Quantenkryptographie für die Schule

am Beispiel von BB84

Überblick

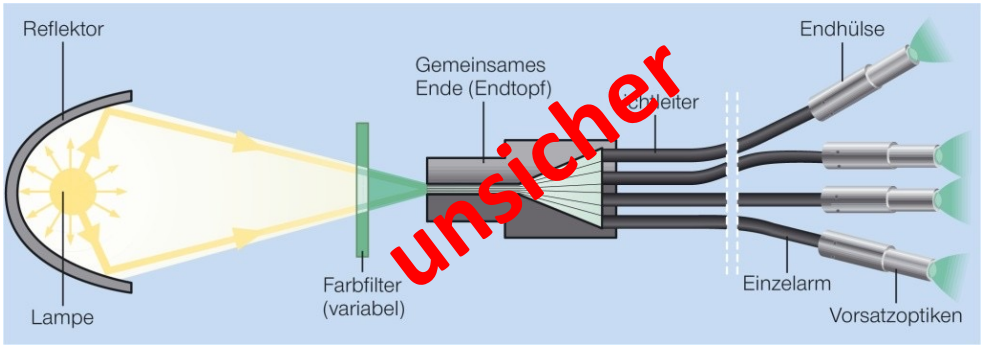
- Informationsübertragung mit Licht
- Verschlüsselung
- Rolle des Zufalls
- Schlüsselerzeugung nach BB84
- Workshop, Unterrichtsszenarios und Diskussion

Informationsübertragung mit Licht

- Licht als klassischer Informationsüberträger
  - Lichtmorsen, Flaggensignale, Optischer Telegraf
  - Unverschlüsselter Broadcast

unsicher

- Licht als moderner Informationsüberträger
  - Lichtleiter als „geschlossener“ Kanal

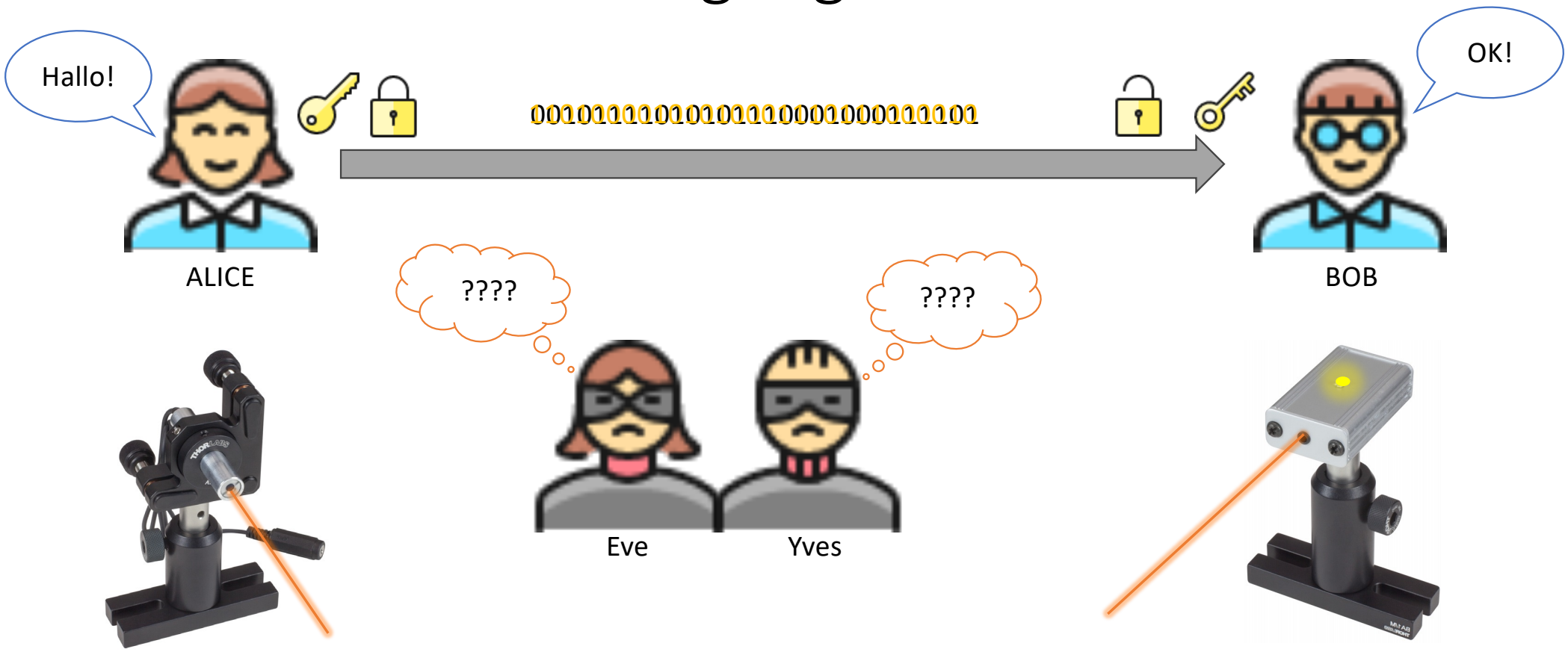


unsicher

Quelle: https://www.wissen.de/lexikon/lichtwellenleiter

Quelle: http://www.vierte-flottille.de/roberto.roth/lichtmorsen/lichtmorsen.html

Informationsübertragung mit Licht



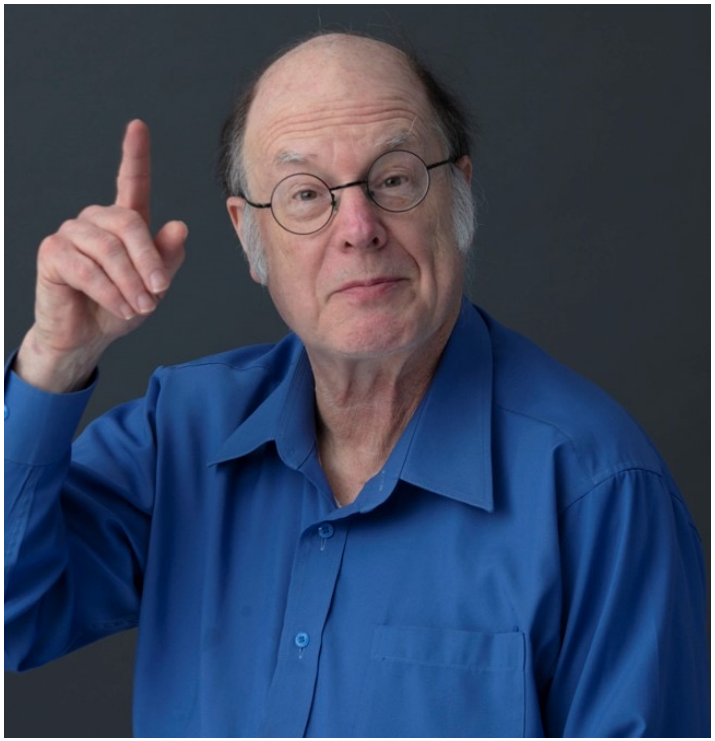
Verschlüsselung

- Es gibt keine sicheren Übertragungswege!
- Grundidee der Kryptographie:
  - Alle übertragenen Daten sind verschlüsselt
  - Verschlüsselungsverfahren ist öffentlich
  - Sicherheit ergibt sich NUR aus den Schlüsseln (Prinzip von Kerckhoff)
    - Schlüssel kann jedes von Alice und Bob geteilte Geheimnis sein
    - Alice benutzt einen Chiffrierschlüssel, Bob den komplementären Dechiffrierschlüssel
    - eine zufällige Folge von 0 und 1 ist ein guter Schlüssel
    - Schlüssel sollten oft gewechselt werden
    - Klassischer Schlüsseltausch erfordert Aufwand
    - Moderne Kryptographie ersetzt den Schlüsseltausch durch Schlüsselerzeugung
- Schlüsselstärke beruht (heute) auf mathematischen „Einwegfunktionen“
  - z.B.: Multiplizieren ist leicht, Faktorisieren ist schwer (RSA)

