Power analysis of a chaos-based random number generator for cryptographic security

This is the author's version of the article that has been presented at IEEE ISCAS2009
The editorial version of the paper is available at http://dx.doi.org/10.1109/ISCAS.2009.5118398

Power Analysis of a Chaos-Based Random Number Generator for Cryptographic Security

Fabio Pareschi,*† Giuseppe Scotti,‡ Luca Giancane,‡ Riccardo Rovatti,§† Gianluca Setti*† and Alessandro Trifiletti‡
*ENDIF, University of Ferrara - via Saragat, 1 - 44100 Ferrara (ITALY)
†ARCES, University of Bologna - via Toffano,2 - 40125 Bologna (ITALY)
‡Dipartimento di Ingegneria Elettronica, Università di Roma "La Sapienza" - Via Eudossiana 18, 00184 Roma (ITALY)
§DEIS, University of Bologna - viale risorgimento, 2 - 40136 Bologna (ITALY)
email: {fabio.pareschi, gianluca.setti}@unife.it, rrovatti@arces.unibo.it,
{scotti, giancane, trifiletti}@die.uniroma1.it

***Abstract*—In this paper we consider a side-channel attack on a chaos-based Random Number Generator (RNG) based on power consumption analysis. The aim of this attack is to verify if it is possible to retrieve information regarding the internal state of the chaotic system used to generate the random bits. In fact, one of the most common arguments against this kind of RNGs is that, due to the deterministic nature of the chaotic circuit on which they rely, the system cannot be truly unpredictable. Here we analyze the power consumption profile of a chaos-based RNG prototype we designed in 0.35 μm CMOS technology, showing that for the proposed circuit the internal state (and therefore the future evolution) of the system cannot be determined with a side-channel attack based on a power analysis. This property makes the proposed RNG perfectly suitable for high-security cryptographic applications.**

I. Introduction

By definition, a Random Number Generator (RNG) is a circuit capable of producing perfectly *unpredictable* bits, which means that it is impossible to predict its outcome with an accuracy greater than the one given by pure luck. These circuits represent a fundamental primitive in many engineering tasks. For instance they are used in all cryptographic applications where they are of paramount importance in the synthesis of confidential keys. Indeed, it is commonly accepted that, in any cryptographic system, a perfect randomly generated key leads to the highest system security [1].

Testing unpredictability according to its definition is a hard task, even from a theoretical point of view. In common practice, one can consider a generated (and supposed random) bit sequence in order to validate the quality of a RNG, and check it with a statistical test. Roughly speaking, this test analyzes the bit sequence looking for regularities or recurrent patterns. The outcome is the indication of whether the sequence can be considered random, as well as the margin of error of this decision [2].

In this paper we consider a prototype of a RNG designed in $0.35\,\mu\mathrm{m}$ technology employing a *chaotic map* [3], [4] as source of randomness. This prototype has been already presented by authors in [5], where it has been tested using the common statistical tests approach. Here we test the prototype from another point of view: we consider, along with the generated bitstream, the power consumption of the prototype, and verify if this additional information can be used to predict the future evolution of the RNG. This method is similar to the power analysis technique, introduced by Kocher in 1999 [6], to perform side channel attacks on cryptographic devices.

Note that this analysis represents an important issue for any chaos-based random generator. A chaotic system is by definition a *deterministic, non-linear system* with a long-term unpredictability, i.e. its evolution cannot be predicted after a short time interval, whose length decreases as the error in the knowledge of the initial system state increases. Despite this property, a common argument against this architecture is the intrinsic deterministic nature of the system. Actually, if an external observer could gather information on the internal state of the chaotic map (which has to be, of course, inaccessible), a prediction of the short-term evolution of the system is possible. Even if it is possible to theoretically prove that, with the architecture used in the prototype, the generated bitstream does not contain information on the actual state of the chaotic map [7], the possibility of retrieving this information from a side-channel attack has not yet been analyzed.

We show here that a power analysis of the prototype is not useful to obtain information on the internal state of the system, since the current profile of the designed chaotic system is independent of it. This effectively ensures the unpredictability of the system even under a side-channel attack based on power analysis, and it is perfectly suitable for chryptographic applications.

