Proof Systems for Post-Quantum Signatures

Internship Summer 2022 - PQShield SAS (Paris, FR)

UPDATE 26/01/2022: THIS INTERNSHIP POSITION IS NOW FILLED. THE OFFER IS NOW CLOSED.

BACKGROUND

In cryptography, a standard way of building digital signatures relies on non-interactive zero-knowledge proofs and one-way functions (OWFs). At a very high level, the principle of these signatures is as follows: the public key is (f, y = f(x)) with f a OWF, the private key is the value x, and each signature is a non-interactive zero-knowledge proof of knowledge of x. A recent but very dynamic field of research consists in using a technique called MPC-in-the-Head, or MPCitH [1], in order to compute this zero-knowledge proof.

An appealing feature of these signatures is that their security can be based on very conservative cryptographic assumptions, similarly to hash-based signatures but by leveraging completely different techniques. In particular, this framework can be easily instantiated to construct plausibly post-quantum signatures. The security and efficiency of these signatures depends on the MPCitH proof system, on the underlying OWF f and on the interplay between the two.

INTERNSHIP

The goal of this internship is to study MPCitH proof systems from which we can build post-quantum signatures.

In the first part of the internship, the intern will get acquainted with existing MPCitH proof systems: KKW [2], the sacrificing method [3], etc. The goal is to understand the core principles of each proof system, their differences and respective advantages.

In the second part of the internship, the intern will work with researchers at PQShield to improve the state of the art. These improvements can take various forms:

- Combine various MPCitH proof systems and/or techniques
- Leverage the structure of the OWF (e.g. the Legendre PRF or an AES-based PRF)
- Exploit the interplay between specific MPCitH proof systems and OWFs

If successful, these improvements may expand the design space or increase the efficiency of MPCitH proof systems and/or signatures based on them.

The duration of the internship is up to 6 months. We have flexible starting and ending dates. Gross salary is about 1400 € / month.

ABOUT US

PQShield is a cybersecurity startup that specialises in post-quantum cryptography, protecting information from today's attacks while readying organisations for the threat landscape of tomorrow. It is the only cybersecurity company that can demonstrate quantum-safe cryptography on chips, in applications and in the cloud. Headquartered in Oxford, with additional teams in the Netherlands and France, its quantum-secure cryptographic solutions work with companies' legacy systems to protect devices and sensitive data now and for years to come.

PQShield SAS concentrates the research activities of PQShield. Our mission is to come up with innovative algorithmic and/or protocol-level solutions to real-world cryptographic problems. Besides post-quantum cryptographic primitives, our research interests include advanced cryptosystems/protocols such as secure messaging, threshold schemes, and multiparty computation. We are located at the co-working space Morning Monceau, in the center of Paris.

REQUIREMENTS AND HOW TO APPLY

We are looking for interns with a strong background in theoretical computer science and/or mathematics. It is recommended to be comfortable with cryptographic security proofs and reductions between computational problems.

To apply, please send your CV and cover letter to *rafael.del.pino (at) pqshield.com* and *thomas.prest (at) pqshield.com*.

REFERENCES

1. Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky and Amit Sahai
   Zero-Knowledge from Secure Multiparty Computation
   STOC 2007. https://web.cs.ucla.edu/~rafail/PUBLIC/77.pdf
2. Jonathan Katz, Vladimir Kolesnikov and Xiao Wang
   Improved Non-Interactive Zero Knowledge with Applications to Post-Quantum Signatures
   CCS 2018. https://eprint.iacr.org/2018/475
3. Carsten Baum and Ariel Nof
   Concretely-Efficient Zero-Knowledge Arguments for Arithmetic Circuits and Their Application to Lattice-Based Cryptography
   PKC 2020. https://eprint.iacr.org/2019/532