An Offset-compensated Oscillator-based Random Bit Source for Security Applications

Holger Bock, Marco Bucci, and Raimondo Luzzi

Infineon Technologies Austria AG
Babenbergerstrasse 10, A-8020 Graz (AUSTRIA)
{holger.bock, bucci.external, raimondo.luzzi}@infineon.com

Abstract. In this paper, a new, patent pending, architecture for a jitter-based random bit source which is cost-effective and suitable for applications in cryptography, is presented. The source is designed to be robust against parameter variations and attacks aimed to force its output. It also features an auto-test which allows to detect faults and to estimate the source entropy. The proposed design is an enhancement of the oscillator-based architecture where a compensation loop is added to maximize the statistical quality of the output sequence, especially in presence of low-jittered oscillators. As a consequence, a fully-digital implementation, without any amplified noise source, can be adopted for the proposed generator. From an analysis of the known techniques for random number generation, the proposed architecture is derived and implementation details are also reported.

Keywords: Random bit source, random numbers, ring oscillators, jitter, entropy.

1 Introduction

A random bit generator (RBG) is a system whose output consists of fully unpredictable (i.e. statistically independent and unbiased) bits. In security applications, the unpredictability of the output also implies that it must not be possible for any attacker to observe and manipulate the generator.

An RBG basically differs from a pseudo-random generator because the complete knowledge of the generator structure and of whatever previously generated sequence does not result in any knowledge of any following bit. In other terms, the entropy of an n-bit output sequence should be ideally equal to n. On the contrary, the entropy of a n-bit output sequence from a pseudo-random generator cannot exceed the entropy of its seed, whatever n is. While pseudo-random generators are suitable in those applications where just a flat statistic is needed [1], random number generators are required in security applications, where unpredictability is a requirement.

A true random bit generator has necessarily to be based on some kind of nondeterministic phenomena that could act as the source of the system randomness.

Electronic noises and time jitter are usually the only stochastic phenomena that are suitable in integrated implementations.

When designing an RBG for a chipcard IC, a wide spectrum of implementation issues has to be considered and fulfilled. Due to cost reasons and mechanical stress requirements, the silicon area is a limited resource in chipcard microcontrollers (a typical area is $5-10mm^2$ for a 8/16-bit card) and, at the same time, there is the demand to integrate non-volatile memory blocks of ever-increasing size. As a consequence, the silicon area for integrating the CPU core and its peripheral devices (including the RBG macro-cell) has to be minimized. Furthermore, no external components can be used due to packaging constraints and security reasons: any externally accessible circuit node seriously affects the chip tamper resistance [2].

To avoid complex power management policies, power consumption is another stringent constraint, especially in a chipcard IC which is designed to be used also in hand-held equipment such as mobile phones. A related issue is the chip resistance to power analysis attacks [3]: for example, when the RBG is employed in a key generation process, a current consumption waveform highly correlated to the RBG's output bit stream can be exploited by an attacker to infer the generated secret values.

Few noise-based RBG's are reported in the technical literature due to the classified nature of most researches in this field; however, four different techniques for generating random streams are widely exploited: direct amplification of a noise source [4–6], jittered oscillator sampling [7–10], discrete-time chaotic maps [11, 12] and metastable circuits [13, 14].

Hardware RBG's can feature a very high throughput, but the random sources commonly used present several statistic defects, due to physical limitations (bandwidth limitation, fabrication tolerances, aging and temperature drifts), implementation issues, deterministic disturbances, and external attacks aimed at manipulation. Substrate and power supply interference are a major concern since their power levels can be higher than the random noise level if proper design techniques are not employed. To address this problem and since different techniques feature different advantages, in [15], a truly RBG which adopts a mixing of three mentioned RBG methods is presented. A source quite resistant to deterministic disturbances is achieved even if, due to the mixing of different techniques, it is difficult to perform a rigorous statistical analysis of the system.

As a more effective solution, the post-processing of the raw bit stream from the source with a carefully designed compressing algorithm can be employed. A lower speed bit stream with increased statistical quality is generated from a high speed near-random input stream by 'distilling' its entropy. In [16], an adaptative decorrelating algorithm is reported which dynamically modifies its compression ratio according to the statistical properties of the input sequence and can reveal failures and external attacks.

