

Kryptographie

Blatt 7, 27.05.05, Abgabe 03.06.05

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 $g, \langle g \rangle, q$ und fordert zu jedem h eine DSA-Signatur von „Testnachricht“.

1. Wie wählt der Fälscher g, q ?
2. Wie real gefährlich ist die Attacke ?
3. Welche Schutzmaßnahme schlagen Sie vor ?
4. 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.

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

Aufgabe 3 Beweise Satz 2', Kap. 2.2: Beschreibe einen prob. Extraktor $AL : (\tilde{P}, h) \mapsto \log_g h$ zu (P^k, V^k) mit erwarteter Laufzeit $O(|\tilde{P}|/\varepsilon)$, sofern \tilde{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.