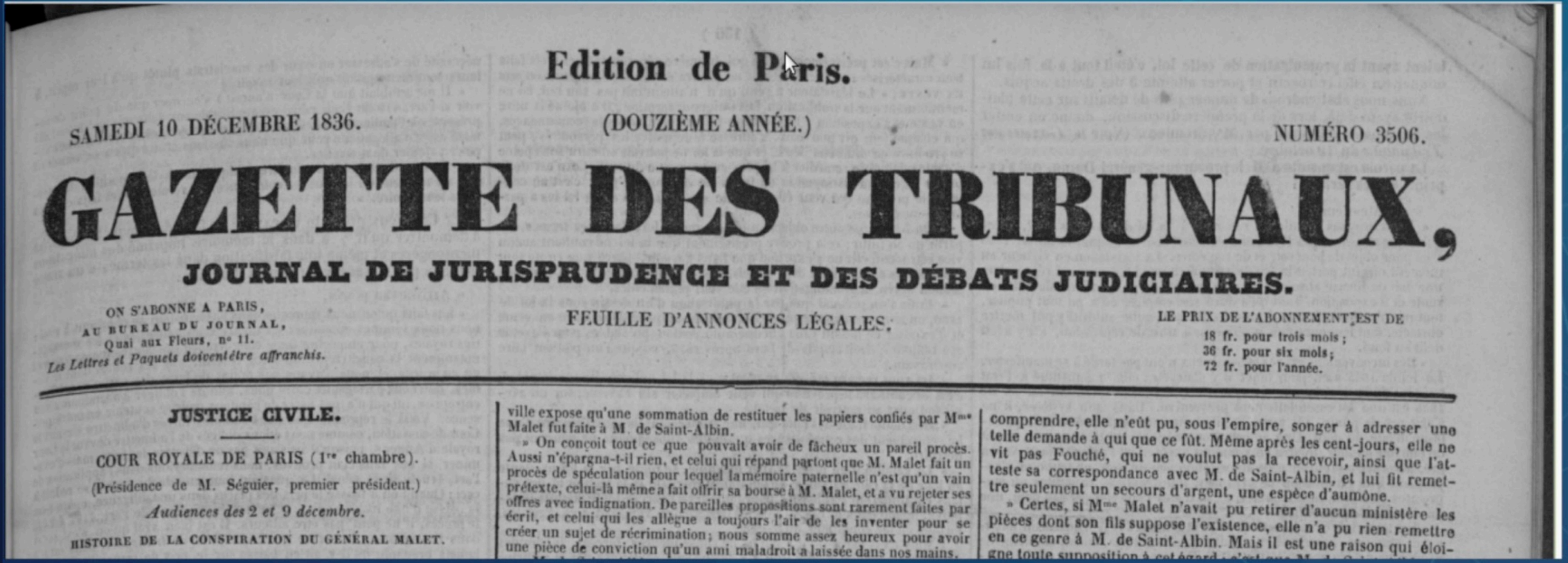
# Antoine Rossignol (1600-1682)



# Claude Chappe (1763-1805)

INVENTIONS ILLUSTRES
Le Télégraphe

LETTRES
SORBONNE
UNIVERSITÉ



Edition de Paris.

SAMEDI 10 DÉCEMBRE 1836. (DOUZIÈME ANNÉE.) NUMÉRO 3506.

# GAZETTE DES TRIBUNAUX,

## JOURNAL DE JURISPRUDENCE ET DES DÉBATS JUDICIAIRES.

FEUILLE D'ANNONCES LÉGALES.

ON S'ABONNE A PARIS,
AU BUREAU DU JOURNAL,
Quai aux Fleurs, nº 11.
*Les Lettres et Paquets doiventêtre affranchis.*

LE PRIX DE L'ABONNEMENT EST DE
18 fr. pour trois mois ;
36 fr. pour six mois ;
72 fr. pour l'année.

### JUSTICE CIVILE.

COUR ROYALE DE PARIS (1re chambre).

(Présidence de M. Séguier, premier président.)

*Audiences des 2 et 9 décembre.*

HISTOIRE DE LA CONSPIRATION DU GÉNÉRAL MALET.

ville expose qu'une sommation de restituer les papiers confiés par Mme Malet fut faite à M. de Saint-Albin.

» On conçoit tout ce que pouvait avoir de fâcheux un pareil procès. Aussi n'épargna-t-il rien, et celui qui répand partout que M. Malet fait un procès de spéculation pour lequel la mémoire paternelle n'est qu'un vain prétexte, celui-là même a fait offrir sa bourse à M. Malet, et a vu rejeter ses offres avec indignation. De pareilles propositions sont rarement faites par écrit, et celui qui les allègue a toujours l'air de les inventer pour se créer un sujet de récrimination; nous somme assez heureux pour avoir une pièce de conviction qu'un ami maladroit a laissée dans nos mains.

comprendre, elle n'eût pu, sous l'empire, songer à adresser une telle demande à qui que ce fût. Même après les cent-jours, elle ne vit pas Fouché, qui ne voulut pas la recevoir, ainsi que l'atteste sa correspondance avec M. de Saint-Albin, et lui fit remettre seulement un secours d'argent, une espèce d'aumône.

» Certes, si Mme Malet n'avait pu retirer d'aucun ministère les pièces dont son fils suppose l'existence, elle n'a pu rien remettre en ce genre à M. de Saint-Albin. Mais il est une raison qui éloigne toute supposition à cet égard

An agent from Paris transmitted to Tour, poste restante, effects such as gloves, aso. The color of these objects indicated the rise or fall. On the sight of these objects, the employee of the telegraph gave an agreed signal. The employee of Tour gave the signal indicative of the word *Error* which was repeated on all the time, and did not appear consequently on the official dispatches.

# Auguste Kerckhoffs (1835-1901)

It is necessary to distinguish between a system of encrypted writing imagined for a momentary exchange of dispatches between a few isolated persons and a method of cryptography intended to regulate for an unlimited time the correspondance of the various heads of the Army.

LA

CRYPTOGRAPHIE MILITAIRE

OU

DES CHIFFRES USITÉS EN TEMPS DE GUERRE

AVEC UN

Nouveau procédé de déchiffrement applicable aux systèmes à double clef

PAR

Aug. KERCKHOFFS

[illegible]

PARIS

LIBRAIRIE MILITAIRE DE L. BAUDOIN ET Cie

[illegible]

Successeurs de J. DUMAINE

30, Rue et Passage Dauphine, 30

1883

[illegible]

The administration must absolutely renounce secret methods.

The value of a cryptographic system intended for the need of war is in inverse proportion to the secrecy that its handling or its composition requires.

A cipher is good as long as it remains unbreakable by the master himself who invented it : *Ars ipsi secreta magistro.*

# Posterity of Auguste Kerckhoffs

Étienne Bazeries

1846-1931

Félix Delastelle

1840-1902

Eugène Valério

19th century

Gaétan de Viaris

1847-1901

LETTRES SORBONNE UNIVERSITÉ

03

# From 1912 to the 1920s

## Innovative Intelligence services: the French Army & Navy's Cipher services in the Great War

Agathe Couderc

LETTRES
SORBONNE
UNIVERSITÉ

# Innovative Intelligence services: the French Army & Navy's Cipher services in the Great War.

- "Cipher services" = sections dealing with cryptography (code or cipher-writing) & cryptanalysis (code-breaking)

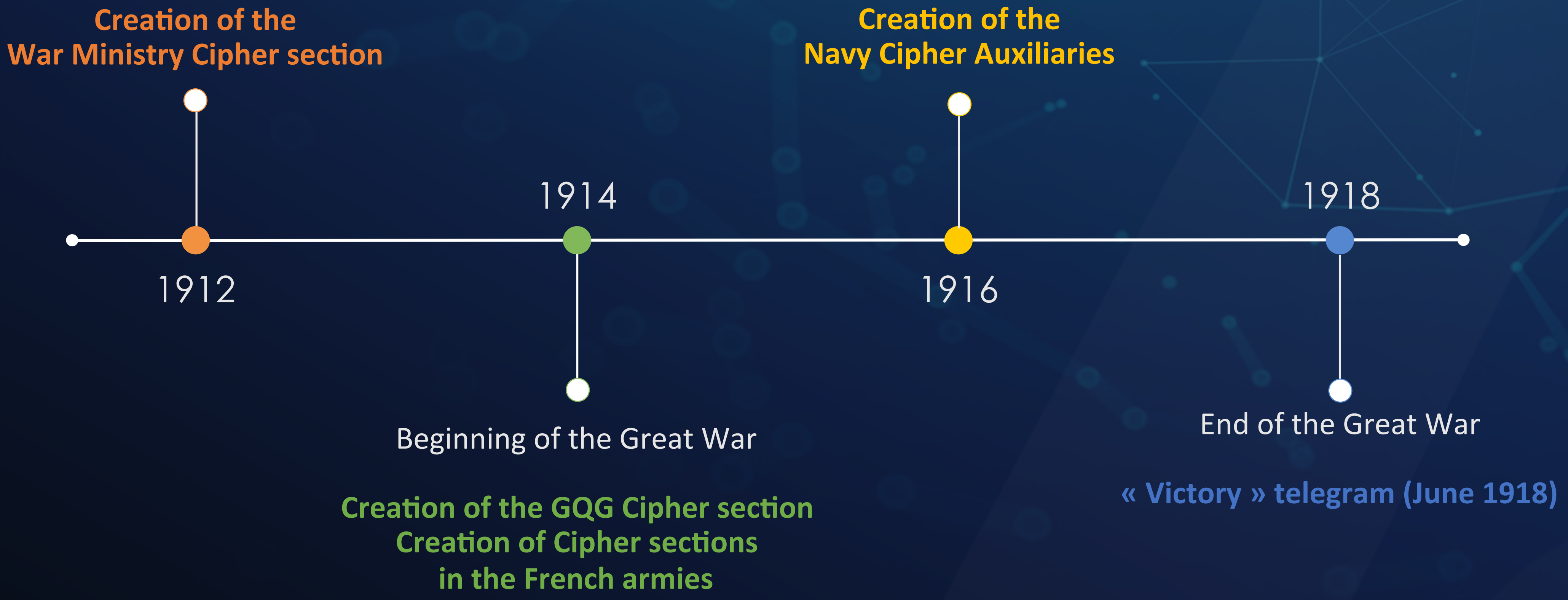
- Some names :
  - ❖ François Cartier (Head of Cipher Section in the cabinet of the War Minister)
  - ❖ Marcel Givierge (Head of Cipher Section in French GHQ)
  - ❖ Georges-Jean Painvin (main code-breaker of the cabinet of the War Minister)

# The French Army & Navy’s Cipher services in the Great War.

- I. Of Birth & Missions throughout the Great War
- II. Snippets of the wartime cooperation between French & Allied Cipher services
- III. Icons & Memory of the French Cipher services

# The French Army & Navy’s Cipher services in the Great War.

## I. Of Birth & Missions throughout the Great War



1912

Creation of the
War Ministry Cipher section

1914

Beginning of the Great War

Creation of the GQG Cipher section
Creation of Cipher sections
in the French armies

1916

Creation of the
Navy Cipher Auxiliaries

1918

End of the Great War

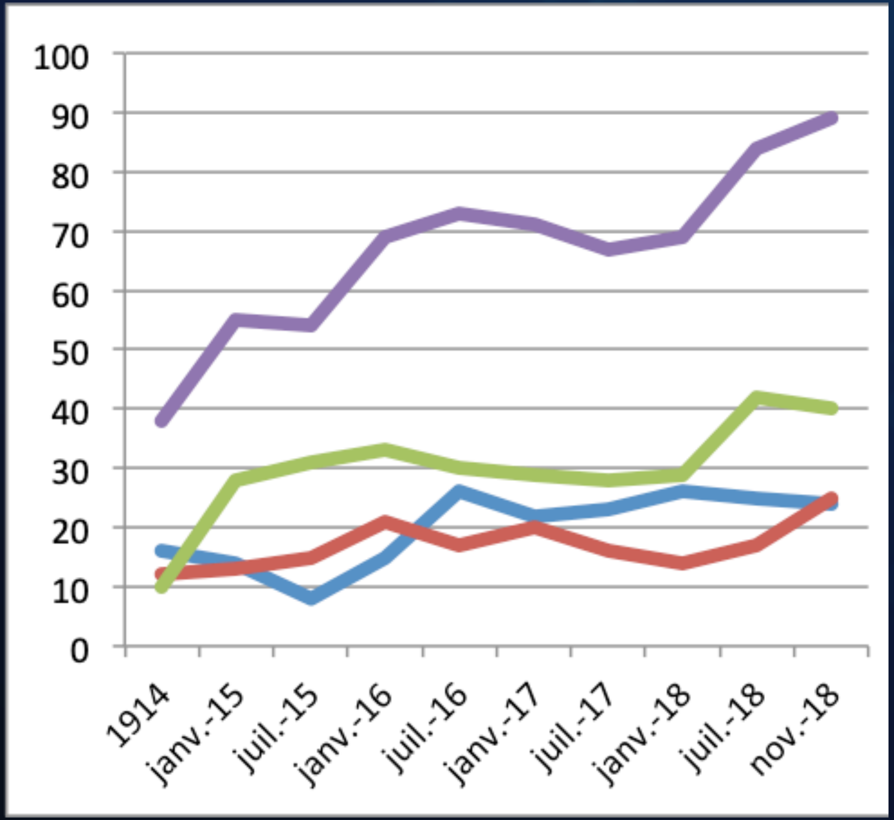
« Victory » telegram (June 1918)

# The French Army & Navy's Cipher services in the Great War.

## I. Of Birth & Missions throughout the Great War

### Growth of Cipher services in the French Army

(from sept 1914 to nov 1918)



**Legend**

— Cipher section for the cabinet

— Cipher section for the GQG

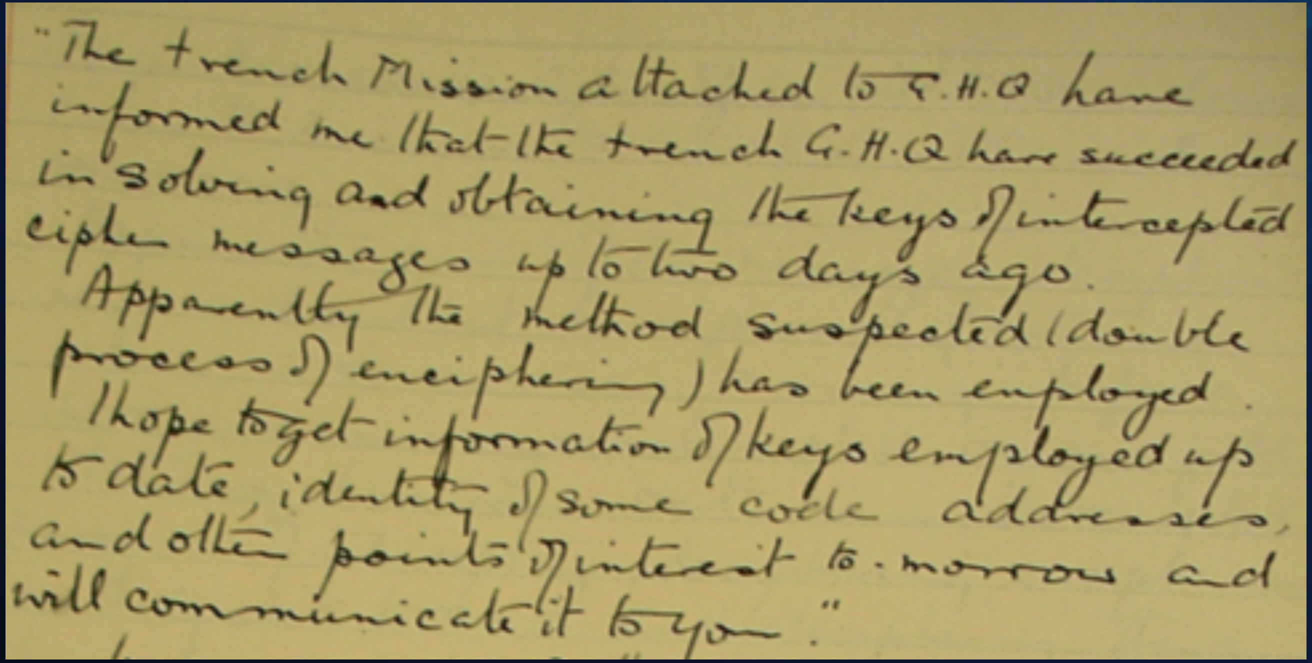
— Cipher sections in the Armies

— Overall Growth

# The French Army & Navy's Cipher services in the Great War.

## II. Snippets of the wartime cooperation between French & Allied Cipher services

### ❖ French & British cooperation



"The French Mission attached to G.H.Q have
informed me that the French G.H.Q have succeeded
in solving and obtaining the keys of intercepted
cipher messages up to two days ago.
Apparently the method suspected (double
process of enciphering) has been employed.
I hope to get information of keys employed up
to date, identity of some code addresses,
and other points of interest to-morrow and
will communicate it to you."

### Transcription

« **The French Mission attached to G.H.Q. have informed me that the French G.H.Q. have succeeded in solving and obtaining the keys of intercepted cipher messages up to two days ago.** Apparently the method suspected (double process of enciphering) has been employed.

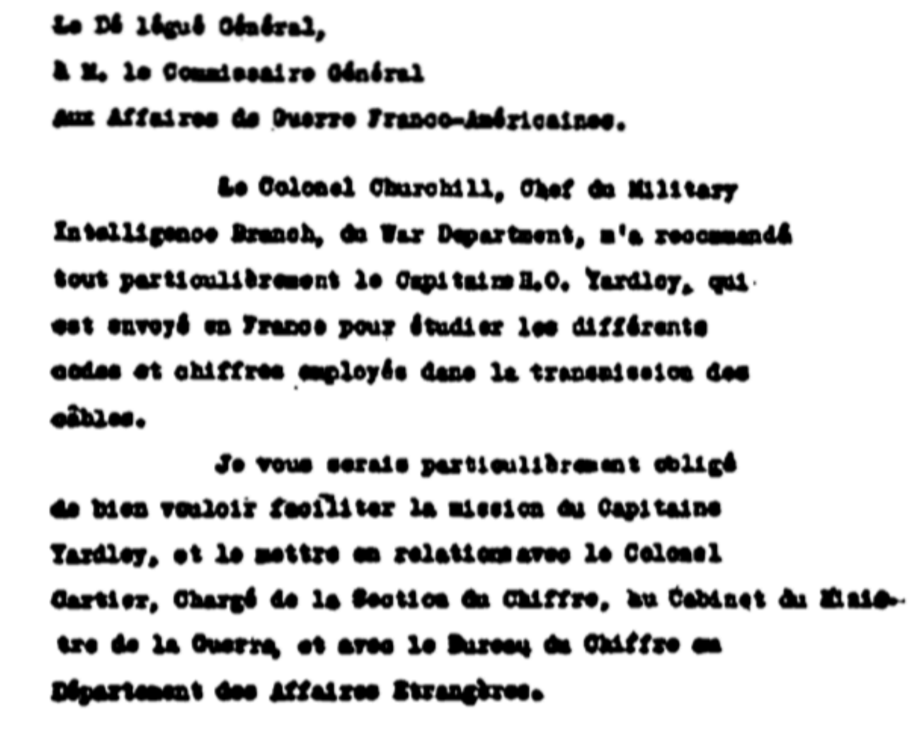
**I hope to get information of keys employed up to date**, identity of some code addresses and other points of interest to morrow and will communicate it to you. »

Source: TNA (Kew), ADM 223/767, MO5(e) War Diary, p.34.
Excerpt from a letter by Henderson (BEF Cipher section) to MO5(e), written on Sept 18th 1914.

# The French Army & Navy’s Cipher services in the Great War.

## II. Snippets of the wartime cooperation between French & Allied Cipher services

### ❖ French & American cooperation



Le Dé légué Général,
à M. le Commissaire Général
aux Affaires de Guerre Franco-Américaines.

Le Colonel Churchill, Chef du Military Intelligence Branch, du War Department, m'a recommandé tout particulièrement le Capitaine H.O. Yardley, qui est envoyé en France pour étudier les différents codes et chiffres employés dans la transmission des câbles.

Je vous serais particulièrement obligé de bien vouloir faciliter la mission du Capitaine Yardley, et le mettre en relation avec le Colonel Cartier, Chargé de la Section du Chiffre, au Cabinet du Ministre de la Guerre, et avec le Bureau du Chiffre au Département des Affaires Etrangères.

## Translation

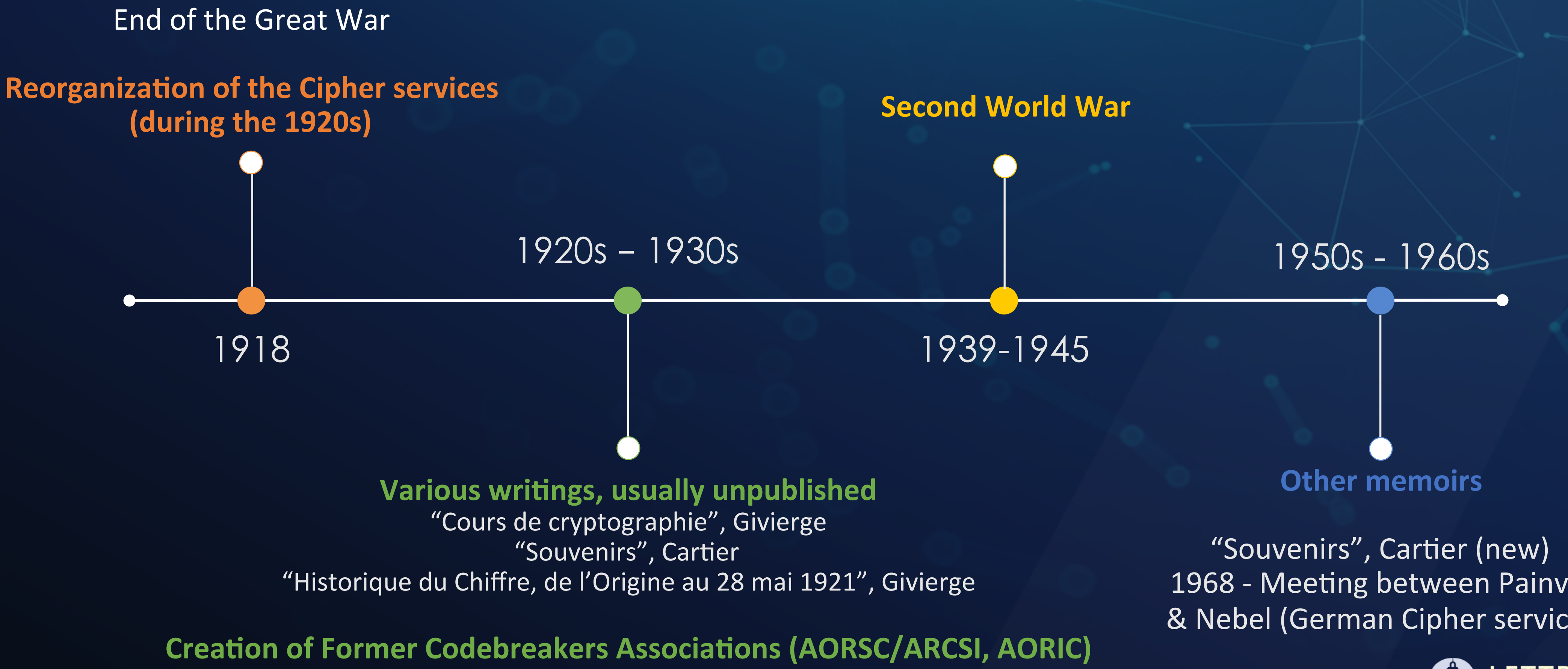
« Colonel Churchill, head of the Military Intelligence Branch of the War Department, has recommended captain H.O. Yardley to me: **he is sent in France in order to study various codes and ciphers employed in cable transmission**.