This paper presents a new architecture for a jitter-based random source which is an enhancement of a standard oscillator-based generator where a feedback compensation is added in order to maximize the statistical quality of the output sequence, especially in presence of low jittered oscillators. At the same time, the proposed generator is not affected by the frequency beating between the sampled and sampling oscillator which, enhancing the pseudo-random behavior of the sequence, makes difficult detecting a lack of randomness condition. As a further advantage, the presented RBG is suitable to be implemented as a fully-digital standard-cell based circuit, with a substantial reduction in terms of design time, power and area requirements with respect to other designs where a significant analog part is present.

In Section 2, a comparison between an amplification-based and an oscillator-based RBG is carried out which allows to establish an equivalence between the two techniques and leads to the definition of the new architecture proposed in this paper as an optimal solution for an integrated noise-based RBG. Circuit details for a standard-cell implementation of the presented architecture are reported in Section 3.

2 Random bit source design

A raw random bit source is a system that generates a sequence X by sampling and quantizing an analog non-deterministic value S. Two quantization modes represent the most common cases: a *sign*-mode and a $mod\,2$-mode. The quality of the output sequence X and the robustness of the random bit source depend on both the quality of the source S and the quantization procedure.

A simple model for the source S can help to clarify the effect of some parameters and issues that are typical in the implementation of a random bit source. The source S is modeled as the sum of a random component $a \cdot R$, its mean value m and a deterministic signal D:

$$S = a \cdot R + m + D \tag{1}$$

where, the factor a represents the intrinsic amplitude of the noise source and a possible amplification, being the actual random source modeled by R as a normalized random process. Of course, due to the physical limitations of the source, R is a bandwidth limited process. As a consequence, the output bits $x[i]$ will show some correlation depending of the sampling rate and their reciprocal position. The mean value m represents the mutual offset error that typically exists between the source and the quantization device. In this model it is modeled by a constant but, actually, it can slowly drift depending on environmental conditions. Finally, the signal D takes into account for every deterministic signal that is superimposed on the random process R. It can consist of disturbances from the surrounding environment, from other components of the device in which the generator is embedded or from an attacker aimed to force the source. In the last case, the amplitude of D could be even greater than the random contribution $a \cdot R$.

The operation of the $sign$ and the $mod\,2$ quantization modes on a source S are depicted in Figure 1. In this example, R is a normalized Gaussian distribution, $a = 0.5$ and $\frac{m+d[i]}{a} = 0.6$. The x-axis is normalized to a and is divided in 0 and 1 zones to show how the source distribution P_S is partitioned between 0 and 1 samples. The $mod\,2$ quantization results in alternated 0 and 1 bands as shown in Figure 1(b). Of course, in actual implementations, these bands could be asymmetric and this issue must be taken into account as a possible cause of offset on the sequence X.

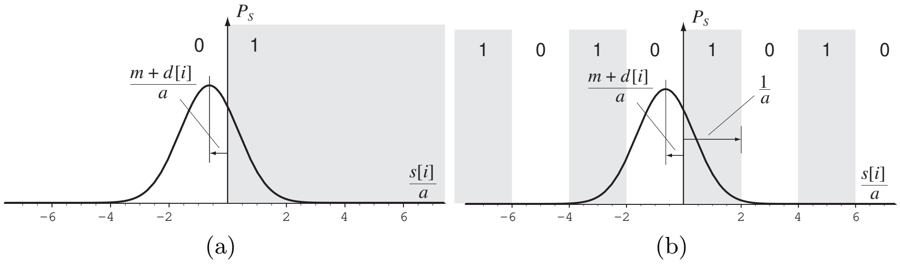


Fig. 1. Source quantization modes: (a) sign-mode ($x[i] = sign(s)$), (b) mod 2-mode ($x[i] = \lfloor s \rfloor \, mod\, 2$).

From Figure 1 it follows that, the quantity $\frac{m+d[i]}{a}$ acts as an instantaneous offset which is superimposed on the distribution of the process R. In principle, in order to reduce this offset, it is possible to reduce $m + d[i]$ as well as to increase a. Unfortunately, in practice, increasing the noise amplification, the factor a increases, but m and D increase too. As a general rule, increasing the noise amplification also results in a reduction of the process R bandwidth, due to the fact that, for a generic amplifying circuit, the gain-bandwidth product is roughly constant.

