QUANTENKRYPTOGRAPHIE

FELIX SCHMIDT, ANDREAS SCHRANZHOFER, EMANUEL PETTER, ALEXANDER LOITZL

ÜBERSICHT

- Kryptographie
  - Verfahren
  - Sicherheit
  - Shor‘s Algorithmus
- Quantenkryptographie
  - Superposition
  - Verschränkung
  - Quantenschlüsselaustausch
  - Eavesdropper
  - Sicherheit
- Fazit

KRYPTOGRAPHIE GESCHICHTE

- Hieroglyphenaustausch 17. Jahrhundert v. Chr.
- Cäsar-Chiffre 100 v. Chr. bis 44 v. Chr.
- Vigenére-Chiffre 15. Jahrhundert
- Diffie-Hellman-Schlüsselaustausch 1976

SYMMETRISCHE VERSCHLÜSSELUNG

- Schlüssel zur Ver- und Entschlüsselung sind gleich
- Benötigt sicheren Kanal zur Übertragung des Schlüssels
- Basiert meist auf Operationen wie Bit-Shifts und XORs

CÄSAR-CHIFFRE
MONOALPHABETISCHE SUBSTITUTION

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W

key = 3

Nachricht: Nicht Sicher → KFZEQPFZEO

VIGENÉRE-CHIFFRE
POLYALPHABETISCHE SUBSTITUTION

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	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

key = zebra → 25 4 1 17 0

Nachricht = Etwas sicherer.

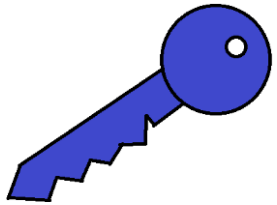
E	t	w	a	s	s	i	c	h	e	r	e	r
25	4	1	17	0	25	4	1	17	0	25	4	1
D	X	X	R	S	R	M	D	Y	E	Q	I	S

ASYMMETRISCHE VERSCHLÜSSELUNG

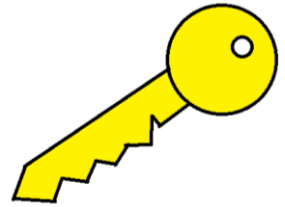
- Schlüssel zur Ver- und Entschlüsselung sind unterschiedlich
- Kann über einen unsicheren Kanal übertragen werden
- Basiert auf Einwegfunktionen (Modulo-Rechenarten, Primzahlen)

