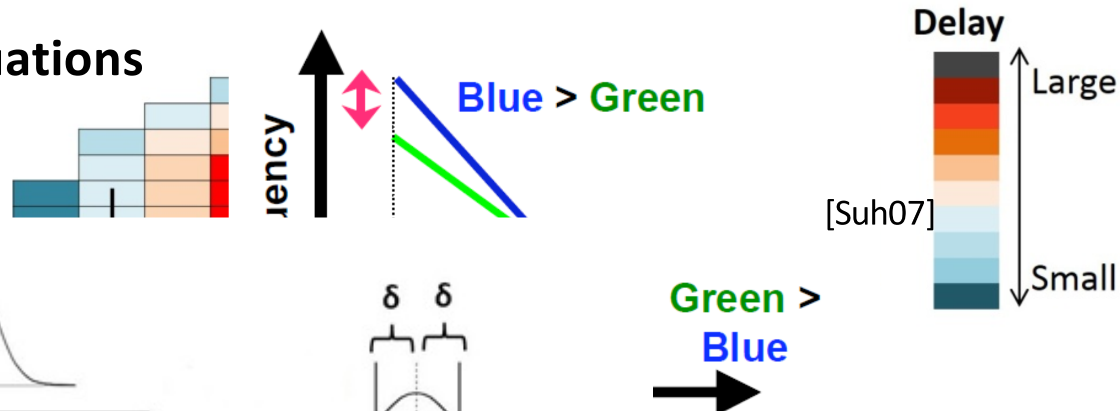
LEDPUF: Stability-Guaranteed Physical Unclonable Functions through Locally Enhanced Defectivity

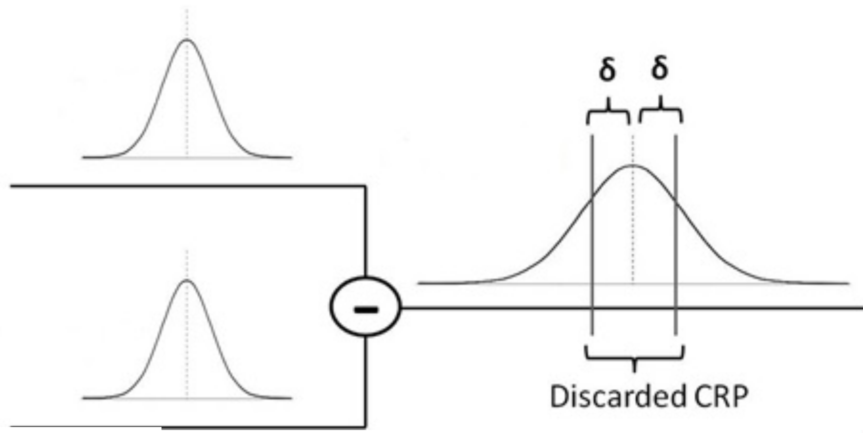
Wei-Che Wang, Prof. Puneet Gupta
Dr. Yair Yona, and Prof. Suhas Diggavi
UCLA Electrical Engineering

