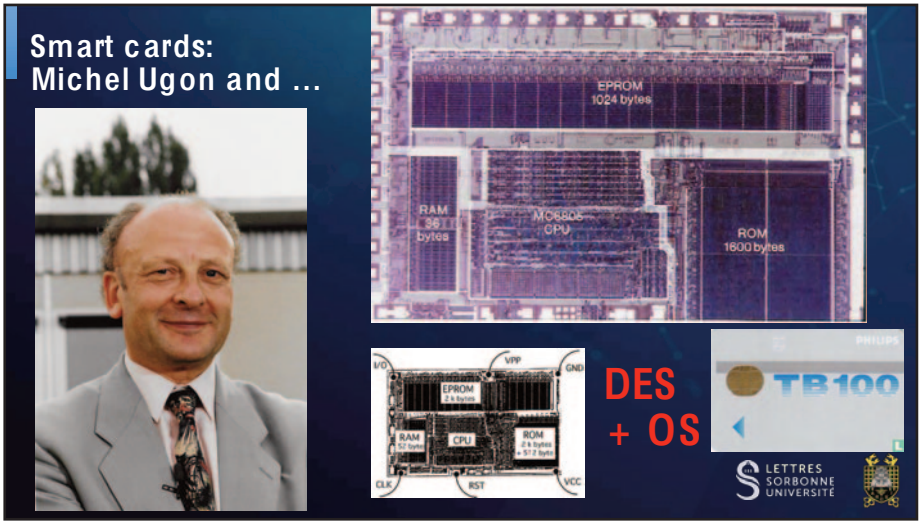
De la carte à puce à nos jours (1967-2022)

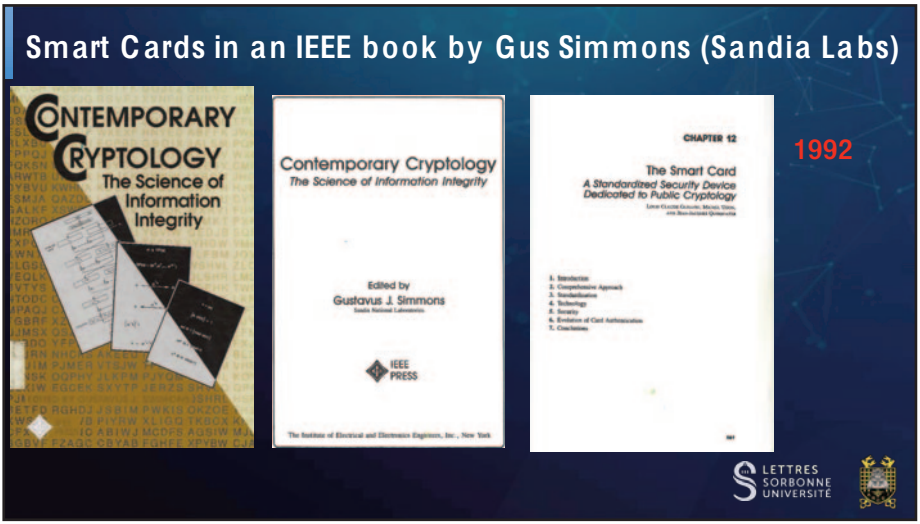
Jean-Jacques Quisquater

Bonjour, 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.

