



Fortgeschrittenen-Praktikum Versuchsprotokoll

Quantenkryptographie

Betreuer: M. Leifgen

Robert Riemann; Matr.Nr.: 521085

Thomas Murach; Matr.Nr.: 517771

21. Oktober 2010

Inhaltsverzeichnis

1 Voraussetzungen

1.1 Versuchsziel	2
1.2 Motivation	2
1.3 Physikalische Grundlagen	2
1.4 Versuchsaufbau	2

Literatur und Programme

2

Abbildungsverzeichnis

Tabellenverzeichnis

1 Voraussetzungen

1.1 Versuchsziel

Im Fortgeschrittenen-Praktikum „Quantenkryptographie“ besteht das Versuchsziel darin, einen digitalen Schlüssel unter Verwendung des BB84-Protokolls quantenkryptographisch verschlüsselt über eine kurze Distanz zu übertragen. Die hierfür benötigten quantenmechanischen Zustände werden durch verschiedene Polarisierungen des zur Übertragung verwendeten Laserlichts repräsentiert.

1.2 Motivation

Um vertrauliche Informationen auszutauschen, ist die Verschlüsselung das Mittel der Wahl. Der Sender wird allgemein mit Alice, der Empfänger mit Bob bezeichnet. Werden während der Überbringung oder Übertragung die Daten von einem Dritten, oft Eve genannt, abgefangen bzw. mitgelesen, so kann dies bei der Wahl eines klassischen Übermittlungsweges nicht bemerkt werden, im Falle von quantenkryptographischen Methoden kann aber mit Hilfe von Vergleichen der Ergebnisse von Sender und Empfänger über statistische Methoden die Existenz von Eve nachgewiesen werden. In einem solchen Fall kann der ausgetauschte Schlüssel einfach verworfen werden, die Nachricht selbst wird demnach auch nicht übermittelt werden.

Mithilfe des sicher übertragenen Schlüssels kann nun auf öffentlichem Wege die chiffrierte Nachricht übermittelt werden. Für jeden, der nicht im Besitz des Schlüssels ist, ist die verschlüsselte Botschaft nicht lesbar und daher nutzlos.

1.3 Physikalische Grundlagen

Die quantenkryptographische Sicherheit kann mit Hilfe des BB84-Protokolls erreicht werden. Hier wird die Polarisationsrichtung von Photonen verwendet, um Informationen zu übertragen. Zunächst erzeugt Alice unpolarisierte Photonen mit Einzelphotonenquellen wie beispielsweise Quantenpunkten. Diese werden durch einen Polarisationsfilter geleitet, der die Photonen linear polarisiert. Die Richtung dieses Filters kann dabei in 45°-Schritten von 0 bis 135° eingestellt werden. Dabei stellen die Positionen bei null und 90 degree die Achsen eines „ungedrehten“, rechtwinkligen Koordinatensystems dar, während die Einstellung bei 45 und 135 degree die Achsen eines gedrehten, ebenfalls rechtwinkligen Koordinatensystems darstellen. Die beiden Koordinatensysteme repräsentieren jeweils eine Basis, bezüglich der die Polarisation der Photonen gemessen wird.

1.4 Versuchsaufbau

Literatur und Programme

[Skript] M. Scholz, Quantum Key Distribution via BB84 - An Advanced Lab Experiment, Humboldt-Universität, 2007