Post-quantum secure PUF authentication using LPN

Han Zhao, May 1, 2017

Fraunhofer
AISEC

Post-quantum secure PUF authentication using LPN

Post-quantum secure PUF authentication using LPN

Fraunhofer AISEC

Introduction

Concept

LPN: Learning Parity with Noise

1. Randomly select a secret s in GF(2)
2. Randomly select A from GF(2)
3. Select a noise e $\longrightarrow Ber_\epsilon$
4. Output b= $<$ A*s+e $>$ as a sample
   $b_i = A_i{}^*s + e_i \quad \text{mod } 2 \quad$ with i=0,1,...,m

The goal:

Find s given only the values of b and A.

Fraunhofer AISEC

Introduction
Motivation

- Fundamental in theory
  - A close connection to the problem of decoding binary random linear codes.
  - Believed to be hard: no polynomial time algorithm is known.

Motivation
LPN – Problem

1. BKW Algorithm[1]

labeled examples: $2^{\Omega\left(\frac{n}{logn}\right)}$

time consuption: $2^{\Omega\left(\frac{n}{logn}\right)}$

2. Algorithm of Lyubashevsky[2]

labeled examples: $n^{1+\epsilon}$

time consuption: $2^{\Omega\left(\frac{n}{loglogn}\right)}$

3. LF1 Algorithm[3]

labeled examples: polynomial number of trials

time consuption: exponential time

Introduction
Motivation

- Fundamental in theory
  - A close connection to the problem of decoding binary random linear codes.
  - Believed to be hard: no polynomial time algorithm is known.
- Many cryptographic applications in practice
  - User authentication, encryption, etc.
  - Post-quantum cryptography.

Post-quantum secure PUF authentication using LPN

Fraunhofer AISEC

The construction of the authentication system

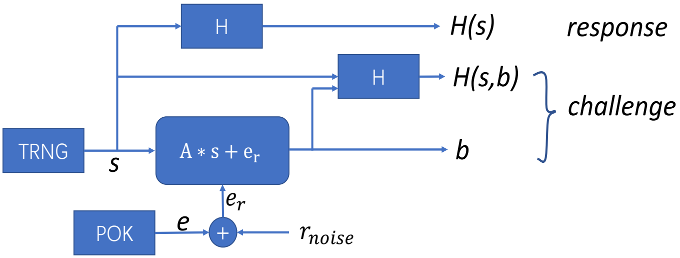
Enrollment phase:

- Collecting response and chanllenge pairs (RCPs)
  - Encoding module

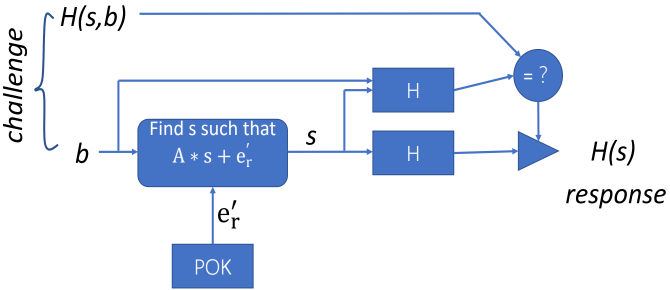
Authentication phase:

- Matching the extracted RCPs with the reference RCPs
  - Decoding module

The construction of the authentication system
Enrollment phase



The construction of the authentication system
Authentication phase



The construction of the authentication system
Authentication phase

Extracting s from the decoding module:

- Gaussian elimination algorithm
- Error correction algorithm

Authentication phase
Error correction codes

Possible Candidates:

Hamming Code

Repetition Code

BCH Code

Reed-Muller Code

LDPC Code

Characteristics:

- the simple construction
- no parity check matrix
- good error correction property

Encoding Algorithm

The Plotkin-Construction[4]

Characterization of RM(r,m) codes with the parameters r and m:

$n = 2^m$

$k = \sum_{i=1}^{r} \binom{m}{i}$

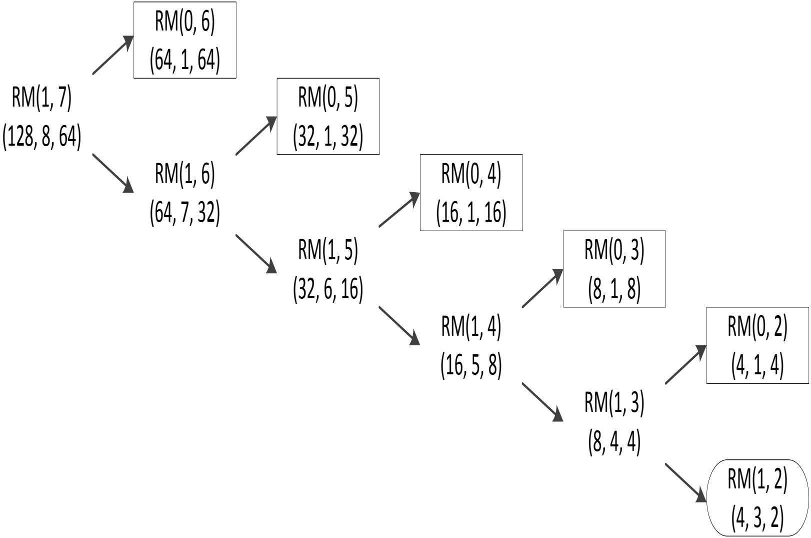
$d = 2^{m\text{-}r}$

Plotkin construction with two subcodes for RM(r,m):

$|u|\ u + v|$: u ϵ RM(r,m-1), v ϵ RM(r-1,m-1)

Reed Muller Code

RM(1,7)