Verschlüsselung

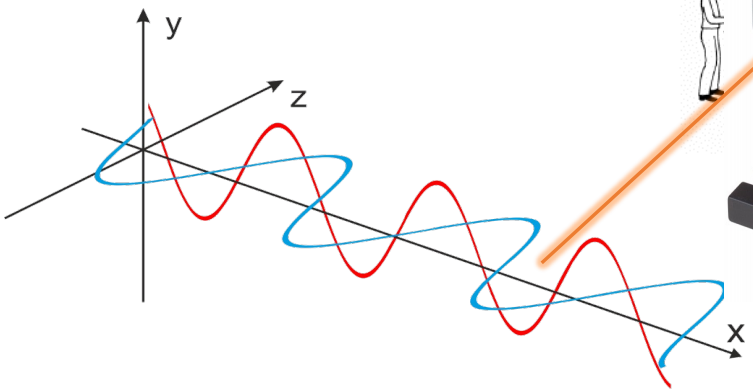
- Vorschlag von Bennett und Brassard (BB84):
  - Schlüsselpaar als zufällige Folge von 0 und 1 wird bei Alice und Bob zeitgleich erzeugt (key generation)
  - Alle Information zur Schlüsselerzeugung werden über offene Kanäle übertragen
  - Abhören der Daten erlaubt Eve&Yves keinen Rückschluss auf den generierten Schlüssel (zero knowledge)
  - Abhörversuch von Eve&Yves kann entdeckt werden

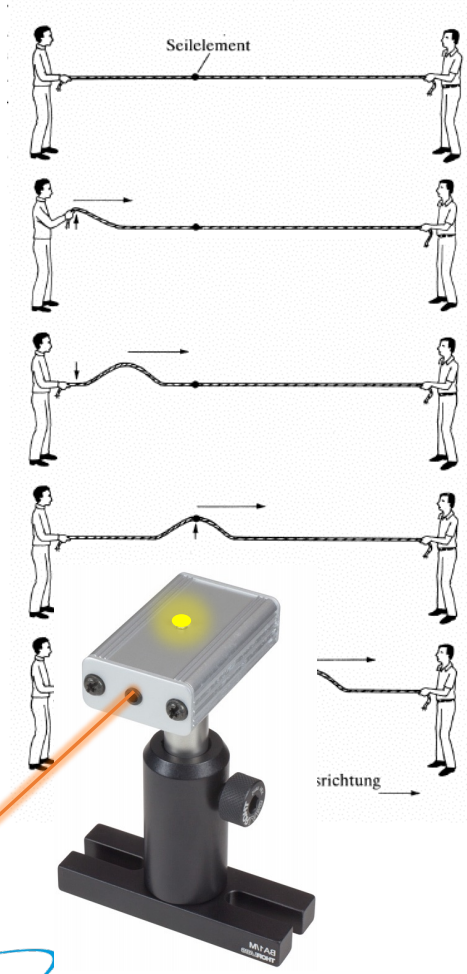
- Die eigentliche Informationsübertragung läuft nach bewährten Protokollen (RSA)



Informationsübertragung mit Licht

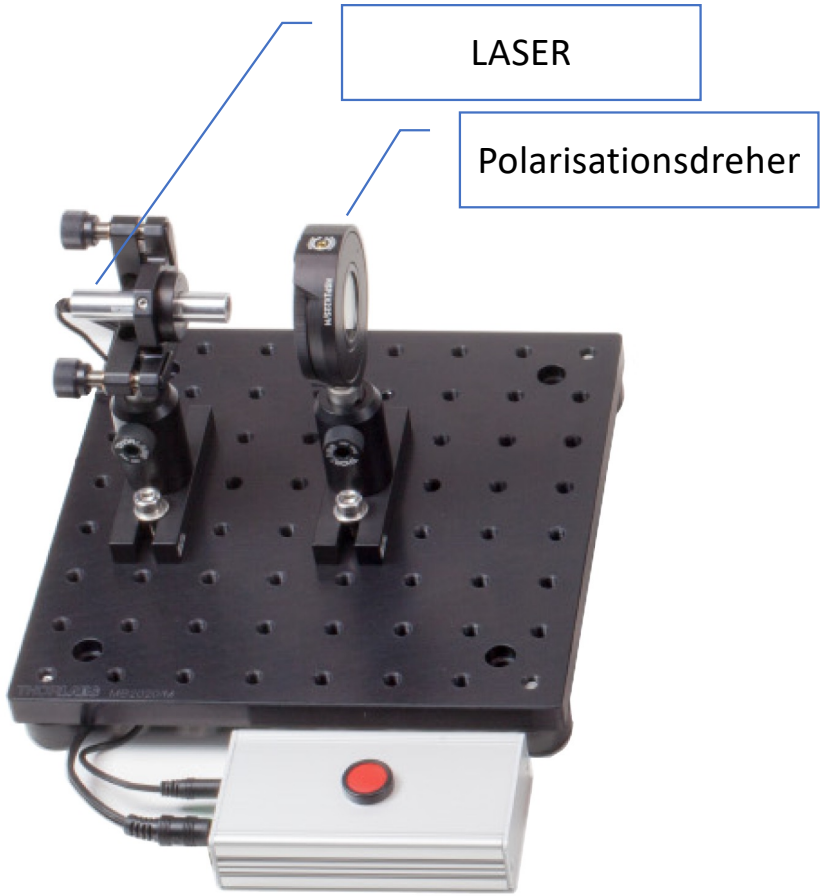
- Codierung über Polarisation des Lichts
  - Licht als elektromagnetische Welle
  - Das elektrische Feld schwingt senkrecht zur Ausbreitungsrichtung („transversal“)
  - Sehr gute Analogie zur Seilwelle
  - Jede Schwingungsrichtung ist möglich
    - Beschränkung auf zwei orthogonale Schwingungen z.B.:
      - Senkrechte Polarisation = 1
      - Horizontale Polarisation = 0



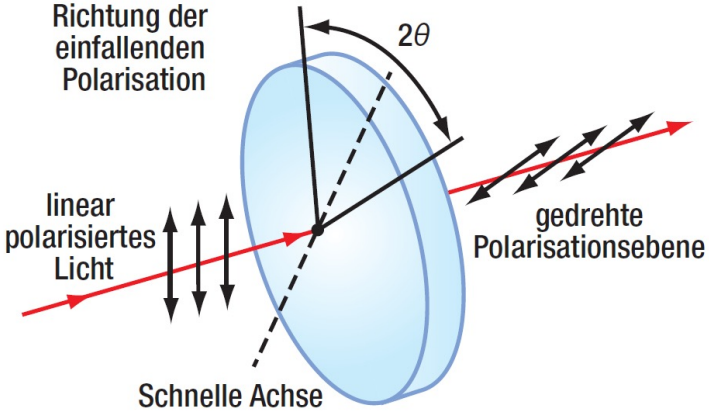


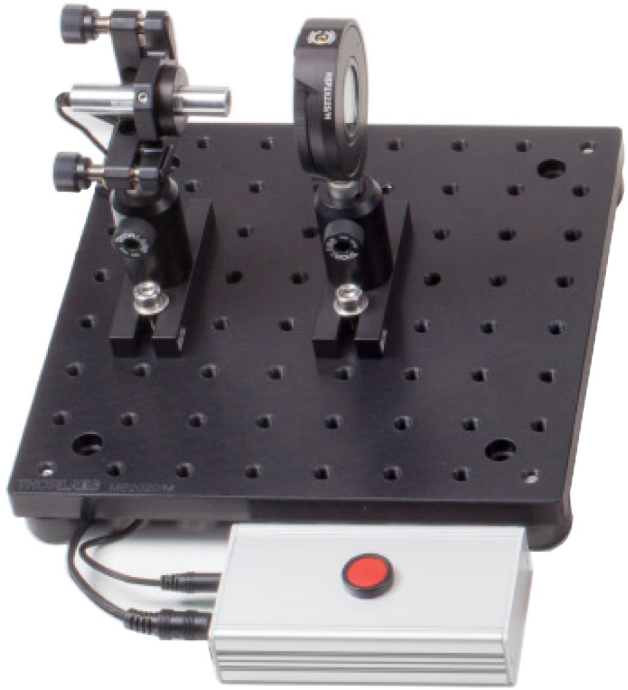
Informationsübertragung mit polarisiertem Licht

- ALICE:
  - Sender = horizontal polarisierter LASER
  - Richtungsänderung durch Polarisationsdreher
    - Poldreher auf 0° lässt horizontal polarisiertes Licht unverändert durch und codiert 0
    - Poldreher auf 90° macht aus horizontal polarisiertem Licht vertikal polarisiertes Licht und codiert 1



