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

Präsenzübungen zur Vorlesung

Kryptographie II

SS 2013

Blatt 1 / 19. April 2013

AUFGABE 1:

Wir betrachten eine Modifikation $\widetilde{\mathsf{KE}}$ des KE-Spiels aus der Vorlesung. Der Angreifer $\widetilde{\mathcal{A}}$ erhält die Challenge $(\mathsf{trans}, K_b, K_{1-b})$ anstelle von (trans, K_b), d.h. $\widetilde{\mathcal{A}}$ bekommt den korrekt erzeugten *und* den zufällig gewählten Schlüssel als Eingabe und muss entscheiden, in welcher Reihenfolge er diese erhalten hat.

$\widetilde{\mathsf{KE}}_{\widetilde{\mathcal{A}},\Pi}(n)$		$\widetilde{\mathcal{A}}$
$(\mathsf{trans}, K_0) \leftarrow \Pi(1^n)$		
$b \in_R \{0,1\}$		
$K_1 \in_R \{0,1\}^n$	$\xrightarrow{(\mathsf{trans}, K_b, K_{1-b})}$	
	$\xleftarrow{b'}$	$b' \in \{0,1\}$
Ausgabe: $= \begin{cases} 1, & b = b' \\ 0, & \text{sonst} \end{cases}$		

Definition: Ein Schlüsselaustauschprotokoll Π heißt *stark sicher* gegen passive Angriffe, falls für alle ppt-Angreifer $\widetilde{A}$ gilt, dass $\mathsf{Ws}[\widetilde{\mathsf{KE}}_{\widetilde{A},\Pi}(n) = 1] \leq \frac{1}{2} + \mathsf{negl}(n)$.

Wir wollen nun hier und in der Hausübung zeigen, dass ein Schlüsselaustauschprotokoll Π *sicher* ist, genau dann wenn es *stark sicher* ist.

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

AUFGABE 2:

Betrachten Sie das folgende Schlüsselaustauschprotokoll:

1) Alice wählt $k, r \in_R \{0,1\}^n$ und sendet $s := k \oplus r$ an Bob.
2) Bob wählt $t \in_R \{0,1\}^n$ und sendet $u := s \oplus t$ an Alice.
3) Alice berechnet $w := u \oplus r$ und sendet w an Bob.
4) Alice gibt den Schlüssel k aus und Bob berechnet den Schlüssel als $w \oplus t$.

(a) Zeigen Sie, dass Alice und Bob denselben Schlüssel berechnen.

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

AUFGABE 3:

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 schreiben kurz $(g, q) \leftarrow \mathcal{G}(1^n)$.

Zeigen Sie:

(a) Wenn das DDH-Problem hart ist bzgl. $\mathcal{G}$, so ist es auch das CDH-Problem.

(b) Wenn das CDH-Problem hart ist bzgl. $\mathcal{G}$, so ist es auch das DL-Problem.