Implementing Ring-LWE Cryptosystems

Supervised by: Prastudy Fauzi

University of Tartu

September 7, 2016

Introduction: public-key cryptosystems

- RSA-OAEP, ElGamal not secure against quantum computers!
- Alternative: post-quantum cryptosystems
  - Security based on NP-hard problems (in the average case)
  - Example: Ring Learning With Errors (Ring-LWE)*

Question

How efficient are these cryptosystems based on Ring-LWE?

* with correctly chosen parameters

Student's task (M.Sc. or Ph.D.)

- Study the cyclotomic ring $R = \mathbb{Z}[X]/(X^{2^d} + 1)$
- Survey the Ring-LWE assumption using such R
- Find how the above is used in LPR and NTRU
- Implement using NFLlib, and compare to ElGamal and RSA-OAEP (e.g. for 80-bit security)

Cryptosystem	Key size (bits)	Encryption (ms)	Decryption (ms)
RSA	1024	?	?
ElGamal	200	?	?
LPR	?	?	?
NTRU	?	?	?

Table 1: Mock comparison of cryptosystems on a Core i5-6600.