Ph.D. student in Quantum Cryptanalysis

Fri, 2018-07-06 13:24 - C. Schaffner [1] **At:** QuSoft / Leiden Unviersity / CWI
Deadline: 15 July, 2018

Location

QuSoft Amsterdam Netherlands
52° 22' 12.7776" N, 4° 53' 42.6048" E
See map: Google Maps [2]

The aim of the PhD project is to carry out quantum cryptanalysis of the most promising schemes in the NIST competition for post-quantum cryptography. The objective ranges from identifying potential vulnerabilities in the design to possibly discovering complete breaks, but also considers the question of finding the right choice of parameters for schemes that (seem to) withstand quantum attacks.

Supervision will be shared between QuSoft and Mathematisch Instituut (MI) Leiden, with Christian Schaffner (University of Amsterdam / QuSoft) and Peter Stevenhagen (MI Leiden) as main supervisors and Serge Fehr (CWI / MI Leiden / QuSoft) and Peter Bruin (MI Leiden) as co-supervisors.

You should hold a Master's degree (or expect to obtain this by the end of the academic year 2017/18) in computer science, mathematics or physics, with excellent grades and outstanding results, or a comparable degree.

Furthermore you should also possess:

- a strong background in cryptography, quantum algorithms and/or mathematics (relevant to post-quantum cryptography);
- demonstrated research abilities, e.g. by completion of an (undergraduate) research project;
- good academic writing and presentation skills;
- good social and organisational skills;
- full professional proficiency in spoken and written English.

See the link below for further information and for the application procedure.

Contact: Dr Christian Schaffner (c.schaffner (at) uva.nl)

More
Information:
http://www.uva.nl/en/content/vacancies/2018/06/18-371-phd-candidate-in-quantum-cryptanalysis.html [3]

- PhD [4]

Source URL: http://qurope.eu/db/jobs/phd-student-quantum-cryptanalysis

Links:
[1] http://qurope.eu/users/cschaffner

[2] http://maps.google.nl?q=%2C+Amsterdam%2C+%2C+nl
[3] http://www.uva.nl/en/content/vacancies/2018/06/18-371-phd-candidate-in-quantum-cryptanalysis.html
[4] http://qurope.eu/db/jobs/type/phd