Der Shor Algorithmus

Übersicht

- Zahlentheoretische Grundlagen: Finden der Ordnung
- Diskrete Fouriertransformation (klassische und quantenmechanische Realisierung)
- Phase Estimation
- Shor Algorithmus in der Übersicht

Das RSA Kryptographieverfahren

- Zerlegung einer Zahl N in Faktoren, Aufwand:

$$e^{logN^{1/3}(log[log(N)])^{2/3}}$$

- Verfahren sicher, solange kein schnellerer Algorithmus existiert.

- Beispiel: Zahl, die in Dezimaldarstellung 300 Stellen hat ⟹ Rechendauer: mehrere Mrd Jahre

Quantencomputer

- Shor‘s Algorithmus: polynomialer Aufwand
- Anwendbar falls N ungerade und N ist keine Potenz einer Primzahl
- Bisher: 15 = 5 * 3

$$O(log(N)^{2/3}) \quad \Longleftrightarrow \quad O(e^{logN^{1/3}(log[log(N)])^{2/3}})$$

Rechnungen in mod N

- Definition: $x = y \bmod \mathrm{N} \Leftrightarrow x = y + n \cdot N$

- Für uns wichtig: x mod N gibt den Rest an, der bei der Division von N durch x übrigbleibt:

$$16 \bmod 11 = 5$$

- Mit den Gleichungen kann man (fast) wie gewohnt rechnen:

$$(x \bmod \mathrm{N} = z_1) \text{ und } (y \bmod \mathrm{N} = z_2) \qquad x \cdot y \bmod \mathrm{N} = z_1 \cdot z_2 \bmod \mathrm{N}$$

Faktorisierung von N

$$r^2 = 1 \bmod N$$

$$1331^2 = 1 \bmod 21$$

$$r^2 - 1 = nN$$

$$1331^2 - 1 = 84360 \cdot 21$$

$$n \in (1, 2, ...)$$

$$(r+1)(r-1) = nN$$

$$1332 \cdot 1330 = n \cdot 21$$

$$(2^2 \cdot 3^2 \cdot 37) \cdot (2 \cdot 5 \cdot 7 \cdot 19) = n \cdot 21$$

- Wenn (r+1) und (r-1) kein trivialer Faktor: bestimme größten gemeinsamen Teiler mit euklidischem Algorithmus (effizienter)

Ordnung

- Als Ordnung einer Zahl q mod N bezeichnet man die kleinste ganze Zahl k mit:

$$q^k \bmod \mathrm{N} = 1$$

$$11^2 \bmod 21 = 121 \bmod 21 = 16 \bmod 21$$

$$11^3 \bmod 21 = 16 \cdot 11 \bmod 21 = 8 \bmod 21$$

$$11^4 \bmod 21 = 8 \cdot 11 \bmod 21 = 4 \bmod 21$$

$$11^5 \bmod 21 = 4 \cdot 11 \bmod 21 = 2 \bmod 21$$

$$11^6 \bmod 21 = 2 \cdot 11 \bmod 21 = 1 \bmod 21$$

- Wir brauchen:

$$r^2 = 1 \bmod \mathrm{N}$$

- Falls man gerade Ordnung k findet:

$$r = q^{k/2}$$

$$\mathrm{p}(\text{k gerade und } q^{k/2} \neq -1 \bmod \mathrm{N}) \geq 1 - 2^{-m}$$

