Formal Design of Composite Physically Unclonable Function

Durga Prasad Sahoo **Debdeep Mukhopadhyay**
Rajat Subhra Chakraborty

Computer Science and Engineering
Indian Institute of Technology, Kharagpur, India

Workshop on Security Proofs for Embedded Systems, 2013

Outline

Physically Unclonable Function

- A silicon Physically Unclonable Function is a mapping

$$\gamma : \{0,1\}^n \longrightarrow \{0,1\}^k$$

where the output k-bit words are unambiguously identified by both the n challenge bits and the unclonable, unpredictable but repeatable instance specific system behavior.

Physically Unclonable Function

- A silicon Physically Unclonable Function is a mapping

$$\gamma : \{0,1\}^n \longrightarrow \{0,1\}^k$$

  where the output k-bit words are unambiguously identified by both the n challenge bits and the unclonable, unpredictable but repeatable instance specific system behavior.

- Unclonability is the result of unique and uncontrollable variations in manufacturing process of silicon chip.

Physically Unclonable Function

- A silicon Physically Unclonable Function is a mapping

$$\gamma : \{0,1\}^n \longrightarrow \{0,1\}^k$$

  where the output k-bit words are unambiguously identified by both the n challenge bits and the unclonable, unpredictable but repeatable instance specific system behavior.

- Unclonability is the result of unique and uncontrollable variations in manufacturing process of silicon chip.

- Physically implies function is clonable in general but not in a physical way.

Physically Unclonable Function

- A silicon Physically Unclonable Function is a mapping

$$\gamma : \{0, 1\}^n \longrightarrow \{0, 1\}^k$$

  where the output k-bit words are unambiguously identified by both the n challenge bits and the unclonable, unpredictable but repeatable instance specific system behavior.

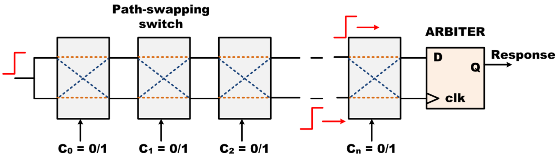
- Unclonability is the result of unique and uncontrollable variations in manufacturing process of silicon chip.

- Physically implies function is clonable in general but not in a physical way.

- Delay PUFs exploit delay variation in CMOS logic components:
  - Arbiter PUF (APUF) [Gassend, 2004]
  - Ring Oscillator PUF (ROPUF) [Suh, 2007]

Silicon PUF

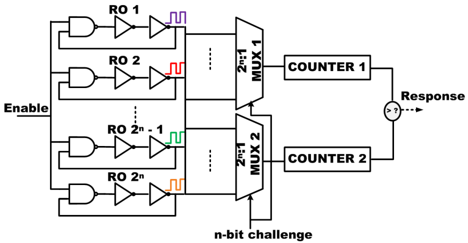
Arbiter PUF:



- Exploits digital race condition on two paths on a chip.
- Paths are designed symmetrically (ideally).
- Ideally, delay difference should be 0, but it does not happen due to process variation that results random offset between the two delays.
- Response $r = \begin{cases} 1, & \text{if } d_1 < d_2 \\ 0, & \text{otherwise} \end{cases}$
  where d_1 and d_2 are propagation delays of two path P_1 and P_2.

Silicon PUF (cont.)

Ring Oscillator PUF:



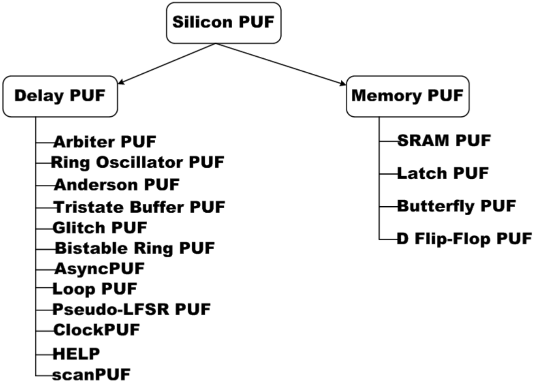
- Consists of identically laid out Ring Oscillators.
- The frequency of ring oscillators depend on process variation.
- Challenge of PUF selects a pair of ring oscillators (A,B) with frequency f_A and f_B.
- Response $r = \begin{cases} 1, & \text{if } f_A > f_B \\ 0, & \text{otherwise} \end{cases}$

PUF Quality Metrics

Metrics used to evaluate a PUF:

- Uniqueness – PUF instances should generate signatures with inter Hamming Distance close to 50% of the signature string size.
- Uniformity – Distribution of 0's and 1's in a signature. It should be uniform.
- Reliability – PUF should have ability to generate same signature repeatedly. Reliability measure in what extent it can do that.
- Bit-aliasing – It happens when different chips produce nearly identical PUF responses, which is undesirable.
- Bit-dependency – Measures dependency among bits of a signature. Autocorrelation Test is used for it.

