souhaitant signer des documents choisit une chaîne de bits secrète et permanente, et publie la transformée de ce nombre par une fonction exponentielle modulaire. La procédure de production de signature d'un document est la suivante :

• choisir un jeton secret utilisable une seule fois (un nombre),

• appliquer une fonction exponentielle modulaire à ce nombre pour en obtenir un témoin,

• former et résoudre une équation qui utilise les valeurs numériques du message à envoyer, la signature secrète, le jeton et son témoin,

• transmettre le document,

• ajouter sa signature composée du témoin et de la solution de l'équation.

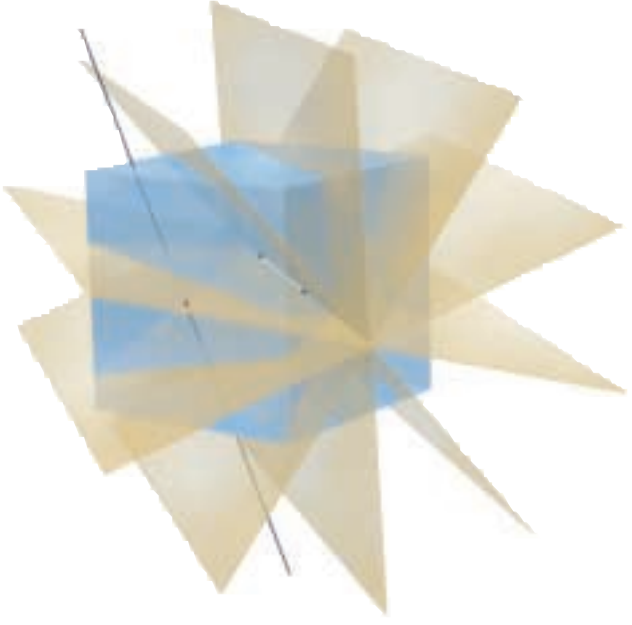
Ainsi n'importe qui peut vérifier que les nombres qui constituent la signature sont bien engendrés par la chaîne privée et par le document émis. Ces dix dernières années, de nombreuses versions de cette technique ont été mises au point.

À la place de cette technique, nous avons cherché comment, pour chaque réseau local d'ordinateur, un service

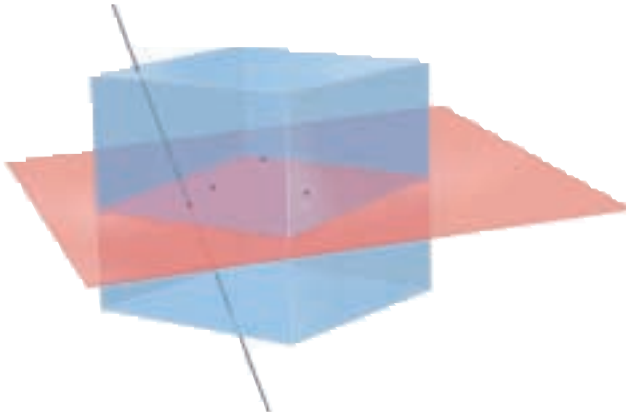
Quand les écoutes téléphoniques deviennent nécessaires

Les techniques de chiffrement que nous avons mises au point satisfont à la fois les particuliers, qui veulent conserver la confidentialité de leurs messages, et les services de police, qui veulent surveiller les échanges. Craignant que les écoutes téléphoniques ne puissent capter que des messages inintelligibles, le gouvernement des États-Unis a réglementé l'utilisation et l'exportation des logiciels de chiffrement. Il promeut également un réseau téléphonique sécurisé qui utilise une puce de chiffrement nommée *Clipper*. Le gouvernement contrôle les clés de cette puce, qui peuvent être obtenues sur demande par des agents officiels. Les détails de ce réseau demeurent secrets. Ce réseau n'inspire guère confiance, car les clés, partagées par les services de police de plusieurs pays, seront difficilement gardées. Ensuite, il peut exister des méthodes de déchiffrement en dehors du cadre des services de police.

En revanche, les méthodes que nous avons mises au point à Karlsruhe peuvent servir de base à un système qui mettrait les utilisateurs et les experts gouvernementaux en cryptographie sur un pied d'égalité. Il fournit un outil puissant pour les échanges de clés et l'authentification qui pourrait fonctionner avec le circuit *Clipper* ou avec d'autres dispositifs de chiffrement plus robustes. Afin d'augmenter la confiance accordée au procédé, on pourrait établir des clés numériques nécessitant la coopération de différents services pour autoriser les écoutes téléphoniques.



LA CONNAISSANCE DE TROIS POINTS peut être répartie entre plusieurs personnes, de manière qu'aucune d'entre elles ne puisse, à elle seule, déduire un point secret. Il existe en effet une infinité de plans passant par deux points confiés à chacune des personnes.



À PARTIR DES DONNÉES DE TROIS POINTS (un plan) et d'une droite publique, on calcule les coordonnées du point d'intersection. Ces coordonnées forment une clé secrète à trois parties.

Pour comprendre comment ce garde-fou pourrait fonctionner, imaginons que la séquence de bits qui code la clé soit constituée non pas d'un seul nombre, mais de trois ou plus. Gustavus Simmons, des Laboratoires *Sandia*, a eu l'idée d'utiliser trois fractions de la clé secrète comme coordonnées d'un point dans un espace à trois dimensions.

