

# Quantum Key Distribution

## Quantenmechanik in der Kryptographie

Kaniuar Bacho

TÜV Informationstechnik

October 6, 2022

- 1 Asymmetrische Kryptographie vs QKD
- 2 Physikalische Vorkenntnisse (Polarisation)
- 3 QKD-Systeme und BB84-Protokoll
- 4 Seitenkanalangriffe

- Um Informationen vertraulich auszutauschen, einigen sich zwei Parteien mittels asymmetrischer Kryptographie auf einen gemeinsamen geheimen Schlüssel, um die Kommunikation mit symmetrischen Verschlüsselungsverfahren (z.B. AES) fortzuführen.

- Um Informationen vertraulich auszutauschen, einigen sich zwei Parteien mittels asymmetrischer Kryptographie auf einen gemeinsamen geheimen Schlüssel, um die Kommunikation mit symmetrischen Verschlüsselungsverfahren (z.B. AES) fortzuführen.
- Ein Beispiel hierfür ist RSA oder der Diffie-Hellman-Schlüsselaustausch.

- Um Informationen vertraulich auszutauschen, einigen sich zwei Parteien mittels asymmetrischer Kryptographie auf einen gemeinsamen geheimen Schlüssel, um die Kommunikation mit symmetrischen Verschlüsselungsverfahren (z.B. AES) fortzuführen.
- Ein Beispiel hierfür ist RSA oder der Diffie-Hellman-Schlüsselaustausch.
- **Angriffsvektoren** bei asymmetrischer Kryptographie:

- Um Informationen vertraulich auszutauschen, einigen sich zwei Parteien mittels asymmetrischer Kryptographie auf einen gemeinsamen geheimen Schlüssel, um die Kommunikation mit symmetrischen Verschlüsselungsverfahren (z.B. AES) fortzuführen.
- Ein Beispiel hierfür ist RSA oder der Diffie-Hellman-Schlüsselaustausch.
- **Angriffsvektoren** bei asymmetrischer Kryptographie:
  - ▶ Je mehr Rechenleistung, desto schneller kann man die geheimen Schlüssel bruteforcen.

- Um Informationen vertraulich auszutauschen, einigen sich zwei Parteien mittels asymmetrischer Kryptographie auf einen gemeinsamen geheimen Schlüssel, um die Kommunikation mit symmetrischen Verschlüsselungsverfahren (z.B. AES) fortzuführen.
- Ein Beispiel hierfür ist RSA oder der Diffie-Hellman-Schlüsselaustausch.
- **Angriffsvektoren** bei asymmetrischer Kryptographie:
  - ▶ Je mehr Rechenleistung, desto schneller kann man die geheimen Schlüssel bruteforcen.
  - ▶ Neue effizientere mathematische Algorithmen, um Sicherheitsniveau zu vermindern. Darunter auch Quantenalgorithmen, wie der Shor-Algorithmus.

- Um Informationen vertraulich auszutauschen, einigen sich zwei Parteien mittels asymmetrischer Kryptographie auf einen gemeinsamen geheimen Schlüssel, um die Kommunikation mit symmetrischen Verschlüsselungsverfahren (z.B. AES) fortzuführen.
- Ein Beispiel hierfür ist RSA oder der Diffie-Hellman-Schlüsselaustausch.
- **Angriffsvektoren** bei asymmetrischer Kryptographie:
  - ▶ Je mehr Rechenleistung, desto schneller kann man die geheimen Schlüssel bruteforcen.
  - ▶ Neue effizientere mathematische Algorithmen, um Sicherheitsniveau zu vermindern. Darunter auch Quantenalgorithmen, wie der Shor-Algorithmus.

Protokolle basierend auf asym. Krypto. sind bloß *computationally secure*.



