A Bias and Correlation Free True Random Number Generator Based on Quantized Oscillator Phase under Sub-Harmonic Injection Locking

Abhishek Khanna[1*], Eslam Elmitwalli[2*], Sourav Dutta[1], Shan Deng[3], Suman Datta[1], Selçuk Köse[2], and Kai Ni[3]
[1]University of Notre Dame; [2]University of Rochester; [3]Rochester Institute of Technology, Email: kai.ni@rit.edu
*Equally contributing authors

Abstract: In this work, we demonstrated a novel oscillator phase based true random number generator (TRNG) design that can be high speed, and bias and correlation free. We are showing that: i) the arbitrary phase difference between the unsynchronized oscillator and injected synchronization signal is collapsed into two random and stable phases under sub-harmonic injection locking (SHIL); ii) the quantized oscillator phases under SHIL are fully symmetric and memoryless, generating bias and correlation free random bits; iii) the proposed oscillator phase TRNG is a generic design, independent of the oscillator platform. Thus, a CMOS ring oscillator based TRNG is also designed and evaluated. All of the generated random numbers pass the National Institute of Standards and Technology (NIST) tests and exhibit negligible bias and correlation from statistical analysis. Therefore, the proposed solution provides a competitive alternative to the existing on-chip TRNG design toolbox.

Introduction: A random number generator is an indispensable component in a range of applications, e.g., cryptography, statistical sampling, gambling, and simulations (Fig.1a). Pseudorandom RNGs based on deterministic algorithms become entirely predictable once the seed is exposed. It therefore poses great risks to apply them in applications where unpredictability is critical, such as security related functionalities in protecting privacy. A TRNG, harnessing the entropy in physical processes, e.g., noise, quantum phenomena, etc., is preferred due to the intrinsic unpredictability. We propose a novel TRNG design based on quantized oscillator phases under SHIL.

A conventional oscillator TRNG design utilizes a high jitter clock signal to sample a high frequency oscillatory data signal [1] (Fig.1b). The clock jitter leads to random sampling of high or low level of the data, hence random bits. However, jitter may not be sufficient in scaled technology nodes and significant correlation among generated bits is present. The proposed TRNG utilizes the quantized oscillator phase under 2nd SHIL (Fig.1c) [2]. A synchronization signal with frequency (f_{sync}) close to twice the free-running oscillator frequency (f_{osc}) is injected to the oscillator. The phase of locked oscillator is binarized and random, 0° or 180° (Fig.2b). This is different from the traditional 1st SHIL, where $f_{sync} \approx f_{osc}$ and the arbitrary oscillator phase before locking is collapsed into a single stable phase during locking (Fig.2a). The phase during locking can be obtained by solving the general Adler's equation [2] (Fig.2c). Therefore, this TRNG design can generate random bits on demand by turning ON or OFF the SHIL process. Since the oscillator phase is immune to process variations and the binarized phases are symmetric and memoryless, the proposed TRNG can be bias and correlation free.

TRNG Demonstration with VO_2 IMT Oscillator: The proposed TRNG is a generic design solution, independent of the oscillator platform. The vanadium oxide (VO_2) insulator metal transition (IMT) oscillator is used for demonstration in this work [3]. The *I-V* curves (Fig.3b) of a two-terminal VO_2 device, as shown in SEM image in Fig.3a, exhibit the classical hysteresis of IMT materials. The abrupt switching corresponds to the phase transition between the metallic and insulating states. When connected in series with a MOSFET drain terminal, the MOSFET loadline can be designed to intersect the unstable transition regions of VO_2 device, leading to self-sustained oscillation (Fig.4a). When injected with a synchronization signal that induces 1st SHIL (Fig.4b), the oscillator is locked with only one stable phase; while two stable phases emerge under 2nd SHIL (Fig.4c). The measured behaviors can be well reproduced by the SPICE circuit simulations. The phases collected from multiple runs show that the arbitrary phases in unsynchronized case collapse into two stable phases during locking (Fig.5a). This binarized random phase has also been used as an artificial spin, going beyond the TRNG design [4]. The generated 10,000 bits exhibit negligible bias (Fig.5b). Furthermore, the bias in random bits is simulated and found to decrease with the increase of noise in IMT threshold (V_{IMT}). With the increase in V_{IMT} noise, the oscillator frequency variation will be larger, which leads to more random oscillator states at the injection locking moment, hence smaller bias. The measured data (the V_{IMT} distribution (Fig.5c) and the random bit bias (Fig.5b)) follows the simulated trend well.