DIFFIE-HELLMAN KEY EXCHANGE

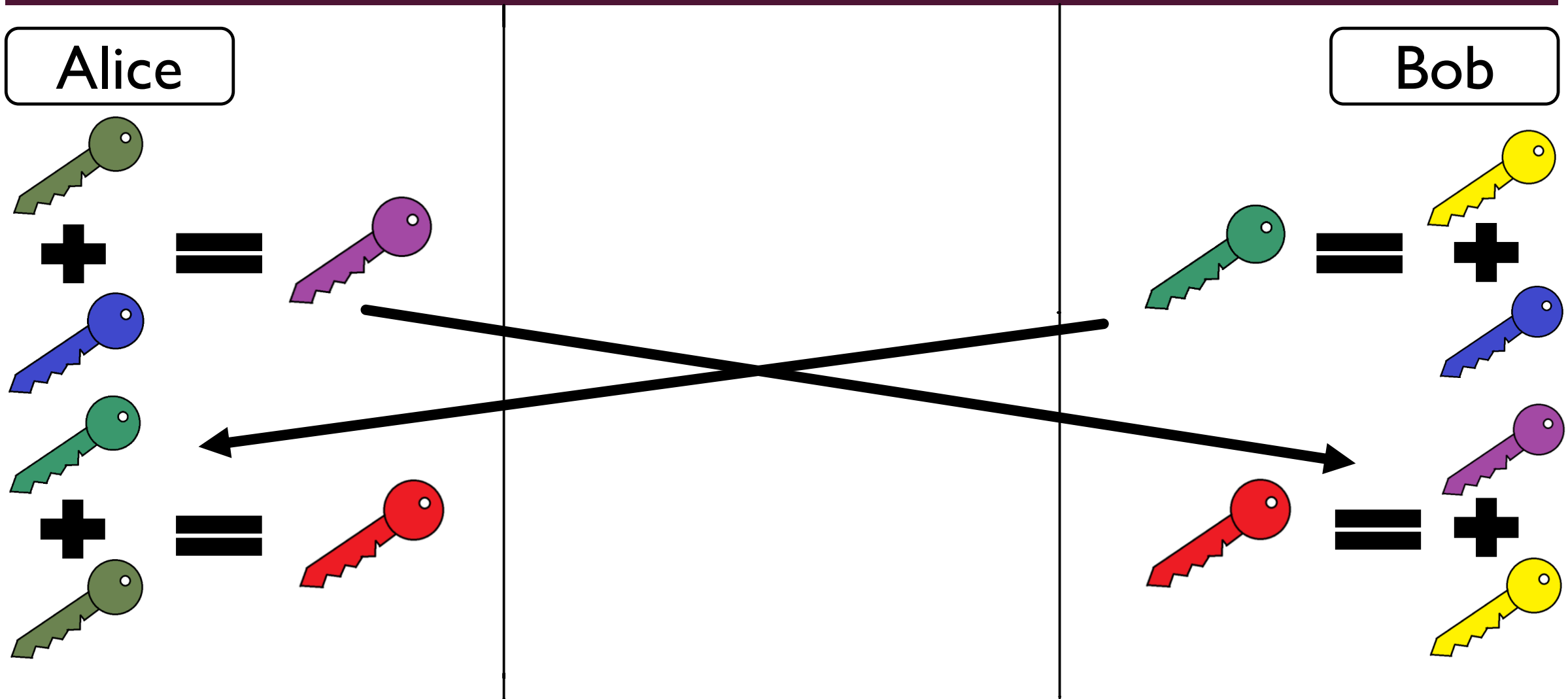
Alice



Bob



DIFFIE-HELLMAN KEY EXCHANGE



SICHERHEIT VON REGULÄRER KRYPTOGRAPHIE

One-Time Pad

1. Zufälliger Schlüssel
2. Schlüssellänge mindestens Länge der Nachricht
3. Schlüssel werden nicht wiederverwendet
4. Schlüssel werden nie öffentlich kommuniziert

Verfahren mit perfekter Sicherheit braucht diese Eigenschaften

Nachteil: Sehr aufwändig und kaum realisierbar

Allerdings: Unbrechbar

SICHERHEIT VON REGULÄRER KRYPTOGRAPHIE

- Verschlüsselung zu brechen braucht Zeit
  - → Sicherheit durch Aufwand
- Einwegfunktionen
  - Faktorisierung
  - Diskrete Logarithmen

$x * y = 10\,057$

$x = 89$

$y = 113$

$2^x \equiv_{11} 5$

$x = 4$

SICHERHEIT VON REGULÄRER KRYPTOGRAPHIE

Faktorisierung durch Quantencomputer

- Primfaktoren großer Zahlen traditionell schwer zu finden
- Primfaktorzerlegung in Zukunft sehr schnell durch Quantencomputer
- Zurzeit durch begrenzten Speicher noch keine Gefahr

