CHES 2011
Nara, Japan
Sep. 28 - Oct. 1

FUJITSU
shaping tomorrow with you

Variety ~~Uniqueness~~ Enhancement of PUF Responses Based on the Locations of Random Outputting RS Latches

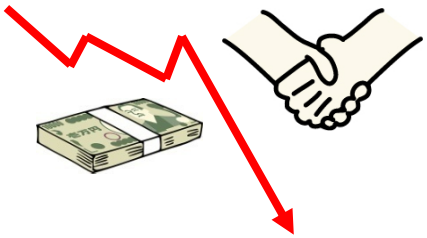
Fujitsu Laboratories Ltd., Japan
Dai Yamamoto

Collaborator:
Kazuo Sakiyama, Mitsugu Iwamoto, Kazuo Ohta
(The University of Electro-Communications)
Takao Ochiai, Masahiko Takenaka, Kouichi Itoh
(Fujitsu Laboratories Ltd.)

Introduction

FUJITSU

- Counterfeit semiconductor has expanded recently.
- Reasons why the counterfeit is evil
  - Monetary damages of original manufacturer
    - Drop in sales
    - Increase costs of analysis of the counterfeit



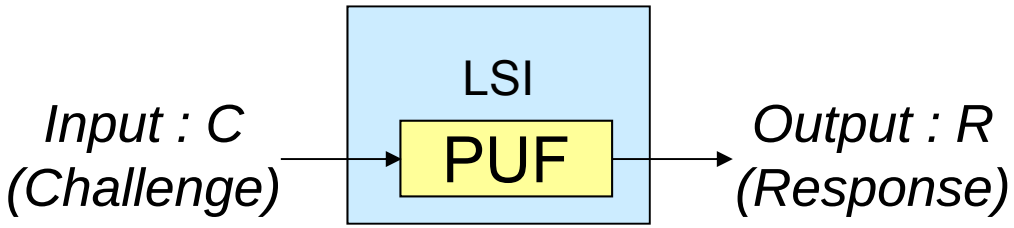
  - Losing the trust of customers who mistake the counterfeit as the original due to poor quality of the counterfeit
  - Risks of accidents threatening our lives
    - Electric vehicle, medical device, smart grid, etc

- Anti-counterfeiting technologies are required.
  - PUF (Physical Unclonable Function) as a solution

PUF (Physical Unclonable Function)

FUJITSU

- Focus on PUFs on LSIs
- PUFs have single input and single output.



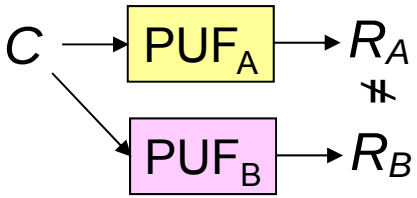
- Outputs depend on process variations of each individual LSIs.
  - Slight difference of wire/gate delay and drive capability etc.
  - Analysis and copy are hard.
- Counterfeiting PUFs is quite difficult.

Requirements of PUFs [1/2]

FUJITSU

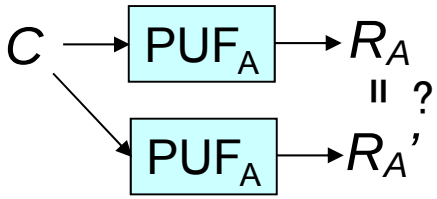
Uniqueness

- Independence among multiple PUFs of responses *R* to the same challenge *C*
- Hamming distance (HD) between 128-bit R_A and R_B
  - Ideal HD is 64 bits (= unpredictable)
- Important to realize high Uniqueness



Reliability

- Consistency of PUF CRPs for repeated measurements
- Lack of consistency due to "randomness" in *R*
- Removing randomness keeps Reliability, while reduces the "**Variety**" of *R*.
- Important to keep Reliability and **Variety**



R_A = 01?010?1??01...
(? = Randomness)

Requirements of PUFs [2/2]

FUJITSU

Variety

- The Variety (pattern / number) of responses *R*
  - 128-bit *R* has 2^{128} Variety ideally.
- Reasons why larger Variety is desirable
  - e.g. 192-bit *R* is more secure than 128-bit *R*.
    - Larger Variety, more unpredictable
- 128-bit *R* includes randomness.
  - Ideal Variety is 2^{128}.
  - Actual Variety is much less than 2^{128}.

Important to enhance the ideal Variety of responses *R*

Overview of This Work

FUJITSU

- Goal
  - Enhance the Variety while keeping Uniqueness & Reliability
  - Focus on Butterfly PUF (BPUF)
- Contribution
  - Use of location information of RS latches outputting random values
  - Propose method to use the location information
- Experimental results by using FPGAs
  - Variety increases 2^{196} » 2^{128}
  - Using 128 RS latches

Table of Contents

FUJITSU

- Introduction (previously-explained)
  - Requirements of PUFs (Uniqueness, Reliability, Variety)
- Background Art
  - RS latch (= A component of BPUF)
  - BPUF
- Proposed methods to enhance Variety
- Evaluation results by using FPGA
  - Uniqueness and Reliability
  - Variety
- Summary / Future work

Table of Contents

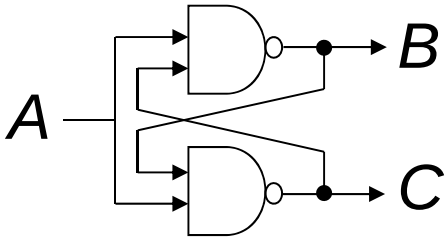
FUJITSU

- Introduction (previously-explained)
  - Requirements of PUFs (Uniqueness, Reliability, Variety)
- Background Art
  - RS latch (= A component of BPUF)
  - BPUF
- Proposed methods to enhance Variety
- Evaluation results by using FPGA
  - Uniqueness and Reliability
  - Variety
- Summary / Future work

