LRR-DPUF: Learning Resilient and Reliable Digital Physical Unclonable Function

Jin Miao[1] Meng Li[2] Subhendu Roy[1] Bei Yu[3]

[1]Cadence Design Systems
[2]University of Texas at Austin
[3]The Chinese University of Hong Kong

Outline

Introduction

Lithography variation

Unit Cell

LRR-DPUF architecture

Evaluation

Conclusion

Outline

Introduction

Lithography variation

Unit Cell

LRR-DPUF architecture

Evaluation

Conclusion

Introduction

Conventional analog silicon PUFs

- **Transistor** analog intrinsic randomness
- Vulnerable to environmental and operational variations
- Need error correction

Expected digital silicon PUF

- **Boolean** type randomness source
- Immune to environmental and operational variations
- Less to no error correction
- Strong resilience to attacks

Introduction

Related work

- Hybrid FPGA digital PUF however need analog PUF to start up [FPL'14]
- First digital PUF by interconnection uncertainty yet only conceptual and less feasible for practice [ISQED'15]

Contributions in our work

- Quantitative justifications of the use of interconnect randomness
- Strongly skewed latches to ensure deterministic transistor behaviors
- Novel highly non-linear logic network to ensure strong security

Outline

Introduction

Lithography variation

Unit Cell

LRR-DPUF architecture

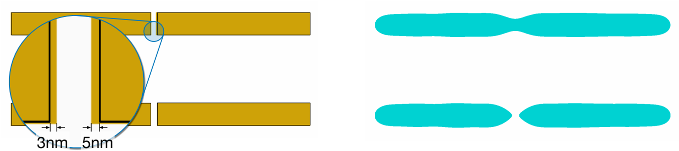
Evaluation

Conclusion

Lithography variations

Identify a feasible source of Boolean randomness is half the battle to make a digital PUF.

Two slightly differed mask stripe-pairs are eventually mapped to have different connectivities on silicon.



Interconnect under lithography variation. Left: mask split of 20nm for top, 28nm for bottom. Right: shapes on wafer.

Lithography variations

Lithography variation categories

- **Systematic**: dose, focus, etc.
- **Local**: mask, line edge roughness (LER), etc.

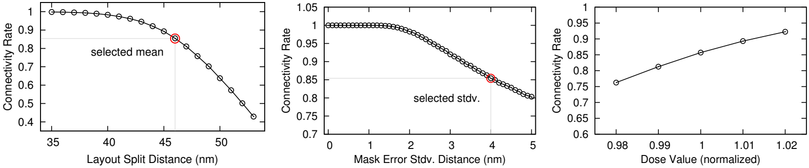
Mask error for interconnect randomness

- Position two interconnect layout line-ends close to each other
- An electron beam system can easily lead to large mask variations
- Mask variation further maps to different connectivity in wafer

Lithography variations

Quantitative justifications of lithography variations

- The existence and control of the configurations to
  - Augment the local variation
  - Suppress the systematic variation



Interconnect connectivity rate under lithography variations:
Left: layout split distance under mask error stdv. of 4nm; Center: mask error stdv. under split of 46nm; Right: dose values.

Conclusion

Lithography variations can be utilized by careful configurations of layout split and E-beam accuracy.

Outline

Introduction

Lithography variation

Unit Cell

LRR-DPUF architecture

Evaluation

Conclusion

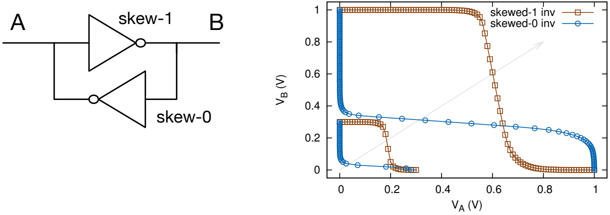
Unit Cell

Naïve random interconnection is incompatible to digital CMOS.

- **Short-circuit**: direct current from Vdd to Gnd, uncertain region, etc.
- **Open-circuit**: floating gate, etc.

Goal: Pure logical circuit compatible for normal and open circuits

Strongly skewed latch!

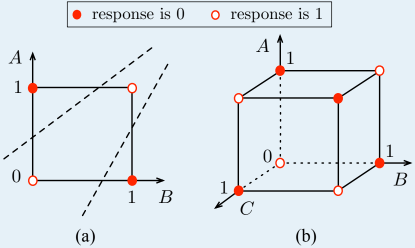


Handling dangled poly-gate by strongly skewed latch.
Left: inverter pair based skewed latch; Right: the VTC relation of a strongly skewed latch.

