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

December 4, 2018

Authors:
Adriano Franci
Thibault Simonetto

Academic Supervisor:
Prof. Dr. Jean-Sébastien Coron

Project Supervisor:
Johann Groszschädl

1 Introduction

Today's cryptography for modern communication systems are mostly based on asymmetric cryptography algorithm, known as public-key cryptography.
One of the widely used public-key cryptography algorithm is RSA[1]. It is designed around computational hardness assumption which, in the early 2000s was still provable. However with the introduction of the quantum computers these mathematical hardness has been shown vulnerable as quantum computer are known to be able to break system based on integer factorisation. Thus a new mathematical model should be found that could be proved quantum resistant.
The NTRU crypto-system is such an alternative based on the closest lattice vector problem (described in background section).
Asymmetric cryptography is also a important part of the concept of Internet of Things (IoT). In fact the challenge for such hardware is the possibility for secure communication while keeping the hardware cost very low. Symmetric cryptography is already widely used and proven to be performant and cost efficient for such small controller and limited hardware. But symmetric cryptography do provide a low security scheme.
The NTRU public-key crypto-system main characteristics are the low memory and computational requirements while keeping a high security level in communication thanks to the asymmetric scheme of encryption. This makes the NTRU crypto-system the perfect candidates for being implemented on IoT hardware (*e.g.* 8 bit AVR controller).

In this work we will go trough the different steps of implementation and performance measurement of the NTRUencrypt algorithm on an 8 bit AVR controller. Specially for the mask generating utility function used to provide of a variable length primitive output. And if such implementation can approximate the performance of a standard 64 bit computer.

[1] Rivest-Shamir-Adleman : link?

2 Background

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

2.1 NTRU

NTRU algorithm which is the abbreviation for $N-th$ degree truncated polynomial ring, is the group of lattice based public key encryption schemes.

Such algorithm relies on the hardness of the *Closest Vector Problem* which in turns is a generalisation of the *Shortest Vector Problem.*

This group of algorithm has couple of advantages the well known RSA algorithm. First, the main operation of NTRU relies on the multiplication of polynomials with constant degree (*e.g.* 438 for 128 bit security) on small integer. Which in turns is much less costly that operation for the same level of security using RSA algorithm that relies on modular exponentiation (for 128 bit security level, operation performed on 3072-bit integers). Second, NTRU is more robust with regards to quantum computing than classic RSA.

Furthermore RSA operation are very costly in terms of resource consumption which make it very unlikely to be implemented on resource limited hardware. Thanks to the possibility of efficiency increase of the NTRU algorithm, an implementation of such high security scheme on small and resource critical devices can be considered.

2.2 Mask Generating Function

Our work will be focused on one of the high resource consuming part of the execution of NTRU algorithm which is the mask generating function (MGF). This MGF is used to ensure that a single bit of the output is generated using multiple bit of the input and that and that a good random distribution is output after encryption.

2.3 IoT & Performance Evaluation

One of the main motivation for the optimisation of high-security level crypto-system is the need of such high security for on low powered small device that have spread out on our networks for the previous 10 years. In fact those Internet of Things (IoT) devices already started to take a important part of information gathering as well as processing.

Those devices take the form of very small controller often equipped with low calculation power coupled with limited battery resource.

Recent news have shown that the security in communication on those devices was very low and sometimes not even considered. Because of the difficulty of combining correct security level with limitation on hardware that such device impose.

Thus, progress in the area of efficient implementation of NTRU algorithm for low-power consumption could be a major advancement on the security of IoT devices.

A good performance testing scheme could be a first estimation of the power consumption (which will be approximated with clock cycle) of the optimised time consuming operation (*e.g.* mask generating function) over existing RSA high resource consuming operation. Such benchmark will give us material to argue on the possibility of optimisation of power consumption as well as enhancement of security level for such device.

3 Implementation & Testing

4 Performance evaluation

5 Conclusion