NANYANG TECHNOLOGICAL UNIVERSITY

An Energy-efficient True Random Number Generator Based on Current Starved Ring Oscillators

Yuan Cao[1], Chip-Hong Chang [1,*], Yue Zheng [1], and Xiaojin Zhao [2]

1 School of Electrical and Electronic Engineering, Nanyang Technological University

2 College of Electronic Science and Technology, Shenzhen University

Outlines

1. Introduction
2. State-of-the-Art Silicon TRNGs
3. Proposed TRNG Based on Current Starved ROs
4. Results and Discussion
5. Conclusion

A Piece of News…

Two Russians used high-tech tools for slot-machine scam*

- Within **3** days in May 2016, they won **$108,995** from cheating at play at Marina Bay Sands and Resorts World Sentosa casinos in Singapore.
- They **reverse engine** the algorithms, known as **pseudorandom number generators**, that govern how slot machine games behave. They can **predict** when certain games are likeliest to spit out money.

Slot machines at Marina Bay Sands and Resorts World Sentosa (pictured) casinos. PHOTO: BLOOMBERG

Radoslav Skubnik, 40, admitted to three charges of cheating

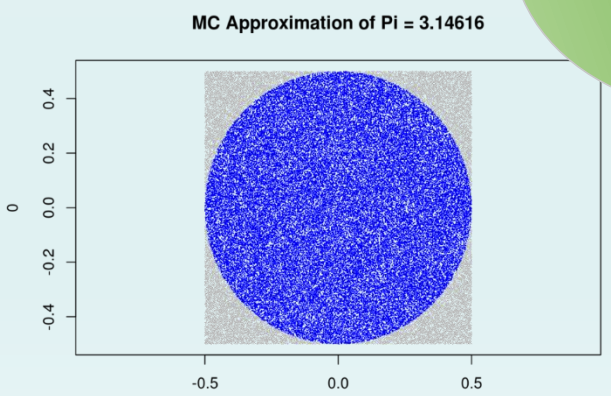
* http://www.straitstimes.com/singapore/two-russians-used-high-tech-tools-for-slot-machine-scam

Random Number Generators (RNGs)

Cryptography

"It is not easy to invent a fool-proof random-number generator." – Don Knuth

RNG



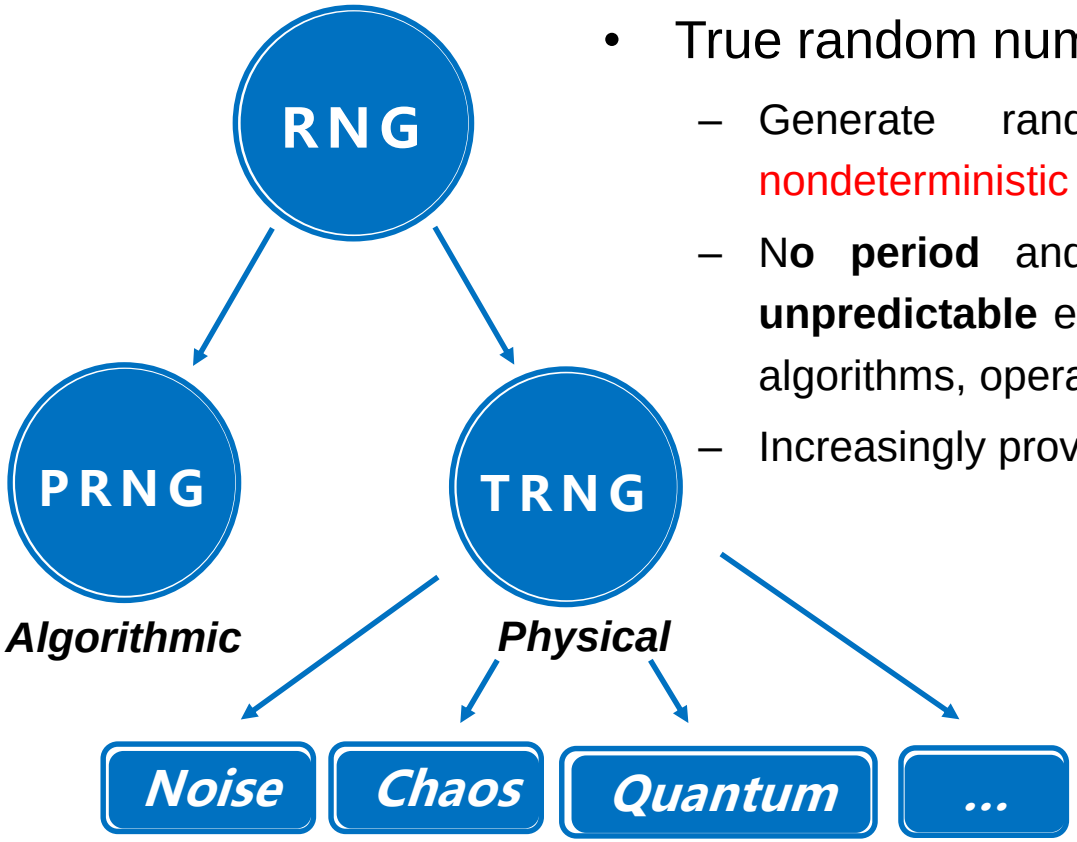
Monte Carlo simulations

Artificial Intelligence

NANYANG TECHNOLOGICAL UNIVERSITY

PRNG Versus TRNG

- Pseudo random number generator (PRNG)
  - Based on mathematical models or formulas.
  - Completely determined by the initial state called seed.
- True random number generator (TRNG)
  - Generate randomness from a fundamentally nondeterministic physical process.
  - N**o period** and **more secure** because they are **unpredictable** even if all the details (e.g., schematics, algorithms, operations, etc.) are known.
  - Increasingly provided on modern processors.