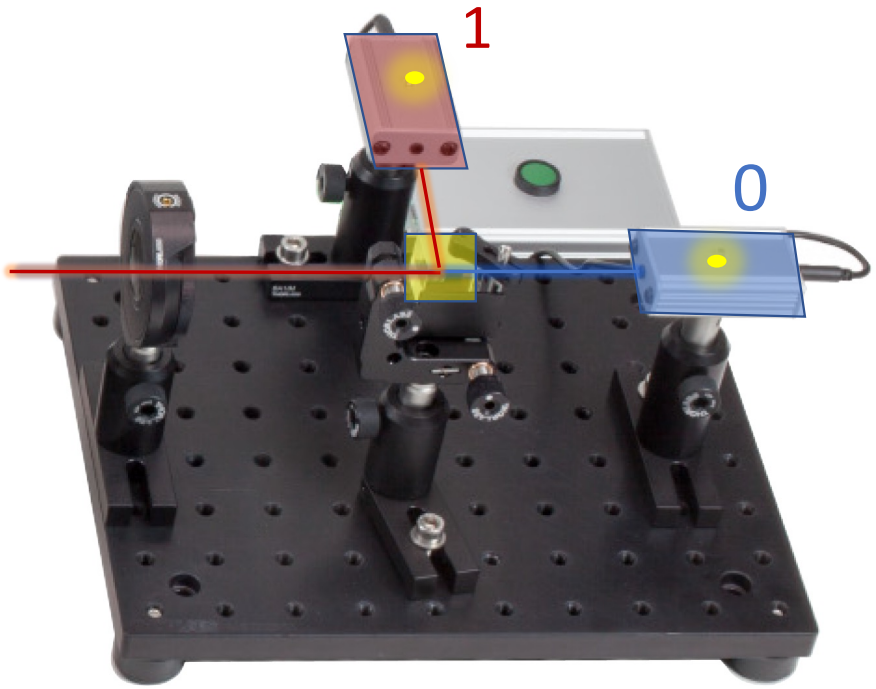
Informationsübertragung mit polarisiertem Licht



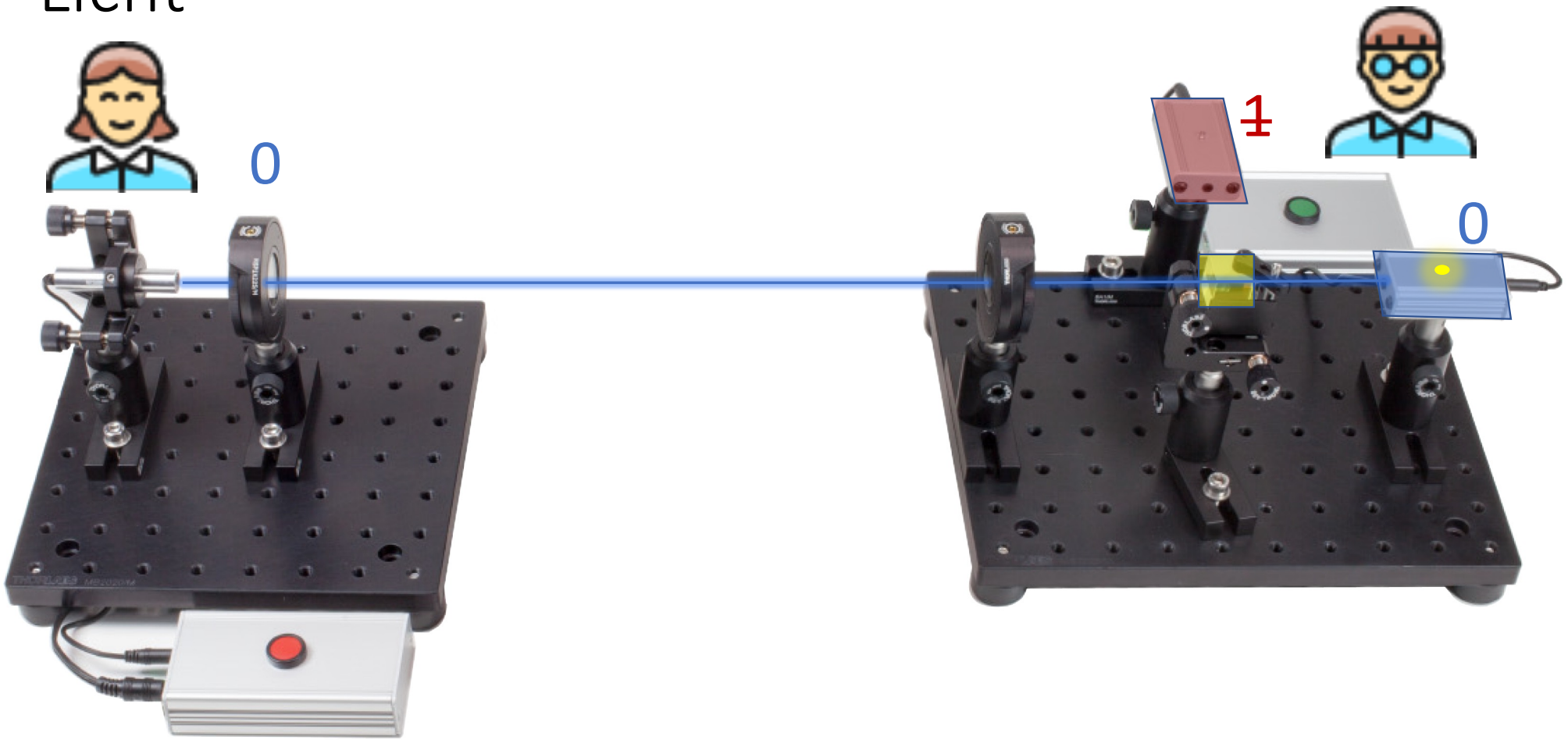


Informationsübertragung mit polarisiertem Licht

- BOB
  - Empfänger reagiert nur auf Amplitude
  - Polarisationsabhängiger Strahlteiler
  - Horizontal polarisiertes Licht wird durchgelassen und fällt auf den Detektor geradeaus (0 Detektor)
  - Vertikal polarisierts Licht wird reflektiert und fällt auf den Detektor im rechten Winkel zum einfallenden Laserstrahl (1 Detektor)