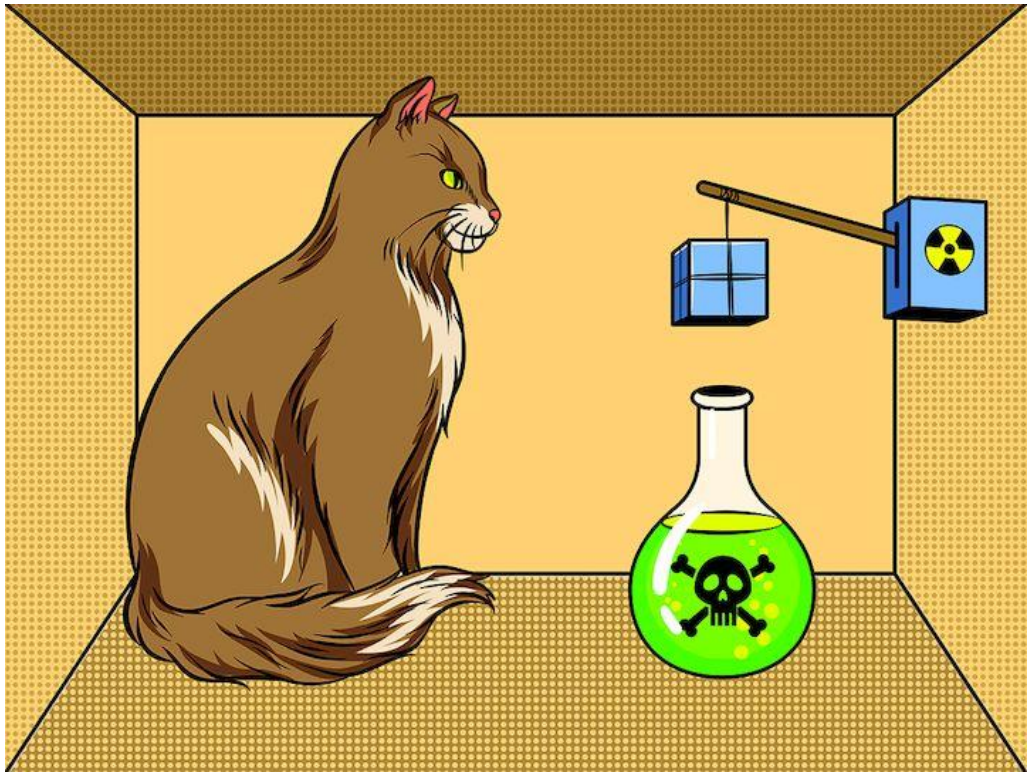
SHOR‘S ALGORITHMUS

Dient zur (Prim-)Faktorenzerlegung

- Gesucht: Faktor der Zahl N
  1. Rate g und prüfe ob ggT(g,N) > 1
  2. Ermittle durch eine Quantenberechnung die kleinste Zahl p sodass $g^p \equiv_N 1$
  3. $g^{\frac{p}{2}} \pm 1$ hat eine bessere Chance ein Faktor von N zu beinhalten

- Zeit um 100-Stellige Zahl zu faktorisieren:
  - Traditioneller Algorithmus: Mehrere Stunden
  - Shor‘s Algorithmus: Wenige Sekunden
- → Verschlüsselung durch Faktorisierung wirkungslos!

