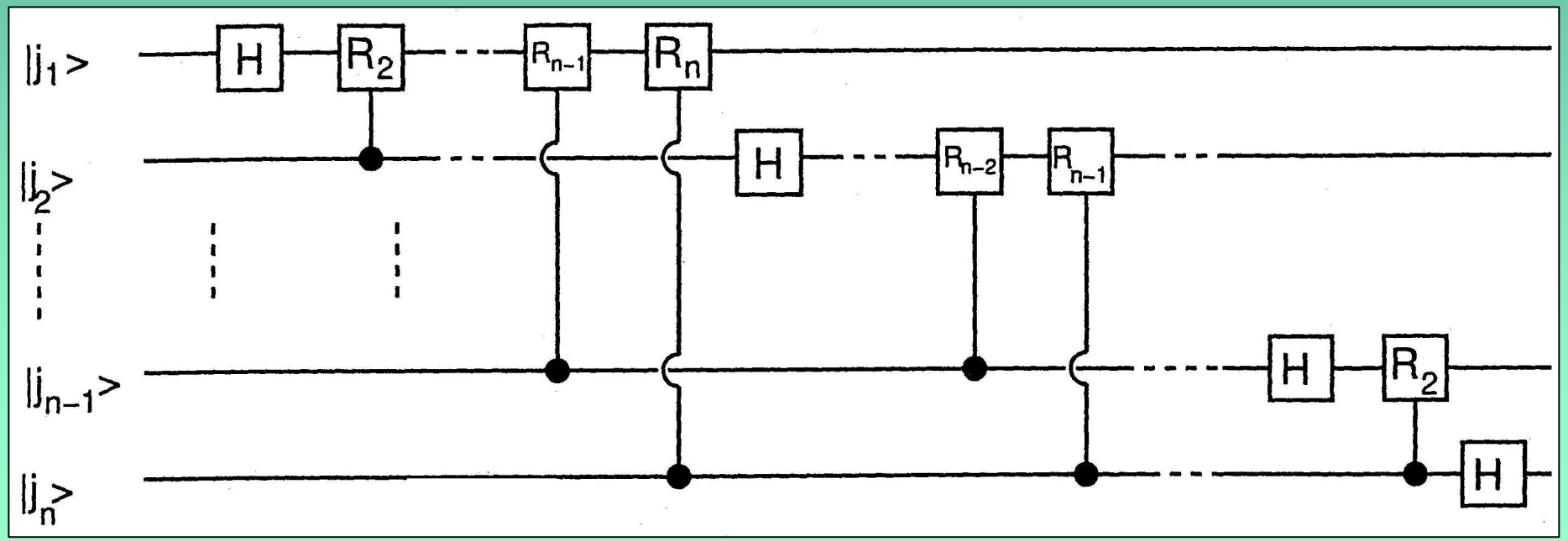
Shor-Algorithmus

Tanja Kempfert



Gliederung

- Einführung
- Laufzeit
- Vorgehen
- Quanten-Fourier-Transformation

Einführung

- Der Shor-Algorithmus liefert zu einer natürlichen Zahl N einen nichttrivialen Faktor
- 1994 von Peter W. Shor veröffentlicht:

Algorithms for quantum computation: Discrete logarithms and factoring,
Proc. 35nd Annual Symposium on Foundations of Computer Science, IEEE Computer Society Press

