Seminar zu Quantum-Computing, Quantenkryptographie

Jim Kallarackal,
RWTH-Aachen

21. Juni 2005

Klassische Kryptographie

- Symmetrische Verfahren
- Asymmetrische Verfahren
- Komplexitätsklassen

Quantenkryptographie

- BB84
- Fehlerrate und Korrektur
- Alternative zu BB84
- Praktische Realisierung

Klassische Kryptographie

Cäsar-Verschlüsselung (etwa 50 vor Christus)

- Nachrichten wurden kodiert, indem das Alphabet um k Stellen verschoben wurde
- Aus "THEORIE" $\xrightarrow{+3}$ "WKHRULH"
- Der Schlüssel zum Kodieren und Dekodieren ist $k = 3$

Sicherheit

- In der deutschen Sprache ist 'e' der häufigste Buchstabe (17,5%)
- Der häufigste Buchstabe in WKHRULH ist 'H', identifiziere $H \longrightarrow E \qquad \Rightarrow k = 3$

Klassifikation

Man unterscheidet zwei Klassen von Kryptographieverfahren

Symmetrische Kryptographieverfahren (z.B. DES)

Nur den Beteiligten bekannter einheitlicher Schlüssel zum kodieren und dekodieren.

Asymmetrische Kryptographieverfahren (z.B. RSA)

Kodiert wird die Nachricht mit einem öffentlichen Schlüssel

Dekodieren erfolgt mit einem geheimen, nur dem Empfänger bekannten Schlüssel

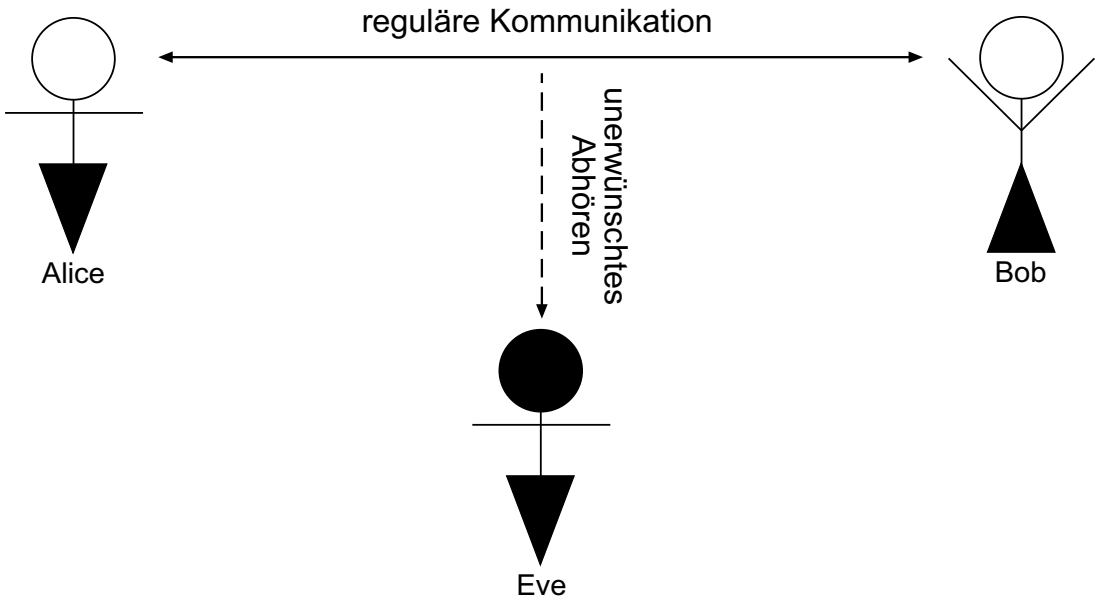
Definitionen

Kryptologie Wissenschaft vom Entwurf, der Anwendung und der Analyse von kryptographischen Verfahren

- Kryptographie
  Verschlüsselung von Nachrichten
- Kryptoanalyse
  Entschlüsselung von Nachrichten und die Analyse der Sicherheit von Verschlüsselungsverfahren

