Warum Postquantenkryptografie?

Frank Fuhlbrück

22.6.2022

Der Vortrag folgt weitgehend:

Nielsen, Michael A. und Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010.

Gliederung

- Grundidee von Quantenalgorithmen
- Faktorisierung und das DLP
- Qubits, Quantensysteme und Messen
- Quantenoperationen und -gatter
- Quantenfouriertransformation
- Ordnung eines Gruppenelements bestimmen
- Faktorisieren und diskreter Logarithmus (Shors Algorithmen)
- Zusammenfassung: Was genau bedeutet PQK?

Quantenalgorithmen (stark vereinfacht)

Quanten(sub)algorithmus A mit Eingabe $x \in \{0,1\}^n$

- Initialzustand $|s\rangle = |s(x)\rangle$ mit n Qubits herstellen
- diverse Quantenoperationen auf $|s\rangle$ anwenden
- Messungen durchführen $\rightarrow$ Zufallsvariable $A(x) = Y \in \{0,1\}^n$ mit bestimmter Verteilung

klassischer Algorithmus B mit A als Blackbox

- ggf. Vorberechnungen
- $Y = A(x)$
- Mit nicht vernachlässigbarer Wkt. tritt das Ereignis $Y \in G$ für eine günstiges Menge G ein (z.B. Y codiert nichttrivialen Teiler).
- Wiederhole A bis $A(x) \in G$ (bzw. polynomiell oft in der Länge $|x|$ von x).

Probleme

Faktorisierung

- geg.: n (für RSA $n = p, q$ unbekannt und prim)
- ges.: k mit $k|n$ und $k \notin \{1, n\}$, falls existent
- Anwendung auf RSA: $d \equiv_{\varphi(n)} e^{-1}$ mit $\varphi(n) = (p-1)(q-1)$, (n, e) ist öffentlicher Schlüssel, (n, d) privat.

Diskretes Logarithmusproblem

- geg.: $\alpha, \beta (= \alpha^a)$ aus endlicher Gruppe G
- ges.: a
- Anwendung auf ElGamal: $G = \mathbb{Z}_p^*$, a ist privater Schlüssel, α, β, p sind öffentlich.

Qubits

Quantenzustände

- Wir schreiben Quantenzustände ψ in Dirac-Notation (Bra-Ket-Notaion): $|\psi\rangle$.
- ψ können wir uns als Element des $\mathbb{C}^{2^n}$ (für n Qubits, s.u.) vorstellen.
- Bra $\langle\psi|$ bzw. Ket $|\psi\rangle$ entspricht grob Zeilen- und Spaltenvektor, v.a. ist $\langle\varphi||\psi\rangle$ das innere Produkt von φ und ψ.

Definition (Qubits)

Ein Qubit $|\psi\rangle$ ist eine Linearkombination $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ aus zwei orthogonalen Zuständen 0 und 1 (also $\langle 1||0\rangle = \langle 0|1\rangle = 0$).

- Dabei sind $\alpha, \beta \in \mathbb{C}$ und
- die Wkt. 0 zu messen ist $|\alpha|^2$, für 1 $|\beta|^2$ und daher $|\alpha|^2 + |\beta|^2 = 1$.
- Nach dem Messen ist entweder $|\psi'\rangle = |0\rangle$ oder $|\psi'\rangle = |1\rangle$.

System aus mehreren Qubits

n Qubits

Betrachten wir ein Systems aus n Qubits, so haben wir eine Linearkombination $|\psi\rangle = \sum_{v \in \{0,1\}^n} \alpha_v |v\rangle$

- z.B. $|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$
- Man kann in einem n-Qubitsystem auch weniger als n Qubits messen.
- Misst man das erste Bit als 0, so ist das System danach im Zustand $(\alpha_{00}|00\rangle + \alpha_{01}|01\rangle)/(|\alpha_{00}|^2 + |\alpha_{01}|^2)$.
- Die Wahrscheinlichkeit danach z.B. das zweite Bit zu 1 zu messen, entspricht dadurch genau der bed. Wkt.
- Beispiel Bell-Zustand: $\alpha_{00} = \alpha_{11} = \frac{1}{\sqrt{2}} \Rightarrow$ max. Verschränkung, zweite Messung deterministisch.
- allgemein: *verschränkt*, wenn beide Messungen nicht unabhängig

