A Design for a Physical RNG with Robust Entropy Estimators

Wolfgang Killmann[1] and Werner Schindler[2]

[1] T-Systems ISS GmbH
Rabinstr. 8
53111 Bonn, Germany
Wolfgang.Killmann@t-systems.com
[2] Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185–189
53175 Bonn, Germany
Werner.Schindler@bsi.bund.de

Abstract. We briefly address general aspects that reliable security evaluations of physical RNGs should consider. Then we discuss an efficient RNG design that is based on a pair of noisy diodes. The main contribution of this paper is the formulation and the analysis of the corresponding stochastic model which interestingly also fits to other RNG designs. We prove a theorem that provides tight lower bounds for the entropy per random bit, and we apply our results to a prototype of a particular physical RNG.

Keywords: Physical RNG, stochastic model, entropy.

1 Introduction

Many cryptographic mechanisms require random numbers, e.g. as session keys, signature parameters, ephemeral keys (DSA, ECDSA), zero-knowledge protocols, challenge response-protocols, nonces. Inappropriate RNGs may allow to break principally strong cryptosystems, e.g. if an adversary is able to determine session keys. *Ideal RNGs* generate random numbers that are uniformly distributed on their range and independent. An ideal RNG, however, is a mathematical construction (lastly a fiction). Following [11] (cf. [21] for further explanations) 'real-world' RNGs can be divided into two classes, which contain the *true RNGs* (TRNGs) and the *deterministic RNGs* (DRNGs; aka pseudo-random number generators), respectively. The TRNGs fall into two subclasses: *Physical TRNGs* use non-deterministic effects of electronic circuits (e.g. shot noise from Zener diodes, inherent semiconductor thermal noise, free running oscillators) or physical experiments (e.g., time between emissions of radioactive decay, quantum photon effects). *Non-physical non-deterministic RNGs* exploit non-deterministic events (e.g., system time, hard disk seek time, RAM content, user interaction). So-called *hybrid RNGs* combine design elements from both, TRNGs and DRNGs.

E. Oswald and P. Rohatgi (Eds.): CHES 2008, LNCS 5154, pp. 146–163, 2008.

Unlike for deterministic RNGs it seems hardly possible to specify approved designs for physical RNGs (in a strict sense) since security-relevant properties do not only depend on the generic design but also on its implementation. A designer of a physical RNG is faced with two challenges. At first he has to develop an appropriate design, and then he has to implement it carefully. The second task may be even more difficult, namely providing evidence that the generic RNG design and its implementation are indeed appropriate.

In the last years several designs of physical RNGs have been proposed [4, 5, 6, 7, 9] etc., and several evaluation guidances and standards were developed and became effective [1, 2, 11, 13, 17]. These documents define properties that strong RNGs should fulfil, and the evaluation guidances explain how these criteria shall be verfied. A comprehensive treatment of evaluation aspects for physical RNGs are given in [22].

In Section 2 we briefly address central aspects and goals that reliable security evaluations of physical RNGs should consider. In Section 3 we discuss an RNG design that exploits a pair of noisy diodes. Section 4 contains the main contribution of our paper. We formulate and analyze a stochastic model that describes this design and, interestingly, also fits to further RNG designs. In particular, we prove a theorem that allows to quantify a tight lower bound for the average entropy per random bit. We apply our results to a particular physical RNG where we derive lower entropy bounds per random bit that are very close to 1. Finally we explain a generic online test scheme that is tailored to RNG designs which belong to the analyzed stochastic model.

2 Security Evaluation of Physical RNGs: Fundamental Aspects

In this section we address central aspects that are relevant for security evaluations of physical RNGs. For a comprehensive treatment of this matter we refer the interested reader to [21, 22, 19].

