

Algebraic Security Analysis of Key Generation with Physical Unclonable Functions

Matthias Hiller¹, Michael Pehl¹, Gerhard Kramer² and Georg Sigl^{1,3}

¹ Chair of Security in Information Technology

² Chair of Communications Engineering

Technical University of Munich

³ Fraunhofer AISEC

PROOFS 20.08.2016

Santa Barbara

Algebraic Security Analysis of Key Generation with **Physical Unclonable Functions**

Matthias Hiller¹, Michael Pehl¹, Gerhard Kramer² and Georg Sigl^{1,3}

¹ Chair of Security in Information Technology

² Chair of Communications Engineering

² Technical University of Munich

³ Fraunhofer AISEC

PROOFS 20.08.2016

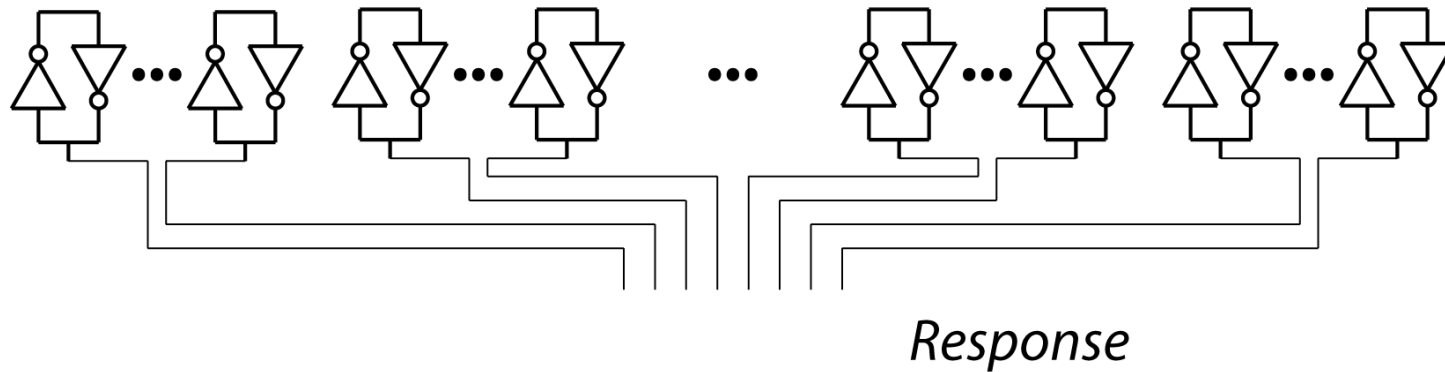
Santa Barbara

Introduction PUFs



Example: SRAM PUF

Guajardo *et al.* (CHES 2007)



Algebraic Security Analysis of **Key Generation** with **Physical Unclonable Functions**

Matthias Hiller¹, Michael Pehl¹, Gerhard Kramer² and Georg Sigl^{1,3}

¹ Chair of Security in Information Technology

² Chair of Communications Engineering

² Technical University of Munich

³ Fraunhofer AISEC

PROOFS 20.08.2016

Santa Barbara

Secret Key Generation

Syndrome Coding

```
0110110010000100000010111001110111101101
1000110101100100100001000101000100100101
0101111001000010111100100110010110110111
011100111111111011011001011100011011111
0100100100011011001010101111101110110000
000111111010001101100100001011100111011101101
001010000010100110101100100100001000101000100100101
1111011110111010000011011111011001101100110100100011
111001100111011110000000000101110011010001110010111
011011011111101001010001100001001001110011110001000
01000101011100011000010001010100001011111111100101
001001011011100101110101111001101001000011001001011
001110010101111011010000111101101010101100001000100100
1110010111110010110101110111011101001010
01101110011111110000110001101001111111100
0100011011110111000101001110100100110101
0010010110111110110100000111101000010101
0011100101011110111101101101111001011110
```

2-part approach

Secret PUF Response
&
Public Helper Data

Secret Key Generation (2)

