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.

Qu'est-ce que la conscience ?

DAVID CHALMERS

Les neurobiologistes et les philosophes explorent l'un des plus grands mystères de l'existence. La connaissance des mécanismes physiques du cerveau semble insuffisante pour comprendre la nature de la conscience.

La conscience est la chose à la fois la plus familière et la plus mystérieuse. Nous la connaissons plus directement que quoi que ce soit d'autre, mais cette connaissance est difficile à concilier avec nos autres savoirs. Pourquoi existe-t-elle ? Que fait-elle ? Comment résulte-t-elle de mécanismes neuronaux ?

D'un point de vue objectif, nous comprenons assez bien le fonctionnement du cerveau : lorsque nous regardons cette page, des photons frappent nos rétines, des signaux électriques sont transmis par les nerfs optiques à différentes régions de notre cerveau et, finalement, nous réagissons par un sourire, un froncement de sourcil ou une remarque. L'aspect subjectif est plus complexe : quand nous regardons la page, nous en sommes conscients, et nous ressentons directement les images et les mots comme une partie de notre vie mentale intime. Les couleurs des fleurs ou du ciel nous émeuvent, tandis que nous ressentons peut-être une émotion et que nous formulons des pensées. Ensemble, ces expériences constituent la conscience, la vie interne, subjective, de l'esprit.

Les chercheurs qui étudient le cerveau et la pensée ont longtemps laissé la conscience de côté : la science, qui repose sur l'objectivité, ne pouvait traiter de quelque chose d'aussi subjectif que la conscience. Le courant béhavioriste, qui a dominé la psychologie au début du siècle, se concentrait sur le comportement externe et interdisait de parler des processus mentaux internes. Plus tard, l'émergence des sciences cognitives a focalisé l'attention sur les mécanismes cérébraux, mais l'étude de la conscience restait exclue ; à peine évoquait-on le problème après les dîners bien arrosés.

Depuis quelques années, un nombre croissant de neurobiologistes, de psychologues et de philosophes a décidé de violer ces interdits et d'explorer les secrets de la conscience. Ils ont proposé de nombreuses théories, variées et parfois opposées, souvent fondées sur des acceptions différentes des concepts fondamentaux. Seul le raisonnement philosophique permettra de sortir de cette confusion.

Aux deux extrêmes, on trouve la position réductionniste, selon laquelle la conscience est explicable par les méthodes des neurosciences et de la psychologie, et la position «mystérieuse», selon laquelle on ne comprendra jamais la conscience. L'analyse montre que ces deux positions sont fausses et que la vérité est probablement à mi-chemin.

Contrairement aux réductionnistes, je pense que les outils des neurosciences, aussi performants soient-ils, ne peuvent pas rendre pleinement compte de la conscience. Contre la position «mystérieuse», je soutiens que la conscience est explicable par un nouveau type de théorie ; nous ne pouvons pas encore élaborer une telle théorie en détail, mais nous pouvons l'esquisser. Cette théorie contiendra de nouvelles lois fondamentales, et le concept d'information y jouera un rôle central. Elle aura des conséquences surprenantes sur notre façon de voir l'Univers, et de nous voir nous-mêmes.

Le mot «conscience» a de nombreuses acceptions. Quels problèmes

1. UNE NEUROBIOLOGISTE qui connaîtrait tout sur la manière dont le cerveau traite les couleurs mais vivrait dans une pièce en noir et blanc, ne saurait pas ce que c'est que de voir les couleurs. La connaissance du cerveau n'apporte pas la connaissance complète de la conscience.