

# Quantenkryptographie

## Quantenkryptographie

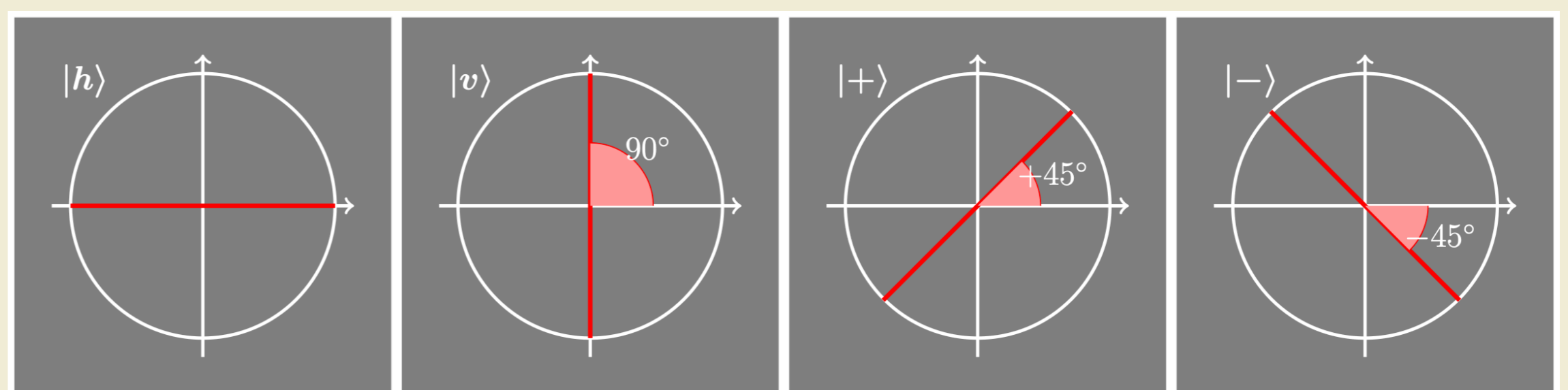
### – das BB84-Protokoll

Die Quantenkryptographie erlaubt eine sichere Übertragung von Nachrichten. Bei den meisten Verfahren (sogenannten „Protokollen“) werden Quanteneffekte allerdings nur genutzt, um einen Schlüssel zu erzeugen, von dem sich überprüfen lässt, ob er ausschließlich dem Sender und Empfänger bekannt ist.

Für den Schlüssel erzeugen Sender (Alice) und Empfänger (Bob) eine Zufallsfolge von 0 und 1. Dazu verwenden sie die quantentheoretischen Eigenschaften der Polarisationszustände von Photonen. Stellen sie dann fest, dass diese Zufallsfolge nur ihnen bekannt ist, verwenden sie das sogenannte One-Time-Pad (siehe „Kryptographie“) zur Verschlüsselung und Übertragung der Nachricht.

### Quantentheoretische Grundlagen

Ein unbekannter Quantenzustand (z. B. der Polarisationszustand eines einzelnen Photons) lässt sich nicht durch eine Messung bestimmen. Bestenfalls kann man für eine Messung eine Basis wählen (d. h. ein Paar orthogonaler Polarisationsmöglichkeiten) und erhält dann bezüglich dieser Basis einen Messwert. Wurde das Photon aber nicht in dieser Basis präpariert, ist der Messwert zufällig. Außerdem lässt sich der Quantenzustand eines Einzelsystems nicht kopieren (No-Cloning-Theorem). Wurde ein einzelnes Photon in einem der vier Polarisationszustände  $h$  (horizontal),  $v$  (vertikal),  $+$  (+45 Grad diagonal) oder  $-$  (-45 Grad diagonal) präpariert, kann man diesen Zustand nur dann bestimmen, wenn man in der passenden Basis, also der  $(h/v)$ -Basis oder der  $(+/-)$ -Basis, misst.



## Das Protokoll

Benannt ist das BB84-Protokoll nach seinen Erfindern Charles H. Bennett und Gilles Brassard und seinem Entstehungsjahr 1984.

Alice verschickt an Bob eine Folge von Photonen, deren Polarisationsrichtungen ( $h$ ,  $v$ ,  $+$ ,  $-$ ) jeweils zufällig gewählt wurden. Bob nimmt an diesen Photonen Polarisationsmessungen vor, wobei er zufällig die  $(h/v)$ - oder die  $(+/-)$ -Basis wählt. Anschließend vergleichen Alice und Bob über einen klassischen Kanal (z. B. ein Telefon) die Basen ihrer Polarisierungen (nur diese! – nicht die Polarisation selbst). In den Fällen, in denen die von Bob gewählte Basis mit der Basis, der von Alice verschickten Photonen, übereinstimmt, kennen sie die Polarisationszustände. Das ist bei rund der Hälfte der Photonen der Fall. Nach der Vorschrift in der  $(h/v)$ -Basis entspricht  $h$  der 0 und  $v$  der 1 und in der  $(+/-)$ -Basis entspricht  $+$  der 0 und  $-$  der 1. So erhalten sie eine Zufallsfolge von 0 und 1, die nur sie beide kennen.

### Der Lauschangriff

Ein möglicher Lauscher („Eve“, vom Englischen „eavesdropping“ = lauschen) kann an den Photonen von Alice ebenfalls nur zufällige Messungen der Polarisation vornehmen, da zu diesem Zeitpunkt die gewählten Basen noch nicht ausgetauscht wurden und ihm somit nicht bekannt sein können.

Dadurch ändert der Lauscher die Polarisation dieser Photonen aber ab, sofern er nicht dieselbe Basis wie Alice gewählt hat. Einige dieser Photonen haben somit nun nicht mehr die Polarisation, die Alice ihnen gegeben hat. Das kann man dadurch feststellen, dass Alice und Bob einen Teil der vermeintlich gemeinsamen Zufallsfolge von 0 und 1 öffentlich vergleichen. Man kann zeigen, dass im Mittel jedes vierte Bit in dieser Folge nicht übereinstimmt. Wenn Alice und Bob dies feststellen, wurde ihr Schlüsselaustausch vermutlich abgehört; diesen Schlüssel sollten sie dann nicht verwenden. Alice und Bob sollten also wesentlich mehr gemeinsame Bits erzeugen, als für den Schlüssel notwendig ist, sodass sie die Sicherheit des Schlüssels überprüfen können.

### Zusammenfassung

Alice	1 1 0 1 1 1 0 0 0 1 0 1 0 1 1	+ x + + x x + x + + x x + +	Information	0	1
Öffentlich		⊕ ⊗ ⊗ ⊕ ⊗ ⊗ ⊗ ⊗ ⊗ ⊕ ⊗ ⊕ ⊗ ⊗ ⊕		+	⊕ ⊕
Bob	+ + + x + x x x + x x + + x x + +	⊕ ⊕ ⊗ ⊗ ⊗ ⊗ ⊗ ⊗ ⊕ ⊗ ⊗ ⊕ ⊗ ⊗ ⊕	Polarisationspaare	x	⊗ ⊗
	1 1 0 0 0 1 0 1 1 0 1 1 0 1 1				

Alice	1 1 0 1 1 1 0 0 0 1 0 1 0 1 1
Öffentlich	+ x + + x x + x + + x x + +
Bob	+ + + x + x x x + x x + + x x + +
	1 1 0 0 0 1 0 1 1 0 1 1 0 1 1

Im Video zum BB84-Protokoll bezeichnet „+“ die  $(h/v)$ -Basis und „x“ die  $(+/-)$ -Basis.

