Design of Testable Random Bit Generators

Marco Bucci and Raimondo Luzzi

Infineon Technologies Austria AG
Babenbergerstrasse 10, A-8020 Graz (AUSTRIA)

{marco.bucci, raimondo.luzzi}@infineon.com

Abstract. In this paper, the evaluation of random bit generators for security applications is discussed and the concept of stateless generator is introduced. It is shown how, for the proposed class of generators, the verification of a minimum entropy limit can be performed directly on the post-processed random numbers thus not requiring a good statistic quality for the noise source itself, provided that a sufficient compression is adopted in the post-processing unit. Assuming that the noise source is stateless, a straightforward entropy estimator to drive an adaptive compression algorithm is proposed. Examples of stateless sources are also discussed.
Finally, an attack scenario against a noise source is defined and an effective approach to the attack detection is presented. The entropy estimator and the attack detection together guarantee the unpredictability of the generated random numbers.

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

1 Introduction

Random numbers are extensively used in many cryptographic operations. Public/private key pairs for asymmetric algorithms are generated from a random bit stream; a random bit generator (RBG) is also needed for key generation in symmetric algorithms, for generating challenges in authentication protocols, and for creating padding bytes and blinding values [1].

Even if, historically, the only requirement for an RBG was to fulfill bunches of statistical tests aimed to reveal defects in the generated data, nowadays in the technical community is well accepted that, for random numbers used in cryptography, a flat statistic is not sufficient and their unpredictability is the main requirement: a potential attacker must not be able to carry out any useful prediction about the generator's output even if its design is known. As a consequence, the focus is on the verification of a minimum entropy requirement and statistical tests are significant only if the statistical model of the random source under evaluation is known [2].

The German IT security certification authority (BSI) has adopted this approach in its AIS 31 publication [3] where the physical noise source is separated from the digital post-processing and, for devices belonging to the functionality class P2 [1], criteria

[1] Devices intended for generation of signature key pairs, generation of DSS signatures, generation of session keys for symmetric encryption mechanisms must belong to the functionality class P2.

and statistical tests are defined for the noise source output (*digitized noise signal*) in order to verify a minimum entropy limit for the post-processor output (*internal random numbers*). Namely, the entropy requirement on the final data is guaranteed by defining a minimum entropy limit for the raw data from the source and, at the same time, requesting that the adopted post-processing algorithm does not reduce its input entropy.

In this paper we propose to go further ahead with this approach defining an RBG based on a stateless (memoryless) noise source and a stateless post-processing algorithm. Since the noise source is assumed memoryless, the generated symbols are independent and, since the post-processor is also memoryless, the internal random numbers are independent too. Therefore, the entropy limit can be verified directly after the post-processor, controlling that the assumed compression ratio in the post-processor is well chosen with respect to the available entropy per bit from the source. In this scheme, very fast noise sources, but with a low entropy per bit ("spread" entropy sources), can be adopted, provided that a sufficient compression is applied. In other terms, the relevant figure of merit becomes the *entropy throughput* (entropy/second) instead of the entropy per bit, and the design of the noise source is not anymore constrained by the statistical quality, but efficiency and robustness can be taken as the main goals.

Moreover, under the hypothesis of independent symbols, a straightforward entropy estimator can be used to evaluate the amount of entropy produced by the source thus allowing an adaptive post-processing (compression) and an on-line test of the source. In fact, even if the source entropy throughput can be evaluated during the characterization of selected prototypes, tolerances of components, temperature drifts and ageing affect the statistical properties of the noise source thus requiring an on-line test during the RBG operation [2].

In addition to technological and environmental variances, attack scenarios when the generator is operated in a real application should be also considered. In this case, the effective entropy is basically the attacker's error rate when observing or forcing the noise source output. Since the estimation of the attacker's error rate should be very conservative, a strong post-processing is required anyway (minimum compression ratio), and requesting a high statistical quality for the noise source operated in a controlled environment loses significance.

In Section 2, the proposed RBG is described focusing on how the hypothesis of statistical independence for both the raw data and the internal random numbers is fulfilled. Examples of stateless noise sources are reported in Section 3 while, in Section 4, the important topic of robustness against attacks is discussed proposing an effective approach to their detection.

