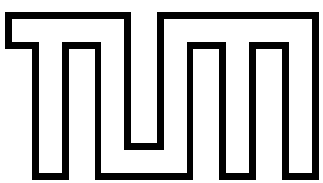
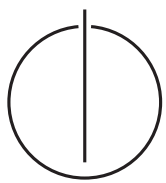
Quantenkryptographie

Tobias Mühlbauer

Technische Universität München

Hauptseminar Kryptographische Protokolle 2009





Outline

Outline

Outline

Outline

Outline

Klassische Kryptographie

Worauf basiert die klassische Kryptographie?

- **Klassischen Verschlüsselungsverfahren**:

Klassische Kryptographie

Worauf basiert die klassische Kryptographie?

- **Klassischen Verschlüsselungsverfahren**:
  - **Faktorisierung** (z.B. RSA)

Klassische Kryptographie

Worauf basiert die klassische Kryptographie?

- **Klassischen Verschlüsselungsverfahren**:
  - **Faktorisierung** (z.B. RSA)
  - **Diskreter Logarithmus** (z.B. ElGamal)

Klassische Kryptographie

Worauf basiert die klassische Kryptographie?

- **Klassischen Verschlüsselungsverfahren**:
  - **Faktorisierung** (z.B. RSA)
  - **Diskreter Logarithmus** (z.B. ElGamal)
- Annahme: Faktorisierung und diskreter Logarithmus **mathematisch hart** $\Rightarrow$ Beweisbar sicher

Klassische Kryptographie

Was macht die klassische Kryptographie angreifbar?

- Annahme der mathematischen Härte könnte falsch sein

Klassische Kryptographie

Was macht die klassische Kryptographie angreifbar?

- Annahme der mathematischen Härte könnte falsch sein
- **Quantencomputer** mit dem **Algorithmus nach Shor**:

Klassische Kryptographie

Was macht die klassische Kryptographie angreifbar?

- Annahme der mathematischen Härte könnte falsch sein
- **Quantencomputer** mit dem **Algorithmus nach Shor**:
  - Faktorisierung in polynomieller Zeit ($O((logN)^3)$)

Klassische Kryptographie

Was macht die klassische Kryptographie angreifbar?

- Annahme der mathematischen Härte könnte falsch sein
- **Quantencomputer** mit dem **Algorithmus nach Shor**:
  - Faktorisierung in polynomieller Zeit ($O((logN)^3)$)
  - Diskreter Logarithmus in polynomieller Zeit

Klassische Kryptographie

Was macht die klassische Kryptographie angreifbar?

- Annahme der mathematischen Härte könnte falsch sein
- **Quantencomputer** mit dem **Algorithmus nach Shor**:
  - Faktorisierung in polynomieller Zeit ($O((logN)^3)$)
  - Diskreter Logarithmus in polynomieller Zeit
- 2001: IBM führt erstmals erfolgreich den Shor-Algorithmus mit der Zahl 15 aus

Klassische Kryptographie

Was macht die klassische Kryptographie angreifbar?

- Annahme der mathematischen Härte könnte falsch sein
- **Quantencomputer** mit dem **Algorithmus nach Shor**:
  - Faktorisierung in polynomieller Zeit ($O((logN)^3)$)
  - Diskreter Logarithmus in polynomieller Zeit
- 2001: IBM führt erstmals erfolgreich den Shor-Algorithmus mit der Zahl 15 aus
- 2008: D-Wave Systems hat angeblich einen 128 Qubit Computerchip hergestellt

Outline

Alternativen zur klassischen Kryptographie

- Anwendbare Alternativen zur klassischen Kryptographie ((noch) keine effizienten Algorithmen bekannt)

Alternativen zur klassischen Kryptographie

- Anwendbare Alternativen zur klassischen Kryptographie ((noch) keine effizienten Algorithmen bekannt)
- **Perfekte Sicherheit**: Verwendung eines **One-Time Pad** (Schlüssel in Länge der Nachricht, welcher nur einmal verwendet wird)

Alternativen zur klassischen Kryptographie

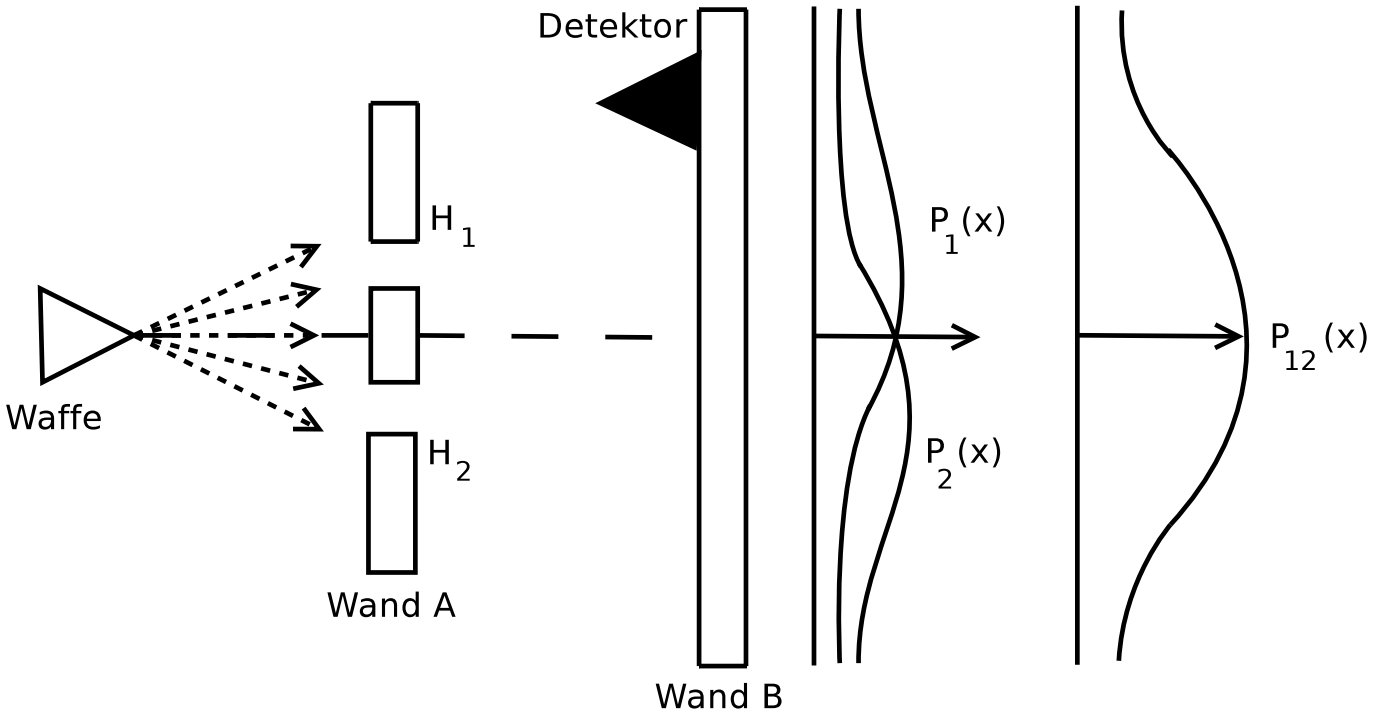
- Anwendbare Alternativen zur klassischen Kryptographie ((noch) keine effizienten Algorithmen bekannt)
- **Perfekte Sicherheit**: Verwendung eines **One-Time Pad** (Schlüssel in Länge der Nachricht, welcher nur einmal verwendet wird)
- Beispiel: TAN als One-Time Pad für Überweisungen

Alternativen zur klassischen Kryptographie

- Anwendbare Alternativen zur klassischen Kryptographie ((noch) keine effizienten Algorithmen bekannt)
- **Perfekte Sicherheit**: Verwendung eines **One-Time Pad** (Schlüssel in Länge der Nachricht, welcher nur einmal verwendet wird)
- Beispiel: TAN als One-Time Pad für Überweisungen
- **Heute: Quantenkryptographie** basierend auf physikalischen Grundlagen und der Anwendung eines One-Time Pads

