A High-Speed Oscillator-Based Truly Random Number Source for Cryptographic Applications on a Smart Card IC

Marco Bucci, Lucia Germani, Raimondo Luzzi, *Member*, *IEEE*,
Alessandro Trifiletti, and Mario Varanonuovo, *Member*, *IEEE*

Abstract—The design of a high-speed IC random number source macro-cell, suitable to be integrated in a Smart Card microcontroller, is presented. The oscillator sampling technique is exploited and a jittered oscillator which features an amplified thermal noise source has been designed in order to increase the output throughput and the statistical quality of the generated bit sequences. The oscillator feedback loop acts as an offset compensation for the noise amplifier, thus solving one of the major issues in this kind of circuit. A numerical model for the proposed system has been developed which allows us to carry out an analytical expression for the transition probability between successive bits in the output stream. A prototype chip has been fabricated in a standard digital $0.18\mu m$ *n*-well CMOS process which features a 10Mbps throughput and fulfills the NIST FIPS and correlation-based tests for randomness. The macro-cell area, excluding pads, is $0.0016mm^2$ ($184\mu m \times 86\mu m$) and a $2.3mW$ power consumption has been measured.

Index Terms—Random number generator, noise source, jittered oscillator, Smart Cards.

1 Introduction

The expanding use of digital communications, electronic financial transactions, and digital signature applications has raised demanding security issues to fulfill the requirements for secrecy, integrity, and nonrepudiability of exchanged information. In this context, cryptographic algorithms and cryptographic tokens, like Smart Cards, play a fundamental role [1].

Both symmetric and asymmetric ciphering algorithms require the availability of a high quality random number source for secret key generation [2]; random numbers are also used for generating challenges in authentication protocols, to create padding bytes and blinding values [3].

Even if pseudorandom number generators (PRNGs) based on cryptographically secure deterministic algorithms [4] are usually employed for these purposes, a physical source of true randomness is needed for algorithm seeding. For this reason, a Smart Card microcontroller always features a truly RNG among its peripheral devices.

The main feature of a well-designed RNG is the unpredictability of the produced bit stream: A potential attacker must not be able to carry out any useful prediction about the generator's output even if its design is known.

A truly RNG produces a random bit stream from a nondeterministic natural source; electronic noise and radioactive decay are two examples of usable processes [5]. In integrated implementations, thermal and shot noise are actually the only white stochastic processes which can be exploited. Moreover, these noise sources have predictable and technology-independent distributions, thus allowing us to obtain a statistical model for the RNG.

When designing an RNG core for Smart Card integration, 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 Smart Card microcontrollers (a typical chip area is about $10mm^2$ for a 32-bit card) and, at the same time, there is the demand to integrate nonvolatile memory blocks of ever-increasing size. As a consequence, the silicon area for integrating the CPU core and its peripheral devices has to be minimized: Usually, just a small percentage of the total chip area is assigned to the RNG macro-cell. 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 [1].

Power consumption is another stringent constraint, especially in hand-held equipment such as mobile terminals [6]; if the RNG analog circuits feature excessive power dissipation, complex power management policies have to be implemented at the software level in order to meet the requirement for power consumption during card operation. A related issue is the chip resistance to power analysis attacks [7]: A current consumption waveform highly correlated to the RNG's output bit stream can be exploited by an external attacker to extract the generated secret values.

- *M. Bucci and L. Germani are with Gemplus S.A., Rome Crypto Design Center, V. Pio Emanuelli 1, I-00143 Rome, Italy.*
  E-mail: marco.bucci@inwind.it, lucia.germani@katamail.com.
- *R. Luzzi is with Infineon Technologies Austria, Development Center Graz, Babenbergerstrasse 10, A-8020, Graz, Austria.*
  E-mail: raimondo.luzzi@infineon.com.
- *A. Trifiletti and M. Varanonuovo are with the Electronic Engineering Department, University of Rome "la Sapienza", V. Eudossiana 18, I-00184, Rome, Italy.*
  E-mail: trifiletti@die.uniroma1.it, mario.varanonuovo@ieee.org.

Manuscript received 15 May 2002; revised 22 Nov. 2002; accepted 22 Nov. 2002.
For information on obtaining reprints of this article, please send e-mail to: tc@computer.org, and reference IEEECS Log Number 117860.

