Kryptoanalyse (1)

Problem: Primfaktorzerlegung großer Zahlen

$$53 \cdot 127 = 6731$$

Standardverfahren: Ausprobieren.
Aber: Laufzeit wächst exponentiell zur Zahlenlänge!

Beispiel

Zahl mit 100 Dezimalstellen ($\approx$ 333 Binärstellen [bit])
Damit sind Zahlen $\{0, \ldots, 10^{100} - 1\}$ darstellbar.

Gegeben Computer, der 10^{10} Operationen/s ausführt.

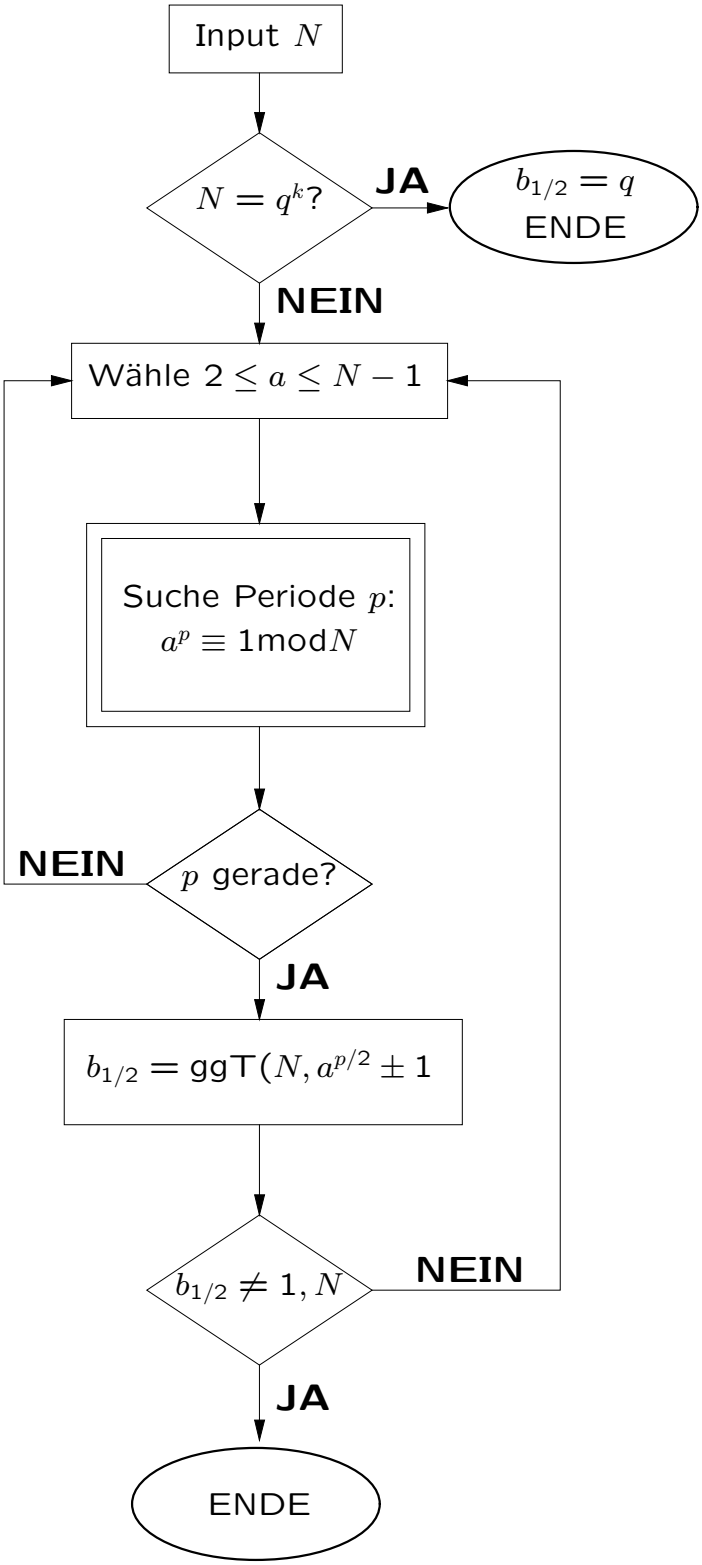
$$\frac{10^{\log(\sqrt{10^{100}})}\text{op}}{10^{10}\text{op/s}} = \frac{10^{100/2}\text{op}}{10^{10}\text{op/s}} = 10^{40}\text{s}$$

