ID de Contribution: **6** Type: **Non spécifié**

Cryptographie post-quantique: alternatives et enjeux

mercredi 9 juin 2021 10:00 (1h 15m)

Depuis l'apparition de l'algorithme de factorisation de P. Shor
en 1994, on sait que l'existence d'un ordinateur quantique suffisamment puissant peut amener à la cryptanalyse immédiate de tous les systèmes cryptographiques actuels basés sur la théorie des nombres utilisés en pratique comme les algorithmes RSA, les systèmes basés sur le logarithme
discret sur Z/pZ ou encore sur les courbes elliptiques. Dans cet exposé nous ferons le point sur les différentes alternatives pour resister à ce type d'attaques et notamment la cryptographie basée sur les réseaux, les codes correcteurs (en Hamming et en métrique rang) ou encore les signatures basées sur les fonctions de hachages ou encore la cryptographie multivariée. Nous considérerons aussi les enjeux au niveau du concours international lancé par le NIST (institut des standards amériain) sur la crypotgraphie post-quantique.

Orateur: Prof. GABORIT, Philippe (Université de Limoges)

Classification de Session: Cryptographie