Evaluation of ASIC Implementation of Physical Random Number Generators using RS Latches

Hirotaka KOKUBO,
Fujitsu Laboratories ltd., Japan

Collaborators:
Dai YAMAMOTO, Masahiko TAKENAKA,
Kouichi ITOH, Naoya TORII

Experimenting in clean room

Outline

FUJITSU

Our Work

- Fabricating Physical True Random Number Generators (PTRNG) using RS Latches on ASIC
- Measuring power consumption / circuit scale
- Evaluating randomness under various environments
  - Temperature: −20℃ ～ 60℃, Voltage: 1.80 ± 0.15V

Results

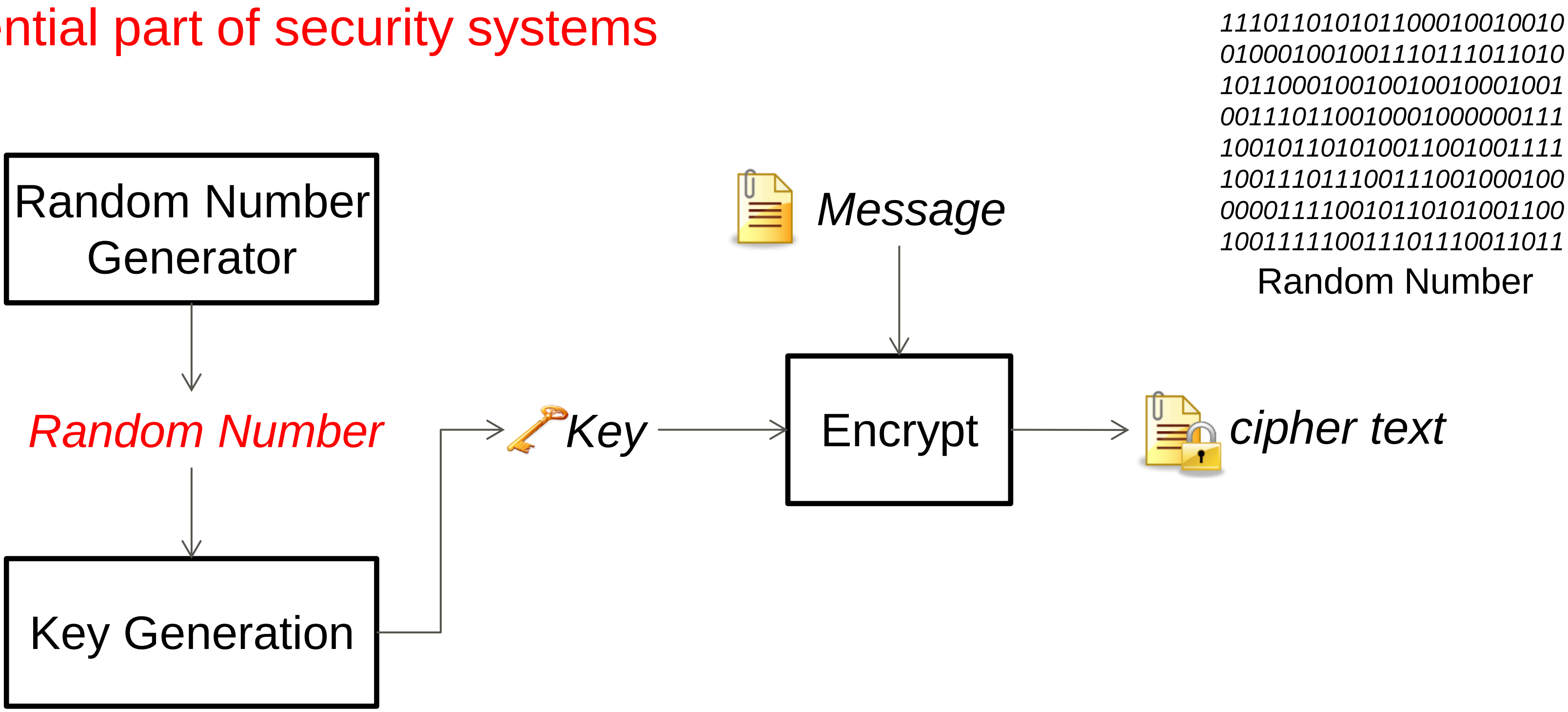
- Our PTRNG is suitable for smart cards
  - Low power consumption / small circuit scale
- Our PTRNG generates high-quality random number in various environments (Pass SP800-90B tests / AIS31 tests)

Background – Importance of Random Number

FUJITSU

Random Number

- Generated by Physical/Pseudo Random Number Generator
  - PTRNG : **P**hysical **T**rue **R**andom **N**umber **G**enerator
- Used for cryptographic-key generation, encryption method, etc.
- Essential part of security systems



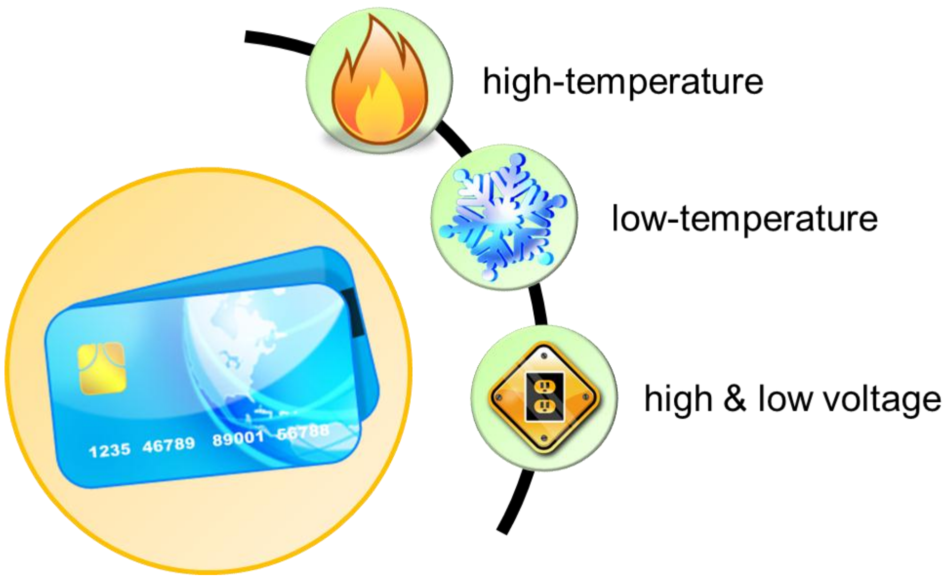
If random number is predictable, an attacker can decipher cipher texts

Background – ASIC Implementation

FUJITSU

- ASIC implementation is necessary for the mass production
  - ASIC: Application Specific Integrated Circuit
  - Lower chip cost, lower power consumption, faster processing

- PTRNGs on ASIC generate high-quality random number?



Embedded devices are influenced from various environment

Motivation

- PTRNGs for mass-product embedded devices should

1. be implemented on ASIC

2. generate high-quality random numbers
   in various environments

Our Contribution

1. Fabricating our PTRNGs on 0.18μm ASIC
   - Lower design costs

2. Validating the fact that our PTRNGs have low power consumption and small circuit scale
   - To confirm whether our PTRNG can be implemented on embedded device

3. Evaluating the quality of random numbers
   - According to NIST SP800-90B and BSI AIS31 statistical tests
   - Experimentally confirming the robustness of our PTRNGs against temperature and voltage fluctuations

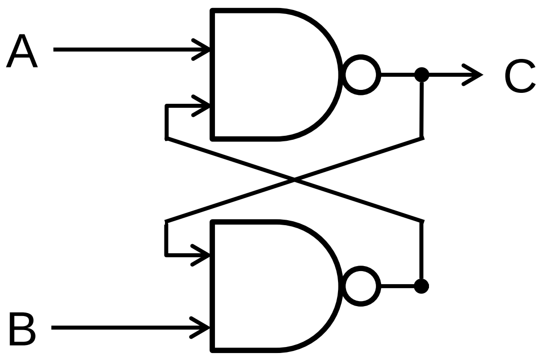
1.Fabricating PTRNGs

2.Measuring power consumption and circuit scale

3.Evaluating the quality of the random numbers

RS Latch : component of our PTRNG

- An RS latch stores 1-bit information
  - Normally, input A = B = 1 is not allowed



