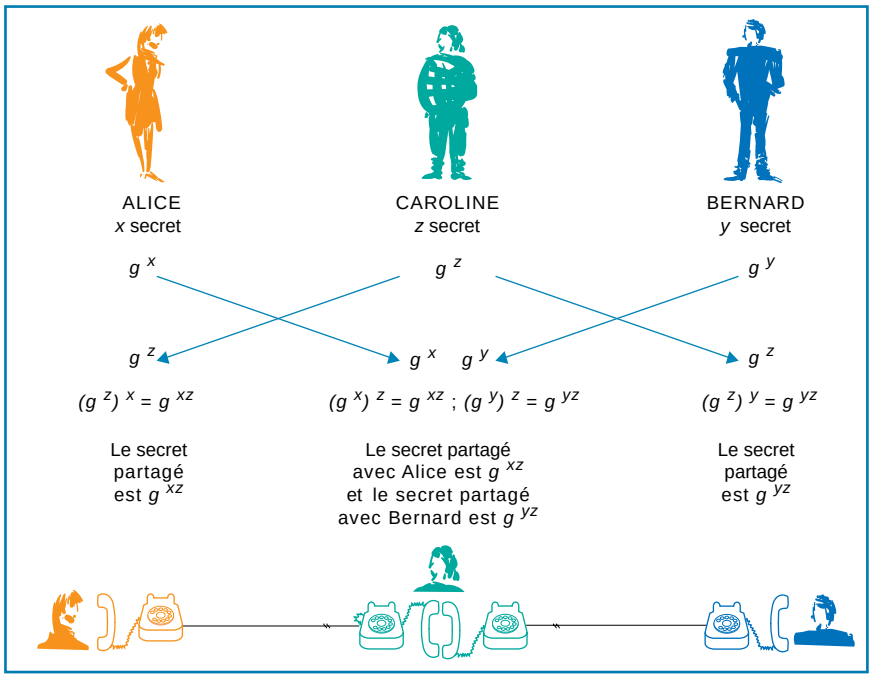


4. LES SYSTÈMES CRYPTOGRAPHIQUES À CLÉ PUBLIQUE sont vulnérables. Interceptant les transmissions entre Alice et Bernard, l'espionne Caroline dupe Bernard en utilisant son propre g^z à la place du g^x d'Alice et trompe Alice en utilisant g^z à la place du g^y de Bernard *(voir l'encadré de la page 40)*. Elle déchiffre et rechiffre à leur insu les messages qu'ils échangent.

que n'autorisent pas les systèmes de chiffrement classiques. Le procédé CAST-256 est une extension des premières architectures CAST à une clé de 256 bits et à des blocs de 128 bits. Le système *Twofish* est mathématiquement plus rigoureux que *Blowfish*, son prédécesseur. La conception de *Serpent* est fondée sur une structure parallèle inhabituelle, qui le rend aussi rapide que DES et qui permet d'engendrer très rapidement des clés autorisant ainsi son utilisation en tant que fonction de hachage. Au département de mathématiques et d'informatique de l'École normale supérieure, l'équipe de Serge Vaudenay a mis au point le système DFC (*Decorrelated Fast Cipher*, soit «codage décorrélé rapide»), très rapide, et dont on peut prouver la sûreté face à certains types d'attaques.

Déchiffrer le futur

Quelle que soit la proposition sélectionnée, AES avantagera les utilisateurs. Aujourd'hui, les meilleurs systèmes de cryptographie sont supérieurs aux meilleures méthodes de cryptanalyse connues. Bien sûr, la cryptanalyse viendra à bout des nouveaux systèmes, mais de nombreux informaticiens estiment que l'écart entre les méthodes de chiffrement et les méthodes de «cassage» se creusera progressivement.

Je partage cette opinion : la cryptographie civile a grandi dans les universités et dans les entreprises privées, et elle a rattrapé la cryptographie militaire. D'ailleurs, les militaires américains ont rendu public leur système de chiffrement *Skipjack*, qu'ils avaient mis au point en secret. Selon une étude d'Eli Biham, cet algorithme serait moins sûr que les meilleurs algorithmes universitaires. Comme le réseau Internet, la cryptographie est sortie du giron militaire. Souhaitons-lui une croissance aussi remarquable!

Philip ZIMMERMANN est l'auteur du programme de chiffrement PGP (*Pretty Good Privacy*). Il travaille pour la Société *Network Associates*.

Bruce SCHNEIER, *Cryptographie appliquée*, Vuibert, 1996.

Doug STINTON, *Cryptographie : théorie et pratique*, Vuibert, 1996.

