Efficient Power and Timing Side Channels for Physical Unclonable Functions

CHES, September 26, 2014

U. Rührmair (a), (*), X. Xu (b), (*), J. Sölter (c), A. Mahmoud (a),
M. Majzoobi (d), F. Koushanfar (d), W. Burleson (b)

(a) TU München, (b) University of Massachusetts at Amherst
(c) Freie Universität Berlin, (d) Rice University
(*) These authors contributed equally

Outline

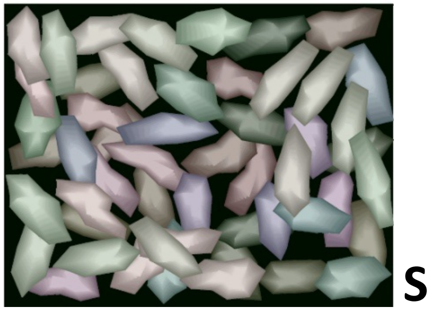
1. **Background: The Arbiter PUF Family, Pure Modeling Attacks, and Their Limitations**
2. Power and Timing Side Channels on XOR Arbiter PUFs
3. Combining Side Channels with Modeling Attacks
4. Our Results
5. Summary

Physical Unclonable Functions (PUFs)

Physical Unclonable Functions (PUFs)

External Stimuli/ **Challenges C_i**

PUF
(= (partly) disordered, unclonable physical system S)



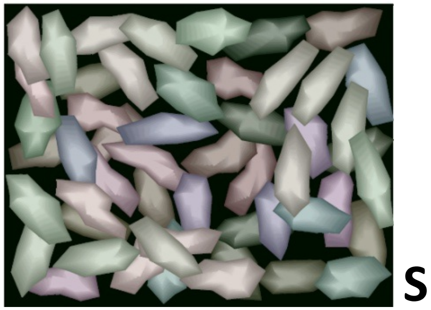
Responses R_i
(R_i is a function of the applied challenge C_i and the specific disorder in S)

(C_i , R_i): Challenge-response pairs **(CRPs)** of the PUF

Physical Unclonable Functions (PUFs)

External Stimuli/
Challenges C_i

PUF
(= (partly) disordered,
unclonable physical system S)



Responses R_i
(R_i is a function of
the applied challenge C_i
and the specific disorder in S)

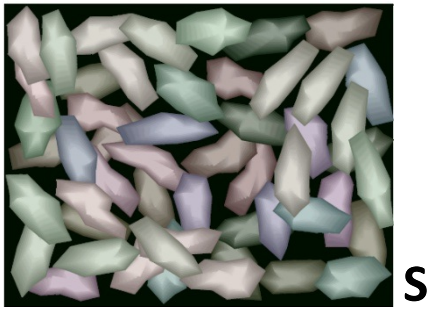
(C_i , R_i): Challenge-response pairs **(CRPs)**
of the PUF

Strong PUFs:

Physical Unclonable Functions (PUFs)

External Stimuli/
Challenges C_i

PUF
(= (partly) disordered,
unclonable physical system S)



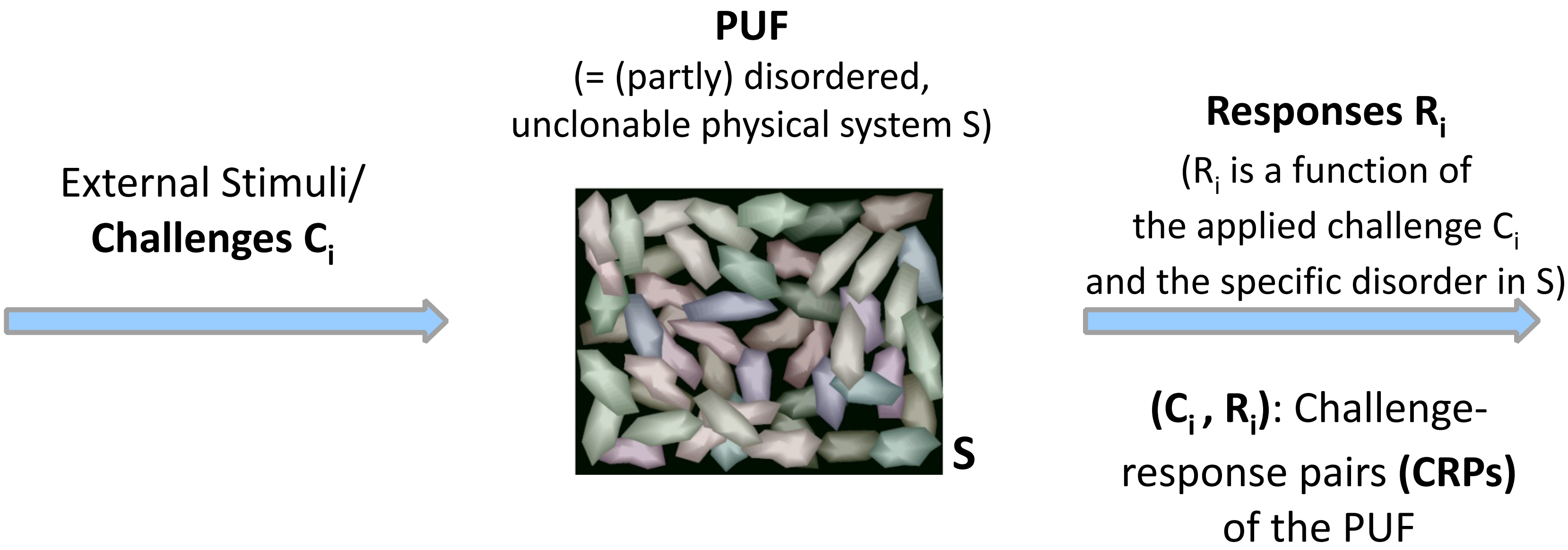
Responses R_i
(R_i is a function of
the applied challenge C_i
and the specific disorder in S)

(C_i , R_i): Challenge-response pairs **(CRPs)** of the PUF

Strong PUFs:

- Challenge-response interface is publicly accessible
  - **Everyone** who holds physical possession of the Strong PUF can freely apply challenges and read out responses

Physical Unclonable Functions (PUFs)



External Stimuli/
Challenges C_i

PUF
(= (partly) disordered,
unclonable physical system S)

S

Responses R_i
(R_i is a function of
the applied challenge C_i
and the specific disorder in S)

(C_i , R_i): Challenge-
response pairs **(CRPs)**
of the PUF

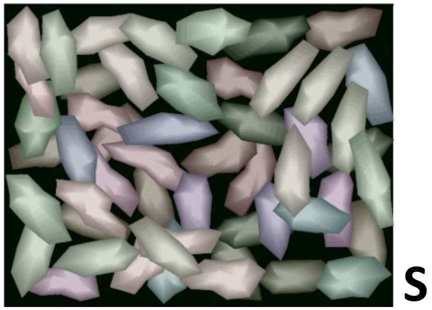
Strong PUFs:

- Challenge-response interface is publicly accessible
  - **Everyone** who holds physical possession of the Strong PUF can freely apply challenges and read out responses
- Very many possible challenges *(ideally exponentially many)*

Physical Unclonable Functions (PUFs)

External Stimuli/
Challenges C_i

PUF
(= (partly) disordered,
unclonable physical system S)



Responses R_i
(R_i is a function of
the applied challenge C_i
and the specific disorder in S)

(C_i, R_i): Challenge-response pairs **(CRPs)** of the PUF

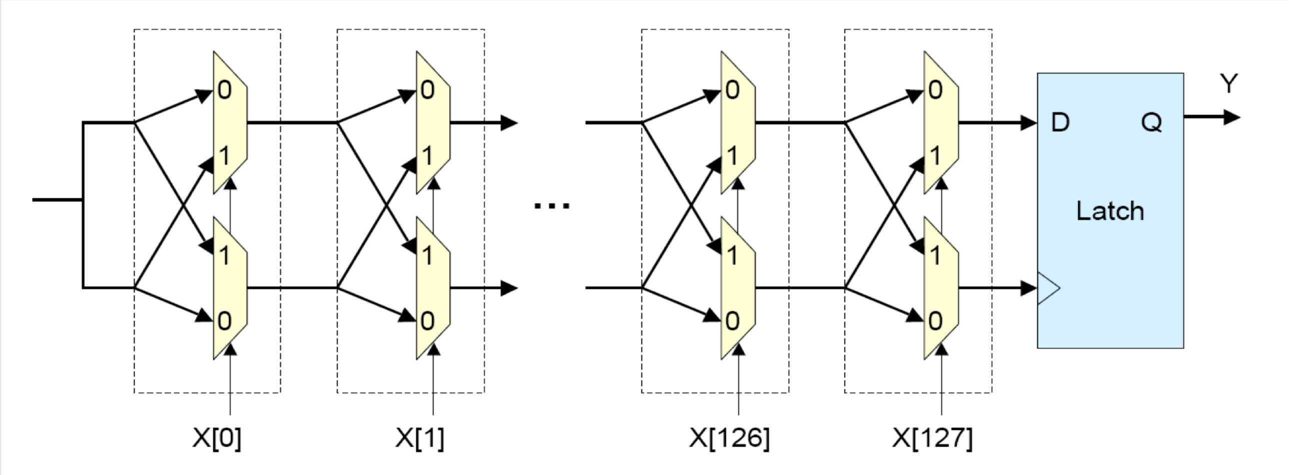
Strong PUFs:

- Challenge-response interface is publicly accessible
  - **Everyone** who holds physical possession of the Strong PUF can freely apply challenges and read out responses
- Very many possible challenges *(ideally exponentially many)*
- Complex: No numerical prediction of unknown responses

The most widespread electrical Strong PUF: **Arbiter PUFs** (1)

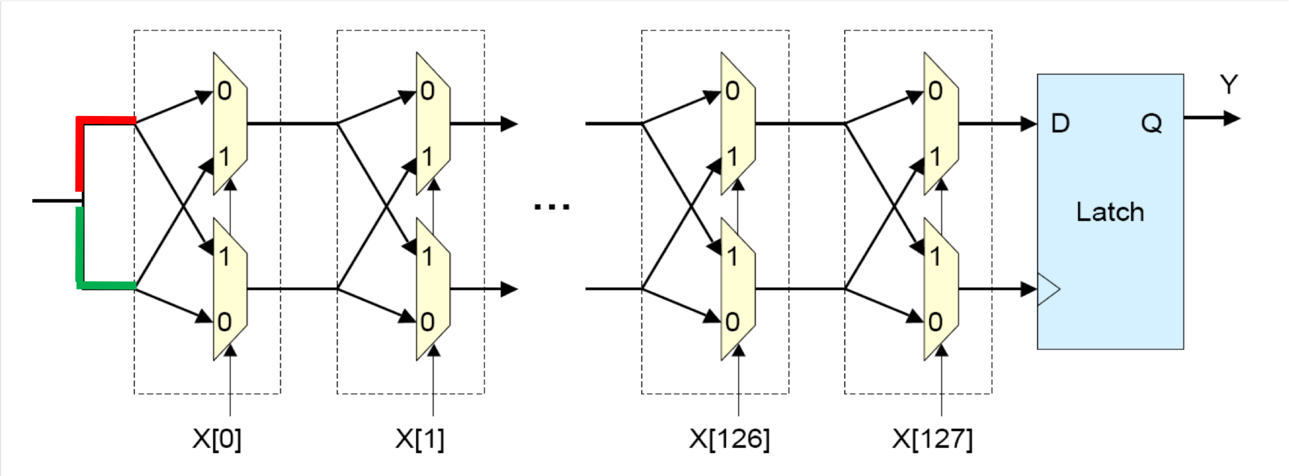
(1) B. Gassend et al, CCS 2002 (2) D. Lim, MIT, 2004, and elsewhere

The most widespread electrical Strong PUF: **Arbiter PUFs** (1)