I would be especially obliged if you would facilitate the mission of Captain Yardley and **put him in touch with Colonel Cartier**, Head of the Cipher Section in the cabinet of the Minister of War, and with the Cipher Bureau of the Department of the Foreign Affairs as well. »

Source: Herbert Yardley, *The American Black Chamber*, French Letter of credentials dated August 6th 1918, to grant access to Yardley to French Cipher services.

# The French Army & Navy's Cipher services in the Great War.

## III. Icons & Memory of the French Cipher services



End of the Great War

Reorganization of the Cipher services
(during the 1920s)

1918

1920s – 1930s

**Various writings, usually unpublished**
"Cours de cryptographie", Givierge
"Souvenirs", Cartier
"Historique du Chiffre, de l'Origine au 28 mai 1921", Givierge

**Creation of Former Codebreakers Associations (AORSC/ARCSI, AORIC)**

Second World War

1939-1945

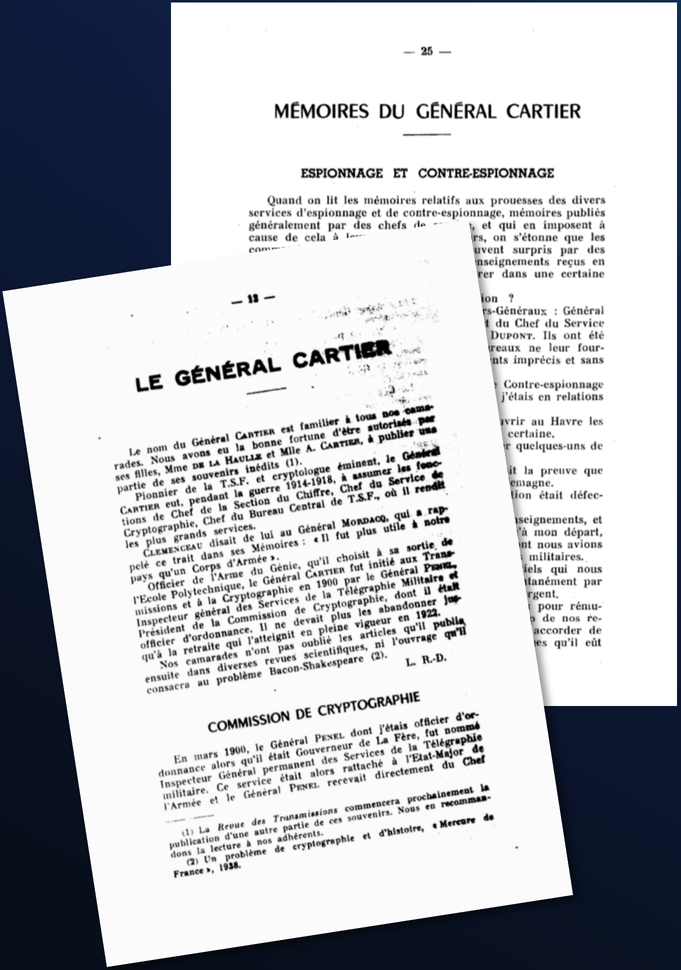
1950s - 1960s

**Other memoirs**

"Souvenirs", Cartier (new)
1968 - Meeting between Painvin
& Nebel (German Cipher service)

# The French Army & Navy's Cipher services in the Great War.

## III. Icons & Memory of the French Cipher services



— 25 —

MÉMOIRES DU GÉNÉRAL CARTIER

ESPIONNAGE ET CONTRE-ESPIONNAGE

Quand on lit les mémoires relatifs aux prouesses des divers services d'espionnage et de contre-espionnage, mémoires publiés généralement par des chefs de
, et qui en imposent à
cause de cela à
rs, on s'étonne que les
uvent surpris par des
nseignements reçus en
rer dans une certaine

ion ?
rs-Généraux : Général
t du Chef du Service
Dupont. Ils ont été
reaux ne leur four-
nts imprécis et sans

Contre-espionnage
j'étais en relations

vrir au Havre les
certaine.
r quelques-uns de

it la preuve que
emagne.
tion était défec-

nseignements, et
'à mon départ,
nt nous avions
militaires.
iels qui nous
tanément par
rgent.
pour rému-
de nos re-
accorder de
es qu'il eût

— 13 —

LE GÉNÉRAL CARTIER

Le nom du Général Cartier est familier à tous nos camarades. Nous avons eu la bonne fortune d'être autorisés par ses filles, Mme de la Haulle et Mlle A. Cartier, à publier une partie de ses souvenirs inédits (1).

Pionnier de la T.S.F. et cryptologue éminent, le Général Cartier eut, pendant la guerre 1914-1918, à assumer les fonctions de Chef de la Section du Chiffre, Chef du Service de Cryptographie, Chef du Bureau Central de T.S.F., où il rendit les plus grands services.

Clemenceau disait de lui au Général Mordacq, qui a rappelé ce trait dans ses Mémoires : « Il fut plus utile à notre pays qu'un Corps d'Armée ».

Officier de l'Arme du Génie, qu'il choisit à sa sortie de l'Ecole Polytechnique, le Général Cartier fut initié aux Transmissions et à la Cryptographie en 1900 par le Général Penel, Inspecteur général des Services de la Télégraphie Militaire et Président de la Commission de Cryptographie, dont il était officier d'ordonnance. Il ne devait plus les abandonner jusqu'à la retraite qui l'atteignit en pleine vigueur en 1922.

Nos camarades n'ont pas oublié les articles qu'il publia ensuite dans diverses revues scientifiques, ni l'ouvrage qu'il consacra au problème Bacon-Shakespeare (2).

L. R.-D.

COMMISSION DE CRYPTOGRAPHIE

En mars 1900, le Général Penel dont j'étais officier d'ordonnance alors qu'il était Gouverneur de La Fère, fut nommé Inspecteur Général permanent des Services de la Télégraphie militaire. Ce service était alors rattaché à l'Etat-Major de l'Armée et le Général Penel recevait directement du Chef

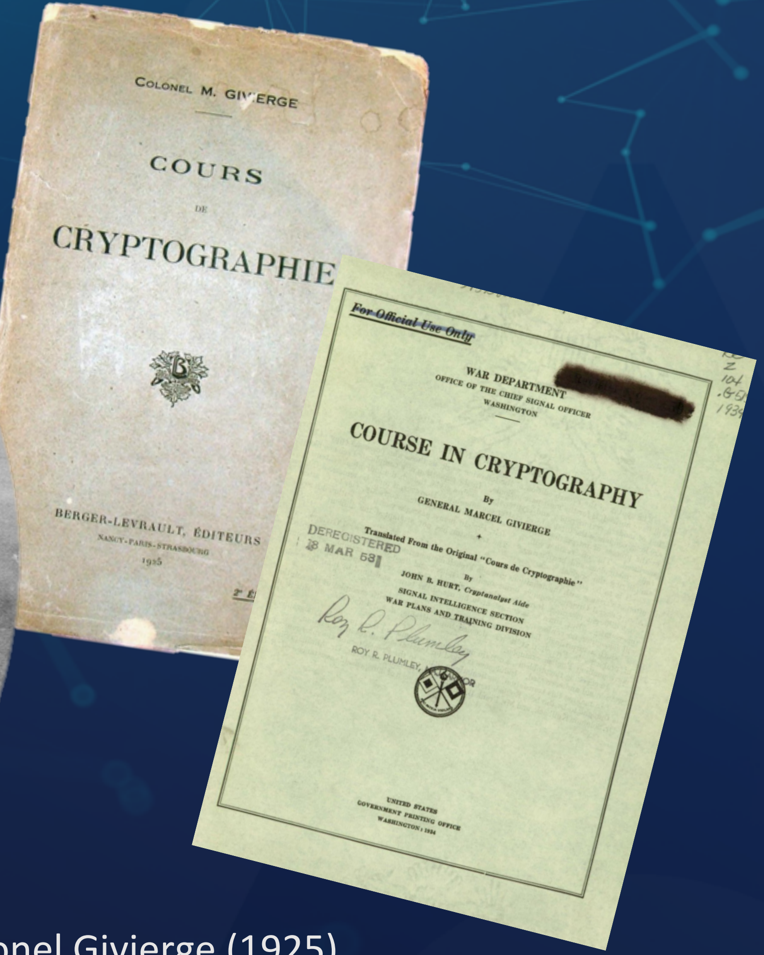
(1) La *Revue des Transmissions* commencera prochainement la publication d'une autre partie de ces souvenirs. Nous en recommandons la lecture à nos adhérents.

(2) Un problème de cryptographie et d'histoire, « Mercure de France », 1938.

*Souvenirs* by General Cartier, published in *Bulletin de l'ARC*, May & December 1958

François Cartier

Marcel Givierge



COLONEL M. GIVIERGE

COURS
DE
CRYPTOGRAPHIE

BERGER-LEVRAULT, ÉDITEURS
NANCY-PARIS-STRASBOURG
1925

2e É

For Official Use Only

WAR DEPARTMENT [redacted]
OFFICE OF THE CHIEF SIGNAL OFFICER
WASHINGTON

COURSE IN CRYPTOGRAPHY

By
GENERAL MARCEL GIVIERGE

Translated From the Original "Cours de Cryptographie"
By
JOHN B. HURT, Cryptanalyst Aide
SIGNAL INTELLIGENCE SECTION
WAR PLANS AND TRAINING DIVISION

DEREGISTERED
18 MAR 58

Roy R. Plumley
ROY R. PLUMLEY,

UNITED STATES
GOVERNMENT PRINTING OFFICE
WASHINGTON : 1934

Z
104
.G5
1934

*Cours de cryptographie*, by Colonel Givierge (1925)
Translated as *Course in cryptography* (1934)

LETTRES
SORBONNE
UNIVERSITÉ

# The French Army & Navy's Cipher services in the Great War.

## III. Icons & Memory of the French Cipher services

### Georges-Jean Painvin

### Quote from H.O. Yardley, *The American Black Chamber* (1931) :

« When I explained my mission to Colonel Cartier, he immediately called in **Captain Georges Painvin, the great cipher genius of France.** For weeks I had looked forward to meeting the brilliant Painvin, the most skilful cryptographer in all the Allied Governments. […] [When] he saw that I followed his analysis of several difficult problems, he gradually thawed out. **Eventually we grew to be fast friends.** I became an intimate member of his household […] Painvin gave me a desk in his office and opened his files to me, and I made the most of the opportunity to study under this master, **whose instruction and inspiration were to stand me in good stead**, when later, from 1919 to 1929, I directed the energies of a group of cryptographers »

LETTRES SORBONNE UNIVERSITÉ

04

# From C-36 to CP8 Smart Card

Jean-Louis Desvignes

LETTRES
SORBONNE
UNIVERSITÉ

# Presentation Outline

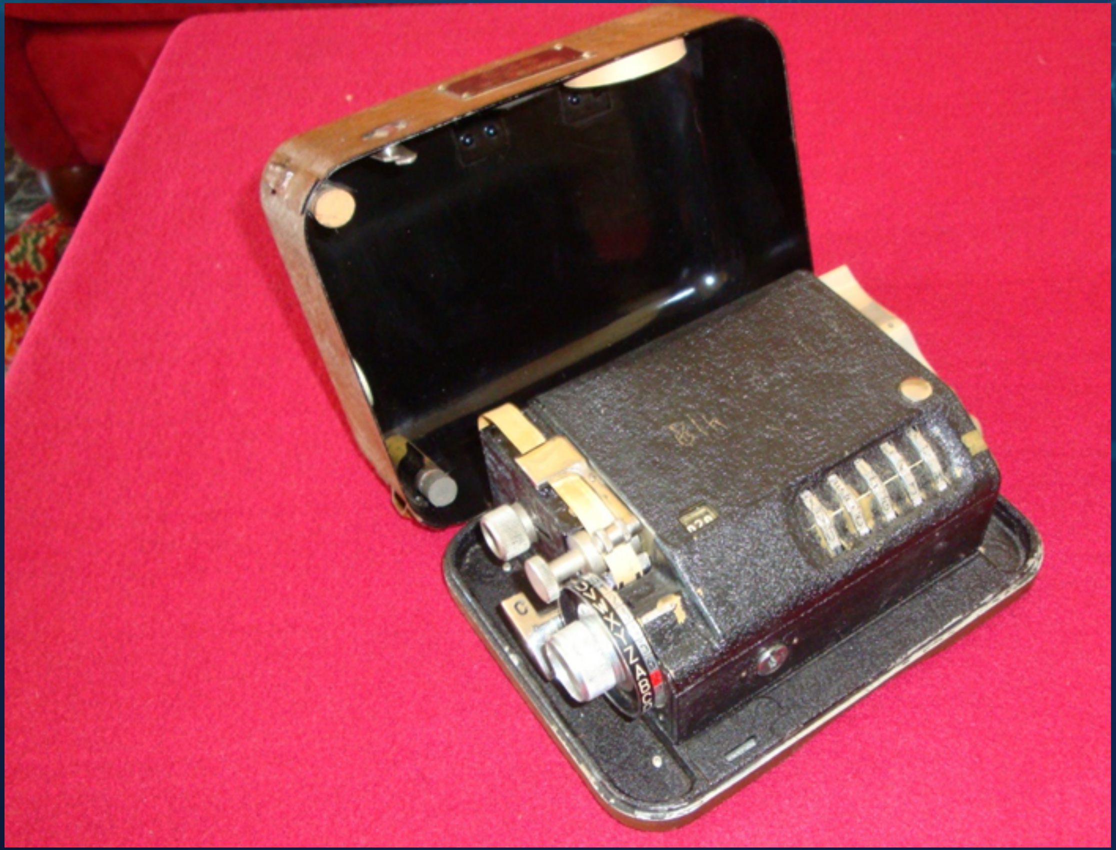
- 1 - Dark period after the successes of WW1
- 2 - New spring: MYOSOTIS
- 3 - Great success for tactical forces: RITA
- 4 - Success for strategic communications: RETINAT
- 5 - Worldwide success: the SMART CARD

LETTRES SORBONNE UNIVERSITÉ

# 1918

- Victors delighted to be asked to keep a low profile on the precious help of cryptanalysis …
- But from discretion to oblivion there was only one step …

# Hagelin C-36 (French) = M-209 (US)



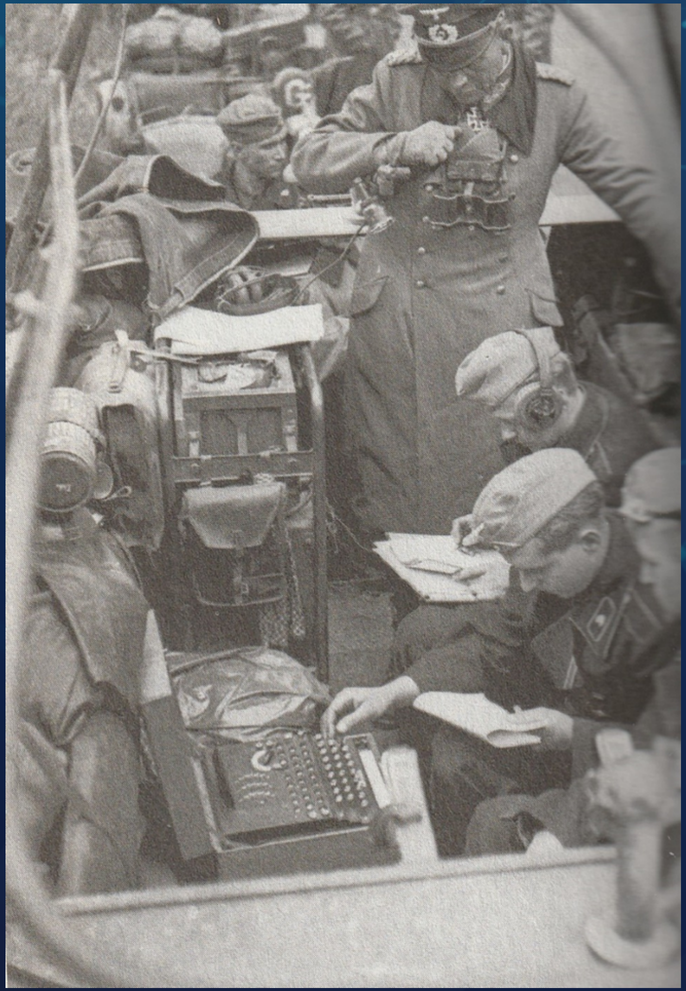
# HAGELIN B211

- B211 = B21 + a printer
- 500 units in 1939
- Strategic level

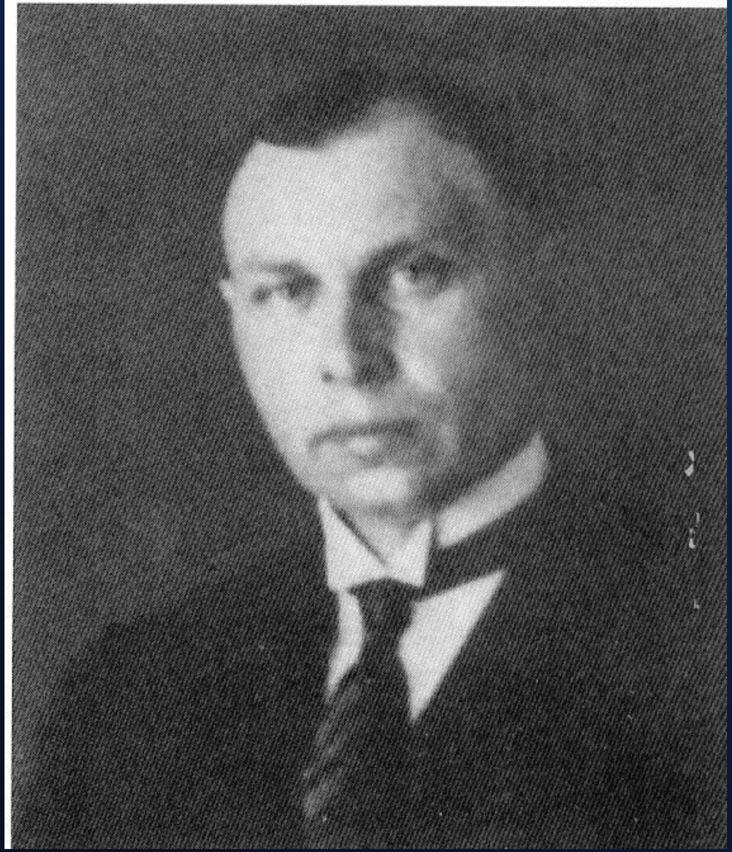
LETTRES
SORBONNE
UNIVERSITÉ

# … then

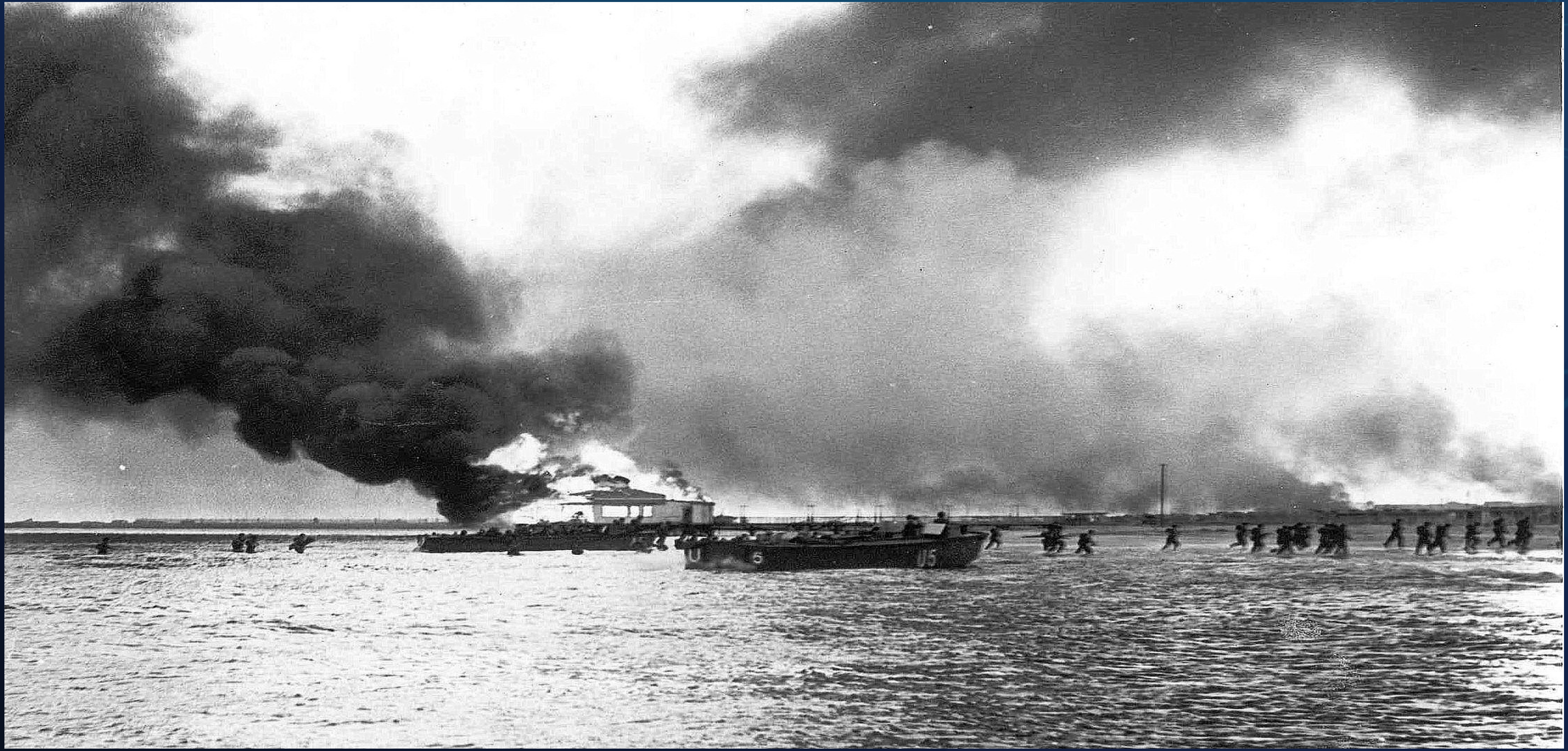
- The ENIGMAs were used inside the armored divisions
- The B211 were fixed



# The betrayal of Hans Thilo Schmidt



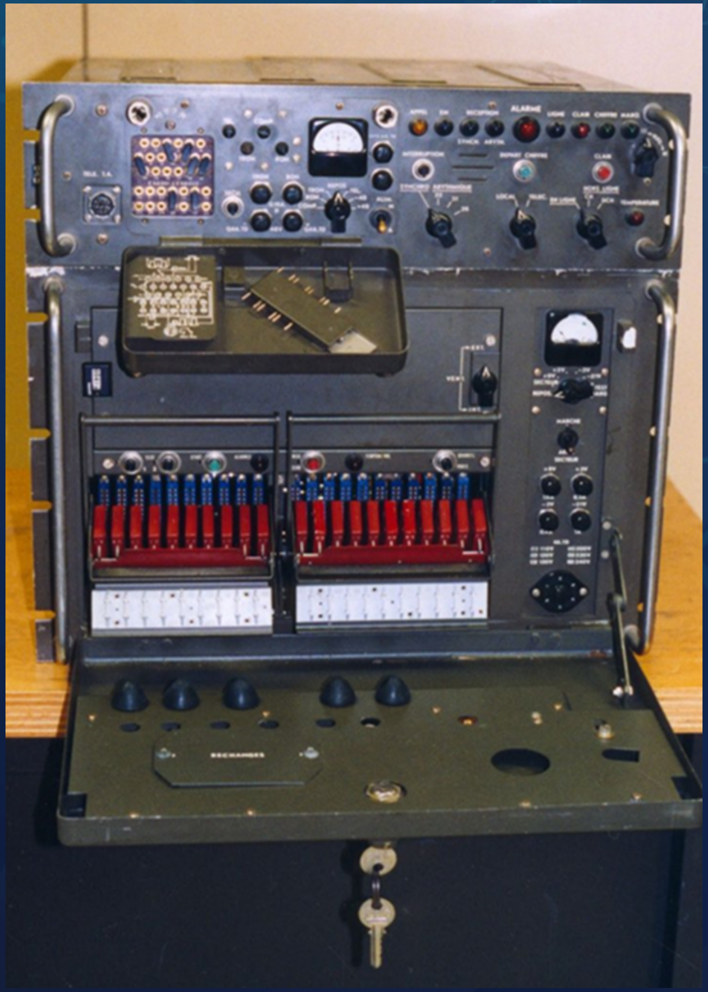
# 1956 Franco-British Expedition on the Suez Canal



LETTRES
SORBONNE
UNIVERSITÉ

# A new spring: Myosotis (Forget me not)

- First french electronic machine (1965)
- No rotor => Permutators
- NATO SECRET approved
- Used by the 3 services and diplomacy



# 2 events that boosted French army telecommunications

- 1967 General de Gaulle makes France go out of the NATO integrated organisation
- The Army has to reinvent its own means of communication

- 1968 the general strike affecting the government's telecommunications pushes it to create a resilient military telecommunications network.