G. DUBERTRET, *Initiation à la cryptographie*, Vuibert, 1998.

Paiements sur l'Internet

OCTAVIAN URECHE • RÉJEAN PLAMONDON

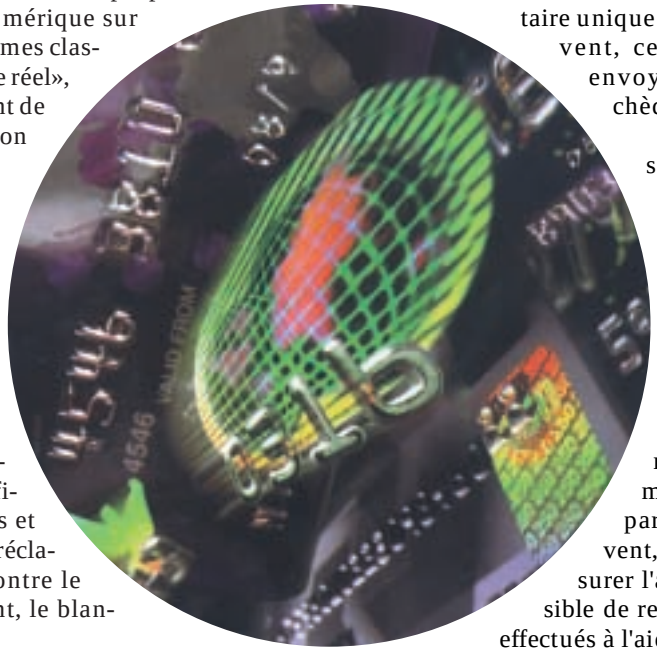
L'essor du commerce électronique nécessite de nouveaux moyens de paiement numériques, adaptés au monde virtuel de l'Internet.

La croissance du commerce sur le réseau Internet est phénoménale : en 1997, le total des achats a atteint 80 milliards de francs dans le monde et, en 2002, ce chiffre atteindrait près de 3 000 milliards de francs. Les communications étant aujourd'hui faciles et rapides, les informaticiens cherchent à faciliter les transactions monétaires.

Ce type de communications nécessite un niveau minimal de confiance, tant de la part des consommateurs que de la part des vendeurs : les acheteurs veulent que leurs cartes de crédit, chèques ou portefeuilles virtuels ne puissent tomber dans les mains d'un tiers malintentionné, et que les biens et services achetés «en ligne» soient livrés ; les fournisseurs de biens et services veulent la garantie qu'ils recevront les fonds qui correspondent aux marchandises vendues. Aujourd'hui, la sécurisation du paiement est essentiellement assurée grâce au chiffrement : les données transactionnelles sont chiffrées, et leur validité peut être vérifiée à l'aide des signatures numériques.

Outre ces méthodes cryptographiques, les transactions sécurisées requièrent des protocoles de transaction qui dépendent de la représentation monétaire : cartes de crédit, chèques ou argent virtuel. Si la plupart des systèmes de paiement numérique sur l'Internet s'inspirent des systèmes classiques de paiement du «monde réel», plusieurs systèmes introduisent de nouveaux moyens de transaction dans le monde virtuel.

Après avoir examiné et évalué divers systèmes électroniques de paiement sur l'Internet, nous décrirons un nouvel instrument transactionnel, nommé *TRANZIX*, qui généralise les concepts et les notions utilisées habituellement dans ces systèmes, et qui offre un compromis raisonnable entre le besoin de confidentialité des consommateurs et le besoin de transparence que réclament les États pour lutter contre le crime organisé et, notamment, le blanchiment d'argent.



Concrètement, deux aspects contribuent à cette solution de compromis : les informations de trace, qui permettent de retracer le parcours d'une transaction en général et d'un billet en particulier, et les moyens cryptographiques, qui offrent une réelle confidentialité aux usagers, en dissimulant ces traces, de façon à les rendre invisibles pour tout accès non autorisé.

Représentation monétaire

Selon le modèle transactionnel, on trouve plusieurs représentations monétaires. Ainsi, le paiement peut se faire à l'aide de cartes de crédit virtuelles : le numéro d'une carte de crédit «réelle» est chiffré, puis envoyé avec un certificat numérique *(voir l'encadré de la page 42)*. Les protocoles fondés sur les cartes de crédit se regroupent autour d'un nouveau standard, nommé SET (*Secure Electronic Transactions*, soit «transactions électroniques sécurisées») soutenu par des sociétés telles que *Visa* et *MasterCard*.

L'équivalent virtuel du chèque est le chèque électronique. Les informations à transmettre comprennent alors un numéro de compte bancaire, un destinataire unique et une date d'expiration. Souvent, ces chèques sont imprimés, envoyés ou encaissés comme des chèques réels.

Une nouvelle forme de représentation monétaire reproduit fidèlement l'argent comptant : c'est l'argent virtuel. L'argent virtuel est constitué de fichiers binaires qui contiennent plusieurs renseignements, parmi lesquels une valeur nominale, un numéro de série, et une ou plusieurs signatures numériques. Comme dans le monde réel, ce type de représentation monétaire a la particularité d'appartenir «au porteur» et, très souvent, on y inclut des moyens d'assurer l'anonymat ; il est donc impossible de retracer les transferts des fonds effectués à l'aide de l'argent virtuel.

Ces représentations monétaires sont échangées à l'aide de systèmes transactionnels qui doivent empêcher l'accès non autorisé aux données – et aux fonds – privées des utilisateurs. Le chiffrement et le contrôle d'accès, tel le mot de passe, protègent relativement bien contre ce type d'intrusion. En revanche, le problème des «dépenses multiples» est plus ardu : comment s'assure-t-on qu'un billet virtuel n'a pas été copié plusieurs fois et dépensé auprès de différents vendeurs de façon illicite? Aujourd'hui, on effectue le contrôle en utilisant le numéro de série du billet et des coordonnées des utilisateurs des billets, qui sont toujours inclus dans les protocoles de paiement au moyen d'argent virtuel. L'émetteur du billet dissuade ainsi les fraudeurs putatifs, qui peuvent être retrouvés. Toutefois, dans les systèmes classiques, aucune donnée n'est fournie sur l'historique du billet ou sur sa date d'expiration.

