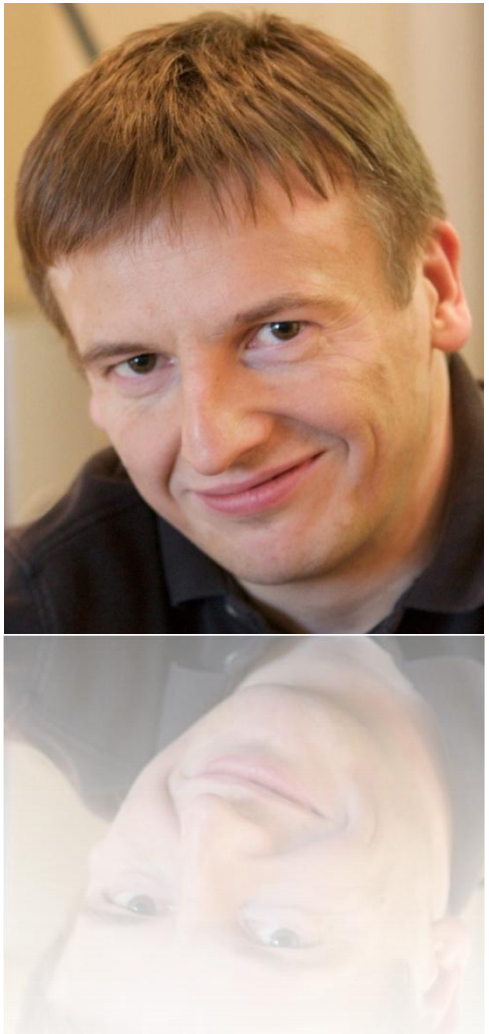
A Comprehensive Set of Schemes for PUF Response Generation

Bilal Habib and Kris Gaj

Cryptographic Engineering Research Group (CERG)
George Mason University
Fairfax, VA, USA

Co-Author

Kris Gaj
Associate Professor

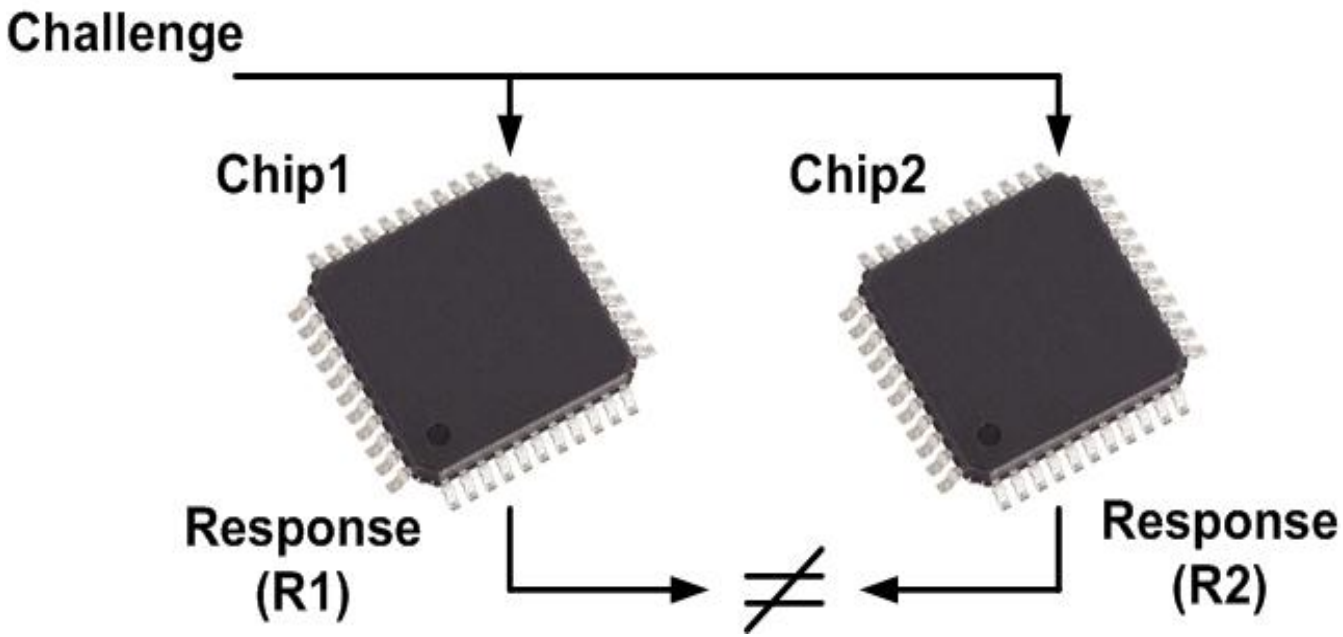


Outline

- PUF Introduction
- PUF Schemes for ID Generation
- Methodology for Ranking the Schemes
- Results
- Conclusions