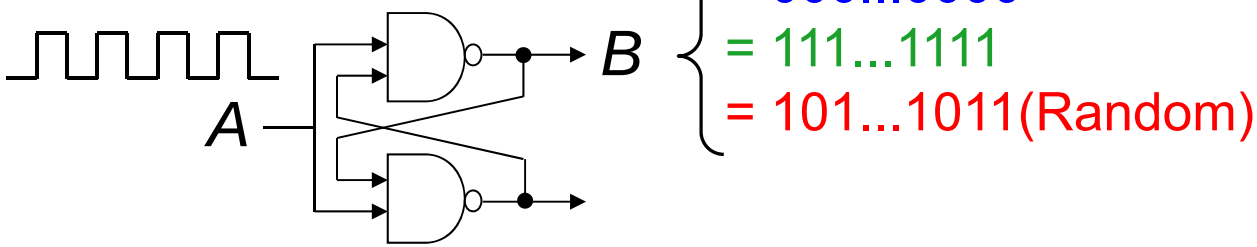
RS Latch (A component of BPUF)

FUJITSU

- Stable state with (*B*, *C*)=(1,1) when *A*=0
- *A* changing from 0 to 1 (rising edge)
  - Stable state with either (*B*, *C*) = (1,0) or (0,1)
  - Due to the difference of drive capabilities of the two NAND gates and the wire length



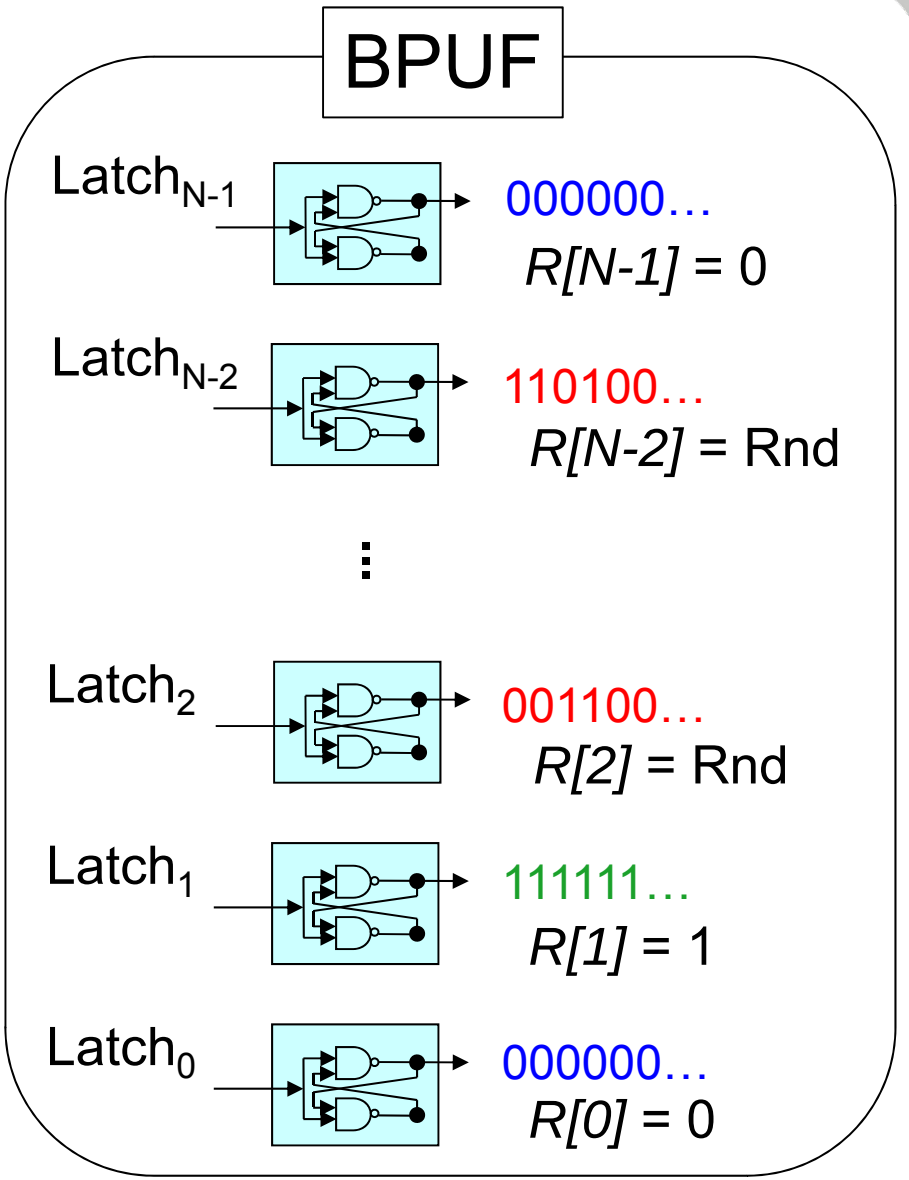
- When a clock signal is applied to input A, *B* from RS latches fall into 3 patterns:
  - Always 0's
  - Always 1's
  - A mixture of 0's and 1's (Random number)



N-bit Butterfly PUF (BPUF)

FUJITSU

- Generate N-bit response *R*
  - Using N RS latches
- RS latches outputting random numbers (= “random latches”)
- Random latches cause some problems.
  - Random latches cannot be used for responses.
  - Outputs from random latches are unstable.



