

Stanford en Californie (qui ont reçu le prix Turing 40 ans après, en 2015, pour leurs travaux), au moment de sa publication. Alors qu'à l'époque, seule la cryptographie à clé secrète – symétrique – était utilisée, les deux cryptologues y proposaient le concept de système à clé publique et montraient l'intérêt de l'arithmétique des grands nombres premiers pour cette approche. Je travaillais alors comme chercheur dans un laboratoire de Philips à Bruxelles dédié aux mathématiques appliquées et, fasciné, je demandai à mon patron la permission de me lancer dans la cryptomathématique. Il accepta et, à sept, nous commençâmes à explorer le domaine, avant même que le premier système à clé publique, l'algorithme de chiffrement RSA, des initiales de ses trois inventeurs, Ronald Rivest, Adi Shamir et Leonard Adleman, toujours utilisé aujourd'hui, soit publié (il fut annoncé en 1977 par Martin Gardner dans *Scientific American*).

En décembre 1979, Philips France prit contact avec nous pour nous demander de participer à un appel d'offres du groupement d'intérêt économique (GIE) Carte à mémoire, rassemblant alors la Direction générale des télécommunications et des

Trouver un code PIN en 1985

Étant donné la carte à puce, il suffisait d'essayer un premier chiffre du code PIN, de déterminer, avec un oscilloscope, la durée du calcul de vérification effectué par la carte et de stopper à temps l'alimentation de la puce afin d'éviter l'enregistrement d'une tentative erronée dans la mémoire de la carte. Vu l'implantation de l'époque, quand le chiffre était juste, le temps de calcul était moins long que quand il était faux. Par essais successifs, on déterminait ainsi le premier chiffre, puis chacun des suivants selon la même méthode.

banques françaises, appel d'offres qui visait à tester la viabilité technique et économique de la carte à puce dans la vie réelle. Deux concurrents, Schlumberger et Bull, relevaient le défi, et Philips France voulait aussi tenter sa chance. Or l'équipe en charge du projet avait le sentiment qu'il fallait mettre de la cryptographie dans la carte à puce, au moins pour l'authentification. D'où son appel, puisque nous étions devenus le laboratoire de Philips dédié à la cryptographie. Ainsi, en 1981, le GIE Carte à mémoire lança trois tests grandeur nature de la carte à puce, respectivement à Blois avec Bull, à Caen avec Philips et à Lyon avec Schlumberger, comptant chacun plusieurs centaines de terminaux et plusieurs dizaines de milliers de cartes à puce. Et en préparation de cette expérience, dès début 1980, nous eûmes des réunions pour ajouter des fonctions cryptographiques et des protocoles de sécurité à la carte à puce.

Seule l'expérience de Blois fut jugée convaincante, et la carte à puce de Bull fut développée par la suite. Néanmoins, les cartes à puce étaient encore loin d'une sécurisation correcte, pour une raison simple : si les protocoles de sécurité entraient bien dans la carte, les algorithmes de cryptographie étaient trop

L'invention de la carte à puce

La carte à puce est un morceau de plastique portant au moins un circuit intégré contenant de l'information. On peut donc faire remonter son aventure à 1958, année où Jack Kilby, de Texas Instruments, inventa le premier circuit intégré : il assembla plusieurs transistors sur un support de silicium, ce qui conduisit à la production de processeurs (Intel 4004 en 1969, puis 8008 en 1972) permettant de réaliser de véritables petits ordinateurs miniatures, sur une seule puce.

Cette miniaturisation poussa très tôt à imaginer des dispositifs portables pour traiter des paiements. Dès les années 1960, l'auteur de science-fiction René Barjavel décrivait dans son roman *La Nuit des temps* un système de paiement au moyen d'une « bague ». Et entre 1968 et 1972, plusieurs brevets ont été déposés dans ce sens au Japon, en Allemagne, en



Grande-Bretagne et aux États-Unis, décrivant des cartes plastiques munies de mémoires électroniques. La paternité de la carte à puce à mémoire est souvent attribuée au Français Roland Moreno, qui déposa en 1974 le brevet de la carte à mémoire avec l'aide de Jean Moulin. Mais l'ingénieur français Michel Ugon (*médaille*), alors chez Bull, est le véritable

père de la carte à puce dite intelligente. C'est lui qui inventa, en 1977, la carte intégrant aussi un microprocesseur, indispensable aux applications exigeant une capacité de calcul à des fins de sécurisation. C'est d'ailleurs Michel Ugon qui, en France, s'impliqua le plus, durant de nombreuses années, dans la sécurisation de l'ensemble de la filière Carte à puce.

En 1977 et 1978, Michel Ugon déposa les deux principaux brevets sur les cartes à microprocesseurs. En mars 1979, il fabriqua la première carte à microprocesseur (à deux puces) et, en octobre 1981, la première carte monopuce à microprocesseur, la carte CP8 de Bull, qui conférait une meilleure sécurité. Les premières commandes industrielles furent lancées, qu'il s'agisse de la télécarte à puce

ou de la carte bancaire. Toutefois, la cryptographie n'y était pas d'un très haut niveau, même si on y pensait. À une exception notable près, cependant : dans les années 1970, les travaux chez IBM sous la direction de Carl Meyer furent très tôt orientés vers l'utilisation de la cryptographie, et une version expérimentale de carte, très différente du modèle actuel, fut testée avec l'algorithme cryptographique Lucifer, ancêtre du DES, dans le cadre d'une expérience de transfert de données à Londres. Mais IBM ne poursuivit pas dans cette voie, sa banque sponsor n'ayant pas été convaincue et la technologie des cartes n'étant alors pas assez avancée. La carte à puce intelligente n'en était alors qu'à ses balbutiements...

– J.-J. Q. et J.-L. D.