DESIGN, AUTOMATION & TEST IN EUROPE
9 – 13 March, 2015 · Grenoble · France
The European Event for Electronic System Design & Test

Efficient Attacks on Robust Ring Oscillator PUF with Enhanced Challenge-Response Set

Phuong Ha Nguyen

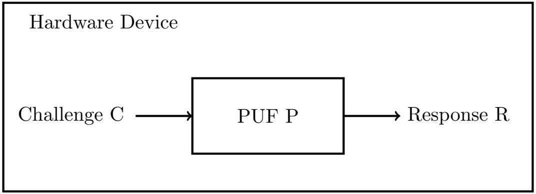
Durga Prasad Sahoo, Rajat Subhra Chakraborty,
Debdeep Mukhopadhyay

Secured Embedded Architecture Laboratory (SEAL)
Dept. of Computer Science and Engineering
Indian Institute of Technology Kharagpur
Kharagpur-721302, INDIA

Outline

What is PUF

- Physically Unclonable Functions (PUF) is a physical embedded entity in hardware device.
- PUF performs a Challenge and Response behavior: for a given challenge **C**, a random response **R** is generated.
- Challenge and Response Behavior of a given PUF can not be physically cloned and it is unique, i.e., different PUF instances have different Challenge-Response Behaviors.



Application of PUF

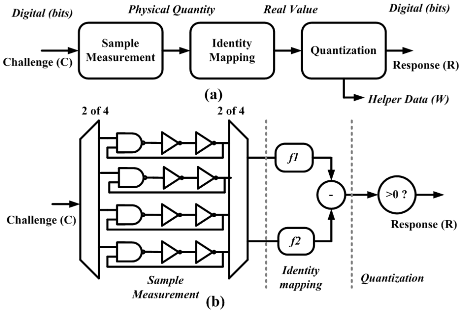
- Since PUF is a device and can not be cloned, it can be used as a secret in secure system which is assumed to be secure against physical attacks. The secure systems based on stored secrets in Non Volatile Memory (NVM) do not provide this property.
- PUF is used for IP protection because of its uniqueness.
- PUF can be used for key generation, etc.

Security Aspects of PUF

- **Unclonability:** Challenge-Response Behavior of a PUF can not be cloned mathematically and physically.
- **Unpredictability:** Generation of the response **r** for a given challenge **c** should be randomly and unpredictable.
- **Reliability:** Reproduction of response for any challenge **c** should be highly reliable
  - In practice, the reliability of reproduction is always less than 100%
  - Error Correction Circuit (ECC) is used to achieve the high reliability property
  - In ECC, to achieve this goal, the concept helper data W

Design Description

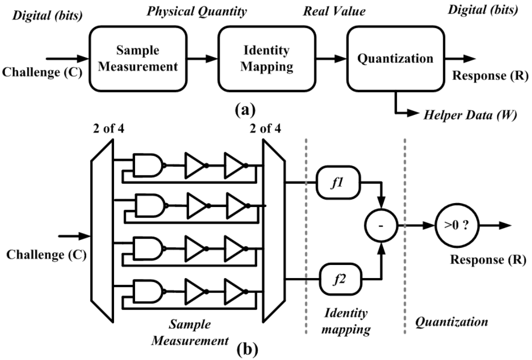
- RO-PUF[1] is constructed based on 2×2^m Ring Oscillators (RO).
- Response r (1-bit) generated by comparing frequencies of a pair of ROs based on challenge $\mathbf{c} = (c_1, \cdots, c_m)$, $c_i \in \{0, 1\}$.



[1] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Design Automation Conference*. New York, NY, USA: ACM Press, 2007, pp. 9–14

Shortcomings

1. **Large hardware overhead:** 2×2^m ROs are required for RO-PUF with *m*-bit challenge.
2. **Poor reliability property:** RO is very sensitive to the environmental variations.



