

Korrekturen und Ergänzungen zum Skript Quantenkryptographie Wintersemester 2007/2008

S. 16, Z. –6 und –5: Ersetze $l(a)$ durch $l(A)$.

S. 17, Erläuterung zum 1. Fall: In der Vorlesung kam die Frage auf, warum der Faktor 2 im Ergebnis nicht vermieden werden kann. Sei p die Wahrscheinlichkeit von $m'_1 = m'_2$, und sei q die Wahrscheinlichkeit von $h(m_2) = a_1$ unter der Bedingung $m'_1 \neq m'_2$. Dann ist $p \leq 1/|A|$ und $q = 1/|A|$. Die gesuchte Wahrscheinlichkeit von $h(m_2) = a_1$ beträgt dann $p + (1 - p)q \leq (2 - 1/|A|) \cdot (1/|A|)$. Der Faktor 2 kann also bei den verwendeten Abschätzungen nur geringfügig verbessert werden.

S. 22, abgesetzte Formel: Ersetze die Definitionen von $|r\rangle$ und $|s\rangle$ wie folgt:

$$|r\rangle = -\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle \quad \text{und} \quad |s\rangle = -\frac{1}{2}|0\rangle - \frac{\sqrt{3}}{2}|1\rangle.$$

S. 24, letzte abgesetzte Formel, und S. 25, obere Rechnung: Der Vektor $|\phi_\mu\rangle$ ist i.A. von der Form

$$|\phi_\mu\rangle = \sum_{j',j''} \alpha_{j',j''} |\phi'_{j'}\rangle \otimes |\phi''_{j''}\rangle.$$

Dadurch sind in der nachfolgenden Rechnungen einige Indizes hinzuzufügen, die Erläuterungen zur Rechnung und das Ergebnis bleiben aber unverändert.

$$\begin{aligned} A_\mu &= \text{tr}_{\text{aux}}(P_\mu(I \otimes \sigma_{\text{aux}})) \\ &= \text{tr}_{\text{aux}} \left(\sum_{j',j'',k',k''} \alpha_{j',j''} \alpha_{k',k''}^* |\phi'_{j'}\rangle |\phi''_{j''}\rangle \langle \phi'_{k'}| \langle \phi''_{k''}| (I \otimes \sigma_{\text{aux}}) \right) \\ &= \sum_{j',j'',k',k''} \alpha_{j',j''} \alpha_{k',k''}^* \text{tr}_{\text{aux}} (|\phi'_{j'}\rangle \langle \phi'_{k'}| \otimes |\phi''_{j''}\rangle \langle \phi''_{k''}| \sigma_{\text{aux}}) \\ &= \sum_{j',j'',k',k''} \alpha_{j',j''} \alpha_{k',k''}^* |\phi'_{j'}\rangle \langle \phi'_{k'}| \cdot \text{tr} (|\phi''_{j''}\rangle \langle \phi''_{k''}| \sigma_{\text{aux}}) \\ &= \sum_{j',j'',k',k''} \alpha_{j',j''} \alpha_{k',k''}^* |\phi'_{j'}\rangle \langle \phi'_{k'}| \cdot \text{tr} (\sqrt{\sigma_{\text{aux}}} |\phi''_{j''}\rangle \langle \phi''_{k''}| \sqrt{\sigma_{\text{aux}}}) \\ &= \sum_{j',j'',k',k''} \alpha_{j',j''} \alpha_{k',k''}^* \text{tr}_{\text{aux}} (|\phi'_{j'}\rangle \langle \phi'_{k'}| \otimes \sqrt{\sigma_{\text{aux}}} |\phi''_{j''}\rangle \langle \phi''_{k''}| \sqrt{\sigma_{\text{aux}}}) \\ &= \text{tr}_{\text{aux}} \left(\sum_{j',j'',k',k''} \alpha_{j',j''} \alpha_{k',k''}^* (I \otimes \sqrt{\sigma_{\text{aux}}} |\phi'_{j'}\rangle |\phi''_{j''}\rangle \langle \phi'_{k'}| \langle \phi''_{k''}| (I \otimes \sqrt{\sigma_{\text{aux}}}) \right) \\ &= \text{tr}_{\text{aux}} ((I \otimes \sqrt{\sigma_{\text{aux}}})^\dagger P_\mu^\dagger P_\mu (I \otimes \sqrt{\sigma_{\text{aux}}}). \end{aligned}$$

S. 30, Z. 5: Hier wird noch folgendes Argument benutzt: Wenn S positiv semidefinit ist und P eine Projektion (und somit $P = PP^\dagger$), folgt zusammen mit der Zyklizität der Spur $\text{tr}(PS) = \text{tr}(P^\dagger SP) \geq 0$. Somit folgt $\text{tr}(P(Q - S)) = \text{tr}(P^\dagger QP) - \text{tr}(P^\dagger SP) \leq \text{tr}(Q)$.