- Um Informationen vertraulich auszutauschen, einigen sich zwei Parteien mittels asymmetrischer Kryptographie auf einen gemeinsamen geheimen Schlüssel, um die Kommunikation mit symmetrischen Verschlüsselungsverfahren (z.B. AES) fortzuführen.
- Ein Beispiel hierfür ist RSA oder der Diffie-Hellman-Schlüsselaustausch.
- **Angriffsvektoren** bei asymmetrischer Kryptographie:
  - ▶ Je mehr Rechenleistung, desto schneller kann man die geheimen Schlüssel bruteforcen.
  - ▶ Neue effizientere mathematische Algorithmen, um Sicherheitsniveau zu vermindern. Darunter auch Quantenalgorithmen, wie der Shor-Algorithmus.

Protokolle basierend auf asym. Krypto. sind bloß *computationally secure*.

⇒ Was jetzt sicher ist, wird bald nicht mehr sicher sein!

- QKD hingegen basiert nicht auf einem mathematischem Problem, welches die Rechenleistung als einzige Grenze setzt.

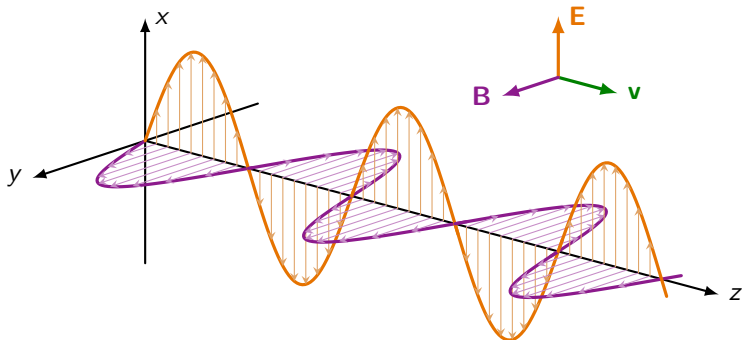
- QKD hingegen basiert nicht auf einem mathematischem Problem, welches die Rechenleistung als einzige Grenze setzt.  
Die Grenzen werden hier allein durch das physikalisch Mögliche gesetzt!

- QKD hingegen basiert nicht auf einem mathematischem Problem, welches die Rechenleistung als einzige Grenze setzt.  
Die Grenzen werden hier allein durch das physikalisch Mögliche gesetzt!
- In der asym. Krypto. könnte ein Angreifer sich den privaten Schlüssel noch theoretisch herleiten, da der öffentliche Schlüssel dazu ausreicht (Shor-Algorithmus).  
QKD besitzt diesen Nachteil nicht.

- QKD hingegen basiert nicht auf einem mathematischem Problem, welches die Rechenleistung als einzige Grenze setzt.  
Die Grenzen werden hier allein durch das physikalisch Mögliche gesetzt!
- In der asym. Krypto. könnte ein Angreifer sich den privaten Schlüssel noch theoretisch herleiten, da der öffentliche Schlüssel dazu ausreicht (Shor-Algorithmus). QKD besitzt diesen Nachteil nicht.
- Insbesondere kann die Quantenphysik die Gegenwart eines Angreifers feststellen, was vorher nicht möglich war.

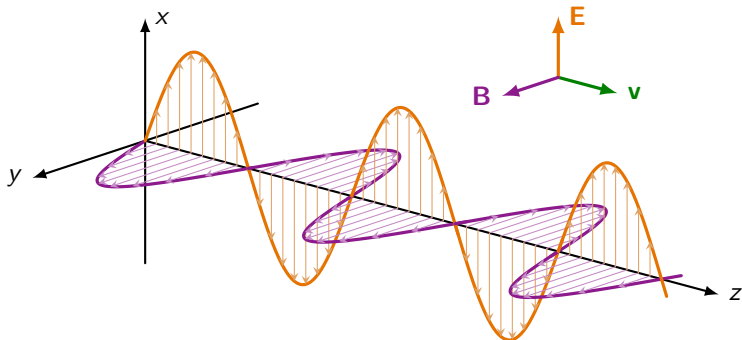
# Polarisation von Licht

- Die Polarisation von Licht ist die Ausbreitung des elektrischen Feldes (hier in Orange):



