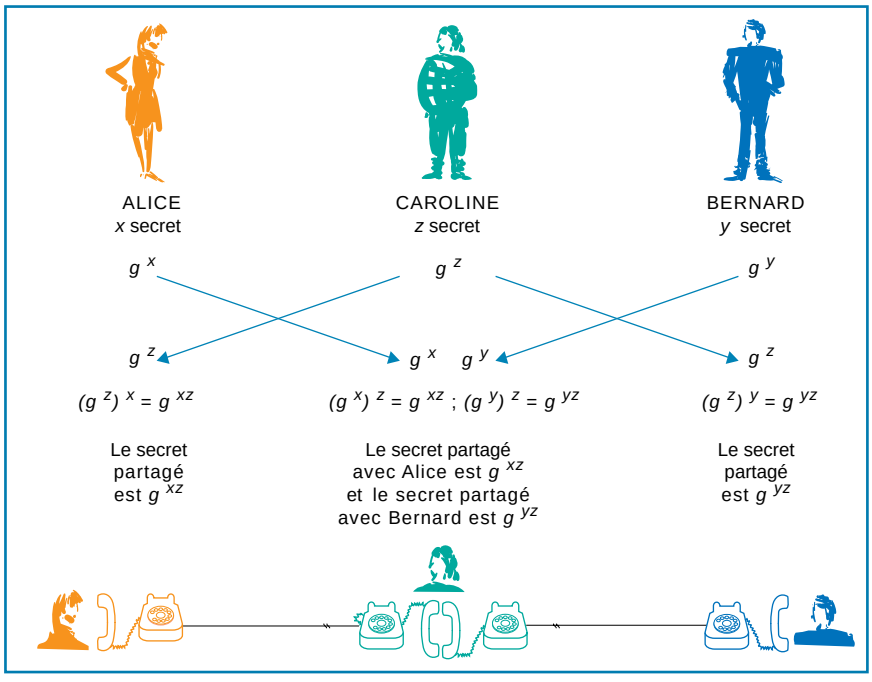


4. LES SYSTÈMES CRYPTOGRAPHIQUES À CLÉ PUBLIQUE sont vulnérables. Interceptant les transmissions entre Alice et Bernard, l'espionne Caroline dupe Bernard en utilisant son propre g^z à la place du g^x d'Alice et trompe Alice en utilisant g^z à la place du g^y de Bernard *(voir l'encadré de la page 40)*.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

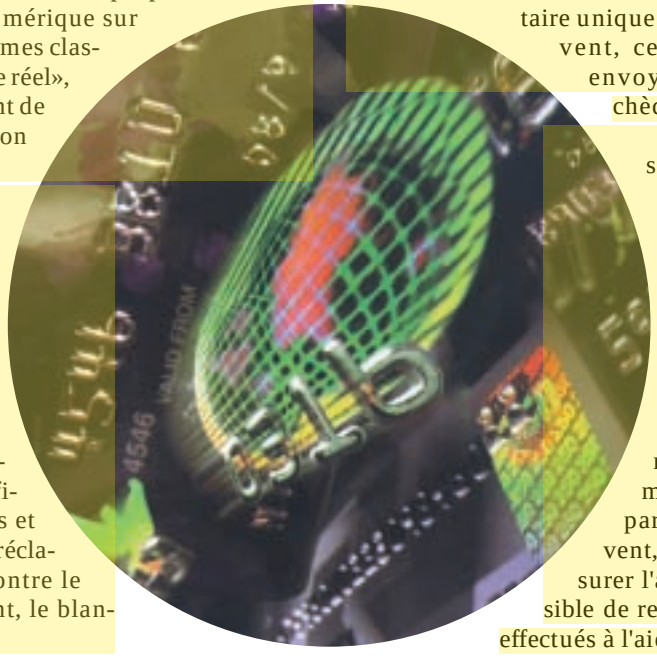
L'essor du commerce électronique nécessite de nouveaux moyens de paiement numériques, adaptés au monde virtuel de l'Internet.

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

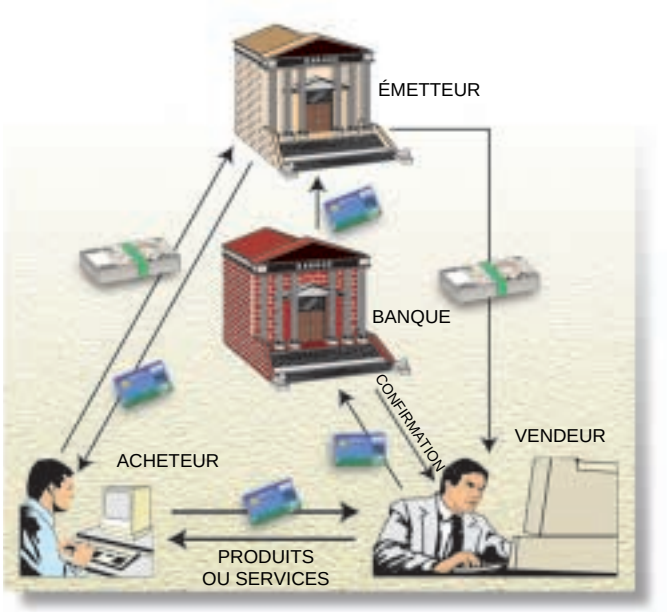
Comment s'effectue une transaction numérique? Plusieurs acteurs y participent : un acheteur, qui désire échanger son argent contre des biens ou des services offerts en ligne ; le vendeur, qui offre ces biens ou ces services ; un intermédiaire, ou courtier virtuel, qui traite les transactions ; une banque, 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.