RS Latch

RS Latch Operation		
A	B	C
0	0	1 (hold state)
0	1	1
1	0	0
1	1	not allowed

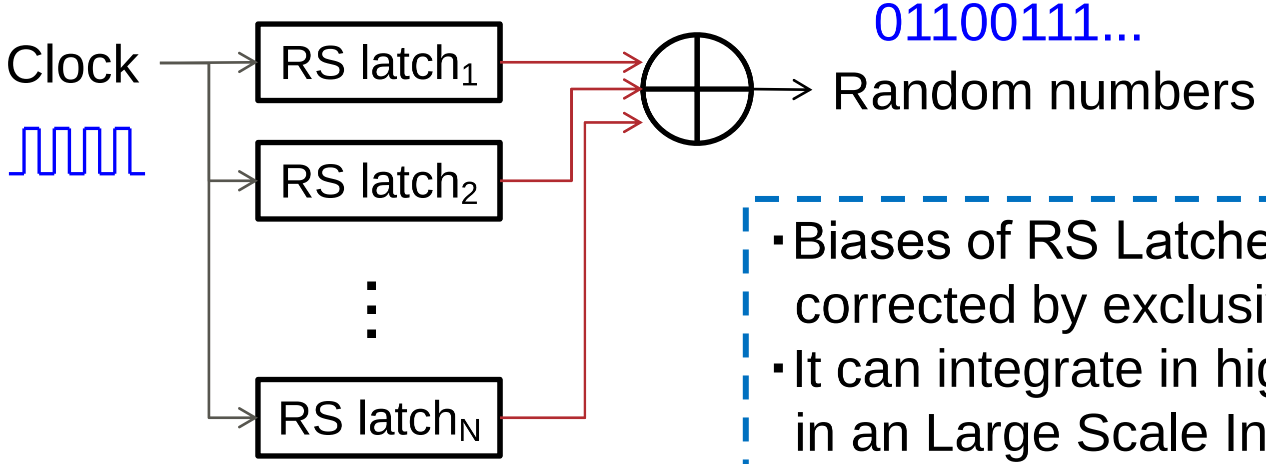
significant behavior

- When A = B = 1, RS Latch enters metastable state, then output C = 0 or 1 (random number)

PTRNG using RS Latches

- Hata et al. implemented PTRNG using RS Latches on FPGAs

[HATA]



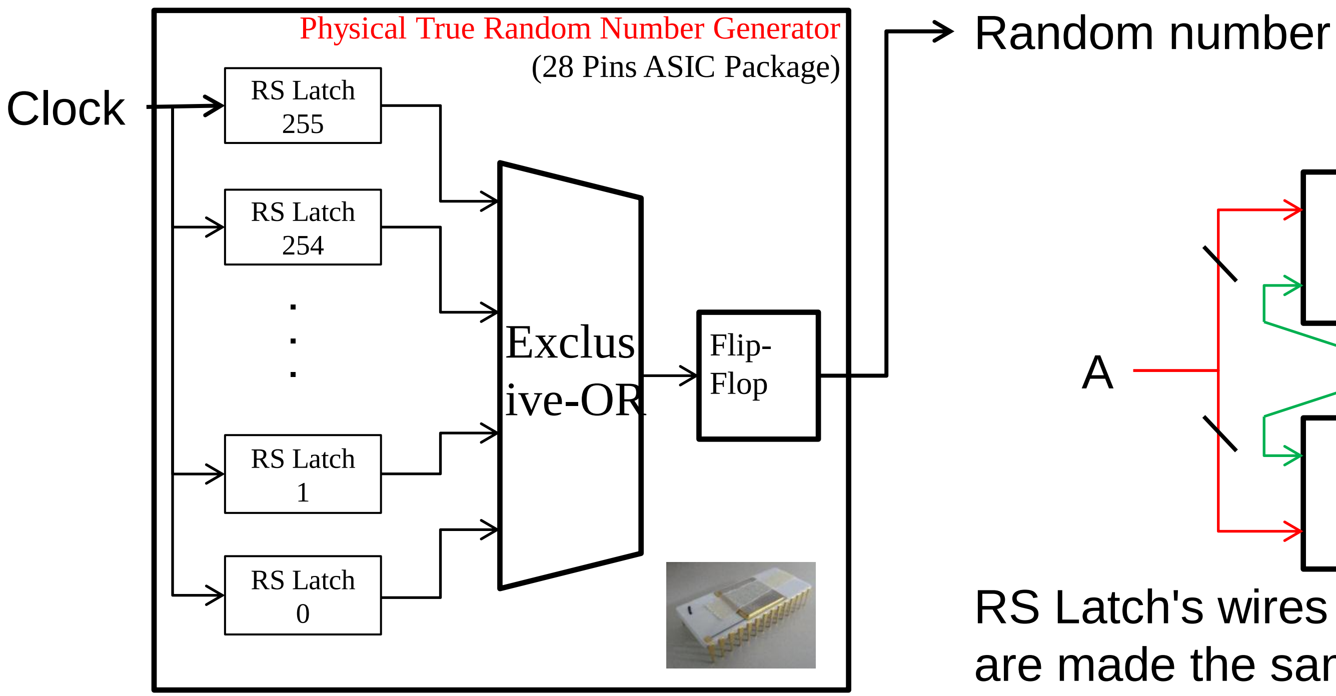
- Biases of RS Latches' outputs are corrected by exclusive-OR
- It can integrate in high-density in an Large Scale Integration (LSI)
- Evaluation of ASIC implementation has not been done yet

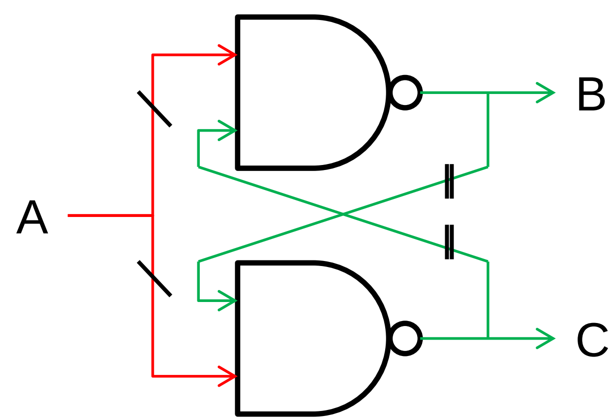
- ASIC implementation is necessary for mass production embedded devices (e.g. smart cards)
  - ASIC have lower power consumption and lower chip cost than FPGAs

[HATA] H.Hata, S.Ichikawa, FPGA Implementation of Metastability-Based True Random Number Generator, IEICE Transactions on Information and Systems, vol.E95-D, no.2, pp.426-436, 2012

Our ASIC Implementation [1/2]

- Our PTRNG generates random numbers from the exclusive-OR of 256 RS Latches' outputs
- The RS Latch was custom-designed on the circuit layout
  - The wire lengths between the two NAND gates are the same
    - The probability of entering a metastable state is improved
    - Implemented as hard macro





RS Latch's wires that have the same mark are made the same length

Our ASIC Implementation [2/2]

- We fabricated our PTRNGs on two types of ASICs
  - N-PTRNG and L-PTRNG
  - One PTRNG per ASIC chip

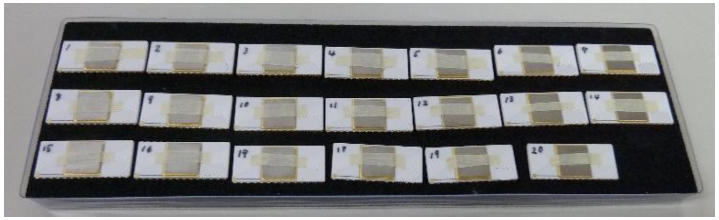
N-PTRNG

- Normal type
- Using standard transistor
- We fabricated 20 chips of PTRNG

L-PTRNG

- Low power type
- Using low leakage transistor
- We fabricated 19 chips of PTRNG

We fabricated total 39 PTRNG chips
(20 N-PTRNG chips and 19 L-PTRNG chips)



