quelqu'un trouverait forcément le code de sa carte. Cela n'avait rien à voir avec la sécurité. L'un de nous (J.-J. Quisquater) en a fait la remarque au directeur, qui ne l'a pas cru. Avec Louis Guillou, un des pionniers de la sécurisation de la carte à puce, nous avons donc imaginé une attaque afin de montrer que l'on pouvait réellement casser le code de la carte *(voir page 74)*. La boîte de Pandore était ouverte.

Nous n'allons pas raconter ici l'histoire de la carte à puce, qui demanderait bien un livre pour rendre justice à tous et à tous les essais, mais nous allons tenter de montrer comment la carte à puce est devenue à la fois un objet de confiance, grâce à l'introduction de la cryptographie, et la gardienne des clés secrètes, un ingrédient essentiel… de la cryptographie elle-même.

Un objet inviolable par nature, pensait-on

Lors de son apparition, la carte à puce semblait être, de par sa nature même, une enceinte à l'abri des investigations malveillantes et un obstacle à la fraude pour les applications essentiellement monétaires auxquelles on la destinait. Il est vrai que la barrière technologique que constituait un circuit électronique pour le commun des mortels était déjà bien au-delà des compétences nécessaires à la lecture et à la manipulation de la simple bande magnétique des cartes alors en usage. Aussi les premiers développements et brevets n'utilisaient-ils pas vraiment la cryptographie. Que ce soient les Gondas dans *La Nuit des temps* de René Barjavel (1968) – une civilisation disparue qui, pour ses paiements, connectait une clé à un ordinateur central –, les premiers brevets japonais, allemands ou américains, ou encore la « bague » à puce conçue par Roland Moreno en 1974, rien n'indiquait que la puce devait contenir de la cryptographie, bien que des éléments de sécurité fussent évoqués *(voir l'encadré page 74)*.

Tout naturellement, la carte bancaire fut la destination privilégiée de la carte à puce, la simple carte en relief et son « fer à repasser » ou la carte à bande magnétique apparaissant vite, du moins aux banques européennes, comme insuffisamment sûres. Néanmoins, c'est une application imprévue qui fit décoller l'industrialisation de masse de cette technologie : la télécarte, simple réservoir d'unités de communication, qui permit de résoudre la question épineuse des milliers de monnayeurs des cabines téléphoniques. Une autre application de moindre étendue, mais touchant une population influente, contribua aussi à la visibilité de la carte à puce : la télévision à péage. C'est d'ailleurs celle-ci qui, alors que je (J.-L. Desvignes) dirigeais le Service central de la sécurité des systèmes d'information (SCSSI, devenu aujourd'hui l'Agence nationale de la SSI ou ANSSI), me conduisit à me pencher sur la sécurisation de cette technologie et à alerter le gouvernement sur la nécessité de s'en occuper d'urgence.

En 1996, une chaîne de télévision britannique, BSkyB, avait été victime d'un piratage à grande échelle de la part d'une société irlandaise. Celle-ci commercialisait ouvertement de fausses cartes d'accès aux programmes à prix bradé, et les rustines successives imaginées pour contrer ce piratage ne résistaient pas au trésor de guerre rapidement constitué par les pirates. C'est cet exemple de développement d'une industrie mafieuse permis par l'absence d'une prise en compte sérieuse des questions de sécurité au départ du projet que j'utilisai à l'époque afin de convaincre le ministère de la Santé d'adopter une démarche sécuritaire pour ses propres cartes : la carte Vitale et la carte des professionnels de santé. Inutile de décrire les risques qu'aurait comportés la distribution de telles cartes duplicables et falsifiables à souhait.

L'usage public de la carte à puce n'était pas le seul enjeu. Dix ans plus tôt, alors que j'étais « Officier chiffre » à l'état-major des armées, je m'étais occupé de la gestion des clés des équipements de chiffrement, et celle-ci était alors loin d'être satisfaisante. Comme tout responsable de ce domaine à l'époque, j'avais en tête la trahison de Hans-Thilo Schmidt, cet employé du chiffre allemand qui, plusieurs années avant la Seconde Guerre mondiale, avait monnayé auprès du service de renseignement français la fourniture du manuel d'utilisation d'Enigma – la machine à chiffrer allemande dont les décryptements ont été conduits successivement par les Polonais aidés des Français, puis par les Britanniques,

Les rustines successives imaginées pour contrer ce piratage ne résistaient pas au trésor de guerre rapidement constitué

■ **LES AUTEURS**


Jean-Jacques QUISQUATER est professeur émérite de cryptologie à l'université catholique de Louvain, en Belgique.