$$N = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_m^{\alpha_m}$$

Beispiel

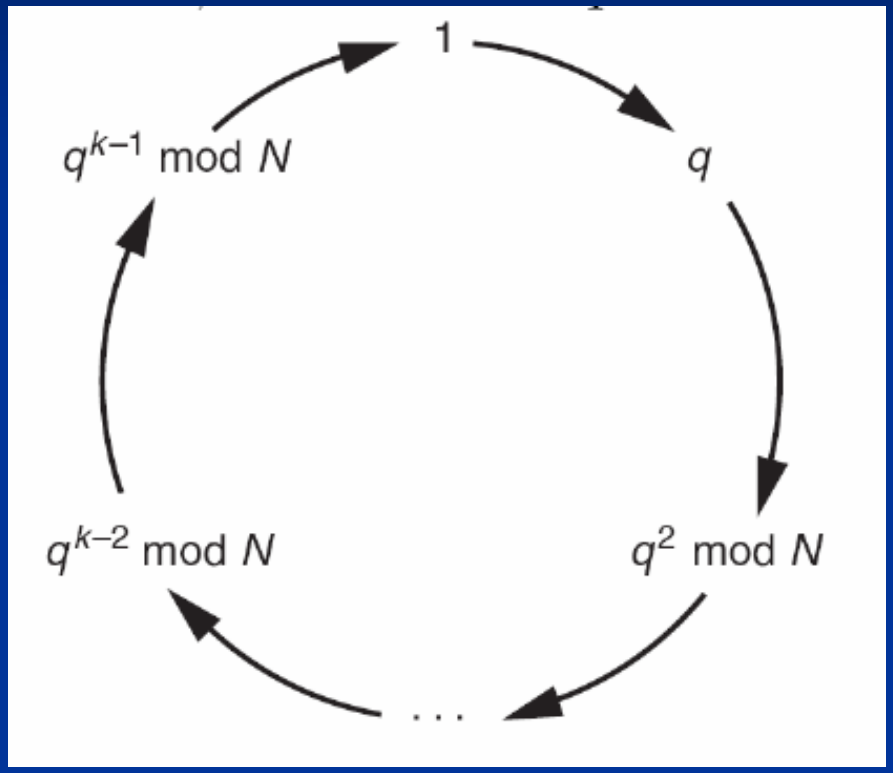
- Ordnung von 11 mod 21 ist 6

$$r = q^{k/2} \quad \Rightarrow \quad r = 11^{6/2} = 11^3 = 1331$$

$$(r+1)(r-1) = nN \quad \Rightarrow \quad 1332 \cdot 1330 = n \cdot 21$$

- ggt(1330, 21)=7
- ggt(1331,21)=3

Idee zur Ordnungsbestimmung



- Definiere den unitären Operator

$$\hat{U}\,|x\rangle = |xq \bmod \mathrm{N}\,\rangle$$

- Für die Eigenwerte gilt wegen

$$\hat{U}^k = I$$

$$\hat{U}\,|u_s\rangle = \lambda_s\,|u_s\rangle \Rightarrow \lambda_s^k = 1 \Leftrightarrow \lambda_s = e^{i2\pi s/k}$$

Diskrete Fouriertransformation

- Definiert als:

$$y_k = \frac{1}{\sqrt{n}} \sum_{l=0}^{n-1} e^{i\frac{2\pi}{n}lk} x_l$$

- In Matrixschreibweise:

$$(F)_{kl} := \frac{1}{\sqrt{n}} e^{i\frac{2\pi}{n}(l-1)(k-1)}$$

$$y = Fx$$

- F ist unitär, insbesondere ist die Umkehrung möglich

$$FF^\dagger = I$$

$$F^\dagger y = x$$

Quantenmechanische FT

$$y_k = \frac{1}{\sqrt{n}} \sum_{l=0}^{n-1} e^{i\frac{2\pi}{n}lk} x_l$$

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

- Zahlen werden durch quantenmechanische Zustände repräsentiert, z.B.:

$$|0\rangle \otimes |1\rangle \otimes |0\rangle \otimes |1\rangle := |5\rangle$$

- Vorteil: simultane Berechnung der Fouriertransformierten für die Zahlen j=0, 1, …, 2^n-1

Quantenmechanische FT

- Dualdarstellung:

$$j = \sum_{l=1}^{n} j_l \cdot 2^{n-l}$$

$$|j\rangle = |j_1\rangle \otimes |j_2\rangle \otimes \cdots \otimes |j_n\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{i\frac{2\pi}{2^n}jk} |k\rangle =$$

$$\frac{1}{\sqrt{2^n}} \sum_{k_1=0}^{1} \sum_{k_2=0}^{1} \cdots \sum_{k_n=0}^{1} e^{i2\pi j(\sum_{l=1}^{n} k_l 2^{-l})} |k_1\rangle \otimes |k_2\rangle \otimes \cdots \otimes |k_n\rangle =$$

$$\frac{1}{\sqrt{2^n}} \sum_{k_1=0}^{1} \sum_{k_2=0}^{1} \cdots \sum_{k_n=0}^{1} \prod_{l=1}^{n} e^{i2\pi j(k_l 2^{-l})} |k_1\rangle \otimes |k_2\rangle \otimes \cdots \otimes |k_n\rangle =$$

$$\frac{1}{\sqrt{2^n}} \bigotimes_{l=1}^{n} [\sum_{k_l=0}^{1} e^{i2\pi j(k_l 2^{-l})} |k_l\rangle]$$