The paper is organized as follows. In section II we describe the architecture of the RNG prototype in order to understand what is the expected current profile. In section III we analyze the RNG power consumption, showing that no relation can be found between the current profile and the internal state of the chaotic map, thus ensuring the effective unpredictability of the generated bitstream. Finally, we draw the conclusions.

II. Architecture of the Designed RNG

The RNG analyzed in this paper has been designed in a $3.3\,\mathrm{V}$ $0.35\,\mu\mathrm{m}$ CMOS technology. A detail microphotograph of it can be seen in Figure 1. The core of this RNG is a *chaotic map*, formally a 1D discrete-time dynamical system whose state evolution is described by:

$$x_k = M\left(x_{k-1}\right) \tag{1}$$

with $M : I \mapsto I$ while the random output bit D_k is given through the quantization function $Q : I \mapsto \{0, 1\}$ from the state of the map:

$$D_k = Q\left(x_{k-1}\right)$$

This is the author's version of the article that has been presented at IEEE ISCAS2009
The editorial version of the paper is available at http://dx.doi.org/10.1109/ISCAS.2009.5118398

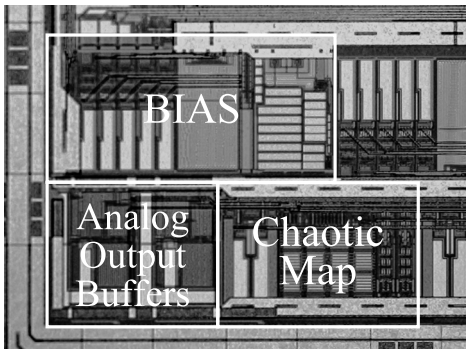

Fig. 1. Microphotograph of the $0.35\,\mu\mathrm{m}$ CMOS prototype (*detail*).

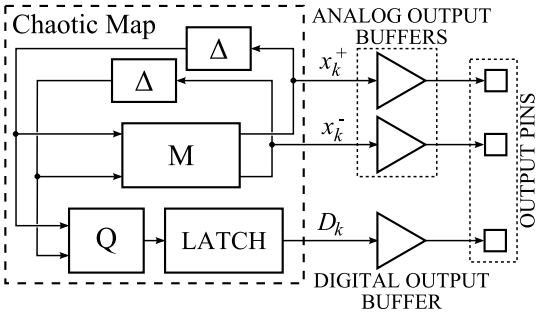

Fig. 2. Basic architecture of the chaos-based RNG prototype. The map state x_k is implemented with the two differential analog voltages x_k^+ and x_k^-, while the random bit is the digital signal D_k.

In the prototype the state x_k of the chaotic map is implemented as a differential voltage ranging in $I = [-1, 1]\,\mathrm{V}$ and the two functions M and Q are respectively:

$$M(x) = \begin{cases} 2x+2 & \text{if } x \le -\frac{1}{2} \\ 2x & \text{if } -\frac{1}{2} < x \le \frac{1}{2} \\ 2x-2 & \text{if } x > \frac{1}{2} \end{cases}$$

$$Q(x) = \begin{cases} 1 & \text{if } -\frac{1}{2} < x \le \frac{1}{2} \\ 0 & \text{elsewhere} \end{cases}$$

Despite the deterministic evolution of the analog state x_k, that is regulated by (1), the succession of the quantized state D_k can be theoretically proved to be effectively a random, unpredictable bitstream. The proof can be found in [7]; here it is enough to recall that the only assumption required is that the initial condition of the system is unknown and randomly drawn according to a *continuous* probability density function (that is verified assuming the initial condition is affected by noise).

