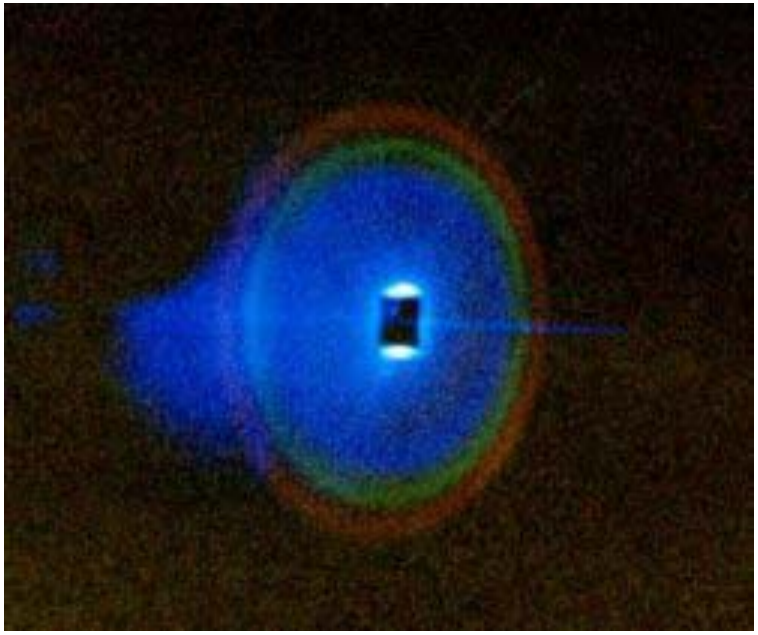
QUANTENKRYPTOGRAPHIE



Alexander Hentschel

betreut von Dr. Alejandro Saenz

Institut für Physik, Humboldt-Universität Berlin

Einleitung

Möglichkeiten der Verschlüsselung:

- Nachricht unverändert mittels sicherem Medium übertragen
  z.B. Bote, verstecktes Glasfaserkabel

Einleitung

Möglichkeiten der Verschlüsselung:

- Nachricht unverändert mittels sicherem Medium übertragen
  z.B. Bote, verstecktes Glasfaserkabel
- Nachricht verändern mittels
  - festgelegtem Algorithmus
    z.B. Verschieben der Buchstaben im Alphabet

Einleitung

Möglichkeiten der Verschlüsselung:

- Nachricht unverändert mittels sicherem Medium übertragen
  z.B. Bote, verstecktes Glasfaserkabel
- Nachricht verändern mittels
  - festgelegtem Algorithmus
    z.B. Verschieben der Buchstaben im Alphabet
  - vorher vereinbartem Schlüssel
    z.B. Reihe Nummern, um die Buchstaben verschoben werden

Einleitung

Möglichkeiten der Verschlüsselung:

- Nachricht unverändert mittels sicherem Medium übertragen
  z.B. Bote, verstecktes Glasfaserkabel
- Nachricht verändern mittels
  - festgelegtem Algorithmus
    z.B. Verschieben der Buchstaben im Alphabet
  - vorher vereinbartem Schlüssel
    z.B. Reihe Nummern, um die Buchstaben verschoben werden
  - bei jeder Übertragung neuen Schlüssel erzeugen
    wie wird Schlüssel *sicher* ausgetauscht?

Einleitung

Ziel der Kryptographie:

Daten sind trotz unbegrenzt hohem technischen und zeitlichen Aufwand für Unbefugte nicht einsehbar

Einleitung

Ziel der Kryptographie:

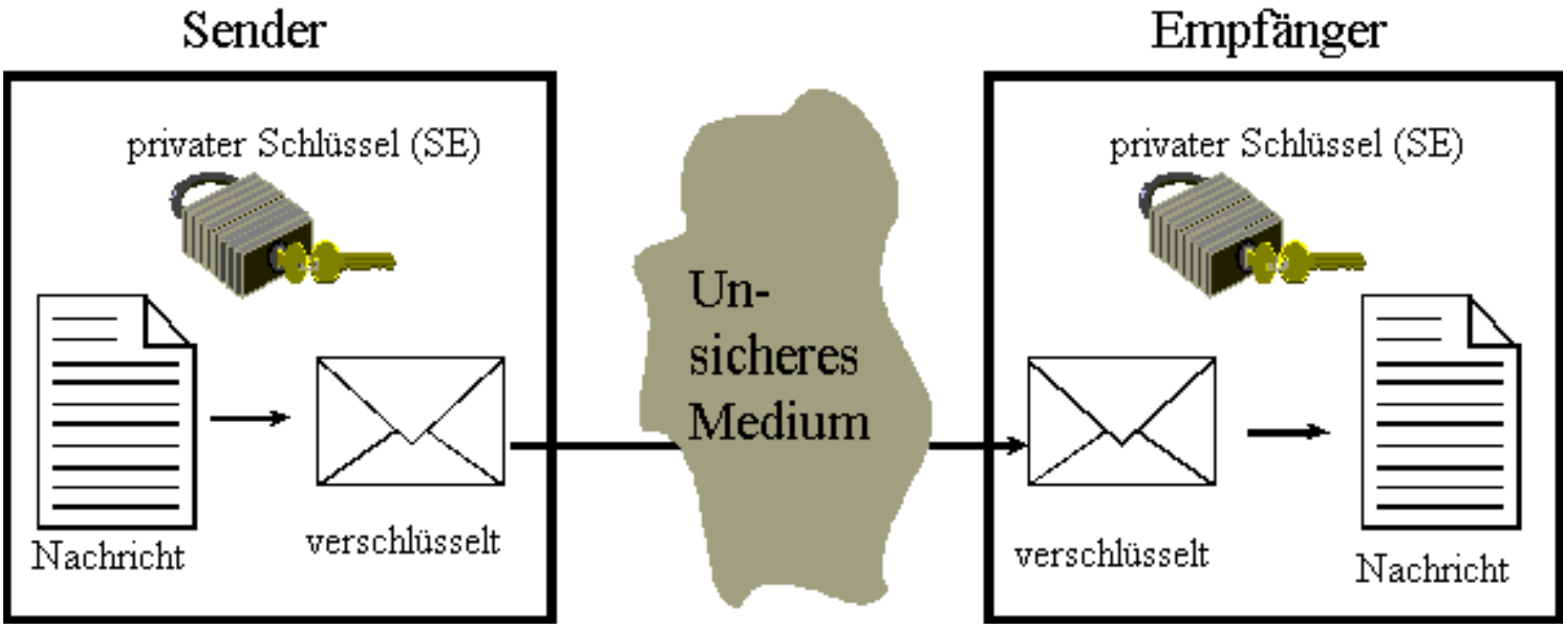
Daten sind trotz unbegrenzt hohem technischen und zeitlichen Aufwand für Unbefugte nicht einsehbar

Methoden:

- Abhörversuche werden definitiv früh genug bemerkt
- Daten sind ohne Zusatzinformationen nicht mehr rekonstruierbar

klassische Krypto-Verfahren

Private-Key-Verfahren

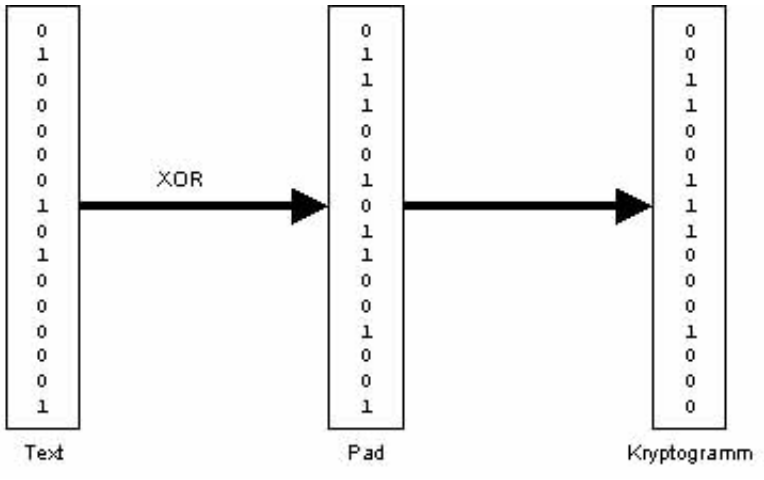


beide Parteien verwenden *gleichen Schlüssel*

klassische Krypto-Verfahren

Private-Key-Verfahren

One-Time-Pad-Verfahren



Schlüssel (Pad):

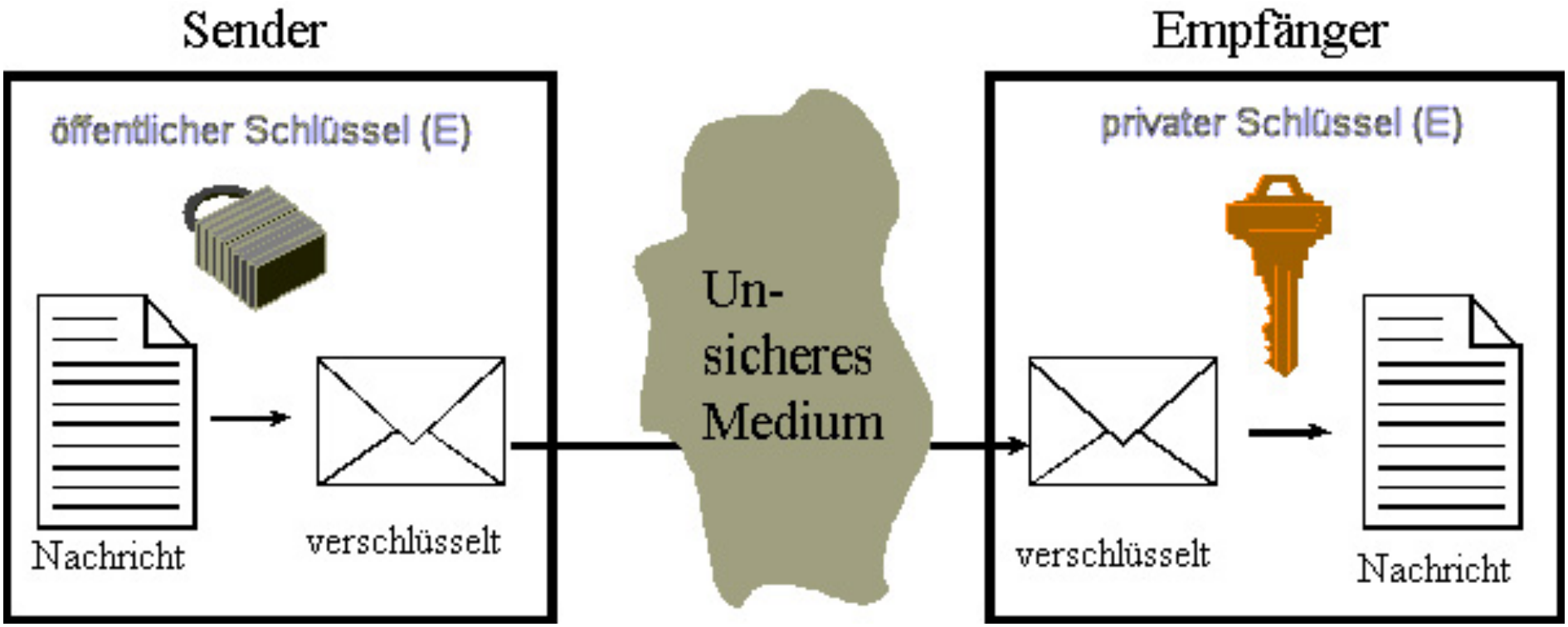
- Zufallszahl in Länge der Nachricht
- darf nur einmal verwendet werden