Advantages

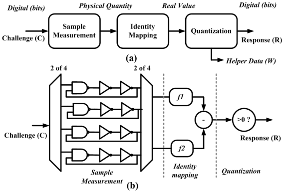
Enhanced RO-PUF[1] has the following advantages:

1. **Small hardware overhead:** m ROs are required for RO-PUF with m-bit challenge. This improvement is made based on subset selection concept. A subset of frequencies is chosen instead of a pair of frequencies for a given challenge **c**.
2. **High reliability property:** ECC-based helper data W is introduced to correct the output of the enhanced RO-PUF.
3. **It is shown that it is a secure PUF**

[1] A. Maiti, I. Kim, and P. Schaumont, "A Robust Physical Unclonable Function With Enhanced Challenge-Response Set," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 333 –345, feb. 2012

Notations

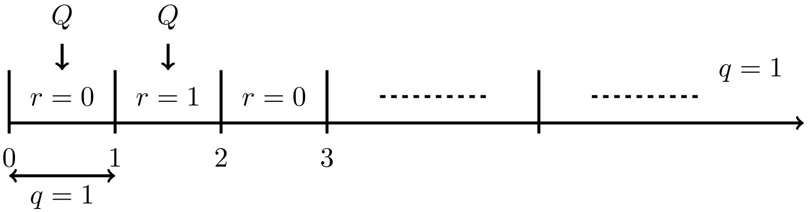
1. **Set of ROs:** m ROs $RO_1, \dots, RO_m$ which have frequencies $f_1, \dots, f_m$, respectively.
2. m**-bit challenge:** $\mathbf{c} = (c_1, \dots, c_m)$.
3. 1**-bit response:** r.
4. **Security parameters:** e, q
5. **Helper data:** W which is a real number.
6. **Quantification value:** Q which is a real number. In the original RO-PUF design, quantification function is the comparision function.



Computation of Response r

$$\begin{array}{l}\mathbf{c} = (c_1, \ldots, c_m) \\ \quad\Big\downarrow {\color{red}(1)} \\ c_{i_1} = \cdots = c_{i_t} = 1 \xrightarrow{\color{red}(2)} f_{i_1}, \ldots, f_{i_t} \xrightarrow{\color{red}(3)} Q \longrightarrow \begin{cases} r & {\color{red}(4)} \\ W & {\color{red}(5)} \end{cases}\end{array}$$

$$Q = \sum_{u=1}^{t-1} \sum_{v=u+1}^{t} Q_{i_u i_v}, \qquad Q_{i_u i_v} = |i_u - i_v||f_{i_u} - f_{i_v}|^e$$



Computation of Helper Data W

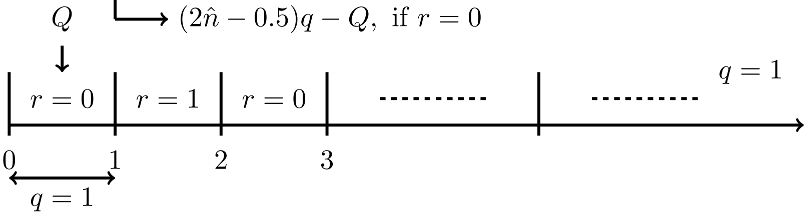
$$\mathbf{c} = (c_1, \ldots, c_m) \qquad Q = \sum_{u=1}^{t-1} \sum_{v=u+1}^{t} |i_u - i_v||f_{i_u} - f_{i_v}|^e$$

$$\downarrow (1)$$

$$c_{i_1} = \cdots = c_{i_t} = 1 \xrightarrow{(2)} f_{i_1}, \ldots, f_{i_t} \xrightarrow{(3)} Q \rightarrow \begin{cases} r & (4) \\ W & (5) \end{cases}$$

$$W = \begin{cases} (2\hat{n} + 0.5)q - Q, & \text{if } r = 1 \\ (2\hat{n} - 0.5)q - Q, & \text{if } r = 0 \end{cases}$$

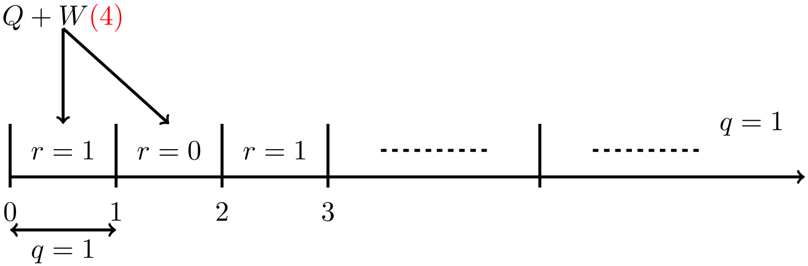
$\hat{n}$ such that $|W| < q$



Response Correction Based on *W*

$$\mathbf{c} = (c_1, \ldots, c_m) \qquad Q = \sum_{u=1}^{t-1} \sum_{v=u+1}^{t} |i_u - i_v||f_{i_u} - f_{i_v}|^e$$

$$\begin{array}{l} \mathbf{c} = (c_1, \ldots, c_m) \\ \quad \Big\downarrow {\color{red}(1)} \\ c_{i_1} = \cdots = c_{i_t} = 1 \xrightarrow{\color{red}(2)} f_{i_1}, \ldots, f_{i_t} \xrightarrow{\color{red}(3)} Q \text{ and } {\color{red}W} \xrightarrow{\color{red}(4)} r \end{array}$$