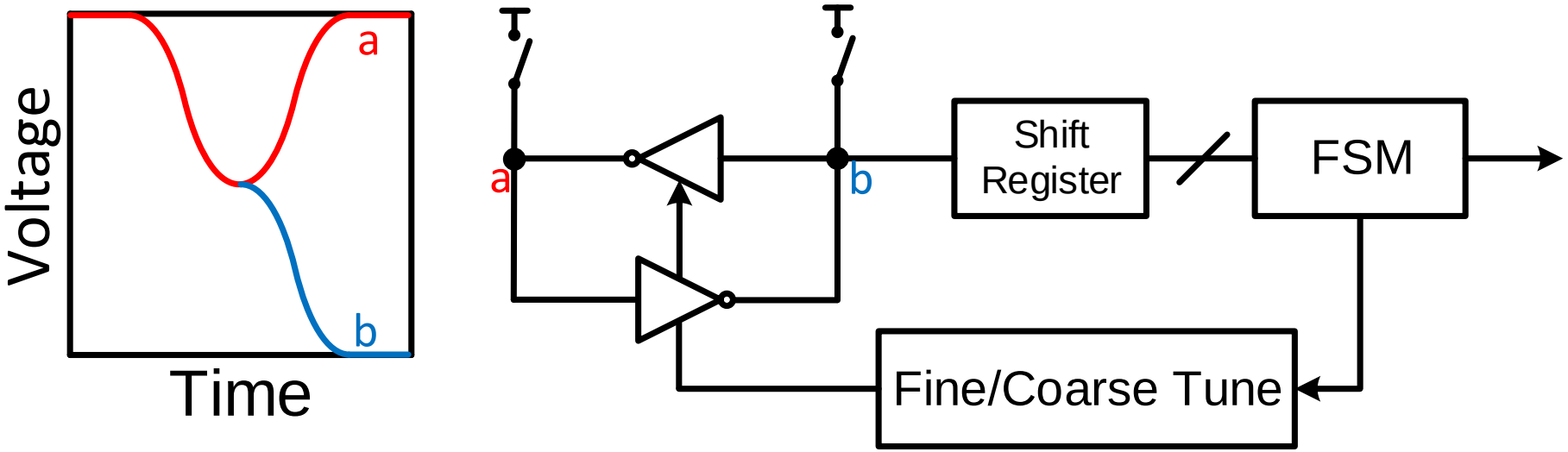
State-of-the-Art Silicon TRNGs

- Direct noise amplification from devices
  - Random Telegraph Noise (R. Brederlow, ISSCC, 2006)
  - Resistor thermal noise (V. Kaenel, CICC 2007)
- Metastability TRNG (C. Tokunaga, JSSC, 2008; S. Mathew, JSSC, 2012)
  - Inverter pair driven to metastable state
  - Requires continuous calibrating loop
- Conventional ROs based TRNG (M. Bucci, Tran. on Comp., 2003)
  - Harvesting noise from oscillator jitter
  - Generally requires noise amplification otherwise yield with low efficiency

Meta-stability Based TRNG

Inverter pair driven to meta-stability and resolved to ‘0’ or ‘1’ depending on noise direction

- Percentage of ‘0’s and ‘1’s is relatively sensitive to inverter pair mismatch (requires $\Delta V_{INV} < 0.24\sigma_{Vnoise}$)
- Limited randomness: P(0) (probability of generating ‘0’s) is 33~49% for a supply range from 0.8V to 1.2V



