Gregor Leander
23.06.2008

Fakultät für Mathematik
Ruhr-Universität Bochum

Kryptographie II – Übungsblatt 10

Aufgabe 1 *Nicht Degenerierte Pairings* 10 Punkte

Seien Gruppen G_1 und G_2 mit $|G_1| = |G_2| = p$, p prim, sowie eine bilineare Abbildung

$$e : G_1 \times G_1 \to G_2$$

gegeben. Wie üblich notieren wir die erste Gruppe additive und die zweite multiplikativ. Zeigen Sie, dass folgende Aussagen äquivalent sind.

1. $P \neq 0 \;\Rightarrow\; e(P,P) \neq 1$
2. $\exists P \neq 0,$ so dass $\; e(P,P) \neq 1$
3. $e(P,Q) = 1 \;\forall Q \quad \Rightarrow\; P = 0$

Lösung: Wir zeigen

$$1) \Rightarrow 2) \Rightarrow 3) \Rightarrow 1)$$

und damit die Äquivalenz.

1. 1) $\Rightarrow$ 2) : Das ist klar, denn wenn für alle $P \neq 0$ gilt, dass $e(P,P) \neq 1$, dann braucht man für 2) nur so eines zu wählen.
2. 2) $\Rightarrow$ 3) : Wir nehmen 2) an, also gibt es ein $P' \neq 0$ so dass $e(P',P') \neq 1$ gilt. Wir müssen zeigen, das
$$e(P,Q) = 1 \;\forall Q \quad \Rightarrow\; P = 0$$
gilt. Dies ist gleichbedeutend mit
$$P \neq 0 \Rightarrow \exists Q \text{ mit } e(P,Q) \neq 1.$$
Sei also $P \neq 0$ gegeben. Da $|G_1|$ prim ist damit P ein Erzeuger. Aus dem selben Grund ist P' aus unserer Annahme ein Erzeuger. Damit gibt es eine $a \in \mathbb{N}$ mit
$$P = aP'$$
und $a \neq 0 \bmod p$. Sei nun $Q = P'$ dann gilt
$$e(P,Q) = e(aP',P') = e(P',P')^a.$$
Nach Annahme ist $e(P',P') \neq 1$ und damit wieder ein Erzeuger in G_2 (da $|G_2| = p$ prim ist). Damit ist auch $e(P,Q) = e(P',P') \neq 1$.

3. 3) $\Rightarrow$ 1) Wir nehmen an dass

$$e(P,Q) = 1 \ \forall Q \quad \Rightarrow \ P = 0$$

gilt. Sei nun ein $P \neq 0$ gegeben. Dann gibt es ein $Q \neq 0$ so dass $e(P,Q) \neq 1$. Da Q wieder ein Erzeuger ist, gilt $P = aQ$ für ein geeignetes $a \neq 0 \bmod p$. Damit ist

$$e(P,Q) = e(P,P)^a \neq 1.$$

und damit ist auch $e(P,P) \neq 1$ was zu zeigen war.

Aufgabe 2 *Noch ein Pairing* 10 Punkte

Sei q prim und sei $G_1 = (\mathbb{Z}_p, +)$ und G_2 eine Untergruppe von $(\mathbb{Z}_q^*, *)$ mit Ordnung p. Zeigen Sie, dass die Abbildung

$$\begin{aligned} e : G_1 \times G_2 &\rightarrow G_2 \\ e(x,y) &= y^x \end{aligned}$$

ein Pairing ist. D.h weisen Sie nach, das e

1. bilinear und
2. nicht degeneriert ist.

Nicht degeneriert sei hier wie folgt definiert:

$$e(P,Q) = 1 \ \forall Q \quad \Rightarrow \ P = 0$$

und

$$e(P,Q) = 1 \ \forall P \quad \Rightarrow \ Q = 1.$$

(Siehe dazu auch die erste Aufgabe.)

Lösung:

1. Bilinear: Hier ist zwischen der ersten und der zweiten Komponente zu Unterscheiden. Zuerst die erste Komponente: Sei $a \in \mathbb{N}$ gegeben. Dann gilt

$$e(ax,y) = y^{ax} = (y^x)^a = e(x,y)^a$$

Nun die zweite. Sei $b \in \mathbb{N}$ gegeben. Die zweite Gruppe ist multiplikativ, also rechnen wir

$$e(x,y^b) = (y^b)^x = (y^x)^b = e(x,y)^b.$$

2. Nicht Degeneriert: Sei also zuerst x gegeben mit $e(x, y) = 1$ für alle $y \in G_2$. Dies gilt also insbesondere für einen Erzeuger g von G_2. Damit folgt

$$e(x, g) = g^x = 1$$

Damit muss x die Ordnung von g teilen, d.h. $x = 0 \bmod p$ und damit ist $x = 0$ in G_1.

Sein nun y gegeben mit $e(x, y) = 1$ für alle $x \in G_1$. Insbesondere gilt dies für $x = 1$ und damit folgt

$$e(1, y) = y^1 = y = 1.$$