Prof. C. P. Schnorr Wintersemester 2008/09

Kryptographie

Blatt 8, 05.12.2008, Abgabe 12.12.2008

Aufgabe 1 Zeige: Wenn das k–Summen Problem über der zyklischen Gruppe $G = \langle g \rangle$ in Zeit T lösbar ist, dann ist das DL–Problem zu $\log_g$ in Zeit O(T) lösbar.

Hinweis: Theorem 2, D. Wagner, Crypto 2002.

Aufgabe 2 Zeige: Die DL–Identifikation nach Okamoto $(P, V)_{\mathrm{Ok}}$ ist perfekt-ZK wenn $2^t = (\log_2 q)^{O(1)}$.

Aufgabe 3 Sei $\mathcal{A}$ ein **aktiver** Angreifer auf $(P, V)_{\mathrm{Ok}}$. Skizziere einen prob. Alg. $\mathrm{AL} : (\mathcal{A}, x_1, x_2) \mapsto \log_{g_1} g_2$ mit $E_w|\mathrm{AL}| = O(|\mathcal{A}|/\varepsilon)$, sofern $\mathcal{A}$ Erfolgsws. $\varepsilon \geq 2^{-t+1}$ hat.
Hinweis: Übertrage den Beweis von Satz 2 zu (P, V).