Nachricht $\stackrel{OTP}{\longrightarrow}$ statistisches Rauschen

Sicherheit mathematisch beweisbar!

klassische Krypto-Verfahren

Public-Key-Verfahren



öffentlicher Schlüssel nur zur Chiffrierung

klassische Krypto-Verfahren

RSA-Verfahren: gebräuchlichstes Kryptographieverfahren

- Empfänger der Nachricht erzeugt:
  öffentlichen Schlüssel und dazugehörigen privaten Schlüssel

klassische Krypto-Verfahren

RSA-Verfahren: gebräuchlichstes Kryptographieverfahren

- Empfänger der Nachricht erzeugt:
  öffentlichen Schlüssel und dazugehörigen privaten Schlüssel

Verfahren:

- generiere 2 ungleiche Primzahlen P und Q

klassische Krypto-Verfahren

RSA-Verfahren: gebräuchlichstes Kryptographieverfahren

- Empfänger der Nachricht erzeugt:
  öffentlichen Schlüssel und dazugehörigen privaten Schlüssel

Verfahren:

- generiere 2 ungleiche Primzahlen P und Q
- finde (durch probieren):
  - Zahl $e \in \mathbb{N}$: e teilerfremd zu $(P-1)\cdot(Q-1)$
  - Zahl $d \in \mathbb{N}$: $e \cdot d = s(P-1)(Q-1)+1$ für $s \in \mathbb{N}$ beliebig

klassische Krypto-Verfahren

RSA-Verfahren: gebräuchlichstes Kryptographieverfahren

- Empfänger der Nachricht erzeugt:
  öffentlichen Schlüssel und dazugehörigen privaten Schlüssel

Verfahren:

- generiere 2 ungleiche Primzahlen P und Q
- finde (durch probieren):
  - Zahl $e \in \mathbb{N}$: e teilerfremd zu $(P-1)\cdot(Q-1)$
  - Zahl $d \in \mathbb{N}$: $e \cdot d = s(P-1)(Q-1)+1$ für $s \in \mathbb{N}$ beliebig
- $\{N = P \cdot Q, e\}$ öffentlicher Schlüssel
  $\{N = P \cdot Q, d\}$ privater Schlüssel

Schwachstellen klassischer Krypto-Verfahren

- beruht auf Schwierigkeit eine natürliche Zahl N in seine Primfaktoren zu zerlegen

Schwachstellen klassischer Krypto-Verfahren

- beruht auf Schwierigkeit eine natürliche Zahl N in seine Primfaktoren zu zerlegen
- nur Algorithmen *bekannt*, deren Laufzeit exponentiell mit der Länge von N skaliert

Schwachstellen klassischer Krypto-Verfahren

- beruht auf Schwierigkeit eine natürliche Zahl N in seine Primfaktoren zu zerlegen
- nur Algorithmen *bekannt*, deren Laufzeit exponentiell mit der Länge von N skaliert
- Nichtexistenz effizienter Faktorisierungsalgorithmen nicht bewiesen

Schwachstellen klassischer Krypto-Verfahren

- beruht auf Schwierigkeit eine natürliche Zahl N in seine Primfaktoren zu zerlegen
- nur Algorithmen *bekannt*, deren Laufzeit exponentiell mit der Länge von N skaliert
- Nichtexistenz effizienter Faktorisierungsalgorithmen nicht bewiesen
- Quantencomputer: *Algorithmus von Shaw* faktorisiert Primzahlen in polynomieller Laufzeit

Schwachstellen klassischer Krypto-Verfahren

- beruht auf Schwierigkeit eine natürliche Zahl N in seine Primfaktoren zu zerlegen
- nur Algorithmen *bekannt*, deren Laufzeit exponentiell mit der Länge von N skaliert
- Nichtexistenz effizienter Faktorisierungsalgorithmen nicht bewiesen
- Quantencomputer: *Algorithmus von Shaw* faktorisiert Primzahlen in polynomieller Laufzeit
- falls Quantencomputer realisierbar sind fast **alle** derzeit verwendeten Public-Key-Verfahren hinfällig
- Quantenphysik ermöglicht neue Kryptographieverfahren

Quanten-Kryptographieverfahren

Ausweg:

Verschlüsselungsverfahren, deren Sicherheit auf physikalischen Gesetzen beruht

Quanten-Kryptographieverfahren

Ausweg:

Verschlüsselungsverfahren, deren Sicherheit auf physikalischen Gesetzen beruht

Beispiele:

- BB84-Protokoll
- Erweiterung: BB92-Protokoll
- EPR-Protokoll

Das BB84-Protokoll

Leistung:

- Übertragung einer zufälligen Bitfolge als Schlüssel
- garantiert die Erkennung eines Abhörversuchs

Das BB84-Protokoll

Leistung:

- Übertragung einer zufälligen Bitfolge als Schlüssel
- garantiert die Erkennung eines Abhörversuchs

mit sicherem Schlüssel:

- klassische Übertragung der Nachricht mittels *One-Time-Pad-Verfahren*

Das BB84-Protokoll

Es sind klassiche Bits zu übertragen

notwendig ist:

- Quantensystem mit zwei Zuständen,
  typisch: Photonen mit Polarisation $|\uparrow\rangle$ und $|\rightarrow\rangle$

Das BB84-Protokoll

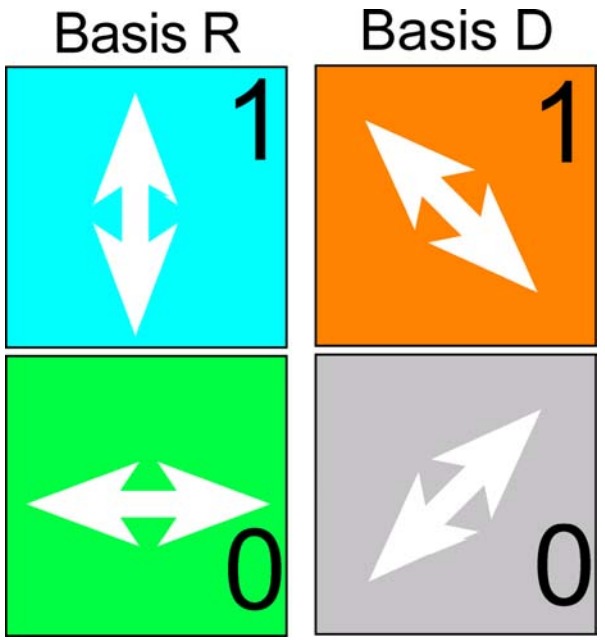
Es sind klassiche Bits zu übertragen

notwendig ist:

- Quantensystem mit zwei Zuständen,
  typisch: Photonen mit Polarisation $|\uparrow\rangle$ und $|\rightarrow\rangle$
- Bit $s \leftrightarrow \begin{cases} |\uparrow\rangle & s \equiv 1 \\ |\rightarrow\rangle & s \equiv 0 \end{cases}$

Das BB84-Protokoll

- Bit $s \leftrightarrow \begin{cases} |\uparrow\rangle & s \equiv 1 \\ |\rightarrow\rangle & s \equiv 0 \end{cases}$
- zwei orthonormale Basen
  - R: $|\rightarrow\rangle$ und $|\uparrow\rangle$
  - D: $|\nearrow\rangle$ und $|\searrow\rangle$

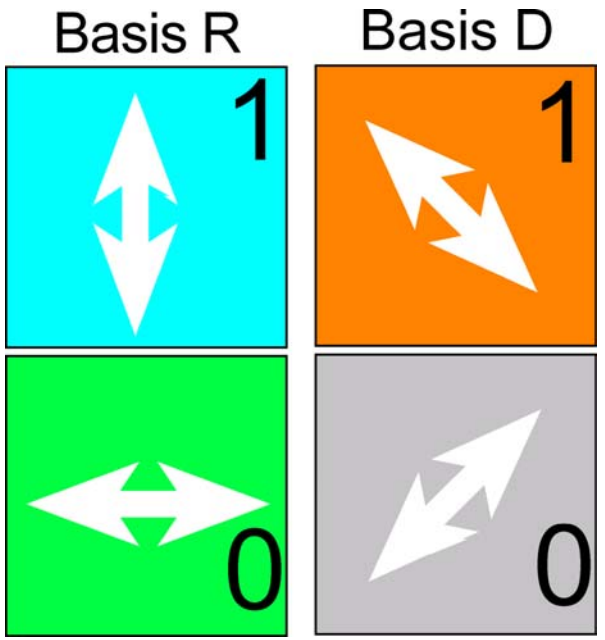


Das BB84-Protokoll

- Bit $s \leftrightarrow \begin{cases} |\uparrow\rangle & s \equiv 1 \\ |\rightarrow\rangle & s \equiv 0 \end{cases}$
- zwei orthonormale Basen
  - R: $|\rightarrow\rangle$ und $|\uparrow\rangle$
  - D: $|\nearrow\rangle$ und $|\searrow\rangle$
- **Basen-Transformation:**

$$|\nearrow\rangle = \frac{1}{\sqrt{2}}\left(|\rightarrow\rangle + |\uparrow\rangle\right)$$

$$|\searrow\rangle = \frac{1}{\sqrt{2}}\left(|\rightarrow\rangle - |\uparrow\rangle\right)$$



