Politecnico di Torino

COMPUTER AND CONTROL ENGINEERING

COMITATO ICT - Quantum Computing applications to Cybersecurity and related algorithms

Funded By	COMITATO PER LA GESTIONE DEL FONDO PER LO SVILUPPO DELLA RICERCA E DELLA FORMAZIONE NEL SETTORE DELL [P.iva/CF:97623280019]

Supervisor	MONTRUCCHIO BARTOLOMEO - bartolomeo.montrucchio@polito.it

Contact	LIOY ANTONIO - antonio.lioy@polito.it MONTRUCCHIO BARTOLOMEO - bartolomeo.montrucchio@polito.it

Context of the research activity	Quantum Computing (QC) is a quite new research field. The Ph.D. candidate will be required to work on cybersecurity issues from an interdisciplinary point of view. In particular Quantum and post quantum cryptography algorithms will be considered, but the target will be on all the applications of QC for security, also on Quantum Key Distribution (QKD). Since many QC based algorithms are related to security (e.g. Shor), also such algorithms will be considered during the research. This broad spectrum is important because QC related security applications are fast changing.

Objectives	Quantum computing (QC), being a totally new paradigm, is going to be a challenge for engineers, who would have not only to re-implement classical algorithms in a quantum way, but also explore uncharted paths of the new way of representing and elaborating information and its processing. In the last five years, QC companies and research institutes have come up with different software stacks, appealing to a wide spectrum of possible users, from Machine Learning to Optimization to Material simulation and of course to Quantum Cybersecurity. These companies are trying to provide the programmer pseudo-standard APIs like the ones already available for conventional computers. Since there are many different technologies, APIs are quite different from one technology to another. From the point of view of the Quantum based cybersecurity, it is possible to use such APIs in an interesting way, even if different technologies can require different approaches. Research objectives will therefore be related to the development of new algorithms and techniques on quantum and post quantum cryptography , also considering all the related algorithms, as e.g. Shor. This work will be developed during the three years, following the usual Ph.D program: - first year, improvement of the basic knowledge, attendance of most of the required courses, submission of at least one conference paper

	- second year, design and implementation of new algorithms and submission of conference papers and at least one journal - third year, finalization of the work, with at least a selected journal publication. Possible venues for publication will be, if possible, journals and conferences related to QC, from IEEE and ACM. An example could be the IEEE Quantum Computing Engineering (QCE) conference. The scholarship, funded by Comitato ICT, is not explicitly referred to a specific project, but it is expected that the candidate will be involved in two European projects, both of them on quantum based cybersecurity and in particular on Quantum Key Distribution (QKD). The work will also be done together with Fondazione Links, with whom there is already a strong collaboration on several projects. The two European projects just cited will be in collaboration with Fondazione Links too.

Skills and competencies for the development of the activity	The ideal candidate should have an interest in Quantum Computing and Cybersecurity. The candidate should also have a good background in programming skills, mainly in Python and a knowledge of classic Cybersecurity. A background in Quantum mechanics is also very useful.