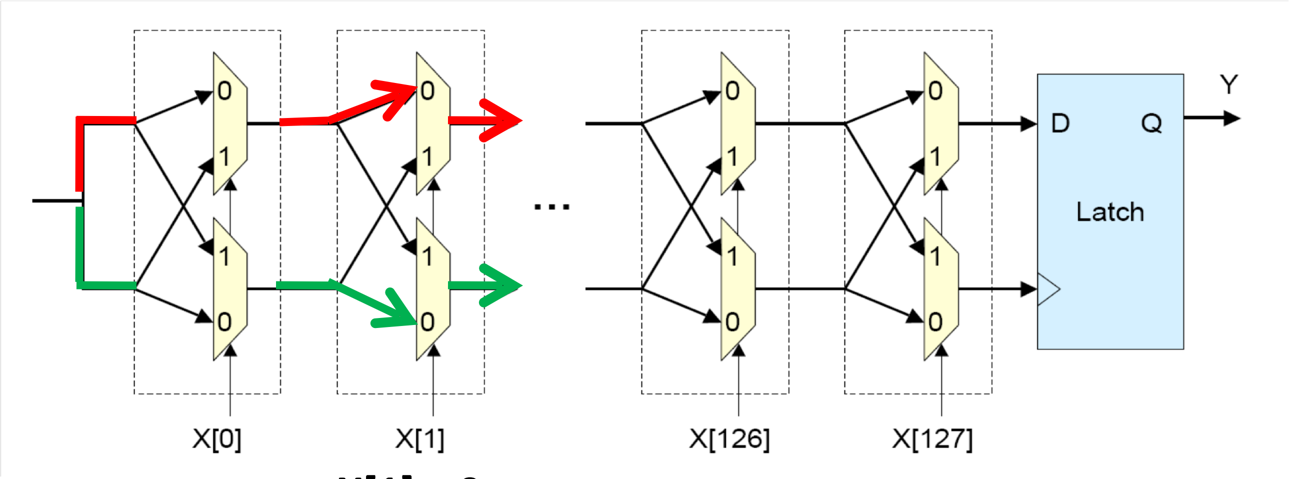
(1) B. Gassend et al, CCS 2002 (2) D. Lim, MIT, 2004, and elsewhere

The most widespread electrical Strong PUF: **Arbiter PUFs** (1)



(1) B. Gassend et al, CCS 2002 (2) D. Lim, MIT, 2004, and elsewhere

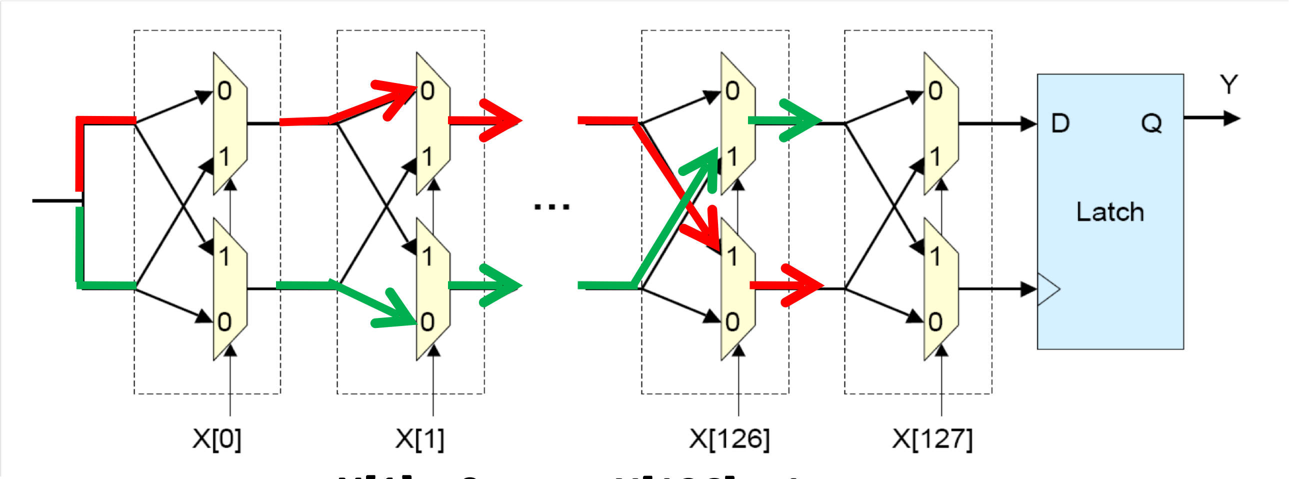
The most widespread electrical Strong PUF: **Arbiter PUFs** (1)



X[1] = 0

(1) B. Gassend et al, CCS 2002 (2) D. Lim, MIT, 2004, and elsewhere

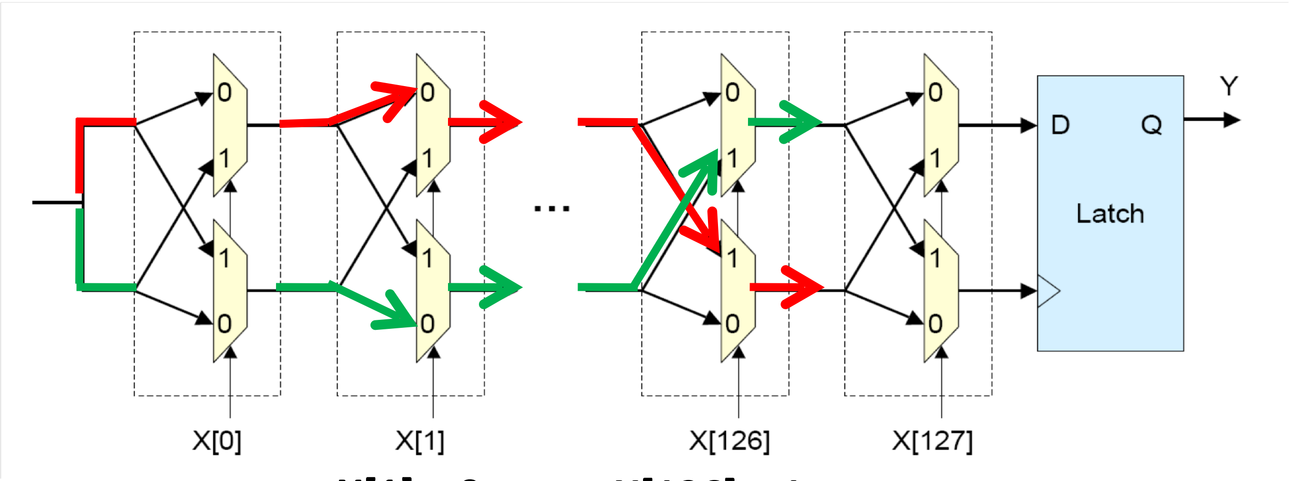
The most widespread electrical Strong PUF: **Arbiter PUFs** (1)



X[1] = 0 **X[126] = 1**

(1) B. Gassend et al, CCS 2002 (2) D. Lim, MIT, 2004, and elsewhere

The most widespread electrical Strong PUF: **Arbiter PUFs** (1)

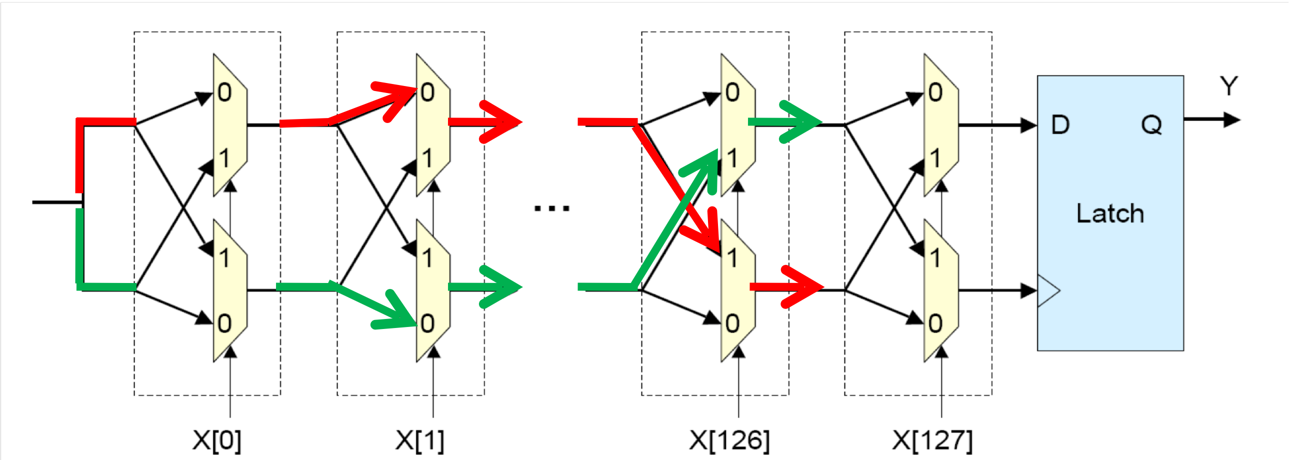


X[1] = 0 **X[126] = 1**

- ***But: Linear!***

(1) B. Gassend et al, CCS 2002 (2) D. Lim, MIT, 2004, and elsewhere

The most widespread electrical Strong PUF: **Arbiter PUFs** (1)



X[1] = 0　　**X[126] = 1**

- ***But: Linear!***
- Adversaries can derive the internal delays via machine learning techniques (in so-called ***„modeling attacks“***) (2)
  – **Complexity of attacks:** *Linear* no. of CRPs, *quadratic* runtime

(1) B. Gassend et al, CCS 2002 　(2) D. Lim, MIT, 2004, and elsewhere

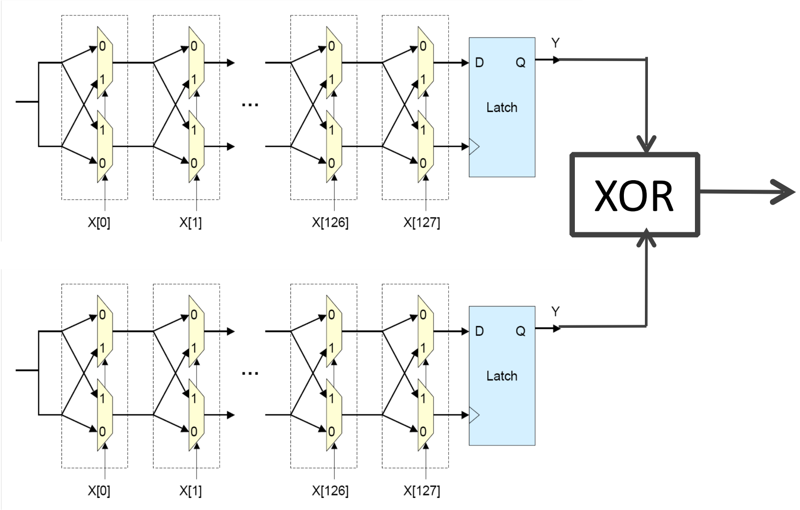
Enhanced Designs of the Arbiter PUF Family