Quantenphysikalische Grundlagen

Besonderheiten von Quanten-Bits:

- Quantensystem kann sich in **Superpositionszustand** befinden:
  $|\Psi\rangle = \frac{1}{\sqrt{2}} \left(| \rightarrow \rangle + | \uparrow \rangle \right)$

Quantenphysikalische Grundlagen

Besonderheiten von Quanten-Bits:

- Quantensystem kann sich in **Superpositionszustand** befinden:
  $|\Psi\rangle = \frac{1}{\sqrt{2}} \left(| \rightarrow \rangle + | \uparrow \rangle \right)$
- Messung $\Rightarrow$ Reduktion des Zustandes
  Informationskollaps

Quantenphysikalische Grundlagen

Besonderheiten von Quanten-Bits:

- Quantensystem kann sich in **Superpositionszustand** befinden:
  $|\Psi\rangle = \frac{1}{\sqrt{2}} \left(|\rightarrow\rangle + |\uparrow\rangle \right)$
- Messung $\Rightarrow$ Reduktion des Zustandes
  Informationskollaps

  nach Messung $|\Psi'\rangle = \begin{cases} |\uparrow\rangle & \text{mit Wahrscheinlichkeit } 50\% \\ |\rightarrow\rangle & \text{mit Wahrscheinlichkeit } 50\% \end{cases}$

Das BB84-Protokoll

Sender $\equiv$ Alice

Empfänger $\equiv$ Bob

Alice hat Nachricht mit N Bits zu versenden

Das BB84-Protokoll

Sender $\equiv$ Alice Empfänger $\equiv$ Bob

Alice hat Nachricht mit N Bits zu versenden

Übertragung des Schlüssels:

- Alice benötigt One-Time-Pad-Schlüssel:
  Zufallsstring s aus $4N$ Bits: $s \in \{0,1\}^{4N}$

Das BB84-Protokoll

Sender $\equiv$ Alice Empfänger $\equiv$ Bob

Alice hat Nachricht mit N Bits zu versenden

Übertragung des Schlüssels:

- Alice benötigt One-Time-Pad-Schlüssel:
  Zufallsstring s aus $4N$ Bits: $s \in \{0,1\}^{4N}$
- Bit s_i soll durch Photonenpolarisation übertragen werden

Das BB84-Protokoll

Sender $\equiv$ Alice Empfänger $\equiv$ Bob

Alice hat Nachricht mit N Bits zu versenden

Übertragung des Schlüssels:

- Alice benötigt One-Time-Pad-Schlüssel:
  Zufallsstring s aus $4N$ Bits: $s \in \{0,1\}^{4N}$
- Bit s_i soll durch Photonenpolarisation übertragen werden
- Alice hat zwei Basen zur Verfügung

Das BB84-Protokoll

Sender $\equiv$ Alice Empfänger $\equiv$ Bob

Alice hat Nachricht mit N Bits zu versenden

Übertragung des Schlüssels:

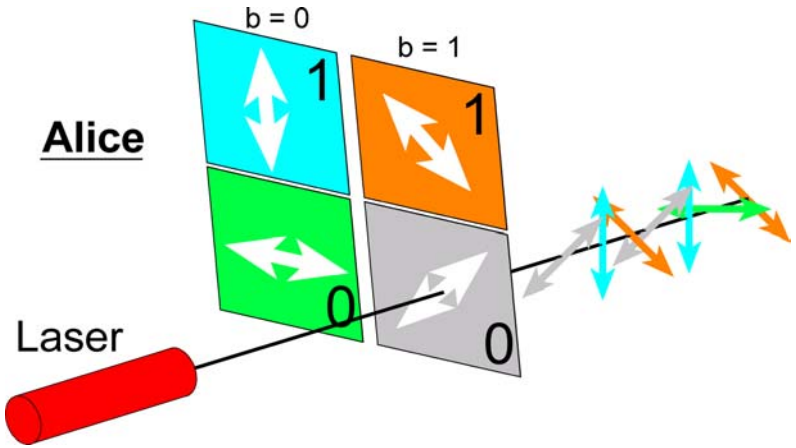
- Alice benötigt One-Time-Pad-Schlüssel:
  Zufallsstring s aus $4N$ Bits: $s \in \{0,1\}^{4N}$
- Bit s_i soll durch Photonenpolarisation übertragen werden
- Alice hat zwei Basen zur Verfügung
  wählt zu jedem Bit s_i die Basis b_i zufällig

Das BB84-Protokoll

Übertragung des Schlüssels:

Alice:

- $s \in \{0,1\}^{4N}$
- $b \in \{0,1\}^{4N}$

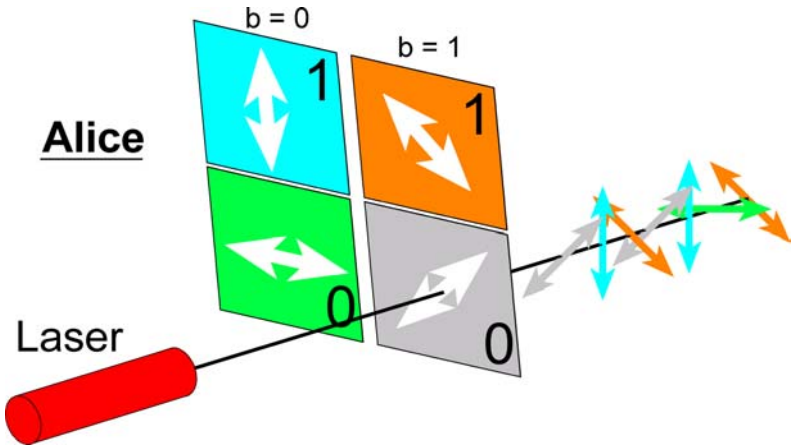


Das BB84-Protokoll

Übertragung des Schlüssels:

Alice:

- $s \in \{0,1\}^{4N}$
- $b \in \{0,1\}^{4N}$



Sende Photon Φ_i

- falls $b_i = 0$: $|\Phi_i\rangle = \begin{cases} |\uparrow\rangle & \text{falls } s_i = 1 \\ |\rightarrow\rangle & \text{falls } s_i = 0 \end{cases}$

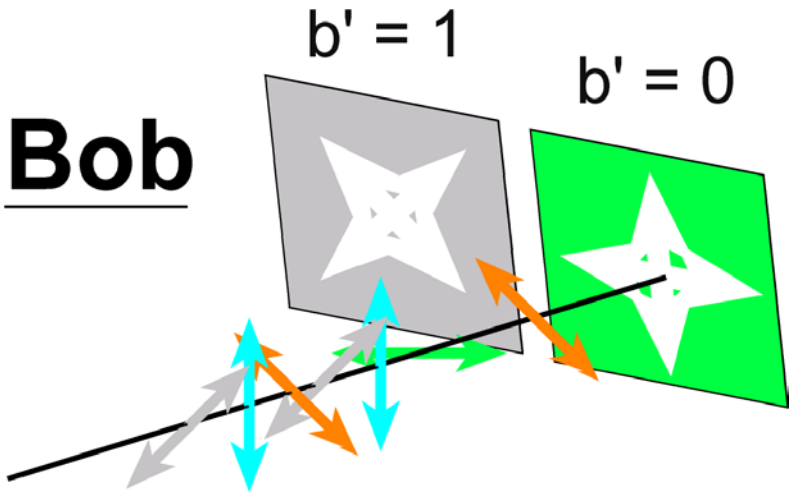
  falls $b_i = 1$: $|\Phi_i\rangle = \begin{cases} |\searrow\rangle & \text{falls } s_i = 1 \\ |\nearrow\rangle & \text{falls } s_i = 0 \end{cases}$

Das BB84-Protokoll

Empfangen des Schlüssels:

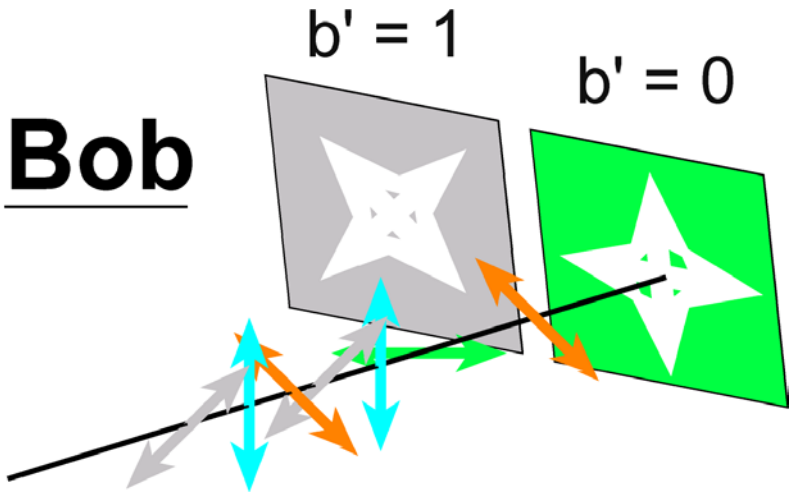
Bob empfängt Strom von Photonen $|\Phi_i\rangle$

- Bob kennt die von Alice gewählten Basen nicht



Das BB84-Protokoll

Empfangen des Schlüssels:

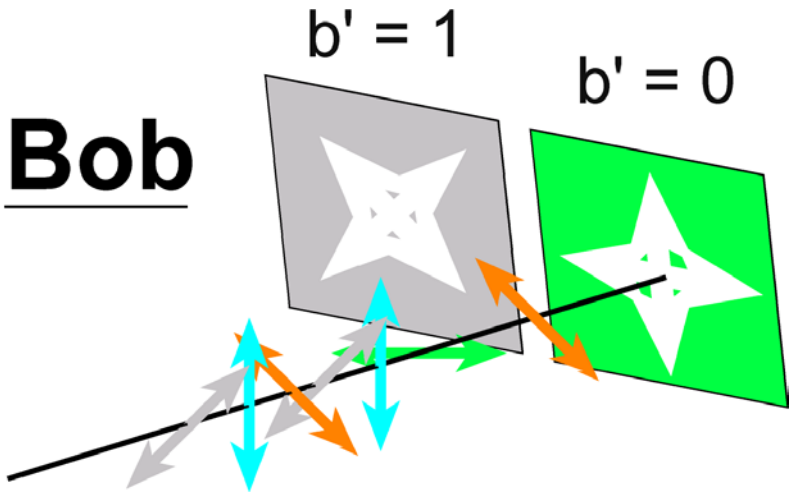


Bob empfängt Strom von Photonen $|\Phi_i\rangle$

- Bob kennt die von Alice gewählten Basen nicht
- Bob wählt zufällig Messbasen b'_i

Das BB84-Protokoll

Empfangen des Schlüssels:



Bob empfängt Strom von Photonen $|\Phi_i\rangle$

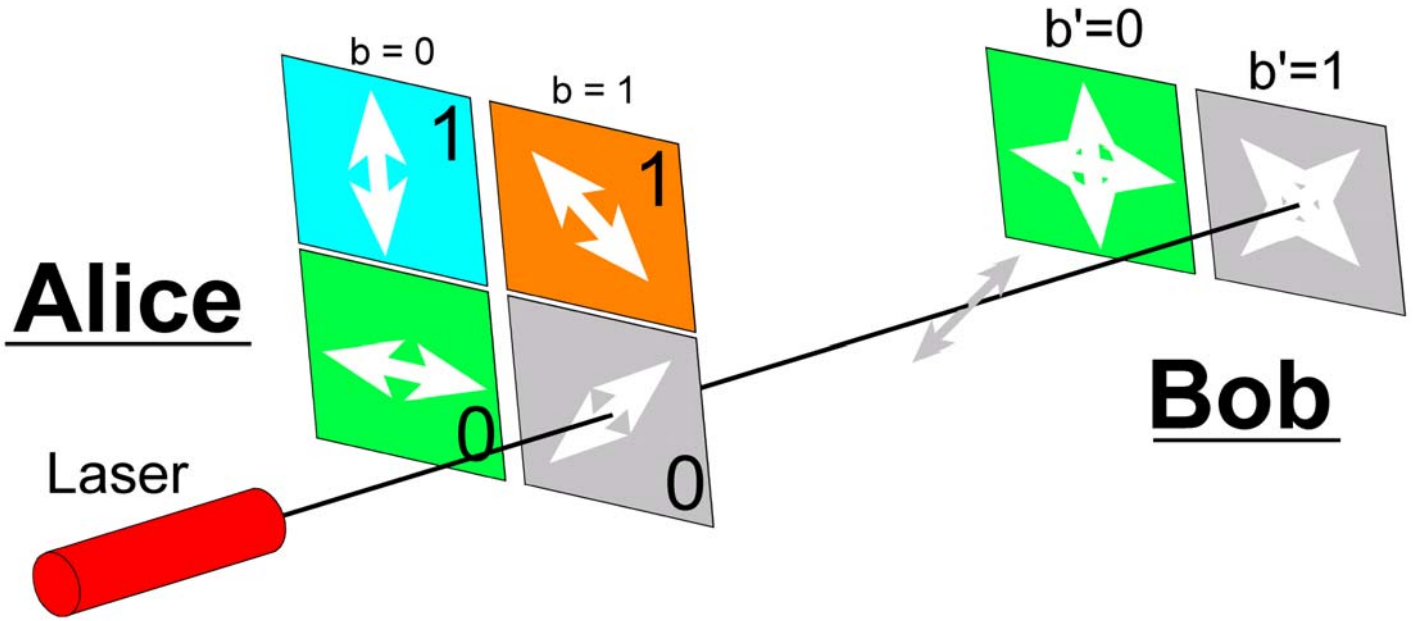
- Bob kennt die von Alice gewählten Basen nicht
- Bob wählt zufällig Messbasen b'_i

Bob merkt sich für jedes Photon $|\Phi_i\rangle$

- gewählte Messbasis b'_i
- Messergebnis s'_i

Das BB84-Protokoll

Empfangen des Schlüssels:

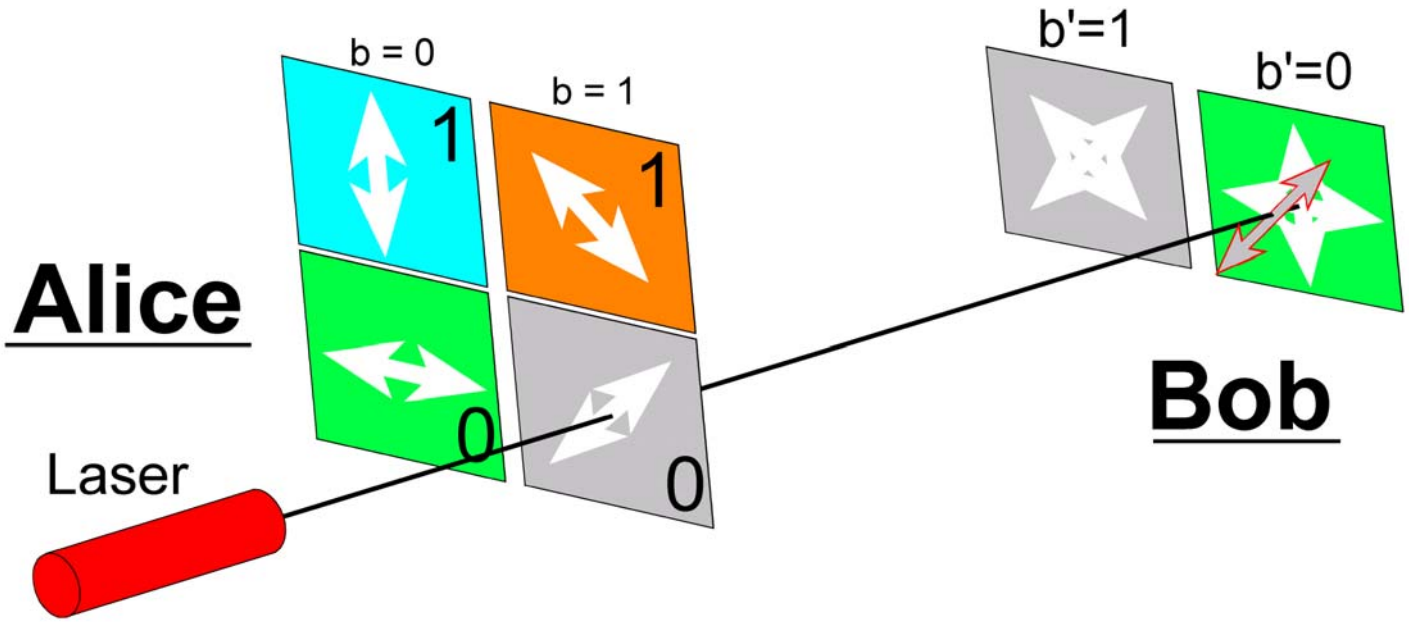


Messung in richtiger Basis:

$s'_i = s_i$ mit 100% Wahrscheinlichkeit

Das BB84-Protokoll

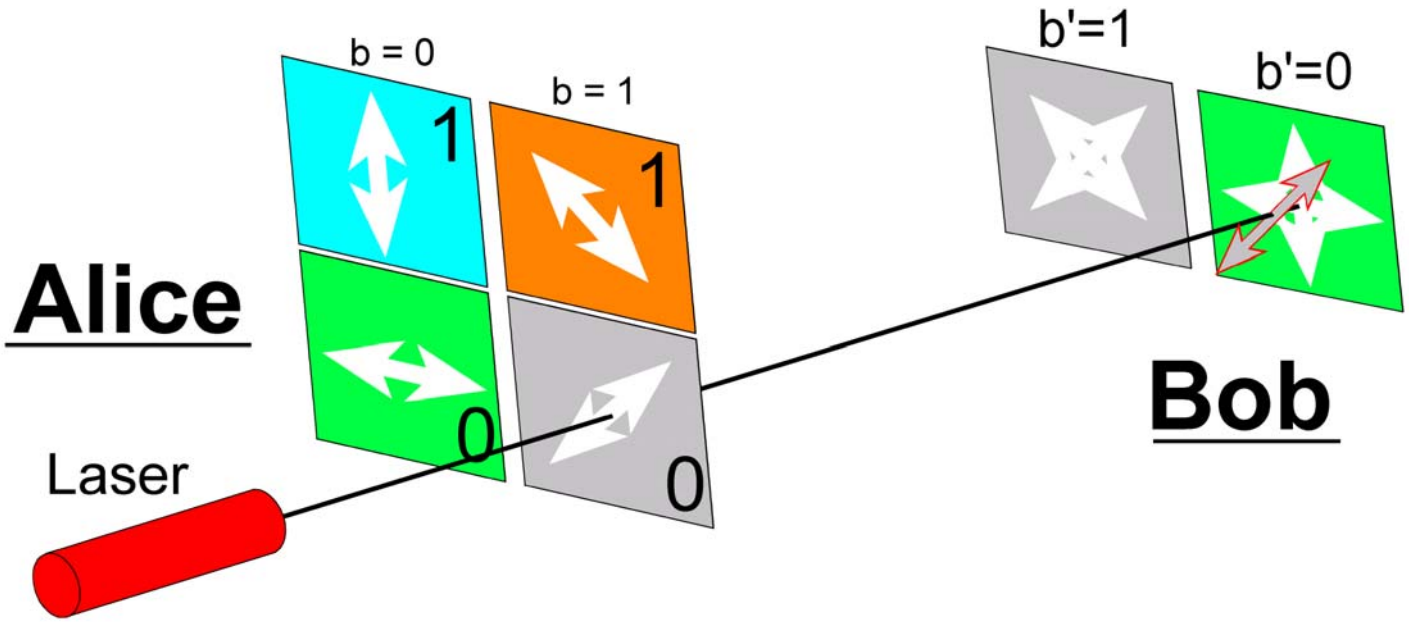
Empfangen des Schlüssels:



Messung in falscher Basis:

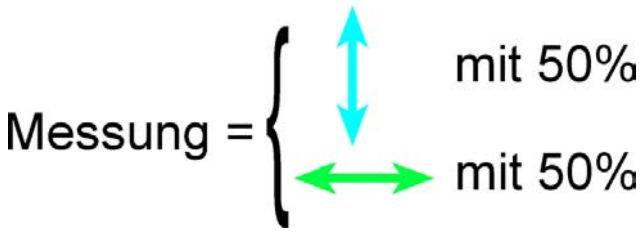
Das BB84-Protokoll

Empfangen des Schlüssels:



Messung in falscher Basis:

$s_i' \neq s_i$ mit 50% Wahrscheinlichkeit:



Das BB84-Protokoll

Erzeugung des One-Time-Pads:

- Abgleich von b und b' über öffentlichen Kanal

Das BB84-Protokoll

Erzeugung des One-Time-Pads:

- Abgleich von b und b' über öffentlichen Kanal
- Alle Bits s_i mit $b_i = b'_i \rightarrow$ Schlüssel K

Das BB84-Protokoll

Erzeugung des One-Time-Pads:

- Abgleich von b und b' über öffentlichen Kanal
- Alle Bits s_i mit $b_i = b'_i \rightarrow$ Schlüssel K

Eigenschaften des Schlüssels K:

- Bob wählt in 50% der Fälle die richtige Basis
  $\Rightarrow$ statistisch hat K die Länge $2N$

Das BB84-Protokoll

Beispiel:

Basis b = 0 

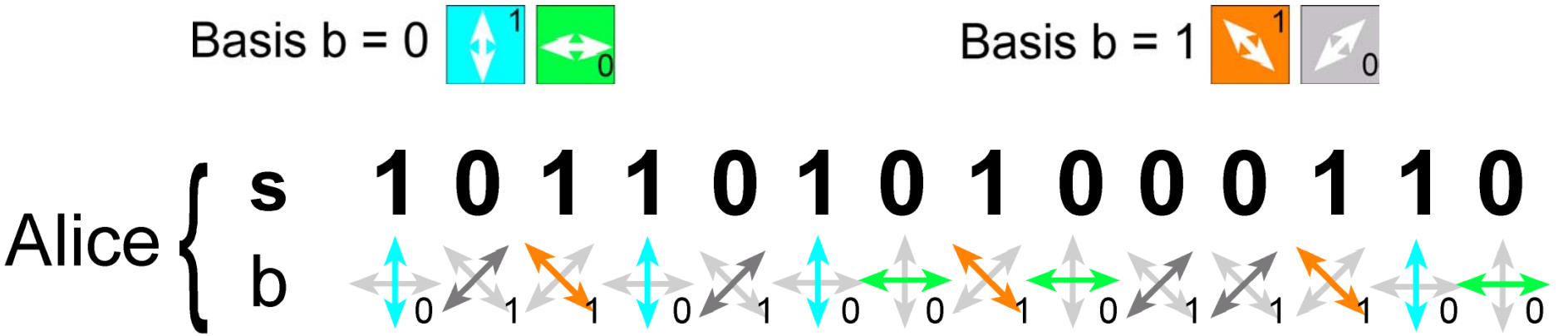
Basis b = 1 

Alice { **s 1 0 1 1 0 1 0 1 0 0 0 1 1 0**

zu übertragen: Rohschlüssel s

Das BB84-Protokoll

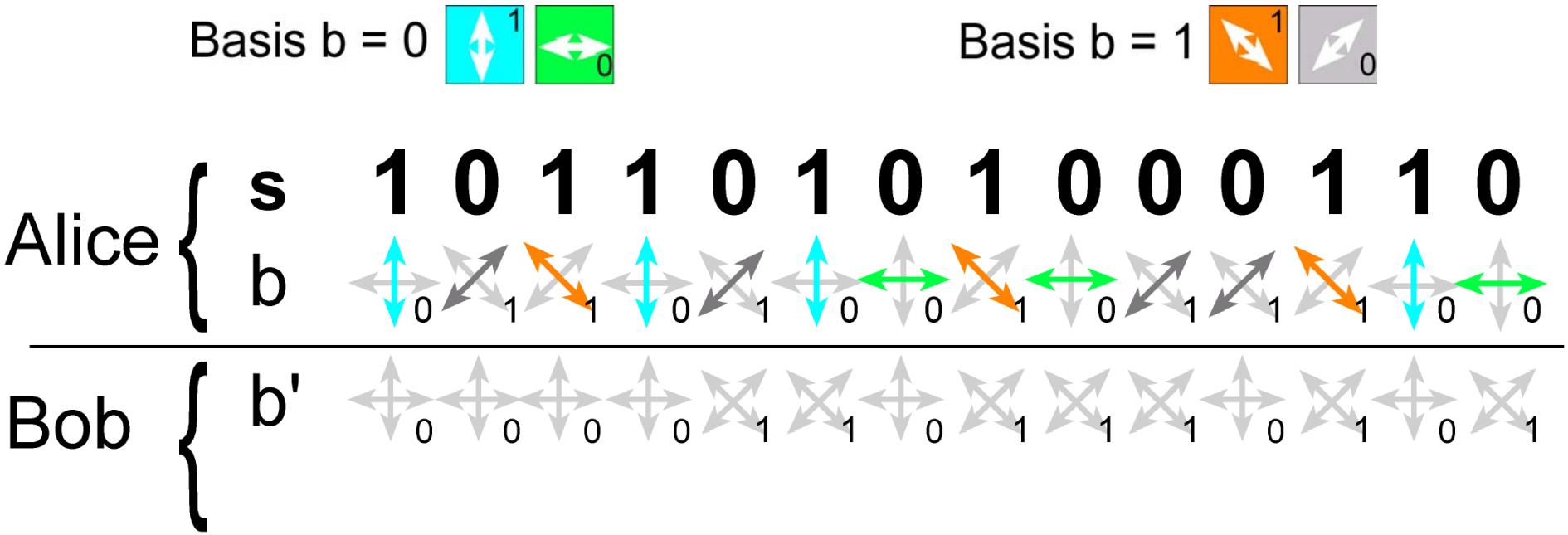
Beispiel:



Versenden der s_i in zufällig gewählten Basen b

Das BB84-Protokoll

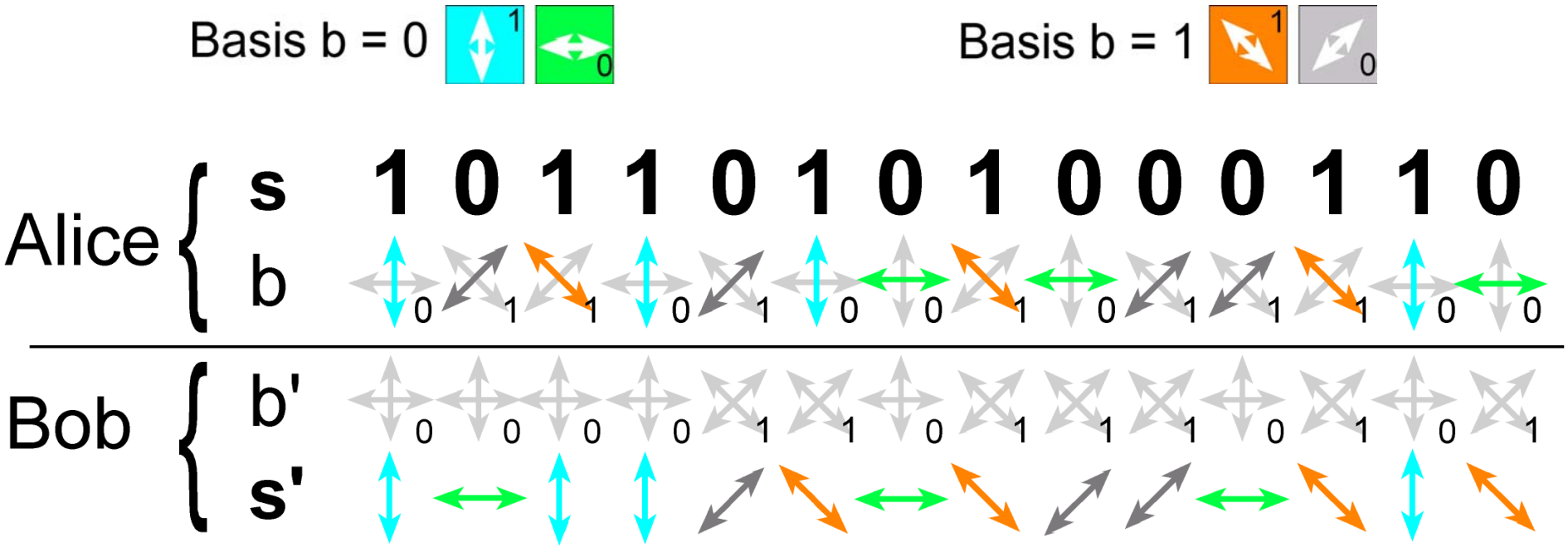
Beispiel:



Messen bezüglich zufälliger Basen b'