Quantenmechanische FT

$$\frac{1}{\sqrt{2^n}} \bigotimes_{l=1}^{n} [\sum_{k_l=0}^{1} e^{i2\pi j(k_l 2^{-l})} |k_l\rangle] =$$

$$\frac{1}{\sqrt{2^n}} \bigotimes_{l=1}^{n} [|0\rangle + e^{i2\pi j 2^{-l}} |1\rangle] =$$

$$\frac{1}{\sqrt{2^n}} [|0\rangle + e^{i2\pi 0.j_n} |1\rangle] \otimes [|0\rangle + e^{i2\pi 0.j_{n-1}j_n} |1\rangle] \otimes \cdots \otimes [|0\rangle + e^{i2\pi 0.j_1 j_2 \ldots j_n} |1\rangle]$$

- Wobei:

$$0.d_1 d_2 \ldots d_n = \sum_{k=1}^{n} d_k \cdot 2^{-k}$$

- z.B.:

$$0.101 = 1 \cdot 2^{-1} + 0 \cdot 2^{-2} + 1 \cdot 2^{-3}$$

Beispiel für 2 Qubits

- Das Gatter sollte folgende Zuweisung realisieren:

$$|j_1\rangle \otimes |j_2\rangle \rightarrow \frac{1}{\sqrt{4}}(|0\rangle + e^{i2\pi(\frac{j_2}{2})}|1\rangle) \otimes (|0\rangle + e^{i2\pi(\frac{j_1}{2}+\frac{j_2}{4})}|1\rangle)$$

Benötigte Information: j_1 j_1 und j_2

- Vorgehen:

$$(|0\rangle + e^{i2\pi(\frac{j_2}{2})}|1\rangle) = \begin{cases} (|0\rangle + |1\rangle) & \text{Falls } j_2 = 0 \\ (|0\rangle - |1\rangle) & \text{Falls } j_2 = 1 \end{cases}$$

Wenn man auf $|j_2\rangle$ das Hadamard Gate wirken lässt, erhält man den gesuchten Zustand

Beispiel für 2 Qubits

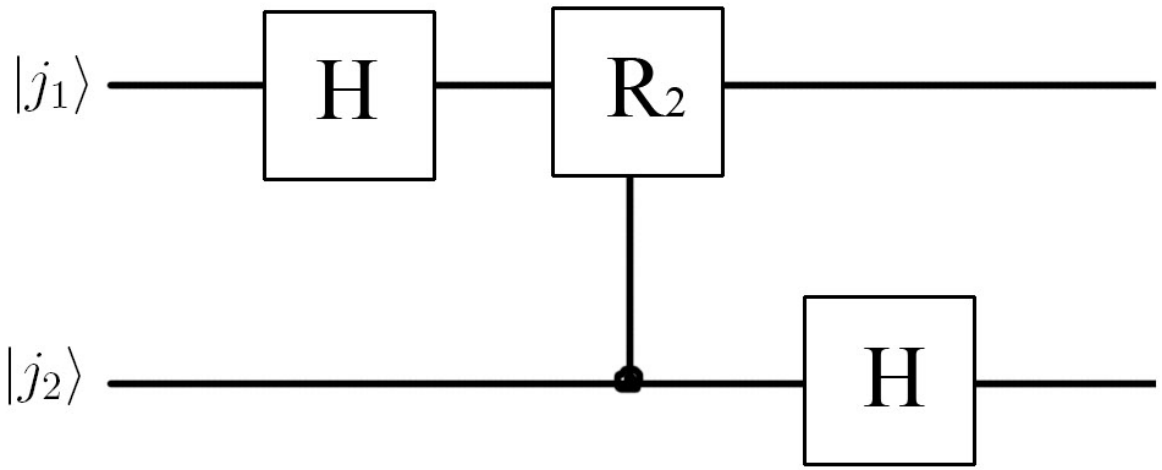
- Nun zur Erzeugung von $(|0\rangle + e^{i2\pi(\frac{j_1}{2}+\frac{j_2}{4})}|1\rangle)$
- Durch die Wirkung des Hadamard Gates auf $|j_1\rangle$ erhält man: $(|0\rangle + e^{i2\pi(\frac{j_1}{2})}|1\rangle)$