Récemment, des informaticiens de la Société *Digital* ont introduit le concept de micropaiement. Ce système, nommé *MilliCent*, utilise des «coupons virtuels» qui abaissent le montant minimal d'une transaction. Tout comme les coupons de réduction dans le «monde réel», ces coupons ne sont utilisables qu'auprès de leur magasin émetteur. Des paiements de quelques centimes sont ainsi possibles. Ce type de transactions ouvre des nouvelles possibilités : les entreprises pourraient faire payer la recherche d'une information, comme une cotation boursière par exemple.

La transaction

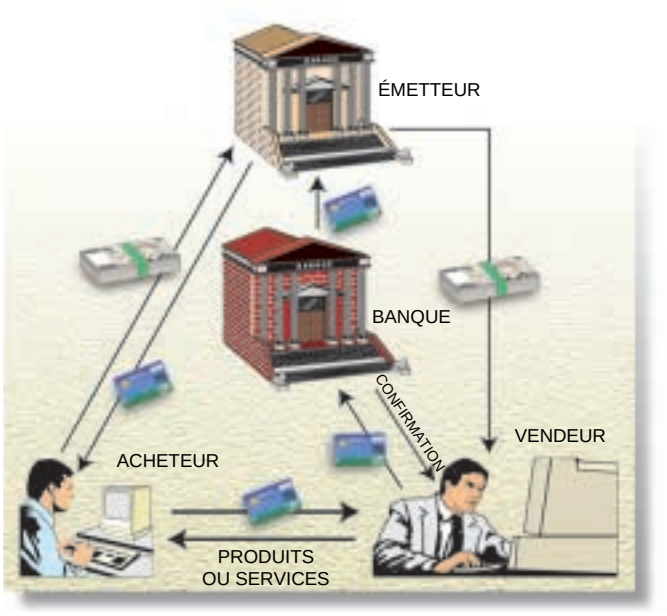
Comment s'effectue une transaction numérique? Plusieurs acteurs y participent : un acheteur, qui désire échanger son argent contre des biens ou des services offerts en ligne ; le vendeur, qui offre ces biens ou ces services ; un intermédiaire, ou courtier virtuel, qui traite les transactions ; une banque, qui gère les comptes des clients et acquitte les transactions ; enfin un émetteur – généralement une banque –, qui émet la représentation monétaire utilisée dans le système, qui protège la qualité de cette représentation monétaire, et, ainsi, les valeurs qu'elle représente.

Par exemple, dans le monde réel, la représentation monétaire émise par la *Deutsche Bundesbank* est le Deutsche Mark qui a, selon les analystes financiers, une qualité supérieure à celle du rouble russe ou du peso chilien ; cette qualité supérieure résulte non seulement d'une très bonne qualité d'impression et de l'utilisation d'un bon papier, mais surtout du fait que cette représentation monétaire est émise par une institution qui inspire confiance.

De façon générale, un client envoie la représentation monétaire chez un vendeur, qui la vérifie en l'envoyant à l'intermédiaire ou directement à la banque. Selon le résultat de cette vérification, le vendeur reçoit – le cas échéant – une confirmation et envoie alors la marchandise au client. L'acheteur achète cette représentation monétaire auprès de l'émetteur, qui peut aussi rembourser le vendeur *(voir la figure 1)*.

L'évaluation du paiement

Au vu du nombre croissant de systèmes numériques de paiement, leur évaluation est primordiale pour tous ceux qui veulent déployer et utiliser de tels systèmes transactionnels. Pour ce faire, nous avons proposé une taxonomie des systèmes de paiement numérique sur l'Internet.



1. LES SYSTÈMES DE PAIEMENT CLASSIQUES nécessitent en général quatre acteurs. L'acheteur achète des biens et des services à l'aide d'une représentation monétaire (carte de crédit virtuelle, chèque électronique, argent virtuel, etc.). Le vendeur est crédité de la somme correspondante par l'émetteur de la représentation monétaire, après vérification par une banque ou par un intermédiaire. La sécurité de la transaction dépend de la représentation monétaire et du type de vérification.

Dans notre classification, les systèmes se divisent en deux grandes catégories, suivant que le système requiert ou non une adhésion de l'acheteur. Chacune des deux catégories contient plusieurs classes selon le modèle transactionnel et le niveau de protection – par exemple, le modèle sans protection, le modèle «débit-crédit», le modèle comptant, etc. Chaque classe contient un ou plusieurs groupes de systèmes de paiement reflétant la technique de transfert de fonds employée – par exemple, les systèmes fondés sur les mots de passe, les chèques électroniques, la facturation et les cartes de crédit, l'argent virtuel, etc.