SUPERPOSITION

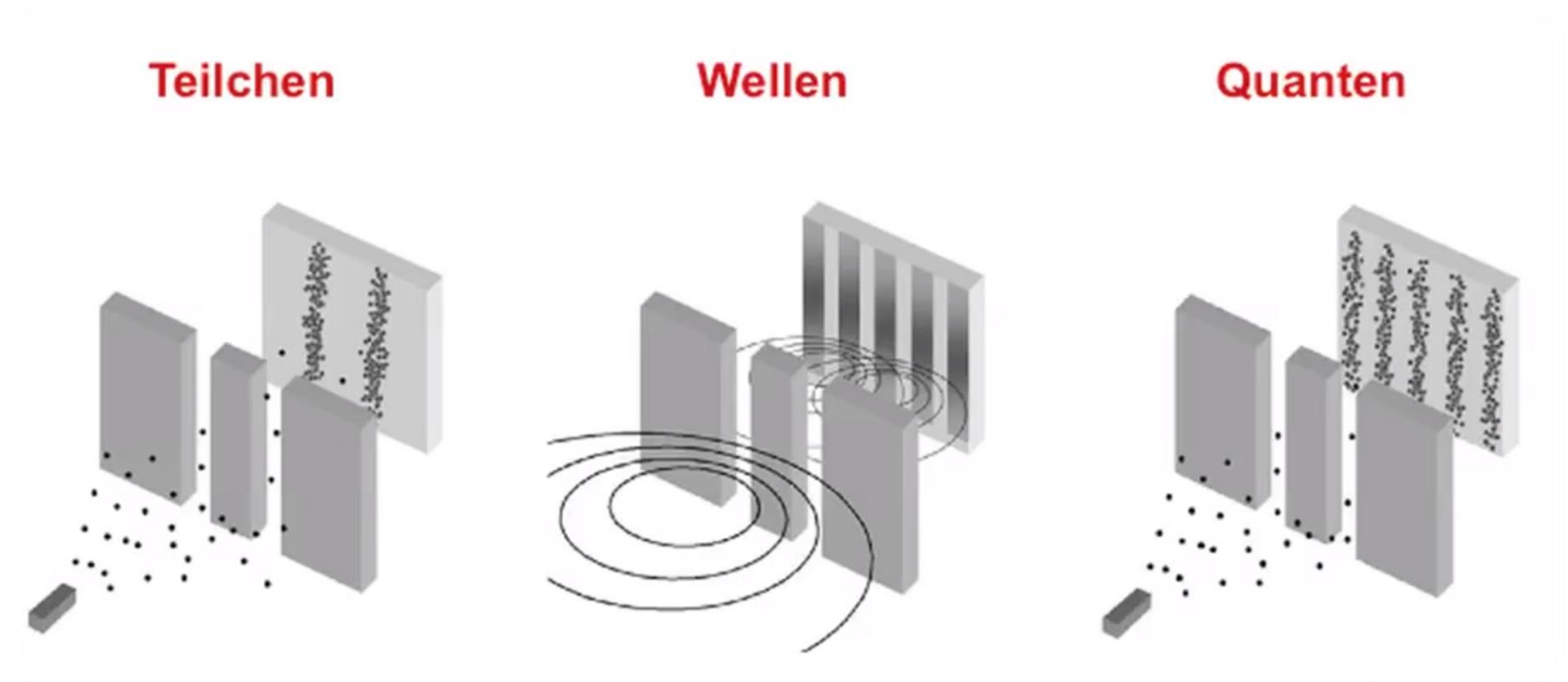


- Klassisches Beispiel: Schrödingers Katze
- Traditionell nur ein Zustand möglich (Informatik: 0 oder 1)
- Überlagerung von Zuständen

