1S-2

An Oscillator-Based True Random Number Generator with Process and Temperature Tolerance

Takehiko Amaki, Masanori Hashimoto and Takao Onoye

Osaka University

hasimoto@ist.osaka-u.ac.jp

1S-2

Security and random number

- Cryptography and authentication system requires unpredictable random numbers.

  ex.) Private/Public key generation,

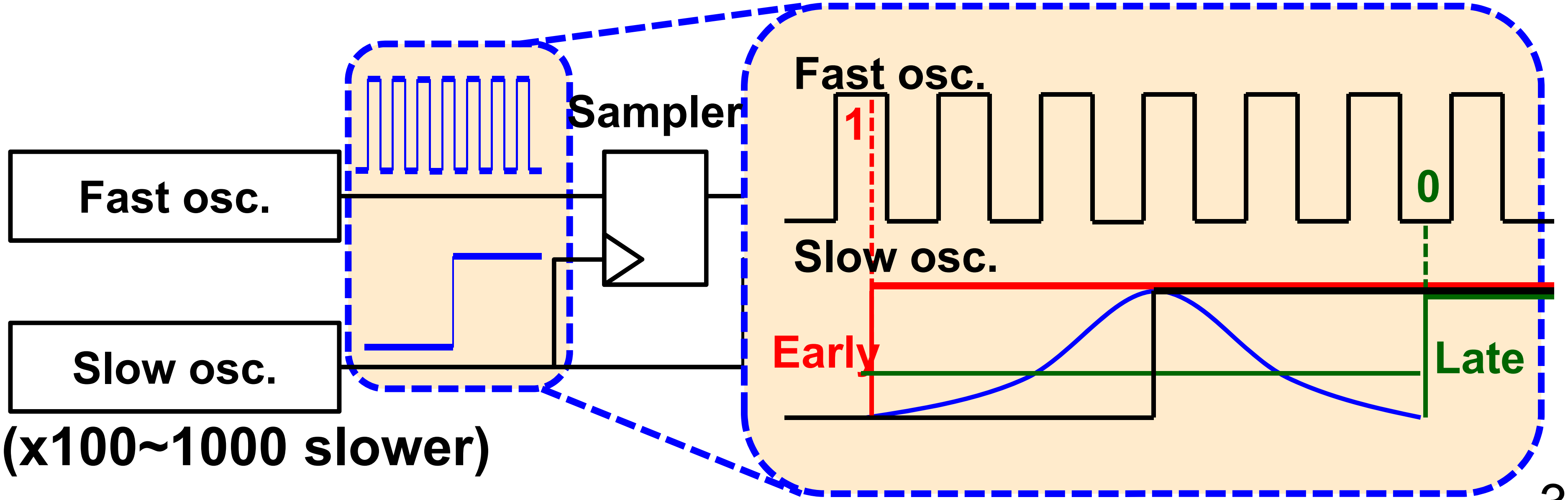
  challenge-and-response authentication, etc.

- Random number generator
  - Pseudo random number generator
    - Mathematical calculation
    - Output is periodic and then predictable.
  - True random number generator (TRNG)
    - Physical random source
    - Output is unpredictable.

1S-2

Oscillator-based TRNG

- Acquires randomness from period jitters of oscs.
- Pro: Easy to implement
- Con: Difficult to generate highly random numbers
  - sensitive to duty cycle of fast osc.

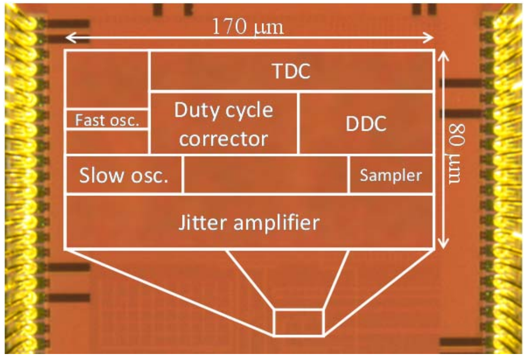


Duty cycle of fast osc. decides 0/1 probability.