Few noise-based IC RNG designs are reported in the literature due to the classified nature of most researches in this field; however, three different techniques for generating random streams are widely exploited: direct amplification of a noise source [8], [9], jittered oscillator sampling [10], [11], [12], and discrete-time chaotic maps [13], [14].

Hardware RNGs can feature a very high throughput, but, even if well-designed, the produced bit streams usually show a certain level of correlation due to bandwidth limitation, fabrication tolerances, aging and temperature drifts, and deterministic disturbances. 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, in [15], a truly RNG which adopts a mixing of the three mentioned RNG methods is presented. A generator resistant to deterministic interference is achieved without employing any special circuitry even if, due to the mixing of different techniques, it is difficult to perform a rigorous statistical analysis of the system.

A common procedure to remove statistical imperfections in the output bit stream from hardware RNGs is to process the sequence with a carefully designed correcting or decorrelating algorithm which, from a high speed near-random input stream, generates a lower speed bit stream with increased statistical quality, "distilling" the entropy contained in the input sequence. 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 the design of a high-speed, thermal noise-based, mixed-signal RNG IC macro-cell, suitable to be integrated in a Smart Card microcontroller, which features a 10Mbps output. The proposed truly RNG exploits the jittered oscillator technique, where the sampling oscillator is provided with an amplified noise source in order to achieve a high jitter to mean period ratio. In fact, this random number generator can be seen as an amplified noise source driving an A/D converter where only the LSB is used as output.

In Section 2, the architecture of the proposed RNG is described, an accurate model for the system is developed, and an analytical expression for the output bit transition probability is carried out. Circuit details are reported in Section 3 with special emphasis on the sampling oscillator design. Finally, in Section 4, the experimental results on the fabricated prototype are reported which show the randomness tests performed on the designed generator.

2 RNG Design

The design of truly RNGs using the oscillator method exploits the random cycle-to-cycle time drift (jitter) in free running oscillators to produce a random bit sequence. In the simplest implementation, a low frequency oscillator samples a fast oscillator in a D flip-flop: If the low frequency oscillator period features a standard deviation much greater than the fast oscillator period, the states of the sampled oscillator in two successive sampling times can be assumed uncorrelated (i.e., independent), thus generating a random bit stream.

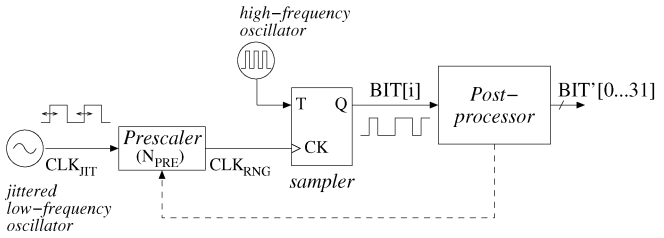

Fig. 1. RNG architecture.

A fully digital implementation which employs CMOS standard-cell ring oscillators can be used for the described system. The required oscillator jitter level is related to the desired random stream speed. Experimental results (see Section 4) have shown a jitter-to-mean period ratio lower than 10^{-4} for CMOS ring oscillators in a $0.18\mu m$ digital library, thus limiting the maximum throughput to 100kbps, if a 1GHz fast oscillator is employed.

In order to achieve faster bit rates, the proposed truly RNG, shown in Fig. 1, features a full-custom oscillator provided with an amplified noise source, as described in Section 3, which yields a standard deviation of about 10 percent of the period length. Such a high jitter level is able to provide a good quality random stream even if a 10MHz frequency is adopted for the oscillator mean frequency.

The high speed oscillator has been implemented with a 10-stage CMOS ring oscillator that typically oscillates at 1 GHz. Furthermore, in order to remove the biasing of the output bit sequence due to an unbalanced duty cycle from the ring oscillator, a T flip-flop is used as a sampling circuit. This detail ensures an output stream with an unbiased mean value. However, the effect of an unbalanced sampled oscillator must be taken into account when evaluating the transition probability between successive bits, as shown in the following.

In Fig. 1, a programmable prescaler is also shown at the output of the low frequency oscillator: Scaling factors from 1 to 128 are provided in order to experiment different jitter to mean frequency ratios. In a final release for production, this prescaler could be used to lower the output bit rate if a decrease in randomness (e.g., due to process variations, aging and temperature drifts) is detected by the digital postprocessor [16].

