Cryptographie et théorie des graphes : de l'intégrité des données aux réseaux de nanosenseurs (Jean-Jacques Quisquater - UCL Crypto Group, Louvain-la-Neuve, Belgium)

La théorie des graphes et la cryptologie interagissent de plus en plus : voici quelques sujets que nous évoquerons de façon très abordable par chacun :

- graphes réguliers de faible diamètre pour le transport physique de secrets,
- preuves de sécurité utilisant les graphes d'expansion (expanders),
- graphes de chiffrement utilisant ou non des graphes de Cayley,
- les fonctions de hâchage et leurs généralisations (la fonction de Zemor-Tillich et ses généralisations), utilisées pour vérifier l'intégrité des données (un domaine en pleine explosion depuis que trois chercheuses chinoises, l'an passé, ont montré que les solutions proposées sont assez faibles :MD4, MD5, SHA, ...),
- isomorphisme de graphes pour des preuves de connaissances,
- problème de la sécurité du logarithme discret,
- ...

Quelques paramètres de ces graphes (constante d'expansion, diamètre, degré, maille, ...) sont souvent reliés au niveau de sécurité des primitives cryptographiques invoquées.

Nous finirons l'exposé en traçant rapidement les nouvelles pistes suggérées par la théorie des réseaux de nanosenseur