Duong Hieu PHAN ⋆ **Functional Encryption**

Résumé : Functional Encryption (is a new paradigm for encryption which extends the traditional "all-or-nothing" requirement of Public-Key Encryption in a much more flexible way. FE allows users to learn specific functions of the encrypted data: for any function f from a class F, a functional decryption key dk_f can be computed such that, given any ciphertext c with underlying plaintext x, using dk_f, a user can efficiently compute $f(x)$, but does not get any additional information about x. This is the most general form of encryption as it encompasses identity-based encryption, attribute-based encryption, broadcast encryption. The objective of this project is to study the state of the art of functional encryption and its applications. **Prérequis :** aucun.

Références :

- Functional encryption: Definitions and challenges.
  Boneh, D., Sahai, A., Waters `https://eprint.iacr.org/2010/543.pdf`

- Efficient Public Trace and Revoke from Inner-Product Functional Encryption
  Shweta Agrawal, Sanjay Bhattacherjee, Duong Hieu Phan, Damien Stehlé and Shota Yamada. `https://eprint.iacr.org/2017/650.pdf`