**TECHNISCHE UNIVERSITÄT BERLIN** WS06/07
**Fakultät II – Institut für Mathematik**
Dozent: Prof. Dr.F. Heß
WM: Dipl.-Math. M. Wagner
`www.math.tu-berlin.de/~hess/krypto-ws2006`

# 14. Übung Kryptographie

## 1. Aufgabe Satz von Blichfeldt (4 Punkte)

Beweise den Satz von Blichfeldt im Fall $S$ kompakt und $\mathrm{vol}(S) = d(\Lambda)$.

## 2. Aufgabe Knapsack (4 Punkte)

Die Paare $AA, AB, \ldots, AZ, BA, \ldots, BZ, \ldots, ZA, \ldots, ZZ$ von Buchstaben werden mit der binären Darstellung der Zahlen $0..26^2 - 1 = 675$ identifiziert. Z.B. entspricht $SO$ dem Bit-String $x_9 \ldots x_0 = 0111100010 = 482 = 18 \cdot 26 + 14$. Nachrichten werden in Blöcke der Länge 2 aufgespalten.

- Der geheime Schlüssel ist $c_9, \ldots c_0, m, w \in \mathbb{N}$ mit $c_{i+1} \geq 2c_i$ für $0 \leq i \leq 8,\ m > \sum_{0 \leq i \leq 9} c_i$ und $\mathrm{ggT}(w, m) = 1$.
- Der öffentliche Schlüssel ist $a_i \equiv wc_i \mod m$ für $i = 0 \ldots 9$.
- Ein Bit-String $x = x_9 x_8 \ldots x_0$ wird verschlüsselt zu $s = \sum_{0 \leq i \leq 9} x_i a_i \in \mathbb{N}$.
- Um zu entschlüsseln berechnet man $t \in \mathbb{N}$ mit $t \equiv w^{-1}s \mod m$ $(0 \leq t < m)$. Dann gilt $t = \sum_{0 \leq i \leq 9} x_i c_i \in \mathbb{N}$ und man berechnet die $x_i$ aus $t$.

(a) Schreibe ein KASH-Programm für obige Ver- und Entschlüsselung und verschlüssele die Nachricht $CRYPTOISFUN$ mit dem vorgegebenen Schlüssel $c_0 = 1,\ c_{i+1} = 2c_i + 1$ für $0 \leq i \leq 8,\ m = 9973$ und $w = 2001$.

(b) Angenommen, wir kennen den öffentlichen Schlüssel

| i | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
|---|---|---|---|---|---|---|---|---|---|---|
| $a_i$ | 3208 | 8694 | 3335 | 1964 | 5982 | 2991 | 6199 | 5741 | 1698 | 8194 |

und fangen folgenden verschlüsselten Text ab:

$$25323, 11402, 18182, 25330, 24037, 11105, 30405, 34024.$$

Versuche mit einer Basisreduktion einige Teile der Nachricht zu entschlüsseln.

## 3. Aufgabe **NTRU-Gitter** **(4 Punkte)**

Gegeben sei der Public Key $H = [0, -5, -11, 0, 14]$ des NTRU-PKCS mit $N = 5, q = 34$ und $p = 3$. 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 dieses Gitter. Wie sieht der Private Key $(f, g)$ aus? Welchen Einfluss hat $\alpha$ aus das NTRU-Gitter?

## 4. Aufgabe **LLL- und Paarreduktion** **(8+12 Punkte)**

(a) Schreiben Sie ein KASH-Programm, daß für eine in Matrixform gegebene Basis eines $\mathbb{Z}$-Gitters $\Lambda \subseteq \mathbb{R}^n$ eine LLL- und Paarreduzierte Basis berechnet.

(b) Vergleichen Sie die Laufzeit beider Reduktionsalgorithmen. Welchen Einfluss hat die Konstante $\delta$ auf die berechnete LLL-reduzierte Basis ?