Übungsblatt 10

Besprechung der mündlichen Aufgaben am 29. 1. 2021
Abgabe der schriftlichen Lösungen bis 2. 2. 2021, 23:59 Uhr

Aufgabe 60 ***mündlich***

Als Alternative zu FDH kann man auch das »Probabilistic Signature Scheme« (PSS) nutzen. Sei $\mathcal{F} = \{f_k \mid k \in K\}$ wieder eine Familie von Falltür-Permutationen auf der Menge $\{0,1\}^{s+l}$ und $(\hat{k}, k)$ ein Schlüsselpaar mit $f_{\hat{k}} = f_k^{-1}$ sowie g, h Hashfunktionen mit $g : \{0,1\}^s \to \{0,1\}^l$ und $h : \{0,1\}^* \to \{0,1\}^s$. Mit $g_1(x)$ bezeichnen wir die ersten m Bits von $g(x)$, mit $g_2(x)$ die restlichen $l - m$ Bits (wobei $m < l$, z.B. $s = m = 256, l = 4096 - s$). Die Funktion g hat u.a. die Aufgabe den vollen Wertebereich auszunutzen, ähnlich wie h bei FDH.
Zum Signieren einer Nachricht x wird ein Zufallsstring $z \in \{0,1\}^m$ gewählt, dann $w = h(xz)$ berechnet. Weiter sei $z' = g_1(w) \oplus z$ (bitweise xor). Dann gilt:

$$\mathrm{sig}(\hat{k}, x) = f_{\hat{k}}(wz'g_2(w)).$$

(a) Geben Sie an, wie die Verifikation ver funktioniert und zeigen Sie $\mathrm{ver}(k, \mathrm{sig}(\hat{k}, x)) = 1$.

(b) Betrachten Sie den Fall das $\mathcal{F}$ RSA ist und die Funktion `FDH-Invert'`(k, v) aus der Vorlesung. Beschreiben Sie wie sich ein u mit $u^d \equiv_n v$ gewinnen lässt, falls im Falle $i = j$ die Hashanfrage nicht mit v sondern $v_j v \mod n$ beantwortet, wird wobei v_j invertierbar ist und aus $v_j = u_j^e$ mit zufälligem u_j berechnet wurde.

(c) Beschreiben Sie, warum man in `FDH-Invert'`(k, v) nicht alle Hash-Fragen wie in b) beantworten kann.

(d) Skizzieren Sie, wie sich `FDH-Invert'`(k, v) zu einer Prozedur `PSS-Invert'`(k, v) ändern lässt, die v wie in b) in alle (neuen) Hash-Antworten für h integriert und begründen Sie, warum dies bei PSS möglich ist.

(e) Welchen Vorteil hat das Vorgehen in d) für die Erfolgswahrscheinlichkeit von `PSS-Invert'`(k, v)?

Aufgabe 61 ***mündlich***

Betrachten Sie das Chaum-van-Antwerpen-Verfahren mit dem Signierschlüssel $\hat{k} = (467, 4, 101)$ und dem Verifikationsschlüssel $k = (467, 4, 449)$.

(a) Welche verbindliche digitale Signatur ergibt sich für den Text $x = 64$?

(b) Beschreiben Sie den Ablauf des Abstreitungsprotokolls zum Nachweis der Ungültigkeit der Signatur $y = 25$ für den Text $x = 157$, falls Bob die Zufallszahlen $e_1 = 46$, $f_1 = 198$, $e_2 = 123$ und $f_2 = 11$ benutzt.

Aufgabe 62 ***mündlich***

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

(a) Bestimmen Sie den zum Signierschlüssel $\hat{k} = (78, 836, 12, 1369)$ gehörigen Verifikationsschlüssel k.

(b) Berechnen Sie die Signatur $y = sig(\hat{k}, x)$ für den Text $x = 42$.

(c) Verifizieren Sie die Gültigkeit der Signatur y für den Text x mit dem Schlüssel k.

(d) Geben Sie unter Benutzung des geheimen Parameters $a = 1567$ die Menge $S(k, x, y)$ an.

(e) Bestimmen Sie den geheimen Signierschlüssel, mit dem die beiden Signaturen $y = (1118, 1449)$ und $y' = (899, 471)$ für die Texte $x = 42$ und $x' = 969$ erzeugt wurden.

Aufgabe 63 ***10 Punkte***

Betrachten Sie das Pedersen-van-Heyst-Signaturverfahren mit den öffentlichen Parametern $p = 5087$, $\alpha = 25$ und $\beta = 1866$.

(a) Bestimmen Sie den zu dem Signierschlüssel $\hat{k} = (144, 874, 1873, 2345)$ gehörigen Verifikationsschlüssel k.

(b) Angenommen, ein Angreifer legt das Paar (x, y) mit dem Text $x = 4785$ und der Signatur $y = (2219, 458)$ vor. Zeigen Sie, dass dieses Paar die Verifikationsbedingung $ver(k, x, y) = 1$ erfüllt.

(c) Zeigen Sie, dass Alice das Paar (x, y) als Fälschung entlarven kann, indem sie den geheimen Parameter a berechnet.