Gregor Leander
7.07.2008

Fakultät für Mathematik
Ruhr-Universität Bochum

Kryptographie II – Lösungsvorschläge zum Übungsblatt 12

Aufgabe 1 *ElGamal ist semantisch sicher* 10 Punkte

Zeigen Sie, dass das ElGamal Verschlüsselungs-Verfahren semantisch sicher ist unter der Annahme das DDH schwer ist.

Lösung: Sei $\mathcal{A}$ ein Algorithmus der die semantische Sicherheit von ElGamal bricht. D.h. nach Eingabe von einem öffentlichen Schlüssel gibt $\mathcal{A}$ zwei Nachrichten m_0 und m_1 aus. Für eine gegebene Verschlüsselung kann $\mathcal{A}$ nun mit einer gewissen Wahrscheinlichkeit $1/2+\epsilon$ entscheiden ob m_0 oder m_1 verschlüsselt wurde. Diesen Algorithmus $\mathcal{A}$ nutzen wir wie folgt um DDH zu lösen. Als Eingabe erhalten wir ein Tupel (g, A, B, C) und sollen entscheiden ob dies ein DH-Tupel ist oder nicht.

1. Wir wir setzen A als den Public Key.
2. Wir starten $\mathcal{A}$ mit Eingabe A.
3. $\mathcal{A}$ gibt zwei Nachrichten m_0 und m_1 aus.
4. Wir wählen zufällig $b_R \in \{0, 1\}$ und berechnen

   $$(B, m_b C)$$

   als Ciphertext und schicken diesen an $\mathcal{A}$.
5. $\mathcal{A}$ gibt ein ein Bit $b' \in \{0, 1\}$ aus.
6. Falls $b = b'$ gilt, dann geben wir "DH-Tupel" aus. Ansonsten geben wir "kein DH-Tupel" aus.

Zur Analyse unterscheiden wir zwei Fälle. Sei zuerst (g, A, B, C) ein DH-Tupel. Dann gibt es $\alpha, \beta \in \mathbb{Z}_p$, so dass $A = g^\alpha$,$B = g^\beta$ und $C = g^{\alpha\beta}$ gilt. Damit ist

$$(B, m_b C) = (g^\beta, (g^\alpha)^\beta m_b) = (g^\beta, A^\beta m_b)$$

eine gültige Verschlüsselung von m_b. In diesem Fall, also falls (g, A, B, C) ein DH-Tupel ist kann damit der Algorithmus $\mathcal{A}$ mit Wahrscheinlichkeit $1/2+\epsilon$ erfolgreich b bestimmen, d.h.

$$\mathcal{P}(b = b' \,|\mathrm{DH}) = 1/2 + \epsilon.$$

Im zweiten Fall, falls (g, A, B, C) kein DH-Tupel ist hat $\mathcal{A}$ keine Information über b denn aus Sicht von $\mathcal{A}$ ist C ein zufälliges Element. Damit kann $\mathcal{A}$ in diesem Fall b nur raten, und da wir b zufällig ausgewählt haben gilt

$$\mathcal{P}(b = b' \ |\text{kein DH}) = 1/2.$$

Damit gilt für die Erfolgswahrscheinlichkeit unserer Reduktion:

$$|\, \mathcal{P}(b = b' \ |\text{DH}) - \mathcal{P}(b = b' \ |\text{kein DH})| = \epsilon$$

Aufgabe 2 *ElGamal ist unsicher gegen adaptive Angriffe* 10 Punkte
Zeigen Sie, dass das ElGamal Verschlüsselungs-Verfahren unsicher gegen CCA-2 Angriffe ist.

Hier nutzen wir, genau wie bei RSA, die Homomorphie aus. Wenn $c = (a, b)$ eine Verschlüsselung für m ist, dann ist $c' = (a, \alpha b)$ eine Verschlüsselung von αm. Man wählt also ein $\alpha \neq 1$ und läßt sich für gegeben Challenge $c = (a, b)$ den Ciphertext $c' = (a, \alpha b)$ entschlüsseln. Eine einfache Division durch α liefert damit den gesuchten Klartext zum Ciphertext c.