Problemstellung der Kryptographie

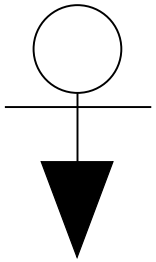
Protagonisten der Kryptographie



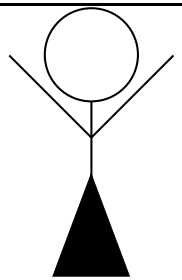
Symmetrische Kryptographiesysteme

1. Alice und Bob einigen sich auf einen geheimen Schlüssel k
2. Alice kodiert die Nachricht mit dem Schlüssel k
3. Bob empfängt die verschlüsselte Nachricht und kann diese mit demselben Schlüssel k dekodieren

Einfaches Beispiel



Nachricht	x = 5	0101
Schlüssel	k = 6	0110
kodiert	c = x XOR k	0011
c = 3		



Schlüssel	k = 6	0110
Verschlüsselt	c = 3	0011
dekodiert	x = c XOR k	0101
x = 5		

Zusammenfassung

- Der Schlüssel k kann nur einmal verwendet werden
- Die Sicherheit symmetrischer Kryptographieverfahren kann gewährleistet werden, falls es gelingt einen geheimen Schlüssel zu vereinbaren

Asymmetrische Kryptographiesysteme

- Bob wählt einen geheimen Schlüssel k_1 und konstruiert daraus einen öffentlichen Schlüssel k_2
- Nachrichten werden mit dem öffentlichen Schlüssel k_2 kodiert
- Nachrichten können nur mit dem geheimen Schlüssel k_1 dekodiert werden.

Grundlegend ist die Existenz einer "One-Way" -Funktion, d.h. $f(x) = y$ ist leicht berechenbar, aber $x = f^{-1}(y)$ ist im Idealfall nicht berechenbar.

RSA (1978) Ronald Rivest, Adi Shamir, Leonard Adleman (MIT 1978)

Bekanntestes und vielfach verwendetes asymmetrisches Verfahren: RSA.

1. Einweg-Funktion:

$$\begin{aligned} f(q,p) &= q \cdot p =: n, \\ q,p &: \text{ sind Primzahlen} \\ \text{Beispiel} &: f(13,19) = 247 \end{aligned}$$

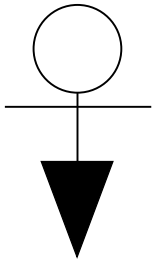
2. $A(p,q) = (p-1) \cdot (q-1)$
   $A(13,19) = 216$

Fortsetzung RSA

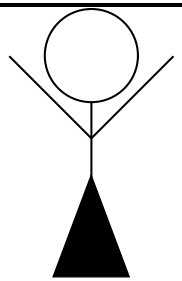
3. Wähle ein $e < n$ mit $\text{ggT}(e, A) = 1$, $\Rightarrow e$ ist ungerade
   $e = 5$
4. bestimme d derart, dass $e \cdot d = 1 \mod A$ und $d < A$
   $d = 173$, denn $5 \cdot 173 = 865 = 4 \cdot A + 1 = 1 \mod A$
5. Insgesamt:

$$\begin{aligned} \text{Öffentlicher Schlüssel } (e, n): &\quad (e, n) = (5, 247) \\ \text{Geheimer Schlüssel } (d, n): &\quad (d, n) = (173, 247) \end{aligned}$$

Kodieren und Dekodieren



Nachricht	$x = 12$
Schlüssel	$(e, n) = (5, 247)$
kodiert	$c = x^e \mod n$
$c = 12^5 \mod 247$	$= 103$



Verschlüsselt	$c = 103$
Schlüssel	$(d, n) = (173, 247)$
dekodiert	$x = c^d \mod n$
$x = 103^{173} \mod 247$	$= 12$

- 'public key' Kryptographiesysteme wurden zuerst 1976 von Whitfield Diffie und Martin Hellman in Stanford vorgeschlagen
- Nach dem britischen Geheimdienst waren solche Verfahren bereits 1973 in Government Communications Headquarters (Cheltenham) bekannt

