COSOI: True Random Number Generator Based on Coherent Sampling using the FD-SOI technology

Licinius Benea, Florian Pebay-Peyroula, Mikael Carmona
Univ. Grenoble Alpes, CEA, Leti,
Grenoble, France
{licinius-pompiliu.benea, florian.pebay, mikael.carmona}@cea.fr

Romain Wacquez
CEA-Leti, Mines Saint-Etienne
Gardanne, France
romain.wacquez@cea.fr

Abstract— **This work presents a proof of concept of the implementation of a Coherent Sampling Ring Oscillator TRNG (COSO-TRNG) using the Fully Depleted Silicon On Insulator (FD-SOI) technology. COSO-TRNG appears as one of the best structures optimizing the throughput per area trade-off and having a model for its entropy source. The back-biasing capability of the FD-SOI technology is proved here to be a very simple and efficient technique for the ring oscillator frequency calibration needed for the coherent sampling method. This is the first demonstration of feasibility of COSO-TRNG validated on ASIC FD22nm. A throughput of 3.36 Mbits/s was obtained, equivalent to results in the literature.**

Keywords— True random number generator, coherent sampling, phase noise, jitter, ring oscillator, Allan variance, noise models, Fully Depleted Silicon On Insulator

I. Introduction

True Random Number Generators (TRNG) are an essential brick for any cryptographic system. In contrast to PRNGs (Pseudo Random Number Generators), which use a known nonce to generate random numbers, TRNGs are based on physical phenomena. As a consequence, current standards imposed by BSI (Bundesamt für Sicherheit in der Informationstechnik) [1], NIST (National Institute of Standards and Technology) [2] and ISO (International Organization for Standardization) [3] demand a stochastic model capable of estimating the entropy of the generated bits. The model should be based on the known characteristics of the physical noise source.

For this reason, ring oscillators (RO) are a widespread choice due to their well-established models. Random number generation originates from phase noise, which represents the difference in time between the expected and the measured clock signal. The position of this variation, called jitter, translates into random values. In the literature, there is a great variety of proposed designs and their respective models: the Elementary Ring Oscillator TRNG [4], the Coherent Sampling Ring Oscillator TRNG [5], [6], the Transition Effect Ring Oscillator TRNG [7], [8], the Edge Sampling TRNG [9] and the Multi-Ring Oscillator TRNG [10], [11].

All principles considered, the Coherent Sampling Ring Oscillator (COSO) TRNG is an interesting choice due to its simplicity, low area and relatively good output [12]. Moreover, the COSO has the unique digitizing architecture that contains the total failure alarm by design. Nevertheless, its functionality is conditioned upon a perfectly controlled ratio between the frequencies of the two ring oscillators, which varies on the basis of the local mismatch inherent to all contemporary silicon technologies. This has thus so far hindered the widespread use of the COSO TRNG. In order to overcome this issue, multiple solutions were proposed. Peetermans *et al.* [13] introduced a dynamic calibration mechanism using a combination of four multiplexers (MUXs) configured statically to switch between a multitude of possible paths, in order to achieve the desired precision on the RO frequencies. Other architecture proposed by Tang *et al.* [14] uses a trimming capacitor bank, which is connected to all inverter stages of the ring oscillators. Despite their benefits, these approaches change the RO architecture for which the existing ring oscillator phase models may not apply directly.

This article proposes a new approach based on the Fully Depleted Silicon on Insulator (FD-SOI) technology specificities. This technology allows the use of a secondary transistor gate (back gate) in order to tune transistor characteristics. As such, the back gate biasing is used here in order to modify the threshold voltage of the transistors constituting the ring oscillator, and, as a consequence the ring oscillator nominal frequency without modifying the RO architecture.

The article is organised in the following way: Section 2 presents a description of the FD-SOI technology, of the working principle of COSO-TRNG and of the utilized ASIC structure. In Section 3, the results obtained on an ASIC structure are presented: inherent technology variability and its impact on the output signal of COSO-TRNG, influence on parameters as a consequence of back-gate voltage variation and the implications on entropy. Finally, conclusion and perspectives are presented in the last section.

II. Methods

This section provides an all level description of the device studied in this work, beginning with general information about the FD-SOI transistor, exposing the working principle of the COSO-TRNG and, finally, a description of the experimental setup.