Die nächste Operation sollte nur auf den Zustand 1 wirken und die Phase mit $e^{2\pi i/4}$ multiplizieren, falls $j_2 = 1$ und den Zustand völlig unverändert lassen, falls $j_2=0$

- Man verwendet folgende unitäre Transformation:

$$R_2 = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/4} \end{pmatrix}$$

Beispiel für 2 Qubits



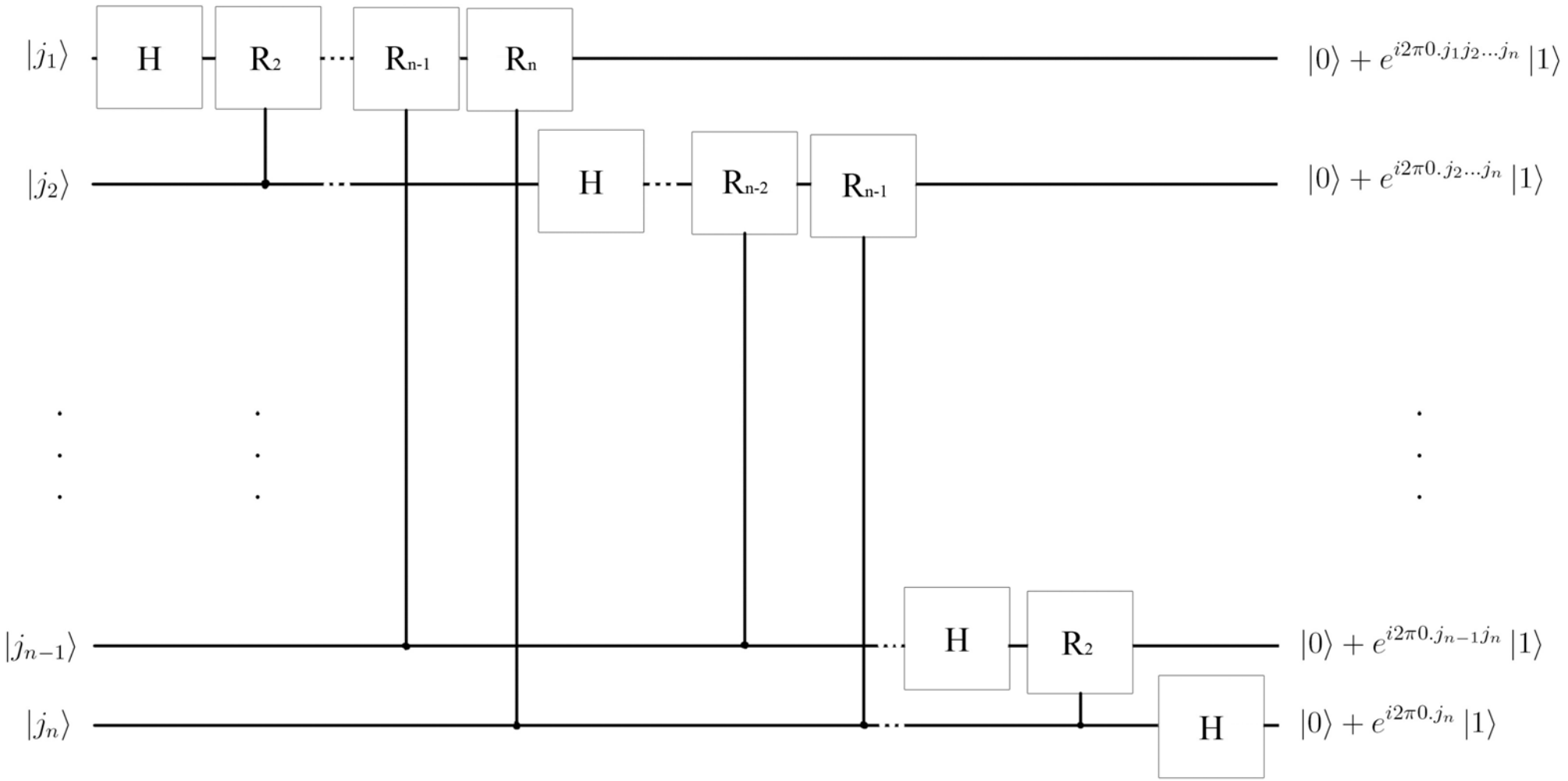
$$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{i2\pi(\frac{j_1}{2}+\frac{j_2}{4})}|1\rangle\right)$$