LETTRES SORBONNE UNIVERSITÉ

# RITA By Thomson-CSF (now THALES)

- The first military tactical digital network with integrated services: phone, telex, fax and data
- Bulk encryption
- Mobile subscribers equiped with enciphered radio set
- In fact, RITA = GSM network 20 years ahead!
- Chosen by D. Reagan for US ARMY  MSE

# A cell phone?? A bit heavy though!!

# RETINAT: the first X.25 Strategic Network

- Réseau
- de Transport
- des Informations
- Numériques
- de l’Armée
- de Terre

- Network
- For Transportation
- of digital
- Informations
- For Land
- Forces

LETTRES
SORBONNE
UNIVERSITÉ

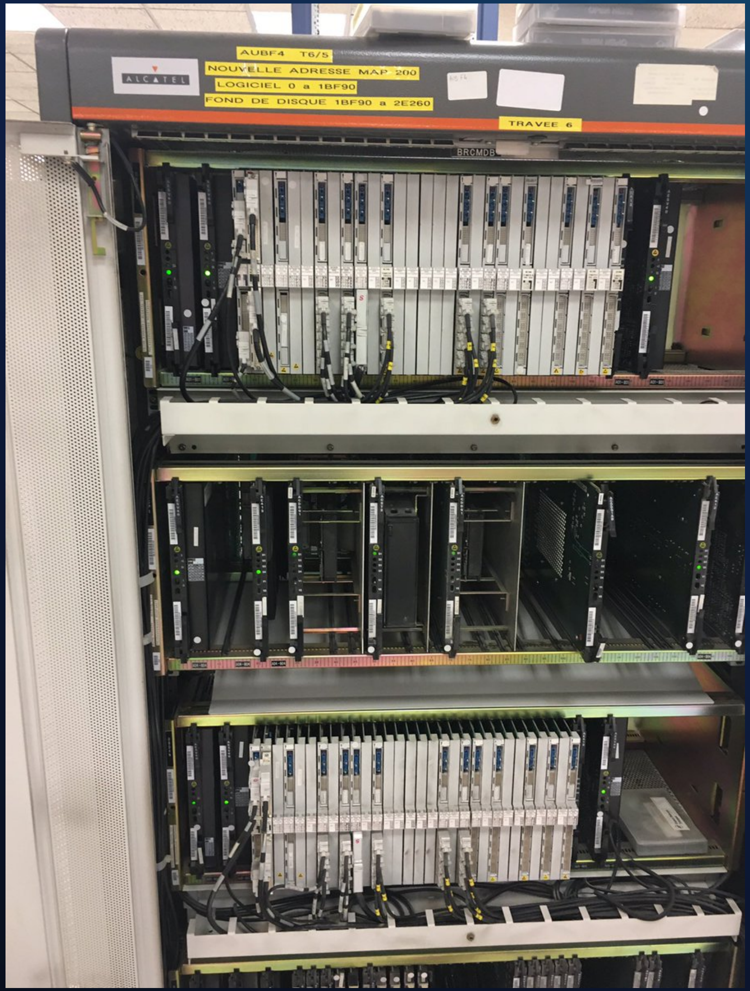
# Louis Pouzin

- Inventor of the datagram
- He created and developed a Network in the early 1970s, based on pure datagrams, and contributed to the development of packet-switched networks, the precursors of the Internet.

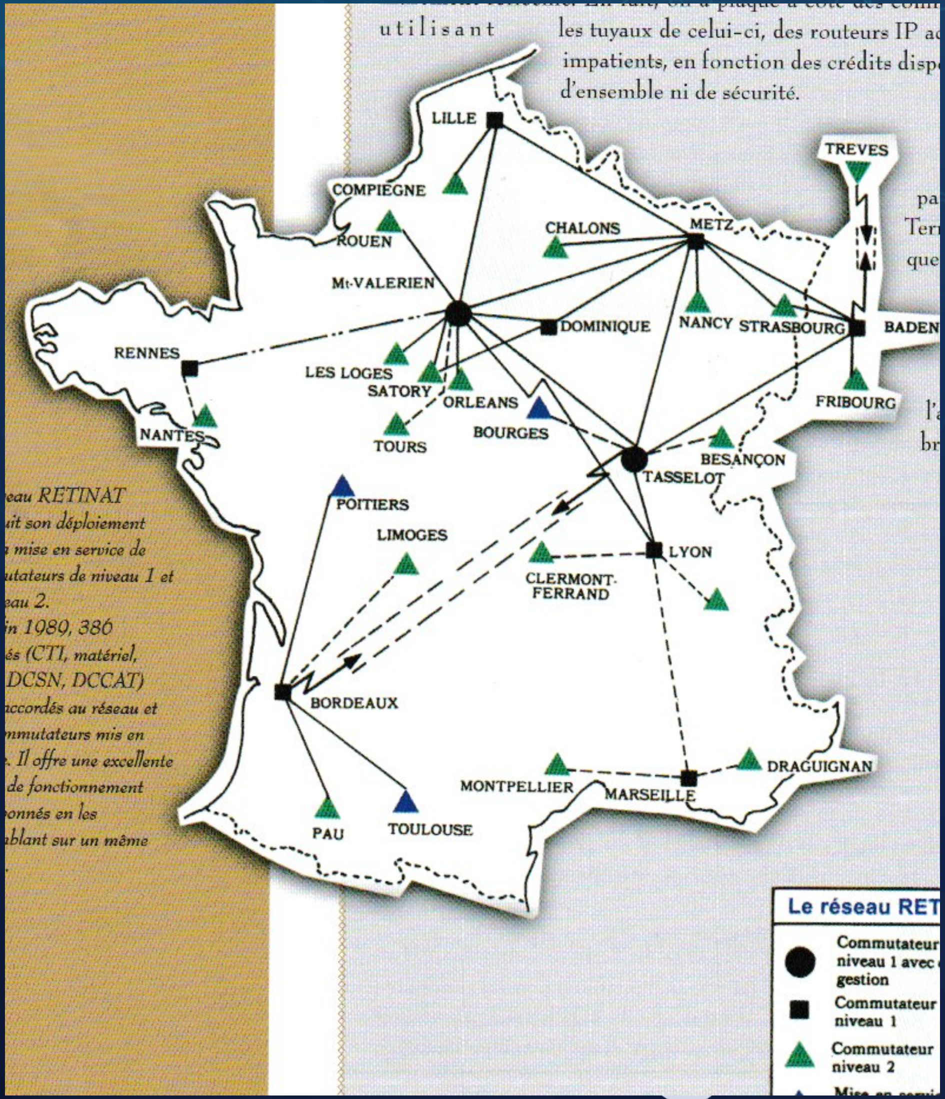
# RETINAT: Some Specifications

- Standard: X.25
- Security of the network:
  - ❖ All the management traffic encrypted  by a specific crypto card grafted on the motherboard of the switches
  - ❖ Very original and innovative  at the time!
- Redundancy of the switches and the links
- Interoperable with the public Network TRANSPAC
- Security of subscribers:
  - ❖ Capucine: the X.25 Packet-switched network crypto equipment

# Switch RETINAT



# SCHEME of the Network


utilisant

les tuyaux de celui-ci, des routeurs IP ac
impatients, en fonction des crédits disp
d'ensemble ni de sécurité.

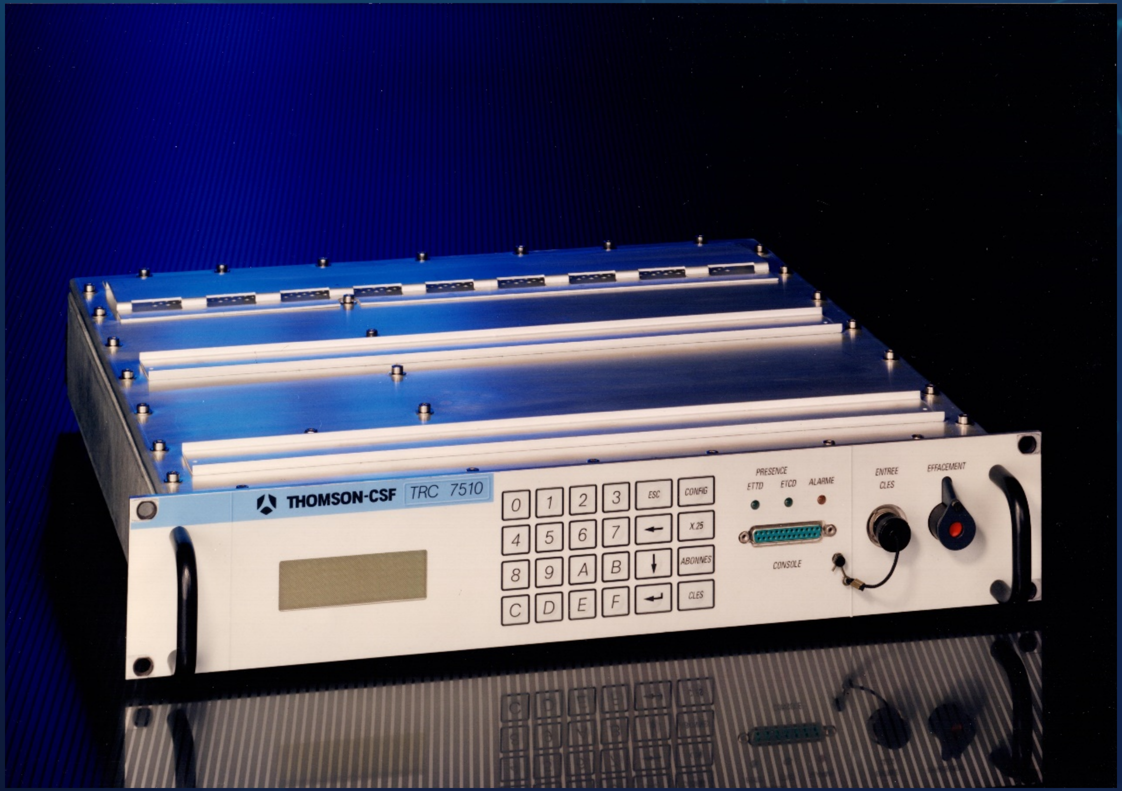
*eau RETINAT*
*uit son déploiement*
*a mise en service de*
*utateurs de niveau 1 et*
*eau 2.*
*in 1989, 386*
*és (CTI, matériel,*
*DCSN, DCCAT)*
*accordés au réseau et*
*mmutateurs mis en*
*. Il offre une excellente*
*de fonctionnement*
*onnés en les*
*ablant sur un même*

Le réseau RET

| | |
|---|---|
| ● | Commutateur niveau 1 avec gestion |
| ■ | Commutateur niveau 1 |
| ▲ | Commutateur niveau 2 |
| ▲ | Mise en servic |

# CAPUCINE (TRC 796)

- Standard: X.25
- SECRET DEFENSE approved by SCSSI and SECRET UEO after a second evaluation by BSI (Germany)
- Presented to an ACCSA  WG during discussions about Packet-switched  crypto equipment



LETTRES SORBONNE UNIVERSITÉ

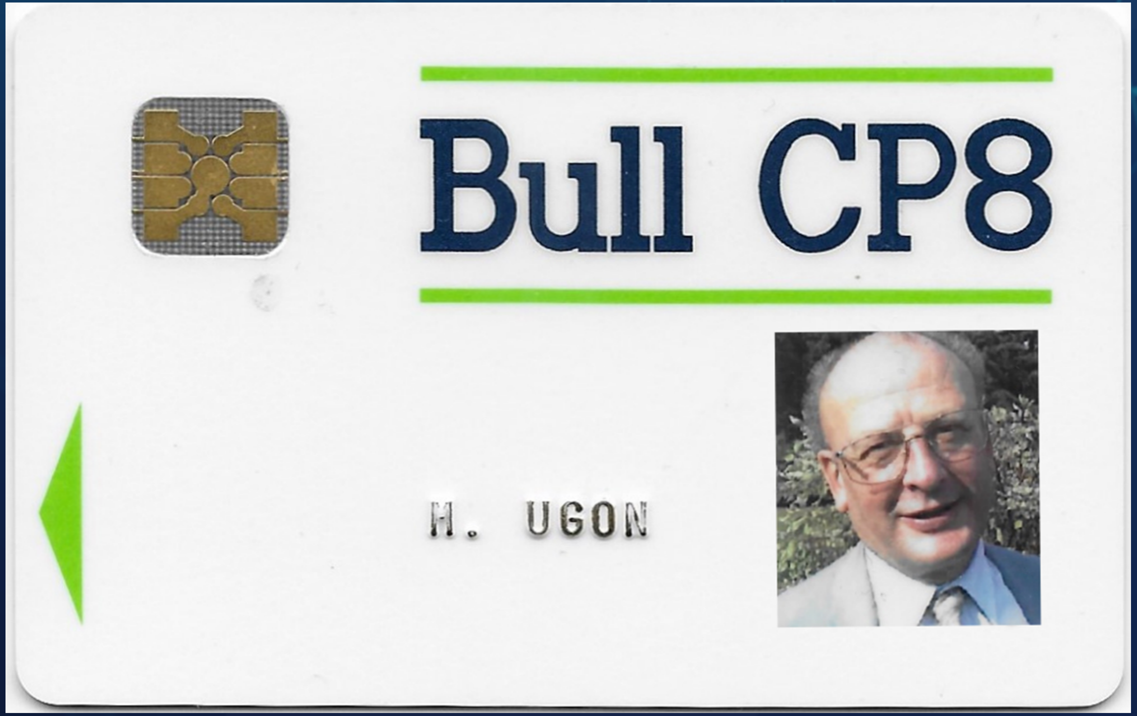
# ECHINOPS: IP Encryptor: second evaluation by CESG

ECHINOPS : *Sécurité des reseaux IP classifiés*

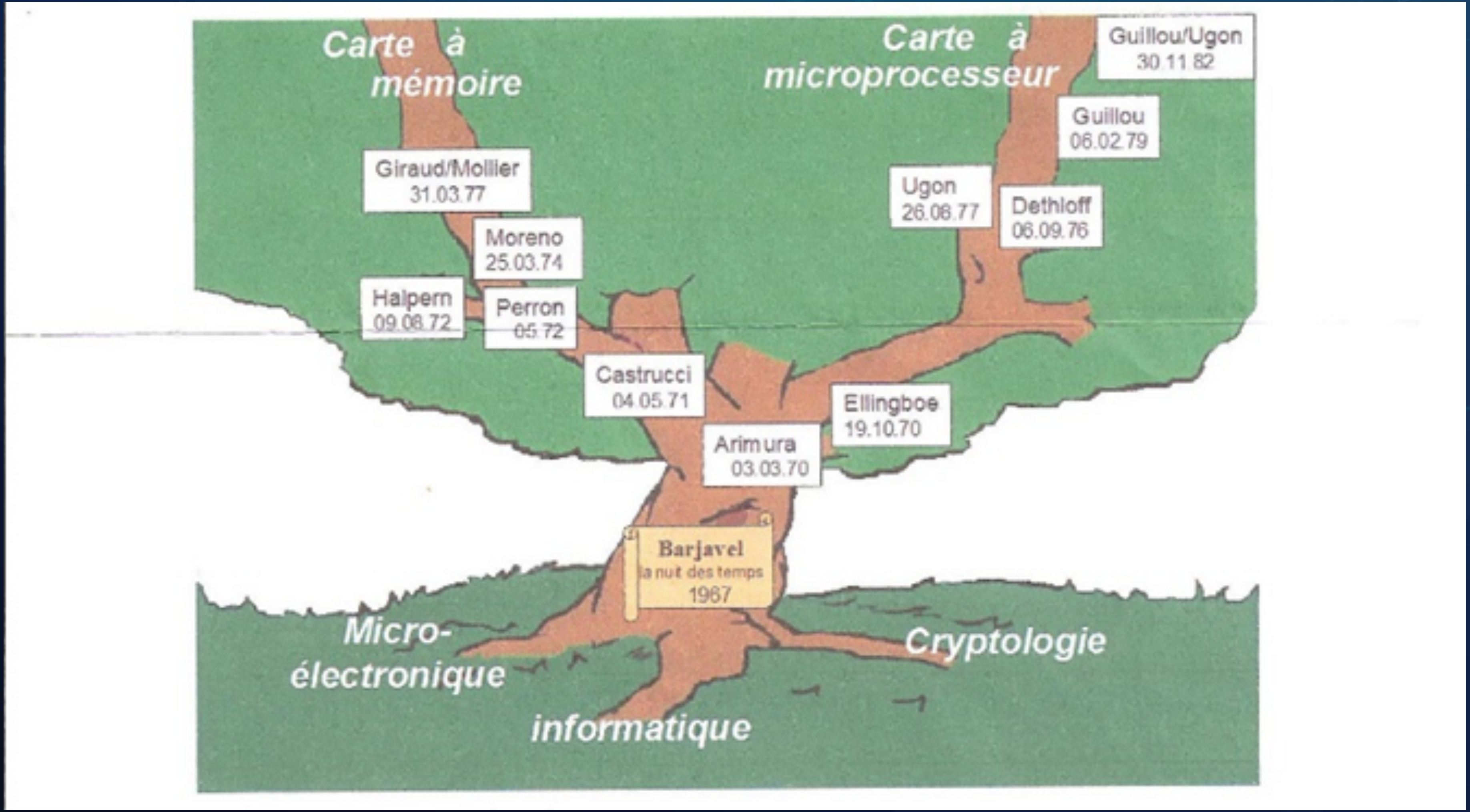
LETTRES
SORBONNE
UNIVERSITÉ

# Michel Ugon

- In March 1979, Michel Ugon from Bull CP8 was the first to design and develop a microprocessor-based card combining a processor and local memory



