Duong Hieu PHAN ⋆ **Cryptographie multi-utilisateurs**

Résumé :
Malgré un nombre important "one-to-one", dans le cas des communications multi-utilisateurs ("one- to-many", "many-to- many"), la plupart des solutions existantes ne sont pas satisfaisantes en pratique. Or, nous sommes dans une ère de développement très rapide des technologies où de nouvelles applications apparaissent régulièrement pour traiter des données de taille de plus en plus massive, liés au développement du cloud. Le cloud permet de stocker des données de taille très importante sur les serveurs et la question essentielle est de savoir comment on peut exploiter ces données de façon sécurisée. Afin d'atteindre cette sécurité, les fonctionnalités cryptographiques qu'il faut obtenir sont à titre d'exemple : la sécurité des calculs sur les données (au sens le plus fort, les calculs sur les données chiffrées), l'anonymat et le contrôle de l'accès aux données. Les primitives cryptographiques classiques "one-to-one" ne sont pas bien adaptées à ces nouveaux usages ; il est donc naturel de considérer des nouvelles primitives dans des communications multi-utilisateurs où les notions de corruptions, collusions, révocation et traçabilités jouent un rôle aussi important que les notions classiques de la confidentialité, de l'authentification et de l'intégrité.

Prérequis : aucun.

Références : Gérard Maze, Chris Monico et Joachim Rosenthal. *Public Key Cryptography Based on Semigroup Actions*; Advances in Mathematics of Communications, Vol. 1, No. 4, 2007, 489-507.