Institut für Physik der Humboldt-Universität zu Berlin

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

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 Polarisationen des zur Übertragung verwendeten Laserlichts repräsentiert.

1.2 Motivation

Um vertrauliche Informationen auszutauschen, ist die Verschlüsselung das Mittel der Wahl. Der Sender wird allgemeinhin 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° die Achsen eines „ungedrehten“, rechtwinkligen Koordinatensystems dar, während die Einstellung bei 45 und 135° die Achsen eines gedrehten, ebenfalls rechtwinkligen Koordinatensystems darstellen. Die beiden Koordinatensysteme repräsentieren jeweils eine Basis, bezüglich der die Polarisation der Photonen gemessen wird. Die konkrete Wahl der Basis von Alice wird zufällig eingestellt. Die polarisierten Photonen werden nun zu Bob geleitet, der das Licht ebenfalls mit einem Polarisationsfilter analysiert. Die Wahl der Basis von Bob erfolgt zufällig. Schließlich können die Photonen, die den Filter passiert haben, mit einem Detektor nachgewiesen werden.

Um aus den Messungen der Photonen einen Schlüssel zu erzeugen, vergleichen Alice und Bob die Wahlen ihrer Basen. Nur wenn beide zufällig die gleichen Basen gewählt haben, werden die in diesen Fällen gemessenen Werte weiter verwendet, da nur hier die Messergebnisse von Bob deterministisch sind und somit Informationen liefern können. Schließlich müssen sie sich einigen, welche der Achsen der beiden Basen von Alice einer Null bzw. einer Eins entsprechen. So können beide nur über den Vergleich der verwendeten Basis und insbesondere ohne den Vergleich der Messwerte einen Schlüssel konstruieren.

Wenn Eve versuchen würde, die Polarisation der von Alice gesendeten Photonen zu messen und

ein Photon gleicher Polarisation zu Bob zu senden, würde dies dadurch auffallen, dass Eve statistisch gesehen in der Hälfte der Fälle die falsche Basis gewählt hat und in diesen Fällen rein zufällige Messungen macht und daher in 50 % der Fälle falsch polarisiertes Licht zu Bob schickt. Alice und Bob können beispielsweise einen Teil ihres Schlüssels veröffentlichen und vergleichen, wie oft sie unterschiedliche Ergebnisse produziert haben, was geschehen würde, wenn Eve eine andere Basis als Alice und Bob gewählt hat. Wenn dies häufig der Fall ist, bedeutet dies, dass ihre Transaktion abgehört wurde.

1.4 Versuchsaufbau

Literatur und Programme

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