PUF Introduction

PUF: Physical Unclonable Function



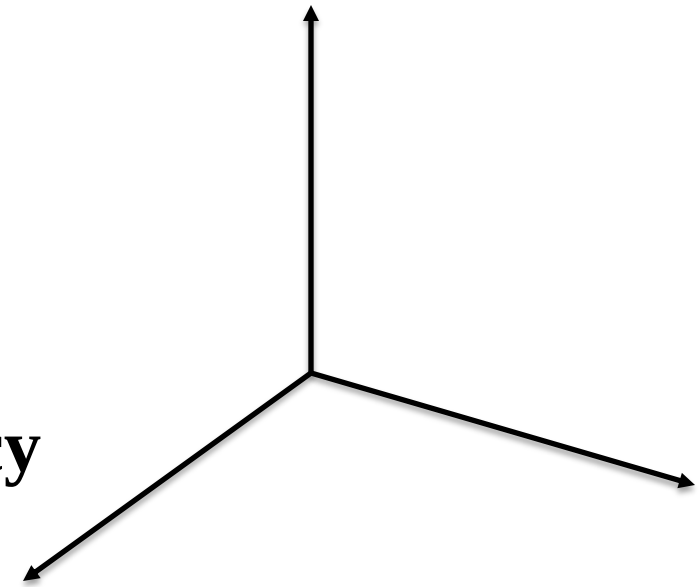
Applications:

- Device Authentication
- <u>Secret Key Generation</u>

PUF Space

PUF Metrics

- Uniqueness
- Uniformity
- Reliability



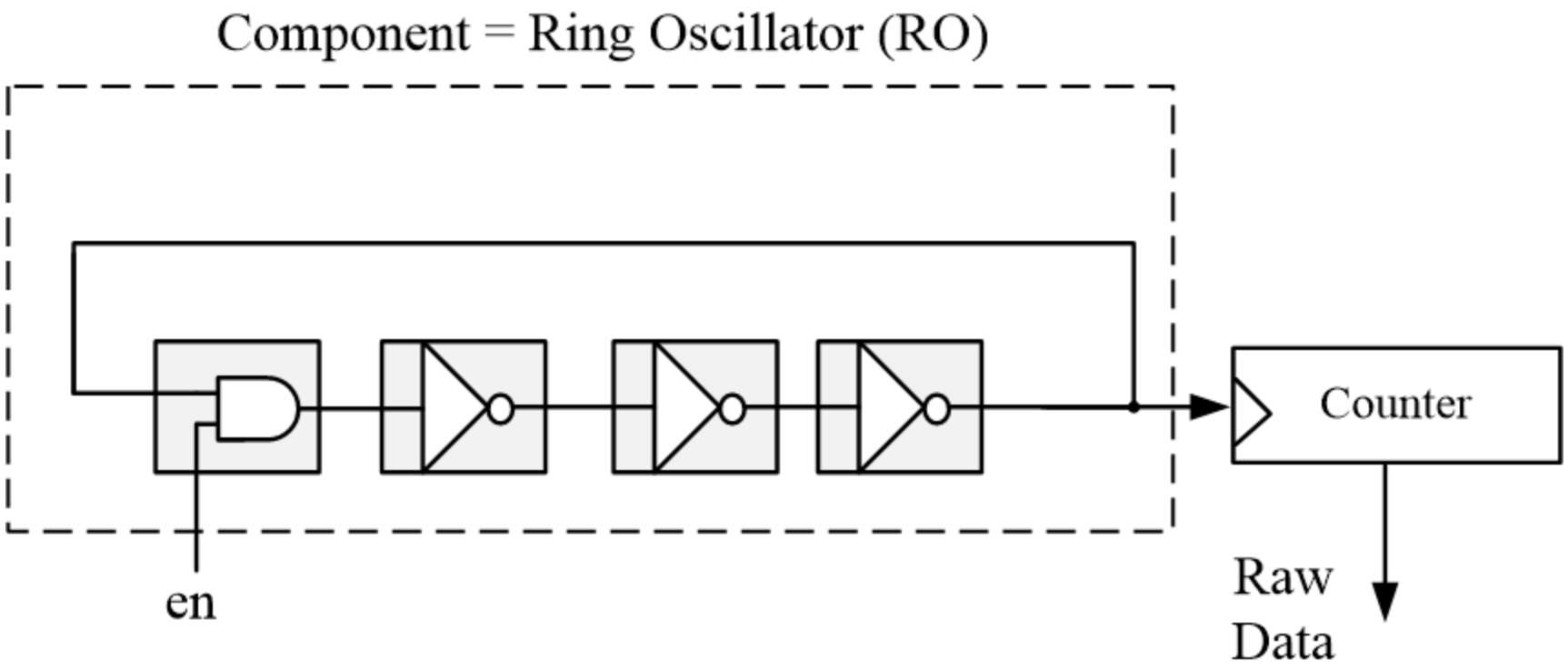
Security

- Unclonability
- Resistance to side-channel
- Resistance to machine learning

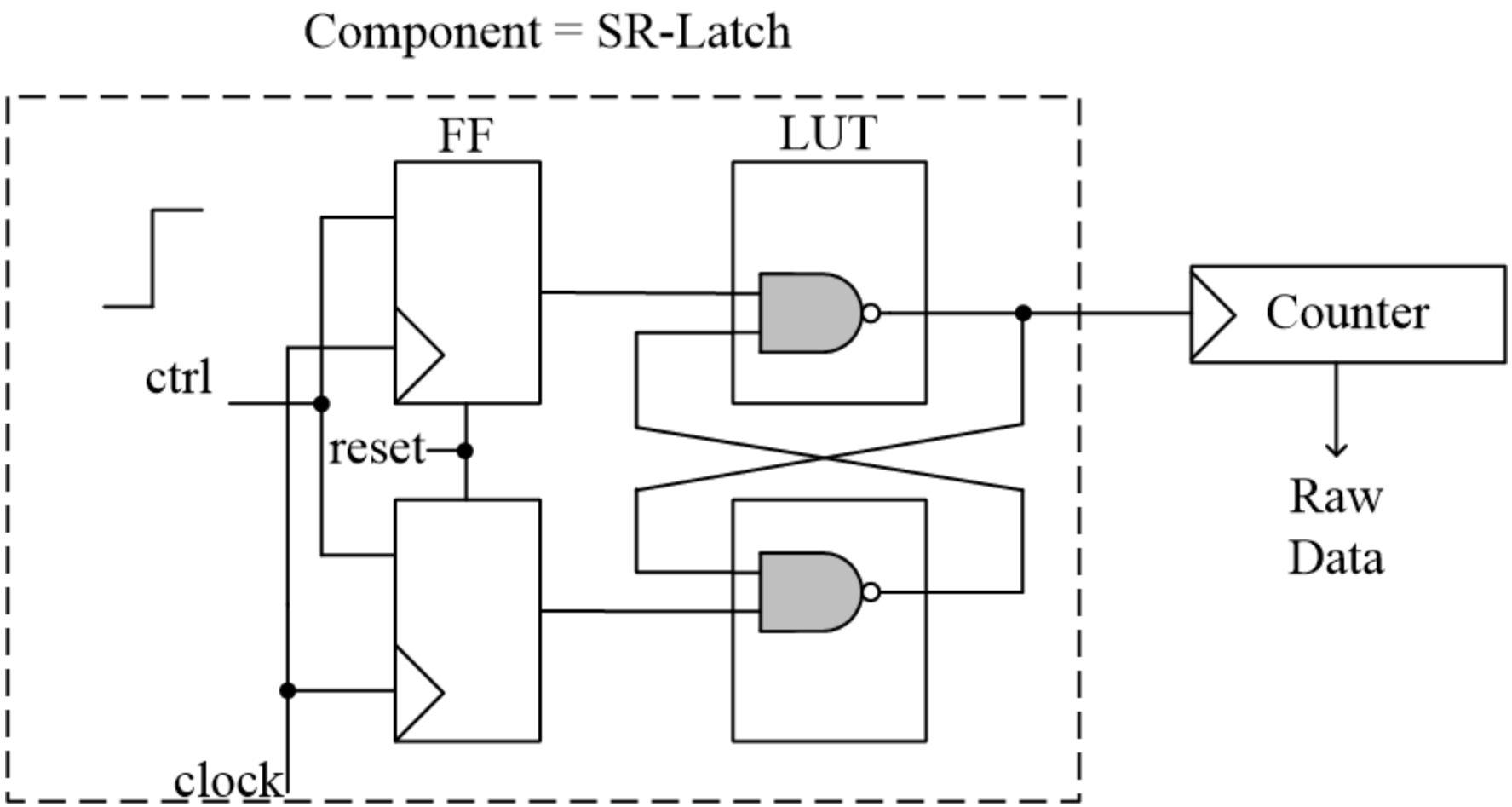
Efficiency

- Area
- Power
- Time