20 N-PTRNG chips

Experimental System

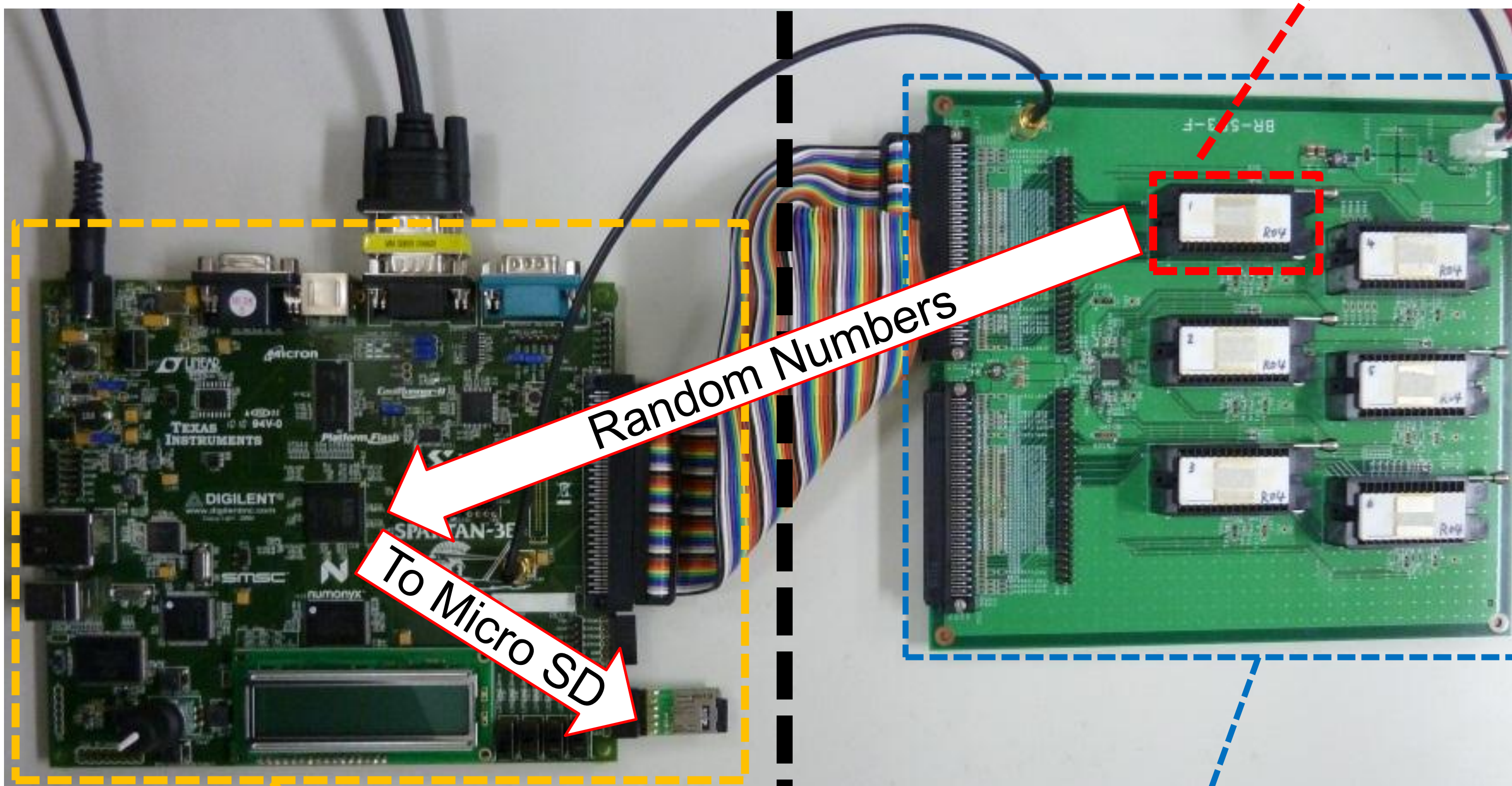
In normal environment

Operated at the rated voltage and room temperature

Into the constant temperature oven

Fluctuating temperature and voltage

ASIC of our PTRNG



FPGA board to control ASICs

Custom-made board for the ASICs

1.Fabricating PTRNGs

2.Measuring power consumption and circuit scale

3.Evaluating the quality of the random numbers

Power Measurement

- Measuring the power and current consumption of the PTRNGs
  - Embedded devices require low-power-consuming PTRNGs

PTRNG's power/current consumption

Type of Chip	current consumption	power consumption
N-PTRNG	0.15mA	0.27mW
L-PTRNG	0.14mA	0.252mW

- Our both PTRNGs are feasible for contactless smart card
  - Typical RFID-ASIC's current consumption is <1mA ～ 10mA *[RFID]*

Our PTRNGs have practicable current consumption

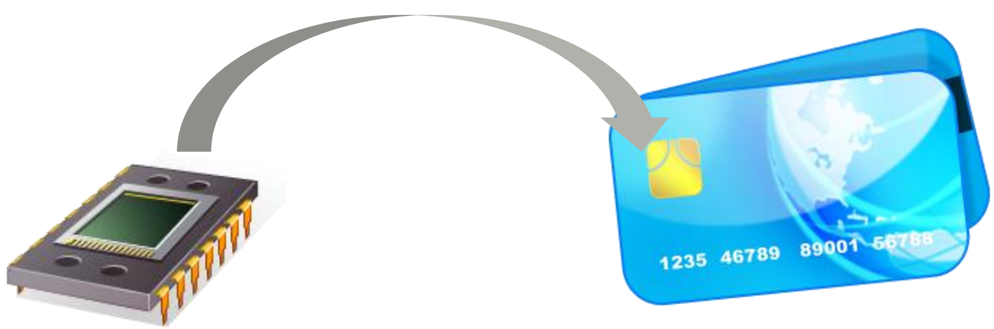
[RFID] Klaus Finkenzeller, RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification, Second Edition, Wiley, 2003.

Scale Measurement

FUJITSU

- <u>Circuit scale of a PTRNG is only 984.3 gates</u>
  - 1 gate is equivalent to a 2-1 NAND gate (2-bit input, 1-bit output)
  - Our PTRNGs have practicable circuit scale

- Our PTRNGs can be embedded in smart cards
  - Triple-DES (≈ 2.3K gates) is used for contactless smart cards
    - MIFARE (NXP semiconductors), FeliCa (Sony), etc.
  - Smaller than implementation of the Triple-DES cipher
    - cf. Ultra-lightweight cipher PRESENT (≈ 1.6K gates) *[PRESENT]*



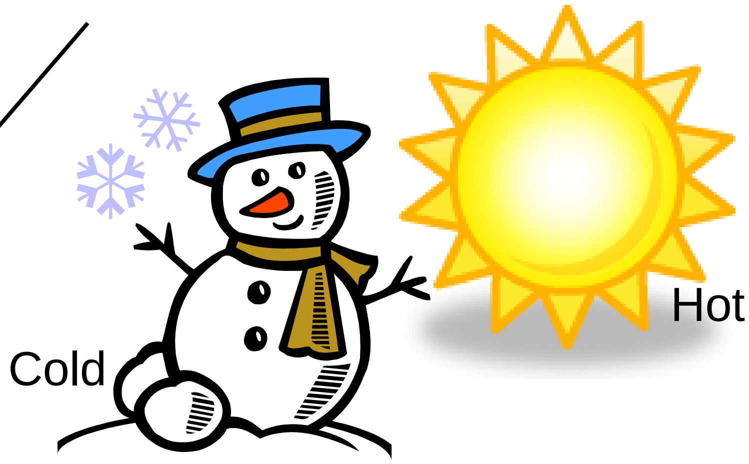
[PRESENT] A.Bogdanov et al., PRESENT: An Ultra-Lightweight Block Cipher, CHES 2007 LNCS, vol.4727, pp.450-466, 2007.

Our PTRNGs

- Power consumption and circuit scale are small enough to be mounted on smart card

- However, how much is...
  - the quality of random numbers?
  - the robustness against irregular conditions?

0001101100111111	*0000000000000100*
0010001000110010	*0000000000001000*
0110010011110011	*0000000000000000*
0100101110011001	*0000010000000010*
Unbiased?	Biased?