A. FD-SOI technology

The FD-SOI technology is semiconductor fabrication technique that offers significant advantages over traditional bulk CMOS (Complementary Metal-Oxide-Semiconductor) processes. Its main characteristic is related to the ultra-thin insulating layer called BOX (Buried Oxide), which physically delimits the transistor channel (Fig. 1). This reduces leakage currents enhancing energy efficiency and enables very efficient electrostatic control of the channel at lower gate length. The N-Well and P-Well doped regions below the thin BOX can act a second gate with a very efficient coupling to the channel forming a very well-established and already adopted option for power management in the market of connectivity. Indeed, the back-biasing capability of FD-SOI is particularly noteworthy, as it allows for dynamic adjustment of the threshold voltage, providing a flexible trade-off between performance and power savings. Moreover, the difference between the capacitances of the front-gate and back-gate allow a precise adjustment of the transistor threshold voltage. Studies in the literature show a threshold voltage tuning capability of the order of 100 mV/V [15]. This signifies that for every 1 V applied on the back-gate, the threshold voltage of the transistor shifts 100mV.

B. COSO-TRNG

The COSO-TRNG working principle is based upon sampling one ring oscillator (RO1) with another ring oscillator (RO0), see Fig. 2 (a). When the signal from RO1 is in advance with respect to the signal of RO0, the D flip-flop generates a "1". Respectively, when the RO1 is behind RO0, the D flip-flop generates a "0" (Fig. 2 (b)). The length of the resulting signal (called "beat") is inversely proportional to the difference in periods of the two ring oscillators according to the following formula:

$$N_{mean} = \frac{T_0}{|T_1 - T_0|} \quad (1)$$

where T_0, T_1 are the average periods of RO0 and RO1, respectively.

The length of the beat signal and the variations around it represent the framework allowing the generation of bits through the LSB (Least Significant Bit) and the characterization of the noise source through, for example, the variance. The mutualisation of bit generation, total failure test and entropy source characterization on a single output variable constitute one of the key advantages of the structure.

C. Our setup

The device under test (DUT) is fabricated using the 22 nm FD-SOI technology. The results presented in this article use a structure with two ring oscillators made up of one NAND gate for the enable/disable function and 216 inverter stages amounting to a nominal frequency of 269 MHz. The physical implementation of the two ROs are fully similar and the difference in frequency is only explained by local variability of the technology. The ROs are designed with LVT transistors, with flipped well, meaning that the application of a back bias to these transistors lead to FBB (Forward Body Bias) which increases the frequencies of the ring oscillators. As the goal of the designed structure was to make a proof of concept, the back bias voltage (V_{BB}) is applied externally on the RO1 oscillator. For the sampling oscillator (RO0) the back bias voltage is set to 0 V. A counter after the D flip-flop measures the length (in periods of RO0) of the beat signal.

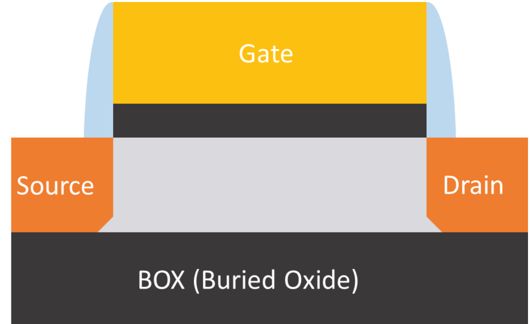


Fig. 1. Schematic representation of a FD-SOI transistor

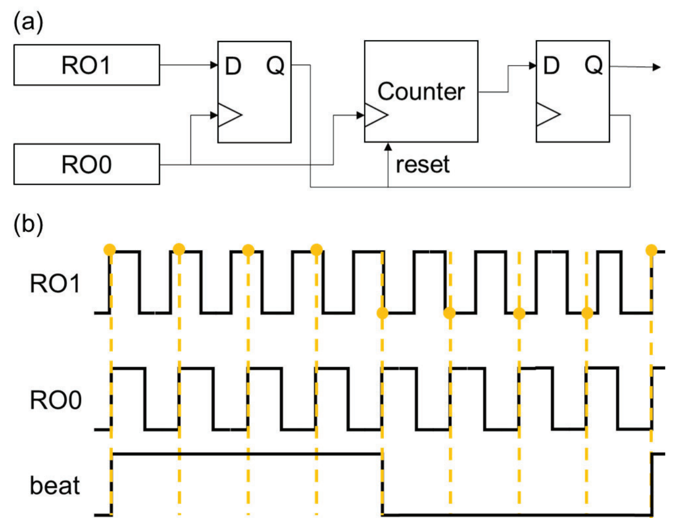


Fig. 2. Architecture of the COSO-TRNG (a) and schematic representations of the signals (b)

III. Results

In this section, we present the results and analysis of the obtained on the structure described in the previous section.

