Übung zur Vorlesung „Sicherheit“
12.06.2014 – Übungsblatt 4

Florian Böhl
florian.boehl@kit.edu

Kummerkasten

- Bei Tafelanschrieben wäre das Tafellicht hilfreich.
- Beim Wischen möglichst nicht mit der zuletzt beschriebenen Tafel anfangen. Das hilft Mitschreibern.

Ok. :)

Sicherheit – Übungsblatt 4 – Aufgabe 1

Aufgabe 1. ElGamal über $\mathbb{G} := Q(\mathbb{Z}_{59}^*) \subseteq \mathbb{Z}_{59}^*$ mit Erzeuger $g := 27$. $ord(g) = |Q(\mathbb{Z}_{59}^*)| = 29 = (59-1)/2$

(a) Berechnen Sie zu dem geheimen Schlüssel $sk := 20$ den öffentlichen Schlüssel pk.

(b) Berechnen Sie das Chiffrat c zu der Nachricht $m := 22$ unter dem in (a) berechneten Schlüssel pk, wobei Sie $r := 12$ als Zufall verwenden.

(c) Es sei $c := (51, 8)$ ein Chiffrat. Verwenden Sie den geheimen Schlüssel aus (a), um die als Gruppenelement codierte Nachricht $m \in \mathbb{G}$ zu berechnen.

Sicherheit – Übungsblatt 4 – Aufgabe 2

Fazit:

- ElGamal-Verschlüsselung geübt
- Rechnen in endlichen Gruppen geübt

Sicherheit – Übungsblatt 4 – Aufgabe 2

Aufgabe 2. $\mathbb{G}$ eine öffentlich bekannte Gruppe primer Ordnung p mit Generator g. Parteien A und B. A kennt Polynom

$$f(x) := \sum_{i=0}^{d} a_i x^i \in \mathbb{F}_p[X]$$

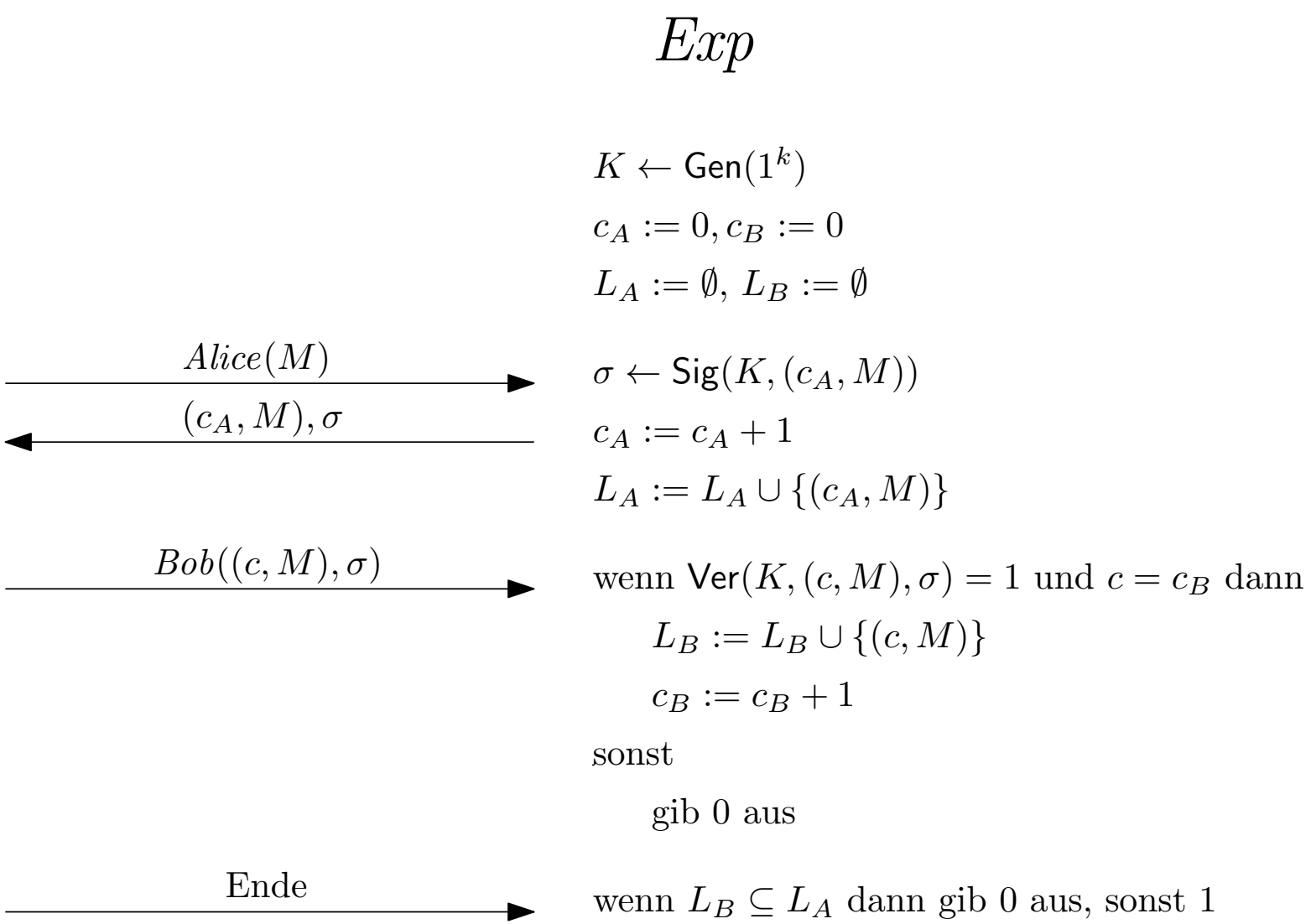
B möchte für Elemente $E \subseteq \mathbb{F}_p$ testen, ob sie Nullstellen von f sind. A will f allerdings nicht preisgeben. Gesucht: Kryptographisches Protokoll auf ElGamal-Basis, das die gewünschte Funktionalität realisiert. A, B verhalten sich „honest but curious“. Kein externer Angreifer. Was erfährt A bei Ihrem Protokoll günstigstenfalls über die Menge E? Was B günstigstenfalls über f? Könnte eine bessere Lösung existieren?

Sicherheit – Übungsblatt 4 – Aufgabe 2

Fazit:

- ElGamal-Verschlüsselung ist
  - Additiv homomorph im Exponenten
  - (Multiplikativ homomorph)
  - Re-Randomisierbar (z.B. nützlich bei elektronischen Wahlverfahren)

Sicherheit – Übungsblatt 4 – Aufgabe 3



Sicherheit – Übungsblatt 4 – Aufgabe 3

Fazit:

- Reduktionistisches Sicherheitsargument: Authentifizierter Kanal aus MAC (und Schlüsselverteilung)
- Nachrichtennummerierung wichtig

Sicherheit – Übungsblatt 4 – Aufgabe 4

Aufgabe 4 Die Jagd auf Doktor Meta.

Organisatorisches

- Nächstes Übungsblatt: 16.6.14 (von Jessi)
- Nächste Übung: 30.6.14 (mit Jessi)