Zum vergleich:

$$\begin{aligned} 1 \text{ Jahr} \quad &\approx 3,2 \cdot 10^7 \text{s} \\ \text{Universum} &\approx 3,8 \cdot 10^{17} \text{s} \end{aligned}$$

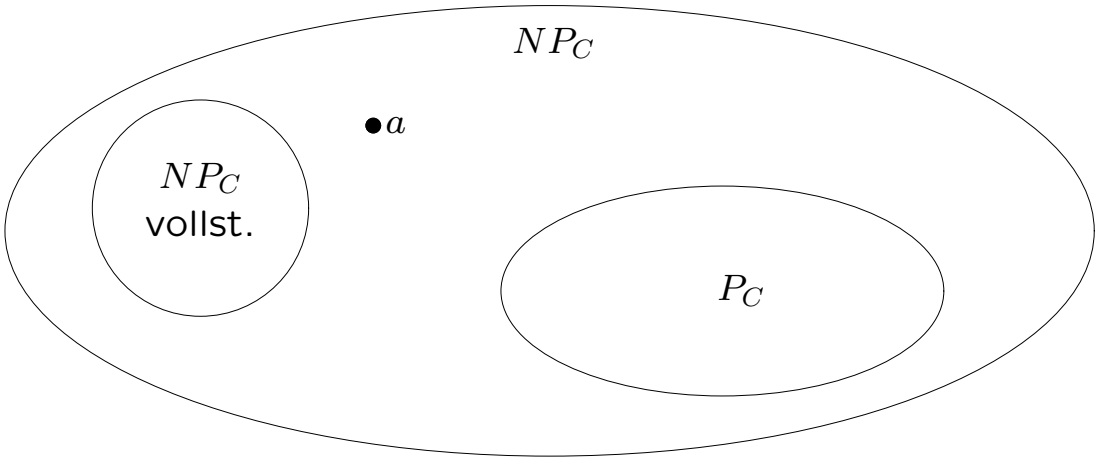
Typische Schlüsselängen heute: 1024 bit

Shor's Algorithmus

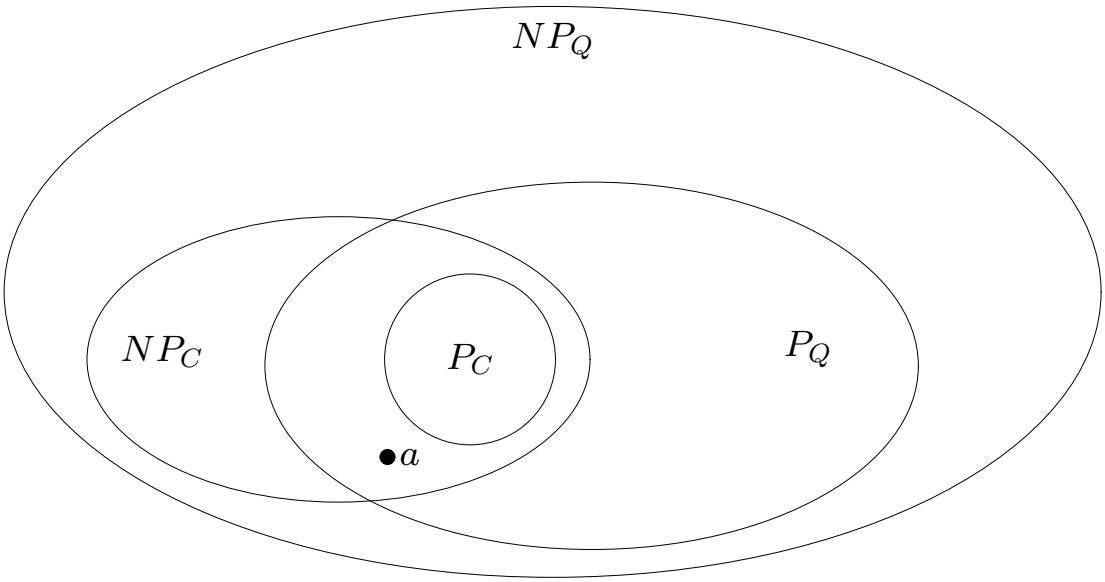


Berechenbarkeitsklassen

Brauchen wie evtl. neue Berechenbarkeitsklassen?
Hier ist a das Faktorisierungsproblem