Need for Error Correction

00
00
0001111111111111000011111111111111111000
0001111111111111000011111111111111111000
0000001110000111000011100001110000111000
0000001110000111000011100001110000111000
0000001110000111000011100001110000111000
0000001110000111000011100001110000111000
0000001110000111000011100001110000111000
0000001110000111000011100001110000111000
0000001110000111000011100001110000111000
0000001110000111000011100001110000111000
0000001110000111000011100001110000111000
0000001110000111000011100001110000111000
0000001110000111000011100001110000111000
0000001110000111000011100001110000111000
00
00

001000000000000000000000000000000000001100000010000000
000100000100000000000000000010000000000000000
01011111111111000001000011111110011100
0001111001111010000111111000111111000
010000110010001111011110000111000111100
0000000010100111010010101001110110111000
0000000110000101000011000001111100111000
0000001110000111000101110001010000111000
0000001100000111001110100000110010111000
0000001100000111111111100101100000111000
0000001110000101111111100001110000011000
00110000000010001000000000001101000000
010000001000100001000000101100000001000

520 Bit - Secret + Redundancy

Reproduction with 15% Bit Error Probability

Motivation

Initial Problem:

Find a **simple and generic** representation of PUF key generation

Main Contribution:

New representation shows if helper data **can** leak key information
(upper bound, **qualitative** result)

For **quantitative** results see e.g. Delvaux *et al.*, CHES 2016

Algebraic Security Analysis of **Key Generation** **with Physical Unclonable Functions**