Fraunhofer AISEC

Decoding Algorithm

The Recursive Decoding Algorithm[4]

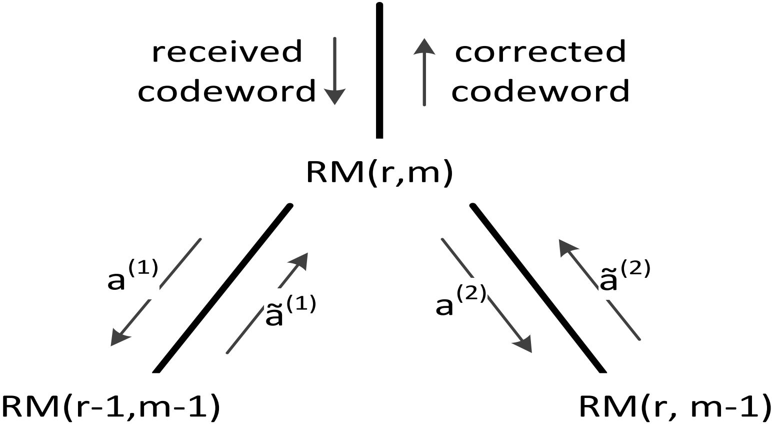
1) SDML-Decoding for Repetition Code or Parity-Check Code

2a) Decoding for the first outer codeword RM(r-1,m-1)

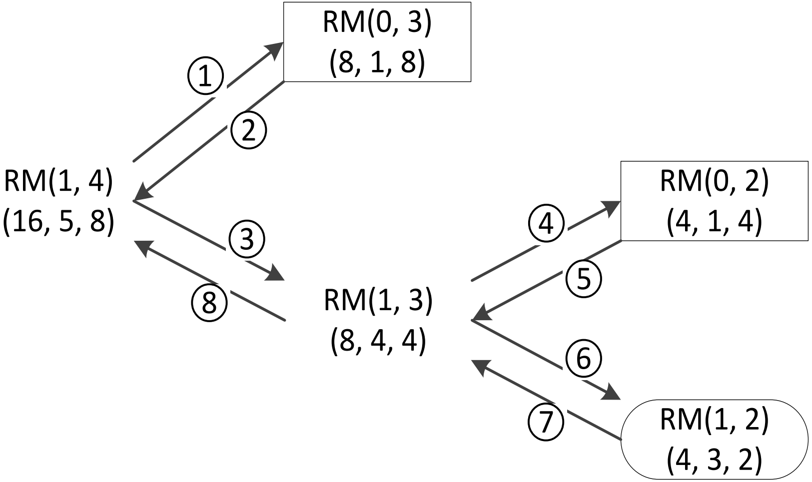
2b) Decoding for the second outer codeword RM(r,m-1)

3) Reconstructing the codeword RM(r,m) with the two subcodes

Decoding Algorithm
The Recursive Decoding Algorithm



Decoding Algorithm
The Recursive Decoding Algorithm



Post-quantum secure PUF authentication using LPN

Fraunhofer AISEC

Conclusion

Trapdoor

Encoding based on PUF-response

The hardness of LPN problem

Hash Function

Decoding with error correction algorithm

Post-quantum secure PUF authentication using LPN

Fraunhofer AISEC

Schedule

WBS	Name	Start	Finish	Work
1	Implementation in software(Python)	May 5	May 12	6d
2	Design the hardware structure of encoder	May 15	May 17	3d
3	Implementation of encoder (VHDL)	May 18	Jun 2	14d
4	Implementation of hash function(VHDL)	Jun 5	Jun 9	5d
5	Design the hardware structure of decoder	Jun 12	Jun 16	5d
6	Implementation of decoder(VHDL)	Jun 19	Jul 21	25d
7	Implementation of the rest part(VHDL)	Jul 24	Aug 4	10d
8	Writing master paper	Jul 10	Sep 1	40d

Post-quantum secure PUF authentication using LPN

Bibliography

[1] A. Blum, A. Kalai, and H. Wasserman, “Noise-tolerant learning, the parity problem, and the statistical query model,” J. ACM, vol. 50, no. 4, pp. 506–519, 2003.
[2] V. Lyubashevsky, “The parity problem in the presence of noise, decoding random linear codes, and the subset sum problem,” in Proc. 8th Int. Workshop Approximation, Randomization Combinatorial Optimization Algorithms Techn., 2005, pp. 378–389.
[3] E. Levieil, and P.-A. Fouque, “An improved LPN algorithm,” in Proc. 5th Int. Conf. Security Cryptography Networks, 2006, pp. 348–359.
[4] Bossert, Martin: Kanalcodierung. 3., überarb. Aufl. München : Oldenbourg, 2013. – XVIII, 531 S. : graph. Darst.. – ISBN 978–3–486–72128–7 – 978–3–486–75516–9

Post-quantum secure PUF authentication using LPN

Discussion

Question?

Post-quantum cryptography

Post-quantum cryptography refers to cryptographic algorithms (usually public-key algorithms) that are thought to be secure against an attack by a quantum computer.
Post-quantum cryptography is distinct from quantum cryptography, which refers to using quantum phenomena to achieve secrecy and detect eavesdropping.
When calculate the subcode of RM-Code, the information-bits s can also be calculated;
the analysis of decoding complexity of RM-Code

Contact Information

Han Zhao

Group Product Protection
Department Security and Trusted OS

Fraunhofer-Institute for
Applied and Integrated Security (AISEC)

Address: Parkring 4
85748 Garching (near Munich)
Germany
Internet: http://www.aisec.fraunhofer.de

Phone: +49 16 25231418
Fax: +49 89 3229986-222
E-Mail: ga84fif@mytum.de