2.1 Entropy

With regard to Section 4 we extend the definition of Shannon entropy to random variables with infinite range. More precisely, to a random variable X that assumes values in a countable (finite or infinite) set Ω (e.g. $\Omega = \mathbb{N}_0$) we assign the term

$$H(X) := -\sum_{\omega \in \Omega} \mathrm{Prob}(X = \omega) \log_2(\mathrm{Prob}(X = \omega)). \tag{1}$$

As usual, we set $0 \cdot \log_2(0) := 0$. Following the common convention we denote the Shannon entropy briefly as 'entropy' in the remainder.

Remark 1. (i) We point out that $H(X) \in [0, \infty]$ where $H(X) = \infty$ is possible for infinite Ω. The 'auxiliary' random variables $V_{(s')}$, which will be relevant in Section 4, yet have finite entropy for any $s' \in (0, \infty)$ (cf. [20], Lemma 2(ii)).

(ii) Random numbers that are generated by physical RNGs can usually be modelled by stationary stochastic processes (cf. Sect. 4). At least the internal random numbers (cf. Subsect. 2.2) typically assume values in $\Omega = \{0, 1\}$, and for all cases of practical relevance the Shannon entropy per internal random bit should be close to 1. Hence the Shannon entropy provides a sound estimate for the average guessing workload, justifying the use of the Shannon entropy for physical RNGs in place of the more conservative min-entropy. For physical RNGs it is usually much easier to compute the Shannon entropy than the min-entropy (cf. [21], Subsect. 5.2, for a more comprehensive treatment of this matter). We mention that it may be necessary to apply the min-entropy in place of the Shannon entropy in specific guessing problems with very imbalanced probability distributions (cf. [15]).

2.2 Central Definitions and Goals of a Security Evaluation

The core of a physical RNG is its *noise source*, which usually generates a time-continuous analog signal that is digitized after uniform time intervals. The digitized values are called *das random numbers* where 'das' abbreviates *digital analog signal*. The das-random numbers may be algorithmically postprocessed, giving the so-called *internal random numbers*. Algorithmic postprocessing may increase the entropy per bit, but only at cost of performance (data compression). If the entropy of the das-random numbers is sufficiently large the algorithmic postprocessing may be saved in favour of higher throughput. Online and tot tests shall detect non-tolerable weaknesses while the RNG is in operation. Upon external request the RNG outputs *external random numbers*.

The main part of a security evaluation considers the generic design and its implementation. The central goal is to quantify (at least a lower bound for) the entropy per random bit. Unfortunately, entropy cannot be measured as voltage or temperature. Instead, entropy is a property of random variables and not of observed realizations (here: random numbers). In particular, entropy cannot be guaranteed by passing a collection of statistical blackbox tests [14, 16] since typically even weak pseudorandom sequences pass these tests [19, 21, 22]. To quantify entropy one has to study the distribution of the random numbers, or more precisely, the distribution of the underlying random variables.

Definition 1. *Random variables are denoted with capital letters.* Realizations *of these random variables, i.e. values that are assumed by these random variables, are denoted by the respective small letters. For instance, the das random numbers* $r_1, r_2, \ldots$ *are interpreted as realizations of random variables* $R_1, R_2, \ldots$. *We denote the internal random numbers and the underlying random variables by* $y_1, y_2, \ldots$ *and* $Y_1, Y_2, \ldots$, *respectively.*

External random numbers are not under control of the RNG designer. Since the external random numbers are usually concatenations of the internal random numbers it is natural to focus on the *conditional entropy*

$$H(Y_{n+1} \mid Y_1 = y_1, \ldots, Y_n = y_n) \tag{2}$$

which corresponds to the real-life situation that an adversary knows a subsequence $y_1, y_2, \ldots, y_n$ of internal random numbers, e.g. due to openly transmitted challenges or session keys which the adversary received legitimately.