(1) Rührmair et al., CCS 2010.   (2) Rührmair et al., T-IFS 2013

Enhanced Designs of the Arbiter PUF Family

k-XOR Arbiter PUF

G. Suh et al, DAC 2007



(1) Rührmair et al., CCS 2010. (2) Rührmair et al., T-IFS 2013

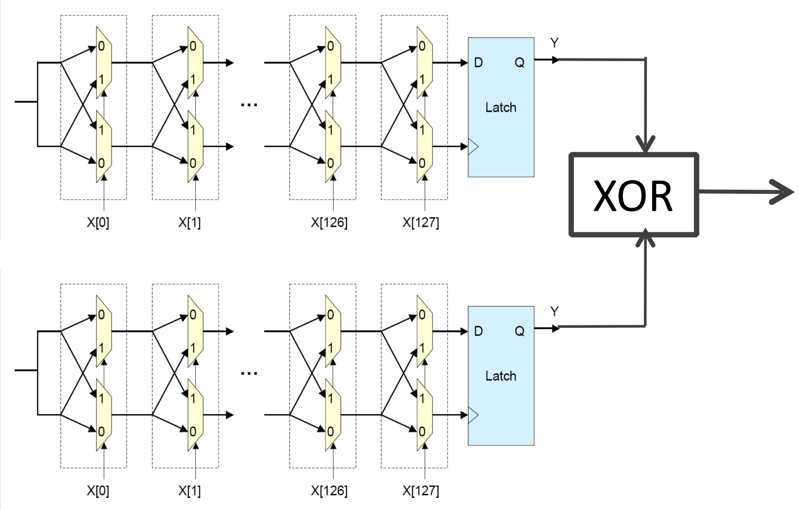
Enhanced Designs of the Arbiter PUF Family

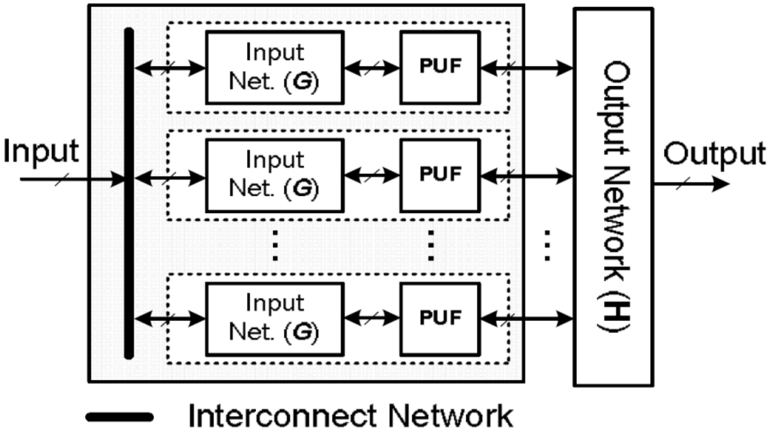
k-XOR Arbiter PUF

G. Suh et al, DAC 2007

Lightweight PUF (LW PUF)

M. Majzoobi et al, ICCAD 2008

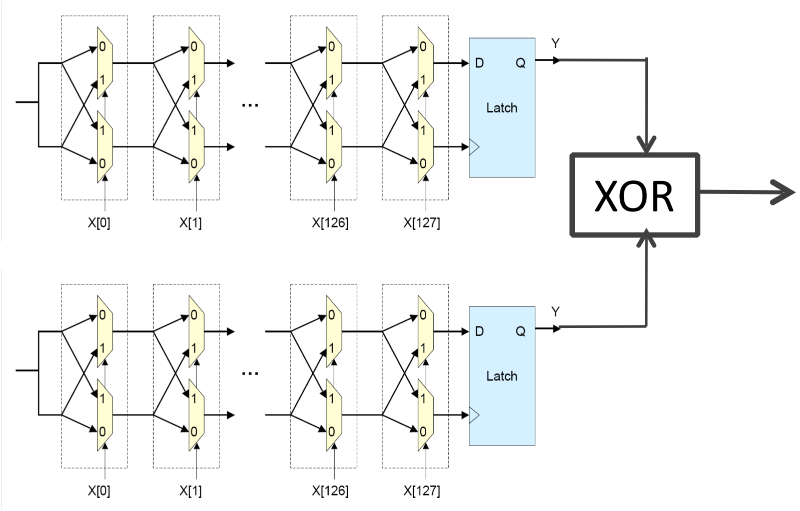




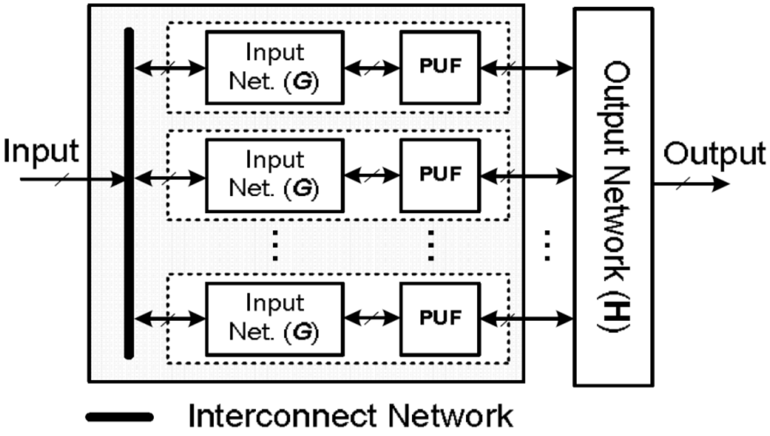
(1) Rührmair et al., CCS 2010. (2) Rührmair et al., T-IFS 2013

Enhanced Designs of the Arbiter PUF Family

k-XOR Arbiter PUF
G. Suh et al, DAC 2007



Lightweight PUF (LW PUF)
M. Majzoobi et al, ICCAD 2008

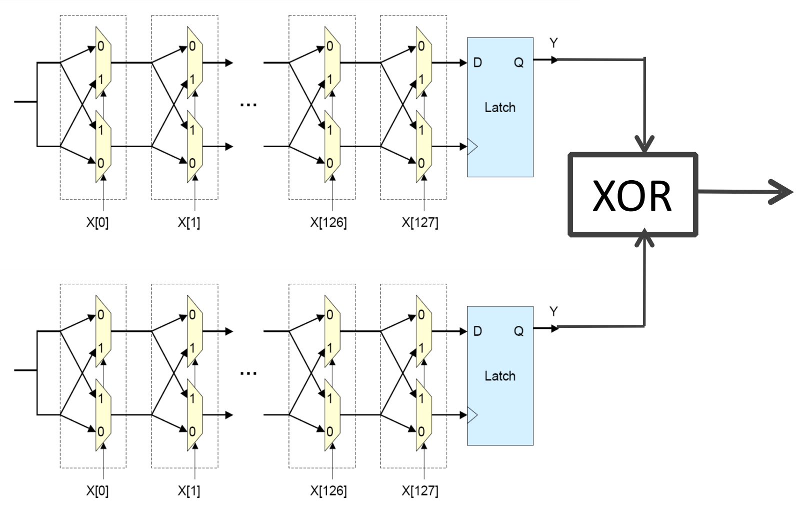


- Both XOR-based… (Also output network of LW PUF is XOR-based)

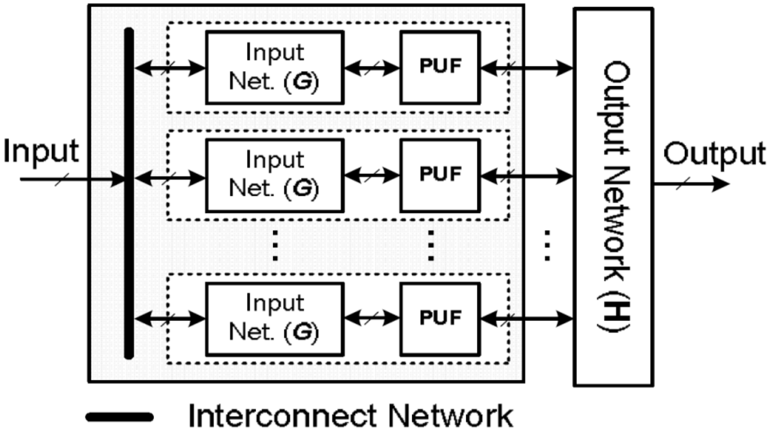
(1) Rührmair et al., CCS 2010. (2) Rührmair et al., T-IFS 2013

Enhanced Designs of the Arbiter PUF Family

k-XOR Arbiter PUF
G. Suh et al, DAC 2007



Lightweight PUF (LW PUF)
M. Majzoobi et al, ICCAD 2008



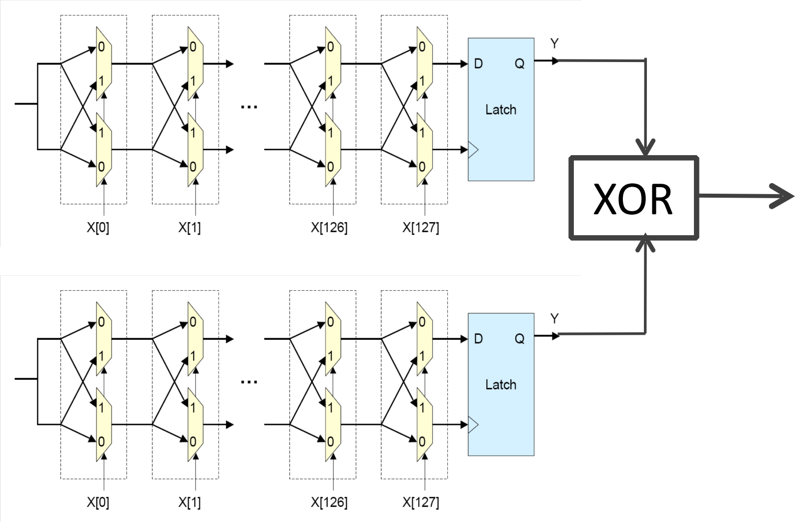
- Both XOR-based… (Also output network of LW PUF is XOR-based)
- ***„Most secure“ members of the Arbiter PUF family!*** (1,2)
  - All others have been broken (1,2)

(1) Rührmair et al., CCS 2010. (2) Rührmair et al., T-IFS 2013

Enhanced Designs of the Arbiter PUF Family

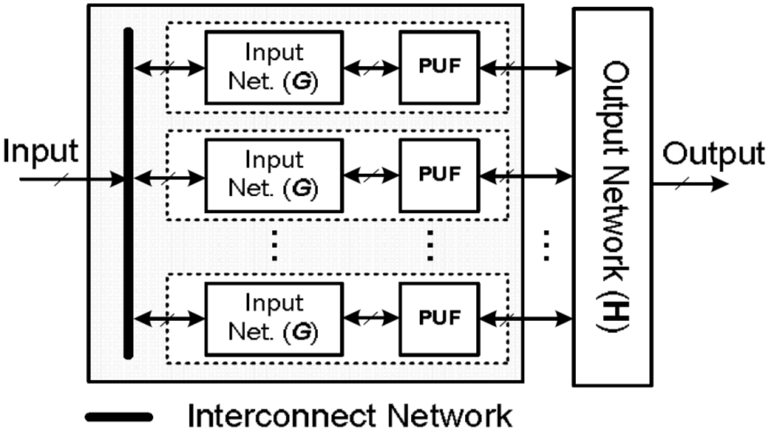
k-XOR Arbiter PUF

G. Suh et al, DAC 2007



Lightweight PUF (LW PUF)