Sicherheit von RSA und Komplexität

- Die Sicherheit des RSA Algorithmus basiert auf der Existenz einer Einwegfunktion
- Das Faktorisieren natürlicher Zahlen gilt als 'schwieriges' Problem (siehe Komplexität)
- Zur Zeit gilt die Kombination aus asymmetrischen und symmetrischen Kryptographieverfahren mit Hilfe klassischer Rechenmaschienen als sicher

Faktorisieren natürlicher Zahlen

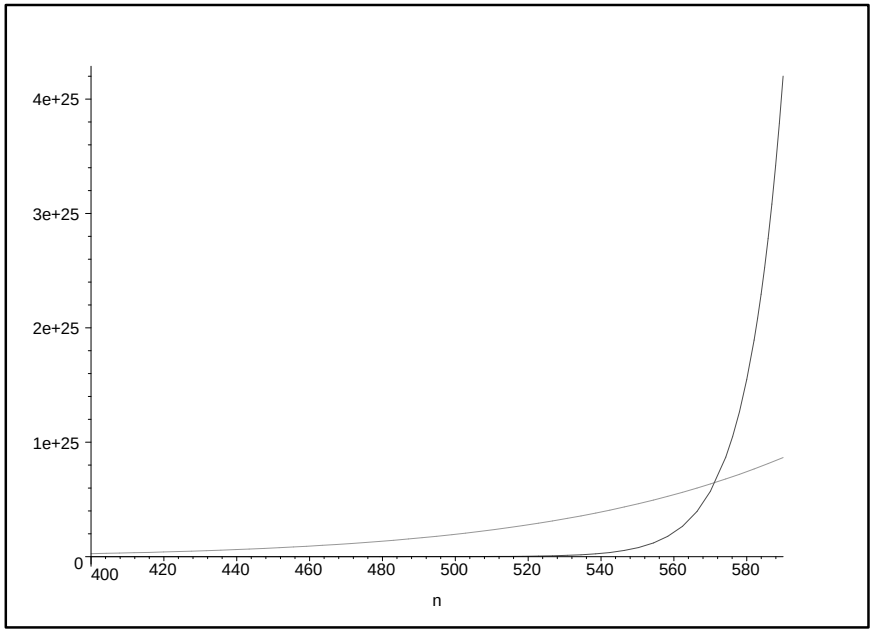


Abbildung: $f(n) = \exp(0.1 \cdot n), \qquad g(n) = n^9$

Komplexität

$$p^r \cdot q^s = 248 \qquad p, q \text{ sind Primzahlen und } r, s \in \mathbf{N}$$
$$p = ? \qquad q = ?$$

- Es ist $2^3 \cdot 31 = 248$
- Das Universum besteht etwa aus 10^{78} Atomen
- Die obige Exponentialfunktion ergibt für $n = 2048$ etwa $8.8 \cdot 10^{88}$. Wäre dies die Rechenzeit eines Algorithmus zum Faktorisieren natürlicher Zahlen, so wird man das Ergebnis nur selten erfahren!

Komplexitätsklassen

In der theoretischen Informatik teilt man Probleme in Komplexitätsklassen ein

Die Klasse P Probleme, für die es eine DTM gibt, dessen Rechenzeit im schlimmsten Fall polynomiell beschränkt ist.

Die Klasse NP Probleme, für die es eine NTM gibt, dessen Rechenzeit im Schlimsten Fall polynomiell beschränkt ist.

NP vollständig Dies sind Probleme aus NP, die bzgl. polynomieller Reduzierbarkeit größer sind als alle anderen Probleme aus NP

DTM entspricht einer Registermaschine oder einem PC
NTM entpricht einem PC mit endlich vielen Prozessoren.

'Schwierige' Probleme

Polynomielle Reduzierbarkeit Es seien L_1 und L_2 Sprachen über Σ_1 bzw. Σ_2. $L_1 \leq L_2$, wenn es eine DTM gibt, die die Funktion

$$w \in L_1 \Leftrightarrow f(w) \in L_2$$

in polynomieller Zeit berechnet.

SAT Gegeben m Klauseln über n Variablen. Gibt es eine Belegung

$$a \in (a_1, \ldots, a_n) \in \{0,1\}^n,$$

welche alle Klauseln erfüllt?