Statistical Analysis of Random Bits: Additional statistical analysis is performed on the measured random bits (Fig.5b) to evaluate their bias and correlation [5]. The bias is analyzed by the probability of '1' in various samples at different sample sizes (e.g., a sample size of 50 corresponds 200 samples for a total of 10,000 bits) and the corresponding distributions exhibit almost perfect Gaussian distributions, centered at 0.5 (Fig.6a), suggesting bias free random bits. The correlation is analyzed by evaluating the conditional probability (e.g., $P(0|0)$ represents the probability of $(i+1)^{th}$ bit is 0, given i^{th} bit is 0) distribution in various samples. Again, almost ideal Gaussian distributions centered at 0.5 indicate correlation free random bits. The correlation can be further analyzed by the conditional entropy in the random bits (Fig.6c). By increasing the sample size, the random bits exhibit close to 1 bit of information per generated bit, indicating correlation free bits. Additionally, all the generated bits pass the NIST SP 800-22 tests (Fig.6d).

CMOS Ring Oscillator TRNG: To demonstrate that the TRNG design is generic and oscillator platform independent, a CMOS ring oscillator based TRNG is demonstrated (Fig.7a). A control switch turns ON/OFF the 2nd SHIL and generates the random bits (Fig.7b). The generated random bits pass all of the NIST tests (Fig.7c-d). This indicates that our proposed design can be readily implemented in CMOS and can be high-speed.

Conclusion: We propose a novel TRNG design based on quantized oscillator phase under 2nd SHIL. Systematic measurement and simulations demonstrate the great premise of this design. As compared to other CMOS-compatible TRNGs, the proposed design can be high-speed, and bias and correlation free (Fig.6e). It therefore represents a competitive solution to on-chip TRNG for a range of applications.

References: [1] M. Bucci et al., *Trans. Computer 2003*; [2] A. Neogy, et al., *DATE* 2012; [3] A. Raychowdhury, et al., *Proceedings of IEEE* 2018; [4] S. Dutta, et al., *IEDM* 2019; [5] T. Steinle, et al., *PRX* 2017; [6] K. Yang et al., *VLSI* 2018; [7] S. Balatti, et al., *JxCDC* 2015; [8] N. Liu et al., *VLSI* 2011.

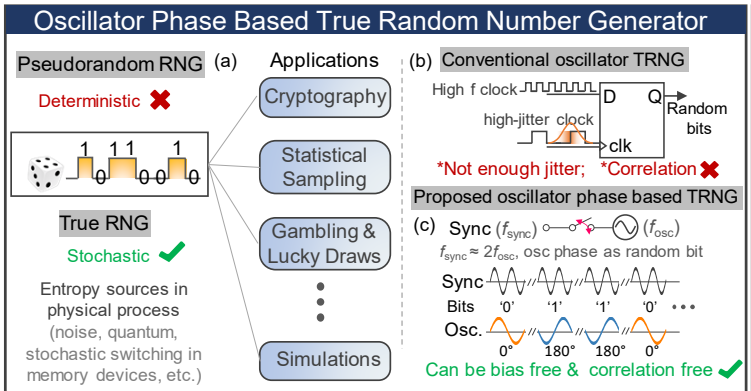

Fig.1. (a) True random number generator (TRNG) is desirable for a range of applications. (b) The conventional oscillator TRNG using jitter suffers from bit correlation. (c) A novel oscillator TRNG is thus proposed by utilizing the oscillator phase under sub-harmonic injection locking (SHIL).