A block diagram of the prototype is depicted in Figure 2. The core of the circuit is the chaotic map, implementing both M and Q functions, and the unity delay blocks required to achieve the dynamic behaviour as in (1). It is designed as a fully-differential switched capacitors circuit, a detailed description of which can be found in [5]. Due to testing purposes both the random generated bit D_k and the differential analog chaotic map state x_k are made available to output pins. The buffers used to drive these output pins have to be taken into account when analyzing the power supply current of the circuit, since due to limitation in the standard I/O cells

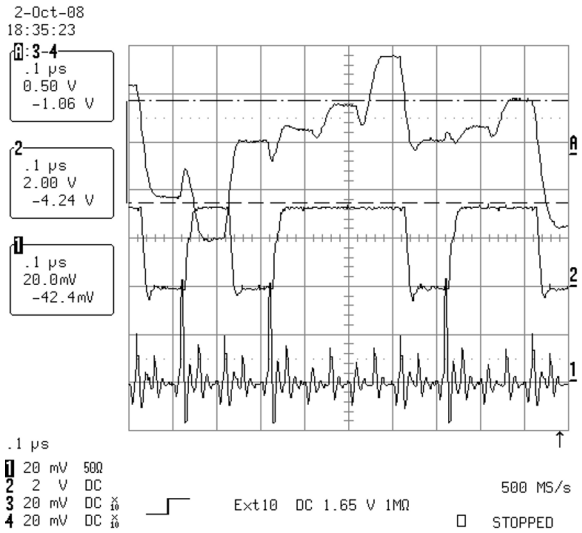

Fig. 3. Prototype measurements. From top to bottom: differential analog internal state of the chaotic map (channel A); generated random bits (channel 2); power supply current (channel 1). The probe used for the the current sensing has a sensitivity of $5\,\mathrm{mV/mA}$.

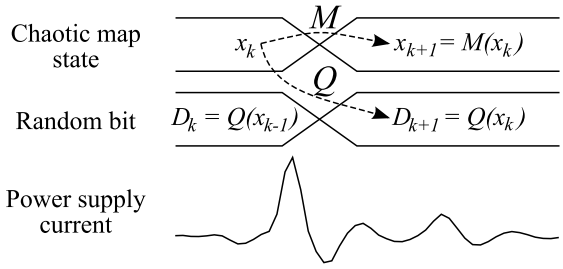

Fig. 4. Typical current profile during a transients.

available for this technology, they share the power supply line with the core circuit.

An example of waveforms generated by the prototype can be seen in Figure 3, showing at the same time the state of the chaotic map, the generated random bit and the current profile on the power supply line. Note that the state of the chaotic map is shown along with the two thresholds of the Q function: when the state is inbetween the threshold, the random bit at the next time step is high, while when it is outside, the next random bit is low. Note also that, since the probe used for sensing the power supply current requires an AC coupling, we are observing only the dynamic power, i.e. the variations with respect to the mean value of the current. Peaks in the current profile are present in correspondence to each clock edge (not shown in the figure); highest peaks can be found when the random output bit has a transition from low to high.

To understand what is the expected current profile, let us consider the diagram of Figure 4. At the rising edge of the clock the analog state of the chaotic map switches with a short transient from the value x_k to the value $x_{k+1} = M(x_k)$, and the output random bit from $D_k = Q(x_{k-1})$ to $D_{k+1} = Q(x_k)$. During these transients, we can observe a peak in the power supply current due to the contribution of these three subcircuits: *a*) the chaotic map; *b*) the analog output buffers;

This is the author's version of the article that has been presented at IEEE ISCAS2009
The editorial version of the paper is available at http://dx.doi.org/10.1109/ISCAS.2009.5118398

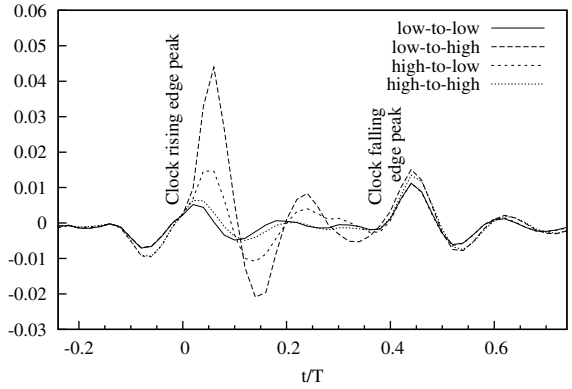

Fig. 5. Example or the four kinds of dynamic current profile, separated according to the random output bit transition.

and *c*) the output digital buffer. Generally, if the chaotic map gives the highest contribution to static power supply (it is designed only with class-A amplifiers), its contribution to the dynamic power is not particularly high. The same behavior can be observed for the analog buffers, while the digital buffer requires only dynamical power. Furthermore, due to the large capacity of the output pins, and to the single-ended configuration, this power is expected to be quite high only when observing a low-to-high transition. This is exactly what we can observe in Figure 3.

