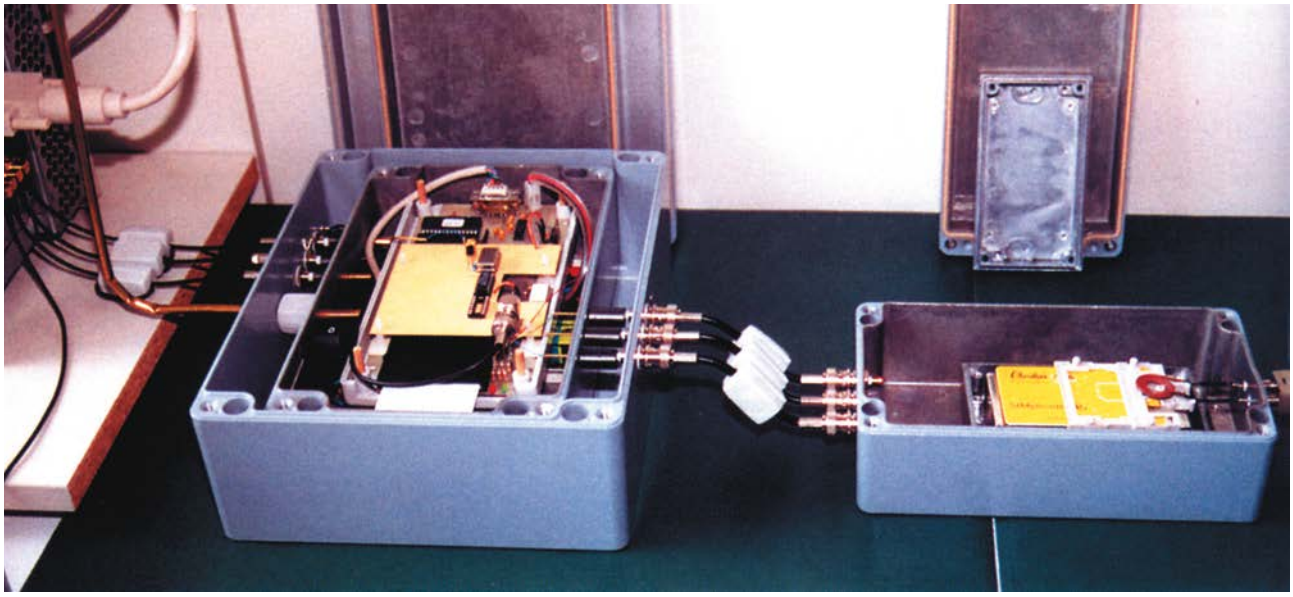

© EISS

AVEC UN DISPOSITIF MODESTE D'ANALYSE DES CARTES À PUCE branché sur un ordinateur, on mesure facilement des temps de calcul ou la consommation électrique, des informations très utiles pour retrouver la clé secrète utilisée dans le cryptosystème RSA des cartes.

cette sécurité manquante. Durant plusieurs mois, nous avons gagné octet par octet, déplaçant les permutations en usage dans le DES et les repliant. Nous avons ainsi réduit l'implantation à un total de 668 octets : chaque octet a coûté environ un jour de travail à une personne…

Le RSA sur une puce

Cependant, pour chacun de nous, le graal cryptographique de la carte à puce n'était pas le DES, mais le RSA. Cet algorithme fondé sur la détermination de deux grands nombres premiers à partir de leur produit était devenu le standard de la cryptographie. L'intégrer à la carte permettrait la signature, la distribution des clés, etc. Paul Barrett, de l'université d'Oxford, en Grande-Bretagne, inventa alors, en 1986, un nouvel algorithme pour le RSA, plus spécifiquement dédié à des processeurs pour traitement du signal. Nous sommes donc partis de cet algorithme. Après quelques tests sur une carte à puce, nous sommes arrivés à près de 100 secondes pour exécuter un algorithme RSA à 512 bits. Et à l'aide de quelques astuces (le stockage des multiples du module public et l'utilisation du théorème des restes chinois, qui permet de résoudre des équations d'arithmétique modulaire), nous avons fourni, toujours pour un module RSA de 512 bits, une signature en moins de 20 secondes. Un beau résultat, mais encore trop lent et trop gourmand en ressources pour être utilisé.