The comparison between Figure 1(a) and 1(b) makes also evident some relevant advantages of the $mod\,2$ quantization. In particular, while the $sign$ quantization can be saturated, the $mod\,2$ mode is not affected by that. As an important consequence, as long as a is large enough, an attacker cannot control the source by injecting a properly chosen D signal. Furthermore, the effective offset error cannot be greater that the distance to the bound of the next quantization band (i.e. half of the band width). This means that the factor a can be increased without taking care of the resulting increasing of m and D. In practice, a can be increased without the need to implement a wide range offset compensation or even without any offset compensation at all. Basically, the $mod\,2$ quantization limits the effect of m and D, making it negligible in case a is large enough. This results in a more robust design both with respect to electrical variances and possible attacks.

As to the entropy source S, in integrated implementations, it usually consists on some kind of electronic or phase noise. Basically, the primary sources are electronic noise contributions, since phase noise is a consequence of electronic noise. Among electronic noise sources, both the thermal noise in a resistor and the pn-junction shot noise offer the advantage of being white noises with a Gaussian distribution whose intensity depends on physical quantities easy to keep under control. This make possible the implementation of sources characterized by a simple statistical model instead of an empirical and technological-dependent one.

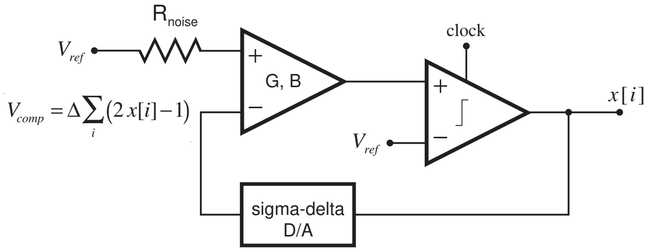


Fig. 2. Amplification-based RBG.

Figures 2, 3 and 4 show three very common solutions for the implementation of a raw random bit source. The scheme depicted in Figure 2 is perhaps the straightest solution: an explicit thermal noise source is amplified and then quantized and sampled. The noise source consists of the resistor R_{noise}, the clocked comparator performs the sampling and the quantization of the amplified noise and the sigma-delta D/A converter compensates the offset due to the amplifier and the comparator. This kind of source can have a very high throughput. In practice, the only limitation is due to the bandwidth B of the noise amplifier since, as the sampling frequency increases, so does the correlation among samples. An interesting feature of this source is that, as long as the noise source is not disturbed by an interfering signal, most of the possible faults can be revealed by simply counting the transitions in the output sequence X. Basically, this is due to the fact that each bit generation restarts from the same state. As a consequence, a lack of entropy is expected to result in a lack of transitions in the generated sequence. Actually, the offset compensation, the status of the clocked comparator and the bandwidth limitation of the noise amplifier make the source not completely "stateless". Nevertheless, the source is "by construction" not capable to deceive even a simple transition test. As a result, this source can be easily tested in real time against faults.

Notice that the offset compensation is a critical issue in this design. A lower precision in the offset zeroing results in the need of a higher noise amplification. On the other hand, a higher noise amplification results in a higher offset on the comparator input and, moreover, in a reduction of the amplifier bandwidth. Definitely, since the noise source has a very low amplitude, the offset compensation must feature both a high dynamic and a high precision.

The accuracy of the offset compensation also impacts the output bias since every error generated in the feedback loop will result in a bias error on X. In principle, the feedback loop could be implemented by a sigma-delta D/A converter as well as by an integrator. Nevertheless, if an integrator is used, errors can arise due to the offset of the integrator and its reference voltage as well as to any possible asymmetry in the waveform of the X signal. On the contrary, the sigma-delta DAC feedbacks X as a digital signal, independently of its analog features (i.e. its waveform). In this latter case, the feedback loop balances the system in such a way that, in the steady state, it holds:

$$P\{x[i] = 0\}/P\{x[i] = 1\} = \Delta_{-}/\Delta_{+} \quad (2)$$

where Δ_{-} and $\Delta_{+}$are the amplitudes of the down and up steps of the sigma-delta DAC.

Due to the low level of the noise source, this circuit is also sensitive to internal or external interfering signals. Since the $sign$-mode is used, an interfering signal D could actually force the source. On the whole, this design can implement a good quality source but an accurate design is required and its robustness against attacks is low.

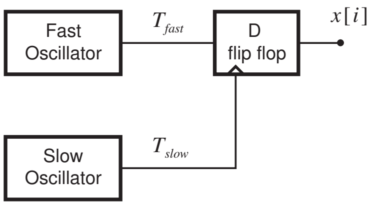


Fig. 3. Oscillator-based RBG.

