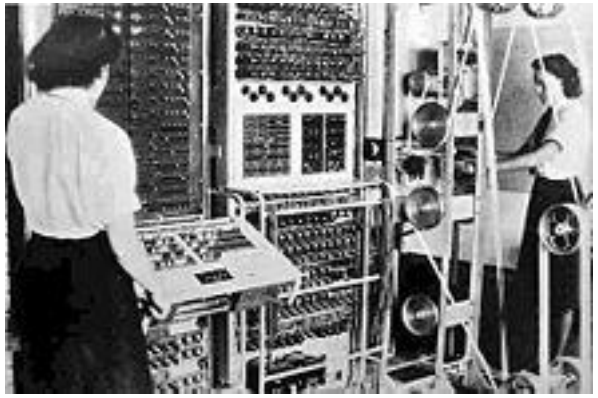
Une courte Histoire de la Cryptographie depuis 1945

Jacques Patarin

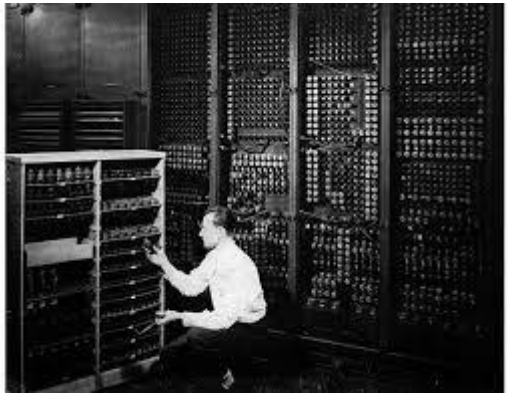
Les premiers ordinateurs, 1941-1946

18 mars **1940** : la Bombe (UK, Enigma)
1941 : Le Z3 de Konrad Zuse (électromécanique, relais)
1942: L'ABC (Atanassoff-Berry Computer) testé avec succès
5 février **1944** : Colossus (UK, tubes à vide, Lorenz)
Février **1946** : ENIAC (tubes à vide)

Bombe



Colossus



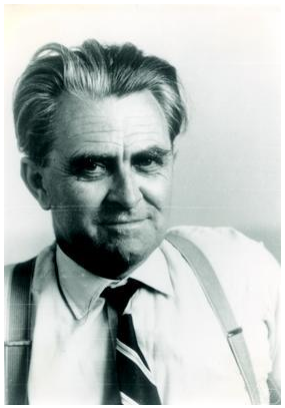
ENIAC

1952 : création de la NSA (National Security Agency)

Le « Téléphone Rouge »
(depuis 1963 entre Moscou et Washington)

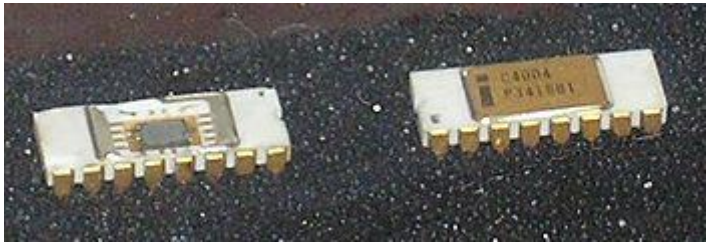
1965 : les « bases de Gröbner » par Bruno Buchberger

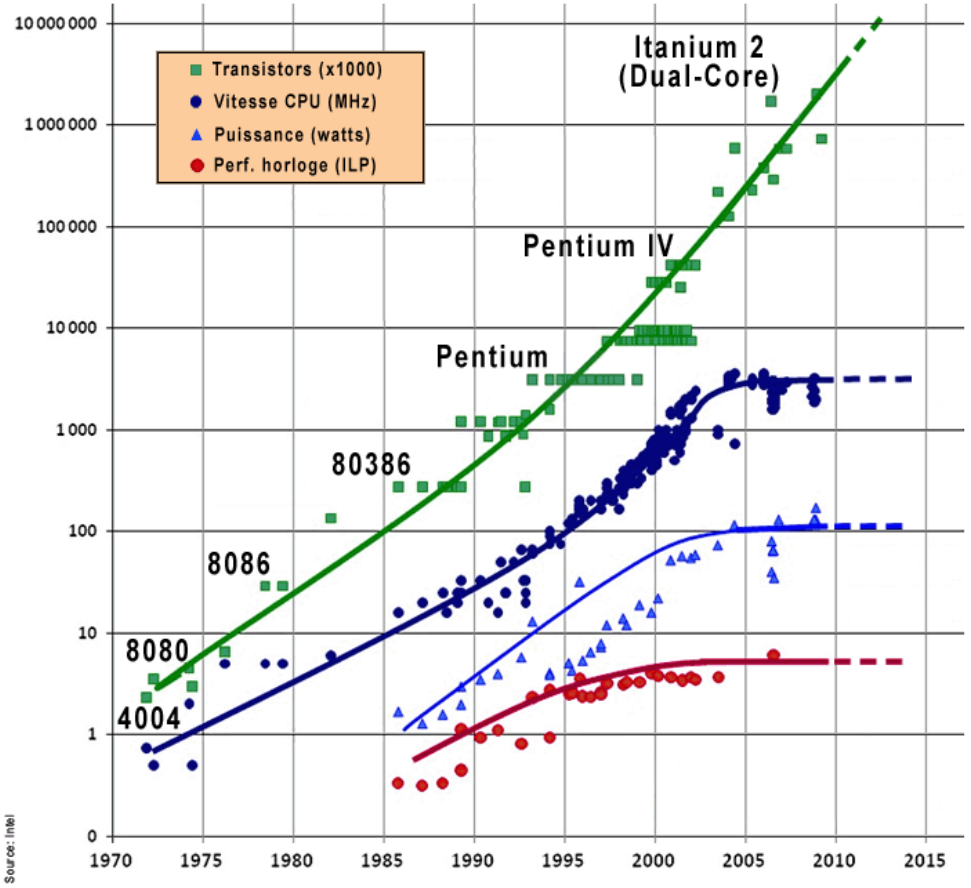
- 1913 : Gjunter (à Leningrad) étudie le concept.
- 1964 : Heisuke Hironaka étudie et retrouve indépendamment le concept.
- 1965 : Bruno Buchberger étudie et retrouve indépendamment le concept et lui donne le nom de son directeur de thèse (Gröbner).
- Depuis : les algorithmes de calculs ont été beaucoup améliorés (en particulier par Jean-Charles Faugère).



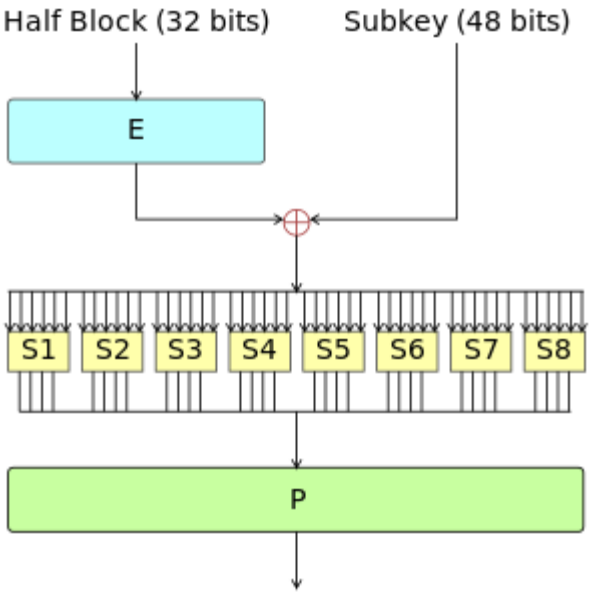
Les microprocesseurs
depuis 1971

15 novembre 1971 : Intel 4004, 4 bits, 2300 transistors, 90 000 opérations /s, 740 kHz