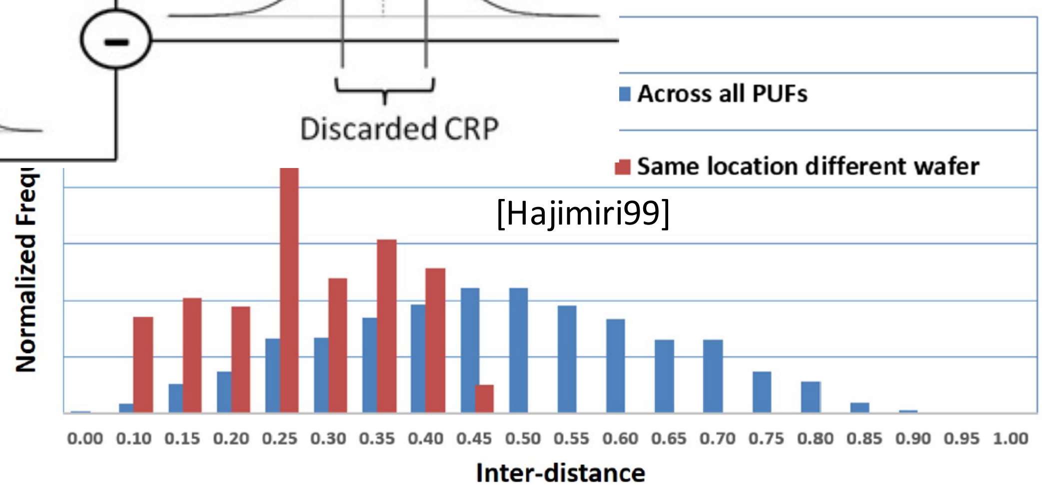
Limitations of Silicon PUFs

- **Stability**
  - Environmental fluctuations
  - Measurement noise

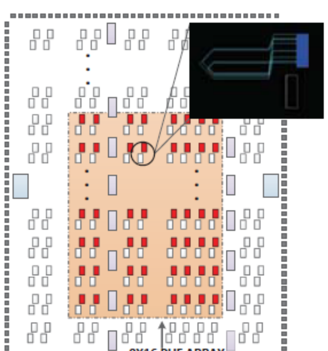


- **Uniquenes**
  - Randomne
  - Routing co





[Gu15]



Locally Enhanced Hard Defectivity (LED)

- **Hard defectivity**
  - Permanent defectivity
  - No parametric variations

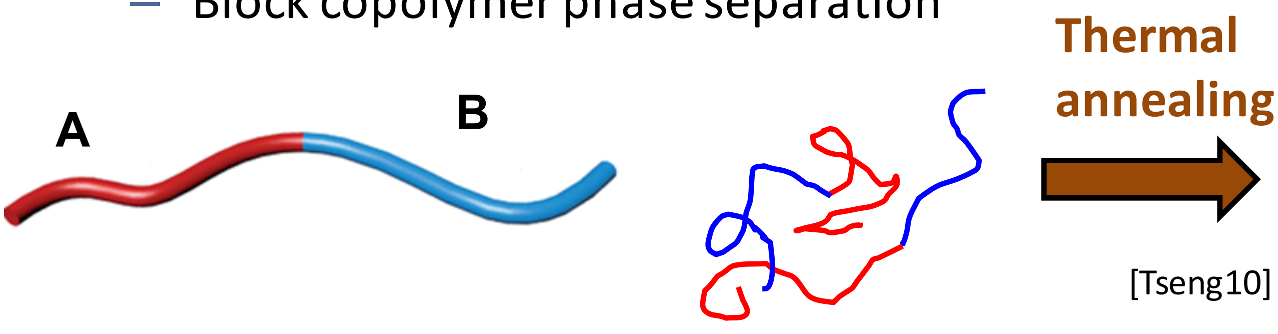
Stable!

- **Locally enhanced randomness**
  - No impact (from hard defectivity) to other parts of the chip
  - Through physical design
  - Compatible with circuit design flow

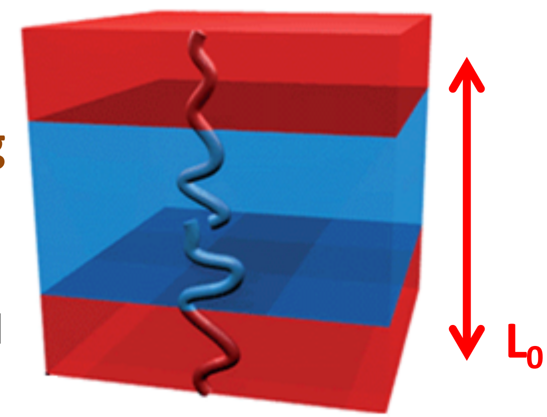
Unique!

Directed Self Assembly

- **Directed Self Assembly (DSA)**
  - Promising patterning candidate for <7nm
  - Block copolymer phase separation



[Tseng10]

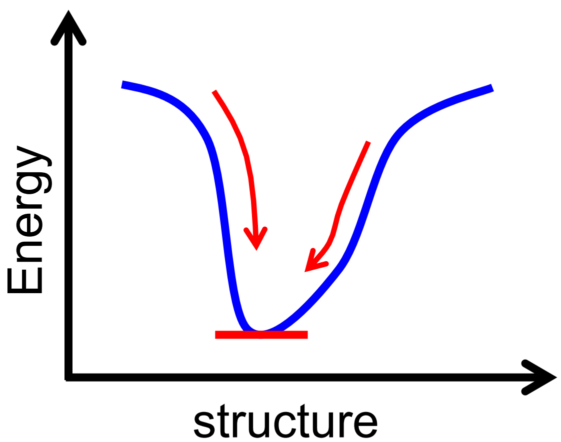


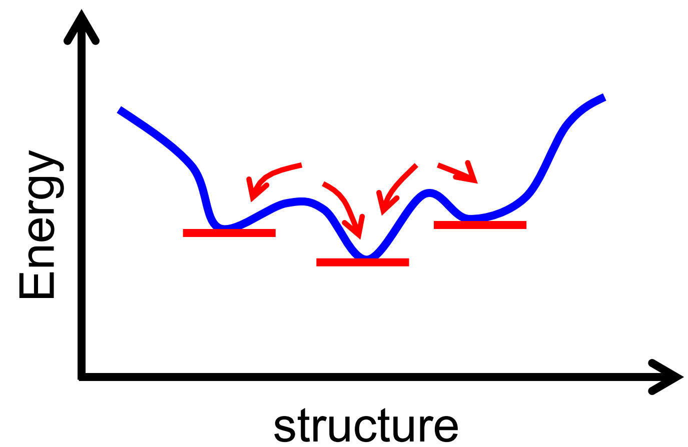
  - Guiding template interaction

[Badr15]

