Shors Algorithmus

Stephan Verbücheln

cnlab Herbsttagung 2023: Bits & Qubits
Gleisarena, Zürich, 6. September 2023

cnlab

Agenda

RSA

Faktorisierung und Perioden

Shors Algorithmus

Quantenteil von Shors Algorithmus

RSA

Öffentlicher Schlüssel (e, N), geheimer Schlüssel d

- $N = pq$ mit p, q prim
- Verschlüsselung
  - $Enc_e(m) = m^e = c$
- Entschlüsselung
  - $Dec_d(c) = c^d = m^{ed} = m$

Mit den Primfaktoren p, q lässt sich d berechnen

Peter Shor

- Algorithmus für diskreten Logarithmus und Faktorisierung
- Nutzt das Auffinden von Perioden

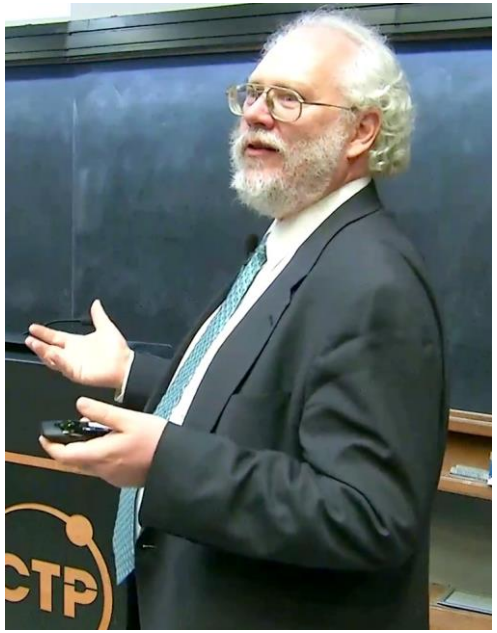


Bild: International Centre for Theoretical Physics (Wikipedia, CC BY 3.0)

Faktorisierung

Wähle eine Zahl g und versuche N zu teilen.

Faktorisierung

Wähle eine Zahl g und berechne $ggT(g, N)$ (Euklidischer Algorithmus).

Falls $ggT(g, N) = 1$, so gilt für ein p:

$$g^p = \mathrm{mN} + 1$$
$$g^p - 1 = \mathrm{mN}$$
$$(g^{\frac{p}{2}}+1)(g^{\frac{p}{2}}-1) = \mathrm{mN}$$

Mit Wahrscheinlichkeit 3/8 erhält man einen Teiler von N.

Faktorisierung und Perioden

Durch Umstellung erkennt man eine periodische Eigenschaft:

$$g^x \bmod \mathrm{N} = \mathrm{r}$$
$$g^{x+p} \bmod \mathrm{N} = \mathrm{r}$$
$$g^{x+2p} \bmod \mathrm{N} = \mathrm{r}$$

Diese Eigenschaft können wir mit Quantenrechnern ausnutzen.

Shors Algorithmus

1. Wähle g und berechne $ggT(g, N)$.
2. Falls kein Teiler gefunden wurde, berechne mit Quantenrechner p mit:

$$g^p = mN + 1$$

3. Falls Probleme auftreten, wiederhole Schritt 1.
4. Berechne $ggT(g^{\frac{p}{2}} \pm 1, N)$

Shors Algorithmus: Beispiel $N = 15$

1. Wähle $g = 7$ und berechne $ggT(7,15)$.
2. Da kein Teiler gefunden wurde, berechne mit Quantenrechner p mit:

$$7^p = \mathrm{m} \cdot 15+1$$

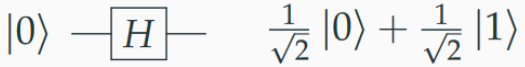
3. Die gefundene Periode $p = 4$ ist gerade.
4. Berechne:

$$ggT(7^{\frac{4}{2}} + 1, 15) = ggT(50, 15) = 5$$

$$ggT(7^{\frac{4}{2}} - 1, 15) = ggT(48, 15) = 3$$

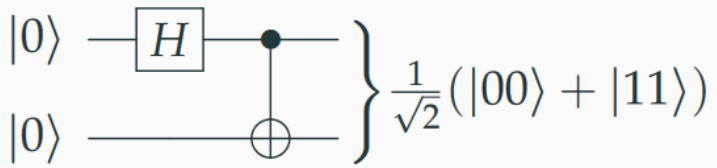
Quantenrechner

Hadamard



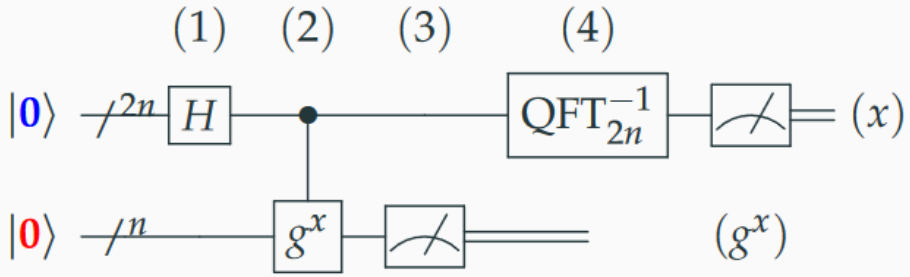
CNOT (Controlled Not)