The random variables $R_1, R_2, \ldots$ describe the stochastic behaviour of the das random numbers. Their distribution clearly depends on the noise source and the digitization mechanism. Usually, it is not feasible to determine these distributions exactly. At least in a strict sense the exact distribution depends on the characteristics of the components of the particular noise source, and these characteristics may differ to some extent even for RNGs from the same production series. A sound security evaluation of a physical RNG should be based on a *stochastic model*.

Stochastic Model. Ideally, the stochastic model comprises a *family of distributions* that contains the true distribution of the internal random numbers. At least, the stochastic model should specify a family of probability distributions that contains the distribution of the das-random numbers or even merely of 'auxiliary' random variables *provided that these random variables enable the verification of a lower entropy bound for the internal random numbers*. We follow this approach in Sect. 4, for instance.

Example 1. (Repeated tossing of a single coin) Since coins have no memory it is reasonable to assume that the random variables R_j are independent and binomially $B(1,p)$-distributed with unknown parameter $p \in [0,1]$, defining a one-parameter family of probability distributions. Given a particular coin the parameter p can be estimated by tossing the coin a large number of times. Substituting the gained estimate $\widetilde{p}$ into the entropy formula yields an estimate for the entropy. The entropy of the internal random numbers depends on p and the algorithmic postprocessing (if there is any).

For 'real life' RNGs the stochastic model is usually more complicated than in Example 1, often depending on several parameters. For most RNG designs it is reasonable to assume that the sequence $R_1, R_2, \ldots$ is stationary (i.e. time-invariant; Definition 2), at least within time periods that are large compared to the output rate. Drifts of process parameters within the life cycle of the RNG (e.g. due to ageing effects) are not problematic if the distribution remains in the acceptable part of the specified class of distributions. In a first step we are interested in

$$H(R_{n+1} \mid R_1 = r_1, \ldots, R_n = r_n) \tag{3}$$

for any history $r_1, \ldots, r_n$, or at least in the average conditional entropy

$$H(R_{n+1} \mid R_1, \ldots, R_n). \tag{4}$$

For dependent random variables the calculation of (4) is in general easier than (3). At least if (4) is too small a suitable (data-compressing) postprocessing algorithm should be applied to the das random numbers that increases the average entropy per bit ([22], Sect. 5). (Of course, even if not necessarily needed, a

strong cryptographic postprocessing algorithm with memeory may serve as an additional security anchor.)

Due to tolerances of components, ageing effects, a total breakdown of the noise source or (depending on the conditions of use) maybe active attacks the RNG may output considerably weaker random numbers than the RNG prototypes which were investigated in the lab. Online tests and tot tests ('total failure test') shall detect non-tolerable weaknesses while the RNG is in operation. Unfortunately, there do not exist statistical tests that are universally strong for any RNG design. Instead, these tests should be tailored to the stochastic model of the das random numbers. The statistical tests may be supported by physical sensors. The second task of a security evaluation is thus to verify the effectiveness of the online and tot tests and the consequence of noise alarms [18, 19, 22]. We will briefly address relevant aspects in Section 6.

Remark 2. A reasonable stochastic model is the core of any CC (Common Criteria) evaluation with regard to the evaluation guidance AIS 31 [2, 13], which has been effective in Germany since 2001. We point out that besides physical RNGs with cryptographic postprocessing the international ISO norm [11] also permits physical RNGs without cryptographic postprocessing provided that a sound stochastic model confirms that the random numbers have enough entropy and that effective online tests are applied.