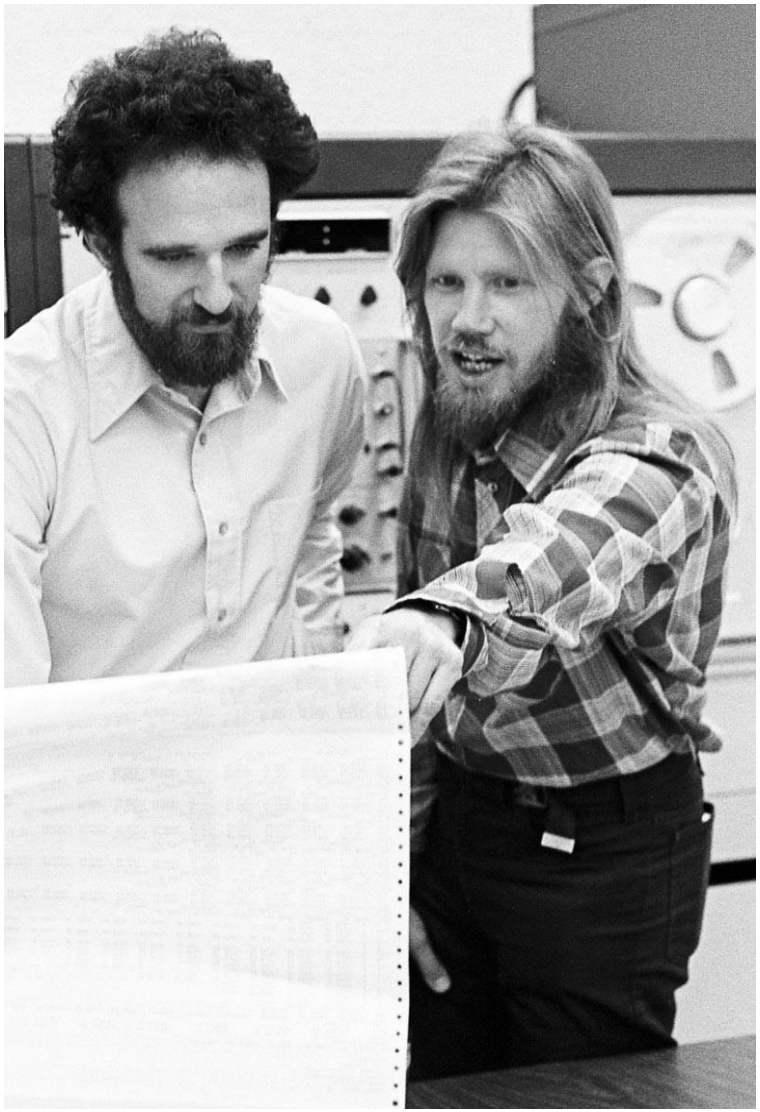




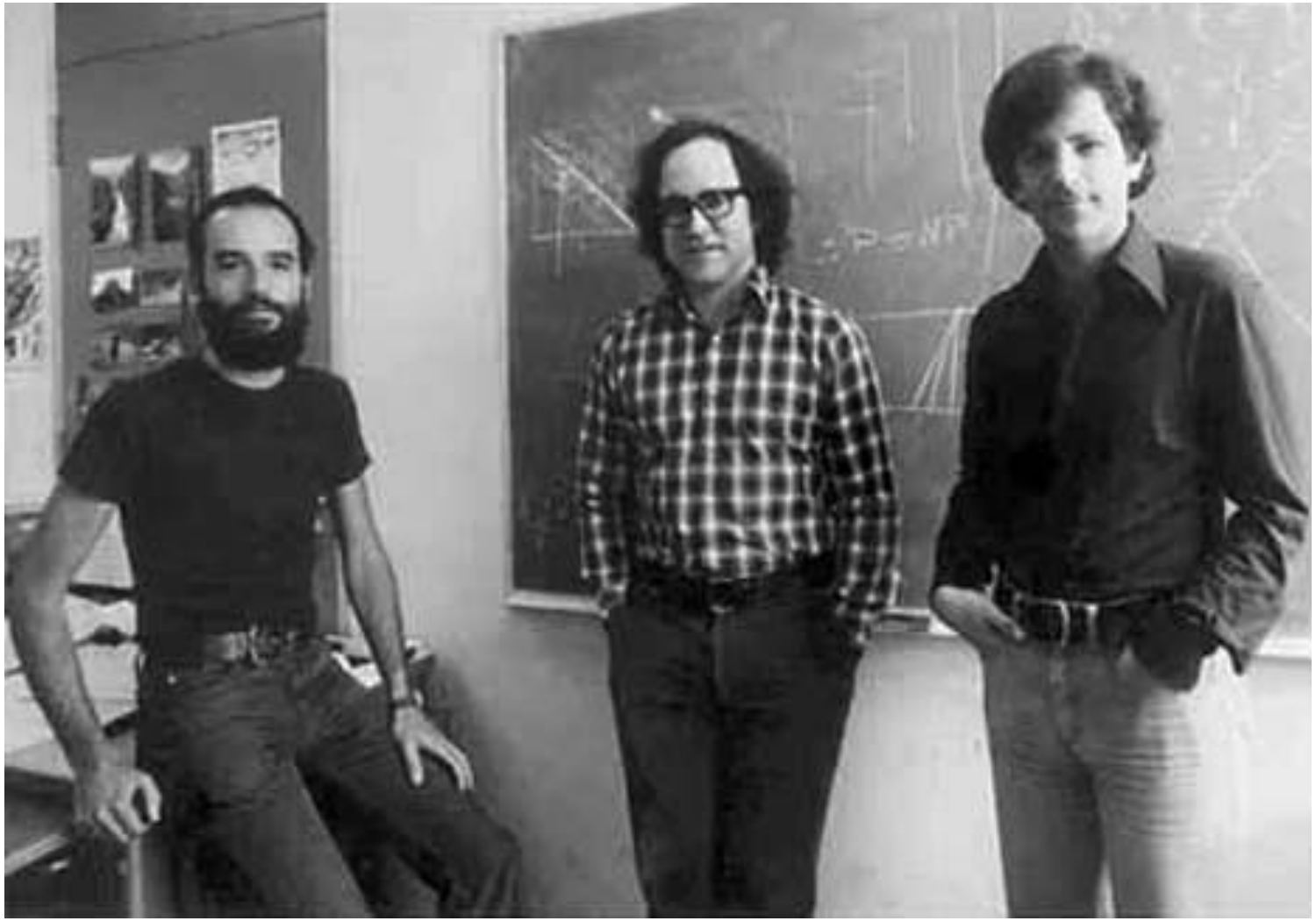
Le DES (Data Encryption Standard), 1974



Le Diffie-Helman
1976, La Cryptographie à clé publique

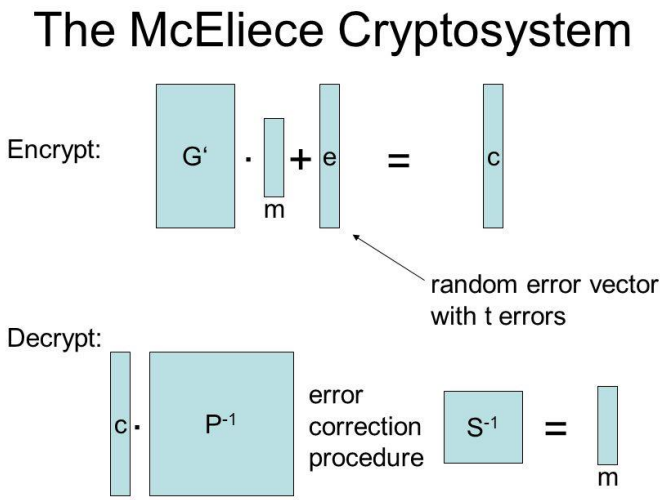


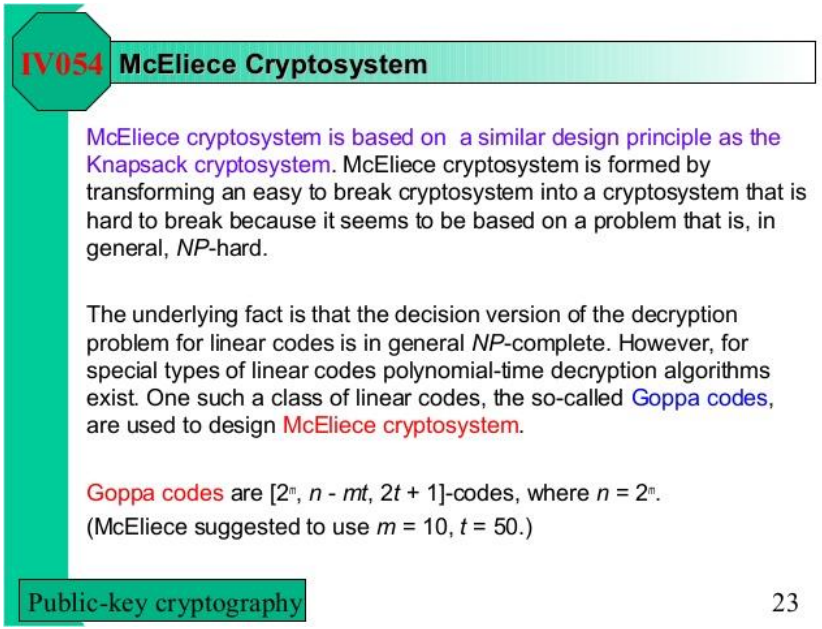
Rivest, Shamir, Adelman (1977)
La Cryptographie à clé publique



Cryptographie à base de Codes Correcteurs

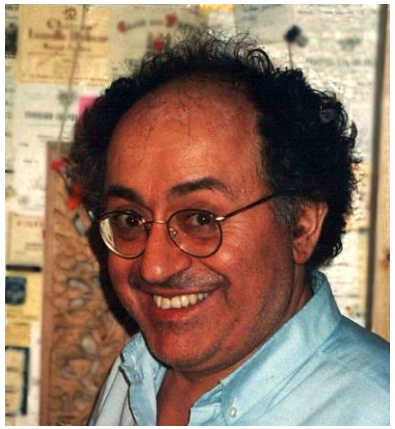
- 1978 : McEliece
- 1986 : Niederreiter
- Taille de la clé publique > 65 000 bits.





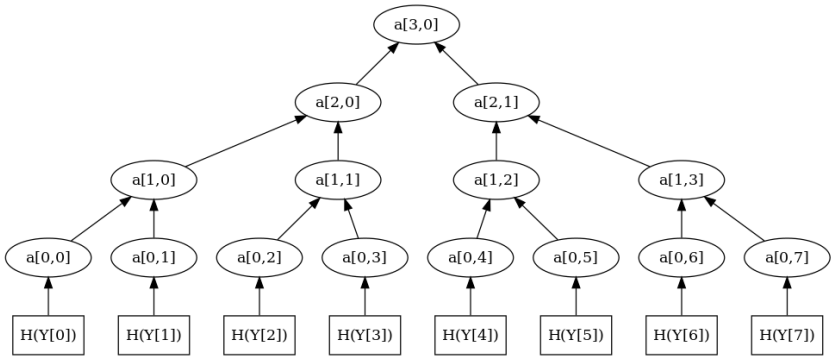
1979 : sortie de la 1ère carte à puce (avec microprocesseur)

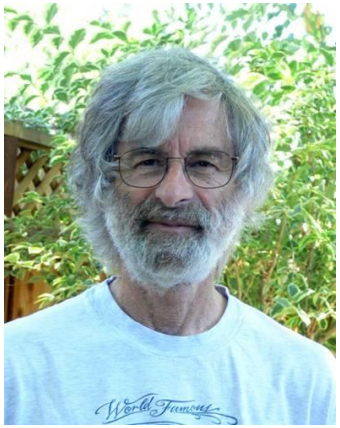
- 1967 : René Barjavel écrit « la nuit des temps »
- 1967 : premiers brevets (jamais utilisés)
- 1974 : Brevets de Roland Moreno sur la carte à puce à mémoire (bague)
- 1977 : Brevet de Michel Ugon sur les cartes à microprocesseurs
