Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Ilya Ozerov

Hausübungen zur Vorlesung

Kryptographie II

SS 2013

Blatt 1 /
Abgabe: 26. April 2013, 10 Uhr (vor der Vorlesung), Kasten NA/02

AUFGABE 1 (5 Punkte)**:**

Sei $\mathcal{G}$ ein ppt-Algorithmus, der zur Eingabe 1^n eine zyklische Gruppe G der *primen* Ordnung q und einen Generator g erzeugt, wobei q Bitlänge n hat. Sei zudem das DDH-Problem hart bzgl. $\mathcal{G}$.

Betrachten Sie das folgende Schlüsselaustauschprotokoll:

1) Alice wählt $(g, q) \leftarrow \mathcal{G}(1^n)$, $x \in_R \mathbb{Z}_q^*$, berechnet $\alpha := g^x$ und schickt (g, q, α) an Bob.

2) Bob wählt $y \in_R \mathbb{Z}_q^*$, berechnet $\beta := g^y$, sowie $\gamma_B := \alpha^y$ und schickt β an Alice.

3) Alice berechnet $\gamma_A := \beta^x$, wählt $s, t \in_R \mathbb{Z}_q^*$ mit $s \neq t$ und $\mathrm{ggT}(s, t) = 1$, wählt $z \in_R \mathbb{Z}_q^*$, berechnet $k_A := g^z$, $\sigma := \gamma_A \cdot (k_A)^s$, sowie $\tau := \gamma_A \cdot (k_A)^t$ und schickt (s, t, σ, τ) an Bob.

4) Bob berechnet mit Hilfe des EEA die Bezoutkoeffizienten $u, v \in \mathbb{Z}_q$, so dass $u \cdot s + v \cdot t = 1 \bmod q$ und berechnet $k_B := (\sigma \cdot \gamma_B^{-1})^u \cdot (\tau \cdot \gamma_B^{-1})^v$.

(a) Zeigen Sie, dass Alice und Bob denselben Schlüssel berechnen, d.h. $k_A = k_B$ gilt.

(b) Analysieren Sie die Sicherheit des Protokolls, d.h. beweisen Sie entweder die Sicherheit oder geben Sie einen konkreten Angriff an.

Bitte wenden!

AUFGABE 2 (5 Punkte)**:**

Betrachten Sie das Spiel $\widetilde{\mathsf{KE}}$ aus der Präsenzübung, die zugehörige Definition eines *stark sicheren* Schlüsselaustauschprotokolls, sowie das Spiel KE und die Definition eines *sicheren* Schlüsselaustauschprotokolls aus der Vorlesung.

Zeigen Sie nun: Jedes *sichere* Schlüsselaustauschprotokoll Π ist auch *stark sicher*.

AUFGABE 3 (5 Punkte)**:**

Sei $\mathcal{G}$ ein ppt-Algorithmus, der zur Eingabe 1^n eine zyklische Gruppe G der Ordnung q und einen Generator g erzeugt, wobei q Bitlänge n hat. Wir definieren das *Square Diffie-Hellman Problem*, kurz SQDH-Problem bzgl. $\mathcal{G}$ wie folgt: Das SQDH-Problem ist hart bzgl. $\mathcal{G}$, falls für jeden ppt-Algorithmus $\mathcal{A}$ gilt

$$\mathsf{Ws}\left[\mathcal{A}(g, q, g^a) = g^{(a^2)}\right] \leq \mathsf{negl}(n)$$

Hierbei wird die Wahrscheinlichkeit über die zufällige Wahl von $(g, q) \leftarrow \mathcal{G}(1^n)$ und $a \in_R \mathbb{Z}_q^*$ sowie $\mathcal{A}$'s Münzwürfe gebildet.

Zeigen Sie: Wenn das SQDH-Problem hart ist bzgl. $\mathcal{G}$, so ist es auch das CDH-Problem.

Hinweis: Beachten Sie, dass ein Angreifer $\mathcal{A}'$ für das CDH-Problem als Eingabe g^x und g^y für *unabhängig gleichverteilte* $x, y \in_R \mathbb{Z}_q^*$ benötigt!

AUFGABE 4 (5 Punkte)**:**

Sei $\mathcal{G}$ ein ppt-Algorithmus, der bei Eingabe 1^n eine n-Bit Primzahl p ausgibt, welche die zyklische Gruppe $\mathbb{Z}_p^*$ definiert, sowie einen Generator g für $\mathbb{Z}_p^*$.

Zeigen Sie, dass das DDH-Problem nicht hart bzgl. $\mathcal{G}$ ist.

Hinweis: Es kann effizient (in Zeit polynomiell in n) entschieden werden, ob ein $a \in \mathbb{Z}_p^*$ quadratischer Rest modulo p ist.