# Polarisation von Licht

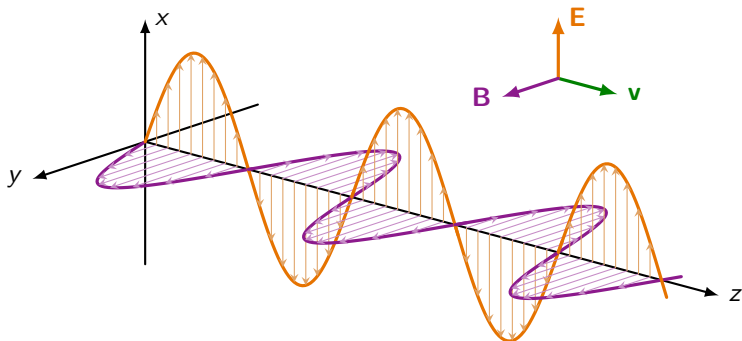
- Die Polarisation von Licht ist die Ausbreitung des elektrischen Feldes (hier in Orange):



- Die Ausbreitung hier ist orthogonal zur yz-Ebene. Wir sprechen von einer *vertikalen Polarisation*.

# Polarisation von Licht

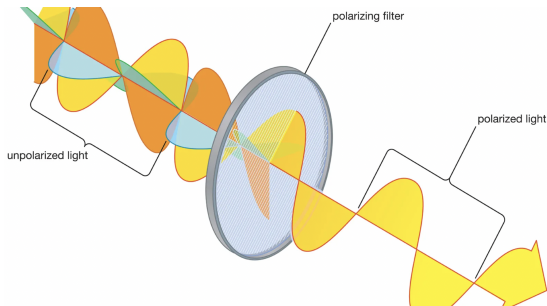
- Die Polarisation von Licht ist die Ausbreitung des elektrischen Feldes (hier in Orange):



- Die Ausbreitung hier ist orthogonal zur  $yz$ -Ebene. Wir sprechen von einer *vertikalen Polarisation*.
- Jede Rotation  $\theta$  um die  $z$ -Achse kann als Polarisation auftreten.

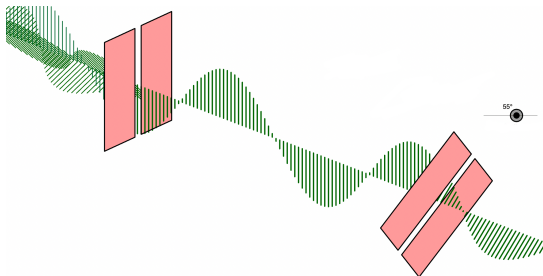


- Licht in der Natur besitzt i.d.R. mehrere Polarisationen auf einmal, man spricht von *unpolarisiertem Licht*.

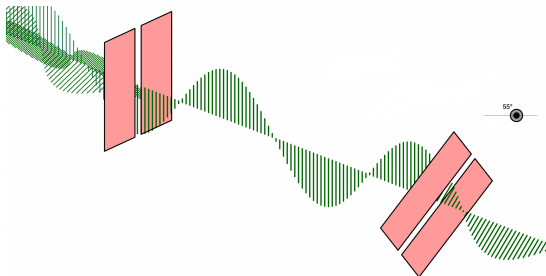


- Der *Polarisator* fungiert als Filter, um Licht einer bestimmten Polarisation zu erzeugen.

- Das Gesetz von Malus beschreibt die Intensität einer polarisierten Welle nach dem Durchgang eines Polarisators in Abhängigkeit vom Winkel  $\theta$ . Diese wird um den Faktor  $\cos(\theta)^2$  vermindert.



- Das Gesetz von Malus beschreibt die Intensität einer polarisierten Welle nach dem Durchgang eines Polarisators in Abhängigkeit vom Winkel  $\theta$ . Diese wird um den Faktor  $\cos(\theta)^2$  vermindert.