Sources based on jittered oscillators have, in general, a simpler and more robust implementation. In Figure 3 a basic scheme is depicted: a slow oscillator T_{slow} samples a fast oscillator T_{fast}. The D flip-flop performs the $mod\,2$ sampling of the phase difference between the two oscillators. Width and symmetry of the quantization bands depend on the frequency and duty cycle of the fast oscillator.

This scheme has an intrinsic periodic behavior due to the phase shifting, i.e. the beating, that always occurs if T_{slow}/T_{fast} is not an integer. In Figure 1(b), this beating can be seen as a deterministic component D that produces a continuous drift between the S distribution and the quantization bands. Of course, since the $mod\,2$ quantization is used, this beating effect is negligible if the phase noise is large with respect to half the period of the fast oscillator. More in general, the $mod\,2$ quantization makes this design robust against any kind of phase signals that could be superimposed on the phase noise.

The achievable throughput depends on the fast oscillator frequency and on the mutual phase noise between the two oscillators. In facts, once the fast oscillator frequency is maximized (i.e. the quantization bands are as narrow as possible), the sampling period T_{slow} must be long enough in order to accumulate a sufficient jitter between two subsequent samples. Notice that in this scheme there is not an explicit noise source. The oscillators can be implemented in different ways and, in general, the statistical model is not known a priori, being determined by several technological and implementation factors. Anyhow, if a better noise characterization is requested, a possible solution is to embed an explicit electronic noise source in one of the oscillators. In [10] a random bit source is presented where a thermal noise source is embedded in a triangular wave oscillator. As a result, the oscillator features a phase noise with a distribution that is directly derived from the thermal noise.

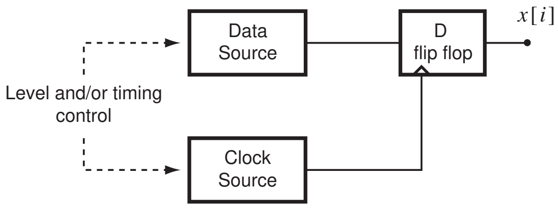


Fig. 4. Metastability-based RBG.

Random sources based on flip-flop metastability also exploit electronic and phase noise. Flip-flop metastability occurs when the data and clock signals are very close to the switching threshold or when they switch very close in time one to each other [14]. In these conditions, a small variation in level or in phase results is a different output value from the flip-flop. Actually, this source can be seen as a degeneration of the previous schemes. Depending whether the metastability is produced by setting a critical input level or a critical input phase, the working principle is very similar to that in Figure 2 or Figure 3 respectively.

In this kind of source, the main implementation issue is the level or phase control of the inputs. In facts, since there is not an explicit electronic or phase noise source, nor any noise amplification mechanism, a very precise control is required in order to force a metastability condition.

To summarize, the oscillator-based scheme has the simplest and most robust implementation. On the other hand, due to the beating effect, the randomness source cannot be tested by a simple transition test. Moreover, if the oscillators are implemented by means of digital ring oscillators, the achievable jitter is very low thus resulting in a very low speed or poor quality generator.

The architecture proposed in this work is depicted in Figure 5. In essence, this scheme merges the direct amplification and the oscillator-based techniques. It features the simple implementation of an oscillator-based RBG but it can be seen as a direct amplification scheme where the electronic noise is replaced by time jitter and the *sign* quantization is replaced by the $mod\,2$ one. A comparison between Figure 2 and Figure 5 can clarify the analogies.

In the proposed scheme, the oscillators are re-synchronized before each bit generation. As a results, the periodical behavior typical of the oscillator-based sources is suppressed and each bit generation restarts from the same state as in

