Algebraic Security Analysis of Key Generation with Physical Unclonable Functions

Matthias Hiller[1], Michael Pehl[1], Gerhard Kramer[2] 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 Hiller[1], Michael Pehl[1], Gerhard Kramer[2] 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

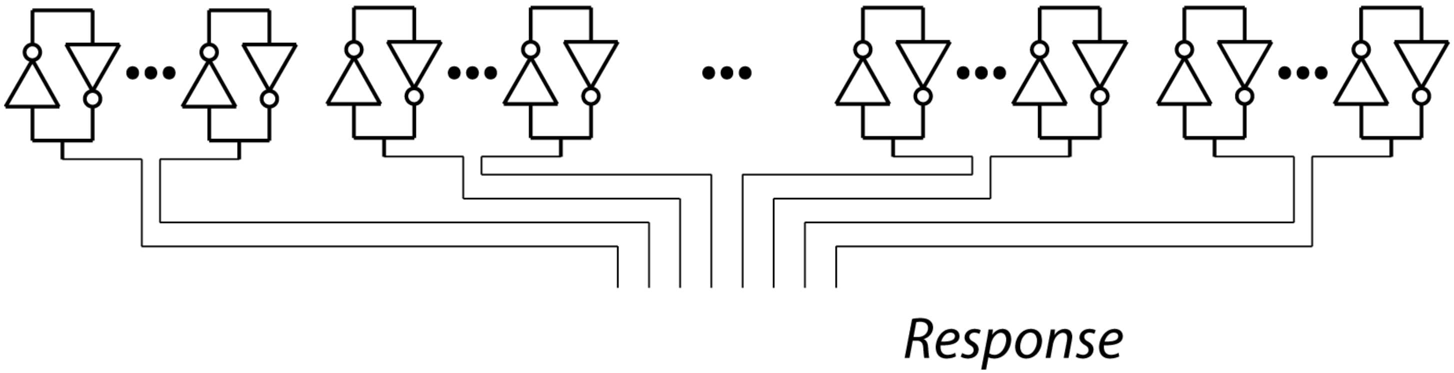
PROOFS 20.08.2016

Santa Barbara

Introduction PUFs

Example: SRAM PUF

Guajardo *et al.* (CHES 2007)



Algebraic Security Analysis of Key Generation with Physical Unclonable Functions

Matthias Hiller[1], Michael Pehl[1], Gerhard Kramer[2] 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

2-part approach

Secret PUF Response

&

Public Helper Data

Secret Key Generation (2)

Need for Error Correction

```
0000000000000000000000000000000000000000
0000000000000000000000000000000000000000
0001111111111111000011111111111111111000
0001111111111111000011111111111111111000
0000001110000111000011100001110000111000
0000001110000111000011100001110000111000
0000001110000111000011100001110000111000
0000001110000111000011100001110000111000
0000001110000111000011100001110000111000
0000001110000111111111100001110000111000
0000001110000111111111100001110000111000
0000000000000000000000000000000000000000
0000000000000000000000000000000000000000
```

520 Bit - Secret + Redundancy

```
0010000000000000000000001100000010000000
0001000001000000000000001000000000000000
0101111111111111000001000011111110011100
0001111001111101000011111110001111111000
0100001100100011110111100001110001111100
0000000010100111010010101001110110111000
0000000110000101000011000001111100111000
0000001110000111000101110001010000111000
0000001100000111001110100000110010111000
0000001100000111111111100101100000111000
0000001110000101111111100001110000011000
0011000000001000100000000000011010000000
0100000010001000010000001011000000010000
```