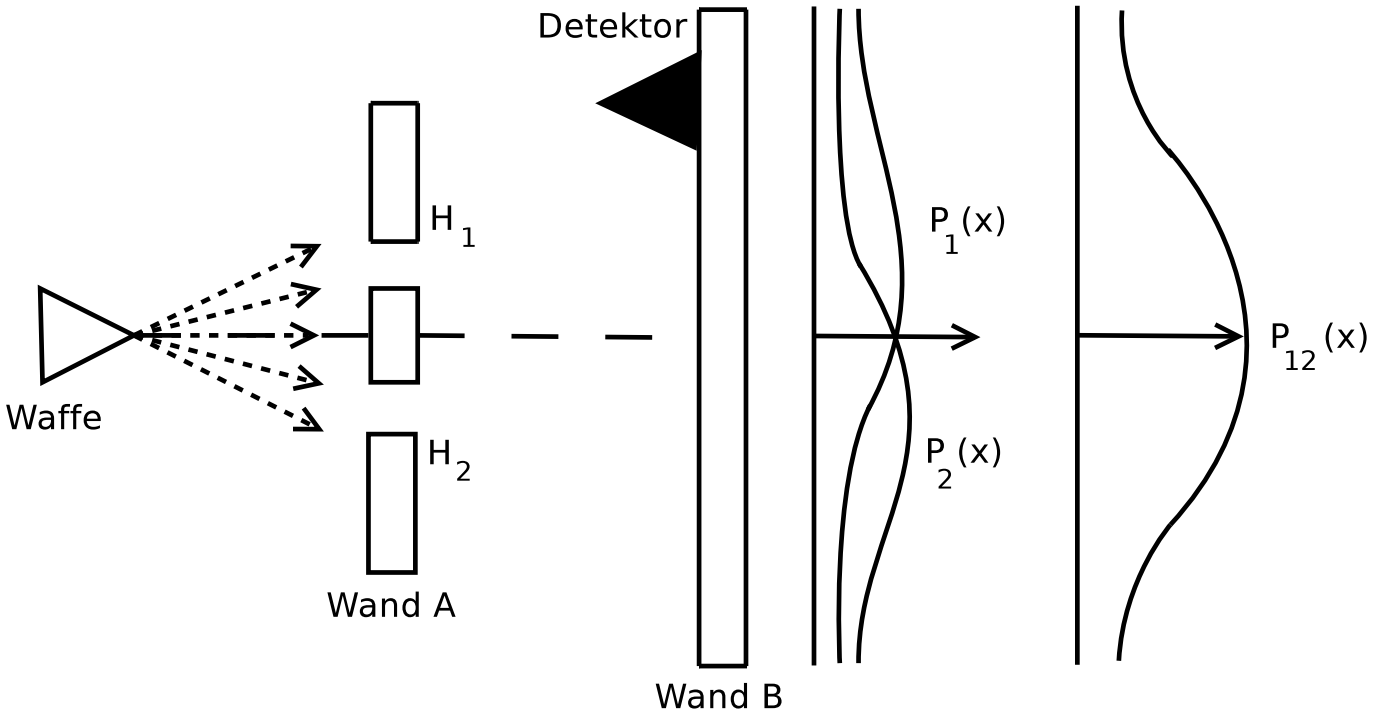
Outline

Klassisches Experiment mit Patronen



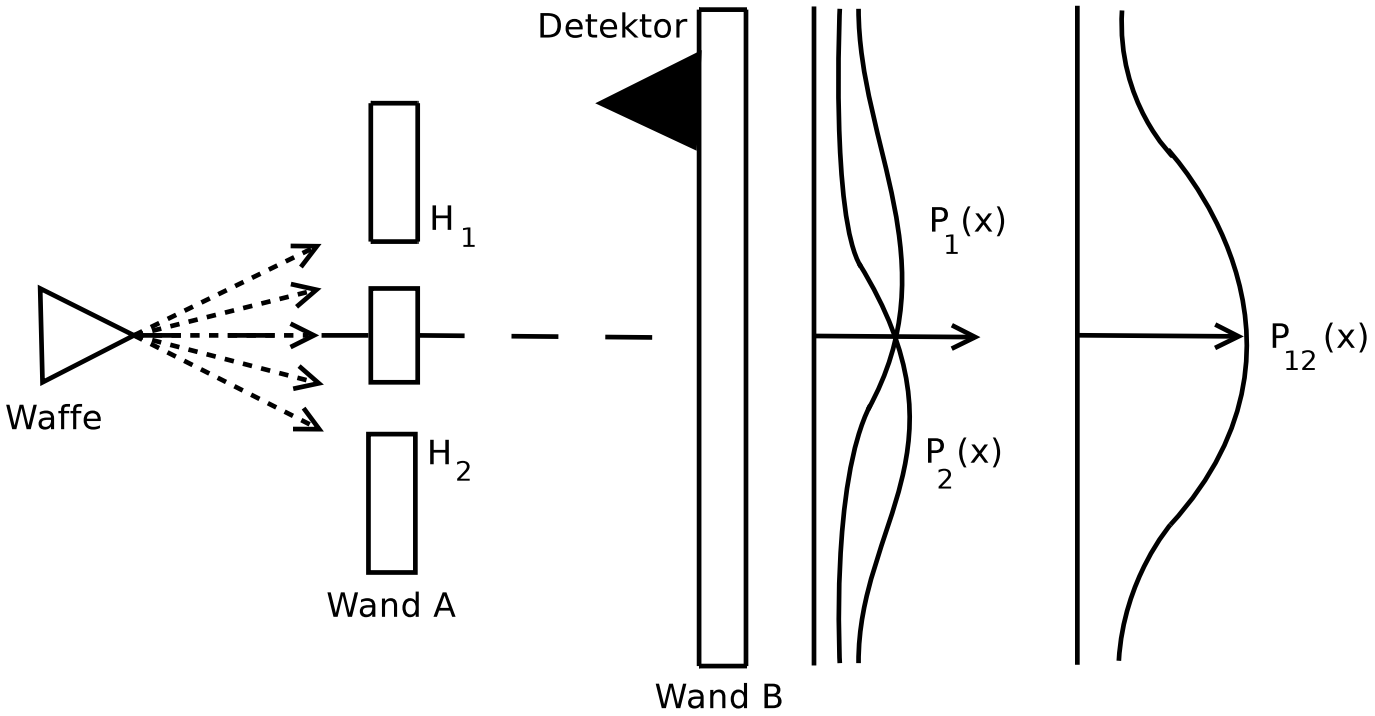
- H_1, H_2: Schlitze in Wand A

Klassisches Experiment mit Patronen



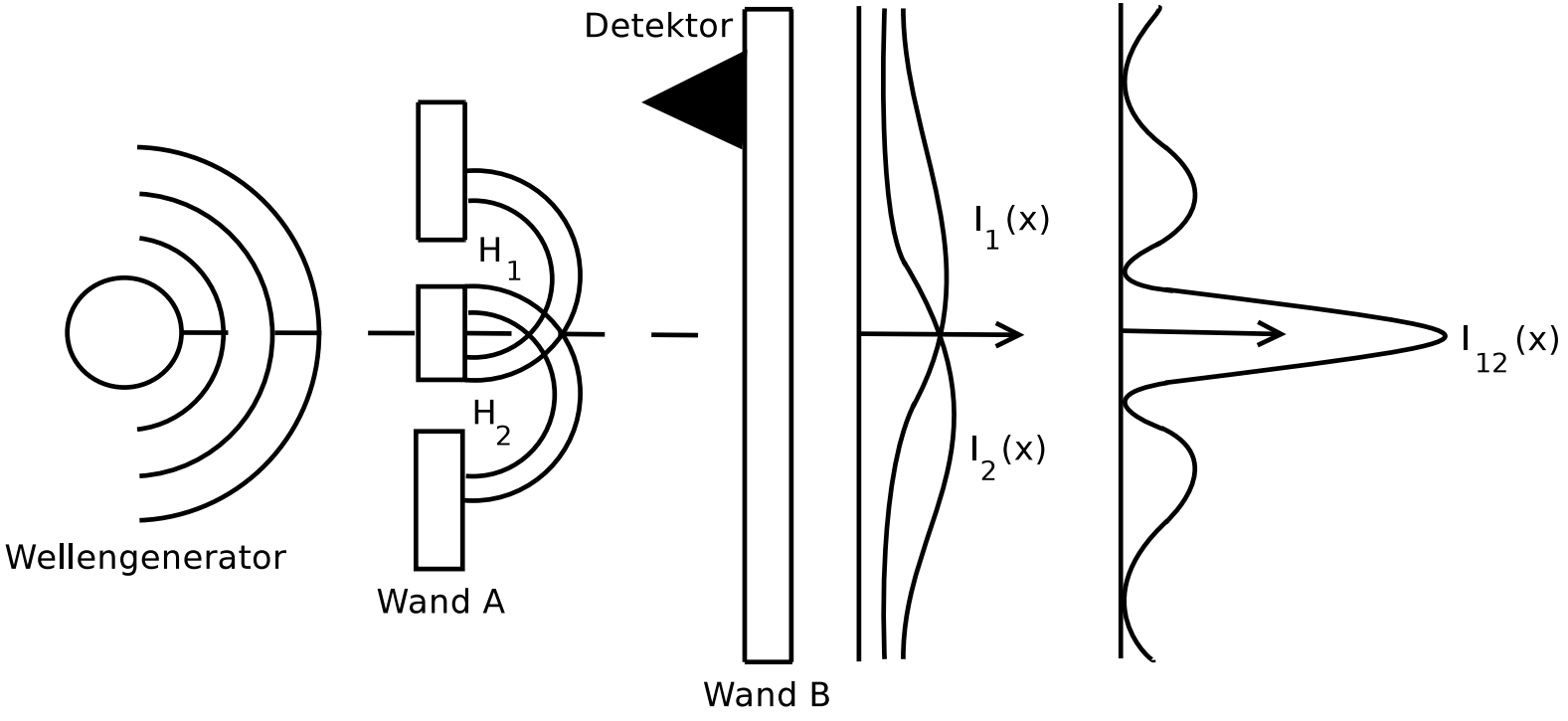
- H_1, H_2: Schlitze in Wand A
- $P_1(x)$, $P_2(x)$: Wahrscheinlichkeitsverteilung für Öffnung einer der beiden Schlitze

Klassisches Experiment mit Patronen



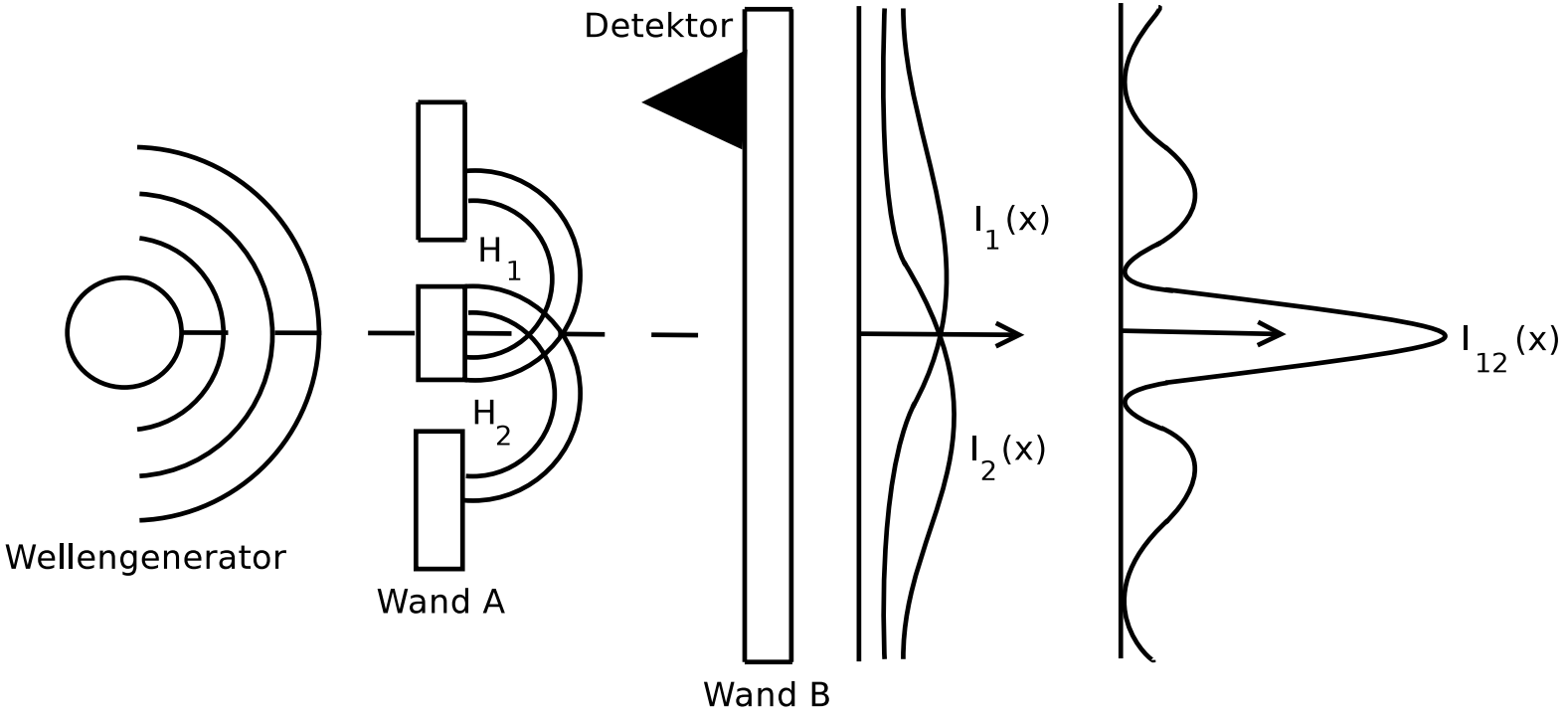
- H_1, H_2: Schlitze in Wand A
- $P_1(x)$, $P_2(x)$: Wahrscheinlichkeitsverteilung für Öffnung einer der beiden Schlitze
- $P_{12}(x)$: Verteilung für Öffnung beider Schlitze

Klassisches Experiment mit Wellen



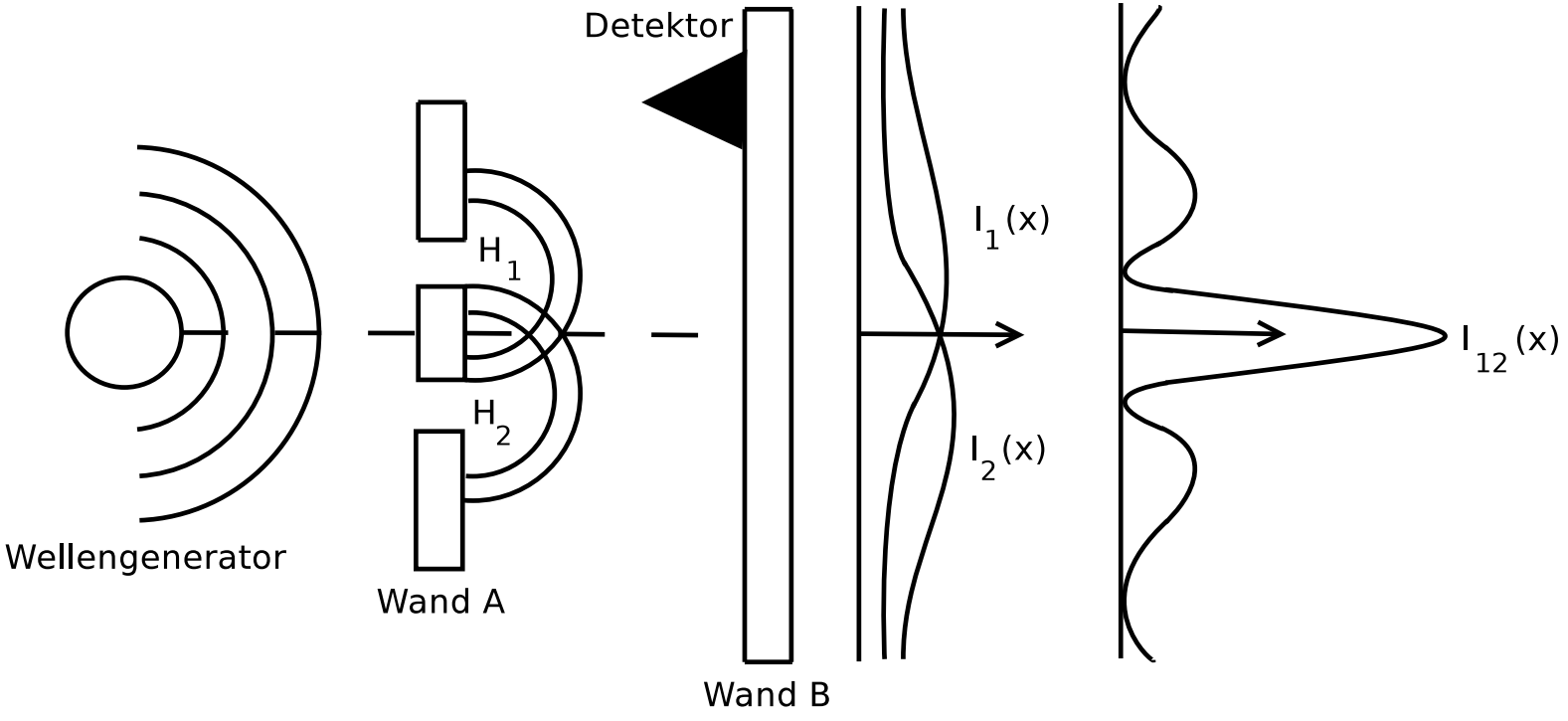
- H_1, H_2: Schlitze in Wand A

Klassisches Experiment mit Wellen



- H_1, H_2: Schlitze in Wand A
- $I_1(x)$, $I_2(x)$: Intensitätsverteilung für Öffnung einer der beiden Schlitze

