Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Alexander Meurer, Felix Heuer

RUHR UNIVERSITÄT BOCHUM RUB

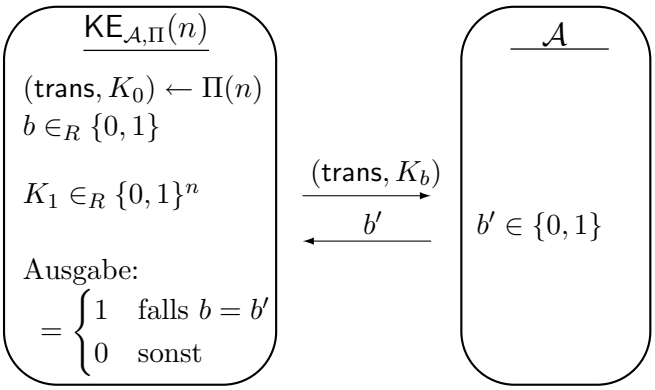
Hausübungen zur Vorlesung

Kryptographie 2

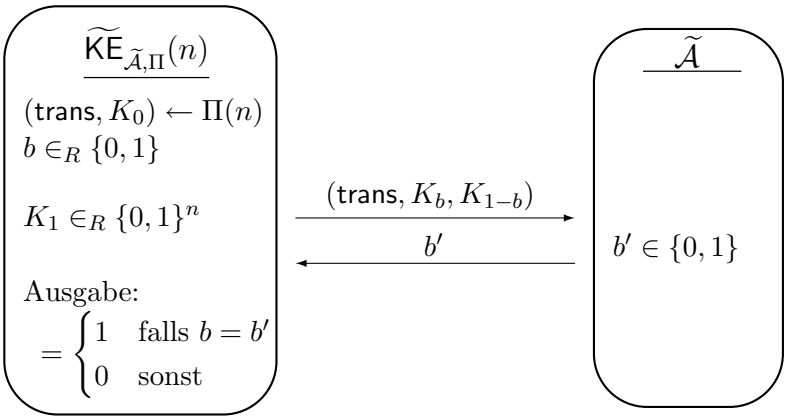
SS 2011

Blatt 1 / 13. April 2010 / Abgabe 20. April, 10:00 Uhr, Kasten NA 02

AUFGABE 1. Definitinossache. (8 Punkte)
Wir erinnern uns kurz an das Spiel für ein Schlüsselaustausch-Protokoll Π:



Wir ändern diese Definition nun wie folgt ab: 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. Wir betrachten also das modifizierte Spiel $\widetilde{\mathsf{KE}}_{\widetilde{\mathcal{A}},\Pi}(n)$:



Zeigen Sie, dass die beiden Definitionen äquivalent sind, d.h. konstruieren Sie aus einem Angreifer $\widetilde{\mathcal{A}}$ bzgl. $\widetilde{\mathsf{KE}}_{\widetilde{\mathcal{A}},\Pi}(n)$ einen Angreifer $\mathcal{A}$ für $\mathsf{KE}_{\mathcal{A},\Pi}(n)$ und umgekehrt. Analysieren sie den Vorteil.

AUFGABE 2. Gruppendiskussion. (7 Punkte)
Sei $G = \{1, g, g^2, \ldots, g^{2m-1}\}$ eine zyklische Gruppe mit Generator g von gerader Ordnung $\text{ord}(g) = 2m$. Zeigen Sie:

a) $\text{dlog}_g(h) \equiv 0 \bmod 2 \Leftrightarrow h \in G^2 := \{x \in G : x = y^2 \text{ für ein } y \in G\}$

b) Die Abbildung $f_g : G \to \{0, 1\}$ definiert als $h \mapsto \text{dlog}_g(h) \bmod 2$ ist mit $\mathcal{O}(\log m)$ Multiplikationen berechenbar.

Hinweis: Definieren Sie hierzu eine Abbildung $J : G \to \{1, g^m\} \subset G$ mittels $J(x) := x^m$ und zeigen Sie $J(x) = 1 \Leftrightarrow x \in G^2$. Benutzen Sie außerdem, dass die Exponentiation x^m in G mit $\mathcal{O}(\log m)$ Multiplikationen durchgeführt werden kann (via Square-and-Multiply).

c) Berechnen Sie $f_2(5) = \text{dlog}_2(5) \bmod 2$ in $G := \mathbb{Z}_{71}^*$.

AUFGABE 3. Diffie-Hellman Variante. (5 Punkte)
Sei $\mathcal{G}$ ein Algorithmus, der eine zyklische Gruppe der Ordnung q und einen Generator g erzeugt, wobei q Bitlänge n hat. Wir definieren das *Square Diffie-Hellman Problem*, kurz SQDH-Problem, bezüglich $\mathcal{G}$ wie folgt: Das SQDH-Problem ist hart bzgl. $\mathcal{G}$, falls für jeden ppt-Algorithmus $\mathcal{A}$ gilt

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

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

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

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!