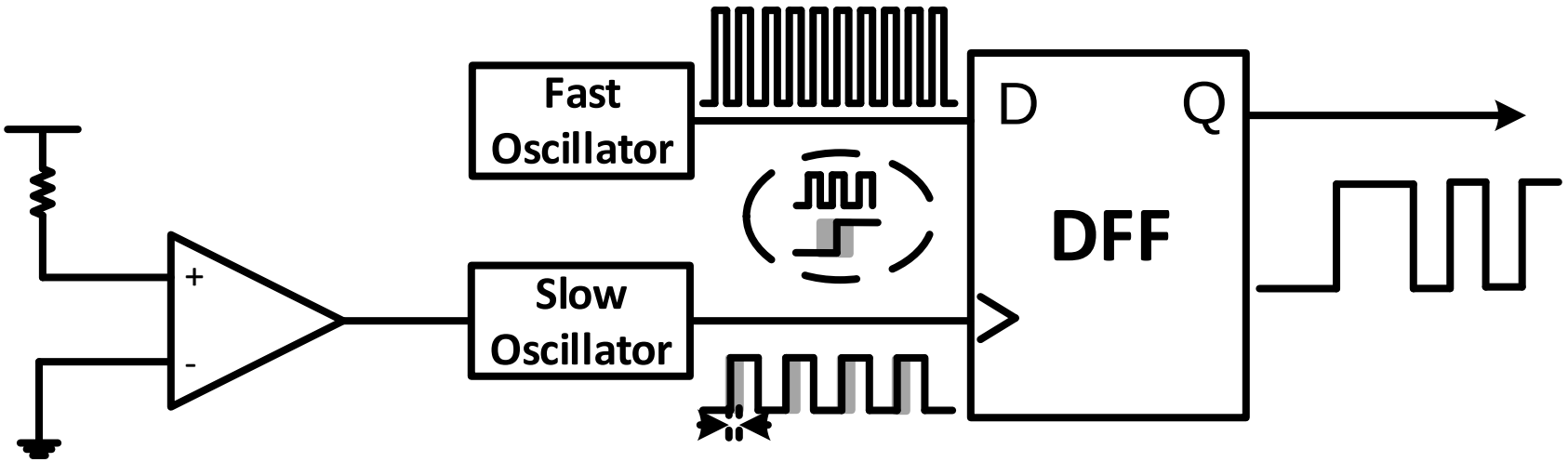
 S. K. Mathew, et al., JSSC, vol. 47, 2012

NANYANG TECHNOLOGICAL UNIVERSITY

Dual Oscillator Based TRNG

Faster oscillator sampled by a much slower oscillator

- Output is truly random only when $\Delta T_{slow} > T_{fast}$
- Amplification is required to enlarge ΔT_{slow}



NANYANG TECHNOLOGICAL UNIVERSITY

Jitter Noise in Weak and Strong Inversion

The RO based TRNG extracts random bits from the jitter noise of inverter based ROs.

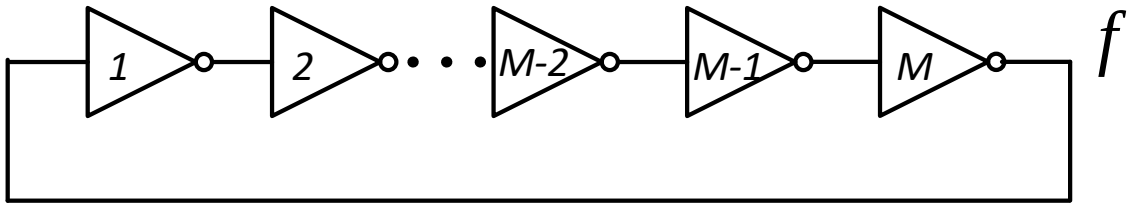
– Jitter for strong inversion RO:

$$\sigma_\tau^2 = \frac{2kT}{If_0}\left(\frac{1}{V_{DD}-V_{th}}(\gamma_N+\gamma_P)+\frac{1}{V_{DD}}\right)$$

– Jitter for weak inversion RO:

$$\sigma_\tau^2 = \frac{q}{If_0}\left((1+e^{-V_{DD}/2V_t}\right)$$

– Notice: in both strong and weak inversion ROs, σ_τ^2 is inversely proportional to the charging/discharging current I and the oscillation frequency f_0.

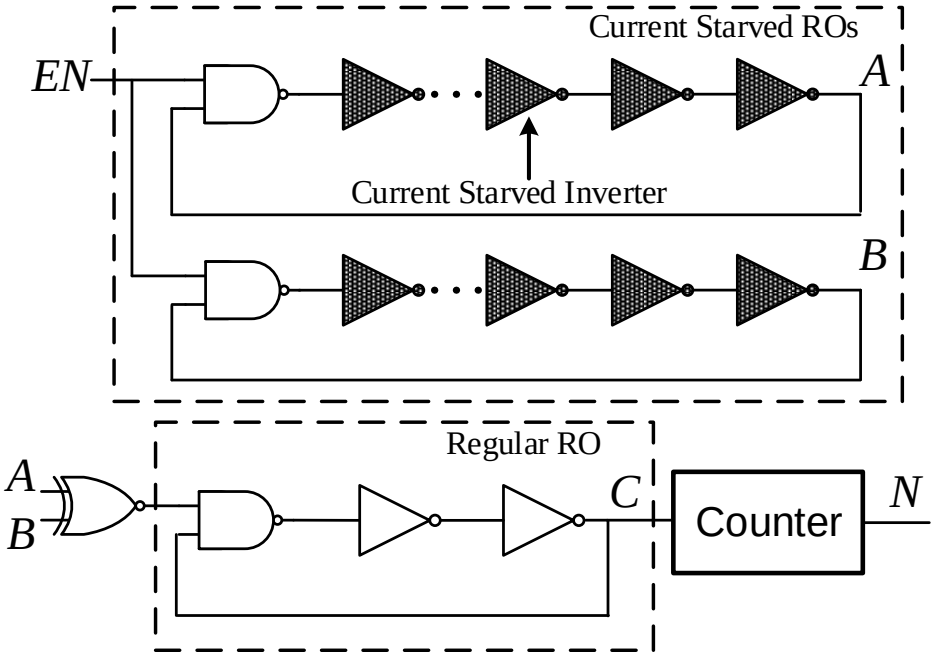


M stage inverter based ROs.

