Towards Secure Strong PUFs

Nils Wisiol · 31st Crypto Day · {Freie, Technische} Universität Berlin · nils.wisiol@fu-berlin.de · 17th October 2019
How do we authenticate securely?
A Basic Way

Oh, hey, who are you?

I am card #1337
The MAC Way

What’s the answer for nonce?

The answer is $f(\text{secret, nonce})$
The Public Key Way

What’s the answer for nonce?

The answer is $f(secret, nonce)$
Anyone in possession of the key can model the card’s behavior!
Optical Physically Unclonable Functions


Arbiter Physical Unclonable Functions (Electric)

\[
c_1^{(1)} = +1 \\
c_2^{(1)} = -1 \\
c_{n-1}^{(1)} \\
c_n^{(1)}
\]
Can the behavior be modeled?
Arbiter Physical Unclonable Functions (Electric)

Bistable Ring PUF

Two possible final stable states (out_0...out_7):

- \(01010101_{\text{BIN}} = 55_{\text{HEX}}\) ("5"-state)
- \(10101010_{\text{BIN}} = AA_{\text{HEX}}\) ("A"-state)
SHIC PUFs

Arbiter PUF Variants: Feed Forward Arbiter PUF


Arbiter PUF Variants: XOR Arbiter PUF

\[ c_1^{(1)} = +1 \]
\[ c_2^{(1)} = -1 \]

\[ c_1^{(k)} = +1 \]
\[ c_2^{(k)} = +1 \]

\[ f(c) \]

Lightweight Secure PUF

http://dl.acm.org/citation.cfm?id=1509456.1509603.

Interpose PUF

\[ c = (c[0], \ldots, c[i], \ldots, c[n-1]) \rightarrow x\text{-XOR APUEF} \]

\[ (c[0], \ldots, c[i], r_x, c[i+1] \ldots, c[n-1]) \rightarrow y\text{-XOR APUEF} \rightarrow r \]
Cryptanalysis of the Interpose PUF
Cryptanalysis of the Interpose PUF

PTF Lengths for n-bit (1,k)-Interpose PUF Approximation and n-bit k-XOR Arbiter PUFs
Cryptanalysis of the Interpose PUF (64 bit)

Accuracy

Training Set Size

Run Time (hrs)
Modeling Attack with Deep Learning

Preliminary results; ongoing research with Christopher Mühl
Interpose PUF needs further improvement!
Thanks!

Nils Wisiol · 31st Crypto Day
{Freie, Technische} Universität Berlin
nils.wisiol@fu-berlin.de
17th October 2019
github.com/nils-wisiol/pypuf

Discussion

- Multi-bit Outputs?
- Improvement for the Interpose PUF?
- Mitigate Deep Learning Attacks?