III. Analysis of the power supply current

As observed in Section II, due to I/O cells constraints we have a dominant contribution to the dynamic current from the output random bit buffer (i.e. the digital buffer). Consequently, we can expect four kinds of current profiles, according to the random bit transition, which have been shown in Figure 5. Two major peaks can be observed, the first one corresponding to the rising edge of the clock, and the second one to the falling edge. Additionally, if we compare the two profiles associated with the low-to-low and high-to-high transition (i.e. the cases where there is no transition in the output random bit), we can see they are very similar.

We can verify from prototype measurements that the dynamic current profile is not directly related to the analog state of the chaotic map, but only to the generated random bit. More precisely, and using the same symbols of Figure 4, i.e. indicating respectively with x_k and x_{k+1} (D_k and D_{k+1}) the chaotic map state (random output bit) before and after the transient, the current profile during the transient does not depends directly on x_k and x_{k+1} but only on D_k and D_{k+1}. To prove this, we have to isolate the contribution given by the $D_k \rightarrow D_{k+1}$ transition considering separately the four cases corresponding to the four transitions considered in Figure 5. For all these cases, we have considered a scatter plot where the internal state of the chaotic map measured from a long acquisition is compared with the observed current profile. Actually, to this purpose we need a numeric indicator of the current profile, which has been chosen as the charge required by the transient in a period T[8]:

$$\Delta q_k = \int_0^T i_D(t - kT)dt$$

where i_D is the measured dynamic current, so Δq_k is actually a differential charge.

In order to check if any relation exists with respect to the the state of the map before the transition (x_k) and after the transition (x_{k+1}), we have drawn in each figure two scatter plots, one comparing the current profile indicator Δq_k with the state x_k and one with x_{k+1}. These scatter plots can be seen in Figure 6. Due to the limited space available, we have included only the Figures corresponding to the cases of a high-to-low transition (Figure 6-a) and an unchanged high bit value (the high-to-high case, Figure 6-b). Note that in the first case we know that $D_{k+1} = Q(x_k) = 0$, so x_k has to be in the range $-1 < x_k < -\frac{1}{2}$ or $\frac{1}{2} < x_k < 1$; in the second case it is $D_{k+1} = Q(x_k) = 1$, i.e. x_k is compelled in the range $-\frac{1}{2} < x_k < \frac{1}{2}$. Conversely, in both cases, x_{k+1} can span in the whole range $[-1, 1]$.

In all plots, the charge Δq_k and the map states x_k and x_{k+1} are apparently randomly distributed in their given range. This means that no relation between the current profile and the state of the chaotic map exists, and from the observation of the current profile it is not possible to retrieve any useful information on x_k or on x_{k+1}.

As an additional test, it may be interesting checking if a relation exists between the observed current profile and the successive random bit D_{k+2}. This test effectively plays the role of the prediction of the following bit given the random bitstream and the current profile.

To get an intuitive idea, let us refer to Figure 7, showing the two distributions of the measured charge Δq_k, which has been separated in two groups according to the value of D_{k+2}. Roughly speaking, given an observed transition $D_k \rightarrow D_{k+1}$ (more precisely, high-to-low transition for the case of Figure 7-a, and a constant high value for the case of Figure 7-b, exactly as in Figure 6) we want to know if the group of Δq_k giving rise to $D_{k+2} = 0$ is distributed as the group of Δq_k giving rise to $D_{k+2} = 1$.

