Prof. C. P. Schnorr Wintersemester 2013/14

Kryptographie

Blatt 9, 31.01.2014, Abgabe 07.02.2014

Aufgabe 1 Sei $A = [a_{i,j}]_{1 \le i,j \le 4} \in (\mathbb{Z}_q^*)^{4\times 4}$, $a_{k,4} = H(f_k, m_k) \in \mathbb{Z}_q^*$ 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 $1 \le i, j \le$ und sonst $a_{i,j} = 0$ sind die $(-1)^k A_k H(f_k, m_k) \in \mathbb{Z}_q^*$ für $k = 1, ..., 4$ zufällig und stat. unabh. Dies gilt auch für alle Elemente der Listen $L_1, ..., L_4$

Aufgabe 2 Beispiel zum Paillier Schema

Setze $N = 143 = 11 \cdot 13$.

Berechne ein $\alpha \in \mathbb{Z}_{N^2}^*$ mit $\mathrm{ord}(\alpha) = \lambda(N^2)$. Kodiere $m = 2$ zu

$\mathrm{cip} = E_\alpha(2, r)$ und dekodiere cip.

Aufgabe 3 Präzisiere und analysiere folgenden Lösungsalgorithmus für das 2-Summenproblem über $\{0,1\}^n$:

Verteile die $x_1 \in L_1, x_2 \in L_2$ in $2^{n/2}$ Fächer nach den niedrigsten $n/2$ Bits. Suche die Teil-Kollisionen über $\{0,1\}^{n/2}$ nach Kollisionen über $\{0,1\}^n$ ab.

Bilde z.B. $L = \{(x_1, x_2, x_1 \oplus x_2) \mid low_{n/2}(x_1) = low_{n/2}(x_2)\}$. Zeige:

Für $|L_1| = |L_2| = 2^{n/2}$ geht das Verfahren in $O(2^{n/2})$ arithm. + Adress-Schritten. Ein $\log n$ Faktor für Sortieren tritt nicht auf.

5 Punkte pro Aufgabe