A. Inherent variability and effect on N_{mean}

By developing equation (1), the inverse for N_{mean} can be determined as:

$$\frac{1}{N_{mean}} = \left|\frac{T_1}{T_0} - 1\right| \quad (2)$$

By assuming a Gaussian distribution of T_0 and T_1 as a result of fabrication, their quotient also follows a Gaussian distribution according to [16]. Therefore, N_{mean} follows an inverse Gaussian, or Wald distribution. Fig. 3 presents the results obtained from 42 identically fabricated ring oscillator pairs on 3 separate chips. By

determining distribution parameters $\mu = 161$ and $\lambda = 170$, one can simulate a Wald distribution results using the invgauss function of the Python scipy library [17]. Results presented in Fig. 3 fit measured data. We conclude that N_{mean} follows a Wald distribution with an average value of 161 for measured devices.

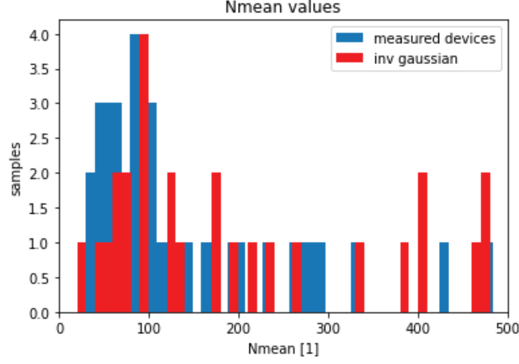


Fig. 3. Histogram of measured Nmean values on 42 devices (blue) and simlulated Wald distribution based on extracted parameters (red).

B. Counter variation against V_{BB}

Body biasing modifies the frequency of RO1, and, therefore the difference in period between RO0 and RO1. This in turn, modifies the value of N_{mean}.

The histograms corresponding to the measured counter values obtained for different V_{BB} varying from 0 V to 1.6 V are traced in Fig. 4. The mean value of the histograms increases as the frequencies of RO0 and RO1 are closer and then decreases when they come apart. Additionally, the histograms corresponding to higher N_{mean} approach more a Gaussian behaviour. This is due to a better measurement precision, which is in this case $1/N_{mean}$. The histograms are, in fact, discrete representations of jitter for different accumulation intervals corresponding to N_{mean} periods. A higher N_{mean} accounts for a better measurement precision of jitter, but also for a higher accumulation time.

For the same sample, Fig. 5 presents the variation of N_{mean} for different V_{BB}. As observed from Fig. 4, the mean counter value increases as the frequencies of the two ring oscillators are closer and decreases when their frequencies are further apart. For the presented device, the maximum value of 121.43 is reached for $V_{BB} = 0.3$V.

The average counter value gives access to the difference in frequency between RO0 and RO1 (equation 1). Assuming a nominal frequency of 269 MHz, one can determine the difference in frequency. The results are presented in Fig. 6 and show a quadratic behaviour. According to [18], the frequency of a ring oscillator is quadratically dependent on the overdrive. The latter represents the difference between the voltage applied to the transistor gate and the threshold voltage of the transistor. Assuming a linear dependency between the threshold voltage and the back-bias voltage, as shown in [15] for the range of values used in this case, the frequency of RO1, and thus the difference in frequency between RO1 and RO0 should vary quadratically depending on V_{BB}. The quadratic fit of the measured values presented in Fig. 6 proved the validity of this assumption. More importantly, we observe that for a large spectrum of low V_{BB} values (inferior to 0.8V), there is a very low variation of the difference in frequency, enabling a fine tuning so that the frequencies of the two ring oscillators are as close as needed.