Example: Computation of Q, r

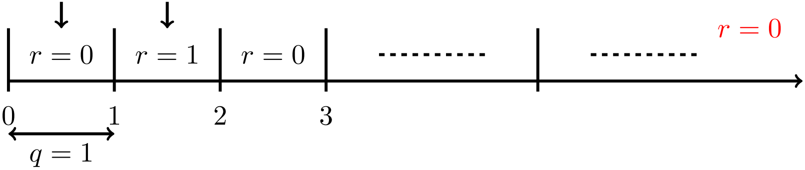
$$\mathbf{c} = (c_1, \dots, c_m) \text{ and } m = 3,\ f_1 = 100, f_2 = 105, f_3 = 110, e = 0.5$$

$$\big\downarrow (1)$$

$$c_1 = c_2 = c_3 = 1 \xrightarrow{(2)} f_1, f_2, f_3 \xrightarrow{(3)} Q \quad \begin{cases} \to r & (4) \\ \to W & (5) \end{cases}$$

$$Q = Q_{12} + Q_{13} + Q_{23} = (105 - 100)^{0.5}$$

$$+2(110 - 100)^{0.5} + (110 - 105)^{0.5} = 10.8$$



Example: Computation of *W*

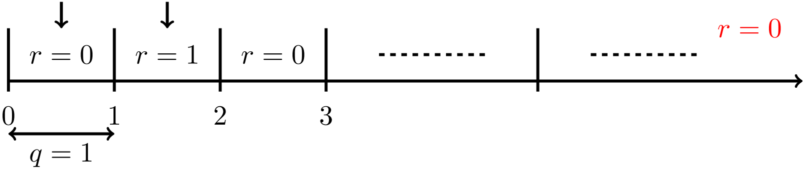
$\mathbf{c} = (c_1, \ldots, c_m)$ and $m = 3,\ f_1 = 100, f_2 = 105, f_3 = 110, e = 0.5$

$$\downarrow (1)$$

$$c_1 = c_2 = c_3 = 1 \xrightarrow{(2)} f_1, f_2, f_3 \xrightarrow{(3)} Q \rightarrow \begin{cases} r & (4) \\ W & (5) \end{cases}$$

$Q = 10.8$ and $r = 0$: $W = (2\hat{n} - 0.5)q + Q$

$= (2.6 - 0.5).1 - 10.8 = 0.7$



Example: Response Correction Based on W

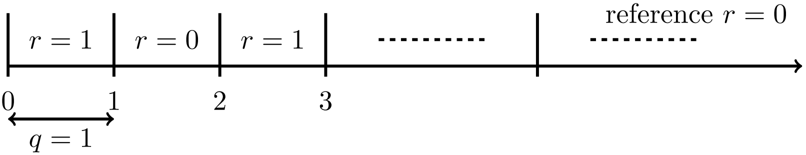
$$\mathbf{c} = (c_1, \ldots, c_m) \qquad Q = \sum_{u=1}^{t-1} \sum_{v=u+1}^{t} |i_u - i_v||f_{i_u} - f_{i_v}|^e$$

$$\Big\downarrow (1)$$

$$c_1 = c_2 = c_3 = 1 \xrightarrow{(2)} f_1, f_2, f_3 \xrightarrow{(3)} Q_{noisy} \text{ and } W \xrightarrow{(4)} r$$

$$Q_{noisy} + W = 10.6 + 0.7 = 11.3, \text{ where } Q_{noisy} = 10.6 \ (4)$$

Thus $r = 0$ and $r =$ reference $r = 0$



Full Examples

Table : Example of Enrollment and Evaluation Phase Computations ($q = 1$ and $Q_{noisy} = Q' = Q$)

r_{ref}	0	0	1	1
Q	8.3	8.7	9.3	9.7
$\hat{n}$	4	5	4	5
W	-0.8	0.8	-0.8	0.8
$Q' + W$	7.5	9.5	8.5	10.5
r	0	0	1	1

Security Notion of Enhanced RO-PUF

Definition

[security notion] Let P denote a PUF instance with m-bit challenge and 1-bit response. A PUF P is considered to be secure if and only if there is no algorithm which can predict, for a given challenge $\mathbf{c}$, the corresponding response r, under the following condition: the accuracy of the prediction is greater than $\frac{1}{2}$.

