Prof. C. P. Schnorr Sommersemester 2017

Kryptographie

Blatt 7, 07.06.2017, Abgabe 17.06.2017

Aufgabe 1 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.
Hinweis: Zu blinden Okamoto-Schnorr Signaturen siehe Seite 5,6 von C.P.Schnorr, Security of Blind Discrete Log Signatures Against Interative Attacks. ICICS 2001.

Aufgabe 2 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 3 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 $t = 2, |\det A = \sum_{k=1}^{4} (-1)^k A_k H(f_k, m_k)$, $A_k := \det A$ nach Entfernen der k-ten Zeile und Spalte.
Zeige: für zufällige, stat. unabh. $a_{i,i}, a_{4,j} \in_R \mathbb{Z}_q^*$ für $1 \leq i, j \leq 3$, $a_{k,4} = H(f_k, m_k) \in \mathbb{Z}_q^*$ 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 $L_1, ..., L_4$ (Der Fall $a_{1,2} = a_{1,3} = a_{2,3} = a_{2,1} = a_{3,2} = 0$ wurde in der Vorlesung behandelt.)

Punktzahl pro Aufgabe 5