Prof. C. P. Schnorr Wintersemester 2013/14

Kryptographie

Blatt 6, 20.12.2013, Abgabe 17.01.2014

Aufgabe 1 Erweitere das Protokoll zur Erzeugung blinder Signaturen von Schnorr Signaturen auf Okamoto Signaturen. Zeige, dass das Protokoll blinde Okamoto Signaturen erzeugt.

Aufgabe 2 Skizziere, wie man aus $l = 2^t - 1$ Interaktionen zu blinden Okamoto Signaturen 2^t korrekte Okamoto Signaturen für *inhaltlich* frei wählbare Nachrichten $m_1, \cdots, m_{2^t}$ im ROM erhält. Wende Wagner's 2^t Summen Alg. über $\mathbb{Z}_q$ an, $t = 2$ genügt.
Hinweis: Zu blinden Okamoto-Schnorr Signaturen siehe Seite 5,6 von C.P.Schnorr, Security of Blind Discrete Log Signatutes Against Interative Attacks.
http://mi.informatik.uni-frankfurt.de, Publications 2001.

Aufgabe 3 Skizziere Wagners 2^t Summen Algorithmus über $\mathbb{Z}_q$ für beliebige $t \geq 2$. Zeige die Laufzeit $O(2^t q^{\frac{1}{t+1}})$ und begründe die Erfolgswahrscheinlichkeit.

Aufgabe 4 Sei $A = [a_{i,j}]_{1 \leq i,j \leq 4} \in \mathbb{Z}^*_{q^{4\times 4}}$, $a_{k,4} = H(f_k, m_k)$ die Matrix zur parallelen Attacke auf blinde Schnorr Signaturen für $t = 2, \det A = \sum_{k=1}^{4} (-1)^k A_k H(f_k, m_k)$.
Zeige: für zufällige, stat. unabh. $a_{i,i}, a_{4,j}, a_{j,4} \in_R \mathbb{Z}^*_q$ für $1 \leq i, j \leq 4$ und sonst $a_{i,j} = 0$ sind die Koeffizienten $(-1)^k A_k H(f_k, m_k) \in \mathbb{Z}^*_q$ zufällig und stat. unabh. Dies gilt auch für alle Elemente der Listen $L_1, ..., L_4$

Punktzahl pro Aufgabe 5