Observation [1/2]

Table : Relationship between Q, n, δ and W where $Q = n + \delta$

Q	8.3	8.7	9.3	9.7
n	8	8	9	9
δ	0.3	0.7	0.3	0.7
W	-0.8	0.8	-0.8	0.8
δ	$\lvert 0.5 + (-0.8) \rvert$	$1 - \lvert 0.8 - 0.5 \rvert$	$\lvert 0.5 + (-0.8) \rvert$	$1 - \lvert 0.8 - 0.5 \rvert$

We define $Q = n + \delta$ where $0 < \delta < 1$ and $n = \lfloor Q \rfloor$. We have the following observation

Observation

1. ***The parity of*** n ***and reference*** r***:*** *if reference* $r = 0$*, then* n *is even, otherwise* n *is odd*
2. ***Computing*** δ ***based on*** W***:*** *if* $W < 0$*, then* $\delta = |0.5 + W|$*, otherwise* $d = 1 - |W - 0.5|$

Observation [2/2]

$$\mathbf{c}_{i_u i_v} = (c_1, \ldots, c_m)$$
$$\Big\downarrow (1)$$
$$c_{i_u} = c_{i_v} = 1 \xrightarrow{(2)} f_{i_u}, f_{i_v} \xrightarrow{(3)} Q_{i_u i_u} \longrightarrow \begin{cases} r_{i_u i_v} & (4) \\ W_{i_u i_v} & (5) \end{cases}$$

$$\mathbf{c} \rightarrow Q = \sum_{u=1}^{t-1} \sum_{v=u+1}^{t} Q_{i_u i_v}, \text{ where } Q_{i_u i_v} \leftarrow \mathbf{c}_{i_u i_v}$$

Linear relationship between challenge $\mathbf{c}$ and challenges $\mathbf{c}_{i_u i_v}$

challenge $\mathbf{c}$=$(1, 1, 1, 0, 0, ..., 0)$, i.e., $c_1 = c_2 = c_3 = 1$

challenge $\mathbf{c}_{12}, \mathbf{c}_{13}, \mathbf{c}_{23}, Q_{12}, Q_{13}, Q_{23}$ and $Q = Q_{123} = Q_{12} + Q_{13} + Q_{23}$

$Q = n + \delta, Q_{12} = n_{12} + \delta_{12}, Q_{13} = n_{13} + \delta_{13}$ and $Q_{23} = n_{23} + \delta_{23}$

$n + \delta = (n_{12} + \delta_{12}) + (n_{13} + \delta_{13}) + (n_{23} + \delta_{23})$

$n + \delta = (n_{12} + n_{13} + n_{23}) + (\delta_{12} + \delta_{13} + \delta_{23})$

Attack 1: With Helper data *W*

$(\mathbf{c}, r)$ is associated with (Q, W, n, δ) where $Q = n + \delta$

The Observation tells us:

1. If $r = 0$, then n is even. Otherwise n is odd
2. If $W < 0$, then $\delta = |0.5 + W|$. Otherwise $\delta = 1 - |W - 0,5|$.

We define the parity function $p(n) = 0$ if n is even and $p(n) = 1$ if n is odd

Without loss of generality, we predict response r of $\mathbf{c} = (1, 1, 1, 0, ..., 0)$

$Q = Q_{12} + Q_{13} + Q_{23} = (n_{12} + n_{13} + n_{23}) + (\delta_{12} + \delta_{13} + \delta_{23})$

The adversary collects: $(\mathbf{c}_{12}, r_{12}, W_{12})$,$(\mathbf{c}_{13}, r_{13}, W_{13})$ and $(\mathbf{c}_{23}, r_{23}, W_{23})$

The adversary knows: (p_{12}, W_{12}),(p_{13}, W_{13}) and (p_{23}, W_{23})

The adversary knows: (p_{12}, δ_{12}), (p_{13}, δ_{13}) and (p_{23}, δ_{23})

The adversary computes: $\Sigma = \delta_{12} + \delta_{13} + \delta_{23}$ and then

The adversary computes: $p(\Sigma)$ and δ_Σ

The adversary computes: $p(n) = (p_{12} + p_{13} + p_{23} + p(\Sigma))\%2$

Based on the observation, the adversary predicts $r = 0$ if $p(n) = 0$. Otherwise $r = 1$

Attack 2: Without Helper data W [1/2]