Contribution

- Duty cycle variation due to temperature
  - Biases 0/1 probability beyond 50±0.125% and makes TRNG fail in NIST randomness test.
  - Cannot be eliminated by static tuning at shipping test

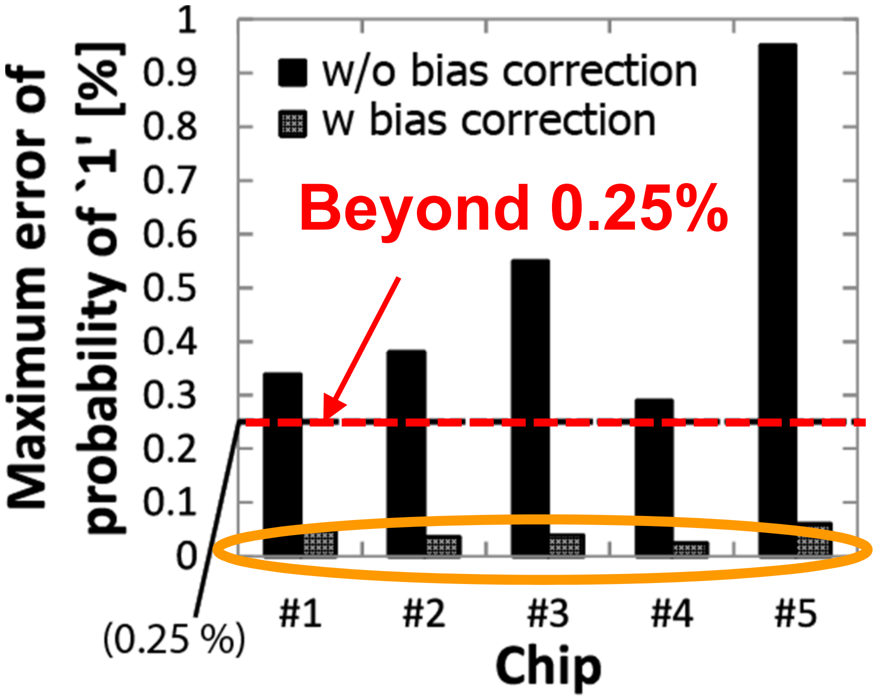
- Developed a TRNG w/ dynamic 0/1 bias correction for process and temperature tolerance
  - Fast duty cycle monitor
  - Duty cycle adjuster

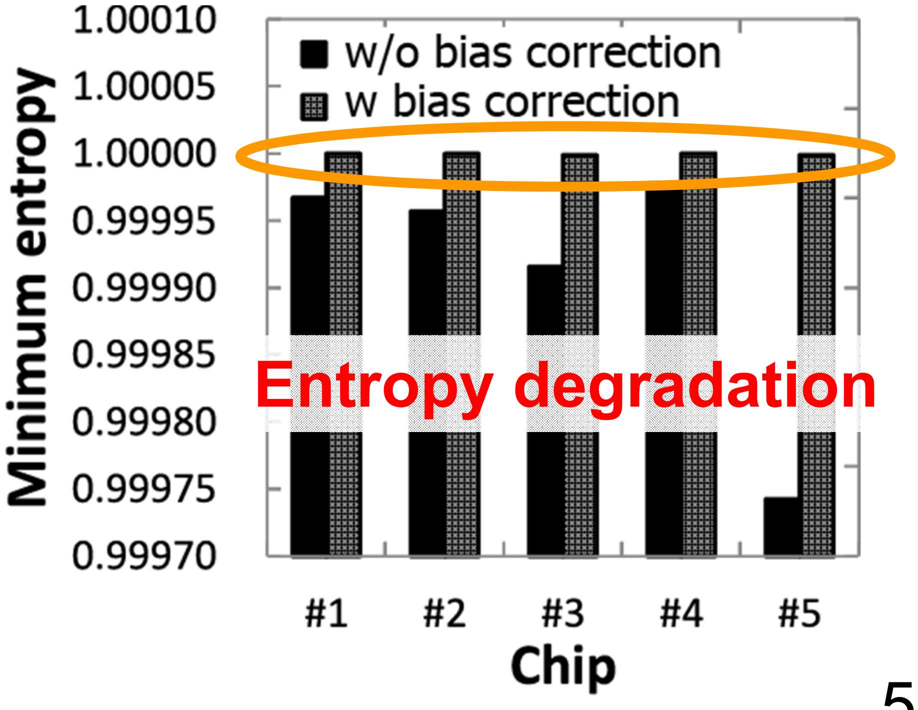


65nm CMOS

Dynamic duty cycle correction

- Proposed duty cycle correction sustained duty cycle and entropy under temperature variation between 0°C and 75°C.
  - Without it, duty cycle and entropy degraded.





1S-2

Comparison w/ existing works

- Among TRNGs that pass NIST tests, area of proposed TRNG is minimum.

	Bucci 2013 [11]	Bucci 2008 [3]	Pareschi 2010 [12]	Srinivasan 2010 [2]	This work
Type	Direct amp.	Osc.	Chaos	Metastable	Osc.
Tech.	180nm	90nm	180nm	45nm	65nm
Area (45nm)	1,563µm^2	3,250µm^2	7,875µm^2	4,004µm^2	3,335µm^2
Randomness test	FIPS140-1 Knuth	AIS31 Entropy	NIST	NIST Entropy Auto corr. Run length	NIST DIEHARD