To characterize the noise source statistical behavior, an analytical expression for the bit transition probability of the raw sequence $BIT[i]$ before the postprocessor has been carried out under the following hypotheses:

- A Gaussian probability density is assumed for the $T_{CLK_{RNG}}$ random variable, as shown in Fig. 2.
- The fast oscillator jitter is neglected, according to the previous considerations.
- An integer frequency ratio is considered:

$$N = \frac{T_{CLK_{FAST}}}{E\{T_{CLK_{RNG}}\}}, \tag{1}$$

where $E\{\cdot\}$ is the expected value operator. It must be observed that this is a worse-case assumption since noninteger frequency ratios produce bit streams

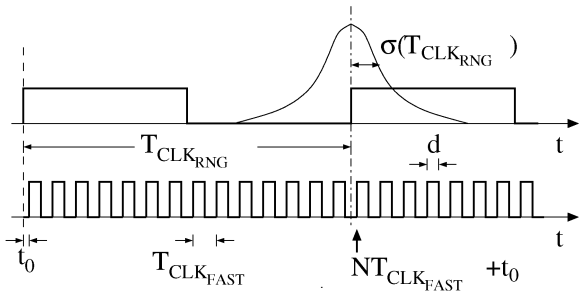

Fig. 2. Oscillator output signals.

which look more random when a randomness test is applied.

- A starting phase shift $t_0 \in [0, T_{CLK_{FAST}})$ is considered.

The transition probability between successive bits is defined as

$$P_t = P\{BIT[i] \neq BIT[i-1]\}, \tag{2}$$

where, for an ideal random sequence, it holds that $P_t = 0.5$. From Fig. 2, the following expression can be carried out:

$$P_t = \sum_{j=-\infty}^{+\infty} \int_{(N+j)T_{CLK_{FAST}}+t_0}^{(N+j+d)T_{CLK_{FAST}}+t_0} p(T_{CLK_{RNG}}) dT_{CLK_{RNG}}, \tag{3}$$

where, $d \in [d_{min}, d_{max}]$ is the fast clock duty cycle and $p(T_{CLK_{RNG}})$ is the jitter probability density function. The above expression can be approximated, limiting the sum to $j \in [-j_{max}, +j_{max}]$, where $j_{max} T_{CLK_{RNG}} \geq 3\sigma\{T_{CLK_{RNG}}\}$ and $\sigma\{T_{CLK_{RNG}}\}$ is the jitter standard deviation.

Finally, introducing the complementary error function, for P_t it holds that

$$P_t = \sum_{j=-j_{max}}^{+j_{max}} \left\{ \frac{1}{2} erfc\left[\frac{jT_{CLK_{FAST}} + t_0}{\sqrt{2}\sigma\{T_{CLK_{RNG}}\}} \right] - \frac{1}{2} erfc\left[\frac{(j+d)T_{CLK_{FAST}} + t_0}{\sqrt{2}\sigma\{T_{CLK_{RNG}}\}} \right] \right\}. \tag{4}$$

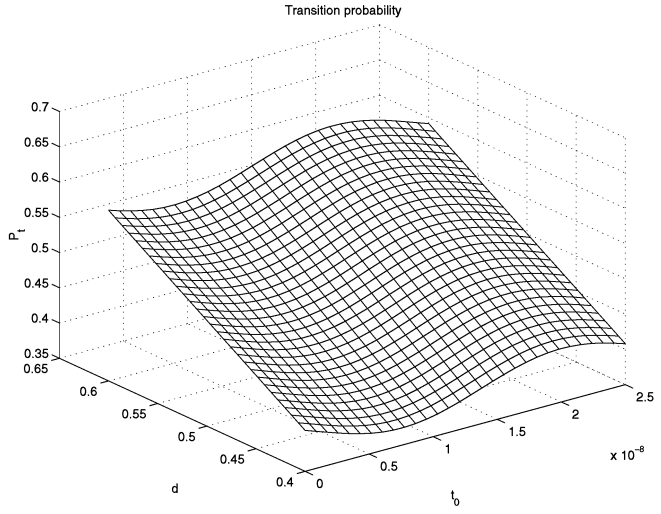

Fig. 3. Bit transition probability P_t.

