Quantum and Classical Cryptography for Social Benefit

Tom Gur

In recent years cryptographic proof protocols found a myriad of applications underlying the technical foundations of real-world technologies, including delegation of computation to the cloud, and decentralised systems such as blockchain technology and cryptocurrencies. Indeed, these protocols are a key ingredient in the future growth and evolution of blockchains and cloud computing, as advances in proof protocols can enhance the auditability and accountability of decentralised and outsourced computation, while obtaining key properties such as user privacy, post-quantum security, increased transaction throughput, off-chain computation, and transparent privacy.

With the rise of quantum information and the accumulating evidence for the feasibility of small-to-medium scale quantum computers, there is an urgent need to establish the foundations of verifiable computing paradigms that are post-quantum secure. Furthermore, it is also crucial to study the possibilities and speed-ups that quantum computing could offer to verifiable computing and outsourcing of computation.

The goal of this project is to study and develop such protocols in three different regimes:

1. **Classical cryptography:** This part is focused on the foundations of blockchain technology and zero-knowledge proofs, aiming to design scalable, transparent, and privacy-preserving means of communication and exchange.

2. **Quantum cryptography:** This part aims to overcome the barriers of classical cryptography by harnessing the power of quantum phenomena and applying it to the foregoing settings.

3. **Post-quantum cryptography:** While the power of quantum computing is very promising, such power could also be very dangerous. Indeed, using Shor's seminal algorithm for factoring, one can break most of the cryptographic systems we currently use to protect our data and communications. This part of the project deals with designing new protocols that are resistant to quantum attacks.

No preliminaries in quantum computing are required for this project.

References

[1] Linear-Size Constant-Query IOPs for Delegating Computation. Eli Ben-Sasson, Alessandro Chiesa, Tom Gur, Lior Goldberg, Michael Riabzev, and Nicholas Spooner. TCC 2019

[2] Spatial Isolation Implies Zero Knowledge Even in a Quantum World. Alessandro Chiesa, Tom Gur, Michael Forbes, and Nicholas Spooner. FOCS 2018