Beispiel zur Quantenkryptographie

Eines mehrerer Modelle sieht vor, zur Verschlüsselung das **One Time Pad-Verfahren** zu verwenden. Für jedes Klartextzeichen wird eine zufällige Folge gleich verteilter 0/1-Bits gewählt und zur Übertragung nach folgender Zuordnung als polarisierter Strom von Lichtteilchen (Photonen) gesendet:

Bit	horizontal	vertikal	+45 Grad	-45 Grad
0	ja		ja	
1		ja		ja

Die Ausrichtung des Polarisators lässt sich der Sender ebenfalls durch eine zufällige, gleich verteilte Folge von 0/1-Bits vorgeben. Auch der Empfänger wählt seine Polarisatorausrichtung nach einer solchen Zufallsfolge. Nach Abschluss der Übertragung gibt der Sender dem Empfänger seine Polarisator-Ausrichtung bekannt. **Alles läuft dabei öffentlich**. Stimmen die Polarisator-Ausrichtungen überein, sind die empfangenen Schlüsselbits korrekt, die anderen werden verworfen. Stimmen sie nämlich nicht überein, so sind die empfangenen Bits zur Hälfte **nicht vorhersagbar** falsch (Physik !):

Sendebits	1	0	0	1	0	1	1	1	0	0	1	0
Sende-Polarisation	+	+	x	+	x	x	x	+	+	+	x	x
Kanal												
Empfangs-Polarisation	+	x	x	x	+	x	+	x	x	+	x	x
Empfangsbits	1	0	0	0	0	1	0	1	0	0	1	0
sichere Bits nach Vergleich	**1**		**0**			**1**				**0**	**1**	**0**

Nun kann die Verschlüsselung erfolgen. Sitzt jedoch ein Angreifer als „man in the middle“ im Übertragungskanal, so befindet er sich in der gleichen Lage, wie der berechtigte Empfänger, mit einem entscheidenden Unterschied: Wenn er ein Photon empfangen hat, so ist dieses „verbraucht“, er muss ein neues erzeugen und dem Empfänger weiterleiten. Da er die vom Sender gewählte Polarisationsrichtung zu diesem Zeitpunkt noch nicht kennt, sendet er zur Hälfte falsche Bits. Nach Abgleich des Empfängers mit dem Sender über die gewählten Polarisationen ergibt sich in diesem Fall keine Gleichverteilung der 0/1-Bits, ein Indiz für einen technischen Fehler oder eine Manipulation: Der Übertragungskanal wird als unsicher verworfen:

Sendebits	1	0	0	1	0	1	1	1	0	0	1	0
Sende-Polarisation	+	+	x	+	x	x	x	+	+	+	x	x
Kanal												
Abhör-Polarisation	+	+	+	+	+	+	+	+	+	+	+	+
abgehörtes Bit	1	0	0	1	1	0	1	1	0	0	0	1
Sende-Polarisation	+	+	+	+	+	+	+	+	+	+	+	+
Kanal												
Empfangs-Polarisation	+	x	x	x	+	x	+	x	x	+	x	x
Empfangsbits	1	1	1	0	0	0	0	0	0	0	0	1
vermeintlich sichere Bits nach Vergleich	**1**		**1**			**0**		**0**		**0**	**0**	

In diesem Beispiel beträgt die Verteilung der 0/1-Bits nicht 50%, wie für eine ungestörte Übertragung zu erwarten ist, sondern 67%, der Empfänger teilt dem Sender mit, dass der Kanal unsicher ist und der Schlüssel nicht verwendet werden darf. - **Die Gefahren der Schlüsselübertragung sind bei einem solchen Ablauf praktisch restlos beseitigt.**