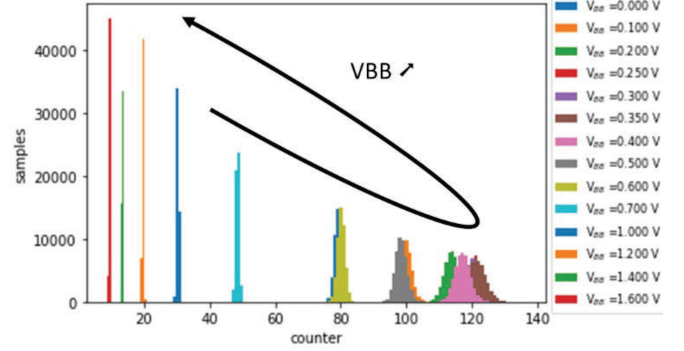


Fig. 4. Histogram of counter values mesured for different V_{BB}

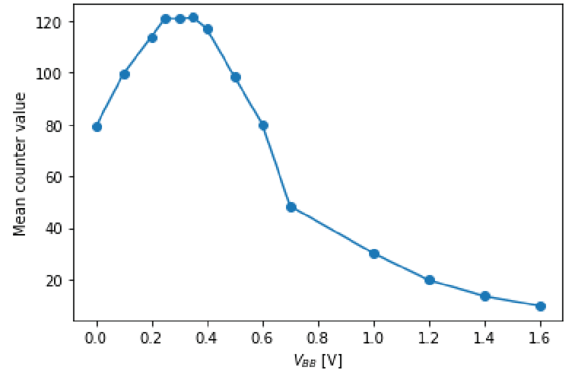
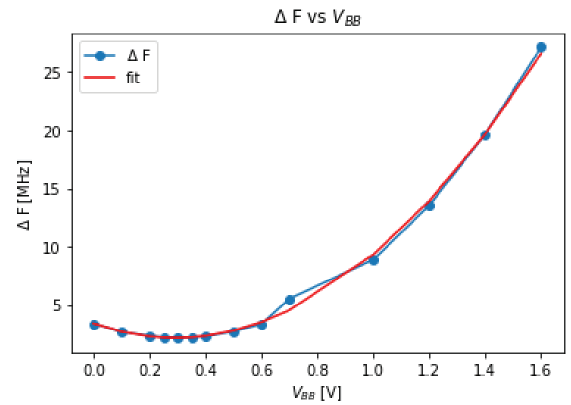


Fig. 5. Variation of N_{mean} in function of V_{BB}



a.

Fig. 6. Calculated difference in frequency $\Delta F = |F_{RO1} - F_{RO0}|$ calculated for different V_{BB}

C. Variance of counter values

The variance of jitter is the property which directly determines the entropy of the TRNG [4]. The variations of counter values are a discrete representation of jitter sampled with a precision of 1 bit. The physical origins of jitter are thermal noise and flicker noise [18]. Thermal noise is completely random and uncorrelated which makes it an ideal source for TRNG applications. On the other hand, flicker noise originates from two major phenomena [19]: carrier number fluctuation due to presence of traps at the interface between the gate oxide and silicon, and mobility fluctuation due to Coulomb scattering. This type of jitter introduces correlations in the bit series extracted from jitter and can decrease the quality of randomness. The variance of the accumulated jitter varies linearly in the case of thermal noise jitter (predominant for low accumulation times) and quadratically for flicker noise jitter (predominant for higher accumulation times) [18]. Depending on the number of accumulation periods N, the variance of jitter follows a quadratic law:

$$\sigma_N^2 = a_0 + a_1 \cdot N + a_2 \cdot N^2 \quad (3)$$

Where a_0, a_1, a_2 are the corresponding coefficients attributed to jitter resulting from quantization, thermal and flicker noise, respectively.

The variance of counter values for different mean counter values (obtained by varying V_{BB}) is traced in Fig. 7. The latter accounts here for the number of accumulated periods. The curve begins with a plateau with values close to 1/12, which corresponds to the quantization noise measured with a precision of 1 bit [20]. The curve has a quadratic behaviour, as expected theoretically.

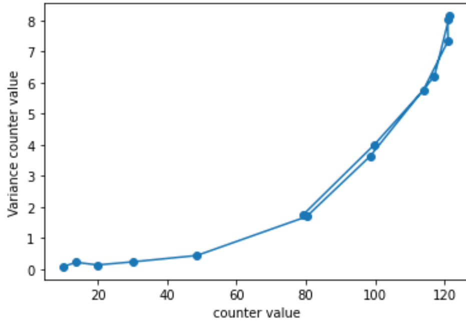


Fig. 7. Variance of counter values for different mean counter values.

In order to further investigate the amplitude of the measured thermal and flicker contributions to jitter, variance was also traced for counter values corresponding to all V_{BB} values (Fig. 8). This time, the accumulation periods are multiples of N_{mean}. Moreover, in this case, the Allan variance [21] was used a proposed in [22], [23]. The curves in a log-log scale show a quadratic behaviour, with slopes equal to 1 for low accumulation times, accounting for the thermal dominant region, and with a slope equal to 2 for higher accumulation times, highlighting the effect of flicker noise. However, the calculated values of Allan variance are higher for curves corresponding to higher N_{mean}. This effect can be observed for equivalent accumulation times, where, in some cases, even an order of magnitude of difference can be seen. Moreover, the curves corresponding to low N_{mean} values present a predominantly linear behaviour, whereas the curves corresponding to high N_{mean} values show a quadratic behaviour. An analysis of the correct noise amplitudes will be carried out in the followings.