Obviously, if these two distributions were defined in two different (or slightly overlapping) regions it would be possible to determine with a high probability if the successive random bit D_{k+2} would be high or low from the measure of Δq_k. On the contrary, as in the case of Figure 7, from two distributions almost superimposing it would not be possible to predict if D_{k+2} would be high or low with an accuracy much greater then the one given by pure chance. This means, by definition, that D_{k+2} is unpredictable.

To formally obtain a numerical measure of the similarity of the two obtained distributions, and therefore of the unpredictability of D_{k+2}, we can use the concept of entropy and mutual information.

While the *entropy* of a random variable X is defined as the average information provided by each of its realization, the average *mutual information* between two random variables X and Y is defined as the average information provided about a realization of X by the occurrence of the realization of Y [9]. Mathematically, given a discrete random variable X with possible values $x_1, x_2, \ldots$ and associated probabilities $P_X(x_1), P_X(x_2), \ldots$, its entropy $H(X)$, measured in bit, is defined as

$$H(X) = -\sum_k P_X(x_k) \log_2 P_X(x_k)$$

This is the author's version of the article that has been presented at IEEE ISCAS2009
The editorial version of the paper is available at http://dx.doi.org/10.1109/ISCAS.2009.5118398

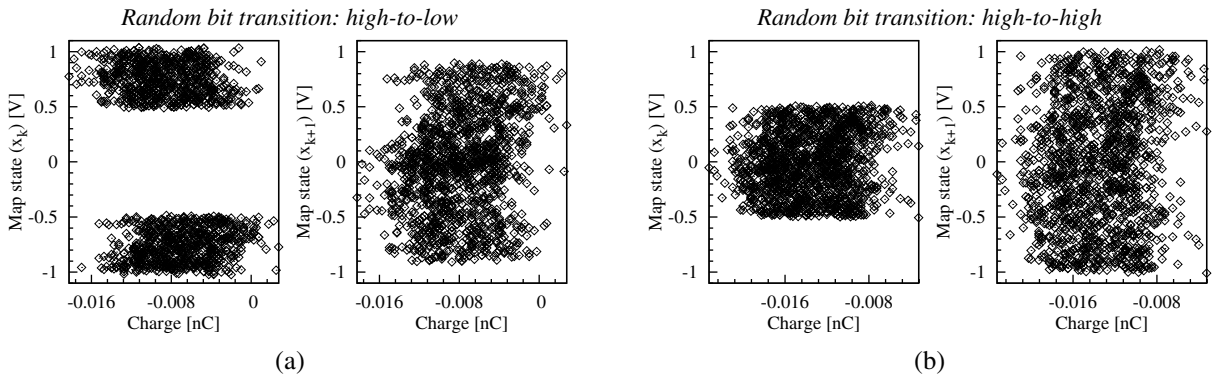

Fig. 6. Scatter plot of the charge Δq_k required during the transient compared with the state of the chaotic map before (x_k) and after (x_{k+1}) the transient, in the case of a high-to-low random bit transition (case a) and of an unchanged high random bit (case b, referred to as high-to-high).

while the average mutual information $I(X;Y)$ between the two discrete random variables X and Y is

$$I(X;Y) = \sum_k \sum_j P_{XY}(x_k, y_j) \log_2 \frac{P_{XY}(x_k, y_j)}{P_X(x_k) P_Y(y_j)}$$

where P_Y is the probability distribution of Y, and P_{XY} is the joint probability distribution of X and Y.

If we consider D_{k+2} as the random variable X, and Δq_k as Y (actually, since Δq_k is a continuous random variable, we need to discretize it in a limited number of bins in order to apply the above definition, as already done in Figure 7), $I(X;Y)$ is the quantity of average information about D_{k+2} we can get from the observation of Δq_k, i.e. the indicator of how well Δq_k can be used to predict D_{k+2}. Note that, according to this notation, the plots of Figure 7 represent the two conditional probability densities $P_{Y|X}$, with $X = 0$ and $X = 1$.