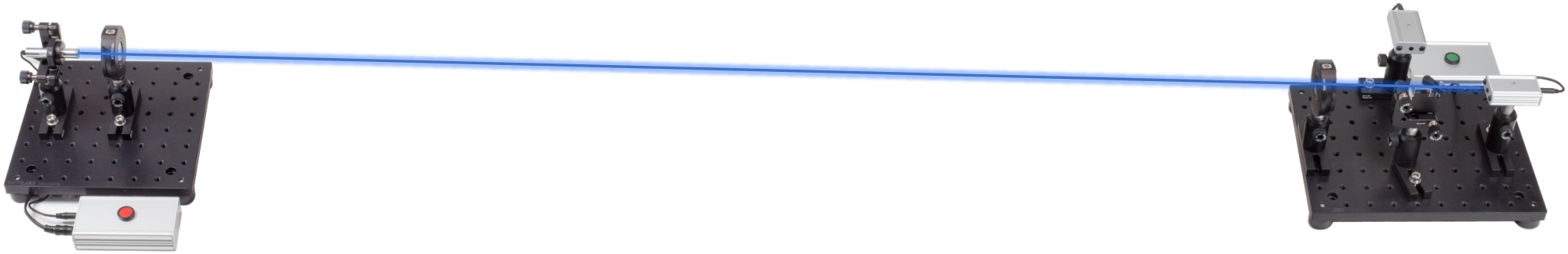


Informationsübertragung mit polarisiertem Licht



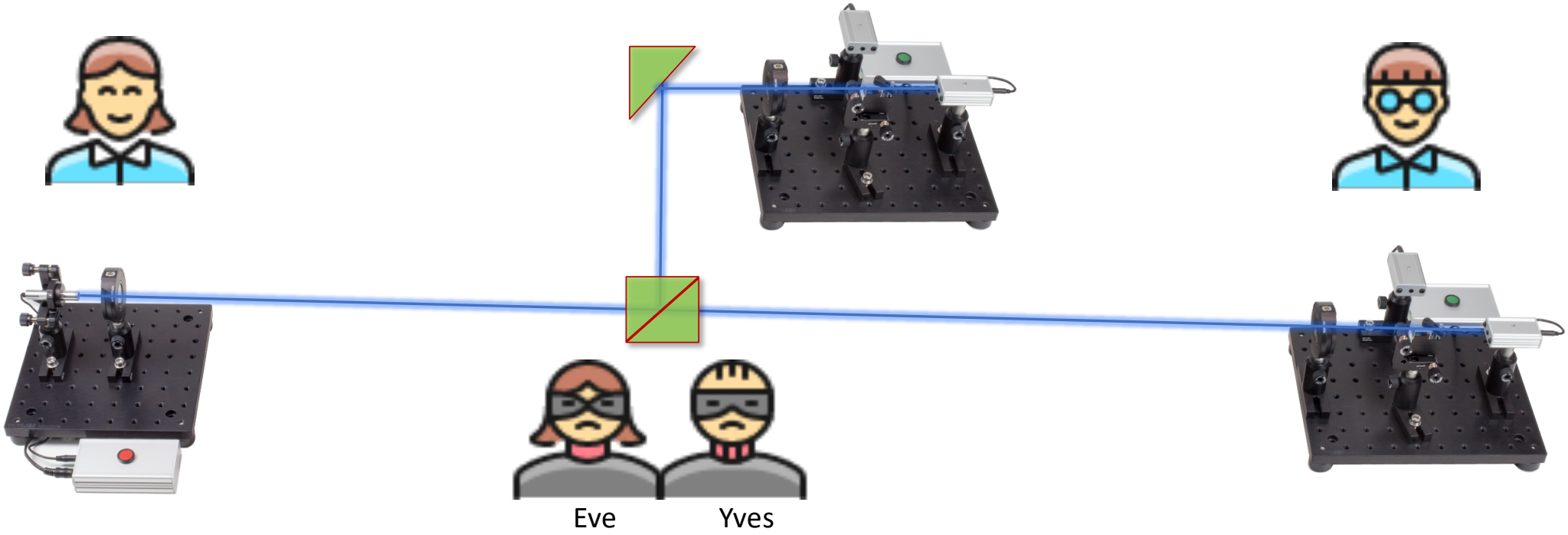
Informationsübertragung mit polarisiertem Licht

- Angriff über (wo-)man in the middle = Eve/Yves



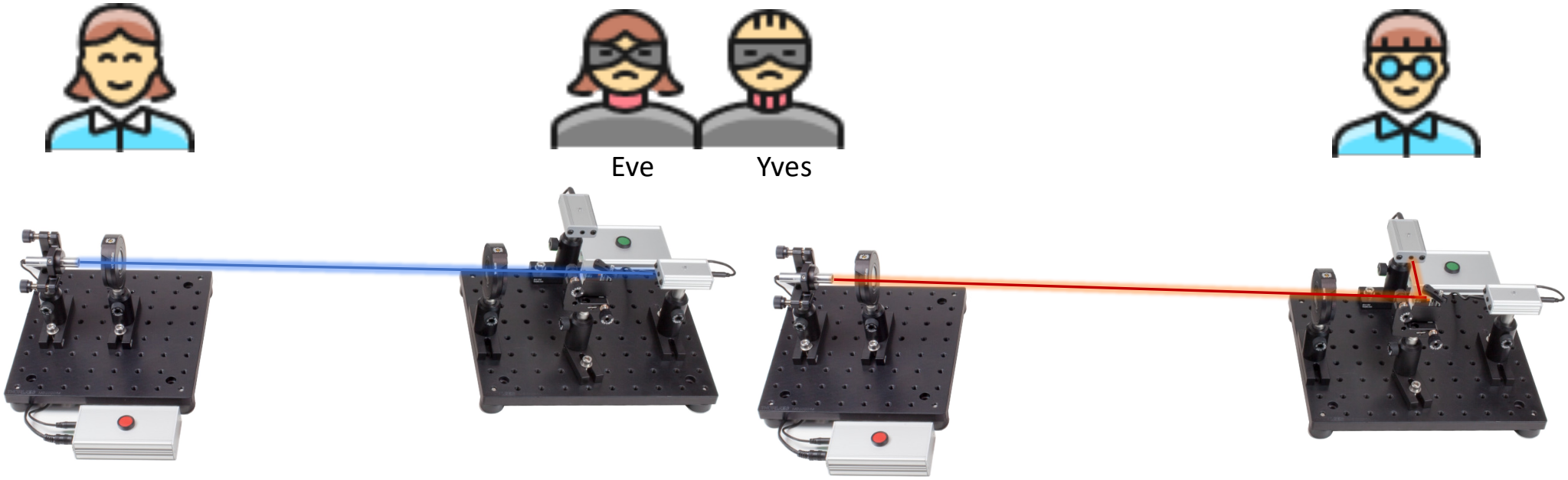
Informationsübertragung mit polarisiertem Licht

- Angriff über (wo-)man in the middle = Eve&Yves lauschen (passiv)



Informationsübertragung mit polarisiertem Licht

- Angriff über (wo-)man in the middle = Eve&Yves verändern (aktiv)

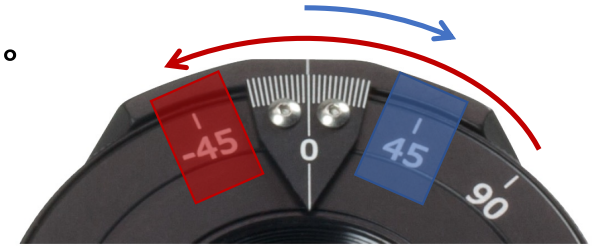


Rolle des Zufalls

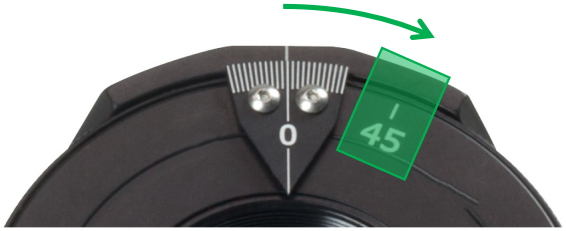
- Der gemeinsame Schlüssel von Alice und Bob soll eine zufällige aber eindeutige Folge von 0 und 1 werden
- Alice sendet weiterhin mit polarisiertem Licht 0 oder 1
- Wenn Bob jede gesendete 0 als 0 und jede gesendete 1 als 1 erkennt, dann können Eve&Yves das auch (deterministische Übertragung)
- BB84 führt deshalb zufällige Bits ein, die die Schlüsselbits verschleiern

Rolle des Zufalls

- Variation durch Drehung der „Polarisationsbasis“
  - Drehung der gesamten Apparatur um 45° ändert nichts
  - Statt den Sendertisch zu kippen dreht Alice mit Poldreher 45° weiter:
    - Aus 0° wird +45°
    - Aus +90° wird +135° = -45°
    - Realisierung mit weiteren Einstellungen an den Polarisationsdrehern



  - Statt den Empfängertisch zu kippen, dreht Bob die Polarisation zurück um -45°
    - Aus +45° wird wieder 0°
    - Aus 135° wird wieder 90°
    - Im Thorlabsaufbau wird der 45° Dreher dazu „falschrum“ montiert oder das poldrehende Lambda-Halbe Glas umgedreht



Rolle des Zufalls

- Variation durch Drehung der Polarisationsbasis

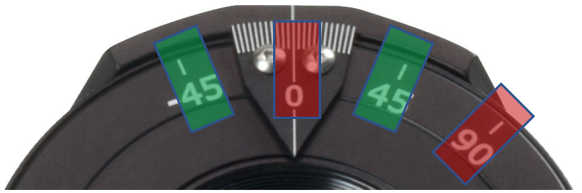
- Bezeichungen
  - Alice sendet in normaler Orientierung (vertikal/horizontal)

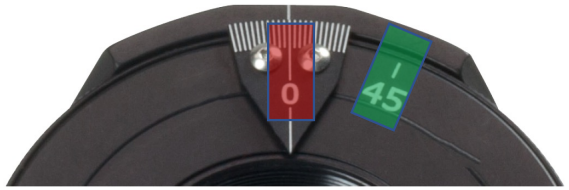
    = Alice wählt BASIS +
  - Alice sendet um 45° gedreht

    = Alice wählt BASIS x
  - Bob empfängt in normaler Orientierung (vertikal/horizontal)