  → Superposition!
- Messung einer Superposition liefert einen Konkreten Wert

  → Superposition geht verloren

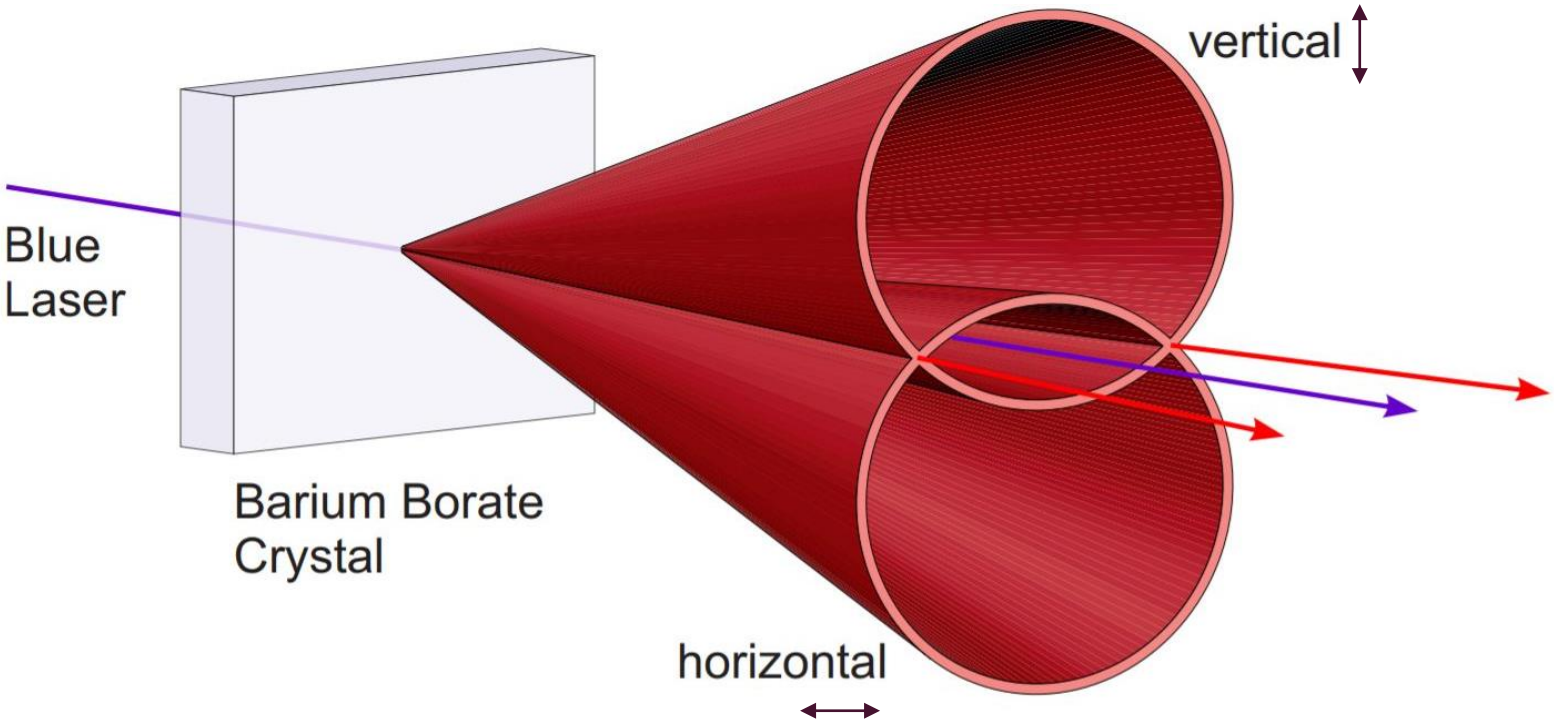
SUPERPOSITION
DOPPELSPALTEXPERIMENT



SUPERPOSITION

$|\Psi\rangle = |\rightarrow\rangle + |\uparrow\rangle$

Wellenfunktion Ψ besteht aus vertikal und Horizontal polarisierten Photonen

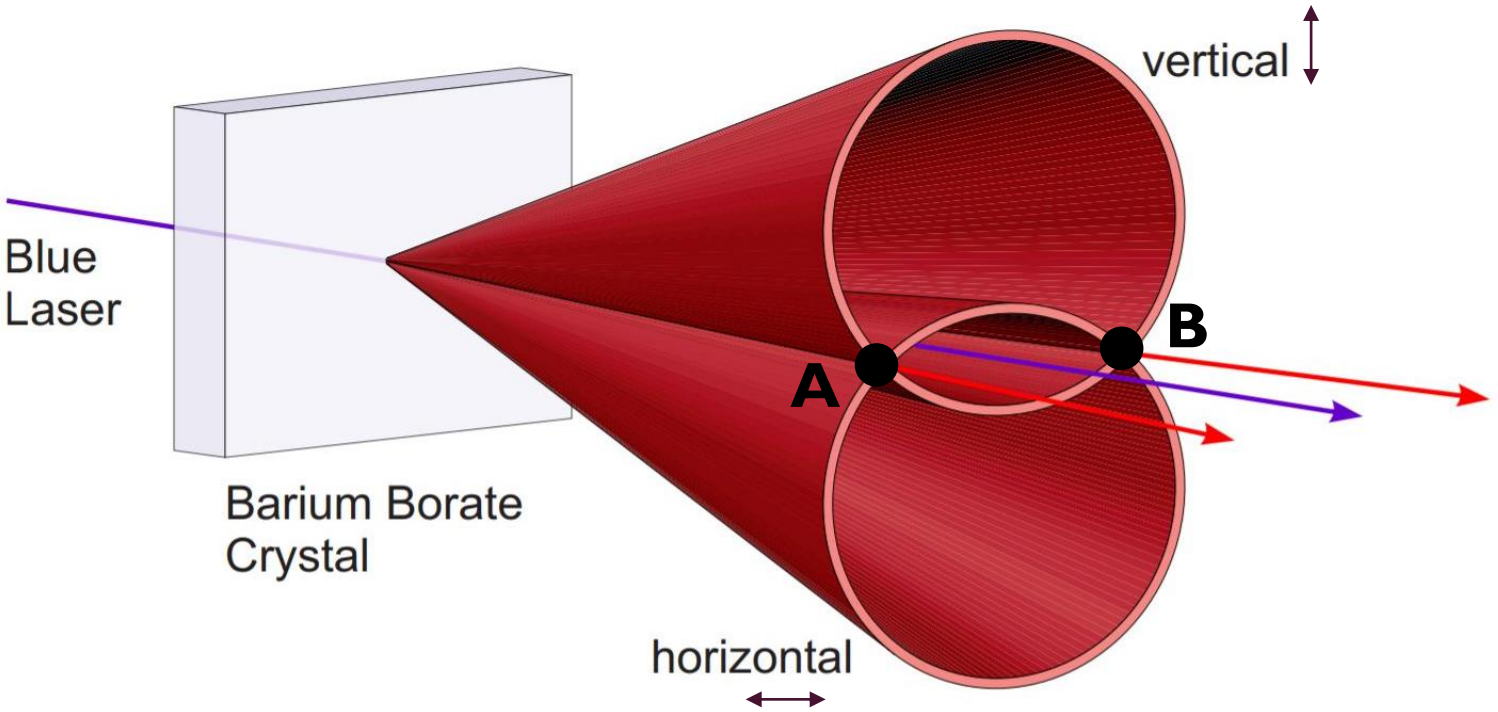


VERSCHRÄNKUNG

- Verschränktes System:
  - Teilsystemen kann kein definierter Zustand zugeordnet werden
