Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Dr. Christopher Wolf
Alexander Meurer, Florian Giesen

RUHR UNIVERSITÄT BOCHUM RUB

Präsenzübungen zur Vorlesung

Kryptographie 2

SS 2010

Blatt 6 / 6. und 7. Juli 2010

AUFGABE 1. Random Oracle Beweise.

a) Betrachten Sie den Beweis zur CPA-Sicherheit von $\mathsf{ROM-RSA}$ (siehe Folien 108 bis 110) und geben Sie an, an welchen Stellen die Eigenschaften von H als Random Oracle benutzt werden.

b) Welche Auswirkungen hat es, wenn wir das Random Oracle H durch einen Pseudozufallsgenerator G ersetzen? Kann man die CPA-Sicherheit weiterhin beweisen oder funktioniert der Beweis nicht mehr? Geben Sie im negativen Fall an, wo genau der Beweis zusammenbricht.

c) Ist die Konstruktion (siehe Folie 107) auch CCA-sicher?

AUFGABE 2. Random Oracle Instanziierung.

Wir erinnern uns an die Konstruktion eines sicheren Message Authentication Codes $\Pi = (\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$ aus Aufgabe 2 vom Hausaufgabenblatt 5: Für Nachrichten der Länge n haben wir $\mathsf{Mac}_k(m) := H(k||m)$ und

$$\mathsf{Vrfy}_k(m, \mathsf{tag}) := \begin{cases} 1 & \text{falls } \mathsf{tag} = H(k||m) \\ 0 & \text{sonst} \end{cases}$$

für einen zufällig gewählten Schlüssel $k \in_R \{0,1\}^n$ definiert.
Zeigen Sie nun, dass diese Konstruktion unsicher ist, wenn wir H durch eine konkrete via *Merkle-Damgård-Transformation* konstruierte Hashfunktion ersetzen.

AUFGABE 3. Gruppentherapie.

Sei $\mathcal{G}$ eine abelsche Gruppe, d.h. je zwei Elemente $x, y \in \mathcal{G}$ kommutieren, d.h. $xy = yx$. Zeigen Sie, dass die Menge der *quadratischen Reste*

$$\mathcal{QR} := \{y \in \mathcal{G} : \exists x \in \mathcal{G} \text{ mit } y = x^2\}$$

eine Untergruppe von $\mathcal{G}$ ist.