Prof. C. P. Schnorr Sommersemester 2007

Kryptographie

Blatt 6, 25.05.07, Abgabe 01.06.07

Aufgabe 1 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.

Aufgabe 2 Zeige: Die DL-Identifikation (P, V) ist honest verifier perfect zeroknowledge. Gebe einen perfekten Simulator $\mathcal{S}$ zu (P, V) an. Warum geht die Simulation nicht für beliebige $\widetilde{V}$?

Aufgabe 3 Beweise Satz 2', Kap. 2.2: Beschreibe einen prob. Extraktor $AL : (\widetilde{P}, h) \mapsto \log_g h$ zu (P^k, V^k) mit erwarteter Laufzeit $O(|\widetilde{P}|/\varepsilon)$, sofern $\widetilde{P}$ mit Ws $\varepsilon > 2^{-tk+1}$ Erfolg hat.

Aufgabe 4 Ein CMA-Angreifer $\mathcal{A}$ auf Schnorr Unterschriften ruft das H-Orakel ℓ-mal auf. Beschreibe einen prob. Extraktor $AL : (\mathcal{A}, h) \mapsto \log_g h$ mit erwarteter Laufzeit $O(\ell|\mathcal{A}|/\varepsilon)$ im ROM, sofern $\mathcal{A}$ mit Ws $\varepsilon > 2^{-t+1}\ell$ Erfolg hat.
Hinweis: Die Signaturen zu Nachrichten seiner Wahl erzeugt A auf triviale Weise: $\mathcal{A}$ wählt $c \in_R [0, 2^t[$ zufällig und setzt $H(g^y h^{-c}, m) := c$.
Theorem 4 in Pointcheval, Stern, J. Cryptology 13, pp. 361–396, 2000