- 1978 : Brevet de Michel Ugon sur les cartes monocomposants
- 21 mars 1979 : sortie de la 1ère carte à microprocesseur
- 1985 : le GIE-CB commande 16 millions de cartes à puce



1979 : les arbres de Merkle et les signatures de Lamport

- C’est une construction Post-Quantique naturelle (très simple) pour l’authentification et les signatures à clé publique (pas le chiffrement).
- La sécurité ne dépend que de fonctions à sens unique.
- Mais la clé est un peu consommée à chaque usage.





1982 : l'algorithme LLL

LLL : algorithme de A. Lenstra, et H. Lenstra, L. Lovasz.

- Entrée : d vecteurs de bases d'un réseau de dimension n et de norme inférieure à B.

- Sortie : une base de réseau LLL-réduite (« presque » orthogonale).

  Complexité en temps polynomial :

  $O(d^5 n \log^3 B)$

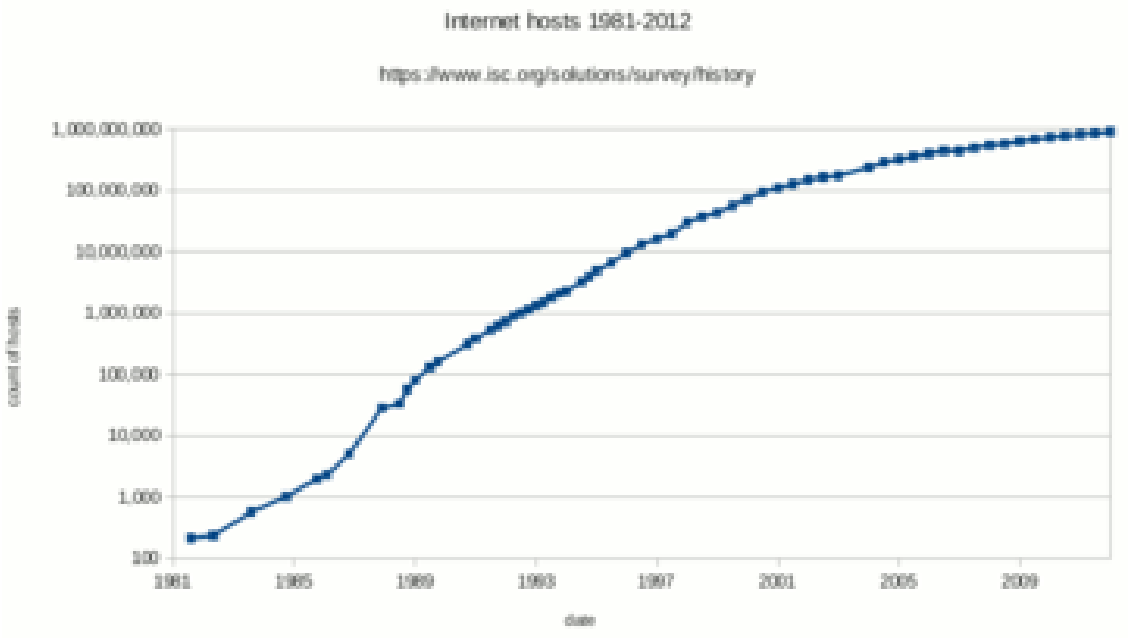
Les débuts d'Internet (vers 1983)