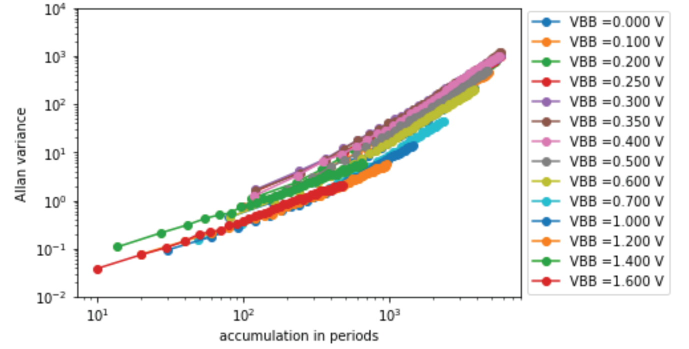


Fig. 8. Allan variance vs. accumulation times corresponding to multiples of N_{mean} for V_{BB} varying from 0V to 1.6V

The amplitudes of the corresponding thermal and flicker contributions to jitter can be determined by fitting the variance curves and extracting the a_1, a_2 coefficients, which correspond to thermal and flicker noise amplitudes, respectively. As the accumulation times cover multiple orders of magnitude, a normalized regression method is needed. A classical method would grant disproportionately higher weights to larger values. The Least-Squares Normalized Error (LSNE) method was used for its simplicity and effectiveness [24].

The obtained coefficients determined from the curves in Fig. 8 are represented in Fig. 9 and Fig. 10 for flicker and thermal noise respectively. One can observe that in both cases, there is an increase in coefficient values, which is correlated with the increase in Nmean, especially for V_{BB} values where Nmean is greater than 100 (V_{BB} between 0.2V and 0.4V). For a_1, we consider those values as an overestimation due to the fact that the curves are essentially in a quadratic domain. Also, the values corresponding to V_{BB} greater than 1.2V also present higher values, which may be attributed to an overestimation of thermal noise due to a poor measurement precision (high quantization noise) as observed in [25]. Consequently, the thermal noise amplitude coefficient can be determined by averaging the obtained coefficients, excluding the values from the ranges mentioned in previous paragraphs. The obtained value of a_1 is $2.73 \cdot 10^{-3}$.

D. Entropy and output

Due to intrinsic correlated behaviour of flicker noise, only the thermal component of jitter is used as a legitimate entropy source.

The COSO-TRNG model presented in [13] makes the assumption that the distribution of counter values is Gaussian, without making any distinction about the origin of the accumulated jitter. The min-entropy is determined as:

$$H_\infty = -\log_2\big(max(p_0, p_1)\big) \quad (4)$$

Where p_0, p_1 are the probabilities that the counter value is even or odd, respectively. i.e. the LSB of the counter value is 0 or 1, respectively.

A model which takes into consideration only the thermal contribution of jitter in order to determine a minimum bound for entropy is presented in [4]. The equation describing the entropy is:

$$H_{min} = 1 - \frac{4}{\pi^2 \ln 2} \cdot exp\left(-4 \cdot \pi^2 \cdot \left(\frac{\sigma_T{}^2 \cdot N}{T_1{}^2}\right) \cdot \frac{T_0}{T_1}\right) \quad (5)$$

Where σ_T is the thermal jitter, T_0, T_1 the periods of the sampling and sampled RO, respectively and N the accumulation time in periods of RO0.

This model is conceived for the Elementary RO TRNG, but the formula can be adapted to the COSO-TRNG by replacing equivalent terms:

$$H_{min} = 1 - \frac{4}{\pi^2 \ln 2} \cdot exp\left(-4 \cdot \pi^2 \cdot a_1 \cdot N \cdot \frac{N_{mean}+1}{N_{mean}}\right) \quad (5)$$

Where $a_1 \cdot N = \frac{\sigma_T{}^2 \cdot N}{T_1{}^2}$ is the normalized variance of jitter coming from thermal noise and $\frac{N_{mean}+1}{N_{mean}} = \frac{T_0}{T_1}$ is the adjustment coefficient equivalent to the ratio of the periods of the two ring oscillators.

