The art of cryptography: Lattices and cryptography, summer 2013

PROF. DR. JOACHIM VON ZUR GATHEN, DR. DANIEL LOEBENBERGER

11. Exercise sheet
Hand in solutions until Sunday, 07 July 2013, 23:59h.

Exercise 11.1 (Sampling). (13+4 points)

In the lecture we have encountered various distributions. As it will turn out, it is necessary to sample efficiently from some of these to successfully implement Peikert's cryptosystem.

(i) Prove the following [3]

Theorem (Inverse transform sampling). *Let F be a continuous cumulative distribution function with inverse F^{-1} for $u \in [0,1]$ defined by*

$$F^{-1}(u) := \inf\{x \in \mathbb{R} \mid F(x) = u\}.$$

If U is uniformly distributed on $[0,1]$, then $F^{-1}(U)$ follows the distribution F'.

(ii) Write a little program that implements (numerically) inverse transform sampling. [4]

(iii) Sample 1000 values from the Gaussian distribution with $r = 1$ and produce a meaningful plot of your result. [3]

(iv) Do the same for the induced distribution on the torus. What do you observe? [3]

(v) Explain the behavior. [+4]

Exercise 11.2 (Hands on LWE). (10+5 points)

Consider the following system of approximate linear equations over $\mathbb{Z}_{17}$:

$$\begin{aligned}
14s_1 + 15s_2 + 5s_3 + 2s_4 &\approx 8 \pmod{17},\\
13s_1 + 14s_2 + 14s_3 + 6s_4 &\approx 16 \pmod{17},\\
6s_1 + 10s_2 + 13s_3 + 1s_4 &\approx 3 \pmod{17},\\
10s_1 + 4s_2 + 12s_3 + 16s_4 &\approx 12 \pmod{17},\\
9s_1 + 5s_2 + 9s_3 + 6s_4 &\approx 9 \pmod{17},\\
3s_1 + 6s_2 + 4s_3 + 5s_4 &\approx 16 \pmod{17},\\
6s_1 + 7s_2 + 16s_3 + 2s_4 &\approx 3 \pmod{17},
\end{aligned}$$

(i) How would you proceed to find $s \in \mathbb{F}_{17}^4$ if the approximations where equations? [2]

(ii) Find $s \in \mathbb{F}_{17}^4$ that satisfies the system, knowing that each equation is correct up to a small additive error ± 1. Explain detailed your approach. [8]

(iii) Estimate the asymptotic runtime of your solution. [+5]