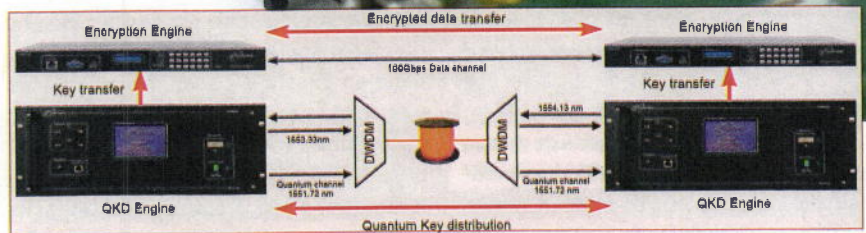
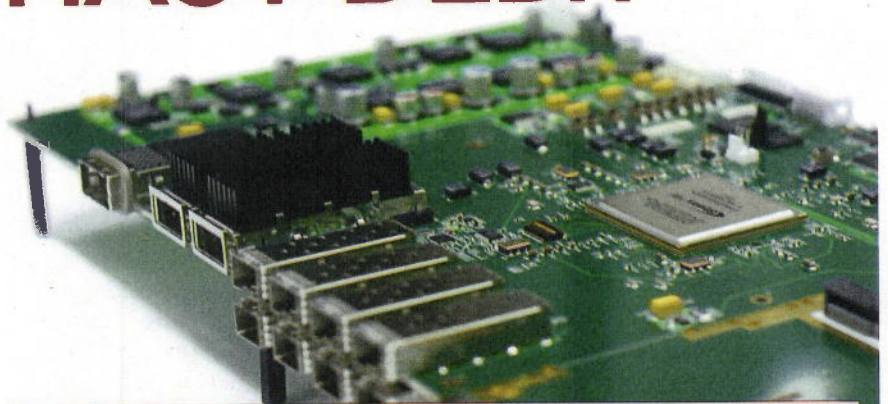


RÉVOLUTION POUR LE TRÈS HAUT DÉBIT

Philippe Cudré-Mauroux

Président du GITI et professeur à l'Université de Fribourg

À L'ORIGINE DE CETTE RÉVOLUTION TECHNOLOGIQUE: LE PROGRAMME NANOTERA, UNE INITIATIVE SUISSE POUR LES SCIENCES DE L'INGÉNIEUR, VISANT À PLACER LA CONFÉDÉRATION HELVÉTIQUE À LA POINTE DE CETTE NOUVELLE RÉVOLUTION TECHNOLOGIQUE. ELLE FAIT APPEL À L'INGÉNIEURIE ET À LA TECHNOLOGIE DE L'INFORMATION AFIN D'AMÉLIORER LA SANTÉ, LA SÉCURITÉ ET L'ENVIRONNEMENT.



Au cœur de cette révolution se trouvent les systèmes embarqués, omniprésents dans notre vie quotidienne et qui utilisent des composants électroniques toujours plus petits, représentant l'aspect «nano» du programme. On se dirige ainsi vers des systèmes basés sur des processeurs nanotechnologiques à faible consommation d'énergie et potentiellement reliés en réseaux, interagissant avec leur environnement au travers de dispositifs tout aussi minuscules et complexes. Ce qui pose de nouveaux défis, puisque ces systèmes devraient être capables de s'autogérer et de traiter des quantités de données d'un niveau sans précédent, définissant ainsi l'aspect «tera» du programme.

L'une des particularités de NanoTera est de faire coexister en son sein des efforts à la fois en matière de formation, de recherche et de développement. Cette approche vise à favoriser un développement technologique et

industriel durable et à accélérer les transferts de technologie, un point traditionnellement faible en Suisse. La première approche du programme s'oriente sur la cryptographie et ses failles.

À l'heure actuelle, une quantité extrêmement importante de données est échangée sur les réseaux informatiques. La cryptographie permet de réaliser ces échanges de manière très sécurisée. Le concept se compose ainsi: l'échange de clés, et le cryptage à l'aide de cette clé. Les systèmes actuels utilisent une clé réputée sûre, mais qui pourrait souffrir de quelques faiblesses, notamment si l'ordinateur quantique venait à faire son apparition. Une réponse à cette faille est donnée par l'usage unique de la clé de cryptage. Bien que fournissant un cryptage totalement sûr, cette technique nécessite d'échanger une clé pour chaque communication, ce qui s'avère impossible aujourd'hui. En effet, la

cryptographie quantique permet un échange de clé sûr, mais le débit ainsi atteint est nettement trop faible.

«Ce projet – appelé QCRYPT* – sur lequel travaille aussi l'UniGe, l'ETHZ, l'entreprise Quantique SA et une HES, vise donc une très nette amélioration de la technologie actuelle. Premièrement, l'échange de clé basé sur les propriétés quantiques sera amélioré afin d'atteindre un débit de 1Mbps, très supérieur à ce qui est proposé actuellement. Ensuite, le cryptage sera également amélioré, et couplé à cet échange de clé. Les débits d'échange d'information cryptée devraient, durant ce projet, passer à 100Gb/s, contre 10Gb/s à l'heure actuelle. De plus, la transmission de données passera par les réseaux de fibre optique standards utilisés par les opérateurs de télécommunications, rendant possible leur déploiement à grande échelle». Explique le professeur Messerli, de l'institut ReDS de la HEIG-VD.