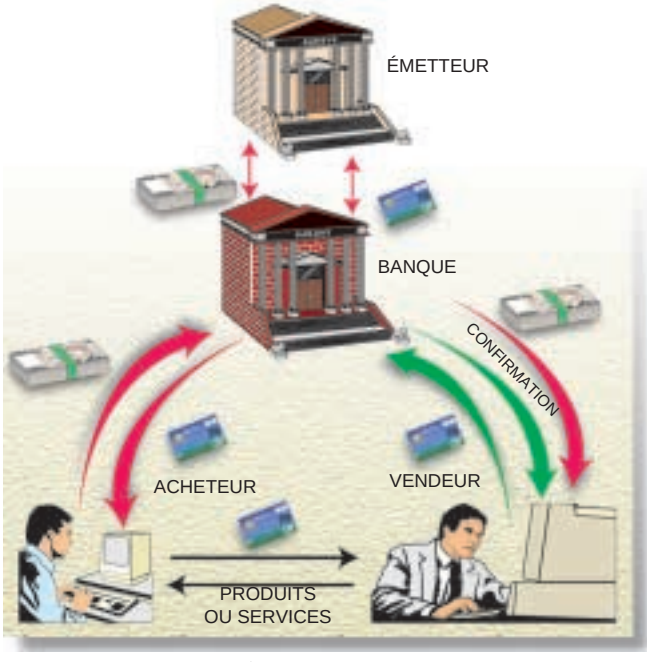
Comment évaluer les systèmes transactionnels? À l'aide de leurs caractéristiques. On distingue les caractéristiques internes, liées au fonctionnement intrinsèque du système, et les caractéristiques externes. Les caractéristiques internes sont la sécurité, la représentation monétaire, la pérennité de cette représentation, sa «granularité» (la plus petite somme que l'on peut échanger, surtout importante pour les micropaiements), la configuration du système et le niveau d'anonymat. Dans les caractéristiques externes, on inclut des critères tels que le délai d'encaissement, le mode d'échange des fonds ou la convertibilité de la représentation monétaire.

Aujourd'hui, le protocole de sécurisation des communications transactionnelles le plus répandu est le protocole SSL (*Secure Socket Layer*, soit «couche de base sécurisée»). Introduit en 1994 par la Société *Netscape Communications*, ce protocole est intégré dans les navigateurs les plus courants, tels *Netscape Navigator* et *Microsoft Internet Explorer*. Ce système est relativement sûr : en Europe, le protocole SSL chiffre les données avec des clés de 40 bits. Autrement dit, pour percer le code de chiffrement, il faudrait trouver les facteurs premiers d'un nombre de 40 bits (ou 10 chiffres), ce qui prendrait des jours à un ordinateur de bureau.

Pour les utilisateurs équipés de ces navigateurs, le chiffrement est transparent : lorsqu'un utilisateur entre son numéro de carte bancaire sur un site sécurisé (reconnaissable à l'adresse Web, où *http* est changé en *https*), celui-ci est chiffré automatiquement par l'ordinateur de l'utilisateur, puis il transite sur le réseau et il est décrypté par la machine du serveur. Cette ergonomie explique la percée de ce système, mais l'utilisation des cartes de crédit réelles restreint son usage à ceux qui en détiennent. De surcroît, avec les cartes de crédit, seuls les montants supérieurs à 50 francs sont économiquement viables, de sorte que ce système n'est pas intéressant pour l'achat d'articles de journaux en ligne, par exemple.

Autres restrictions de ce système transactionnel, il n'offre pas la non-répudiation (un usager pourrait prétendre ne pas être celui qui a fait la commande), et seule la communication est protégée : l'accès aux informations transactionnelles – notamment aux numéros des cartes de crédit utilisées – étant accessible aux vendeurs et aux intermédiaires, le niveau de sécurité de ce système est considéré comme moyen. Notons cependant que l'achat dans une boutique à l'aide d'une carte de crédit possède un niveau de sécurité analogue : la facturette où figure votre numéro de carte et sa date d'expiration est également accessible au vendeur.

Le système de paiement proposé par la Société *CyberCash* corrige certaines faiblesses du protocole SSL par l'ajout d'un «porte-monnaie électronique». De cette manière, *CyberCash* assure l'authentification des intervenants et un niveau raisonnable de non-répudiation des transactions, aspect totalement absent de SSL, qui n'est qu'un protocole cryptographique utilisé pour sécuriser les communications. La solution française *Klebox* possède des caractéristiques analogues.



2. AVANT UN PAIEMENT À L'AIDE DE *TRANZIX*, l'acheteur achète de l'argent numérique. L'acheteur clique sur un lien dans un magasin virtuel. Le portefeuille virtuel du vendeur contacte alors celui de l'acheteur en lui envoyant une requête de paiement pour la marchandise demandée. Lorsque le paiement est approuvé par l'acheteur, le vendeur reçoit un ou plusieurs billets numériques qu'il peut déposer immédiatement à la banque afin de vérifier leur validité, prévenant ainsi toute tentative de dépenses multiples. Le vendeur peut faire les vérifications hors ligne *(les flèches vertes représentent des transactions qui se font en ligne ou hors ligne ; les flèches rouges représentent des transactions hors ligne et les flèches noires des transactions en ligne)*.

Les cartes à puce

Les cartes à puce sont bien connues en Europe depuis près de 20 ans. Utilisées principalement comme cartes bancaires et téléphoniques, elles trouvent une nouvelle utilisation comme moyen ergonomique de paiement sur l'Internet. La Société britannique *Mondex* va permettre l'utilisation sur l'Internet de sa carte de paiement : à l'aide de lecteurs spécifiques branchés sur un port de communication d'un ordinateur, deux cartes *Mondex* effectueront des transactions sécuritaires. Le niveau de sécurité de ce système est élevé. La disponibilité, l'intégrité, la confidentialité et l'authentification sont assurées par des techniques cryptographiques. Seul le critère de non-répudiation n'est pas respecté, car un usager pourrait prétendre ne pas être celui qui a effectué la commande. Si les projets pilotes sont des succès, cette méthode sera généralisée à des transactions à l'aide de cartes à puce classiques.

