Extrablatt Reduktionsbeweise

Kryptographie 2

SS 2011

Definition 1. Eine **Hashfunktion** Π ist ein Paar $\Pi = (\mathsf{Gen}, H)$ von ppt-Algorithmen mit

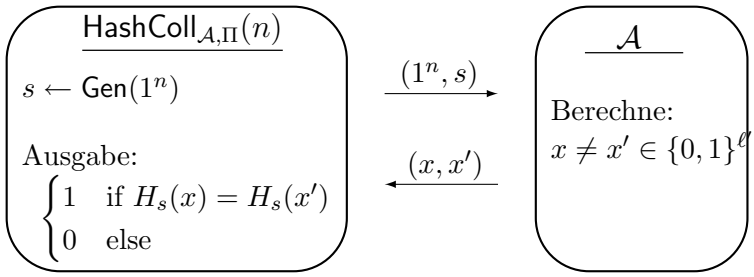
- Gen erzeugt zum Sicherheitsparameter 1^n einen Index s (dieser beschreibt eine Funktion H_s). Gen ist probabilistisch.
- H berechnet für jedes s eine Abbildung $H_s : \{0,1\}^{\ell'} \to \{0,1\}^{\ell}$ mit $\ell' > \ell$. H_s ist deterministisch.

Eine Hashfunktion Π heißt **kollisionsresistent** , wenn für alle ppt-Angreifer $\mathcal{A}$ gilt, dass

$$\mathbf{Pr}\left[\mathsf{HashColl}_{\mathcal{A},\Pi}(n) = 1\right] \leq \mathrm{negl}(n) \ .$$

Hierbei ist das Spiel $\mathsf{HashColl}_{\mathcal{A},\Pi}$ definiert wie folgt:

- $s \leftarrow \mathsf{Gen}(1^n)$
- $(x, x') \leftarrow \mathcal{A}(s)$
- $\mathsf{HashColl}_{\mathcal{A},\Pi}(n) = \begin{cases} 1 & \text{falls } H_s(x) = H_s(x') \text{ und } x \neq x' \\ 0 & \text{sonst} \end{cases}$



AUFGABE 1. Kollisionsresistenz.
Sei $\widetilde{\Pi} = (\widetilde{\mathsf{Gen}}, g)$ mit $g_s : \{0,1\}^{2\ell} \to \{0,1\}^{\ell}$ eine kollisionsresistente Hashfunktion. Konstruieren Sie $\Pi = (\mathsf{Gen}, h)$ durch $h_s(x) := (x_1, g_s(x_2)$ mit $x_1 \in \{0,1\}^{\ell}$ und $x_2 \in \{0,1\}^{2\ell}$. Beweisen Sie, dass Π kollisionsresistent ist, indem Sie aus einem Angreifer $\mathcal{A}$ für Π einen Angreifer $\widetilde{\mathcal{A}}$ für $\widetilde{\Pi}$ konstruieren.

AUFGABE 2. Diskreter Logarithmus.
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 $(G, g, q) \leftarrow \mathcal{G}(1^n)$.

Zeigen Sie: Wenn CDH hart ist bzgl. $\mathcal{G}$, so ist auch das *diskrete Logarithmus Problem* DLog (siehe Folie 15) hart bzgl. $\mathcal{G}$.