Assumptions in quantum cryptography

Author(s):
Beaudry, Normand J.

Publication Date:
2014

Permanent Link:

https://doi.org/10.3929/ethz-a-010432410 →

DISS. ETH NO. 22269

ASSUMPTIONS IN QUANTUM CRYPTOGRAPHY

A thesis submitted to attain the degree of
DOCTOR OF SCIENCES of ETH ZURICH
(Dr. sc. ETH Zurich)

presented by

NORMAND JAMES BEAUDRY

Master of Science The University of Waterloo
born on *19.09.1984*
citizen of Canada

accepted on the recommendation of

Prof. Dr. Renato Renner, examiner
Prof. Dr. Christian Schaffner, coexaminer
Prof. Dr. Norbert Lütkenhaus, coexaminer

2014

Abstract

Quantum cryptography uses techniques and ideas from physics and computer science. The combination of these ideas makes the security proofs of quantum cryptography a complicated task.

To prove that a quantum-cryptography protocol is secure, assumptions are made about the protocol and its devices. If these assumptions are not justified in an implementation then an eavesdropper may break the security of the protocol. Therefore, security is crucially dependent on which assumptions are made and how justified the assumptions are in an implementation of the protocol.

This thesis analyzes and clarifies the connection between the security proofs of quantum-cryptography protocols and their experimental implementations. In particular, we focus on quantum key distribution: the task of distributing a secret random key between two parties.

We propose a framework that decomposes quantum-key-distribution protocols and their assumptions into several classes. Protocol classes can be used to clarify which proof techniques apply to which kinds of protocols. Assumption classes can be used to specify which assumptions are justified in implementations and which could be exploited by an eavesdropper.

We provide a comprehensive introduction to several concepts: quantum mechanics using the density operator formalism, quantum cryptography, and quantum key distribution. We define security for quantum key distribution and outline several mathematical techniques that can either be used to prove security or simplify security proofs. In addition, we analyze the assumptions made in quantum cryptography and how they may or may not be justified in implementations.

Zusammenfassung

Quantenkryptographie nutzt Techniken und Ideen aus einer Vielzahl verschiedener wissenschaftlicher Teilgebiete: Physik, Informationstheorie und Informatik. Die Kombination dieser unterschiedlichen Ideen macht die Sicherheitsanalyse zu einer anspruchsvollen Aufgabe.

Um zu beweisen dass ein quantenkryptographisches Protokoll sicher ist, trifft man notwendigerweise Annahmen über das Protokoll und die verwendeten physikalischen Apparate. Falls diese Annahmen in einer physikalischen Implementierung des Protokolls nicht gerechtfertigt sind, ist dessen Sicherheit offensichtlich gefärdet. Deswegen hängt die Sicherheit einer Implementierung wesentlich von der Korrektheit der getroffenen Annahmen ab.

Diese Doktorarbeit stellt eine Verbindung zwischen Sicherheitsbeweisen von quantenkryptographischen Protokollen und ihrer experimentellen Implementierungen her und untersucht diese. Dabei wird insbesondere der Fall von Quantenschlüsselverteilung betrachtet – die Aufgabe einen sicheren Schlüssel zwischen zwei Parteien zu verteilen.

Dazu wird eine Klassifikation von Protokollen zur Schlüsselverteilung mit Quantenzuständen entwickelt, die verschiedenen Protokolle mögliche Beweistechniken zuordnet. Diese Klassifizierung kann dann auch genutzt werden um zu überprüfen welche Annahmen in verschiedenen experimentellen Implementierungen gerechtfertigt sind und welche nicht – die dann bei einem möglichen Lauschangriff ausgenutzt werden können.

Diese Doktorarbeit gibt ausserdem eine verständliche Eiführung in die verschiedenen benötigten mathematischen Konzepte. Darunter fallen der Formalismus von Dichtematrizen in der Quantenmechanik, sowie die Theorie kryptographischer Protokolle mit Hilfe von Quantenzuständen, insbesondere die Quantenschlüsselverteilung. Es wird erklärt, wann ein Protokoll sicher ist, wie dies bewiesen werden kann und welche mathematischen Herangehensweisen dafür notwendig sind. Des Weiteren werden die benötigten Annahmen diskutiert, und in welcher Weise diese in experimentellen Implementierungen gerechtfertigt sind.