Duong Hieu PHAN ⋆ **Decentralized Cryptography**

Résumé : Un axe de recherche très actif en ce moment est d'étudier la décentralization des schémas cryptographiques où aucune confiance en autorités n'est demandé et chaque utilisateur contribue à la génération des parametrès du système. Blockchain est une méthode intéressante pour décentralizer la validation des transactions mais cette technique ne peut pas être appliquée à des objectif plus avancés, à nommer les calculs distribués. L'objectif de ce projet est d'étudier des méthodes de décentralizer les calculs entre plusieurs acteurs. **Prérequis :** aucun.

Références :

- Decentralized Dynamic Broadcast Encryption
  Duong Hieu Phan, David Pointcheval and Mario Strefler `https://www.di.ens.fr/users/phan/2012_scn.pdf`
- Decentralized Multi-Client Functional Encryption for Inner Product
  Jérémy Chotard, Edouard Dufour Sans, Romain Gay, Duong Hieu Phan and David Pointcheval. `https://eprint.iacr.org/2017/989.pdf`