1.Fabricating PTRNGs

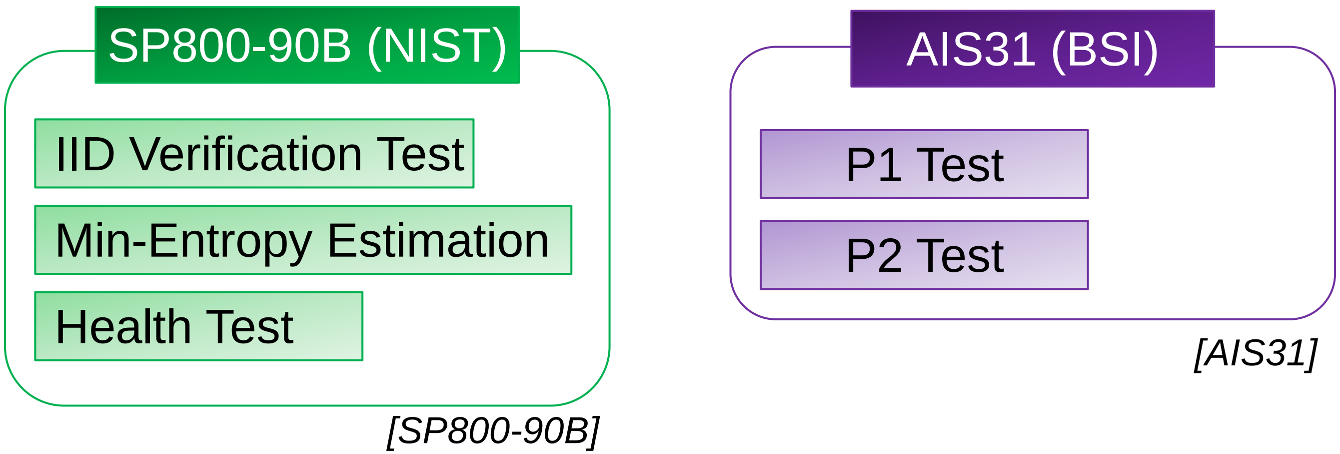
2.Measuring power consumption and circuit scale

3.Evaluating the quality of the random numbers

Evaluation

FUJITSU

- We evaluate whether our PTRNGs generate high-quality random numbers regardless of environmental changes
  - PTRNGs may be influenced by both of temperature and voltage

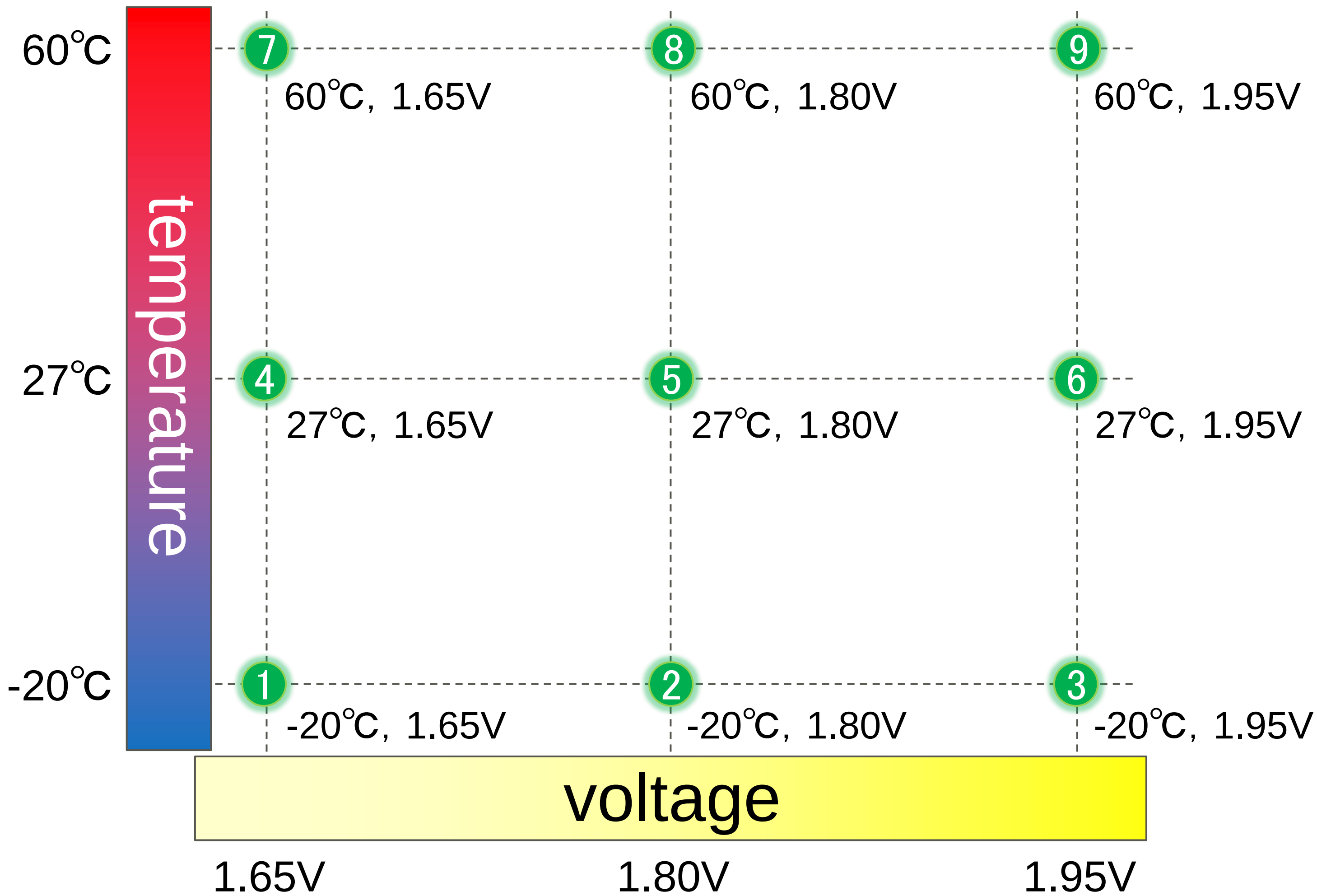


We evaluate comprehensively random numbers in various environments

[SP800-90B] NIST, Special Publication 800-90B, Recommendation for the Entropy Sources Used for Random Bit Generation, 2012.
[AIS31] BSI, AIS31, Functionality classes and evaluation methodology for true (physical) random number generators, 2001.