Operationen auf Quantensystemen

$|\psi\rangle \to |\psi'\rangle : |\psi'\rangle = U|\psi\rangle$

- Jede Zustandsänderung in einem Quantensystem lässt sich durch eine unitäre Transformation beschreiben.
- Im Falle von n Qubits heißt das, dass U eine unitäre Matrix aus $\mathbb{C}^{2^n \times 2^n}$ ist.
- D.h. $U^H U = I$, wobei für die Einträge $u'_{i,j}$ aus U^H gilt: $u'_{i,j} = \overline{u_{j,i}}$ (d.h. U^H ist transponiert und komplex konjugiert).
- gleichbedeutend: Spaltenvektoren sind orthonormal
- Insbesondere muss U also invertierbar sein.

Quantengatter

ein Qubit

- $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$; $X \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix}$
- $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$; $H \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} \alpha + \beta \\ \alpha - \beta \end{pmatrix}$
- $S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{2}} \end{pmatrix}$; $S \begin{pmatrix} \alpha \\ re^{i\varphi} \end{pmatrix} = \begin{pmatrix} \alpha \\ re^{i(\varphi + \frac{\pi}{2})} \end{pmatrix}$
- $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}$; $S \begin{pmatrix} \alpha \\ re^{i\varphi} \end{pmatrix} = \begin{pmatrix} \alpha \\ re^{i(\varphi + \frac{\pi}{4})} \end{pmatrix}$

globale Phasen werden ignoriert

Sei $A = I_{2^n} \cdot e^{i\varphi}$, $|\psi\rangle = \sum_{v \in \{0,1\}^n} \alpha_v |v\rangle$. Da für $\alpha_v = re^{i\theta}$ gilt $|\alpha_v|^2 = r^2$, sind $A|\psi\rangle$ und $|\psi\rangle$ nicht durch Messungen unterscheidbar.

Quantengatter II

Ein-Qubit-Operation als Operation auf n Qubits

- Wir nehmen an, wir modifizieren nur das letzte Qubit mit Operation $U \in \mathbb{C}^{2\times 2}$. Dann entsprechen die Zeilen der Basis $\ldots, v0, v1, v'0, v'1, \ldots$ $(v, v' \in \{0,1\}^{n-1})$.
- U auf Gesamtsystem ist also:

$$\begin{pmatrix} A & 0 & 0 & \ldots \\ 0 & A & 0 & \ldots \\ 0 & 0 & A & \ldots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

Quantengatter III

Operationen auf 2 Qubits

- CONTROLLED-U, $U = \begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix}$: $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 00 \\ 0 & 0 & u_{11} & u_{12} \\ 0 & 0 & u_{21} & u_{22} \end{pmatrix}$
- speziell: CNOT = CONTROLLED-X
- Auch das Kontrollqubit (d.h. das erste) kann sich auch ändern, wenn das System keinen der 4 Basiszustände zu Beginn hat. Wendet man z.B. H auf beide Qubits vor und nach CNOT an, so entspricht dies CNOT mit vertauschen Qubits.
- CNOT kann als XOR $= \oplus$ und Identität betrachtet werden: $\text{CNOT}|ab\rangle = |a(a \oplus b)\rangle$.
- AND auf 2 Qubits ist nicht möglich: Falls $a \wedge b = 0$, so gibt es drei Fälle $a = b = 0$; $a = 1 - b = 1$; $1 - a = b = 1$, aber neben $a \wedge b$ nur 1 Ausgabequbit.

Quantengatter IV

Ancilla-Qubits

- Idee: Wir bauen ein kontrolliertes AND und präparieren das Kontrollbit immer zu $|0\rangle$: $\text{AND}|ab0\rangle = |ab(a \wedge b)\rangle$.
- Das Verhalten bei $|1\rangle$ wird so gewählt, dass wir eine Bijektion auf $\{0,1\}^3$ bekommen: $\text{AND}|ab1\rangle = |ab\neg(a \wedge b)\rangle$
- als Matrix: $\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$
- AND ist also ein „doppelt kontrolliertes“ NOT: beide Eingabebits müssen gesetzt sein, um das Ancillabit zu flippen.
- OR etc. funktionieren analog.