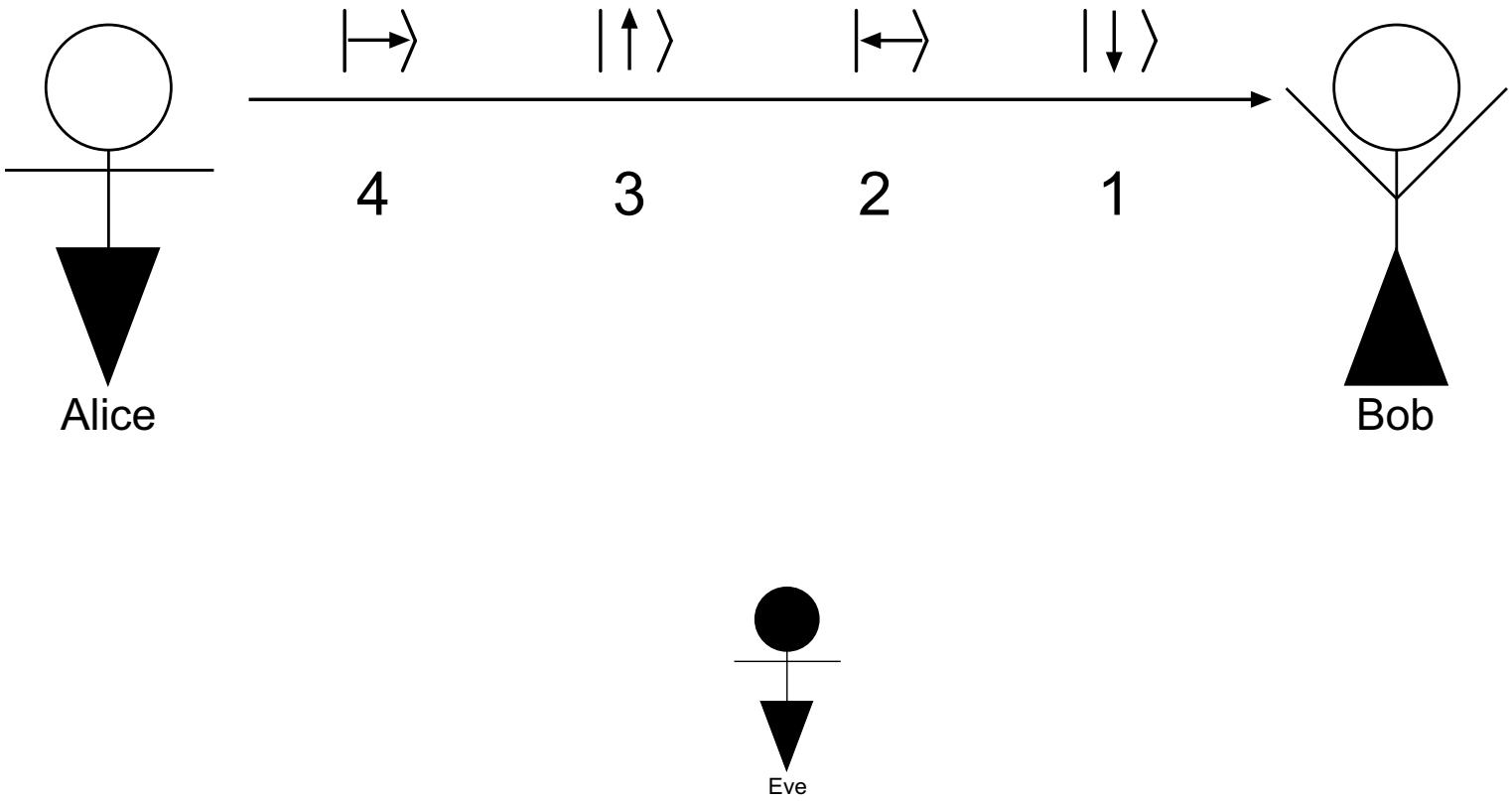
3-SAT Schon der Spezialfall wobei jede Klausel genau 3 Literale enthält, ist NP-vollständig.