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

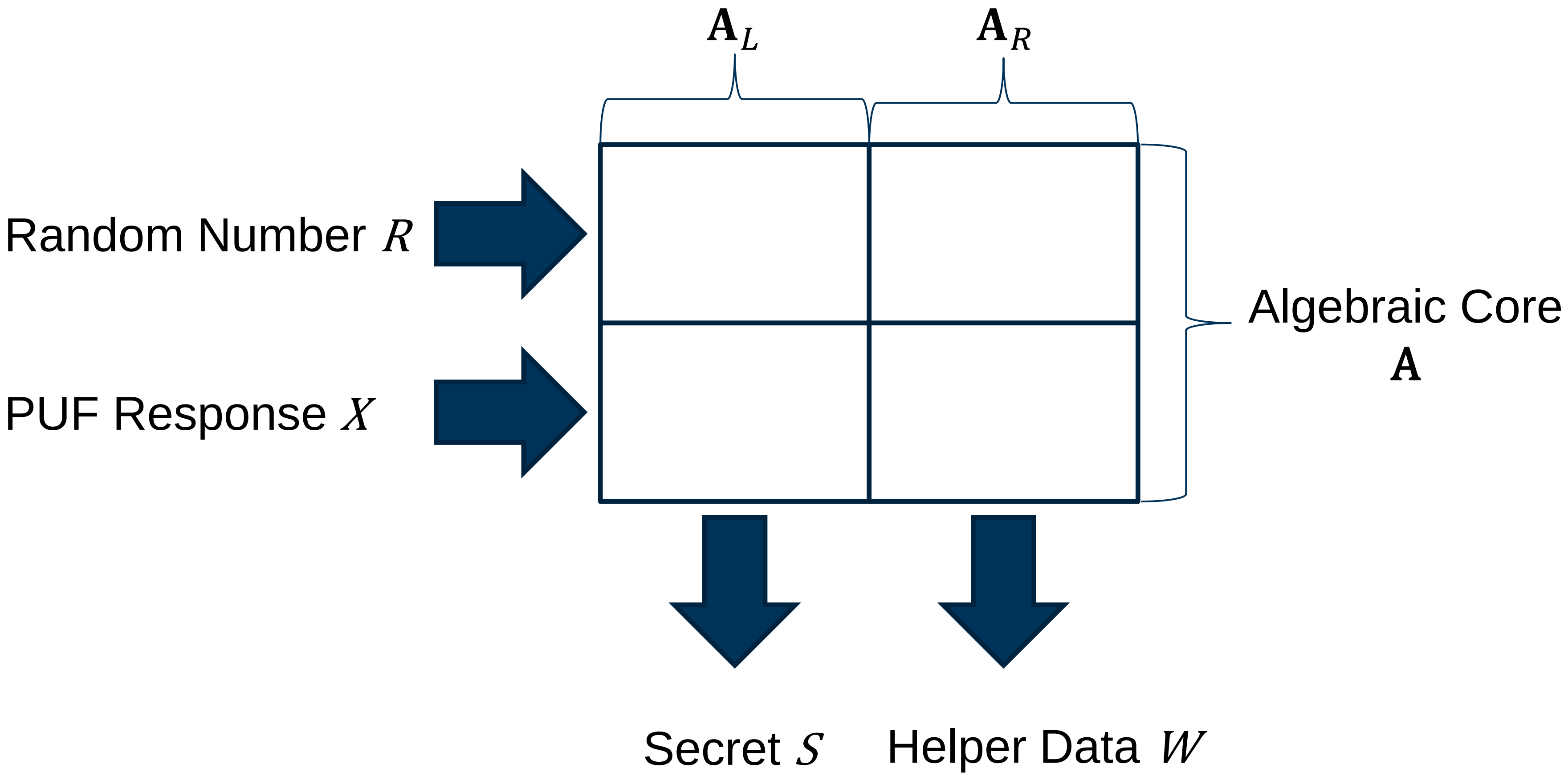
Algebraic Security Analysis of Key Generation with Physical Unclonable Functions

Matthias Hiller[1], Michael Pehl[1], Gerhard Kramer[2] and Georg Sigl[1,3]

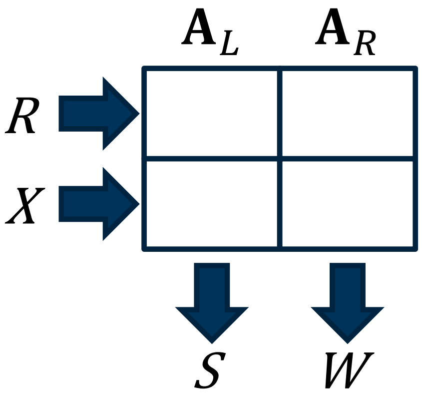
[1] Chair of Security in Information Technology
[2] Chair of Communications Engineering
[2] Technical University of Munich
[3] Fraunhofer AISEC