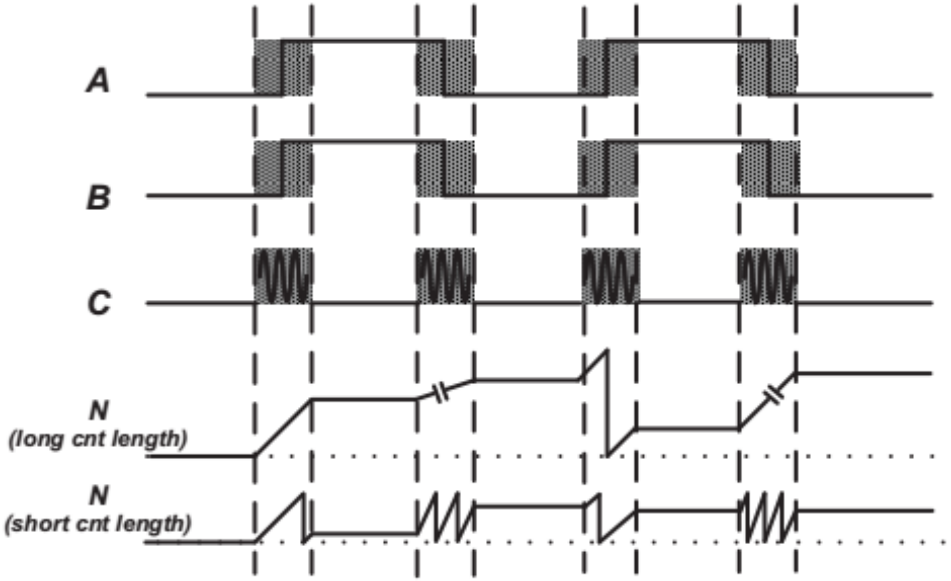
Proposed TRNG Based on CS-ROs

The proposed TRNG is to capture and quantize the jitter noise between two independent current starved (CS) ROs.

- Inverters in the two CS ROs operates in the subthreshold region.
- Inverters in the regular RO operates in the strong inversion region.



Block diagram of the proposed TRNG.

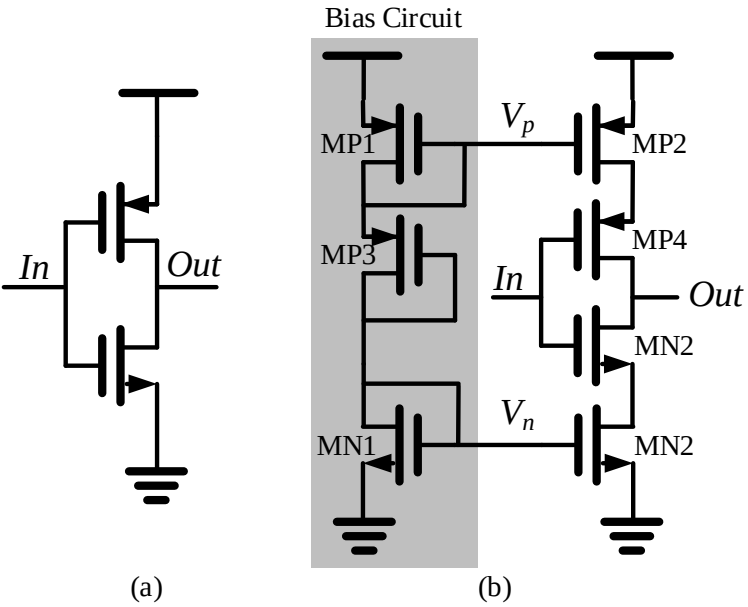


Timing diagram of waveforms at internal circuit nodes of the proposed TRNG

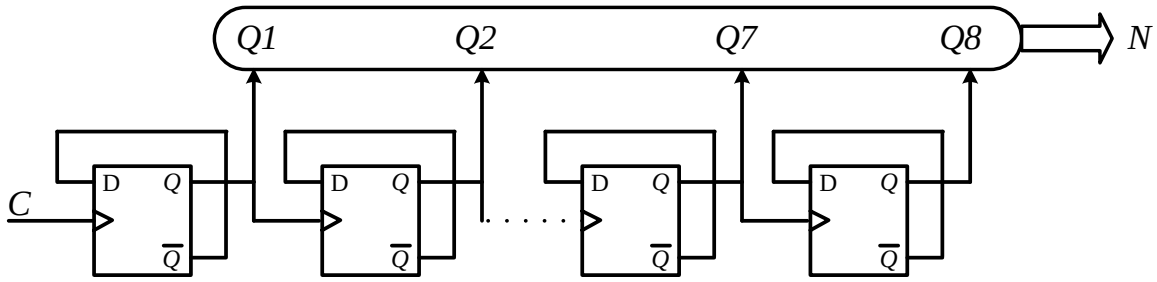
NANYANG TECHNOLOGICAL UNIVERSITY

Proposed TRNG Based on CS-ROs

- The bias V_p and V_n for the CS inverter are generated on chip and shared with other CS inverters.
- An asynchronous *L*-bit counter with E-TSPC DFFs is faster and consumes less power.