Problems on Variety from random latches

FUJITSU

- Unable to use random latches for responses

- Variety decreases as random latches increase.
  - e.g. BPUF with 128 RS latches has 40 random latches.
    - Reduced from 2^{128} to $2^{88(=128-40)}$
  - Reducing unpredictability

Random latches reduce the Variety

Table of Contents

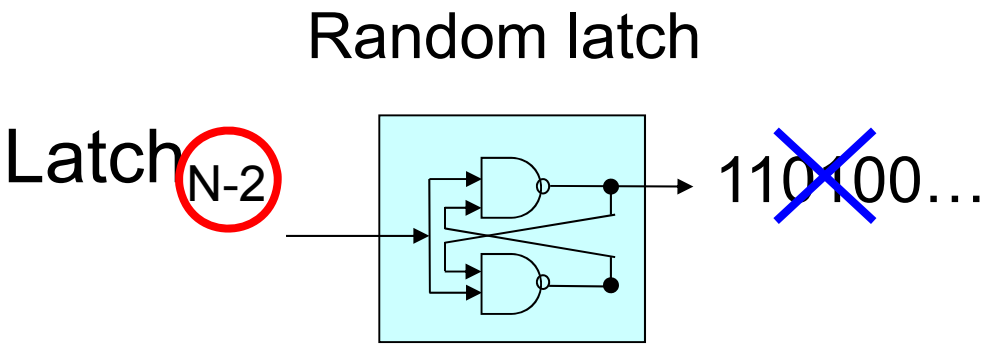
FUJITSU

- Introduction (previously-explained)
  - Requirements of PUFs (Uniqueness, Reliability, Variety)
- Background Art
  - RS latch (= A component of BPUF)
  - BPUF
- Proposed methods to enhance Variety
- Evaluation results by using FPGA
  - Uniqueness and Reliability
  - Variety
- Summary / Future work

Our Core Idea

FUJITSU

- (Conventional) Derive entropy from outputs
  - Need to discard random latches



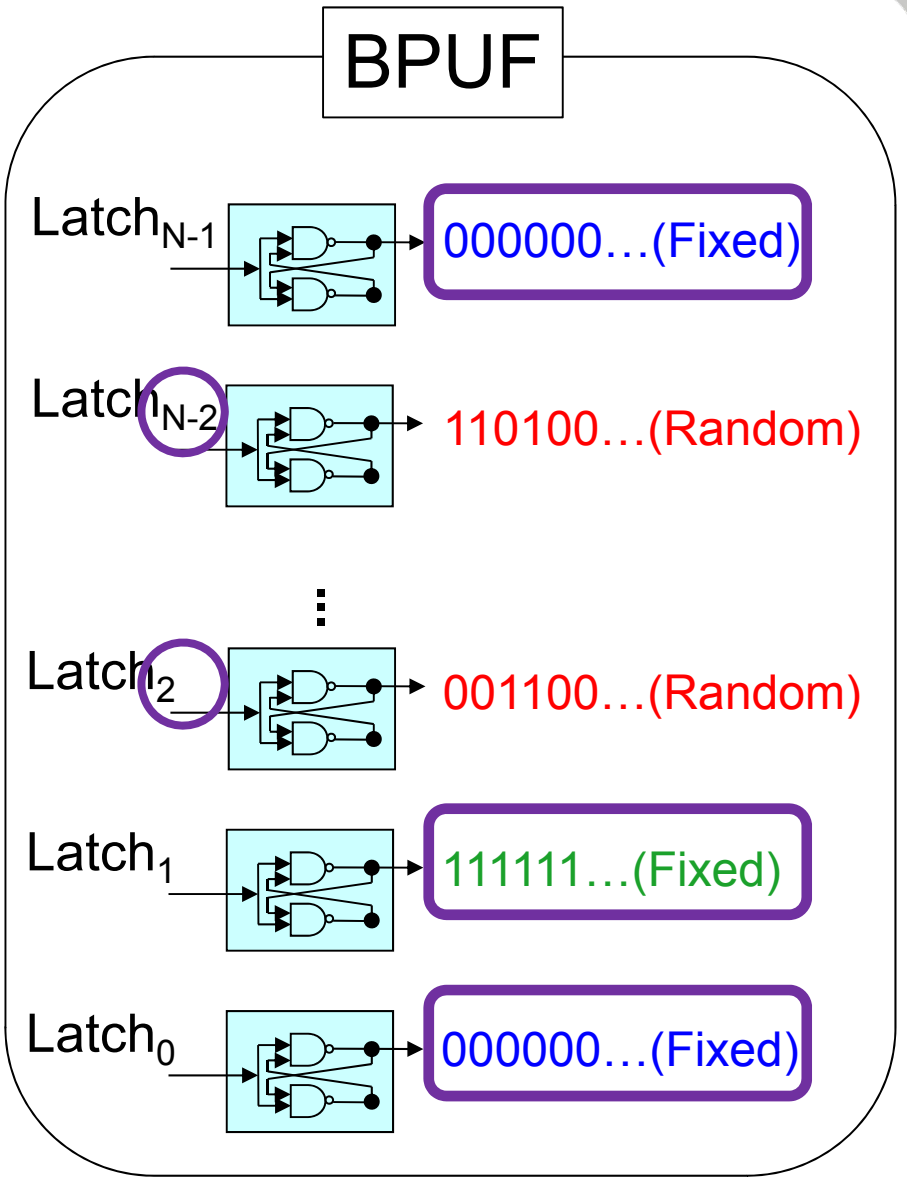
- (Our) Derive entropy from location information
  - Entropy from location information increases as random latches increase
  - Enhance the Variety while keeping Uniqueness & Reliability
    - Location info. of random latches: Almost stable

