Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Gottfried Herold

Hausübungen zur Vorlesung

Quantenalgorithmen

SS 2016

Blatt 4 / 2. Juni 2016

Abgabe: 13. Juni 2016, 10.00 Uhr (vor der Vorlesung), Kasten NA/02

AUFGABE 1 (4 Punkte)**:**

Sei $f\colon\ \mathbb{F}_2^n \to \mathbb{F}_2$ eine beliebige Funktion. Gegeben sei ein Quanten-Schaltkreis Q auf $n+1$ Qubits, der für alle $\vec{x} \in \mathbb{F}_2^n$, $y \in \mathbb{F}_2$ die Abbildung $|\vec{x}y\rangle \mapsto (-1)^{f(\vec{x})y}|\vec{x}y\rangle$ berechnet.

Konstruieren Sie unter Verwendung von Q und Standard-Quantengates (Toffoli, CNOT, W_2) einen Quantenschaltkreis, der die reversible Einbettung $U_f\colon\ |\vec{x}y\rangle \mapsto |\vec{x}\rangle \otimes |f(\vec{x}) \oplus y\rangle$ berechnet.

AUFGABE 2 (6 Punkte)**:**

Betrachten Sie die Abbildung $f : \mathbb{F}_2^4 \to \mathbb{F}_2^4$, $f(x_1, x_2, x_3, x_4) := (x_1{+}x_2, x_2{+}x_3, x_3{+}x_4, x_4{+}x_1)$. Sie dürfen als bekannt voraussetzen, dass dies eine $2:1$-Abbildung mit $f(\vec{x}) = f(\vec{x} \oplus \vec{s})$ für geeignetes $\vec{s}$ ist.

Wir möchten den Algorithmus von Simon anwenden, um s zu finden.

(a) Geben einen Quantenschaltkreis für die reversible Einbettung von f an.

(b) Geben Sie den Quantenschaltkreis Q_S des Algorithmus von Simon für dieses f an.

(c) Angenommen Sie messen (in der Notation der Vorlesung) in 3 Iterationen von Q_S die Ergebnisse $y_1 = (1,1,0,0),\ y_2 = (1,0,1,0),\ y_3 = (1,0,0,1)$.
Berechnen Sie daraus $\vec{s}$.

(d) Zeigen Sie, dass $n-1$ Vektoren aus $\mathbb{F}_2^n$ mit Wahrscheinlichkeit

$$\prod_{i=0}^{n-2}(1-2^{i-n})$$

linear unabhängig über $\mathbb{F}_2$ sind. Mit welcher Wahrscheinlichkeit reicht Ihnen die Messung von 3 Vektoren, um $\vec{s}$ in (c) eindeutig zu bestimmen?

Bitte wenden!

AUFGABE 3 (3 Punkte)**:**

Zeigen Sie, dass das Toffoli-Gate $\{T\}$ r-universell ist.

Erinnerung/Klarstellung: Beachten Sie, dass laut Definition von r-Universalität Hilfvariablen und Konstanten 0,1 zur Verfügung haben.

AUFGABE 4 (7 Punkte)**:**

In dieser Aufgabe wollen wir zeigen, dass man mit einem Algorithmus zum Finden der Periode nicht nur RSA brechen, sondern sogar faktorisieren kann. Sei hierzu $N = p_1 \cdots p_k$ Produkt von $k \geq 2$ ungeraden Primzahlen. Wir nehmen der Einfachheit halber an, dass die p_i paarweise verschieden sind.
Sei $a \in \mathbb{Z}_N^*$ uniform gewählt. Sei $t = \mathrm{ord}_{\mathbb{Z}_N^*}(a)$ die Ordnung von a in $\mathbb{Z}_N^*$. Sei weiterhin $t_i = \mathrm{ord}_{\mathbb{Z}_{p_i}^*}(a)$ die Ordnung von a in $\mathbb{Z}_{p_i}^*$.

Schreibe $t = 2^s \cdot u$ sowie $t_i = 2^{s_i} \cdot u_i$ mit u, u_i ungerade.
Schreibe $|\mathbb{Z}_{p_i}^*| = p_i - 1 = 2^{r_i} \cdot q_i$ mit $r_i \geq 1$ und q_i ungerade (nicht notwendig prim).

(a) Zeigen Sie, dass $t = \mathrm{kgV}(t_1, \ldots, t_k)$ und $s = \max\{s_1, \ldots, s_k\}$ gilt.

(b) Zeigen Sie, dass für jedes i unabhängig voneinander gilt:
Mit Wahrscheinlichkeit $\frac{1}{2}$ ist $s_i = r_i$.

(c) Zeigen Sie, dass mit Wahrscheinlichkeit $\geq \frac{1}{4}$ ein Paar $i \neq j$ mit $s_i \neq s_j$ existiert.

(d) Zeigen Sie, dass $a^{2^{s_i-1}u} \bmod p_i = -1$ ist, falls $s_i \geq 1$ gilt.

(d) Sei $s \geq 1$. Zeigen Sie, dass

$$a^{2^{s-1}u} \bmod p_i = \begin{cases} -1, \text{ falls } s_i = s \\ +1 \text{ falls } s_i < s \end{cases}$$

gilt.

(e) Zeigen Sie, dass mit Wahrscheinlichkeit $\geq \frac{1}{4}$ gilt, dass $\mathrm{ggT}(N, a^{2^{s-1}u} + 1)$ ein nicht-trivialer Teiler von N ist.

(f) Sei `PERIODE`(N, a) ein Algorithmus, der zu gegebenem $N = p_1 \cdots p_k$ von obiger Form und $a \in \mathbb{Z}_N^*$ in Laufzeit $T(N)$ die Ordnung $t = \mathrm{ord}_{\mathbb{Z}_N^*}(a)$ ausgibt. Konstruieren Sie mittels `PERIODE` einen Algorithmus, der in erwarteter Laufzeit $\mathcal{O}(T(N)\log(N)^3)$ einen nicht-trivialen Teiler von N ausgibt.

Hinweis: Verwenden Sie den chin. Restsatz. Sie dürfen verwenden, dass $\mathbb{Z}_{p_i}^*$ zyklisch ist. $s_i = r_i$ gilt gdw. a kein quadratischer Rest modulo p_i ist. Beachten Sie, dass im Fall $s_i \neq s_j$ stets $s \geq 1$ ist. Der Algorithmus, den Sie in (f) angeben sollen, benutzt keine Quanten (ausser `PERIODE` tut dies).