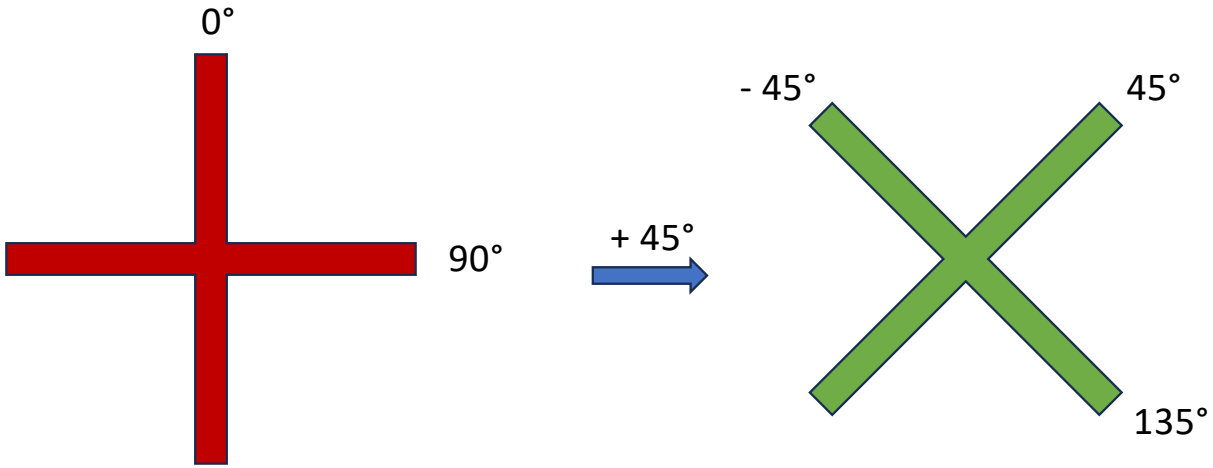
    = Bob wählt BASIS +
  - Bob empfängt um 45° gedreht

    = Bob wählt BASIS x



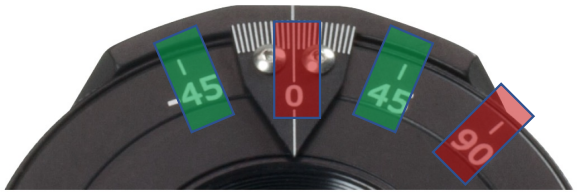


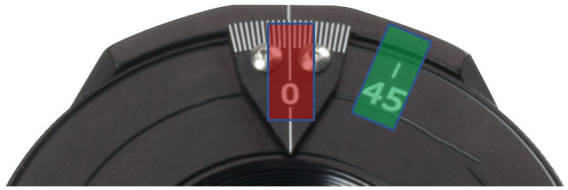
Rolle des Zufalls



Basis +

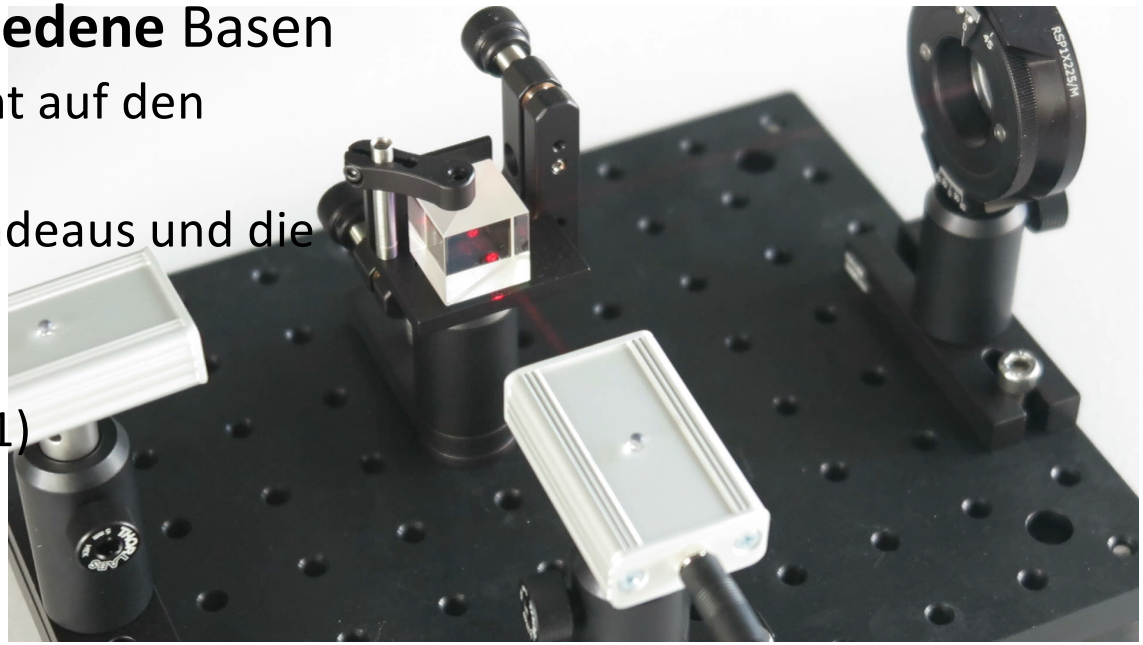
Basis x





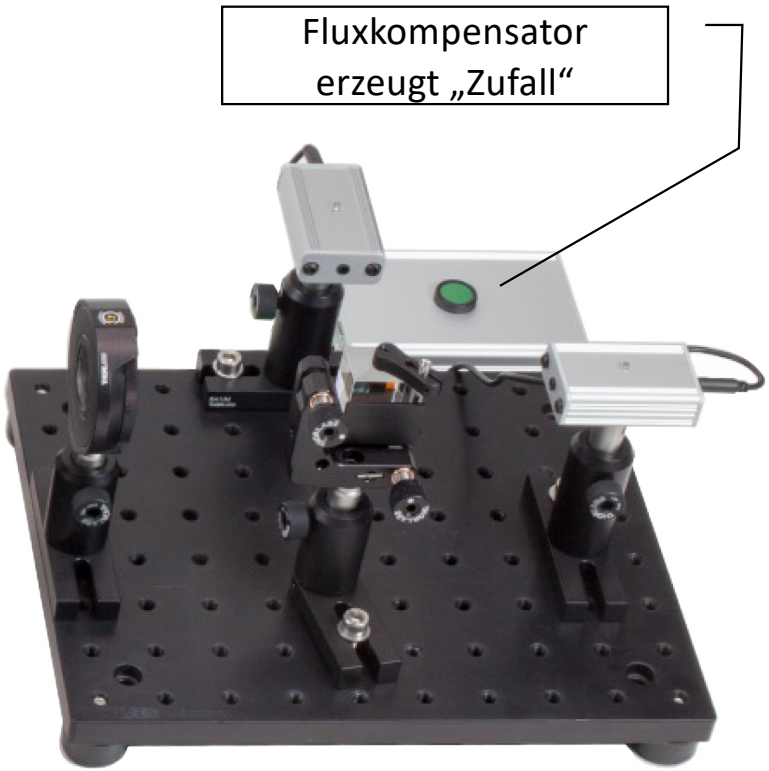
Rolle des Zufalls

- Wählen Alice und Bob die **gleiche** Basis ist die Übertragung **deterministisch**
- Wählen Alice und Bob **verschiedene** Basen
  - Trifft diagonal polarisiertes Licht auf den Strahlteiler
  - geht die Hälfte des Lichtes geradeaus und die andere Hälfte wird reflektiert
  - BEIDE Sensoren lösen aus
  - Undefinierter Zustand (0 UND 1)

