Randomness From Non-Local Correlations

Author(s):
Galliard, Viktor

Publication Date:
2012

Permanent Link:

https://doi.org/10.3929/ethz-a-007619147 →

Diss. ETH No. 20654

Randomness From Non-Local Correlations

A dissertation submitted to

ETH ZURICH

for the degree of
Doctor of Sciences

presented by

VIKTOR GALLIARD
Dipl. Inf.-Ing. ETH

born July 2, 1974
citizen of Untervaz, GR, Switzerland

accepted on the recommendation of

Prof. Dr. Stefan Wolf, examiner
Dr. Roger Colbeck, co-examiner
Prof. Dr. Renato Renner, co-examiner
Prof. Dr. Alain Tapp, co-examiner

2012

Abstract

Randomness is a fundamental and indispensable resource in various disciplines in computer science, such as algorithms and computational science. In *classical* and *quantum cryptography*, it is in general implicitly assumed that randomness is available and, in particular, it is assumed to be *free*, i.e., independent of the entire past and, therefore, unknown to a potential adversary at the time of generation. Especially device-independent models, where no assumptions are made on the internal behavior of the devices, are rendered partially, or even completely, insecure when the randomness cannot be trusted. In this work, we study the possibility of weakening the assumption on the required randomness, more precisely, we investigate whether the quality of partially free randomness can be amplified.

Quantum physics allows for *non-local correlations* which are, classically speaking, only explainable by communication, but not by shared randomness. We analyze a particular set of non-local correlations in order to determine whether it is possible to expand free randomness or amplify partially free randomness from such correlations.

Our main result is that *amplification of any partially free randomness* is possible, more explicitly, we show that, given a source of partially free bits, randomness can be generated that is strictly more free

than the initial one: Arbitrarily weak free randomness turns out to be amplifiable.

Quantum non-locality is not only a precious resource, but also fascinating phenomenon and, therefore, an interesting object of study by itself. A so-called *quantum pseudo-telepathy game* is a deterministic manifestation of non-locality. A given condition can be satisfied with certainty with shared quantum information, whereas this is impossible with shared classical information. We consider a specific such game and prove a connection to a graph-coloring problem. The findings on the chromatic number of the graph imply that the game is indeed a pseudo-telepathy game already for small parameters.

Zusammenfassung

Zufallszahlen sind eine grundlegende und unverzichtbare Ressource in verschiedenen Gebieten der Informatik, insbesondere in der Algorithmik und in den rechnergestützten Wissenschaften. In der *klassischen* und der *Quanten-Kryptographie* wird im Allgemeinen implizit angenommen, dass Zufallszahlen verfügbar sind, das heisst Werte, die zum Zeitpunkt ihrer Entstehung nicht eine Funktion der Vergangenheit sind, sondern spontan erzeugt werden und damit auch einem möglichen Gegner unbekannt sind. Vor allem geräteunabhängige Modelle, bei denen keine Annahme über das interne Verhalten der Geräte getroffen wird, werden teilweise oder völlig unsicher, falls den Zufallsquellen nicht vertraut werden kann. In dieser Arbeit untersuchen wir, ob es möglich ist, die Annahmen über die Zufälligkeit zu lockern. Genauer gesagt klären wir die Frage, ob die Qualität des nur schwachen Zufalls erhöht werden kann.

Die Quantenphysik sagt *nichtlokale Korrelationen* voraus, welche klassisch nur durch Kommunikation erklärbar sind und nicht durch geteilte klassische Daten, also vorab vereinbarte Strategien. Wir analysieren eine bestimmte Menge von nichtlokalen Korrelationen mit dem Ziel, zu untersuchen ob es mit deren Hilfe möglich ist, Zufall zu vermehren oder zu verstärken.

Unser Hauptresultat ist, dass die *Verstärkung von beliebig schwacher*

Zufälligkeit möglich ist. Genauer gesagt können wir, ausgehend von einer Quelle von beliebig schwachen Zufallsbits, mittels der studierten nichtlokalen Korrelationen, echt stärkere zufällige Bits erzeugen.

Quanten-Nichtlokalität ist nicht nur eine wertvolle Ressource, sondern auch ein faszinierendes Phänomen und daher ein interessantes Studienobjekt *per se*. Ein sogenanntes *"Quanten-Pseudotelepathie-Spiel"* ist eine deterministische Manifestation von Nichtlokalität. Ein solches Spiel besteht darin, dass zwei oder mehr Parteien in ihren gemeinsamen, aber getrennt gegebenen, Antworten eine bestimmte Bedingung mit Sicherheit erfüllen; dies ist möglich mit geteilter Quanten-, aber nicht mit klassischer Information.

Wir betrachten ein spezielles solches Spiel und zeigen seine Verbindung zu einem bestimmten Graphenfärbungs-Problem. Die erreichten Resultate über die Färbungszahl des Graphen zeigen, dass das Spiel sogar für kleine Parameter ein Pseudotelepathie-Spiel ist.