DR

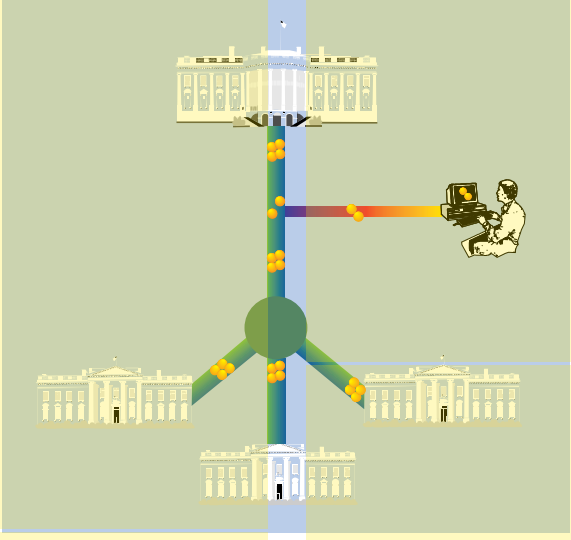
Haie brise-vent au milieu d'un champ de maïs, dans la plaine de Valence.

recommandent d'éviter certaines essences, par exemple le baguenaudier, dans une haie qui jouxte un verger de pommiers, parce que l'on favoriserait alors la prolifération des zeyzères, un gros ver qui détruit les rameaux. De même, on évitera le buis à côté des arbres à noyaux (pêchers, cerisiers, abricotiers), car il semble attirer les pince-oreilles (forficules). Inversement, de nombreuses essences apportent surtout des insectes utiles aux vergers : ce sont des arbustes tels que noisetiers, charmes, lauriers-tins, cornouillers, ou bien des arbres tels que micocouliers ou chênes pédonculés.

Un réseau quantique

Durant la guerre froide, le «téléphone rouge», qui reliait Moscou à Washington, était protégé par un système de chiffrement absolument sûr. Malheureusement, ce système nécessitait l'échange préalable, avant chaque communication, d'une clé de chiffrement à usage unique. Cet échange nécessite un courrier fiable. Au laboratoire de *British Telecom*, Paul Townsend a mis au point un système de communication chiffré multi-utilisateurs, fondé sur la mécanique quantique. Cette méthode permet à plusieurs utilisateurs d'échanger en toute sécurité des clés de chiffrement.

Aujourd'hui, les canaux de télécommunication reposent sur le déplacement d'ondes électromagnétiques. Un espion qui souhaite «écouter» une communication peut aisément le faire. Certes, il ne suffit pas d'écouter pour comprendre. Encore faut-il que l'espion déchiffre le message. Les méthodes classiques de chiffrement utilisent une clé publique (un grand nombre) que l'espion devra factoriser pour déchiffrer le message. S'il est vrai que les moyens de calculs actuels ne permettent pas cette factorisation en des temps raisonnables, on ne peut prédire ce que seront ces moyens dans dix ans, alors même que les données chiffrées aujourd'hui seront encore en circulation. Pour que la sécurité soit totale, une clé à usage unique, aussi longue que le message, doit être utilisée.



La cryptographie quantique peut être utilisée pour échanger des clés de chiffrement confidentielles entre l'Élysée et des ministères reliés par fibre optique. Un espion qui écouterait cet échange altérerait le signal et serait aussitôt repéré.

La cryptographie quantique fournit la solution rêvée : un moyen parfaitement sûr d'échanger des clés, sans possibilité d'écoute discrète. Cette méthode est fondée sur la mécanique quantique. Cette dernière stipule qu'il est impossible de mesurer parfaitement l'état d'une particule, telle la polarisation d'un photon. De plus, ces mesures perturbent l'état des particules. On transmet une information en la codant sur des photons individuellement polarisés au travers d'un canal quantique. L'espion ne peut écouter la transmission sans mesurer l'état des photons, ce qui introduit des erreurs dans la transmission. Le récepteur légitime du message détecte alors qu'il y a eu écoute.

Malheureusement, le récepteur ne peut pas non plus mesurer l'état des photons de manière exacte, mais ces problèmes se résolvent par des techniques «classiques» mises au point par les fondateurs de la cryptographie quantique, Charles Bennett et Gilles Brassard. Un tel procédé permet ainsi à deux personnes de constituer à distance une clef secrète arbitrairement longue, et de manière sécurisée. Après cet échange, les interlocuteurs utilisent la clé pour échanger des messages de manière parfaitement sûre en utilisant un chiffrement classique.

Le procédé d'échange de clefs par un canal quantique doit surmonter plusieurs obstacles technologiques, notamment l'élaboration du canal. Par la nature même du procédé, il est en effet impossible d'amplifier le signal par un procédé actif, ce qui limite la portée de telles communications. La première expérimentation d'un canal quantique a été réalisée en 1989 sur une distance de 32 centimètres dans les laboratoires d'IBM. En 1995, au CERN, un canal quantique de 23 kilomètres, composé de fibres optiques, a été testé sous le lac de Genève.

Ces procédés ne permettaient que les communications entre deux personnes. Au laboratoire de recherche de *British Telecom*, Paul Townsend a mis au point un «réseau optique quantique» : un réseau qui permet à un émetteur d'échanger des clefs secrètes avec trois récepteurs différents sur plus de cinq kilomètres. Un tel réseau pourrait, par exemple, permettre à l'Élysée de communiquer de manière parfaitement sécurisée avec ses différents ministères.

D'autres expériences tentent d'utiliser la cryptographie quantique pour changer les clés de chiffrement de satellites de communication en orbite basse. Malheureusement, la portée de ces transmissions quantiques est trop faible...

Serge VAUDENAY, CNRS, ENS, Paris