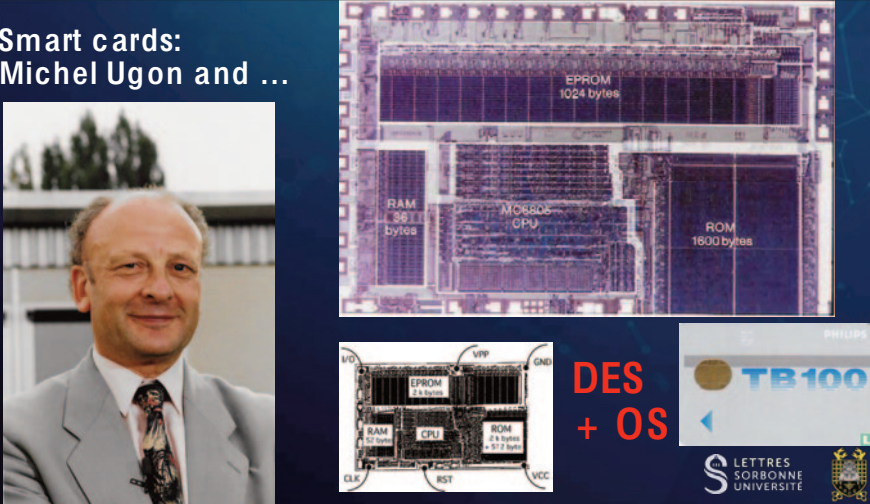


# De la carte à puce à nos jours (1967-2022)

Jean-Jacques Quisquater

**B**onjour, merci beaucoup Jean-Louis pour cette présentation. Nous allons commencer par reparler de carte à puce, puis je vous donnerai mon sentiment sur la recherche française en Cryptologie. OK allons-y.

**Smart cards:  
Michel Ugon and ...**



**DES  
+ OS**

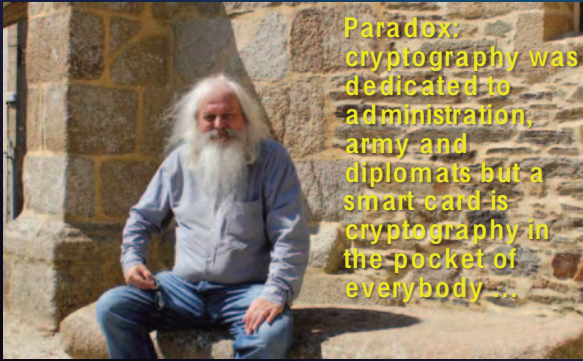
PHILIPS  
**TB100**

LETTRES  
SORBONNE  
UNIVERSITÉ

Voici donc de nouveau, Michel Ugon, l'inventeur des cartes à puce à microprocesseurs. Vous voyez ici le premier circuit (photo du haut) avec très peu de mémoire. Le problème principal était vraiment la RAM, avec 36 octets, ce n'est pas beaucoup comme vous pouvez l'imaginer. En fait, la version suivante (photo du bas) possédait une RAM de 52 octets. C'était suffisant avec la ROM de 2k octets pour y mettre le DES et/ou un petit système d'exploitation. Ce fut finalement la carte à puce TB100 de TRT (Philips) et BULL qui a eu de nombreuses utilisations.

... Louis Guillou

2004:  
Session president :  
Jean-Louis Desvignes



126 Actes du Séminaire Collaure sur l'États de l'Informatique et des Télécommunications

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

**Louis Guillou**

*Expert Émérite  
Direction IRI de France Telecom  
MATHIS, 4 Rue des Clois Courtil,  
BP 41228, 93122 Gagny, France  
TÉL: 01 47 27 54 02 Fax: 01 47 27 30 00  
l.guillou.guy@tiscali.fr et a.s.m., y.u.m.*

**Résumé.** Il y a une correspondance entre les débuts de la carte à puce et les premières pas de la cryptologie dans le domaine public. Aujourd'hui, nous examinons cette correspondance, la carte à puce ne constituant en plus les banques, et pour la télévision à puce, en plus le téléphone mobile ne peut pas être un cas de cette. La carte à puce est une puce et cryptologie est à son tour la carte à puce dans les cas d'application, elle constitue une propre technologie, elle constitue une personne. Dans ce, la sécurité absolue n'est pas, mais la sécurité pour rendre à l'utilisateur. Le contenu des cartes expose un des aspects spécifiques, relatifs avec la méthodologie des entreprises communes et des profils de protection.