$$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{i2\pi(\frac{j_2}{2})}|1\rangle\right)$$

$$R_2 = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/4} \end{pmatrix}$$

- Die Reihenfolge der Qubits muss noch umgedreht werden:

$$|j_1\rangle \otimes |j_2\rangle \rightarrow \frac{1}{\sqrt{4}}(|0\rangle + e^{i2\pi(\frac{j_2}{2})}|1\rangle) \otimes (|0\rangle + e^{i2\pi(\frac{j_1}{2}+\frac{j_2}{4})}|1\rangle)$$



$$|j\rangle = |j_1\rangle \otimes |j_2\rangle \otimes \cdots \otimes |j_n\rangle$$

Input

$$\frac{1}{\sqrt{2^n}}[|0\rangle + e^{i2\pi 0.j_n} |1\rangle] \otimes [|0\rangle + e^{i2\pi 0.j_{n-1} j_n} |1\rangle] \otimes \cdots \otimes [|0\rangle + e^{i2\pi 0.j_1 j_2 \ldots j_n} |1\rangle]$$

Output

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

Phase Estimation

Faktorisierung ⇨ Ordnung finden ⇨ Phase bestimmen

$$\hat{U}\,|u_s\rangle = e^{2\pi i\phi}\,|u_s\rangle$$

Die Phase lässt sich nicht unmittelbar messen, sie spielt aber die entscheidende Rolle bei Interferenzerscheinungen.

Wir wollen folgenden Zustand erzeugen:

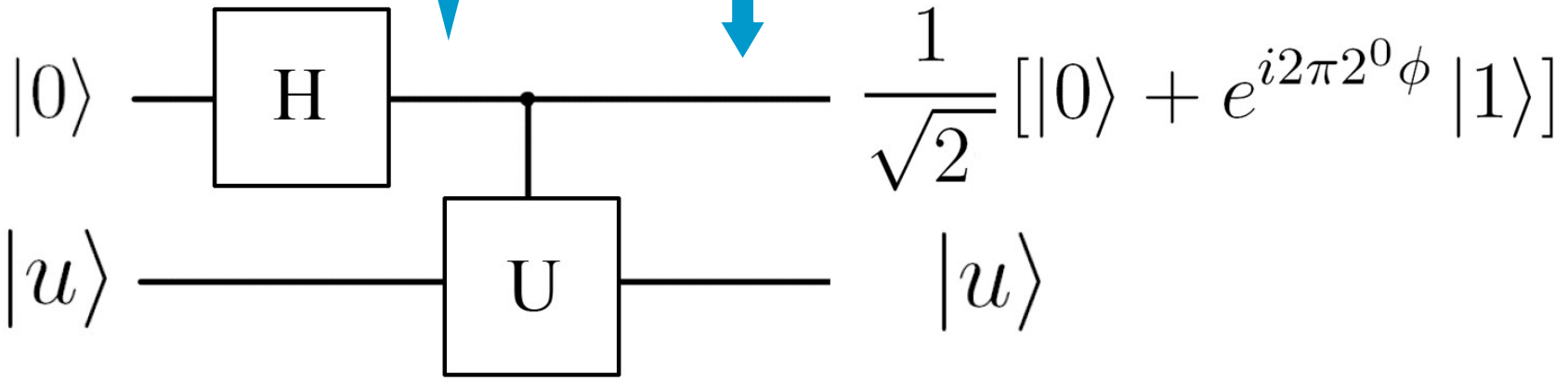
$$\frac{1}{\sqrt{2^t}}[|0\rangle + e^{i2\pi 2^{t-1}\phi}\,|1\rangle] \otimes [|0\rangle + e^{i2\pi 2^{t-2}\phi}\,|1\rangle] \otimes \cdots \otimes [|0\rangle + e^{i2\pi 2^{0}\phi}\,|1\rangle]$$

