Faculty of Informatics, USI   Stefan Wolf
Fall term 19   Arne Hansen

Quantum Computing

Exercise 1

1.1 Introduction

a) To get an overview of Quantum Computing, read the article "What is Quantum Information Processing?"[1] of Geza Giedke.

b) Read chapter *1.1 Global perspectives* (pp. 1–12) from the book "Quantum Computation and Quantum Information"[2] of Michael Nielsen and Isaac Chuang.

1.2 Quantum cryptography: idQuantique vs. MagiQ

Companies like *idQuantique*[3] in Geneva (this company is a spin-off of the university of Geneva) and *MagiQ*[4] provide devices for quantum cryptography. Below you find some references to read about these companies and their achievements. There is, however, criticism towards the security (see the last task).

a) To get an overview over the field of quantum cryptography, read the article "Quantum cryptography: when your link has to be really, really secure"[5] from the online magazine EDN.

b) Have a look at this article[6] about quantum cryptography.

c) Have a peek at this *black paper*[7] about problems of quantum key distribution. Do they above articles consider these problems?

---

[1]https://web.archive.org/web/20081121073043/http://www.magiqtech.com/products/whatisqip.php
[2]see iCorsi
[3]http://www.idquantique.com/
[4]http://www.magiqtech.com/
[5]http://www.edn.com/design/systems-design/4320843/Quantum-cryptography-when-your-link-has-to-be-really-really-secure
[6]https://www.wired.com/2017/02/physicists-test-quantum-cryptography-playing-catch-photons-plane/
[7]https://arxiv.org/abs/0906.4547

1.3 Quantum computer: D-Wave vs. Scott Aaronson

In comparison with quantum cryptography, the subject of quantum computers is much more controversial. On the one hand, in academic research one tries to build stable quantum systems of at most a dozen of quantum bits (qubits), on the other hand, the Canadian company *D-Wave*[8] claims to have built a quantum computer with 2048 qubits. Obviously, academic research is sceptical over such a claim. An important figure in objecting the possibility of building such a quantum computer is the MIT professor *Scott Aaronson*[9]. Below, you find some hints where to read up on the debate about quantum computers. (If you're impatient, and you directly want to know where the discussion is heading, have a look at Scott Aaronson's latest article mention in the last task.)

a) Read the *Scientific American* article "First Commercial Quantum Computer Solves Sudoku Puzzles"[10] about the first commercial quantum computer *Orion*.

b) Read Scott Aaronson's blog post[11] (and, if interested, the following comments) which was written four days before D-Wave's presentation of *Orion*.

c) Read the *Technology Review* article "Did D-Wave really demonstrate the world's first commercial quantum computer?"[12] which questions whether D-Wave really have built a quantum computer.

d) Read Scott Aaronson's reaction[13] to the *Technology Review* article (if interested, read the following comments).

e) Read the guest blog post[14] of Umesh Vazirani (professor at the University of California, Berkeley) on Scott Aaronson's blog.

f) Read Scott Aaronson's more recent post[15].

g) What do you consider good arguments for or against D-Wave actually having built a quantum computer?

---

[8] http://www.dwavesys.com/
[9] http://www.scottaaronson.com/
[10] http://www.scientificamerican.com/article/first-commercial-quantum-computer/
[11] http://www.scottaaronson.com/blog/?p=198
[12] http://www.technologyreview.com/Infotech/18495/
[13] http://scottaaronson.com/blog/?p=223
[14] http://scottaaronson.com/blog/?p=225
[15] https://www.scottaaronson.com/blog/?p=1400