Evaluation of Security Protocols for the Internet of Things

Package 2 Report #3

Lapin

Submitted by:

Anh Le Pham

Sinan Özdemir

Submitted To:

Prof. Frederik Armknecht

Vasily Mikhalev

# 1. Introduction

Lapin is the last protocol based on hard learning problem described in this work. Unlike previous protocols Lapin is provably secure based in a ring variant of the learning parity with noise (Ring-LPN) problem. The author of the paper “Lapin: An Efficient Authentication Protocol Based on Ring-LPN” assumes that their approach is more efficient regarding smaller communication complexity and code size compared to AES-type protocols. These characteristics are suitable for devices with small computational capabilities. In further text the algorithm and the implementation on the Arduino UNO R3 will be explained.

# 2. Lapin Algorithm

# 3. Lapin Implementation on the Arduino UNO R3

# 4. Lapin Evaluation

This last subsection provides the evaluation results of Lapin. This evaluation is based on code size, memory size, computational complexity and the power consumption.

The code size of Lapin is 7664 bytes, which corresponds to 23% of the total capacity. Memory size is 480 bytes this is 23% out of the available 2,048 bytes. Computational complexity is 667 ms.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Protocols | Parameters | Code Size | Memory Size | Computational Complexity | Power Consumption |
| Lapin | secPar = 80  degf = 621  e = 0.166666667  u = 0.29 | 7664 Bytes (23%) | 480 Bytes (23%) | 667 ms | … |