Post-quantum secure PUF authentication using LPN

Han Zhao, May 9, 2017

Fraunhofer

AISEC

Post-quantum secure PUF authentication using LPN

Introduction
- Concept
- Motivation

The construction of the authentication system
- Enrollment phase
- Authentication phase

Conclusion

Schedule

Bibliography

Discussion

Post-quantum secure PUF authentication using LPN

Introduction
- Concept
- Motivation

The construction of the authentication system
- Enrollment phase
- Authentication phase

Conclusion

Schedule

Bibliography

Discussion

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 bit offset e $\longrightarrow Ber_\epsilon$
4. Output b= $<$ A*s+e $>$ as a sample

$$b_i = A_i{}^*s + e_i \mod 2 \quad \text{with i=0,1,...,m}$$

The goal:

Find s given only the values of b and A.

Fraunhofer AISEC

Introduction
Motivation

- Fundamental in theory for LPN
  - Equivalent to decoding random linear codes
  - Believed to be hard

Motivation
LPN – Problem

Solving LPN-Algorithms	Time Complexity(t)	Query Complexity(n)	Example: n=128, ε=0.5
BKW[1]	$2^{\Omega(\frac{n}{log n})}$	$2^{\Omega(\frac{n}{log n})}$	$2^{60.75} / 2^{60.75}$
Lyubashevsky[2]	$2^{\Omega(\frac{n}{log log n})}$	$n^{(1+\varepsilon)}$	$2^{395.42} / 2^{19.80}$
The best algorithm[3]	$2^{\Theta(n)}$	$\Theta(n)$	$2^{128} / 2^{7}$

Introduction
Motivation

- Many applications in Cryptographic
  - User authentication, encryption, etc
  - Cryptographic primitives

Strong PUF-authentication:

— information-theoretical complexity

— no protection mechanisms

— not post-processed on chip

LPN-authentication:

— computational complexity

— no known quantum-attacks

— post-quantum cryptography

Post-quantum secure PUF authentication using LPN

Introduction
- Concept
- Motivation

The construction of the authentication system
- Enrollment phase
- Authentication phase

Conclusion

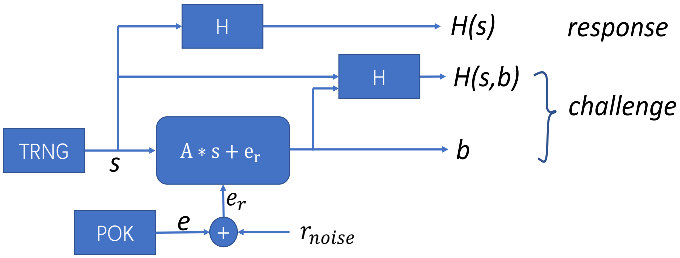
Schedule

Bibliography

Discussion

Fraunhofer AISEC

The construction of the authentication system
Enrollment phase

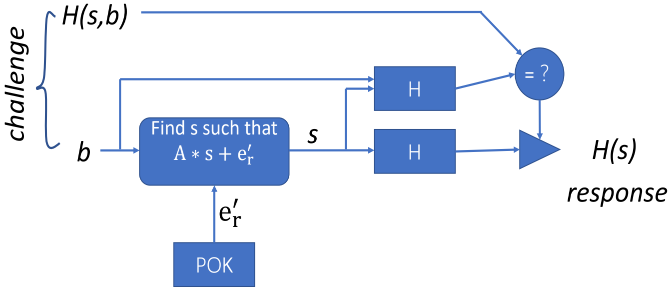


Gen:

random s + one-time-pad → unique b

The construction of the authentication system

Authentication phase



How to extract correct s?

The construction of the authentication system
Authentication phase

Extracting s in the decoding module:

- Gaussian elimination algorithm
  - suitable for linear equations
  - complex implementation in hardware
- Error correction algorithm
  - accurate extraction
  - no security reduction

Fraunhofer AISEC

Authentication phase
Error correction codes

LDPC Code

- complex construction of PC matrix
- complex encoding module
- suitable for long code

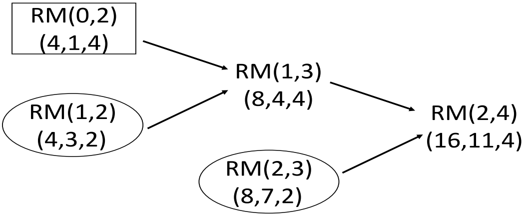
Reed-Muller Code

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

Reed Muller Code

The Plotkin-Construction[4]