The obtained results for the min-entropy estimation are presented in Fig. 11. While the results obtained from [13] are discrete, as they are obtained from counter values, the model in [4] allows obtaining a continuous function based on the value a_1 determined in the previous section. In order to obtain an entropy greater than 0.9998, the minimal accumulation times in periods of RO0 are N > 80 for [13] and N > 74 for [4]. In order to accommodate both conditions and considering the frequency of RO0 at 269 MHz, the calculated output of the TRNG is 3.63MHz. This is equivalent to results obtained in the literature [12], [13].

E. Discussion about noise composition

The point of equivalence between thermal and flicker noise contributions (N_C) can be determined by calculating the ratio a_1/a_2. The obtained values for different V_{BB} are presented in Fig. 12. The results prove that thermal domain is limited to accumulation times lower than N = 100 periods of RO0. This may explain the cause of the greater values of variance observed for N_{mean} greater than 100.

By using the coefficients for the worst case at V_{BB} = 0.2V, the thermal noise and flicker noise composition is traced in Fig. 13. One can observe that even for low accumulation times, flicker noise plays an important part in the mix. For example, a combination of 10% flicker and 90% thermal is already reached at N=11 periods. This might be enhanced by the use of the advanced 22nm FD-SOI technology. This shows that for newer technological nodes, flicker noise represents a major part of the mixture and its influence on entropy estimation needs to be understood [26].

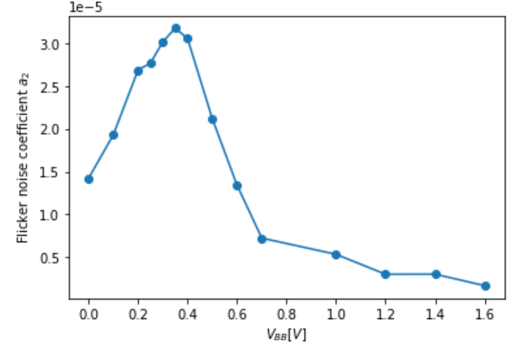


Fig. 9. Flicker noise coefficient for different V_{BB} values

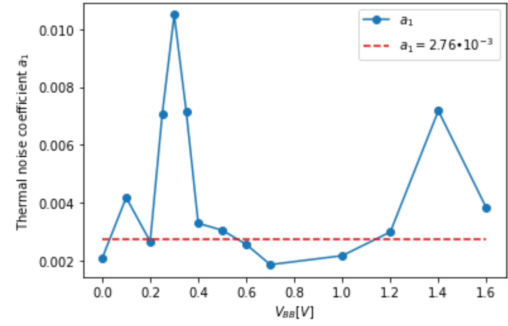


Fig. 10. Thermal noise coefficient for different V_{BB} values

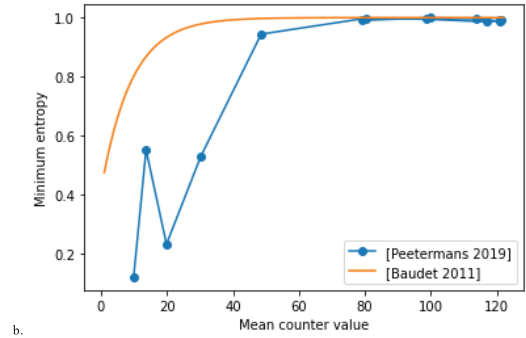


Fig. 11. Measured minimum entropy estimation of our TRNG according to [13] and [4]

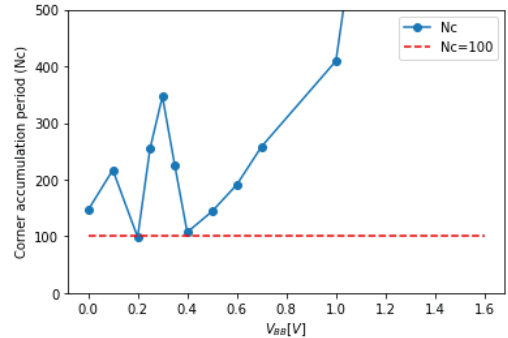


Fig. 12. Accumulation time in periods of RO0 (N_C) at thermal-flicker equivalence.

