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

8. Übung Kryptographie II

1. Aufgabe Nearest Plane und das Einbettungsverfahren (8 Punkte)

Implementiere den Nearest Plane Algorithmus und das Einbettungsverfahren in KASH und vergleiche beide Verfahren anhand einiger Beispiele. Versuche anhand einer Tabelle eine heuristische Laufzeitabschätzung beider Algorithmen zu machen.

2. Aufgabe Identitätsbasierte Signaturen (6 Punkte)

Heutzutage ist das Internet mit seinen vielen Möglichkeiten wie z.B. Online-Shopping oder Online-Banking nicht mehr aus unserem Alltag wegzudenken. Dabei ist es z.B. wichtig darauf vertrauen zu können, dass man wirklich mit der Person kommuniziert, von der man es meint und das staatliche Autoritäten nicht zu mächtig sind. Nenne mindestens zwei Möglichkeiten zur Realisierung multipler Trust-Authorities.

3. Aufgabe Babai's Round Off Algorithmus (2 Punkte)

Sei $(b_1, \ldots, b_d)$ die LLL-reduzierte Basis des $\mathbb{Z}$-Gitters Λ. Ferner bezeichne θ_k den Winkel zwischen b_k und dem $\mathbb{R}$-Vektorraum $U_k := \sum_{j \neq k} \mathbb{R} b_j$. Zeige, dass dann für $1 \leq k \leq d$

$$\sin \theta_k \geq \left(\frac{\sqrt{2}}{3} \right)^d$$

gilt.