- Durch eine Messung wird gleichzeitig der polarisierte Zustand verändert!

# Anschauliches Beispiel

- Polarisator filtert horizontal polarisiertes Licht:



# Anschauliches Beispiel

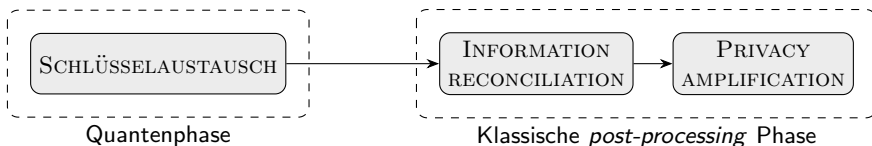
- Polarisator filtert horizontal polarisiertes Licht:



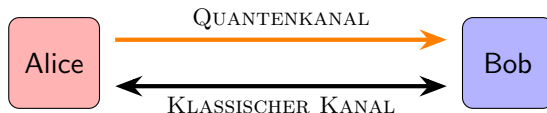
- Da die Winkel der Polarisatoren  $\theta = 90^\circ$  zueinander sind, kommt nach Malus' Gesetz kein Licht durch:



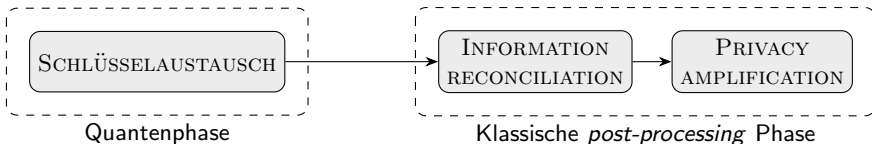
- QKD-Systeme auf Protokoll-Ebene:



- Benötigte Kanäle für Informationsaustausch:



- QKD-Systeme auf Protokoll-Ebene:



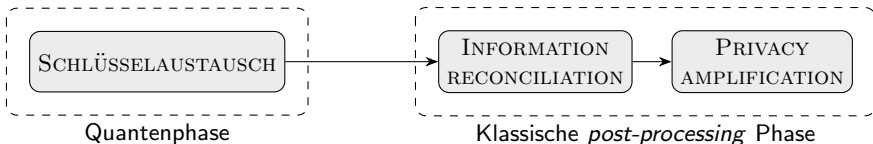
- Benötigte Kanäle für Informationsaustausch:



- Quantenphase:

Alice möchte ihre Bits mittels quantenmechanischen Zuständen (z.B. Polarisierung von Licht) codieren und dieses physikalische Medium (z.B. Photonen) übersenden, s.d. Bob es wieder decodieren kann.

- QKD-Systeme auf Protokoll-Ebene:



- Benötigte Kanäle für Informationsaustausch:




- Post-processing Phase:  
Fehler können bei der Übertragung auftreten (durch Angreifer oder technologischen Umständen). Diese werden durch *Error-Correction-Protokolle* korrigiert. Zuletzt wird ein Protokoll benutzt, was die Schlüssel hasht, s.d. der Informationsgehalt des Angreifers auf nahezu Null reduziert wird.




- Bennett und Brassard stellten 1984 das erste QKD-Protokoll vor.







- Bennett und Brassard stellten 1984 das erste QKD-Protokoll vor.

- Wir benutzen zwei Basen für die Polarisation von Photonen:

Standardbasis: 

Diagonalebasis: 

Mit folgender Codierungsvorschrift:

Basis	0	1
		
		

- Bennett und Brassard stellten 1984 das erste QKD-Protokoll vor.