Phase Estimation

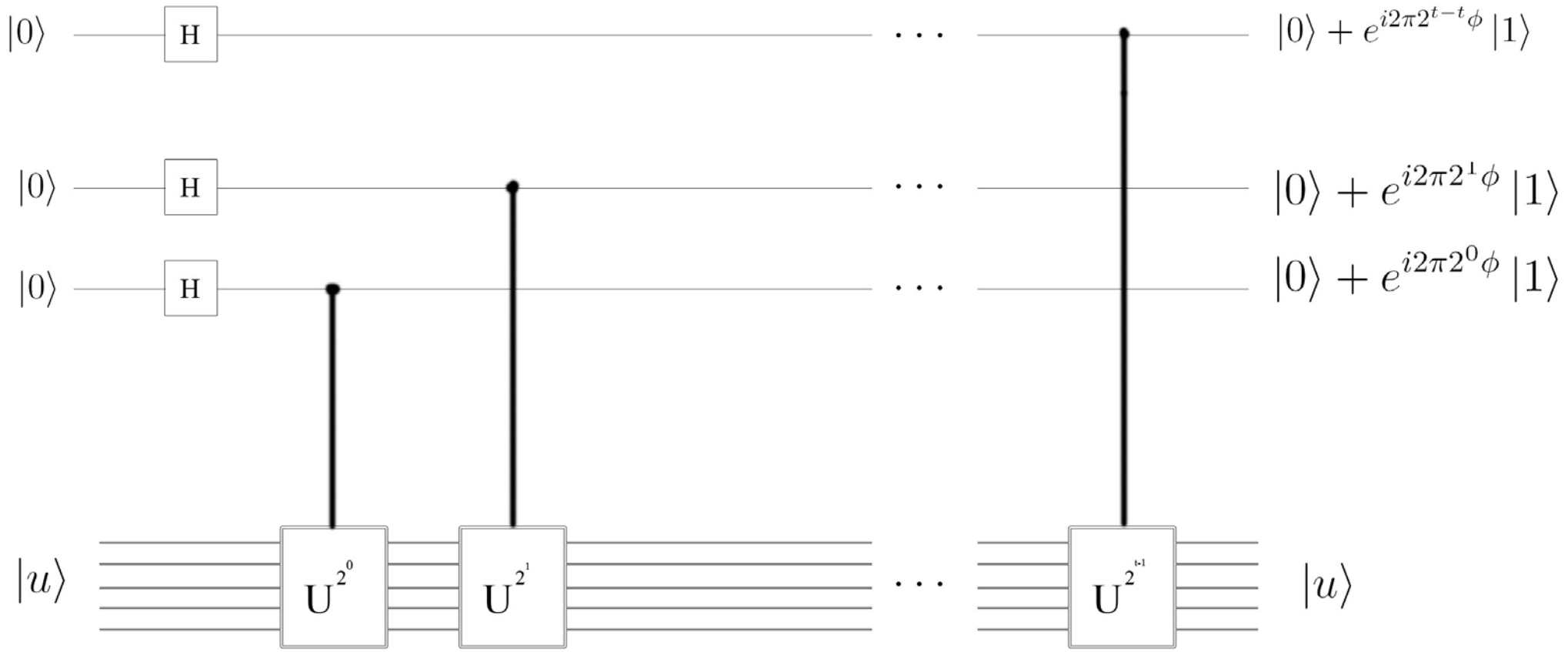
- Erzeugung von: $[|0\rangle + e^{i2\pi 2^0\phi}|1\rangle]$

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |u\rangle = \frac{1}{\sqrt{2}}|0\rangle \otimes |u\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |u\rangle$$

$$\frac{1}{\sqrt{2}}|0\rangle \otimes |u\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes e^{i2\pi(\frac{\phi}{2})}|u\rangle$$