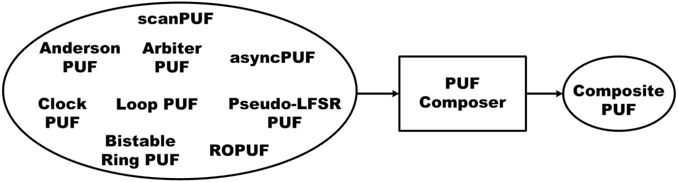
Silicon PUF Zoo



None of the PUFs satisfies following aspects:

- Good performance profile (Quality metrics)
- Lightweight (Resource required for implementation)

PUF Synthesis



- PUF design paradigm that exploits smaller PUFs (both *weak* and *strong* PUFs) as design blocks.
- Resultant PUF is termed as Composite PUF.
- Composite PUFs have large challenge-space and good performance profile than component PUFs.

Composite PUF

Definition

A composite PUF (ζ) over set of PUFs $\Gamma = \{\gamma_1, \gamma_2, ..., \gamma_m\}$ is a PUF circuit that is defined by recursively applying following rules:

a. $\gamma_i : C_i \longrightarrow R_i$, where $C_i, R_i \subseteq \{0, 1\}^+$ and $\gamma_i \in \Gamma$.

b. $(\gamma_i \lhd \gamma_j)(x) = \gamma_i(\gamma_j(x))$, where $x \in C_j$.

c. $(\gamma_i \parallel \gamma_j)(x, y) = \gamma_i(x) \cdot \gamma_j(y))$, where $x \in C_i$, $y \in C_j$, and $'.'$ is binary strings concatenation operator.

d. $(\gamma_i \oplus \gamma_j)(x, y) = \gamma_i(x) \oplus \gamma_j(y)$, where $x \in C_i$, $y \in C_j$, $\oplus$ is bit-wise exclusive-OR operator.

e. $(\gamma_i \bowtie \gamma_j)(x) = \gamma_j(\gamma_i(\gamma_j(x)))$, where $x \in C_j$

f. $\gamma_i(perm(x))$ and $perm(\gamma_i(x))$ are PUFs with input and output permutation network $perm(y)$ respectively, and $y \in \{0, 1\}^*$ and $x \in C_i$.

Motivation behind Composition Operators selection

Lemma (Operator $\|$)

Let X and Y be two independent random variables with entropy $H(X)$ and $H(Y)$, respectively. Then, $H(X,Y) = H(X) + H(Y)$.

Lemma (Operator $\oplus$)

Let X and Y be two Bernoulli random variables with probability p and q, respectively. Then, random variable $Z = X \oplus Y$ also follows Bernoulli distribution with probability $p + q - 2pq$. It implies that if any of the component distributions is uniform, then Z is also uniform.

Lemma (Operator $\triangleleft$)

Let X and Y be two random variables. If $Y = f(X)$ is a deterministic function of X, then $H(Y) \leq H(X)$ with equality if and only if $f(.)$ is one-to-one.

Validity of Composition

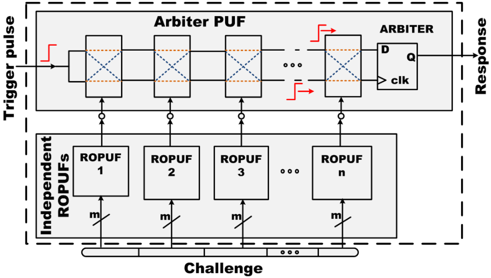
Definition (Well-formed composite PUF)

Let ζ be a composite PUF having n-input and m-output – written as $\zeta : n \otimes m$– and defined over Γ. The PUF ζ is said to be well-formed if and only if each of its sub-circuit obeys the rules of type system $\tau : \Gamma \rightarrow \mathbb{N} \times \mathbb{N}$ given below. Otherwise, ζ is said to be ill-formed.