29 octobre **1969** : envoie de « Login » entre l'UCLA et Standford (réseau de transfert de paquet)

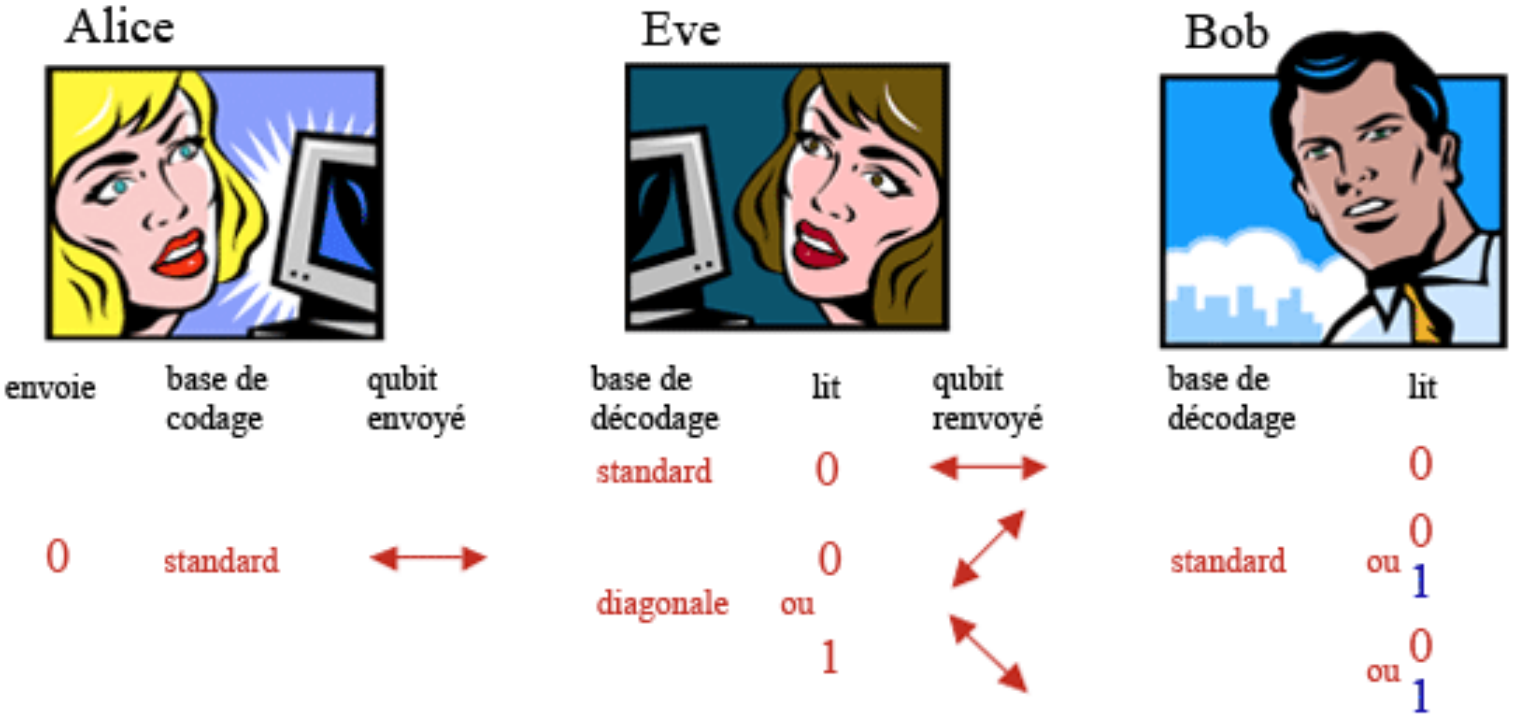
1974 : début de TCP/IP sur une partie d'ARPANET

1er janvier **1983** : tout ARPANET en protocole TCP/IP

1989 : début du www au CERN (système hypertexte)



La Cryptographie Quantique
BB84 : 1984

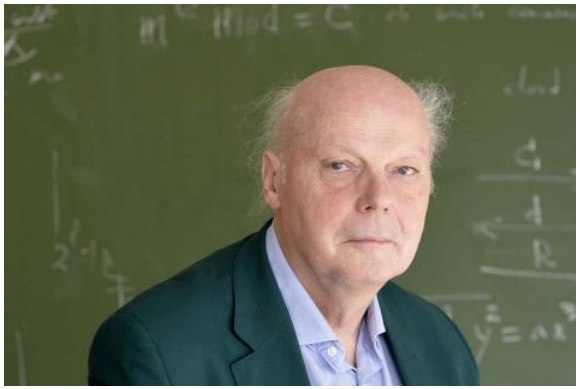


Le Zero-Knowledge

1984 : Fisher-Micali-Rackoff

1986 : Fiat-Shamir

1988 : Guillou-Quisquater

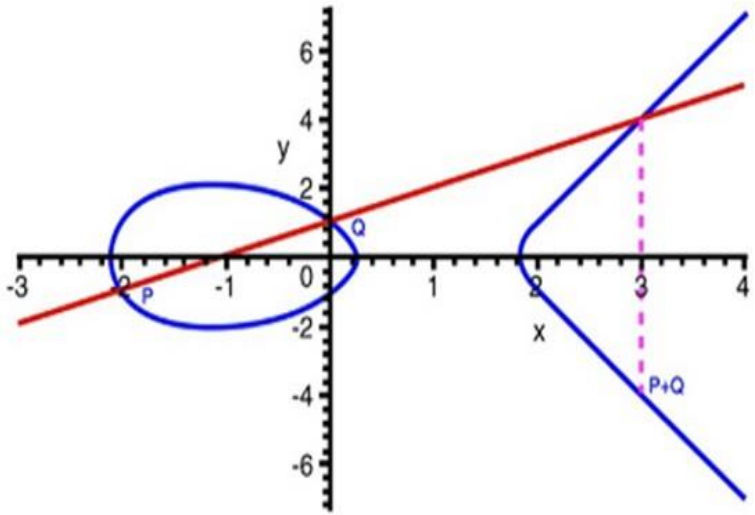


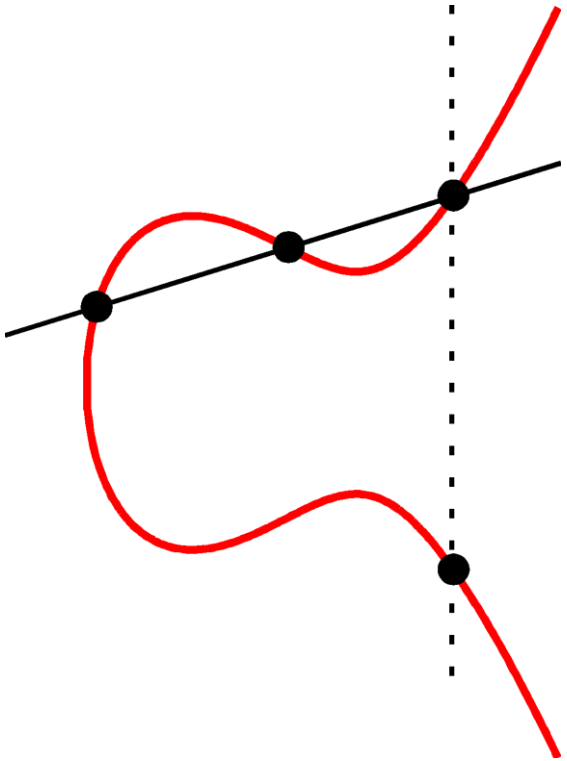
Les algorithmes de ElGamal
Taher ElGamal, 1985

