

Extrait du Spyworld Actu

<http://www.spyworld-actu.com/spip.php?article3402>

Une nouvelle méthode de cryptage développée

- Informatique - Sécurité Informatique -



Date de mise en ligne : vendredi 12 janvier 2007

Spyworld Actu

La confidentialité du transfert de données à très haut débit pourra être assurée par une nouvelle méthode de cryptage associant les techniques mathématiques classiques et la physique quantique, a annoncé vendredi la société genevoise id Quantique SA.

Cette méthode, développée par id Quantique en collaboration avec la société australienne Senetas Corporation, permet de déceler toute tentative d'interception des clés de cryptage, transmises par des photons (particules de lumière) obéissant aux lois de la physique quantique.

En vertu de ces lois, il n'est pas possible de consulter une information ainsi transmise sans générer une perturbation. Ainsi, si un espion tente d'intercepter les photons (porteurs des éléments de la clé de cryptage) lors de leur transmission, une perturbation sera automatiquement enregistrée, permettant de mettre en évidence cette attaque, explique le communiqué d'id Quantique SA.

« Cette technologie permet donc de transmettre des clés (de cryptage) et de vérifier leur confidentialité avant leur usage », relève encore la société genevoise.

« Les premiers tests clients débuteront prochainement », a annoncé M. Grégoire Ribordy, Pdg d'id Quantique.

« Les détails des failles de sécurité récemment mises au jour et causant la perte de millions de dollars, mettent clairement en évidence le besoin de techniques plus robustes pour la transmission de données, tant sur des réseaux publics que privés », a relevé de son côté le pdg de Senetas, M. John Dubois.

Post-scriptum :

<http://technaute.lapresseaffaires.c...>