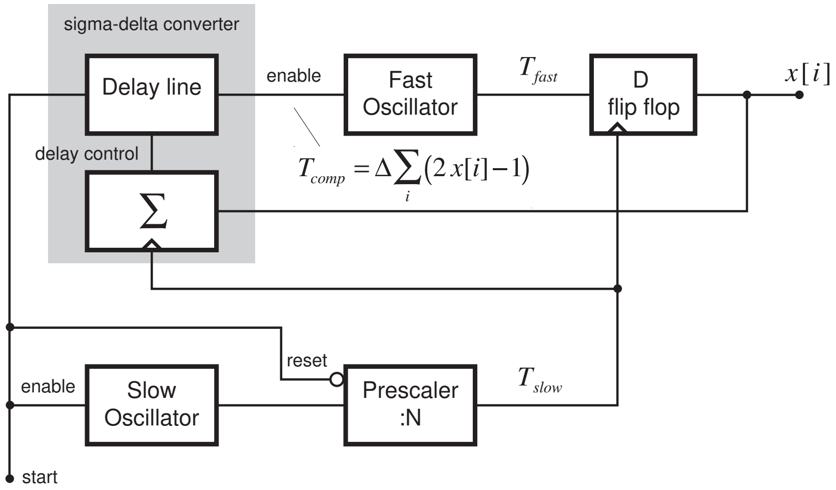


Fig. 5. The RBG proposed in this work.

a direct-amplification source. The T_{slow} prescaler actually implements a noise amplification mechanism since, scaling down the oscillator frequency, the accumulation period for the jitter increases. The analogy between the "jitter amplifier" (i.e. the prescaler) and the noise amplifier in Figure 2 is very close: in both cases, a higher noise amplification costs in term of bandwidth. In fact, in Figure 5, noise amplification is obtained by reducing the sampling frequency. In a similar way, in Figure 2, as the gain G increases, the amplifier bandwidth B decreases and, to maintain the same correlation among samples, the sampling frequency must be reduced.

The delay line performs a time offset compensation that is similar to the voltage offset compensation implemented by the D/A converter in Figure 2. A T_{comp} delay is generated in such a way the slow oscillator samples the fast one on its edges. Therefore, the random bit $x[i]$ is, actually, the least significant bit of the ratio between the period T_{slow} of the slow oscillator and period of the fast one T_{fast}:

$$x[i] = \left\lfloor \frac{T_{slow}[i]/2 - T_{comp}[i]}{T_{fast}/2} \right\rfloor mod\, 2 \tag{3}$$

where T_{comp} makes sure the $floor$ function works around one of its discontinuities. This quantization mode combines the offset compensation of the direct-amplification scheme with the $mod\,2$-mode of the oscillator-based architecture. As a result, the required jitter can be reduced by increasing the precision Δ of the offset compensation (Figure 6). Basically, the device can operate with a minimal jitter intensity of about $\Delta/2$, while, without the offset compensation, the required jitter is about $T_{fast}/2$. Therefore, the ratio $\alpha = T_{fast}/\Delta$ can be seen as equivalent to a jitter amplification and represents the gain obtained by this design. Since the $mod\,2$ quantization is adopted, the source cannot be saturated and cannot be easily forced by means of external signals. In fact, in order to force the source, an attacker should control the phase between the two oscillators with a precision better than $T_{fast}/4$. Basically, the $mod\,2$-mode makes the device robust with respect to large T_{slow} variations, while the T_{comp} compensation makes the device robust with respect to T_{slow}/T_{fast} variations.

As a further advantage of the proposed architecture, the T_{comp} feedback suppresses the effect of several source asymmetries that could be difficult to control. Asymmetries in the waveform of the fast oscillator (e.g. an unbalanced duty cycle) as well as asymmetries in setup and hold times of the sampling flip-flop are automatically compensated. Finally, it can be noticed that, if the offset compensation is very precise, the device degenerates in a metastability-based source due to the feedback loop that forces the sampling flip-flop to operate in a metastable state.

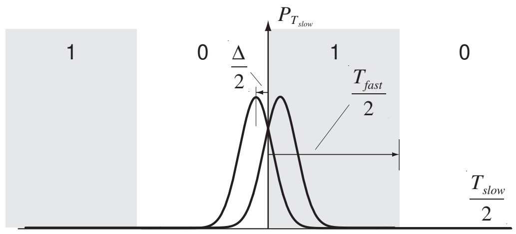


Fig. 6. Offset compensated $mod\,2$ quantization.

3 Circuit details

A fully digital implementation on a $90nm$ CMOS standard-cell library has been adopted for the design and simulation of the proposed RBG and a detailed block scheme is depicted in Figure 7. Both oscillators are implemented as ring oscillators. The fast one is designed for the maximal frequency which allows a saturated waveform. Really, this is not strictly required since an amplitude as large as needed for the sampling flip-flop toggling is enough. Nevertheless, even under this conservative constraint, a nominal value of about $250ps$ is expected for T_{fast}. Note that an attacker aimed to force the source will need a precision better than $T_{fast}/4 = 75ps$ (Figure 6).

