

Quantenalgorithmen (ab Vorlesung 09)

Alexander May

Fakultät für Mathematik
Ruhr-Universität Bochum

Wintersemester 08/09

Verallgemeinertes Problem von Simon

Verallgemeinertes Problem von Simon

Gegeben: $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ mit $f(x) = f(y) \Leftrightarrow x \oplus y \in S$
für einen Untervektorraum $S \subset \mathbb{F}_2^n$.

Gesucht: Basis für S

- Verwenden gleichen Quantenschaltkreis wie bei Simon's Problem.
- D.h. wir führen $H_n \otimes I_n$, U_f und wieder $H_n \otimes I_n$ durch.
- Nach Durchführung von Hadamard und U_f auf $|0\rangle|0\rangle$ erhalten wir

$$\frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x\rangle |f(x)\rangle.$$

- Messung der letzten n Register liefert ein $f(x_0)$, d.h.

$$\frac{1}{|S|^{1/2}} \sum_{s \in S} |x_0 + s\rangle \otimes |f(x_0)\rangle.$$

- Anwendung von Hadamard liefert

$$\begin{aligned} & \frac{1}{(2^n |S|)^{1/2}} \sum_{y \in \{0,1\}^n} \sum_{s \in S} (-1)^{(x_0 + s)y} |y\rangle \\ &= \frac{1}{(2^n |S|)^{1/2}} \sum_{y \in \{0,1\}^n} (-1)^{x_0 y} \sum_{s \in S} (-1)^{s y} |y\rangle. \end{aligned}$$

Messung für Simons Schaltkreis

- **Fall 1:** Sei $y \in S^\perp$, d.h. $sy = 0$.
- Für jedes y ist die Amplitude ist $\frac{\pm|S|}{(2^n|S|)^{\frac{1}{2}}}$, d.h. wir messen jedes y mit Ws $\frac{|S|}{2^n}$.
- Wegen $\dim(S) + \dim(S^\perp) = n$, gilt $|S| \cdot |S^\perp| = 2^n$.
- Damit wird jedes $y \in S^\perp$ mit Ws $\frac{1}{|S^\perp|}$ gemessen.
- D.h. die Ws für alle $y \notin S^\perp$ müssen 0 sein. Wir rechnen kurz nach.
- **Fall 2:** Sei $y \notin S^\perp$ und $s' \in S$ mit $s'y = 1$. Es gilt

$$\begin{aligned}\sum_{s \in S} (-1)^{sy} &= -(-1)^{s'y} \sum_{s \in S} (-1)^{sy} = - \sum_{s \in S} (-1)^{(s+s')y} \\ &= - \sum_{s \in S} (-1)^{sy}.\end{aligned}$$

- Damit verschwindet die Summe und alle Amplituden für $y \notin S^\perp$.

Bestimmung von S

- Messung liefert gleichverteilte $y_i \in S^\perp$.
- Da $\dim(S^\perp)$ unbekannt ist, berechnen wir solange y_i bis die Anzahl der linear unabhängigen y_i stabil bleibt.
- Dazu genügen $\dim(S^\perp) + 4$ Werte mit hoher Ws.
- Wir berechnen aus den y_i eine Basis B^\perp von S^\perp .
- Wir lösen das lineare Gleichungssystem $B^\perp s^T = \mathbf{0}$.
- Sei $B = \{s_1, \dots, s_m\}$ eine Generatorenmenge des Lösungsraums.
- B ist die gesuchte Basis von S .

Speedup und Interpretation von Simons Problem

Speedup gegenüber klassischen Algorithmen:

- Jeder klassische Algorithmus für Simons Problem muss Kollisionen $f(x) = f(y)$ finden.
- Für zufällige x, y ist die Wahrscheinlichkeit einer Kollision $2^{\dim(S)-n}$.
- Geburtstagsparadoxon: Erwarten Kollision nach $2^{\frac{n-\dim(S)}{2}}$ Schritten.
- Quantenalgorithmus liefert Basis für ca. $\dim(S^\perp) = n - \dim(S)$ Auswertungen.
- Damit erhalten wir einen exponentiellen Speedup (Orakel-Modell).

Interpretation

- Simons Algorithmus findet versteckte Untergruppe S in $(\mathbb{F}_2^n, +)$.
- Interpretation als Algorithmus zum Finden einer Periode.
- $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ ist periodisch: $f(x) = f(x \oplus s)$ mit Periode $s \in S$.
- Frage: Können wir $(\mathbb{F}_2, +)$ durch $(\mathbb{Z}, +)$ ersetzen?
 - ▶ $(r\mathbb{Z}, +)$ ist eine Untergruppe von $(\mathbb{Z}, +)$ für $r \in \mathbb{N}$.
 - ▶ D.h. $f : \mathbb{Z} \rightarrow \mathbb{Z}$, $f(x) = f(x + r\mathbb{Z})$ mit gesuchter Periode r .