Quantenfouriertransformation

Diskrete Fourier-Transformation (DFT)

- Sei $(x_0, \ldots, x_{N-1}) \in \mathbb{C}^N$. Nach DFT wird daraus $(y_0, \ldots, y_{N-1}) \in \mathbb{C}^N$ mit $y_k = \sum_{j=0}^{N-1} x_j e^{2\pi i \frac{jk}{N}}$
- Wenn wir dies mit $N^{-\frac{1}{2}}$ multiplizieren, $N = 2^n$ setzen und j und k als Binärvektoren verstehen, ergibt dies die unitäre Matrix F mit $F_{jk} = 2^{-\frac{n}{2}} e^{2\pi i \frac{jk}{2^n}}$.

Quantenfouriertransformation

Diskrete Fourier-Transformation (DFT)

- Sei $(x_0, \ldots, x_{N-1}) \in \mathbb{C}^N$. Nach DFT wird daraus $(y_0, \ldots, y_{N-1}) \in \mathbb{C}^N$ mit $y_k = \sum_{j=0}^{N-1} x_j e^{2\pi i \frac{jk}{N}}$
- Wenn wir dies mit $N^{-\frac{1}{2}}$ multiplizieren, $N = 2^n$ setzen und j und k als Binärvektoren verstehen, ergibt dies die unitäre Matrix F mit $F_{jk} = 2^{-\frac{n}{2}} e^{2\pi i \frac{jk}{2^n}}$.
- F lässt sich mit einer Abfolge von H und Gattern CONTOLLED-R_l als Quantenschaltkreis realisieren, wobei $R_l = \begin{pmatrix} 1 & 0 \\ 0 & e^{\pi i 2^{1-l}} \end{pmatrix}$.
- Idee ist hier, dass $e^{j2^{-n}} = \prod_l e^{2^l 2^{-n}}$, wobei das Produkt genau über die l geht, sodass das l. Bit in j 1 ist.
- S, T sind Spezialfälle der R_l.

Phasenschätzung (vereinfacht)

geg.: unitäres U; Eigenvektor $|u\rangle$ von U sowie alle U^{2^j}

- ges.: Phase $\varphi \in [0, 1]$ des Eigenwerts $e^{2\pi i\varphi}$ von U (Radius ist immer 1).
- Eingabe t $|0\rangle$-Qubits (Index $0, \ldots, t-1$); $|u\rangle$
- Jedes der t Qubits wird durch H überlagert.
- Für $j \leftarrow 0, \ldots, t-1$, wende CONTROLLED-$U^{2^{t-j}}$ auf Qubit j und $|u\rangle$ an.
- Der Phasenshift φ durch $U^{2^{t-j}}$ wirkt sich auf Qubit j aus: $\frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i 2^{t-j}\varphi}|1\rangle$.
- Beobachtung: Hätten wir F auf einen Zustand $|b_1 \ldots b_t\rangle$ der ersten t Nachkommabits von φ angewendet, ergäbe dies dieselben j Qubits.
- F^{-1} wird realisiert durch umgekehrten Quantenschaltkreis und gibt uns $|b_1 \ldots b_t\rangle$.
- Nach Messen: t-Bit Näherung von φ (nicht mit Wkt. 1, falls $\forall k \in \mathbb{Z} : \varphi \neq \frac{k}{2^t}$).
- mit $\mathcal{O}(-\log \varepsilon)$ Extraqubits sind die ersten t gemessenen Bits auch für bel. φ mit Wkt. $1 - \varepsilon$ korrekt.

Ordnung finden

geg.: Gruppe $G \subseteq \{0,1\}^n$, Quantenschaltkreis $U_x|y\rangle = |xy\rangle$ für alle $x, y \in G$

- ges.: minimales r mit $x^r = 1$.
- Gibt es einen Eigenvektor $|u\rangle$, sodass r sich aus dem passenden Eigenwert ermitteln lässt?