Nach Shor ist aber $a \in P_Q$, also wohl eher



No-cloning-Theorem

Angenommen es gäbe einen Quantenkopierer. Dieser habe vor dem Kopieren den Zustand $|k_0\rangle$. Gegeben Quantenzustände $|1\rangle$ und $|2\rangle$.

$$|1\rangle\,|x\rangle\,|k_0\rangle \longrightarrow |1\rangle\,|1\rangle\,|k_1\rangle$$

und

$$|2\rangle\,|x\rangle\,|k_0\rangle \longrightarrow |2\rangle\,|2\rangle\,|k_2\rangle$$

Dann folgt für einen verschränkten Zustand

$$(\alpha\,|1\rangle + \beta\,|2\rangle)\,|x\rangle\,|k_0\rangle \longrightarrow \alpha\,|1\rangle\,|x\rangle\,|k_0\rangle + \beta\,|2\rangle\,|x\rangle\,|k_0\rangle$$

$$\longrightarrow \alpha\,|1\rangle\,|1\rangle\,|k_1\rangle + \beta\,|2\rangle\,|2\rangle\,|k_2\rangle$$

Eine „echte“ Kopie wäre aber

$$(\alpha\,|1\rangle + \beta\,|2\rangle)\,(\alpha\,|1\rangle + \beta\,|2\rangle)\,\left|k'\right\rangle$$

Das ist aber nur für $\alpha = 0$ oder $\beta = 0$ wahr.

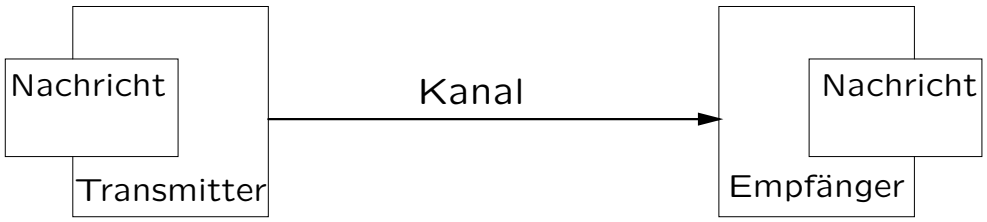
Also ist Q.-Inf. „mächtiger“ als klassische Inf.

$$\boxed{\text{Q.-Inf.}} \xrightarrow{!} \boxed{\text{klassische Inf.}} \longrightarrow \boxed{\text{Q.-Inf.}}$$

Shannon-Information

Brauchen wir neuen Informationsbegriff?

$$H = \sum_{a=0}^{n} p_a \cdot \log_2(1 - p_a)$$



Dafür spricht:

- Q.-Inf. kann nicht kopiert werden
- Q.-Register speichern exponentiell viele Werte
- Q.-Kommunikation übersteigt scheinbar das C/H Limit
  C Kapazität des Kanals [bits/s], H Entropie [bits/Nachricht]

Dagegen spricht:
Information steckt nicht in den Bits! Information ist die Beziehung der Bits zur vereinbarten Nachrichten. Bits dienen dem Empfänger zur eindeutigen Auswahl der Nachricht.