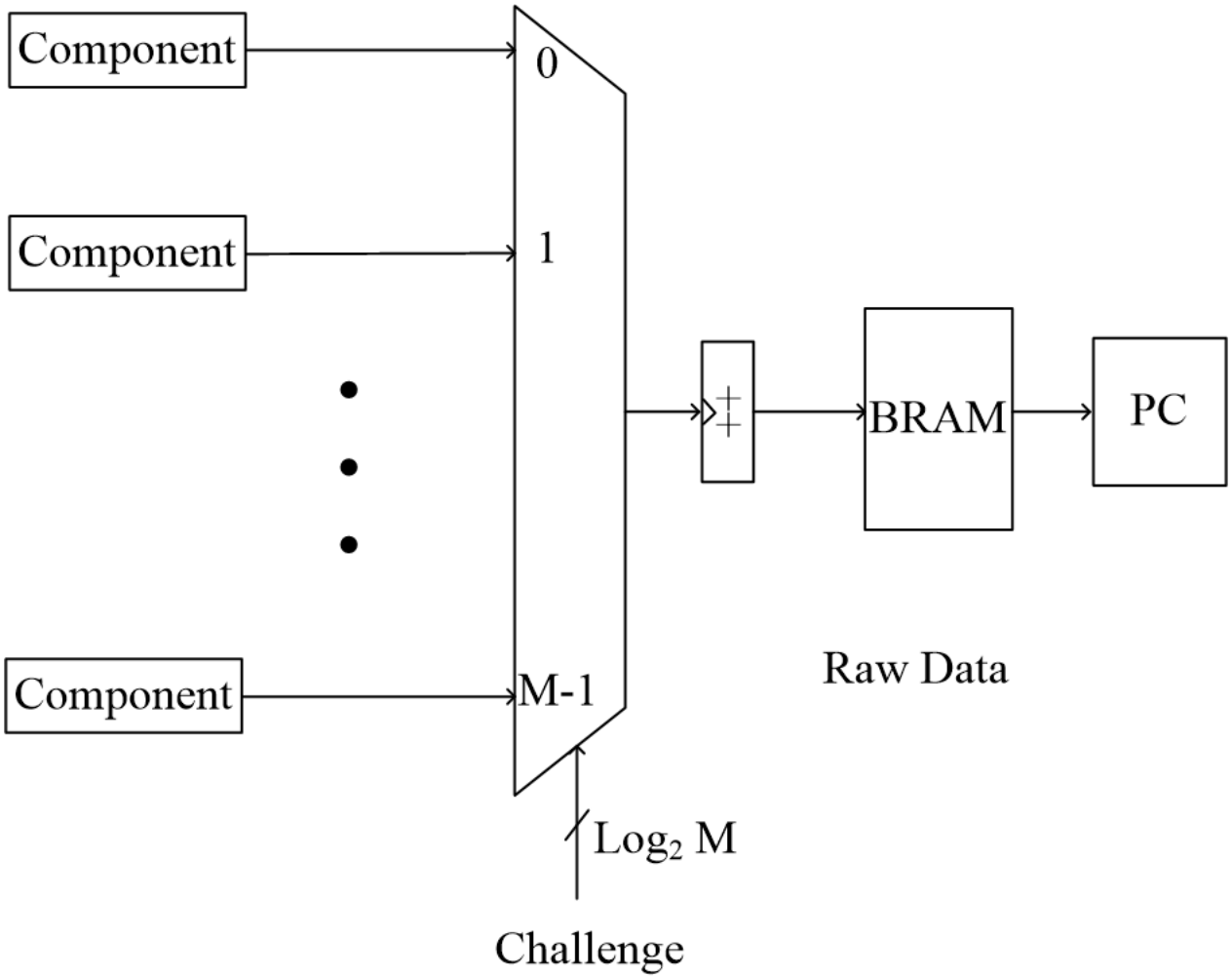
Raw Data for RO-based PUF



Raw Data for SR-Latch PUF

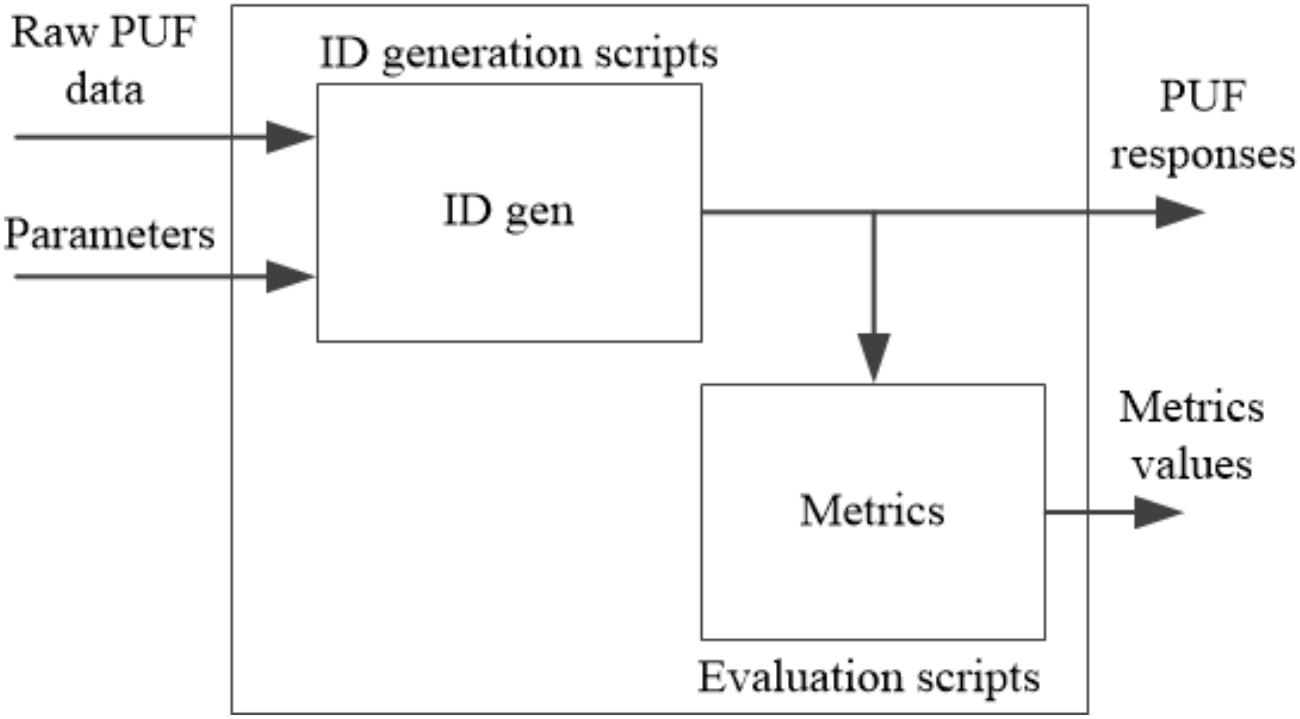


Collection of Raw Data From PUF



PUF ID Generation Schemes

ID Generation and Evaluation



Software scripts were developed for PUF ID Generation and Evaluation

PUF ID Generation Schemes

More
Challenge-Response Pairs