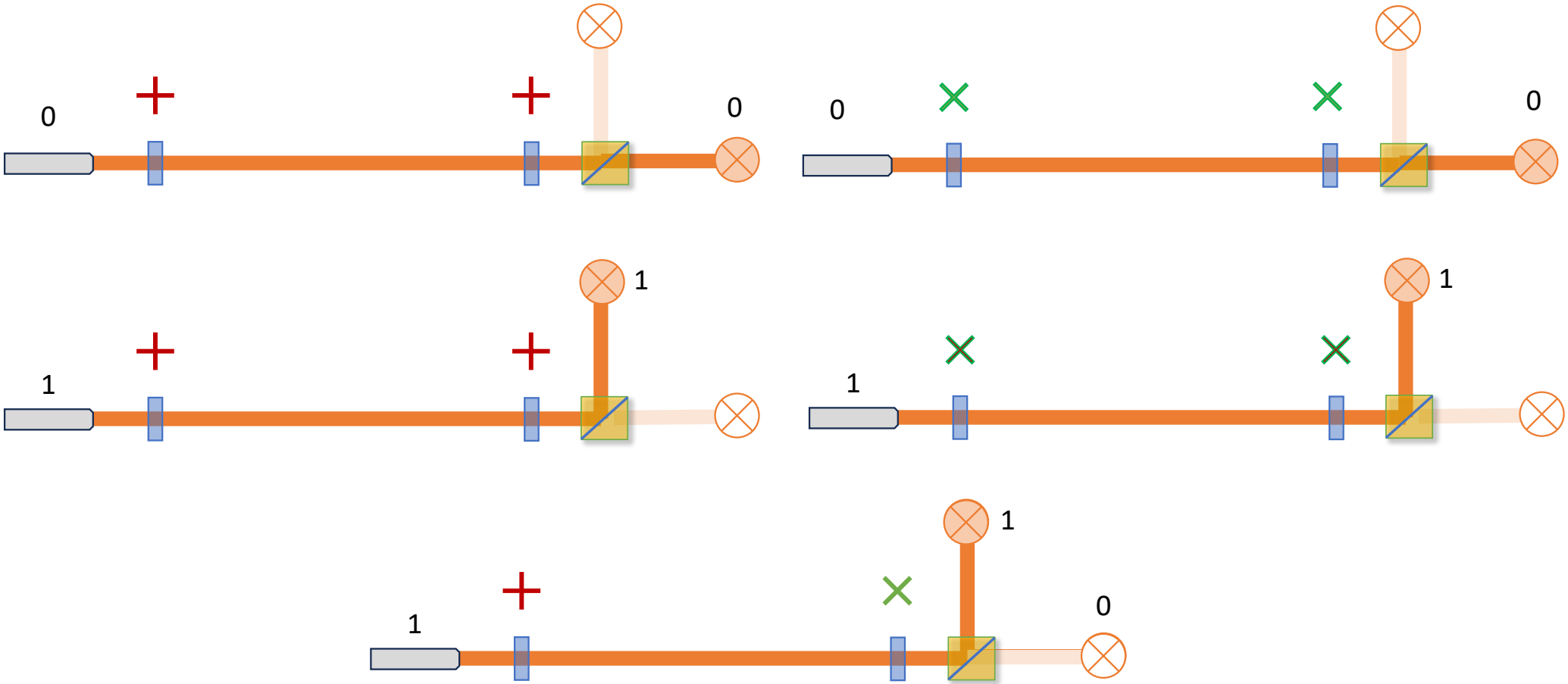


Rolle des Zufalls

- Wählen Alice und Bob die **gleiche** Basis ist die Übertragung **deterministisch**
- Wählen Alice und Bob **verschiedene** Basen,
  - so soll nach der Idee von B&B, statt beider Sensoren ZUFÄLLIG einer der beiden Sensoren auslösen
  - In unserem Laseraufbau vergleicht der „Fluxkompensator“ die Signale und würfelt elektronisch, welcher Sensor „zufällig“ auslöst



Rolle des Zufalls



Schlüsselerzeugung nach BB84

- Wählen Alice und Bob die **gleiche** Basis ist die Übertragung **deterministisch**
- Wählen Alice und Bob **verschiedene** Basen ist die Übertragung „**zufällig**“
- Idee der Schlüsselerzegung
  - Alice wählt zufällige Bits (0 oder 1) und zufällige Basen (+ oder x)
  - Bob wählt unabhängig zufällige Basis (+ oder x) und misst (0 oder 1)
  - Nach vielen Wiederholungen haben Alice und Bob eine Tabelle mit gewählten Basen und gesendeten bzw. gemessenen Bits

Schlüsselerzeugung nach BB84

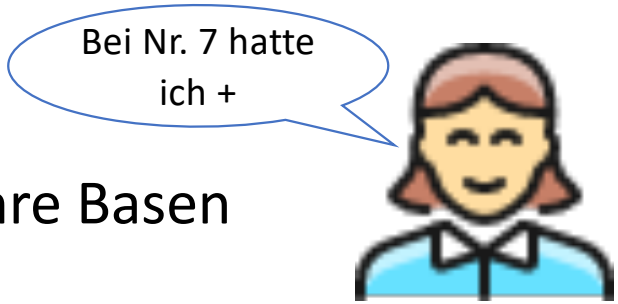
Alice

Nummer	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Basis	x	x	x	+	x	+	+	x	x	x	+	x	+	+	+	+	x	+	x	x	+	+	+	x	+
Bits	0	0	1	0	1	1	1	0	1	0	0	0	0	0	0	1	1	0	1	1	0	1	0	1	1

Bob

Nummer	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Basis	x	+	+	+	x	x	+	+	+	x	+	x	x	x	x	+	+	+	x	+	x	+	+	+	+
Bits	0	0	0	0	1	0	1	0	0	0	0	0	1	1	0	1	1	0	1	0	1	1	0	0	1

Schlüsselerzeugung nach BB84



- DANACH vergleichen Alice und Bob öffentlich Ihre Basen

Alice

Nummer	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Basis	x	x	x	+	x	+	+	x	x	x	+	x	+	+	+	+	x	+	x	x	+	+	+	x	+
Bits	0	0	1	0	1	1	1	0	1	0	0	0	0	0	0	1	1	0	1	1	0	1	0	1	1

Bob

Nummer	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Basis	x	+	+	+	x	x	+	+	+	x	+	x	x	x	x	+	+	+	x	+	x	+	+	+	+
Bits	0	0	0	0	1	0	1	0	0	0	0	0	1	1	0	1	1	0	1	0	1	1	0	0	1

Schlüsselerzeugung nach BB84

- Bei gleichen Basen wissen Sie, dass sie das gleiche (geheime) Bit haben

Alice

Nummer	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Basis	x	x	x	+	x	+	+	x	x	x	+	x	+	+	+	+	x	+	x	x	+	+	+	x	+
Bits	0	0	1	0	1	1	1	0	1	0	0	0	0	0	0	1	1	0	1	1	0	1	0	1	1

Bob

Nummer	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Basis	x	+	+	+	x	x	+	+	+	x	+	x	x	x	x	+	+	+	x	+	x	+	+	+	+
Bits	0	0	0	0	1	0	1	0	0	0	0	0	1	1	0	1	1	0	1	0	1	1	0	0	1

Schlüsselerzeugung nach BB84

- Bei verschiedenen Basen ist das Bit zufällig gleich oder verschieden

Alice

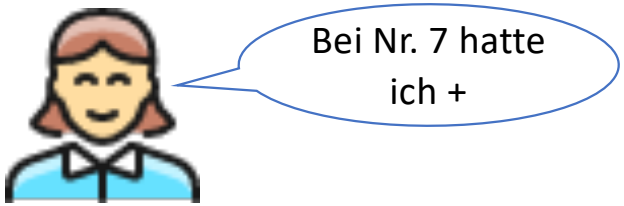
Nummer	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Basis	x	x	x	+	x	+	+	x	x	x	+	x	+	+	+	+	x	+	x	x	+	+	+	x	+
Bits	0	0	1	0	1	1	1	0	1	0	0	0	0	0	0	1	1	0	1	1	0	1	0	1	1

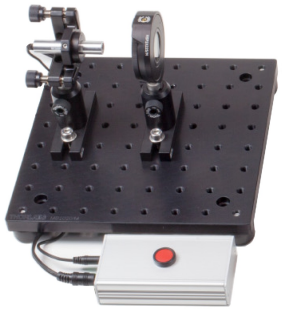
Bob

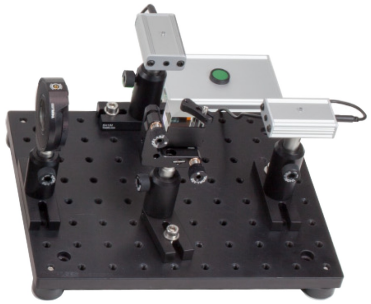
Nummer	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Basis	x	+	+	+	x	x	+	+	+	x	+	x	x	x	x	+	+	+	x	+	x	+	+	+	+
Bits	0	0	0	0	1	0	1	0	0	0	0	0	1	1	0	1	1	0	1	0	1	1	0	0	1