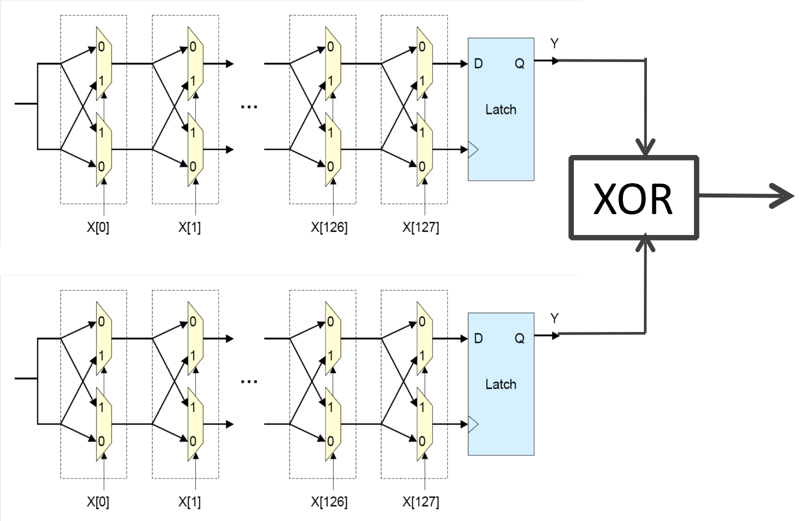
M. Majzoobi et al, ICCAD 2008



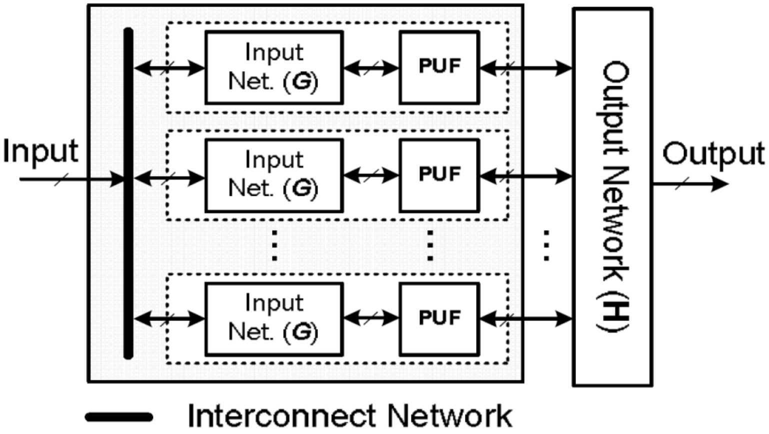
(1) Rührmair et al., CCS 2010. (2) Rührmair et al., T-IFS 2013

Enhanced Designs of the Arbiter PUF Family

k-XOR Arbiter PUF
G. Suh et al, DAC 2007



Lightweight PUF (LW PUF)
M. Majzoobi et al, ICCAD 2008



- ***How secure?***
  - Modeling attacks have **exponential** complexity (in no. of XORs) (1,2)
    - Downside: Also **exponentially bad** stability (in no. of XORs)...
  - 8 XORs **explicitly recommended as secure in literature** (1,2)

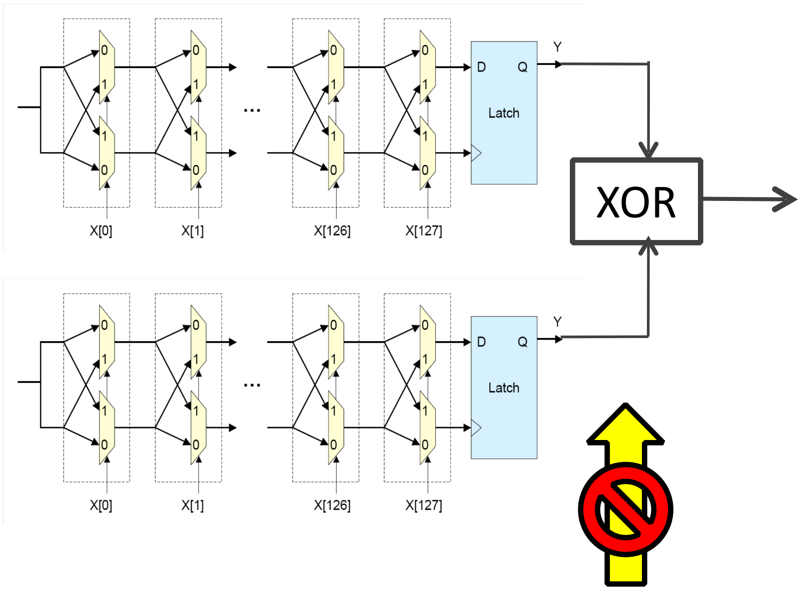
(1) Rührmair et al., CCS 2010. (2) Rührmair et al., T-IFS 2013

Outline

1. Background: Arbiter PUF Variants, Pure Modeling Attacks, and Their Limitations
2. **Power and Timing Side Channels on XOR Arbiter PUFs and LW PUFs**
3. Combining Side Channels with Modeling Attacks
4. Our Results
5. Summary

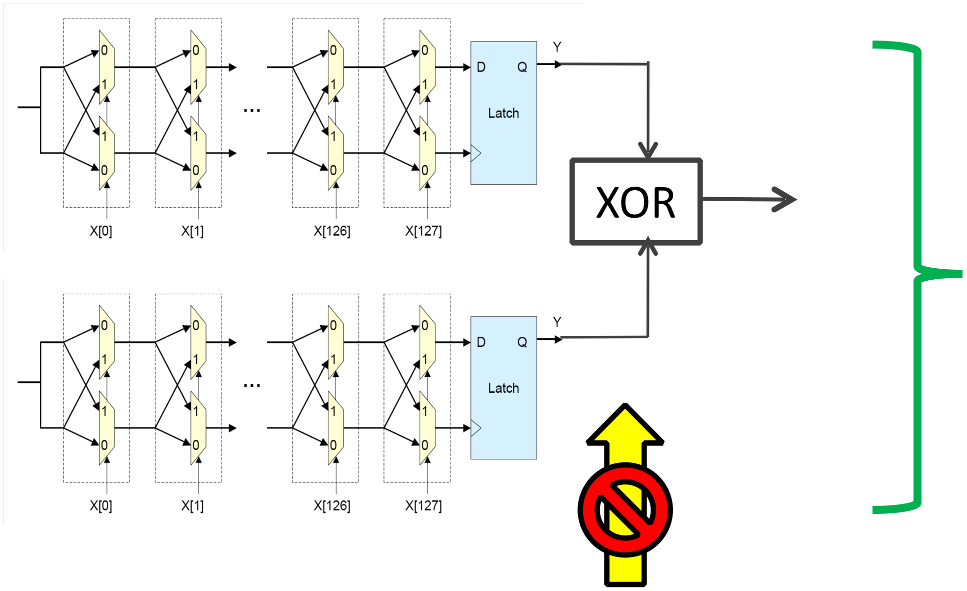
Basic Idea of the Side Channels

Basic Idea of the Side Channels



Ideal, but difficult!!!

Basic Idea of the Side Channels



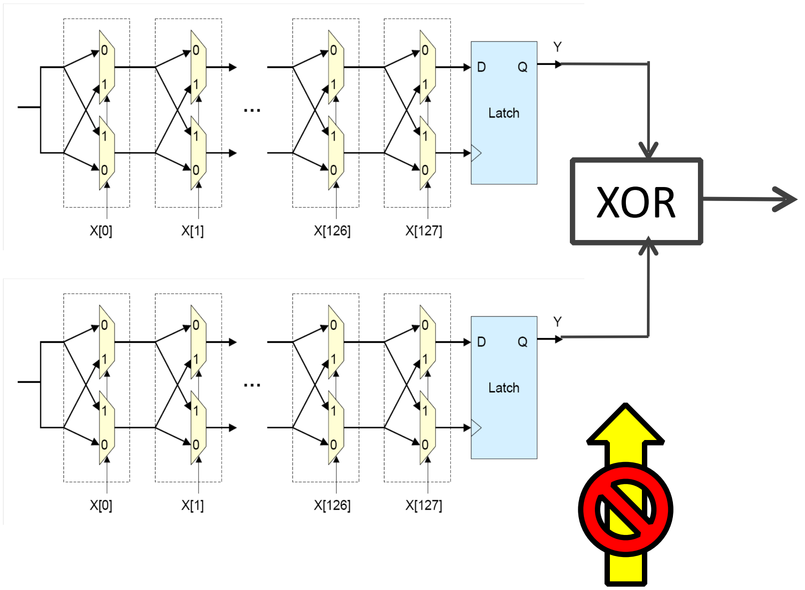
Ideal, but difficult!!!

Since direct access is difficult, we measure a global parameter instead:

The cumulative number of ones (and zeros)
in the individual outputs
of the parallel Arbiter PUFs!

For example: In an 8 XOR Arbiter PUF, 5 individual ouputs are one, 3 are zero
(but unknown which are 0/1)

Basic Idea of the Side Channels



Ideal, but difficult!!!

Since direct access is difficult, we measure a global parameter instead:

The cumulative number of ones (and zeros)
in the individual outputs
of the parallel Arbiter PUFs!

For example: In an 8 XOR Arbiter PUF, 5 individual ouputs are one, 3 are zero
(but unknown which are 0/1)

- ***Either by power analysis or by timing analysis…***

Power Side Channel (PSC)

Power Side Channel (PSC)

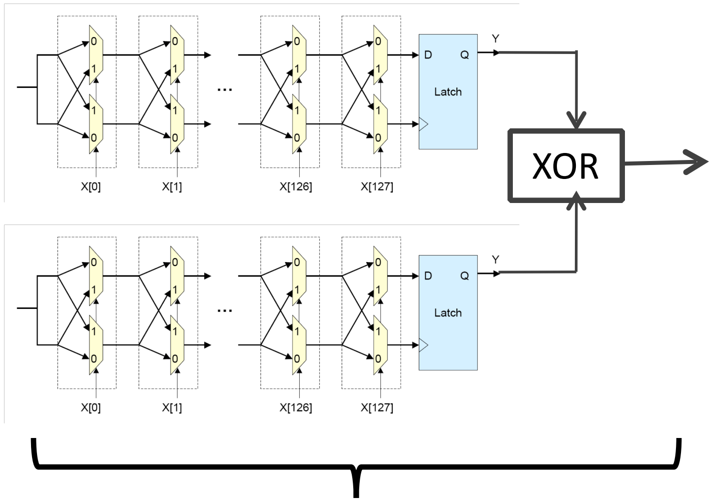
- **Basic idea:** Transition in the latches **from zero to one** draws power…

Power Side Channel (PSC)

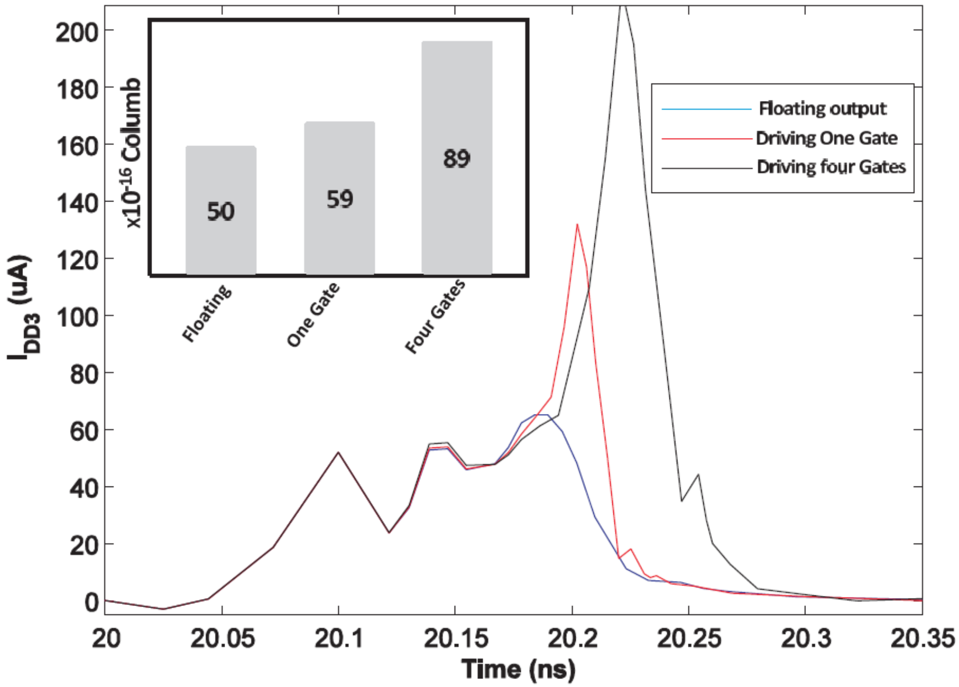
- **Basic idea:** Transition in the latches **from zero to one** draws power…
- More power consumption ***means*** more transitions ***means*** more ones!
  - Provides **cumulative** number of ones/zeros in single Arb PUF outputs