3 An RNG Design Based on Two Noisy Diodes

Figure 1 illustrates an RNG design that exploits two identical noisy diodes. (E.g.) Zener diodes have a reverse avalanched effect (depending on the diode type 3 - 4 Volt or about 10 V) and generate more than 1 mV noisy voltage with a frequency of about 10 MHz. The outlets of both diodes provide symmetrical input to an operational amplifier that amplifies the difference of the voltages. We point out that, depending on the implementation, the device and the conditions of use, a design with only one noisy diode may be more vulnerable to manipulations by active adversaries, e.g. by external electromagnetic fields. The circuit of the AC coupling, the negative feedback for the operational amplifier, the stabilizing mechanism for the power supply or compensating effects of temperature are omitted in the graphic. The output of the operational amplifier (with very high amplification rate) is fed into a Schmitt trigger. The mean voltage of the amplifier output signal is about the middle of the two threshold values of the Schmitt trigger. Due to the steep edges of the input and usage of the 0-1-upcrossings only the hysteresis effect should be negligible. Moreover, the proposed design only exploits 0-1-crossings. The output signal of the Schmitt trigger consists of zeros ('low') and ones ('high'). The time lengths of these signals is random.

Each 0-1 crossing (up-crossing) within the Schmitt trigger clocks an intermediate flip-flop. This flip-flop inverts the D-input of a second (final) flip-flop, which is latched by a clock after constant time intervals. The number of 0-1-crossings within the n^{th} clock cycle gives the das random number r_n. Hence

$y_{n+1} = y_n \oplus r_{n+1} (\mathrm{mod}\, 2)$ where y_n and y_{n+1} denote the internal random numbers in Step n and $n+1$, respectively. (We mention that more efficient algorithmic postprocessing algorithms than the addition (mod 2) may exist but this is outside the scope of this paper.)

Unlike for related designs that exploit both 0-1- and 1-0-crossings it is irrelevant whether the intervals between 0-1- and 1-0-crossings and the intervals between 1-0- and 0-1-crossings are identically distributed. This feature increases robustness at cost of halving the output rate.

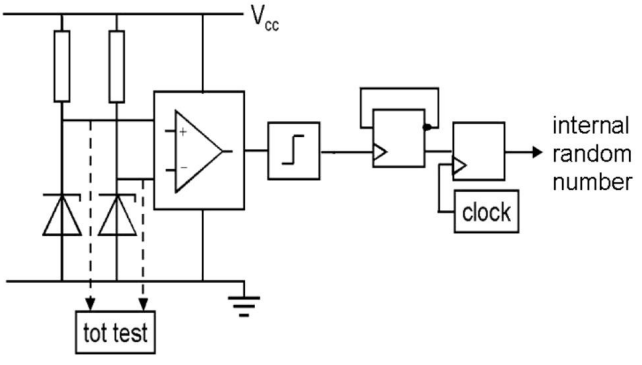

Fig. 1. RNG with two noisy diodes: generic design

The uncertainty on the number of switchings of the Schmitt trigger per time interval is crucial for the entropy of the random numbers. Hence the ratio beteen the cycle length of the clock and the average length between two consecutive 0-1-crossings should not be selected too small. If the distribution of the interval lengths changes considerably, causing a smaller or larger number of switchings within the particular clock cycles, this may have significant influence on the entropy per output bit. Online and tot test should detect such behaviour (cf. Subsect. 6). The tot test may separately check the generation of the noisy voltage for each diode in order to detect a total breakdown or abnormality of the noise.

4 Formulation and Analysis of the Stochastic Model

In this section we formulate and analyze a stochastic model for the RNG design discussed in the previous section. Interestingly, the same stochastic model fits to to other RNG designs as well (cf. Remark 3(ii), (iii)). Theorem 1 collects the main results.

In the following we assume that the analogue part of the noise source is in equilibrium state (since a sufficient amount of time has passed since the start of the RNG; a fraction of a second should suffice). We begin with the analysis of the das random numbers $r_0, r_1, \ldots$ at time $t = 0$. The internal random numbers $y_1, y_2, \ldots$ are latched at equidistant times $s_1 := s, \ldots, s_j := js, \ldots$ where $s > 0$

denotes the cycle length of the clock that latches the final flip-flop (cf. Fig. 1). Recall that the das random number r_n denotes the number of 0-1-switchings of the Schmitt trigger within the time interval $I_n := (s_{n-1}, s_n] = ((n-1)s, ns]$. Clearly