Phase Estimation



$$\frac{1}{\sqrt{2^t}}[|0\rangle + e^{i2\pi 2^{t-1}\phi}|1\rangle] \otimes [|0\rangle + e^{i2\pi 2^{t-2}\phi}|1\rangle] \otimes \cdots \otimes [|0\rangle + e^{i2\pi 2^0\phi}|1\rangle]$$

Phase Estimation

- Lässt sich die Phase in Dualdarstellung genau hinschreiben: $\phi = 0.\phi_1\phi_2...\phi_t$

- So ist der resultierende Zustand:

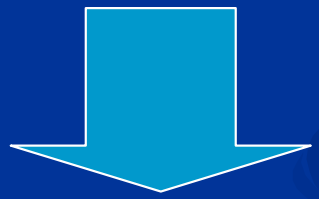
$$\frac{1}{\sqrt{2^t}}[|0\rangle + e^{i2\pi 2^{t-1}\phi}|1\rangle] \otimes [|0\rangle + e^{i2\pi 2^{t-2}\phi}|1\rangle] \otimes \cdots \otimes [|0\rangle + e^{i2\pi 2^{0}\phi}|1\rangle]$$

$$\frac{1}{\sqrt{2^t}}[|0\rangle + e^{i2\pi 0.\phi_t}|1\rangle] \otimes [|0\rangle + e^{i2\pi 0.\phi_{t-1}\phi_t}|1\rangle] \otimes \cdots \otimes [|0\rangle + e^{i2\pi 0.\phi_1\phi_2...\phi_t}|1\rangle]$$

Phase Estimation

- Wende die inverse Fouriertransformation an:

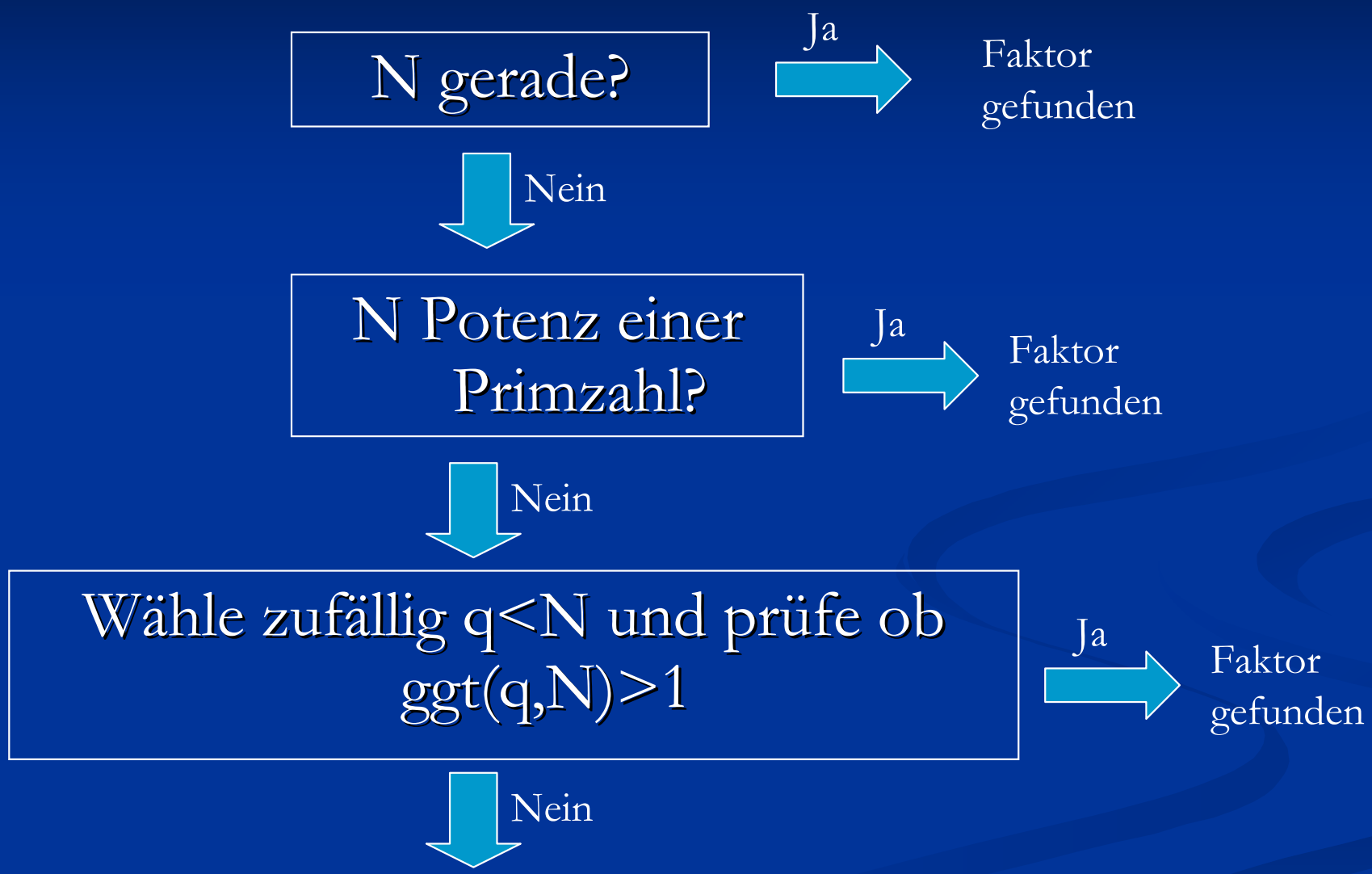
$$\frac{1}{\sqrt{2^t}}[|0\rangle + e^{i2\pi 0.\phi_t}|1\rangle] \otimes [|0\rangle + e^{i2\pi 0.\phi_{t-1}\phi_t}|1\rangle] \otimes \cdots \otimes [|0\rangle + e^{i2\pi 0.\phi_1\phi_2\ldots\phi_t}|1\rangle]$$