Das BB84-Protokoll

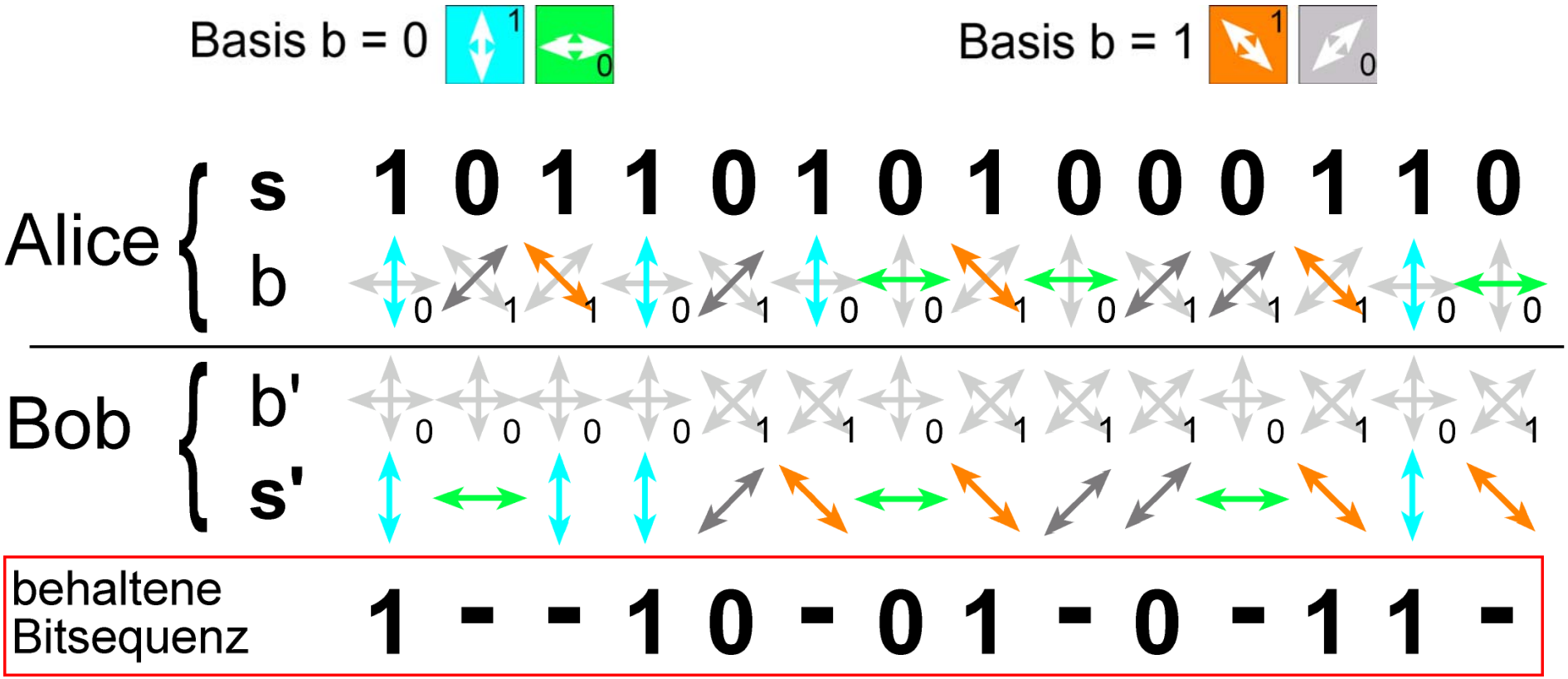
Beispiel:



empfangener Rohschlüssel s'

Das BB84-Protokoll

Beispiel:



Abgleich von b und b'

$\Rightarrow$ behaltene Bitsequenz

Das BB84-Protokoll

Abhörversuch: durch Eve

Das BB84-Protokoll

Abhörversuch: durch Eve

- Zum Zeitpunkt der Übertragung kennt Eve die Sendebasis b nicht.

Das BB84-Protokoll

Abhörversuch: durch Eve

- Zum Zeitpunkt der Übertragung kennt Eve die Sendebasis b nicht.

Taktik?

- Quantenzustand $|\Phi_i\rangle$ kopieren

Das BB84-Protokoll

Abhörversuch: durch Eve

- Zum Zeitpunkt der Übertragung kennt Eve die Sendebasis b nicht.

Taktik?

- Quantenzustand $|\Phi_i\rangle$ kopieren

- nach Bekanntgabe von b: Kopie in Sendebasis messen

Das BB84-Protokoll

Abhörversuch: durch Eve

- Zum Zeitpunkt der Übertragung kennt Eve die Sendebasis b nicht.

Taktik?

- Quantenzustand $|\Phi_i\rangle$ kopieren

- nach Bekanntgabe von b: Kopie in Sendebasis messen
- damit s komplett bekannt

Das BB84-Protokoll

Abhörversuch: durch Eve

- Zum Zeitpunkt der Übertragung kennt Eve die Sendebasis b nicht.

Taktik?

- Quantenzustand $|\Phi_i\rangle$ kopieren
  verboten durch No-Cloning-Theorem
- nach Bekanntgabe von b: Kopie in Sendebasis messen
- damit s komplett bekannt

unmöglich!

No-Cloning-Theorem

Kopieren von Superpositionszuständen ist nicht möglich:

No-Cloning-Theorem

Kopieren von Superpositionszuständen ist nicht möglich:

No-Cloning-Theorem:

Es gibt keine quantenmechanische Operation $\widehat{U}$, die ein Quanten-Bit kopieren kann.

No-Cloning-Theorem

Kopieren von Superpositionszuständen ist nicht möglich:

No-Cloning-Theorem:

Es gibt keine quantenmechanische Operation $\widehat{U}$, die ein Quanten-Bit kopieren kann.

Kopieren von reinen Zuständen wie $|\Psi\rangle = |\uparrow\rangle$ jedoch möglich

Das BB84-Protokoll

Abhörversuch: durch Eve

- Zum Zeitpunkt der Übertragung kennt Eve die Sendebasis b nicht.
- Kopieren des Schlüssels s unmöglich

Das BB84-Protokoll

Abhörversuch: durch Eve

- Zum Zeitpunkt der Übertragung kennt Eve die Sendebasis b nicht.
- Kopieren des Schlüssels s unmöglich

Taktik:

- bei jeder Messung Basis $\widetilde{b}_i$ raten

Das BB84-Protokoll

Abhörversuch: durch Eve

- Zum Zeitpunkt der Übertragung kennt Eve die Sendebasis b nicht.
- Kopieren des Schlüssels s unmöglich

Taktik:

- bei jeder Messung Basis $\widetilde{b}_i$ raten
- Messung in falscher Basis zerstört Superpositionszustand $|\Phi_i\rangle$

Das BB84-Protokoll

Abhörversuch: durch Eve

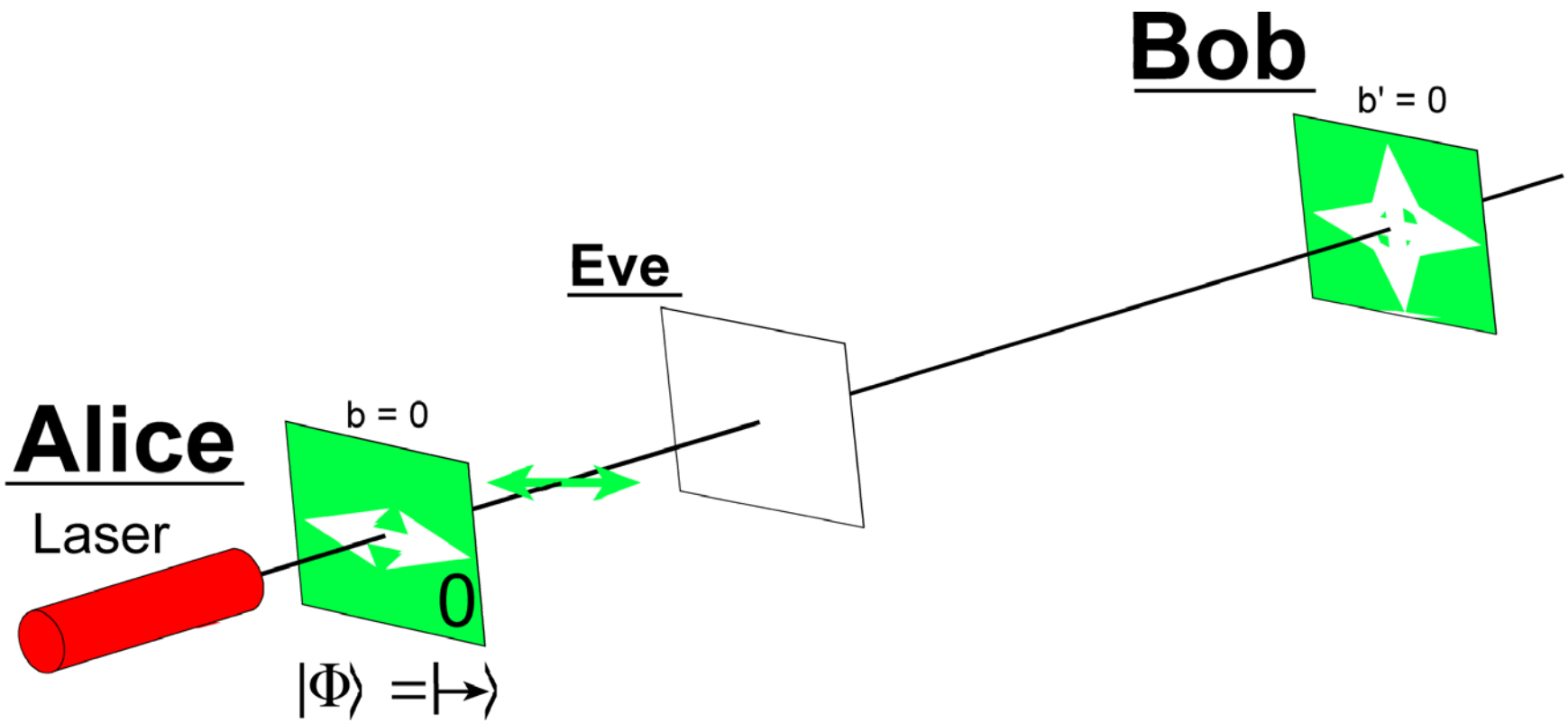
- Zum Zeitpunkt der Übertragung kennt Eve die Sendebasis b nicht.
- Kopieren des Schlüssels s unmöglich

Taktik:

- bei jeder Messung Basis $\widetilde{b}_i$ raten
- Messung in falscher Basis zerstört Superpositionszustand $|\Phi_i\rangle$
- Weiterschicken des Messergebnisses $|\widetilde{\Phi}_i\rangle$ an Bob

