Prof. C. P. Schnorr Sommersemester 2007

Kryptographie

Blatt 7, 01.06.07, Abgabe 08.06.07

Aufgabe 1 Ein Fälscher will DSA-Signaturen zur Nachricht „Einzugsermächtigung über 100 EURO zugunsten des XYZ-Service Providers“ für viele öffentliche Schlüssel h fälschen. Hierzu benutzt er den vom NIST vorgeschlagenen SHA H, wählt geeignete Parameter $G = \langle g \rangle \subset \mathbb{Z}_p^*$, q und fordert zu jedem h eine DSA-Signatur zu „Testnachricht“.

1. Wie wählt der Fälscher g, q ?
2. Wie gefährlich ist die Attacke ? Gibt es Schutzmaßnahmen ?
3. Warum geht dieser Angriff nicht für Schnorr Signaturen ?

Hinweis: http://www.itl.nist.gov/fipspubs/fip186.htm
Serge Vaudenay: Hidden Collisions on DSS, Crypto 96, LNCS 1109 pp.83-88.
http: //lasecwww.epfl.ch/ vaudenay/

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

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).

Aufgabe 4 Sei $N = p \cdot q$ eine *Blumzahl*, d.h. $p, q = 3 \bmod 4$. Zeige:
Rabin_N: $\mathrm{QR}_N \to \mathrm{QR}_N$, $a \mapsto a^2 \bmod N$ ist ein Isomorphismus.
Hinweis: $-1 \notin \mathrm{QR}_p, -1 \notin \mathrm{QR}_q$.