Newcastle University

Composable security of quantum digital signatures

Supervision team

Main Supervisor: Dr. Itttoop Vergheese Puthoor (ittoop.puthoor@newcastle.ac.uk)

Research project

Interested in understanding the interplay between computer science and physics in the field of quantum technologies? Working in collaboration with various universities (Heriot-Watt, Edinburgh and ETH Zurich) across UK and EU, this PhD will investigate computer science techniques for the development of quantum security systems.

Information security is critical and cryptographic techniques such as digital signatures are used for validating the authenticity and integrity of messages, software or digital documents. Quantum digital signatures (QDS) are crypto-techniques that uses the laws of quantum physics to provide security that cannot be broken even if the adversary has unlimited computing power. All works on QDS have worked on developing the security of the protocol entirely on its own. This project builds from our previous works [1] on QDS and takes a new challenging direction to incorporate composable security approaches in order to address the key security issue that arises in real QDS implementations. The project intends to develop a security framework of universal composability [2] for proving the security of QDS.

This research would be extremely useful as the security of a complex protocol can be analysed in terms of the security of each individual component in a systematic and error-proof manner, and will help to build highly efficient and secure QDS protoocol that could be integrated with other computation systems without compromising the overall security of the system.

Applicant skills/background

This project requires a strong background in Computer Science/ Physics/ Mathematics. The applicant should have or expect a first class or high 2:1 Honours degree in Computer Science, Mathematics, Physics or another relevant discipline. A Masters qualification in a relevant subject area will be highly advantageous. Enthusiasm for research, the ability to think and work independently and strong analytical skills are essential requirements. Work Experience in related research areas (like quantum computing, quantum communications and formal methods) will be highly advantageous.

References

[1] Puthoor, I. V., Amiri, R., Wallden, P., Curty, M. and Andersson, E. (2016). Measurement-device-independent quantum digital signatures. *Physical Review A*, 94, 022328.

[2] Maurer, U. and Renner, R.. (2011). Abstract cryptography. *In Proceedings of Innovations in Computer Science*, ICS 2010, pages 1–21. Tsinghua University Press.