**Abstract.** The start of smart card coincides with the advent of cryptography in the public domain. Today, although an ubiquitous cryptography, the smart card could be inappropriate for banking, pay-TV, mobile phone, health, and so on. The fact however some cards could be applicable in any setting, the smart card enables data and algorithms, it remains the same card to recognize its holder. Smartcard security does not exist, but security may always be required. Card security relies on specific software evaluation according to common criteria methodology and protection profile.

**1 Les débuts de la carte à puce**

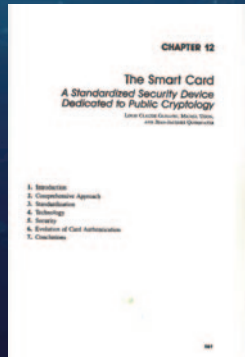
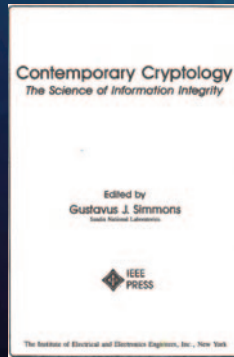
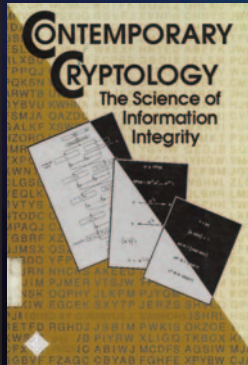
**1.1 Les premiers leviers**

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. J'ai vu beaucoup de choses à la fin de la route pour aller dans le futur. Ne faites pas attendre vos idées ou bien d'autres. En fin de compte, les débuts de la carte à puce reviennent à ceux de l'écriture: beaucoup d'années de culture sur des milliers de personnes dans y parvenir.



Beaucoup de choses ont été faites en collaboration avec Louis Guillou. Il y avait un paradoxe à cette époque car la cryptographie était principalement réservée à l'administration, à l'armée et aux diplomates or, une carte à puce, c'est de la cryptographie dans la poche de tout le monde. Vous pouvez donc imaginer que cela posait beaucoup de problèmes, mais cela a été résolu compte tenu des enjeux industriels.

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



1992



Une coopération très étroite s'est instaurée entre Michel Ugon, Louis Guillou et moi-même. Une contribution importante figure dans le livre IEEE de Gustave Simmons, qui consacre un long chapitre sur les cartes à puce. C'était donc très important et c'était en 1992.

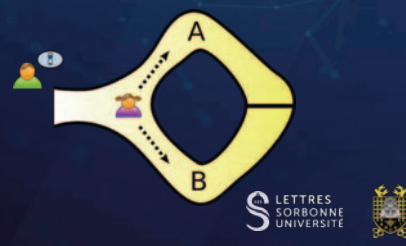
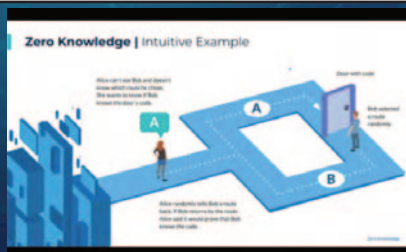
# GQ – GQ2 – aso used by Novell

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

**ZKP-IPF**  
 •FFS Protocol  
 •GQ Protocol  
**ZKP-DLP**  
 •Schorr 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  $J_A = f(1_A)$  is  $J_A^s \bmod n$
- Protocol Messages (Repeat  $t$  times)**
  - A sends to B(Commit):  $J_A, x = r^e \bmod n$  for a random  $r$
  - B sends to A(Challenge): a random  $e$  with  $1 = ce = cv$
  - A sends to B(Response):  $y = s_A^e \bmod n$
- Verify**
  - B computes  $z = J_A^y \bmod n$
  - Accept A's proof of identity if  $z = x$  and  $z \neq 0$

Comparative Study on Zero-Knowledge Identification Protocols



Il y avait aussi beaucoup de protocoles, le brevet GQ (Guillou Quisquater), également le GQ2. Celui-ci a d'ailleurs été utilisé par la société Novell pour de nombreuses applications, c'était dans les années 90 et suivantes. Nous avons également produit une définition et un nouvel algorithme pour expliquer leur fonctionnement, la bien nommée caverne d'Alibaba, par exemple.