Use of Locations of Random Latches

FUJITSU

- Generate responses using two sources
  - Output values themselves from “Fixed latches”(0/1)
  - Locations of RS latches outputting random values (location)
- e.g. if a BPUF with *N* latches has *T* random latches...
  - Fixed latches: 2^{N-T}
  - Random latches: ${}_NC_T$
- Variety $= 2^{N-T} * {}_NC_T$

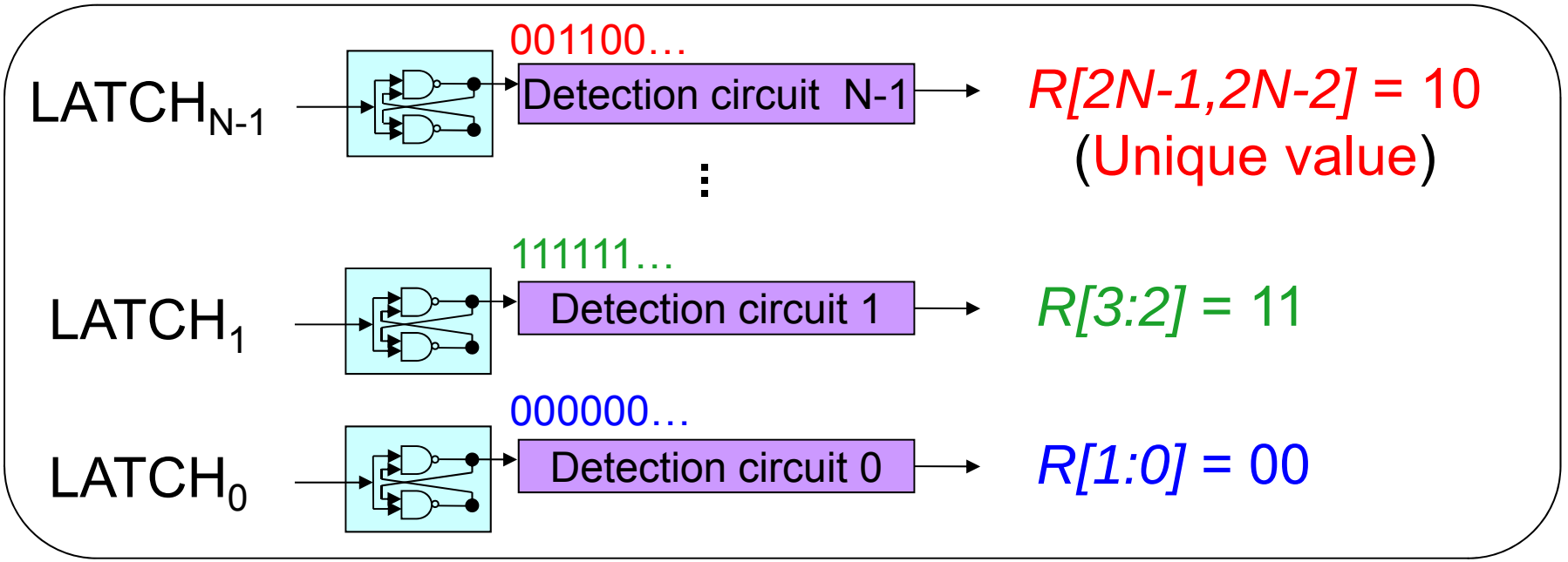
How transform locations to Variety?



Proposed method

FUJITSU

- Method of transforming locations to responses
  - Compact detection CKT (28 gates) located after a RS latch
  - The CKT generates ternary values (00/10/11) based on output values (0/1/random).
    - Random values → Third unique value '10'
  - Total Variety = 3^N regarding outputs as 3 types (0/1/random)



Estimated Variety using proposed method

FUJITSU

- Total Variety = 3^N
- # of random latches (=T) is determined by PUF properties.
  - Variety for given T = $2^{N-T} * {}_NC_T < 3^N$
    - T-th term of the binomial expansion of $(2+1)^N = 3^N$
    - The same as the previous estimate
- Variety vs T (N=128)
  - The Variety takes on its maximum value (=2^{203}) when T is around 43 (≈128/3).