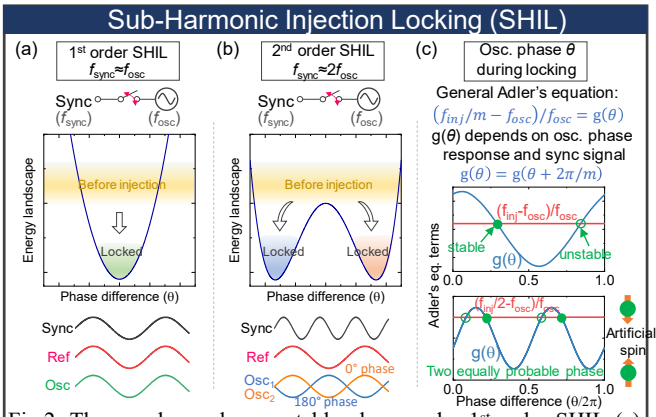

Fig.2. The osc. has only one stable phase under 1st order SHIL (a) while two stable phases under 2nd order SHIL (b). The random two stable phases under 2nd order SHIL are determined by Adler's equation (c) and have been used as artificial spin for Ising Machine.

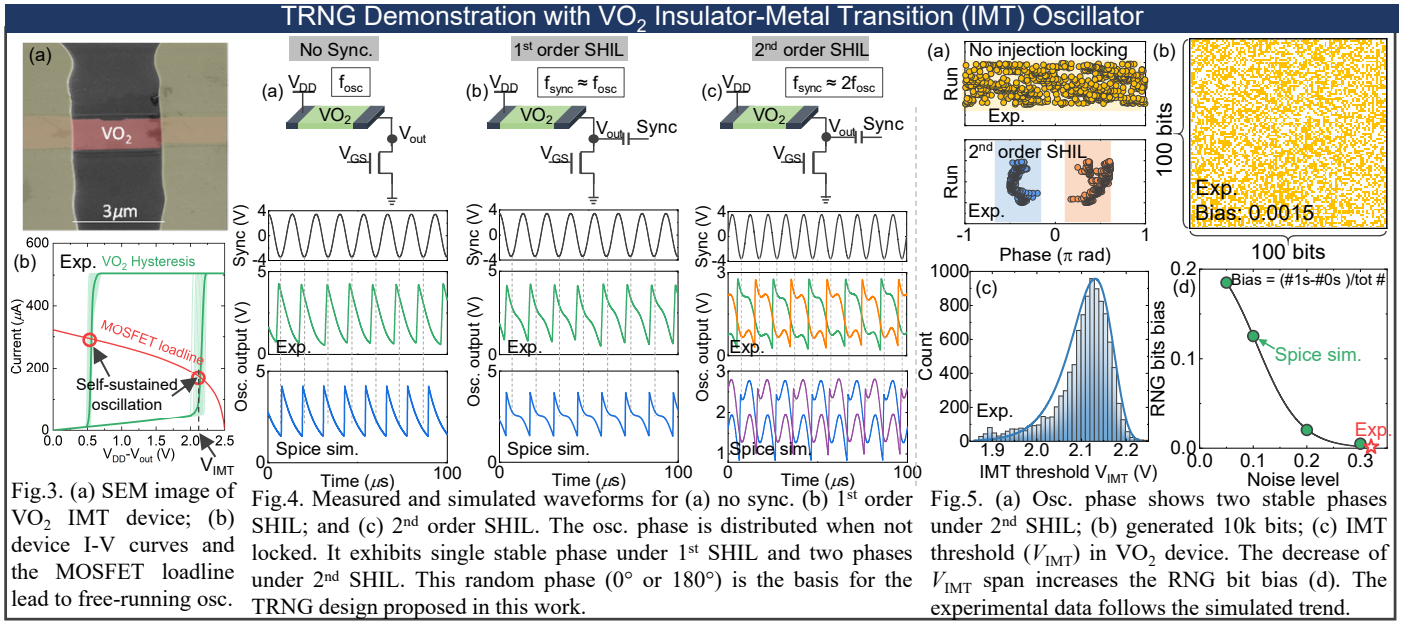

Fig.3. (a) SEM image of VO_2 IMT device; (b) device I-V curves and the MOSFET loadline lead to free-running osc.