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



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

Decoding Algorithm
GMC algorithm VS Recursive algorithm

GMC Algorithm:

analysis for AWGN-channel

complex to realise in hardware

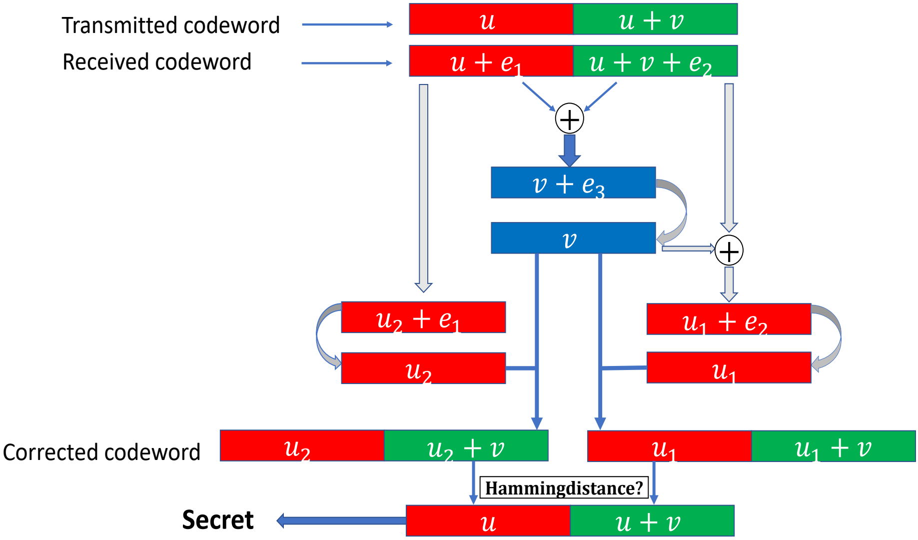
Recursive Algorithm:

analysis for BEC

easy to operate in hardware

Reed Muller Code

The Recursive Decoding Algorithm[4]



Post-quantum secure PUF authentication using LPN

Introduction
- Concept
- Motivation

The construction of the authentication system
- Enrollment phase
- Authentication phase

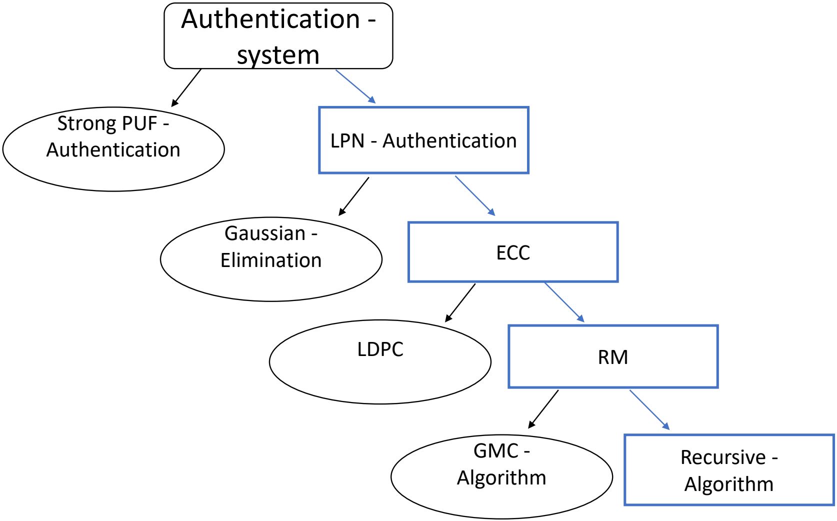
Conclusion

Schedule

Bibliography

Discussion

Conclusion


Authentication - system
Strong PUF - Authentication
LPN - Authentication
Gaussian - Elimination
ECC
LDPC
RM
GMC - Algorithm
Recursive - Algorithm

Post-quantum secure PUF authentication using LPN

Introduction
- Concept
- Motivation

The construction of the authentication system
- Enrollment phase
- Authentication phase

Conclusion

Schedule

Bibliography

Discussion

Fraunhofer AISEC

Schedule

WBS	Name	Start	Finish	Work
1	Implementation in software(Python)	May 1	May 15	15d
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 10	Jun 18	9d
6	Implementation of decoder(VHDL)	Jun 19	Jul 21	25d
7	Implementation of the rest part(VHDL)	Jul 22	Aug 4	12d
8	Writing master paper	Jul 10	Sep 1	40d

Post-quantum secure PUF authentication using LPN

Introduction
- Concept
- Motivation

The construction of the authentication system
- Enrollment phase
- Authentication phase

Conclusion

Schedule

Bibliography

Discussion

Fraunhofer AISEC

[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] **Qian Guo, Thomas Johansson, and Carl Londahl. Solving LPN Using Covering Codes. In Palash Sarkar and Tetsu Iwata, editors, Advances in Cryptology - ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014. Proceedings, Part I, volume 8873 of Lecture Notes in Computer Science, pages 1–20. Springer, 2014.**

[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

Introduction
- Concept
- Motivation

The construction of the authentication system
- Enrollment phase
- Authentication phase

Conclusion

Schedule

Bibliography

Discussion

Discussion

Question?

Post-quantum cryptography

Post-quantum cryptography:

- refers to cryptographic algorithms (usually public-key algorithms)
- secure against an attack by a quantum computer.
- distinct from quantum cryptography, which uses quantum phenomena to achieve secrecy and detect eavesdropping

Weak PUF vs Strong PUF

Weak PUF:

key generation
input and output with same length
a small number of CRPs

Strong PUF:

authentication protocol
long input, short output
large enough CRP space

Security parameter

for this system a key size of n :

- each of the 3 famous algorithms performs worse than brute-force or does not succeed at all[5].
- for a security parameter of k= 128 against the best known attacks.

Parameter setting

for this system a key size of n :

- Plan A: 2 * RM(3,7) (128,64,16)
- Plan B: 1 * RM(3,9) (512,130,64)

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

Fraunhofer AISEC