Fewer components per
key bit

Smaller area

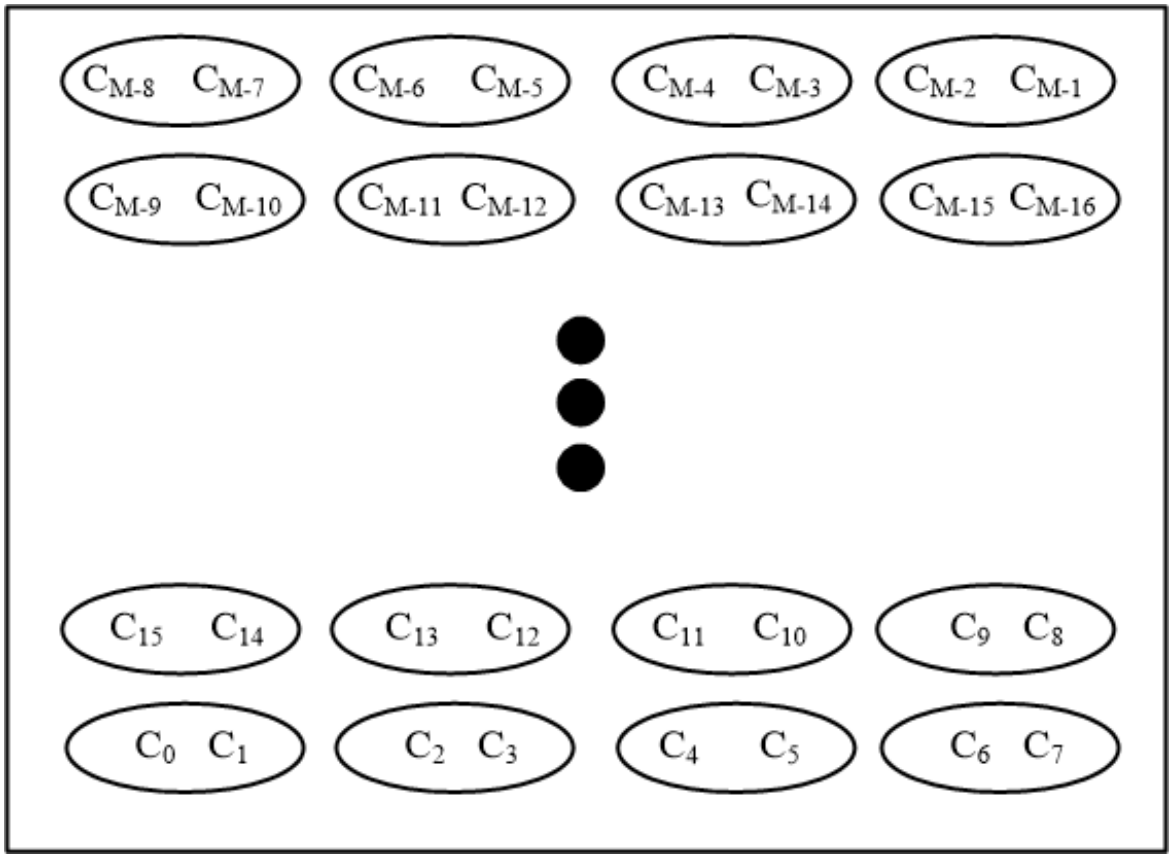
Scheme
Pairwise Comparison (PC)
Comparing the Neighboring Components (CNC)
Binary Lehmer-Gray (BLG)
S-ArbRO-2
Identity Mapping (Id-Map)

More
independent bits

Higher uniqueness

Higher resistance
to machine learning attacks

Pairwise Comparison (PC)