TABLE 1
Bit Transition Probability P_t versus Fast Clock Period $T_{CLK_{FAST}}$

$T_{CLK_{FAST}}$	$25ns$	$15ns$	$1ns$
$P_t(min)$	0.374	0.399	0.400
$P_t(max)$	0.626	0.601	0.600

From (4), the main RNG's parameters have to be chosen to fulfill the constraint

$$P_t = 0.5(1 \pm \varepsilon), \quad \forall t_0 \in [0, T_{CLK_{FAST}}), \forall d \in [d_{min}, d_{max}],$$

where $[d_{min}, d_{max}]$ is the assumed range for the fast clock duty cycle and ε is the desired probability error.

If $T_{CLK_{FAST}} = 25ns$, $\sigma\{T_{CLK_{RNG}}\} = 10ns$, and $d \in [0.4, 0.6]$, the function $P_t(d, t_0)$ is plotted in Fig. 3 and it results $0.37 \leq P_t \leq 0.63$. The probability values for faster ring oscillator frequencies are reported in Table 1. It can be noted that, for high CLK_{FAST} frequencies, the effect of t_0 becomes negligible and the transition probability P_t approaches the duty cycle d. As a consequence, to obtain a good quality random sequence, a fast and balanced CLK_{FAST} signal is needed.

The low-speed oscillator is based on a triangular wave oscillator [17] where an amplified thermal noise source is added in the loop before the Schmitt trigger, as depicted in Fig. 4. A transconductance amplifier is used to reduce the triangular signal at the charge pump's output, thus increasing the output jitter. In Fig. 5, the amplifier's noisy output signal $V(t)$ is shown: Its period is

$$T_{CLK_{JIT}} = t_1 + t_2, \tag{5}$$

where t_1 and t_2 are independent random variables with the same statistical proprieties, in particular, being

$$V(t) = -\mathrm{V_{TL}} + st + v_n(t), \tag{6}$$

where $v_n(t)$ is the noise process at the amplifier's output and s is the triangular wave slope, it follows:

$$t_1 = \frac{V_{TH} + |V_{TL}| - v_n(t)}{s}. \tag{7}$$

Finally, from (5) and (7), for the CLK_{RNG} signal, it results

$$E\{T_{CLK_{RNG}}\} = \frac{2N_{PRE}}{s}(V_{TH} + |V_{TL}|) \tag{8}$$

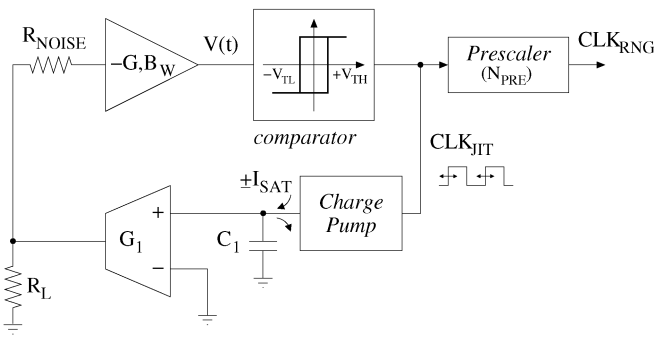

Fig. 4. Triangular wave oscillator.

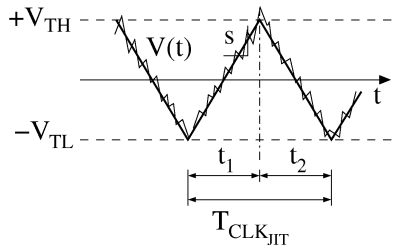

Fig. 5. Noisy triangular wave.

$$\sigma\{T_{CLK_{RNG}}\} = \frac{\sqrt{2N_{PRE}}}{s}\sigma\{v_n\}, \tag{9}$$

where the prescaler factor N_{PRE} has also been taken into account, even if the presented design will assume $N_{PRE} = 1$.

The triangular wave slope s and the white noise rms value $\sigma\{v_n\}$ can be expressed as a function of the circuit parameters in Fig. 4; in particular, it holds

$$s = \pm\frac{I_{SAT}}{C_1}G_1 R_L G \tag{10}$$

$$\sigma\{v_n\} = \sqrt{4kTB_W 2R_{NOISE}G^2}. \tag{11}$$

Using the values reported in Table 2, it results

$$\sigma\{v_n\} = 35mV\ rms,$$
$$E\{T_{CLK_{RNG}}\} \cong 101ns,$$

and

$$\sigma\{T_{CLK_{RNG}}\} \cong 7.2ns,$$

thus obtaining a 10Mbps output random stream with a transition probability $P_t = d$, if a 1GHz fast clock is employed.