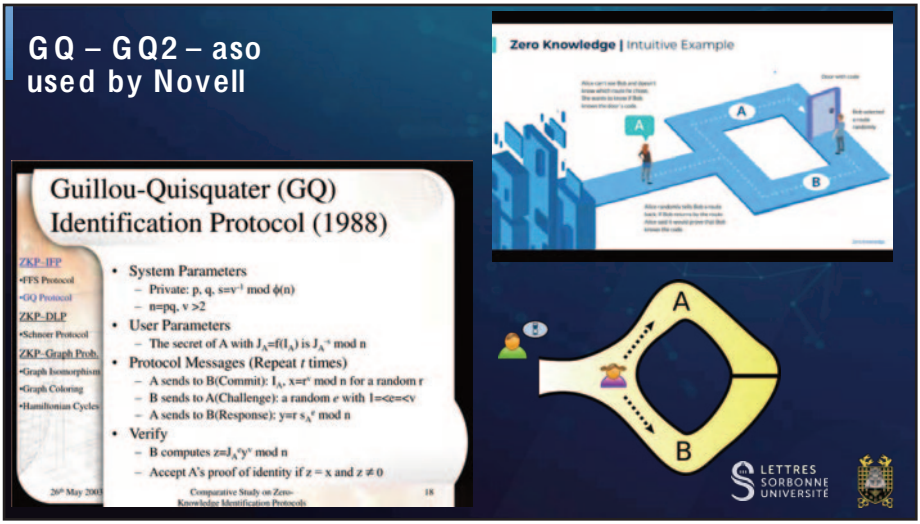


Voici donc de nouveau, Michel Ugon, l'inventeur des cartes à puce à microprocesseurs. Vous voyez ici le premier circuit (photo du haut) avec très peu de mémoire. Le problème principal était vraiment la RAM, avec 36 octets, ce n'est pas beaucoup comme vous pouvez l'imaginer. En fait, la version suivante (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.

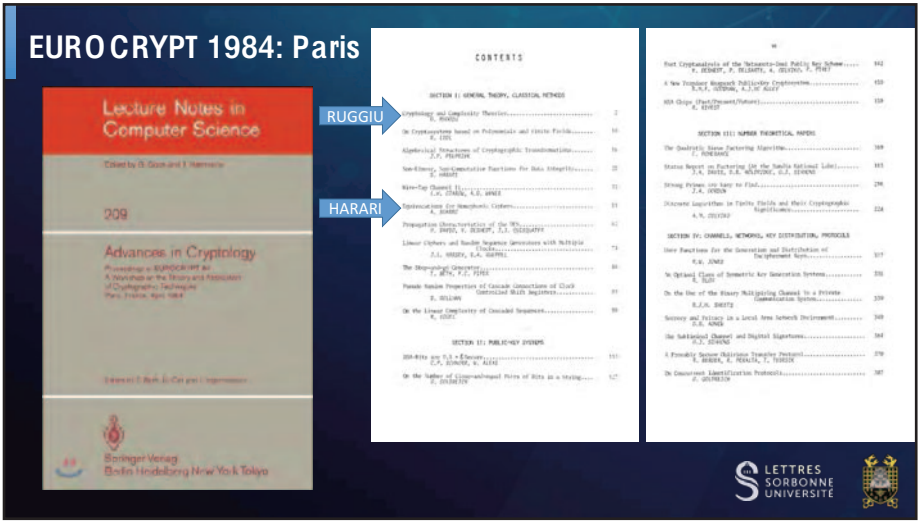
Beaucoup de choses ont été faites en collaboration avec Louis Guillou. Il y avait un paradoxe à cette époque car la cryptographie était principalement réservée à l'administration, à l'armée et aux diplomates or, une carte à puce, c'est de la cryptographie dans la poche de tout le monde. Vous pouvez donc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



