Open Quantum Safe (libOQS), Cryptographic Research Architect position

This position is available immediately in Professor Mosca's Research group. You will be working with a team of researchers and developers from academia and industry on the Open Quantum Safe project (openquantumsafe.org). You will help integrate new post-quantum cryptographic algorithms into the libOQS open-source library, and design and implement techniques for evaluating and benchmarking these cryptographic algorithms in a variety of contexts. You will be required to participate in weekly sprint meetings and perform software development tasks assigned by the project team lead, ensuring that all code contributions developed by self or integrated from 3rd party contribution sources adhere to a cohesive design and framework. The field of post-quantum cryptography is rapidly evolving, and you will need to track ongoing changes to algorithms due to peer review and advances by researchers via the the NIST Post-Quantum Cryptography project forum. Any significant findings relating to a particular PQ algorithm's effectiveness or efficiency should be brought to the attention of team lead, and may be disclosed to other researchers in forum. In addition to algorithm research, tasks cover all aspects of the software development lifecycle and include design, programming cryptographic algorithms, integrating other cryptographic implementations into the libOQS framework, integrating libOQS into 3rd party opensource projects, testing, benchmarking and documentation. You may be required to take an ownership role in coordinating the development of a sub-component of the Open Quantum Safe project.

Qualifications:

- Undergraduate or Graduate degree in Mathematics, Computer Science or Electrical and Computer Engineering
- Essential: C and C++ programming experience, at least 3 years.
- Essential: Familiarity with cryptographic algorithms including public key and symmetric key cryptography, digital signatures, message digest and hashing algorithms
- Familiarity with cryptographic protocols such as TLS and SSH

- Familiarity with code analysis tools like Coverity and valgrind
- Familiarity with one or more of: Python, C#, Java
- Essential: Familiarity with version control systems (Git & Github workflow)
- Familiarity with software build systems (Make, autoconf, Visual Studio)
- Familiarity with continuous integration systems (Travis CI, Appveyor)

Quantum information science aims to develop transformational technologies that harness the power of quantum mechanics. The Institute for Quantum Computing (IQC) is a world-leading institute for research in quantum information at the University of Waterloo. IQC has 30 faculty members whose research programs span the areas of Applied Mathematics, Chemistry, Combinatorics & Optimization, Computer Science, Electrical & Computer Engineering & Physics. IQC members have the opportunity to interact with other research groups at the University, such as the Centre for Applied Cryptographic Research and the nearby Perimeter Institute for Theoretical Physics. New infrastructure, including an advanced nanofabrication and metrology centre support an expansion of experimental research programs at IQC. We are based in the new Mike & Ophelia Lazaridis Quantum-Nano Centre, a state-of-the-art facility at the heart of the University of Waterloo campus, which provides unprecedented opportunities for research, collaboration and innovation.

The appointment will be for 12 months with the possibility of additional 6-month extension, pending on research funding. The salary is competitive and commensurate with experience. The University of Waterloo respects, appreciates and encourages diversity. We welcome applications from all qualified individuals including women, members of visible minorities, Aboriginal peoples and persons with disabilities. All qualified candidates are encouraged to apply; however, Canadian citizens and permanent residents will be given priority

Please submit your CV to michele.mosca@uwaterloo.ca.