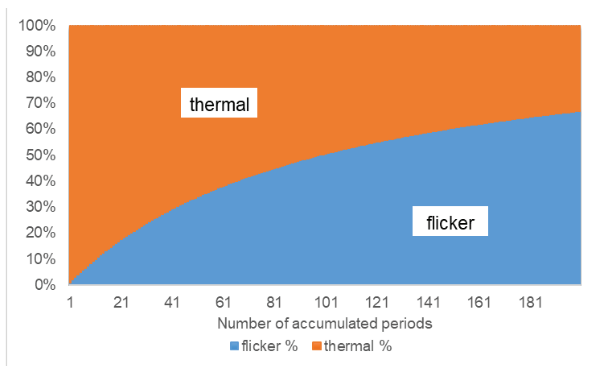


Fig. 13. Noise composition for $V_{BB} = 0.2V$

IV. Conclusions

This work presents a proof of concept of the implementation of a COSO-TRNG using the FD-SOI technology. The back-biasing technique, specific to this technology, proved to be well suited for the ring oscillator frequency calibration needed for the coherent sampling method.

The isolation of thermal noise needed to determine the entropy proved to be a complex issue. A deep analysis needs to be done by varying different parameters to obtain the correct estimation. By applying two distinct models, a throughput of 3.36 Mbits/s was obtained, equivalent to results in the literature.

Further work need to be realized on the study of the different noise sources present in the architecture, optimisation of the design, improvement of the figures of merit and on the statistical tests adapted to the COSO-TRNG.

References

[1] M. Peter and W. Schindler, 'A Proposal for Functionality Classes for Random Number Generators', *02.06.2023*, [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Certification/Interpretations/AIS_31_Functionality_classes_for_random_number_generators_e_2023.html?nn=910324

[2] M. S. Turan, E. Barker, J. Kelsey, K. A. McKay, M. L. Baish, and M. Boyle, 'Recommendation for the entropy sources used for random bit generation', National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-90b, Jan. 2018. doi: 10.6028/NIST.SP.800-90B.

[3] 'ISO/IEC JTC 1/SC 27. Test and analysis methods for random bit generators 541 within ISO/IEC 19790 and ISO/IEC 15408', ISO. [Online]. Available: https://www.iso.org/standard/68296.html

[4] M. Baudet, D. Lubicz, J. Micolod, and A. Tassiaux, 'On the Security of Oscillator-Based Random Number Generators', *J Cryptol*, vol. 24, no. 2, pp. 398–425, Apr. 2011, doi: 10.1007/s00145-010-9089-3.

[5] P. Kohlbrenner and K. Gaj, 'An embedded true random number generator for FPGAs', in *Proceeding of the 2004 ACM/SIGDA 12th international symposium on Field programmable gate arrays - FPGA '04*, Monterey, California, USA: ACM Press, 2004, p. 71. doi: 10.1145/968280.968292.

[6] F. Bernard, V. Fischer, and B. Valtchanov, 'Mathematical model of physical RNGs based on coherent sampling', *Tatra Mountains Mathematical Publications*, vol. 45, no. 1, pp. 1–14, Dec. 2010, doi: 10.2478/v10127-010-0001-1.

[7] M. Varchola and M. Drutarovsky, 'New High Entropy Element for FPGA Based True Random Number Generators', in *Cryptographic Hardware and Embedded Systems, CHES 2010*, vol. 6225, S. Mangard and F.-X. Standaert, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 351–365. doi: 10.1007/978-3-642-15031-9_24.

[8] P. Haddad, V. Fischer, F. Bernard, and J. Nicolai, 'A Physical Approach for Stochastic Modeling of TERO-Based TRNG', in *Cryptographic Hardware and Embedded Systems -- CHES 2015*, vol. 9293, T. Güneysu and H. Handschuh, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2015, pp. 357–372. doi: 10.1007/978-3-662-48324-4_18.

[9] B. Yang, V. Rožic, M. Grujic, N. Mentens, and I. Verbauwhede, 'ES-TRNG: A High-throughput, Low-area True Random Number Generator based on Edge Sampling', *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 267–292, Aug. 2018, doi: 10.13154/tches.v2018.i3.267-292.

[10] B. Sunar, W. Martin, and D. Stinson, 'A Provably Secure True Random Number Generator with Built-In Tolerance to Active Attacks', *IEEE Trans. Comput.*, vol. 56, no. 1, pp. 109–119, Jan. 2007, doi: 10.1109/TC.2007.250627.

[11] D. Lubicz and V. Fischer, 'Entropy Computation for Oscillator-based Physical Random Number Generators', *J Cryptol*, vol. 37, no. 2, p. 13, Feb. 2024, doi: 10.1007/s00145-024-09494-6.

