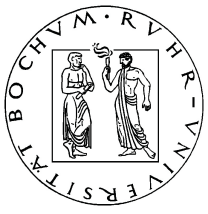
Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Mathias Herrmann



Präsenzübungen zur Vorlesung

Kryptographie 2

SS 2009

Blatt 7 / 22. Juli 2009

AUFGABE 1:
In dieser Aufgabe stellen wird ein Verfahren vorgestellt, welches sicher im Random Oracle Modell ist, aber unsicher wenn das Random Oracle mit SHA-1 instantiiert wird.
Sei Π ein im Standardmodell sicheres Signaturverfahren. Wir konstruieren daraus ein Signaturverfahren Π_y bei dem das Signieren folgendermaßen abläuft: Falls $H(0) = y$ dann gebe den geheimen Schlüssel aus und falls $H(0) \neq y$ dann berechne die Signatur mit Π und gebe diese aus.

1. Zeigen Sie, dass für jeden Wert von y das Verfahren Π_y im Random Oracle Modell sicher ist.

2. Zeigen Sie, dass ein bestimmtes y existiert, für das das Verfahren Π_y nicht sicher ist, wenn das Random Oracle durch SHA-1 instantiiert ist.

AUFGABE 2:
Wir sagen ein Public-Key Verschlüsselungsverfahren $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ ist ein Einwegverfahren falls für jeden ppt. Angreifer $\mathcal{A}$ die Erfolgswahrscheinlichkeit in dem folgenden Spiel nur vernachlässigbar ist:

- $(pk, sk) \leftarrow \mathsf{Gen}(1^n)$
- Eine Nachricht $m \leftarrow \{0,1\}^n$ wird zufällig und gleichverteilt gewählt und $c \leftarrow \mathsf{Enc}_{pk}(m)$ wird berechnet.
- $\mathcal{A}$ erhält den öffentlichen Schlüssel pk und den Chiffretext c und gibt eine Nachricht m' aus. $\mathcal{A}$ gewinnt, falls $m' = m$.

1. Konstruieren Sie aus einem Einwegverfahren ein CPA-sicheres Public-Key Verfahren im Random Oracle Modell.

2. Kann ein Public-Key Verfahren mit deterministischer Verschlüsselungsfunktion ein Einwegverfahren sein? Falls ja, dann geben Sie eine Konstruktion basierend auf einer Komplexitätsannahme an. Falls nein, beweisen Sie dies.