- Verschränkung wird beendet wenn man ein Teilsystem auf einen Zustand festlegt (Messung)
- Kommunikation in Überlichtgeschwindigkeit ?

VERSCHRÄNKUNG

$$|\Phi\rangle_{AB} = |\rightarrow\rightarrow\rangle_{AB} + |\uparrow\uparrow\rangle_{AB}$$
$$= |\nearrow\nearrow\rangle_{AB} + |\searrow\searrow\rangle_{AB}$$



Alice		Bob	
↗/↘	↘	↗/↘	↘
→/↑	↑	↗/↘	↘
→/↑	↑	↗/↘	↗
→/↑	↑	→/↑	↑
↗/↘	↗	↗/↘	↗
→/↑	↑	↗/↘	↘
→/↑	→	→/↑	→

Lokal:	Zufällig
Global:	Perfekte Korrelation

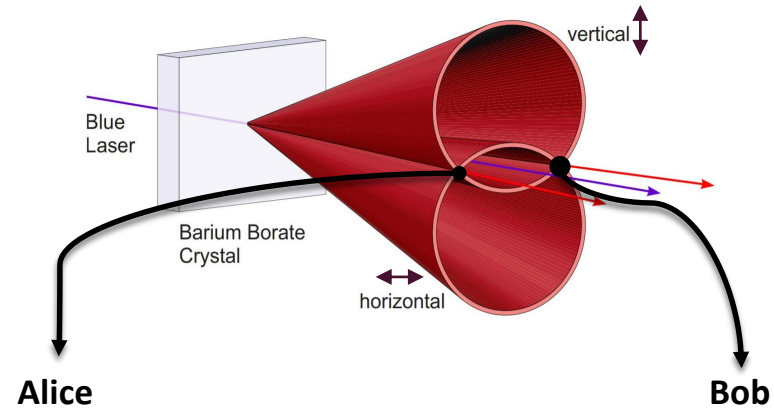
QUANTENSCHLÜSSELAUSTAUSCH (QKD)