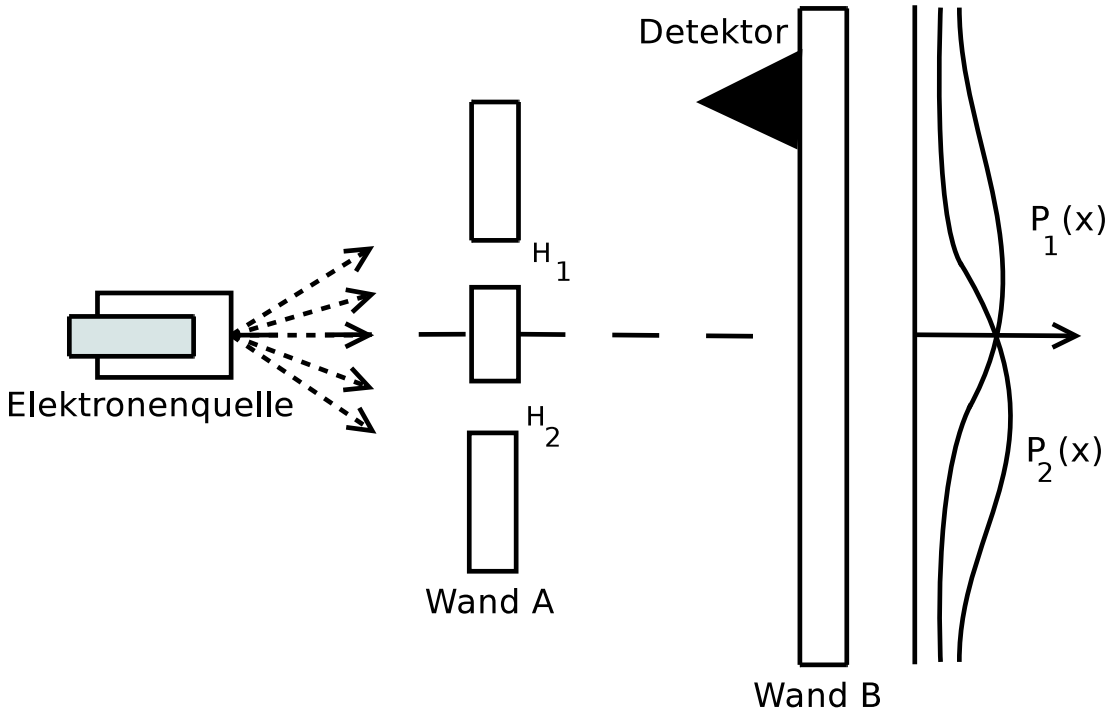
Klassisches Experiment mit Wellen



- H_1, H_2: Schlitze in Wand A
- $I_1(x)$, $I_2(x)$: Intensitätsverteilung für Öffnung einer der beiden Schlitze
- $I_{12}(x)$ Verteilung für Öffnung beider Schlitze

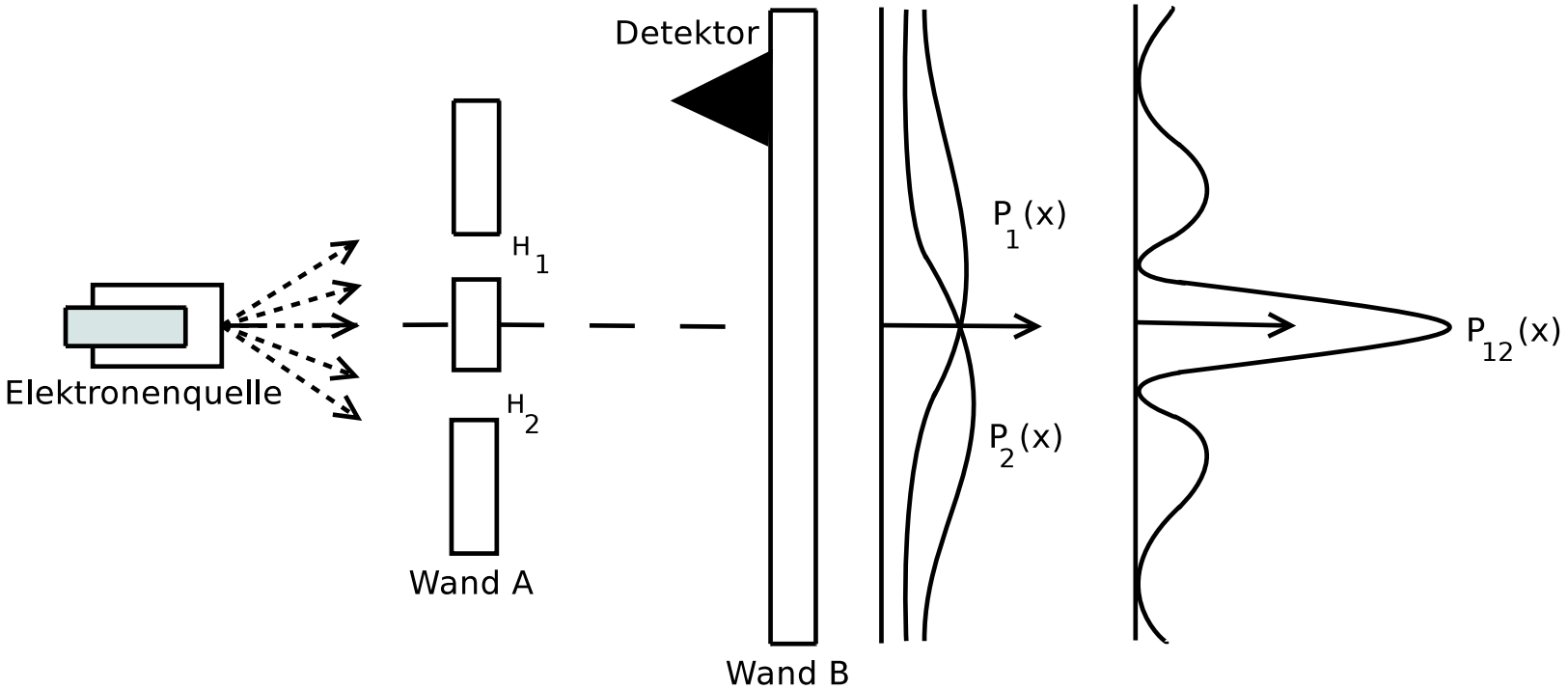
Outline

Doppelspaltexperiment mit Elektronen



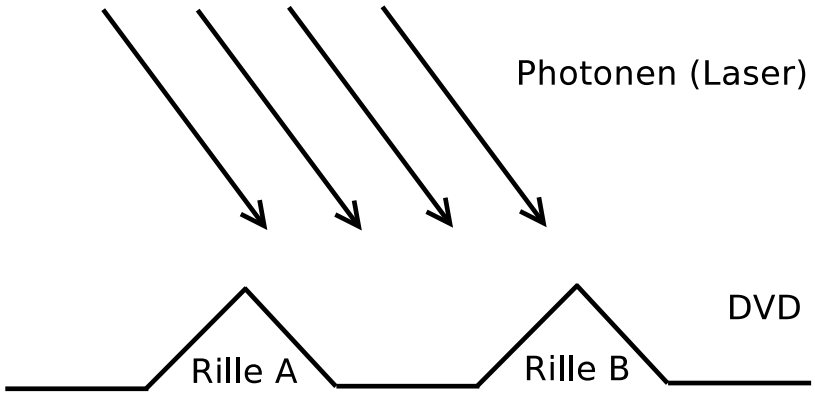
- Quantenwelt: Versuche mit Elektronen (Photonen)

Doppelspaltexperiment mit Elektronen



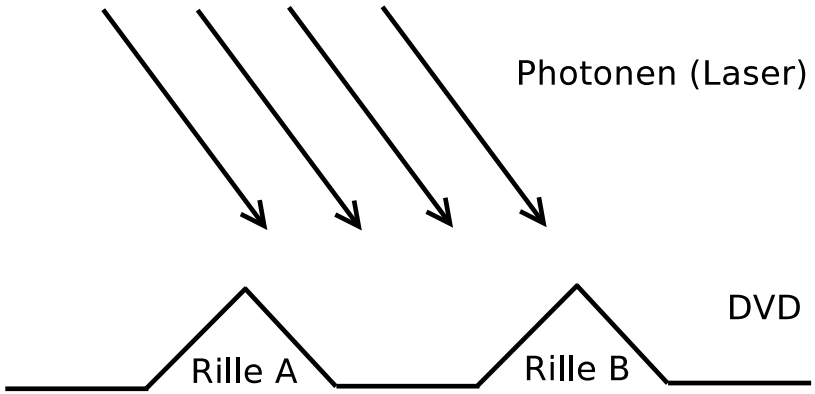
- Elektronen sind Teilchen, verhalten sich aber anscheinend manchmal wie Wellen

Mehrspaltexperiment mit Photonen



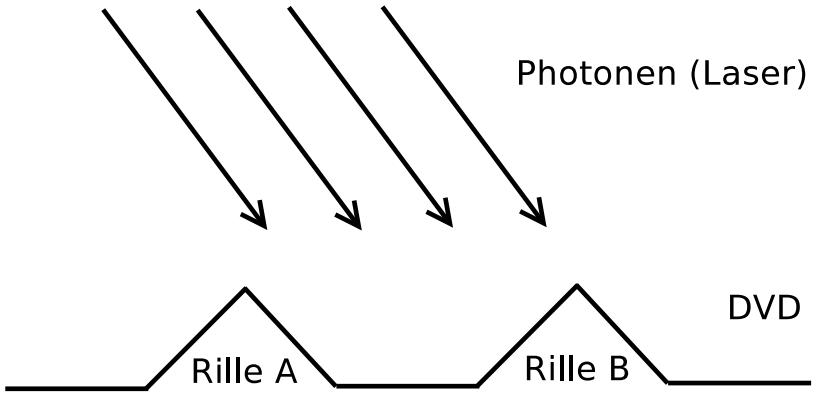
- Anstelle von Schlitzen in einer Wand haben wir Rillen in einer DVD

Mehrspaltexperiment mit Photonen



- Anstelle von Schlitzen in einer Wand haben wir Rillen in einer DVD
- Photonen werden an den Rillen reflektiert

Mehrspaltexperiment mit Photonen



- Anstelle von Schlitzen in einer Wand haben wir Rillen in einer DVD
- Photonen werden an den Rillen reflektiert
- Auch Photonen zeigen das Interferenzmuster

Beobachtungen

- Elektronen und Photonen zeigen das **Welleninterferenzmuster**

Beobachtungen

- Elektronen und Photonen zeigen das **Welleninterferenzmuster**
- Interferenzmuster entsteht auch dann, wenn ein Elektron (Photon) erst nach Erreichen der Wand des Vorherigen abgefeuert wird

