Prof. C. P. Schnorr Sommersemester 2011

Kryptographie

Blatt 7, 03.06.2011, Abgabe 10.06.2011

Aufgabe 1 Zeige: das Protokoll $(\mathcal{P}^k, \mathcal{V}^k)$ der k-fach sequentiellen DL-Identifikation ist perfekt zeroknowledge falls $2^t = (\log q)^{O(1)}$, d.h. 2^t ist polynomial in der Eingabelänge $\log_2 q$.

Aufgabe 2 Abwehr der MIM Attacke zu $(\mathcal{P}, \mathcal{V})_{\mathrm{DL}}$. Der Prover $\mathcal{P}$ sendet an die email–Adresse emV von $\mathcal{V}$, der Verifier sendet an emP. H ist eine Zufallsfunktion. Welche der folgenden Verifikationen wehrt die MIM–Attacke im ROM ab? Begründe

1. $H(\overline{g}, \mathrm{emV}, \mathrm{emP}) = H(g^y h^{-c}, \mathrm{emV}, \mathrm{emP})$,

2. $H(\overline{g}, \mathrm{emV}) = H(g^y h^{-c}, \mathrm{emV})$,

3. $H(\overline{g}, \mathrm{emP}) = H(g^y h^{-c}, \mathrm{emP})$.

Aufgabe 3 In der parallelen Variante von $(\mathcal{P}^k, \mathcal{V}^k)_{FS}$ werden die Schritte 1, 2, 3, 4 von $(\mathcal{P}, \mathcal{V})_{\mathrm{FS}}$ jeweils k–mal mit unabhängigen Münzwurf durchgeführt, also Schritt 1 k–mal,..., Schritt 4 k–mal.
Zeige: Satz 3.12 gilt auch für die parallele Variante von $(\mathcal{P}^k, \mathcal{V}^k)_{\mathrm{FS}}$.

Satz 3.12. Es gibt einen probabilistischen Algorithmus AL : $(\tilde{\mathcal{P}}, \mathbf{v}, N) \to (c, s_c)$ mit $\mathrm{E}_w \mid \mathrm{AL} \mid = \mathcal{O}(|\tilde{\mathcal{P}}|/\varepsilon)$, sofern $\tilde{\mathcal{P}}$ mit $\mathbf{v}$ Erfolgswahrscheinlichkeit $\varepsilon \geq 2^{-tk+1}$ hat, so dass $c \in \{\pm 1, 0\}^t \backslash \{\mathbf{0}\}$ und $s_c^2 = \prod_{i=1}^t v_i^{c_i}$.

Punktzahl pro Aufgabe 5.