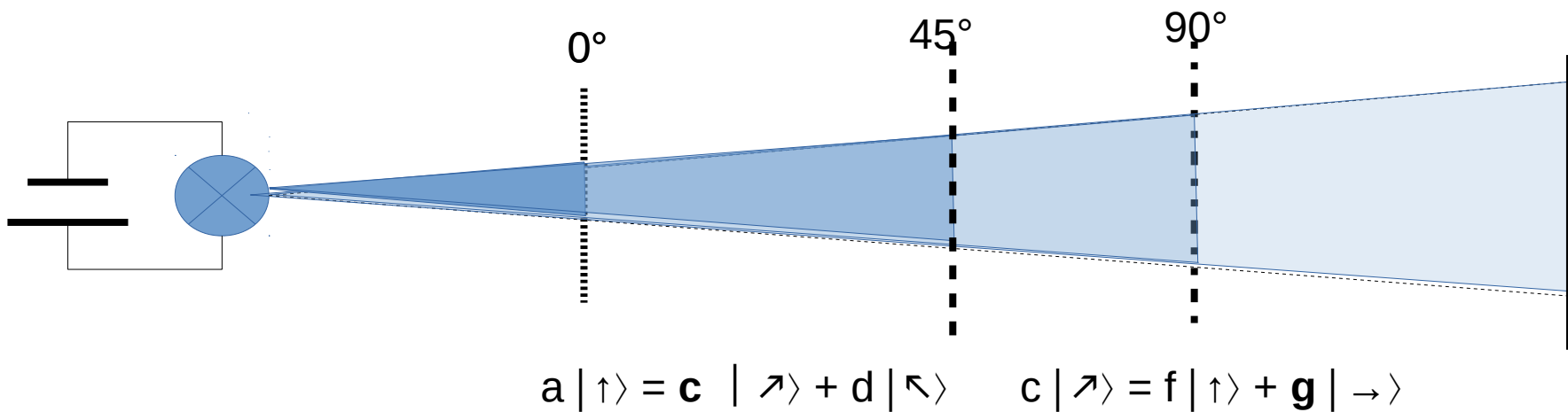
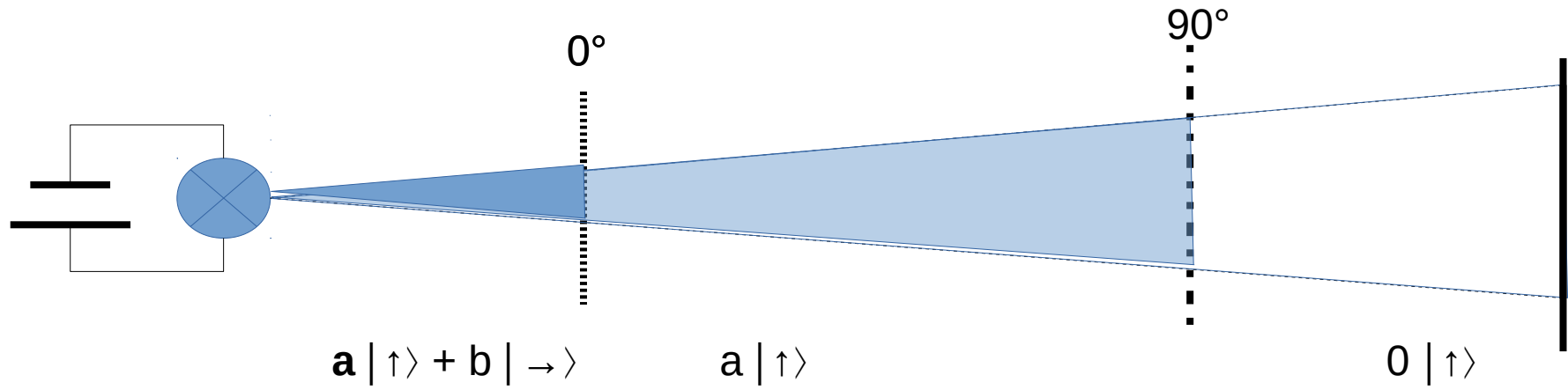