S. 30, erste abgesetzte Formel im Beweis von Satz 4.6: Die Abschätzung \leq ergibt sich durch die folgende Rechnung:

$$\begin{aligned} |\text{tr}(E_i(Q - S))| &= \left| \text{tr}(\sqrt{E_i}Q\sqrt{E_i}) - \text{tr}(\sqrt{E_i}S\sqrt{E_i}) \right| \\ &\leq \text{tr}(\sqrt{E_i}Q\sqrt{E_i}) + \text{tr}(\sqrt{E_i}S\sqrt{E_i}) \\ &= \text{tr}(E_i(Q + S)). \end{aligned}$$

Hierbei wird wieder ausgenutzt, dass E_i positiv semidefinit sind und die Spur zyklisch ist.

S. 34, Satz 4.10: Ersetze φ_1 durch $|\varphi_1\rangle$ und φ_2 durch $|\varphi_2\rangle$.

S. 37, letzte Zeile: Wähle hier $|\varphi_0\rangle = \alpha_0 \begin{pmatrix} \sqrt{2} + 1 \\ -1 \end{pmatrix}$. (Der im Skript angegebene Ausdruck ist zwar richtig, passt aber nicht zur Zeichnung.)

S. 42, Z. 7: Ersetze „seperat“ durch „separat“.

S. 42, letzte abgesetzte Formel (und analog in der folgenden Rechnung): Ersetze H durch $H^{\otimes n}$.

S. 43, Z. 8f.: Der Zustand $H^{\otimes n}|\psi\rangle$ hat auch nach der beschriebenen Ersetzung von C_1 durch C_2^\perp nicht genau die Form wie in (3). Die Argumente von oben stimmen aber weiterhin. Man benötigt nun eine unitäre Operation U_2 mit $U_2(|x\rangle \otimes |0\rangle) = |x\rangle \otimes |H_2^\perp x\rangle$. Da $z' \in C_2^\perp$, folgt analog $U_2|z' + e_2\rangle \otimes |0\rangle = |z' + e_2\rangle \otimes |H_2^\perp e_2\rangle$.

S. 47, Z. 25: Pricacy \rightarrow Privacy

S. 57, Z. 4: $[n, k_1] \rightarrow [n/2, k_1]$ und $[n, k_2] \rightarrow [n/2, k_2]$.

S. 58, Z. 4: $u \in \{0, 1\}^n / C_2^\perp \rightarrow u \in \{0, 1\}^{n/2} / C_2^\perp$ und $v \in \{0, 1\} / C_2^\perp \rightarrow v \in \{0, 1\}^{n/2} / C_2^\perp$.

S. 68ff. (Abschnitt 8.8) und S. 93f. (Beweis von Lemma 8.7): Damit diese Abschnitte mit dem Rest von Kapitel 8 konsistent sind, muss n durch $n' := n/2$ ersetzt werden.

S. 71, C3: der \rightarrow das.

S. 71, C13: $u \in \{0, 1\}^n / C_2^\perp \rightarrow u \in \{0, 1\}^{n/2} / C_2^\perp$ und $v \in \{0, 1\} / C_2^\perp \rightarrow v \in \{0, 1\}^{n/2} / C_2^\perp$.

S. 78, Schritt G7: k' setzt sich aus $k \in C_1$ und $v \in \{0, 1\}^{n/2} / C_1$ zusammen. Alice bestimmt aus k' mit klassischer Rechnung $k \in C_1$ und hieraus die Nebenklasse $k^* \in C_1 / C_2$, die k enthält. Den Schlüssel erhält sie durch Berechnung von $f_{C_1, C_2}^{-1}(k^*)$.

S. 79, Schritt G8: Bob interpretiert die Messergebnisse auf den Datenbits als $k^* + y + v + e_1$. Er hat v von Alice erhalten und kann somit $k^* + y + e_1$ berechnen, wobei $k^* \in C_1/C_2$, $y \in C_2$ und $e_1 \in \{0, 1\}^{n/2}/C_1$ ist. Mit klassischer Rechnung bestimmt er k^* und hieraus analog zu Alice in Schritt G7 den vereinbarten Schlüssel.

S. 79, Z. 5f.: Der Code C_1 dient also der Fehlerkorrektur. Die Bestimmung von k^* aus k realisiert eine Privacy Amplification. Somit wird hier der Code C_2 für eine Privacy Amplification benutzt.

Letzte Änderung: 4.2.2008