TABLE 2
RNG Circuit Parameters

Parameter	Description	Value
R_{NOISE}	Noise resistors	$30k\Omega$
G	Amplifier gain	$45dB$
B_W	Amplifier bandwidth	$\cong$ 40MHz
R_L	OTA load	$\cong 400\Omega$
G_1	OTA gain	$0.08mA/V$
C_1	Charge pump capacitor	$2.3pF$
I_{SAT}	Charge pump output current	$4\mu A$
$V_{TH} + \lvert V_{TL}\rvert$	Comparator hysteresis	$500mV$

3 Circuit Details

The complete circuit schematic of the proposed RNG is depicted in Fig. 6: The triangular wave oscillator has been designed using the parameter values reported in Table 2 and, to minimize the deterministic interference at the noise amplifier's input, two separate power supplies are used for the linear analog blocks and the switching circuits, respectively. Moreover, a signal to switch off the generator is provided to reduce the card consumption when random bits are not needed. The power supplies are also automatically switched off when the output FIFO is full, exploiting the small start-up time featured by the jittered oscillator.

A two-stage CMOS topology has been used for the noise op-amp, with a PMOS input stage in order to maximize the circuit PSRR. The main closed loop op-amp parameters are summarized in Table 3. Note that the output noise is greater than the value carried out from (11) due to the noise contributions of the amplifier itself.

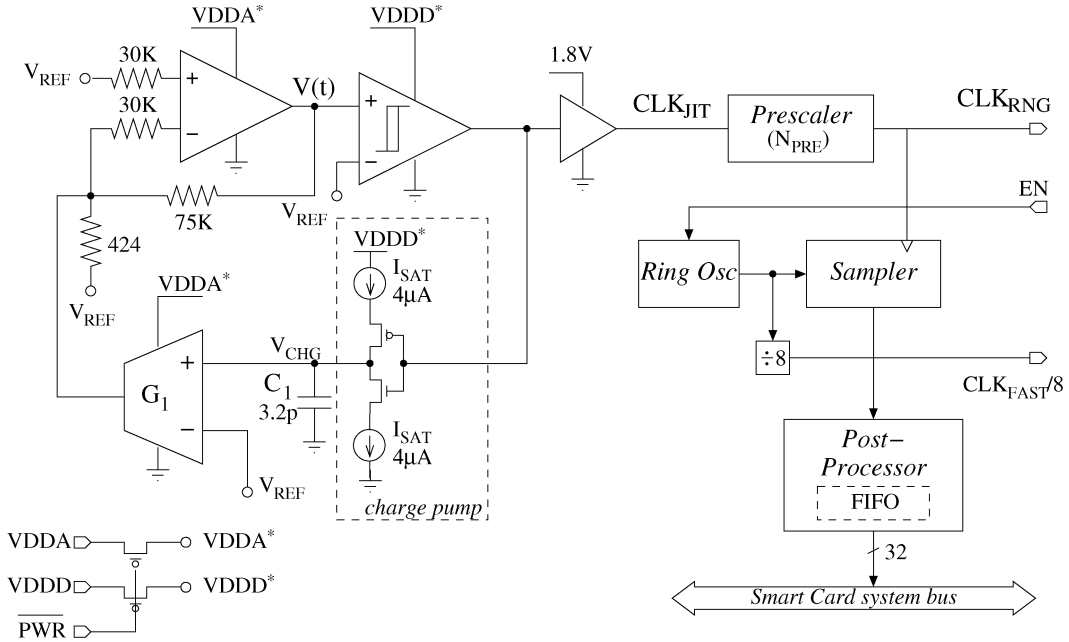

Fig. 6. RNG complete schematic.

TABLE 3
Op-Amp Characteristics

Parameter	Description	Value
G	gain	$45dB$
B_W	bandwidth	$\cong 45$MHz
$PSRR$	—	$40dB$ @1MHz
$\sigma(v_n)$	output noise	$54mV\ rms$

A digital postprocessor has been included in the designed prototype which features a 16×32 bit FIFO as interface between the RNG's asynchronous output and the Smart Card system bus. For testing purposes, the jittered oscillator's output CLK_{RNG} is available on pad. The fast ring oscillator's output CLK_{FAST} can also be observed to measure the actual oscillating frequency.

