Algebraic Security Analysis of Key Generation with Physical Unclonable Functions

Matthias Hiller\textsuperscript{1}, Michael Pehl\textsuperscript{1}, Gerhard Kramer\textsuperscript{2} and Georg Sigl\textsuperscript{1,3}

\textsuperscript{1} Chair of Security in Information Technology
\textsuperscript{2} Chair of Communications Engineering
Technical University of Munich
\textsuperscript{3} Fraunhofer AISEC

PROOFS 20.08.2016
Santa Barbara
Algebraic Security Analysis of Key Generation with Physical Unclonable Functions

Matthias Hiller\textsuperscript{1}, Michael Pehl\textsuperscript{1}, Gerhard Kramer\textsuperscript{2} and Georg Sigl\textsuperscript{1,3}

\textsuperscript{1} Chair of Security in Information Technology
\textsuperscript{2} Chair of Communications Engineering
\textsuperscript{2} Technical University of Munich
\textsuperscript{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
\(^3\) 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

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 Sigl¹,³

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

Random Number $R$ → $A_L$ → Secret $S$

PUF Response $X$ → $A_R$ → Helper Data $W$
Algebraic Core

\[ [S \; W] = [R \; X] A \]

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 Sigl¹,³

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

PROOFS 20.08.2016
Santa Barbara
Generic Security Criterion

\[ S = [R \; X] A_L \]
\[ W = [R \; X] A_R \]
Generic Security Criterion

We define the rank loss $\Delta$ as

$$\Delta = \text{rank}(A_L) + \text{rank}(A_R) - \text{rank}(A)$$

Result without proof:
No leakage between $S$ and $W$ if $\Delta = 0$

$S$ and $W$ can only be linearly independent iff

$$\text{rank}(A) = \text{rank}(A_L) + \text{rank}(A_R)$$
Analysis of the State of the Art

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

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

\[
S = X \\
W = RG + X
\]

\[
A = \begin{pmatrix} 0 & G \\ I & I \end{pmatrix}
\]
Analysis of the State of the Art

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

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

\[
\begin{align*}
\text{rank}(A_L) &= n \\
\text{rank}(A_R) &= n \\
\text{rank}(A) &= n + k \\
\Delta &= \text{rank}(A_L) + \text{rank}(A_R) - \text{rank}(A) \\
&= 2n - (n + k) \\
&= n - k
\end{align*}
\]
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

<table>
<thead>
<tr>
<th>Approach</th>
<th>$\Delta$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fuzzy Commitment (CCS 1999)</td>
<td>0</td>
</tr>
<tr>
<td>Code Offset Fuzzy Extractor (Eurocrypt 2004)</td>
<td>n-k</td>
</tr>
<tr>
<td>Syndrome Construction (Eurocrypt 2004)</td>
<td>n-k</td>
</tr>
<tr>
<td>Parity Construction (S&amp;P 1998)</td>
<td>2k-n</td>
</tr>
<tr>
<td>Systematic Low Leakage Coding (ASIACCS 2015)</td>
<td>0</td>
</tr>
</tbody>
</table>
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