Schlüsselerzeugung nach BB84

- Das öffentliche Austauschen der Basen enthält keine Information über die Bits

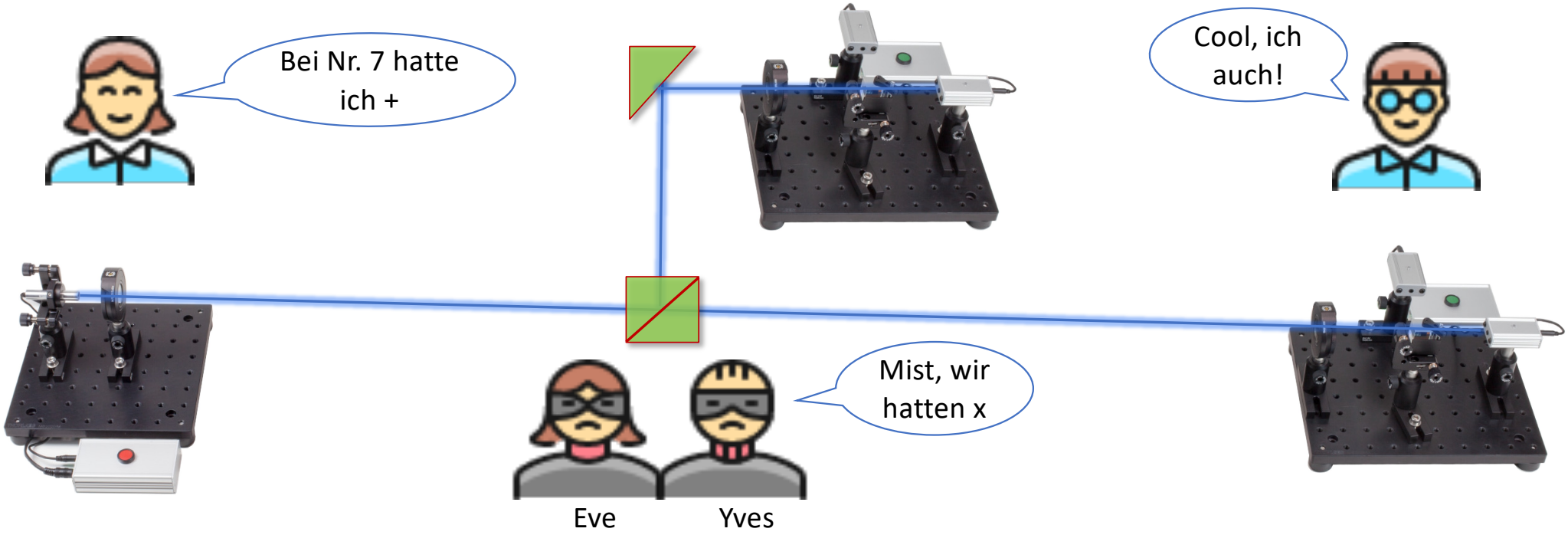






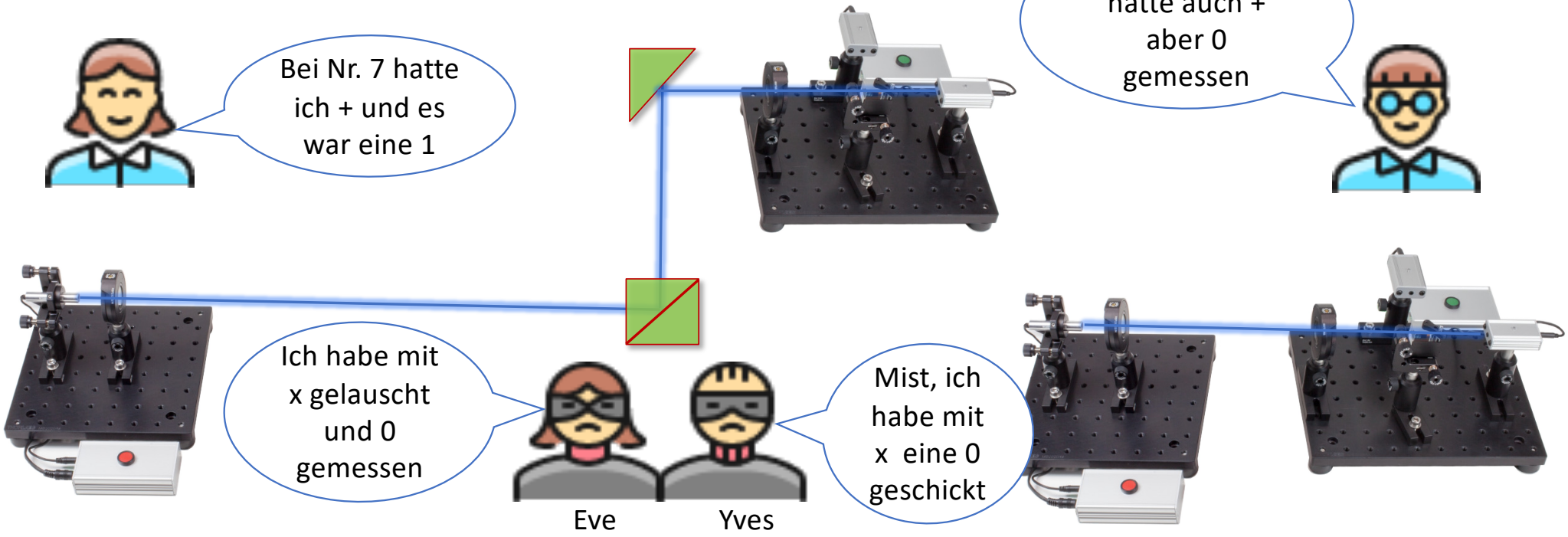
Schlüsselerzeugung nach BB84

- Eve&Yves erhalten beim passiven Angriff nur 25% der Schlüsselbits



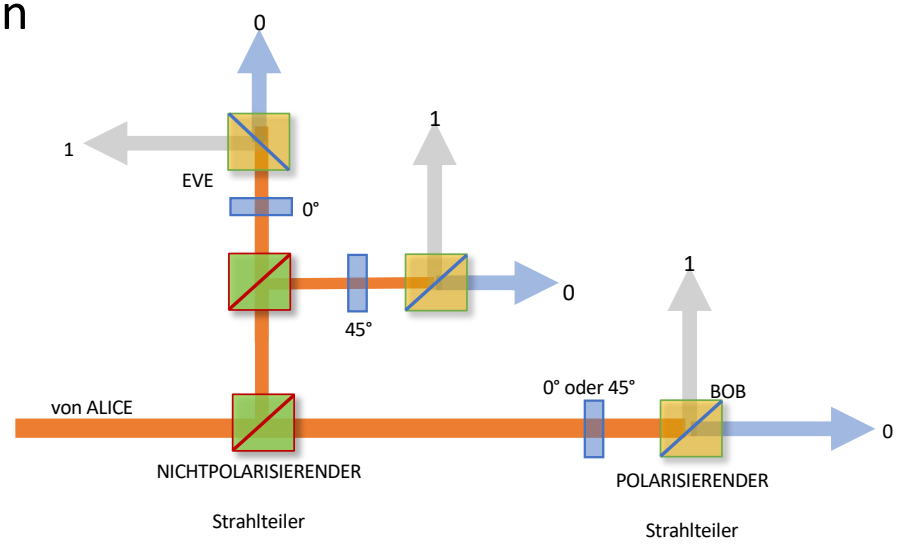
Schlüsselerzeugung nach BB84

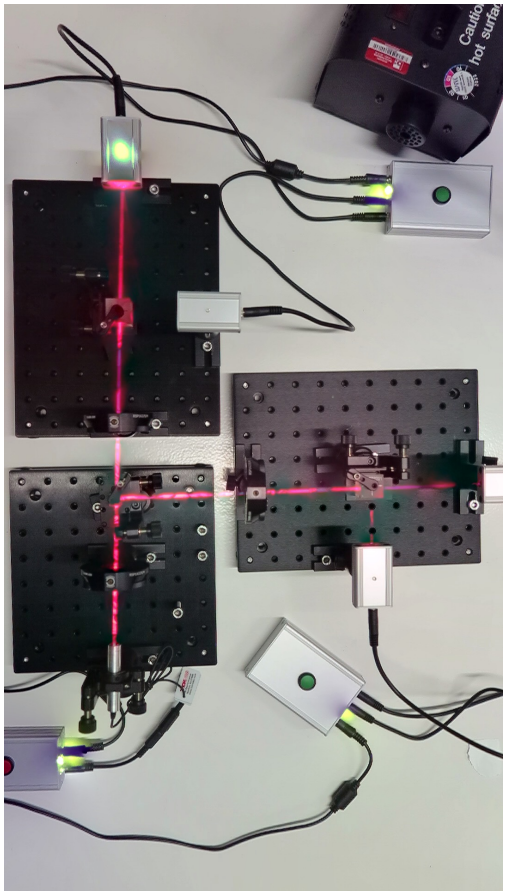
- Eve&Yves schicken beim aktiven Angriff 25% der Schlüsselbits falsch weiter



Schlüsselerzeugung nach BB84

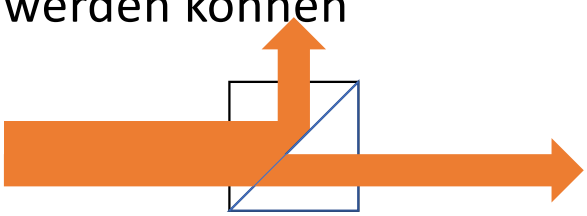
- Schwachstellen
  - Der Fluxkompensator erzeugt nur „Pseudozufall“
  - Eve&Yves können noch immer einen „(wo)man in the middle“ Angriff ausführen, indem sie in beiden Basen messen

