Prof. C. P. Schnorr Sommersemester 2017

Kryptographie

Blatt 5, 24.05.2017, Abgabe 31.05.2017

Aufgabe 1. Seien $X_1, \ldots, X_i, \ldots$ unabh. Zufallsvariable über $\{0,1\}$ mit $\Pr_D[X_i = 1] = \varepsilon$. Zeige für $u := \min\{i \mid X_i = 1\}$ und $k\varepsilon^{-1} \in \mathbb{N}$:

1. $0 < \mathrm{Ws}[u \leq k\varepsilon^{-1}] = 1 - (1-\varepsilon)^{k\varepsilon^{-1}} = 1 - e^{-k} + O(ke^{-k}\varepsilon)$.
2. $0 < e^{-k} - \mathrm{Ws}[u > \varepsilon^{-1}k] = O(ke^{-k}\varepsilon)$.

Benutze dass $0 < e^{\pm 1} - (1 \pm \frac{1}{n})^n = O(\frac{1}{n})$.

Aufgabe 2. Ändere den Extraktionsalgorithmus $\mathrm{AL}(\tilde{P}, h)$ zu $(P,V)_{DL}$ wie folgt ab: In Stufe 2 mache $k \cdot u$ neue Proben zum Auffinden einer zweiten 1 in der durch Stufe 1 fixierten Zeile. Wie hängt die erwartete Laufzeit $E_{w_{\mathrm{AL}}}|\mathrm{AL}|$ von k ab? Für welches k wird sie minimal?

Aufgabe 3. 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 p, g, q ?
2. Wie gefährlich ist die Attacke ? Gibt es Schutzmaßnahmen ?
3. Warum geht dieser Angriff nicht für Schnorr Signaturen ?

Hinweis: Serge Vaudenay: Hidden Collisions on DSS, Crypto 96

Punktzahl pro Aufgabe 5