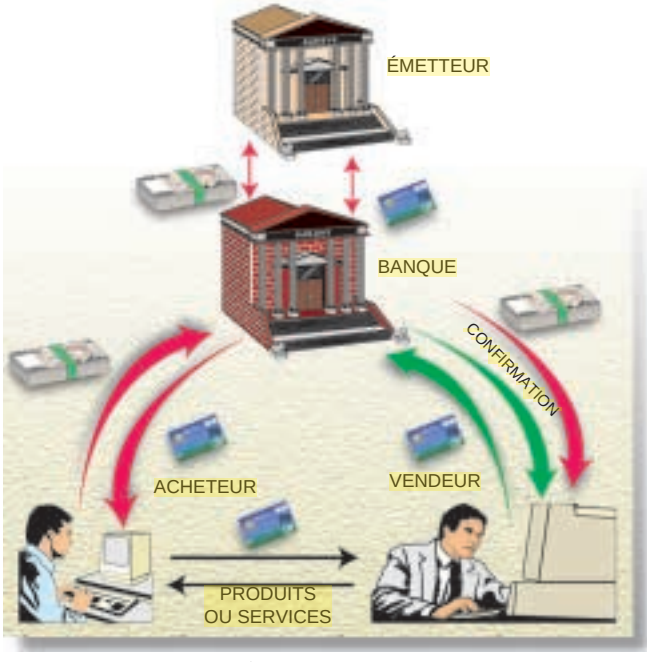
Pour les utilisateurs équipés de ces navigateurs, le chiffrement est transparent : lorsqu'un utilisateur entre son numéro de carte bancaire sur un site sécurisé (reconnaissable à l'adresse Web, où *http* est changé en *https*), celui-ci est chiffré automatiquement par l'ordinateur de l'utilisateur, puis 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.