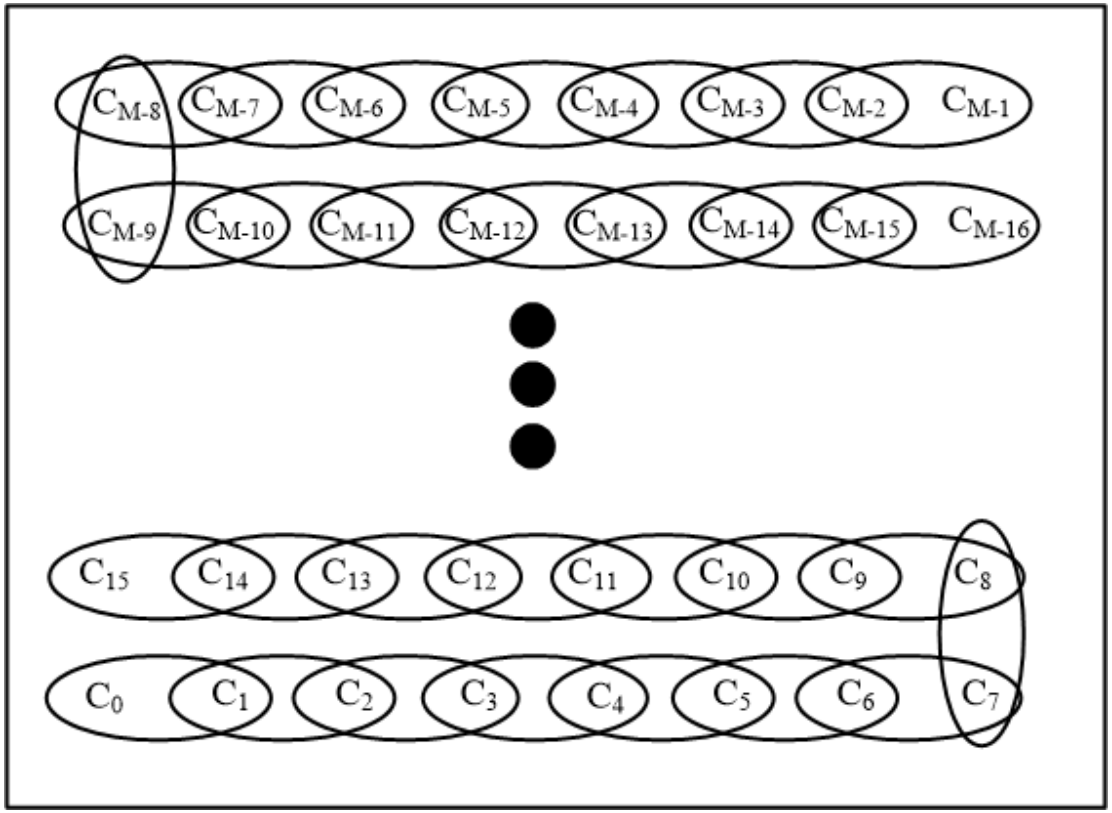


PUF Response Length = | M/2 |

Pairwise Comparison (PC)

- Components: 15, 10, 14, 16, 17, 11
- Pairs: (15 >= 10) (14 < 16) (17 >= 11)
- Response: 1 0 1

Comparing the Neighboring Components (CNC)



PUF Response Length = M-1

Comparing The Neighboring Components (CNC)

- Components: 15, 10, 14, 16, 17, 11
- Pairs:(15>=10) (10<14) (14<16) (16<17) (17>=11)
- Response: 1 0 0 0 1

Binary Lehmer-Gray (BLG) ID Generation

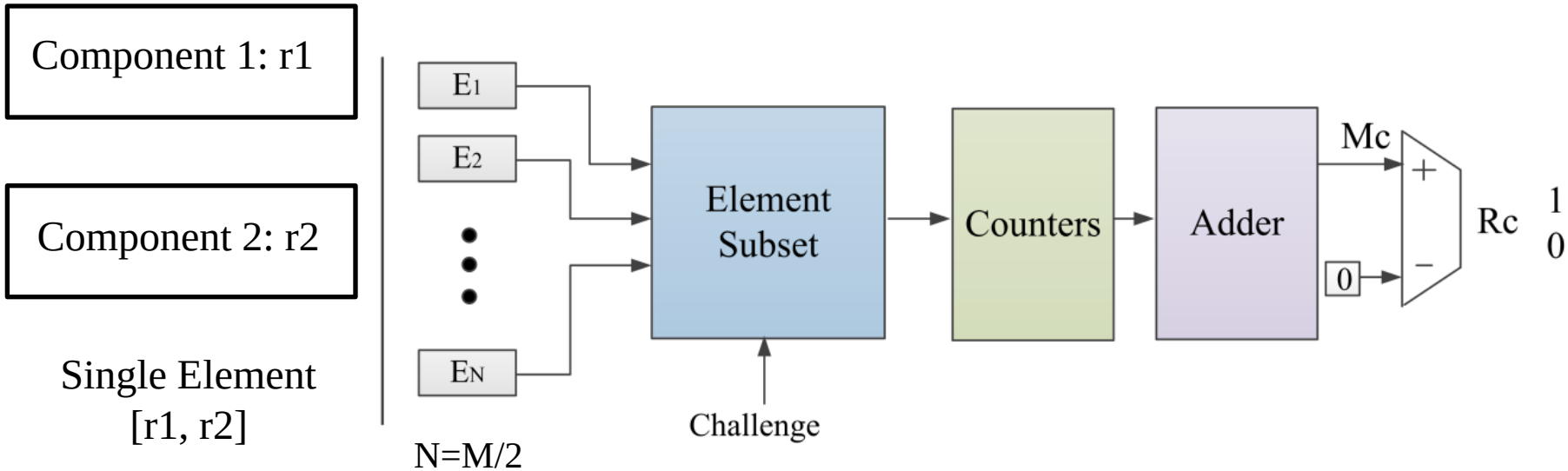
- No. of Components, M = 4 , Set Size, S = 4
- Raw Data from Components: 10, 12, 5, 17.