# Themen zur Computersicherheit

## Quantencomputer und Kryptographie -- Eine kurze Einführung --

PD Dr. Reinhard Bündgen  
buendgen@de.ibm.com

# Quantenmechanik der Polarisation



Superposition

# Quantenbits (Qubits)

## Ket Notation

$$x \in \{ a|0\rangle + b|1\rangle \mid$$

$$a, b \in \mathbf{C} \wedge a^2 + b^2 = 1 \}$$

a und b heißen Amplituden

## Spezielle Zustände

- $|+\rangle = 2^{-1/2} (|0\rangle + |1\rangle)$
- $|-\rangle = 2^{-1/2} (|0\rangle - |1\rangle)$
- $|i\rangle = 2^{-1/2} (|0\rangle + i|1\rangle)$
- $|-i\rangle = 2^{-1/2} (|0\rangle - i|1\rangle)$

## Orthonormalbasen

- Standardbasis:  $\{|0\rangle, |1\rangle\}$
- Hadamard Basis:  $\{|+\rangle, |-\rangle\}$

## Bloch Sphäre

$$x \in \{ (a,b,c) \mid$$

$$a, b, c \in \mathbf{R} \wedge a^2 + b^2 + c^2 = 1 \}$$

## Ket $\rightarrow$ Bloch

- $|0\rangle \mapsto (0, 0, 1)$
- $|1\rangle \mapsto (0, 0, -1)$
- $|+\rangle \mapsto (1, 0, 0)$
- $|-\rangle \mapsto (-1, 0, 0)$
- $|i\rangle \mapsto (0, 1, 0)$
- $|-i\rangle \mapsto (0, -1, 0)$

### Notation

- $\mathbf{C}$ : komplexe Zahlen
- $\mathbf{R}$ : Reelle Zahlen

# Operationen auf Qubits

Operationen auf Qubits können durch unitäre Matrizen beschrieben werden.

– A unitär wenn  $(A^*)^T = A^{-1}$

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad x = x_0 |0\rangle + x_1 |1\rangle = \begin{pmatrix} x_0 \\ x_1 \end{pmatrix}$$

$$Ax = (ax_0 + bx_1) |0\rangle + (cx_0 + dx_1) |1\rangle$$

Beispiel: Hadamardmatrix

$$H = 1/\sqrt{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$H |0\rangle = H (1,0)^T = 2^{-1/2} (|0\rangle + |1\rangle)$$

$$H |1\rangle = H (0,1)^T = 2^{-1/2} (|0\rangle - |1\rangle)$$

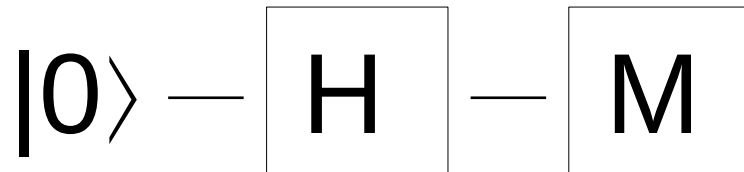
## Notation

- $A^{-1}$  inverse Matrix zu A
- $A^T$  transponierte Matrix von A
- $A^*$  konjugiert komplexe Matrix zu A

# Messen von Qubits

- beim Messen eines Qubits wird sein Zustand zerstört
- gemessen wird bzgl einer Basis  $\{A, B\}$ :
  - $x = aA + bB$
  - dann ist das Messergebnis gleich
    - A mit der Wahrscheinlichkeit  $|a|^2$
    - B mit der Wahrscheinlichkeit  $|b|^2$
  - a und b können nicht gemessen werden

# Quantenalgorithmus: Zufallsgenerator



$x := |0\rangle$

$x := \text{H } x$

miss  $x$  bzgl  $\{ |0\rangle, |1\rangle \}$

$$2^{-1/2} |0\rangle + 2^{-1/2} |1\rangle$$

Ergebnis entweder  $|0\rangle$  oder  $|1\rangle$ ,  
je mit Wahrscheinlichkeit  $1/2$

