



## **Master-/ Diplomarbeit**

### **Softwareentwicklung für ein Quantenkryptographieexperiment**

Die Quantenkryptographie ist eine Methode zur absolut sicheren Übermittlung von Nachrichten beruhend auf einigen Prinzipien der Quantenphysik. Sie ist ein sehr aktives Forschungsfeld und kann als Schnittstelle zwischen Quantenphysik, Informationstheorie und Informatik angesehen werden. Zur Übermittlung der Daten (vielmehr: des Schlüssels zum Verschlüsseln) werden einzelne Lichtteilchen benutzt. Man kann sich das Grundprinzip der Sicherheit in etwa so vorstellen, das bei einem Versuch des Abhörens diese einzelnen Lichtteilchen in einem Maße gestört werden, dass der Versuch nicht unentdeckt bleibt. Bei der Quantenkryptographie werden in einer ersten Phase die „Quantenbits“ in Form von Einzelphotonen zwischen Sender und Empfänger verschickt, bspw. über Glasfasern. In einer zweiten Phase der klassischen Kommunikation über eine Internetverbindung müssen dann bestimmte Messeinstellungen abgeglichen werden und zur Erhöhung der Sicherheit des Schlüssels die auf Kommunikation zwischen Sender- und Empfänger beruhenden Algorithmen der so genannten „error correction“ und „privacy amplification“ angewendet werden. Eine solche Quantenkryptographieeinheit, bestehend aus Sender und Empfänger, wird bei uns in der Gruppe aufgebaut.

Die ausgeschriebene Masterarbeit hat die Implementierung der klassischen Kommunikation zum Ziel. Dafür muss die Idee der angewendeten Algorithmen verstanden werden. Außerdem soll die Kommunikation zwischen Sender und Empfänger automatisiert werden.

Interessierte Studierende sollten durch Ihre Vorbildung in Informatik in der Lage sein, eigenständig die vorgegebenen Aufgaben der Programmierung zu bearbeiten.

Gerne erteilen wir weitere Informationen:

Matthias Leifgen  
Institut für Physik/ AG Nano-Optik  
Hausvogteiplatz 5-7  
10117 Berlin

Tel: (030) 2093-4842  
E-Mail: leifgen@physik.hu-berlin.de