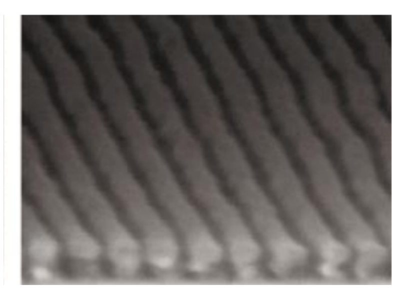
Minimum Energy State

- **One of the minimum energy states is reached**

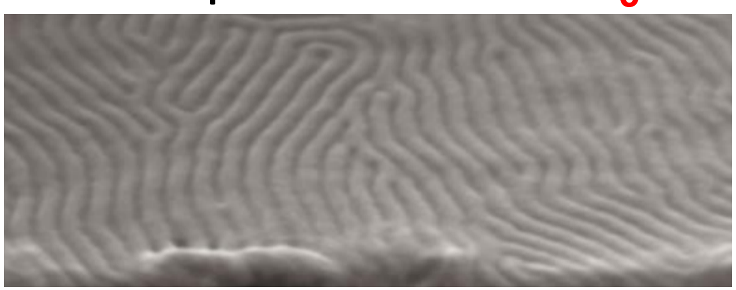




Template width ~ L_0



Template width >> L_0



[Kim03]

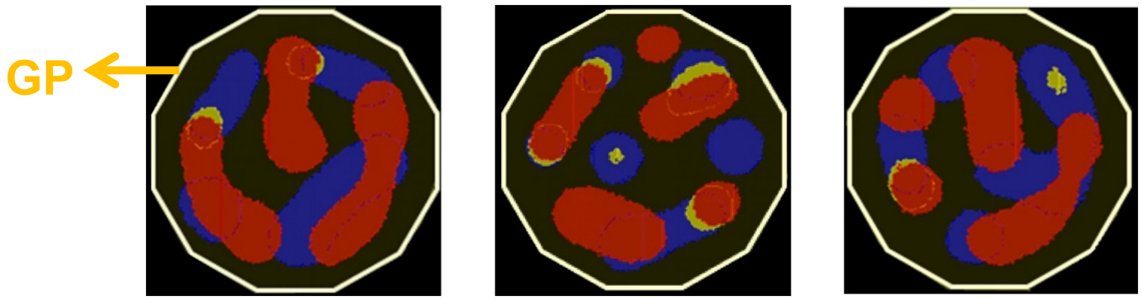
ITRS Roadmap

Table 1: Key targets and challenges for implementation of new patterning options.

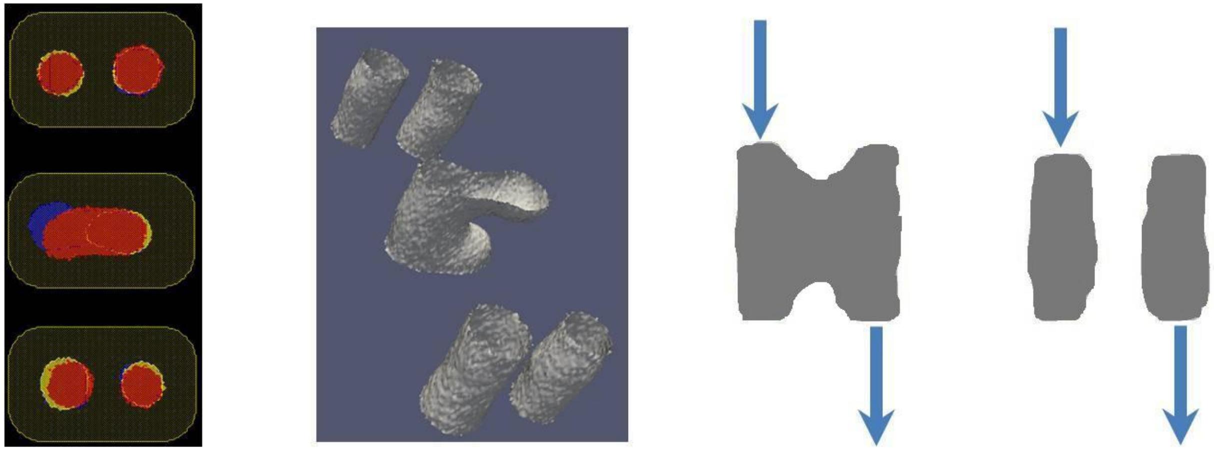
Next-generation technology	First possible use in mfg	Feature type	Device type	Key challenges	Required date for decision making
Multiple patterning extension	2019	Sub-l0-nm hp fins in finFETs	'5-nm' node logic	– Printing and overlay of cut levels – Cost due to many masks	2017
EUV	2017 2018	22 nm to 26 nm hp CH/cut levels 16 nm to 20 nm hp LS	'10=nm' node logic extension, '7-nm' node logic, 19-nm DRAM	– Enough throughput – Defects from mask – Resist sensitivity and roughness	2015
Nanoimprint	2016	14-nm hp LS	Flash memory	– Detectivity – Overlay – Throughput – Template infrastructure	2015
DSA (for pitch multiplication)	2017 2018	Contact holes/ cut levels	DRAM logic	– Detectivity – Pattern placement – Design	2015
Maskless lithography (ML)	2018	Contact holes/ cut levels	'7-nm' node logic	– Throughput – Demonstrated – Multibeam tool	2016

