Hochschule Bonn-Rhein-Sieg

Angewandte Kryptographie 2, SoSe 2024

Vorlesungsteil “Kryptographie mit elliptischen Kurven”
Guntram Wicke (guntram.wicke@lehrbeauftragte.h-brs.de)

2 Ergänzung zu Kapitel 2 (“Background on Elliptic Curves, Computation with Group Elements”)

2.1 Herleitung der Formeln zur Punktaddition auf elliptischen Kurven über $GF(p)$

1. Ausgangssituation: 3 verschiedene Punkte $P = (x_1, y_1)$, $Q = (x_2, y_2)$ und $R = (x_3, y_3)$ der elliptischen Kurve seien kolinear, d.h. sie liegen nicht nur auf der Kurve, sondern auch gemeinsam auf einer Geraden.

2. Dann gelten für diese Punkte zwei Gleichungen “gleichzeitig”, d.h. wir haben ein Gleichungssystem aus Geradengleichung (mit Steigung s) und der Gleichung für die elliptische Kurve :

$$y = sx + n$$

$$y^2 = x^3 + ax + b$$

3. Durch Einsetzen der ersten in die zweite Gleichung eliminieren wir y und erhalten:

$$(sx + n)^2 = x^3 + ax + b$$

4. Umformen ergibt

$$x^3 + ax + b - (s^2x^2 + 2sxn + n^2) = 0$$

5. Die x-Koordinaten der drei Punkte sind also Lösungen (Nullstellen) einer kubischen Gleichung. Für die Nullstellen kann man daher schreiben

$$(x - x_1)(x - x_2)(x - x_3) = x^3 - s^2x^2 + ax - 2sxn - n^2 + b = 0$$

6. Ausmultiplizieren bzw. Ausklammern ergibt

$$x^3-x^2x_1-x^2x_2-x^2x_3+xx_1x_2+xx_1x_3+xx_2x_3-x_1x_2x_3 = x^3-s^2x^2+x(a-2sn)-n^2+b$$

7. Zusammenfassen der Terme mit gleichen Potenzen in x erlaubt einen Koeffizientenvergleich:

$$x^3-(x_1 + x_2 + x_3)x^2+(x_1x_2+x_1x_3+x_2x_3)x-x_1x_2x_3 = x^3-s^2x^2+x(a-2sn)-n^2+b$$

8. Für die Addition zweier gegebener Punkte $P = (x_1, y_1)$ und $Q = (x_2, y_2)$ ist zunächst der Zwischenpunkt $R = (x_3, y_3)$ auf der Geraden gesucht. Die Steigung s (engl. slope) der Geraden ergibt sich bei zwei gegeben Punkten der Gerade aus dem Differenzenquotienten:

   $$s = \frac{y_2 - y_1}{x_2 - x_1}$$

   Den y-Achsenabschnitt n (eng. intercept) erhalten wir dann durch Einsetzen eines gegebenen Punktes in die Geradengleichung:

   $$n = y_1 - sx_1$$

9. Aus $x_1 + x_2 + x_3 = s^2$ erhalten wir durch Umstellen die x-Koordinate des gesuchten Zwischenpunktes:

   $$x_3 = s^2 - x_1 - x_2$$

10. Die entsprechende y-Koordinate erhalten wir durch Einsetzen in die Geradengleichung:

    $$y_3 = sx_3 + n = sx_3 + (y_1 - sx_1) = s(x_3 - x_1) + y_1$$

11. Für die Punktaddition ist der Zwischenpunkt noch an der x-Achse zu spiegeln:

    $$P + Q = -R = (x_3, -y_3) = (s^2 - x_1 - x_2, s(x_1 - x_3) - y_1)$$