Prof. C. P. Schnorr Sommersemester 2016

Gitter und Kryptographie

Blatt 11, 01.07.2016, Abgabe 08.07.2016

Zusatzblatt

Zur Arbeit NTRU: A Ring–Based Public Key Cryptosystem, ANTS, 1998

Aufgabe 1. Berechne Schlüssel zum NTRU Kryptoschema: $f \in_R \mathcal{L}(8,7)$, $g \in_R \mathcal{L}(6,6)$, $F_p = f^{-1} \bmod p$, $F_q = f^{-1} \bmod q$, $h = F_q * g \bmod q$ zu $N = 53,\ p = 3,\ q = 64$. Wie gross sind $\sqrt{\#\mathcal{L}(8,7)},\ \sqrt{\#\mathcal{L}(5,5)}$?

Aufgabe 2. Kodiere mit dem öffentlichen Schlüssel h von Aufgabe 1 die Nachricht $m = (1^5, -1^5, 1^5, 0^{38}) \in \{-1,0,1\}^{53}$ zu $e := p\phi * h + m \bmod q$ mit $\phi \in_R \mathcal{L}(5,5)$ und dekodiere e mit dem f von Aufgabe 1.
Ist die notwendige Bedingung $\|f*m+p\phi*g\|_\infty < q$ für korrekte Dekodierung erfüllt?

Aufgabe 3.

1. Berechne $s = \sqrt{\frac{N\alpha q}{\pi e}}$ für $\alpha = \|g\|_2/\|f\|_2$,
   $c_h = \sqrt{\frac{2\pi e||f||_2||g||_2}{Nq}},\ c_m = \sqrt{\frac{2\pi e||m||_2||\phi||_2}{Nq}}$.
2. Wie angreifbar erscheint f und e von m ?
3. Vergleiche $\|(\alpha f, g)\|_2$ mit der unteren Schranke s zu $\lambda_1(\mathcal{L}_{\mathrm{NTRU}})$.
   Gilt $||(\alpha f, g)||_2 \approx s$?

pro Aufgabe 5 Punkte