Duong Hieu PHAN ⋆ **Machine learning on encrypted data**

Résumé :

Machine learning provides invaluable tools for applications such as medical predictions, face recognition, spam detection etc. However, many of these applications handle sensitive data and it is thus important to protect the private data and the result of the machine learning algorithm.

Recent advances in cryptography allow to preserve data confidentiality when outsourcing computation: encrypt the data before uploading it to the cloud. This may limit the utility of the data, but recent methods allow to search and perform operations on encrypted data, all without decrypting it.

The goal of this project is to study how some models in machine learning can be implemented on encrypted data

Références

- Machine Learning Classification over Encrypted Data `https://eprint.iacr.org/2014/331.pdf`
- Machine Learning on Encryted Data: the Consistency Model (Master's Report of Hebant Chloé) `https://www.dropbox.com/s/v6fdsvrpbf96mxz/2017_HEBANT_rapport.pdf?dl=0`