Quantenkryptographie

Robert Meyer

16.07.2010.

Grundlagen

- Eine Verschlüsselte Übertragung besteht immer aus einem Verfahren, nach dem verschlüsselt wird und einen Schlüssel.
- Ein Beispiel ist die monoalphabetische Substitution. Das Verfahren besagt, dass jeder Buchstabe mit einem anderen ersetzt. Der Schluessel besagt, um wie viele Buchstaben man im Alphabet man witerzählen muss, um den verschlüsselten Buchstaben zu finden.
- Die Sicherheit der Verschlüsselung darf nicht davon abhängen, dass das Verfahren unbekannt ist.
- Formell ausgedrückt: $M^* = f(M, k)$, resp. $M = f^{-1}(M^*, k)$

Wann ist eine verschlüsselte Übertragung sicher

- Man kann aus der Informationstheorie herleiten, dass eine verschlüsselung unter den folgenden Bedingungen nicht entschlüsselt werden kann:
    1. Der Schlüssel muss ähnlich lang sein, wie die Nachricht
    2. Der Schlüssel darf nur einmal verwendet werden
    3. Der Schlüssel muss zufällig sein
    4. Der Schlüssel darf nur dem Empfänger und dem Absender bekannt sein
- Diese Verfahren sind als one-time-pad Verfahren bekannt
- Nur Punkt 4 ist heutzutage wirklich schwer zu gewährleisten. Aber hier kann die Quantenphysik helfen. Dafür braucht es allerdings einen kurzen Exkurs in die Quantenphysik.

Quantenmechanische Zustände

- In der klassischen Physik sind Zustände immer exakt bekannt.
- In der Quantenphysik ist der Zustand eines Teilchens nicht definiert.
- Das einzige, dass man weiss, ist die Wahrscheinlichkeit, dass ein Teilchen sich in einem Zustand befindet.
- Nach einer Messung befindet sich das System allerdings in eimem definierten Zustand.
- Das bedeutet, dass eine Messung immer auch das verändert, was man misst.

Verschränkte Teilchen I

- Unter bestimmten Voraussetzungen können Photonen erzeugt werden, die dieselbe Polarisation haben.
- Man kennt die Richtung der Polarisation nicht.
- Eine Messung an einem dieser Teilchen, bestimmt somit die Polarisation des anderen Teilchens, auch wenn dieses weit entfernt ist. Dies wird als nicht-lokales Verhalten bezeichnet.
- Dieses Verhalten wird beim sogenannten Ekert Verfahren ausgenutzt, um einen Schlüssel sicher auszutauschen.

Verschränkte Teilchen II

- Entdeckt wurde diese Sachverhalt von Einstein, Podolski und Rosen, und war ursprünglich als Argument gegen die Quantenphysik gedacht.
- Bell konnte aber 1964 aber eine Obergrenze für die Korrelation von Messwerten bei lokalen Theorien herleiten
- Es konnte experimentell belegt werden, dass diese Bellsche Ungleichung in der Quantenphysik verletzt wird. Die Quantenphys ist folglich nicht-lokal.

Das Ekert Verfahren I

- Beim Ekert Verfahren wird der zuerst über eine spezielle Leitung gemeinsam ein Schlüssel erstellt.
- Diese Leitung muss in der Lage sein einzelne Photonen zu transportieren, ohne deren Polarisation zu beeinflussen.
- Zudem braucht es einen Mechanismus, der zwei verschränkte Photonen erzeugt und an Alice und Bob verschickt.
- Alice und Bob messen nun die Polarisation ihres Photones in einer zufällig aus drei Richtungen ausgewählten Richtung.
- Über eine seperate Leitung tauschen sie untereinander ihre Messrichtungen aus.
- Allerdings muss sicher gestellt sein, dass wirklich Alice und Bob miteinander kommunizieren
- Wenn beide dieselbe Richtung gewählt haben, werden sie auch dasselbe Messergebnis erhalten.

Das Ekert Verfahren II

- Dieses kann zur erzeugung eines Schlüssels verwendet werden
- Wenn Eve die Verbindung abhört, wird die Verschränkung zwischen den Ergebnissen von Bob und Alice aufgehoben.
- Dies wird dann automatisch entdeck, da dann ja unterschiedliche Schlüssel erstellt werden.
- Zudem kann man an Hand der Messergebnisse überprüfen, ob die Bellsche Ungleichung verletzt wurde.
- Sind die beiden identischen Schlüssel erstellt, werden diese benutzt, um die Kommunikation zu verschlüsseln

Die Praxis

- In der Praxis ist dieses Verfahren sehr schwer einzusetzen.
- Man muss in der Lage sein zuverlässig einzelne Photonen zu messen.
- Man muss einzelne Photonen von A nach B transportieren, ohne die Polarisation zu beeinflussen.
- Da jede Messung den Zustand beeinflusst, können weder Verstärker noch switches eingesetzt werden. Man braucht eine point-to-point Verbindung.
- Aus diesen Gründen wird sich die Quantencryptographie wohl nur in ganz speziellen Situationen durchsetzen.
- Am letzten ccc gab es einen Vortrag, in dem gezeigt wurde, wie ein Schlüsselaustauch abgehört werden kann.
- Dabei wurde allerdings eine Schwäche in der Messung von Photonen ausgenutzt.