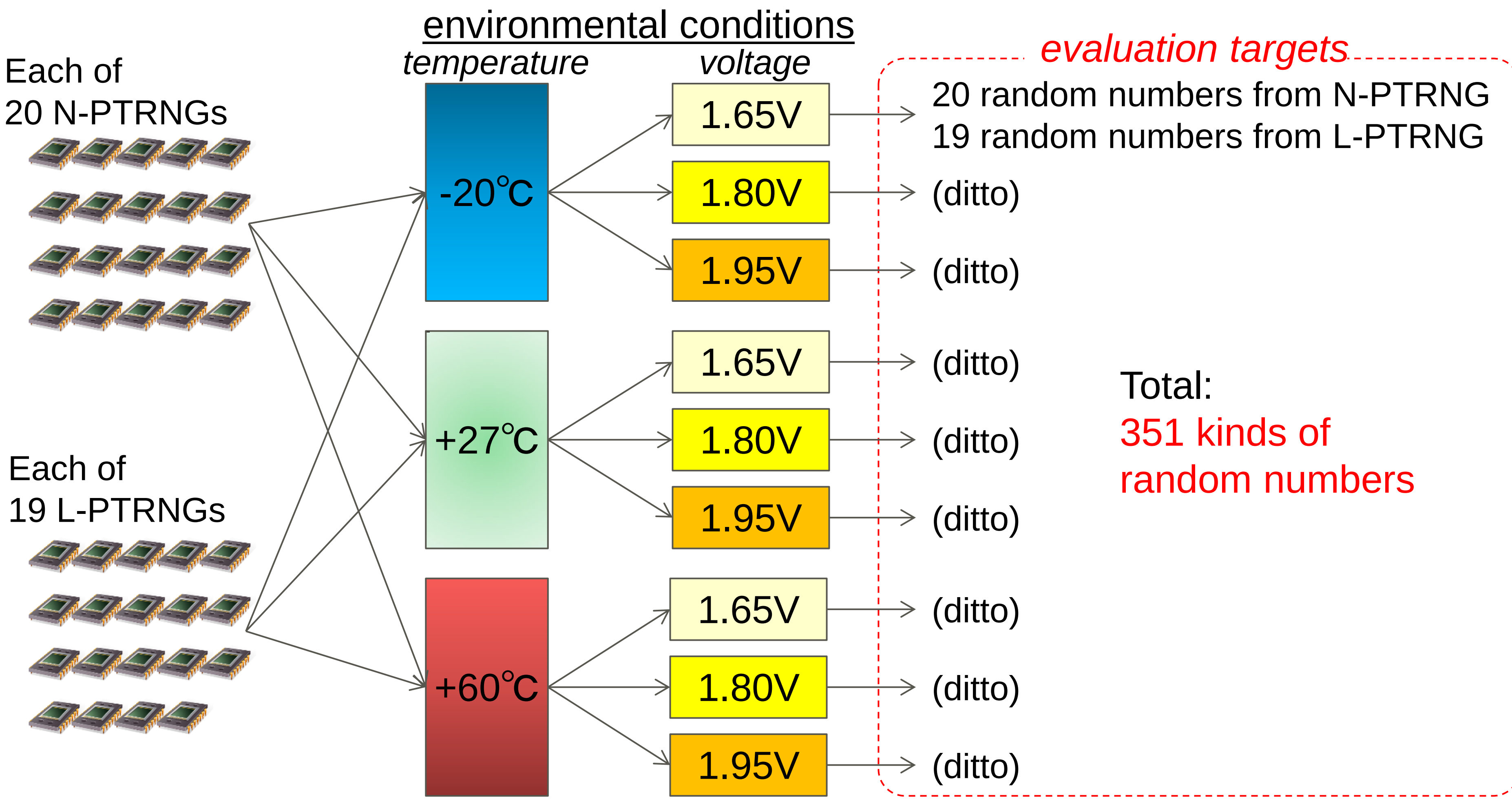
Evaluation Environments

- PTRNGs was evaluated at various temperatures and voltages
  - There are 9 kinds of environments



Evaluation Targets

- Each PTRNGs generate random number in various environments
  - Length of a random number from a PTRNG is about 5.5 million bits



Experimenting in clean room

Evaluation

- We evaluate whether our PTRNGs generate high-quality random numbers regardless of environmental changes
  - PTRNGs may be influenced by both of temperature and voltage

SP800-90B (NIST)

- IID Verification Test
- Min-Entropy Estimation
- Health Test

[SP800-90B]

AIS31 (BSI)

- P1 Test
- P2 Test

[AIS31]

We evaluate comprehensively random numbers in various environments

[SP800-90B] NIST, Special Publication 800-90B, Recommendation for the Entropy Sources Used for Random Bit Generation, 2012.
[AIS31] BSI, AIS31, Functionality classes and evaluation methodology for true (physical) random number generators, 2001.

SP800-90B IID Verification Test

- We verified whether random numbers are **I**ndependent and **I**dentically **D**istributed (IID)
  - IID : A sequence of random variables for which each element of the sequence has the same probability distribution as the other values and all values are mutually independent.*[SP800-90B]*

- 351 random numbers were verified by following tests

Shuffling Test

- Compression Score
- Over/Under Runs Scores
- Excursion Score
- Directional Runs Scores
- Covariance Score
- Collision Score

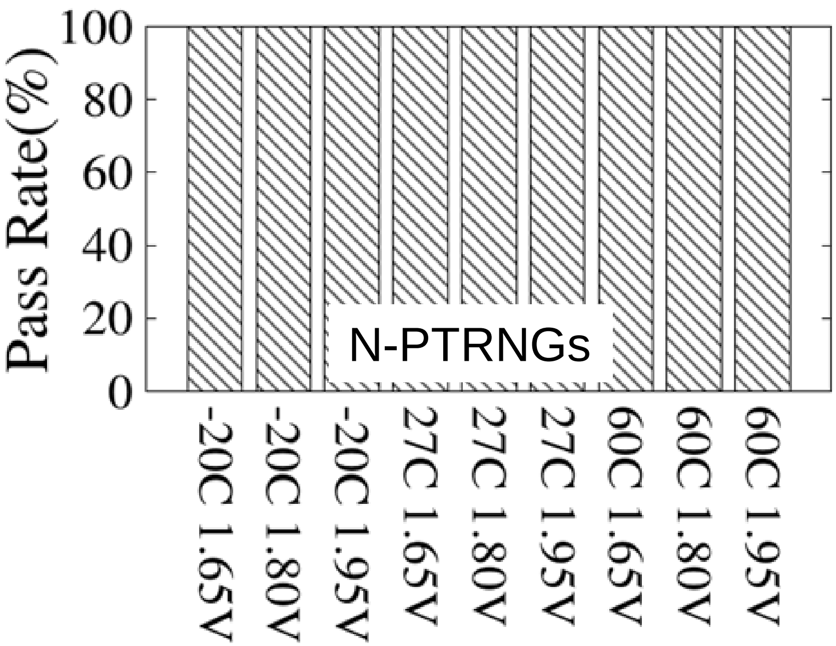
Chi-Square Test

- Testing Independence
- Testing for Stability of Distribution

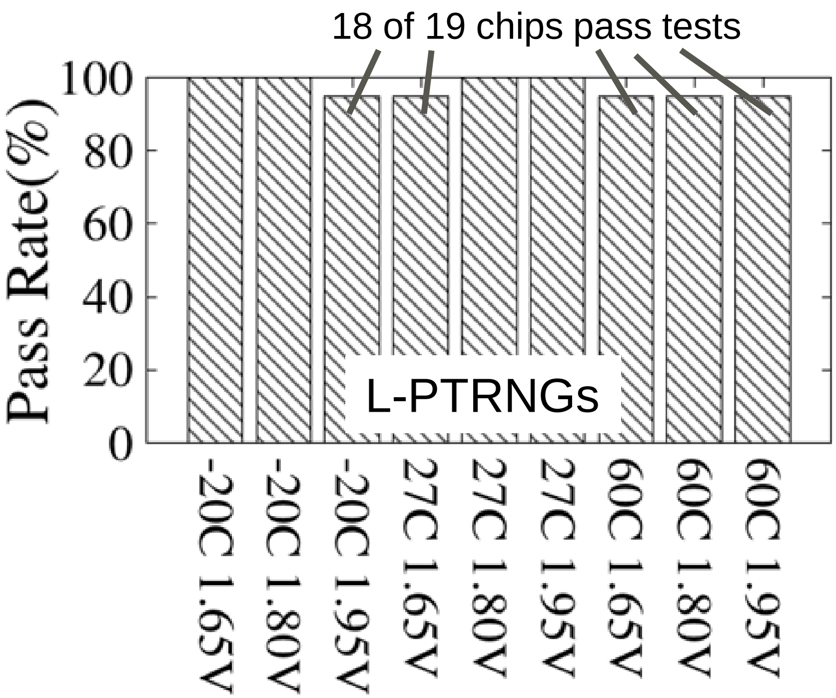
SP800-90B IID Verification Test

- Almost every random numbers are IID in these environments
  - All N-PTRNGs and almost all L-PTRNGs pass the tests

Results



All N-PTRNGs were IID



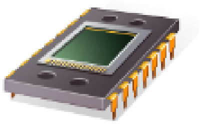
Average 97% of L-PTRNGs were IID

Pass Rate = the number of passing (N or L) PTRNGs / the number of all (N or L) PTRNGs
The number of all N-PTRNGs and all L-PTRNGs are 20 and 19, respectively.

