Specialised Zero-Knowledge Proofs

Crypto Internship Proposal

Snips UVSQ

Spring 2017

Motivation

Zero-knowledge proofs are, among other things, used to enforce desired behaviour in cryptographic protocols, such as proving that an encrypted value lies in a certain domain or that an output was computed according to a pre-described function of unknown values. It is well-known that zero-knowledge proofs exist for all statements with short proofs (i.e. all languages in NP), yet these general constructions are often far from efficient and hence often more of theoretical interest.

Instead, in practice, specialised zero-knowledge proofs are often developed to fit a specific application and the cryptographic primitives that it uses. For example, if the application uses ElGamal encryption, where an encryption of m under public key h and using randomness r is given by (g^r, mh^r), proving knowledge of a discrete log of g^r corresponds to proving knowledge of m. Hence, by following a simple three message zero-knowledge protocol for discrete logs (known as Schnorr's protocol), we can prove that we correctly generated an ElGamal ciphertext, as opposed to, say, simply made a copy of someone else's.

Objectives

- Research and develop zero-knowledge proofs for use with our application for private data aggregation, based on secret sharing and homomorphic encryption
- Provide technical report detailing the proofs, either as internal documentation or as research paper
- Optional implementation (proof-of-concept or production-ready) depending on focus; preferred language is Rust but not a strict requirement

Skills

- Suitable for Math/CS/Engineering student with some mathematical maturity (algebra)
- No prior programming experience needed but a plus

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 engineering or research in cryptography

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.