- Wir benutzen zwei Basen für die Polarisierung von Photonen:

Standardbasis:  $\leftrightarrow$

Diagonalebasis:  $\nwarrow \nearrow$

Mit folgender Codierungsvorschrift:

Basis	0	1
$\leftrightarrow$	$\leftrightarrow$	$\updownarrow$
$\nwarrow \nearrow$	$\nearrow$	$\nwarrow$

- Alice's zufällige Bits: 1 0 0 1 0 0
- Alice's zufällige Basen:  $\leftrightarrow$   $\nwarrow \nearrow$   $\leftrightarrow$   $\leftrightarrow$   $\nwarrow \nearrow$   $\leftrightarrow$

- Bennett und Brassard stellten 1984 das erste QKD-Protokoll vor.

- Wir benutzen zwei Basen für die Polarisierung von Photonen:

Standardbasis:  $\updownarrow$

Diagonalbasis:  $\nwarrow \nearrow$

Mit folgender Codierungsvorschrift:

Basis	0	1
$\updownarrow$	$\longleftrightarrow$	$\updownarrow$
$\nwarrow \nearrow$	$\nearrow$	$\nwarrow$

1. Alice's zufällige Bits:	1	0	0	1	0	0
2. Alice's zufällige Basen:	$\updownarrow$	$\nwarrow \nearrow$	$\updownarrow$	$\updownarrow$	$\nwarrow \nearrow$	$\updownarrow$
3. Codierte Photonen:	$\updownarrow$	$\nearrow$	$\longleftrightarrow$	$\updownarrow$	$\nearrow$	$\longleftrightarrow$

- Bennett und Brassard stellten 1984 das erste QKD-Protokoll vor.

- Wir benutzen zwei Basen für die Polarisation von Photonen:

Standardbasis:  $\updownarrow$

Diagonalebasis:  $\nearrow\searrow$

Mit folgender Codierungsvorschrift:

Basis	0	1
$\updownarrow$	$\longleftrightarrow$	$\updownarrow$
$\nearrow\searrow$	$\nearrow$	$\searrow$

1.	Alice's zufällige Bits:	1	0	0	1	0	0
2.	Alice's zufällige Basen:	$\updownarrow$	$\nearrow\searrow$	$\updownarrow$	$\updownarrow$	$\nearrow\searrow$	$\updownarrow$
3.	Codierte Photonen:	$\updownarrow$	$\nearrow$	$\longleftrightarrow$	$\updownarrow$	$\nearrow$	$\longleftrightarrow$
4.	Bobs zufällige Basen:	$\updownarrow$	$\nearrow\searrow$	$\nearrow\searrow$	$\nearrow\searrow$	$\nearrow\searrow$	$\updownarrow$

- Bennett und Brassard stellten 1984 das erste QKD-Protokoll vor.

- Wir benutzen zwei Basen für die Polarisation von Photonen:

Standardbasis:  $\updownarrow$

Diagonalebasis:  $\nearrow\searrow$

Mit folgender Codierungsvorschrift:

Basis	0	1
$\updownarrow$	$\longleftrightarrow$	$\updownarrow$
$\nearrow\searrow$	$\nearrow$	$\searrow$

1. Alice's zufällige Bits:	1	0	0	1	0	0
2. Alice's zufällige Basen:	$\updownarrow$	$\nearrow\searrow$	$\updownarrow$	$\updownarrow$	$\nearrow\searrow$	$\updownarrow$
3. Codierte Photonen:	$\updownarrow$	$\nearrow$	$\longleftrightarrow$	$\updownarrow$	$\nearrow$	$\longleftrightarrow$
4. Bobs zufällige Basen:	$\updownarrow$	$\nearrow\searrow$	$\nearrow\searrow$	$\nearrow\searrow$	$\nearrow\searrow$	$\updownarrow$
5. Bobs Messungen:	$\updownarrow$	$\nearrow$	$\searrow$	$\searrow$	$\nearrow$	$\longleftrightarrow$

- Bennett und Brassard stellten 1984 das erste QKD-Protokoll vor.