En 1989, Henri Molko, de Philips France et Allemagne, nous proposa un projet audacieux : créer un coprocesseur RSA en symbiose avec un processeur 80C51 pour réaliser une signature RSA sur 512 bits en moins d'une seconde (nous ferons 0,2 seconde). Sans moyens financiers, nous nous sommes lancés dans le projet CORSAIR *(Coprocessor RSA In a Rush)*. En cinq semaines, plusieurs versions du coprocesseur ont été imaginées à partir d'un nouvel algorithme que j'avais trouvé peu avant. Cela conduisit à une première accélération du RSA pour carte à puce par un facteur 500. Un premier prototype en silicium fut obtenu début 1990 : tout fonctionna, sauf l'écriture dans la mémoire morte effaçable de la carte (E^2PROM), « trop » optimisée en aval de notre projet *(voir la figure page 75)*.

Un nouvel algorithme, l'algorithme de Quisquater, avait donc été imaginé. Il se différenciait des autres par le fait que le coprocesseur était indépendant de la longueur de la clé et que l'exécution avait lieu à temps constant de bout en bout, car aucun test n'était effectué en cours de calcul, ce qui, *a priori*, évitait les attaques par mesure du temps d'exécution de l'algorithme.

Une course aux coprocesseurs de deuxième génération fut lancée parmi les fabricants : Fortress, Siemens, Infineon… et Philips. En 1995, Philips élabora un nouveau projet pour reprendre le dessus : FAME, qui nous conduisit à une nouvelle version 500 fois plus rapide que celle de CORSAIR. Son secret ? L'amélioration des circuits électroniques, avec l'ajout d'un multiplieur d'horloge qui augmentait de 16 fois sa fréquence, un multiplieur calculant le produit de nombres codés sur 32 bits (au lieu de 8), un bus (la ligne de transmission de l'information) plus large, une mémoire RAM à double accès très vaste et une meilleure chaîne de traitement au sein du coprocesseur. Ce coprocesseur est toujours utilisé dans des variantes optimisées. Au total, en dix ans, une accélération d'un facteur 250 000 a été obtenue entre la première version logicielle en 8 bits et celle de FAME.

Le développement des grandes applications de la carte à puce coïncida avec la volonté de plusieurs pays de définir une méthodologie pour évaluer la sécurité des systèmes informatiques. Les premiers, les Américains proposèrent à l'Otan, à travers l'*Orange Book*, les critères à respecter pour obtenir un niveau de sécurité donné. Ceux-ci apparaissant vite comme une arme de concurrence efficace pour imposer les produits américains, certains pays européens réagirent en proposant chacun un livre de couleur différente : vert pour les Allemands, jaune pour les Britanniques et… bleu-blanc-rouge pour les Français ! Finalement, la Commission européenne s'empara du sujet et ainsi naquirent les ITSEC (critères d'évaluation de la sécurité de la technologie de l'information) qui permirent aux pays européens de mettre en place leur schéma de certification. Notons que les ITSEC différaient de l'*Orange Book* : celui-ci vérifiait la présence de mécanismes

de sécurité, tandis que les ITSEC vérifiaient leur pertinence et leur efficacité.

Bientôt émergea l'idée de critères universels acceptables des deux côtés de l'Atlantique et même au-delà. C'est ainsi que naquirent les « Critères Communs » bientôt transformés en norme ISO, à la rédaction desquels la France prit une part déterminante, la présidence du groupe de travail lui étant revenue.

De fait, alors que les États-Unis et le Royaume-Uni se concentraient sur la certification de différents systèmes d'exploitation et dispositifs de sécurité tels les pare-feu, la France trouva dans la carte à puce un champ d'application privilégié. Son expertise dans ce domaine l'amena même à exercer une sorte de monopole. À ce titre, des firmes prestigieuses coréennes, japonaises et même américaines telle Motorola en vinrent à lui confier les évaluations de leurs produits. Cette grande compétence était le fait d'une petite équipe de chercheurs de France Télécom répartie entre Grenoble et Caen. Une dizaine de personnes qui avaient su, en collaboration avec le SCSSI, développer les méthodes d'investigation à la fois sur le matériel et sur le logiciel et automatiser la recherche de failles. Cette équipe fut ensuite transférée au sein du Laboratoire des technologies de l'information (LETI) du CEA.

Ce travail sur la sécurisation des composants de cartes à puce impliquait un effort considérable de la part des industriels se lançant dans le processus et parfois des changements substantiels dans l'organisation de la chaîne de production à l'intérieur même des salles blanches, pour lesquelles les investissements avaient été considérables. C'est ainsi qu'en 1999 à Tours, lors de l'opération de lancement de Moneo, ce porte-monnaie électronique qui malheureusement n'a pas eu le succès escompté, un PDG de la société, en recevant officiellement son certificat de sécurité, déclara que ce certificat lui avait coûté 20 % de logiciel et de dépenses supplémentaires, un dépassement de 30 % des délais, et 50 % de sueur et de stress en plus pour les premiers composants. Mais il se félicitait du gain en rapidité de développement et de mise au point obtenu ensuite.