- Für das Faktorisieren natürlicher Zahlen gelang es nicht zu zeigen, dass es zur Klasse NP-vollst. gehört
- Die Sicherheit heutiger kryptographischer Systeme, die in vielen kritischen Fällen benuzt werden (Online-Banking), basieren auf den RSA Algorithmus
- $\Rightarrow$ Quantentheorie ermöglicht einen sicheren Austausch einer zufälligen Bitfolge.

Quantentheorie elektromagnetischer Felder

- Photonen sind Spin-1 Teilchen
- Der Spin hängt mit der Polarisation der Photonen zusammen
- Die Eichung $\nabla A = 0$ führt dazu, dass der Spin für Photonen lediglich ± 1 sein kann
- Polarisationszustände könnnen in verschiedenen Basen angegeben werden. z.B. rechtwinklig, zirkular oder diagonal polarisierte Photonen
- Wir betrachten rechtwinklig und diagonal polarisierte Photonen: $|V\rangle$, $|H\rangle$ in der Basis $\bigoplus$ bzw. $|R\rangle$ $|L\rangle$ in der Basis $\bigotimes$
- Identifiziere Bitwerte
  1: $|V\rangle$ oder $|R\rangle$
  0: $|H\rangle$ oder $|L\rangle$

Prinzip der Quantenkryptographie



BB84

Alice

Basis	$\oplus$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\otimes$	$\otimes$	$\oplus$	$\oplus$
Zustand	$\|H\rangle$	$\|R\rangle$	$\|V\rangle$	$\|H\rangle$	$\|L\rangle$	$\|L\rangle$	$\|R\rangle$	$\|H\rangle$	$\|H\rangle$	$\|V\rangle$
Bitwert	0	1	1	0	0	0	1	0	0	1

Bob

Basis	$\otimes$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$
Zustand	$\|R\rangle$	$\|R\rangle$	$\|R\rangle$	$\|H\rangle$	$\|H\rangle$	$\|L\rangle$	$\|V\rangle$	$\|L\rangle$	$\|L\rangle$	$\|V\rangle$
Bitwert	1	1	1	0	1	0	1	0	0	1

Schlüssel

Bitwert		1		0		0		0		1

Im Durchschnitt entspricht die Länge des bereinigten Schlüssels der Hälfte der Sequenz von Alice bzw. Bob (bei idealen Bedingungen)

BB84 (ideal und ohne Dritte)

1. Alice wählt zufällig eine der zwei Basen und präpariert den Wert 1 oder 0
2. Bob empfängt das Teilchen und ermittelt den Eigenwert, wobei er wegen seiner Unkenntnis über die Basis eine beliebige wählt
3. Sind hinreichend viele Teilchen auf diese Weise übertragen, so offenbart Bob seine jeweilige Wahl der Basen
4. Alice teilt mit, welche Teilchen mit Bob's Wahl der Basis übereinstimmten

Beachte: Die Eigenwerte werden zu keinem Zeitpunkt mitgeteilt

Effekte des Abhörens

Alice

Basis	$\oplus$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\otimes$	$\otimes$	$\oplus$	$\oplus$
Zustand	$\|H\rangle$	$\|R\rangle$	$\|V\rangle$	$\|H\rangle$	$\|L\rangle$	$\|L\rangle$	$\|R\rangle$	$\|H\rangle$	$\|H\rangle$	$\|V\rangle$
Bitwert	0	1	1	0	0	0	1	0	0	1

Eve

Basis	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\otimes$	$\oplus$	$\oplus$	$\otimes$
Zustand	$\|H\rangle$	$\|R\rangle$	$\|V\rangle$	$\|R\rangle$	$\|L\rangle$	$\|H\rangle$	$\|R\rangle$	$\|V\rangle$	$\|H\rangle$	$\|L\rangle$
Bitwert	0	1	1	1	0	1	1	1	1	0

Bob

Basis	$\otimes$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$
Zustand	$\|R\rangle$	$\|R\rangle$	$\|L\rangle$	$\|H\rangle$	$\|H\rangle$	$\|L\rangle$	$\|V\rangle$	$\|L\rangle$	$\|L\rangle$	$\|V\rangle$
Bitwert	1	1	0	1	1	0	1	1	0	1

