Prof. C. P. Schnorr Sommersemester 2017

Kryptographie

Blatt 6, 31.05.2017, Abgabe 07.06.2017

Aufgabe 1. Skizziere einen Beweis von Satz 2', Kap. 2.2 zu (P^k, V^k) mit Details zum Algorithmus AL$(\widetilde{P}, h)$.
Satz 2'. Zu (P^k, V^k) gibt es einen prob. Alg. AL: $(\widetilde{P}, h) \longmapsto \log_g h$ mit $E_w|AL| = O(|\widetilde{P}|/\varepsilon)$ sofern $\widetilde{P}$ Erfolgsws $\varepsilon > 2^{-tk+1}$ für $(\widetilde{P}, V^k)$ hat.

Aufgabe 2. Beweise Lemma 3', Kap. 2.2.
Lemma 3'. Zu (P^k, V^k) gibt es einen perfekten Simulator $\mathcal{S} : (\widetilde{V}, h) \longmapsto (\underline{g}, \underline{c}, \underline{y})$ der die Verteilung der von $(P^k, \widetilde{V})$ übertragenen Daten $(\underline{g}, \underline{\widetilde{c}}, \underline{y})$ erzeugt mit $E_w|\mathcal{S}(\widetilde{V}, h)| \leq O(|P^k|+|\widetilde{V}|)2^t$ — nicht 2^{t+k} — wobei $\underline{g} = (g_1, \ldots g_k)$, $\underline{\widetilde{c}} = (\widetilde{c}_1, \ldots, \widetilde{c}_k)$, $\underline{y} = (y_1, \ldots, y_k)$. $\mathcal{S}$ errät das $\widetilde{c}_i \in [0, 2^t[$ von $\widetilde{V}$ und stellt bei Misserfolg die blackbox $\widetilde{V}$ zurück.

Aufgabe 3. Übertrage das Protokoll zur Erzeugung blinder Schnorr Signaturen auf Okamoto Signaturen und zeige Korrektheit und Blindheit.

Punktzahl pro Aufgabe 5