Longtemps, la carte à puce ainsi sécurisée fut réputée comme le moyen de paiement le plus sûr, avec une fraude affichée de 0,03 %. Ce taux ne militait pas pour un renforcement de la sécurité. Ainsi la taille des clés, pourtant jugée bien trop faible par les experts, fut maintenue bien trop longtemps. Aussi, quand le GIE Carte bancaire fut confronté à l'affaire Humpich, un vent de panique souffla sur ce bel optimisme.

Sécurisation et législation

Un des problèmes rencontrés pour sécuriser la carte a été la législation française, car les moyens cryptologiques, classés dans la catégorie des armes de guerre, étaient soumis au régime défini par le décret de 1939. Ainsi, lors d'une réunion du Directoire de la cryptologie, vers 1985, le représentant du ministère de l'Industrie, en entrant à Matignon, s'excusa d'avoir pénétré dans ce lieu en portant une arme de deuxième catégorie : sa carte bancaire… Celle-ci contenait en effet un algorithme cryptographique qui interdisait sa possession. Un aménagement au décret fut donc adopté pour ne pas pénaliser cette technologie dont on commençait à percevoir le potentiel… Arme de guerre ou non ? La question refait surface alors que la carte est utilisée pour des moyens de télécommunication ou de diffusion tels que la télévision à péage ou la téléphonie mobile.

L'affaire Humpich

En 1997, Serge Humpich, ingénieur autodidacte de la puce, réussit à casser la signature RSA, alors statique et stockée dans la carte, notamment à l'aide du processus décrit page 74. Il réalisa ensuite des cartes trompant les terminaux de la RATP (les yescards) qui n'exigeaient pas une identification forte, car traitant des transactions d'un faible montant. Il tenta de monnayer son savoir-faire, mais se fit interpeller dans le cadre de la loi Godfrain. Son procès en 2000 suscita quelque effroi, car lui et ses soutiens étaient en mesure de compromettre la clé RSA en la diffusant.

En fait, les fraudes d'origine technologique sont généralement restées d'assez bas niveau, l'essentiel des escroqueries étant à imputer à une incroyable naïveté des victimes et à l'habileté des escrocs en matière d'ingénierie sociale. Pourtant, une vraie vulnérabilité est apparue lorsque les cartes ont été dotées d'une capacité « sans contact ». Il s'est en effet avéré que cette technologie était piratable à courte distance et entraînait le risque d'exfiltration d'informations hautement sensibles. La Commission nationale de l'informatique et des libertés (CNIL) s'en est émue et impose désormais aux banques de désactiver cette fonctionnalité sur demande du porteur ou de lui fournir un étui « cage de Faraday » évitant la sollicitation électromagnétique non désirée.

Mais un risque bien plus inquiétant se profile. Avec ou sans contact, la carte à puce est un instrument de sécurité en elle-même. Or on entend beaucoup qu'elle pourrait disparaître en raison des offres nouvelles des géants de l'Internet et de la téléphonie. Que le téléphone utilise une puce SIM ayant de nouvelles capacités ou qu'il remplisse lui-même ces nouvelles fonctions, il n'y aurait alors plus de séparation entre l'outil de communication et le moyen d'identification et d'authentification – la puce. Une situation qui devrait faire le bonheur des pirates… et offrir aux géants du Web Google, Apple, Facebook et Amazon la mainmise sur un des rares domaines pas encore complètement sous la domination américaine. ■

BIBLIOGRAPHIE

Carte à puce et cryptographie : je t'aime moi non plus, conférence de J.-L. Desvignes et J.-J. Quisquater au Musée des arts et métiers du Cnam, 2015 : http://bit.ly/29mT1Lk

S. Bouzefrane et P. Paradinas, **Les Cartes à puce**, Hermès Science Publications, 2013.

C. Tavernier, **Les Cartes à puce. Théorie et mise en œuvre**, 2e édition, Dunod, 2011.

W. Rankl et W. Effing, **Smart Card Handbook**, 4e édition, Wiley, 2010.

M. Éluard et S. Lelievre, **YesCard, entre mythe et réalité ou un aperçu du système bancaire français**, MISC, hors-série n° 002, novembre 2008.