Einfacher Schaltkreis



Quantenteil

$g = 7$
$N = 15$



(1) Superposition von x:

$$|1,0\rangle + |2,0\rangle + |3,0\rangle + |4,0\rangle + |5,0\rangle + |6,0\rangle + |7,0\rangle + \ldots$$

(2) $7^x \mod N$ berechnen:

$$|1,7\rangle + |2,49\rangle + |3,343\rangle\,|4,2401\rangle + |5,16807\rangle + |6,117649\rangle + |7,823543\rangle + \ldots$$
$$|1,7\rangle + |2,4\rangle + |3,14\rangle + |4,1\rangle + |5,7\rangle + |6,4\rangle + |7,14\rangle + \ldots$$

(3) 7^x auslesen:

$$|1,7\rangle + |5,7\rangle + |9,7\rangle + |13,7\rangle + |17,7\rangle + |21,7\rangle + |25,7\rangle + \ldots$$

(4) QFT ermittelt $p = 4$

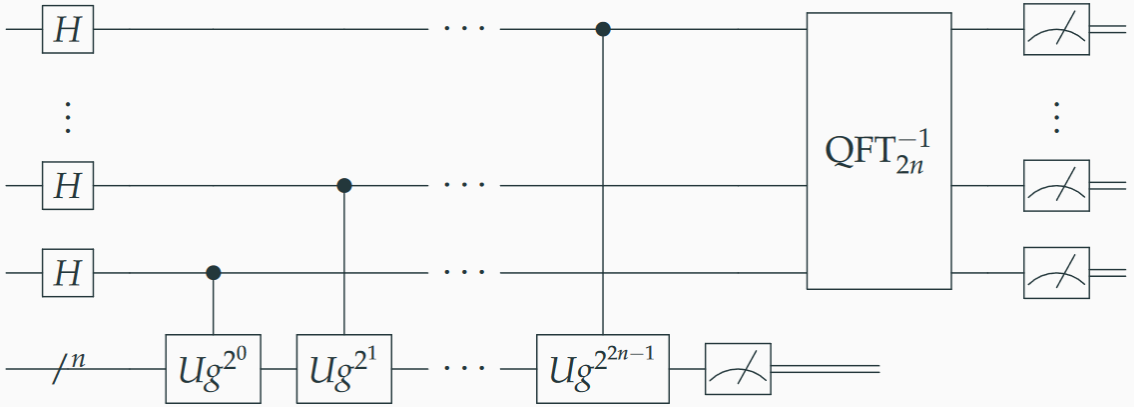
Aufwand (Grössenordnung)

RSA mit 2000 Bits

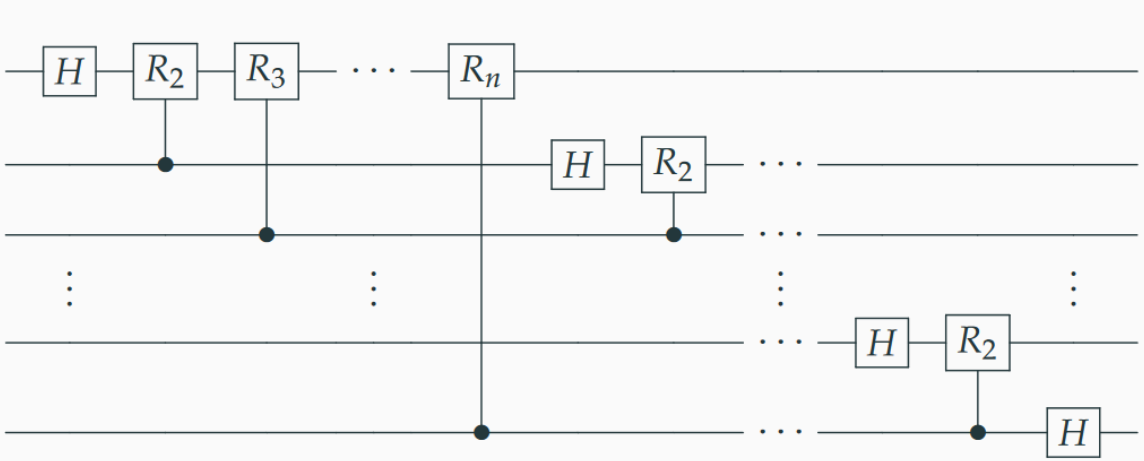
Benötigte Qubits: 6000

Sequenzielle Operationen:
8'000'000'000 (n^3)

Shors Algorithmus



Quantenfouriertransformation



Vielen Dank für Ihre Aufmerksamkeit_

Stephan Verbücheln

info@cnlab-security.ch
+41 55 214 33 40

cnlab security AG
Obere Bahnhofstrasse 32b
CH-8640 Rapperswil-Jona
Switzerland

cnlab