Fig.4. Measured and simulated waveforms for (a) no sync. (b) 1st order SHIL; and (c) 2nd order SHIL. The osc. phase is distributed when not locked. It exhibits single stable phase under 1st SHIL and two phases under 2nd SHIL. This random phase (0° or 180°) is the basis for the TRNG design proposed in this work.

Fig.5. (a) Osc. phase shows two stable phases under 2nd SHIL; (b) generated 10k bits; (c) IMT threshold (V_{IMT}) in VO_2 device. The decrease of V_{IMT} span increases the RNG bit bias (d). The experimental data follows the simulated trend.

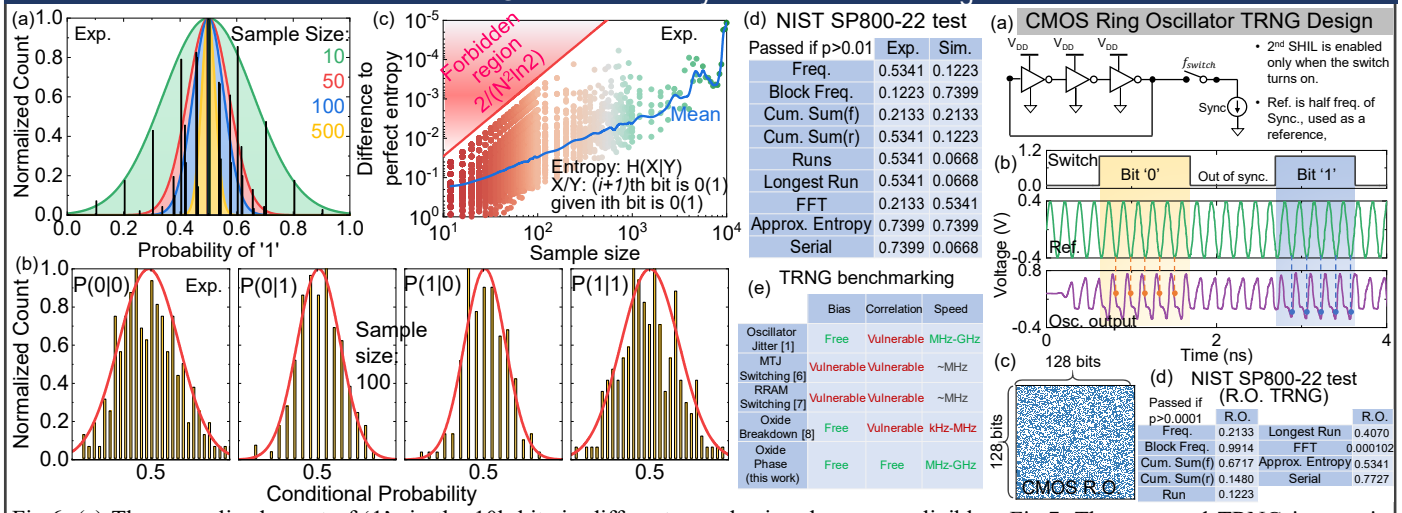

Fig.6. (a) The normalized count of '1's in the 10k bits in different sample size shows a negligible bias. (b) Negligible correlation also exists between consecutive bits. (c) Entropy analysis of the conditional entropy among consecutive bits for different sample sizes. With the increase of sample size, the random bits show close to perfect entropy (1 bit information per 1 random bit). (d) Both the measured and simulated 10k bits pass all the NIST SP800-22 test. (e) Oscillator phase based TRNG can be fast and bias and correlation free.

Fig.7. The proposed TRNG is generic to be oscillator platform independent. A CMOS ring oscillator TRNG is simulated (a-d). Osc. waveform shows random phases. The generated random bits pass all the NIST tests.