$$y_n \equiv y_{n-1} + r_n \equiv y_0 + r_1 + \cdots + r_n (\mathrm{mod} 2) \quad \text{for } n \geq 1 \tag{5}$$

where y_0 denotes the internal random number at time $t = 0$. Our goal is to determine a lower bound for

$$H(R_{n+1} \mid R_1, \ldots, R_n) \quad \text{and finally for} \quad H(Y_{n+1} \mid Y_0, Y_1, \ldots, Y_n), \tag{6}$$

the average conditional entropy per das-random number, resp. the average conditional entropy per internal random number. Recall that the second formula corresponds to the real-world situation where an adversary knows several internal random numbers $y_0, y_1, y_2, \ldots, y_n$ (cf. Sect. 2). Since the algorithmic post-processing is very elementary results on the das random numbers can directly be transferred to the internal random numbers.

Definition 2. *As usually, iid stands for 'independent and identically distributed'. A sequence of random variables $X_1, X_2, \ldots$ or $\ldots, X_{-1}, X_0, X_1, \ldots$ is called* (strictly) stationary *if for each integer $r \geq 1$ the distribution of $(X_{m+1}, \ldots, X_{m+r})$ does not depend on the shift parameter m. The* generalized variance *of the sequence $X_1, X_2, \ldots$ is defined as*

$$\sigma^2 = \mathrm{Var}(X_1) + 2 \sum_{i=2}^{\infty} E\left((X_1 - \mu)(X_i - \mu)\right). \tag{7}$$

The sequence $X_1, X_2, \ldots$ is called q-dependent *if the vectors $(X_a, \ldots, X_b)$ and $(X_c, \ldots, X_d)$ are independent whenever $c - b > q$.*

As usually, $N(\mu, \sigma^2)$ denotes a normal distribution with mean μ and variance σ^2. The cumulative distribution function of the standard normal distribution $N(0,1)$ is denoted with Φ, i.e. $\Phi(x) = \int_{-\infty}^{x} e^{-t^2/2}\, dt/\sqrt{2\pi}$ for $x \in \mathbb{R}$.

Stochastic Model. We interpret the lengths $t_1, t_2, \ldots$ of the time intervals between consecutive 0-1-switchings as realizations of a q-dependent stationary stochastic process $T_1, T_2, \ldots$. We set $\mu := E(T_1)$ and $\sigma_T^2 := \mathrm{Var}(T_1)$ while the generalized variance of $T_1, T_2, \ldots$ simplifies to

$$\sigma^2 = \sigma_T^2 + 2 \sum_{i=2}^{q+1} E\left((T_1 - \mu)(T_i - \mu)\right) \tag{8}$$

We assume $\sigma_T^2 > 0$ (otherwise the das-random numbers were deterministic), $E(|T_j|^3) < \infty$ (needed for the proof of Lemma 2(iii); cf. also Remark 3(iii)) and $\mathrm{Prob}(T_1 = 0) = 0$.

The term z_n denotes the index of the first 0-1-switching that follows after time $s_n = ns$ (i.e., when the clock latches the n^{th} time) while $w_n := t_{z_n} - s_n$. That is, w_n equals the time span from s_n to the next 0-1-switching. In particular,

$w_0 + t_1 + \cdots + t_{z_n-1} \le s_n < w_0 + t_1 + \cdots + t_{z_n}$. Recall that the stochastic model of an RNG shall enable to determine (at least a lower bound for) the conditional entropy $H(Y_{n+1} \mid Y_0, \ldots, Y_n)$. This defines our central goal.

