Offre de Stage - Internship Offer

Study and Improvement of Recent (Zero-Knowledge) Proof Systems

October 2023

| Type of internship:        | Master 2 or last year engineer student (6 months) |
| Field:                     | Cryptography                                      |
| Company:                   | CryptoExperts                                     |
| Workplace:                 | 41 boulevard des Capucines, 75002 Paris           |
| Period:                    | First semester of 2024                            |
1 Company presentation

CryptoExperts is an SME providing outsourced R&D services in cryptography. The company has a team of experts from industry and academia, with PhDs in cryptography, and specialized in various fields. They include public key cryptography, symmetric cryptography, efficient and secure implementations, security protocols and proofs, side-channel attacks, and security of embedded systems. CryptoExperts develops innovative cryptographic solutions for various contexts, and offers security auditing, custom conception of cryptographic protocols, and implementation of cryptographic libraries. The company is also very active in the field of scientific research in cryptography, producing every year several publications in the main conferences in the field, and taking part in various academic and industrial projects on advanced research issues (such as white-box cryptography, homomorphic encryption, proven security against physical attacks, post-quantum cryptography and zero-knowledge proofs).

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 [12], 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) [11, 14, 4] 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 [14] 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 zero-knowledge proofs (zk-SNARKs) 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 context 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 [9].

- 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 [5].

Besides securely delegating computation, scaling blockchains and building anonymous credentials, ZKP are instrumental to further applications such as, for instance, electronic voting [13], anonymous e-cash [21], efficient post-quantum signatures [7], or fighting disinformation [8]. Many efficient proof systems have been recently proposed in the scientific literature and several start-up companies have emerged which develop SNARK technologies (see for instance [19, 17, 18]).

### 2.2 Subject

Several recent SNARKs are built on top of so-called lookup arguments [10, 20, 15]. Proving a program execution typically consists in producing a computation trace made of all the intermediate values in the execution of the program and then producing a (succinct) proof that each of them was genuinely computed from previous ones (from input to output). Efficient proof systems requires that these intermediate values are represented as elements of a finite field \( \mathbb{F} \) while, in practice, they belong to some integer range, typically \( \{0, 1, \ldots, 2^{32} - 1\} \) for a 32-bit program. It is then up to the prover to show that the field elements composing the computation trace indeed belongs to the admitted range (a.k.a. range check) and that they are well computed as the output of a given instruction, e.g., a 32-bit XOR. This is usually ensured using a lookup argument: for a given lookup table \( T \), a lookup argument provides a proof that an intermediate value \( v \in \mathbb{F} \) of the computation belongs to \( T \). This is typically use for range check where the table \( T \) is defined as the target range, e.g., \( \{0, 1, \ldots, 2^{32} - 1\} \).

This can also be used to check the consistency of a program instruction, e.g., by checking that \( (v_1, v_2, v_3) \in T \) where \( T \) contains all the triplets satisfying \( v_3 = v_1 \oplus v_2 \) for the XOR operation \( \oplus \) (or any other operation involved in the program).

The goal of this internship is to study SNARKs based on lookup arguments, and in particular the recent proposals Lasso and Jolt [16, 3] (see also https://a16zcrypto.com/posts/article/building-on-lasso-and-jolt/). The first objective will be to deep dive into these schemes to gain a good understanding of the underlying techniques. Then the internship will aim at improving them in different directions:

- Efficiency. The first objective will be to analyze the bottleneck of these schemes in terms of prover efficiency (computation time) and succinctness (proof compactness and
verifier efficiency) and to investigate possible ways to improve them.

- **Zero-knowledge.** The original description of these schemes does not integrate the zero-knowledge property. The second objective will be to study how to make them zero-knowledge.

- **Post-quantum resilience.** Lasso [16] is based on a so-called *multivariate polynomial commitment scheme* which, in the original proposal, is not post-quantum secure. The third objective will be to investigate alternative commitment schemes to make the construction post-quantum secure. We will notably study commitment schemes based on hash functions [2, 4] or lattice problems [1, 6].

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.) and 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


