Humboldt-Universität zu Berlin
Prof. Dr. Johannes Köbler

Übungsblatt 7

Aufgabe 49 ***mündlich***

(a) Falls sich bei der Berechnung einer ElGamal-Signatur der Wert $\delta = 0$ ergibt, muss eine neue Zufallszahl z gewählt werden. Überlegen Sie, wie sich aus einer ElGamal-Signatur (γ, δ) mit $\delta = 0$ und dem öffentlichen Verifikationsschlüssel der geheime Signaturschlüssel berechnen lässt.

(b) Beim DSA muss auch im Fall $\gamma = 0$ eine neue Zufallszahl z gewählt werden. Überlegen Sie, wie aus einer DSA-Signatur (γ, δ) mit $\gamma = 0$ die benutzte Zufallszahl z bestimmt werden kann, und wie sich daraus für ein beliebiges Dokument x eine gefälschte Signatur (γ, δ) mit $\gamma = 0$ erhalten lässt.

Aufgabe 50 ***mündlich***

Wir haben gesehen, dass das ElGamal-Signaturverfahren gebrochen werden kann, wenn die gleiche Zufallszahl z mehrmals verwendet wird. Zeigen Sie, wie ähnliche Angriffe auf das Schnorr-Signaturverfahren, DSA und ECDSA möglich sind.

Aufgabe 51 ***mündlich***

(a) Betrachten Sie folgende Angriffsmöglichkeit auf DSA: Für ein gegebenes Dokument x sei $w = x^{-1} \bmod q$ und $\epsilon \equiv_p \beta^w$. Nehmen Sie an, dass $\gamma, \lambda \in \mathbb{Z}_q^*$ mit

$$\Big((\alpha\epsilon^\gamma)^{\lambda^{-1} \bmod q} \bmod p\Big) \bmod q = \gamma$$

gefunden werden können. Zeigen Sie, dass (γ, δ) für $\delta \equiv_q \lambda x$ eine gültige Signatur für x ist.

(b) Beschreiben sie eine ähnliche Angriffsmöglichkeit auf ECDSA.

Aufgabe 52 ***mündlich***

Sei E die durch $y^2 = x^3 + x + 26$ über $\mathbb{Z}_{127}$ definierte elliptische Kurve mit $\|E\| = 131$ Elementen. Betrachten Sie ECDSA in E mit $A = (2, 6)$ und $m = 54$.

(a) Berechnen Sie den öffentlichen Schlüssel $B = mA$.

(b) Berechnen Sie die Signatur für die Nachricht $x = 10$ unter Verwendung der Zufallszahl $z = 75$.

(c) Prüfen Sie die Verifikationsbedingung für die in (b) berechnete Signatur.

Aufgabe 53 ***mündlich***

Was wären die Folgen, wenn man beim ECDSA-Signaturverfahren Signaturen (γ, δ) mit $\gamma = 0$ oder $\delta = 0$ zulassen würde?

Aufgabe 54 ***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 $A_x = \big\{(i, x_i) \,\big|\, i = 1, \dots, n\big\}$ aus der Indexmenge $A = \{1, \dots, n\} \times \{0, 1\}$ ausgewählt. Eine Familie $\big\{A_i \subseteq A \,\big|\, i \in I\big\}$ 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 55 ***10 Punkte***

Bei der Verifikation einer Signatur im ElGamal-Signaturverfahren (oder einer seiner Varianten) ist es nötig, einen Wert der Form $\alpha^e\beta^d$ zu berechnen. Wenn e und d zufällige ℓ-Bit-Exponenten sind, würde die naheliegende Implementierung durch wiederholtes Quadrieren und Multiplizieren (im Durchschnitt) jeweils $\ell/2$ Multiplikationen und ℓ Quadrierungen benötigen. Das Ziel dieser Aufgabe ist es, $\alpha^e\beta^d$ effizienter zu berechnen.

(a) Beschreiben Sie eine Variante des wiederholten Quadrierens und Multiplizierens, bei der in jeder Iteration höchstens eine Multiplikation nötig ist, wenn das Produkt $\alpha\beta$ schon im Voraus berechnet wurde.

(b) Sei $e = 26$ und $d = 17$. Zeigen Sie, wie Ihr Algorithmus $\alpha^e\beta^d$ berechnet, indem Sie für jede Runde die Exponenten i und j des Zwischenergebnisses $z = \alpha^i\beta^j$ angeben.

(c) Begründen Sie, warum Ihr Algorithmus im Durchschnitt ℓ Quadrierungen und $3\ell/4$ Multiplikationen benötigt, wenn e und d zufällige ℓ-Bit-Zahlen sind.

(d) Schätzen Sie den Geschwindigkeitsgewinn im Vergleich zum ursprünglichen Algorithmus ab, bei dem α^e und β^d unabhängig voneinander berechnet und am Schluss multipliziert werden. Nehmen Sie an, dass Quadrieren und Multiplizieren ungefähr gleich viel Zeit brauchen.