		sum	bin	Gray
J=1	12>10	Sum = 1	1	1
J=2	5<10, 5<12	Sum = 0	00	00
J=3	17>10, 17>12, 17>5	Sum = 3	11	10

- PUF Response: 1 00 10
- Total Response Length :

$$(M/S) * \sum_{i=2}^{S} \lceil \log_2 i \rceil$$

S-ArbRO-2 Scheme



K = Subset Size

ri – Raw Data for Component i

$$\text{PUF Response Length} = \frac{N!}{K! * (N-K)!} * 2^{K-1}$$

S-ArbRO-2 Scheme
ID Generation

- M=6, K=2, N=3: E1=[10, 5], E2=[6, 4], E3=[17, 11]
- Three Subsets:

  {E1, E2}, {E1, E3}, {E2, E3} =

  {[10, 5], [6, 4]}, {[10, 5], [17, 11]},{[6, 4], [17, 11]}
- Subset-Choice Challenge = (01) ⇒

  Group selected: {E1, E3}
- Subset-Processing Challenge = (10) ⇒

  E1: r2-r1 = 5-10 = -5

  E3: r1-r2 = 17-11 = 6
- Sum: -5+6 = 1
- 1>0 ⇒ PUF response = 1

Identity Mapping
ID Generation

Total Bits Generated = $2^M - M - 1$

- M = 3, Raw Data from Components: 52, 49, 48

- Pairs: {(52,49), (52,48), (49,48)}

  $d(f_1,f_2) = (f_1-f_2)^2 \Rightarrow 9,16,1$

- Triplets: {(52,49,48)}

  $d(f_1,f_2,f_3) = (f_1-f_2)^2 + (f_1-f_3)^2 + (f_2-f_3)^2 \Rightarrow 26$

Q = [9, 16, 1, 26]

- Response : $\lfloor Q[i]/q \rfloor \% 2$
- If q = 5, Parameter
- Response bits = 1101

Methodology

Ranking of ID Generation Schemes

- Ranking of Schemes based on PUF Metrics
  - Worst Case (WC) **Uniqueness**
  - Average **Uniformity**
  - Worst Case (WC) **Reliability**
- In ideal case,
  - WC Uniqueness should be **50%**
  - Avg Uniformity should be **50%**
  - WC Reliability should be **100%**

Worst Case Uniqueness

- Any two devices should be least similar.
  - Number of Devices: N
  - Response Size: L bits
  - Hamming Distance: $HD(R_i, R_j)$
- Worse Case Uniqueness:

$$\text{WC Uniqueness} = \text{Min}_{i=1}^{i=N-1}\text{Min}_{j=i+1}^{j=N}\left(\frac{\min(HD(Ri, Rj), L - HD(Ri, Rj))}{L}\right) * 100\%$$

- Choose the two most similar devices

Average Uniformity

- Number of 1s and 0s should be equal in PUF response
- Response size = L bits
- Uniformity of a device:

$$Uniformity(i) = \frac{1}{L}\sum_{l=1}^{L} r_{i,l} * 100\,\%$$

- Average over N devices:

$$Avg\ Uniformity = \frac{1}{N}\sum_{i=1}^{N} Uniformity(i)$$

Worst Case Reliability

- PUF response should be the same under different conditions in the field
  - Number of Devices : N
  - #Field Conditions : C
  - PUF Response Length: L bits
  - Hamming Distance : HD
- Worst Case Reliability:

$$\text{WC Reliability} = \text{Min}_{i=1}^{N}\left(1 - \frac{\underset{c=1}{\overset{C}{\text{Max}}}\ \text{HD}(R_i, R_{i,c})}{L}\right) * 100\%$$

Balance Among the Three Metrics

- All metrics important
- Which one should be sacrificed?
- Distance from Ideal PUF (DfI)

w_1•(50%-WC Uniqueness) + w_2•|50%-Avg Uniformity| + w3•(100%-WC Reliability)
where w1, w2, w3 are weights dependent on application

- We choose the ID Generation scheme with the smallest value of DfI

- In case of Reliability:
  - (100%-WC Reliability) < Error Correction Capability

Results

Data Set

PUF Type	FPGA Family	No. of Devices	Components/ Device	Source
Ring Oscillator	Spartan-3	193	512	VT
SR-Latch	Spartan-6	25	256	GMU
SR-Latch	Zynq-7000	10	256	GMU

	PC	CNC	BLG	S-ArbRO-2	Id-Map
Parameters			Set Size = 16	K=2	t=2
PUF Response Length (L)	$\lfloor M/2 \rfloor$	M-1	$(M/S) * \sum_{i=2}^{S} \lceil \log_2 i \rceil$	$\binom{M}{K} * 2^{k-1}$	$\binom{M}{t}$
Min Components Required for (L=128 bits)	256	129	48	24	17

Worst Case Uniqueness

Data Set	PC	CNC	BLG	S-ArbRO	ID-Map
Spartan-3 VT	**30.47%**	28.91%	26.56%	13.28%	24.22%
Spartan-6 GMU	33.59%	**35.16%**	32.81%	16.41%	34.38%
Zynq-7000 GMU	**41.41%**	38.28%	36.72%	28.12%	39.84%