(a) Regular and (b) current starved inverter.

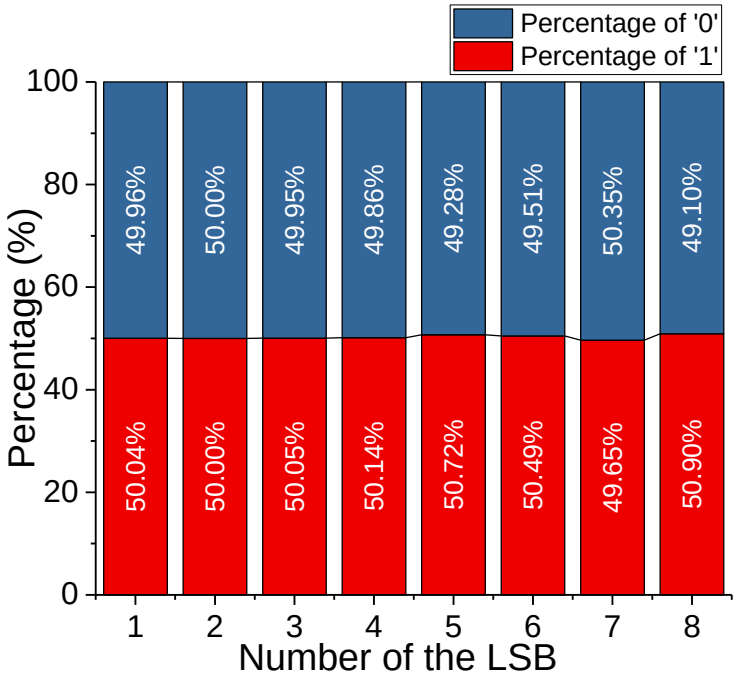


Block diagram of an asynchronous L-bit counter with E-TSPC D-FFs.

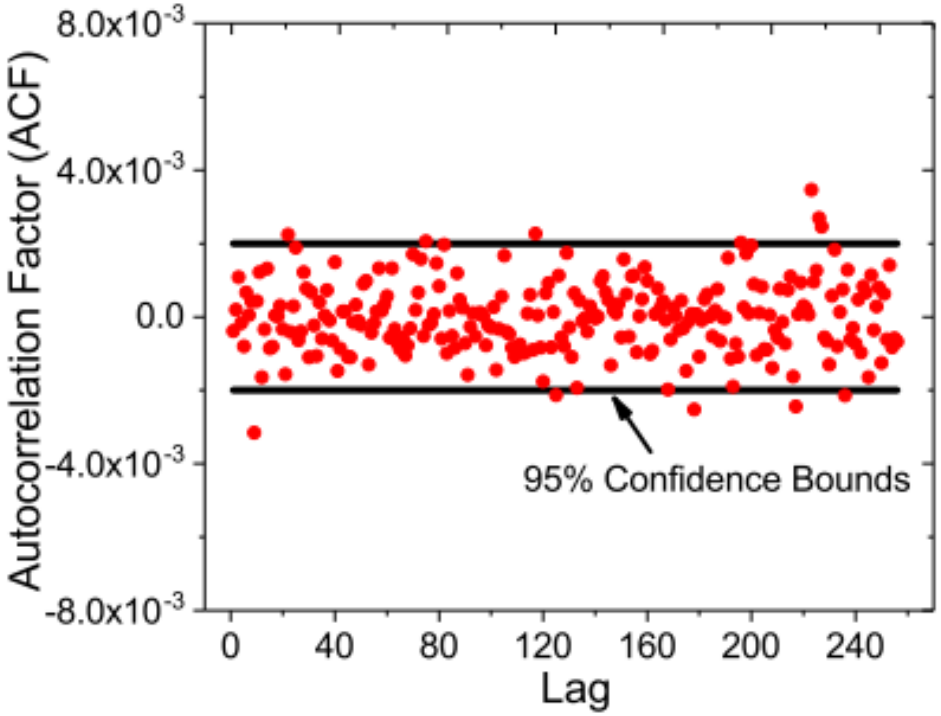
NANYANG TECHNOLOGICAL UNIVERSITY

Results and Discussion

Transistor-level simulation of proposed TRNG using 65nm 1.2V CMOS technology at 27℃ by Cadence Virtuoso Spectre.



Bias test result for the 10,000,000 output bit stream of an 8-bit E-TSPC counter.



Autocorrelation measurements of 10,000,000 consecutive bits.