Un niveau de sécurité encore supérieur a été mis au point par la Société hollandaise *DigiCash*. Le système, nommé *eCash*, utilise le concept d'argent électronique pour le paiement sur l'Internet. Il s'agit de pièces de monnaie virtuelles que l'on achète avec de l'argent réel (moyennant un transfert bancaire par exemple) et que l'on échange à chaque achat contre des produits et des services. Une méthode de chiffrement asymétrique assure la disponibilité et la confidentialité de l'information, et un système de signatures numériques assure l'intégrité de l'information, l'authentification des intervenants et la non-répudiation des transactions. De surcroît, le système permet des paiements anonymes grâce au concept de la signature aveugle : le numéro de série d'une pièce électronique est «caché» avant que la banque ne le signe, à l'aide d'un «facteur d'aveuglement» avec lequel ce numéro sera multiplié arithmétiquement.

Pour les micropaiements, même si plusieurs systèmes ont été proposés récemment, seul *MilliCent*, mis au point par la Société *Digital*, a dépassé la phase de recherche. Aujourd'hui en phase de tests, il permet le paiement de montants de quelques centimes à l'aide de coupons émis par chaque vendeur. Les coupons sont achetés et échangés auprès de courtiers virtuels.

Transactions généralisées

En analysant tous ces systèmes, nous avons déterminé les besoins à combler. Nous avons alors proposé un nouveau système transactionnel qui autorise le transport de valeurs numériques sans restrictions sur leur nature intrinsèque.

Bien qu'ils varient par la manière dont ils effectuent une transaction, tous les systèmes actuels ne font qu'une seule opération : un paiement électronique. Pour étendre cette fonction, nous avons mis au point le système *TRANZIX*, qui ouvre la porte à toute autre transaction, tels le transport, le transfert ou l'échange de valeurs. La notion de valeur généralise le concept de paiement.

Est-ce risqué d'acheter en ligne ?

Est-il plus risqué d'acheter sur l'Internet que de faire un achat par Minitel ou par téléphone ? Lorsque l'on achète sur l'Internet, le site propose en général plusieurs options.

Si le site n'est pas sécurisé (le navigateur prévient l'internaute lorsqu'il passe sur un site sécurisé), on vous proposera le plus souvent d'imprimer le bon de commande et de l'envoyer par fax ou par la poste, ce qui revient à un achat par correspondance, dont on ne discutera pas le sécurité.

Parfois, on vous proposera d'entrer votre numéro de carte de crédit en clair. Évitez de le faire, car même si, à l'instar du téléphone, tout le monde n'est pas sur écoute, il existe de logiciels conçus pour enregistrer les messages qui transitent sur le réseau et qui repèrent les suites de 16 chiffres, tels les numéros de carte de crédit. Ainsi, on a saisi des listes de millions de numéros de cartes de crédit chez des pirates américains.

Lorsque le site est sécurisé, le chiffrement dépend du lieu de la boutique et de l'endroit où vous êtes. S'il s'agit d'une boutique américaine, telle la librairie en ligne Amazon.com, la sécurisation théorique est SSL 128 bits. Toutefois, si vous êtes en France, le navigateur que vous utilisez sera bridé en 40 bits, le temps que les navigateurs acceptant plus apparaissent, ou en 56 bits, car, jusqu'à présent, le gouvernement américain refusait l'exportation de logiciels de cryptographie avec une clé secrète plus longue que 56 bits. Si la boutique est en France, vous aurez vraisemblablement affaire à un chiffrement SSL 40 bits.

Le chiffrement SSL avec une clé de 40 bits est-il sûr ? En juillet 1994, un informaticien lança un défi : pouvait-on facilement percer un message chiffré par ce système. Un informaticien français, Damien Doligez, de l'Institut national de recherche en informatique et automatique (INRIA), explora toutes les clés possibles et décrypta le message après huit jours de calculs sur différents ordinateurs dont il disposait, dont des machines parallèles. Aujourd'hui, la vitesse de calcul des ordinateurs a considérablement cru et on obtiendrait le même résultat avec des ordinateurs à base de *Pentium* (PC) ou de *PowerPc* (Mac), facilement disponibles. Cela signifie-t-il qu'il faut avoir peur de mettre son numéro de carte de crédit en ligne ? Le risque est faible, car quel pirate passerait des jours à décrypter un message pour obtenir un numéro de carte de crédit alors que des facturettes de cartes de crédit traînent dans les magasins ?

Quand des systèmes de cryptographie avec des clés secrètes de 128 bits seront disponibles en France et en Europe, ce risque minime n'existera plus : même avec les ordinateurs les plus puissants au monde, des messages chiffrés à l'aide de systèmes tels que PGP, nécessiteraient des années pour être percés.

Ainsi, pour *TRANZIX*, la notion de valeur représente tout objet virtuel ayant une valeur non intrinsèque quelconque, donc tout document numérique valant quelque chose pour quelqu'un. Ces documents incluent les billets virtuels, les certificats numériques, les attestations électroniques (diplômes d'études, preuves d'achat ou de vente, etc.), les moyens d'identification (carte santé, permis de conduire, passeport, etc.)...