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

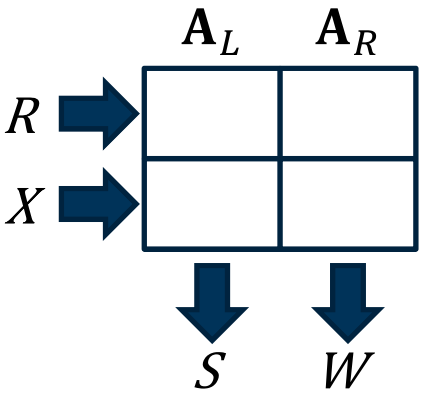
Matthias Hiller[1], Michael Pehl[1], Gerhard Kramer[2] and Georg Sigl[1,3]

[1] Chair of Security in Information Technology
[2] Chair of Communications Engineering
[2] Technical University of Munich
[3] Fraunhofer AISEC

PROOFS 20.08.2016

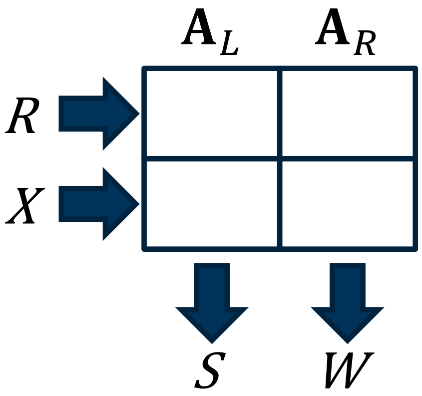
Santa Barbara

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

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

Result without proof:

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

S and W can only be linearly independent iff

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

Analysis of the State of the Art

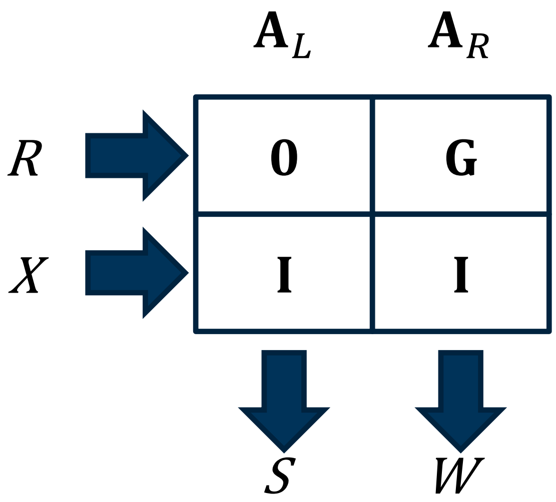
Example: Code-Offset Fuzzy Extractor (Dodis *et al*., Eurocrypt 2004)

(n,k,d) code with generator Matrix $\mathbf{G}$

$$S = X$$

$$W = R\mathbf{G} + X$$

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



Analysis of the State of the Art

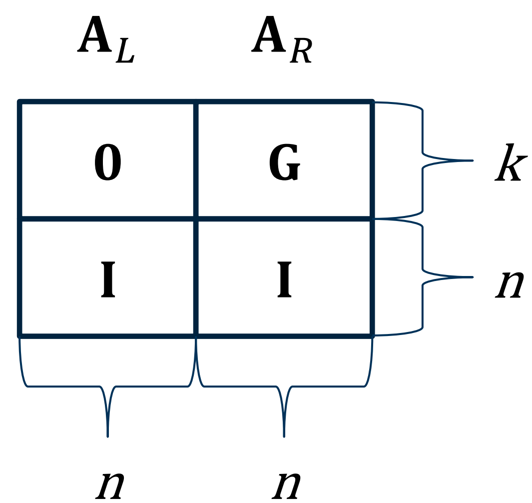
Example: Code-Offset Fuzzy Extractor (Dodis *et al*., Eurocrypt 2004)

(n,k,d) code with generator Matrix $\mathbf{G}$

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

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

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



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