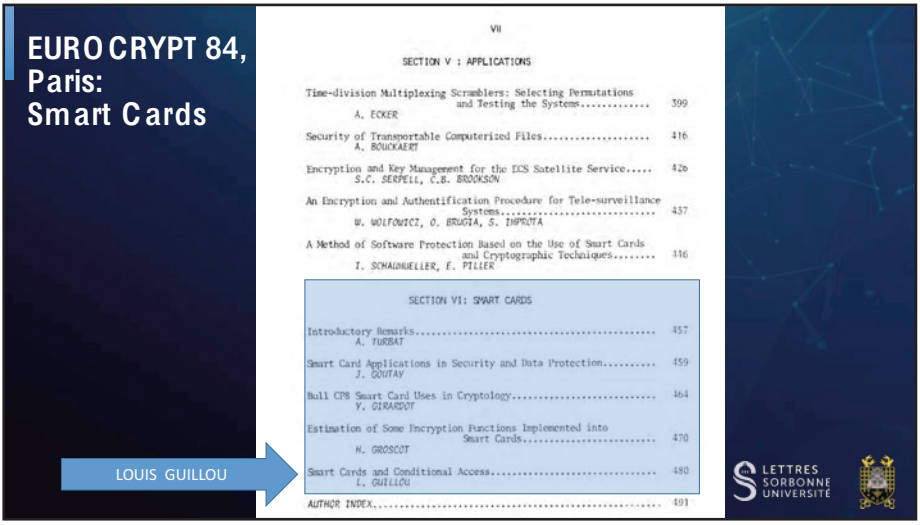
Une coopération très étroite s'est instaurée entre Michel Ugon, Louis Guillou et moi-même. Une contribution importante figure dans le livre IEEE de Gustave Simmons, qui consacre un long chapitre sur les cartes à puce. C'était donc très important et c'était en 1992.



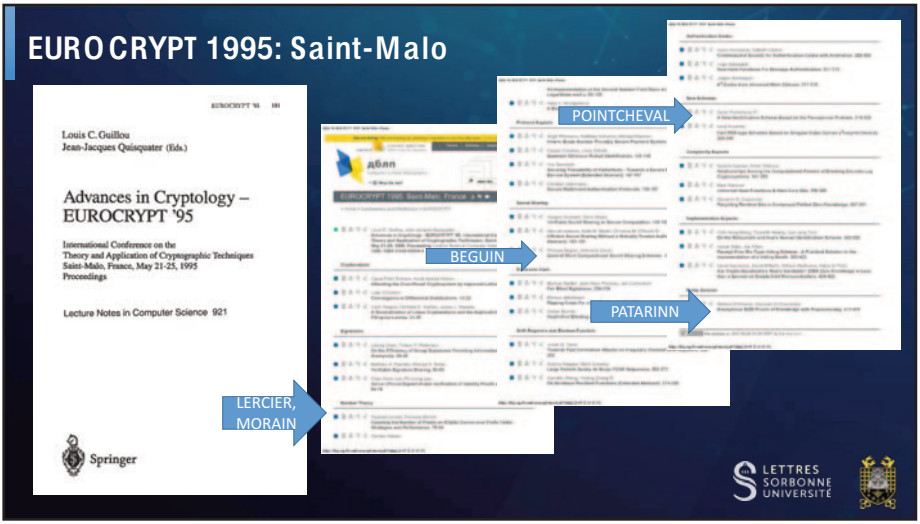
Il y avait aussi beaucoup de protocoles, le brevet GQ (Guillou Quisquater), également le GQ2. Celui-ci a d'ailleurs été utilisé par la société Novell pour de nombreuses applications, c'était dans les années 90 et suivantes. Nous avons également produit une définition et un nouvel algorithme pour expliquer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



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.

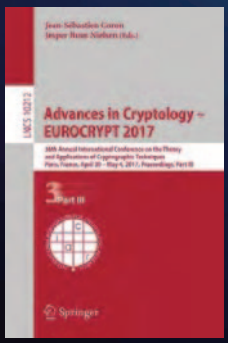


Mais le point principal de cette participation fut la dernière session. Il eut cinq présentations sur les cartes à puce. Ce n'était pas vraiment de la recherche, c'était plutôt une description d'idées et de produits. Mais la principale présentation, la dernière, fut celle donnée par Louis Guillou. C'était 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.



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 !