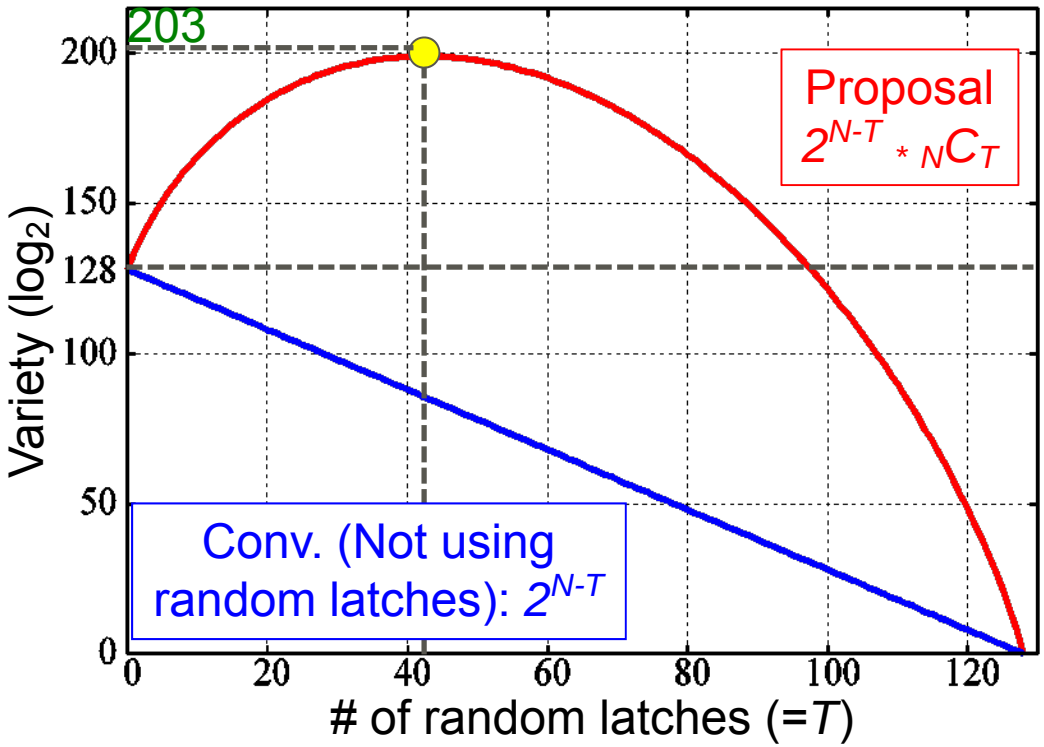


Table of Contents

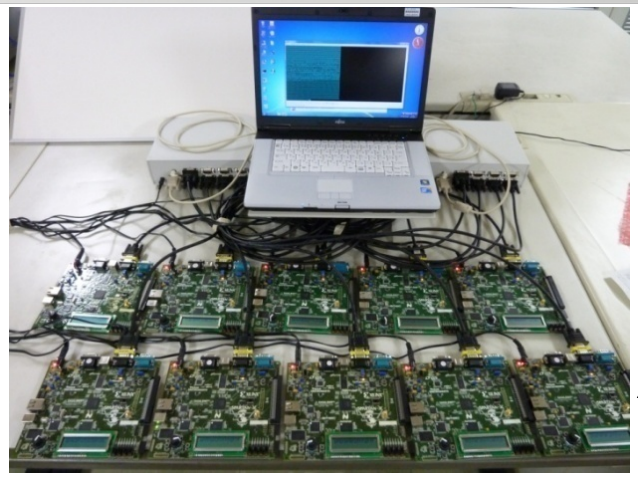
FUJITSU

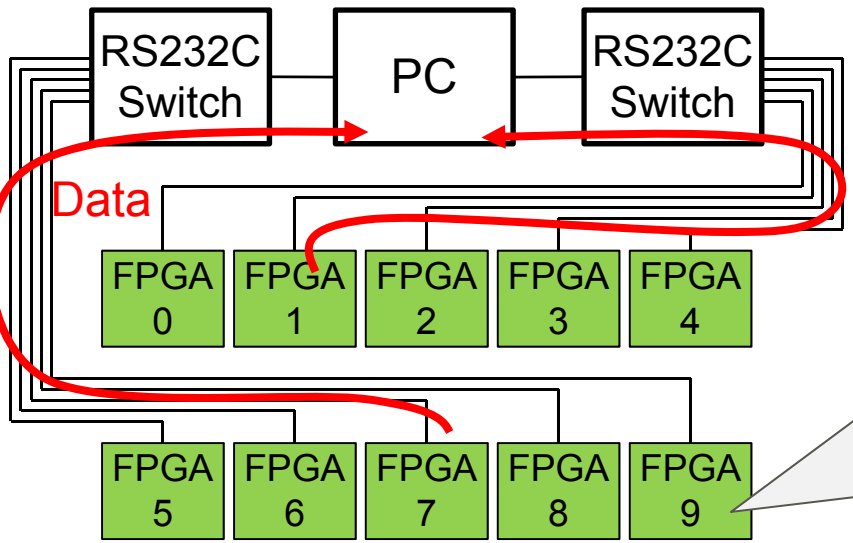
- Introduction (previously-explained)
  - Requirements of PUFs (Uniqueness, Reliability, Variety)
- Background Art
  - RS latch (= A component of BPUF)
  - BPUF
- Proposed methods to enhance Variety
- Evaluation results by using FPGA
  - Uniqueness and Reliability
  - Variety
- Summary / Future work

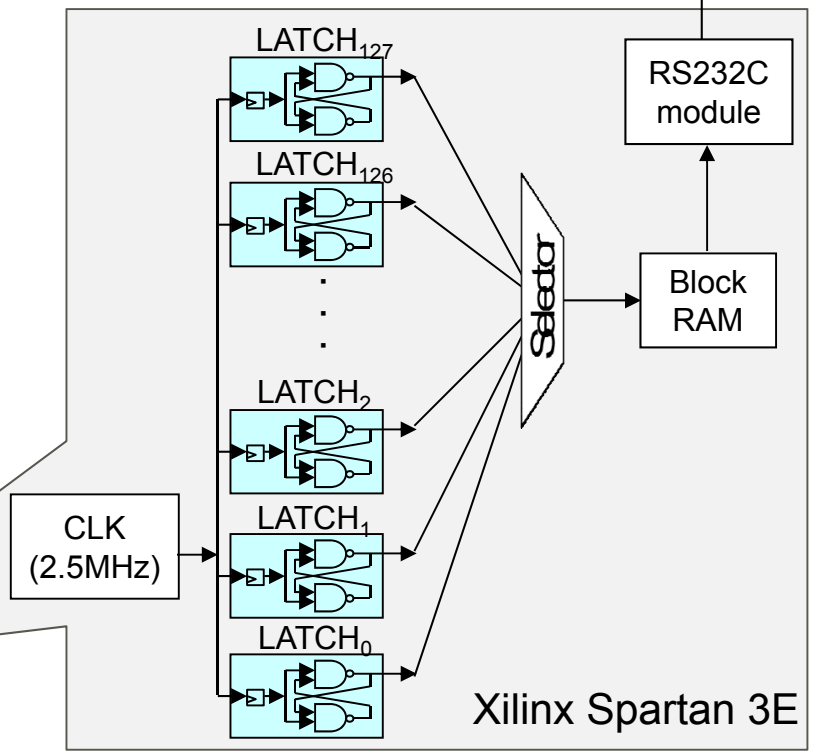
Experimental Environment

FUJITSU

- Evaluate using 40 **virtual** FPGAs
  - Using 10 actual FPGA boards
  - Implemented at 4 different locations
- Implement 128 latches
- Outputs are transmitted to PC.