N-PTRNGs outputs random numbers of IID

- N-PTRNGs generates high-quality random numbers of IID !
- N-PTRNGs <u>do not need a conditioner</u>
  - Conditioner is a unit for reducing bias and/or increasing entropy rate
  - Total circuit scale become small to generate unbiased random numbers

Non-IID PTRNGs

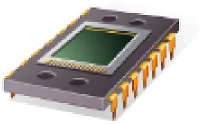


Biased
random number

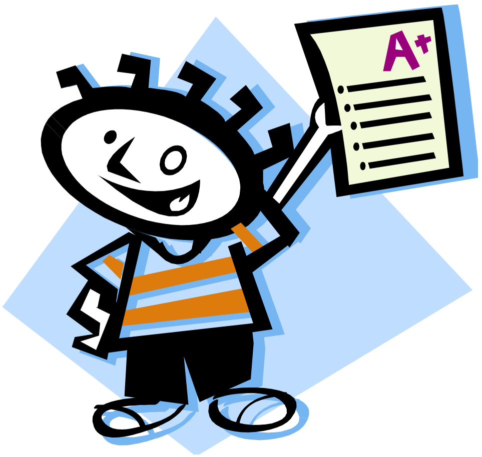
Conditioner
(e.g. Hash Function)

Unbiased
random number

Our N-PTRNGs



Unbiased
random number



Evaluation

- We evaluate whether our PTRNGs generate high-quality random numbers regardless of environmental changes
  - PTRNGs may be influenced by both of temperature and voltage

SP800-90B (NIST)
- IID Verification Test
- Min-Entropy Estimation
- Health Test

[SP800-90B]

AIS31 (BSI)
- P1 Test
- P2 Test

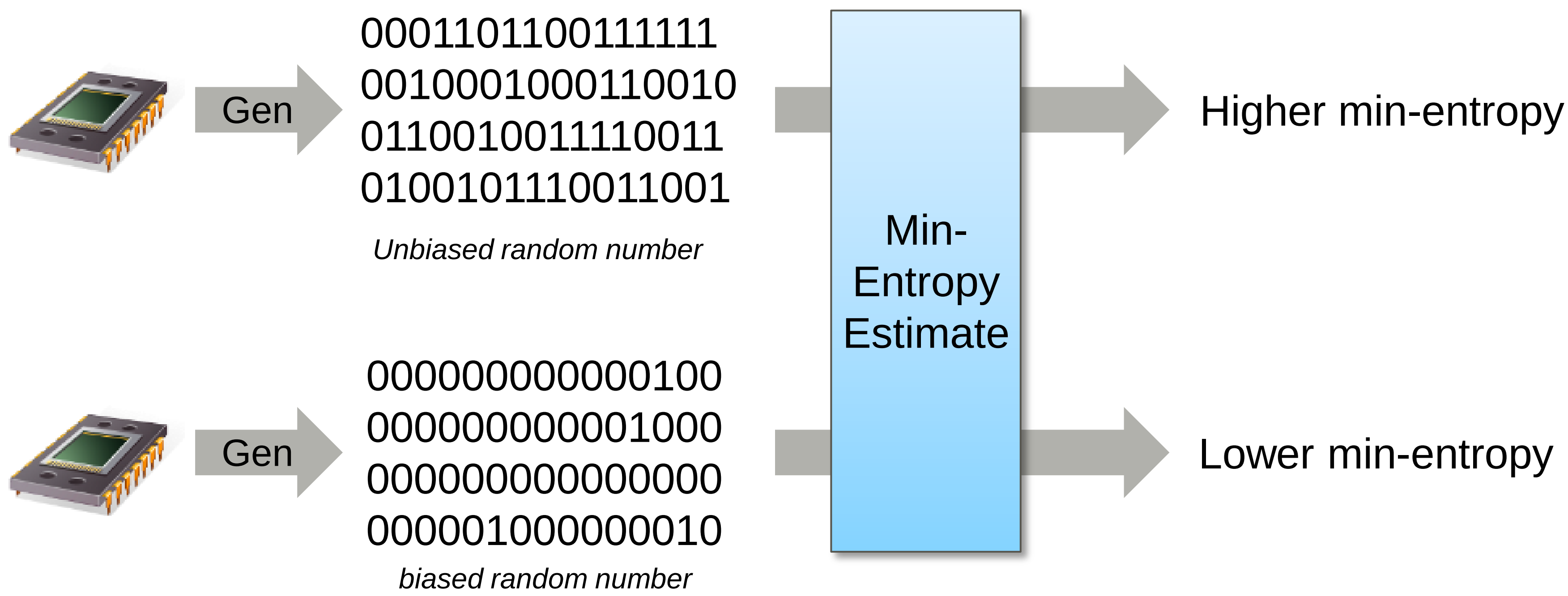
[AIS31]

We evaluate comprehensively random numbers in various environments

[SP800-90B] NIST, Special Publication 800-90B, Recommendation for the Entropy Sources Used for Random Bit Generation, 2012.
[AIS31] BSI, AIS31, Functionality classes and evaluation methodology for true (physical) random number generators, 2001.

SP800-90B Min-Entropy Estimation

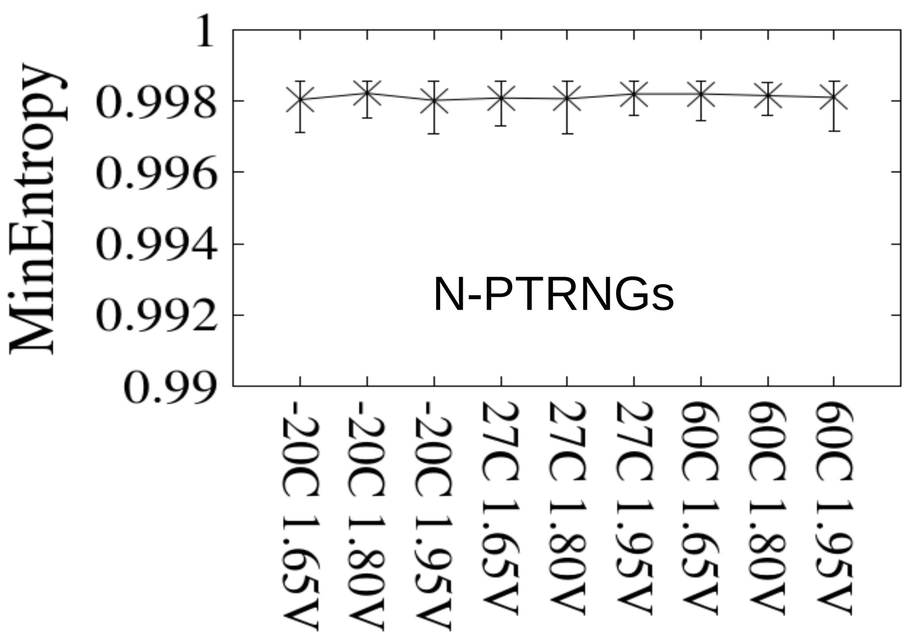
- We estimated min-entropy of random numbers
  - Min-entropy
    - Lower bound of the information amount of Random Numbers
  - Min-entropy is 1.00/bit in true random numbers
  - We regarded random numbers from our PTRNGs as IID

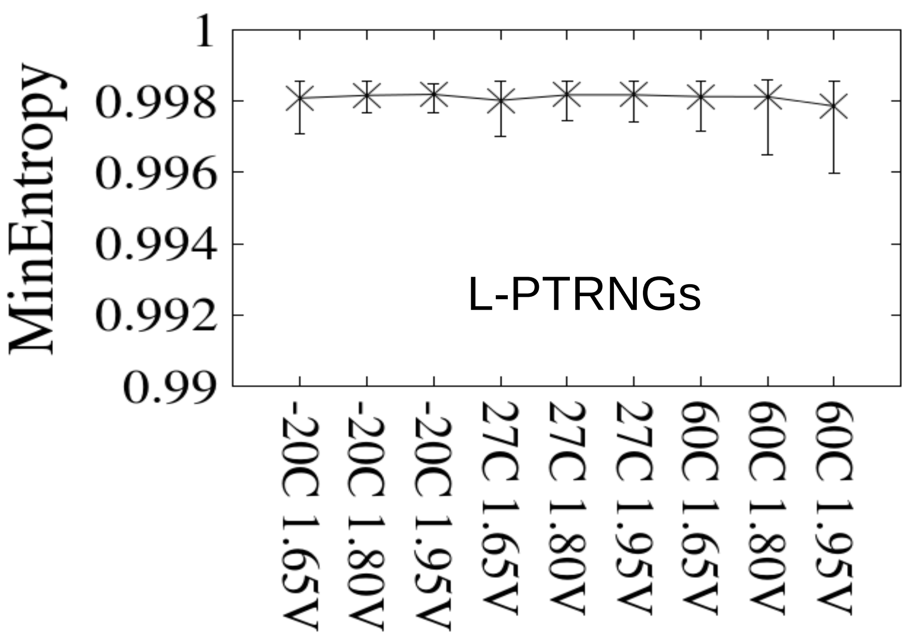


Our PTRNGs can generate high-quality random numbers

- Our PTRNGs' min-entropy are nearly 1.00/bit in these environments
- All PTRNGs' min-entropy are high level