EUROCRYPT 2017: Paris



15 authors

LETTRES SORBONNE UNIVERSITÉ

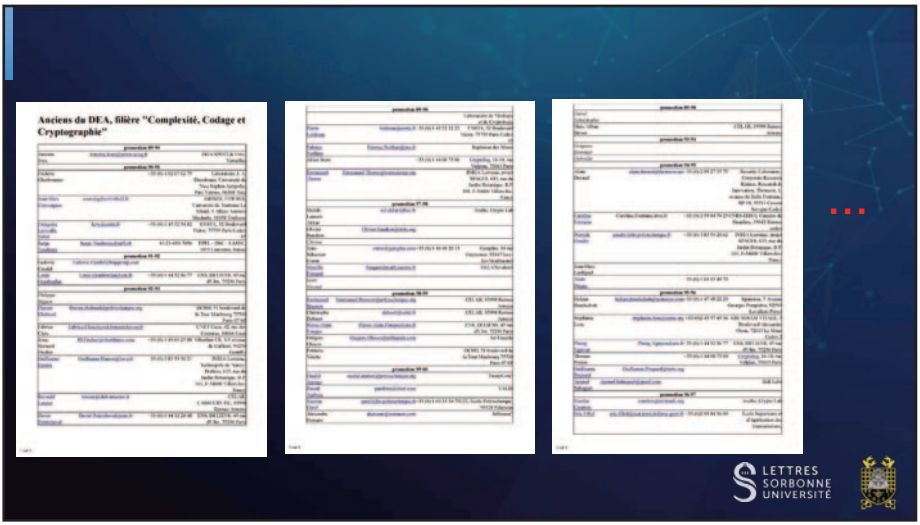
Enfin, la dernière fois qu'Eurocrypt s'est déroulé en France, à Paris, en 2017, il y avait 15 auteurs français. Donc ça augmente vraiment, ça augmente, ça augmente.

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.

LETTRES 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.

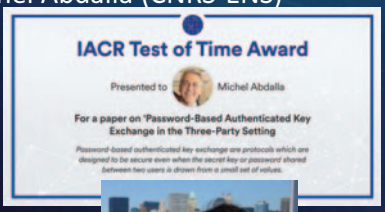


Vous pouvez voir ici la liste des inscrits pour chaque année. La première année, il n'y avait qu'une seule personne mais beaucoup plus par la suite. Toutes les personnes importantes jusqu'en 2010, vous pouvez dire qu'elles viennent principalement d'ici.

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

LETTRES SORBONNE UNIVERSITÉ

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.

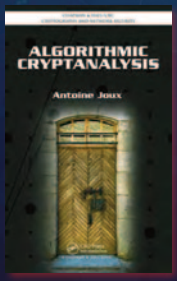
Jacques Stern (master of secrets)

LETTRES SORBONNE UNIVERSITÉ

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

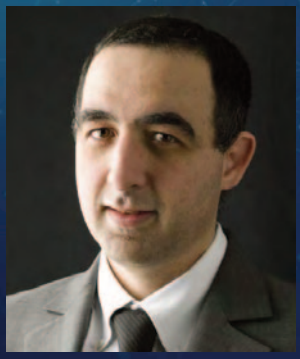


LETTRES SORBONNE UNIVERSITÉ

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.



LETTRES SORBONNE UNIVERSITÉ

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

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/

Multiple research, Multiple publications, New protocols ...

LETTRES SORBONNE UNIVERSITÉ

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.

