TECHNISCHE UNIVERSITÄT BERLIN Wintersemester 2004/ 2005
Fakultät II – Institut für Mathematik
Dozent: Prof. Dr. F. HESS
WM: M. WAGNER
www.math.tu-berlin.de/~hess/krypto2

5. Übung Kryptographie II

1. Aufgabe Einheiten in $(\mathbb{Z}/q\mathbb{Z})[X]/(X^N-1)$ (6 Punkte)

Seien $N, q \in \mathbb{N}^{>1}$. Wir betrachten den Ring $R := (\mathbb{Z}/qZ)[X]/(X^N-1)$ und wollen die Einheiten $R^\times$ bestimmen. Ein Element f aus R schreiben wir auch in der Form $f = [f_0, \ldots, f_{N-1}]$ mit $f_i \in \mathbb{Z}/qZ$ $(i = 0, \ldots, N-1)$. Betrachte die Vorschrift

$$\Phi : R \longrightarrow (\mathbb{Z}/q\mathbb{Z}), \quad [f_0, \ldots, f_{N-1}] \longmapsto \sum_{i=0}^{N-1} f_i.$$

(a) Zeige, daß Φ ein wohldefinierter surjektiver Ringhomomorphismus ist und beweise oder widerlege folgende Aussage: $f \in R^\times \Leftrightarrow \Phi(f) \in (\mathbb{Z}/q\mathbb{Z})^\times$

(b) Für $g \in R$ betrachten wir folgenden Ringhomomorphismus

$$\psi : R \longrightarrow R, \quad f \longmapsto g \cdot f$$

und die bezüglich des $\mathbb{Z}/q\mathbb{Z}$-Erzeugendensystemes $\{1, X, X^2, \ldots, X^{N-1}\}$ von R zugehörige $N \times N$-Matrix A mit i-ter Spalte $f_i = [f_{0,i}, \ldots, f_{N-1,i}]^t$ wobei $f_i = g \cdot X^{i-1}$ ist $(i = 1, \ldots, N)$. Widerlege oder beweise:

$$\det A \in (\mathbb{Z}/q\mathbb{Z})^\times \Leftrightarrow g \in R^\times.$$

(c) Schreibe in KASH/KANT einen Algorithmus, der für ein Element $f \in R$ entscheidet, ob es sich um eine Einheit handelt und gegebenfalls das Inverse berechnet.

2. Aufgabe NTRU (6 Punkte)

Implementiere das Kryptosystem NTRU (d.h. Schlüsselerezeugung, Ver- und Entschlüsselung) in KANT/KASH.

Wichtige Befehle: $f \mod g$ berechnet Rest von f bzeüglich g in Quotientenkörper der Koeffizienten von f und $f \mod q$ berechnet alle Koeffizienten von f modulo q, welche im Intervall $[-q/2, \ldots q/2]$ liegen.

3. Aufgabe NTRU-Gitter (4 Punkte)

Gegeben sei der public key $H = [0, -5, -11, 0, 14]$ des NTRU-PKCS mit $N = 5, q = 34, p = 3$. Das NTRU-Gitter wird dann von den Zeilen der folgenden Matrix erzeugt:

$$\left(\begin{array}{ccccc|ccccc} \alpha & 0 & 0 & 0 & 0 & 9 & -1 & 8 & 2 & 16 \\ 0 & \alpha & 0 & 0 & 0 & 16 & 9 & -1 & 8 & 2 \\ 0 & 0 & \alpha & 0 & 0 & 2 & 16 & 9 & -1 & 8 \\ 0 & 0 & 0 & \alpha & 0 & 8 & 2 & 16 & 9 & -1 \\ 0 & 0 & 0 & 0 & \alpha & -1 & 8 & 2 & 16 & 9 \\ \hline 0 & 0 & 0 & 0 & 0 & q & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & q & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & q & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & q & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & q \end{array}\right)$$

wobei einmal $\alpha = 0.51639777$ und $\alpha = 1$ gewählt werden soll. Starte jeweils eine LLL Attacke auf diese Gitter. Wie sieht der private key $(f, g) \in R^2$ aus? Welchen Einfluss hat α auf das NTRU-Gitter?