## EURO CRYPT 1984: Paris

RUGGIU

HARARI

CONTENTS	
SECTION I: GENERAL THEORY, CLASSICAL METHODS	
Cryptology and Complexity Theoretic.....	1
On Cryptosystems Based on Polynomial and Finite Fields.....	10
Algebraic Foundations of Cryptographic Transmutations.....	17
Non-Linear, Non-Commutative Functions for Data Integrity.....	22
New-Top (Shamir).....	31
Synchronization for Broadcast Codes.....	39
Proposition Characterizations of the MDS.....	42
Linear Codes and Coding Systems Generated with Algebraic.....	71
The Mersenne Primes.....	80
Fermat-Dirichlet Properties of Certain Conjectures of Clark.....	81
On the Linear Complexity of Cyclic Sequences.....	89
SECTION II: PUBLIC-KEY SYSTEMS	
On the Use of a $t$ -Error Correcting Code in a Private.....	101
On the Number of Computational Steps of Bits in a String.....	127
SECTION III: NUMBER THEORETICAL METHODS	
The Dirichlet Series Generating Functions.....	169
Strong Pigeon Hole Lemma to Fiat.....	276
Algebraic Structures in Finite Fields and Their Cryptographic.....	224
SECTION IV: CHANNELS, NETWORKS, KEY DISTRIBUTION, PROTOCOLS	
User Reaction for the Generation and Distribution of.....	317
On Optimal Plans of Insecure Key Distribution Systems.....	323
On the Use of the Error-Correcting Codes in a Private.....	330
Security and Privacy in a Local Area Network Environment.....	340
On Self-Organizing Channel and Digital Algorithms.....	343
A Family of Error-Correcting Codes.....	379
On Discreet, Secret-Exchange Protocols.....	387

À présent, nous pouvons examiner le développement de la cryptographie en France, je parle de la cryptographie civile. La première grande conférence européenne sur la cryptographie, Eurocrypt, s'est tenue en France, à Paris, en 1984. Et vous pouvez voir que dans la table des matières, il n'y avait que deux personnes de France: une de l'industrie Gilles Ruggiu et une de l'université, Sami Harari.

# EUROCRYPT 84, Paris: Smart Cards

VII

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. SERPELLI, T.B. BROOKSON	
An Encryption and Authentication Procedure for Tele-surveillance Systems.....	437
W. WOLFOVICZ, O. BRUGLIA, S. IMPROTA	
A Method of Software Protection Based on the Use of Smart Cards and Cryptographic Techniques.....	446
T. SCHALNBUELLER, F. PILLER	

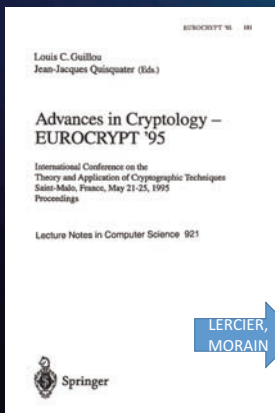
SECTION VI: SMART CARDS	
Introductory Remarks.....	457
A. TURBAT	
Smart Card Applications in Security and Data Protection.....	459
J. GOUTAY	
Bull CP8 Smart Card Uses in Cryptology.....	464
Y. GIRARDOT	
Estimation of Some Encryption Functions Implemented into Smart Cards.....	470
H. GROSCHOT	
Smart Cards and Conditional Access.....	480
L. GUILLOU	
AUTHOR INDEX.....	491

LOUIS GUILLOU



Mais le point principal de cette participation fut la dernière session. Il eut cinq présentations sur les cartes à puce. Ce n'était pas vraiment de la recherche, c'était plutôt une description d'idées et de produits. Mais la principale présentation, la dernière, fut celle donnée par Louis Guillou. C'était très important parce que c'était la première fois que quelqu'un parlait publiquement d'algorithmes cryptographiques dans les cartes à puce. Et cette présentation a été le début de l'histoire des cartes à puce DES et des cartes à puce RSA.

# EUROCRYPT 1995: Saint-Malo

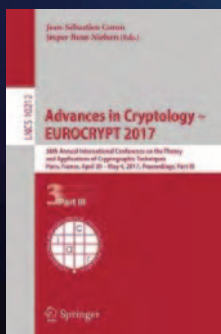


LERCIER,  
MORAIN



La conférence suivante, en France, Eurocrypt, eut lieu en 1995. Encore Louis Guillou et moi-même pour l'organisation. Et vous pouvez voir ici que nous sommes passés de deux (à la première conférence) à cinq personnes scientifiques de France, cette fois-ci. Bon, ça augmentait !