Jean-Louis DESVIGNES, général, est président de l'Association des réservistes du chiffre et de la sécurité de l'information (ARCSI).

notamment le mathématicien Alan Turing – et de ses tableaux de clés, les paramètres de la machine qui permettaient de déchiffrer les messages. Ces renseignements avaient notablement facilité les travaux de cryptanalyse. Or jusqu'aux années 1990, les réseaux de chiffrement gouvernementaux tels que ceux de l'Alliance atlantique avaient peu évolué. Il s'agissait toujours de systèmes à clé secrète – ou systèmes symétriques (la même clé, privée, était utilisée pour chiffrer et déchiffrer) – dont l'initialisation (l'introduction de la même clé dans toutes les machines) était manuelle et permettait donc aux opérateurs d'y avoir accès physiquement.

Quelle que soit la rigueur du processus de sélection de ces opérateurs, il n'était pas exclu de recruter un individu susceptible de compromettre les éléments secrets qu'il manipulait. Certes, des efforts avaient été accomplis pour diminuer cette vulnérabilité en recourant à différentes astuces : des blocs de feuillets détachables journellement évitaient que la compromission des clés s'étale sur une période trop longue. Les techniques de grattage empruntées à certains jeux avaient aussi été envisagées. Sont ensuite apparus des conteneurs de bandes perforées impossibles à rembobiner après lecture (des sortes d'escargot), puis des injecteurs électroniques quelque peu blindés, simples mémoires dotées d'interfaces exotiques impossibles à lire pour un profane, mais d'un coût élevé.

Pour ma part, afin d'augmenter la sécurité des réseaux les plus étendus, j'avais paradoxalement commencé par allonger la cryptopériode de certaines clés pour diminuer le nombre d'exploitants amenés à les manipuler ! En passant de 24 heures à une semaine, je divisais par 5 ou 6 le risque de confier nos plus grands secrets à une brebis égarée.

C'est pourquoi, dès que la carte à puce est apparue, et notamment la carte Bull CP8 au milieu des années 1980, je cherchai à exploiter ses capacités pour initialiser à un coût modeste les nouveaux équipements de chiffrement. Au départ, la carte ne fut donc qu'un réservoir sécurisé de clés secrètes, comme dans le cas de l'équipement de cryptophonie gouvernemental DCS500 de Sagem *(voir la figure ci-contre en bas)*. Il fallut attendre la fin des années 1990 pour que la Défense utilise la carte à puce comme élément contenant les certificats de sécurité dans le cadre d'une « infrastructure de gestion de clés », c'est-à-dire recourant à des systèmes cryptologiques asymétriques. Ceux-ci, communément dits à clé publique (ces systèmes ont deux clés, une publique pour le chiffrement, une privée pour le déchiffrement), étaient apparus au milieu des années 1970, mais leur développement à grande échelle n'intervint qu'avec celui d'Internet.

© Wikimedia commons/ Papardelle

CES ANCÊTRES DE LA CARTE BANCAIRE *(en haut, la carte à deux puces de Philips, en bas, la carte CP8 de Bull)* portent l'élément clé qui rendit possible la sécurisation de la carte à puce : un processeur.

Toutefois, pour que de telles utilisations soient possibles et fiables, encore fallait-il que la carte à puce soit réellement un système sécurisé. Si l'on veut éviter certaines attaques, il faut associer à la puce une certaine puissance de calcul. Prenons le cas simple du mot de passe stocké sur la carte et utilisé pour avoir accès à une ressource, comme c'était le cas au début de la télévision à péage et du Minitel. Supposons une carte, associée à un utilisateur par un code PIN, qui tente de prouver son identité en communiquant ce mot de passe. Pour stocker ce mot de passe, il faut que la puce ait une mémoire inviolable et, par extension, qu'elle soit elle-même inviolable.

La cryptographie, une nécessité

En outre, si le mot de passe est transmis tel quel, en clair, il est facile à copier. Sa transmission ne doit donc pas se faire directement, mais en utilisant un détour, par exemple une question non prévue au sujet de ce mot de passe. En pratique, l'idée est d'utiliser des nombres aléatoires ou le mot de passe en coordination avec un algorithme cryptographique, par exemple une fonction de chiffrement ou un algorithme sans transfert de connaissance (visant à montrer qu'on connaît la solution d'un problème sans la révéler et, inversement, à contrôler la solution d'un problème sans en prendre connaissance).

Or cette idée qu'il fallait introduire une cryptographie forte dans la carte à puce faisait vite son chemin entre 1980 et 1984, notamment chez Bull avec Michel Ugon (inventeur de l'algorithme Telepass), au Centre commun d'études de télévision et télécommunications avec Louis Guillou (inventeur de l'algorithme GOC, générateur d'octets chiffrants) et chez Philips avec l'un de nous (J.-J. Quisquater). J'avais (J.-J. Quisquater) eu la chance, en 1976, de lire l'article *New directions in cryptography* de Whitfield Diffie et Martin Hellman, chercheurs à l'université

LE DCS500 DE SAGEM fut le premier équipement de cryptophonie numérique recourant à une carte à puce pour sa mise à la clé (l'introduction de la clé permettant de chiffrer et déchiffrer les messages). Il a été utilisé par les hautes autorités de l'État et les forces armées à partir des années 1990.

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 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

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.

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 *(médaillon)*, 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.