Quantenalgorithmen
(ab Vorlesung 09)

Alexander May

Fakultät für Mathematik
Ruhr-Universität Bochum

Wintersemester 2011/12

Problem von Simon (1994)

Problem von Simon

Gegeben: $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ mit $f(x) = f(y) \Leftrightarrow y = x + s$
Gesucht: $s \in \mathbb{F}_2^n$

Anmerkungen:

- Je zwei Urbilder x und $x + s$ werden auf dasselbe Bild abgebildet.
- Damit ist f eine (2:1)-Abbildung.

Klassischer Algorithmus:

- Werte paarweise verschiedene $x_1, \ldots, x_k$ aus, bis eine Kollision $f(x_i) = f(x_j)$ gefunden wird.
- Nach Schubfachprinzip genügen $k \leq 2^{n-1} + 1$ Auswertung von f.
- Probabilistisch genügen $k = \Theta(2^{\frac{n}{2}})$ mit hoher Ws.
- Definiere eine Indikatorvariable mit $X_{i,j} = 1$ gdw $f(x_i) = f(x_j)$.
- Die erwartete Anzahl von Kollisionen ist damit
$$E(\mathit{Kollisionen}) = \sum_{1 \leq i < j \leq k} \mathrm{Ws}[X_{i,j} = 1] = \frac{k^2}{2^n - 1}.$$
- Das heißt, wir benötigen $k = \Theta(2^{\frac{n}{2}})$, um Kollisionen zu erhalten.

Ermittle Vektor orthogonal zu s.

Quantenschaltkreis Q_S:

- Sei U_f die reversible Einbettung der Funktion f.
- Anwendung von $H_n \otimes I_n$ und U_f auf $0^n 0^n$ liefert
$$\frac{1}{2^n} \sum_{x \in \{0,1\}^n} |x\rangle \otimes |f(x)\rangle.$$
- Messung der letzten n Register liefert für ein festes $f(x_0)$
$$\frac{1}{\sqrt{2}}(|x_0\rangle + |x_0 + s\rangle) \otimes f(x_0).$$
- Anwendung von $H_n \otimes I_n$ führt zu
$$\begin{aligned} & \frac{1}{\sqrt{2}} \frac{1}{2^{\frac{n}{2}}} \left(\sum_{y \in \{0,1\}^n} ((-1)^{x_0 y} + (-1)^{(x_0+s)\cdot y}) |y\rangle \right) \otimes f(x_0) \\ = \quad & \frac{1}{\sqrt{2}} \frac{1}{2^{\frac{n}{2}}} \left(\sum_{y \in \{0,1\}^n} (-1)^{x_0 y} (1 + (-1)^{sy}) |y\rangle \right) \otimes f(x_0) \\ = \quad & \frac{1}{2^{\frac{n-1}{2}}} \left(\sum_{y \in \{0,1\}^n, ys=0} (-1)^{x_0 y} |y\rangle \right) \otimes f(x_0). \end{aligned}$$
- Messung der ersten n Register liefert gleichverteiltes y mit $ys = 0$.

Quantenalgorithmus für Simons Problem

Algorithmus Simon

EINGABE: Quantenschaltkreis Q_S

1. Konstruiere leere $(n \times n)$-Matrix Y.
2. Wiederhole bis $\mathrm{rang}(Y) = n$:
   1. Konstruiere mittels Q_S gleichverteiltes $y \in \{0,1\}^n$ mit $ys = 0$.
   2. Falls y linear unabhängig zu Vektoren aus Y, füge y zu Y hinzu.
3. Löse das Gleichungssystem $Y \cdot s = \mathbf{0}$ über $\mathbb{F}_2$.

AUSGABE: $s \in \mathbb{F}_2^n$ mit $f(x) = f(x+s)$ für alle $x \in \mathbb{F}_2^n$

- Korrektheit: Für $\mathrm{rang}(Y) = n$ ist s eindeutig bestimmt.
- Laufzeit: $\mathcal{O}(n)$ Gatteranwendungen ($+\mathcal{O}(n^3)$ für lineare Algebra).
- Exponentieller Speedup gegenüber der klassischen Lösung.

Verallgemeinertes Problem von Simon

Verallgemeinertes Problem von Simon

Gegeben: $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ 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.
- Durchführung von Hadamard und U_f auf $|0^n\rangle|0^n\rangle$ führt zu
$$\frac{1}{2^{\frac{n}{2}}} \sum_{x \in \{0,1\}^n} |x\rangle|f(x)\rangle.$$
- Messung der letzten n Register liefert ein $f(x_0)$, d.h.
$$\frac{1}{|S|^{\frac{1}{2}}} \sum_{s \in S} |x_0 + s\rangle \otimes |f(x_0\rangle.$$
- Anwendung von Hadamard liefert
$$\frac{1}{(2^n|S|)^{\frac{1}{2}}} \sum_{y \in \{0,1\}^n} \sum_{s \in S} (-1)^{(x_0+s)y} |y\rangle$$
$$= \frac{1}{(2^n|S|)^{\frac{1}{2}}} \sum_{y \in \{0,1\}^n} (-1)^{x_0 y} \sum_{s \in S} (-1)^{sy} |y\rangle.$$

Messung für Simons Schaltkreis

- **Fall 1:** Sei $y \in S^{\perp}$, d.h. $sy = 0$. Für jedes y ist die Amplitude $\frac{\pm|S|}{(2^n|S|)^{\frac{1}{2}}}$, 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 $y \notin S^{\perp}$. Damit existiert ein $s' \in S$ 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 $B = \{s_1, \ldots, s_m\}$ 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.
- $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ 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. $f : \mathbb{Z} \to \mathbb{Z}$, $f(x) = f(x + r\mathbb{Z})$ 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 $f_{RSA} : \mathbb{Z}_N \to \mathbb{Z}_N$ mit

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

Anmerkung:

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

Beweis:

- Sei $\langle m \rangle = \{m, m^2, \ldots, m^{\mathrm{ord}(m)}\}$ die von m erzeugte Untergruppe.
- Es gilt $\mathrm{ord}(m) = |\langle m \rangle|$. 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. $\mathrm{ord}(m) \mid \phi(N)$.
- Wegen $\mathrm{ggT}(e, \phi(N)) = 1$ gilt damit ebenfalls $\mathrm{ggT}(e, \mathrm{ord}(m)) = 1$.
- Damit existieren $d, k \in \mathbb{Z}$ mit $ed + \mathrm{ord}(m)k = 1$.
- D.h. $m = m^{ed+\mathrm{ord}(m)k} = m^{ed} \cdot (m^{ord(m)})^k = (m^e)^d \bmod N$.
- 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. $\mathrm{ord}(m) = |\langle m \rangle| = |\langle m^e \rangle| = \mathrm{ord}(m^e)$.

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 $\mathrm{ord}(m^e)$ kann m in Zeit $\mathcal{O}(\log^3 N)$ berechnet werden.

Beweis:

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