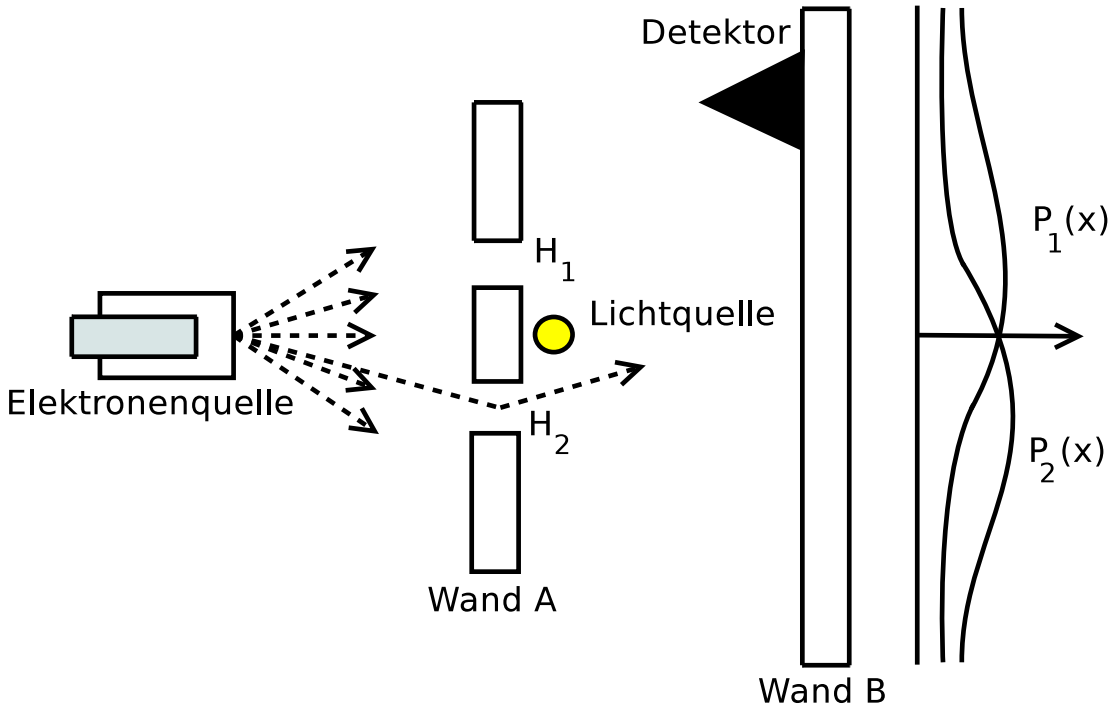
Beobachtungen

- Elektronen und Photonen zeigen das **Welleninterferenzmuster**
- Interferenzmuster entsteht auch dann, wenn ein Elektron (Photon) erst nach Erreichen der Wand des Vorherigen abgefeuert wird
- Jedes Elektron (Photon) scheint beide Schlitze gleichzeitig zu passieren (**Superpositionsprinzip**)

Beobachtungen

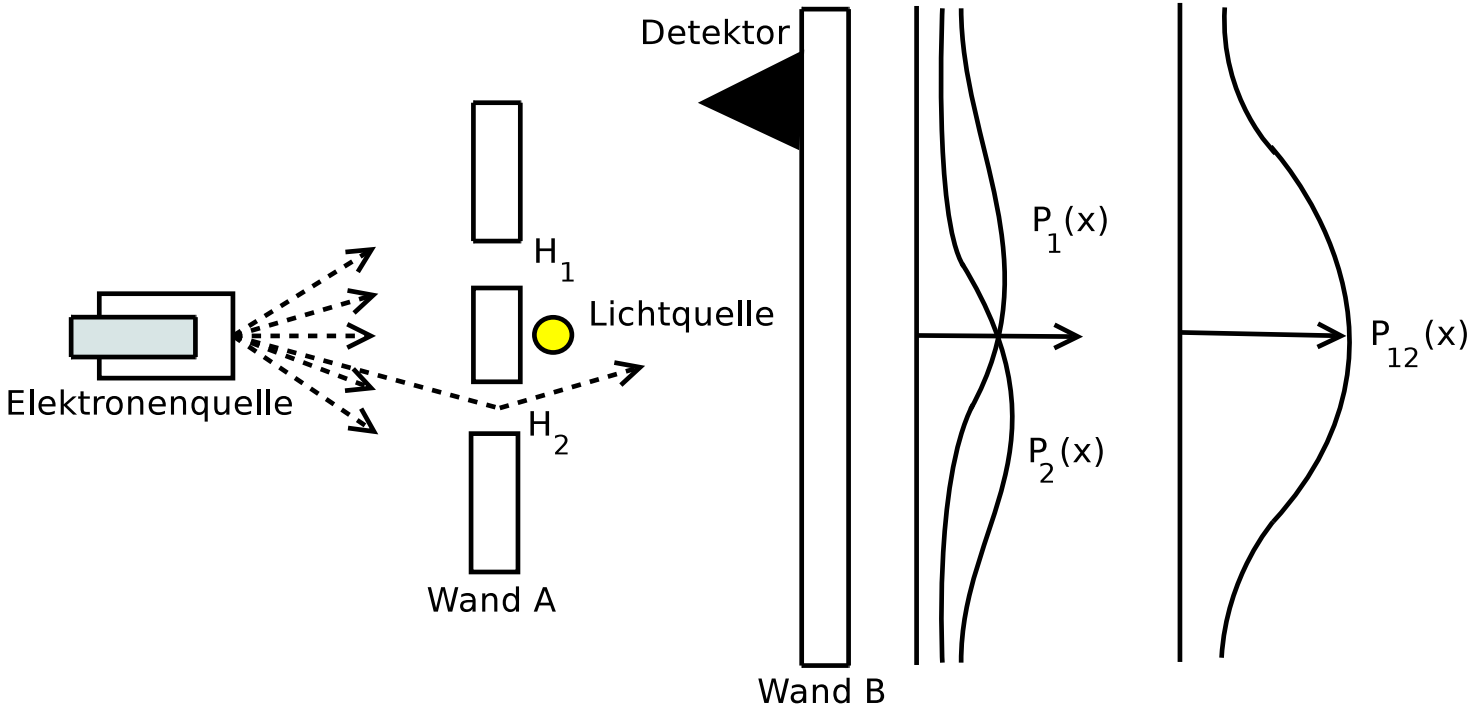
- Elektronen und Photonen zeigen das **Welleninterferenzmuster**
- Interferenzmuster entsteht auch dann, wenn ein Elektron (Photon) erst nach Erreichen der Wand des Vorherigen abgefeuert wird
- Jedes Elektron (Photon) scheint beide Schlitze gleichzeitig zu passieren (**Superpositionsprinzip**)
- **Idee:** **Messen** oder **Beobachten**, welchen Schlitz das Elektron passiert

Doppelspaltversuch mit Beobachtung



- Beobachtung durch Reflexion von Licht durch das Elektron

Doppelspaltversuch mit Beobachtung



- Es ergibt sich eine Wahrscheinlichkeitsverteilung P_{12} wie im Doppelspaltversuch mit Patronen (**Dekohärenz**)

Outline

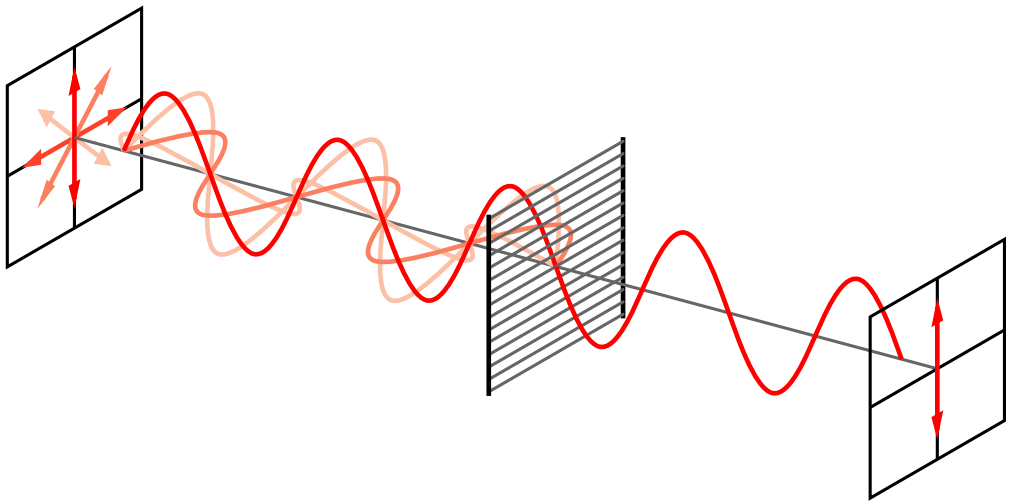
- Zustand eines Quantensystems kann als **Vektor** betrachtet werden

- Zustand eines Quantensystems kann als **Vektor** betrachtet werden
- **Messbasis** (Beobachtungssystem) kann nur **orthogonale Zustände** unterscheiden

- Zustand eines Quantensystems kann als **Vektor** betrachtet werden
- **Messbasis** (Beobachtungssystem) kann nur **orthogonale Zustände** unterscheiden
- Ein zur Messbasis nicht orthogonaler Zustand kann als **Superposition** der Messbasis betrachtet werden

- Zustand eines Quantensystems kann als **Vektor** betrachtet werden
- **Messbasis** (Beobachtungssystem) kann nur **orthogonale Zustände** unterscheiden
- Ein zur Messbasis nicht orthogonaler Zustand kann als **Superposition** der Messbasis betrachtet werden
- Messen eines zur Messbasis nicht orthogonalen Zustands kann als Projektion auf einen Zustand der Messbasis betrachtet werden (**Dekohärenz**)

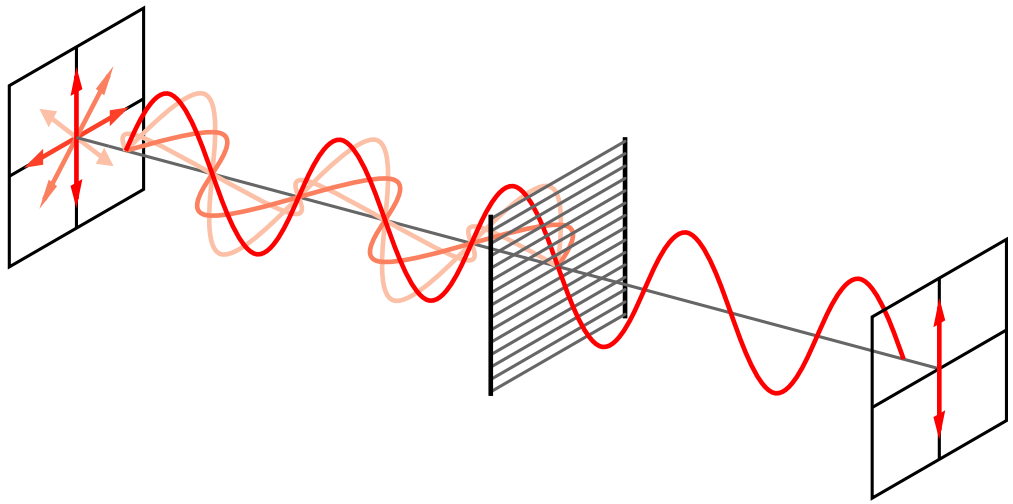
Polarisierte Photonen als Informationsträger



GNU Free Documentation License

- **Polarisierte Photonen** (Polarisationsfilter) zur Übertragung von Quantenzuständen

Polarisierte Photonen als Informationsträger



GNU Free Documentation License

- **Polarisierte Photonen** (Polarisationsfilter) zur Übertragung von Quantenzuständen
- **Qubits** (2 Zustände für 0 und 1) können durch Photonen, die in Richtung ϕ und $\phi + 90°$ polarisiert werden, übertragen werden

Zusammenfassend

- **Wichtig:** **Messen** und **Beobachten** eines Quantensystems führt zum irreversiblen Verlust seiner quantenmechanischen Eigenschaften (**Dekohärenz**)

Zusammenfassend

- **Wichtig:** **Messen** und **Beobachten** eines Quantensystems führt zum irreversiblen Verlust seiner quantenmechanischen Eigenschaften (**Dekohärenz**)
- **Konsequenz:** Mit dem Dekohärenz-Phänomen sind Angriffe und Mithören erkennbar

Zusammenfassend

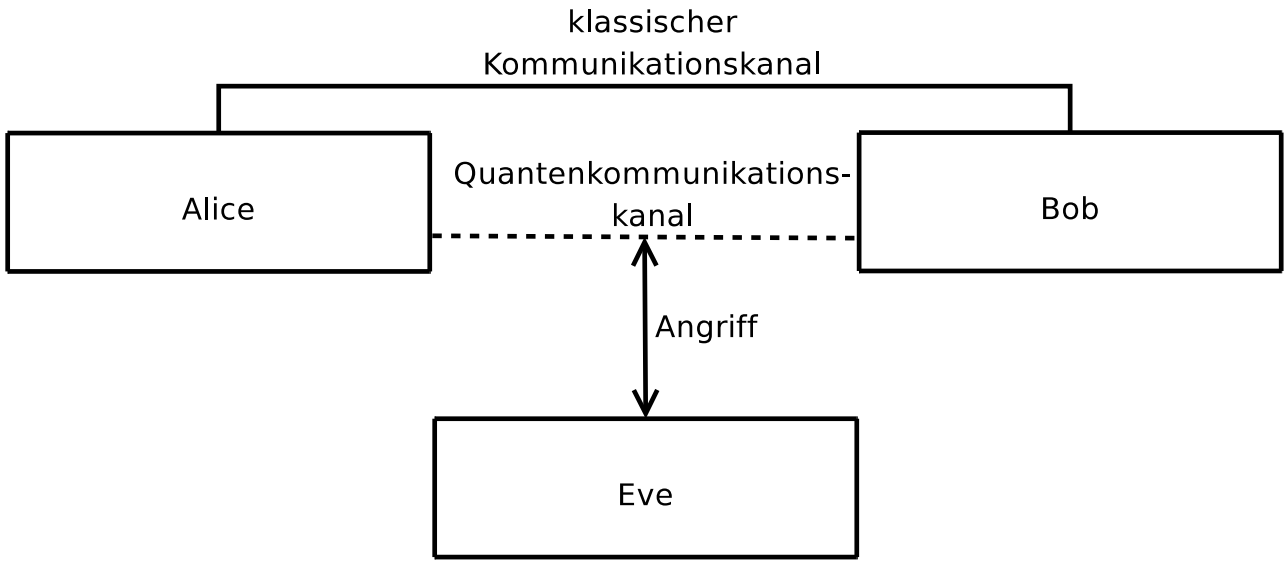
- **Wichtig:** **Messen** und **Beobachten** eines Quantensystems führt zum irreversiblen Verlust seiner quantenmechanischen Eigenschaften (**Dekohärenz**)
- **Konsequenz:** Mit dem Dekohärenz-Phänomen sind Angriffe und Mithören erkennbar
- **Polarisierte Photonen** sind die bisher einfachste Möglichkeit Quantenzustände zu übertragen