- Wir benutzen zwei Basen für die Polarisation von Photonen:

Standardbasis:  $\updownarrow$

Diagonalbasis:  $\nwarrow \nearrow$

Mit folgender Codierungsvorschrift:

Basis	0	1
$\updownarrow$	$\longleftrightarrow$	$\updownarrow$
$\nwarrow \nearrow$	$\nearrow$	$\nwarrow$

1.	Alice's zufällige Bits:	1	0	0	1	0	0
2.	Alice's zufällige Basen:	$\updownarrow$	$\nwarrow \nearrow$	$\updownarrow$	$\updownarrow$	$\nwarrow \nearrow$	$\updownarrow$
3.	Codierte Photonen:	$\updownarrow$	$\nearrow$	$\longleftrightarrow$	$\updownarrow$	$\nearrow$	$\longleftrightarrow$
4.	Bobs zufällige Basen:	$\updownarrow$	$\nwarrow \nearrow$	$\nwarrow \nearrow$	$\nwarrow \nearrow$	$\nwarrow \nearrow$	$\updownarrow$
5.	Bobs Messungen:	$\updownarrow$	$\nearrow$	$\nwarrow$	$\nwarrow$	$\nearrow$	$\longleftrightarrow$
6.	Bobs Bits:	1	0	1	1	0	0

- Bennett und Brassard stellten 1984 das erste QKD-Protokoll vor.

- Wir benutzen zwei Basen für die Polarisation von Photonen:

Standardbasis:  $\updownarrow$

Diagonalbasis:  $\nwarrow \nearrow$

Mit folgender Codierungsvorschrift:

Basis	0	1
$\updownarrow$	$\longleftrightarrow$	$\updownarrow$
$\nwarrow \nearrow$	$\nearrow$	$\nwarrow$

1.	Alice's zufällige Bits:	1	0	0	1	0	0
2.	Alice's zufällige Basen:	$\updownarrow$	$\nwarrow \nearrow$	$\updownarrow$	$\updownarrow$	$\nwarrow \nearrow$	$\updownarrow$
3.	Codierte Photonen:	$\updownarrow$	$\nearrow$	$\longleftrightarrow$	$\updownarrow$	$\nearrow$	$\longleftrightarrow$
4.	Bobs zufällige Basen:	$\updownarrow$	$\nwarrow \nearrow$	$\nwarrow \nearrow$	$\nwarrow \nearrow$	$\nwarrow \nearrow$	$\updownarrow$
5.	Bobs Messungen:	$\updownarrow$	$\nearrow$	$\nwarrow$	$\nwarrow$	$\nearrow$	$\longleftrightarrow$
6.	Bobs Bits:	1	0	1	1	0	0
7.	Basisabgleich:	OK	OK			OK	OK



- Bennett und Brassard stellten 1984 das erste QKD-Protokoll vor.

- Wir benutzen zwei Basen für die Polarisisation von Photonen:

Standardbasis:  $\updownarrow$

Diagonalbasis:  $\nwarrow \nearrow$

Mit folgender Codierungsvorschrift:

Basis	0	1
$\updownarrow$	$\longleftrightarrow$	$\updownarrow$
$\nwarrow \nearrow$	$\nearrow$	$\nwarrow$

1.	Alice's zufällige Bits:	1	0	0	1	0	0
2.	Alice's zufällige Basen:	$\updownarrow$	$\nwarrow \nearrow$	$\updownarrow$	$\updownarrow$	$\nwarrow \nearrow$	$\updownarrow$
3.	Codierte Photonen:	$\updownarrow$	$\nearrow$	$\longleftrightarrow$	$\updownarrow$	$\nearrow$	$\longleftrightarrow$
4.	Bobs zufällige Basen:	$\updownarrow$	$\nwarrow \nearrow$	$\nwarrow \nearrow$	$\nwarrow \nearrow$	$\nwarrow \nearrow$	$\updownarrow$
5.	Bobs Messungen:	$\updownarrow$	$\nearrow$	$\nwarrow$	$\nwarrow$	$\nearrow$	$\longleftrightarrow$
6.	Bobs Bits:	1	0	1	1	0	0
7.	Basisabgleich:	OK	OK			OK	OK
8.	Gemeinsamer Schlüssel(?):	1	0			0	0

- Bennett und Brassard stellten 1984 das erste QKD-Protokoll vor.