RSA Verschlüsselung und Perioden

RSA Verschlüsselung

Sei $N = pq$ mit p, q prim und $\phi(N) = (p - 1)(q - 1)$. Ferner sei $e \in \mathbb{Z}_{\phi(N)}^*$. Die *RSA Funktion* ist die Abbildung $f_{RSA} : \mathbb{Z}_N \rightarrow \mathbb{Z}_N$ mit

$$m \mapsto m^e \bmod N.$$

Anmerkung:

- Sei $m \in \mathbb{Z}_N^*$. Wir definieren $\text{ord}(m) = \min\{i \in \mathbb{N} \mid m^i = 1 \bmod N\}$.
- Betrachten die Exponentiations-Funktion $f : \mathbb{Z} \rightarrow \mathbb{Z}_N$ mit
$$i \mapsto m^i \bmod N.$$
- f ist für jedes $m \in \mathbb{Z}_N^*$ periodisch, denn
$$f(i) = f(i + \text{ord}(m)k) \text{ für } k \in \mathbb{Z}.$$
- D.h. $\text{ord}(m)$ ist die Periode für die Exponentiations-Funktion.
- Unser Ziel ist die effiziente Ermittlung dieser Periode $\text{ord}(m)$.
- *Kleines Problem:* Angreifer kennt nur m^e und nicht m .

Ordnung von Plain- und Chiffretexten

Lemma

Seien N, e RSA Parameter und $m \in \mathbb{Z}_N^*$. Dann gilt $\text{ord}(m) = \text{ord}(m^e)$.

Beweis:

- Sei $\langle m \rangle = \{m, m^2, \dots, m^{\text{ord}(m)}\}$ die von m erzeugte Untergruppe.
- Es gilt $\text{ord}(m) = |\langle m \rangle|$. Zeigen zunächst $\langle m^e \rangle \subseteq \langle m \rangle$.
- Sei $m^{ei} \in \langle m^e \rangle$. Dann gilt offenbar $m^{ei} \in \langle m \rangle$.
- Andererseits zeigen wir $\langle m \rangle \subseteq \langle m^e \rangle$.
- Nach Satz von Euler gilt $m^{|\mathbb{Z}_N^*|} = m^{\phi(N)} = 1$.
- Die Elementordnung teilt die Gruppenordnung, d.h. $\text{ord}(m) \mid \phi(N)$.
- Wegen $\text{ggT}(e, \phi(N)) = 1$ gilt damit ebenfalls $\text{ggT}(e, \text{ord}(m)) = 1$.
- Damit existieren $d, k \in \mathbb{Z}$ mit $ed + \text{ord}(m)k = 1$.
- D.h. $m = m^{ed + \text{ord}(m)k} = m^{ed} \cdot (m^{\text{ord}(m)})^k = (m^e)^d \pmod{N}$.
- Daraus folgt $m \in \langle m^e \rangle$ und damit auch $m^i \in \langle m^e \rangle$ für alle $i \in \mathbb{N}$.
- Insgesamt: $\langle m \rangle = \langle m^e \rangle$, d.h. $\text{ord}(m) = |\langle m \rangle| = |\langle m^e \rangle| = \text{ord}(m^e)$.

Brechen von RSA mit Hilfe der Ordnung von m

Satz

Seien N, e RSA-Parameter und $m^e \in \mathbb{Z}_N^*$. Mit Hilfe von $\text{ord}(m^e)$ kann m in Zeit $\mathcal{O}(\log^3 N)$ berechnet werden.

Beweis:

- Beweis zuvor liefert $\text{ord}(m) = \text{ord}(m^e)$ und $\text{ggT}(e, \text{ord}(m)) = 1$.
- Der Erweiterte Euklidische Algorithmus liefert bei Eingabe $e, \text{ord}(m) \in \mathbb{Z}_N$ in Zeit $\mathcal{O}(\log^2 N)$ Zahlen d, k mit $ed + \text{ord}(m)k = 1$.
- Wir berechnen $(m^e)^d = m^{1 - \text{ord}(m)k} = m \cdot (m^{\text{ord}(m)})^{-k} = m \pmod N$ in Zeit $\mathcal{O}(\log^3 N)$.