Power Side Channel (PSC)

- **Basic idea:** Transition in the latches **from zero to one** draws power…
- More power consumption ***means*** more transitions ***means*** more ones!
  - Provides **cumulative** number of ones/zeros in single Arb PUF outputs



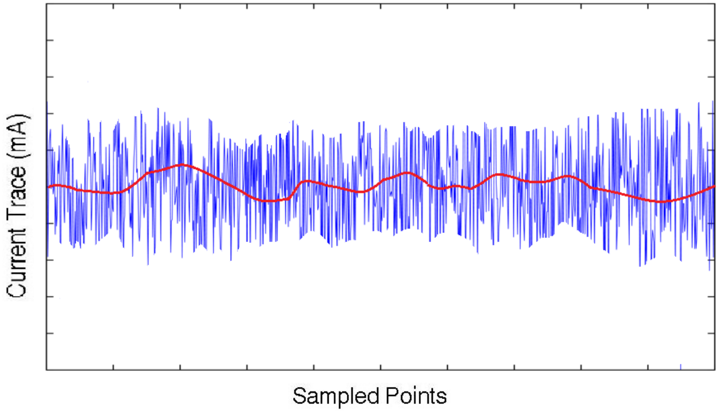
Measure „global“ power consumption



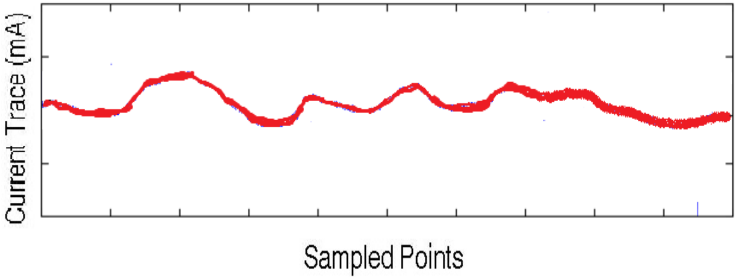
Power Side Channel (PSC) and Noise

- The PUF embedding device has other parts that draw power
- Can we isolate the effect of the latches?
  - Develop **specialized statistical technique** in the paper: Repeat measurements, analyze probability distribution

Power trace of the whole design



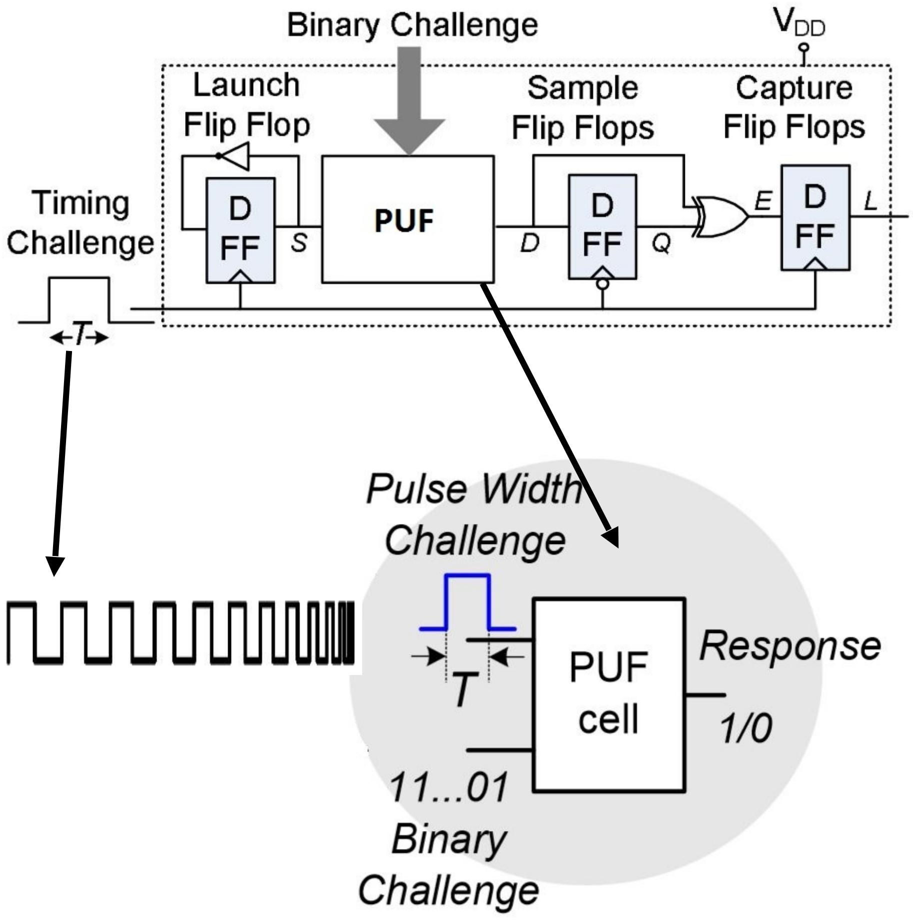
Power SC info we want



Timing Side-Channel (TSC)

(1) M. Majzoobi et al., T-IFS 2011

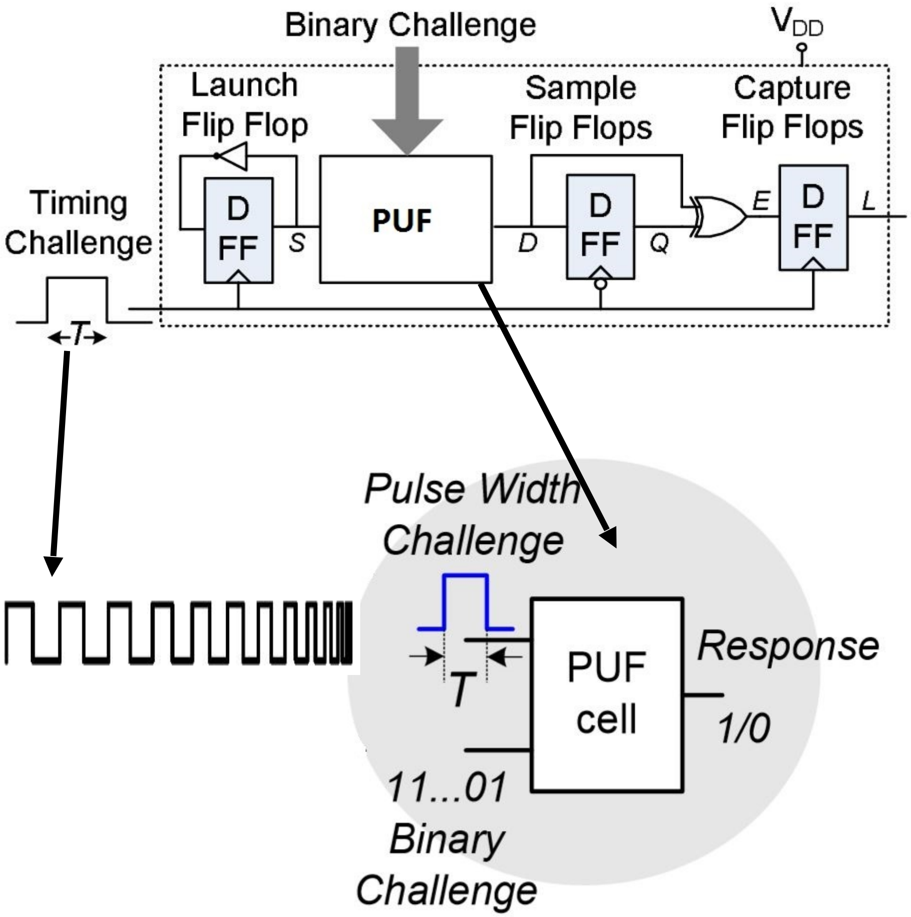
Timing Side-Channel (TSC)



TSC extraction schematic [1]

[1] M. Majzoobi et al., T-IFS 2011

Timing Side-Channel (TSC)



- Sweep clock to approximate the timing of XOR inputs
- Toggle will be created by changes from individual Arbiter PUFs
- Estimate the number of flipping XOR inputs with a good probability

TSC extraction schematic [1]

[1] M. Majzoobi et al., T-IFS 2011

Overview: Power and Timing Side Channels

Overview: Power and Timing Side Channels

- Both provide the **cumulative** number of zeros and ones in the ***k*** individual Arbiter PUF outputs within a ***k***-XOR Arbiter PUF or LW PUF

Overview: Power and Timing Side Channels

- Both provide the **cumulative** number of zeros and ones in the ***k*** individual Arbiter PUF outputs within a ***k***-XOR Arbiter PUF or LW PUF
- **Non-invasive**, **non-destructive**, **inexpensive**

Overview: Power and Timing Side Channels

- Both provide the **cumulative** number of zeros and ones in the ***k*** individual Arbiter PUF outputs within a ***k***-XOR Arbiter PUF or LW PUF
- **Non-invasive**, **non-destructive**, **inexpensive**
- **Timing SC:** Requires only an FPGA board, measurement of one CRP and side channel info takes about 1ms.

Overview: Power and Timing Side Channels

- Both provide the **cumulative** number of zeros and ones in the ***k*** individual Arbiter PUF outputs within a ***k***-XOR Arbiter PUF or LW PUF
- **Non-invasive**, **non-destructive**, **inexpensive**
- **Timing SC:** Requires only an FPGA board, measurement of one CRP and side channel info takes about 1ms.
- **Power SC:** Requires only an FPGA board and an oscilloscope, measurement of one CRP and side channel info takes about 1ms.

Outline

1. Background: Arbiter PUF Variants,
   Pure Modeling Attacks, and Their Limitations
2. Power and Timing Side Channels on
   XOR Arbiter PUFs and LW PUFs
3. **Combining Side Channels with Modeling Attacks**
4. Our Results
5. Summary

Are the Side Channels Useful At All?

Are the Side Channels Useful At All?

- At first sight, the **cumulative** number of zeros/ones appears **useless**…
  - No straightforward relevance for the underlying machine learning (ML) problem…

Are the Side Channels Useful At All?