Teleportation

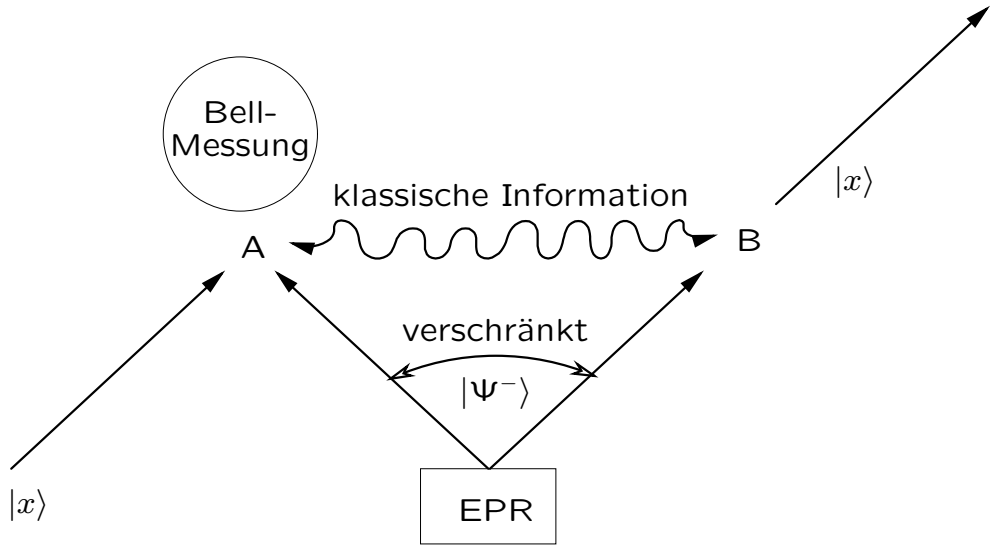
Wir brauchen sog. *Bell-Zustände*

$$\left|\Psi^+\right\rangle = (|01\rangle + |10\rangle)/\sqrt{2} \quad \left|\Phi^+\right\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$$
$$|\Psi^-\rangle = (|01\rangle - |10\rangle)/\sqrt{2} \quad |\Phi^-\rangle = (|00\rangle - |11\rangle)/\sqrt{2}$$

Zustände lassen sich ineinander überführen indem nur **ein** Qubit verändert wird.

Bitflip: $0 \rightarrow 1$, $1 \rightarrow 0$
Phasenwechsel: $0 \rightarrow 0$, $1 \rightarrow -1$

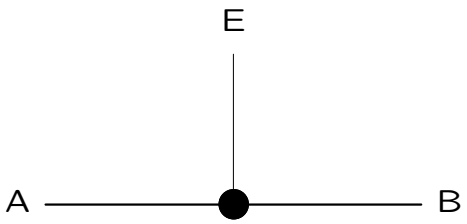
Beispiel



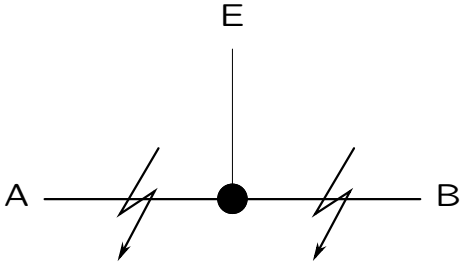
Ergibt die Bell-Messung z.B. $\left|\Phi^-\right\rangle$, muß Bob ein Bitflip ausführen.

Quantenkryptographie (1)

klassisch



Quantenkanal



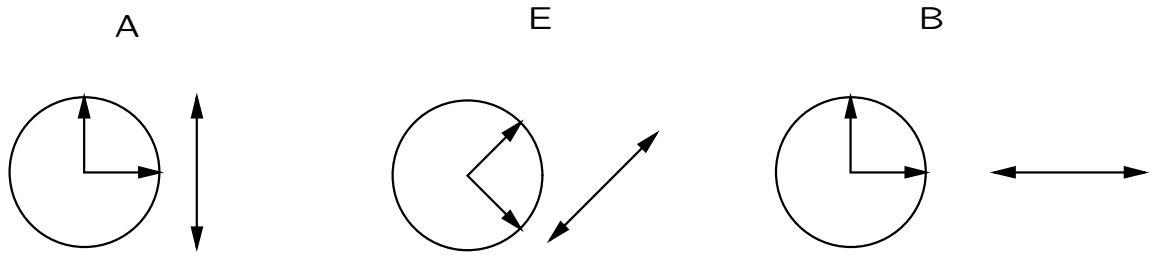
Schlüsseltausch

1. Alice wählt zufällig eine der Basen $\{|\uparrow\rangle, |\rightarrow\rangle\}$ oder $\{|\nearrow\rangle, |\searrow\rangle\}$ je Qubit und sendet es Bob.

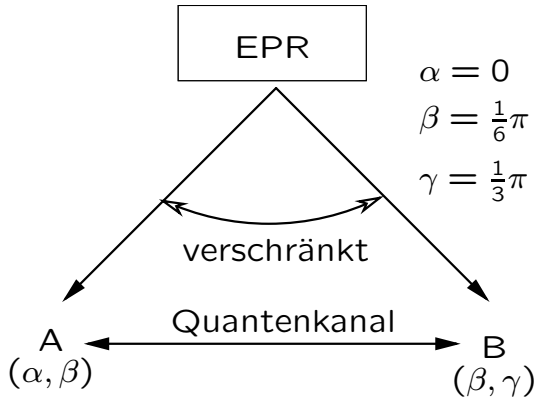
2. Bob schaltet ebenfalls zufällig zwischen der $\{|\uparrow\rangle, |\rightarrow\rangle\}$ und $\{|\nearrow\rangle, |\searrow\rangle\}$ Basis und teilt die Einstellung Alice mit. (nicht das Ergebnis!)