Quelle: MIT, http://www-math.mit.edu/~shor/

Einführung

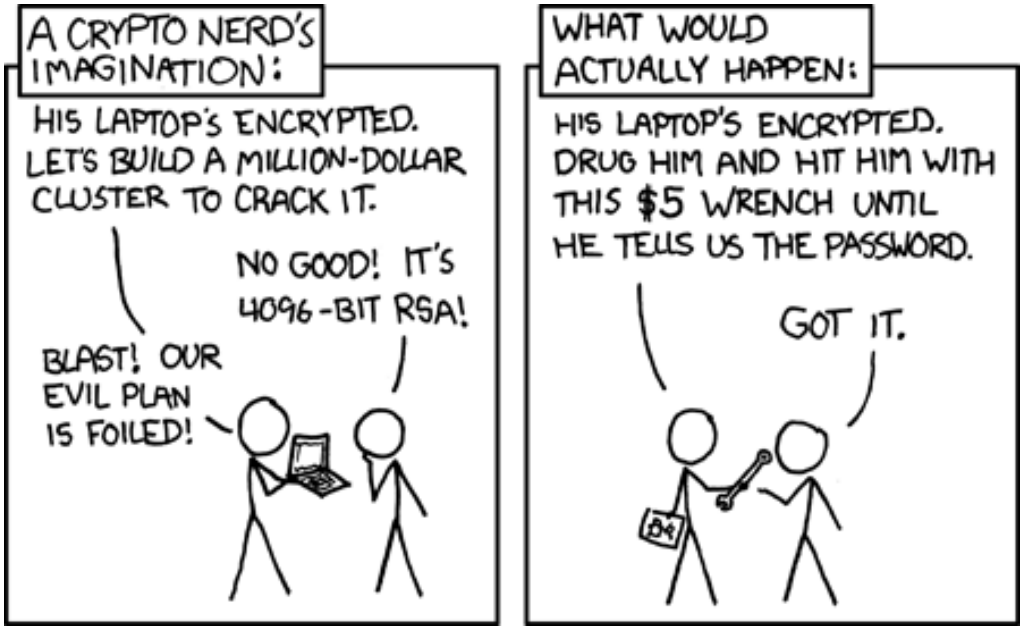
- RSA beruht darauf, dass Faktorisierung großer Zahlen nicht effizient möglich ist

- Fast überall, wo digitale Information sicher übertragen/ gespeichert werden soll, wird RSA verwendet