DSA Randomness Extraction

- With a large guiding template, random interactions begin to dominate the assembly process

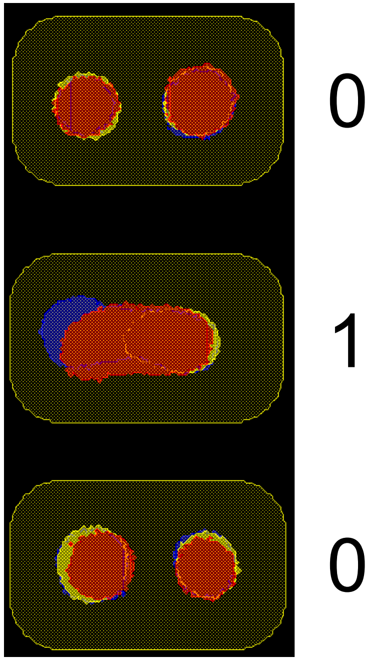


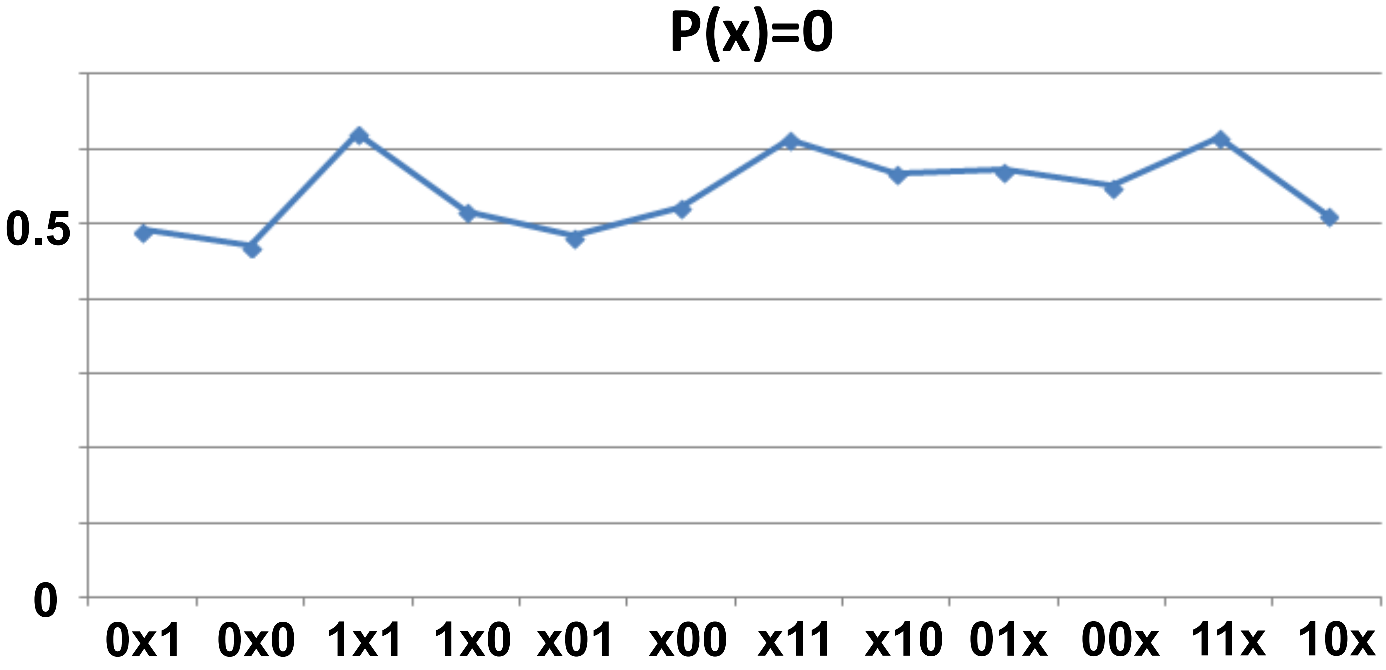
- The guiding shape is designed so that two vias are connected with certain probability