## EURO CRYPT 2017: Paris



15 authors

LETTRÉS  
SORBONNE  
UNIVERSITÉ



Enfin, la dernière fois qu'Eurocrypt s'est déroulé en France, à Paris, en 2017, il y avait 15 auteurs français. Donc ça augmente vraiment, ça augmente, ça augmente.

## Teaching first, next research, then applications ...

CRYPTIS, Limoges, from 1986 (Jean-Louis Nicolas):

❖ Mainly number theory at the beginning,

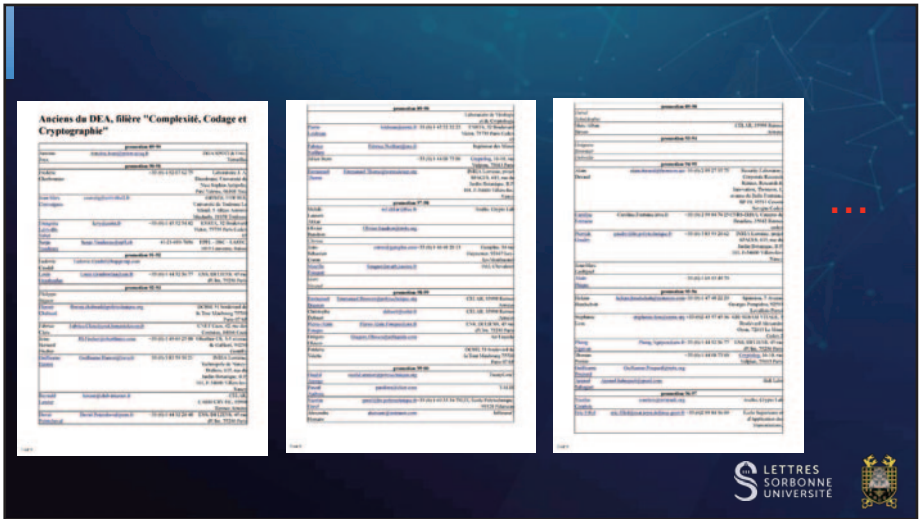
DEA ENS-X (filière Codage, Complexité et Cryptographie), Paris, from 1991: the main source of scientists about cryptography, courses organized by Jacques Stern, main teacher: JJQ.

LETTRÉS  
SORBONNE  
UNIVERSITÉ



Enseigner la cryptographie au début des années 80 n'était pas facile vu les contraintes. Il n'y avait qu'un seul enseignement à Limoges appelé Cryptis à partir de 1986. Ce fut surtout un début et ouvrant de plus en plus la recherche sur la cryptographie. Le principal lieu d'enseignement, un DEA, était à Paris à l'École Normale Supérieure (ENS) organisé par Jacques Stern à partir de 1991. À cette époque, j'étais l'enseignant désigné en collaboration chaque année avec un grand professeur (Gilles Brassard, Claude Crépeau, Adi Shamir...). Et cet enseignement était la principale source de scientifiques en cryptographie en France.





Vous pouvez voir ici la liste des inscrits pour chaque année. La première année, il n'y avait qu'une seule personne mais beaucoup plus par la suite. Toutes les personnes importantes jusqu'en 2010, vous pouvez dire qu'elles viennent principalement d'ici.

## IACR: International Association for Cryptologic Research

- President: Michel Abdalla (CNRS-ENS) 2020-2022
- Fellows:
  - ❖ Jacques Stern
  - ❖ Antoine Joux
  - ❖ Louis Guillou
  - ❖ David Naccache

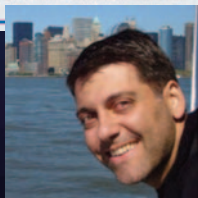
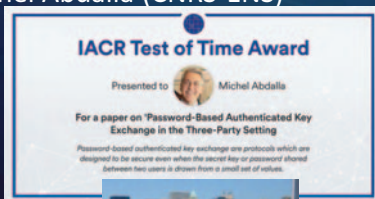
Vous savez qu'il existe une association internationale sur la recherche en cryptographie, l'IACR et le président est aujourd'hui Michel Abdalla, jusqu'à la fin de cette année, et il vient de l'ENS. Il y a également quatre associés (fellow) pour cet organisme: Jacques Stern à nouveau, Antoine Joux qui a été le premier élève du DEA, Louis Guillou à nouveau et David Naccache.

# IACR: International Association for Cryptologic Research

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

Fellows:

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



Vous pouvez voir ici que Michel était un bon chercheur, faisant beaucoup de publications et qu'il a reçu un test de renommée de l'IACR.