Finally, in Fig. 7, a back-annotated simulation of the triangular wave oscillator is shown: The V_{CHG} signal (thin line) is the capacitor voltage at the charge pump's output, whereas the thick line represents the comparator's output CLK_{JIT}. The clock period is about $107ns$ and a very short start-up time is achieved (about $450ns$). During the start-up time, the oscillator feedback loop compensates for the amplifier offset, thus solving one of the major issues in this kind of circuits, compared with other oscillator-based RNGs where a noise controlled VCO is exploited [11].

4 Experimental Results

A prototype of the presented RNG was fabricated in a $0.18\mu m$ n-well 1-poly 6-metal CMOS process available from TSMC. The macro-cell area, excluding pads, is $0.016mm^2$ ($184\mu m \times 86\mu m$).

A $3.3V$ supply has been used for the analog circuits, whereas the digital part, including the ring oscillator, the sampler, the postprocessor, and some test logics, has been synthesized on a $1.8V$ digital library available from Artisan Corp. The total macro-cell power consumption is about $2.3mW$.

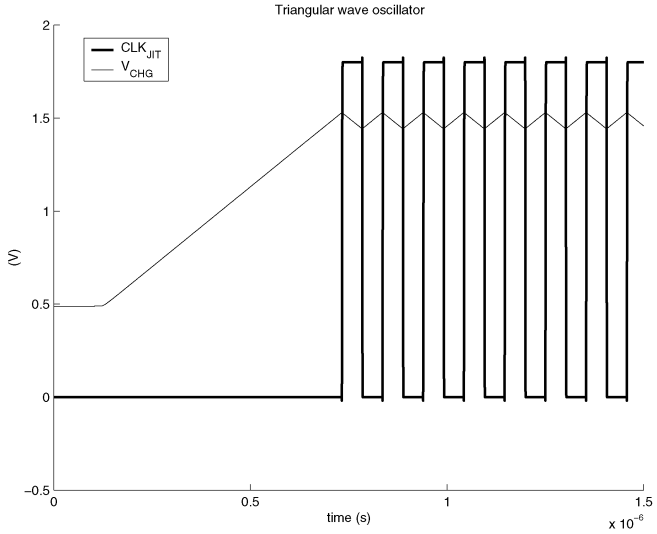

Fig. 7. Back-annotated oscillator simulation.

TABLE 4
Measured Parameters of the Triangular Wave Oscillator Output CLK_{RNG}

Chip #	Mean period (ns)	Jitter value (ns)
1	107.5	9.0
2	100.3	8.3
3	101.0	7.8
4	101.8	8.1
5	110.3	9.8
6	104.7	8.2
7	105.6	8.5
8	108.1	9.2

Mean period, jitter, and duty cycle of the triangular wave oscillator have been measured on several chip samples in order to obtain an estimate of the circuit sensitivity to process variations. The measured values are reported in Table 4, whereas, in Fig. 8, an oscilloscope snapshot is depicted which shows the high jitter level achieved for the CLK_{RNG} signal. From Table 4, it follows that the RNG's output rate is very close to 10Mbps, the rms jitter value is about $9ns$, and the circuit is highly insensitive to process variations. A very good agreement with the back-annotated simulation results is achieved, e.g., a 7 percent maximum error has been observed for the mean period.

Temperature stability has been also verified: Mean period and jitter variations over the 0-70°C temperature range are summarized in Table 5.

The fast CMOS ring oscillator measured parameters are reported in Table 6 for different dies. As shown in Fig. 6, the fast oscillator's output is scaled down for testing purposes: In Table 6, the actual frequency is also shown. The 1 GHz target frequency has been almost matched and, as expected, its jitter level is negligible with respect to the low frequency oscillator.