TRANZIX généralise non seulement la notion de valeur, mais aussi l'opération de paiement. Ainsi, une valeur peut être transportée du lieu *A* au lieu *B* sans que cette valeur change de possesseur. Elle peut être transférée de *B* à *C*, non seulement en changeant d'endroit – par transport –, mais en changeant aussi de possesseur. Enfin, elle peut être échangée, lors d'une même transaction, contre d'autres valeurs ; la notion d'échange implique donc deux transferts, lors d'une même transaction. Par exemple, *TRANZIX* permet à un usager de transporter une autorisation électronique de chez lui à son bureau, de transférer cette autorisation à son employé afin d'ouvrir une porte ou d'accéder à une imprimante.

Le système utilise des billets numériques personnalisés à l'aide de signatures manuscrites des clients. Un prototype mis au point par notre laboratoire a été utilisé pour des microfacturations. Ce prototype permet de facturer l'utilisation des ressources physiques sur un réseau local (notamment l'impression des documents à l'aide de jetons numériques distribués de manière centralisée) et de facturer l'accès à des ressources virtuelles sur l'Internet (pour l'achat d'informations contenues dans des pages Web, par exemple, à l'aide de billets virtuels prépayés).

Le système assure un niveau de sécurité très élevé, obtenu grâce à un chiffrement asymétrique (deux clés de chiffrement complémentaires sont utilisées ; voir *Cryptographie et réseau*, page 38). De surcroît, la granularité est réglable. C'est une solution exclusivement logicielle, où les utilisateurs peuvent acheter ou vendre en ligne ou hors ligne à l'aide d'un même portefeuille virtuel.

En pratique, comment s'effectue une transaction ? Après avoir acheté des billets numériques, l'acheteur active son portefeuille virtuel en suivant un lien hypertexte payant dans un magasin virtuel. Le portefeuille virtuel du vendeur contacte alors celui de l'acheteur en lui envoyant une requête de paiement pour la marchandise demandée *(voir la figure 2)*. Une fois le paiement approuvé par l'acheteur, un ou plusieurs billets numériques sont envoyés au vendeur, qui peut les déposer immédiatement à la banque afin de vérifier leur validité, prévenant ainsi toute tentative de dépenses multiples.

Le vendeur peut aussi choisir d'effectuer des transactions hors ligne, afin d'augmenter la vitesse de traitement pour les microtransactions, par exemple ; les billets sont alors déposés par lots à la banque à la fin de la journée ou de la semaine. De cette manière, en réduisant les coûts de traitement des transactions, tant pour les vendeurs que pour les banques, *TRANZIX* rend économiquement viables les microtransactions.

Tout comme dans le monde réel, où plusieurs systèmes de paiement coexistent, plusieurs moyens de paiement numérique seront présents dans le portefeuille virtuel du consommateur de demain. En définitive, les consommateurs décideront quels moyens transactionnels répondent le mieux à leurs besoins spécifiques et quels types de systèmes particuliers survivront dans l'économie virtuelle du futur.

Octavian URECHE prépare sa thèse de doctorat au laboratoire SCRIBENS de l'École polytechnique de Montréal dont Réjean PLAMONDON est le directeur.

O. URECHE et R. PLAMONDON, *Document Transport, Transfer and Exchange : Security and Commercial Aspects*, 5th International Conference on Document Analysis and Recognition, in *IEEE Computer Society*, Bangalore, 1999.

O. URECHE et R. PLAMONDON, *Système électronique de transfert numérique de valeur : étude de faisabilité*, École polytechnique de Montréal, EPM / RT-96 / 22, 1996.

Pour la libéralisation de la cryptographie

RONALD RIVEST

L'un des pionniers de la sécurité informatique s'oppose au contrôle gouvernemental de la cryptographie.

Le développement de la cryptographie est une conséquence inéluctable de la révolution informatique. Avec l'apparition des communications entre les ordinateurs, les utilisateurs cherchent à sécuriser les conversations et les transactions. La cryptographie est la… clé de cette sécurisation, mais sa généralisation est débattue. Aux États-Unis, le gouvernement veut restreindre l'usage de la cryptographie, car il craint que les criminels et les espions ne l'utilisent.

Avant 1970, la cryptographie était trop compliquée et trop onéreuse pour un usage courant. Grâce à deux inventions – la cryptographie à clé publique et le microprocesseur –, les méthodes cryptographiques sont devenues si performantes qu'il faudrait des années de calcul sur ordinateur pour décoder un message dont on ignore la clé. Les ordinateurs capables d'exécuter ces méthodes sont devenus largement accessibles.

Toutefois, vers la fin des années 1980, lorsqu'une cryptographie civile devint ainsi possible, deux agences américaines s'inquiétèrent de sa généralisation. L'Agence de sécurité américaine (NSA, soit *National Security Agency*), qui surveille les communications électroniques mondiales, s'alarma de ne plus pouvoir décrypter les messages chiffrés d'espions ou de terroristes potentiels. D'autre part, le FBI craignit que les criminels n'usent de logiciels de cryptographie pour déjouer la surveillance de leurs communications. Durant la dernière décennie, ces organismes ont poussé le gouvernement américain à réglementer l'usage de la cryptographie et à limiter l'exportation de logiciels de cryptographie performants.

Doit-on priver l'ensemble des utilisateurs de techniques, sous prétexte que quelques criminels pourraient les utiliser à leur avantage? L'argument est spécieux : on n'empêche pas le public d'acheter des gants sous prétexte que les voleurs en utilisent pour éviter de laisser des empreintes digitales. Restons sur ce dernier exemple.