Simulation Result

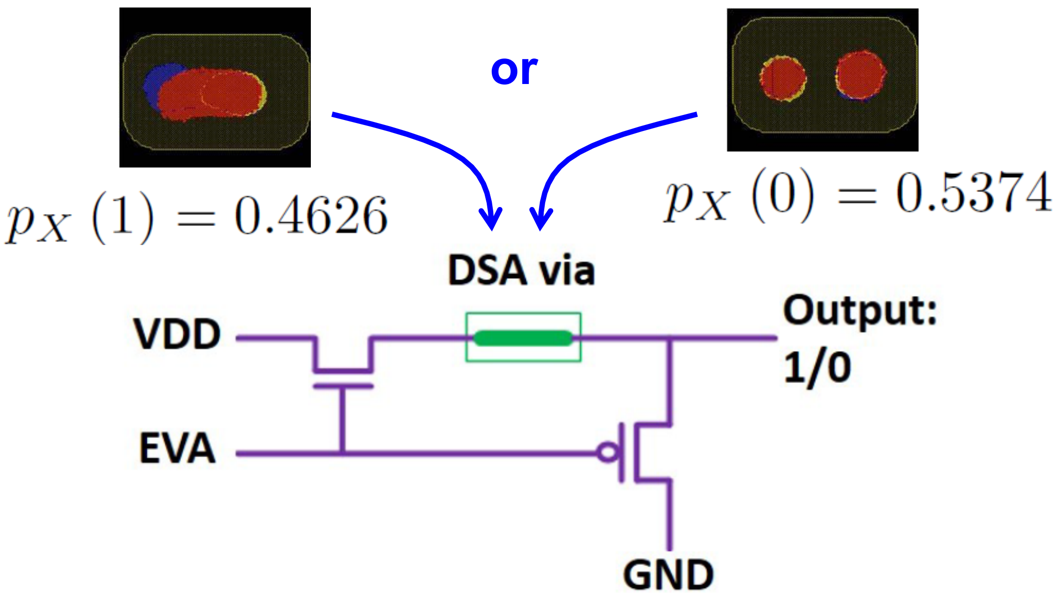
- **3x500 simulations**
  - **zero: 53.73%**
  - **one: 46.26%**
- **Bits are independent**