Das BB84-Protokoll

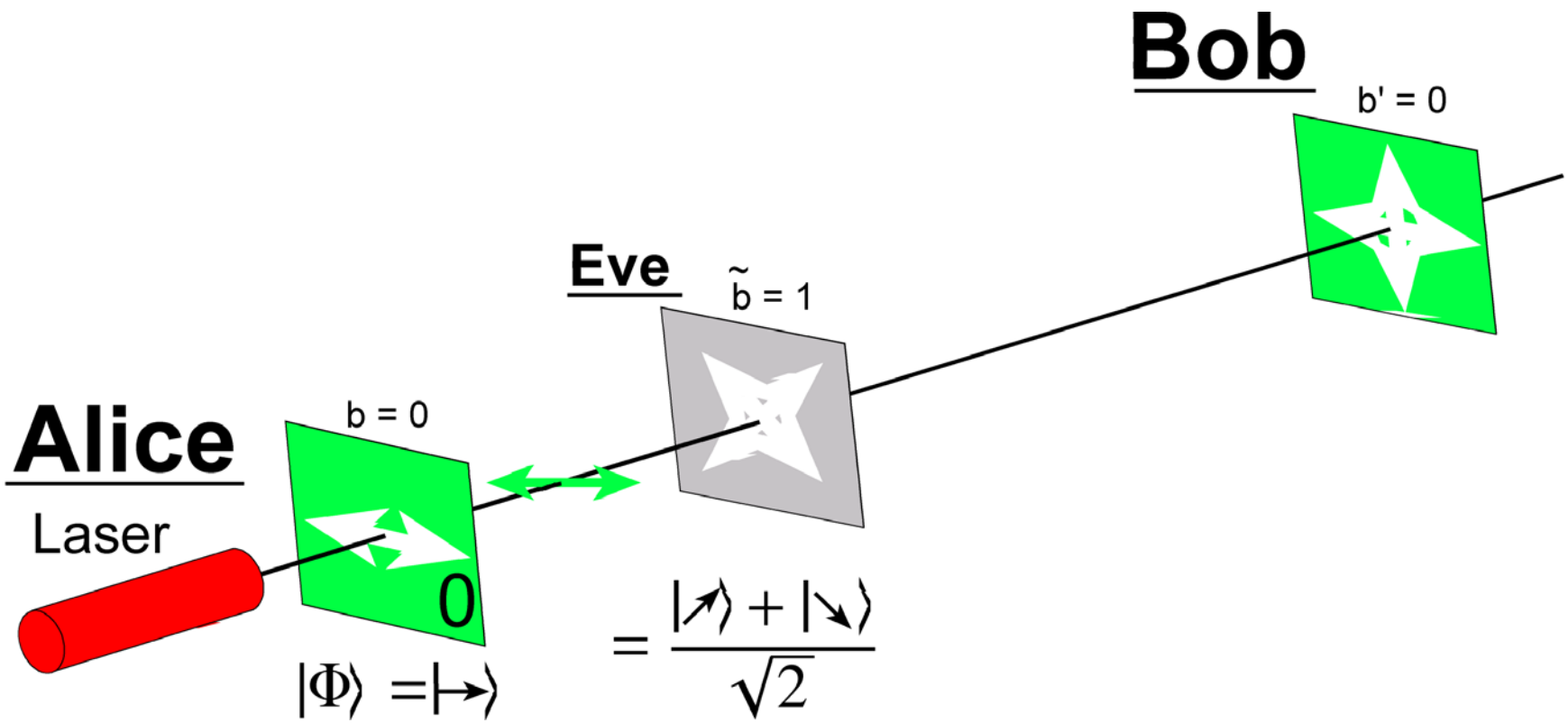
Abhörversuch:



Alice versendet Bit $s_i = 0$ in Basis $b_i = 0$:

Das BB84-Protokoll

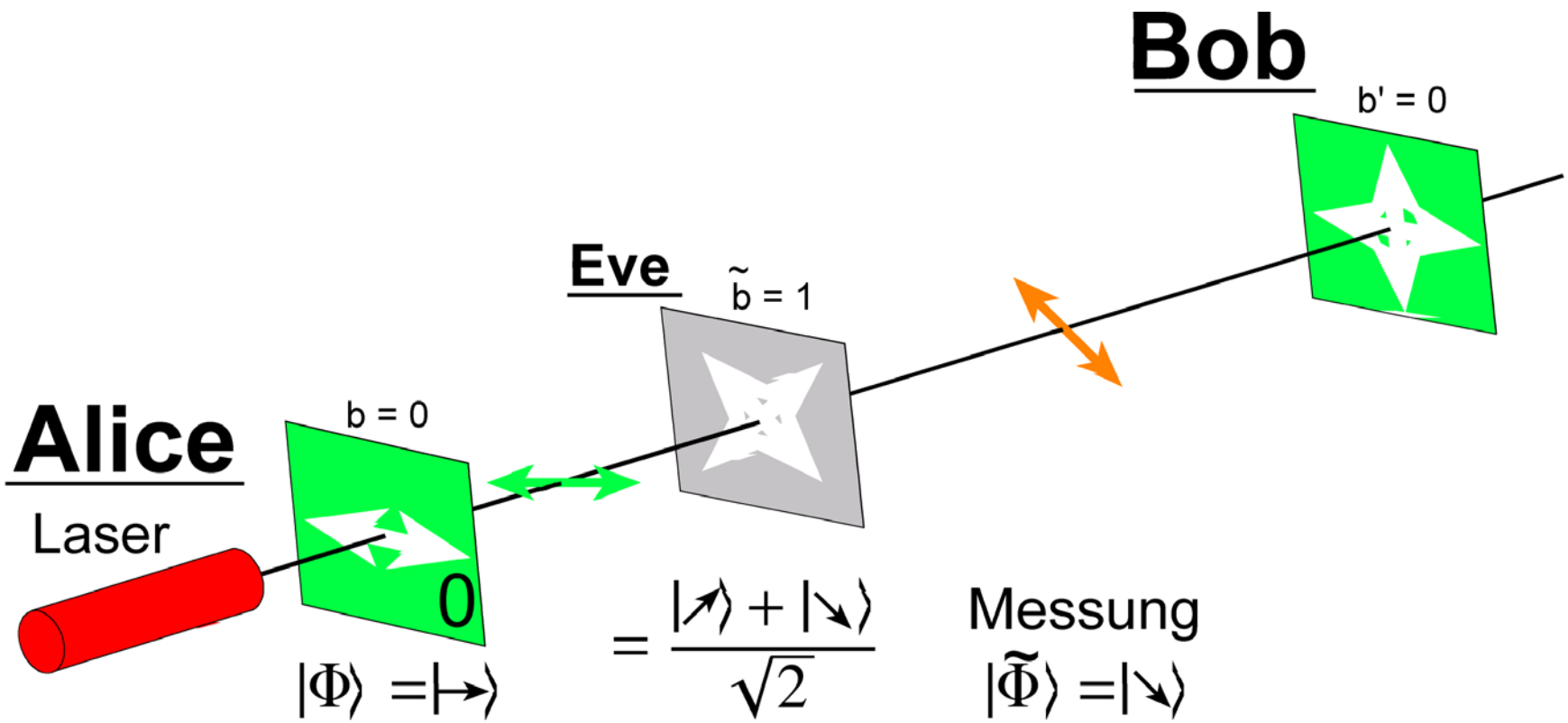
Abhörversuch:



Eve wählt Basis $\widetilde{b}_i = 1$

Das BB84-Protokoll

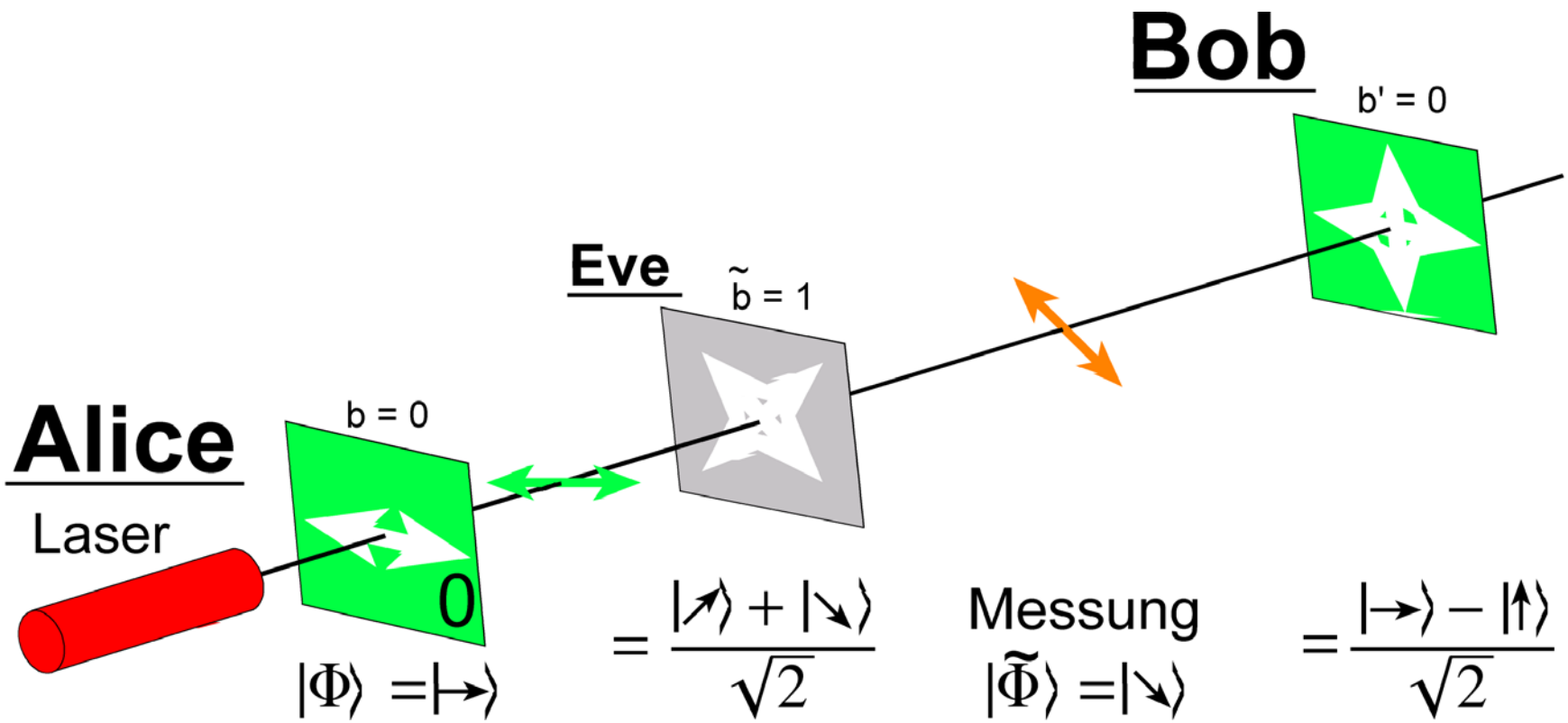
Abhörversuch:



