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

RUHR UNIVERSITÄT BOCHUM RUB

Präsenzübungen zur Vorlesung

Kryptographie 2

SS 2011

Blatt 6 / 29. Juni / 1. Juli 2011

AUFGABE 1. Malleability.
Zeigen Sie, dass das Pallier Verschlüsselungsverfahren *nicht* CCA-sicher ist, indem Sie einen Angreifer konstruieren.

AUFGABE 2. Verallgemeinerte FDH-Signaturen.
Sei $\Pi_f = (\mathsf{Gen}, \mathsf{Samp}, f, \mathsf{Inv})$ eine Trapdoor-Einwegpermutation. Konstruieren Sie daraus ein Signaturverfahren $\Pi = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$, welches existentiell unfälschbar gegen CMA-Angreifer (siehe Folie 123) im *Random-Oracle Modell* ist. Beweisen Sie die Sicherheit von Π, indem Sie aus einem Fälscher für Π einen Invertierer für Π_f konstruieren.

Hinweis: Orientieren Sie sich bei der Konstruktion und beim Beweis am FDH-RSA Schema (Folie 129).

AUFGABE 3. Doppelter Lamport.
Wir betrachten das Lamport One-Time Signaturschema (Folie 141). Beschreiben Sie einen Angreifer, der Signaturen von zwei Nachrichten seiner Wahl erhält und anschließend Signaturen für beliebige Nachrichten fälschen kann.