Offre de Stage - Internship Offer

Efficient Zero-Knowledge Proofs for all Programs

October 2022

<table>
<thead>
<tr>
<th>Type of internship:</th>
<th>Master 2 or last year engineer student (6 months)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field:</td>
<td>Cryptography</td>
</tr>
<tr>
<td>Company:</td>
<td>CryptoExperts</td>
</tr>
<tr>
<td>Workplace:</td>
<td>41 boulevard des Capucines, 75002 Paris</td>
</tr>
</tbody>
</table>
1 Company presentation

CryptoExperts is an SMB providing outsourced R&D services in cryptography. The company has a team of experts from industry and academia, most of whom have PhDs in cryptography, and specialized in various fields (public key cryptography, post-quantum cryptography, efficient and secure implementations, security protocols and proofs, side-channel attacks, security of embedded systems, ...). CryptoExperts develops innovative solutions for various applications involving cryptography, and further offers services of custom design, security auditing, and implementation of cryptographic algorithms or protocols. The company is also very active in the field of scientific research in cryptography, producing every year several publications in the main conferences of the field, and taking part in various academic and industrial projects on advanced research issues (homomorphic encryption, zero-knowledge proofs, proven security against side-channel attacks, white-box cryptography, lattices-based cryptography, group signatures and anonymous accreditations, etc.).

2 Internship description

2.1 Context

Zero-Knowledge proofs (ZKP) have been studied for a while in the crypto theory literature since their introduction by Goldwasser, Micali and Rackoff in the mid 80's [7], but they have lately known a tremendous practical development for a wide range of innovative applications. In a nutshell, a proof system allows one party (a prover) to convince another party (a verifier) that some computational statement is correct. Specifically, the prover produces a proof $\pi$ that she knows some input $x$ such that $C(x) = y$ for some computation $C$ (e.g. a circuit or a program) and some output $y$. The proof system is said zero-knowledge if the verifier does not learn anything about the input $x$ from the proof $\pi$ (besides the fact that $C(x) = y$).

Efficient zero-knowledge proof systems have been recently designed and engineered which achieve impressive performances. In particular Succinct Non-Interactive Arguments of Knowledge (SNARK) [6, 9] and Scalable Transparent Argument of Knowledge (STARK) [1] can prove any arbitrary large computation $C$ while enjoying proof sizes and verification times which are exponentially small with respect to the execution time of $C$. For instance, the Groth'16 construction [9] produces proofs of only 200 bytes which can be verified in less than 2ms for any arbitrarily large computation $C$ (while the running time of constructing the proof scales with the number of operations in $C$).

Succinct/scalable zero-knowledge proofs (SNARK, STARK) are versatile tools to offer scalability and privacy to a wide range of applications:

- **Scalability.** Imagine a use case in which a constrained device wishes to delegate some heavy computation $C$ to a powerful server without necessarily trusting this server to return the right result. This is a typical use case for succinct/scalable ZKP: the server can perform the computation $y = C(x)$ and produce a proof $\pi$ for this computation. Then the constrained device can verify the proof for a small computational cost and
thus be convinced that the result is correct. Such a use case typically arises in the con-
text of the Ethereum blockchain on which performing heavy computation is very costly. 
Zero-knowledge rollups are ZKP-based solutions that scale Ethereum by outsourcing
the computation from the main chain and verifying the computation on-chain [5].

• Privacy. Imagine a use case in which a party owns some private data (e.g. ID card
data) on which she wants to prove some attributes (e.g. she lives in the US and is
above the legal voting age of 18) without revealing further information on this private
data. She can use a zero-knowledge proof for $y = C(x)$ where $x$ is the private data
and $C$ is the computation which verifies the validity of the data (e.g. some signature
of the ID card data), verifies the considered attributes (country = US, age $\geq 18$),
and outputs “accept” iff the two verifications work. Such advanced privacy-preserving
authentication schemes are known as anonymous attribute-based credentials [2].

Besides securely delegating computation, scaling blockchains and building anonymous
credentials, ZKP are instrumental to further applications such as, for instance, electronic
voting [8], anonymous e-cash [13], efficient post-quantum signatures [3], or fighting disinforma-
tion [4].

Many efficient proof systems have been recently proposed in the scientific literature. In
ddition to this scientific progress, zero-knowledge proofs have recently known a intensive
 technological development (see for instance [12, 10, 11]), with several start-up companies
engaging in the development of proof systems for blockchain and Web3 applications.

2.2 Subject

The goal of this internship is to study the recently developed ZKP systems (in particular
SNARK/STARK), and to design/implement a proof-of-concept ZKP system that can prove
standard programs. The internship shall be organized with the following phases:

1. Review of the technological choices made by recent start-up companies developing
zero-knowledge proof systems. As an output of this review, we will select the relevant
scientific literature to be deep-dived into.

2. Study of the selected scientific papers and identification of the advantage and limi-
tations of the different schemes in terms of performances (succinctness of the proof,
verification time, proving time) and in terms of security (e.g. requirement of a trusted
setup, alleged post-quantum security).

3. Research of improvements/optimizations of the existing schemes for their efficient ap-
lication to standard programs.

---

1 See https://zkp.science/ for an overview.
4. Implementation of a prototype ZKP system to prove simple programs e.g. made of standard (32-bit and/or 64-bit) CPU instructions. This prototype implementation shall be based on a simple high-level programming language (typically Python, SageMath).

3 Candidates

This internship offer is for a Master student who has a taste for cryptography and applied research. The candidate will have to demonstrate a solid background in mathematics and/or computer science with a specialization in cryptography. The technical background required for this internship combines skills in algebra (finite fields, polynomials, etc.) as well as ease in programming. The candidate will have to demonstrate autonomy and dynamism. A good level of English shall also be considered as a plus.

4 Contact

To apply for this internship offer, please send your resume to Matthieu Rivain at 

matthieu.rivain@cryptoexperts.com

References


