

Kryptographie

Blatt 10, 18.06.05, Abgabe 25.06.05

Sei $(\mathcal{P}, \mathcal{V})_{OS}$ die Ong-Schnorr Identifikation mit $N = pq$,
 $\mathbf{s} = (s_1, \dots, s_t) \in_R (\mathbb{Z}_N^*)^t$, $\mathbf{v} = (s_1^{2^k}, \dots, s_t^{2^k})$. Siehe Jaeger-Skript 3.1.

Aufgabe 1. Zeige: in $(\mathcal{P}, \mathcal{V})_{OS}$ benötigen P und V jeweils maximal $kt + k$ (im Mittel $\frac{t+2}{2}k$) Multiplikationen/Quadrierungen in \mathbb{Z}_N .

Hinweis: Sei $e_i = \sum_{j=1}^k e_{i,j} 2^{j-1}$, dann beginnt P Schritt 3 mit $\prod_{i=1}^t s_i^{e_i, k}$.

Aufgabe 2. Der Betrüger \tilde{P} zu $(\mathcal{P}, \mathcal{V})_{OS}$ habe Erfolgsws. $\varepsilon \geq 2^{-kt+1}$.

Zeige Prop. 3.1.11, Jaeger-Skript 3.1.:

Es gibt einen prob. Alg. $AL : (\mathcal{P}, \mathbf{v}, N) \mapsto (X, Y, l)$ mit

$Y^{2^k} = X^{2^{k+l}}$, $X, Y \in \mathbb{Z}_N^*$, $Y = Y(\mathbf{v})$, $X = X(\mathbf{s})$, $0 \leq l < k$ und

$E_w |AL| = O(|\tilde{P}|/\varepsilon)$.

Aufgabe 3, 4. Setze zu X, Y von Aufgabe 2: $Z := Y^{2^{k-l-1}}/X^{2^{k-1}}$.

Sei i minimal mit $Z^{2^i} = 1$, $0 \leq i \leq l + 1$. Zeige für $2^k | p - 1$:

Aufg. 3. Für $i \leq 1$ gilt $\text{ggT}(Z \pm 1, N) = \{p, q\}$ mit $\text{Ws} \geq \frac{1}{2}$.

Aufg. 4. Für $i \geq 2$ gilt im Fall $Z^{2^{i-1}} \neq -1$ dass $\text{ggT}(Z^{2^{i-1}} \pm 1, N) = \{p, q\}$.

Wie zerlegt man N im Fall $Z^{2^{i-1}} = -1$?

Hinweis: Die Erfolgsws. ε bezieht sich auf zuf. \mathbf{s} und den Münzwurf von $(\mathcal{P}, \mathcal{V})_{OS}$. Man konstruiert entweder stat. unabh. Quadratw. von $-1 \pmod N$ oder erniedrigt i wie im Jaeger-Skript.