Wolfgang K. Seiler
Tel. 2515

B6, B4.18

11. Mai 2020

9. Übungsblatt Elliptische Kurven

Aufgabe 1: *(5 Punkte)*

Beim Verschlüsselungsverfahren nach Elgamal gibt es bekanntlich Probleme, wenn der Absender für mehrere Blöcke die gleiche Zufallszahl verwendet. Gibt es diese Probleme auch bei Unterschriften nach Elgamal?

Aufgabe 2: *(5 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 unter m ist (R, t).

a) Wie läßt sich diese Unterschrift verifizieren?

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

Aufgabe 3: *(5 Punkte)*

$p = 2^{16} + 3 = 65\,539$ ist eine Primzahl, und die Gleichung $y^2 = x^3 + 3x + 5$ definiert eine elliptische Kurve über $\mathbb{F}_p$.

a) Welche Zahlen lassen sich nach der Methode von Koblitz als Punkte dieser Kurve kodieren?

b) Finden Sie einen Punkt für die Nachricht $m = 100$.

c) Welche Nachricht wird durch den Punkt $(12345, 29272)$ kodiert?

Aufgabe 4: *(5 Punkte)*

Wir arbeiten mit der elliptische Kurve E von Aufgabe 1*c)* des letzten Übungsblatts mit Basispunkt $(0, 1)$ für Elgamal-Unterschriften.

a) Ein Teilnehmer A verwendet den geheimen Schlüssel sechs. Was ist sein öffentlicher Schlüssel?

b) Wie kann er die Nachricht „3“ unterschreiben?

c) Zeigen Sie mit der öffentlich verfügbaren Information, daß diese Unterschrift korrekt ist!

Abgabe bis zum Freitag, dem 15. Mai 2020, um 12.00 Uhr