

Übungsblatt 10

Aufgabe 74

mündlich

Ein wesentlicher Nachteil des Lamport-Signaturverfahrens ist die Größe der Schlüssel. In Aufgabe 71 wurde gezeigt, wie die Größe der öffentlichen Schlüssel durch Einsatz einer Hashfunktion reduziert werden kann. Zeigen Sie, wie auch die privaten Schlüssel verkleinert werden können. Verwenden Sie hierfür einen Pseudozufallsgenerator.

Aufgabe 75

mündlich

Betrachten Sie das Pedersen-van-Heyst-Signaturverfahren mit den Parametern $p = 3467$, $\alpha = 4$, $a_0 = 1567$ und $\beta = 514$.

- Bestimmen Sie den zum Signierschlüssel $\hat{k} = (78, 836, 12, 1369)$ gehörigen Verifikationsschlüssel k .
- Berechnen Sie eine Fail-Stop-Signatur y für das Dokument $x = 42$ unter dem Signierschlüssel \hat{k} .
- Verifizieren Sie die Gültigkeit von y für x unter k .
- Geben Sie unter Benutzung von a_0 die Menge $S(k, x, y)$ an.
- Bestimmen Sie den geheimen Signierschlüssel, mit dem die beiden Signaturen

x	y
42	(1118, 1449)
969	(899, 471)

erzeugt wurden.

Aufgabe 76

mündlich

Betrachten Sie das Pedersen-van-Heyst-Signaturverfahren mit den Parametern $p = 5087$, $\alpha = 25$ und $\beta = 1866$, sowie dem von Alice erzeugten Schlüsselpaar (\hat{k}, k) mit $\hat{k} = (144, 874, 1873, 2345)$ und $k = (5065, 5076)$.

- Zeigen Sie, dass $(\hat{k}, k) \in S$ ist.
- Zeigen Sie, dass die Verifikationsbedingung $ver(k, x, y) = 1$ für das Dokument $x = 4785$ und die Signatur $y = (2219, 458)$ erfüllt ist.

- Angenommen, Bob legt als Beweis für seine Behauptung, dass Alice das Dokument $x = 4785$ unterschrieben hat, die Signatur $y = (2219, 458)$ vor. Zeigen Sie, wie Alice das Paar (x, y) dazu benutzen kann, um a_0 zu berechnen.

Aufgabe 77

mündlich

Betrachten Sie den durch $s_i \equiv_m a s_{i-1} + b$ definierten linearen Kongruenzgenerator mit $a \in \mathbb{Z}_m \setminus \{0\}$.

- Zeigen Sie für alle $i \geq 0$: $s_i \equiv_m s_0 a^i + \frac{b(a^i - 1)}{a - 1}$
- Die *Periode* eines linearen Kongruenzgenerators ist die kleinste positive Zahl t mit $z_{i+t} = z_i$ für alle $i \geq 0$.
Zeigen Sie, dass die Periode $t = 1$ ist, falls $s_0 \equiv_m b/(a - 1)$ gilt.
- Zeigen Sie, dass für die Periode $t \leq \text{ord}_m(a)$ gilt.

Aufgabe 78

mündlich

Sei g ein (k, ℓ) -Bitgenerator. Ein (ϵ, i) -previous bit predictor für g ist ein Algorithmus $P: \{0, 1\}^i \rightarrow \{0, 1\}$ mit

$$\Pr_x[P(z_{\ell-i+1} \cdots z_\ell) = z_{\ell-i} \text{ mit } z = g(x)] \geq \frac{1}{2} + \epsilon.$$

- Zeigen Sie, dass wenn es einen (ϵ, i) -previous bit predictor für g gibt, es auch einen ϵ -Unterscheider für g gibt.
- Zeigen Sie, dass wenn es einen ϵ -Unterscheider für g gibt, es auch einen $(\epsilon/\ell, i)$ -previous bit predictor für g gibt (für ein $i \in \{0, \dots, \ell - 1\}$).