La cryptographie protège les données ; les gants protègent les mains. La cryptographie protège contre les intrus et les espions industriels ; les gants protègent contre les coupures, la chaleur, le froid et les infections. La cryptographie peut gêner la police, qui ne pourra plus pratiquer d'écoutes téléphoniques ; les gants peuvent gêner la police qui trouve difficilement des empreintes digitales. La cryptographie est devenue bon marché et d'emploi facile ; les gants le sont depuis longtemps. Enfin, on peut télécharger des logiciels de cryptographie à partir du réseau Internet pour un coût inférieur à celui d'une bonne paire de gants.

Le travail de la police deviendra certainement plus difficile si tous les utilisateurs du réseau chiffrent leurs échanges, mais nous ne sortirons correctement de ce dilemme que si nous pesons les avantages et les inconvénients collectifs de l'innovation. La plupart des utilisateurs envisagent d'utiliser la cryptographie pour prévenir les crimes plutôt que pour les cacher, comme ils utilisent les gants pour protéger leurs mains plutôt que pour dissimuler leurs empreintes. En assurant la confidentialité et l'authentification des opérations bancaires et commerciales, la cryptographie empêche le vol et la fraude aux cartes de crédit, et elle évite le piratage industriel. Paradoxalement, on créera une société plus sûre si l'on adopte une technique qui entrave quelque peu l'application des lois.

Certains ont souhaité un compromis qui généraliserait les systèmes cryptographiques élaborés en permettant aux États de déchiffrer les messages en cas de besoin : par exemple, on pourrait demander aux utilisateurs d'enregistrer leurs clés de chiffrement auprès d'organismes assermentés ou de donner aux autorités des moyens secrets d'accéder à ces clés. Une version cryptée de la clé qui a chiffré le message serait envoyée en même temps que celui-ci. Un centre de recouvrement des clés pourrait utiliser une super clé secrète pour déchiffrer la clé, puis déchiffrer le message lui-même.

La réglementation en France

Pendant longtemps, la cryptographie a été considérée comme une arme ; son usage était réglementé, aussi bien pour la fourniture et l'exportation que pour l'utilisation à titre personnel.

En février 1998, toutefois, l'État français à autorisé tout procédé nécessaire à l'authentification de données ou d'entités (intégrité, signature numérique et contrôle d'accès), ainsi que le chiffrement des communications, en limitant, dans ce dernier cas, la clé secrète à 40 bits. Une telle taille de clé ne garantissait pas un niveau de confidentialité suffisant pour des applications «sérieuses» : à raison d'un million d'essais par seconde, une station de travail trouve la clé en moins de 15 jours.

Comment accroître la sécurité ? En augmentant la taille de la clé et en déposant alors la clé secrète auprès d'un tiers de confiance. Ce dépôt permettait alors aux instances judiciaires d'obtenir, de ce tiers de confiance, la clé secrète nécessaire au déchiffrement de communications chiffrées, en cas de besoin justifié.

Le 19 janvier 1999, le premier ministre, Lionel Jospin, annonçait une proche libéralisation de l'usage de la cryptographie. Après avoir interrogé les acteurs, les experts et les partenaires internationaux, le gouvernement a retenu les orientations suivantes : libéraliser complètement la cryptographie ; supprimer le recours obligatoire aux tiers de confiance pour le dépôt des clés secrètes de chiffrement ; compléter le dispositif juridique afin d'obliger la remise aux autorités judiciaires de la transcription en clair des documents chiffrés, lors de leur demande. De telles modifications législatives nécessiteront plusieurs mois.

Pour lever rapidement les principales entraves au développement du commerce électronique et pour assurer la confidentialité des communications, des décrets, parus le 19 mars 1999, relèvent le seuil de la cryptographie libre de toute autorisation de 40 bits à 128 bits. Plus précisément, ces décrets stipulent que «les matériels ou logiciels offrant un service de confidentialité mis en œuvre par un algorithme dont la clé est d'une longueur inférieure ou égale à 40 bits sont totalement libres» et que «les matériels ou logiciels offrant un service de confidentialité mis en œuvre par un algorithme dont la clef est d'une longueur supérieure 40 bits et inférieure ou égale 128 bits sont libres sans condition pour un usage privé, et soumis à déclaration dans les autres cas».

Ces décrets représentent l'étape essentielle, car des clés de 128 bits garantissent une sécurité plus que suffisante : une attaque par recherche exhaustive (essai de toutes les clés) nécessiterait plusieurs siècles, même avec tous les ordinateurs de la planète réunis. Une autre étape importante, sera «d'assurer, avec toutes les garanties nécessaires, la valeur probante du document sous forme numérique et des signatures électroniques. Les obstacles juridiques qui demeurent au développement des transactions dématérialisées seront ainsi levés».

David POINTCHEVAL, École normale supérieure, Paris

Ces systèmes ne satisferont personne, car ils sont faciles à détourner. Les espions et les criminels peuvent modifier les logiciels de chiffrement pour empêcher la recherche de la clé ou utiliser d'autres logiciels disponibles sur le réseau Internet. De surcroît, avec ces solutions, la recherche des clés serait très onéreuse et le coût du recouvrement des clés n'a pas été envisagé : qui paiera ? Enfin, la confiance dans le gouvernement risquerait de s'éroder, et la procédure serait très compliquée : imaginez qu'à chaque achat de gants vous soyez légalement tenus de coudre des copies en latex de vos empreintes digitales aux doigts de ces gants !