The main threat for a oscillator-based RBG is the mutual synchronization between the two oscillators. That could occur because of a direct coupling or because of a coupling between the oscillators and some other signal (e.g. the system clock) [17]. In both cases, the mutual jitter between T_{slow} and T_{fast} will be low whatever pre-scaling factor N is employed. In order to address this synchronization issue, the slow oscillator is implemented as a spread spectrum oscillator

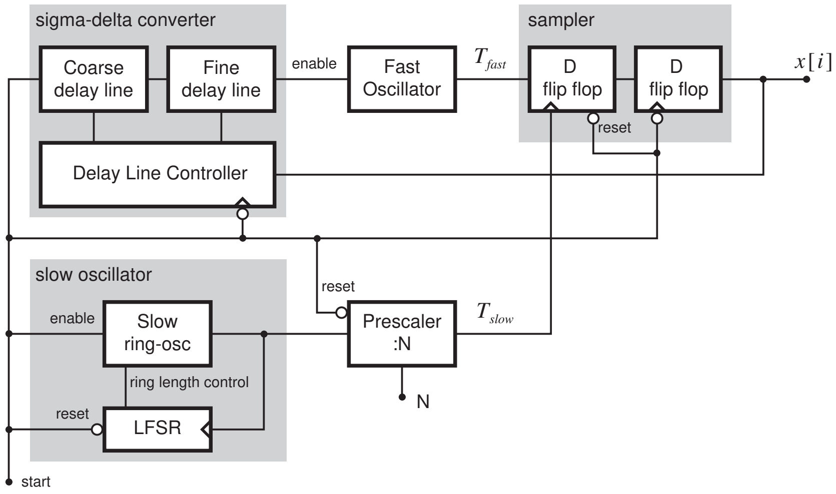


Fig. 7. Detailed block scheme for the proposed RBG.

by means of a ring oscillator whose length is controlled by a linear feedback shift register (LFSR). Note that the frequency spreading does not produce any artificial pseudo-randomness on the output sequence X. Actually, since the LFSR is reset before the generation of each bit, it produces every time the same sequence. Therefore, after the prescaler, variations on T_{slow} are due to the intrinsic oscillator jitter and no pseudo-random modulation is visible. A mean value of about $5ns$ is adopted for T_{slow} and the pre-scaling factor N will be chosen according to the available jitter. Different trade-offs between statistical quality and speed could be adopted depending on the post-processing compressing ratio [16].

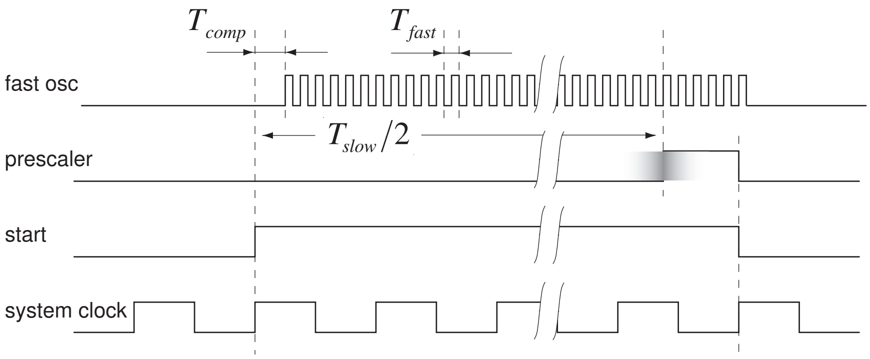
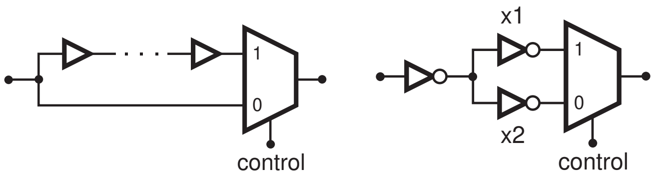


Fig. 8. Waveforms of the main signals.

On the raising edge of the *start* signal, the slow oscillator is enabled whereas the fast one is enabled after a delay T_{comp} which is adjusted by the feedback loop in Figure 7 according to the mean value of the output stream, thus forcing the slow oscillator to sample the fast one close to its edges (Figure 8).

