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

Hausübungen zur Vorlesung

Quantenalgorithmen

SS 2016

Blatt 3 / 19. Mai 2016

Abgabe: 30. Mai 2016, 10.00 Uhr (vor der Vorlesung), Kasten NA/02

AUFGABE 1 (3 Punkte)**:**

Zeigen Sie, dass die Menge $\{\text{nor}, c\}$ universell ist.

Dabei ist c die Kopierfunktion $c(x) = (x, x)$ und nor ist definiert als $\text{nor}(x, y) := \neg(x \vee y)$.

AUFGABE 2 (3 Punkte)**:**

Geben Sie einen Schaltkreis über der Menge $\{\text{nor}, c\}$ an, der das XOR zweier Bits x, y berechnet.

AUFGABE 3 (4 Punkte)**:**

Für einen Booleschen Schaltkreis C sei die *Tiefe* des Schaltkreises definiert als die Länge des längsten Weges von einem Eingabe- zu einem Ausgabeknoten.

Sei $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ beliebige Funktion. Zeigen Sie, dass es stets einen Schaltkreis C über $S = \{c, \wedge, \vee, \oplus, \neg\}$ der Tiefe $O(n)$ gibt, der f realisiert.

Bemerkung: Die Wahl der universellen Menge S spielt für diese Aufgabe keine Rolle und ist lediglich groß gewählt, um Schaltkreise komfortabel aufschreiben zu können.

Bitte wenden!

AUFGABE 4 (14 Punkte)**:**

Wir wollen in dieser Aufgabe die Sicherheit des BB92 - Protokolls gegen passive Angreifer analysieren. Dazu betrachen wir folgendes Modell für einen passiven Angreifer E:

1. Alice wählt $a \in_R \{0,1\}$ uniform. Setze $|z\rangle := \begin{cases} |0\rangle & \text{falls } a = 0 \\ |x\rangle & \text{falls } a = 1, \end{cases}$
   wobei $|x\rangle := \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big)$. Sende $|z\rangle$ an Eve.

2. Eve wählt eine Orthonormalbasis $|\alpha\rangle, |\beta\rangle$ und misst $|z\rangle$ in dieser Basis.
   Das Ergebnis der Messung sei M. Der Zustand nach der Messung sei $|z'\rangle$.
   Sende $|z'\rangle$ an Bob.

3. Bob wählt $a' \in_R \{0,1\}$ uniform. Bob misst $|z'\rangle$ in der

   - Z-basis für $a' = 0$. Falls Ergebnis $|0\rangle$, setze $b = 0$, sonst $b = 1$.
   - X-basis für $a' = 1$. Falls Ergebnis $|x\rangle$, setze $b = 0$, sonst $b = 1$.

   Bob sendet b and Eve und Alice.

4. Falls $b = 0$: Zurück zu Schritt 1.
   Falls $b = 1$: Alice Schlüsselbit ist $k_A = a$, Bobs Schlüsselbit ist $k_B = 1 - a'$.

(a) Drücken Sie die Wahrscheinlichkeit P, dass $b = 0$ in Schritt 3 gilt, als Funktion von Eves Wahl von $|\alpha\rangle, |\beta\rangle$ aus. (D.h. Ihr Ergebnis wird Ausdrücke der Form $\langle\alpha|0\rangle, \langle\beta|0\rangle$ etc. enthalten)

(b) Berechnen Sie P für den Fall, dass Eve in der Basis $|0\rangle, |1\rangle$ misst.

(c) Zeigen Sie, dass stets $P \leq \frac{3}{4}$ gilt.

(d) Zeigen Sie: Falls Eve Ihre Basis α, β so wählt, dass $P = \frac{3}{4}$ gilt (um nicht detektiert zu werden), so ist M unabhängig von k_A und k_B falls $b = 1$.

Bemerkungen: Es ist ratsam in (a) bzw. (c), $|\langle\beta|0\rangle|, |\langle\beta|x\rangle|$ durch $|\langle\alpha|0\rangle|, |\langle\alpha|x\rangle|$ auszudrücken. Die Ungleichung von Präsenzblatt 3, Aufgabe 5 ist in (c) hilfreich. Beachten Sie, dass auf Grund von Eves Messung im Allgemeinen *nicht* mehr $k_A = k_B$ gilt.