Matthias Hiller¹, Michael Pehl¹, Gerhard Kramer² and Georg Sigl^{1,3}

¹ Chair of Security in Information Technology

² Chair of Communications Engineering

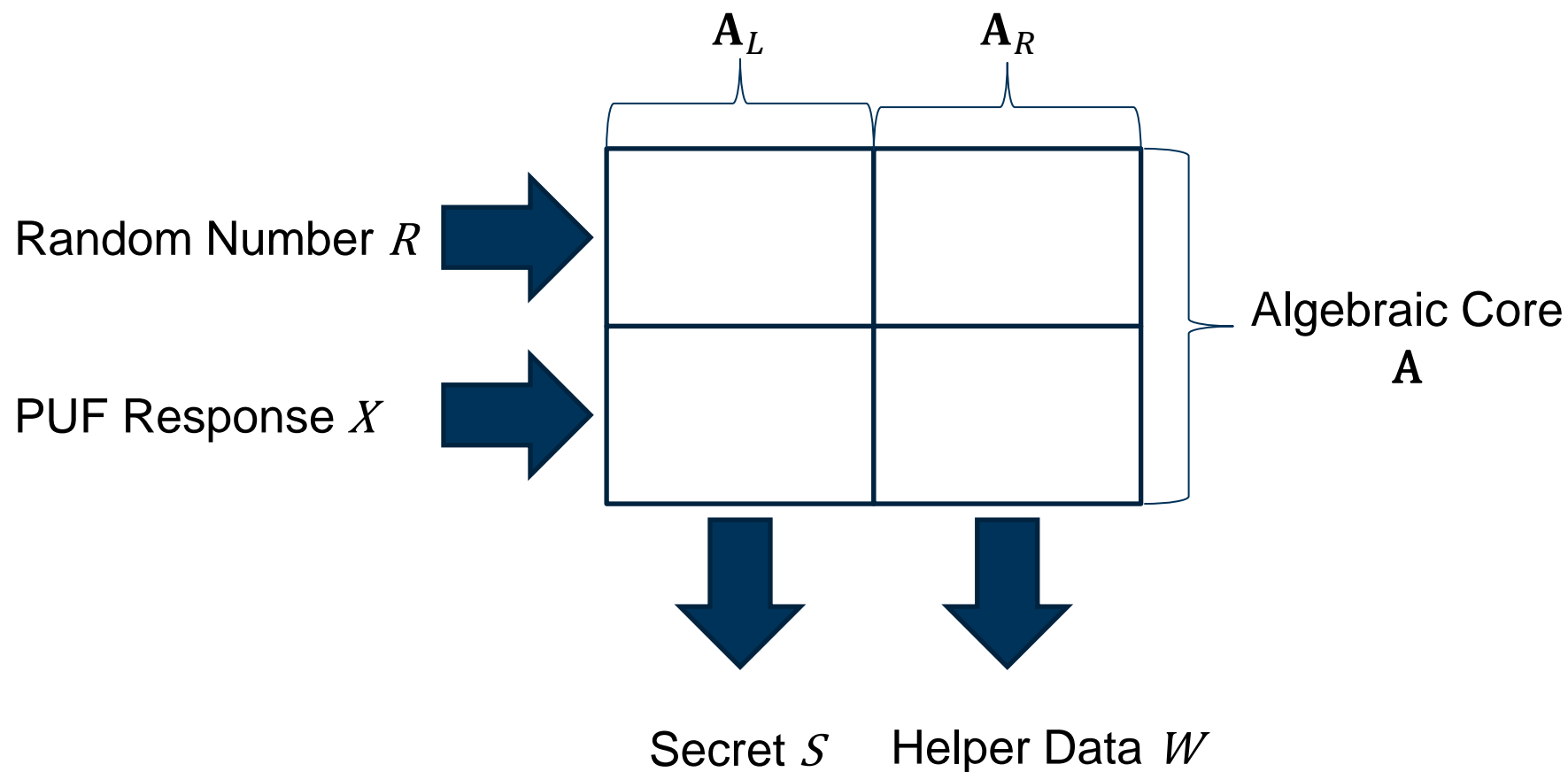
² Technical University of Munich

³ Fraunhofer AISEC

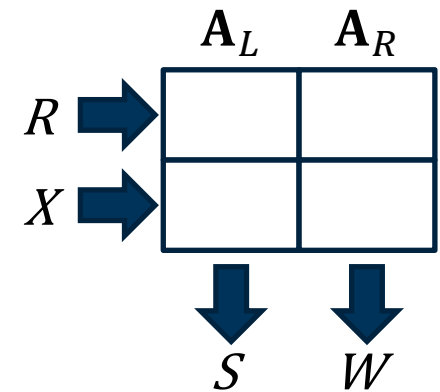
PROOFS 20.08.2016

Santa Barbara

Algebraic Core



Algebraic Core



$$[S \ W] = [R \ X] \mathbf{A}$$

See paper for the algebraic cores of several key generation schemes

Algebraic Security Analysis of Key Generation with Physical Unclonable Functions

Matthias Hiller¹, Michael Pehl¹, Gerhard Kramer² and Georg Sigl^{1,3}

¹ Chair of Security in Information Technology

² Chair of Communications Engineering

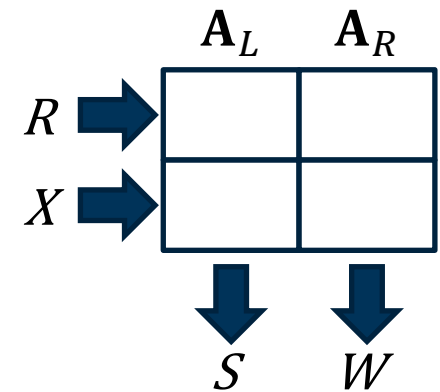
² Technical University of Munich

³ Fraunhofer AISEC

PROOFS 20.08.2016

Santa Barbara

Generic Security Criterion



$$S = [R \ X] \mathbf{A}_L$$
$$W = [R \ X] \mathbf{A}_R$$

Generic Security Criterion

We define the rank loss Δ as

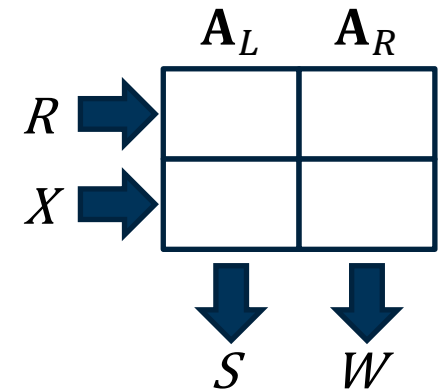
$$\Delta = \text{rank}(\mathbf{A}_L) + \text{rank}(\mathbf{A}_R) - \text{rank}(\mathbf{A})$$

