Humboldt-Universität zu Berlin
Prof. Dr. Johannes Köbler

Kryptologie - SoSe 2018
28. Juni 2018

Übungsblatt 9

Aufgabe 55 ***mündlich***

Zeigen Sie, dass die Prozedur Lamport-Urbild'(v) aus der Vorlesung für ein zufälliges $v \in_R V$ mit Wahrscheinlichkeit $\geq \varepsilon/2\ell$ ein Urbild u mit $f(u) = v$ findet, falls Lamport-Fälschung'(k) ein $(\varepsilon, 1)$-Fälscher für die auf der Basis von f arbeitende one-time Signatur ist.

Bemerkung: Modifizieren Sie Lamport-Urbild'(v) zu einer Prozedur Lamport-Urbild* (also ohne Eingabe), deren Ausgabeverhalten für ein zufälliges $v \in_R V$ mit der von Lamport-Urbild'(v) identisch ist und die mit Wahrscheinlichkeit $\geq \varepsilon/2\ell$ Erfolg hat (also nicht Fragezeichen ausgibt).

Aufgabe 56 ***mündlich***

Bei der Lamport-Signatur wird ein Dokument $x = x_1 \dots x_n \in \{0,1\}^n$ durch die Folge $(u_{(i,x_i)})_{i=1,\dots,n}$ signiert, d. h. durch x wird die Teilmenge $A_x = \{(i, x_i) \mid i = 1, \dots, n\}$ aus der Indexmenge $A = \{1, \dots, n\} \times \{0,1\}$ ausgewählt. Eine Familie $\{A_i \subseteq A \mid i \in I\}$ heißt *Spernersystem* über A, falls für alle $i, j \in I$ gilt: $i \neq j \Rightarrow A_i \not\subseteq A_j$.

(a) Zeigen Sie, dass die Spernereigenschaft notwendig für die Sicherheit der Lamport-Signatur ist.

(b) Bestimmen Sie für $B = \{1, \dots, 2m\}$ ein Spernersystem der Größe $\|I\| = \binom{2m}{m}$.

(c) Benutzen Sie das Spernersystem aus Teilaufgabe (b) für die Konstruktion einer Signatur, deren Signaturlänge gegenüber der Lamport-Signatur um ca. 50% verkürzt ist. Beschreiben Sie hierzu den Signieralgorithmus und die Verifikationsbedingung.
Hinweis: Verwenden Sie die Gleichheit $\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$, um eine injektive Funktion $f\colon \{0,1\}^n \to I$ anzugeben.

(d) Zeigen Sie, dass kein Spernersystem der Größe $\|I\| > \binom{2m}{m}$ über der Grundmenge $B = \{1, \dots, 2m\}$ existiert.

Aufgabe 57 ***mündlich***

Geben Sie eine Variante der Lamport-Signatur an, bei der mehrere Nachrichten signiert werden können. Die Größe der öffentlichen Schlüssel soll nicht linear in der Anzahl der Nachrichten wachsen, sondern nur vom Sicherheitsparameter abhängen. Beweisen Sie die Fälschungssicherheit Ihrer Konstruktion.

Hinweis: Konstruieren Sie einen Baum, dessen Blätter öffentliche Lamport-Schlüssel sind und dessen innere Knoten einen Hashwert über ihre Kinder enthalten.

Aufgabe 58 ***mündlich***

Ein wesentlicher Nachteil des Lamport-Signaturverfahrens ist die Größe der Schlüssel. In Aufgabe 57 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 59 ***10 Punkte***

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).