Humboldt-Universität zu Berlin
Prof. Dr. Johannes Köbler

Übungsblatt 11

Besprechung der mündlichen Aufgaben am 19. 1. 2023
Abgabe der schriftlichen Lösungen bis 24. 1. 2023, 23:59 Uhr

Aufgabe 64 ***mündlich***

Angenommen, Alice signiert mit der Lamport-Signatur zwei Texte x und x', die an l Bitpositionen differieren. Für wie viele verschiedene neue Nachrichten kann der Gegner dann eine gültige Signatur berechnen?

Aufgabe 65 ***mündlich***

Zeigen Sie, dass die Prozedur `FDH-Invert'`(k, v) aus der Vorlesung für einen zufälligen Verifikationsschlüssel k und ein zufälliges $v \in_R U$ mit Wahrscheinlichkeit $\geq \varepsilon/q$ ein f_k-Urbild von v findet, falls `FDH-Fälschung'`(k) für einen zufällig gewählten Verifikationsschlüssel k mit Wahrscheinlichkeit ε ein Paar (x, y) mit $f_k(y) = G(x)$ berechnet und dabei für q Texte x_i den Wert $G(x_i)$ sowie im Fall $x_i \neq x$ evtl. auch die Signatur $sig(\hat{k}, x_i)$ erfragt.
Bemerkung: Modifizieren Sie die Prozedur `FDH-Invert'`(k, v) zu einer Prozedur `FDH-Invert`$^*(k)$ (also ohne Eingabe v), so dass `FDH-Invert`$^*(K)$ und `FDH-Invert'`(K, V) die gleiche Ausgabeverteilung haben und `FDH-Invert`$^*(K)$ mit Wahrscheinlichkeit $\geq \varepsilon/q$ Erfolg hat (also kein Fragezeichen ausgibt).

Aufgabe 66 ***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 FDH-Signaturen sowie die Funktion `FDH-Invert'`(k, v) aus der Vorlesung für den Fall, dass $\mathcal{F}$ RSA ist. Beschreiben Sie wie sich ein u mit $u^e \equiv_n v$ 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 analog die Fragen (an h, g und sig) eines Algorithmus `PSS-Fälschung'`(k) beantwortet und die dabei den Wert v wie in b) in alle (neuen) Hash-Antworten für h integriert. 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 67 ***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 68 ***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.