- Zuerst Kodierung für Basen wählen

→/↑	
→	0
↑	1

↗/↘	
↗	0
↘	1

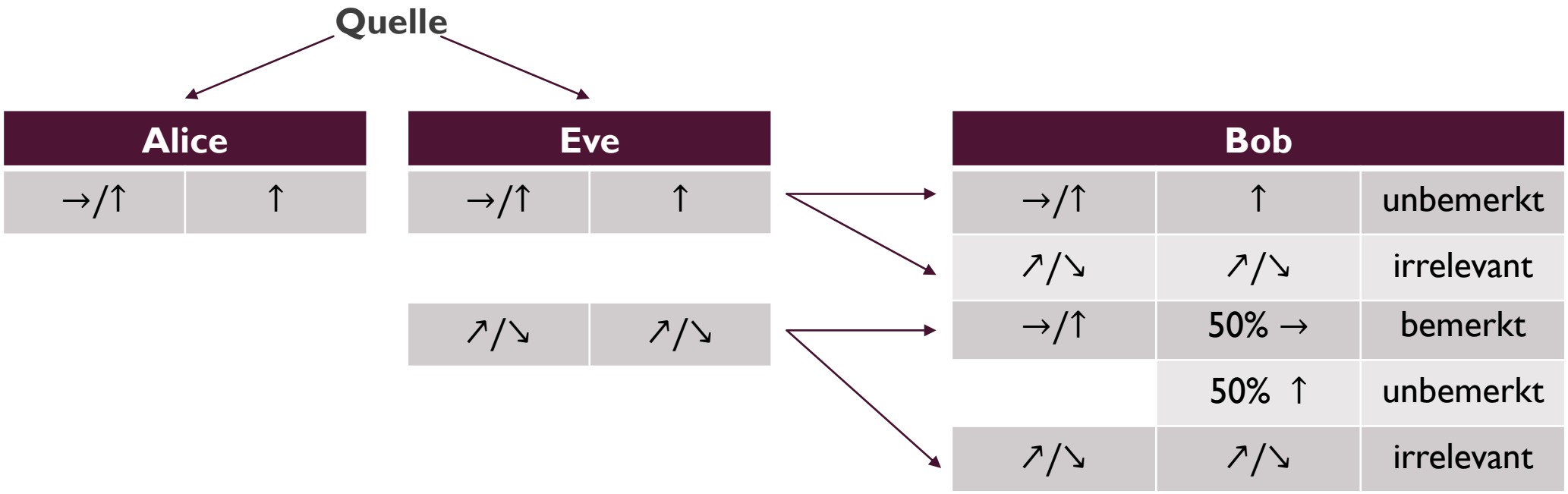
- Was mitteilen?
- Basen **und** Bits!



→/↑	↑	1	↗/↘	↘	1
↗/↘	↘	1	↗/↘	↘	1
↗/↘	↗	0	→/↑	↑	1
→/↑	↑	1	→/↑	↑	1
↗/↘	↗	0	↗/↘	↗	0
→/↑	↑	1	↗/↘	↗	0
→/↑	→	0	→/↑	→	0
⋮					