Schlüssel

Alice		1		0		0		0		1
Bob		1		1		0		1		1

BB84 (ideal mit Eve)

- Strategien des Abhörens (Intercept-resend)
  Eve führt eine Messung in einer der zwei Basen durch und präpariert ein neues Photon mit den gemessenen Eigenschaften und überträgt es an Bob.
- Fehlerrate
  In 50% der Fälle gelingt es Eve die Basis in Übereinstimmung mit Alice zu wählen ohne ihre Anwesenheit zu enthüllen. In den verbleibenden Fällen wird sie 50% der Photonen zufällig korrekt präparieren.
  $\Rightarrow$ Der bereinigte Schlüssel hat eine Fehlerrate von 25%
- Mit Wahrscheinlichkeit $\frac{1}{2} + \frac{1}{4} = \frac{3}{4}$ erhält Bob denselben Zustand wie Alice

Folgende zwei Eigenschaften der Quantentheorie gewährleisten die Sicherheit dieser Methode

Unschärfe direkte Konsequenz aus der Nicht-Kommutativität von Operatoren im Hilbertraum

No-Cloning Ein unbekannter Quantenzustand kann nicht kopiert werden.
Begr.:
Der Operator U muss linear und unitär sein
$|\psi,\psi\rangle = \widehat{U}|\psi,\varphi\rangle$
mit $|\psi\rangle = a \cdot |\uparrow\rangle + b \cdot |\downarrow\rangle$
$\Leftrightarrow a \cdot |\uparrow,\uparrow\rangle + b \cdot |\downarrow,\downarrow\rangle =$
$a^2 \cdot |\uparrow,\uparrow\rangle + b^2 \cdot |\downarrow,\downarrow\rangle + ab \cdot (|\uparrow,\downarrow\rangle + |\downarrow,\uparrow\rangle)$
$\Rightarrow ab = 0, \qquad a, b \in \{0, 1\}$
Dies ist der klassische Grenzfall!

Maßnahmen zur Fehlerkorrektur und Erhöhung der Sicherheit

- Fehlerrate
  Alice und Bob vergleichen eine Teilmenge ihres bereinigten Schlüssels und stellen die Fehlerrate ihres Schlüssels fest
- Fehlerkorrektur
  Alice wählt beliebige zwei Bits des Schlüssels und teilt Bob das Resultat der XOR Verknüpfung mit. Erhält Bob denselben Wert, so behalten sie jeweils das erste Bit.
- Erhöhung der Sicherheit
  Alice wählt beliebige zwei Bits und teilt Bob ihre Wahl mit. Beide ersetzen die Bits mit dem Resultat der XOR Verknüpfung

Güte der Übertragung

Obige Überlegung legt einen Grenzwert für die Güte der Übertragung fest

- Es sei p die Wahrscheinlichkeit dafür, dass z.B. aus $|V\rangle$ der Zustand $|H\rangle$ wird.
- Die Fehlerkorrektur ist nur dann sinvoll, wenn die Wahrscheinlichkeit dafür, dass zwei beliebige Zustände gleichzeit falsch sind geringer als 25% ist: $\Rightarrow p^2 = \frac{1}{4} \Rightarrow p = \frac{1}{2}$

Alternative Protokolle

- Protokolle mit Zweiteilchenzuständen
- EPR und Bellsche Ungleichungen

EPR-Protokoll

Es gilt die Bellsche Ungleichung

$$|P(\mathbf{a},\mathbf{b}) - P(\mathbf{a},\mathbf{c})| \leq \int_{\lambda\in\Lambda} \rho(\lambda)\cdot(1 - A(\mathbf{a},\lambda)A(\mathbf{b},\lambda)) = 1 - P(\mathbf{b},\mathbf{c})$$

$A(\mathbf{a},\lambda) = \pm 1$ Messung des Spins an Teilchen 1 in Richtung $\mathbf{a}$

$B(\mathbf{b},\lambda) = \pm 1$ Messung des Spins an Teilchen 2 in Richtung $\mathbf{b}$