More abstract, the corresponding random variables can be described as follows:

$$T_1, T_2, \ldots \quad \text{are stationary} \tag{9}$$

$$R_n := Z_n - Z_{n-1} \quad \text{with} \tag{10}$$

$$Z_n := min_{m \in \mathbb{N}}\{W_0 + T_1 + T_2 + \ldots + T_m > s_n\} \tag{11}$$

Remark 3. (i) Relations (9) to (11) remain valid if we substitute the two noisy diodes by a single noisy diode.
(ii) We note that (9) to (11) also fits to a RNG design, which was introduced in [23] and later analyzed in [8,20]. This noise source consists of two independent ring oscillators. To simplify analysis we assumed $W_0 = 0$ in [20]. Since the ratios $(s_n - s_{n-1})/\mu$ and thus the das random numbers $r_1, r_2, \ldots$ were extremely large this simplification had little impact.
(iii) The assumption that the T_j are q-dependent may be relaxed as long as a version of the central limit theorem for dependent random variables remains valid (cf. Lemma 2(iii)).
(iv) Due to the nature of shot noise one may assume that q is very small, presumably $q \le 1$ (cf. Sect. 5).
(v) In our context s should be selected considerably larger than μ so that at least one 0-1-switching should occur in each time interval $(sn, s(n+1)]$ with overwhelming probability. Then z_n equals the index of the first 0-1-switching within this interval.

With regard to Remark 3(i), (ii) it should be profitable to study the system (9) to (11) under general (weak) assumptions as well as for specific conditions on the distribution of the T_j (e.g., for iid or Markovian T_j). Note, however, that although (9) to (11) fit to several RNG designs the distributions of the random variables $T_1, T_2, \ldots$ and, consequently, the distribution of $R_1, R_2, \ldots$ and $Y_1, Y_2, \ldots$ may be very different. Lemma 1 below considers the 'transfer' of the stationarity property.

Lemma 1. *(Stationarity Lemma) Let* $\ldots, T'_{-1}, T'_0, T'_1, \ldots$ *denote a doubly infinite sequence of stationary random variables with* $\mathrm{Prob}(T'_j \in [0, s)) = 1$ *and* $\mathrm{Prob}(T'_j = 0) < 1$. *Assume that the sequence* $\ldots, S'_{-1}, S'_0, S'_1, \ldots$ *fulfils* $S'_{j+1} - S'_j \equiv T'_{j+1} (\mathrm{mod}\, s)$ *for each integer* j. *Assume further that* S'_J *is uniformly distributed on* $[0, s)$ *and independent from the random variables* $\ldots, T'_{-1}, T'_0, T'_1, \ldots$ *for a particular integer* J.
(i) S'_j *is uniformly distributed on* $[0, s)$ *for each integer* j, *and the random variables* $\ldots, S'_{-1}, S'_0, S'_1, \ldots$ *are stationary.*
(ii) For $j \ge 1$ *let* z'_j *denote the* j^{th} *index* $m > 0$ *for which* $S'_m < S'_{m-1}$, *and* $W'_j := S'_{z_j}$. *For* $R'_j = Z'_j - Z'_{j-1}$ *the random vectors* (W'_j, R'_j) *and the random variables* W'_j, R'_j *and* $Y' := f(R'_j)$ *(with* $f : \mathbb{R} \to \mathbb{R}$*) are stationary.*