Long bit streams have been acquired using a digital oscilloscope and a PC data acquisition board to control the chip operation. Using the measured bit streams, for the bit transition probability of the raw sequence $BIT[i]$, it results

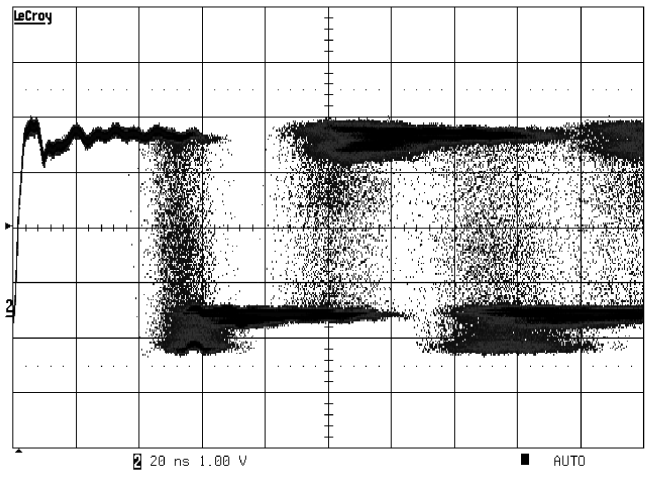

Fig. 8. Jittered oscilator measure (CLK_{JIT}).

TABLE 5
Triangular Wave Oscillator: Temperature Stability

Temperature (°C)	Mean period (ns)	Jitter (ns)	Jitter/Mean period (%)
0	97.6	8.32	8.5
23	106.6	9.04	8.5
70	139.3	14.4	10.3

$$P_t \cong 0.486,$$

very close to the ideal probability value $P_t = 0.5$.

The statistical quality of the generated bit streams has been verified by means of the main randomness tests that can be found in the technical literature [18], [19].

In Table 7, the results of the performed tests on the raw bit streams before the postprocessor are reported. All the tests in the table have been executed over a $1.6 \cdot 10^6$ bit long sequence. For the FIPS tests, that are defined over a 20,000 bit sequence, multiple executions have been performed and the passing rates are also reported in the table.

The applied statistical tests show a substantial random behavior. In order to remove the residual first order correlation, different postprocessing algorithms have been tested [16]. In general, these algorithms can sensibly improve the sequence randomness; in this case, thanks to the high quality of the designed random source, the obtained improvement is negligible.

TABLE 6
Measured Parameters of the Fast Ring Oscillator Output CLK_{FAST}

Chip #	Period $\times 8$ (ns)	Jitter $\times\sqrt{8}$ (ns)	Freq (MHz)
1	8.90	0.10	899
2	8.67	0.09	923
3	8.89	0.09	900
4	8.56	0.09	935

TABLE 7
Test Results before the Postprocessor

Test	Pass low	Pass high	Avg. score	% passed
Mean	-	-	.5001	-
Correlation 1	$-.0158$	.0158	.0287	-
Correlation 2	$-.0158$	.0158	.0016	-
Correlation 3	$-.0158$	.0158	.0007	-
Correlation 4	$-.0158$	.0158	.0001	-
Monobit	9655	10346	9994	100
Poker	1.03	57.4	27.5	100
Runs 1	2267	2733	2371	100
Runs 2	1079	1421	1210	100
Runs 3	502	748	625	100
Runs 4	223	402	319	100
Runs 5	90	223	164	100
Runs 6+	90	223	175	100
Long Runs	1	33	–	100

5 Conclusions

A high-speed truly random number generator suitable to be integrated in a Smart Card microcontroller has been presented. The proposed RNG is based on the oscillator sampling technique and a jittered oscillator with an explicit thermal noise source has been designed in order to improve output rate and statistical quality of the generated bit sequence. A numerical model has been developed for the system which results in an analytical expression for the bit transition probability of the random stream as a function of the main circuit parameters. Using the developed model, a 10Mbps RNG has been designed.

A prototype chip in a $0.18\mu m$ CMOS process has been fabricated and measured. The macro-cell area is $0.016mm^2$ and no external components are employed. Randomness tests applied to the acquired raw bit sequences, before the digital postprocessor, have shown very good random behavior.

Acknowledgments

This work has been carried out in the framework of a cooperation between the University of Rome "La Sapienza" and Gemplus S.A. The authors wish to thank Johannes Bühler from TSMC for his kindly assistance during the design of the prototype.