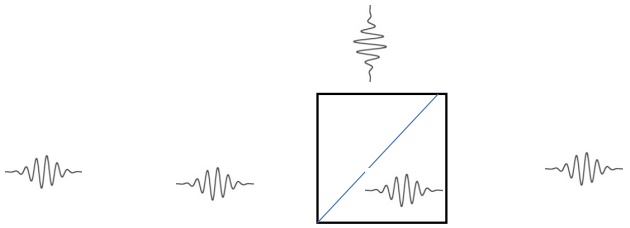




Schlüsselerzeugung nach BB84

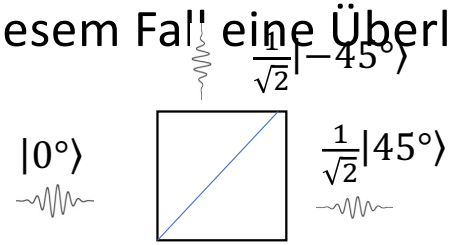
- Angreifbarkeit beruht auf Möglichkeit das Licht beliebig zu teilen und/oder zu „kopieren“
- Idee von BB84:
  - Der Algorithmus wird sicher, wenn das Licht „unteilbar“ und „unkopierbar“ ist
- Einsteins einfaches Photonen - Modell
  - Licht ist ein Strom von teilchenartigen Energiepaketen (Photonen), die sich bewegen, ohne sich zu teilen und nur als Ganzes emittiert und absorbiert werden können





Schlüsselerzeugung nach BB84

- Angreifbarkeit beruht auf Möglichkeit das Licht beliebig zu teilen und/oder zu „kopieren“
- Idee von BB84:
  - Der Algorithmus wird sicher, wenn das Licht „unteilbar“ und „unkopierbar“ ist
- Alice sendet genau ein Photon
  - Ein von Alice der X – Basis gesendetes einzelnes Photon nimmt bei Bob in der + Basis löst mit Wahrscheinlichkeit 50% einen der beiden Detektoren aus und erzeugt somit 0 oder 1 mit ECHTEM Zufall
  - Quantenphysikalisch erzeugt der Strahlteiler in diesem Fall eine Überlagerung der möglichen Zustände mit 50 – 50 Amplituden



Schlüsselerzeugung nach BB84

- Angreifbarkeit beruht auf Möglichkeit das Licht beliebig zu teilen und/oder zu „kopieren“
- Idee von BB84:
  - Der Algorithmus wird sicher, wenn das Licht „unteilbar“ und „unkopierbar“ ist
- Alice sendet genau ein Photon

$$|45°\rangle = \frac{1}{\sqrt{2}}|0°\rangle + \frac{1}{\sqrt{2}}|90°\rangle$$
$$|-45°\rangle = \frac{1}{\sqrt{2}}|0°\rangle - \frac{1}{\sqrt{2}}|90°\rangle$$
$$|0°\rangle = \frac{1}{\sqrt{2}}|45°\rangle + \frac{1}{\sqrt{2}}|-45°\rangle$$
$$|90°\rangle = \frac{1}{\sqrt{2}}|45°\rangle - \frac{1}{\sqrt{2}}|-45°\rangle$$

$$|\langle 45°|0°\rangle|^2 = \left|\frac{1}{\sqrt{2}}\underbrace{\langle 45°|45°\rangle}_{=1} + \frac{1}{\sqrt{2}}\underbrace{\langle 45°|-45°\rangle}_{=0}\right|^2 = \frac{1}{2}$$

$$\widehat{M}_+|45°\rangle = |0°\rangle\langle 0°|\left(\frac{1}{\sqrt{2}}|0°\rangle + \frac{1}{\sqrt{2}}|90°\rangle\right) - |90°\rangle\langle 90°|\left(\frac{1}{\sqrt{2}}|0°\rangle + \frac{1}{\sqrt{2}}|90°\rangle\right)$$
$$= \frac{1}{\sqrt{2}}|0°\rangle\langle 0°|0°\rangle + \frac{1}{\sqrt{2}}|0°\rangle\langle 0°|90°\rangle - \frac{1}{\sqrt{2}}|90°\rangle\langle 90°|0°\rangle$$
$$- \frac{1}{\sqrt{2}}|90°\rangle\langle 90°|90°\rangle = \frac{1}{\sqrt{2}}|0°\rangle - \frac{1}{\sqrt{2}}|90°\rangle$$

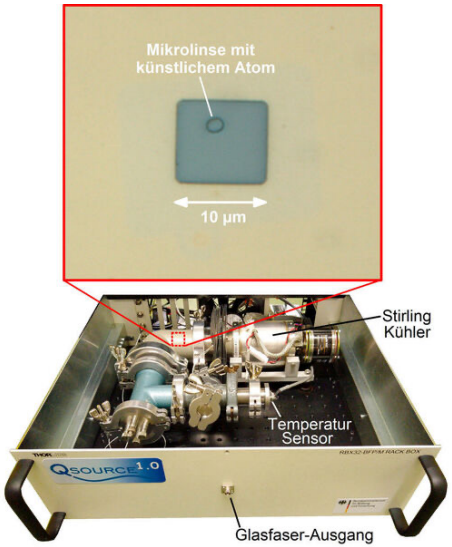
$$\widehat{M}_+|-45°\rangle = \frac{1}{\sqrt{2}}|0°\rangle + \frac{1}{\sqrt{2}}|90°\rangle$$

Schlüsselerzeugung nach BB84

- Angreifbarkeit beruht auf Möglichkeit das Licht beliebig zu teilen und/oder zu „kopieren“
- Idee von BB84:
  - Der Algorithmus wird sicher, wenn das Licht „unteilbar“ und „unkopierbar“ ist
- Alice sendet genau ein Photon
  - Eve kann das Photon von Alice nicht vollständig analysieren (in beiden Basen), jede erste Messung zerstört die Information über Zustand vor der Messung
  - Das „No – Clone Theorem“ von 1982 sichert, dass Alice vor der Messung keinen Zwilling des Photons erzeugen kann

Unterrichtsszenarios und Diskussion

- Problem der Realisierung
  - Einzelne Photonen zu erzeugen, gezielt zu übertragen und nachzuweisen ist „schwer“ und teuer und störungsanfällig:
    - Arbeitsgruppen von Prof. Becher und Prof. Eschner an der UdS (Störstellen in Diamanten und Ionenfallen)
    - 2022 gab es laut Google keinen kommerziellen Anbieter
    - 2026 gibt es (laut KI) etliche kommerzielle Anbieter
  - Realisierung als Simulation der Firma Thorlabs
    - Polarisierte Laser für Dauer- und Pulsbetrieb (<1mW)
    - Dauerbetrieb für Justage und Funktionskontrolle
    - Pulsbetrieb simuliert Einzelphotonquelle
    - Elektronischer Komparator generiert Pseudozufall bei gleichen Amplituden



Unterrichtsszenarios und Diskussion

- Realisierung bis jetzt
  - Seminarfach (KT, LE)
  - LK – Informatik (LE, KT)
  - Workshop am Tag der Informatik (LE, KT)
- Zeitbedarf bei Realisierung
  - Ca. 2h – 3h gemäß Erprobung in Informatik mit möglichst wenig Physik, Durchführung nur exemplarisch (Arbeitsblätter, Präsentation)
  - Ca. 4h – 6h gemäß Erprobung im Seminarfach mit mehr Physik, Durchführung als entdeckendes Lernen (Arbeitsblätter, Lehrervortrag, Präsentation)

Unterrichtsszenarios und Diskussion

- PHYSIK
  - Licht als Welle
  - Polarisation
  - LASER
  - Lichtsensoren
  - Optische Komponenten (Strahlteiler, Polarisatoren, Poldreher)
  - Photonen im einsteinschen Sinn
  - Photonen als echte Quanten, …

  - Danke an:
    AG Prof. Dr. Rolf Pelster

QUANTAG

UNIVERSITÄT DES SAARLANDES

Unterrichtsszenarios und Diskussion

- Lehrpläne und Bildungsstandards
  - Licht als Welle
  - Polarisation
  - ~~LASER~~
  - ~~Lichtsensoren~~
  - Optische Komponenten (Strahlteiler, ~~Polarisatoren, Poldreher~~)
  - Photonen im einsteinschen Sinn
  - ~~Photonen als echte Quanten~~, …
  - … Interferometer, Determinismus, Realität, …

Unterrichtsszenarios und Diskussion

- Danke an:
  AG Prof. Dr. Rolf Pelster

QUANTAG

UNIVERSITÄT DES SAARLANDES

- Und jetzt ran an den Speck!