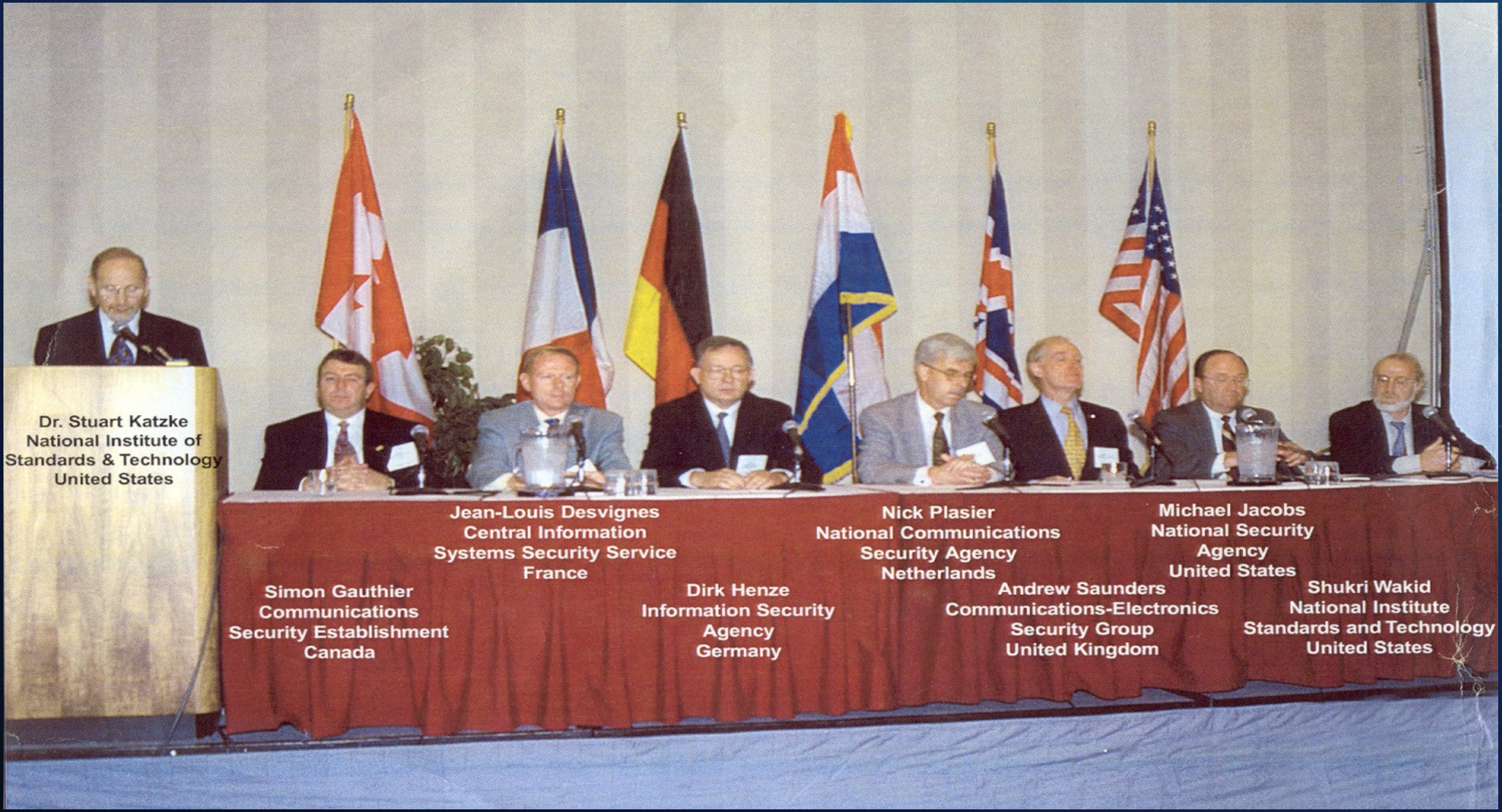
# The smart card patent tree



# A Global Commercial Success

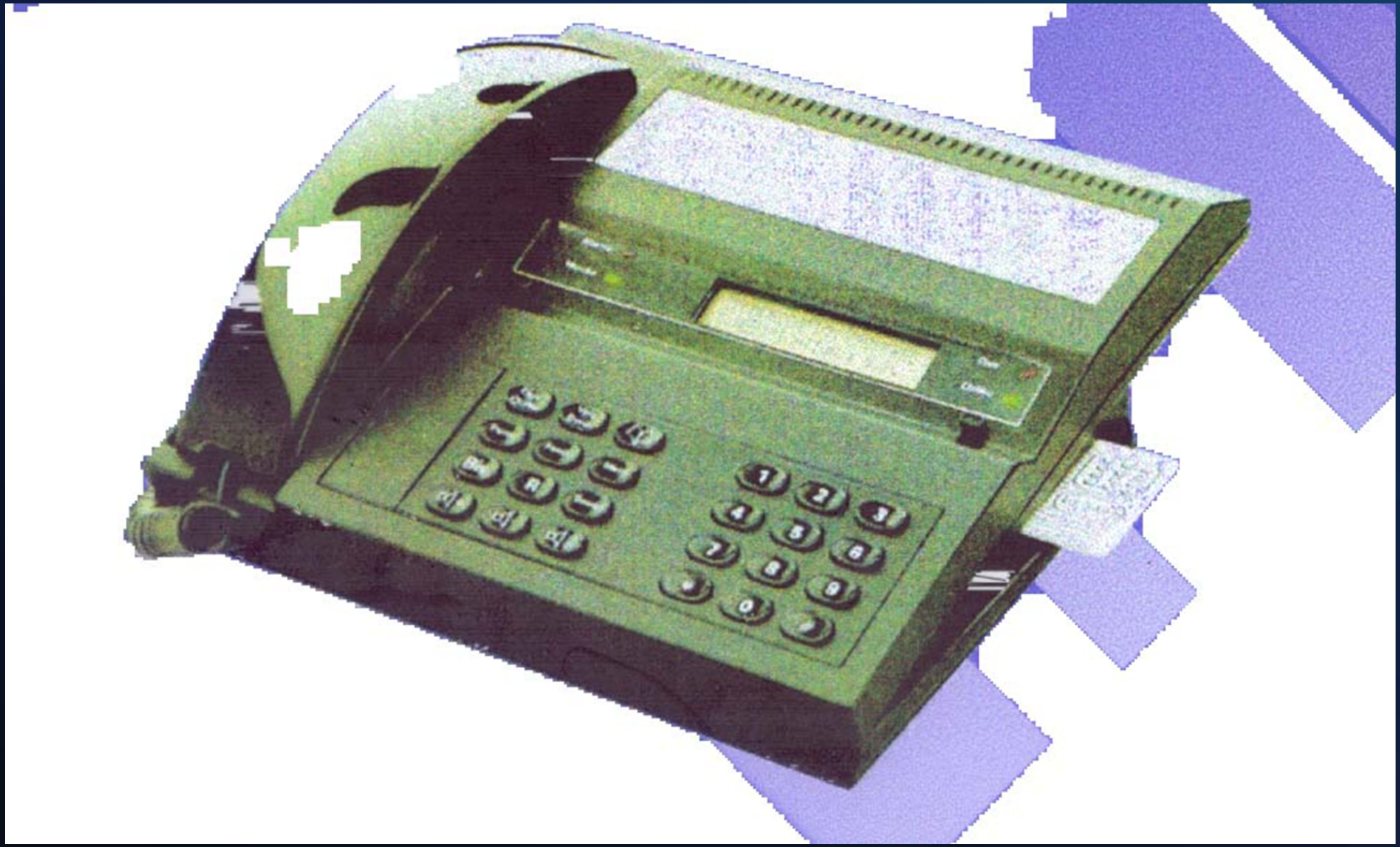
- Billions of smart cards around the world in all areas

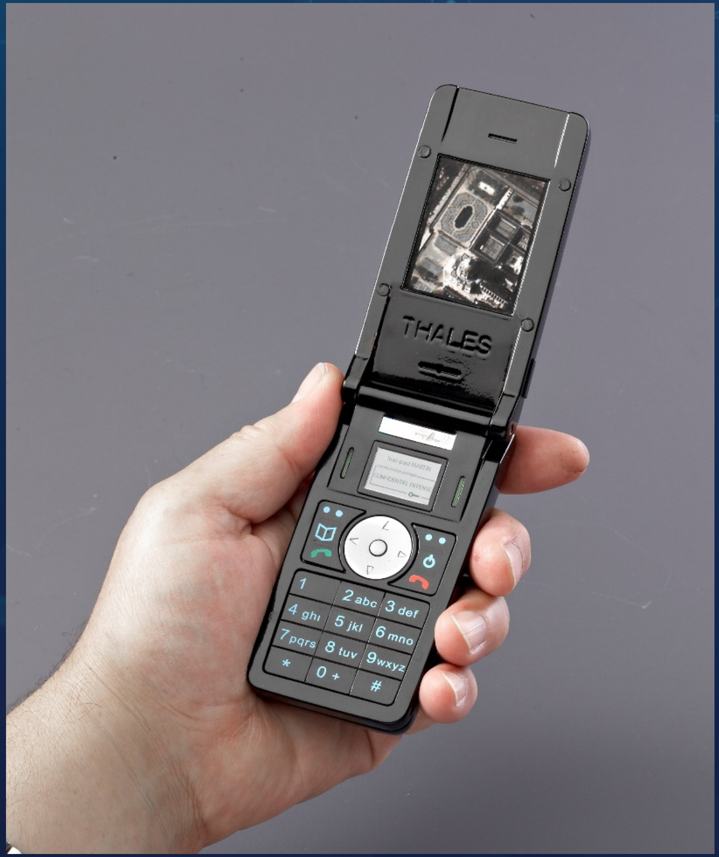
# 1998 Signature of mutual recognition agreements



# Smart cards for keing crypto equipments: Symmetric system: DCS 500 Asymmetric system: TEOREM

- Ssyems





# Conclusion

- After the setbacks of the Second World War, France experienced a real revival in terms of security of its information systems. It approaches the 21st century in good conditions, as Jean-Jacques Quisquater will show you.
- Thank you for your attention.

05

# From Smart Cards to Today 1967-2022

Jean-Jacques Quisquater

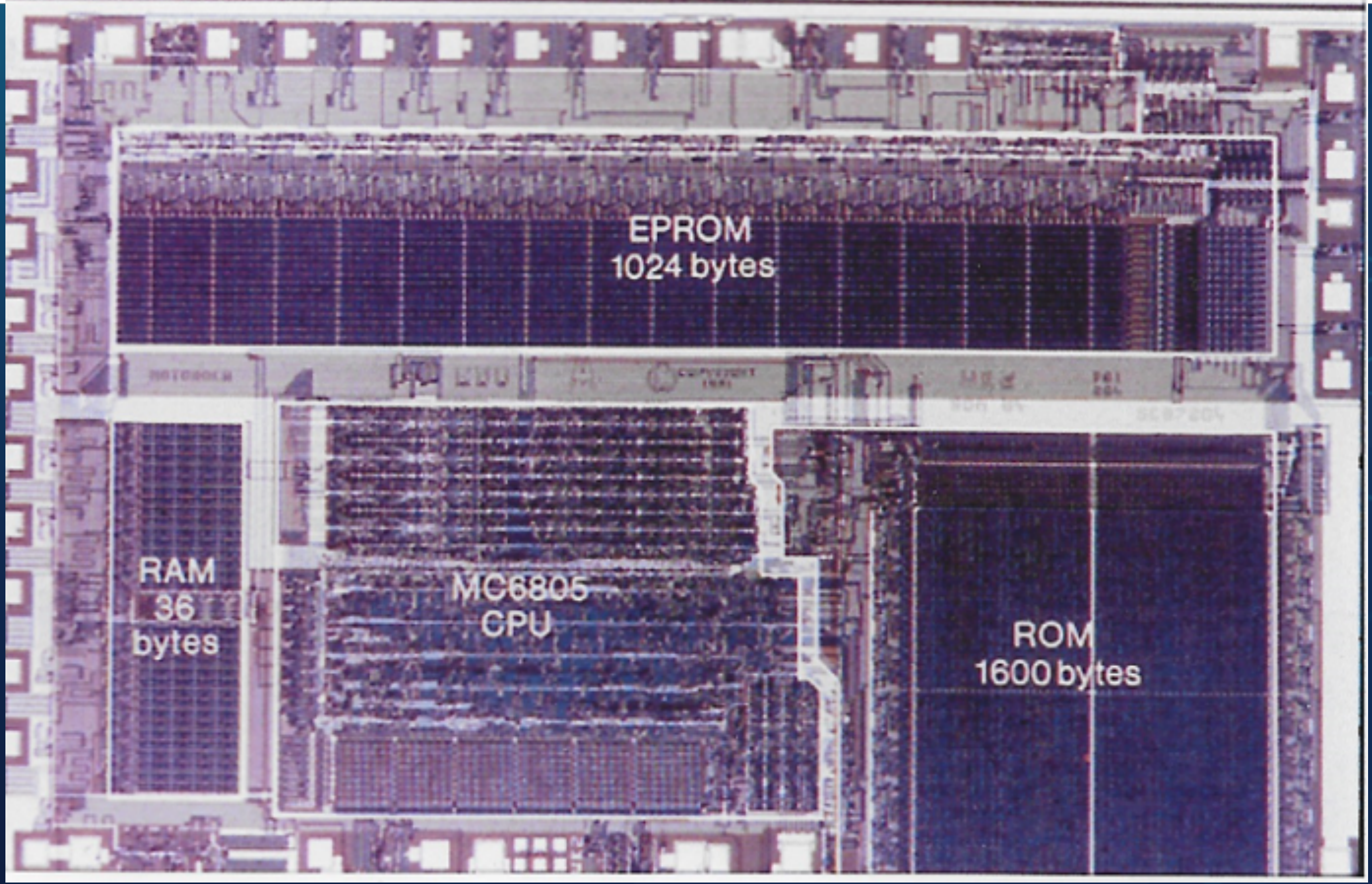
UCLouvain

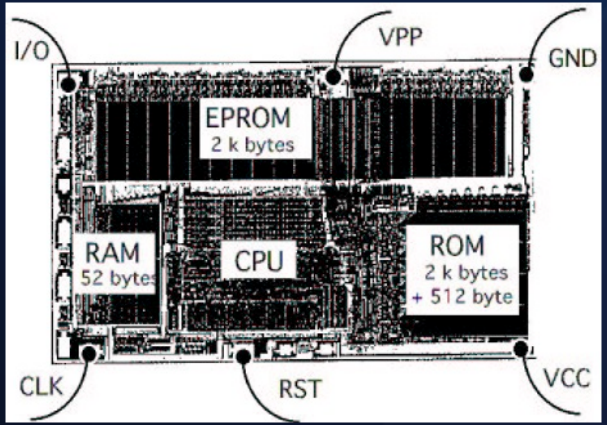
jjq@uclouvain.be

jjq@mit.edu

LETTRES SORBONNE UNIVERSITÉ

# Smart cards:
# Michel Ugon and …



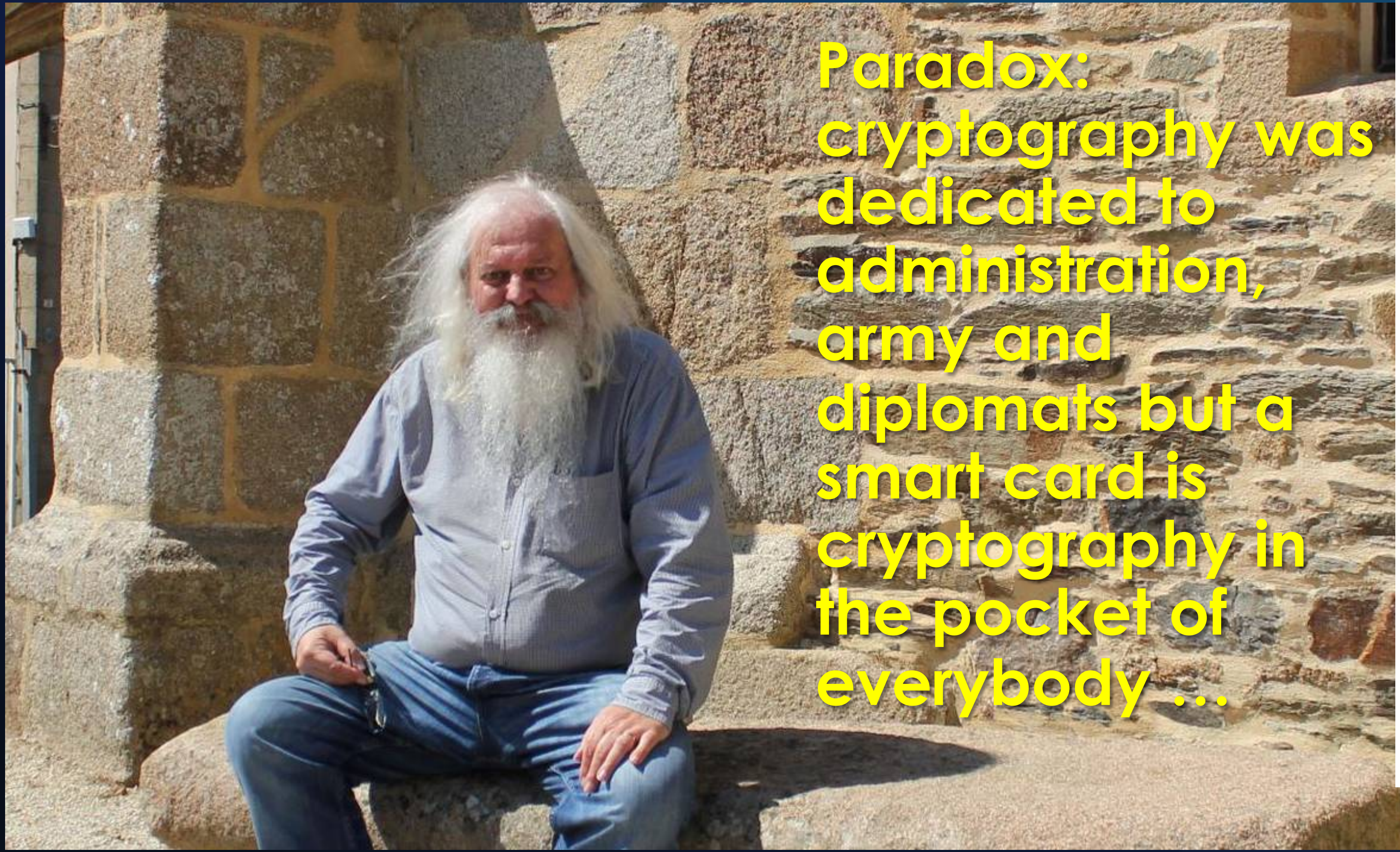


DES
+ OS

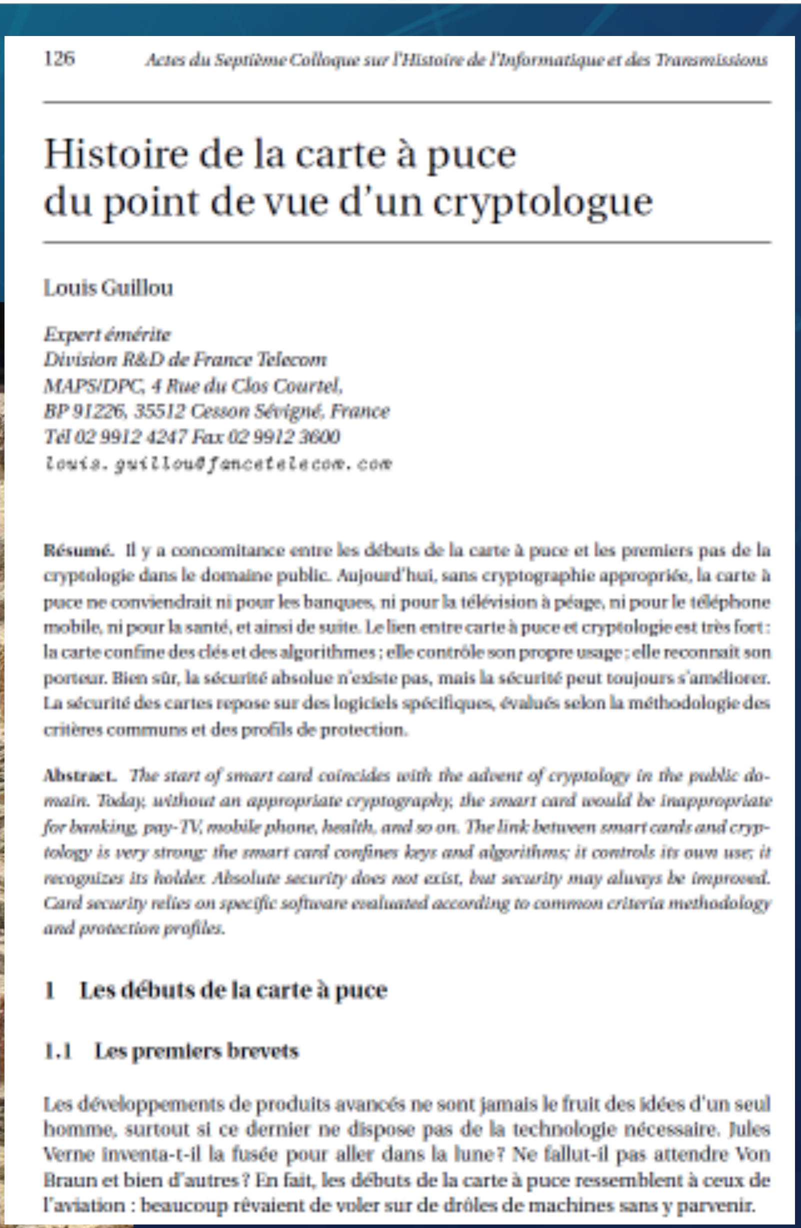
LETTRES
SORBONNE
UNIVERSITÉ

# … Louis Guillou

**2004:**
**Session president :**
**Jean-Louis Desvignes**



Paradox: cryptography was dedicated to administration, army and diplomats but a smart card is cryptography in the pocket of everybody …



## Histoire de la carte à puce du point de vue d'un cryptologue

Louis Guillou

*Expert émérite*
*Division R&D de France Telecom*
*MAPS/DPC, 4 Rue du Clos Courtel,*
*BP 91226, 35512 Cesson Sévigné, France*
*Tél 02 9912 4247 Fax 02 9912 3600*
`louis.guillou@fancetelecom.com`

**Résumé.** Il y a concomitance entre les débuts de la carte à puce et les premiers pas de la cryptologie dans le domaine public. Aujourd'hui, sans cryptographie appropriée, la carte à puce ne conviendrait ni pour les banques, ni pour la télévision à péage, ni pour le téléphone mobile, ni pour la santé, et ainsi de suite. Le lien entre carte à puce et cryptologie est très fort : la carte confine des clés et des algorithmes ; elle contrôle son propre usage ; elle reconnait son porteur. Bien sûr, la sécurité absolue n'existe pas, mais la sécurité peut toujours s'améliorer. La sécurité des cartes repose sur des logiciels spécifiques, évalués selon la méthodologie des critères communs et des profils de protection.

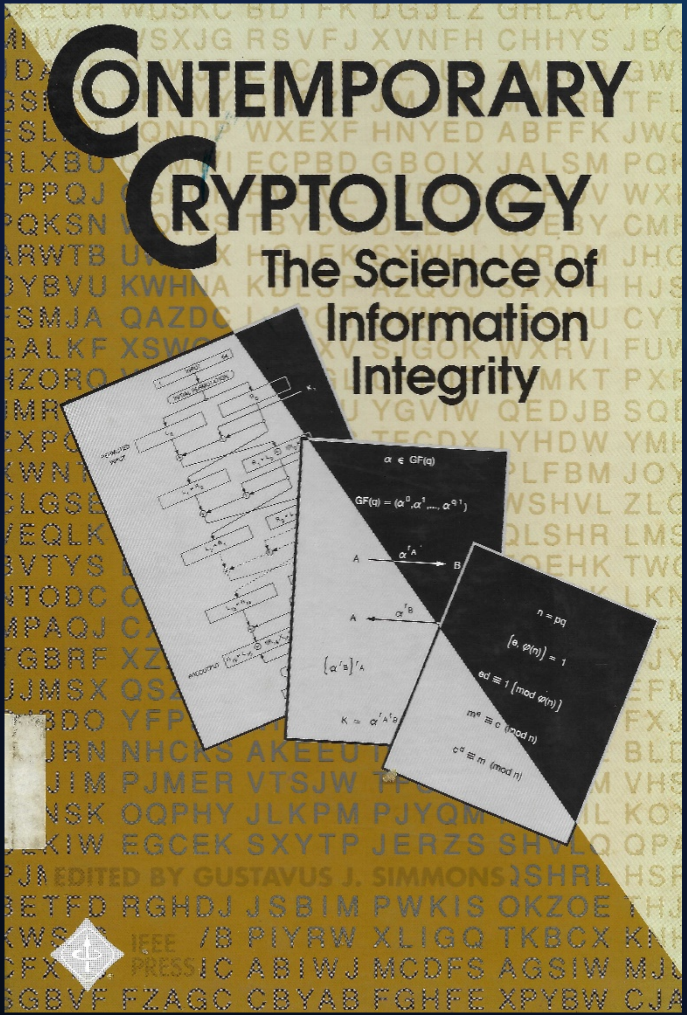
**Abstract.** *The start of smart card coincides with the advent of cryptology in the public domain. Today, without an appropriate cryptography, the smart card would be inappropriate for banking, pay-TV, mobile phone, health, and so on. The link between smart cards and cryptology is very strong: the smart card confines keys and algorithms; it controls its own use; it recognizes its holder. Absolute security does not exist, but security may always be improved. Card security relies on specific software evaluated according to common criteria methodology and protection profiles.*

### 1 Les débuts de la carte à puce

#### 1.1 Les premiers brevets

Les développements de produits avancés ne sont jamais le fruit des idées d'un seul homme, surtout si ce dernier ne dispose pas de la technologie nécessaire. Jules Verne inventa-t-il la fusée pour aller dans la lune? Ne fallut-il pas attendre Von Braun et bien d'autres? En fait, les débuts de la carte à puce ressemblent à ceux de l'aviation : beaucoup rêvaient de voler sur de drôles de machines sans y parvenir.