Zusammenfassend

- **Wichtig:** **Messen** und **Beobachten** eines Quantensystems führt zum irreversiblen Verlust seiner quantenmechanischen Eigenschaften (**Dekohärenz**)
- **Konsequenz:** Mit dem Dekohärenz-Phänomen sind Angriffe und Mithören erkennbar
- **Polarisierte Photonen** sind die bisher einfachste Möglichkeit Quantenzustände zu übertragen
- Schwierigkeit bereitet die über weite Strecken auftretende Dekohärenz durch Wechselwirkung mit der Umwelt

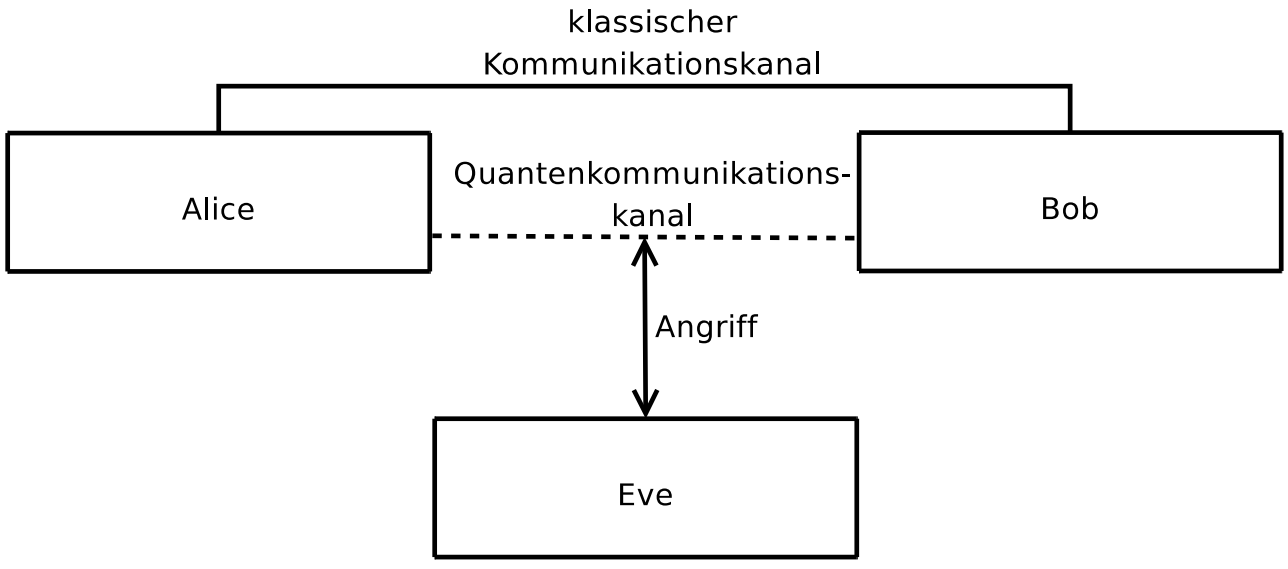
Outline

Ausgangslage



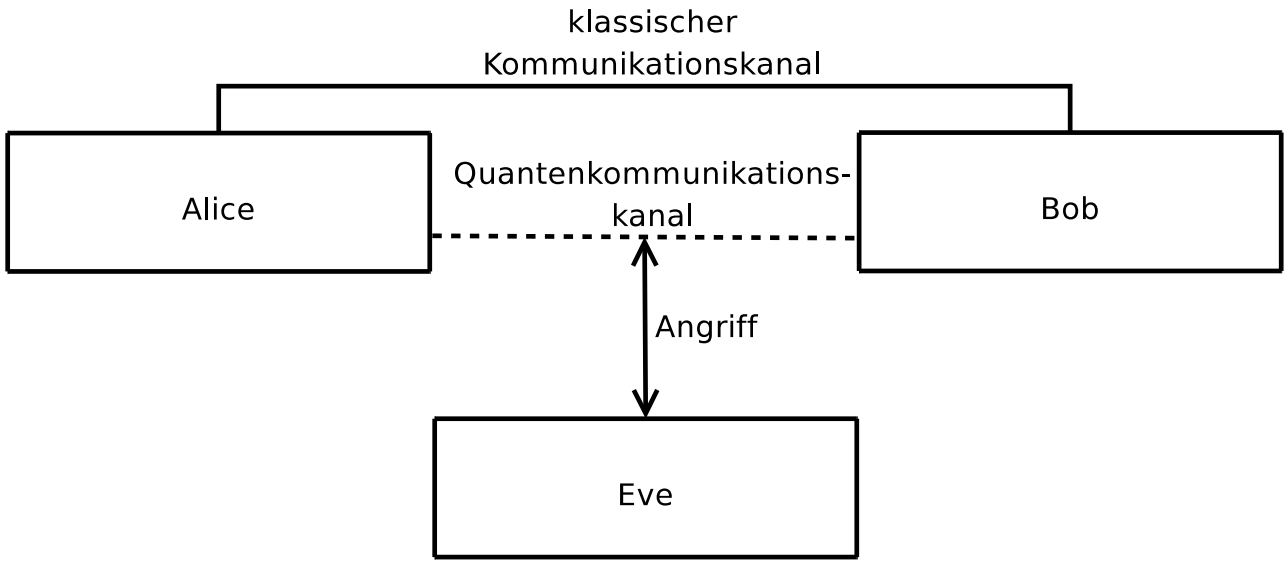
- Ausgangslage mit Alice, Bob und Angreifer Eve

Ausgangslage



- Ausgangslage mit Alice, Bob und Angreifer Eve
- **Klassischer Kommunikationskanal** zur Übertragung von Nachrichten

Ausgangslage



- Ausgangslage mit Alice, Bob und Angreifer Eve
- **Klassischer Kommunikationskanal** zur Übertragung von Nachrichten
- **Quantenkommunikationskanal** zur Übertragung von Zuständen eines Quantensystems

Warum braucht man zwei Kanäle?

- Quantenkryptographie ist kein Kryptographieverfahren im klassischen Sinne

Warum braucht man zwei Kanäle?

- Quantenkryptographie ist kein Kryptographieverfahren im klassischen Sinne
- **Ziel:** Erstellen eines geheimen, sicheren Schlüssels für ein **One-Time Pad**

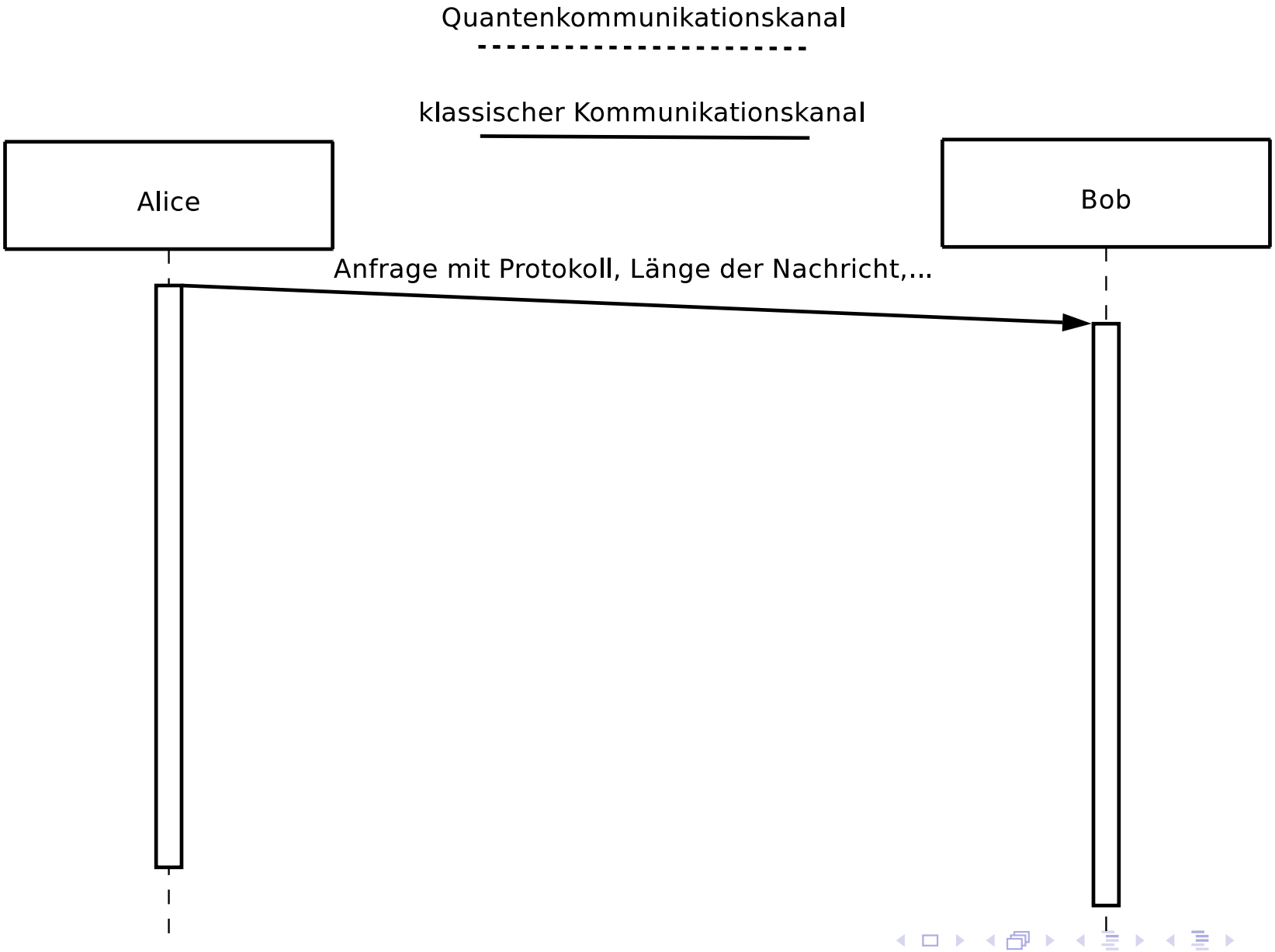
Warum braucht man zwei Kanäle?

