Wolfgang K. Seiler
Tel. 2515

A5, C201

12. November 2013

9. Übungsblatt Elliptische Kurven

Aufgabe 1: *(6 Punkte)*

a) Welche Angriffsmöglichkeiten hat ein Gegner, wenn der Absender beim Verschlüsselungsverfahren von ElGamal für jeden Block dieselbe Zufallszahl verwendet?

b) Gibt es auch Probleme, wenn bei der Unterschrift nach ElGamal zweimal dieselbe Zufallszahl verwendet wird?

Aufgabe 2: *(4 Punkte)*

van Duin hat folgende Variante des Unterschriftenalgorithmus von ElGamal vorgeschlagen: Der Unterschreibende wählt einen Körper $\mathbb{F}_p$, eine elliptische Kurve E darüber, einen Punkt $A \in E(\mathbb{F}_p)$ mit primer Ordnung q sowie als privaten Schlüssel eine Zahl $a \in \{1, 2, \ldots, q-1\}$; er berechnet $B = aA$ und veröffentlicht p, E, q, A und B. Zum Unterschreiben einer Nachricht $m \in \{1, 2, \ldots, q-1\}$ wählt er ein zufälliges $k \in \{1, 2, \ldots, q-1\}$, berechnet $R = kA$ und $t = mk + a \bmod q$; die Unterschrift ist das Tripel (m, R, t).

a) Wie läßt sich diese Unterschrift verifizieren?

b) Vergleichen Sie die Variante mit der klassischen ElGamal Unterschrift!

Aufgabe 3: *(5 Punkte)*

a) (m, R, s) sei eine klassische ElGamal Unterschrift, $f(R)$ sei teilerfremd zur Ordnung q des Basispunkts G, und h sei eine weitere natürliche Zahl mit $\mathrm{ggT}(h, q) = 1$. Zeigen Sie, daß dann auch (m', R', s') mit

$$R' = hR, \quad s' = s \cdot f(R') \cdot f(R)^{-1} \cdot h^{-1} \bmod q \quad \text{und} \quad m' = m \cdot f(R') \cdot f(R)^{-1}$$

als ElGamal Unterschrift akzeptiert wird!

b) Inwieweit gefährdet dies die Sicherheit des Systems?

c) Wie sieht es mit Sicherheitsfragen aus, wenn m ein kryptographisch sicherer Hashwert zu einer Nachricht ist?

Aufgabe 4: *(5 Punkte)*

Bestimmen Sie für die elliptische Kurve E von Aufgabe eins des letzten Übungsblatts mit Basispunkt $(1, 1)$ die ElGamal-Unterschrift unter die Nachricht „3“!

Abgabe bis zum Dienstag, dem 19. November 2013, um 15.25 Uhr