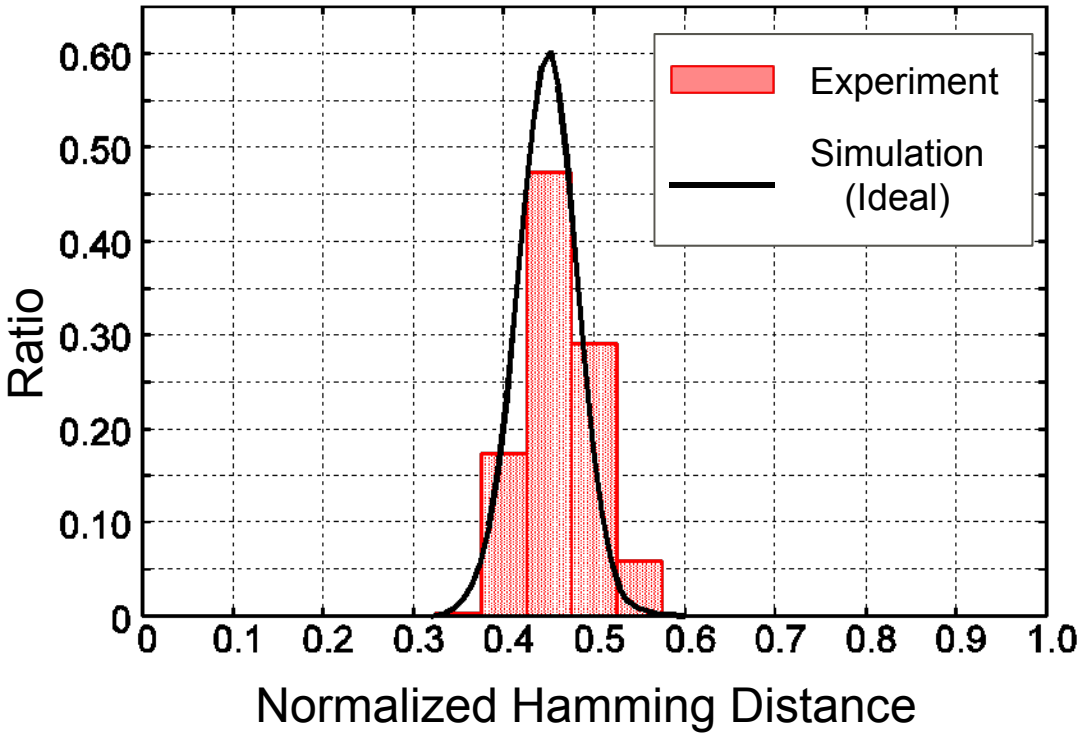


Evaluation: Uniqueness

FUJITSU

- **Uniqueness:** 2 PUFs generate the different responses?
  - Generate a total of 40 responses using all 40 FPGAs
    - One response per FPGA
  - Normalized hamming distance between two arbitrary responses among the 40 responses ($_{40}C_2$ = 780 combinations).

- **Results**
  - High Uniqueness
    - The difference in responses = 46%
  - Ideal difference: Black line
    - RS latches output (0/1/R) with equal probability.