Result without proof:

No leakage between S and W if $\Delta = 0$

S and W can only be linearly independent iff

$$\text{rank}(\mathbf{A}) = \text{rank}(\mathbf{A}_L) + \text{rank}(\mathbf{A}_R)$$



Analysis of the State of the Art

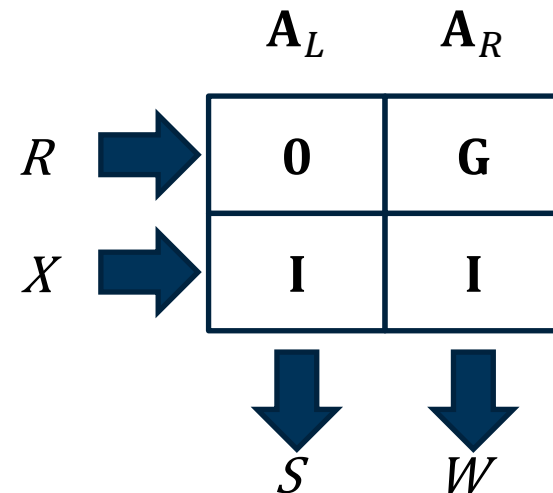
Example: Code-Offset Fuzzy Extractor (Dodis *et al.*, Eurocrypt 2004)

(n,k,d) code with generator Matrix G

$$S = X$$

$$W = RG + X$$

$$A = \begin{pmatrix} \mathbf{0} & \mathbf{G} \\ \mathbf{I} & \mathbf{I} \end{pmatrix}$$



Analysis of the State of the Art

Example: Code-Offset Fuzzy Extractor (Dodis *et al.*, Eurocrypt 2004)

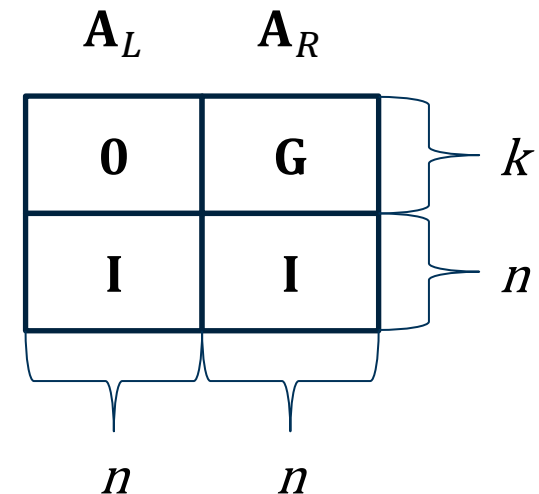
(n,k,d) code with generator Matrix G

$$\text{rank}(\mathbf{A}_L) = n$$

$$\text{rank}(\mathbf{A}_R) = n$$

$$\text{rank}(\mathbf{A}) = n + k$$

$$\begin{aligned} \Delta &= \text{rank}(\mathbf{A}_L) + \text{rank}(\mathbf{A}_R) - \text{rank}(\mathbf{A}) \\ &= 2n - (n + k) \\ &= n - k \end{aligned}$$



Analysis of the State of the Art

Example: Code-Offset Fuzzy Extractor

Result consistent with previous work but easier to obtain
(e.g. Delvaux *et al.*, CHES 2016)

Analysis of the State of the Art

Approach	Δ
Fuzzy Commitment (CCS 1999)	0
Code Offset Fuzzy Extractor (Eurocrypt 2004)	$n-k$
Syndrome Construction (Eurocrypt 2004)	$n-k$
Parity Construction (S&P 1998)	$2k-n$
Systematic Low Leakage Coding (ASIACCS 2015)	0

Take Home Message

- Algebraic representation of key generation for PUFs
- Rank loss enables first security check
- Some state-of-the-art approaches enable zero leakage

Long-term vision

- Develop and characterize more complex approaches