# Smart Cards in an IEEE book by Gus Simmons (Sandia Labs)

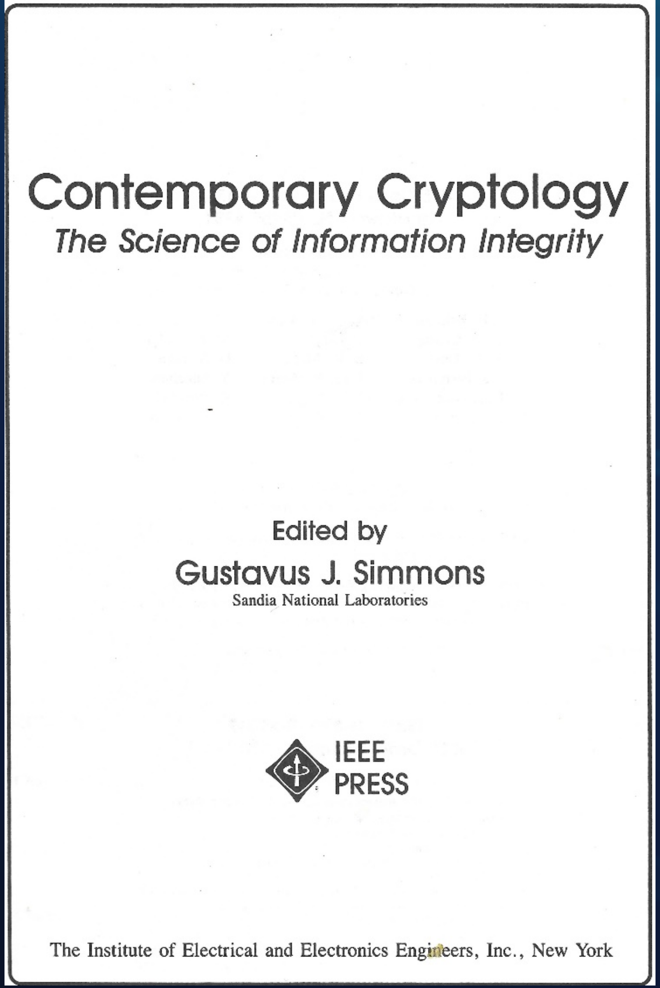


CONTEMPORARY CRYPTOLOGY

The Science of Information Integrity

EDITED BY GUSTAVUS J. SIMMONS

IEEE PRESS



Contemporary Cryptology

*The Science of Information Integrity*

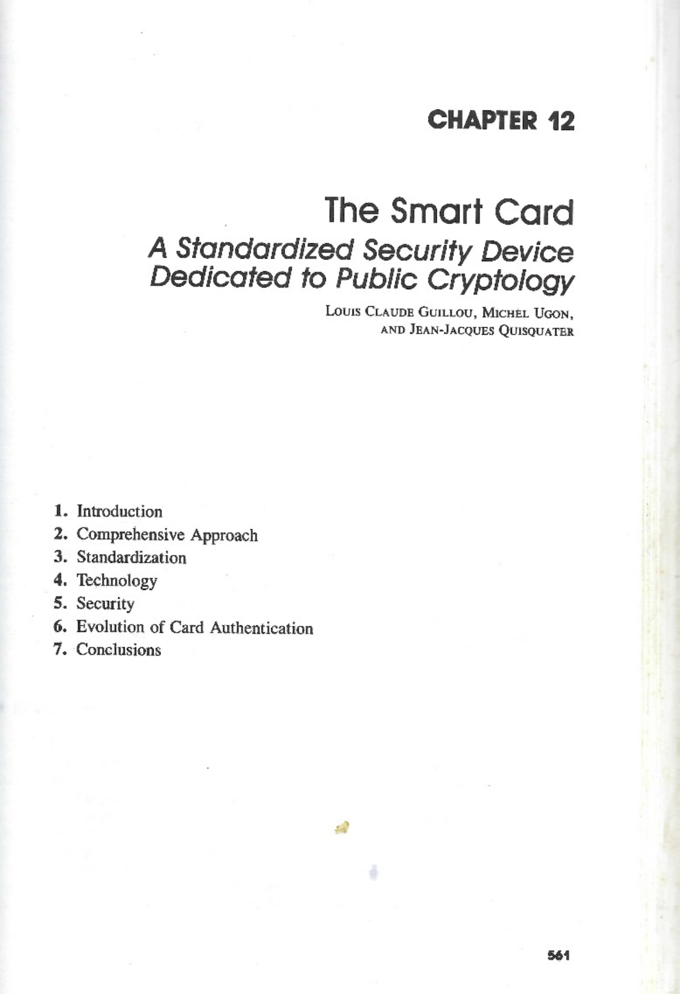
Edited by

Gustavus J. Simmons

Sandia National Laboratories

IEEE PRESS

The Institute of Electrical and Electronics Engineers, Inc., New York



CHAPTER 12

The Smart Card

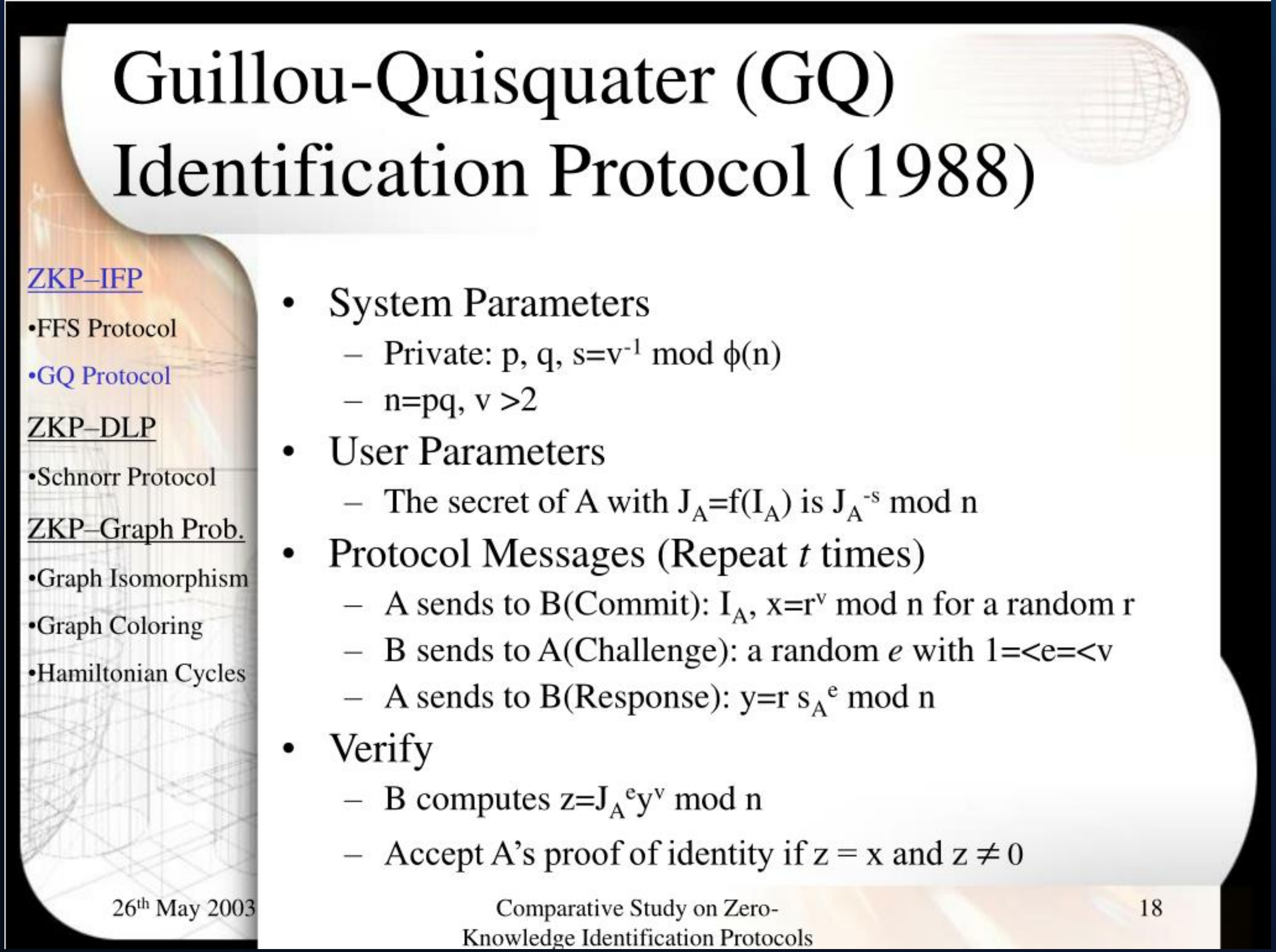
*A Standardized Security Device Dedicated to Public Cryptology*

Louis Claude Guillou, Michel Ugon, and Jean-Jacques Quisquater

1. Introduction
2. Comprehensive Approach
3. Standardization
4. Technology
5. Security
6. Evolution of Card Authentication
7. Conclusions

1992

# GQ – GQ2 – aso used by Novell



## Guillou-Quisquater (GQ) Identification Protocol (1988)

ZKP–IFP

•FFS Protocol

•GQ Protocol

ZKP–DLP

•Schnorr Protocol

ZKP–Graph Prob.

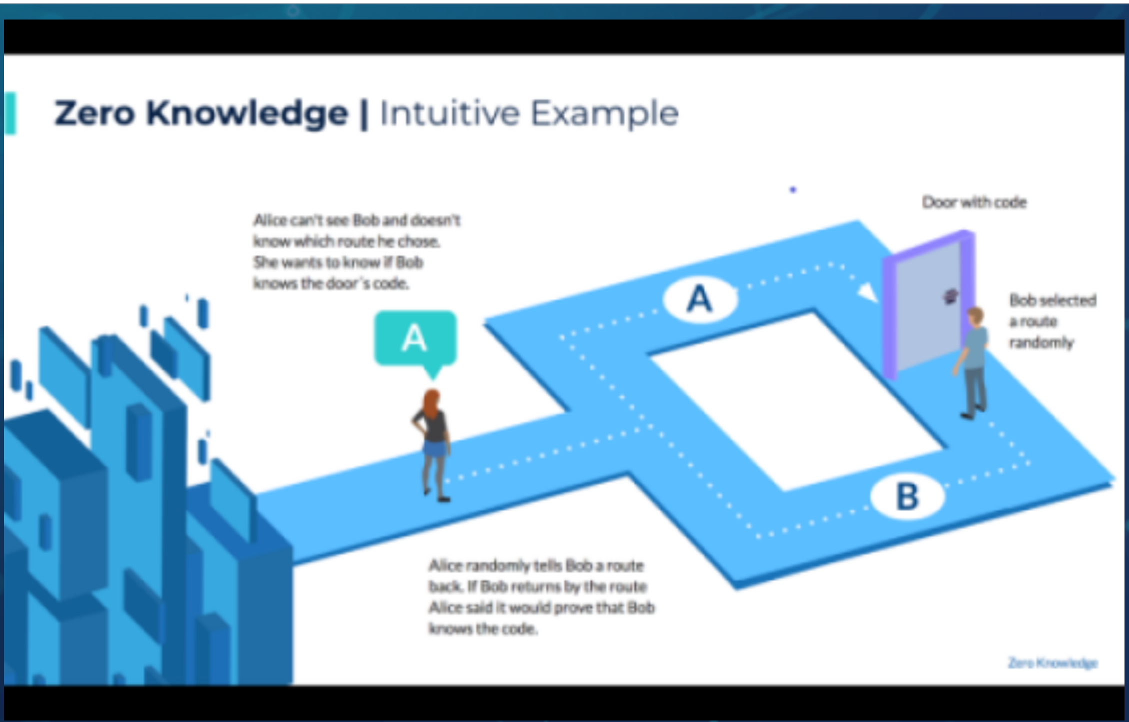
•Graph Isomorphism

•Graph Coloring

•Hamiltonian Cycles

- System Parameters
  - Private: p, q, $s=v^{-1} \bmod \phi(n)$
  - $n=pq$, $v>2$
- User Parameters
  - The secret of A with $J_A=f(I_A)$ is $J_A^{-s} \bmod n$
- Protocol Messages (Repeat *t* times)
  - A sends to B(Commit): $I_A$, $x=r^v \bmod n$ for a random r
  - B sends to A(Challenge): a random *e* with 1=<e=<v
  - A sends to B(Response): $y=r\, s_A^e \bmod n$
- Verify
  - B computes $z=J_A^e y^v \bmod n$
  - Accept A's proof of identity if $z = x$ and $z \neq 0$

26th May 2003 Comparative Study on Zero-Knowledge Identification Protocols 18



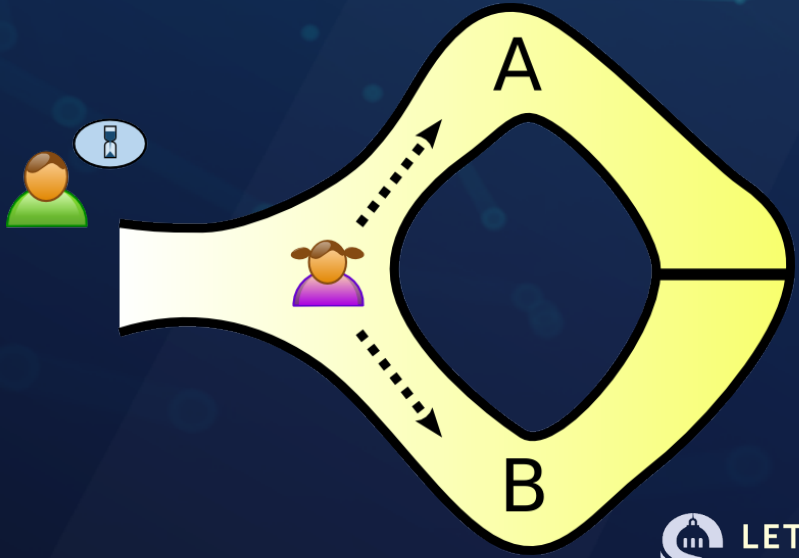
**Zero Knowledge** | Intuitive Example

Alice can't see Bob and doesn't know which route he chose. She wants to know if Bob knows the door's code.

Door with code

Bob selected a route randomly

Alice randomly tells Bob a route back. If Bob returns by the route Alice said it would prove that Bob knows the code.



LETTRES SORBONNE UNIVERSITÉ

# EUROCRYPT 1984: Paris

Lecture Notes in Computer Science

Edited by G. Goos and J. Hartmanis

209

Advances in Cryptology

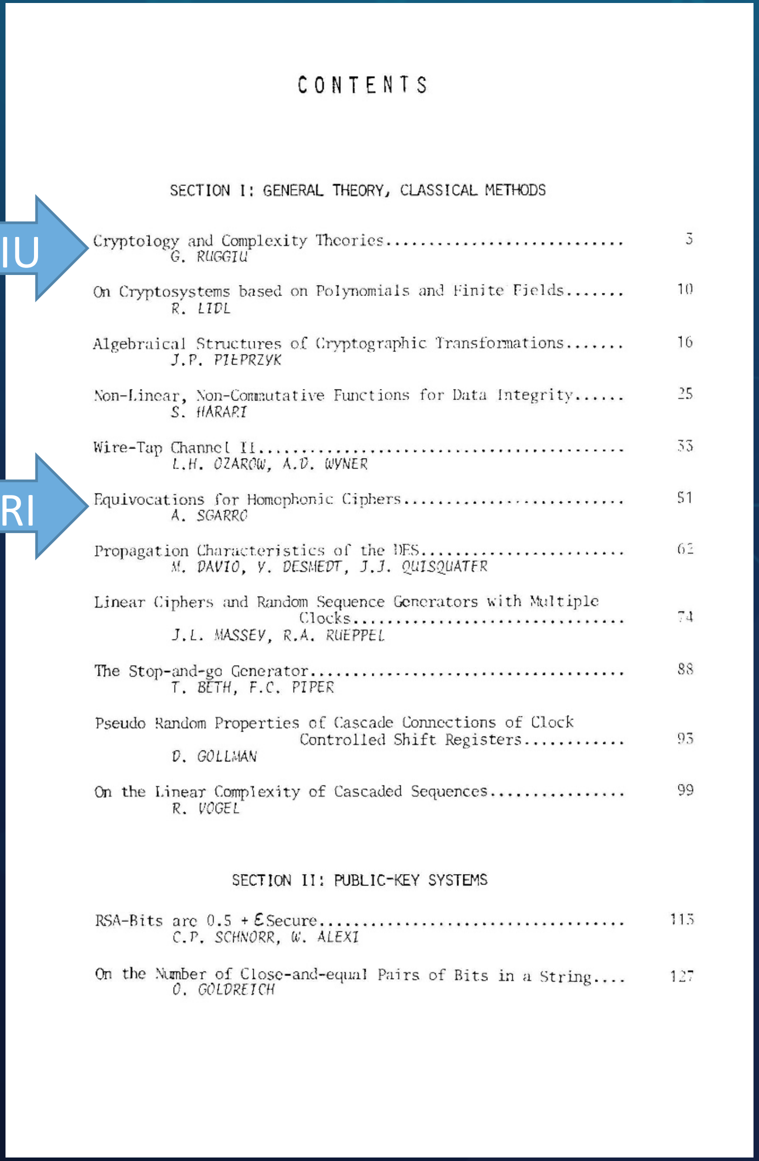
Proceedings of EUROCRYPT 84
A Workshop on the Theory and Application
of Cryptographic Techniques
Paris, France, April 1984

Edited by T. Beth, N. Cot and I. Ingemarsson

Springer-Verlag
Berlin Heidelberg New York Tokyo

RUGGIU

HARARI



CONTENTS

SECTION I: GENERAL THEORY, CLASSICAL METHODS

Cryptology and Complexity Theories.......................... 3
G. RUGGIU

On Cryptosystems based on Polynomials and Finite Fields....... 10
R. LIDL

Algebraical Structures of Cryptographic Transformations....... 16
J.P. PIEPRZYK

Non-Linear, Non-Commutative Functions for Data Integrity...... 25
S. HARARI

Wire-Tap Channel II.......................................... 33
L.H. OZAROW, A.D. WYNER

Equivocations for Homophonic Ciphers......................... 51
A. SGARRO

Propagation Characteristics of the DES....................... 62
M. DAVIO, Y. DESMEDT, J.J. QUISQUATER

Linear Ciphers and Random Sequence Generators with Multiple Clocks.............................. 74
J.L. MASSEY, R.A. RUEPPEL

The Stop-and-go Generator.................................... 88
T. BETH, F.C. PIPER

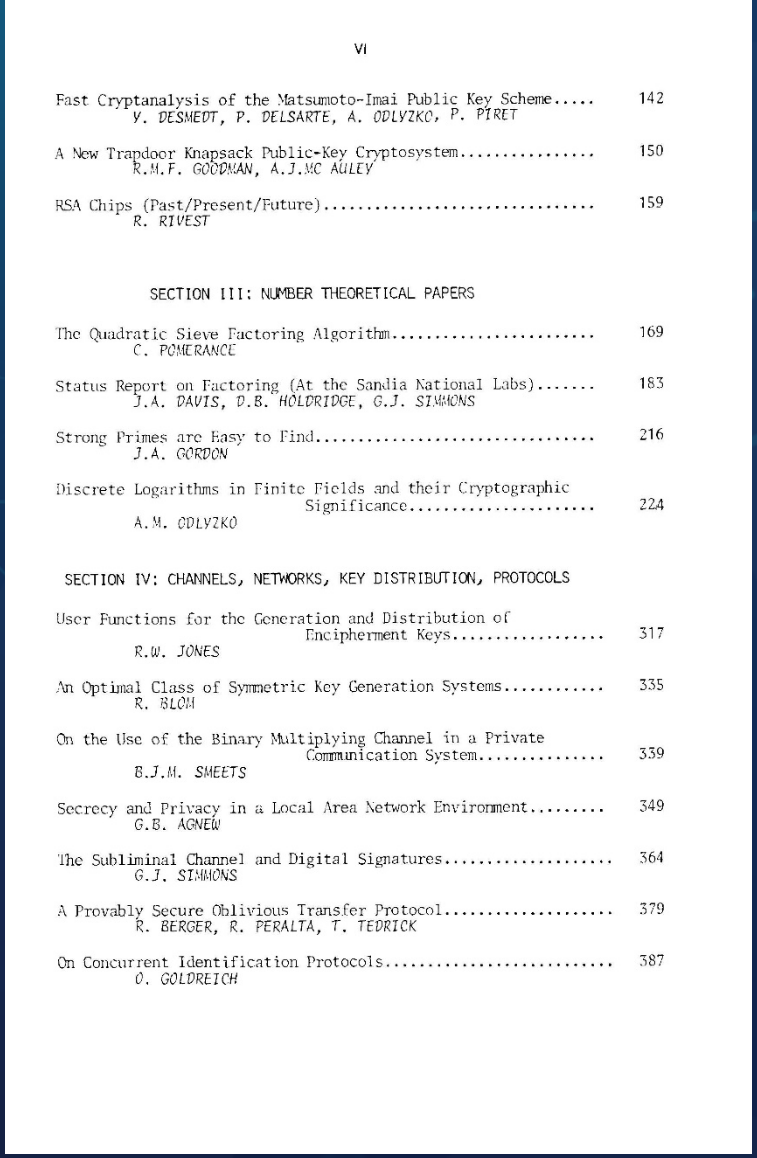
Pseudo Random Properties of Cascade Connections of Clock Controlled Shift Registers........... 93
D. GOLLMAN