2 Stateless random bit generators

Random bit generators used in applications where the unpredictability is a key requirement are based on non-deterministic phenomena that act as the source of randomness. In integrated circuit implementation, electronic noises (thermal and shot) and time jitter are usually the only available randomness sources.

Every noise source, even if well-designed, produces a bit stream that usually shows statistical defects due to bandwidth limitation, fabrication tolerances, ageing and tem-

perature drifts, deterministic disturbances and, in case, signals forced by an attacker. As a consequence, the noise source should be always followed by a strong digital post-processing as shown in Figure 1, where the definitions reported in [3] have been adopted.

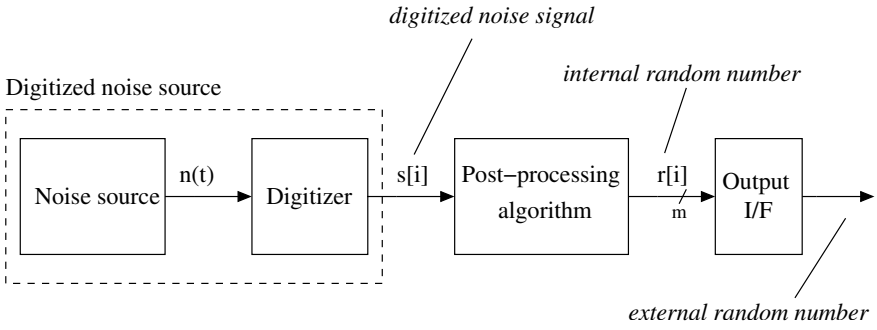


Fig. 1. Generic architecture for an RBG.

A noise source generates an analog signal $n(t)$ which is input into a digitizer. The digitizer samples the analog signal and converts the sampled values into a stream of random bits $s[i]$ (*digitized noise signal*). The non-deterministic source and the digitizer together form the digitized noise source. The random bits $s[i]$ are then fed into the post-processing unit which then produces a stream of m-bit random words $r[i]$ (*internal random numbers*).

The post-processing unit fulfills two purposes: Firstly, it is necessary to adjust the probability distribution of the raw random bits $s[i]$ thus overcoming statistical defects present in the non-deterministic noise source or in the digitizer (e.g. input offset of a voltage comparator). The probability distribution of the resultant random words $r[i]$ is much closer to a uniform distribution than that of the input stream $s[i]$.

Secondly, the post-processor is used to increase the entropy per bit of the output stream. The entropy per bit is increased adopting a compressing function that collects ("distills") the entropy in the input stream $s[i]$ to produce a lower speed output stream with increased randomness.

Due to the presence of mathematical post-processing in an RBG, it is not straightforward for a certification authority to discriminate between a truly RBG and a pseudo random generator which is able to deceive statistical tests producing a uniform probability distribution without, however, producing any entropy.

In order to guarantee that the generated random numbers are indeed unpredictable and not just uniformly distributed, the AIS 31 guidelines [3] require, in P2.c), - in addition to the requirement that the statistical behavior of the internal random numbers should be inconspicuous - that "*the prospects of success for systematic guessing of the external random numbers*[2] *(realised through systematic exhaustion attacks) - even if*

[2] As shown in Figure 1, random numbers that the RBG external interface delivers to the application are named external random numbers.

external random number sub-sequences are known - should at best be negligibly higher than would be the case if the external random numbers had been generated by an ideal random number generator".

To certify that this is the case, in P2.d)(vii), [3] states that the sequence of raw random bits $s[i]$ has "*to meet particular criteria or pass statistical tests intended to rule out features such as multi-step dependencies*" and a suite of statistical tests to be fulfilled is provided. Basically, by testing the random bits before the post-processing it can be guaranteed that the random words $r[i]$ do indeed have entropy as a physical non-deterministic noise source is involved in their generation.

Although the AIS 31 has finally focused the attention on the entropy, the described approach has the disadvantage to consider as the relevant figure of merit the entropy per bit produced by the source and not its entropy throughput (entropy/second). Therefore, fast sources but with low entropy per bit, that could produce good quality random numbers if a sufficient compression is applied and, in general, have a more robust implementation than sources with a better probability distribution, are ruled out.

Moreover, it is not always possible to separate the noise source from the post-processing. For example, RBG's based on discrete chaotic systems [4,5] present an intrinsic pseudo-random behavior superimposed to a random evolution. Therefore, even if statistical tests applied on the source output $s[i]$ pass, that is not sufficient to state that a chaotic source produces enough entropy per bit.

