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

RUHR UNIVERSITÄT BOCHUM RUB

Hausübungen zur Vorlesung

Kryptographie 2

SS 2011

Blatt 5 / 1. Juni 2011 / Abgabe 22. Juni, 08:30 Uhr, Kasten NA 02

AUFGABE 1. Angriff mit quadratischen Resten. (5 Punkte)
Sei $\mathcal{G}$ ein Polynomialzeitalgorithmus, der zur Eingabe 1^n eine n-Bit Primzahl p und einen Generator g von $\mathbb{Z}_p^*$ ausgibt. Zeigen Sie, dass das DDH-Problem *nicht* hart ist bzgl. $\mathcal{G}$.

Hinweis: Erklären und benutzen Sie, dass man in $\mathbb{Z}_p^*$ effizient testen kann, ob $x \in \mathcal{QR}(\mathbb{Z}_p^*)$ gilt.

Die nächste Aufgabe dient zur Vorbereitung von Aufgabe 3.

AUFGABE 2. Hilfsmittel. (5 Punkte)

a) Sei GenModulus ein ppt-Algorithmus, der zur Eingabe 1^n einen Modul $N = pq$ mit $\log_2 p = \log_2 q = n$ ausgibt. Zeigen Sie, dass wenn die quadratische Residuositätsannahme bzgl. GenModulus gilt, so ist das Unterscheiden von zufällig gewählten Elementen aus $\mathcal{QR}_N$ *oder* $\mathcal{J}_N^{+1}$ hart. Hierbei ist

$$\mathcal{J}_N^{+1} := \left\{ x \in \mathbb{Z}_N^* : \left(\frac{x}{N}\right) = +1 \right\}$$

die Menge aller x mit Jacobi-Symbol $+1$.

b) Sei $N = pq$ für prime, ungerade $p \neq q$. Seien $x \in \mathcal{QR}_N$ und $y \in \mathcal{QNR}_N^{+1}$. Zeigen Sie: $[x^{-1} \bmod N] \in \mathcal{QR}_N$ und $[y^{-1} \bmod N] \in \mathcal{QNR}_N^{+1}$.

AUFGABE 3. Goldwasser-Micali Variante. (5 Punkte)
Betrachten Sie die folgende Variante der Goldwasser-Micali Verschlüsselung: $\mathsf{GenModulus}(1^n)$ liefert (N, p, q), der öffentliche Schlüssel ist N und der geheime Schlüssel (p, q). Um eine 0 zu verschlüsseln, wählt der Sender n zufällige Elemente $c_1, \ldots, c_n \leftarrow \mathcal{QR}_N$. Um eine 1 zu verschlüsseln, wählt der Sender n zufällige Elemente $c_1, \ldots, c_n \leftarrow \mathcal{J}_N^{+1}$. In beiden Fällen ist der Chiffretext $c^* = \langle c_1, \ldots, c_n \rangle$.

a) Zeigen Sie, dass der Sender ein zufälliges Element aus $\mathcal{J}_N^{+1}$ in (erwarteter) Polynomialzeit erzeugen kann.

b) Wie kann der Empfänger effizient den Chiffretext entschlüsseln? Mit welcher Wahrscheinlichkeit tritt dabei ein Entschlüsselungsfehler auf?

c) Zeigen Sie, dass wenn die Quadratische Residuositätsannahme bzgl. $\mathsf{GenModulus}$ gilt, so ist das Schema CPA-sicher.

Hinweis: Ein Unterscheider $\mathcal{D}$ kann seine Challenge z benutzen, um eine Challenge $(c_1, \ldots, c_n)$ für den CPA-Angreifer $\mathcal{A}$ zu berechnen, indem er $x_i \in_R \mathcal{QR}_N$ wählt und $c_i = z^{b_i} x_i$ für ein Challengebit $b_i \in_R \{0, 1\}$ setzt. Für die Reduktion ist es hilfreich, zu begründen, dass in Abhängigkeit von z die c_i entweder in $\mathcal{QR}_N$ oder in $\mathcal{J}_N^{+1}$ *gleichverteilt* sind. Für die Begründung der Gleichverteilung ist Aufgabe 2b) hilfreich.

AUFGABE 4. Rabin Variante. (5 Punkte)
Ziel ist die Konstruktion einer alternativen Rabin Trapdoor-Permutation (wir verzichten auf den Nachweis der Einwegeigenschaft basierend auf der Faktorisierungsannahme) . Sei N eine Blum-Zahl. Definiere eine Menge $S := \{x \in \mathbb{Z}_N^* \mid x < N/2 \text{ und } \left(\frac{x}{N}\right) = 1\}$. Definiere hiermit eine Abbildung $f_N : S \to \mathbb{Z}_N^*$ via

$$f_N(x) := \begin{cases} [x^2 \bmod N] & \text{falls } [x^2 \bmod N] < N/2 \\ [-x^2 \bmod N] & \text{sonst} \end{cases}$$

a) Zeigen Sie, dass f_N eine *Permutation* auf S ist. Zeigen Sie zunächst $f_N(S) \subseteq S$ und begründen Sie, warum f_N surjektiv ist.

b) Konstruieren Sie aus f_N eine Familie von Trapdoor-Permutationen $\Pi = (\mathsf{Gen}, \mathsf{Samp}, f, \mathsf{Inv})$. Geben Sie die Algorithmen konkret an und begründen Sie deren Effizienz.