Unit Cell

Exclusive-OR (XOR) cell property

- **Linear non-separable**

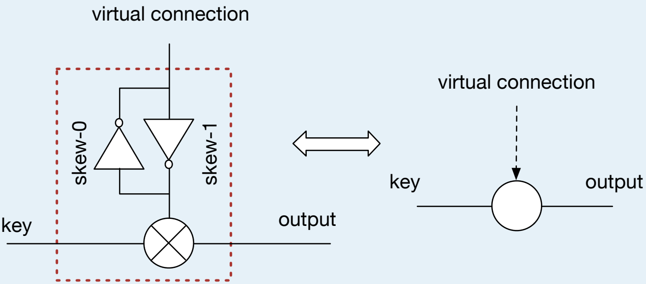


Linear non-separable nature for XOR logic.

- **Equal output probability**
  If $\Pr[a=1]=\Pr[a=0]=0.5,\ \forall b\in B$, then $\Pr[y=1]=\Pr[y=0]=0.5$.

Unit Cell

The proposed unit cell



Left: the complete unit cell logic structure; Right: simplified symbolic representation.

A unit cell may or may not invert its **key** depending on **virtual connection**.

Outline

Introduction

Lithography variation

Unit Cell

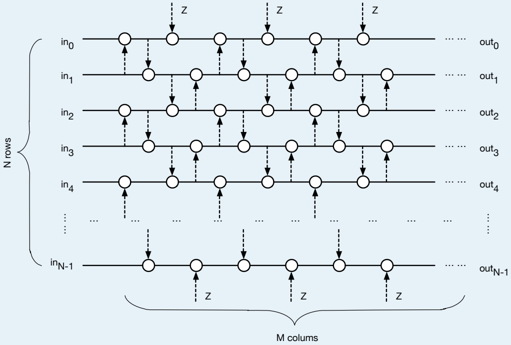
LRR-DPUF architecture

Evaluation

Conclusion

LRR-DPUF architecture

The proposed LRR-DPUF architecture



A N-row by M-col LRR-DPUF architecture. Some boundary virtual connections are marked by "Z" indicating dangling status.

Each row is a *signal tunnel* where the 1-bit input signal may be inverted depending on the virtual connections associated to this row.

LRR-DPUF architecture

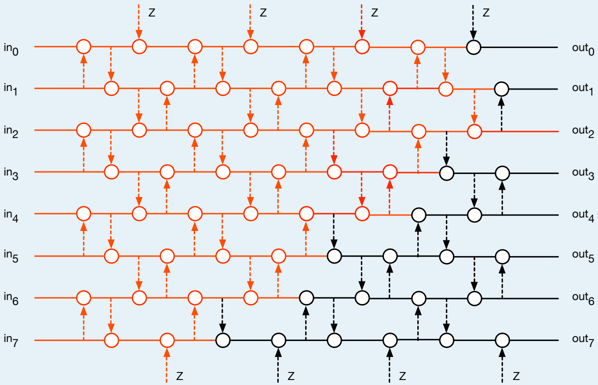
LRR-DPUF formula

$$k_{i,j} = \begin{cases} k_{i,j-1} \oplus (v \cdot k_{i+1,j-1} + \overline{v}), & i \text{ even}, j \text{ even}; \\ k_{i,j-1} \oplus (v \cdot k_{i-1,j-1} + \overline{v}), & i \text{ even}, j \text{ odd}; \\ k_{i,j-1} \oplus (v \cdot k_{i-1,j} + \overline{v}), & i \text{ odd}, j \text{ even}; \\ k_{i,j-1} \oplus (v \cdot k_{i+1,j} + \overline{v}), & i \text{ odd}, j \text{ odd}. \end{cases}$$

Here $k_{i,j}$ refers to *i-row j-column* output, and v refers to virtual connection status.

LRR-DPUF architecture

Logic cone of an 8×8 LRR-DPUF



Logic cone of out_2 is highlighted in red color.