The approach proposed in this paper is to consider the noise source only as a source of entropy, without requiring good statistical properties for it, and to transfer to the post-processor the task of adjusting the statistic quality and increasing the entropy per bit by means of a sufficiently high compression. Of course that requires a different procedure to certify the generator since, in general, the noise source will not pass the AIS 31 suite of statistical tests as requested in P2.d)(vii).

Actually, this different approach is still compatible with [3], where *alternative criteria* to statistical tests on the source are also provided. In particular, according to the alternative criteria - type 1, "*the applicant may alternatively submit the following proof:*

- *Internal random number sequences pass statistical tests specified in P2.i)(vii).*
- *Clear proof that the internal random numbers achieve the goal set with criterion P2.d)(vii).*
  The proof must the provided taking into account the mathematical post-processing and on the basis of the empirical properties of the digitized noise signal sequence."

Criterion P2.d)(vii) and the statistical tests specified in P2.i(vii) are aimed "*to guarantee P2.c) for selected prototypes by verifying a minimum entropy limit for each internal random bit with a negligibly small error probability*". In other words, criterion P2.d)(vii) requires that the random stream after the post-processor meets a minimum entropy limit in order to guarantee the unpredictability of the generated numbers.

Now, if the adopted noise source is assumed to be stateless (memoryless), then the generated symbols $s[i]$ are independent. As a consequence, if the post-processing unit is also stateless, the internal random numbers $r[i]$ are independent too and the obtained entropy per bit can be evaluated from the uniformity of their estimated (empirical) probability distribution. In particular, a χ^2 test with $k-1$ degrees of freedom can be applied,

where $k = 2^m$ is the cardinality of the output alphabet [1]. Obviously, to keep the test feasible, the output parallelism m must be limited; a typical output interface for a RBG is 8-bit wide.

The stateless hypothesis can be fulfilled by resetting to a constant value every state variable both in the source[3] and the post-processor[4] before the generation of a new bit $s[i]$ and a new word $r[i]$ respectively, as depicted in Figure 2.

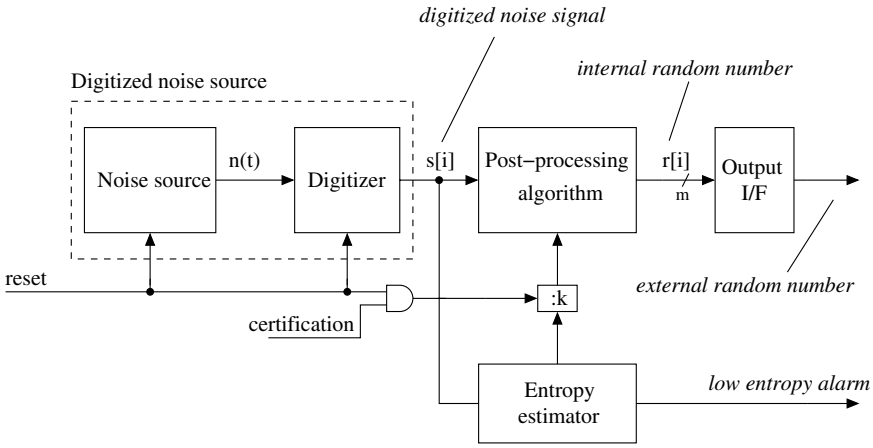


Fig. 2. A stateless random bit generator.

While it is perfectly clear what resetting the digital post-processor means, the implementation of the noise source reset depends on the particular source we adopt and two examples of stateless sources will be discussed in Section 3.

It is interesting to observe that the source reset before each bit generation is not strictly necessary. In fact, if a compression factor k is used in the post-processor, the independence of the input $(k \cdot m)$-bit sub-sequences $\{s[(k \cdot m)i + j]\}$, $j = 0, \ldots, (k \cdot m) - 1$, is sufficient to prove the independence of the m-bit output symbols $r[i]$. Therefore, resetting the noise source every time a new output word $r[i]$ is generated would be sufficient.