## Jacques Stern (master of secrets)

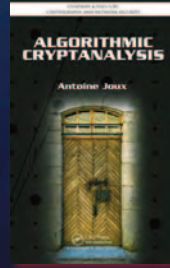


Jacques Stern ici avec deux livres importants, hélas uniquement en français pour le moment.

## 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



LETRES  
SORBONNE  
UNIVERSITÉ



Antoine Joux recevant (photos de gauche) le prix Gödel mais ayant aussi écrit un livre très important sur la cryptanalyse.

## David Naccache

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



LETRES  
SORBONNE  
UNIVERSITÉ



David Naccache également à l'ENS et avec de nombreuses phases de recherche.



## ANSSI: Guillaume Poupard



Multiple research,  
Multiple publications,  
New protocols ...

Since 2014, Guillaume Poupard is the director general of the National Agency for Information Systems Security (ANSSI)

<https://www.ssi.gouv.fr/en/>

LETRES  
SORBONNE  
UNIVERSITE



Nous avons également l'ANSSI: l'agence nationale pour la sécurité des systèmes d'information, une petite NSA avec à sa tête aujourd'hui Guillaume Poupard. Celui-ci fut un très bon élève du DEA et vous voyez à droite la liste des nombreux articles qu'il a publiés. Il est donc important de voir qu'à la tête de l'ANSSI, il y a un docteur auteur de nombreuses publications.

## Post quantum Research



Normal Shakespeare:  
TO BE OR NOT TO BE

Quantum Shakespeare:  
TO BE AND NOT TO BE

LETRES  
SORBONNE  
UNIVERSITE



Maintenant, nous pouvons parler d'aujourd'hui. Il y a beaucoup de recherches sur la cryptologie post-quantique car nous avons grand besoin de nouveaux et bons algorithmes. Oui, la recherche quantique doit être et ne pas être dans un certain sens.



Suite à l'appel du NIST, il y a eu plusieurs tours, on est aujourd'hui au tour numéro trois, et il y a eu beaucoup de soumissions. Du tour un au tour trois, on est passé de 55 à 7 soumissions retenues.

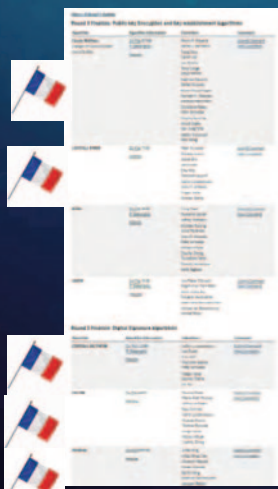
## Postquantum cryptography (PQC)

- 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/>

Il est intéressant de voir qu'il existe de nombreux papiers et panels sur ce sujet et le NIST espère publier des projets de normes dans les prochaines années. Vous voyez également un lien sur le point de vue de l'ANSSI au sujet de la transition vers la cryptographie post-quantique. Il est important en effet de passer de l'AES, du RSA et des courbes elliptiques à un nouvel algorithme, ce n'est pas facile.

## NIST: PQC



The image shows a screenshot of the NIST PQC candidate list. Five entries are highlighted with small French flags to the left of their names. The highlighted entries are: 1. 'FHE (Fully Homomorphic Encryption)', 2. 'HE (Homomorphic Encryption)', 3. 'ML-HE (Machine Learning Homomorphic Encryption)', 4. 'PHE (Public Key Encryption)', and 5. 'SHE (Somewhat Homomorphic Encryption)'. The rest of the list is partially visible but not highlighted.

Plus alternate versions

LETRES  
SORBONNE  
UNIVERSITÉ



Récemment la liste des sept candidats en lice a été publiée. Vous voyez la liste ici et vous voyez que cinq des sept algorithmes incluent des français. Il y a donc beaucoup de monde et en fait il y en a plus parce qu'il y a aussi des versions alternatives qui ne seront peut-être pas des normes dans un premier temps mais peut-être plus tard.

### 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.

LETRES  
SORBONNE  
UNIVERSITÉ



La conclusion pour ma part est que la France en matière de cryptologie est à nouveau au centre de la recherche, de la conception, de l'application et de la production. Cela s'est fait d'abord grâce à un enseignement de haut niveau, avec de très bonnes personnes c'est important, et ensuite ces personnes se retrouvent partout en France : dans de Grandes Écoles, des universités, des laboratoires de recherche, des entreprises, dans l'administration, les services et j'en passe. Comme vous pouvez le voir un très bon résultat a été obtenu en une vingtaine d'années d'efforts. Je vous remercie de votre attention.