[12] O. Petura, U. Mureddu, N. Bochard, V. Fischer, and L. Bossuet, 'A survey of AIS-20/31 compliant TRNG cores suitable for FPGA devices', in *2016 26th International Conference on Field Programmable Logic and Applications (FPL)*, Lausanne, Switzerland: IEEE, Aug. 2016, pp. 1–10. doi: 10.1109/FPL.2016.7577379.

[13] A. Peetermans, V. Rozic, and I. Verbauwhede, 'A Highly-Portable True Random Number Generator Based on Coherent Sampling', in *2019 29th International Conference on Field Programmable Logic and Applications (FPL)*, Barcelona, Spain: IEEE, Sep. 2019, pp. 218–224. doi: 10.1109/FPL.2019.00041.

[14] Q. Tang, B. Kim, Y. Lao, K. K. Parhi, and C. H. Kim, 'True Random Number Generator circuits based on single- and multi-phase beat frequency detection', in *Proceedings of the IEEE 2014 Custom Integrated Circuits Conference*, San Jose, CA, USA: IEEE, Sep. 2014, pp. 1–4. doi: 10.1109/CICC.2014.6946136.

[15] C. Navarro, M. Bawedin, F. Andrieu, B. Sagnes, F. Martinez, and S. Cristoloveanu, 'Supercoupling effect in short-channel ultrathin fully depleted silicon-on-insulator transistors', *Journal of Applied Physics*, vol. 118, no. 18, p. 184504, Nov. 2015, doi: 10.1063/1.4935453.

[16] J. M. Hernández-Lobato, 'Balancing Flexibility and Robustness in Machine Learning: Semi-parametric Methods and Sparse Linear Models'.

[17] 'SciPy -'. [Online]. Available: https://scipy.org/

[18] A. Hajimiri, S. Limotyrakis, and T. H. Lee, 'Jitter and phase noise in ring oscillators', *IEEE J. Solid-State Circuits*, vol. 34, no. 6, pp. 790–804, Jun. 1999, doi: 10.1109/4.766813.

[19] G. Ghibaudo, O. Roux, Ch. Nguyen-Duc, F. Balestra, and J. Brini, 'Improved Analysis of Low Frequency Noise in Field-Effect MOS Transistors', *physica status solidi (a)*, vol. 124, no. 2, pp. 571–581, 1991, doi: 10.1002/pssa.2211240225.

[20] W. R. Bennett, 'Spectra of Quantized Signals', *Bell System Technical Journal*, vol. 27, no. 3, pp. 446–472, Jul. 1948, doi: 10.1002/j.1538-7305.1948.tb01340.x.

[21] D. W. Allan, 'Statistics of atomic frequency standards', *Proc. IEEE*, vol. 54, no. 2, pp. 221–230, 1966, doi: 10.1109/PROC.1966.4634.

[22] P. Haddad, Y. Teglia, F. Bernard, and V. Fischer, 'On the assumption of mutual independence of jitter realizations in P-TRNG stochastic models', in *Design, Automation & Test in Europe Conference & Exhibition (DATE), 2014*, Dresden, Germany: IEEE Conference Publications, 2014, pp. 1–6. doi: 10.7873/DATE.2014.052.

[23] E. Noumon Allini, M. Skórski, O. Petura, F. Bernard, M. Laban, and V. Fischer, 'Evaluation and Monitoring of Free Running Oscillators Serving as Source of Randomness', *IACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. Volume 2018, pp. 214-242 Pages, Aug. 2018, doi: 10.13154/TCHES.V2018.I3.214-242.

[24] B. E. Grantham and M. A. Bailey, 'A Least-Squares Normalized Error Regression Algorithm with Application to the Allan Variance Noise Analysis Method', in *2006 IEEE/ION Position, Location, And Navigation Symposium*, Coronado, CA: IEEE, 2006, pp. 750–756. doi: 10.1109/PLANS.2006.1650671.

[25] L. Benea, M. Carmona, F. Pebay-Peyroula, and R. Wacquez, 'On the Characterization of Jitter in Ring Oscillators using Allan variance for True Random Number Generator Applications', in *2022 25th Euromicro Conference on Digital System Design (DSD)*, Maspalomas, Spain: IEEE, Aug. 2022, pp. 534–538. doi: 10.1109/DSD57027.2022.00077.

[26] L. Benea, M. Carmona, V. Fischer, F. Pebay-Peyroula, and R. Wacquez, 'Impact of the Flicker Noise on the Ring Oscillator-based TRNGs', *IACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 2024, no. 2, Art. no. 2, Mar. 2024, doi: 10.46586/tches.v2024.i2.870-889.