**Notation**

$:=$  Zuweisung

# Quantenregister

- Quantenregister: Array von Qubits
- Zustände von klassischen Registern:
  - Für klassische Register  $R$ ,  $R_1$ ,  $R_2$  mit  $R = R_1 \parallel R_2$  gilt: für jeden Zustand  $Z$  von  $R$  gibt es Zustände  $Z_1$  von  $R_1$  und  $Z_2$  von  $R_2$ , so dass  $Z = Z_1 \parallel Z_2$ .
- Zustände von Quantenregistern:
  - Für Quantenregister  $Q$ ,  $Q_1$ ,  $Q_2$  mit  $Q = Q_1 \parallel Q_2$  gilt: es gibt Zustände  $Z$  von  $Q$  zu denen es keine Zustände  $Z_1$  von  $Q_1$  und  $Z_2$  von  $Q_2$  gibt, so dass  $Z = Z_1 \parallel Z_2$ .
- Der Zustandsraum eines Quantenregisters kann als Tensorprodukt der Zustandsräume seiner Teilregister beschrieben werden.
- Es gibt keine Methode einen beliebigen Zustand eines Quantenregisters zu kopieren: No Cloning

# Beispiel $R = R_1 \parallel R_2$

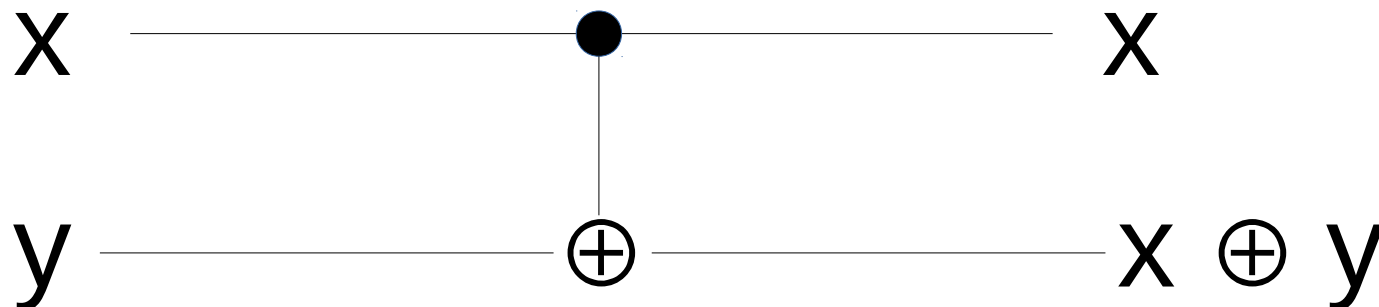
- Der Zustandsraum  $Z = Z_1 \otimes Z_2$  von  $R$  hat die Basis
  - $|0\rangle \otimes |0\rangle = |00\rangle$
  - $|0\rangle \otimes |1\rangle = |01\rangle$
  - $|1\rangle \otimes |0\rangle = |10\rangle$
  - $|1\rangle \otimes |1\rangle = |11\rangle$
- Jeder Zustand von  $R$  kann als Linearkombination
  - $x_0 |00\rangle + x_1 |01\rangle + x_2 |10\rangle + x_3 |11\rangle$
  - beschrieben werden
- Die *Basis* des Zustandsraums eines Quantenregisters aus  $n$  Qubits hat  $2^n$  Elemente



# Operation auf 2-Qubit-Register

- unitäre Operation
- CNOT:  $|x, y\rangle \mapsto |x, x \oplus y\rangle$
- controlled not: ist das erste Qubit 1, so wird das zweite negiert

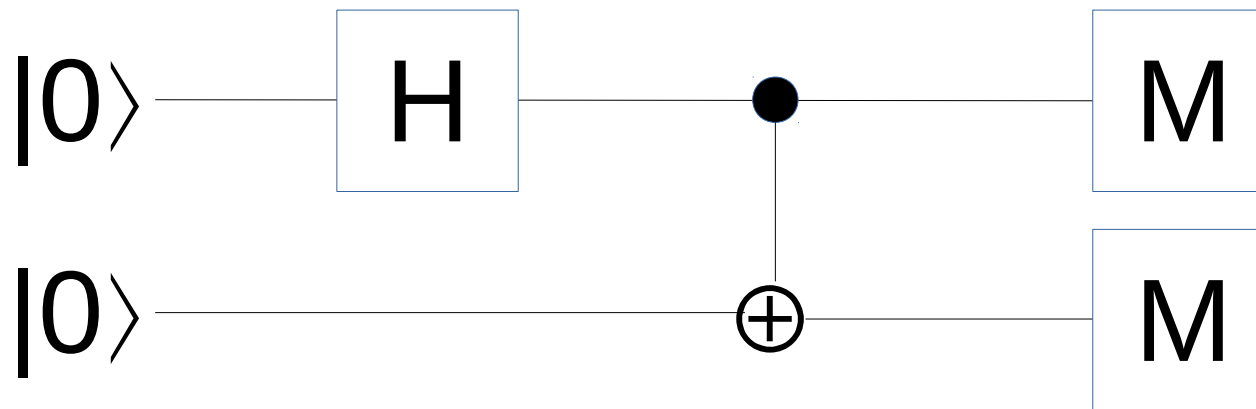
$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad \text{CNOT} \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} a \\ b \\ d \\ c \end{pmatrix}$$



