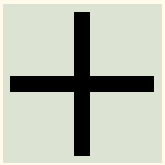
Quantenkryptografie – Absolut sichere Geheimnisse

B3 Verschlüsselung einer Nachricht

B4 Entschlüsselung einer Nachricht

diagonales Detektorschema



rektilineares Detektorschema

B5 Bobs Detektoren

Schon seit Jahrhunderten tobt ein weitgehend von der Öffentlichkeit unbeachteter Kampf um die Verschlüsselung von Informationen (**Kryptografie**) und deren Entschlüsselung (**Kryptoanalyse**). Im Augenblick liegt der Vorteil auf der Seite der Kryptografen: Das zur Zeit fortschrittlichste Verschlüsselungsverfahren RSA, das auf der Primfaktorzerlegung sehr großer Zahlen beruht, kann nach aktuellem Stand der Computertechnik nicht geknackt werden. Und zwar aus rein praktischen Gründen: Der Zeitaufwand, eine einzige Nachricht zu entschlüsseln, beliefe sich auf mehrere Jahrzehnte, wenn man weltweit alle Rechnerresourcen verwenden würde.

Doch durch die Entwicklung sehr leistungsfähiger Quantencomputer (→ **S. 113**), könnte man eine mittels RSA codierte Nachricht innerhalb weniger Minuten entschlüsseln. Ein absolut sicheres Verschlüsselungsverfahren wird nun benötigt. Dazu bietet sich die seit 1918 bekannte Vernam-Chiffre an (→ **B1**). Sie funktioniert wie folgt: Es wird ein binärer Zufallsschlüssel erstellt, der ein einziges Mal verwendet werden darf (**one-time pad**). Nur Sender (Alice) und Empfänger (Bob) besitzen diesen Schlüssel, der genauso lang sein muss wie der Klartext. Dann wird der Klartext in einen Binärcode übersetzt. Alice addiert nun den Zufallsschlüssel zum binären Klartext und übermittelt das Ergebnis. Bob kann mittels des Schlüssels den Originaltext wieder erlangen.

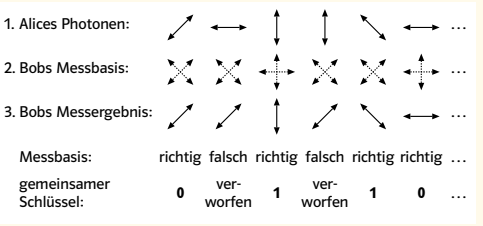
Klartext	P	H	Y	S	I	K
Ascii-Code	80	72	89	83	73	75
Binär	1010000	1001000	1011001	1010011	1001001	1001011
Zufallszahl	1100100	0011010	0100010	0111001	1100001	0010010
Addition	0110100	1010010	1111011	1101010	0101000	1011001
Ascii-Code	52	82	123	106	40	89
Geheimtext	4	R	{	j	(	Y

B1 Vernam-Chiffre

Für Dritte (Eve, von engl. eavesdropping = Lauschen), die den Text abfangen, handelt es sich um eine reine Zufallsfolge ohne den geringsten Informationsgehalt. Dieses absolut sichere Verfahren wird in der Praxis kaum angewendet. Es würde einen enormen Aufwand bedeuten, die nötige Anzahl von Schlüsseln zu erstellen und zu verteilen. Außerdem besteht die Gefahr, dass ein Schlüssel in die falschen Hände gerät.

Für dieses Problem stellt die Quantenkryptografie eine Lösung bereit. Sie erlaubt die Erzeugung und abhörsichere Übermittlung eines beliebig langen Zufallsschlüssels auf relativ einfache Art und Weise. Dazu benötigt man polarisierte Photonen (→ **S. 113**). Es wird folgende Vereinbarung getroffen: Photonen mit senkrechter oder diagonaler Polarisation stehen für eine Eins, Photonen mit waagerechter oder antidiagonaler Polarisation stehen für eine Null. Alice sendet eine zufällige Folge von polarisierten Photonen an Bob. Bob muss nun herausfinden, ob die Photonen in waagrechter, senkrechter, diagonaler oder antidiagonaler Polarisation vorliegen. Dazu besitzt er zwei verschiedene Detektoren (→ **B5**).

Der diagonale Detektor eignet sich zur Unterscheidung von diagonal und antidiagonal polarisiertem Licht, der rektilineare Detektor zur Unterscheidung von senkrecht und waagerecht polarisiertem Licht. Wird für ein Photon der falsche Detektor verwendet, gibt es ein zufälliges Messergebnis. Es ist im Folgenden unbrauchbar. Da Bob nicht weiß, welche Art von Photonen ihm Alice übermittelt, misst er zufällig mal mit dem einen und mal mit dem anderen Detektor. In etwa 50 % der Fälle verwendet er dabei zufällig den passenden Detektor. Im Anschluss zu dieser Messung teilt Alice Bob über einen offenen Kanal mit, welchen Detektor er jeweils hätte verwenden müssen, ohne jedoch dabei das Messergebnis preiszugeben. Die unbrauchbaren Messergebnisse werden verworfen, der Rest bildet den binären Zufallsschlüssel, der nur Bob und Alice bekannt ist (→ **B2**).



B2 Zufallsfolge von Alice und Bob

Dieses Verfahren ist absolut abhörsicher. Sollte Eve das Photon von Alice abfangen, muss sie, um an die Information zu gelangen, eine Messung durchführen. Dies führt nach den Gesetzen der Quantenmechanik zwangsläufig dazu, dass Eve das Photon durch die Messung verändert. Bob wird nun teilweise falsche Messwerte erhalten. Wenn nun Alice und Bob einen Teil ihres Zufallsschlüssels vergleichen, werden sie dies bemerken und Eve ist „aufgeflogen".

© Ernst Klett Verlag GmbH, Stuttgart, 2012