Device-Independent Quantum Key Distribution

Author(s):
Hänggi, Esther

Publication Date:
2010

Permanent Link:

https://doi.org/10.3929/ethz-a-006264278 →

Diss. ETH No. 19226

Device-Independent Quantum Key Distribution

A dissertation submitted to

ETH ZURICH

for the degree of
Doctor of Sciences

presented by

ESTHER HÄNGGI
MSc in Physics, EPFL

born February 11, 1982
citizen of Nunningen, SO, Switzerland

accepted on the recommendation of

Prof. Dr. Stefan Wolf, examiner
Prof. Dr. Artur Ekert, co-examiner
Prof. Dr. Renato Renner, co-examiner

2010

Abstract

Quantum key distribution allows two parties connected by a quantum channel to establish a secret key that is unknown to any unauthorized third party. The secrecy of this key is based on the laws of quantum physics. For security, however, it is crucial that the honest parties are able to control their physical devices accurately and completely. The goal of *device-independent* quantum key distribution is to remove this requirement and base security only on the (observable) behaviour of the devices, i.e., the probabilities of the measurement results given the choice of measurement.

In this thesis, we study two approaches to achieve device-independent quantum key distribution: in the first approach, the adversary can distribute any system to the honest parties that cannot be used to communicate between the three of them, i.e., it must be *non-signalling*. This constraint is strictly weaker than the ones imposed by quantum physics, i.e., the adversary is strictly stronger. Security can then be concluded *only* based on the observed correlations. In the second approach, we limit the adversary to strategies which can be implemented using quantum physics. More precisely, we demand that the behaviour of the system shared between the honest parties and the adversary can be obtained by measuring *some* kind of entangled quantum state. Security is then based on the laws of quantum physics, but it does not rely on the exact details of the physical systems and devices used to create the observed correlations. In particular, it is independent of the dimension of the Hilbert space describing them.

For both approaches, we show how device-independent quantum key distribution can be achieved when imposing an additional condition. In

the non-signalling case this additional requirement is that communication by means of the quantum system is impossible between *all* subsystems, while, in the quantum case, we demand that measurements on different subsystems must commute. We give a generic security proof for device-independent quantum key distribution in these cases and apply it to an explicit quantum key distribution protocol, thus proving its security. We also show that, *without* any additional such requirement there exist means of non-signalling adversaries to attack several systems *jointly*. Some extra constraints are, hence, necessary for efficient device-independent secrecy.

Zusammenfassung

Quanten-Schlüsselverteilung erlaubt zwei durch einen Quantenkanal verbundenen Parteien einen Schlüssel zu erzeugen, der vor jeder unberechtigten Drittpartei geheim ist. Die Sicherheit dieses Schlüssels basiert auf den Gesetzen der Quantenphysik. Sie kann aber nur garantiert werden, wenn die ehrlichen Parteien die physikalischen Apparate genau und vollständig kontrollieren können. Das Ziel *geräteunabhängiger* Quanten-Schlüsselverteilung ist, diese Bedingung zu lockern, und die Sicherheit nur auf das (testbare) Verhalten der Apparate zu basieren, genauer gesagt, auf die Wahrscheinlichkeiten von Messresultaten, gegeben die Wahl einer bestimmten Messung.

In dieser Arbeit betrachten wir zwei mögliche Vorgehensweisen um geräteunabhängige Quanten-Schlüsselverteilung zu erreichen: in der ersten kann der Gegner den ehrlichen Parteien jede beliebige Art von Systemen zukommen lassen, die nicht zur Kommunikation verwendet werden kann. Diese Bedingung ist strikte schwächer als diejenigen, die durch die Quantenphysik vorgegeben sind, der tolerierte Gegner ist also stärkerer. Sicherheit wird in dieses Fall *nur* von den beobachteten Korrelationen hergeleitet. In der zweiten Vorgehensweise beschränken wir die möglichen Strategien des Gegners auf solche, die durch Quantensysteme implementiert werden können. Genauer gesagt verlangen wir, dass das System der ehrlichen Parteien und des Gegners durch das Messen eines verschränkten Quantenzustandes erzeugt werden kann. Sicherheit beruht in diesem Fall auf den Gesetzen der Quantenphysik, ist aber unabhängig von den Details der physikalischen Systemen und der Apparate, mit Hilfe derer die Korrelationen zustande kamen. Insbesondere ist die Dimension des Hilbertraumes, der die Systeme beschreibt, beliebig.

Für beide Vorgehensweisen zeigen wir, wie geräteunabhängige Quanten-Schlüsselverteilung erreicht werden kann, falls noch eine weitere Bedingung eingehalten wird: für den Fall, wo die Systeme nicht zur Kommunikation gebraucht werden können, entspricht diese der Vorgabe, dass Kommunikation auch zwischen Teilsystemen unmöglich ist; während im quantenmechanischen Fall Messungen auf verschiedenen Teilsystemen kommutieren müssen. Wir geben in beiden Fällen einen allgemeinen Sicherheitsbeweis für geräteunabhängige Quanten-Schlüsselverteilung und wenden diesen auf ein konkretes Protokoll an, von dem wir zeigen, dass es auch unter diesen schwachen Annahmen sicher ist. Wir zeigen weiter, dass *ohne* eine solche zusätzliche Bedingung gute Strategien existieren, mit denen ein Gegner, der nur durch die Unmöglichkeit von Kommunikation beschränkt ist, mehrere Systeme *gemeinsam* attackieren kann. Weitere Einschränkungen sind deshalb im Allgemeinen notwendig für effiziente geräteunabhängige Sicherheit.