Evaluation of Security Protocols for the Internet of Things

Package 2 Report #2

AUTH, MAC1, MAC2

Submitted by:

Anh Le Pham

Sinan Özdemir

Submitted To:

Prof. Frederik Armknecht

Vasily Mikhalev

# 1. Introduction

Since, the HB and HB+ protocols introduced by Hopper and Blum are insecure against efficient active attacks, several enhancements are made to fix that issue. However, it has been found that these extensions are also insecure. Hence, Kiltz et al. shows a new variant of two-round authentication protocol (AUTH in short) assuming to be secure against active attacks. Kiltz et al. further provides two massage authentication codes (MACs). All mentioned protocols relying on the learning parity with noise problem (LPN). These protocols are referenced from the paper titled “Efficient Authentication from Hard Learning Problems”. In the following subsection the algorithms of the protocols will be explained.

# 2. AUTH, MAC1, MAC2 Algorithms

tbd

AUTH

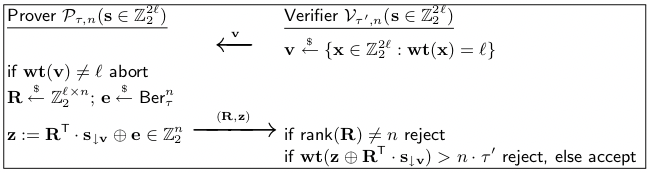
The AUTH protocol shown in Figure 3 was introduced by Kiltz et al. [KPV+17] and represents a two-round authentication protocol secure against active attacks and man-in-the-middle attacks, even in a quantum setting. The security of this protocol relies on the subspace LPN problem which is reducible to LPN.

Figure 3: Two-round authentication protocol AUTH

Whereas the random challenges R ∈ Zl×n (each row of the matrix RT corresponding to one challenge a in HB) were computed by the Verifier V in HB, they are now computed by the Prover P. V instead sends a random vector v ∈ Z2l with Hamming weight wt(v) = l to select l of the 2l key bits 2 of s to produce a key subset s↓v which is derived from s by deleting all bits s[i] where v[i] = 0. Then, z ∈ Zn2 is computed as RT ·s↓v ⊕e and sent to V along with R. V rejects the authentication if either rank(R) ̸= n or if the number of unsuccessful iterations denoted as wt(z ⊕ RT · s↓v ) is greater than the threshold n · τ′ with τ′ = 0.25 + τ/2.

MAC1

tbd

MAC2

# 3. AUTH, MAC1, MAC2 Implementation on the Arduino Uno R3

# 4. AUTH, MAC1, MAC2 Evaluation

In this subsection AUTH and MAC1 will be evaluated in regard to code size, memory size, computational complexity and power consumption

This last subsection provides the evaluation results of the AUTH, MAC1 and MAC2 protocols with different parameters. This evaluation is based on code size, memory size, computational complexity and the power consumption.

The code size of the AUTH protocol is 5492 bytes, which corresponds to 17% of the total capacity. Memory size is 398 bytes this is 23% out of the available 2,048 bytes. Computational complexity is …

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Protocols** | **Parametes** | **Code Size** | **Memory Size** | **Computational Complexity** | **Power Consumption Current at 200mA** |
| **Auth** | n = 48  e = 0.1  l = 96  k = (2\*l)/8 | 5492 Bytes (17%) | 398 Bytes (19%) | 656 ms | 27.9 - 28.3 |
| **MAC1** |  |  |  |  |  |