NANYANG TECHNOLOGICAL UNIVERSITY

Results and Discussion

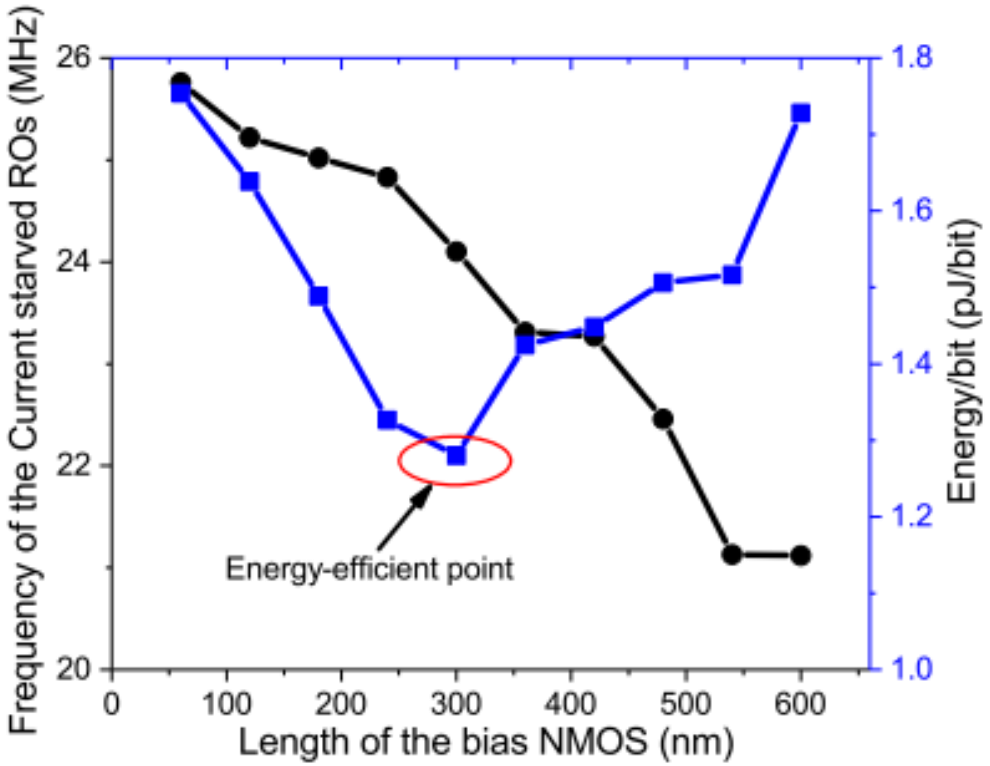
- 10,000,000 raw bits are tested by the NIST Pub 800 statistical test suite with recommended settings.
- Counter length $L \approx \log_2 2N$, where $N \propto \sigma_\tau / \tau$. τ : period of regular RO.
- For counter length longer than 2, only 2 LSBs passed all 15 NIST tests. Higher order bits failed NIST tests due to monotonic correlation.
- To extract more random bits, N should be increased to avoid monotonic correlation.

Test	1st LSB		2nd LSB		3rd LSB		4th LSB		Final with 2-bit counter	
	P-Val	Prop.	P-Val	Prop.	P-Val	Prop.	P-Val	Prop.	P-Val	Prop.
Frequency	0.739918	0.99	0.699313	1.00	0.045675	1.00	Failed	Failed	0.739918	0.99
Block Frequency	0.935716	0.99	0.987896	1.00	Failed	Failed	Failed	Failed	0.935716	0.99
*Cumulative Sums	0.437274	0.99	0.129620	1.00	0.002971	1.00	Failed	Failed	0.437274	0.99
Runs	0.419021	0.98	0.350174	0.98	Failed	Failed	Failed	Failed	0.419021	0.98
Longest Run	0.657933	1.00	0.037566	0.98	Failed	Failed	Failed	Failed	0.739918	1.00
Rank	0.924076	1.00	0.699313	0.98	0.534146	1.00	0.719747	0.99	0.924076	0.97
FFT	0.987896	0.99	0.181557	0.98	Failed	Failed	Failed	Failed	0.025193	1.00
*Nonoverlapping Temp.	0.978072	0.97	0.102526	0.99	Failed	Failed	Failed	Failed	0.350485	1.00
Overlapping Template	0.289667	1.00	0.350485	1.00	Failed	Failed	Failed	Failed	0.289667	1.00
Universal	0.236810	0.99	0.213309	0.99	Failed	Failed	Failed	Failed	0.236810	0.99
Approximate Entropy	0.224821	0.98	0.366918	0.98	Failed	Failed	Failed	Failed	0.224821	0.98
*Random Excursions	0.654467	0.97	0.242986	0.98	Failed	Failed	Failed	Failed	0.035174	1.00
*Rand Excursions Var.	0.170294	0.98	0.029796	0.97	Failed	Failed	Failed	Failed	0.128379	0.98
*Serial	0.213309	1.00	0.554420	1.00	Failed	Failed	Failed	Failed	0.213309	1.00
Linear Complexity	0.437274	1.00	0.350485	1.00	0.129620	1.00	0.224821	1.00	0.437274	1.00

* Tests with two or more sub-tests, P-val and Prop. shown here are the smaller values of two sub-tests or median values of more than two sub-tests.

Results and Discussion

- Throughput is decided by conflicting demand of the number of extracted bits per count and system clock frequency.
- The working frequency and energy/bit can be adjusted by the length of the NMOS biasing transistor in the CS inverter.



Energy efficiency and oscillation frequency of the current starved RO versus the length of the biasing NMOS transistor.