# Verschränkte Zustände

- englisch: entangled
- Ein Zustand  $Z$  von  $R$  heißt verschränkt bzgl einer Dekomposition  $R = R_1 \parallel R_2$ , wenn  $Z$  nicht als Tensorprodukt  $Z_1 \otimes Z_2$  von Zuständen der Register  $R_1$  bzw  $R_2$  beschrieben werden kann
- Beispiel:
  - Der Zustand  $1/2^{-1/2} (|00\rangle + |11\rangle)$  ist verschränkt bzgl der einzelnen Qubits eines 2-Qubit-Registers
  - denn  $(a_0|0\rangle + b_0|1\rangle) \otimes (a_1|0\rangle + b_1|1\rangle)$   
 $= a_0a_1|00\rangle + a_0b_1|01\rangle + b_0a_1|10\rangle + b_0b_1|11\rangle$
  - wenn  $a_0b_1$  und  $b_0a_1$  gleich Null sind auch  $a_0a_1$  oder  $b_0b_1$  gleich Null

# Verschränken von 2 Qubits



- $|00\rangle \xrightarrow{-(H \times I)-} 2^{-1/2}(|0\rangle + |1\rangle) \otimes |0\rangle = 2^{-1/2}(|00\rangle + |10\rangle)$
- $2^{-1/2}(|00\rangle + |10\rangle) \xrightarrow{-\text{CNOT}-} 2^{-1/2}(|00\rangle + |11\rangle)$
- Messung
  - $|00\rangle$  oder  $|11\rangle$ , je mit Wahrscheinlichkeit 0,5
  - verschränkte Qubits können auch einzeln gemessen werden, dann sind Messungen beider Qubits immer gleich
  - Fernwirkung: Trenne Qubits
    - Alice bekommt 1. Qubit
    - Bob bekommt 2. Qubit

**Notation**  
I Identität

# Suchen mit Grover Algorithmus

- Was bedeutet suchen?
  - unstrukturierte DB Suche
    - z.B. Suche nach Besitzer von Telefonnr. im Telefonbuch
  - suche in einer Menge nach Element, das ein Prädikat erfüllt
    - Nachricht, die einen bestimmten Hashwert hat
    - Schlüssel, der einen Geheimtext entschlüsselt
    - NP-vollständige Probleme
- Sei  $N$  die Größe der Menge in der gesucht wird und es gibt genau ein Element, das die Lösung der Suche ist
  - klassischer Aufwand:  $O(N)$ ,  $\Omega(N)$
  - Aufwand mit QC:  $O(\sqrt{N})$ 
    - mit Grover Algorithmus – von Lev Grover (1996)
    - **halbiert Sicherheitsniveau von symmetrischen Chiffren und Hashes**
    - reicht nicht um  $N=NP$  zu zeigen

# Idee des Grover-Algorithmus

- $N$  sei  $2^n$ , das  $n$ -Qubit-Register  $X$  mit Zustand
- $a_0|0\dots 0\rangle + a_1|0\dots 01\rangle + \dots + a_N|1\dots 1\rangle$  mit  $a_i = 1/\sqrt{N}$  für alle  $i$  und  $|x_1\dots x_n\rangle$  repräsentiert das  $k$ -te Element wenn  $k$  binär durch  $x_1\dots x_n$  dargestellt wird.
- Sei  $U$  eine Quantenoperation, die die Amplitude des gesuchten Elements negiert und alle anderen Amplituden gleich lässt.
- Sei  $S$  eine Quantenoperation, jede Amplitude am Mittelwert aller Amplituden spiegelt:  $a_i := -(a_i - 2\sum_k a_k)$
- Wiederhole mehrfach
  - wende  $U$  auf  $X$  an
  - wende  $S$  auf  $X$  an
- Miss  $X$

