Lazlo Kish invente la crypto quantique du pauvre

- Informatique - Sécurité Informatique -

Date de mise en ligne : vendredi 23 dÃ©cembre 2005

Spyworld Actu

Lazlo Kish, de la Texas A&M Univerity, vient de publier un mémoire intitulé « Communications classiques entièrement sécurisées reposant sur l'effet Johnson et la loi de Kirchoff ». Dans les grandes lignes, le procédé permet d'établir des liaisons impossibles à écouter sans que les correspondants légitimes s'en aperçoivent. Et ceci sans la complexité des échanges de photons polarisés d'un réseau quantique, sans les limitations de distance liées aux pertes des fibres optiques, et sans un impact aussi important sur la bande passante que celui provoqué par la sensibilité des capteurs de photons uniques.

L'astuce consiste à échanger la clef de cryptage en commutant, de part et d'autre de la ligne, des résistances. De simples résistances « couche carbone », deux à chaque extrémité de la paire torsadée, elles-mêmes « branchées » au câble selon un ordre aléatoire. Prenons, par exemple, une 120 Ohm et une 4,7 K. Chaque correspondant (Alice et Bob) mesurera la valeur du circuit, qui, selon les hasards de la commutation, atteindra 240, 4 820 ou 9400 Ohms. Eve, l'écouteur supposé, parviendra très aisément à deviner à quel moment les deux parties utilisent une résistance de même valeur. Mais lorsque, dans 50 % des cas, les résistances seront de valeurs différentes, il lui sera impossible de déterminer si la 120 Ohms est du côté de Bob ou du côté d'Alice... à moins de couper le circuit et de mesurer la résistance finale en injectant un courant de mesure. Eve est alors immanquablement repérée. Bob ou Alice, en revanche, possèdent la moitié de la solution, puisque la valeur d'une des deux résistances utilisées est connue. Si, réfléchit Bob, la mesure est de 4 820 Ohms et que la valeur locale est de 120 Ohms, alors, Alice utilise un composant de 4,7 K. Pas de quoi surmener les méninges d'un polytechnicien. On retrouve là plus ou moins le principe de comparaison des photons polarisés et des filtres utilisés en réception quantique, le spectre de Bennett et Brassard rôde encore sur les communications sécurisées.

Tout comme dans le cadre des transmissions quantiques, ce que l'on pourrait appeler le « lien QDK » doit être constitué d'un seul et unique tronçon de ligne cuivre. Les transmissions kirchoviennes ne sont donc pas adaptées à un maillage commuté physiquement ou temporellement. Elle doivent également se heurter à certaines contraintes limitant les distances absolues, notamment dès que la résistivité du matériau de transmission devient trop importante. Or, même le meilleur des cuivres présente une résistance non nulle... souvenons-nous, « R=ro.L/S ». Contrairement également aux transmissions quantiques « photoniques », le principe du réseau de Lazlo Kish ne peut être utilisé dans l'espace. BBN, en revanche, utilise depuis des années des canons laser pour établir des réseaux quantiques « sans fil et sans fibre » au sens propre du terme. Mais malgré ces limitations, il faut reconnaître aux transmissions Kish un avantage indéniable : son coût d'exploitation ridicule. Il ne nécessite qu'une « paire sèche » -hélas, disparue du catalogue de F.T. et de Transpac depuis quelques années- un commutateur rapide (quelques euros), une horloge (quelques euros encore) et quatre résistances (quelques centimes d'euros). La logique de traitement générant la clef est à la portée d'un PC tout à fait conventionnel, voir d'un DSP simple. Mieux encore, il ne faut pas être sorcier pour imaginer quelques transpositions. En mesurant la réactance d'une ligne équipée d'un filtre à capacités commutées à chaque extrémité, par exemple. En admettant même que certaines limitations viennent entacher ce principe prometteur, il est tout à fait envisageable d'en tirer une série de produits « hautement sécurisés » à faible coût et destiné à un public qui n'aura de toute manière jamais les moyens de s'offrir du quantique au prix du quantique.

Post-scriptum :

http://www.reseaux-telecoms.net/act...