Eve misst Zustand $|\widetilde{\Phi}_i\rangle = |\searrow\rangle$

Das BB84-Protokoll

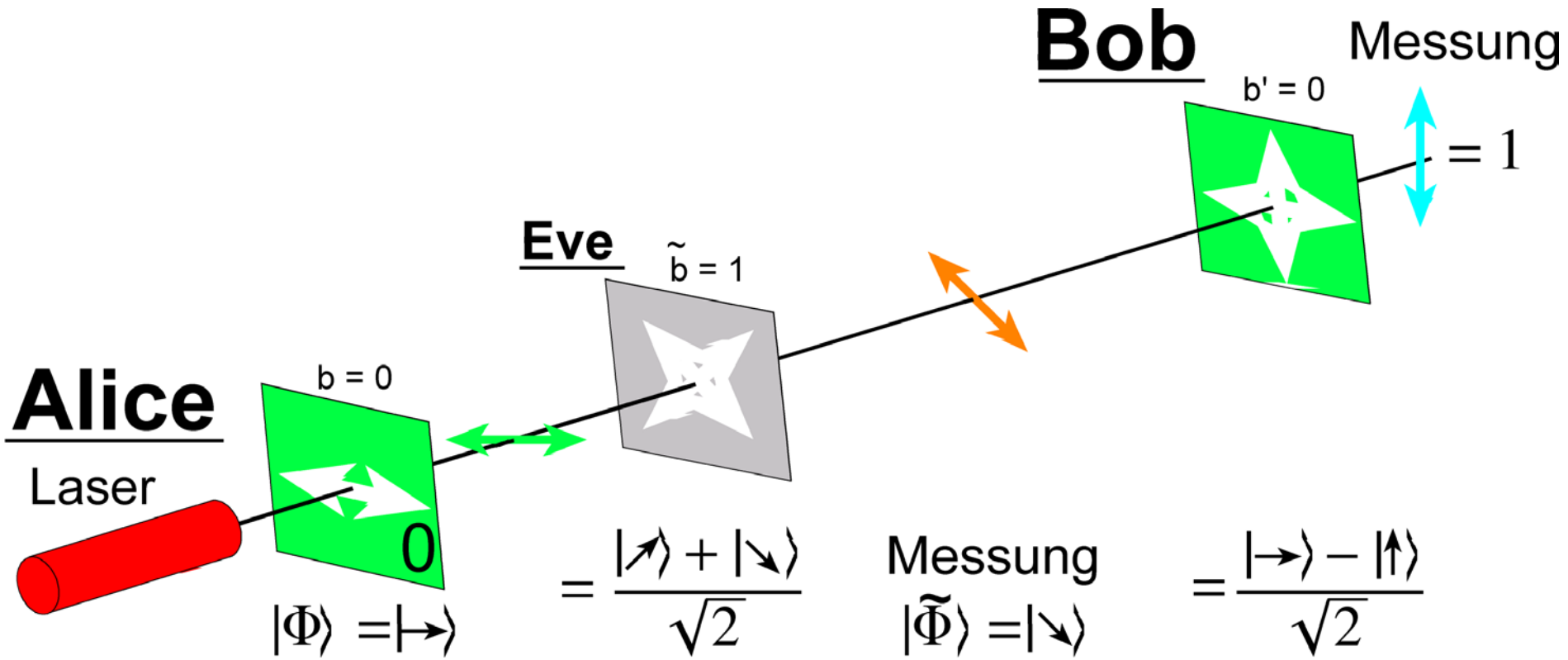
Abhörversuch:



Bob wählt gleiche Basis wie Alice:

Das BB84-Protokoll

Abhörversuch:



Bob wählt gleiche Basis wie Alice:
misst falschen Wert $1 = s_i' \neq s_i = 0$

Das BB84-Protokoll

Abhörversuch:

Betrachtung der $2N$ Bits, bei denen Alice und Bob gleiche Basis wählen:

Das BB84-Protokoll

Abhörversuch:

Betrachtung der $2N$ Bits, bei denen Alice und Bob gleiche Basis wählen:

- Eve wählt falsche Basis mit $\frac{1}{2}$ Wahrscheinlichkeit

Das BB84-Protokoll

Abhörversuch:

Betrachtung der $2N$ Bits, bei denen Alice und Bob gleiche Basis wählen:

- Eve wählt falsche Basis mit $\frac{1}{2}$ Wahrscheinlichkeit
  - Eve schickt Superpositionszustand an Bob

Das BB84-Protokoll

Abhörversuch:

Betrachtung der $2N$ Bits, bei denen Alice und Bob gleiche Basis wählen:

- Eve wählt falsche Basis mit $\frac{1}{2}$ Wahrscheinlichkeit
  - Eve schickt Superpositionszustand an Bob
  - Bob misst mit $\frac{1}{2}$ Wahrscheinlichkeit ein Ergebnis $s_i' \neq s_i$

Das BB84-Protokoll

Abhörversuch:

Betrachtung der $2N$ Bits, bei denen Alice und Bob gleiche Basis wählen:

- Eve wählt falsche Basis mit $\frac{1}{2}$ Wahrscheinlichkeit
  - Eve schickt Superpositionszustand an Bob
  - Bob misst mit $\frac{1}{2}$ Wahrscheinlichkeit ein Ergebnis $s_i' \neq s_i$

Wahrscheinlichkeit für falsches Ergebnis bei Bob: $\frac{1}{4} = 25\%$

Das BB84-Protokoll

Abhörversuch:

Betrachtung der $2N$ Bits, bei denen Alice und Bob gleiche Basis wählen:

- Eve wählt falsche Basis mit $\frac{1}{2}$ Wahrscheinlichkeit
  - Eve schickt Superpositionszustand an Bob
  - Bob misst mit $\frac{1}{2}$ Wahrscheinlichkeit ein Ergebnis $s_i' \neq s_i$

Wahrscheinlichkeit für falsches Ergebnis bei Bob: $\frac{1}{4} = 25\%$

abhörfreie Übertragung:

gemessenes Bit s_i' ist immer gleich versendetem Bit s_i

Das BB84-Protokoll

Entdecken eines Abhörversuchs:

- Alice und Bob haben bei $2N$ Bits gleiche Basis gewählt

Das BB84-Protokoll

Entdecken eines Abhörversuchs:

- Alice und Bob haben bei $2N$ Bits gleiche Basis gewählt
- Vergleichen von N dieser Bits:

Das BB84-Protokoll

Entdecken eines Abhörversuchs:

- Alice und Bob haben bei $2N$ Bits gleiche Basis gewählt
- Vergleichen von N dieser Bits:
  - alle N Bits stimmen überein
    $\Rightarrow$ Übertragung war sicher

Das BB84-Protokoll

Entdecken eines Abhörversuchs:

- Alice und Bob haben bei $2N$ Bits gleiche Basis gewählt
- Vergleichen von N dieser Bits:
  - alle N Bits stimmen überein
    $\Rightarrow$ Übertragung war sicher
  - es stimmen Bits nicht überein
    $\Rightarrow$ Übertragung wird abgehört

Das BB84-Protokoll

Entdecken eines Abhörversuchs:

- Alice und Bob haben bei $2N$ Bits gleiche Basis gewählt
- Vergleichen von N dieser Bits:
  - alle N Bits stimmen überein
    $\Rightarrow$ Übertragung war sicher
  - es stimmen Bits nicht überein
    $\Rightarrow$ Übertragung wird abgehört

Es bleiben N Bits:

bei denen Alice und Bob die gleiche Basis gewählt haben,

Das BB84-Protokoll

Entdecken eines Abhörversuchs:

- Alice und Bob haben bei $2N$ Bits gleiche Basis gewählt
- Vergleichen von N dieser Bits:
  - alle N Bits stimmen überein
    $\Rightarrow$ Übertragung war sicher
  - es stimmen Bits nicht überein
    $\Rightarrow$ Übertragung wird abgehört

Es bleiben N Bits:

bei denen Alice und Bob die gleiche Basis gewählt haben, die nie öffentlich ausgetauscht wurden

Das BB84-Protokoll

Entdecken eines Abhörversuchs:

- Alice und Bob haben bei $2N$ Bits gleiche Basis gewählt
- Vergleichen von N dieser Bits:
  - alle N Bits stimmen überein
    $\Rightarrow$ Übertragung war sicher
  - es stimmen Bits nicht überein
    $\Rightarrow$ Übertragung wird abgehört

Es bleiben N Bits:

bei denen Alice und Bob die gleiche Basis gewählt haben, die nie öffentlich ausgetauscht wurden
$\rightarrow$ **One-Time-Pad-Schlüssel**

Das BB84-Protokoll

Schwachstellen des BB84-Protokolls

- BB84 benötigt Einzelphotonenpulse
- durch dauerhaftes Abhören wird Übertragung unmöglich

Das BB84-Protokoll verbietet ein *vollständiges* Abhören der Nachricht.
Eve kann über Teile der Nachricht Informationen erhalten.

- durch Verstecken im Leitungsrauschen
- nicht perfektes Quantenclonen möglich

Das BB84-Protokoll

Realisierung:

Firma	Trägermedium	Reichweite
id Quantique Schweiz	optisches Glasfasersystem	max. 100km
QinetiQ England	Luft	max. 10km
NEC Japan	optisches Glasfasersystem	max. 150km

Literatur

Quantum Computation and Quantum Information
von: Michael A. Nielsen & Isaac L. Chuang
Cambridge University Press

Quantum cryptography
von: N. Gisin, G. Ribordy, W. Tittel & H. Zbinden
Reviews of Modern Physics 74, Januar 2002

Quantum copying: Beyond the no-cloning-theorem
von: V. Bužek & M. Hillery
Physical Review Articles 54-3, September 1996

Optimal Quantum Cloning Machines
von: N. Gisin & S. Massar
Physical Review Letters 79-11, September 1997

Ende