On the Linear Complexity of Cascaded Sequences............... 99
R. VOGEL

SECTION II: PUBLIC-KEY SYSTEMS

RSA-Bits are 0.5 + $\varepsilon$ Secure.................................... 113
C.P. SCHNORR, W. ALEXI

On the Number of Close-and-equal Pairs of Bits in a String.... 127
O. GOLDREICH



Fast Cryptanalysis of the Matsumoto-Imai Public Key Scheme.... 142
Y. DESMEDT, P. DELSARTE, A. ODLYZKO, P. PIRET

A New Trapdoor Knapsack Public-Key Cryptosystem............... 150
R.M.F. GOODMAN, A.J.MC AULEY

RSA Chips (Past/Present/Future).............................. 159
R. RIVEST

SECTION III: NUMBER THEORETICAL PAPERS

The Quadratic Sieve Factoring Algorithm...................... 169
C. POMERANCE

Status Report on Factoring (At the Sandia National Labs)....... 183
J.A. DAVIS, D.B. HOLDRIDGE, G.J. SIMMONS

Strong Primes are Easy to Find............................... 216
J.A. GORDON

Discrete Logarithms in Finite Fields and their Cryptographic Significance..................... 224
A.M. ODLYZKO

SECTION IV: CHANNELS, NETWORKS, KEY DISTRIBUTION, PROTOCOLS

User Functions for the Generation and Distribution of Encipherment Keys................. 317
R.W. JONES

An Optimal Class of Symmetric Key Generation Systems........... 335
R. BLOM

On the Use of the Binary Multiplying Channel in a Private Communication System.............. 339
B.J.M. SMEETS

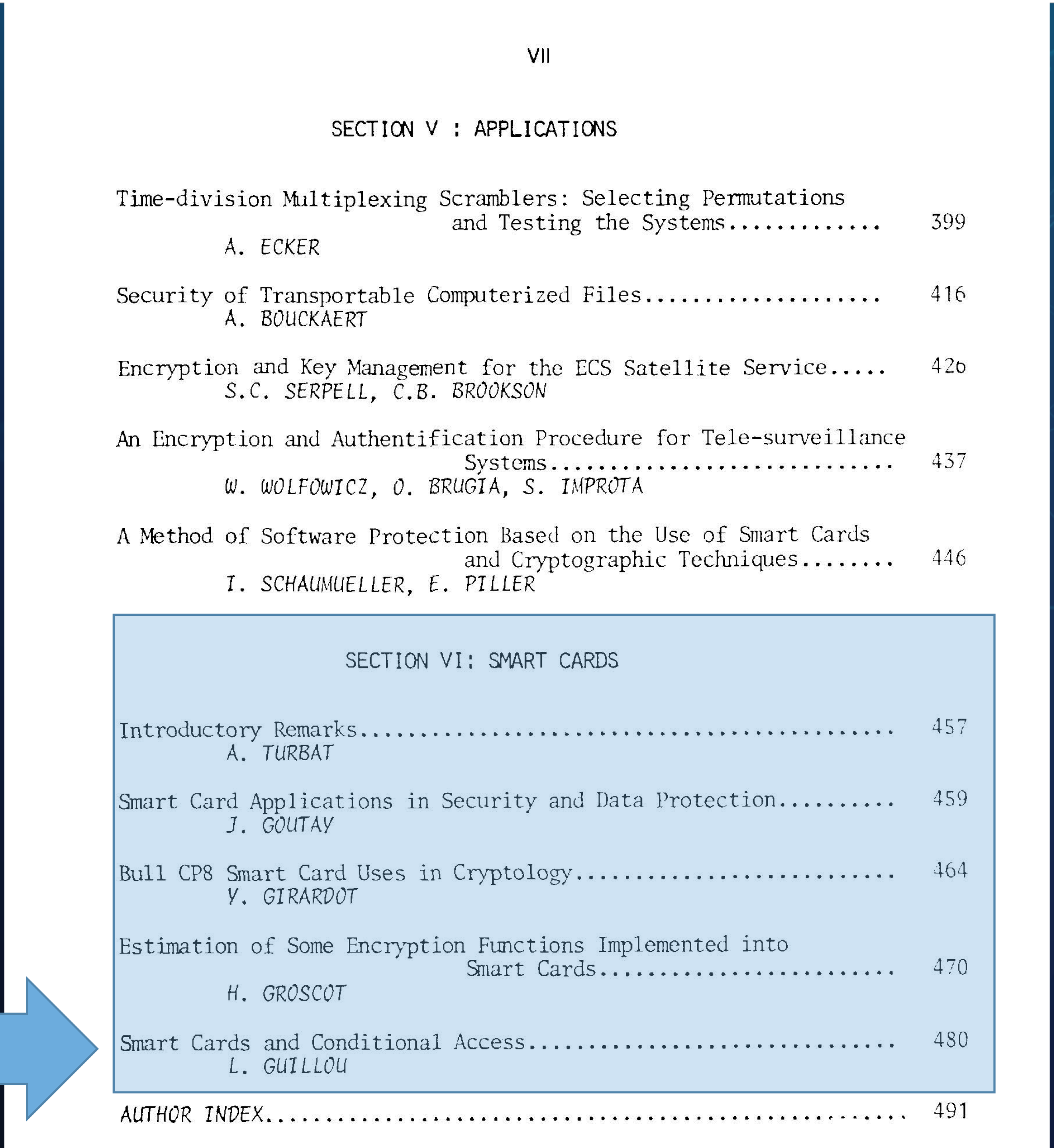
Secrecy and Privacy in a Local Area Network Environment........ 349
G.B. AGNEW

The Subliminal Channel and Digital Signatures.................. 364
G.J. SIMMONS

A Provably Secure Oblivious Transfer Protocol.................. 379
R. BERGER, R. PERALTA, T. TEDRICK

On Concurrent Identification Protocols......................... 387
O. GOLDREICH

# EUROCRYPT 84, Paris: Smart Cards



SECTION V : APPLICATIONS

Time-division Multiplexing Scramblers: Selecting Permutations and Testing the Systems............ 399
A. ECKER

Security of Transportable Computerized Files.................... 416
A. BOUCKAERT

Encryption and Key Management for the ECS Satellite Service..... 426
S.C. SERPELL, C.B. BROOKSON

An Encryption and Authentification Procedure for Tele-surveillance Systems............................ 437
W. WOLFOWICZ, O. BRUGIA, S. IMPROTA

A Method of Software Protection Based on the Use of Smart Cards and Cryptographic Techniques........ 446
I. SCHAUMUELLER, E. PILLER

SECTION VI: SMART CARDS

Introductory Remarks.............................................. 457
A. TURBAT

Smart Card Applications in Security and Data Protection.......... 459
J. GOUTAY

Bull CP8 Smart Card Uses in Cryptology.......................... 464
Y. GIRARDOT

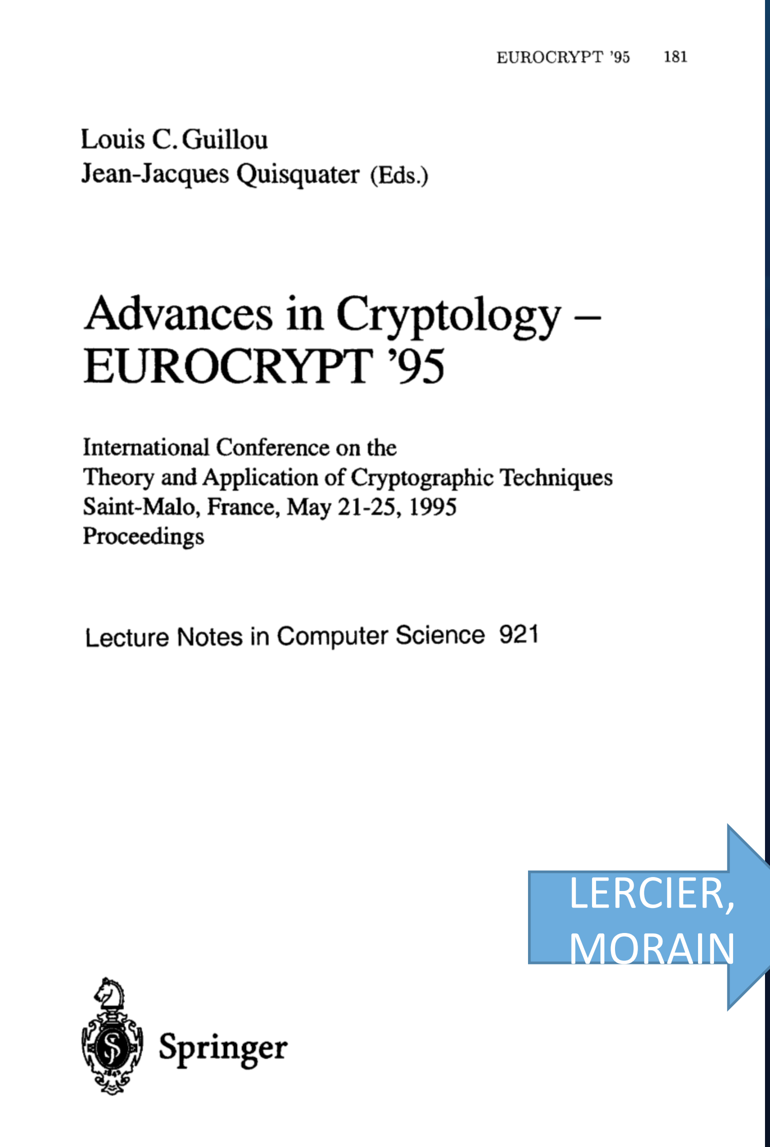
Estimation of Some Encryption Functions Implemented into Smart Cards.......................... 470
H. GROSCOT

Smart Cards and Conditional Access.............................. 480
L. GUILLOU

AUTHOR INDEX...................................................... 491

LOUIS GUILLOU

# EUROCRYPT 1995: Saint-Malo



EUROCRYPT '95 181

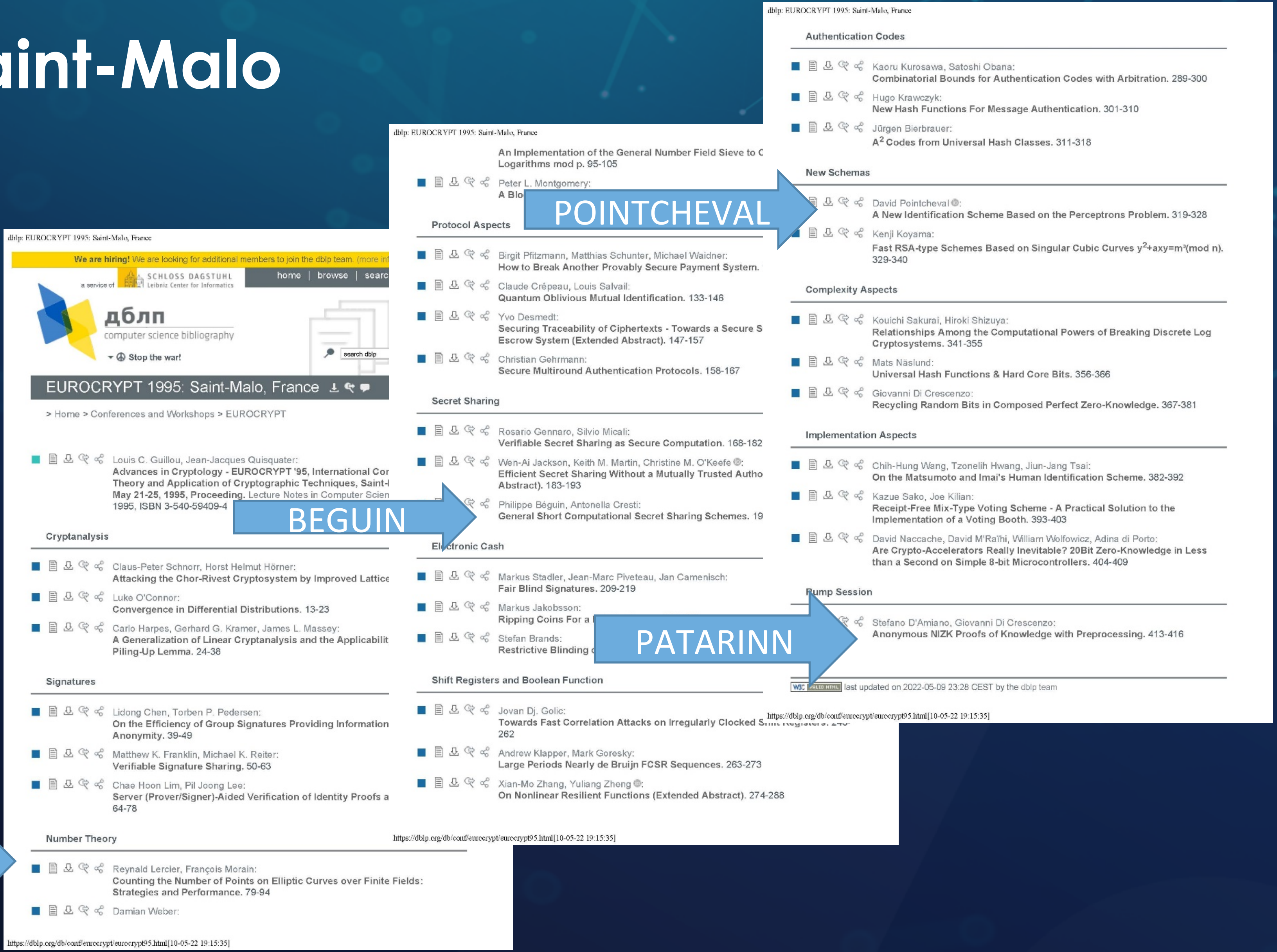
Louis C. Guillou
Jean-Jacques Quisquater (Eds.)

## Advances in Cryptology – EUROCRYPT '95

International Conference on the
Theory and Application of Cryptographic Techniques
Saint-Malo, France, May 21-25, 1995
Proceedings

Lecture Notes in Computer Science 921

Springer



dblp: EUROCRYPT 1995: Saint-Malo, France

We are hiring! We are looking for additional members to join the dblp team. (more inf

a service of SCHLOSS DAGSTUHL Leibniz Center for Informatics

home | browse | searc

дблп computer science bibliography

Stop the war!

search dblp

EUROCRYPT 1995: Saint-Malo, France

> Home > Conferences and Workshops > EUROCRYPT

Louis C. Guillou, Jean-Jacques Quisquater:
**Advances in Cryptology - EUROCRYPT '95, International Cor Theory and Application of Cryptographic Techniques, Saint-I May 21-25, 1995, Proceeding.** Lecture Notes in Computer Scien 1995, ISBN 3-540-59409-4

### Cryptanalysis

Claus-Peter Schnorr, Horst Helmut Hörner:
**Attacking the Chor-Rivest Cryptosystem by Improved Lattice**

Luke O'Connor:
**Convergence in Differential Distributions.** 13-23

Carlo Harpes, Gerhard G. Kramer, James L. Massey:
**A Generalization of Linear Cryptanalysis and the Applicabilit Piling-Up Lemma.** 24-38

### Signatures

Lidong Chen, Torben P. Pedersen:
**On the Efficiency of Group Signatures Providing Information Anonymity.** 39-49

Matthew K. Franklin, Michael K. Reiter:
**Verifiable Signature Sharing.** 50-63

Chae Hoon Lim, Pil Joong Lee:
**Server (Prover/Signer)-Aided Verification of Identity Proofs a** 64-78

### Number Theory

LERCIER, MORAIN

Reynald Lercier, François Morain:
**Counting the Number of Points on Elliptic Curves over Finite Fields: Strategies and Performance.** 79-94

Damian Weber:

https://dblp.org/db/conf/eurocrypt/eurocrypt95.html[10-05-22 19:15:35]

dblp: EUROCRYPT 1995: Saint-Malo, France

**An Implementation of the General Number Field Sieve to C Logarithms mod p.** 95-105

Peter L. Montgomery:
**A Blo**

### Protocol Aspects

Birgit Pfitzmann, Matthias Schunter, Michael Waidner:
**How to Break Another Provably Secure Payment System.**

Claude Crépeau, Louis Salvail:
**Quantum Oblivious Mutual Identification.** 133-146

Yvo Desmedt:
**Securing Traceability of Ciphertexts - Towards a Secure S Escrow System (Extended Abstract).** 147-157

Christian Gehrmann:
**Secure Multiround Authentication Protocols.** 158-167

### Secret Sharing

Rosario Gennaro, Silvio Micali:
**Verifiable Secret Sharing as Secure Computation.** 168-182

Wen-Ai Jackson, Keith M. Martin, Christine M. O'Keefe:
**Efficient Secret Sharing Without a Mutually Trusted Autho Abstract).** 183-193

BEGUIN

Philippe Béguin, Antonella Cresti:
**General Short Computational Secret Sharing Schemes.** 19

### Electronic Cash

Markus Stadler, Jean-Marc Piveteau, Jan Camenisch:
**Fair Blind Signatures.** 209-219

Markus Jakobsson:
**Ripping Coins For a**

Stefan Brands:
**Restrictive Blinding**

### Shift Registers and Boolean Function

Jovan Dj. Golic:
**Towards Fast Correlation Attacks on Irregularly Clocked Shift Registers.** 248-262

Andrew Klapper, Mark Goresky:
**Large Periods Nearly de Bruijn FCSR Sequences.** 263-273

Xian-Mo Zhang, Yuliang Zheng:
**On Nonlinear Resilient Functions (Extended Abstract).** 274-288

https://dblp.org/db/conf/eurocrypt/eurocrypt95.html[10-05-22 19:15:35]

dblp: EUROCRYPT 1995: Saint-Malo, France

### Authentication Codes

Kaoru Kurosawa, Satoshi Obana:
**Combinatorial Bounds for Authentication Codes with Arbitration.** 289-300

Hugo Krawczyk:
**New Hash Functions For Message Authentication.** 301-310

Jürgen Bierbrauer:
**$A^2$ Codes from Universal Hash Classes.** 311-318

### New Schemas

POINTCHEVAL

David Pointcheval:
**A New Identification Scheme Based on the Perceptrons Problem.** 319-328

Kenji Koyama:
**Fast RSA-type Schemes Based on Singular Cubic Curves $y^2+axy=m^3$(mod n).** 329-340

### Complexity Aspects

Kouichi Sakurai, Hiroki Shizuya:
**Relationships Among the Computational Powers of Breaking Discrete Log Cryptosystems.** 341-355

Mats Näslund:
**Universal Hash Functions & Hard Core Bits.** 356-366

Giovanni Di Crescenzo:
**Recycling Random Bits in Composed Perfect Zero-Knowledge.** 367-381

### Implementation Aspects

Chih-Hung Wang, Tzonelih Hwang, Jiun-Jang Tsai:
**On the Matsumoto and Imai's Human Identification Scheme.** 382-392

Kazue Sako, Joe Kilian:
**Receipt-Free Mix-Type Voting Scheme - A Practical Solution to the Implementation of a Voting Booth.** 393-403

David Naccache, David M'Raïhi, William Wolfowicz, Adina di Porto:
**Are Crypto-Accelerators Really Inevitable? 20Bit Zero-Knowledge in Less than a Second on Simple 8-bit Microcontrollers.** 404-409

### Rump Session

PATARINN

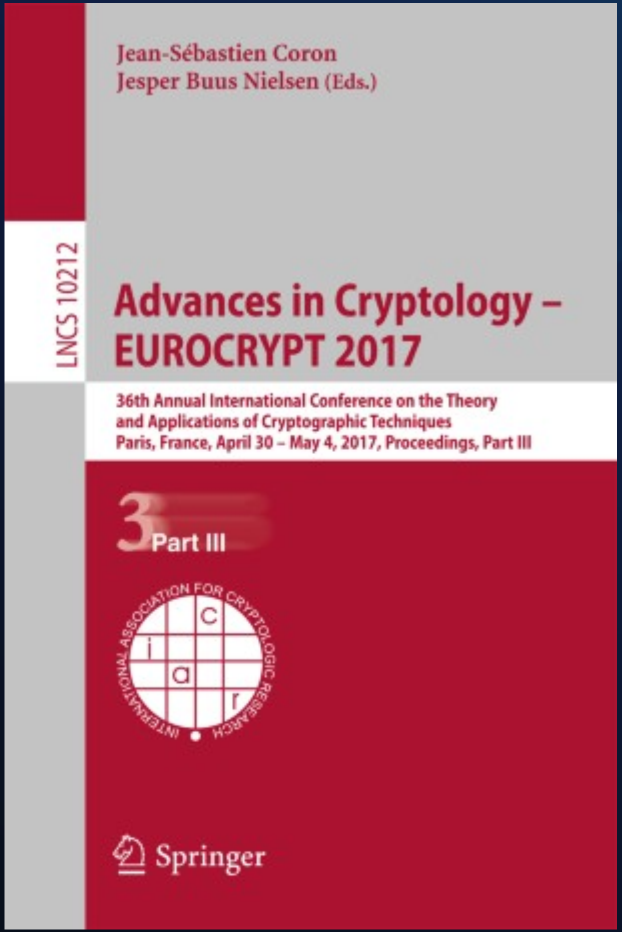
Stefano D'Amiano, Giovanni Di Crescenzo:
**Anonymous NIZK Proofs of Knowledge with Preprocessing.** 413-416

W3C VALID HTML last updated on 2022-05-09 23:28 CEST by the dblp team

https://dblp.org/db/conf/eurocrypt/eurocrypt95.html[10-05-22 19:15:35]

LETTRES SORBONNE UNIVERSITÉ

# EUROCRYPT 2017: Paris



Jean-Sébastien Coron
Jesper Buus Nielsen (Eds.)