Nevertheless, the additional hypothesis of independence of each raw bit allows to adopt the counting of the transitions in the sequence $s[i]$ as a straightforward *entropy estimator* (Figure 2) for the source [6]:

$$N_{trans} = \sum_i \left(s[i] \oplus s[i-1] \right). \tag{1}$$

A lack of transitions with respect to what is expected from an ideal random source signals a lack of entropy. Using (1), a post-processor with adaptive compressing can be

[3] Resetting the noise source implies resetting the underlying noise process too. Alternatively, a bit generation frequency sufficiently slower than the noise process bandwidth must be adopted.

[4] Patent pending.

defined [7], processing raw bits from the source until a minimum number of transitions has been counted. For example, if 16 transitions must be counted before an 8-bit output word $r[i]$ is released, that is equivalent to have a mean dynamic compression equal to 4 for an ideal input sequence, which increases automatically as the entropy from the source decreases.

The mean compression is chosen according to the entropy throughput expected from the source. In addition, an upper limit for the compression ratio can be fixed (e.g. $k = 16$), after that an alarm is asserted thus detecting faults in the source.

Even if the post-processing reset is necessary during the entropy evaluation (certification), it can be disabled during the normal operation (Figure 2). In fact, if a linear post-processing algorithm is employed (e.g. a linear-feedback shift register), it can be easily proved that the output is equivalent to the sum of the reset post-processing output and the output when the state is maintained and there is no input string from the source (free evolution). Therefore, the resulting entropy per bit is not lower than that evaluated during the RBG certification.

3 Examples of stateless sources

Even if every noise source can be turned into a stateless source simply switching off and on again its power supply before the generation of each new bit [5], in practice, an ad hoc designed source is necessary. In particular, a *reset state* must be implemented where every memory of the previous generated bit is canceled. A recovery time from the reset negligible with respect to the bit generation time is the main condition to fulfill.

A first example of stateless noise source can be obtained from the well-know oscillator-based random bit generator [8,9,10,11] if both oscillators are stopped after each bit generation (Figure 3), thus avoiding the phase shifting between f_{fast} and f_{slow}. If digital ring oscillators are employed to implement f_{fast} and f_{slow}, the start-up time is usually a small fraction of the their oscillating period.

On the trailing edge of a start pulse, both oscillators are enabled and, after $T_{slow}/2$, the f_{slow} raising edge samples f_{fast} and disables both oscillators. A new start pulse is necessary to trigger the generation of a new bit $s[i]$.

The phase shift between the oscillators is not the only state variable which must be canceled in this system. In fact, the digitized (a flip-flop in Figure 3) has a memory and its behavior in commutation depends somehow on the current state (e.g. different switching timings). As depicted in Figure 3, this further state variable can be easily canceled resetting the flip-flop too.

An RBG based on this noise source is reported in [12] where an additional feedback loop is employed to control a starting delay on f_{fast} in order to force the slow oscillator to sample the fast one close to one of its edges. Such compensation delay is controlled according to the mean value of the generated bit stream $\{s[i]\}$ and, as a consequence, the source is not stateless any more. Anyway, if the feedback loop is stopped once the steady-state has been reached, thus alternating compensation and normal operation phases, the stateless hypothesis still holds.

[5] External asynchronous disturbances and signals forced by an attacker are neglected in this context. An attack scenario and how to detect it is discussed in Section 4.

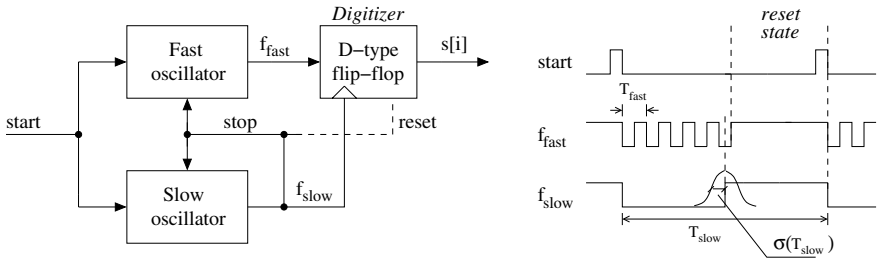


Fig. 3. A stateless oscillator-based noise source.

As a second example, a noise source based on a well known chaotic circuit [13] is depicted in Figure 4. The circuit state is the voltage across the capacitor C and a reset state can be easily implemented with an additional switch. In general, that holds for every chaotic source based on as a switched capacitor circuit.