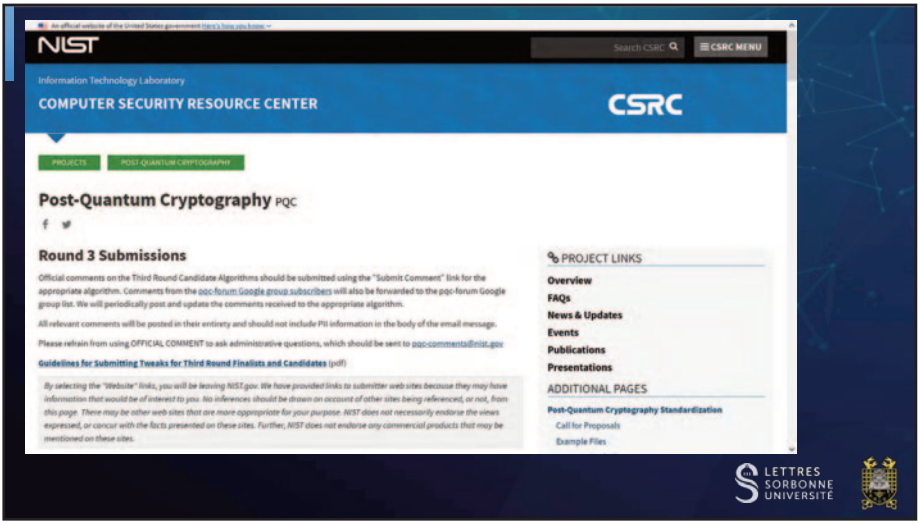
Post quantum Research

Normal Shakespeare:
TO BE OR NOT TO BE

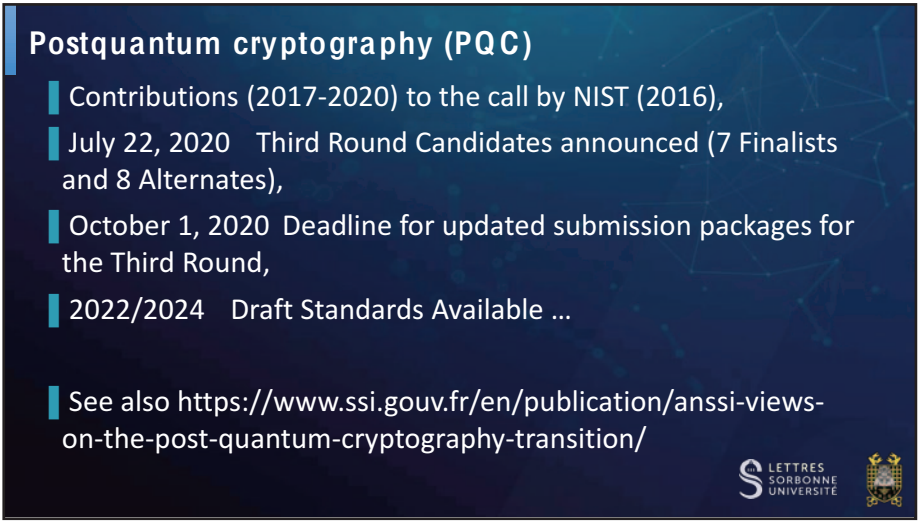
Quantum Shakespeare:
TO BE AND NOT TO BE

LETTRES SORBONNE UNIVERSITÉ

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.

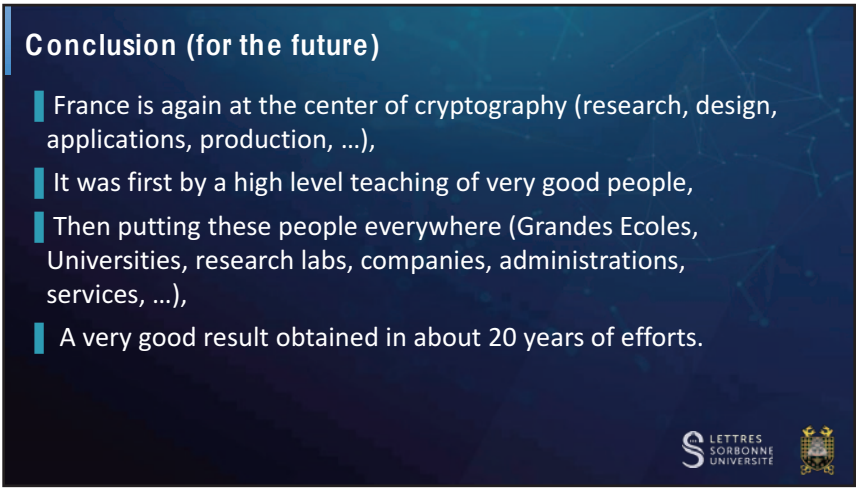


Suite à l'appel du NIST, Il y a eu plusieurs tours, on est aujourd'hui au tour numéro trois, et il y a eu beaucoup de soumissions. Du tour un au tour trois, on est passé de 55 à 7 soumissions retenues.



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.

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.



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.