→ hohes Interesse RSA zu knacken

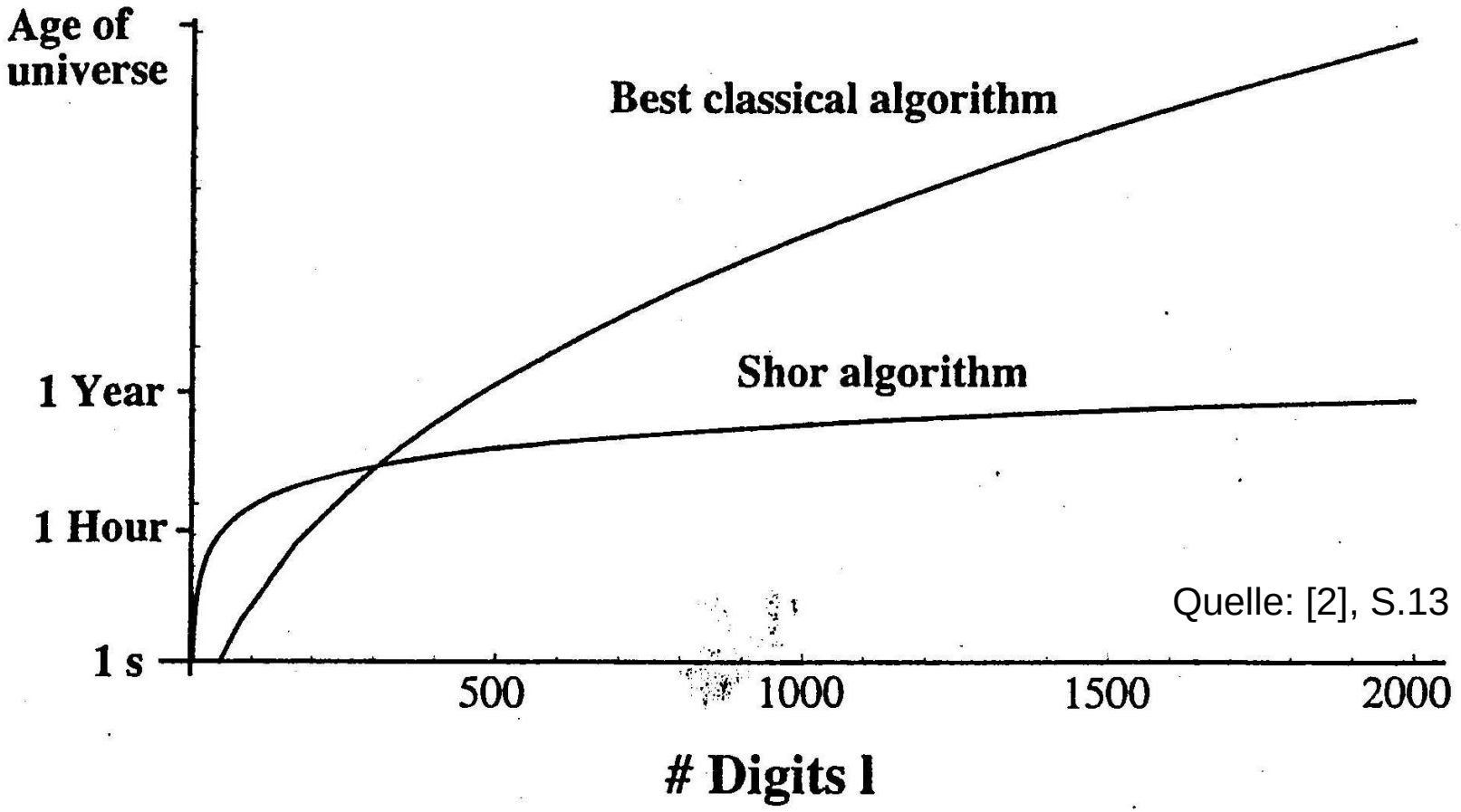
Laufzeit: klassisch vs. Shor

- Klassische Faktorisierungsalgorithmen: Laufzeit nimmt exponentiell mit der Bit-Anzahl zu
- Shor-Algorithmus: Laufzeit nimmt polynomiell zu:
  $\sim \mathcal{O}(log_2 N)^3$



Quelle: xkcd #538, www.xkcd.com

Laufzeit: klassisch vs. Shor



Quelle: [2], S.13

Vorgehen: Vorbemerkungen

- Faktorisierung kann zurückgeführt werden auf Bestimmung der Periode von $a \bmod N$: kleinstes r mit $a^r \bmod N = 1$

- Grundlegender Baustein ist die Quanten-Fourier-Transformation (QFT)

Vorgehen: Vorbemerkungen

Betrachte $F_N(x) = a^x \mod N$ mit Ordnung r

$$F_N(x+r) = F_N(x)$$

$$r \leq N$$

Es können 3 Fälle auftreten:

- r ungerade
- r gerade und $a^{r/2} \mod N = -1$
- r gerade und $a^{r/2} \mod N \neq -1$