On the rising edges of the clock clk, the capacitor C is charged with a time constant $\tau_1 = R_1C$. When the voltage across C reaches a reference level V_R, C is discharged with a time constant $\tau_2 = R_2C$. If τ_1, τ_2 and the clock period are properly chosen, the circuit shows a chaotic behavior. Every N clock periods an output bit $s[i]$ is generated and C is reset.

The down-sampling parameter N must be properly chosen in order to obtain a sufficient number of transitions (1). Its value is strictly dependent on the actual divergence speed of the chaotic circuit (Lyapunov exponent). As a consequence, the transition test (1) detects whether or not the circuit is actually having a chaotic behavior, i.e. if all the critical parameters of the circuit are currently in range.

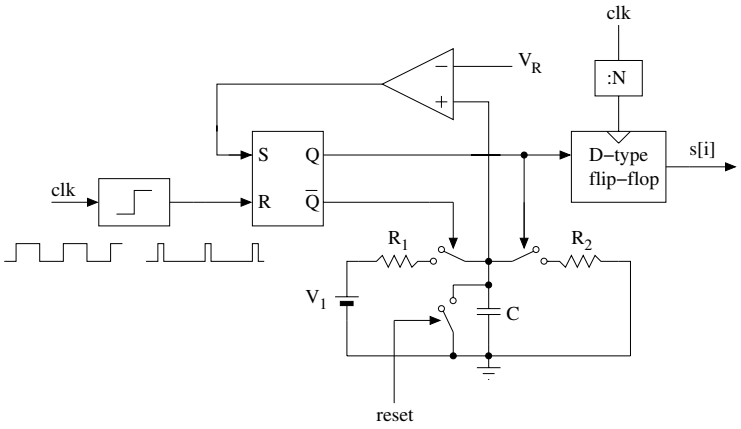


Fig. 4. A stateless noise source based on a chaotic circuit.

4 Attack detection in stateless noise sources

An entropy estimator based on the transition counter (1) has been introduced in Section 3, stating that a lack of transitions signals a lack of entropy. Unfortunately, if attack scenarios are taken into account, the inverse implication does not hold. In fact, an attacker will force the noise source with a pseudo-random disturbance thus deceiving the transition counter. Therefore, an additional attack detection mechanism is necessary, while the transition counter is solely intended to detect faults in the noise source.

From the attacker point of view, the actual entropy of the noise source is his error probability when observing or forcing the generator. An RBG can be observed with the same techniques employed against cryptographic processors, in particular side-channel attacks. However, in this case, averaging techniques are not helpful thus limiting the effectiveness of the attack. On the other hand, since noise sources are based on very weak random signals, forcing attacks by means of strong disturbances are a threat for RBG's and must be taken into account.

The attack model depicted in Figure 5 is assumed in the following: the attacker can superimpose an own random signal $d(t)$ to the noise output $n(t)$ thus obtaining a probability distribution that, after the digitizer, is indistinguishable from what the generator produces in normal conditions. It is then clear that an attack detection is possible only before the digitization.

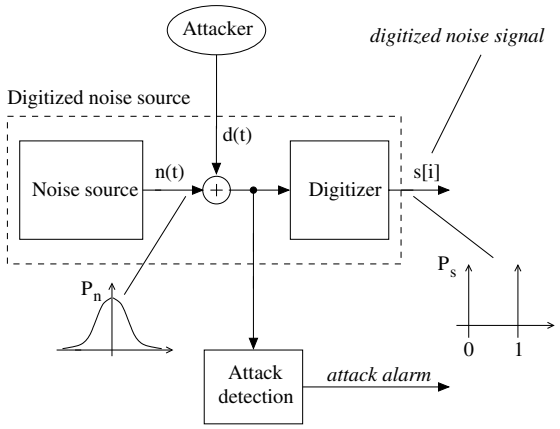
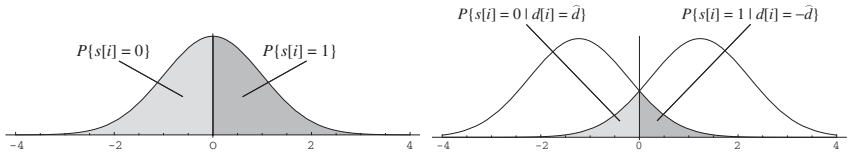


Fig. 5. Forcing attack on a noise source.