As shown in Figure 7, the delay T_{comp} is implemented with a two stages adjustable delay line where the coarse grained line fixes the dynamic of the time offset compensation whereas its precision is determined by the fine grained line, thus obtaining a high dynamic and high precision without an excessive area requirement. Each delay line consists of a string of identical delay elements (Figure 9) and, thanks to the $mod\,2$ quantization, only the differential delays are relevant for the system operation. In particular, a maximum differential delay for the coarse line greater than $\pm T_{fast}/2$ is required and the maximum differential delay of the fine line must be long enough to cover at least a single step of the coarse line. These constraints assure the correct system operation.

According to a post-layout simulation, the fine grained delay line is expected to have a precision of $10ps$ which results in a gain factor $\alpha > 25$. Given that there are no constraints on the absolute delays, differential delays can be fined controlled by exploiting slight differences in signal propagation paths (Figure 9(b)), thus obtaining such a high precision. Moreover, since the delay cells are identical, a full-custom layout can guarantee the same parasitics on each cell. Notice that the connection between cells is not critical because it does not affect the differential delay. Regarding the symmetry between the sigma-delta DAC increasing and decreasing steps (Δ_+, Δ_- in (2)), it is guaranteed by construction since each increasing/decreasing delay step is obtained by adding/removing the same delay element.



(a) (b)

Fig. 9. Implementation of the coarse (a) and fine (b) differential delay elements. The fine delay cell exploits the differential delay between two inverters having different drive strength (x1 and x2). Since the inverters are driven in parallel, inputs signals are aligned while, on the output, the stronger inverter (x2) switches faster.

On the falling edge of the *start* signal, both oscillators are stopped, the sampling flip-flop is reset and the sampled bit is saved in the output flip-flop. The sampling flip-flop reset is required to remove the dependency that, in a real flip-flop, exists between its input thresholds and timings, and its logic state. Such dependency, and in general every state variables in the system, can generate a pseudo-random evolution which prevents the detection of a lack of entropy condition.

Disturbances coming from the system clock are typically very intense and can heavily influence the oscillators. Therefore, a further implicit state variable results from the phase shift between the start of a new bit generation and the system clock. In order to clear this state dependence too, the start signal is synchronized with the system clock (Figure 8) in such a way clock disturbances are the same during each bit generation and their effects are compensated by the feedback loop.

4 Fault detection and entropy evaluation

An important feature of the presented source is the possibility to check its operation in real time. This feature can be exploited to detect faults as well as to adapt the post-processing compression ratio depending on the estimation of the source entropy. Basically, a source is as easier to check as much as it cannot deceive tests by means of pseudo-random behaviors. On the other hand, the ability of a system to behave pseudo-randomly is limited by the state space in which its free evolution can take place. As a consequence, a source having a very small state space can be checked even by means of a very simple test.

In the presented scheme several measures are adopted to suppress explicit or implicit state variables, hence, a lack of jitter condition can be immediately recognized since, in absence of jitter, the device has a straightforward deterministic model. Actually, if the jitter is not sufficient, the device produces the periodic sequence "...010101..." that results from the delay feedback loop. The other potential deterministic behaviors can arise because of a transient or a fault status of the feedback. In this case, the constant sequences "...000000..." or "...111111..." are expected. As a consequence, the following transition counting has been adopted in the proposed source:

$$N_{trans} = \sum_i x[i] \oplus x[i-2]. \tag{4}$$

In fact, for a maximal entropy sequence, this counter is expected to return half the number of the generated symbols, whereas, for the discussed deterministic sequences, it does not increase at all. It is also noticeable that N_{trans} is equally sensitive to both symbol and transition biasing. Actually, N_{trans} is an indicator of how much the source differs from its deterministic model, i.e. an estimator of its entropy. Therefore, it allows to choose a suitable pre-scaling factor as well as to detect faults and to perform an adaptative post-processing depending on the quality of the source [16]. As an example, in order to produce a 32 bit random block, the post-processing compression can be carried on until $N_{trans} = 64$. As a result, the compressing ratio will be about 4 if the source features a large jitter and will increase automatically in a low jitter condition.

5 Conclusions

A new, patent pending, architecture for an integrated random bit source has been presented which is low demanding in terms of area and power consumption and suitable for security applications. The proposed generator is an enhancement of the oscillator-based architecture but, at the same time, it presents the advantages of a direct amplification-based RBG, thus resulting in a reliable and robust solution for high quality random bit generation. The source also features a tuning and a real-time test of its statistical quality. A standard-cell based implementation, without any amplified noise source, can be adopted for the proposed generator and implementation details have been also discussed.