- At first sight, the **cumulative** number of zeros/ones appears **useless**…
  - No straightforward relevance for the underlying machine learning (ML) problem…
- *It requires a **„tailormade“ ML approach** to exploit this info*
  - Quite non-trivial…
  - One of the main contributions of the paper
  - Summary over next two slides
  - Details: See paper

Machine Learning and Side Channels

(1) Rührmair et al., CCS 2010 (2) Rührmair et al., T-IFS 2013

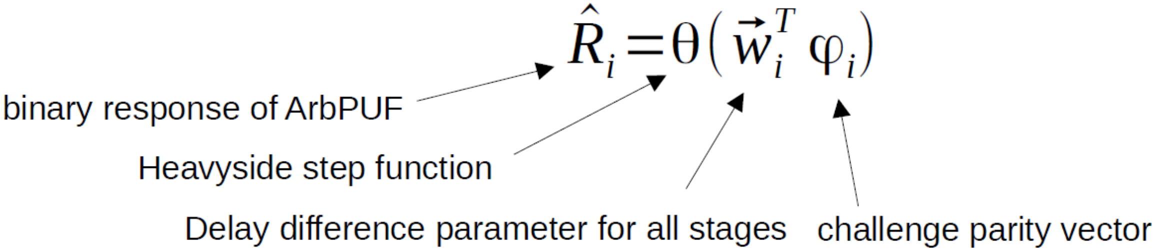
Machine Learning and Side Channels

- General model for i-th Arbiter PUF within k-XOR Arbiter PUF (1,2):

(1) Rührmair et al., CCS 2010 (2) Rührmair et al., T-IFS 2013

Machine Learning and Side Channels

- General model for i-th Arbiter PUF within k-XOR Arbiter PUF (1,2):



$$\hat{R}_i = \theta\left(\vec{w}_i^{\,T}\,\varphi_i\right)$$

binary response of ArbPUF

Heavyside step function

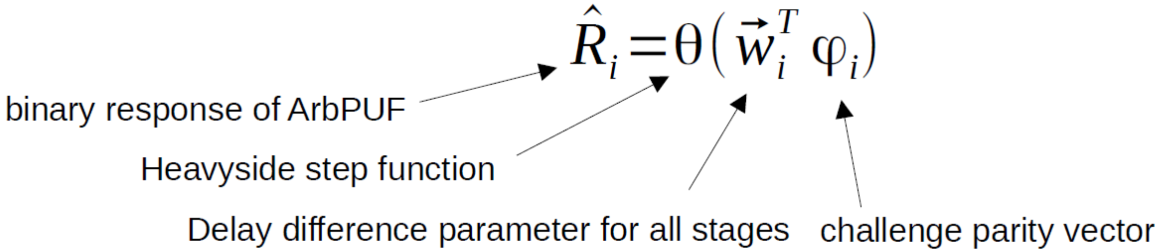
Delay difference parameter for all stages

challenge parity vector

(1) Rührmair et al., CCS 2010 (2) Rührmair et al., T-IFS 2013

Machine Learning and Side Channels

- General model for i-th Arbiter PUF within k-XOR Arbiter PUF (1,2):



$$\hat{R}_i = \theta(\vec{w}_i^T \varphi_i)$$

binary response of ArbPUF

Heavyside step function

Delay difference parameter for all stages

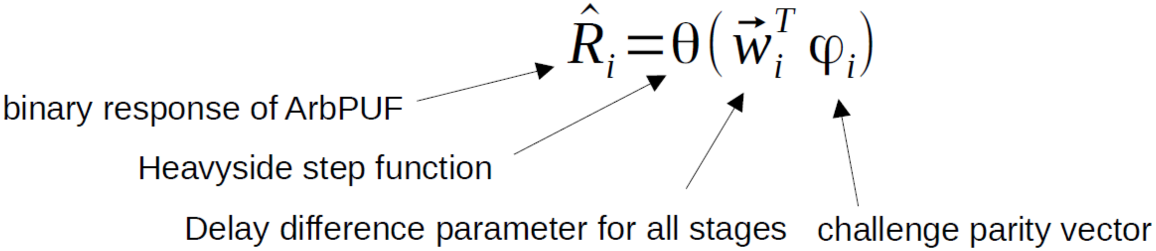
challenge parity vector

- Model the cumulative number of ones as:

(1) Rührmair et al., CCS 2010 (2) Rührmair et al., T-IFS 2013

Machine Learning and Side Channels

- General model for i-th Arbiter PUF within k-XOR Arbiter PUF (1,2):



$$\hat{R}_i = \theta(\vec{w}_i^T \varphi_i)$$

binary response of ArbPUF

Heavyside step function

Delay difference parameter for all stages

challenge parity vector

- Model the cumulative number of ones as:

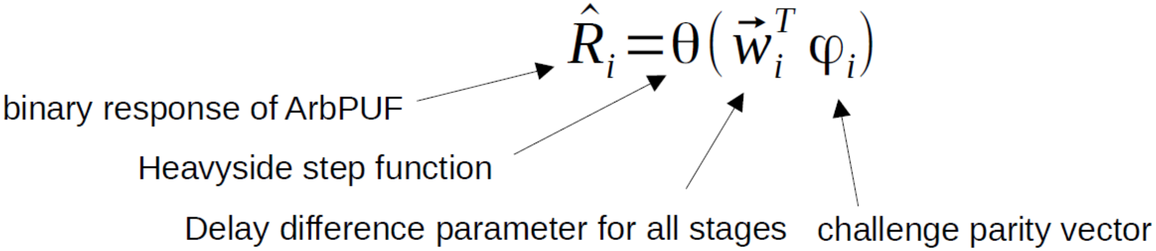
$$\hat{n} = \sum_i \hat{R}_i = \sum_i \theta(\vec{w}_i^T \varphi_i)$$

- **Optimize** PUF-model ***w*** and minimize prediction error ***l*** :

(1) Rührmair et al., CCS 2010 (2) Rührmair et al., T-IFS 2013

Machine Learning and Side Channels

- General model for i-th Arbiter PUF within k-XOR Arbiter PUF (1,2):



$$\hat{R}_i = \theta\left(\vec{w}_i^T \varphi_i\right)$$

binary response of ArbPUF

Heavyside step function

Delay difference parameter for all stages

challenge parity vector

- Model the cumulative number of ones as:

$$\hat{n} = \sum_i \hat{R}_i = \sum_i \theta\left(\vec{w}_i^T \varphi_i\right)$$

- **Optimize** PUF-model ***w*** and minimize prediction error ***l*** :

$$l(\vec{w}, CRPs) = \sum_{(C,n)\in CRPs} \left(\hat{n}(\vec{w}) - n\right)^2$$

(1) Rührmair et al., CCS 2010 (2) Rührmair et al., T-IFS 2013

Machine Learning and Side Channels

(1) Rührmair et al., CCS 2010 (2) Rührmair et al., T-IFS 2013

Machine Learning and Side Channels

- Use the following gradient in the optimization of ***w***:

$$\nabla_{\vec{w}_i} l = \sum_{(C,n)\in CRPs} 2(\hat{n}-n)\,\sigma(\vec{w}_i^T \varphi_i)(1-\sigma(\vec{w}_i^T \varphi_i))\,\varphi_i$$

(1) Rührmair et al., CCS 2010   (2) Rührmair et al., T-IFS 2013

Machine Learning and Side Channels

- Use the following gradient in the optimization of ***w***:

$$\nabla_{\vec{w}_i} l = \sum_{(C,n)\in CRPs} 2(\hat{n}-n)\,\sigma(\vec{w}_i^T \varphi_i)\,(1-\sigma(\vec{w}_i^T \varphi_i))\,\varphi_i$$

- In each summand, only terms with index „**i**“ appear…

(1) Rührmair et al., CCS 2010 (2) Rührmair et al., T-IFS 2013

Machine Learning and Side Channels

- Use the following gradient in the optimization of ***w***:

$$\nabla_{\vec{w}_i} l = \sum_{(C,n)\in CRPs} 2(\hat{n}-n)\,\sigma(\vec{w}_i^T\varphi_i)(1-\sigma(\vec{w}_i^T\varphi_i))\,\varphi_i$$

- In each summand, only terms with index „**i**“ appear…

- Contrary to case **w/o** side channels (1,2) :

$$\nabla_{\vec{w}_i} l = \sum_{(C,n)\in CRPs} 2(\hat{r}-r)\,\varphi_i \prod_{j\neq i} \vec{w}_{\boxed{j}}^T\varphi_j$$

(1) Rührmair et al., CCS 2010   (2) Rührmair et al., T-IFS 2013

Machine Learning and Side Channels

- Use the following gradient in the optimization of ***w***:

$$\nabla_{\vec{w}_i} l = \sum_{(C,n)\in CRPs} 2(\hat{n}-n)\,\sigma(\vec{w}_i^T\varphi_i)(1-\sigma(\vec{w}_i^T\varphi_i))\,\varphi_i$$

- In each summand, only terms with index „**i**“ appear…

- Contrary to case **w/o** side channels (1,2) :

$$\nabla_{\vec{w}_i} l = \sum_{(C,n)\in CRPs} 2(\hat{r}-r)\,\varphi_i \prod_{j\neq i} \vec{w}_{\textcircled{j}}^{T}\varphi_j$$

- This leads to a strong ***(exponential!)*** efficiency improvement

(1) Rührmair et al., CCS 2010 (2) Rührmair et al., T-IFS 2013

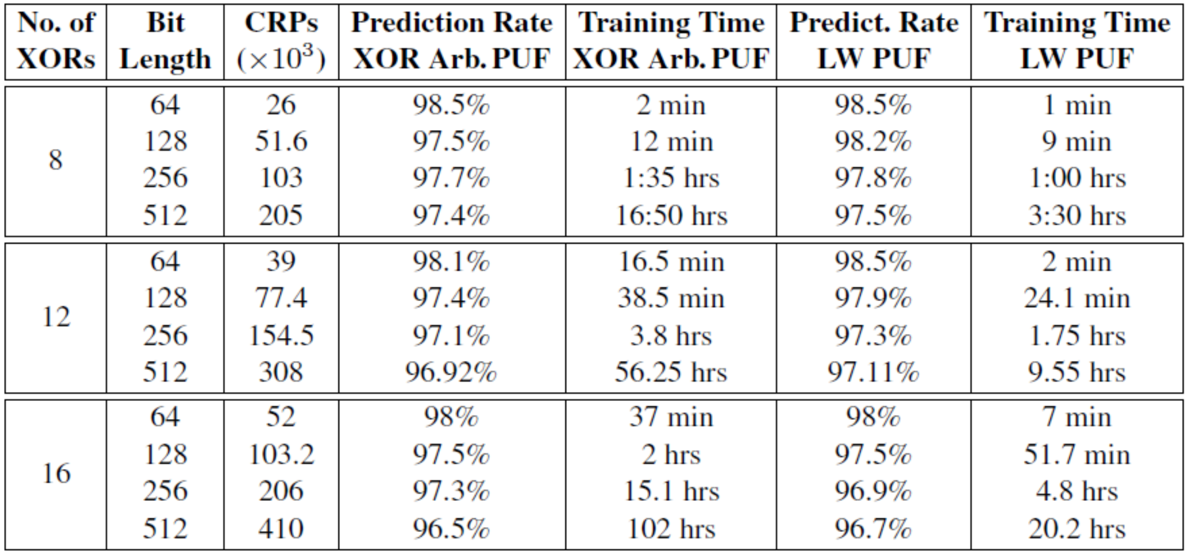
Outline

1. Background: Arbiter PUF Variants,
   Pure Modeling Attacks, and Their Limitations
2. Power and Timing Side Channels on
   XOR Arbiter PUFs and LW PUFs
3. Combining Side Channels with Modeling Attacks
4. **Our Results**
5. Summary

Attack Results on Silicon CRP Data (from FPGAs)

Attack Results on Silicon CRP Data (from FPGAs)

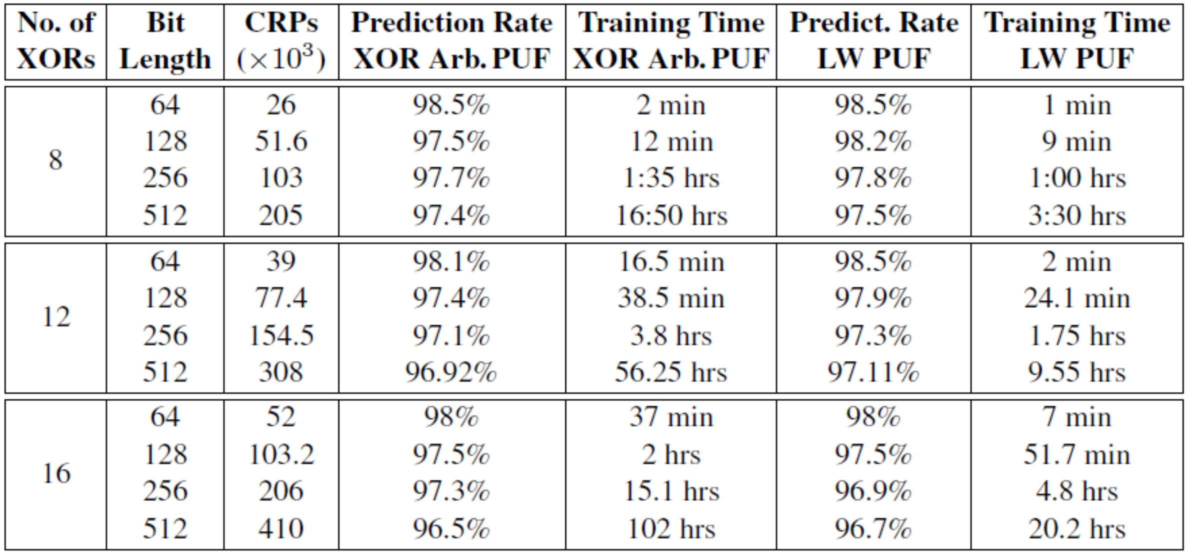
- Timing SC:



No. of XORs	Bit Length	CRPs ($\times 10^3$)	Prediction Rate XOR Arb. PUF	Training Time XOR Arb. PUF	Predict. Rate LW PUF	Training Time LW PUF
8	64	26	98.5%	2 min	98.5%	1 min
	128	51.6	97.5%	12 min	98.2%	9 min
	256	103	97.7%	1:35 hrs	97.8%	1:00 hrs
	512	205	97.4%	16:50 hrs	97.5%	3:30 hrs
12	64	39	98.1%	16.5 min	98.5%	2 min
	128	77.4	97.4%	38.5 min	97.9%	24.1 min
	256	154.5	97.1%	3.8 hrs	97.3%	1.75 hrs
	512	308	96.92%	56.25 hrs	97.11%	9.55 hrs
16	64	52	98%	37 min	98%	7 min
	128	103.2	97.5%	2 hrs	97.5%	51.7 min
	256	206	97.3%	15.1 hrs	96.9%	4.8 hrs
	512	410	96.5%	102 hrs	96.7%	20.2 hrs

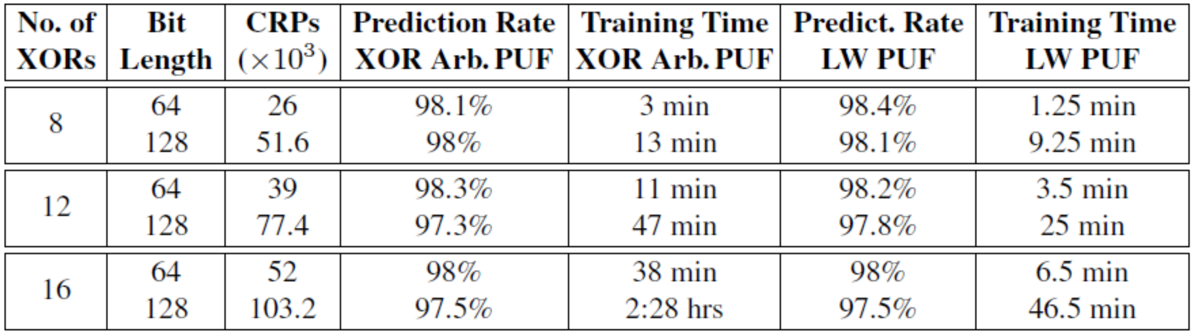
Attack Results on Silicon CRP Data (from FPGAs)

- Timing SC:



No. of XORs	Bit Length	CRPs ($\times 10^3$)	Prediction Rate XOR Arb. PUF	Training Time XOR Arb. PUF	Predict. Rate LW PUF	Training Time LW PUF
8	64	26	98.5%	2 min	98.5%	1 min
	128	51.6	97.5%	12 min	98.2%	9 min
	256	103	97.7%	1:35 hrs	97.8%	1:00 hrs
	512	205	97.4%	16:50 hrs	97.5%	3:30 hrs
12	64	39	98.1%	16.5 min	98.5%	2 min
	128	77.4	97.4%	38.5 min	97.9%	24.1 min
	256	154.5	97.1%	3.8 hrs	97.3%	1.75 hrs
	512	308	96.92%	56.25 hrs	97.11%	9.55 hrs
16	64	52	98%	37 min	98%	7 min
	128	103.2	97.5%	2 hrs	97.5%	51.7 min
	256	206	97.3%	15.1 hrs	96.9%	4.8 hrs
	512	410	96.5%	102 hrs	96.7%	20.2 hrs

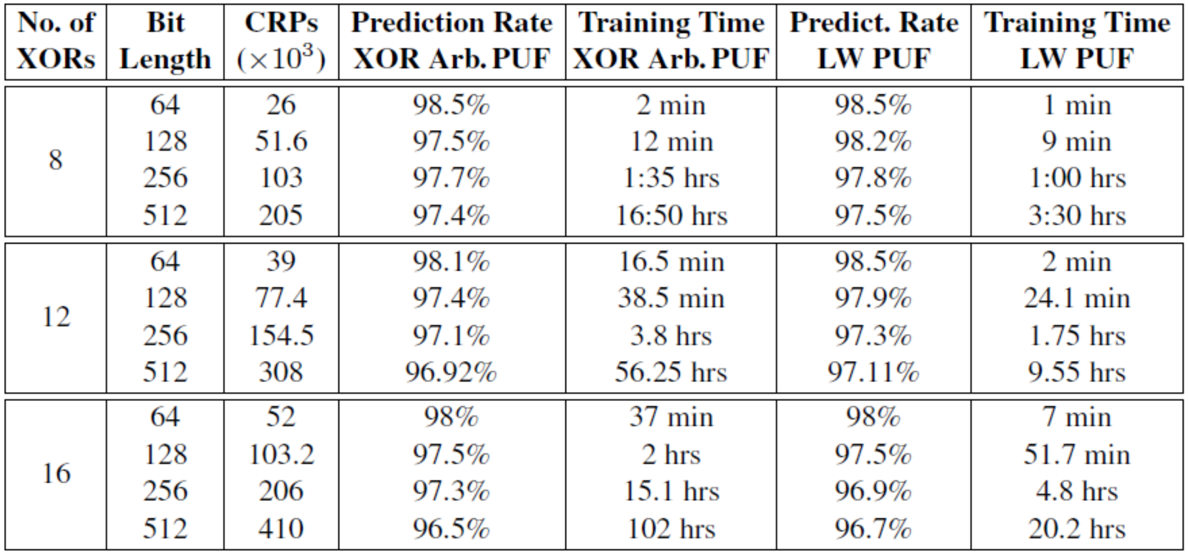
- Power SC:



No. of XORs	Bit Length	CRPs ($\times 10^3$)	Prediction Rate XOR Arb. PUF	Training Time XOR Arb. PUF	Predict. Rate LW PUF	Training Time LW PUF
8	64	26	98.1%	3 min	98.4%	1.25 min
	128	51.6	98%	13 min	98.1%	9.25 min
12	64	39	98.3%	11 min	98.2%	3.5 min
	128	77.4	97.3%	47 min	97.8%	25 min
16	64	52	98%	38 min	98%	6.5 min
	128	103.2	97.5%	2:28 hrs	97.5%	46.5 min

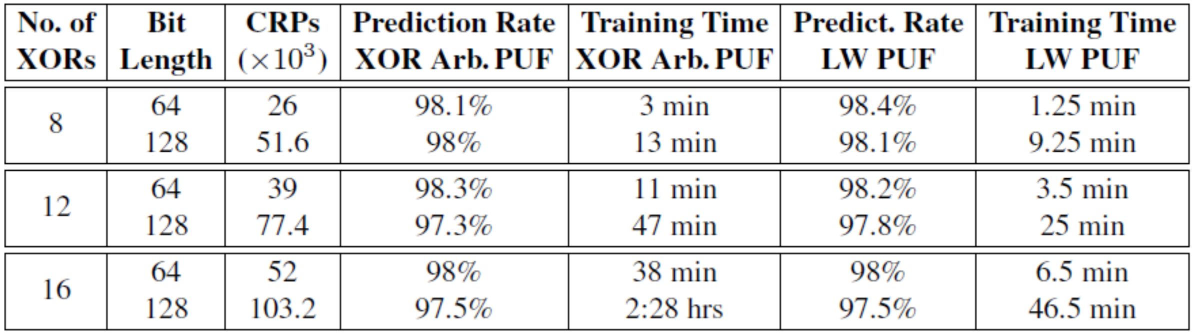
Attack Results on Silicon CRP Data (from FPGAs)

- Timing SC:



No. of XORs	Bit Length	CRPs ($\times 10^3$)	Prediction Rate XOR Arb. PUF	Training Time XOR Arb. PUF	Predict. Rate LW PUF	Training Time LW PUF
8	64	26	98.5%	2 min	98.5%	1 min
	128	51.6	97.5%	12 min	98.2%	9 min
	256	103	97.7%	1:35 hrs	97.8%	1:00 hrs
	512	205	97.4%	16:50 hrs	97.5%	3:30 hrs
12	64	39	98.1%	16.5 min	98.5%	2 min
	128	77.4	97.4%	38.5 min	97.9%	24.1 min
	256	154.5	97.1%	3.8 hrs	97.3%	1.75 hrs
	512	308	96.92%	56.25 hrs	97.11%	9.55 hrs
16	64	52	98%	37 min	98%	7 min
	128	103.2	97.5%	2 hrs	97.5%	51.7 min
	256	206	97.3%	15.1 hrs	96.9%	4.8 hrs
	512	410	96.5%	102 hrs	96.7%	20.2 hrs

- Power SC:

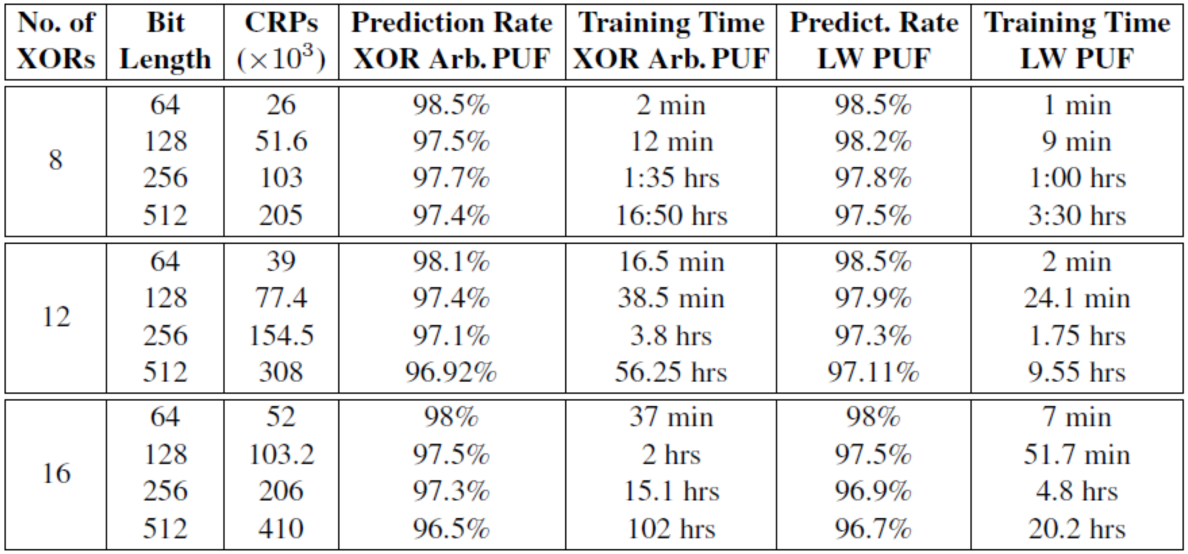


No. of XORs	Bit Length	CRPs ($\times 10^3$)	Prediction Rate XOR Arb. PUF	Training Time XOR Arb. PUF	Predict. Rate LW PUF	Training Time LW PUF
8	64	26	98.1%	3 min	98.4%	1.25 min
	128	51.6	98%	13 min	98.1%	9.25 min
12	64	39	98.3%	11 min	98.2%	3.5 min
	128	77.4	97.3%	47 min	97.8%	25 min
16	64	52	98%	38 min	98%	6.5 min
	128	103.2	97.5%	2:28 hrs	97.5%	46.5 min

Stronger noise in the power SC for large bitlengths!

