CRYPTARCHI 2017 Smolenice
"Formalism to Assess the Entropy and Reliability of Loop PUF"

Jean-Luc Danger\textsuperscript{1,2}
Olivier Rioul\textsuperscript{1}
Sylvain Guilley\textsuperscript{1,2}
Alexander Schaub\textsuperscript{1}

\textsuperscript{1} Télécom ParisTech, LTCI, UPSAY
\textsuperscript{2} Secure-IC
Outline

- Loop PUF architecture
- Entropy assessment
- Reliability assessment
- Results on real silicon
- Conclusions

* Depends on algorithm, not implementation
Loop PUF architecture

Diagram of a loop PUF architecture with
- Enable signal
- Oscillator measurement
- Clock reference

Symbols:
- $c_1$
- $c_n$
- ID
Algorithm 2.1 Operating Mode with 2 complementary challenges

**Input:** Challenge $C$ (a word of $n$ bits)

**Output:** Response $B$

1. Set challenge $C$
2. Measure $d_C \leftarrow \left[ L \sum_{i=1}^{n} d(c_i) \right]$
3. Set challenge $\neg C$
4. Measure $d_{\neg C} \leftarrow \left[ L \sum_{i=1}^{n} d(\neg c_i) \right]$
5. Compute $\Delta = d_C - d_{\neg C}$
6. Return $B = \text{sign}(\Delta) \in \{\pm 1\}$

The information for each challenge is $\Delta$

Sign = identifier
Module = reliability
Balance of Delay Elements in ASIC

duplication
Balance of Delay Elements in FPGA

Cluster 1
Cluster 2
Cluster N

duplication
N duplications
Delay measurement

\[ d_C = L \cdot \frac{f_{osc}}{f_{ref}} \]
**Entropy**

- For a n-delay LPUF
  - If challenge = Hadamard codeword of n bits => Entropy = n *

For instance for n = 12, the n by n Hadamard Matrix is:

\[
C_{12} = \begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\
1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\
1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\
1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\
1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\
1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\
1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\
1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\
1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\
1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1
\end{pmatrix}
\]

Entropy with more than n challenges

Figure 4: Entropy for n elements as a function of the number M of challenges.
**LPUF reliability**

\[
BER = \mathbb{P}(\text{sign}(\Delta + N) \neq \text{sign}(\Delta)) = \Phi\left(\frac{|\Delta|}{\sigma}\right)
\]

\[
N \sim \mathcal{N}(0, \sigma^2) \quad Q(x) = \frac{1}{2}
\left(1 - \text{erf}\left(\frac{x}{\sqrt{2}}\right)\right) = \frac{1}{2} \text{erfc}\left(\frac{x}{\sqrt{2}}\right)
\]

\[
\hat{BER} = \int_{0}^{+\infty} \mathbb{P}(\Delta) \cdot BER(\Delta) \cdot d\Delta
\]

With

\[
SNR = \frac{\Sigma}{\sigma}
\]

\[
\hat{BER} = \frac{1}{4} - \frac{1}{2\pi} \arctan(SNR)
\]
The Reliability is not enough $\sim 10^{-3}$ even with high SNR

$\Rightarrow$ Needs of secure sketch : Error Correcting codes and Helper data
Reliability enhancement by delay knowledge

The bits in the unreliable area "B" are discarded
The helper data indicates the unreliable bits

Bit unreliable ⇔ |delay| < Th

Th = Wσ

pdf(Δ) = N(0,σ²)
pdf(Δ + noise) = N(Δ,σ²)
New BER with filtered bits

\[ \widehat{BER}_{filt} = T(W, \frac{1}{SNR}) + \frac{1}{4} \text{erf}\left( \frac{W}{\sqrt{2} \cdot SNR} \right) \left( \text{erf}\left( \frac{W}{\sqrt{2}} \right) - 1 \right) \]
Entropy after bit filtering

Number of delay elements to reach n bits of entropy with Hadamard codes

\[ n' = \frac{n}{1 - \mathbb{P}(\text{Bit unreliable})} = \frac{n}{\text{erfc}(\frac{W}{SNR})} \]
Results on real silicon

- n=54 cells, 65nm technology

7x7 PUF matrix
i.i.d. check

Correlation matrix on the 64 elements of the 49 PUFs

No correlation between the 64 delay elements
=> entropy ~ 64 with Hadamard codes
Impact of the measurement window on the SNR

$\text{SNR} \sim 60$ for $\log_2 L = 14$
Entropy

The graph shows the number of bits required to reach 100 bits of entropy as a function of the parameter $W$. The graph includes three lines representing different Signal-to-Noise Ratios (SNR): SNR=10 (red), SNR=60 (green), and measured (black). The x-axis represents the value of $W$, while the y-axis shows the number of bits required. The lines indicate an increasing trend with higher $W$ values for all SNR settings.
Reliability: BER results

![BER results graph]

- Theory SNR=10
- Theory SNR=60
- Measured
Conclusions

- The Entropy of the Loop PUF can be formally obtained if Hadamard codes are used:
  - Entropy = number of delay elements n
  - The entropy increases non linearly if M > n
- The reliability of the Loop PUF is low (BER \( \sim 10^{-3} \))
- It can be easily improved by exploiting the delay knowledge
  - The unreliable bits are discarded
  - BER can go down \( 10^{-9} \)
  - But more bits are needed to reach the same entropy

\( N = \) Number of challenges
THANK YOU
FOR YOUR ATTENTION