Nur der letzte Fall ist für uns interessant

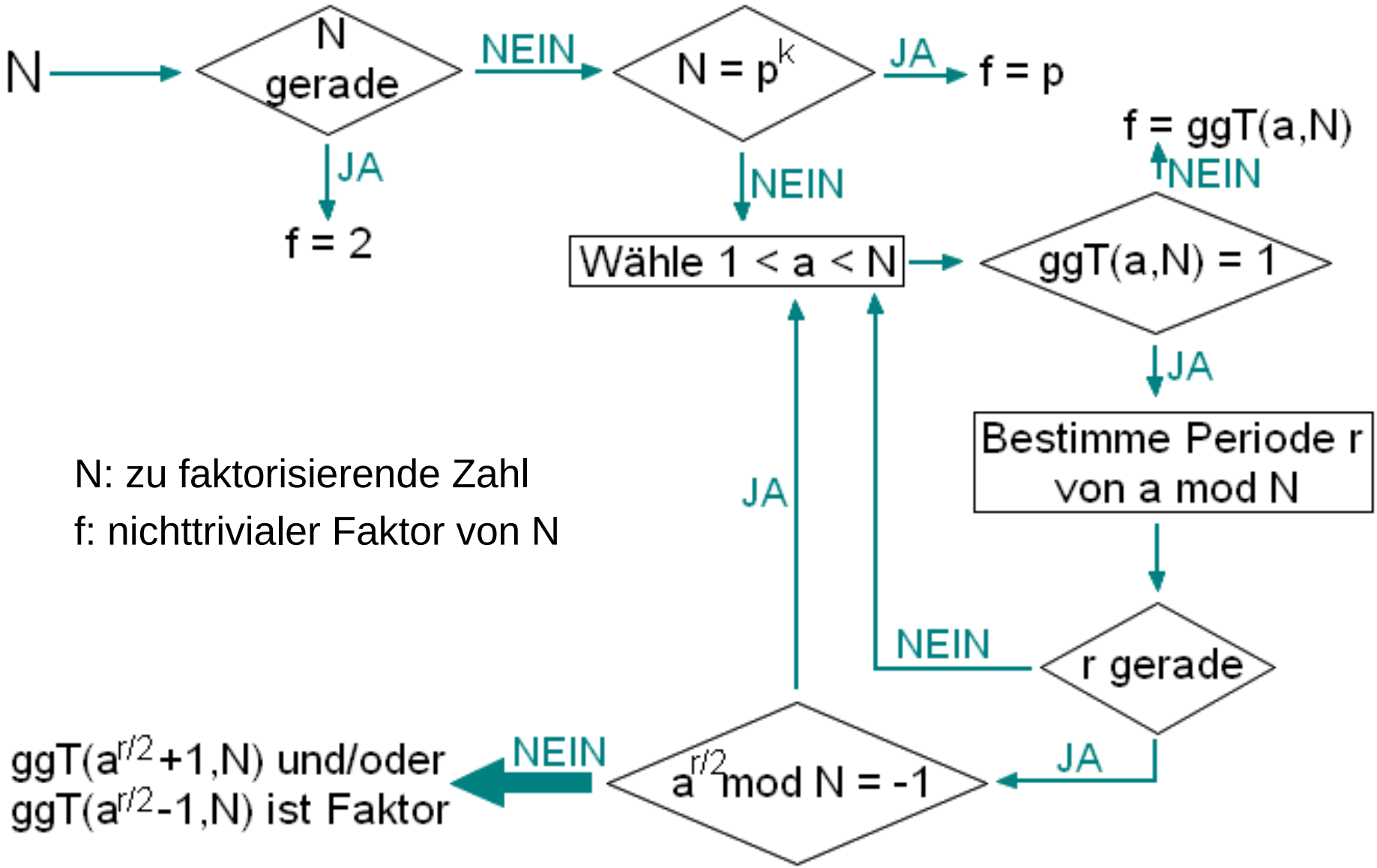
Vorgehen: Vorbemerkungen

Setze $x = a^{r/2}$ und betrachte $x^2 \bmod N = 1$
$x \bmod N = \pm 1$ ist immer Lösung

$\Rightarrow (x^2 - 1) \bmod N = (x-1)(x+1) \bmod N = 0$

$\Rightarrow$ N hat gemeinsamen Faktor mit $(x \pm 1)$
falls x nichttriviale Lösung

Vorgehen



N: zu faktorisierende Zahl

f: nichttrivialer Faktor von N

Vorgehen: Periodenbestimmung

Wir verwenden 2 Quantenregister. Das erste wird in eine Überlagerung aller Zustände überführt

$$|\Psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle|0\rangle$$

Auf das zweite wird $a^k \bmod N$ angewendet

$$|\Psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle|a^k \mathrm{mod} N\rangle$$

Vorgehen: Periodenbestimmung

Messung an Register 2

$$|\Psi_3\rangle = \frac{1}{\sqrt{2^n/r}} \sum_{k=0}^{\frac{2^n}{r}-1} |kr+l\rangle|c\rangle$$

Wende QFT auf Register 1 an

$$|\Psi_4\rangle = \frac{\sqrt{r}}{2^n} \sum_{b=0}^{2^n-1} \sum_{k=0}^{\frac{2^n}{r}-1} \exp(2\pi i(kr+l)b/2^n)|b\rangle$$

Vorgehen: Periodenbestimmung

$$|\Psi_4\rangle = \frac{\sqrt{r}}{2^n} \sum_{b=0}^{2^n-1} \sum_{k=0}^{\frac{2^n}{r}-1} \exp(2\pi i(kr+l)b/2^n)|b\rangle$$