Toute clé secrète serait composée de trois nombres appartenant à une droite dans cet espace. Cette droite, connue de tous, serait néanmoins sûre en raison du nombre infini de ses points. On effectuerait le partage de l'information concernant le point secret en faisant passer un plan par ce point et en choisissant trois autres points au hasard sur ce plan. Ces points seraient utilisés pour reconstruire le plan et trouver son intersection avec la droite.

Chacun des membres de la commission d'autorisation des écoutes téléphoniques recevrait les coordonnées de deux des points. Deux membres en accord pourraient alors déterminer le point secret. Toutefois, grâce à SELANE, ils obtiendraient les coordonnées précises sans connaître le nombre secret, ce qui compromettrait la sécurité du système. S'ils donnent à leurs partenaires la version chiffrée de leur point, la même relation mathématique existera entre ces points et l'image de la droite codée qu'entre les vrais points et la véritable droite sur laquelle se trouve le point secret.

Ce principe est généralisable quelle que soit la taille de la commission et le quorum nécessaire. Des responsabilités partagées de cette façon compliquent n'importe quelle tentative de percer le secret, que ce soit par la violence, le chantage ou la corruption. Je pense que le monde des affaires accepterait volontiers un tel système, qui éviterait la mainmise de l'État. Les gouvernements pourraient également l'accepter pour éviter la prolifération des codages robustes, ce qui se produit aujourd'hui.

des clés pourrait remplacer les services de délivrance des passeports. Avant d'attribuer le premier identificateur, le service des clés élabore ses propres clés de signature : un nombre secret et la version publique, obtenue à l'aide d'une exponentielle modulaire. Quiconque désire vérifier les identificateurs attribués par le service des clés a juste besoin d'une copie de la clé publique.

Le service des clés fournit un certificat (une puce électronique résistant aux altérations et placée dans une carte de crédit ou dans une montre spéciale) à chaque personne, terminal ou ordinateur de son réseau. Ce certificat peut être utilisé dans toutes les transactions. Lorsque Alice demande un numéro d'identification au service des clés, elle obtient un certificat dont la mémoire contient le message suivant : «Le propriétaire de cette carte est Alice Wunderkind, professeur d'informatique à l'Université de Paris», suivi d'une signature du type ElGamal fondée sur ce message.

Ultérieurement, afin de convaincre Bob que son numéro d'identification est valide, Alice utilise son certificat pour lui envoyer un message ainsi que le témoin du jeton utilisé dans la signature. En utilisant ces valeurs et la clé publique du service des clés, Bob calcule le partie de la signature que le certificat n'a pas révélé. Pour s'assurer que l'identificateur est valide, Bob dialogue avec le certificat en lui posant des questions dont les réponses sont justes seulement s'il connaît la partie secrète de la signature.

Mes collègues et moi-même avons conçu un protocole qui intègre l'authentification et la vérification avec l'échange des clés. Ce protocole est exécuté en une fraction de seconde par un microprocesseur placé dans une carte à puce. Si leurs numéros d'identification sont bons, les deux partenaires terminent leur premier échange par une clé commune qui servira dans les transactions futures. Si l'authentification échoue, chacun reçoit une séquence différente, sans utilité aucune.

Chaîne de confidentialité

Cette méthode d'identification repose sur la confiance que Bob accorde au service de délivrance des clés d'Alice. Pour vérifier le numéro d'identification, on devra connaître la signature de tous les services des clés. Dans le cas des transactions internationales, cette méthode n'est utilisable que si les services des clés sont hiérarchisés : chacun d'entre eux devrait se légitimer en se procurant un identificateur d'un service des clés supérieur.

Une station de distribution centrale devrait garantir la confiance que l'on accorde à chacun des services des clés universitaires, qui, à leur tour, garantiraient les services des clés internes. Ce schéma est extensible à un nombre quelconque de niveaux. Une station centrale française pourrait se légitimer en utilisant l'identificateur numérique d'un centre européen qui, à son tour, serait validé par une organisation mondiale. La carte à puce détenue par une personne pourrait contenir une cascade de messages : une identification individuelle signée par le service des clés local, une identification de l'institution signée par l'autorité régionale, et ainsi de suite. La vérification d'un identificateur ne nécessite de connaître que la signature numérique d'un petit nombre d'autorités et de leur faire confiance. Ainsi pourrait-on échanger des informations à distance avec autant de confiance que si le correspondant était présent.

Thomas BETH est professeur d'informatique à l'Université de Karlsruhe et directeur de l'Institut européen des systèmes de sécurité.

Taher ELGAMAL, *A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms*, in *IEEE Transactions on Information Theory*, vol. 31, n° 4, pp. 469-472, juillet 1985.

T. BETH, *Efficient Zero-Knowledge Identification Scheme for Smart Cards*, in *Advances in Cryptology : EUROCRYPT '88*, sous la direction de Christoph Günther, Springer-Verlag, 1988.

Public-Key Cryptography : State of the Art and Future Directions, sous la direction de T. Beth, M. Frisch et G.J. Simmons, Springer-Verlag, 1992.

Gustavus J. SIMMONS, *Contemporary Cryptology : The Science of Information Integrity*, IEEE Press, 1992.

T. BETH, *Keeping Secrets a Personal Matter or the Exponential Security System*, in *Cryptography and Coding III*, sous la direction de M.J. Ganley, Oxford University Press, 1993.

H. DANISCH, *RFC 1824 : The Exponential Security System TESS* in European Institute for System Security World Wide Web site at http : / / avalon.ira.uka.de / eiss / indexe.html.