



Präsenzübungen zur Vorlesung
Kryptographie II
SS 2013
Blatt 5 / 21. Juni 2013

AUFGABE 1:

Sei $\Pi' = (\text{Gen}', \text{Samp}, f, \text{Inv})$ eine Familie von Trapdoor Einwegpermutationen und hc ein Hardcoreprädikat für Π' . Wir konstruieren daraus folgendes asymmetrische Verfahren $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ für Nachrichten $m \in \{0, 1\}$.

$\text{Gen}(1^n) : (I, \text{td}) \leftarrow \text{Gen}'(1^n)$. Gib $\text{pk} = I$ und $\text{sk} = \text{td}$ zurück.

$\text{Enc}_{\text{pk}}(m) : \text{Wähle ein } x \in_R \mathcal{D}_I, \text{ so dass } \text{hc}_I(x) = m \text{ und gib den Chiffretext } c := f_I(x) \text{ zurück.}$

- Begründen Sie, dass die Verschlüsselung in (erwarteter) Polynomialzeit berechnet werden kann.
- Geben Sie eine effiziente Entschlüsselungsfunktion an und zeigen Sie die Korrektheit.
- Zeigen Sie, dass Π CPA-sicher ist.

AUFGABE 2:

Sei $A_N := \{(a, 1) \in \mathbb{Z}_N \times \mathbb{Z}_N^* \mid a \in \mathbb{Z}_N\}$. Zeigen Sie, dass es *nicht* schwer ist zu unterscheiden, ob ein Element $y \in_R \mathbb{Z}_{N^2}^*$ oder $y \in_R A_N$ ist.

Bitte wenden!

AUFGABE 3:

Sei $H : \{0, 1\}^n \rightarrow \{0, 1\}^{\ell(n)}$ ein Random Oracle. Zeigen Sie:

- (a) Für $\ell(n) = 2n$ verhält sich H wie ein Pseudozufallsgenerator.
- (b) Für $\ell(n) = n$ verhält sich H wie eine Einwegfunktion.
- (c) Für $\ell(n) = n/2$ verhält sich H wie eine kollisionsresistente Hashfunktion.

AUFGABE 4:

Sei $\Pi_f = (\text{Gen}, \text{Samp}, f_I)$ mit $f_I : \{0, 1\}^n \rightarrow \{0, 1\}^n$ eine Einwegpermutationsfamilie. Sei dh ein deterministischer ppt Algorithmus. $\text{dh} : \{0, 1\}^n \rightarrow \{0, 1\}^2$ heißt Doppelhardcoreprädikat für f , falls für alle ppt-Algorithmen \mathcal{A} gilt

$$\text{Ws}[\mathcal{A}(1^n, I, f_I(x)) = \text{dh}(x)] \leq \frac{1}{4} + \text{negl}(n).$$

Sei $\Pi_f = (\text{Gen}, \text{Samp}, f_I)$ eine Familie von Einwegpermutationen und $H : \{0, 1\}^n \rightarrow \{0, 1\}^2$ ein Random Oracle. Zeigen Sie, dass H dann ein Doppelhardcoreprädikat für Π_f ist.