3. Alice teilt Bob mit, wann sie gleiche Basis verwendeten.

Abhörsicherheit



Quantenkryptographie (2)



1. Alice wählt zufällig eine Einstellung (α oder β) und sendet ein Qubit an Bob
2. Bob wählt zufällig eine Einstellung (β oder γ) und teilt sie Alice mit.
3. Alice teilt Bob mit, wann sie gleiche Einstellung (β) verwendeten.
4. Die Qubits, die bei ungleicher Basiseinstellung übertragen wurden, werden zur Bell-Analyse benutzt

$$\boxed{N(1_\alpha, 1_\beta) \leq N(1_\alpha, 1_\gamma) + N(1_\beta, 0_\gamma)}$$

Kryptoanalyse (2)

Innovation: Shor's Algorithmus

Äquivalentes Problem: finde Periode von $f(x) := a^x \mathrm{mod} N$, wenn N das Produkt ist.

Vorgeplänkel

$$(a^m - 1)(a^m + 1) = a^{2m} - a^m + a^m - 1 = a^{2m} - 1$$

- Suche ein m, so dass sich eine durch N teilbare Zahl ergibt.

$\Rightarrow$ $[(a^m - 1)\mathrm{mod}N][(a^m + 1)\mathrm{mod}N]$ ist durch N teilbar

$\Rightarrow$ eine der Zahlen hat einen Faktor mit N gemeinsam

Berechne sukzessive $a^0 = 1$ bis $a^p \equiv 1 \mathrm{mod} N$. p ist die Periode der Funktion.
Ist p gerade, berechne $b_1 = \mathrm{ggT}(N, a^{p/2} - 1)$ und $b_2 = \mathrm{ggT}(N, a^{p/2} + 1)$.
Ist $b_1 \neq 1$ und $b_2 \neq 1$, so sind b_1 und b_2 Teiler von N.

Kryptoanalyse (3)
Beispiel

$N = 21$. Wähle $a = 2$.

$2^0 \equiv 1; 2^1 \equiv 2; 2^2 \equiv 4; 2^3 \equiv 8; 2^4 \equiv 16; 2^5 \equiv 11; 2^6 \equiv 1$

Also ist $p = 6$

$$b_1 = \text{ggT}(21, 2^3 - 1) = (21, 7) = (14, 7) = (7, 7)$$
$$b_2 = \text{ggT}(21, 2^3 + 1) = (21, 9) = (12, 9) = (3, 3)$$

Wir hätten auch Pech haben können

$N = 21$. Wähle $a = 4$.

$$4^0 \equiv 1; 4^1 \equiv 4; 4^2 \equiv 16; 4^3 \equiv 1$$

Also ist $p = 3$. **STOP!**

und auch hier geht's nicht

$N = 21$. Wähle $a = 5$.

$5^0 \equiv 1; 5^1 \equiv 5; 5^2 \equiv 4; 5^3 \equiv 20; 5^4 \equiv 16; 5^5 \equiv 17; 5^6 \equiv 1$

Also ist $p = 6$

$$b_1 = \text{ggT}(21, 5^3 - 1) = (21, 124) = (21, 19)$$
$$b_2 = \text{ggT}(21, 5^3 + 1) = (21, 126) = (21, 21)$$

Kryptoanalyse (4)

Shor's Quantenalgorithmus

Sei $L = \log_2(N)$ länge der Produktzahl.

1. Erzeuge Superposition
   $\Phi_1 = \frac{1}{\sqrt{2^N}} \sum_{x=0}^{2^L-1} |x\rangle$ indem jedes Qubit in Zustand $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ versetzt wird (L Schritte).

2. Berechne $f(x) = a^x \mathrm{mod} N$
   $\Phi_2 = \frac{1}{\sqrt{2^N}} \sum_{x=0}^{2^L-1} |x, f(x)\rangle$
   Das geht in pol(L) Schritten.

3. Quantenfouriertransformation (QFT)
   Messe $|f\rangle = |f(k)\rangle$ für ein bestimmtes k. Nach der Messung ist $|x\rangle$ eine Superposition aller $k, k+p, k+2p, \ldots$
   ???

4. Messung der Periode von f

5. Verifikation der Messung