- Quantenkryptographie ist kein Kryptographieverfahren im klassischen Sinne
- **Ziel:** Erstellen eines geheimen, sicheren Schlüssels für ein **One-Time Pad**
- Nutzen quantenphysikalischer Eigenschaften zur Schlüsselerzeugung (**Quantenkommunikationskanal**)

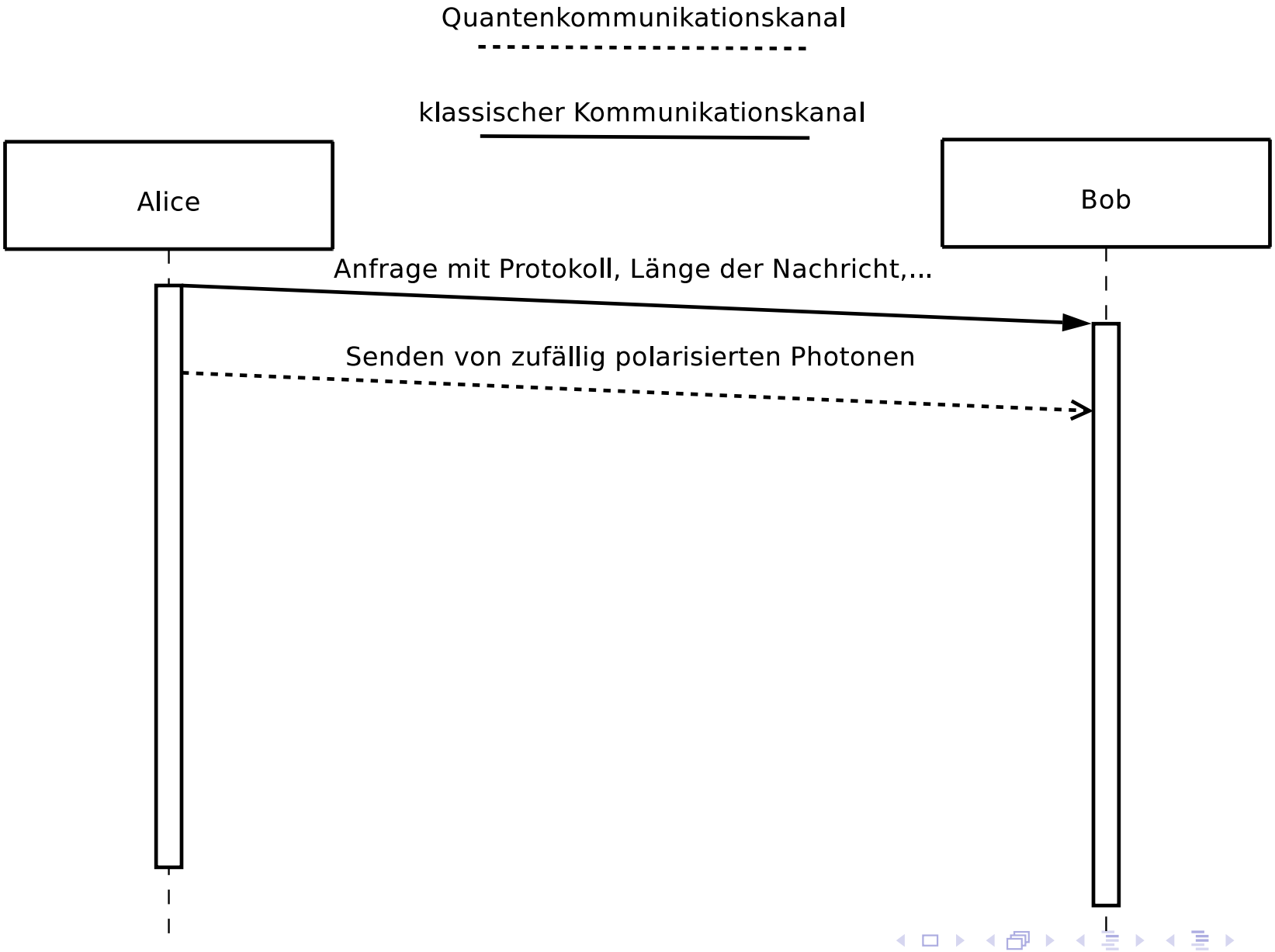
Warum braucht man zwei Kanäle?

- Quantenkryptographie ist kein Kryptographieverfahren im klassischen Sinne
- **Ziel:** Erstellen eines geheimen, sicheren Schlüssels für ein **One-Time Pad**
- Nutzen quantenphysikalischer Eigenschaften zur Schlüsselerzeugung (**Quantenkommunikationskanal**)
- Verschlüsselte Nachricht wird weiterhin über den **klassischen Kommunikationskanal** versendet

