Lattice-based Homomorphic Encryption

Crypto Internship Proposal

Snips UVSQ

Spring 2017

Motivation

Computing on encrypted data carries many promises when it comes to data aggregation. Today, data used for training machine learning models is typically stored unencrypted on central servers, putting not only user privacy but also company reputation at risk, and in turn discouraging the use of valuable but sensitive information. With the promise of *homomorphic encryption* this may change, since companies would be able to perform learning on encrypted data and only be able to decrypt the final model.

While a limited form of homomorphic encryption has been around for a while, recent developments allowing any function to be computed on encrypted data have naturally excited several research communities, including for example machine learning groups at Google and Microsoft that have started experimenting with training deep learning models on encrypted data. Unfortunately, not only does it seem that fundamental improvements are still needed before these systems can be made sufficiently efficient, even instantiating the current state-of-the-art constructions is non-trivial, requiring insight in the underlying mathematics and knowledge about the specific application

Objectives

- Investigate and understand existing lattice-based homomorphic encryption schemes, including algorithmic underpinnings of parameter generation and implementations
- Develop expertise in using simulators for estimating application and security requirements
- Benchmark current implementations for specific applications (private data aggregation)
- Expected outcome is technical report and proof-of-concept implementations of experiments (using existing libraries such as HElib, SEAL, or NFLlib)

Skills

- Suitable for Math/CS student with strong mathematical maturity (algebra and algorithms)
- Prior programming experience a plus (expect to do some prototyping)

Format

- 4-6 month full-time internship position at Snips
- collaboration with the CRYPTO research team at Université de Versailles – Saint-Quentin
- Suitable for those interested in pursuing research in cryptography (especially lattice-based)

Company

Snips is young start-up located in the centre of Paris. Our primary focus is on data science and machine learning, but since we encourage the principle of *Privacy by Design*, we also have a growing team working on privacy enhancing technologies, such as secure computation, homomorphic encryption, and differential privacy. We are currently around 40 employees, including data scientists, software engineers, designers, and cryptographers.