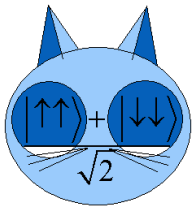
Theoretisch-Physikalisches Seminar
QuantenComputer – WS 2007/2008
Prof. Dr. Heiko Rieger mit Dr. Yu-Cheng Lin



Quantenkryptographie

Norbert Schaudinnus

Kryptographie ist noch vor der Zeit der Quantenmechanik gerade im Bereich des Militärs ein wichtiges Schlagwort: Die abhörsichere Übertragung von geheimen Nachrichten von A nach B ist jedoch klassisch gesehen nicht zu 100% sicher. Folgende spezielle Eigenschaften der Quantenmechanik erlauben jedoch die Konstruktion eines abhörsicheren Datenaustausches: Das No-Cloning Theorem sichert, dass es unmöglich ist, einen Quantenzustand zu kopieren. Außerdem äußert sich ein Abhörvorgang in einem Messprozess, der den quantenmechanischen Zustand eines Systems stört. Die Tatsache, dass Messprozesse unumkehrbar sind ist der letzte wichtige Punkt. Eine Datenübertragung ist damit nicht unbedingt abhörsicher gestaltbar, etwaige Störungen durch einen Lauschangriff äußern sich jedoch in widersprüchlichen Messergebnissen. Die Übertragung erfolgt wie auch in der klassischen Kryptographie über einen Schlüssel. Der quantenmechanische Teil besteht in der Konstruktion des Schlüssels über die sogenannte "Quantum Key Distribution". In diesem Verfahren lässt sich feststellen, ob während der Bereitstellung des Schlüssels ein Lauschangriff stattgefunden hat und der Schlüssel wird gegebenenfalls fallengelassen. Das bekannteste Verschlüsselungsprotokoll ist BB84, das auf der Übertragung über einen klassischen Kanal (der idealerweise zwar abhörbar aber nicht anfällig für Störsignale sein darf) und einem Kanal, der über Quantenkommunikation betrieben wird, beruht. In letzterem werden einzelne Photonen in zwei verschiedenen zufällig gewählten Basen von A nach B gesandt. Die Willkür der Wahl der Basen wird sich als Problempunkt für einen Lauschangriff erweisen. Das B92-Protokoll sieht eine Übertragung des Schlüssels in nur zwei nichtorthogonalen Zuständen: über Polaristationsfilter erfolgt die Messung der Zustände bei B. Analog zu BB84 existiert das 6-State Protokoll, dass Kommunikation über den Quantenkanal in drei Basen vorsieht Das Ekert-Protokoll (EPR-Protokoll) beruht auf dem EPR-Effekt.Grundliegender Unterschied zu den anderen Protokollen ist, dass eine Quelle verschränkte Photonen an A und B sendet, die dann unabhängig voneinander den Zustand ihres jeweiligen Photons messen. Diese Messungen stellen den Schlüssel dar, solange sie die Bell'sche Ungleichung verletzen (kein Lauschangriff vorliegt). Auch aus der Sicht des Eavesdroppers ergeben sich in der Quantenmechanik viele Möglichkeiten: Am naheliegendsten ist ein Eingriff in die Konversation zwischen A und B über die sogenannte Intercept-Resend-Strategie, in der ein Zustand in einer zufälligen Basis gemessen wird und in seiner so präparierten Form weitergeleitet wird. Dekohärentes Eavesdropping ist eine weitere Strategie. Der Lauschangriff im Falle von BB84 bedient sich einer "Zwischenbasis" die sich als Linearkombination der beiden Basen ausdrücken lässt. Kohärentes Eavesdropping bedient sich der Verschränkung.

Mi, 23.Jan.2008, 16-18 Uhr
E2.6 Seminarraum 4.18