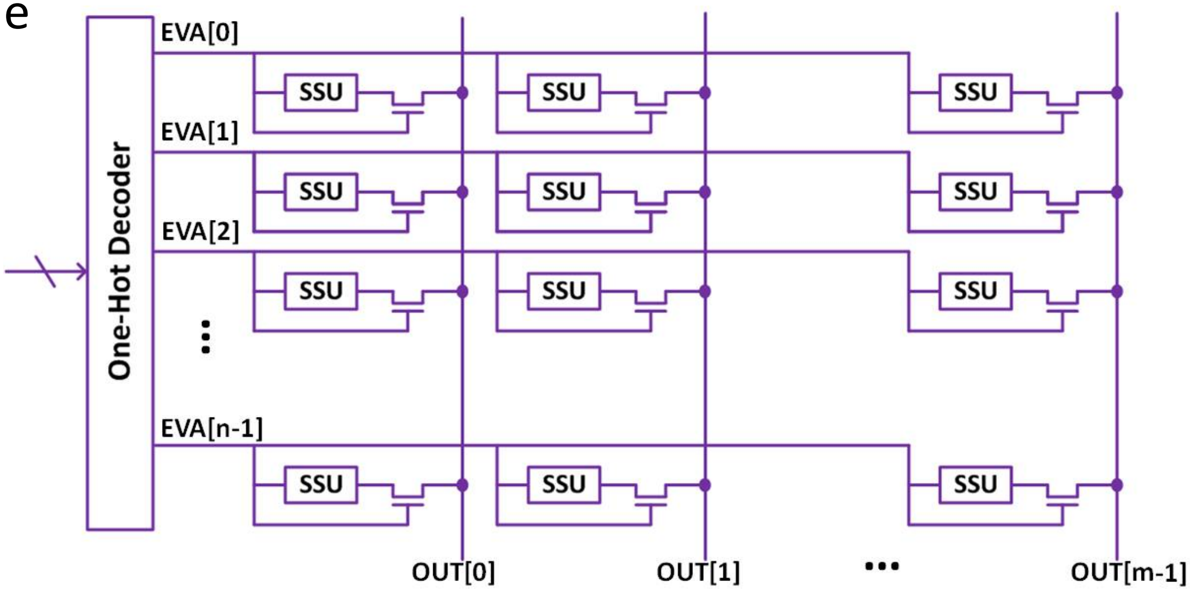
Stable Signal Unit

- A Stable Signal Unit (SSU) is constructed from a pair of DSA vias and two transistors
- When EVA. is high
  - DSA defective connection is formed → Output is VDD (logic one)
  - DSA defective connection is not formed → Output is GND (logic zero)



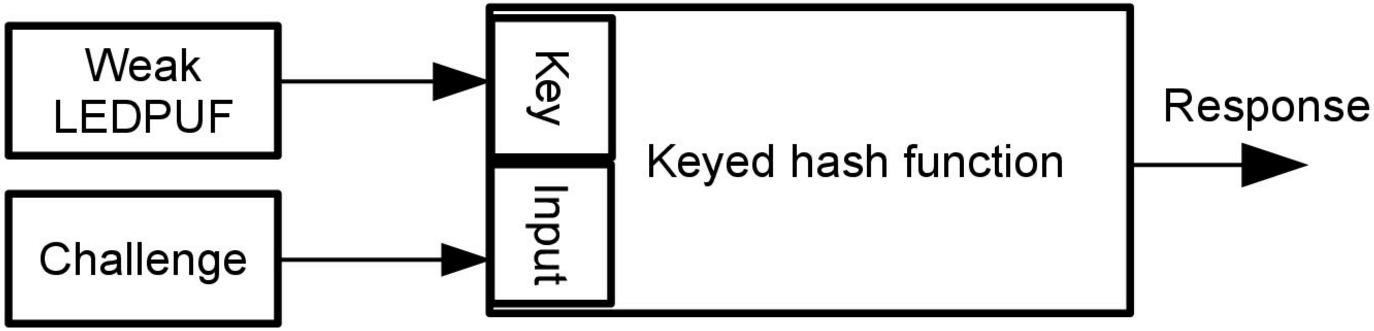
Weak LEDPUF

- A weak LEDPUF is constructed by arranging SSUs in arrays
  - **Challenge:** *log(n)* bits
  - **Response:** *m* bits
- Compared with SRAM PUF
  - More resistant to attacks
  - Completely stable



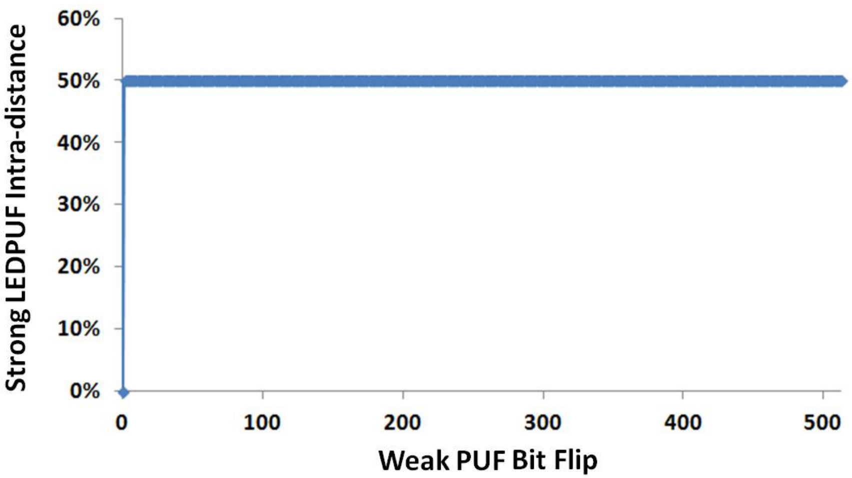
Strong LEDPUF

- A strong LEDPUF is composed of **HMAC-SHA-256** and keys from a **weak LEDPUF**
  - Completely stable requirement for the cryptographic hash
  - 2x256 bits from the stable weak LEDPUF (Initial Vectors)
  - **Challenge:** *any number of bits*
  - **Response:** *256* bits
- Compared with an Arbiter PUF
  - No efficient attacks to cryptographic hash functions
  - Completely stable