$$|\phi\rangle$$

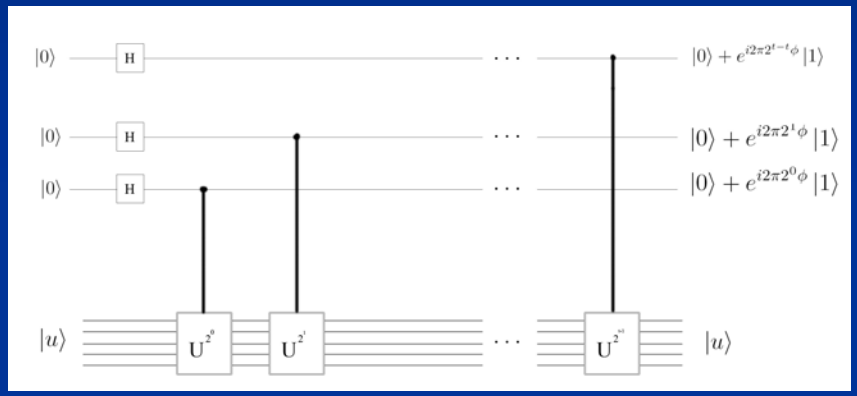
- Messung liefert die Phase

Zusammenfassung

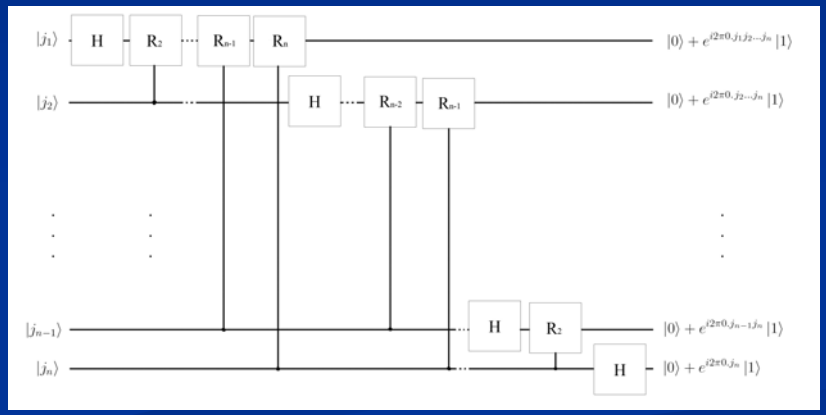


Zusammenfassung

- Finde die Ordnung von q mod N:



Phase Estimation



Inverse Fouriertransformation

Messung liefert die Phase

Ordnung

Passende Ordnung?

N

Wähle neues q

J

fertig