- Wir benutzen zwei Basen für die Polarisation von Photonen:

Standardbasis:  $\updownarrow$

Diagonalbasis:  $\nwarrow \nearrow$

Mit folgender Codierungsvorschrift:

Basis	0	1
$\updownarrow$	$\longleftrightarrow$	$\updownarrow$
$\nwarrow \nearrow$	$\nearrow$	$\nwarrow$

1.	Alice's zufällige Bits:	1	0	0	1	0	0
2.	Alice's zufällige Basen:	$\updownarrow$	$\nwarrow \nearrow$	$\updownarrow$	$\updownarrow$	$\nwarrow \nearrow$	$\updownarrow$
3.	Codierte Photonen:	$\updownarrow$	$\nearrow$	$\longleftrightarrow$	$\updownarrow$	$\nearrow$	$\longleftrightarrow$
4.	Bobs zufällige Basen:	$\updownarrow$	$\nwarrow \nearrow$	$\nwarrow \nearrow$	$\nwarrow \nearrow$	$\nwarrow \nearrow$	$\updownarrow$
5.	Bobs Messungen:	$\updownarrow$	$\nearrow$	$\nwarrow$	$\nwarrow$	$\nearrow$	$\longleftrightarrow$
6.	Bobs Bits:	1	0	1	1	0	0
7.	Basisabgleich:	OK	OK			OK	OK
8.	Gemeinsamer Schlüssel(?):	1	0			0	0
9.	Bob enthüllt zufällige Bits:	1					0

- Bennett und Brassard stellten 1984 das erste QKD-Protokoll vor.

- Wir benutzen zwei Basen für die Polarisisation von Photonen:

Standardbasis:  $\updownarrow$

Diagonalbasis:  $\nwarrow \nearrow$

Mit folgender Codierungsvorschrift:

Basis	0	1
$\updownarrow$	$\longleftrightarrow$	$\updownarrow$
$\nwarrow \nearrow$	$\nearrow$	$\nwarrow$

1.	Alice's zufällige Bits:	1	0	0	1	0	0
2.	Alice's zufällige Basen:	$\updownarrow$	$\nwarrow \nearrow$	$\updownarrow$	$\updownarrow$	$\nwarrow \nearrow$	$\updownarrow$
3.	Codierte Photonen:	$\updownarrow$	$\nearrow$	$\longleftrightarrow$	$\updownarrow$	$\nearrow$	$\longleftrightarrow$
4.	Bobs zufällige Basen:	$\updownarrow$	$\nwarrow \nearrow$	$\nwarrow \nearrow$	$\nwarrow \nearrow$	$\nwarrow \nearrow$	$\updownarrow$
5.	Bobs Messungen:	$\updownarrow$	$\nearrow$	$\nwarrow$	$\nwarrow$	$\nearrow$	$\longleftrightarrow$
6.	Bobs Bits:	1	0	1	1	0	0
7.	Basisabgleich:	OK	OK			OK	OK
8.	Gemeinsamer Schlüssel(?):	1	0			0	0
9.	Bob enthüllt zufällige Bits:	1					0
10.	Alice bestätigt:	OK					OK

- Bennett und Brassard stellten 1984 das erste QKD-Protokoll vor.