ECC: Elliptic Curve Cryptography

Neal Koblitz, Victor Miller, 1985

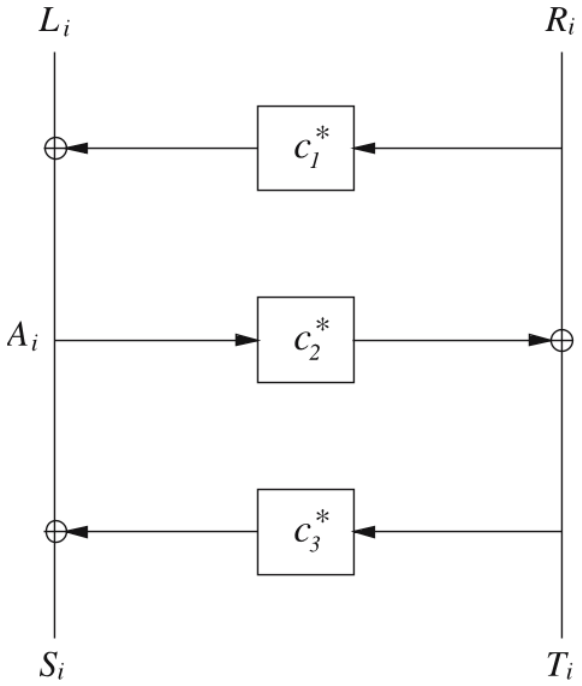
$$y^2 = x^3 + ax + b$$





1988 : le théorème de Luby et Rackoff

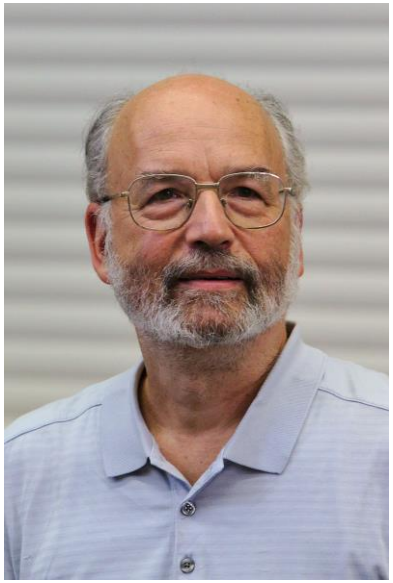
- Il permet de générer des permutations (i.e. bijections) pseudo aléatoires de 2n bits vers 2n bits à partir de (3 ou 4) fonctions pseudo aléatoires de n bits vers n bits.



1989 : la Cryptanalyse différentielle

- 1989 : Eli Biham et Adi Shamir découvrent et publient la Cryptanalyse différentielle.

(Elle était connue d'IBM depuis 1974 et de la NSA probablement avant).



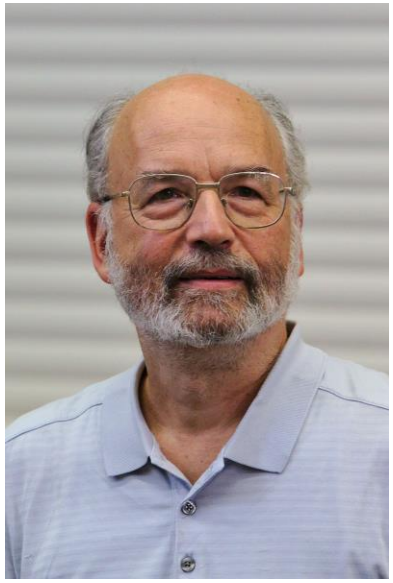
Don Coppersmith, IBM

"After discussions with NSA, it was decided that **disclosure of the design considerations would reveal the technique of differential cryptanalysis**, a powerful technique that could be used against many ciphers. This in turn **would weaken the competitive advantage the United States enjoyed over other countries** in the field of cryptography."

see: Coppersmith, Don (May 1994). "The Data Encryption Standard (DES) and its strength against attacks" (PDF). *IBM Journal of Research and Development* **38** (3): 243. http://www.research.ibm.com/journal/rd/383/coppersmith.pdf.

1989 : l’algorithme PKP de Shamir

- En 1989 Adi Shamir publie un algorithme d’authentification à clé publique qui est à la fois Zero-Knowlege, et basé sur un problème NP complet combinatoire : le problème des noyaux permutés (Permuted Kernel Problem).
- Cet algorithme, très efficace en authentification, peut être aussi utilisé en signature (mais pas en chiffrement). C’est un candidat naturel de Cryptographie Post-Quantique pour l’authentification ou la signature.



1989-1990 : découverte de l'algorithme de factorisation NFS

Pommerance, Buh, Lenstra, Coppersmith

$$O\left\{\exp\left[\left(\frac{64}{9}\log n\right)^{\frac{1}{3}}(\log\log n)^{\frac{2}{3}}\right]\right\}$$

avec $(64/9)^{1/3} \backsimeq 1.923$

David Chaum
DigiCash 1990-1999

Philip Zimmermann (PGP, 1991)

1993 : la Cryptanalyse Linéaire

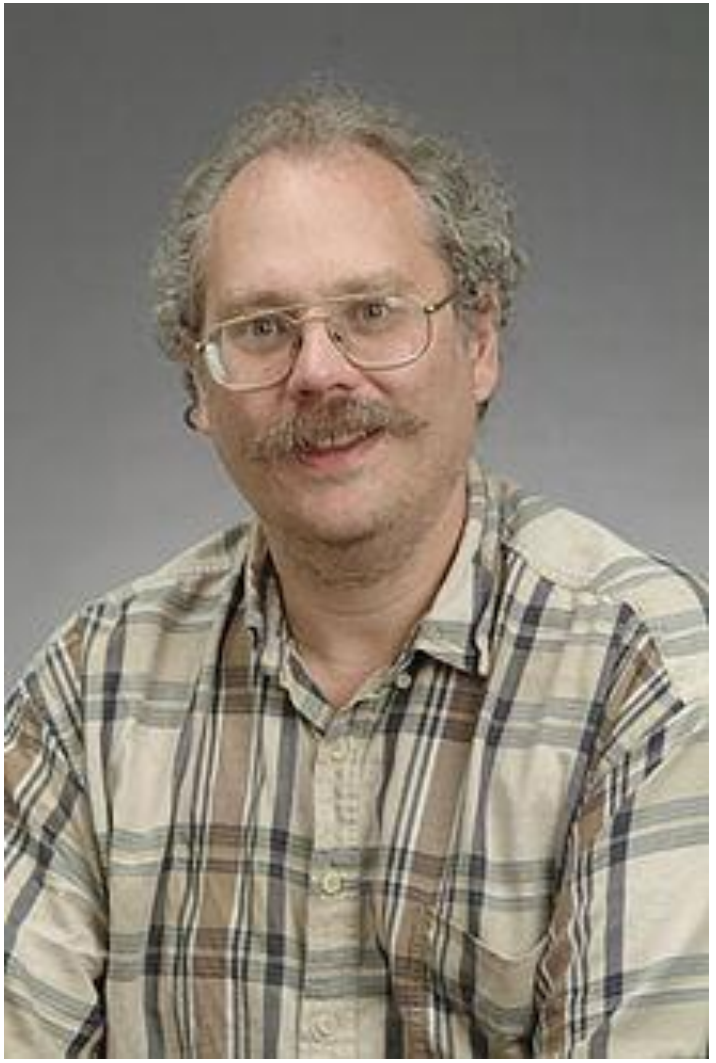
- 1991 : Henri Gilbert et Anne Tardy-Corfdir publient une attaque sur FEAL à partir d'expressions linéaires probabilistes.
- 1993 : Mitsuru Matsui publie la Cryptanalyse Linéaire du DES.