Future work will involve the experimental verification of the presented architecture and the obtained results will be reported in a following paper.

References

1. B. Schneier, *Applied Cryptography*, second ed., New York, John Wiley & Sons, 1996.
2. D. Naccache and D. M'Raibi, *Cryptographic Smart Cards*, IEEE Micro, vol. 16, no. 3, pp. 14-24, June 1996.
3. P. Kocher, J. Jaffe, and B. Jun, *Differential Power Analysis*, Advances in Cryptology (Crypto '99), M. Wiener, ed., pp. 388-397, 1999.
4. W.T. Holman, J.A. Connelly, and A.B. Downlatabadi, *An Integrated Analog/Digital Random Noise Source*, IEEE Trans. Circuits and Systems I, vol. 44, no. 6, pp. 521-528, June 1997.
5. V. Bagini and M. Bucci, *A Design of Reliable True Random Number Generator for Cryptographic Applications*, Proc. 1st Workshop Cryptographic Hardware and Embedded Systems (CHES '99), Heidelberg, Germany, Springer-Verlag, 1999, vol. 1717, pp. 204-218.
6. M. Bucci, L. Germani, R. Luzzi, P. Tommasino, A. Trifiletti, and M. Varanonuovo, *A High-Speed IC Random-Number Source for SmartCard Microcontrollers*, IEEE Trans. Circuits and Systems I, vol. 50, no. 11, pp. 1373-1380, Nov. 2003.
7. M. Dicht and N. Janssen, *A High Quality Physical Random Number Generator*, Proc. Sophia Antipolis Forum Microelectronics (SAME 2000), pp. 48-53, 2000.
8. B. Jun and P. Kocher, *The Intel Random Number Generator*, Cryptographic Research Inc., white paper prepared for Intel Corp., Apr. 1999, http://www.cryptography.com/resources/white papers/IntelRNG.pdf.
9. C.S. Petrie and J.A. Connelly, *Modeling and Simulation of Oscillator-Based Random Number Generators*, Proc. IEEE Int'l Symp. Circuits and Systems (ISCAS '96), vol. 4, pp. 324-327, 1996.
10. M. Bucci, L. Germani, R. Luzzi, A. Trifiletti, and M. Varanonuovo, *A High-Speed Oscillator-Based Truly Random Number Source for Cryptographic Applications*, IEEE Trans. Computers, vol. 52, no. 4, pp. 403-409, April 2003.
11. T. Stojanovski and L. Kocarev, *Chaos-Based Random Number Generators - Part I: Analysis*, IEEE Trans. Circuits and Systems I, vol. 48, no. 3, pp. 281-288, Mar. 2001.
12. T. Stojanovski, J. Pihl, and L. Kocarev, *Chaos-Based Random Number Generators - Part II: Practical Realization*, IEEE Trans. Circuits and Systems I, vol. 48, no. 3, pp. 382-385, Mar. 2001.

13. M.J. Bellido, A.J. Acosta, et al., *A Simple Binary Random Number Generator: new approaches for CMOS VLSI*, Proc. 35th Midwest Symposium on Circuits and Systems, Aug. 1992.
14. M. Epstein, Laszlo Hars, R. Krasinski, M. Rosner, and H. Zheng, *Design and Implementation of a True Random Number Generator Based on Digital Circuit Artifacts*, Proc. 5th Workshop Cryptographic Hardware and Embedded Systems (CHES '03), Heidelberg, Germany, Springer-Verlag, 2003, vol. 2779, pp. 152-165.
15. C.S. Petrie and J.A. Connelly, *A Noise-Based IC Random Number Generator for Applications in Cryptography*, IEEE Trans. Circuits and Systems I, vol. 47, no. 5, pp. 615-621, May 2000.
16. E. Trichina, M. Bucci, D. De Seta, and R. Luzzi, *Supplementary Cryptographic Hardware for Smart Cards*, IEEE Micro, vol. 21, no. 6, pp. 26-35, Nov./Dec. 2001.
17. T. Pialis and K. Phang, *Analysis of Timing Jitter in Ring Oscillators Due to Power Supply Noise*, Proc. IEEE Int. Symp. Circuits and Systems (ISCAS 2003), vol. 1, pp. 685-688, May 2003.