Ordnung finden

geg.: Gruppe $G \subseteq \{0,1\}^n$, Quantenschaltkreis $U_x|y\rangle = |xy\rangle$ für alle $x, y \in G$

- ges.: minimales r mit $x^r = 1$.
- Gibt es einen Eigenvektor $|u\rangle$, sodass r sich aus dem passenden Eigenwert ermitteln lässt?
- Zunächst Eigenvektor: $|u\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |x^k\rangle$; $U_x|u\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |x^{k+1}\rangle = |u\rangle$
- Zwei Probleme: Eigenwert ist 1; $|u\rangle$ nicht ohne Kenntnis von r präparierbar.

Ordnung finden

geg.: Gruppe $G \subseteq \{0,1\}^n$, Quantenschaltkreis $U_x|y\rangle = |xy\rangle$ für alle $x, y \in G$

- ges.: minimales r mit $x^r = 1$.
- Gibt es einen Eigenvektor $|u\rangle$, sodass r sich aus dem passenden Eigenwert ermitteln lässt?
- Zunächst Eigenvektor: $|u\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |x^k\rangle$; $U_x|u\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |x^{k+1}\rangle = |u\rangle$
- Zwei Probleme: Eigenwert ist 1; $|u\rangle$ nicht ohne Kenntnis von r präparierbar.
- 1. Idee: Überlagerung mit Phasenshift: $|u\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi \frac{k}{r}} |x^k\rangle$

  Eigenwert ist dann $e^{2\pi i \frac{1}{r}}$.

Ordnung finden

geg.: Gruppe $G \subseteq \{0,1\}^n$, Quantenschaltkreis $U_x|y\rangle = |xy\rangle$ für alle $x, y \in G$

- ges.: minimales r mit $x^r = 1$.
- Gibt es einen Eigenvektor $|u\rangle$, sodass r sich aus dem passenden Eigenwert ermitteln lässt?
- Zunächst Eigenvektor: $|u\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |x^k\rangle$; $U_x|u\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |x^{k+1}\rangle = |u\rangle$
- Zwei Probleme: Eigenwert ist 1; $|u\rangle$ nicht ohne Kenntnis von r präparierbar.
- 1. Idee: Überlagerung mit Phasenshift: $|u\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi \frac{k}{r}} |x^k\rangle$
  Eigenwert ist dann $e^{2\pi i \frac{1}{r}}$.
- 2.Idee: Wir können die Phasenschätzung auch mit mehreren Überlagerten Eigenvektoren durchführen:
- Sei $|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi s \frac{k}{r}} |x^k\rangle$. Dann ist
  $\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = \frac{1}{r} \sum_{k=0}^{r-1} \sum_{s=0}^{r-1} e^{-2\pi s \frac{k}{r}} |x^k\rangle = \frac{1}{r} \sum_{s=0}^{r-1} e^{-2\pi s \frac{0}{r}} |x^0\rangle = |1\rangle \quad (1 \in G)$

Ordnung finden II

geg.: Gruppe $G \subseteq \{0,1\}^n$, Quantenschaltkreis $U_x|y\rangle = |xy\rangle$ für alle $x, y \in G$

- Neben der Präparierung des (überlagerten) Einheitsevektors $|1\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle$ müssen wir noch $U_x^{2^j}$ realisieren, d.h. beliebige 2^j-Potenzen von x:
  das geht durch iteriertes Quadrieren.
- Algorithmus (Ordnung von x):
  - präpariere t-Qubitzustand $|0\rangle$ $(t > n)$, n Qubitzustand als $|1\rangle$ mit $(1 \in G)$.
  - Phasenschätzung (inkl. Messen) liefert t-Bit-Approximation von s/r für zufälliges $s \in \{0, \ldots, r-1\}$.
  - Finde rationales $s'/r' \approx s/r$ durch Kettenbruchexpansion, sodass $r' \leq 2^n$.
  - Falls $s' \neq 0$ und $x^{r'} = 1$, gib r' zurück.
- Wir haben (sofort) Erfolg, falls $\mathrm{ggT}(s, r) = 1$. Fall $s \neq 0$ können wir aber x durch $x^{r'}$ ersetzten, da $r'|r$.