- PC scheme offers the best result for Spartan-3 and Zynq-7000
- CNC scheme offers the best results for Spartan-6

Average Uniformity

Data Set	PC	CNC	BLG	S-ArbRO	ID-Map
Spartan-3 VT	52.25%	49.71%	47.70%	**50.24%**	57.80%
Spartan-6 GMU	44.71%	44.03%	44.65%	**52.96%**	63.68%
Zynq-7000 GMU	46.79%	46.87%	**47.89%**	54.14%	47.34%

- S-ArbRO scheme offers the best result for Spartan-3 and Spartan-6
- BLG scheme offers the best results for Zynq

Worst Case Reliability
Test Conditions

Data Set	Voltage Variation	Temperature
Spartan-3 VT	±10%	65°C
Spartan-6 GMU	±5%	0°C-85°C
Zynq-7000 GMU	±5%	0°C-85°C

Worst Case Reliability
Spartan-3

	PC	CNC	BLG	S-ArbRO	Id-Map
Rel @ +10% V	**91.40%**	**87.50%**	**83.59%**	48.14%	94.53%
Rel @ -10% V	92.96%	91.40%	84.37%	**38.2%**	**92.96%**
Rel @ 65°C	92.96%	95.31%	90.62%	39.06%	97.65%

Worst Case Reliability
Spartan-6

	PC	CNC	BLG	S-ArbRO	Id-Map
Rel @ +5% V	97.65%	99.21%	94.57%	96.87%	89.84%
Rel @ -5% V	96.09%	95.31%	90.62%	96.09%	**85.93%**
Rel @85°C	**96.09%**	**94.53%**	**85.93%**	**89.06%**	89.84%
Rel @0°C	96.09%	96.87%	92.18%	93.75%	90.62%

Worst Case Reliability
Zynq-7000

	PC	CNC	BLG	S-ArbRO	Id-Map
Rel @ +5% V	93.75%	93.75%	86.71%	92.18%	75.81%
Rel @ -5% V	93.75%	93.75%	85.93%	92.96%	91.4%
Rel @ 85°C	**89.84%**	**91.40%**	**78.90%**	**83.59**	**64.84%**
Rel @ 0°C	94.53%	94.53%	89.84%	92.96	92.18%

Balance Among the Three Metrics
Spartan-3

Best Worst

Distance from Ideal	PC	CNC	BLG	S-ArbRO	Id-Map
50%-WC Uniqueness	**19.53%**	21.08%	23.44%	**36.72%**	25.78%
|50%-Avr Uniformity|	**2.25%**	0.29%	2.30%	**0.24%**	7.80%
100%-WC Reliability	**8.60%**	12.50%	16.41%	**61.80%**	7.04%
DfI(0.3, 0.2, 0.5)	**10.61%**	12.63%	15.70%	**41.96%**	12.81%
DfI(0.4, 0.2, 0.4)	**11.70%**	13.49%	16.40%	**39.46%**	14.69%

DfI (w1,w2 ,w3)

Balance Among the Three Metrics
Spartan-6

Best Worst

Distance from Ideal	PC	CNC	BLG	S-ArbRO	Id-Map
50%-WC Uniqueness	16.41%	14.84%	17.19%	33.59%	15.62%
|50%-Avr Uniformity|	5.29%	5.97%	5.35%	2.96%	13.68%
100%-WC Reliability	3.91%	5.47%	14.07%	10.94%	14.07%
DfI(0.3, 0.2, 0.5)	7.94%	8.38%	13.26%	16.14%	14.46%
DfI(0.4, 0.2, 0.4)	9.19%	9.32%	13.57%	18.40%	14.61%

DfI (w1,w2 ,w3)

Balance Among the Three Metrics
Zynq-7000

	Best				Worst
Distance from Ideal	**PC**	**CNC**	**BLG**	**S-ArbRO**	**Id-Map**
50%-WC Uniqueness	**8.59%**	**11.72%**	**13.28%**	**21.88%**	**10.16%**
|50%-Avr Uniformity|	**3.21%**	**3.13%**	**2.11%**	**4.14%**	**2.66%**
100%-WC Reliability	**10.16%**	**8.60%**	**21.10%**	**16.41%**	**35.16%**
DfI(0.3, 0.2, 0.5)	**8.30%**	**8.44%**	**14.96%**	**15.60%**	**21.16%**
DfI(0.4, 0.2, 0.4)	**8.14%**	**8.75%**	**14.17%**	**16.14%**	**18.66%**

DfI (w1,w2 ,w3)

Conclusions

- **Binary Lehmer-Gray, S-ArbRO-2, and Identity Mapping** offer the ability to use **less components**
- **PC** is the **most expensive** scheme, in terms of area

- In case of **WC Uniqueness**, **PC scheme** offers the best result for two data sets
- In case of **Avg Uniformity**, **S-ArbRO** offers the best results for two data sets
- In case of **WC Reliability**, **three different schemes** offer the best results for each data set, respectively

Python scripts for

PUF ID generation and Evaluation

available at

https://cryptography.gmu.edu/puf

Questions