Les systèmes de recouvrement de clés seraient également dangereux. La procédure secrète utilisée par le FBI pour déchiffrer les messages pourrait être détournée au profit de criminels, d'intrus, d'espions ou même d'employés mécontents du FBI. En volant une super clé secrète, ces indélicats pourraient déchiffrer toutes les communications. Des millions de secrets appartenant à des sociétés, à des personnes privées ou au gouvernement seraient brusquement vulnérables.

En 1993, le Congrès américain a réclamé une étude de ces problèmes. Après deux années de travail, la commission réunie pour l'occasion a estimé que la libéralisation de la cryptographie était plus avantageuse que son interdiction. Aucune loi ne devrait limiter la fabrication, la vente et l'utilisation des systèmes cryptographiques à l'intérieur des États-Unis.

Les membres de la commission ont également estimé que l'État ne pourrait pas faire respecter une interdiction de la cryptographie. Pourtant, le FBI et la NSA prônent toujours la mise en place d'un service de recouvrement des clés ; ils s'opposent au relâchement des contrôles à l'exportation, tant que la possibilité de retrouver les clés secrètes n'est pas incorporée dans les logiciels exportés.

Entre-temps, la cryptographie s'est développée, les utilisateurs se sont familiarisés avec les programmes de cryptographie, et le contrôle deviendra inéluctablement difficile. Les entreprises adoptent des standards publics de cryptographie que même des lycéens peuvent convertir en programmes. De surcroît, il existe de nouvelles techniques qui ne chiffrent pas le message, mais permettent la confidentialité en le cachant dans un fouillis de données aléatoires. D'où la difficulté d'un contrôle !

Je maintiens que les citoyens doivent avoir le droit d'avoir des conversations privées. La démocratie repose sur la possibilité que possède chaque citoyen de partager librement ses façons de voir, sans crainte de surveillance ou de représailles. Ce principe doit être appliqué au «cyberespace», comme il l'est au monde réel. Si les États-Unis restreignaient le droit d'utiliser la cryptographie, ce serait un recul de la démocratie et une victoire de *Big Brother*.

Donald RIVEST est l'un des inventeurs de la méthode de chiffrement RSA. Il enseigne à l'Institut de technologie du Massachusetts.

Whitfield DIFFIE et Susan LANDAU, *Privacy on the Line : The Politics of Wiretapping and Ecryption*, MIT Press, 1998.

Les galets, outils du Paléolithique

SOPHIE A. DE BEAUNE

Des galets non taillés révèlent l'invention de gestes techniques avant la fabrication d'outils spécialisés.

Les silex taillés sont parmi les vestiges les plus impressionnants et les plus abondants laissés par les hommes de la Préhistoire. Des images et des récits ont popularisé la vision de l'«homme des cavernes» taillant un silex ou le brandissant pour chasser. C'est aussi par la typologie de cet outillage de pierre taillée et de l'outillage en os façonné que les grands ensembles culturels ont été définis : l'Aurignacien, le Gravettien, le Solutréen, le Magdalénien…

Toutefois, nos ancêtres ne taillaient pas la pierre plus que nécessaire : pour la plupart des outils en roche non cassante utilisés pour leurs besoins domestiques et techniques courants, ils ménageaient leur peine et choisissaient des blocs, des plaquettes ou des galets dont la forme naturelle était proche de celle qu'ils recherchaient. Ainsi, pour obtenir des récipients en roche dure, ils ramassaient des galets ronds ou ovales dont ils n'avaient plus qu'à creuser l'une des faces. Ils utilisaient aussi fréquemment des galets bruts, pourvu qu'ils aient la taille, la forme, la dureté et la densité voulues. Ils en faisaient alors des enclumes, des broyeurs, des molettes, des pilons-broyeurs, des maillets, des lissoirs, des polissoirs… Bien que rudimentaires, ces outils étaient conservés et exploités très longtemps.

Ces outils «naturels», ou façonnés par des techniques autres que la taille (piquetage, martelage, raclage, plus rarement polissage), ont été longtemps négligés. Les préhistoriens du XIX^e^ siècle et de la première moitié du XX^e^ siècle les abandonnaient le plus souvent dans les déblais. Dans le meilleur des cas, ils les conservaient sous une rubrique «divers».

Heureusement, quelques sites font exception, telles les grottes pyrénéennes de La Vache, fouillée de 1866 à 1940, et d'Isturitz, de 1912 à 1954, dont l'intégralité du matériel a été conservée : les galets utilisés y sont si abondants (presque 500 pour chaque site) que leur

Dessins de N. Deneux. Photographies de S.A. de Beaune

1. DES MOLETTES, ou meules à main, étaient utilisées pour le broyage, de végétaux par exemple, par un mouvement de bascule d'avant en arrière et de droite à gauche. De nombreuses formes naturelles des galets se prêtent à cet usage. Le plus ancien témoignage en est un galet de roche volcanique *(à droite, hauteur réelle : 7,5 centimètres)*, manipulé par des Néandertaliens il y a 70 000 à 40 000 ans dans le Petit Abri de Laussel, en Dordogne. L'usure a légèrement aplati sa face inférieure. De même, le frottement répété a poli les deux faces et le pourtour d'un petit galet de quartzite quasi circulaire, découvert dans la grotte d'Isturitz, dans les Pyrénées-Atlantiques, et daté de 28 000 à 22 000 ans *(au milieu, diamètre réel : 6,5 centimètres)*.