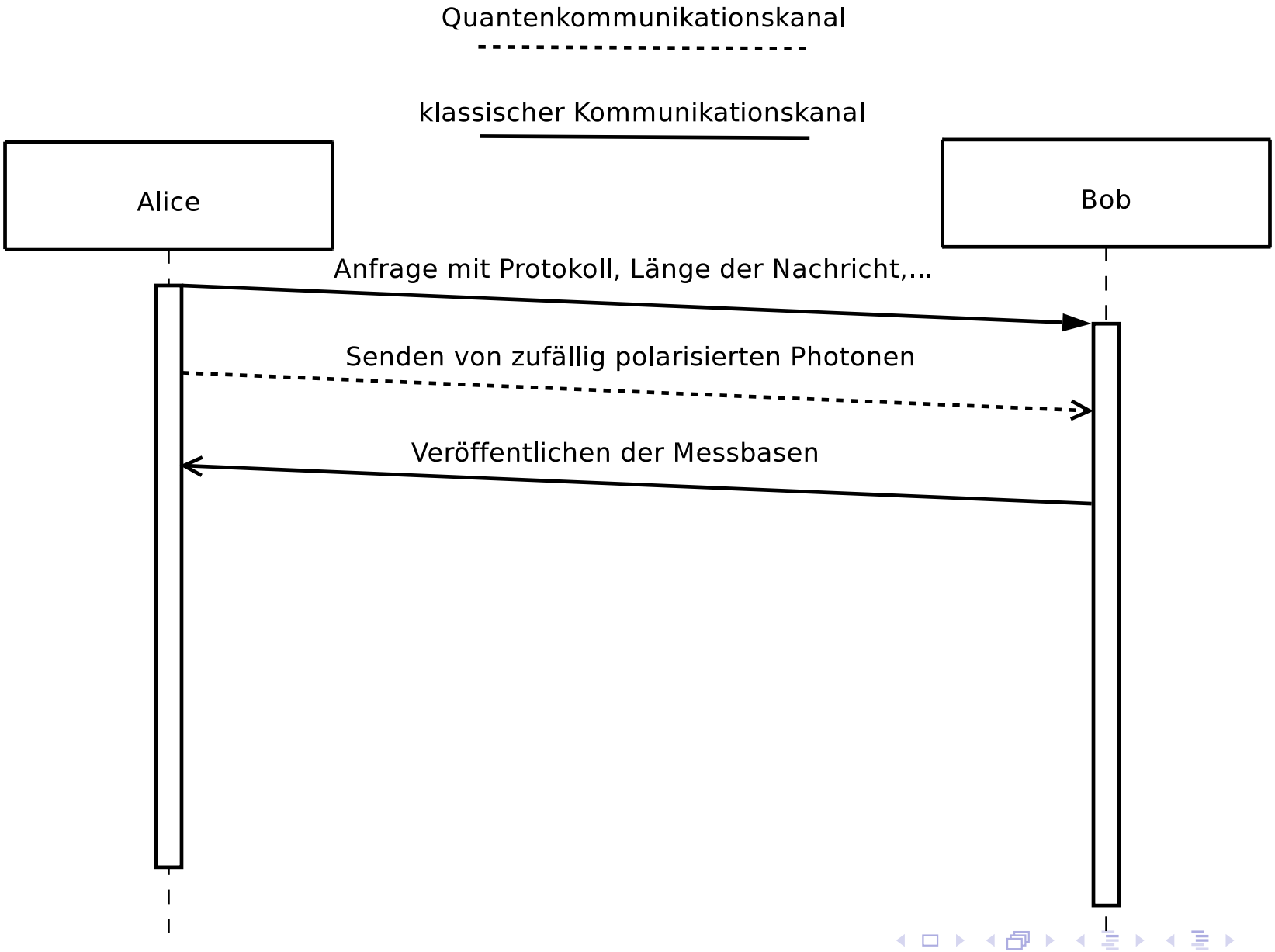
Theoretischer Ablauf



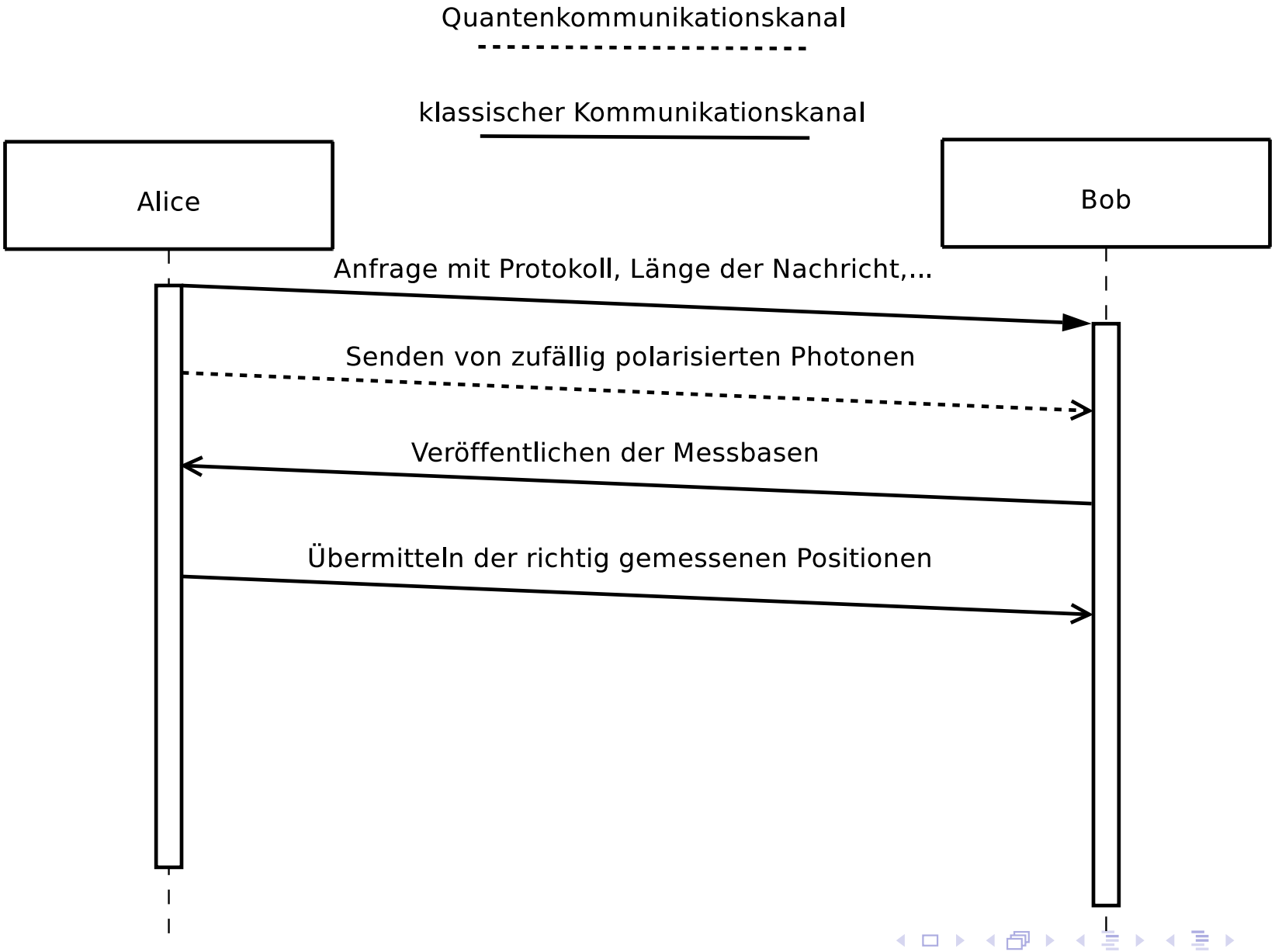
Theoretischer Ablauf



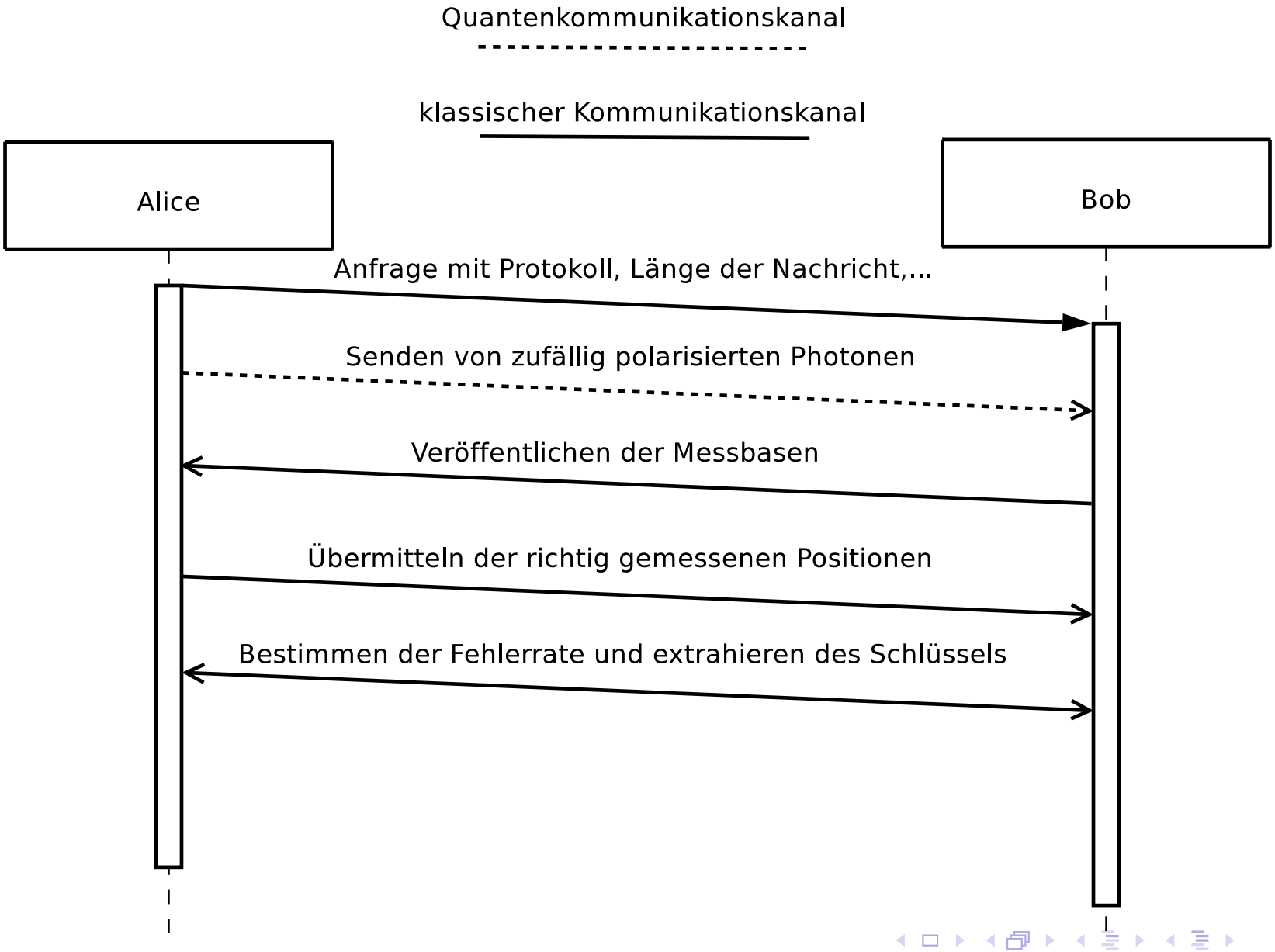
Theoretischer Ablauf



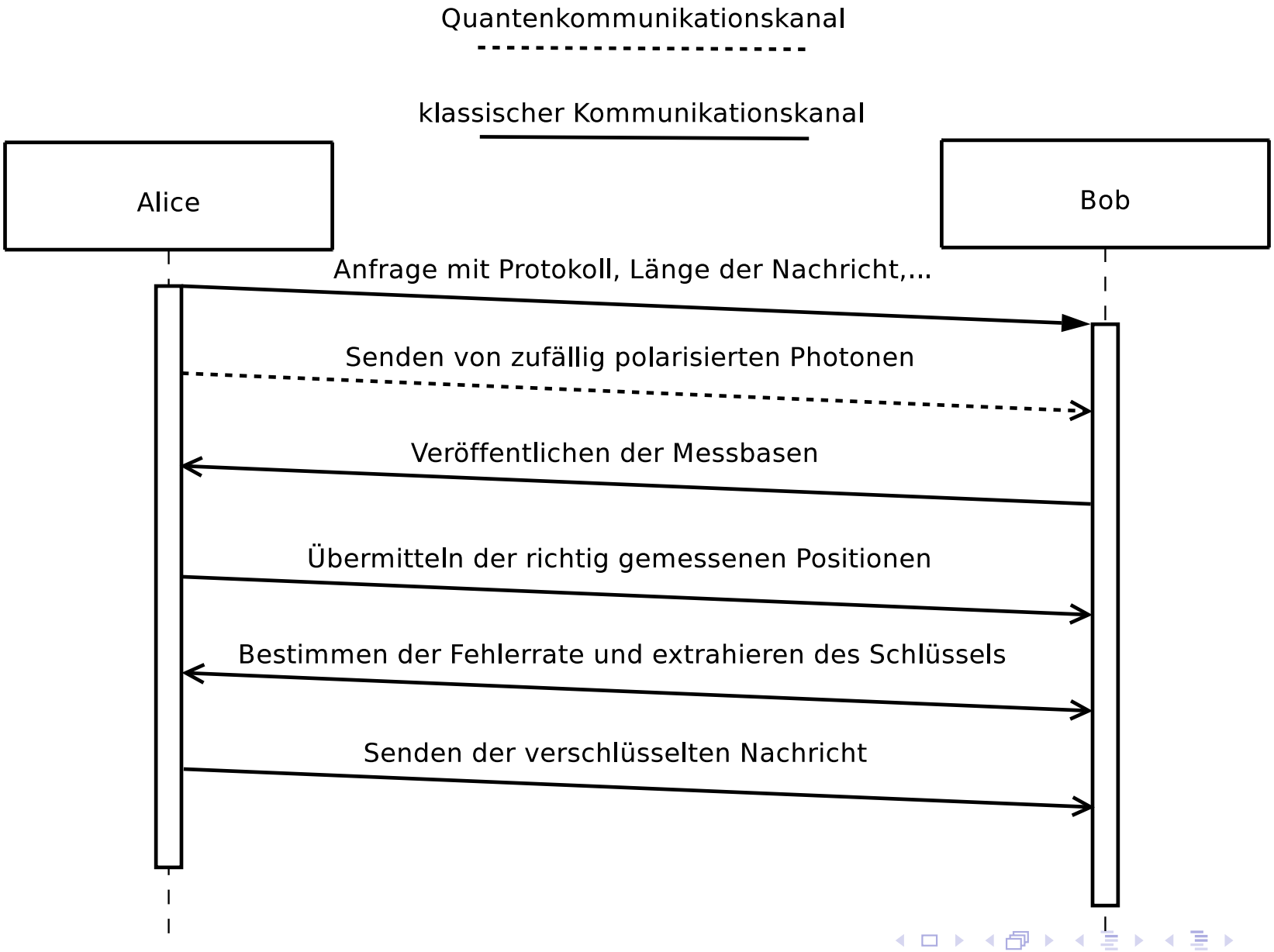
Theoretischer Ablauf



Theoretischer Ablauf



Theoretischer Ablauf



Outline

Grundlagen der Sicherheit

- Nur QKG muss betrachtet werden (später greift Sicherheit des One-Time Pad)

Grundlagen der Sicherheit

- Nur QKG muss betrachtet werden (später greift Sicherheit des One-Time Pad)
- Sicherheit der QKG basiert nicht auf Annahmen der Komplexitätstheorie, sondern auf **Annahme der Richtigkeit des quantentheoretischen Modells**

Grundlagen der Sicherheit

- Nur QKG muss betrachtet werden (später greift Sicherheit des One-Time Pad)
- Sicherheit der QKG basiert nicht auf Annahmen der Komplexitätstheorie, sondern auf **Annahme der Richtigkeit des quantentheoretischen Modells**
- **Folgen:** Durchführung der QKG derart möglich, dass:

Grundlagen der Sicherheit

- Nur QKG muss betrachtet werden (später greift Sicherheit des One-Time Pad)
- Sicherheit der QKG basiert nicht auf Annahmen der Komplexitätstheorie, sondern auf **Annahme der Richtigkeit des quantentheoretischen Modells**
- **Folgen:** Durchführung der QKG derart möglich, dass:
  - Eve nur mit vernachlässigbarer Wahrscheinlichkeit den Schlüssel erhält

Grundlagen der Sicherheit

- Nur QKG muss betrachtet werden (später greift Sicherheit des One-Time Pad)
- Sicherheit der QKG basiert nicht auf Annahmen der Komplexitätstheorie, sondern auf **Annahme der Richtigkeit des quantentheoretischen Modells**
- **Folgen:** Durchführung der QKG derart möglich, dass:
  - Eve nur mit vernachlässigbarer Wahrscheinlichkeit den Schlüssel erhält
  - Angriffe und Mithören auf dem Quantenkommunikationskanal entdeckt werden können

Grundlagen der Sicherheit

- Nur QKG muss betrachtet werden (später greift Sicherheit des One-Time Pad)
- Sicherheit der QKG basiert nicht auf Annahmen der Komplexitätstheorie, sondern auf **Annahme der Richtigkeit des quantentheoretischen Modells**
- **Folgen:** Durchführung der QKG derart möglich, dass:
  - Eve nur mit vernachlässigbarer Wahrscheinlichkeit den Schlüssel erhält
  - Angriffe und Mithören auf dem Quantenkommunikationskanal entdeckt werden können
  - Beide Parteien so sicher wie nötig sein können, dass der Schlüssel geheim ist

Fehlerrate (1)

- **Fehlerrate** bezeichnet den Anteil der übertragenen Zustände, die bei der Übertragung zerstört werden

Fehlerrate (1)

- **Fehlerrate** bezeichnet den Anteil der übertragenen Zustände, die bei der Übertragung zerstört werden
- Natürliche Ursachen für Fehler bei der Übertragung:

Fehlerrate (1)

- **Fehlerrate** bezeichnet den Anteil der übertragenen Zustände, die bei der Übertragung zerstört werden
- Natürliche Ursachen für Fehler bei der Übertragung:
  - Fehlerhafter Kanal

Fehlerrate (1)

- **Fehlerrate** bezeichnet den Anteil der übertragenen Zustände, die bei der Übertragung zerstört werden
- Natürliche Ursachen für Fehler bei der Übertragung:
  - Fehlerhafter Kanal
  - Rauschen im Kanal (**natürliche Dekohärenz**)

Fehlerrate (1)

- **Fehlerrate** bezeichnet den Anteil der übertragenen Zustände, die bei der Übertragung zerstört werden
- Natürliche Ursachen für Fehler bei der Übertragung:
  - Fehlerhafter Kanal
  - Rauschen im Kanal (**natürliche Dekohärenz**)
  - Fehler an der Quelle und im Detektor

Fehlerrate (2)

- Fehler durch einen Angreifer:

Fehlerrate (2)

- Fehler durch einen Angreifer:
  - Dekohärenz durch Messen oder eines Kopierversuchs

Fehlerrate (2)

- Fehler durch einen Angreifer:
  - Dekohärenz durch Messen oder eines Kopierversuchs
  - **Worst Case:** Eve kennt das Protokoll und somit die benutzten Messbasen

Fehlerrate (2)

- Fehler durch einen Angreifer:
  - Dekohärenz durch Messen oder eines Kopierversuchs
  - **Worst Case:** Eve kennt das Protokoll und somit die benutzten Messbasen
  - $\Rightarrow$ Pr[Eve macht Fehler] = $\frac{1}{4}$

Fehlerrate (2)

- Fehler durch einen Angreifer:
  - Dekohärenz durch Messen oder eines Kopierversuchs
  - **Worst Case:** Eve kennt das Protokoll und somit die benutzten Messbasen
  - $\Rightarrow$ Pr[Eve macht Fehler] = $\frac{1}{4}$
  - $\Rightarrow$ Pr[Eve macht keinen Fehler] = $1 - \frac{1}{4} = \frac{3}{4}$

Fehlerrate (2)

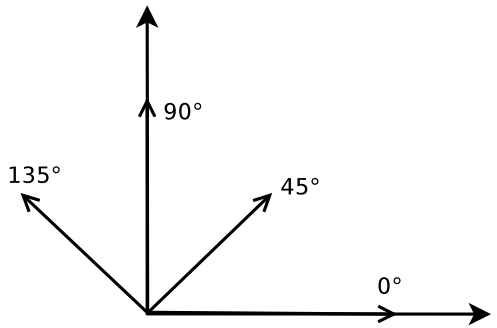
- Fehler durch einen Angreifer:
  - Dekohärenz durch Messen oder eines Kopierversuchs
  - **Worst Case:** Eve kennt das Protokoll und somit die benutzten Messbasen
  - $\Rightarrow$ Pr[Eve macht Fehler] = $\frac{1}{4}$
  - $\Rightarrow$ Pr[Eve macht keinen Fehler] = $1 - \frac{1}{4} = \frac{3}{4}$
  - $\Rightarrow$ Pr[Eve macht bei n Messungen keinen Fehler] = $(\frac{3}{4})^n$

Fehlerrate (2)

- Fehler durch einen Angreifer:
  - Dekohärenz durch Messen oder eines Kopierversuchs
  - **Worst Case:** Eve kennt das Protokoll und somit die benutzten Messbasen
  - $\Rightarrow$ Pr[Eve macht Fehler] = $\frac{1}{4}$
  - $\Rightarrow$ Pr[Eve macht keinen Fehler] = $1 - \frac{1}{4} = \frac{3}{4}$
  - $\Rightarrow$ Pr[Eve macht bei n Messungen keinen Fehler] = $(\frac{3}{4})^n$
- Fehlern im Kanal kann mit Error Correction Codes begegnet werden