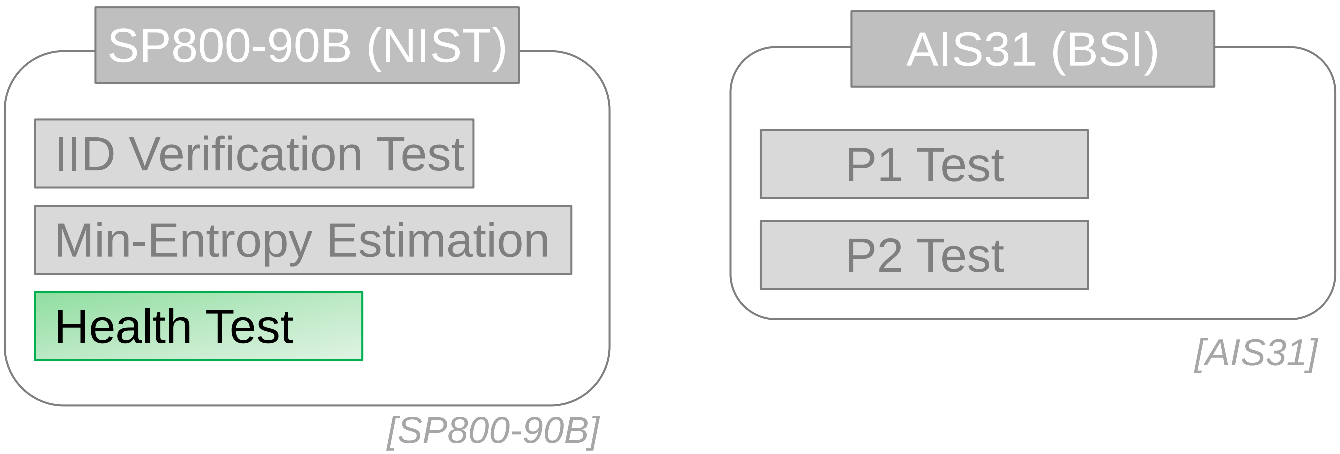
Results





Evaluation

- We evaluate whether our PTRNGs generate high-quality random numbers regardless of environmental changes
  - PTRNGs may be influenced by both of temperature and voltage

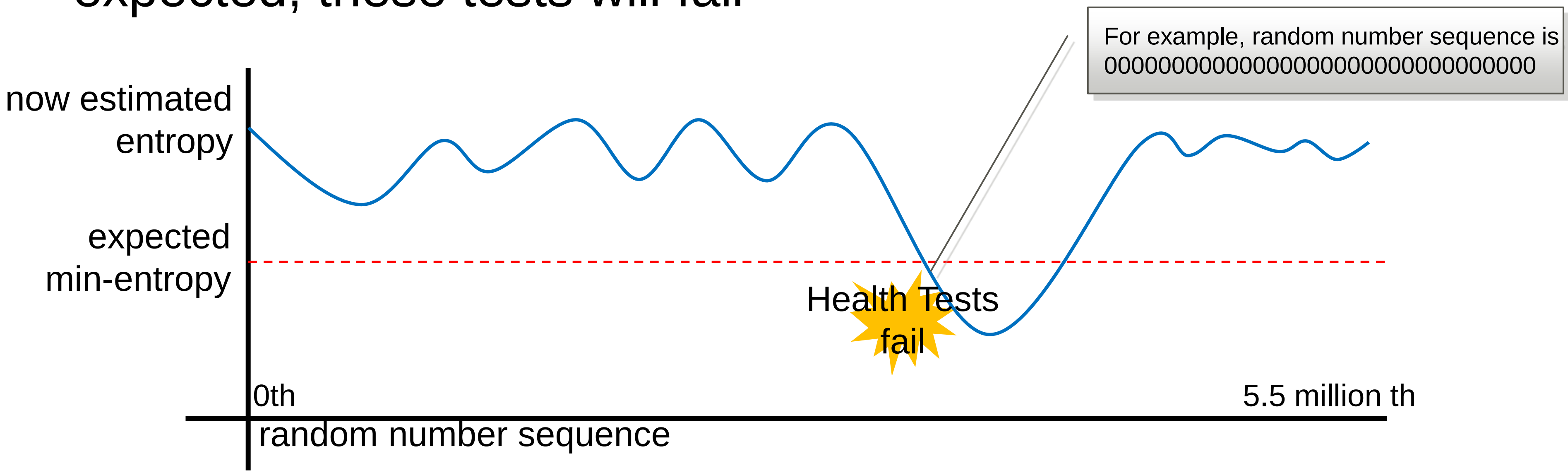


We evaluate comprehensively random numbers in various environments

[SP800-90B] NIST, Special Publication 800-90B, Recommendation for the Entropy Sources Used for Random Bit Generation, 2012.
[AIS31] BSI, AIS31, Functionality classes and evaluation methodology for true (physical) random number generators, 2001.

SP800-90B Health Test

- We evaluated whether our PTRNGs can continuously generate high-entropy random numbers
  - By using Repetition Count Test and Adaptive Proportion Test from SP800-90B
- If PTRNG generate random number with lower entropy than expected, these tests will fail

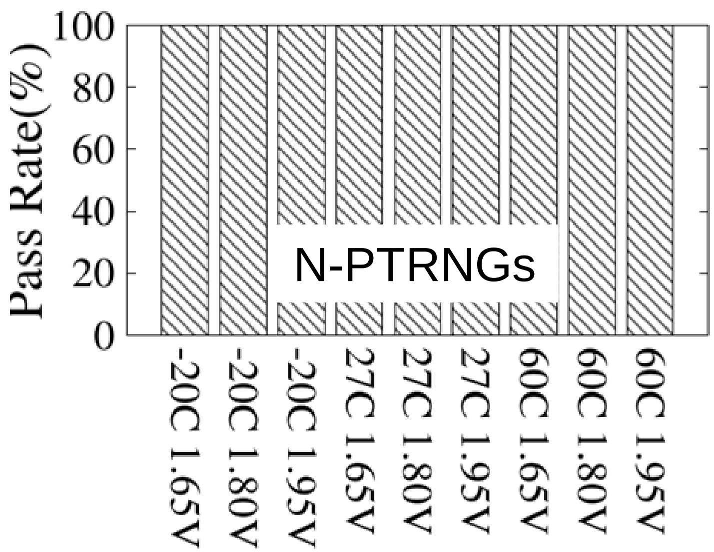


Conceptual Diagram of Health Test

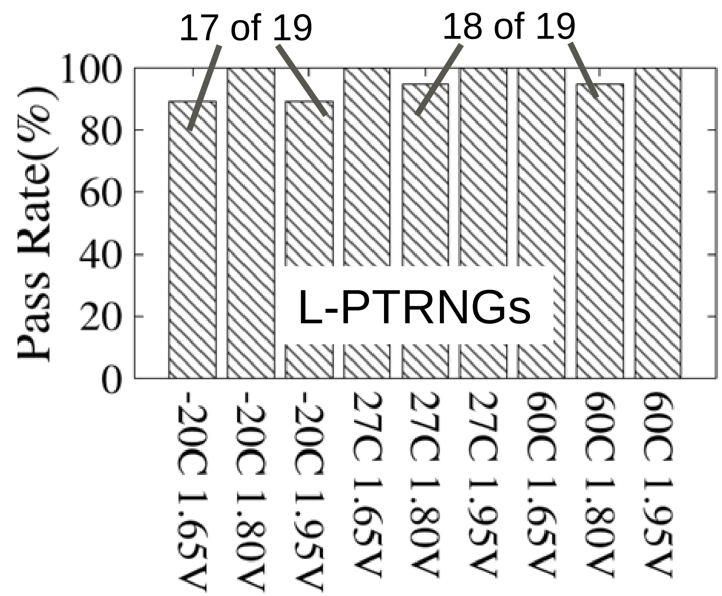
SP800-90B Health Test

- N-PTRNGs can generates high-quality random number continuously
  - All N-PTRNGs pass both Health Tests in these environments
    - Pass : failure was not found by both Health Tests
  - L-PTRNGs require some methods to improve