Messung an Register 1, Ergebnis sei b_0

b_0 erfüllt mit hoher Wahrscheinlichkeit folgende Bedingung:

$$|\frac{b_0}{2^n} - \frac{m}{r}| \leq \frac{1}{2^{n+1}}$$

r lässt sich durch einen Kettenbruch approximieren

QFT

Diskrete Fourier-Transformation

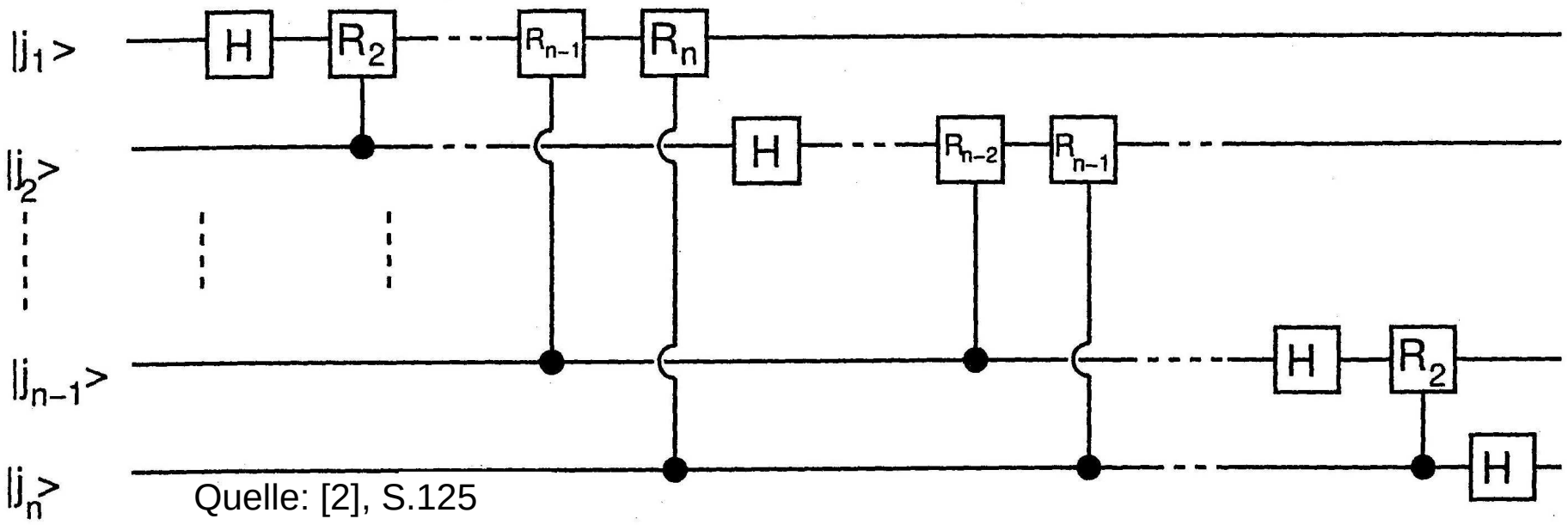
$$y_j = \frac{1}{\sqrt{Q}} \sum_{k=0}^{Q-1} \exp(\frac{2\pi i}{Q} jk) x_k$$

Analog dazu: Quanten-Fourier-Transformation

$$|j\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \exp(\frac{2\pi i}{2^n} jk) |k\rangle$$

$$= 2^{-n/2} \bigotimes_{l=1}^{n} [|0\rangle_l + \exp(2\pi i j 2^{-l}) |1\rangle_l]$$

QFT



Quelle: [2], S.125

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

Hadamard-Gatter

$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^k}} \end{pmatrix}$$

Phase-Shift-Gatter

Experimentelle Umsetzung

- 2001: Faktorisierung von 15 durch IBM
  (erste experimentelle Umsetzung überhaupt)

- 2012: Faktorisierung von 21 an der Universität Bristol

  E. Martín-López, A. Laing, T. Lawson, R. Alvarez, X-Q. Zhou, J. L. O'Brien:

  Experimental realization of Shor's quantum factoring algorithm using qubit recycling

  Nature Photonics 6, 773-776 (2012), arXiv:1111.4147 [quant-ph]

Quellen

[1] P. Shor: Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer
SIAM Journal of Computing 26 (1997)
(erweiterte und überarbeitete Version des Original-Papers)

[2] J. Stolze, D. Suter: Quantum Computing. A Short Course from Theory to Experiment
Wiley (2008)

[3] A. Ekert, R. Jozsa: Quantum computation and Shor‘s factoring algorithm
Reviews of Modern Physics, Vol. 68 (1996)

[4] D. Aharonov: Quantum Computation - A Review.
Annual Reviews of Computational Physics, World Scientific, Vol. VI (1998)