Proof. For $k \geq 0$ trivially $S'_{J+k} \equiv S'_J + T'_{J+1} + \cdots + T'_{J+k} (\mathrm{mod}\, s)$, and the independence of S'_J and $T'_{J+1} + \cdots + T'_{J+k}$ proves the first assertion of (i). The case $k < 0$ can be handled analogously. We point out that the sequence $(S'_j - S'_{j-1})(\mathrm{mod}\, s) \equiv T'_j (\mathrm{mod}\, s)$ is stationary. We claim that S'_{J+j} and $(T'_i, \ldots, T'_k)$ are independent for any triple of integers (j, i, k) with $i \leq k$. Let $M := \{J+1, \ldots, J+j, i, \ldots, k\}$ and assume $j \geq 0$ for the moment. Then $\mathrm{Prob}(S'_{J+j} \in A \mid T'_\tau = t'_\tau \text{ for all } \tau \in M\} = \mathrm{Prob}(S'_J + T'_{J+1} + \cdots + T'_{J+j} (\mathrm{mod}\, s) \in A \mid T'_\tau = t'_\tau$ for all $\tau \in M\} = \mathrm{Prob}(S_J \in (A - t'_{J+1} - \cdots - t'_{J+j})(\mathrm{mod}\, s)) = \mathrm{Prob}(S'_J \in A)$ for each Borel subset $A \subseteq [0, s)$ and any realizations $t'_{J+1}, \ldots, t'_{J+j}, t'_i, \ldots, t'_k$ since the random variables S'_J and $(T'_{J+1}, \ldots, T'_{J+j}, T'_i, \ldots, T'_k)$ are independent, and S_J is uniformly distributed on $[0, s)$. This proves the claim for $j \geq 0$. For $j \leq 0$ we have $S'_J \equiv S'_{J+j} + T_{J+j+1} + \cdots + T'_J (\mathrm{mod}\, s)$, and the claim can be shown analogously. Let k and j be fixed for the moment. By the preceding $\mathrm{Prob}(S'_{j+1}, (T'_{j+2}, \ldots, T'_{j+k}) \in A \times B) = \mathrm{Prob}(S'_{j+1} \in A)\mathrm{Prob}(T'_{j+2}, \ldots, T'_{j+k} \in B) = \mathrm{Prob}(S'_1 \in A)\mathrm{Prob}(T'_2, \ldots, T'_k \in B) = \mathrm{Prob}(S'_1, (T'_2, \ldots, T'_k) \in A \times B)$ for any Borel subsets $A \subseteq [0, s)$ and $B \subseteq [0, s)^{k-1}$. Hence $(S'_1, T'_2, \ldots, T'_k)$ and $(S'_{j+1}, T'_{j+2}, \ldots, T'_{j+k})$ are identically distributed. Let the diffeomeorphism $\chi_k : [0, s)^k \to [0, s)^k$ be given by $\chi(x_1, \ldots, x_k) := (x_1, x_1 + x_2 (\mathrm{mod}\, s), \ldots, x_1 + \cdots + x_k (\mathrm{mod}\, s))$. Since $(S'_{j+1}, S'_{j+2}, \ldots, S'_{j+k}) = \chi_k(S'_{j+1}, T'_{j+2}, \ldots, T'_{j+k})$, the random vectors $(S'_1, S'_2, \ldots, S'_k)$ and $(S'_{j+1}, S'_{j+2}, \ldots, S'_{j+k})$ are identically distributed. Since j and k were arbitrary, this completes the proof of (i).

Let $j_1 > 0$ denote the smallest index for which $S'_{j_1} < S'_{j_1 - 1}$. Divide the random variables $\ldots, S'_{-1}, S'_0, S'_1, \ldots$ into increasing subsequences $\ldots, (\ldots, S'_{j_1 - 1}), (S'_{j_1}, \ldots, S'_{j_2 - 1}), (S'_{j_2}, \ldots), \ldots$ such that $S'_{j_m - 1} > S'_{j_m}$. (As $\mathrm{Prob}(T'_j = 0) < 1$ these subsequences are finite with probability 1.) Alternatively, these subsequences can be described by the sequence $(W'_j, R'_j)_{j \in Z}$ (and index j_0). For any $k \geq 1$, integers $r_1, \ldots, r_k \geq 1$ and subsets $A_1, \ldots, A_k \subseteq [0, s)$ the probability $\mathrm{Prob}((W'_{1+\tau}, R'_{1+\tau}) \in A_1 \times \{r_1\}, \ldots, (W'_{k+\tau}, R'_{k+\tau}) \in A_k \times \{r_k\})$ depends on the distribution of the $r := (r_1 + \cdots + r_k + 2)$-tuple $(S'_{j_1 - 1}, \ldots, S'_{j_1 + r - 2})$. Since the sequence $\ldots, (S'_1, \ldots, S'_r), (S'_2, \ldots, S'_{r+1}), \ldots$ is stationary the above probability is independent of τ. This proves the stationarity of $(W'_j, R'_j)_{j \in Z}$. The random variables W'_j, R'_j and Y'_j are functions of (W'_j, R'_j), which completes the proof of (ii).