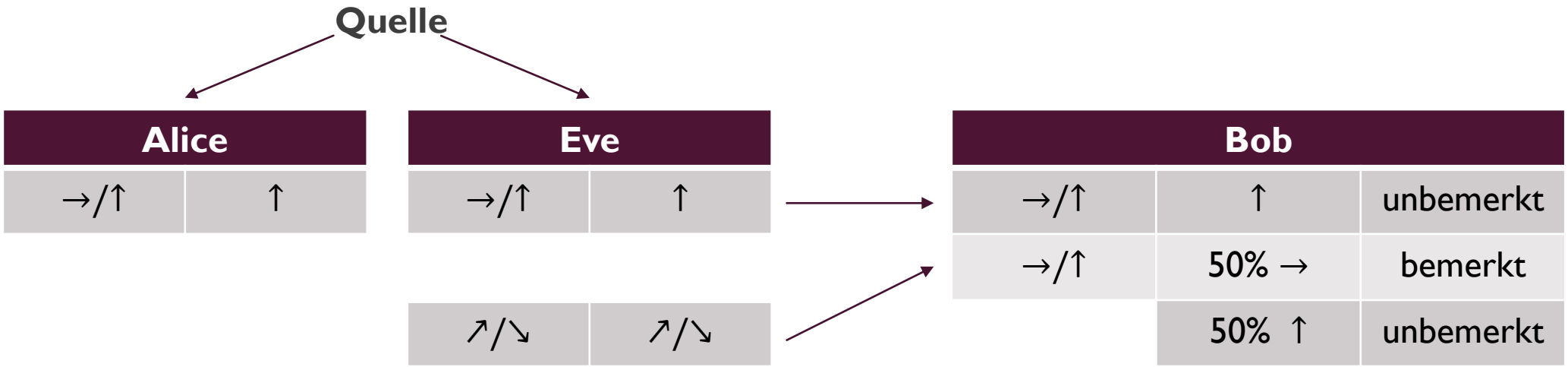
QUANTENSCHLÜSSELAUSTAUSCH (QKD)
EAVESDROPPER / INTERCEPT AND RESEND

- Eve fängt Nachricht die an Bob adressiert ist ab und schickt Ergebnis an Bob



QUANTENSCHLÜSSELAUSTAUSCH (QKD)
EAVESDROPPER / INTERCEPT AND RESEND

- Eve und Bob haben jeweils 50% gleiche Basis wie Alice
- $P_{bemerkt} = \frac{1}{2} * \frac{1}{2} = \frac{1}{4} \rightarrow P_{unbemerkt} = \frac{3}{4}$



QUANTENSCHLÜSSELAUSTAUSCH (QKD)
EAVESDROPPER / INTERCEPT AND RESEND

- Für die Anzahl der verglichenen Bits n gilt:
- $P_{bemerkt} = 1 - \left(\frac{3}{4}\right)^n$

#Bits	$P_{bemerkt}$
1	25%
5	~ 76%
10	~ 94%
20	~ 99,7%
40	~ 99,999%
80	~99,99999999%

QKD-SICHERHEIT

One-Time Pad

1. Zufälliger Schlüssel
2. Schlüssellänge mindestens Länge der Nachricht
3. Schlüssel werden nicht wiederverwendet
4. Schlüssel werden nie öffentlich kommuniziert

FAZIT

- Quantencomputer bedrohen herkömmliche asymmetrische Verfahren
- QKD bietet gleichzeitig aber Lösung durch:
  - Mögliche Umsetzung des One-Time Pad durch echten Zufall
  - Abhörsicheren Key-Austausch (physikalische Gesetze)
- Verschlüsseln/Entschlüsseln der Nachricht bleibt gleich
  - Symmetrische Verfahren weiterhin relevant

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT

FRAGEN?

- Kryptographie
  - Symmetrische Verfahren
  - Asymmetrische Verfahren
  - Sicherheit
  - Shor‘s Algorithmus
- Quantenkryptographie
  - Superposition
  - Verschränkung
  - Quantenschlüsselaustausch
  - Eavesdropper
  - Sicherheit

QUELLEN

- Schrödingers Katze:
  https://nz.bfn.today/schrdingers-cat-st_10400/news/physicists-save-schrdingers-cat-and-bring-us-closer-to-quantum-computers-sn_65338/
- Doppelspaltexperiment:
  https://youtu.be/Cb79hh_Hlsg?t=296
- Verschränkung:
  Experiment 05: Entanglement and Bell‘s inequality, Universität Innsbruck