L’algorithme de factorisation quantique de Peter Shor, 1994

2001 : 15 = 3 * 5

2012 : 21 = 3 * 7

143 = 11 * 13



1996 : début de la Cryptographie à base de réseaux (« Lattice based Cryptography »)

- 1996 : schéma initial de Miklos Ajtai (avec preuve).
- 1996 également : schéma NTRU de Jill Pipher et Joseph Silverman (sans preuve).
- 2005 : chiffrement de Oded Regev (basé sur le problème LWE : Learning with Errors).
- 2013 : BLISS signatures
- 2015 : Algorithme d’échange de clés « New Hope ».

1996 : l'algorithme multivariable HFE

- 1988 : Matsumoto et Imai présentent l'algorithme multivariable C* (cassé en 1995). Début traditionnel de la Cryptographie Multivariable.
- 1996 : HFE : Hidden Field Equation, (J. Patarin)
- 1999 : UOV : Unbalanced Oil and Vinegar (J. Patarin, Louis Goubin, Aviad Kipnis).
- La Cryptographie multivariable est actuellement la technique qui permet d'avoir les signatures les plus courtes.

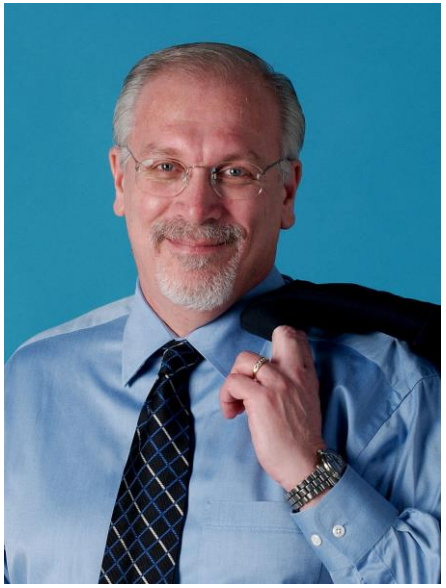
$$y1 = x1x2 + x1x3 + x2x3 + x2x5 + x3x4 + x2 + x3 + 1$$
$$y2 = x1x3 + x2x3 + x2x4 + x2x5 + x4x5 + x4$$
$$y3 = x2x4 + x2x5 + x3x4 + x3x5 + x4x5 + x1 + x3$$
$$y4 = x1x4 + x1x3 + x2x5 + x4x5 + x2 + x5 + 1$$
$$y5 = x1x2 + x1x4 + x1x5 + x2x3 + x2x4 + x3x5 + x4 + x5 + 1$$

Septembre 1996 : les attaques par fautes DFA

- DFA : Differential Fault Analysis, par Dan Boneh, Richard DeMillo, et Richard Lipton

(ou « attaques de Berkeley », « attaques de Bellcore », « attaques du micro-onde », « attaques par stress »).

C’est un cas particulier d’attaques par « canaux cachés » (« side chanel attacks »).

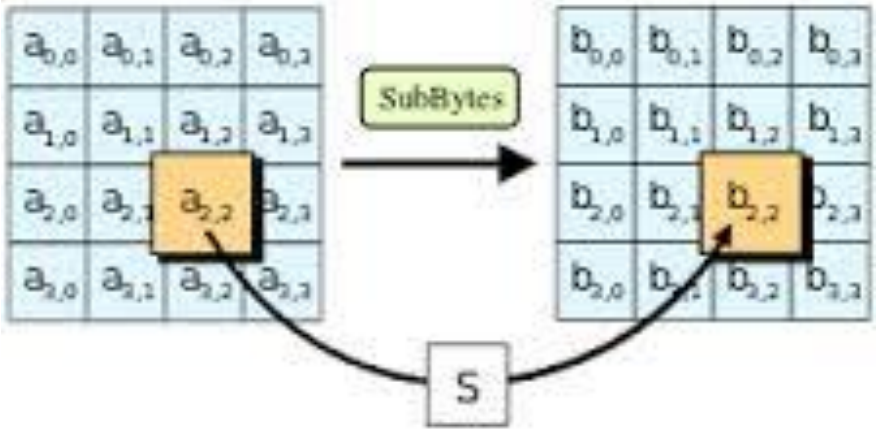


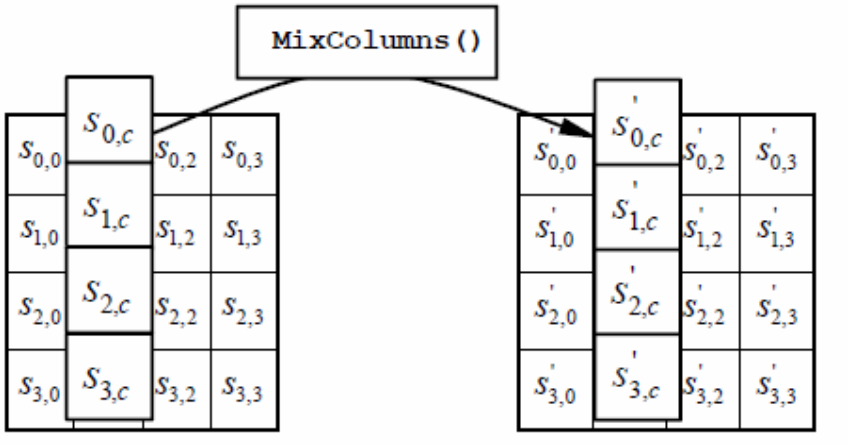
SPA, DPA

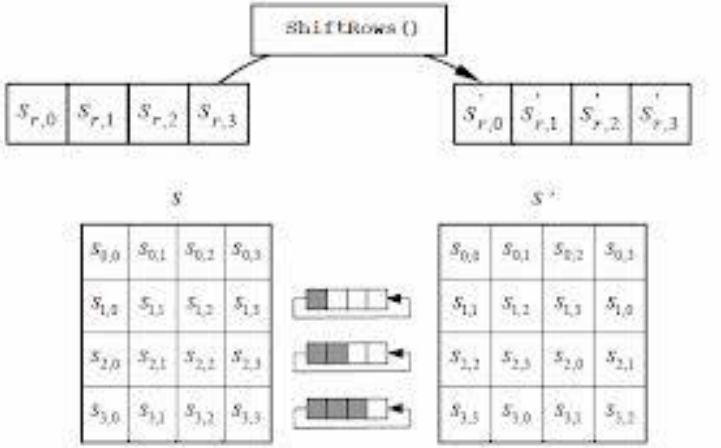
(Simple Power Analaysis, Differential Power Analysis)

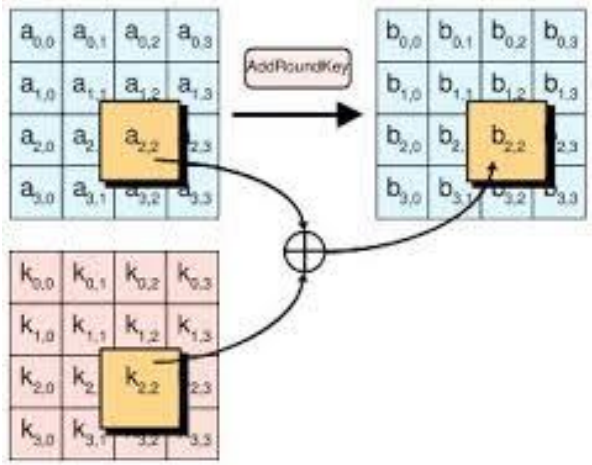
Paul Kocher, 1998

AES : Advanced Encryption Standard
Joan Daemen, Vincent Rijmen, 2000









addRoundKey step

2000-2001 : pairing based Cryptography
2000 : Joux (DH à 3 joueurs)
2001 : Boneh-Franklin (Identity based Encryption)