$O(\sqrt{N})$  mal

# Faktorisieren mit Shors Algorithmus

- Shors Algorithmus ermittelt einen Teiler einer ganzen Zahl der Länge  $n$  in  $O((\log n)^4)$ 
  - benutzt Quanten Fouriertransformation
- Eine Variante von Shors Algorithmus kann zum Berechnen diskreter Logarithmen genutzt werden
- **Gegeben einen Quantencomputer ausreichender Größe: ECDH, ECDSA, DH, DSA und RSA sind nicht mehr sicher.**

# NIST Wettbewerb zur Suche von Post-Quantum Verfahren für asymmetrische Kryptographie

- Ziel: Signatur- und Schlüsselaustauschverfahren
- Auswahlkriterien: Sicherheit, Performance, weitere
- Zeitplan
  - 20.12.2016: Request for Nominations
  - 30.11.2017: Einsendeschluss
  - 21.12.2017: 1. Runde (69 Einreichungen akzeptiert)
  - 30.01.2019: 2. Runde
    - 17 Schlüsselaustausch und 9 Signaturverfahren
  - 2020/2021: 3. Runde oder Algorithmenauswahl
  - 2022/2024: Draft-Standard verfügbar

# Eigenschaften der Post-Quantum-Verfahren

(auch Quantum-safe oder Quantum-resistant genannt)

- Schlüsselgrößen
- Größen der Geheimtexte, Signaturen
- Zeit-/Speicherkomplexität
  - der kryptografischen Operation
  - der Schlüsselerzeugung



# Quanten-Computer

- Ankündigungen von Q-Computern mit  $n$  physischen Qubits
  - 11/2017 IBM: 50 Qubits
  - 01/2018 Intel: 49 Qubits
  - 03/2018 Google: 72 Qubits
  - heute: 200 Qubits?
- Probleme mit QC:
- Stabilität der Qubit Zustände
  - müssen Q-Schaltkreis „überleben“
    - je komplexer die Rechnung, je tiefer und langsamer die Schaltkreise
  - Fehlertoleranz
    - Qubit Zustände sind analog
    - Fehlervermeidungs- und Fehlerkorrekturverfahren
  - Physische vs Logische Qubits
    - sehr viele physische Qubits werden zur Implementierung eines logischen Qubits benötigt

# Wie viele Qubits braucht man?

Schätzung der benötigten Ressourcen zum Brechen von klassischen kryptographischen Verfahren mit QC.

Verfahren	Schlüsselgröße/ Sicherheitsmaß	# log. Qubits	# phys. Qubits	Zeit
AES-GCM	256 / 256	6600	$3 \cdot 10^7$	$2 \cdot 10^{32}$ y
RSA	4096 / 128	8400	$1,5 \cdot 10^7$	230 h
ECC	512 / 256	4700	$8 \cdot 10^6$	95 h
SHA256/Bitcoin	- / 72	2400	$2 \cdot 10^6$	$2 \cdot 10^4$ y
PBKDF2 ( $10^4$ Iter.)	- / 66	2400	$2 \cdot 10^6$	$2 \cdot 10^7$ y

Quelle: „Quantum Computing: Progress and Prospects“ E. Grumbling & M. Horowitz, Eds, National Academies of Sciences, Engineering and Medicine 2018 (prepublication report), Washington DC: The National Academies Press.

# Literatur / Referenzen

- Matthias Homeister: Quantum Computing verstehen, Springer 2015
- E. Rieffel & W. Polak: Quantum Computing a Gentle Introduction, MIT Press 2014
- Web Seite des NIST PQC Wettbewerbs:  
<https://csrc.nist.gov/Projects/Post-Quantum-Cryptography>
  - Präsentation von Dustin Moody: Let's Get Ready to Rumble - The NIST PQC "Competition"  
[https://csrc.nist.gov/CSRC/media/Presentations/Let-s-Get-Ready-to-Rumble-The-NIST-PQC-Competiti/images-media/PQCrypto-April2018\\_Moody.pdf](https://csrc.nist.gov/CSRC/media/Presentations/Let-s-Get-Ready-to-Rumble-The-NIST-PQC-Competiti/images-media/PQCrypto-April2018_Moody.pdf)