Assuming X and Y are unrelated, $I(X;Y) = 0$; if instead X and Y are completely dependent, $I(X;Y) = H(X) = 1\,\text{bit}$. In the two cases of the example of Figure 7 the mutual information is measured in $I = 0.03\,\text{bits}$ for the high-to-low transition case, and $I = 0.021\,\text{bits}$ for the high constant value case. Very similar values are computed for the cases not shown here. These very low values clearly show the lack of mutual information, i.e. the impossibility to retrieve information on D_{k+2} from the observation of Δq_k.

IV. Conclusion

In this paper we have considered a power analysis on a prototype of a chaos-based RNG designed in $0.35\,\mu\text{m}$ CMOS technology. Despite the fact that the RNG is based on a chaotic, thus deterministic, system, where an observer gaining access to information on the internal state of the system could predict the short-term evolution of the RNG, we show in this paper that it is not possible to get information on the internal state either from the observation of the generated bitstrem, or from a side-channel attack based on power analysis. The power supply current trace is shown to depend only on the random digital bit, principally for the presence of the buffer driving the chip pad, while a dependency between the current trace and the internal state of the chaotic map cannot be observed. This makes the proposed RNG a high-security generator, perfectly suitable for any cryptographic application.

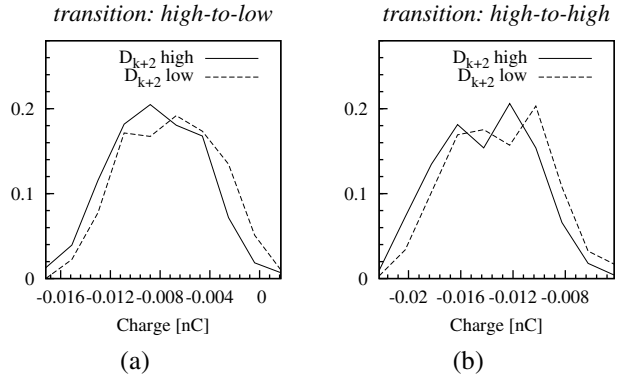

Fig. 7. Conditional distribution density of the charge Δq_k during a transient, assuming the successive random bit D_{k+2} is high (continuous line) or low (dotted line), in the case of a high-to-low random bit transition (case a) and of an unchanged high random bit (case b, referred to as high-to-high). The distributions are obtained with a 10 bins histogram of frequencies.

References

[1] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.

[2] National Institute for Standards and Technology (NIST), "A statistical test suite for random and pseudorandom number generators for cryptographic applications", Special publication 800-22, May 2001.

[3] A. Lasota, and M. C. Mackey, *Chaos, Fractals, and Noise. Stochastic Aspects of Dynamics*, Springer-Verlag, 1994.

[4] G. Setti, G. Mazzini, R. Rovatti, and S. Callegari, "Statistical modeling of discrete time chaotic processes: Basic finite dimensional tools and applications", in *Proceedings of IEEE*, vol. 90, no. 5, pp. 662–690, May 2002.

[5] F. Pareschi, G. Setti and R. Rovatti, "A Fast Chaos-based True Random Number Generator for Cryptographic Applications", in *Proceedings of ESSCIRC2006*, pp 130–133. Montreux, Switzerland, Sep. 2006.

[6] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis", in *Advances in Cryptology-Proc. 19th Ann. Int'l Cryptology Conf.* (CRYPTO '99), pp. 388-397, 1999.

[7] S. Callegari, R. Rovatti, and G. Setti, "Embeddable ADC-Based True Random Number Generator for Cryptographic Applications Exploiting Nonlinear Signal Processing and Chaos", in *IEEE Transaction on Signal Processing*, vol. 53, no. 2, pp. 793–805, Feb. 2005.

[8] K. Tiri, M. Akmal, and I. Verbauwhede, "A Dynamic and Differential CMOS Logic with Signal Independent Power Consumption to Withstand Differential Power Analysis on Smart Cards", in *Proc. of European Solid-State Circuits Conf*, pp 403–406, Florence, Sept. 2002.

[9] R. G. Gallager, *Information theory and reliable communication*. Wiley and Sons, 1968.