Wang Xiaoyun, 2004-2005
Attaques sur MD5 et SHA_1

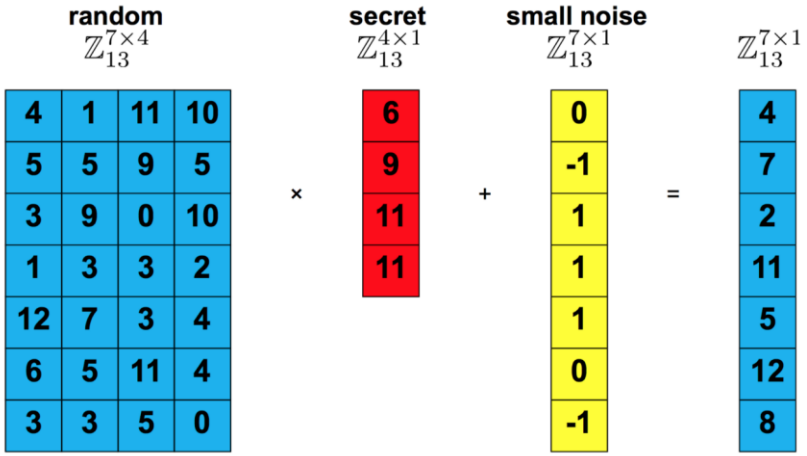
LWE (Learning with Errors), 2005

- 2005: Oded Regev (Gödel prize 2018) introduce and study the LWE problem in Cryptography.

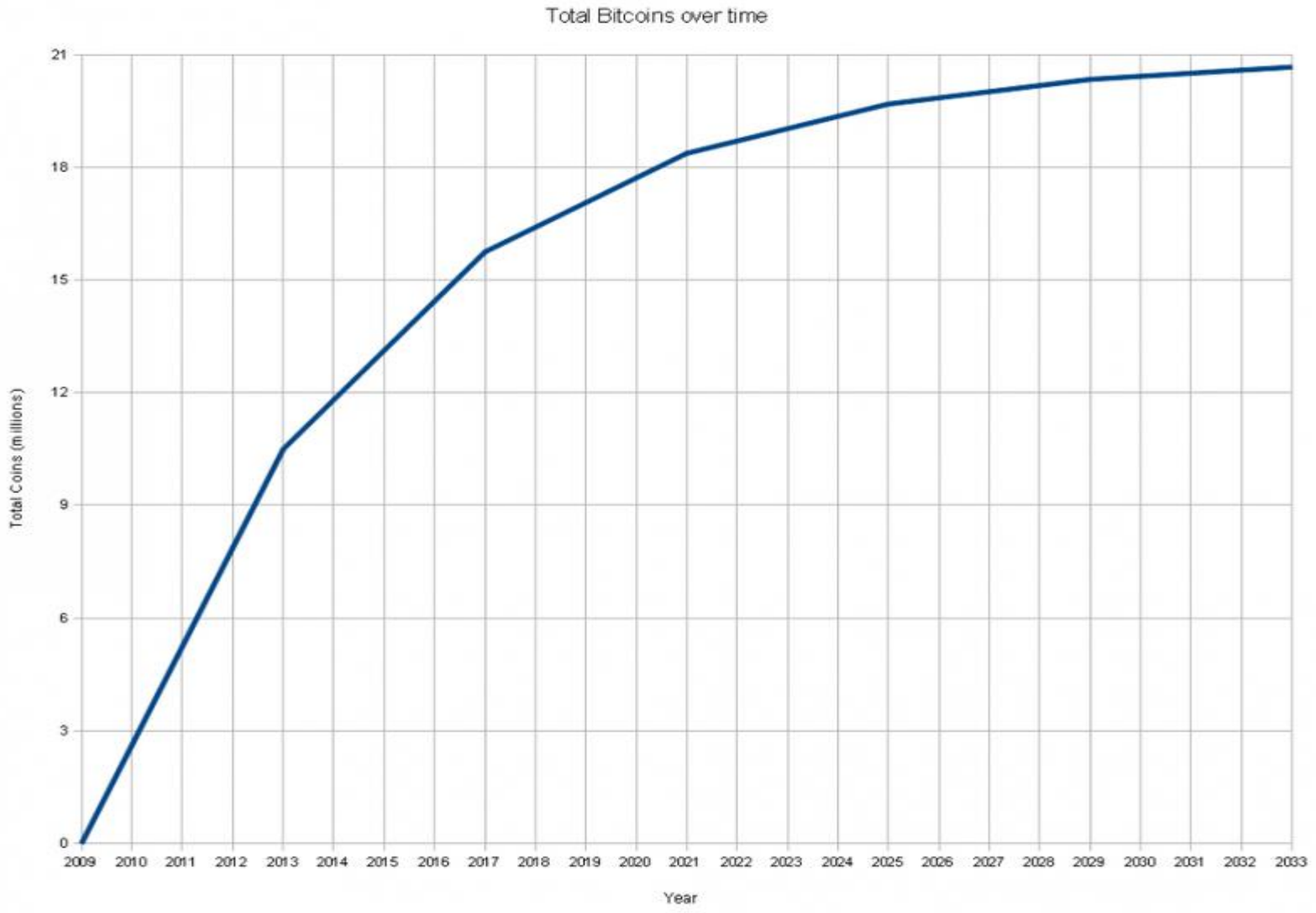
  LWE is NOT proved to be a NP hard problem (and in fact is probably not NP hard).

  However:

  - SVP (Smallest Vector Problem on Euclidian lattices) with a polynomial approximation factor can be solved from LWE. (SVP with much smaller approximation factors are N hard).
  - LWE is expected to be Post Quantum (i.e. not to be polynomial on quantum computers).
  - Average complexity is similar to worst case complexity



Les Bitcoins (depuis janvier 2009)



Fully Homomorphic Encryption
Craig Gentry, 2009

- Un algorithme de chiffrement « totalement homomorphe » est un algorithme de chiffrement à clé publique tel qu'il est possible de chiffrer x + y et x.y à partir du chiffré de x et du chiffré de y (sans avoir à connaître les valeurs en clair de x et y).

RLWE (Ring Learning with Errors), 2010

- 2010: V. Lyubashevsky, C. Peikert and O. Regev introduce RLWE in Cryptography.

This RLWE problem usually gives much more efficient cryptographic schemes than LWE (typically the square roots of the number of bits, or 8 000 bits instead of millions of bits).

- With LWE (cf for example [BV1]) we have linear equations modulo p, but with some small errors with a Gaussian distribution.
- With RLWE (cf for example [BV2]) we work modulo a polynomial (ring with polynomials).

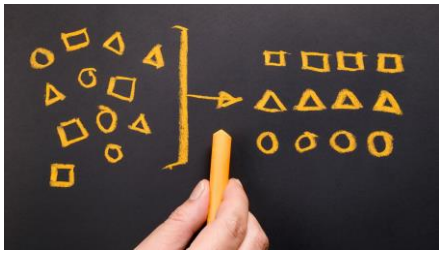
However:

■ The security of RLWE is proved to be at least as hard as approximate SVP (Short vector problem in the worst case) on ideal (special class of lattices with a structure) lattices.

■ Since the problem is now on structured lattices it is more difficult (from practical and theoretical point of view) to have confidence in the security of some specific instances.

