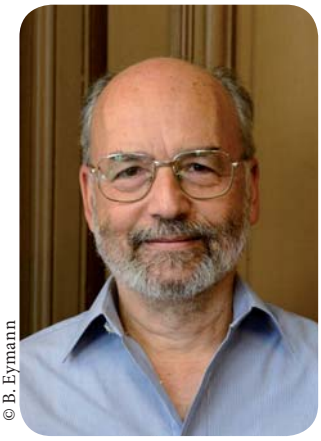
© B. Eymann

Adi Shamir

Né en 1952 à Tel Aviv, Israël
Professeur à l'Institut Weizmann, Israël

L'essor prodigieux de l'informatique ces dernières décennies, accompagné de la prolifération de documents électroniques immatériels, a rendu nécessaires de nouvelles formes de cryptographie (transactions bancaires, cartes de crédit, transactions Internet…). Les travaux d'Adi Shamir couvrent un large spectre, allant des questions fondamentales sur la complexité, aux questions extrêmement concrètes touchant à la sécurité et à la confidentialité des transactions. En 1976, il est un des inventeurs de l'algorithme RSA (Rivest, Shamir, Adleman) qui permet l'authentification de la signature d'un document électronique et est actuellement implanté sur la quasi-totalité des ordinateurs reliés à l'Internet. Au cours des dernières décennies, Adi Shamir travaille sur la génération de séquences pseudo-aléatoires, ce qui est la base de la cryptographie. Il évoque la possibilité de se passer des certificats en cryptographie asymétrique, en faisant en sorte que la clé publique soit tout simplement l'identité de son propriétaire. En 2005, il a introduit la méthode *Cache Attacks* qui exécute un processus d'attaque en parallèle de l'exécution du calcul cryptographique. En 2008, il introduit la méthode *Bug Attacks* qui exploite un bug de calcul dans une opération de base du processeur, comme le fameux bug de la division flottante dans le Pentium Pro d'Intel. Enfin, outre ses propres recherches, Adi Shamir a créé une véritable école ; ses étudiants dirigent aujourd'hui les départements d'informatique des trois principales universités d'Israël.

Born in 1952 in Tel Aviv, Israel
Professor, Weizmann Institute of Science, Israel

With the stupendous rise of computer science in recent decades, accompanied by the proliferation of electronic documents, new forms of cryptography have become of central importance (for banking transactions, credit cards, Internet transactions and so on). Adi Shamir's work spans a wide spectrum of issues, from fundamental questions on complexity to extremely tangible ones on the security and confidentiality of transactions. In 1976, he was one of the inventors of the RSA (Rivest, Shamir, Adleman) algorithm, which allows e-signature to be authenticated and is currently installed on practically all computers connected to the Internet. In the last decades, Adi Shamir has been working on pseudo-random sequence generation, which forms the basis of cryptography. He is considering the possibility of doing without certificates in asymmetric cryptography, by quite simply making sure that the public key is the identity of its owner. In 2005, he introduced the Cache Attacks *method, which executes an attack process in conjunction with a cryptographic computation. In 2008, he introduced the* Bug Attacks *method, which exploits a computational bug in a basic operation of the processor, such as the famous floating point bug affecting the Intel Pentium Pro. Finally, besides his own research, Adi Shamir has created an effective school, and his students now lead the computer science departments of the three main universities of Israel.*

CV

- 1973 : *Bachelor of arts* en Mathématiques, Université de Tel Aviv, Israël
- 1977 : Ph.D. en informatique, *Weizmann Institute of Sciences* (WIS), Israël
- 1977-1980 : Chercheur au *Massachussetts Institute of Technology*, Etats-Unis
- 1984-Présent : Professeur au Département d'informatique, *Weizmann Institute of Sciences* (WIS), Israël
- 2002 : Prix Turing (avec Ron Rivest et Len Adleman)
- 2003 : *Docteur Honoris Causa*, École Normale Supérieure, Paris, France
- 2008 : Prix Israël
- 2012 : Grande médaille de l'Académie des sciences, France

- *1973: Bachelor of arts in Mathematics, University of Tel Aviv, Israel*
- *1977: PhD Computer Science, Weizmann Institute of Science, Israel*
- *1977-1980: Researcher, Massachusetts Institute of Technology (MIT), United States*
- *1984-Present: Professor in the Department of Computer Science, Weizmann Institute of Science, Israel*
- *2002: Turing Award (with Ron Rivest and Len Adleman)*
- *2003: Doctor Honoris Causa,* École Normale Supérieure, *France*
- *2008: Israel Prize*
- *2012:* Grande médaille *of the Académie des sciences, France*