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?

Lösung: Die verwendete elliptische Kurve sei E, der Basispunkt P, und x sei der geheime Schlüssel. Angenommen, die Nachrichten m_1, m_2 werden mit Hilfe der gleichen Zufallszahl y unterschrieben. Der erste Teil der Unterschrift ist dann in beiden Fällen der Punkt $V = yP$, woran ein potentieller Angreifer erkennt, daß zweimal die gleiche Zufallszahl verwendet wurde. Der zweite Teil ist für m_i die Zahl $s_i = y^{-1}\big((m_i - xf(V)\big) \bmod q$, d.h.

$$s_2 - s_1 = y^{-1}(m_2 - m_1) \quad \text{und} \quad y = \frac{m_2 - m_1}{s_2 - s_1},$$

wobei alle Rechnungen in $\mathbb{F}_q$ ausgeführt werden. Damit ist y bekannt, und $f(V)$ ist ohnehin öffentlich. Mit dieser Information kann dann ein Angreifer den geheimen Schlüssel

$$x = \frac{m_1 - ys_1}{f(V)}$$

berechnen und künftig beliebige Nachrichten im Namen von dessen Besitzer unterschreiben.

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?

Lösung: Für eine korrekte Unterschrift ist $tA = (mk + a)A = mR + B$, und diese Bedingung kann mit öffentlicher Information verifiziert werden.

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

Lösung: Abgesehen von der verschiedenen Bezeichnung der Variablen unterscheiden sich die beiden Verfahren nur in der zweiten Komponente der Unterschrift. van Duins Variante ist etwas einfacher, da keine Inversen in $\mathbb{F}_q$ berechnet werden müssen; anderseits müssen für die Berechnung von Vielfachen von Punkten so viele Divisionen in $\mathbb{F}_p$ durchgeführt werden, daß dies für den Gesamtaufwand praktisch nicht ins Gewicht fällt.

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?

Lösung: Nach KOBLITZ lassen sich Nachrichten m mit $0 \le m < \frac{p}{100}$ verschlüsseln, d.h. $0 \le m \le 654$

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

Lösung: Nach KOBLITZ müssen wir für $j = 0, 1, 2, \ldots$ die Zahlen $x = 100m + j = 10\,000 + j$ betrachten und untersuchen, ob $f(x) = x^3 + 3x + 5$ ein Quadrat in $\mathbb{F}_p$ ist; ist $f(x) = y^2$, können wir den Punkt (x, y) nehmen.

$p \equiv 3 \bmod 2^{16}$, also erst recht modulo vier; wir können daher Quadratwurzeln modulo p, so sie existieren, als Potenzen mit Exponent $e = \frac{1}{4}(p+1) = 2^{14}+1 = 16\,385$ berechnen, d.h. durch vierzehnmaliges Quadrieren gefolgt von einer gewöhnlichen Multiplikation. (Das läßt man natürlich zweckmäßigerweise einen Computer ausführen.) Für $x = 10\,000$ ist $f(x) = 1\,000\,000\,030\,005 \equiv 3956 \bmod p$. Die e-te Potenz davon in $\mathbb{F}_p$ ist 2610 mit Quadrat $61583 \equiv -3956 \bmod p$; somit ist 3956 kein Quadrat in $\mathbb{F}_p$.

$f(10\,001) = 1\,000\,300\,060\,009 \equiv 61\,957 \bmod p$. Die e-te Potenz in $\mathbb{F}_p$ ist 4734, und das Quadrat davon ist 61 957. Somit können wir die Nachricht $m = 100$ beispielsweise durch den Punkt $(10\,001, 4734)$ kodieren.

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

Lösung: Wir müssen einfach die letzten beiden Ziffern der x-Koordinate abschneiden und erhalten $m = 123$.

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?

Lösung: Wie wir auf dem letzten Übungsblatt gesehen haben, bilden die Punkte der Kurve bilden eine zyklische Gruppe der Ordnung sieben, erzeugt beispielsweise vom Punkt $(0, 1)$. Der öffentliche Schlüssel ist daher der Punkt $6P = -P = (0, -1) = (0, 6)$,

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

Lösung: Er wählt zunächst eine Zufallszahl y, z.B. $y = 4$, und berechnet dann als ersten Teil der Unterschrift den Punkt $V = 4P$; wie wir vom letzten Übungsblatt wissen, ist dies gleich $(3, 2)$.

Für den zweiten Teil s der Unterschrift muß zunächst $y^{-1} \bmod 7$ berechnet werden; da $2 \cdot 4 = 8$, ist $y^{-1} = 2$. Somit ist

$$s = y^{-1}\big(m - xf(V)\big) \bmod q = 2(3 - 6 \cdot 3) \bmod 7 = 5\,,$$

wenn wir für die Funktion f die x-Koordinate, aufgefaßt als Element von $\{0, 1, 2, 3, 4\}$, wählen. Die Unterschrift ist also $\big((3, 2), 5\big)$.

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

Lösung: Dazu muß die Gleichung $f(V)U + sV \equiv mP$ verifiziert werden. Dabei ist U der öffentliche Schlüssel, den wir in *a)* als $(0,6)$ berechnet haben, $V = (3,2)$, $s = 5$ und $m = 3$. Üblicherweise muß man nun mit der Addition- und der Verdoppelungsformel arbeiten; da wir auf dem letzten Übungsblatt aber *de facto* das diskrete Logarithmenproblem zur Basis $(0,1)$ auf E gelöst haben, können wir die Rechnung zurückführen auf Additionen in $\mathbb{Z}/7$: Die zu überprüfende Gleichung ist

$$3 \cdot (0,6) + 5 \cdot (3,2) = 3 \cdot (0,1) .$$

$(0,6) = -P$, d.h. $3 \cdot (0,6) = -3P = 4P = (3,2)$ und

$$(3,2) + 5 \cdot (3,2) = 6 \cdot (3,2) = -(3,2) = (3,3) .$$

Das ist nach der Tabelle vom letzten Übungsblatt in der Tat gleich $3P$, so daß die Unterschrift akzeptiert wird.