References

[1] D. Naccache and D. M'Raihi, "Cryptographic Smart Cards," *IEEE Micro*, vol. 16, no. 3, pp. 14-24, June 1996.
[2] A.J. Memezes, P.C. Oorschot, and S.A. Vanstone, *Handbook of Applied Cryptology*. CRC Press, 2001.
[3] W. Rankl and R. Effing, *Smart Card Handbook*, second ed. New York: John Wiley & Sons, 2000.
[4] B. Schneier, *Applied Cryptography*, second ed. New York: John Wiley & Sons, 1996.
[5] J. Walker, "HotBits: Genuine Random Numbers Generated by Radioactive Decay," http://www.fourmilab.ch/hotbits, 2002.
[6] ETSI TR 122 907, "Universal Mobile Telecommunications System (UMTS); Terminal and Smart Card Concepts," ETSI, Sophia Antipolis, 2000.
[7] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," *Advances in Cryptology (Crypto '99)*, M. Wiener, ed., pp. 388-397, 1999.
[8] 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.
[9] V. Bagini and M. Bucci, "A Design of Reliable True Random Number Generator for Cryptographic Applications," *Proc. Workshop Cryptographic Hardware and Embedded Systems (CHES '99)*, pp. 204-218, 1999.
[10] M. Dichtl and N. Janssen, "A High Quality Physical Random Number Generator," *Proc. Sophia Antipolis Forum Microelectronics (SAME 2000)*, pp. 48-53, 2000.

[11] B. Jun and P. Kocher, "The Intel Random Number Generator," Cryptography Research Inc., white paper prepared for Inter Corp., Apr. 1999, http://www.cryptography.com/resources/whitepapers/IntelRNG.pdf.
[12] 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.
[13] 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.
[14] 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.
[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] R.J. Baker, H.W. Li, and D.E. Boyce, *CMOS—Circuit Design, Layout and Simulation.* IEEE Press, 1998.
[18] FIPS 140-1, "Security Requirements for Cryptographic Modules," Nat'l Inst. of Standards and Technology, G.P.O., Washington, D.C., Jan. 1994.
[19] D.E. Knuth, *The Art of Computer Programming,* second ed. Addison-Wesley, 1981.

Marco Bucci received the Laurea degree in electronic engineering from the University of Rome "La Sapienza", Italy, in 1986. He was in the Cryptography Group of Fondazione Ugo Bordoni, Italy, from 1986 to 2000. His activity was focused on hardware and software implementation of cryptographic devices, including multiprecision algorithms, systolic architectures, and fast serial-parallel multipliers. Starting in 1993, he has cooperated with AMTEC, Italy, by designing different RSA coprocessors for high-speed cryptographic applications. Since 2000, he has been with the Rome Crypto Design Center of Gemplus, where he has been involved in projects concerning random number generators, HW countermeasures against DPA attacks, and related design and security evaluation techniques.

Lucia Germani received the master's degree in electronic engineering in 1998 from the University of Rome "La Sapienza". From 1998, she was involved in research activities at Centro Studi Giorgio Barzilai (Electronic Engineering Department, University of Rome "La Sapienza"). In 2000, she joined Gemplus Card International and started to work as a hardware designer at the Rome Crypto Design Center. Her current activities include design, testing, and characterization of Smart Card components like crypto-processors for secure applications.

Raimondo Luzzi (M'94) received the MS degree (with honors) and the PhD degree in electronic engineering from the University of Rome "La Sapienza", Italy, in 1998 and 2003, respectively. From 1998, he was with the Electronic Engineering Dept., University of Rome "La Sapienza", working on cryptographic hardware design. In 2002, he joined Infineon Technologies, Microelectronics Design Center, Graz, Austria, where he is currently with the Security and Chipcard IC's Group. His research interests are in design of mixed-signal circuits and System-On-Chip design techniques, with special emphasis on hardware for cryptographic applications. He is a member of the IEEE.

Alessandro Trifiletti joined the Electronic Engineering Department of the University of Rome "La Sapienza" in 1991 as a research assistant and is currently an assistant professor. His research interests include high-speed circuit design techniques and III-V device modeling.

Mario Varanonuovo (M'00) received the MS degree in electronic engineering from the University of Rome "La Sapienza" in 1999. Since 2000, he has been with the Electronic Engineering Department, University of Rome "La Sapienza", where he has been involved in the design of integrated circuits for cryptographic applications. His research interests include System-On-Chip applications and design of mixed signal integrated circuits. He is a member of the IEEE.