Prof. C. P. Schnorr Wintersemester 2008/09

Kryptographie

Blatt 7, 28.11.2008, Abgabe 05.12.2008

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 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.

Aufgabe 3 Präzisiere und analysiere folgenden Lösungsalgorithmus für das 2-Summenproblem über $\{0,1\}^n$:

Verteile die $x_1 \in L_1, x_2 \in L_2$ in $2^{n/2}$ Fächer nach den niedrigsten $n/2$ Bits. Suche die Teil-Kollisionen über $\{0,1\}^{n/2}$ nach Kollisionen über $\{0,1\}^n$ ab. Bilde z.B. $L = \{(x_1, x_2, x_1 \oplus x_2) \mid low_{n/2}(x_1) = low_{n/2}(x_2)\}$.) Zeige:

Für $|L_1| = |L_2| = 2^{n/2}$ geht das Verfahren in $O(2^{n/2})$ arithm. + Adress-Schritten. Ein $\log n$ Faktor für Sortieren tritt nicht auf.