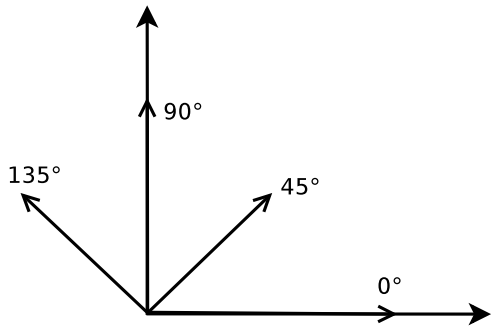
Outline

Grundlagen des BB84 Protokolls



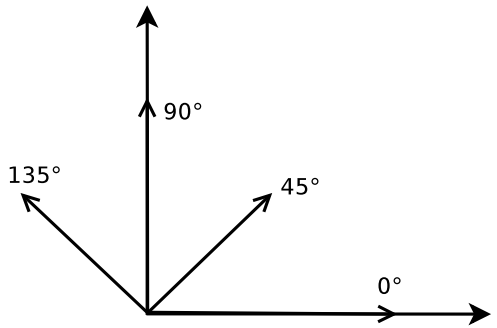
- Erstes Protokoll der Quantenkryptographie nach Bennett und Brassard, 1984

Grundlagen des BB84 Protokolls



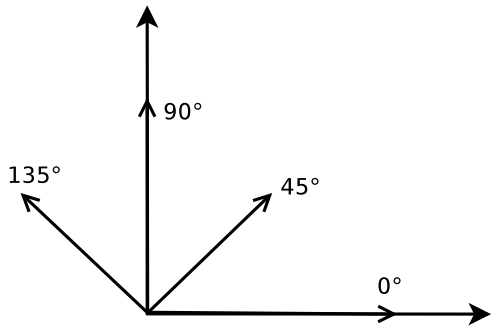
- Erstes Protokoll der Quantenkryptographie nach Bennett und Brassard, 1984
- Alice benutzt vier Polarisationen: 0°: $\rightarrow$, 90°: $\uparrow$, 45°: $\nearrow$, 135°: $\nwarrow$

Grundlagen des BB84 Protokolls



- Erstes Protokoll der Quantenkryptographie nach Bennett und Brassard, 1984
- Alice benutzt vier Polarisationen: 0°: $\rightarrow$, 90°: $\uparrow$, 45°: $\nearrow$, 135°: $\nwarrow$
- Bob misst entweder mit der Standardbasis $\mathcal{B} = \{\uparrow, \rightarrow\} = +$ oder der dualen Basis $\mathcal{D} = \{\nwarrow, \nearrow\} = \times$

Grundlagen des BB84 Protokolls



- Erstes Protokoll der Quantenkryptographie nach Bennett und Brassard, 1984
- Alice benutzt vier Polarisationen: 0°: $\rightarrow$, 90°: $\uparrow$, 45°: $\nearrow$, 135°: $\nwarrow$
- Bob misst entweder mit der Standardbasis $\mathcal{B} = \{\uparrow, \rightarrow\} = +$ oder der dualen Basis $\mathcal{D} = \{\nwarrow, \nearrow\} = \times$
- Alice sendet Photonen in regelmäßigen Abständen, Bob erkennt somit verlorene Photonen

Beschreibung des BB84 Protokoll

Alices Polarisation	Bobs Messbasis	Resultat	Wahrscheinlichkeit
$0 \mapsto \quad \uparrow$	$0 \rightarrow \mathcal{B} = +$	0	1
	$1 \rightarrow \mathcal{D} = \times$	$0/1$	$0,5$

Beschreibung des BB84 Protokoll

Alices Polarisation	Bobs Messbasis	Resultat	Wahrscheinlichkeit
$0 \mapsto \quad \uparrow$	$0 \rightarrow \mathcal{B} = +$	0	1
	$1 \rightarrow \mathcal{D} = \times$	$0/1$	$0,5$
$0 \mapsto \quad \nearrow$	$0 \rightarrow \mathcal{B} = +$	$0/1$	$0,5$
	$1 \rightarrow \mathcal{D} = \times$	1	1

Beschreibung des BB84 Protokoll

Alices Polarisation	Bobs Messbasis	Resultat	Wahrscheinlichkeit
$0 \mapsto \quad \uparrow$	$0 \rightarrow \mathcal{B} = +$	0	1
	$1 \rightarrow \mathcal{D} = \times$	$0/1$	$0,5$
$0 \mapsto \quad \nearrow$	$0 \rightarrow \mathcal{B} = +$	$0/1$	$0,5$
	$1 \rightarrow \mathcal{D} = \times$	1	1
$1 \mapsto \quad \rightarrow$	$0 \rightarrow \mathcal{B} = +$	0	1
	$1 \rightarrow \mathcal{D} = \times$	$0/1$	$0,5$

Beschreibung des BB84 Protokoll

Alices Polarisation	Bobs Messbasis	Resultat	Wahrscheinlichkeit
$0 \mapsto \uparrow$	$0 \rightarrow \mathcal{B} = +$	0	1
	$1 \rightarrow \mathcal{D} = \times$	$0/1$	$0,5$
$0 \mapsto \nearrow$	$0 \rightarrow \mathcal{B} = +$	$0/1$	$0,5$
	$1 \rightarrow \mathcal{D} = \times$	1	1
$1 \mapsto \rightarrow$	$0 \rightarrow \mathcal{B} = +$	0	1
	$1 \rightarrow \mathcal{D} = \times$	$0/1$	$0,5$
$1 \mapsto \nwarrow$	$0 \rightarrow \mathcal{B} = +$	$0/1$	$0,5$
	$1 \rightarrow \mathcal{D} = \times$	1	1

Beschreibung des BB84 Protokoll

Alices Polarisation	Bobs Messbasis	Resultat	Wahrscheinlichkeit
$0 \mapsto \uparrow$	$0 \rightarrow \mathcal{B} = +$	0	1
	$1 \rightarrow \mathcal{D} = \times$	$0/1$	$0,5$
$0 \mapsto \nearrow$	$0 \rightarrow \mathcal{B} = +$	$0/1$	$0,5$
	$1 \rightarrow \mathcal{D} = \times$	1	1
$1 \mapsto \rightarrow$	$0 \rightarrow \mathcal{B} = +$	0	1
	$1 \rightarrow \mathcal{D} = \times$	$0/1$	$0,5$
$1 \mapsto \nwarrow$	$0 \rightarrow \mathcal{B} = +$	$0/1$	$0,5$
	$1 \rightarrow \mathcal{D} = \times$	1	1

- Nach den Messungen veröffentlicht Bob seine Messbasen für die einzelnen Photonen

Beschreibung des BB84 Protokoll

Alices Polarisation	Bobs Messbasis	Resultat	Wahrscheinlichkeit
$0 \mapsto \uparrow$	$0 \rightarrow \mathcal{B} = +$	0	1
	$1 \rightarrow \mathcal{D} = \times$	$0/1$	$0,5$
$0 \mapsto \nearrow$	$0 \rightarrow \mathcal{B} = +$	$0/1$	$0,5$
	$1 \rightarrow \mathcal{D} = \times$	1	1
$1 \mapsto \rightarrow$	$0 \rightarrow \mathcal{B} = +$	0	1
	$1 \rightarrow \mathcal{D} = \times$	$0/1$	$0,5$
$1 \mapsto \nwarrow$	$0 \rightarrow \mathcal{B} = +$	$0/1$	$0,5$
	$1 \rightarrow \mathcal{D} = \times$	1	1

- Nach den Messungen veröffentlicht Bob seine Messbasen für die einzelnen Photonen
- Alice schickt Bob über den klassischen Kommunikationskanal die Stellen, an denen richtig gemessen wurde

Beispielübertragung im BB84 Protokoll

1	0	0	1	0	Alices Zufallsstring

Beispielübertragung im BB84 Protokoll

1	0	0	1	0	Alices Zufallsstring
→	↗	↑	↖	↗	Alices Polarisation

Beispielübertragung im BB84 Protokoll

1	0	0	1	0	Alices Zufallsstring
$\rightarrow$	$\nearrow$	$\uparrow$	$\nwarrow$	$\nearrow$	Alices Polarisation
0	1	1	0	1	Bobs Zufallsstring

Beispielübertragung im BB84 Protokoll

1	0	0	1	0	Alices Zufallsstring
$\rightarrow$	$\nearrow$	$\uparrow$	$\nwarrow$	$\nearrow$	Alices Polarisation
0	1	1	0	1	Bobs Zufallsstring
$\mathcal{B} = +$	$\mathcal{D} = \times$	$\mathcal{D} = \times$	$\mathcal{B} = +$	$\mathcal{D} = \times$	Bobs Messbasis

Beispielübertragung im BB84 Protokoll

1	0	0	1	0	Alices Zufallsstring
$\rightarrow$	$\nearrow$	$\uparrow$	$\nwarrow$	$\nearrow$	Alices Polarisation
0	1	1	0	1	Bobs Zufallsstring
$\mathcal{B} = +$	$\mathcal{D} = \times$	$\mathcal{D} = \times$	$\mathcal{B} = +$	$\mathcal{D} = \times$	Bobs Messbasis
1	0	Z	Z	0	Resultat

Beispielübertragung im BB84 Protokoll

1	0	0	1	0	Alices Zufallsstring
$\rightarrow$	$\nearrow$	$\uparrow$	$\nwarrow$	$\nearrow$	Alices Polarisation
0	1	1	0	1	Bobs Zufallsstring
$\mathcal{B} = +$	$\mathcal{D} = \times$	$\mathcal{D} = \times$	$\mathcal{B} = +$	$\mathcal{D} = \times$	Bobs Messbasis
1	0	Z	Z	0	Resultat

- Z heißt, dass das Resultat zufällig 1 oder 0 ist

Vergleich zu weiteren Protokollen

- B92 nach Bennett, 1992

Vergleich zu weiteren Protokollen

- B92 nach Bennett, 1992
  - Alice verwendet nur die Polarisationen 90°: ↑ und 135°: ↖

Vergleich zu weiteren Protokollen

- B92 nach Bennett, 1992
  - Alice verwendet nur die Polarisationen 90°: ↑ und 135°: ↖
  - B92 ist das minimale Protokoll der QKG, weil im Gegensatz zum BB84 Protokoll nur 2 Polarisationen verwendet werden

Vergleich zu weiteren Protokollen

- B92 nach Bennett, 1992
  - Alice verwendet nur die Polarisationen 90°: ↑ und 135°: ↖
  - B92 ist das minimale Protokoll der QKG, weil im Gegensatz zum BB84 Protokoll nur 2 Polarisationen verwendet werden
- Protokoll nach Eckert, 1991

Vergleich zu weiteren Protokollen

- B92 nach Bennett, 1992
  - Alice verwendet nur die Polarisationen 90°: ↑ und 135°: ↖
  - B92 ist das minimale Protokoll der QKG, weil im Gegensatz zum BB84 Protokoll nur 2 Polarisationen verwendet werden
- Protokoll nach Eckert, 1991
  - Nutzt das Phänomen der verschränkten Zustände

Vergleich zu weiteren Protokollen

- B92 nach Bennett, 1992
  - Alice verwendet nur die Polarisationen 90°: ↑ und 135°: ↖
  - B92 ist das minimale Protokoll der QKG, weil im Gegensatz zum BB84 Protokoll nur 2 Polarisationen verwendet werden
- Protokoll nach Eckert, 1991
  - Nutzt das Phänomen der verschränkten Zustände
  - Funktionsweise ähnelt sonst der des BB84 Protkolls

Kürzliche Errungenschaften der Forschung

- **2004:** Erster durch Quantenkryptographie verschlüsselter Banktransfer in Wien

Kürzliche Errungenschaften der Forschung

- **2004:** Erster durch Quantenkryptographie verschlüsselter Banktransfer in Wien
- **2006:** Erfolgreiches Abhören eines Teils der Schlüsselerzeugung nach dem BB84-Protokoll im Labor (MIT)

Kürzliche Errungenschaften der Forschung

- **2004:** Erster durch Quantenkryptographie verschlüsselter Banktransfer in Wien
- **2006:** Erfolgreiches Abhören eines Teils der Schlüsselerzeugung nach dem BB84-Protokoll im Labor (MIT)
- **2006:** Erfolgreiches Erstellen eines Schlüssels über eine Strecke von 184,6 km mit einem Glasfaserkabel

Kürzliche Errungenschaften der Forschung

- **2004:** Erster durch Quantenkryptographie verschlüsselter Banktransfer in Wien
- **2006:** Erfolgreiches Abhören eines Teils der Schlüsselerzeugung nach dem BB84-Protokoll im Labor (MIT)
- **2006:** Erfolgreiches Erstellen eines Schlüssels über eine Strecke von 184,6 km mit einem Glasfaserkabel
- **2007:** Einsatz der Quantenkryptographie bei der Schweizer Parlamentswahl