LNCS 10212

Advances in Cryptology – EUROCRYPT 2017

36th Annual International Conference on the Theory
and Applications of Cryptographic Techniques
Paris, France, April 30 – May 4, 2017, Proceedings, Part III

3 Part III

Springer

15 authors

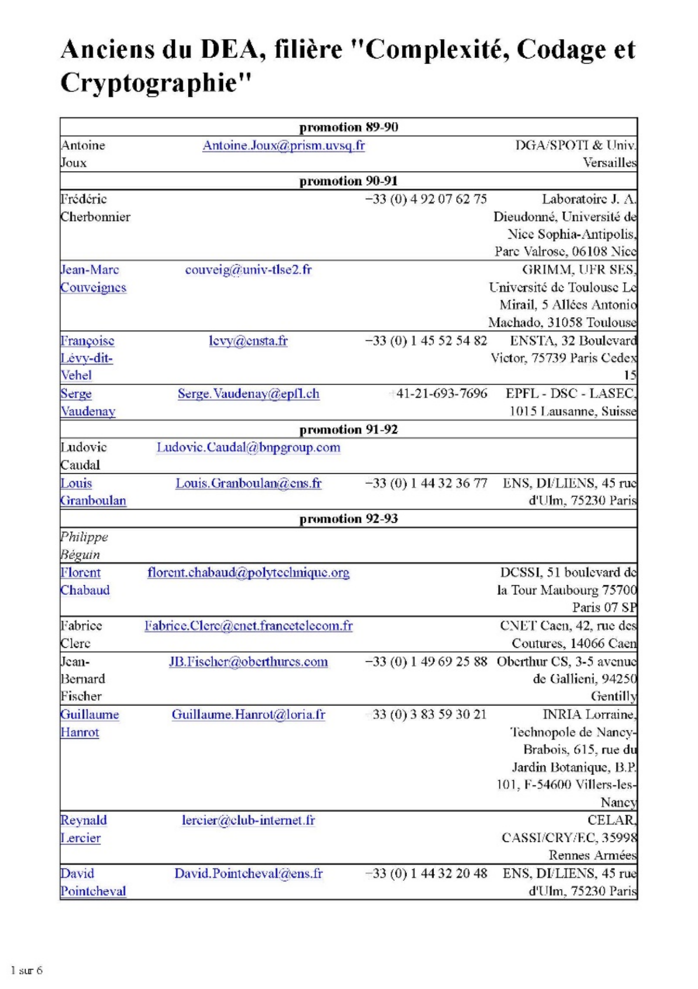
LETTRES
SORBONNE
UNIVERSITÉ

# Teaching first, next research, then applications …

- CRYPTIS, Limoges, from 1986 (Jean-Louis Nicolas):
  - ❖ Mainly number theory at the beginning,

- DEA ENS-X (filière Codage, Complexité et Cryptographie), Paris, from 1991: the main source of scientists about cryptography, courses organized by Jacques Stern, main teacher: JJQ.

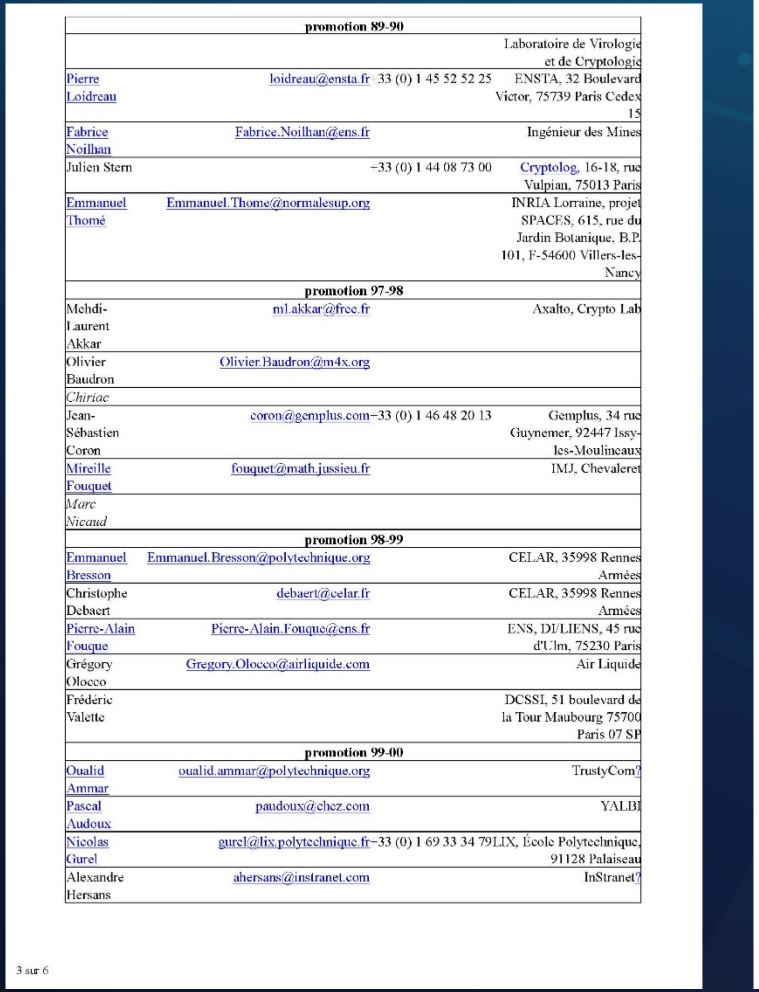
LETTRES SORBONNE UNIVERSITÉ



## Anciens du DEA, filière "Complexité, Codage et Cryptographie"

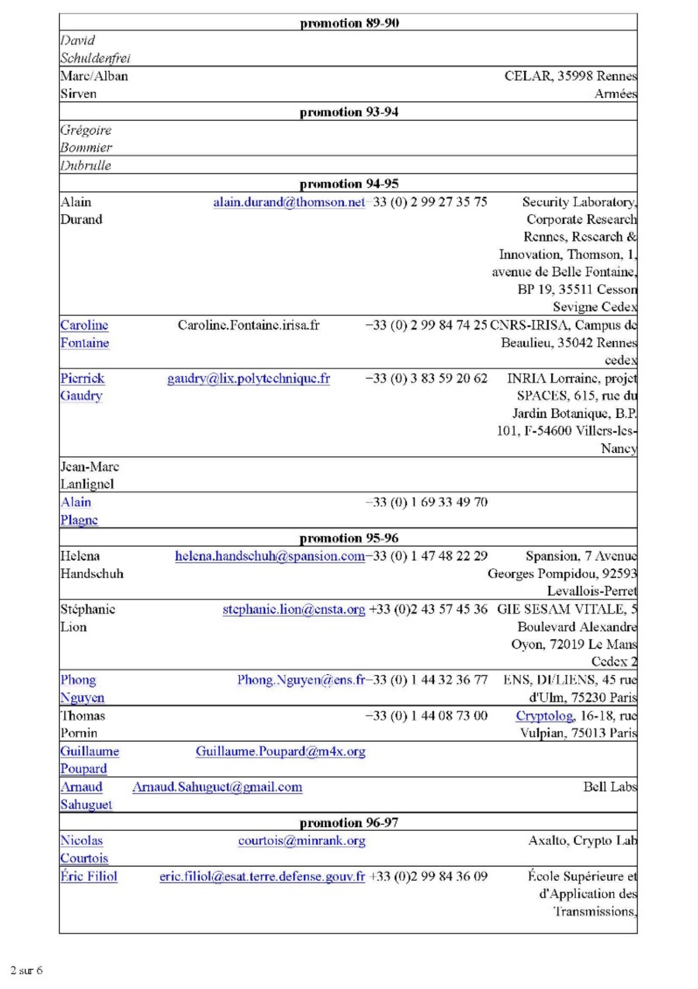
| | | | |
|---|---|---|---|
| **promotion 89-90** | | | |
| Antoine Joux | Antoine.Joux@prism.uvsq.fr | | DGA/SPOTI & Univ. Versailles |
| **promotion 90-91** | | | |
| Frédéric Cherbonnier | | −33 (0) 4 92 07 62 75 | Laboratoire J. A. Dieudonné, Université de Nice Sophia-Antipolis, Parc Valrose, 06108 Nice |
| Jean-Marc Couveignes | couveig@univ-tlse2.fr | | GRIMM, UFR SES, Université de Toulouse Le Mirail, 5 Allées Antonio Machado, 31058 Toulouse |
| Françoise Lévy-dit-Vehel | levy@ensta.fr | −33 (0) 1 45 52 54 82 | ENSTA, 32 Boulevard Victor, 75739 Paris Cedex 15 |
| Serge Vaudenay | Serge.Vaudenay@epfl.ch | +41-21-693-7696 | EPFL - DSC - LASEC, 1015 Lausanne, Suisse |
| **promotion 91-92** | | | |
| Ludovic Caudal | Ludovic.Caudal@bnpgroup.com | | |
| Louis Granboulan | Louis.Granboulan@ens.fr | −33 (0) 1 44 32 36 77 | ENS, DI/LIENS, 45 rue d'Ulm, 75230 Paris |
| **promotion 92-93** | | | |
| *Philippe Béguin* | | | |
| Florent Chabaud | florent.chabaud@polytechnique.org | | DCSSI, 51 boulevard de la Tour Maubourg 75700 Paris 07 SP |
| Fabrice Clerc | Fabrice.Clerc@cnet.francetelecom.fr | | CNET Caen, 42, rue des Coutures, 14066 Caen |
| Jean-Bernard Fischer | JB.Fischer@oberthurcs.com | −33 (0) 1 49 69 25 88 | Oberthur CS, 3-5 avenue de Gallieni, 94250 Gentilly |
| Guillaume Hanrot | Guillaume.Hanrot@loria.fr | +33 (0) 3 83 59 30 21 | INRIA Lorraine, Technopole de Nancy-Brabois, 615, rue du Jardin Botanique, B.P. 101, F-54600 Villers-les-Nancy |
| Reynald Lercier | lercier@club-internet.fr | | CELAR, CASSI/CRY/EC, 35998 Rennes Armées |
| David Pointcheval | David.Pointcheval@ens.fr | −33 (0) 1 44 32 20 48 | ENS, DI/LIENS, 45 rue d'Ulm, 75230 Paris |

1 sur 6



| | | | |
|---|---|---|---|
| **promotion 89-90** | | | |
| | | | Laboratoire de Virologie et de Cryptologie |
| Pierre Loidreau | loidreau@ensta.fr | +33 (0) 1 45 52 52 25 | ENSTA, 32 Boulevard Victor, 75739 Paris Cedex 15 |
| Fabrice Noilhan | Fabrice.Noilhan@ens.fr | | Ingénieur des Mines |
| Julien Stern | | −33 (0) 1 44 08 73 00 | Cryptolog, 16-18, rue Vulpian, 75013 Paris |
| Emmanuel Thomé | Emmanuel.Thome@normalesup.org | | INRIA Lorraine, projet SPACES, 615, rue du Jardin Botanique, B.P. 101, F-54600 Villers-les-Nancy |
| **promotion 97-98** | | | |
| Mehdi-Laurent Akkar | ml.akkar@free.fr | | Axalto, Crypto Lab |
| Olivier Baudron | Olivier.Baudron@m4x.org | | |
| *Chiriac* | | | |
| Jean-Sébastien Coron | coron@gemplus.com | −33 (0) 1 46 48 20 13 | Gemplus, 34 rue Guynemer, 92447 Issy-les-Moulineaux |
| Mireille Fouquet | fouquet@math.jussieu.fr | | IMJ, Chevaleret |
| *Marc Nicaud* | | | |
| **promotion 98-99** | | | |
| Emmanuel Bresson | Emmanuel.Bresson@polytechnique.org | | CELAR, 35998 Rennes Armées |
| Christophe Debaert | debaert@celar.fr | | CELAR, 35998 Rennes Armées |
| Pierre-Alain Fouque | Pierre-Alain.Fouque@ens.fr | | ENS, DI/LIENS, 45 rue d'Ulm, 75230 Paris |
| Grégory Olocco | Gregory.Olocco@airliquide.com | | Air Liquide |
| Frédéric Valette | | | DCSSI, 51 boulevard de la Tour Maubourg 75700 Paris 07 SP |
| **promotion 99-00** | | | |
| Oualid Ammar | oualid.ammar@polytechnique.org | | TrustyCom? |
| Pascal Audoux | paudoux@chez.com | | YALBI |
| Nicolas Gurel | gurel@lix.polytechnique.fr | −33 (0) 1 69 33 34 79 | LIX, École Polytechnique, 91128 Palaiseau |
| Alexandre Hersans | ahersans@instranet.com | | InStranet? |

3 sur 6



| | | | |
|---|---|---|---|
| **promotion 89-90** | | | |
| *David Schuldenfrei* | | | |
| Marc/Alban Sirven | | | CELAR, 35998 Rennes Armées |
| **promotion 93-94** | | | |
| *Grégoire Bommier* | | | |
| *Dubrulle* | | | |
| **promotion 94-95** | | | |
| Alain Durand | alain.durand@thomson.net | +33 (0) 2 99 27 35 75 | Security Laboratory, Corporate Research Rennes, Research & Innovation, Thomson, 1, avenue de Belle Fontaine, BP 19, 35511 Cesson Sevigne Cedex |
| Caroline Fontaine | Caroline.Fontaine.irisa.fr | −33 (0) 2 99 84 74 25 | CNRS-IRISA, Campus de Beaulieu, 35042 Rennes cedex |
| Pierrick Gaudry | gaudry@lix.polytechnique.fr | −33 (0) 3 83 59 20 62 | INRIA Lorraine, projet SPACES, 615, rue du Jardin Botanique, B.P. 101, F-54600 Villers-les-Nancy |
| Jean-Marc Lanlignel | | | |
| Alain Plagne | | −33 (0) 1 69 33 49 70 | |
| **promotion 95-96** | | | |
| Helena Handschuh | helena.handschuh@spansion.com | −33 (0) 1 47 48 22 29 | Spansion, 7 Avenue Georges Pompidou, 92593 Levallois-Perret |
| Stéphanie Lion | stephanie.lion@ensta.org | +33 (0)2 43 57 45 36 | GIE SESAM VITALE, 5 Boulevard Alexandre Oyon, 72019 Le Mans Cedex 2 |
| Phong Nguyen | Phong.Nguyen@ens.fr | −33 (0) 1 44 32 36 77 | ENS, DI/LIENS, 45 rue d'Ulm, 75230 Paris |
| Thomas Pornin | | −33 (0) 1 44 08 73 00 | Cryptolog, 16-18, rue Vulpian, 75013 Paris |
| Guillaume Poupard | Guillaume.Poupard@m4x.org | | |
| Arnaud Sahuguet | Arnaud.Sahuguet@gmail.com | | Bell Labs |
| **promotion 96-97** | | | |
| Nicolas Courtois | courtois@minrank.org | | Axalto, Crypto Lab |
| Éric Filiol | eric.filiol@esat.terre.defense.gouv.fr | +33 (0)2 99 84 36 09 | École Supérieure et d'Application des Transmissions, |

2 sur 6

# IACR: International Association for Cryptologic Research

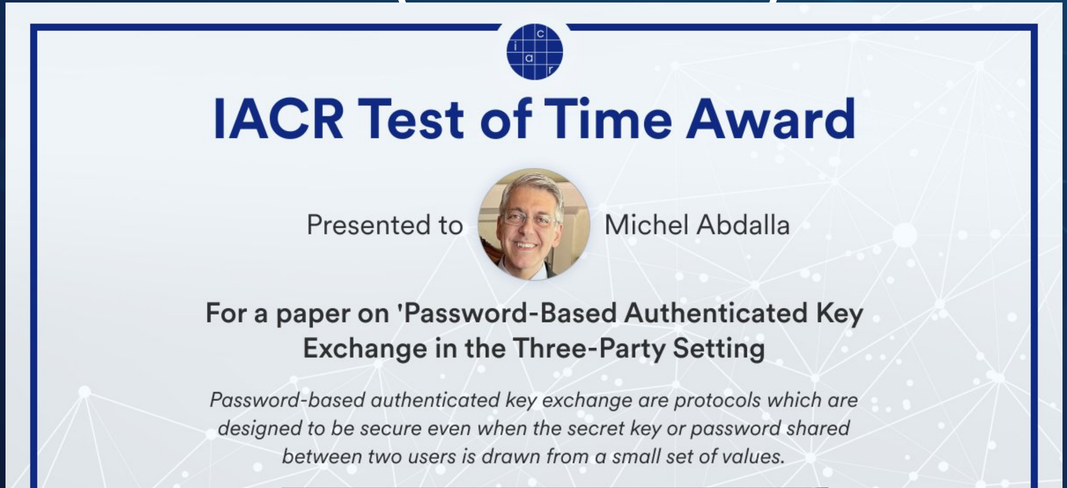
- President: Michel Abdalla (CNRS-ENS) 2020-2022

- Fellows:
  - ❖ Jacques Stern
  - ❖ Antoine Joux
  - ❖ Louis Guillou
  - ❖ David Naccache

# IACR: International Association for Cryptologic Research

- President: Michel Abdalla (CNRS-ENS) 2020-2022

- Fellows:
  - ❖ Jacques Stern
  - ❖ Antoine Joux
  - ❖ Louis Guillou
  - ❖ David Naccache



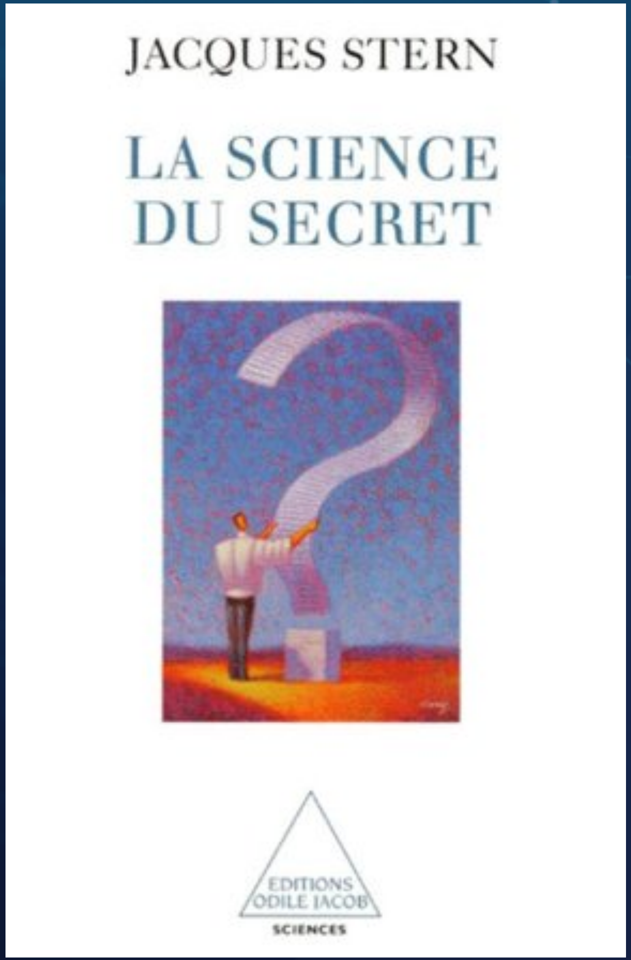
## IACR Test of Time Award

Presented to Michel Abdalla

**For a paper on 'Password-Based Authenticated Key Exchange in the Three-Party Setting**

*Password-based authenticated key exchange are protocols which are designed to be secure even when the secret key or password shared between two users is drawn from a small set of values.*

# Jacques Stern (master of secrets)

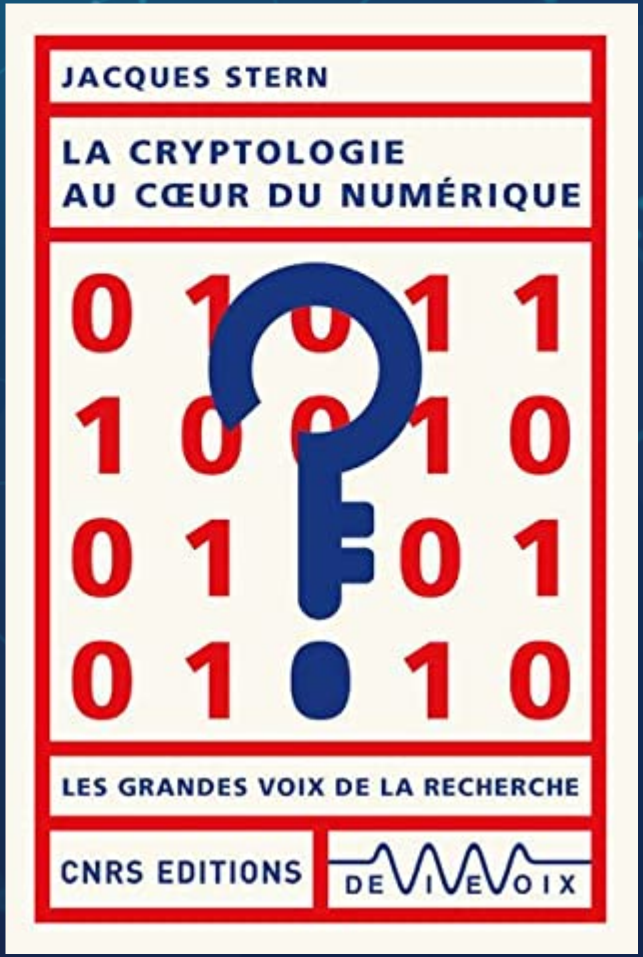


JACQUES STERN

LA SCIENCE DU SECRET

EDITIONS ODILE JACOB

SCIENCES



JACQUES STERN

LA CRYPTOLOGIE AU CŒUR DU NUMÉRIQUE

LES GRANDES VOIX DE LA RECHERCHE

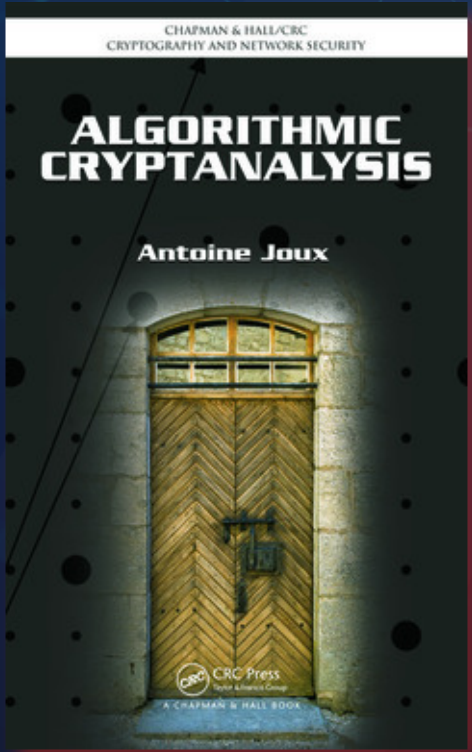
CNRS EDITIONS

DE VIVE VOIX

LETTRES SORBONNE UNIVERSITÉ

# Antoine Joux (Gödel prize)

- Antoine Joux won the prestigious Gödel Prize in 2013 for the introduction and use of the concept of coupling in cryptography



