Performance Evaluation of the NTRU Encryption Scheme on an 8-bit AVR Microcontroller

December 3, 2018

Authors:
Adriano Franci
Thibault Simonetto

Academic Supervisor:
Prof. Dr. Jean-Sébastien Coron

Project Supervisor:
Johann Groszschädl

1 Introduction

2 Background

This sections presents the concepts, methodologies and technologies used to produce the implementation and the test evaluation.

2.1 NTRU - Closest latice vector problem

The NTRU algorithm is based on the closest latice vector problem

2.2 Mask Generating Function

2.3 8 bit AVR controller

2.4 Performance testing

3 Implementation & Testing

4 Performance evaluation

5 Conclusion