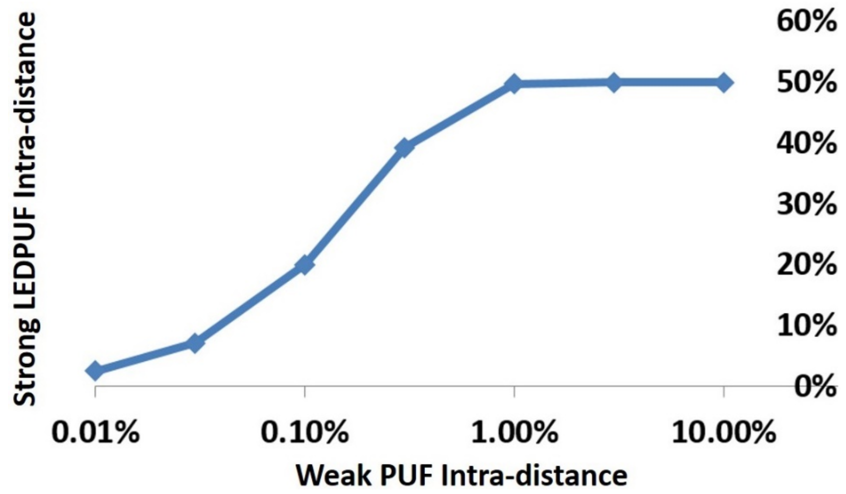


Weak LEDPUF Stability Requirement

- A single bit-flip in the weak LEDPUF will cause a complete different strong LEDPUF response



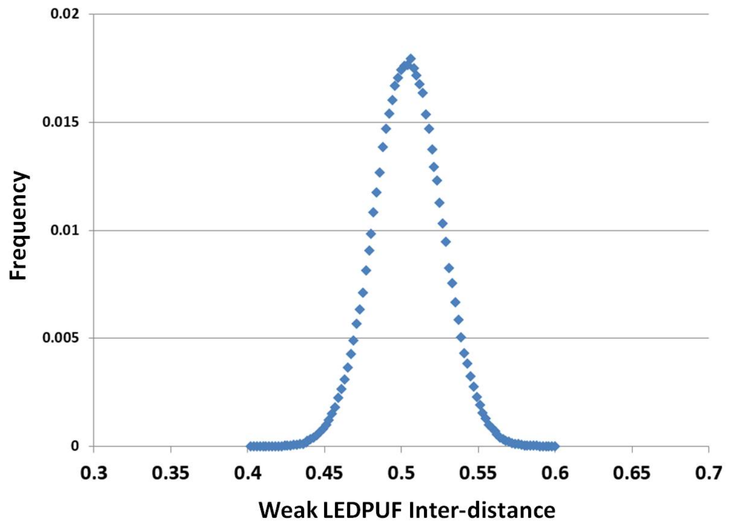
- The intra-distance of a strong LEDPUF grows dramatically as the weak LEDPUF intra-distance increases

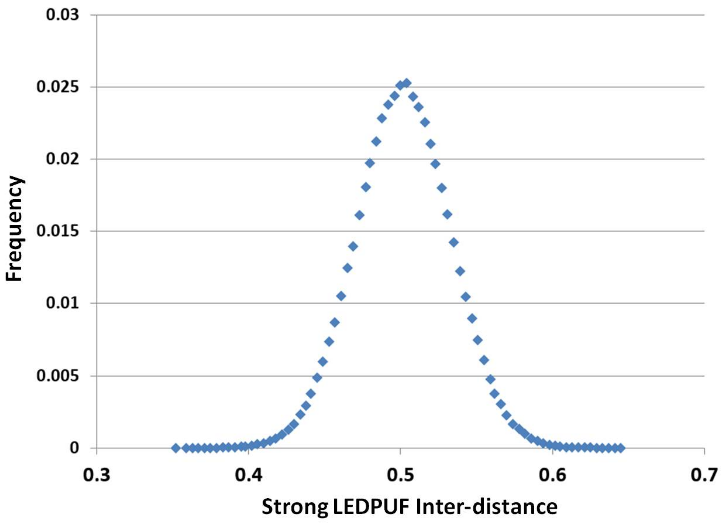


Uniqueness Evaluation

- 1000 weak/strong LEDPUFs are simulated
- Inter-distances are close to ideal **50%**

	Response Bits	Mean	Standard Deviation
Weak LEDPUF	512	**50.3%**	2%
Strong LEDPUF	256	**50.0%**	3%