- Wir benutzen zwei Basen für die Polarisation von Photonen:




























Standardbasis:  $\updownarrow$

Diagonalbasis:  $\nwarrow \nearrow$

Mit folgender Codierungsvorschrift:

Basis	0	1
$\updownarrow$	$\longleftrightarrow$	$\updownarrow$
$\nwarrow \nearrow$	$\nearrow$	$\nwarrow$

1.	Alice's zufällige Bits:	1	0	0	1	0	0
2.	Alice's zufällige Basen:	$\updownarrow$	$\nwarrow \nearrow$	$\updownarrow$	$\updownarrow$	$\nwarrow \nearrow$	$\updownarrow$
3.	Codierte Photonen:	$\updownarrow$	$\nearrow$	$\longleftrightarrow$	$\updownarrow$	$\nearrow$	$\longleftrightarrow$
4.	Bobs zufällige Basen:	$\updownarrow$	$\nwarrow \nearrow$	$\nwarrow \nearrow$	$\nwarrow \nearrow$	$\nwarrow \nearrow$	$\updownarrow$
5.	Bobs Messungen:	$\updownarrow$	$\nearrow$	$\nwarrow$	$\nwarrow$	$\nearrow$	$\longleftrightarrow$
6.	Bobs Bits:	1	0	1	1	0	0
7.	Basisabgleich:	OK	OK			OK	OK
8.	Gemeinsamer Schlüssel(?):	1	0			0	0
9.	Bob enthüllt zufällige Bits:	1					0
10.	Alice bestätigt:	OK					OK
11.	Gemeinsamer Schlüssel(!):		0			0	

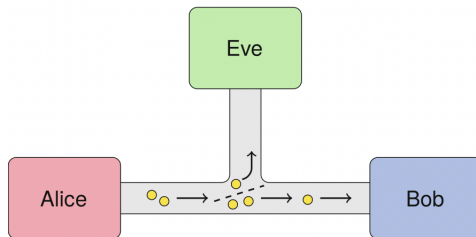
Codierungsvorschrift:		Basis	0	1		
						
						
1.	Alice's zufällige Bits:		1	0	1	0
2.	Alice's zufällige Basen:					
3.	Codierte Photonen:					
Eves zufällige Basen:						
Eves Messungen:						
4.	Bobs zufällige Basen:					
5.	Bobs Messungen:					
6.	Bobs Bits:		1	0	0	0
7.	Basisabgleich:		OK	OK	OK	OK
8.	Gemeinsamer Schlüssel(?):		1	0	0	0
9.	Bob enthüllt zufällige Bits:		1		0	
10.	Alice bestätigt:		OK			
11.	Gemeinsamer Schlüssel(!):			0		

- Es gibt eine Vielzahl an Seitenkanalangriffen.

- Es gibt eine Vielzahl an Seitenkanalangriffen.
- BB84 erfordert genau ein Photon für jedes Bit. In der Praxis ist dies kaum möglich aus einer einzigen Quelle, s.d. mehrere Photonen gleichzeitig geschickt werden.

# Seitenkanalangriffe: Photon-number-splitting attack

- Es gibt eine Vielzahl an Seitenkanalangriffen.
- BB84 erfordert genau ein Photon für jedes Bit. In der Praxis ist dies kaum möglich aus einer einzigen Quelle, s.d. mehrere Photonen gleichzeitig geschickt werden.
- *Photon-number-splitting attack:*



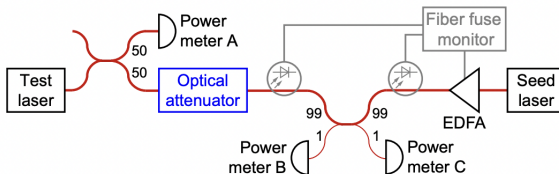


- Um einzelne Photonen zu erhalten, wird ein optisches Dämpfungsglied benutzt.

- Um einzelne Photonen zu erhalten, wird ein optisches Dämpfungsglied benutzt.
- Dieses Dämpfungsglied kann man jedoch mit einem starken Laser beschießen und zerstören.

# Seitenkanalangriffe: Laser-damage attack

- Um einzelne Photonen zu erhalten, wird ein optisches Dämpfungsglied benutzt.
- Dieses Dämpfungsglied kann man jedoch mit einem starken Laser beschießen und zerstören.
- *Laser-damage attack:*



Danke für die Aufmerksamkeit!  
Gibt es Fragen?