NANYANG TECHNOLOGICAL UNIVERSITY

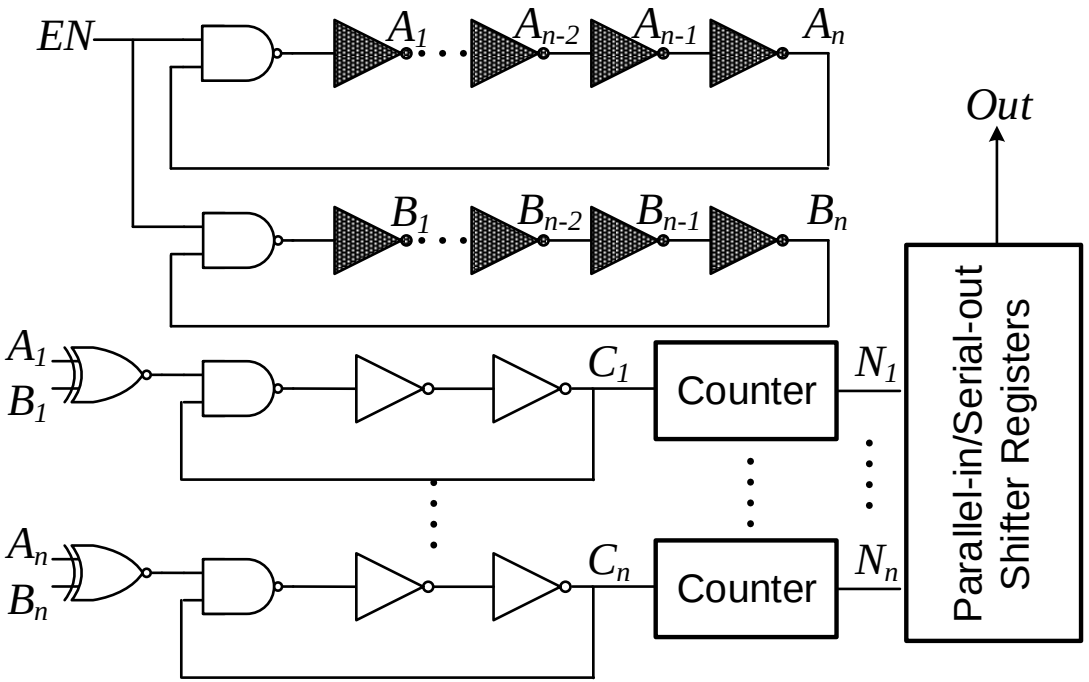
Results Comparison

	ISSCC'14	CICC'14	JSSC'12	ASSCC'14	VLSI'15	JSSC'16	This Work
Tech. (nm)	28/65	65	45	40	40	180	65
Entropy Source	Oscillator Jitter	Oscillator Jitter	Meta-stability	Meta-stability	Oscillator Jitter	Oscillator Jitter	Oscillator Jitter
Bit Rate (Mbps)	23.16/2.8	2	2400	0.5	2/0.45	0.8	**96**
Power (uW)	540/1590	130	7000	0.214	46/5	3.7	**122.9**
Efficiency (pJ/bit)	23/57	66	2.9	0.43	23/11	21	**1.28**

Can We Do Better?

The jitter in each stage of the CS RO is sampled and converted into random numbers.

- The jitter noise in each stage is uncorrelated, each RO stage will introduce a slightly different jitter.
- The random numbers from each counter will be output through a parallel-in serial-out shift register to increase the throughput.



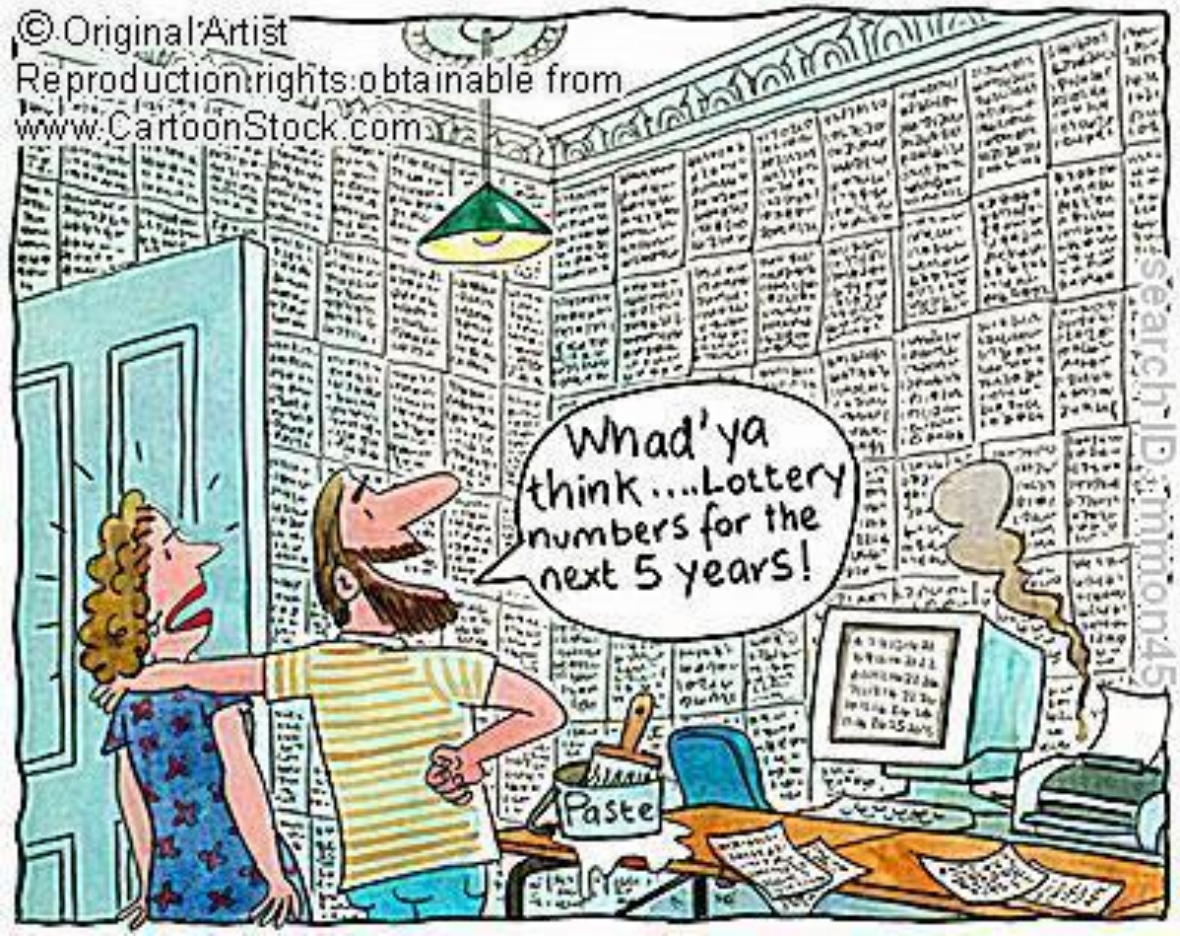
Multi-Phase Random Number Extraction Scheme