Results



All N-PTRNGs pass health tests



A few L-PTRNGs fail health tests

Evaluation

- We evaluate whether our PTRNGs generate high-quality random numbers regardless of environmental changes
  - PTRNGs may be influenced by both of temperature and voltage

SP800-90B (NIST)
- IID Verification Test
- Min-Entropy Estimation
- Health Test

[SP800-90B]

AIS31 (BSI)
- P1 Test
- P2 Test

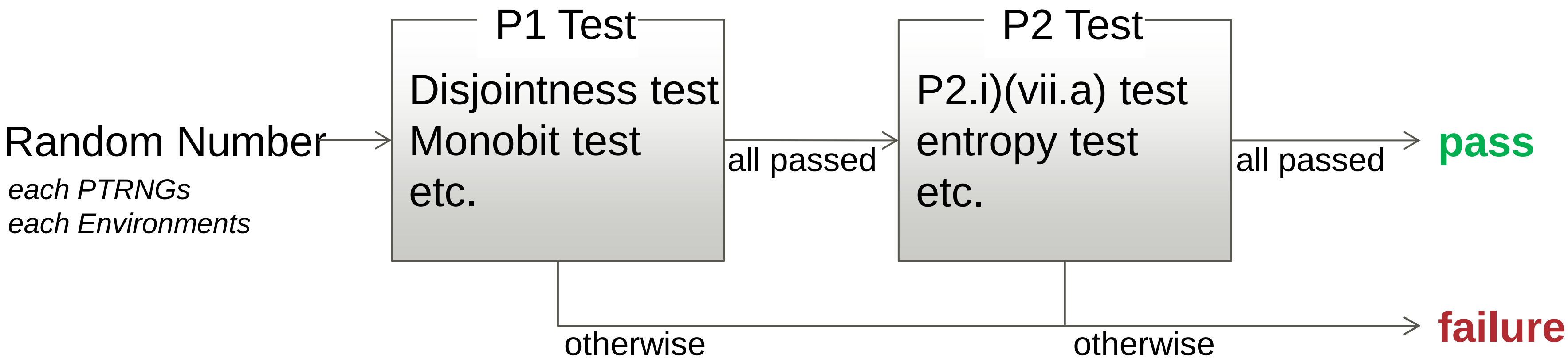
[AIS31]

We evaluate comprehensively random numbers in various environments

[SP800-90B] NIST, Special Publication 800-90B, Recommendation for the Entropy Sources Used for Random Bit Generation, 2012.
[AIS31] BSI, AIS31, Functionality classes and evaluation methodology for true (physical) random number generators, 2001.

AIS31 P1,P2 Tests

- AIS31 classifies PTRNGs into P1 Class and P2 Class
  - P1 Class : For challenge & response auth, etc.
  - P2 Class : For key and seed generations of pseudo RNG, etc.
    - P2 requires higher security than P1
- These tests include various statistical tests
  - Poker Test, the Long Run Test, the Uniform Distribution Test etc.
- If the PTRNG fails either P1 or P2 Tests, we consider it to have failed the tests

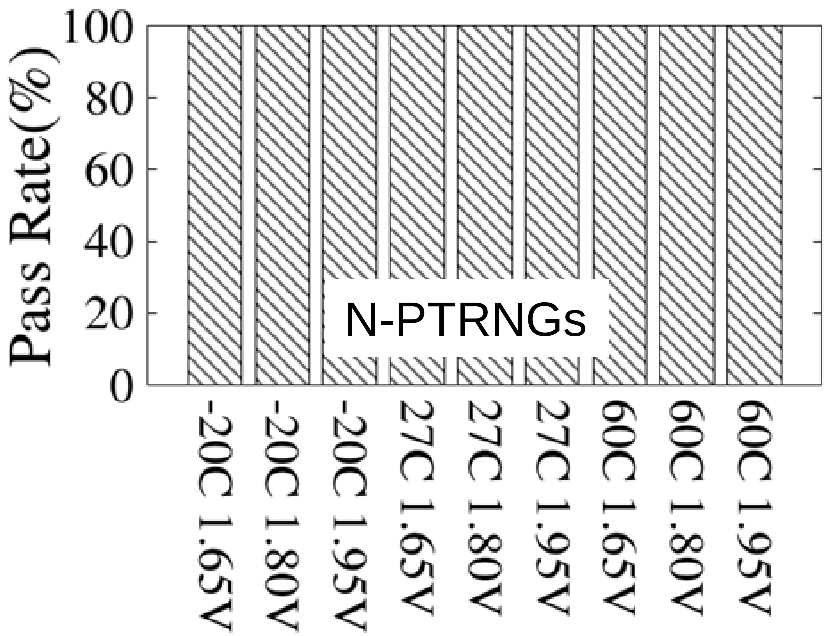


FUJITSU

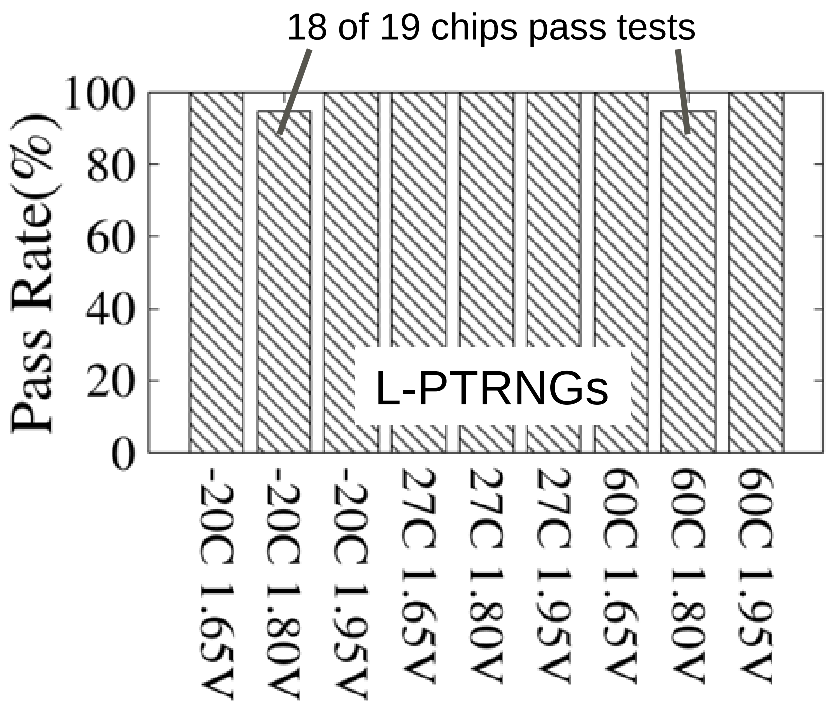
AIS31 P1,P2 Tests

- All N-PTRNGs generate random numbers that meet P2 class
  - These PTRNGs can be used in the field where high security is required
- Some of L-PTRNGs failed P1 or P2 Tests
  - L-PTRNGs require some methods to enhance randomness

Results



All N-PTRNGs pass P1 and P2 Tests



Almost all L-PTRNGs pass P1 and P2 Tests

Conclusion

FUJITSU

1. Our PTRNGs on 0.18μm ASIC have low power consumption and small circuit scale
2. Our PTRNGs can generate high-quality random number
3. Our PTRNGs have high robustness against various environmental changes

PTRNG	Power / Current consumption	Circuit scale	IID Test	Min-Entropy (avg.)	Health Test	AIS31 Test
N-PTRNG	0.27mW / 0.15mA	984.3 gates	All passing	0.9981	All passing	All passing
L-PTRNG	0.252mW / 0.14mA		Almost passing	0.9981	Almost passing	Almost passing

Our PTRNGs are suitable for smart cards

Future Work

- Evaluation in larger environments fluctuations
- Resistant evaluation to side channel and fault attacks
- Experiment of continuous running

FUJITSU

shaping tomorrow with you