CHAPMAN & HALL/CRC
CRYPTOGRAPHY AND NETWORK SECURITY

ALGORITHMIC CRYPTANALYSIS

Antoine Joux

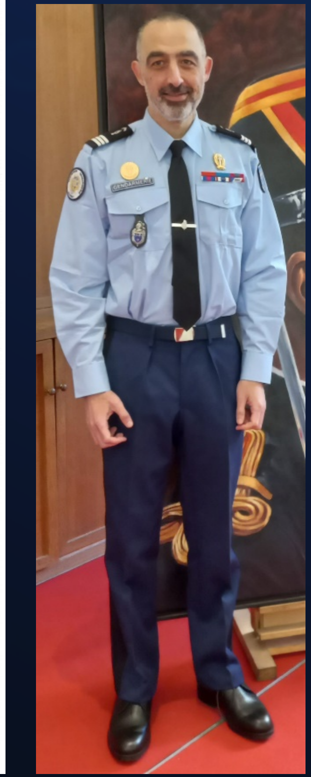
CRC Press
Taylor & Francis Group

A CHAPMAN & HALL BOOK

LETTRES
SORBONNE
UNIVERSITÉ

# David Naccache

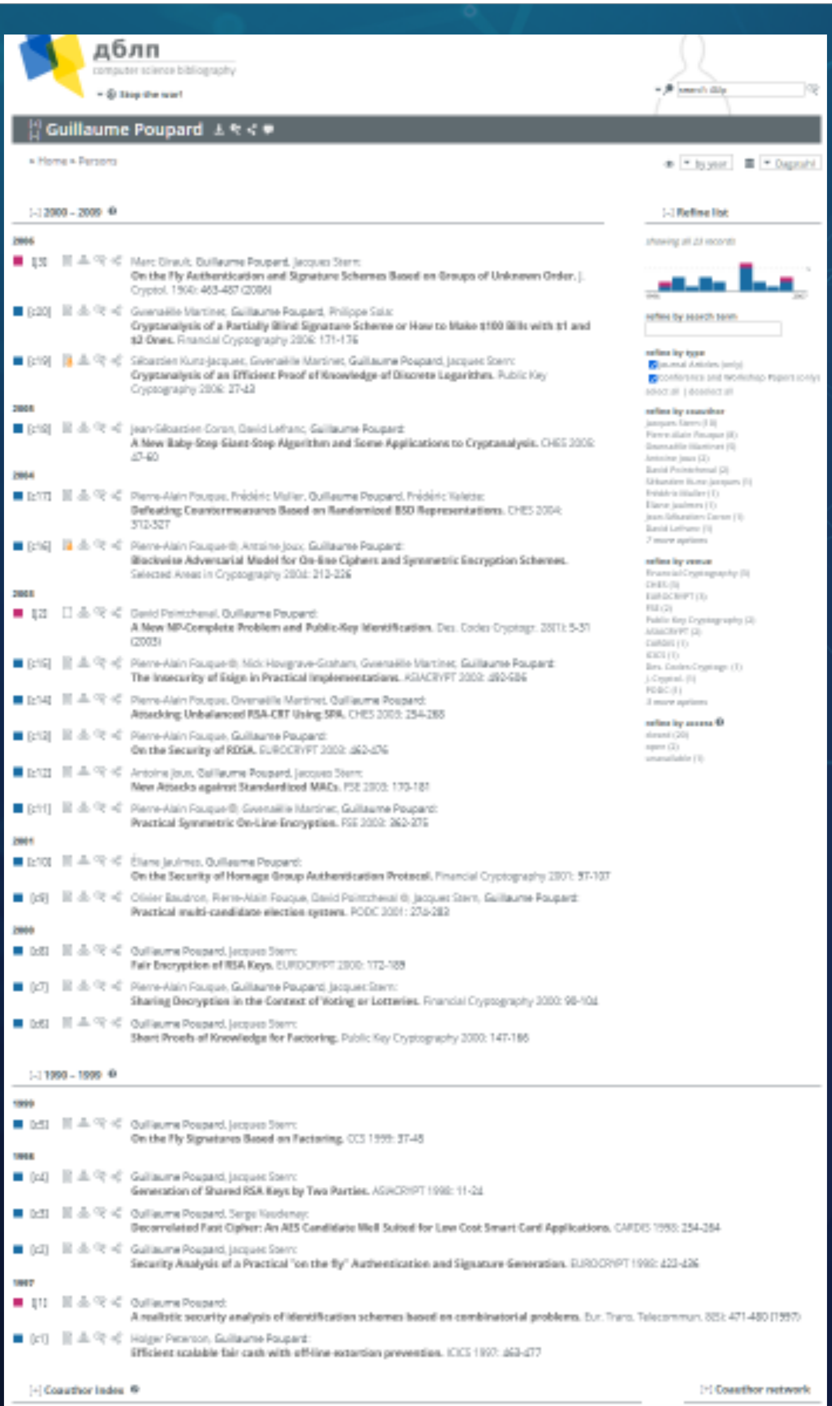
David Naccache is a French cryptologist, professor and researcher at the École Normale Supérieure where he heads the Information Security team.



LETTRES
SORBONNE
UNIVERSITÉ

# ANSSI: Guillaume Poupard

- Since 2014, Guillaume Poupard is the director general of the National Agency for Information Systems Security (ANSSI)
- https://www.ssi.gouv.fr/en/



## Guillaume Poupard

» Home » Persons

[–] 2000 – 2009

2006

- [j3] Marc Girault, Guillaume Poupard, Jacques Stern: **On the Fly Authentication and Signature Schemes Based on Groups of Unknown Order.** J. Cryptol. 19(4): 463-487 (2006)
- [c20] Gwenaëlle Martinet, Guillaume Poupard, Philippe Sola: **Cryptanalysis of a Partially Blind Signature Scheme or How to Make $100 Bills with $1 and $2 Ones.** Financial Cryptography 2006: 171-176
- [c19] Sébastien Kunz-Jacques, Gwenaëlle Martinet, Guillaume Poupard, Jacques Stern: **Cryptanalysis of an Efficient Proof of Knowledge of Discrete Logarithm.** Public Key Cryptography 2006: 27-43

2005

- [c18] Jean-Sébastien Coron, David Lefranc, Guillaume Poupard: **A New Baby-Step Giant-Step Algorithm and Some Applications to Cryptanalysis.** CHES 2005: 47-60

2004

- [c17] Pierre-Alain Fouque, Frédéric Muller, Guillaume Poupard, Frédéric Valette: **Defeating Countermeasures Based on Randomized BSD Representations.** CHES 2004: 312-327
- [c16] Pierre-Alain Fouque, Antoine Joux, Guillaume Poupard: **Blockwise Adversarial Model for On-line Ciphers and Symmetric Encryption Schemes.** Selected Areas in Cryptography 2004: 212-226

2003

- [j2] David Pointcheval, Guillaume Poupard: **A New NP-Complete Problem and Public-Key Identification.** Des. Codes Cryptogr. 28(1): 5-31 (2003)
- [c15] Pierre-Alain Fouque, Nick Howgrave-Graham, Gwenaëlle Martinet, Guillaume Poupard: **The Insecurity of Esign in Practical Implementations.** ASIACRYPT 2003: 492-506
- [c14] Pierre-Alain Fouque, Gwenaëlle Martinet, Guillaume Poupard: **Attacking Unbalanced RSA-CRT Using SPA.** CHES 2003: 254-268
- [c13] Pierre-Alain Fouque, Guillaume Poupard: **On the Security of RDSA.** EUROCRYPT 2003: 462-476
- [c12] Antoine Joux, Guillaume Poupard, Jacques Stern: **New Attacks against Standardized MACs.** FSE 2003: 170-181
- [c11] Pierre-Alain Fouque, Gwenaëlle Martinet, Guillaume Poupard: **Practical Symmetric On-Line Encryption.** FSE 2003: 362-375

2001

- [c10] Éliane Jaulmes, Guillaume Poupard: **On the Security of Homage Group Authentication Protocol.** Financial Cryptography 2001: 97-107
- [c9] Olivier Baudron, Pierre-Alain Fouque, David Pointcheval, Jacques Stern, Guillaume Poupard: **Practical multi-candidate election system.** PODC 2001: 274-283

2000

- [c8] Guillaume Poupard, Jacques Stern: **Fair Encryption of RSA Keys.** EUROCRYPT 2000: 172-189
- [c7] Pierre-Alain Fouque, Guillaume Poupard, Jacques Stern: **Sharing Decryption in the Context of Voting or Lotteries.** Financial Cryptography 2000: 90-104
- [c6] Guillaume Poupard, Jacques Stern: **Short Proofs of Knowledge for Factoring.** Public Key Cryptography 2000: 147-166

[–] 1990 – 1999

1999

- [c5] Guillaume Poupard, Jacques Stern: **On the Fly Signatures Based on Factoring.** CCS 1999: 37-45

1998

- [c4] Guillaume Poupard, Jacques Stern: **Generation of Shared RSA Keys by Two Parties.** ASIACRYPT 1998: 11-24
- [c3] Guillaume Poupard, Serge Vaudenay: **Decorrelated Fast Cipher: An AES Candidate Well Suited for Low Cost Smart Card Applications.** CARDIS 1998: 254-264
- [c2] Guillaume Poupard, Jacques Stern: **Security Analysis of a Practical "on the fly" Authentication and Signature Generation.** EUROCRYPT 1998: 422-436

1997

- [j1] Guillaume Poupard: **A realistic security analysis of identification schemes based on combinatorial problems.** Eur. Trans. Telecommun. 8(5): 471-480 (1997)
- [c1] Holger Petersen, Guillaume Poupard: **Efficient scalable fair cash with off-line extortion prevention.** ICICS 1997: 463-477

[+] Coauthor Index

[+] Coauthor network

[–] Refine list

showing all 23 records

refine by search term

refine by type

☑ Journal Articles (only)
☑ Conference and Workshop Papers (only)
select all | deselect all

refine by coauthor

Jacques Stern (11)
Pierre-Alain Fouque (8)
Gwenaëlle Martinet (5)
Antoine Joux (2)
David Pointcheval (2)
Sébastien Kunz-Jacques (1)
Frédéric Muller (1)
Éliane Jaulmes (1)
Jean-Sébastien Coron (1)
David Lefranc (1)
7 more options

refine by venue

Financial Cryptography (3)
CHES (3)
EUROCRYPT (3)
FSE (2)
Public Key Cryptography (2)
ASIACRYPT (2)
CARDIS (1)
ICICS (1)
Des. Codes Cryptogr. (1)
J. Cryptol. (1)
PODC (1)
3 more options

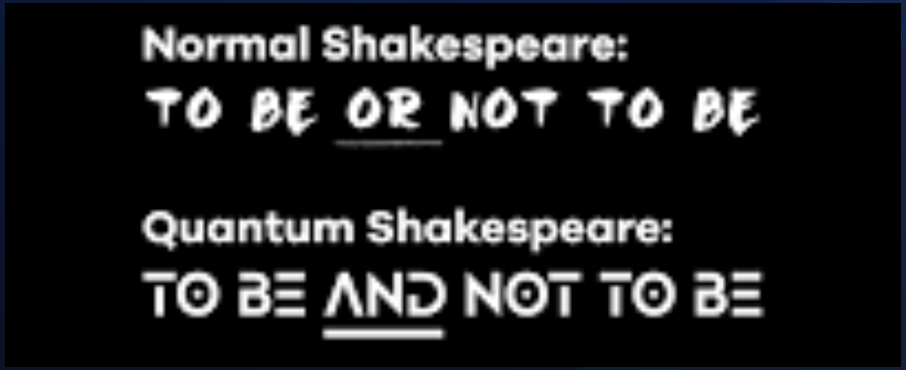
refine by access

closed (20)
open (2)
unavailable (1)

Multiple research, Multiple publications, New protocols …

# Post quantum Research

HOW'S YOUR QUANTUM COMPUTER PROTOTYPE COMING ALONG?
GREAT!
Dilbert.com DilbertCartoonist@gmail.com
THE PROJECT EXISTS IN A SIMULTANEOUS STATE OF BEING BOTH TOTALLY SUCCESSFUL AND NOT EVEN STARTED.
4-17-12 ©2012 Scott Adams, Inc./Dist. by Universal Uclick
CAN I OBSERVE IT?
THAT'S A TRICKY QUESTION.



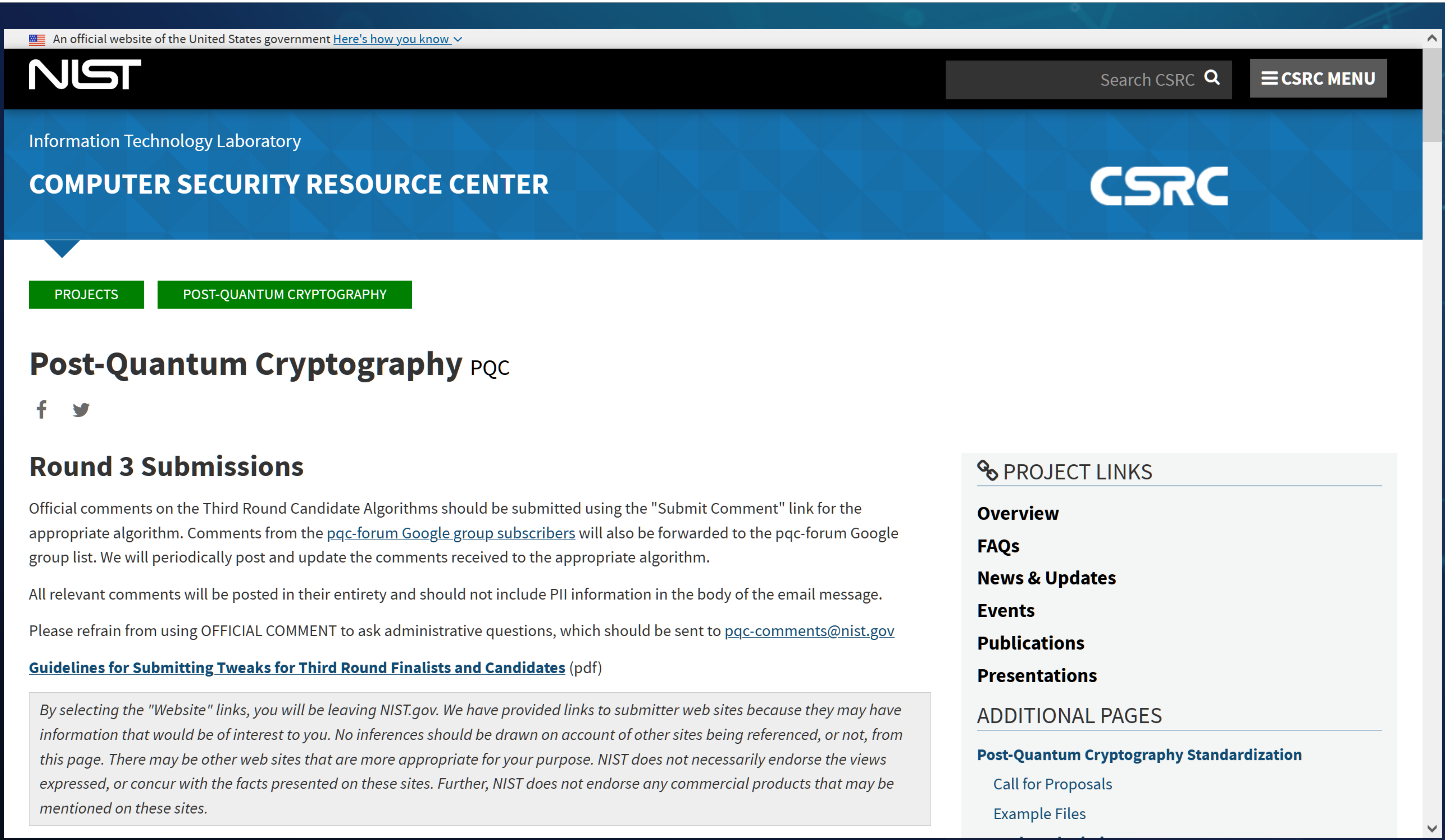
Normal Shakespeare:

TO BE OR NOT TO BE

Quantum Shakespeare:

TO BE AND NOT TO BE

LETTRES
SORBONNE
UNIVERSITÉ



An official website of the United States government Here's how you know
NIST
Search CSRC
CSRC MENU
Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER
CSRC
PROJECTS
POST-QUANTUM CRYPTOGRAPHY

# Post-Quantum Cryptography PQC

## Round 3 Submissions

Official comments on the Third Round Candidate Algorithms should be submitted using the "Submit Comment" link for the appropriate algorithm. Comments from the pqc-forum Google group subscribers will also be forwarded to the pqc-forum Google group list. We will periodically post and update the comments received to the appropriate algorithm.

All relevant comments will be posted in their entirety and should not include PII information in the body of the email message.

Please refrain from using OFFICIAL COMMENT to ask administrative questions, which should be sent to pqc-comments@nist.gov

**Guidelines for Submitting Tweaks for Third Round Finalists and Candidates** (pdf)

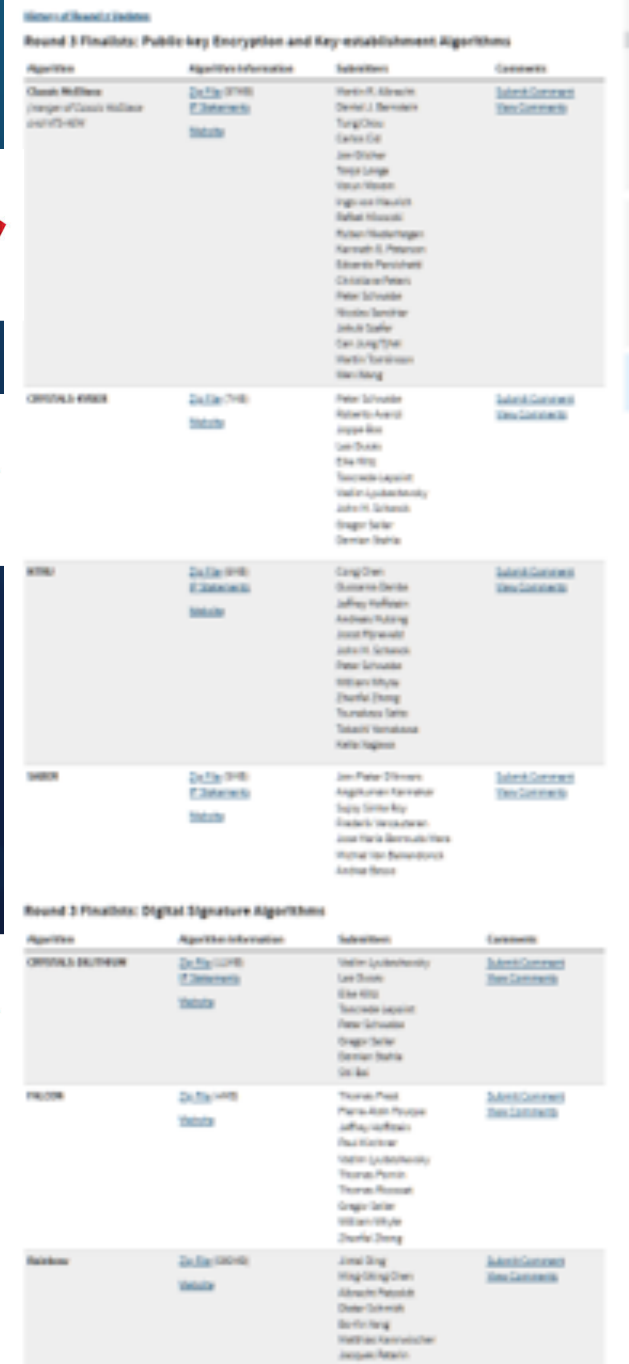
*By selecting the "Website" links, you will be leaving NIST.gov. We have provided links to submitter web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites.*

# Postquantum cryptography (PQC)

- Contributions (2017-2020) to the call by NIST (2016),
- July 22, 2020 Third Round Candidates announced (7 Finalists and 8 Alternates),
- October 1, 2020 Deadline for updated submission packages for the Third Round,
- 2022/2024 Draft Standards Available …

- See also https://www.ssi.gouv.fr/en/publication/anssi-views-on-the-post-quantum-cryptography-transition/

# NIST: PQC



History of Round 3 Updates

Round 3 Finalists: Public-key Encryption and Key-establishment Algorithms

| Algorithm | Algorithm Information | Submitters | Comments |
|---|---|---|---|
| **Classic McEliece**<br>(merger of Classic McEliece and NTS-KEM) | Zip File (7MB)<br>IP Statements<br>Website | Martin R. Albrecht<br>Daniel J. Bernstein<br>Tung Chou<br>Carlos Cid<br>Jan Gilcher<br>Tanja Lange<br>Varun Maram<br>Ingo von Maurich<br>Rafael Misoczki<br>Ruben Niederhagen<br>Kenneth G. Paterson<br>Edoardo Persichetti<br>Christiane Peters<br>Peter Schwabe<br>Nicolas Sendrier<br>Jakub Szefer<br>Cen Jung Tjhai<br>Martin Tomlinson<br>Wen Wang | Submit Comment<br>View Comments |
| **CRYSTALS-KYBER** | Zip File (7MB)<br>Website | Peter Schwabe<br>Roberto Avanzi<br>Joppe Bos<br>Léo Ducas<br>Eike Kiltz<br>Tancrède Lepoint<br>Vadim Lyubashevsky<br>John M. Schanck<br>Gregor Seiler<br>Damien Stehlé | Submit Comment<br>View Comments |
| **NTRU** | Zip File (9MB)<br>IP Statements<br>Website | Cong Chen<br>Oussama Danba<br>Jeffrey Hoffstein<br>Andreas Hülsing<br>Joost Rijneveld<br>John M. Schanck<br>Peter Schwabe<br>William Whyte<br>Zhenfei Zhang<br>Tsunekazu Saito<br>Takashi Yamakawa<br>Keita Xagawa | Submit Comment<br>View Comments |
| **SABER** | Zip File (3MB)<br>IP Statements<br>Website | Jan-Pieter D'Anvers<br>Angshuman Karmakar<br>Sujoy Sinha Roy<br>Frederik Vercauteren<br>Jose Maria Bermudo Mera<br>Michiel Van Beirendonck<br>Andrea Basso | Submit Comment<br>View Comments |

Round 3 Finalists: Digital Signature Algorithms

| Algorithm | Algorithm Information | Submitters | Comments |
|---|---|---|---|
| **CRYSTALS-DILITHIUM** | Zip File (11MB)<br>IP Statements<br>Website | Vadim Lyubashevsky<br>Léo Ducas<br>Eike Kiltz<br>Tancrède Lepoint<br>Peter Schwabe<br>Gregor Seiler<br>Damien Stehlé<br>Shi Bai | Submit Comment<br>View Comments |
| **FALCON** | Zip File (4MB)<br>Website | Thomas Prest<br>Pierre-Alain Fouque<br>Jeffrey Hoffstein<br>Paul Kirchner<br>Vadim Lyubashevsky<br>Thomas Pornin<br>Thomas Ricosset<br>Gregor Seiler<br>William Whyte<br>Zhenfei Zhang | Submit Comment<br>View Comments |
| **Rainbow** | Zip File (183MB)<br>Website | Jintai Ding<br>Ming-Shing Chen<br>Albrecht Petzoldt<br>Dieter Schmidt<br>Bo-Yin Yang<br>Matthias Kannwischer<br>Jacques Patarin | Submit Comment<br>View Comments |

Plus alternate versions

# Conclusion (for the future)

- France is again at the center of cryptography (research, design, applications, production, …),
- It was first by a high level teaching of very good people,
- Then putting these people everywhere (Grandes Ecoles, Universities, research labs, companies, administrations, services, …),
- A very good result obtained in about 20 years of efforts.

LETTRES SORBONNE UNIVERSITÉ

# We will gladly answer any of your questions

LETTRES
SORBONNE
UNIVERSITÉ