LRR-DPUF architecture

LRR-DPUF properties

- The non-linearity of LRR-DPUF increases along with a higher connectivity rate.
- There is a sufficiently large space of unique LRR-DPUFs even if the connectivity rate is high.
- Increasing the number of columns strengthens the resilience to learning attacks.
- Any subtle change on virtual connections will be reflected to multiple outputs.

Outline

Introduction

Lithography variation

Unit Cell

LRR-DPUF architecture

Evaluation

Conclusion

Evaluation

Statistical evaluation

Table: Statistical evaluation on 8×8 LRR-DPUF with 256 exhaustive CRPs

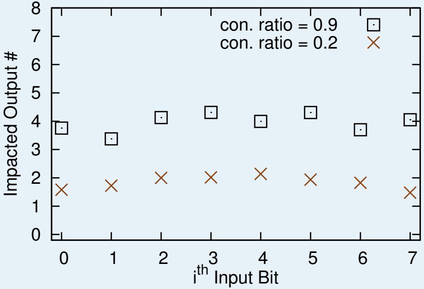
Type (Ideal Value)	conn. rate = 0.2		conn. rate = 0.9	
	Mean	Stdv.	Mean	Stdv.
Inter HD (0.5)	0.4188	0.0302	0.4943	0.0061
Intra HD (0.0)	0	0	0	0
Bit Alias (0.5)	0.5000	0.2067	0.5000	0.0730
Uniformity (0.5)	0.5000	0.1768	0.5000	0.1678

Table: Statistical evaluation on 64×64 LRR-DPUF with 100K CRPs

Type (Ideal Value)	conn. rate = 0.2		conn. rate = 0.9	
	Mean	Stdv.	Mean	Stdv.
Inter HD (0.5)	0.4999	0.0009	0.5000	0.0009
Intra HD (0.0)	0	0	0	0
Bit Alias (0.5)	0.5000	0.0504	0.5000	0.0499
Uniformity (0.5)	0.5000	0.0625	0.5000	0.0624

Evaluation

Avalanche effect

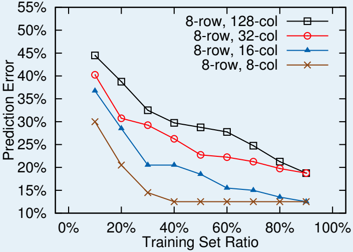


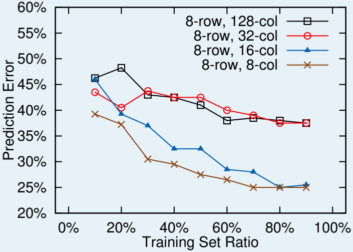
Avalanche effect of 8×8 LRR-DPUF over each input.

Under high connectivity rate, the adversary prediction via one bit change at a time is **no better** than a simple random guess.

Evaluation

Adversary attacks: 8-row by various number of columns

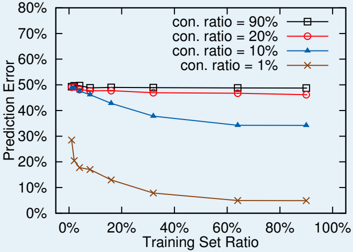


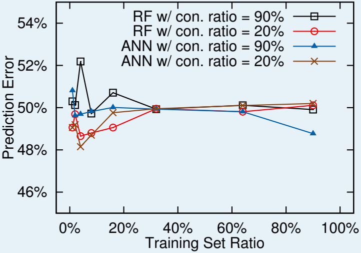


SVM attack for 8-row LRR-DPUFs over different configurations: Left: connectivity rate of 0.2 over different column sizes and training sizes; Right: connectivity rate of 0.9 over different column sizes and training sizes;

Evaluation

Adversary attacks: 64-row by 64-colum





Left: SVM attacks over different connectivity rate and training size. Right: additional learning model attacks including i) Artificial neural network (ANN) with 10 hidden layers using Sigmoid function, and ii) Random Forest (RF) with 15 trees in the forest.

Outline

Introduction

Lithography variation

Unit Cell

LRR-DPUF architecture

Evaluation

Conclusion

Conclusion

- A novel learning resilient and reliable digital PUF
- Justification for the use of interconnect randomness
- Strongly skewed latches for CMOS compatibility
- A highly non-linear logic architecture

Thank You

Jin Miao (jmiao@cadence.com)

Meng Li (meng_li@utexas.edu)

Subhendu Roy (subhroy@cadence.com)

Bei Yu (byu@cse.cuhk.edu.hk)