Faktorisierung

Algorithmus geg.: n; ges.: $k \in \{2, \ldots, n-1\}$ mit $k|n$

- Teste ob $2|n$ oder $n = a^b$ (mit $b \leq \log_2 n$) und brich mit $k = 2$ bzw. $k = a$ ab.
- Wähle $x \in \mathbb{Z}_n^*$ zufällig (also in $x \in \mathbb{Z}_n$ und Abbruch bei $k = \mathrm{ggT}(x, n) > 1$).
- Berechne $r = \mathrm{ord}_{\mathbb{Z}_n^*}(x)$.
- Falls r gerade ist und $x^{r/2} \not\equiv_n -1$, berechne $\mathrm{ggT}(x^{r/2} + 1 \mod n, n)$ und $\mathrm{ggT}(x^{r/2} - 1 \mod n, n)$ und gib sie zurück, sofern ungleich 1. Sonst gib ? zurück.

Faktorisierung

Algorithmus geg.: n; ges.: $k \in \{2, \ldots, n-1\}$ mit $k|n$

- Teste ob $2|n$ oder $n = a^b$ (mit $b \leq \log_2 n$) und brich mit $k = 2$ bzw. $k = a$ ab.
- Wähle $x \in \mathbb{Z}_n^*$ zufällig (also in $x \in \mathbb{Z}_n$ und Abbruch bei $k = \mathrm{ggT}(x, n) > 1$).
- Berechne $r = \mathrm{ord}_{\mathbb{Z}_n^*}(x)$.
- Falls r gerade ist und $x^{r/2} \not\equiv_n -1$, berechne $\mathrm{ggT}(x^{r/2} + 1 \mod n, n)$ und $\mathrm{ggT}(x^{r/2} - 1 \mod n, n)$ und gib sie zurück, sofern ungleich 1. Sonst gib ? zurück.

Satz

Für $n = pq$ und $x \in \mathbb{Z}_n^*$ gleichverteilt, gilt $\Pr[2 \not| r \text{ oder } x^r \equiv_n -1] \leq \frac{1}{2}$.

Faktorisierung II

Satz

Für $n = pq$ und $x \in \mathbb{Z}_n^*$ gleichverteilt, gilt $\Pr[2 \not| r \text{ oder } x^{r/2} \equiv_n -1] \leq \frac{1}{2}$.

Beweis.

- Da $\mathbb{Z}_n^*$ und $\mathbb{Z}_p^* \times \mathbb{Z}_q^*$ isomorph sind, betrachten wir $r_p = \mathrm{ord}_{\mathbb{Z}_p^*}(x)$ (analog r_q). Sei d (analog d_p, d_q) maximal mit $2^d | r$.
- Da $\mathbb{Z}_p^*/\mathbb{Z}_q^*$ zyklisch sind, haben höchstens die Hälfte der Elemente ungerade Ordnung. Wegen $r_p | r$ und $r_q | r$, genügt es den Fall $d_p = d_q = 0$ auszuschließen.
- Wenn $x^{\frac{r}{2}} \equiv_n -1$, so auch $x^{\frac{r}{2}} \equiv_p -1$ und damit $r_p \not| \frac{r}{2}$. Daher gilt dann bereits $d_p = d$ (und analog $d = d_q$).
- Daher: $\Pr[2 \not| r \text{ oder } x^{r/2} \equiv_n -1] \leq \Pr[r_p \equiv_2 r_q] = \frac{1}{2}$.

T □

Ordnung finden $\rightarrow$ DLP

grobe Skizze; geg. $G, \alpha, \beta = \alpha^a$

- Zusätzlich zu r mit $\alpha^r = 1$ suchen wir r_1, r_2 mit $\alpha^{r_1}\beta^{r_2} = 1$.

Ordnung finden $\rightarrow$ DLP

grobe Skizze; geg. $G, \alpha, \beta = \alpha^a$

- Zusätzlich zu r mit $\alpha^r = 1$ suchen wir r_1, r_2 mit $\alpha^{r_1}\beta^{r_2} = 1$.
- Dann gilt $r_1 \equiv_r -sr_2$.