Conclusion and Future Work

- **The first stability-guaranteed PUF is proposed**
  - Weak LEDPUF
  - Strong LEDPUF
- **Randomness extraction from locally enhanced DSA process**
- **Our future work includes**
  - **Finding sources of LED that are**
    - More **secure** than DSA
    - More **compatible** with existing CMOS technology
  - **Developing a quantitative security analysis of stable/unstable PUF**

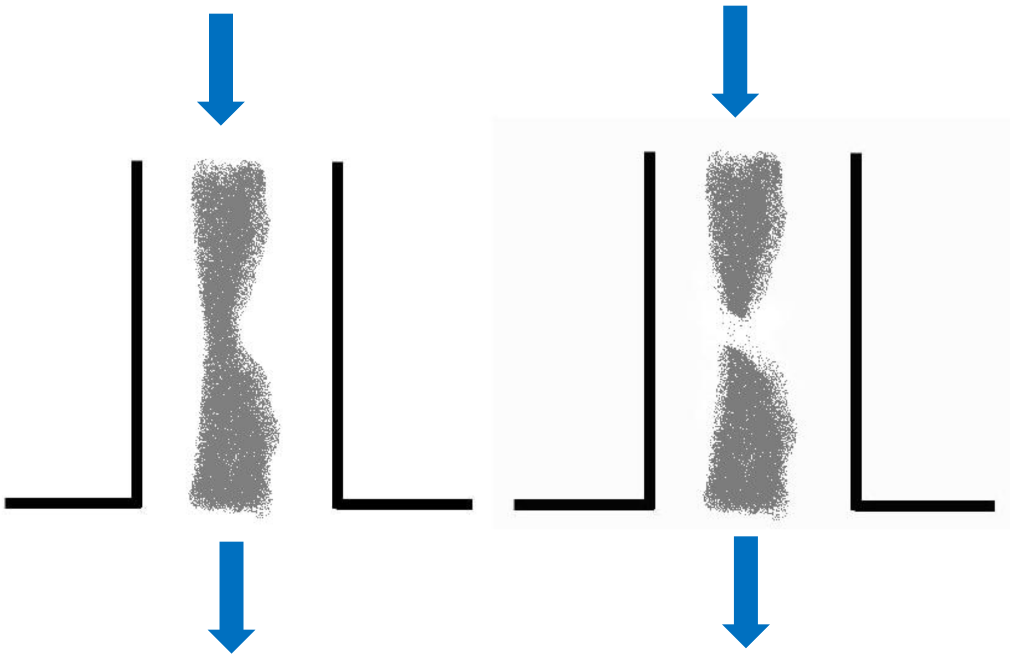
Thank you!

Questions?

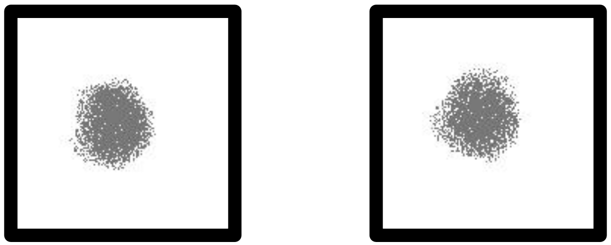
Backup Slides

Imaging Attack

- Cross section image ineffective because it destroys neighboring SSUs
- Top down image could be prevented by using a “tall” guiding template



Cross section view



Top down view

Guess Work Analysis

- Probability mass function of a bit from 1500 DSA connections

  $p_X(1) = 0.4626 \qquad p_X(0) = 0.5374$

- Single round guessing attack
  - min-entropy $H_{\min}(X) = -\log_2\left(\max_i p_i\right) = 0.8962$
  - For a m-bit response, the success rate of a single guessing is $2^{-0.8962m}$
  - With m=512 bits, the success rate is ~ 0%
- Dictionary guessing attack
  - Multiple guesses from the most probable response
  - Shannon-entropy $H_{Sh}(x) = \sum_i -P_i \log_2(p_i) = 0.996$
  - Number of expected attempts is lower-bounded by

    $$E\{G\} \geq \frac{1}{4}2^{mH_{Sh}(x)} = \frac{1}{4}2^{0.996m}$$

  - With m=512 bits, the expected attempts becomes unfeasibly large!

Guess Work Growth Rate

- Renyi entropy:

$$\lim_{m\to\infty} \frac{1}{m} \log_2 E\{G\} = H_{1/2}(X) = 2 \cdot \log_2 \left(\sum_i p_i^{1/2} \right) = 0.998$$

- $E\{G\}$ is upper bounded by $2^{0.998m}$ for a m-bit response
- **1.002m bits of LEDPUF = m bits fair coin tosses**