Eigenes „Gesamtbild" CRYPTO1 – Quantencomp. (II) / Shor (bisher: Bauteile)

(VL vom 29.6.22) 23.9.22 & 24. & 26.

de.wiki: Faktorisiere N:

sog. „Orakel"

(1) Wähle eine Zahl $1<a<N$ mit $ggT(a, N)=1$ (ansonsten schon fertig).
(2) Bestimme mithilfe des Quantenteils das kleinste $r \in \mathbb{N}$ mit $a^r \equiv 1 \pmod N$.
(3) Falls r ungerade oder $a^{r/2} \equiv -1 \pmod N$ (anstatt $\equiv 1$): wiederhole (1).
(4) Gebe $ggT(a^{r/2}-1, N)$ als Lösung zurück.
(oder $ggT(a^{r/2}+1, N)$)

r muss(!) nichttriviale Teiler von N enthalten, da:

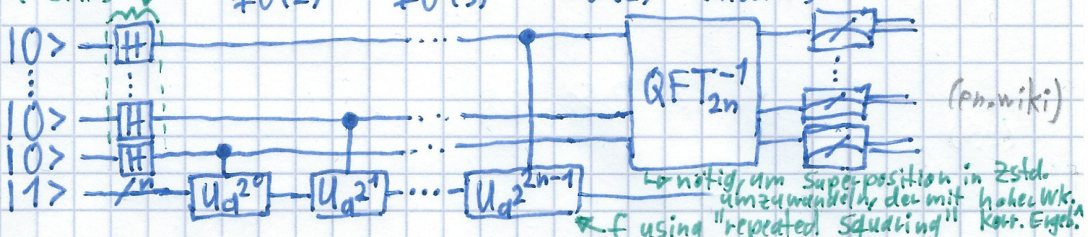
$(a^{r/2}-1) \cdot (a^{r/2}+1) = a^r - 1$

$\not\equiv 0\ (2)$ $\not\equiv 0\ (3)$ $\equiv 0\ (2)$ $(\mathrm{mod}\ N)$

"create a superposition of states"

Quantenteil:

("custom designed for each choice of N and each choice of the random a")

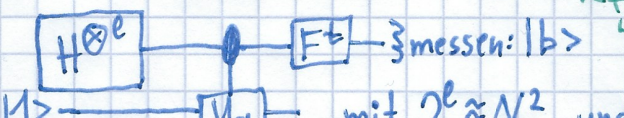


↳ nötig, um Superposition in Zstd. umzuwandeln, der mit hoher Wk. korr. Eigenw.

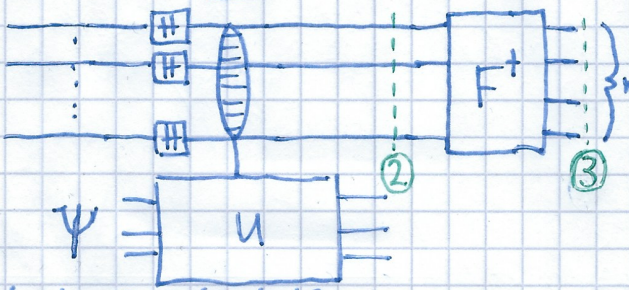
↳ f using "repeated squaring"

↳ $f(x) = |a^x \bmod N\rangle$

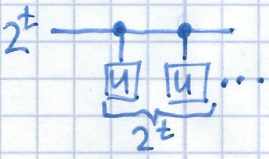
↳ berechne für alle x gleichzeitig!



mit $2^\ell \approx N^2$ und $\frac{b}{2^\ell}$ Kettenbruch: $\frac{s_1}{r_1}, \ldots, \frac{s_m}{r_m}$ (VL)



Wenn $|x\rangle$ angelegt: U^x ausgeführt (VL)



Wie funktioniert der Quantenteil?:

/