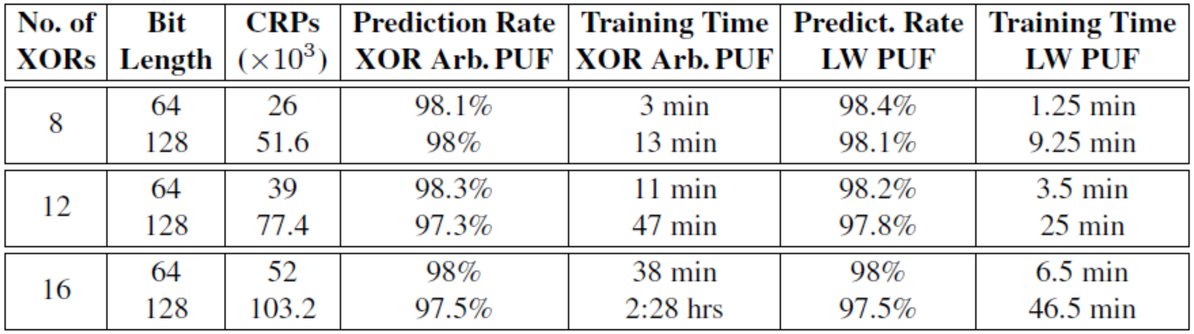
Attack Results on Silicon CRP Data (from FPGAs)

- Timing SC:



No. of XORs	Bit Length	CRPs ($\times 10^3$)	Prediction Rate XOR Arb. PUF	Training Time XOR Arb. PUF	Predict. Rate LW PUF	Training Time LW PUF
8	64	26	98.5%	2 min	98.5%	1 min
	128	51.6	97.5%	12 min	98.2%	9 min
	256	103	97.7%	1:35 hrs	97.8%	1:00 hrs
	512	205	97.4%	16:50 hrs	97.5%	3:30 hrs
12	64	39	98.1%	16.5 min	98.5%	2 min
	128	77.4	97.4%	38.5 min	97.9%	24.1 min
	256	154.5	97.1%	3.8 hrs	97.3%	1.75 hrs
	512	308	96.92%	56.25 hrs	97.11%	9.55 hrs
16	64	52	98%	37 min	98%	7 min
	128	103.2	97.5%	2 hrs	97.5%	51.7 min
	256	206	97.3%	15.1 hrs	96.9%	4.8 hrs
	512	410	96.5%	102 hrs	96.7%	20.2 hrs

- Power SC:



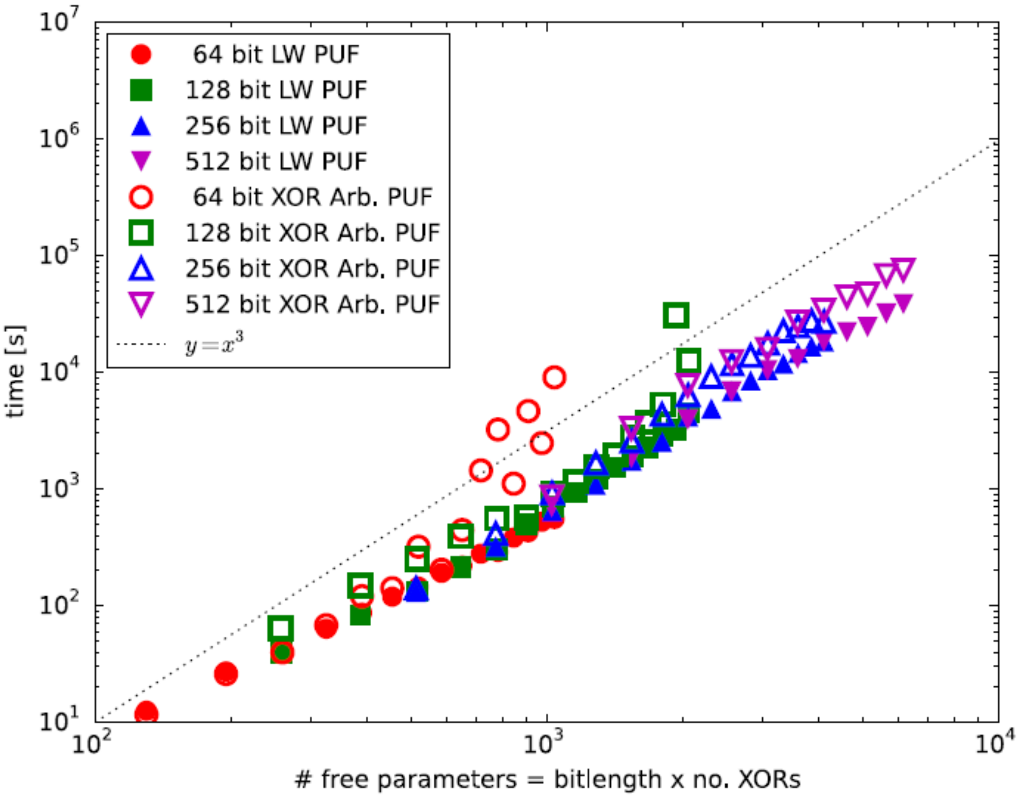
No. of XORs	Bit Length	CRPs ($\times 10^3$)	Prediction Rate XOR Arb. PUF	Training Time XOR Arb. PUF	Predict. Rate LW PUF	Training Time LW PUF
8	64	26	98.1%	3 min	98.4%	1.25 min
	128	51.6	98%	13 min	98.1%	9.25 min
12	64	39	98.3%	11 min	98.2%	3.5 min
	128	77.4	97.3%	47 min	97.8%	25 min
16	64	52	98%	38 min	98%	6.5 min
	128	103.2	97.5%	2:28 hrs	97.5%	46.5 min

Stronger noise in the power SC for large bitlengths!

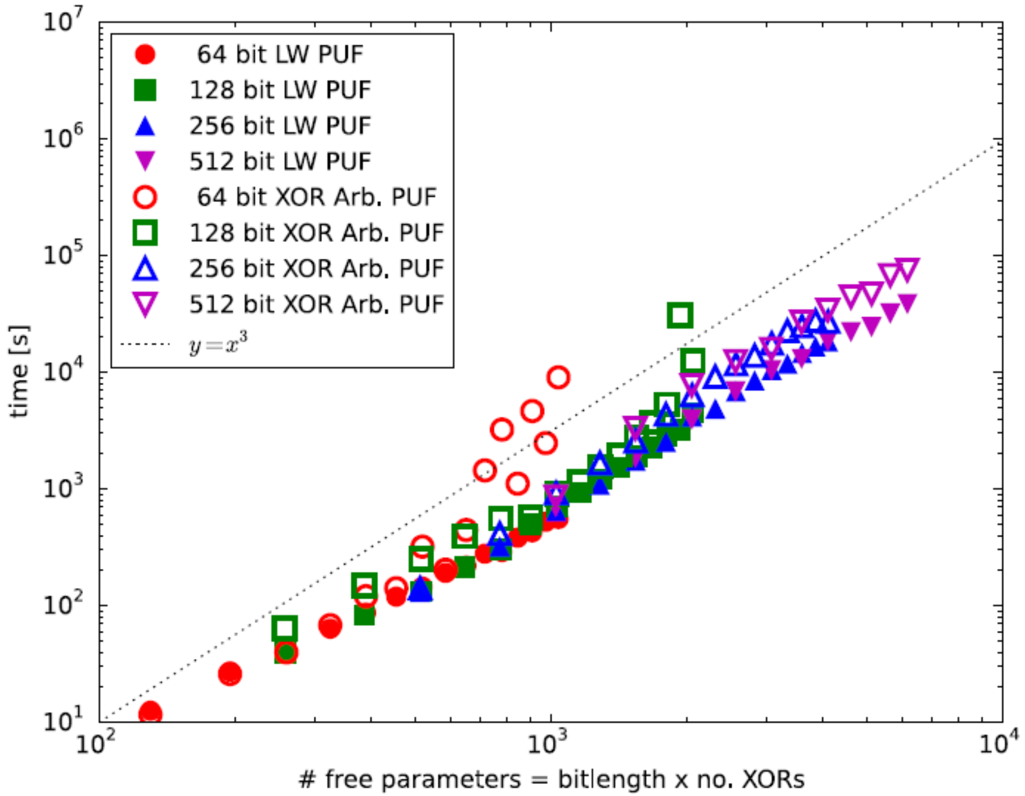
Recall: *8 XORs had explicitly been suggested as secure…*

Asymptotic Performance Analysis on Simulated CRP Data

Asymptotic Performance Analysis on Simulated CRP Data



Asymptotic Performance Analysis on Simulated CRP Data



- Only ***cubic*** runtime and ***linear*** no. of CRPs required!
  - ***Compare:*** *Quadratic* runtime complexity and *linear* no. of CRPs of pure modeling attacks on **standard Arb PUFs** (i.e., without XORs)

Outline

1. Background: Arbiter PUF Variants,
   Pure Modeling Attacks, and Their Limitations
2. Power and Timing Side Channels on
   XOR Arbiter PUFs and LW PUFs
3. Combining Side Channels with Modeling Attacks
4. Our Results
5. **Summary**

Summary

(1) Merli et al., TRUST 2011. (2) Delvaux et al., HOST 2013. (3) Rührmair et al., CCS 2010 and IEEE T-IFS 2013.

Summary

- New attack strategy on XOR-based Arbiter PUFs:
  Combined modeling and side channel attacks
  - **Non-invasive, non-destructive,** inexpensive, very efficient…

(1) Merli et al., TRUST 2011. (2) Delvaux et al., HOST 2013. (3) Rührmair et al., CCS 2010 and IEEE T-IFS 2013.

Summary

- New attack strategy on XOR-based Arbiter PUFs: Combined modeling and side channel attacks
  - **Non-invasive, non-destructive,** inexpensive, very efficient…
- Presented side channels are:
  - The first **power** and **timing** side channels on PUFs
  - The first **direct** side channels on Strong PUFs that can notably **increase** attack performance (compare [1,2,3])

[1] Merli et al., TRUST 2011. [2] Delvaux et al., HOST 2013. [3] Rührmair et al., CCS 2010 and IEEE T-IFS 2013.

Summary

- New attack strategy on XOR-based Arbiter PUFs:
  Combined modeling and side channel attacks
  - **Non-invasive, non-destructive,** inexpensive, very efficient…
- Presented side channels are:
  - The first **power** and **timing** side channels on PUFs
  - The first **direct** side channels on Strong PUFs
    that can notably **increase** attack performance (compare (1,2,3))
- Enables low-degree polynomial attacks for
  LW PUFs and XOR Arbiter PUFs
  - These were considered the most secure members
    of the Arbiter PUF family prior to our attacks
  - Only ***linear*** no. of CRPs and ***cubic*** runtime required

(1) Merli et al., TRUST 2011. (2) Delvaux et al., HOST 2013. (3) Rührmair et al., CCS 2010 and IEEE T-IFS 2013.

Summary

Summary

- *As long as no countermeasures are* ***developed and put in place****,* no existing member of the Arbiter PUF remains secure
  - Some countermeasures are sketched in our paper, but this topic is mainly **ongoing work**

Summary

- *As long as no countermeasures are **developed and put in place**,* no existing member of the Arbiter PUF remains secure
  - Some countermeasures are sketched in our paper, but this topic is mainly **ongoing work**
- *Arms race between codemakers and codebreakers on Strong PUFs continues!*

Summary

- *As long as no countermeasures are **developed and put in place,*** no existing member of the Arbiter PUF remains secure
  - Some countermeasures are sketched in our paper, but this topic is mainly **ongoing work**
- *Arms race between codemakers and codebreakers on Strong PUFs continues!*
- ***Watch this space, there‘s more to come!*** ☺