i) $\frac{\tau(\gamma)=(n,m)}{\gamma:n\otimes m}\gamma \in \Gamma$ ii) $\frac{\gamma_i:n_i\otimes m_i,\gamma_j:n_j\otimes m_j}{\gamma_i\|\gamma_j:n_i+n_j\otimes m_i+m_j}$ iii) $\frac{\gamma_i:n_i\otimes m_i,\gamma_j:n_j\otimes m_j,n_i=m_j}{\gamma_i\lhd\gamma_j:n_j\otimes m_i}$

iv) $\frac{\gamma_i:n_i\otimes m_i,\gamma_j:n_j\otimes m_j,m_i=m_j}{\gamma_i\oplus\gamma_j:n_i+n_j\otimes m_i}$ v) $\frac{\gamma_i:n_i\otimes m_i,\gamma_j:n_j\otimes m_j,n_i=m_j,n_j=m_i}{\gamma_i\bowtie\gamma_j:n_j\otimes m_i}$

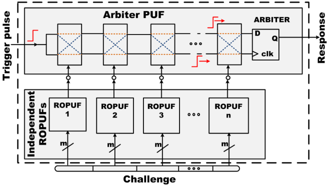
Composite PUF Instance



$$\chi_{n,m} = \gamma_{n+1}((\gamma_1 \parallel \gamma_2 \parallel \gamma_3 \parallel \cdots \parallel \gamma_{n-1} \parallel \gamma_n)(c_1, c_2, c_3, \ldots, c_{n-1}, c_n))$$
$$= \gamma_{n+1}((\gamma_1(c_1) \cdot \gamma_2(c_2) \cdot \gamma_3(c_3) \cdot \cdots \cdot \gamma_{n-1}(c_{n-1}) \cdot \gamma_n(c_n))$$

where γ_{n+1} is an n-bit Arbiter PUF, and γ_i, $1 \leq i \leq n$, are m-bit ROPUFs.

How does it work?



- Externally applied challenge is divided into n equal size sub-challenge, each of size m.
- Sub-challenges are applied to n independent ROPUFs.
- Responses of the ROPUFs together form the (internal) challenge for the APUF.
- Response of APUF is the response of Composite PUF.

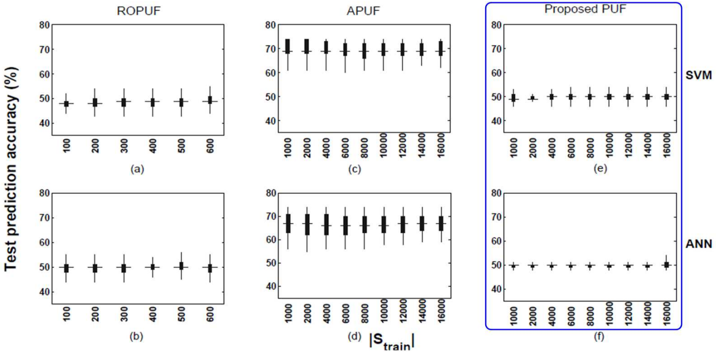
Performance Quality

Metrics	Ideal Value	Composite PUF				APUF	ROPUF
		Min.	Max.	Avg.	Std. Div.	Avg.	Avg.
Uniqueness(%)	50	32.42	54.30	47.57	4.06	37.40	31.34
Reliability(%)	100	89.26	92.97	90.70	1.12	100	99.85
Uniformity(%)	50	36.33	55.27	47	3.27	70.63	51.56
Bit-aliasing[0,50]	0	4.55	50	14.95	10.26	30.90	28.20
Autocorrelation Coefficient[0,1]	0.5	0.43	0.57	0.50	0.23	0.42	0.49

[†]Challenge size of composite PUF, APUF, and ROPUF are 60, 60, and 10 bits, respectively.

- 60-bit Composite PUF with 15 4-bit ROPUF and one 15-bit APUF.
- Implemented on 11 Altera Cyclone-III EP3C80F780I7 FPGAs.
- Uniqueness and Bit-aliasing are significantly improved. Uniqueness is most important metric for PUF.
- Reliability is reduced, but acceptable.
- Uniformity is better than APUF.

Robustness Against Modeling Attacks



- Machine Learning Tool: SVM (Support Vector Machine) and ANN (Artificial Neural Network).
- $|S_{train}|$ - size of training set.
- Derived models were tested on 5000 unseen challenges for the proposed composite PUF and APUFs, and 400 CRPs for ROPUF.
- prediction accuracy of target composite PUF design is close to 50% (**random prediction**).

Advantage of this design

Three aspects:

1. shows better modeling robustness than APUF,
2. consumes less resource than ROPUF, and
3. has better performance profile than both ROPUF and APUF.

Summary & Outlook

Summary:

- None of existing PUFs is good from all aspects.
- Combine them to improved the design – PUF Synthesis.

Outlook:

Finding of optimal composition from the large composite PUF space.

Thank You