$P(\mathbf{a},\mathbf{b})$ Enspricht dem Erwartungswert des Produktes der Spin-Messungen:

$$P(\mathbf{a},\mathbf{b}) = \int_{\lambda\in\Lambda} \rho(\lambda)\cdot A(\mathbf{a},\lambda)B(\mathbf{b},\lambda)$$

Prinzip EPR

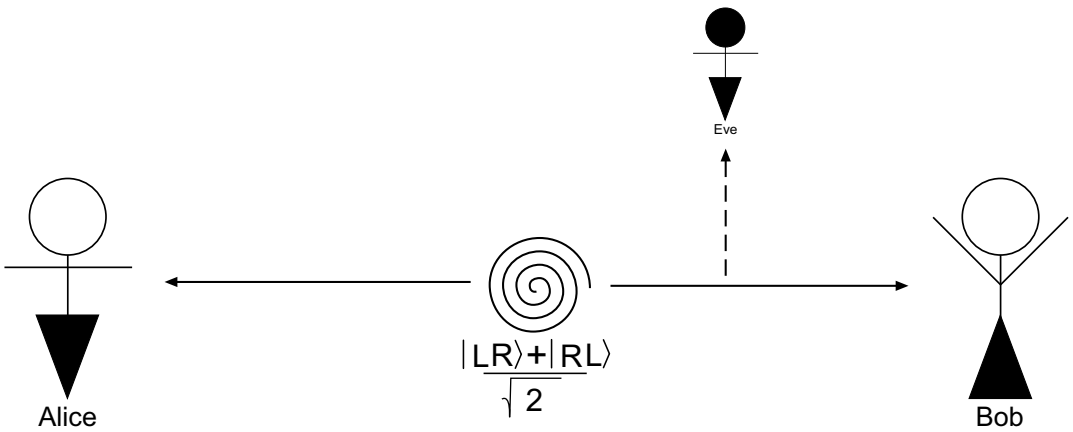


Abbildung: EPR Protokoll

Verschränkte Zustände

Der Zustand

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|V\rangle|H\rangle - |H\rangle|V\rangle\right)$$

verletzt die Bellsche Ungleichung !

- Alice und Bob verfahren analog wie bei BB84, benutzen allerdings eine weitere Basis
- Die verschränkten Zustände werden in einer Quelle, die zwischen Alice und Bob platziert wird, präpariert.
- Zustände sind in einer von drei Basen $\oplus, \otimes, \oslash$
- Alice und Bob ermitteln $P(\mathbf{b}, \mathbf{c})$ und testen die Bellsche Ungleichung

Fortsetzung: EPR

- Ist die Bellsche Ungleichung nicht maximal verletzt, so deutet dies auf eine Manipulation durch Eve hin
  Begr.: Damit Eve Informationen über den Quantenzustand erhält, muss sie eine Messung in einer Basis durchführen
  (Annahme: Eve hat Zugang zu Teilchen 1)
  Betrachte beispielsweise $\langle V, \cdot \,|\psi\rangle$

$$\begin{aligned}\langle V, \cdot \,|\psi\rangle &= \frac{1}{\sqrt{2}}\left(\langle V, \cdot \,|V, H\rangle - \langle V, \cdot \,|H, V\rangle\right) \\ &= \frac{1}{\sqrt{2}}\left(\langle V|V\rangle\langle \cdot|H\rangle - \underbrace{\langle V|H\rangle\langle \cdot|V\rangle}_{=0}\right)\end{aligned}$$

- Die Verschränkung wird also aufgehoben!

Technische Realisation

http://www.idquantique.com

http://www.magiqtech.com

Bisherige Experimente

1989-1992 Brassard (1989), Bennet, Bessette (1992) Übertragung durch Luft mit polarisierten Photonen: 32cm

1995 Müller, Breguet, Gisin, Zbinden (1993-1996) Übertragung durch Glasfaser mit polarisierten Photonen: 22,8 km

1999 Forschungsgruppe in Los Alamos, Übertragung durch Glasfaser mit phasenkodierten Photonen: 48km