

Scientifiques européens contre l'écoute électronique et l'espionnage

Un projet de l'UE visant au développement d'un réseau de communications parfaitement sécurisé annonce une nouvelle ère dans le domaine de la sécurité des réseaux informatiques

Vienne, 1 avril 2004 La sécurité de la cryptographie quantique est fondée sur les lois de la nature et non pas sur la complexité de certains problèmes mathématiques, comme le sont les techniques d'encryption actuellement utilisées. Le remplacement de ces technologies obsolètes est dorénavant proche. Durant ces quatre prochaines années la production rentable d'un système de distribution de clé quantique devrait démarrer. Un prototype proche de la commercialisation, permettant une connexion cryptée entre deux points sera développé, ainsi qu'une infrastructure de réseau à haute performance pour couvrir de plus longues distances.

Afin d'atteindre ces objectifs ambitieux, les physiciens quantiques collaboreront avec des spécialistes des réseaux et des experts dans les domaines de la cryptographie, de l'électronique, des techniques de sécurité électronique, ainsi que dans le domaine du développement de logiciels. La participation d'experts en économie et de consultants assurera l'applicabilité économique et l'intégration dans des produits existants.

SECOQC – « Développement d'un réseau global pour une communication sûre fondée sur la cryptographie quantique (Development of a Network for Secure Communication based on Quantum Cryptography) »

Débutant en avril 2004, SECOQC est le premier projet du 6^{ème} programme cadre de l'UE à être lancé par un centre de recherche autrichien. Le projet est géré par son coordinateur, l'unité commerciale *Quantum Technologies* à ARC Seibersdorf Research GmbH.

“Nous allons fournir un instrument, fondé sur les technologies quantiques, qui permettra aux entreprises économiques de protéger leurs actifs contre l'espionnage industriel. Dans le passé, des pertes financières importantes dues à l'espionnage industriel ont été attribuées aux activités du réseau de surveillance et d'interception des communications ECHELON. Notre but est d'apporter une contribution significative à l'indépendance et à la compétitivité économique européenne”, explique le Dr. Christian Monyk, chef de l'unité commerciale *Quantum Technologies*, et également initiateur du projet.

La cryptographie quantique est l'élément fondamental pour des réseaux de communications hautement sécurisés

La cryptographie quantique (ou plus précisément, la génération de clés de cryptage par les méthodes de la physique quantique) apporte des solutions à deux problèmes majeurs des systèmes de cryptage contemporains. Le premier défi est celui de la génération de clés aléatoires ; le second est celui de leur distribution. Un autre avantage est la capacité intrinsèque de cette technique de détecter toute écoute déjà lors de la génération de la clé, et donc avant la transmission du message. Ainsi toute tentative d'attaque du système ne fera, dans le pire des cas, qu'empêcher la transmission du message, sans aucunement le révéler. De plus, une fois qu'un message a été encrypté à l'aide d'une clé générée quantiquement, il ne peut par principe pas être décrypté. Ceci est un avantage énorme par rapport aux techniques de distribution traditionnelles de clé et d'encryption asymétrique.

SECOQC posera la pierre angulaire d'un réseau de communications à haute sécurité, en développant la recherche expérimentale de la technologie quantique et en la connectant à la cryptographie, à la technologie des réseaux, et à d'autres disciplines liées aux technologies de l'information.

La durée du projet est de quatre ans et il sera financé par l'UE avec une somme de 11,4 millions d'euros.

Au total 41 participants de 12 pays (Allemagne, Autriche, Belgique, Canada, Danemark, France, Grande-Bretagne, Italie, République tchèque, Russie, Suède et Suisse) prennent part à ce projet. Ce consortium est constitué de trois PME, 25 universités, cinq centres de recherche nationaux, et huit entreprises privées.

La recherche fondamentale et les applications pratiques unissent leurs forces

Le projet est divisé en huit sous-projets, chacun d'eux couvrant un aspect essentiel. Après une période de 18 mois les différentes méthodes de cryptographie quantique seront évaluées en ce qui concerne leur faisabilité du point de vue technique et économique.

Selon le Dr Christian Monyk, "L'applicabilité économique et la contribution de la recherche fondamentale aux technologies futures sont des objectifs du projet aussi importants l'un que l'autre".

L'unité commerciale *Quantum Technologies* de la division de recherche "Information Technologies" à ARC Seibersdorf a été créée en 2002, avec comme objectif d'accompagner vers une concrétisation économique les futures technologies émergentes dans le domaine de la physique quantique.

Pour contact:

Maga Julia Petschinka
ARC Seibersdorf research GmbH
Geschäftsbereich Informationstechnologien - Arbeitsgruppe Quantentechnologien
Projektkoordination und Öffentlichkeitsarbeit
TechGate Vienna
Donau-City Straße 1
1220 Wien
T: +43-050550-4161
M: +43-(0)664-8251064
E: Julia.Petschinka@arcs.ac.at