Ordnung finden $\rightarrow$ DLP

grobe Skizze; geg. $G, \alpha, \beta = \alpha^a$

- Zusätzlich zu r mit $\alpha^r = 1$ suchen wir r_1, r_2 mit $\alpha^{r_1}\beta^{r_2} = 1$.
- Dann gilt $r_1 \equiv_r -sr_2$.
- Also ist $s = -\frac{r_1}{r_2}$.

Zusammenfassung – Was bedeutet Postquantenkryptografie?

Konsequenzen

- Shors Algorithmen hängen nur unwesentlich von der speziellen Gruppe ab, diese muss aber als Quantenschaltkreis realisiert werden, ggf. mit Ancillabits.

Zusammenfassung – Was bedeutet Postquantenkryptografie?

Konsequenzen

- Shors Algorithmen hängen nur unwesentlich von der speziellen Gruppe ab, diese muss aber als Quantenschaltkreis realisiert werden, ggf. mit Ancillabits.
- D.h. große Gruppen mit kleinen Schlüsseln (z.B. elliptische Kurven) bringen allenfalls eine Verzögerung, aber ihr diskretes Logarithmusproblem ist ebenfalls nicht grundsätzlich schwer für Quantenalgorithmen.

Zusammenfassung – Was bedeutet Postquantenkryptografie?

Konsequenzen

- Shors Algorithmen hängen nur unwesentlich von der speziellen Gruppe ab, diese muss aber als Quantenschaltkreis realisiert werden, ggf. mit Ancillabits.
- D.h. große Gruppen mit kleinen Schlüsseln (z.B. elliptische Kurven) bringen allenfalls eine Verzögerung, aber ihr diskretes Logarithmusproblem ist ebenfalls nicht grundsätzlich schwer für Quantenalgorithmen.
- Beiden Algorithmen gemein ist der Ansatz die Periode r einer periodischen Funktion f mit $\forall x \in \mathbb{Z} f(x+r) = f(x)$ zu finden. zu finden.

Zusammenfassung – Was bedeutet Postquantenkryptografie?

Konsequenzen

- Shors Algorithmen hängen nur unwesentlich von der speziellen Gruppe ab, diese muss aber als Quantenschaltkreis realisiert werden, ggf. mit Ancillabits.
- D.h. große Gruppen mit kleinen Schlüsseln (z.B. elliptische Kurven) bringen allenfalls eine Verzögerung, aber ihr diskretes Logarithmusproblem ist ebenfalls nicht grundsätzlich schwer für Quantenalgorithmen.
- Beiden Algorithmen gemein ist der Ansatz die Periode r einer periodischen Funktion f mit $\forall x \in \mathbb{Z} f(x+r) = f(x)$ zu finden. zu finden.
- PQK sollte also insbesondere keine solchen periodischen Funktionen nutzen, bei der die Periode Teil des (privaten) Schlüssels ist.

Zusammenfassung – Was bedeutet Postquantenkryptografie?

Konsequenzen

- Shors Algorithmen hängen nur unwesentlich von der speziellen Gruppe ab, diese muss aber als Quantenschaltkreis realisiert werden, ggf. mit Ancillabits.
- D.h. große Gruppen mit kleinen Schlüsseln (z.B. elliptische Kurven) bringen allenfalls eine Verzögerung, aber ihr diskretes Logarithmusproblem ist ebenfalls nicht grundsätzlich schwer für Quantenalgorithmen.
- Beiden Algorithmen gemein ist der Ansatz die Periode r einer periodischen Funktion f mit $\forall x \in \mathbb{Z} f(x+r) = f(x)$ zu finden. zu finden.
- PQK sollte also insbesondere keine solchen periodischen Funktionen nutzen, bei der die Periode Teil des (privaten) Schlüssels ist.
- Wenn wir von PQK sprechen, garantieren wir für diese System **nicht**, dass sie sicher gegen Quantenberechnungen sind (wie RSA etc. wissen wir nicht einmal, ob sie komplexitätstheoretisch sicher gegen klassische Angriffe sind.)