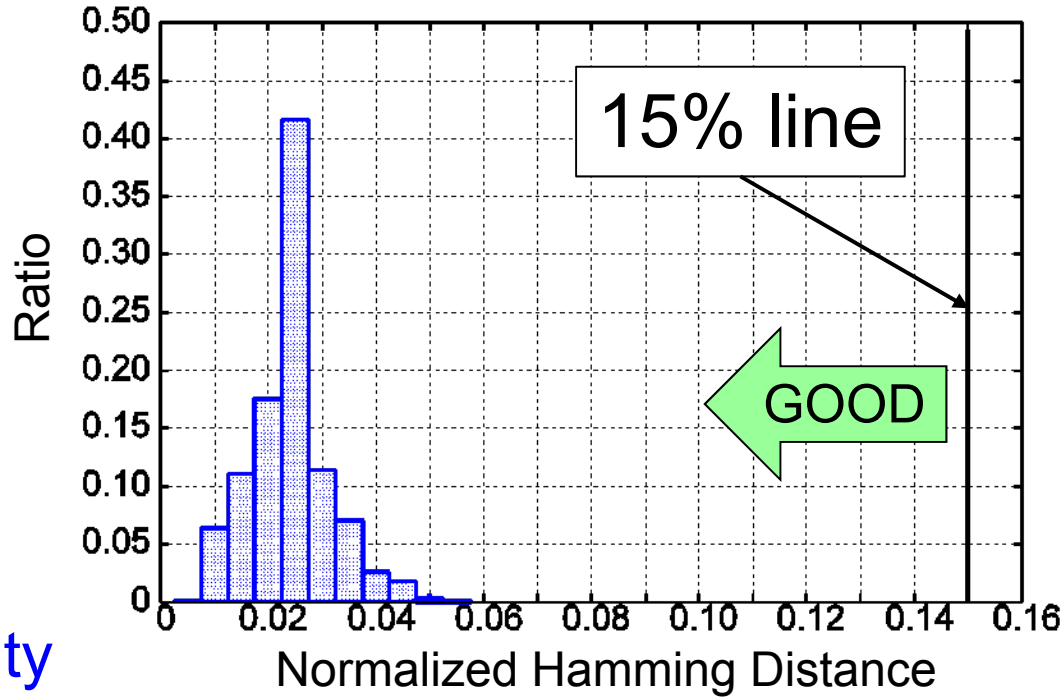


Evaluation: Reliability

FUJITSU

- Reliability = A PUF always generates the same response?
  - Generate 40 responses repeatedly using only a specific FPGA
  - Normalized HD between two arbitrary responses among the 40 responses (= the same as Uniqueness evaluation).

- Results
  - High Reliability
    - Average error rate
      = 2.4% « 15%
  - Redundant data of ECC
    - Reasonable size

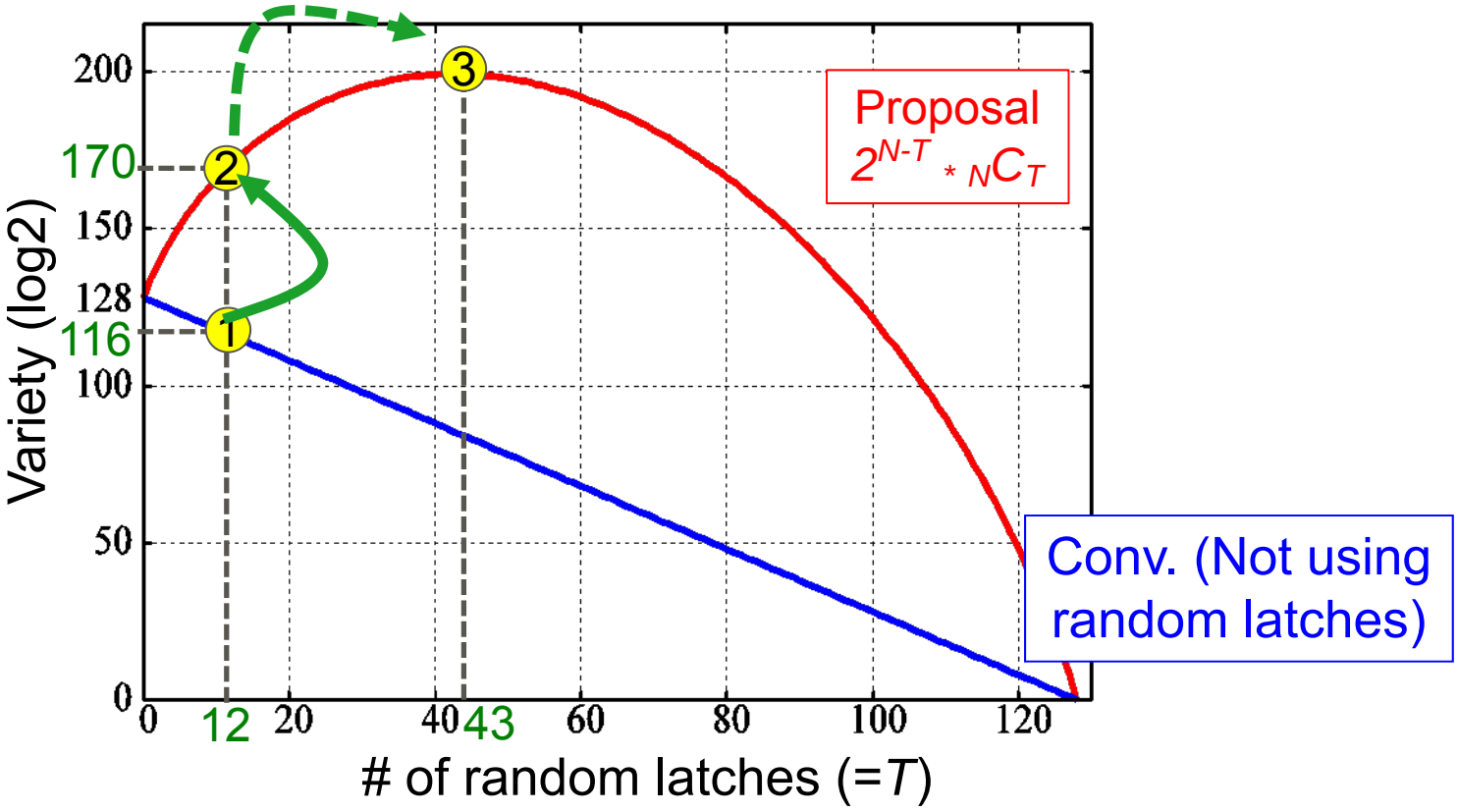


Proposed PUF gives
high Uniqueness & Reliability
(satisfy PUF requirements)

Evaluation: Variety [1/2]

FUJITSU

1. Conventional method (Not using random latches): 2^{116}
2. Proposed method: 2^{170}
3. Proposed method (Best Variety)



Evaluation: Variety [2/2]

FUJITSU

- Propose new implementation technique
  - Improve the effectiveness of proposed method
  - For details, please see proceeding.
- Ave. # of random latches
  - A BPUF with 128 latches
    - W/O our tech. ≈ 12
    - With our tech. ≈ 32

③ Proposed method with our technique : 2^{196}

Proposed methods dramatically enhance Variety.