$(\mathbf{c}, r)$ is associated with $(Q, \cancel{W}, n, \delta)$ where $Q = n + \delta$

The Observation tells us:

1. If $r = 0$, then n is even. Otherwise n is odd

~~2. If $W < 0$, then $\delta = |0.5 + W|$. Otherwise $\delta = 1 - |W - 0,5|$.~~

We define $p(n) = 0$ if n is even and $p(n) = 1$ if n is odd

Without loss of generality, we predict response r of $\mathbf{c} = (1, 1, 1, 0, ..., 0)$

$Q = Q_{12} + Q_{13} + Q_{23} = (n_{12} + n_{13} + n_{23}) + (\delta_{12} + \delta_{13} + \delta_{23})$

The adversary collects: $(\mathbf{c}_{12}, r_{12}, \cancel{W_{12}})$,$(\mathbf{c}_{13}, r_{13}, \cancel{W_{13}})$ and $(\mathbf{c}_{23}, r_{23}, \cancel{W_{23}})$

The adversary knows: $(p_{12}, \cancel{W_{12}})$,$(p_{13}, \cancel{W_{13}})$ and $(p_{23}, \cancel{W_{23}})$

The adversary knows: $(p_{12}, \cancel{\delta_{12}})$, $(p_{13}, \cancel{\delta_{13}})$ and $(p_{23}, \cancel{\delta_{23}})$

~~The adversary computes: $\Sigma = \delta_{12} + \delta_{13} + \delta_{23}$ and then~~

~~The adversary computes: $p(\Sigma)$ and δ_Σ~~

The adversary computes: $p(n) = (p_{12} + p_{13} + p_{23} + p(\cancel{\Sigma}))\%2$

The adversary CAN NOT predict r

Attack 2: Without Helper data *W* [2/2]

$(\mathbf{c}, r)$ is associated with $(Q, \cancel{W}, n, \delta)$ where $Q = n + \delta$

The Observation tells us:

1. If $r = 0$, then n is even. Otherwise n is odd

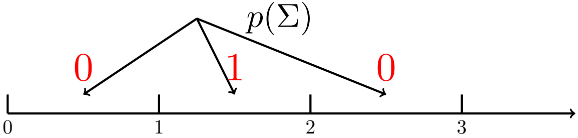
~~2. If $W < 0$, then $\delta = |0.5 + W|$. Otherwise $\delta = 1 - |W - 0,5|$.~~

We define $p(n) = 0$ if n is even and $p(n) = 1$ if n is odd

Without loss of generality, we predict response r of $\mathbf{c} = (1, 1, 1, 0, ..., 0)$

$Q = Q_{12} + Q_{13} + Q_{23} = (n_{12} + n_{13} + n_{23}) + (\delta_{12} + \delta_{13} + \delta_{23})$

The adversary focuses on : $\Sigma = \delta_{12} + \delta_{13} + \delta_{23}$ where $0 < \delta_{12}, \delta_{13}, \delta_{23} < 1$



The adversary computes: $Pr(p(\Sigma) = 0)$=$2/3$ and $Pr(p(\Sigma) = 1) = 1/3$

The adversary computes: $p(n) = (p_{12} + p_{13} + p_{23} + p(\Sigma)\%2$

The adversary CAN predict r with prediction accuracy $= 2/3 > 1/2$

Experimental Results

- **Ring oscillator dataset:**
  [Online] http://rijndael.ece.vt.edu/puf/download.html

Table : Theoretical bias vs. Average Observed bias

t	Theoretical Bias (%)	Average Observed Bias(%)
3	(2/3)*100 = 66.66	66.99
4	(2/4)*100 = 50.00	50.05
5	(3/5)*100 = 60.00	56.77
6	(7/13)*100 = 53.84	50.18

1. PUF Introduction
2. Classic RO-PUF Design
3. Enhanced RO-PUF Design
4. Proposed Attacks on Enhanced RO-PUF
5. Experimental Results
6. **Conclusion**

Conclusion

- Security of the Enhanced RO-PUF is not guaranteed.
  - **With helper data** W**:** the adversary can predict the response r for a given challenge $\mathbf{c}$ with very high prediction accuracy.
  - **Without helper data** W**:** the adversary can still develop a cryptanalytic algorithm to predict the response r for a given challenge $\mathbf{c}$ with prediction accuracy > 0.5.
- Our future work:
  - Improve the efficiency of the attack without helper data W.
  - Improve the security of Enhanced RO-PUF by modifying the original design.

Thank You for Your Attention

Any Question, Please ?