In order to force the source, the attacker shifts the source probability distribution P_n adding a disturbance $\pm\widehat{d}$ and, to obtain an effective entropy reduction (taking into account the compression in the post-processor), his error probability $Pr\{s[i] = 1 \mid d[i] = -\widehat{d}\}$ must be sufficiently small (Figure 6). In other terms, a disturbance amplitude $\widehat{d}$ larger than the P_n standard deviation is required.

Therefore, an attacker cannot force a noise source without increasing its intensity and the attack detection is based on a source intensity test, assuming that its intensity in normal conditions is known.



(a) normal conditions.

(b) conditional distributions and residual error under attack.

Fig. 6. Source probability distribution.

A simple statistical test to detect the attack is counting the number of samples falling beyond two fixed thresholds as shown in Figure 7, triggering an alarm if the counted value is too high with respect to the expected value.

Such approach is general and can be applied to the noise signal $n(t)$ produced by every kind of stateless noise sources. As an example, for the oscillator-based RBG discussed in Section 3, the attack detection is implemented adding a second flip-flop which samples f_{fast}/n, where the down-scaling factor n is chosen according to the ratio $\sigma(T_{slow})/T_{fast}$ measured in a controlled environment. If the number of transitions in this second stream is too high an alarm is generated or, in a borderline condition, the compression rate can be increased to counterbalance the entropy loss.

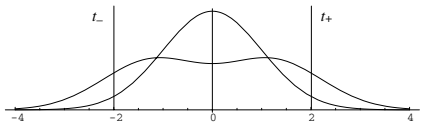


Fig. 7. Noise source intensity test.

5 Conclusions

The concept of stateless random bit generator has been introduced, defining a class of generators where both the noise source and the post-processing unit are assumed stateless. The assumption is satisfied introducing a reset state to cancel the memory of the previous generated bits. The noise source is reset after each bit generation while, for the post-processor, a reset after a word generation is required. The stateless property

implies the independence of the external random numbers thus allowing to shift the verification of a minimum entropy limit after the post-processing.

In this approach, the noise source plays the role of entropy source and the relevant figure of merit is its entropy throughput. In other words, the statistic quality of the source itself is not a requirement, provided that a sufficient compression is implemented in the post-processing algorithm. The independence of the raw bits from the source allows to define a straightforward on-line entropy estimator to drive an adaptive compressing thus adapting the compression ratio to the actual entropy available from the source.

Implementation aspects have been also discussed pointing out that, while the post-processing reset is not an issue, the implementation of the source reset depends on the source architecture. Two examples have been provided to clarify the general principle.

The stateless hypothesis is sufficient to define an entropy estimator only if disturbances from an attacker aimed to force the source are not taken into account. As a consequence, in a real application, a further attack detection mechanism is required and an effective statistical test on the source before the digitizer has been discussed.

References

1. A. J. Menezes, P. C. Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, Boca Raton, FL, 2001.
2. W. Schindler, *Efficient Online Tests for True Random Number Generators*, Proc. 3rd Workshop Cryptographic Hardware and Embedded Systems (CHES '01), LNCS (Springer-Verlag), vol. 2162, pp. 103-117, 2001.
3. W. Killmann and W. Schindler, *AIS 31: Functionality classes and evaluation methodology for true (physical) random number generators*, version 3.1, Bundesamt fur Sicherheit in der Informationstechnik (BSI), Bonn, 2001.
4. 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.
5. 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.
6. 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), LNCS (Springer-Verlag), vol. 1717, pp. 204-218, 1999.
7. 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.
8. M. Dichtl and N. Janssen, *A High Quality Physical Random Number Generator*, Proc. Sophia Antipolis Forum Microelectronics (SAME 2000), pp. 48-53, 2000.
9. 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.
10. 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.
11. 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.

12. H. Bock, M. Bucci, and R. Luzzi, *An Offset-Compensated Oscillator-based Random Bit Source for Security Applications*, Proc. 6th Workshop Cryptographic Hardware and Embedded Systems (CHES '04), LNCS (Springer-Verlag), vol. 3156, pp. 268-281, 2004.
13. S. Mandal and S. Banerjee, *An Integrated CMOS Chaos Generator*, Proc. 1st Indian National Conf. Nonlinear Systems & Dynamics (NCNSD '03), pp. 313-316, Dec. 2003.