Conclusion

- A novel energy-efficient current starved RO based TRNG is proposed.
- The jitter noise is **boosted** by lowering the **oscillation frequency** and reducing the **charging and discharging currents**.
- Simulation based on a standard 65nm 1.2V CMOS technology implementation shows that the proposed TRNG can generate random bit stream at a high throughput rate of **96 Mbps** by consuming only **1.28 pJ per random bit**.

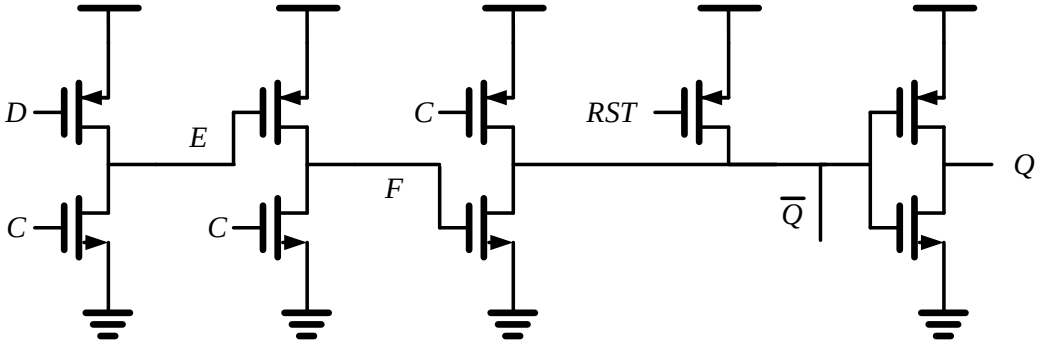
thank you!

Questions?

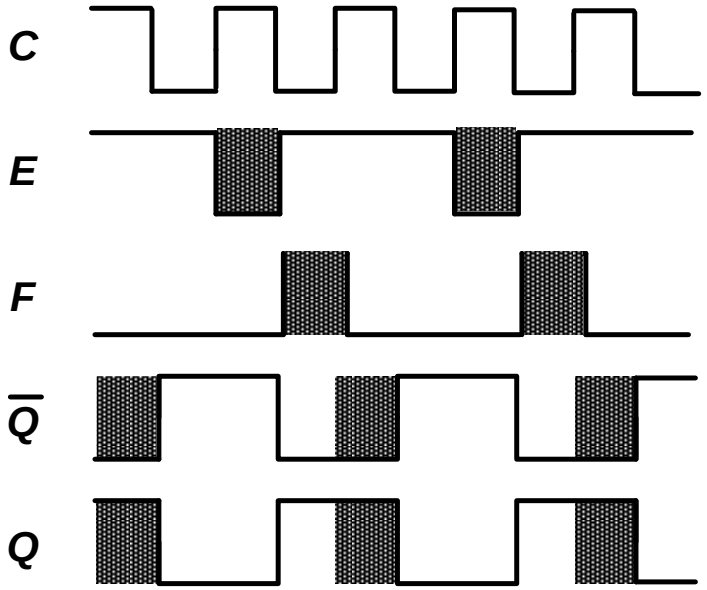


NANYANG TECHNOLOGICAL UNIVERSITY

Proposed TRNG Based on CS-ROs



The schematic of the E-TSPC DFF.



The timing diagram of the E-TSPC DFF in the asynchronous counter.

NANYANG TECHNOLOGICAL UNIVERSITY