Transmissions quantiques à 10 Gb/s (made in Switzerland)

- Informatique - Sécurité Informatique -

Date de mise en ligne : jeudi 18 janvier 2007

Les Suisses d'id Quantique et les australiens de Senetas viennent de signer un accord de partenariat et de développement visant à associer d'une part la technologie « réseau quantique » conçue par les anciens de l'EPFL et d'autre part, par les spécialistes des systèmes de chiffrement haut débit.

D'un point de vue technique, le « brin quantique » (QKD, ou Quantum Key Distribution) transmet entre deux terminaux et à vitesse très lente (quelques kilobits/s), une clef considérée comme inviolable. C'est cette clef qui sera utilisé par les outils de chiffrement gigabit de l'Australien, lesquels seront installés à chaque extrémité du réseau sécurisé.

La pérennité de la clef de chiffrement n'excède pas quelques millisecondes -Senetas emploie un AES 256-, le temps qu'une autre clef soit acheminée par le réseau QKD. Les puristes feront remarquer que l'on met ainsi entre parenthèse la véritable notion d'OTP (One Time Pad), clef unique, à usage unique et de longueur équivalente au document à chiffrer. Reste que la lenteur propre aux transmissions d'une clef quantique continue limiterait, dans ce cas, le débit de l'information ainsi cryptée. Il est donc plus pratique d'employer des « morceaux » de clef quantique de 256 bits, et d'utiliser cette clef durant toute la période nécessaire à la réception des 256 bits quantiques (Qbits) suivants. Ce fonctionnement en mode Fifo est la seule technique capable d'atteindre des débits élevés. Les français de Smart Quantum utilisent d'ailleurs une méthode légèrement semblable afin d'atteindre des flux de données exploitables dans un « véritable » milieu industriel.

Post-scriptum :

http://securite.reseaux-telecoms.ne...