Prof. C. P. Schnorr Sommersemester 2011

Kryptographie

Blatt 8, 08.06.2011, Abgabe 17.06.2011

Aufgabe 1 Erweitere das Protokoll zur Erzeugung blinder Signaturen von Schnorr Signaturen auf Okamoto Signaturen. Zeige, dass das Protokoll blinde Okamoto Signaturen erzeugt.

Aufgabe 2 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. Wende Wagner's 2^t Summen Alg. über $\mathbb{Z}_q$ an, $t = 2$ genügt.
Hinweis: Zu blinden Okamoto-Schnorr Signaturen siehe Seite 5,6 von C.P.Schnorr, Security of Blind Discrete Log Signatutes Against Interative Attacks. http://mi.informatik.uni-frankfurt.de, Publications 2001.

Aufgabe 3 Skizziere Wagners 2^t Summen Algorithmus über $\mathbb{Z}_q$ für beliebige $t \geq 2$.

Punktzahl pro Aufgabe 5.