This is why ANSSI, and the German analogue do not recommend cryptography based on RLWE but prefer LWE.

(for example for the Post-Quantum competitions).



2013 : une percée théorique importante pour obtenir l'Obfuscation

- 1936 : Alan Turing prouve l'indécidabilité du problème d'arrêt.
- 1953 : Théorème de Rice : pour toute propriété qui n'est ni jamais toujours vraie ni jamais toujours fausse, savoir si un logiciel satisfait cette propriété est indécidable.
- 1997 : Canetti montre qu'il est possible d'obfusquer les certaines fonctions avec des fonctions de hachage, ou via le problème Decision Diffie-Hellman.
- 2001 : Certaines fonctions ne peuvent pas être (au sens de VBB : Virtual Black Box) obfusquées (Barak, Goldreich, Impagliazzo, Rudich, Sahai, Vadhan et Yang).
- 2013 : Il est possible d'obfusquer (au sens iO : indistinguishability Obfuscator, au lieu de VBB) si l'on dispose de Fully Homorphic Encryption et de Multilinear Maps (Garg, Gentry, Halevi, Raykova, Sahai et Waters).

Mais… les Multilinear Maps sont en crise actuellement…

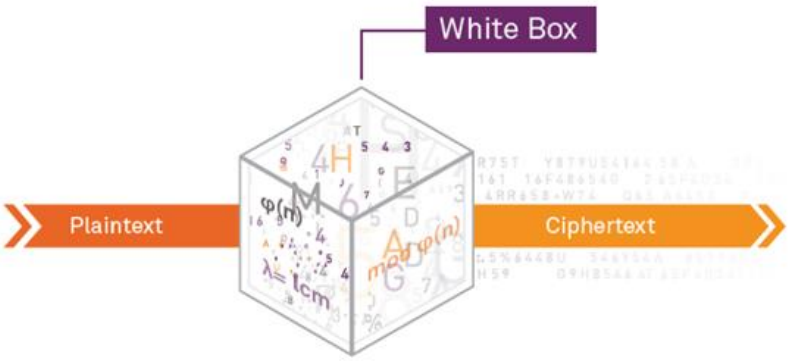
Edward Snowden (2013)

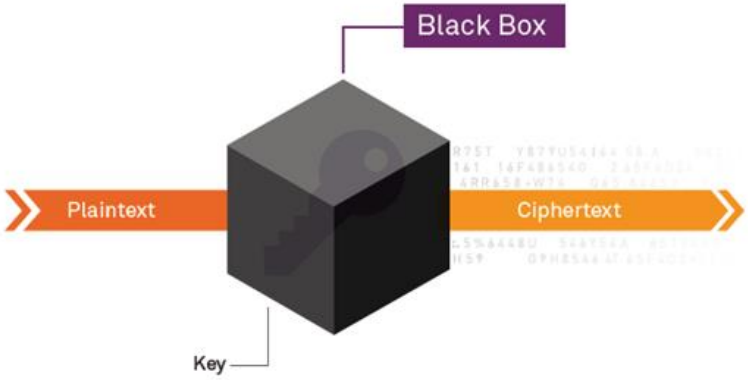
2015 : Differential Computation Analysis (DCA)

2002 : Chow, Eisen, Johnson et van Oorschot proposent des constructions white-box de l'AES et du DES.

Elles seront cassées mais laisseront une forte impression.

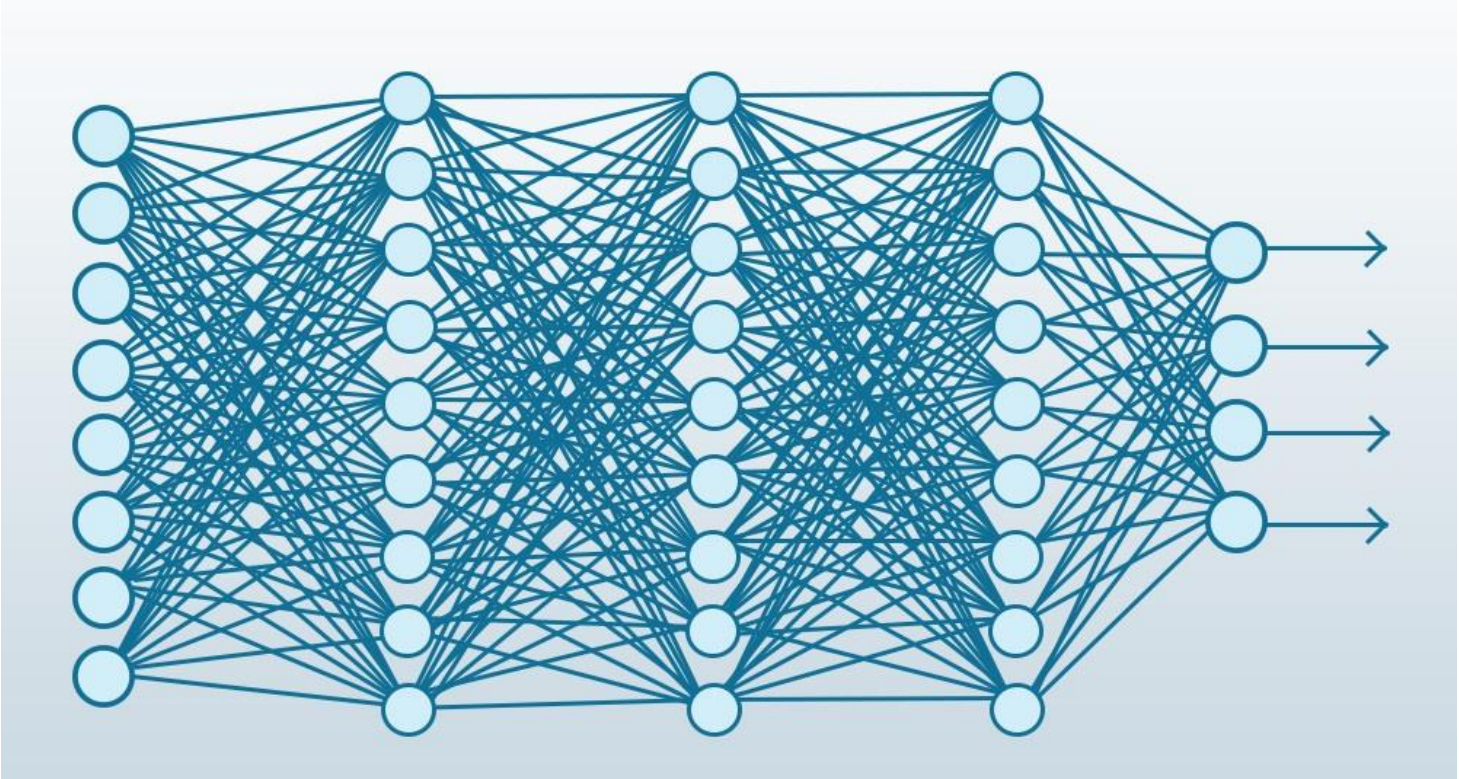
2015 : Bos, Hubain, Michiels et Teuwen publient les attaques DCA.





2017 : Deep Learning sur les Side Channels Attacks

Réseaux Neuronaux et Deep Learning sur les attaques par canaux cachés.



2022: NIST-PQ Competition

5 July 2022: first group of winners:

Type	PKE/KEM	Signature
Lattice	•CRYSTALS-Kyber	•CRYSTALS-Dilithium •Falcon
Hash-based		•SPHINCS+

5 July 2022: 4 candidates for future standardization:

Type	PKE/KEM
Code-based	•BIKE •Classic McEliece •HQC
Supersingular elliptic curve isogeny	•SIKE