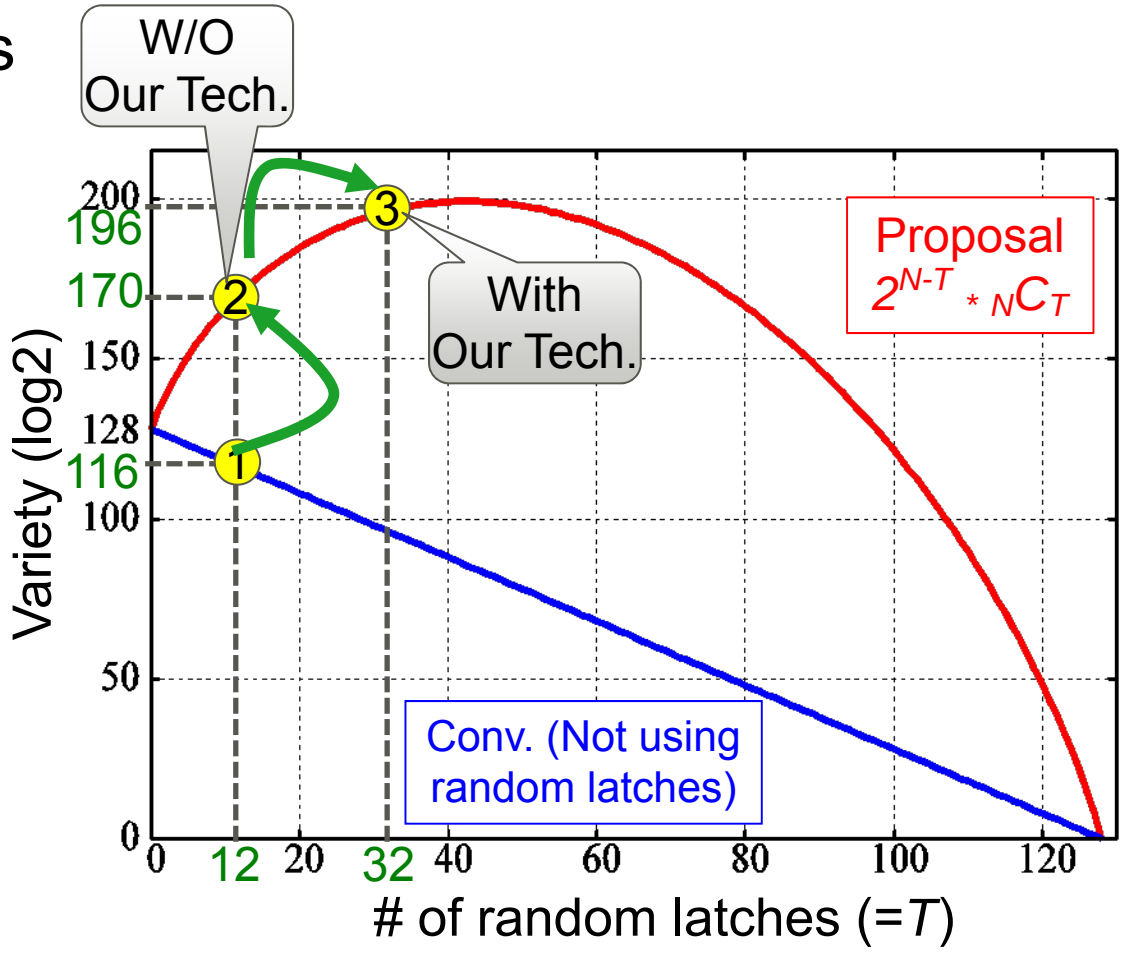


Table of Contents

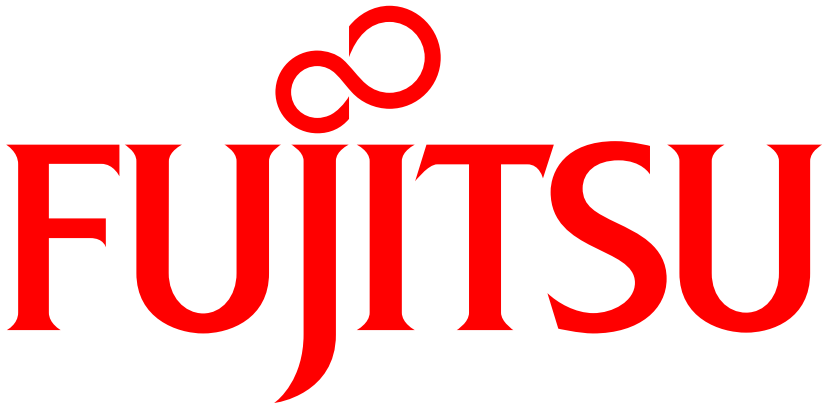
FUJITSU

- Introduction (previously-explained)
  - Requirements of PUFs (Uniqueness, Reliability, Variety)
- Background Art
  - RS latch (= A component of BPUF)
  - BPUF
- Proposed methods to enhance Variety
- Evaluation results by using FPGA
  - Uniqueness and Reliability
  - Variety
- Summary / Future work

Summary

FUJITSU

- Our goal
  - Enhance the Variety while keeping Uniqueness & Reliability
- Propose method
  - Use Entropy from Location information of random latches
  - Generate ternary values (00/10/11) from output values (0/1/random)
- Experimental results with FPGAs
  - Variety increases from 2^{116} to 2^{196} with proposed methods.
- Future Work
  - Evaluation of voltage resistance
  - Application of proposals to other kinds of PUFs
    - Improve not only BPUF



shaping tomorrow with you