Assumption 1. Unlike $\mathrm{Prob}(T'_j \geq s)$ in Lemma 1 the probability $\mathrm{Prob}(T_j \geq s)$ may be not 0 but negligible if $\mu \ll s$. It is reasonable to assume that for 'large' indices j the term $T_1 + \cdots + T_j (\mathrm{mod}\, s)$ is uniformly distributed on $[0, s)$ ($\rightarrow$ uniformity assumption on S'_j), and that $T_1, T_2, \ldots$ may be assumed to be stationary. Note that the intervals between the 0-1 switchings from the start of the RNG to time $t = 0$ can be described by random variables T_j with negative indices. The assumptions on the T_j seem to be natural and very mild, and with regard to Lemma 1 (and its proof) we assume in the following that besides the T_j also $(R_j)_{j \in \mathbb{N}}, (W_j)_{j \in \mathbb{N}_0}$, $(R_j (\mathrm{mod}\, 2))_{j \in \mathbb{N}}$ and finally $(Y_j)_{j \in \mathbb{N}}$ are stationary.

Definition 3. *The cumulative distribution functions of the random variables T_j and W_n are denoted by $G_T(\cdot)$ and $G_W(\cdot)$. For $u \in (0, \infty)$ the random variable*

$V_{(u)} := \inf\left\{\tau \in \mathbb{N} \mid \sum_{j=1}^{\tau+1} T_j > u\right\} = \sup\left\{\tau \in \mathbb{N} \mid \sum_{j=1}^{\tau} T_j \le u\right\}$ *quantifies the number of 0-1-switchings in the interval* $[0,u]$ *if* $W_0 \equiv 0$.

Lemma 2 collects some useful properties that will be needed later. Note that (12) formally confirms the intuition that the knowledge of more random numbers should not weaken the adversary's position. We point out that (12) might become false without the stationarity property, namely when R_n (for what reasons ever!) is easier to guess than R_{n+1}.

Lemma 2

(i)
$$H(R_n \mid R_0, R_1, \ldots, R_{n-1}) \ge H(R_{n+1} \mid R_0, R_1, \ldots, R_n) \quad \textit{and} \tag{12}$$
$$H(Y_n \mid Y_0, Y_1, \ldots, Y_{n-1}) \ge H(Y_{n+1} \mid Y_0, Y_1, \ldots, Y_n) \quad \textit{for all } n \in \mathbb{N}.$$

In particular, $\lim_{n\to\infty} H(R_{n+1} \mid R_1, \ldots, R_n)$ *and* $\lim_{n\to\infty} H(Y_{n+1} \mid Y_1, \ldots, Y_n)$ *exist.*
(ii) For $k \ge 1$ *we have*

$$\mathrm{Prob}(V_{(u)} = k) = \mathrm{Prob}\,(T_1 + \cdots + T_k \le u) - \mathrm{Prob}\,(T_1 + \cdots + T_{k+1} \le u)\,. \tag{13}$$

Further,

$$\mathrm{Prob}(V_{(u)} = 0) = 1 - \mathrm{Prob}\,(T_1 \le u)\,,\ \ \mathrm{Prob}(V_{(u)} = \infty) = 0 \quad \textit{and} \tag{14}$$
$$H(V_{(u)}) < \infty. \tag{15}$$

(iii) The distributions of the random variables $(\sum_{j=1}^{k} T_j - k\mu)/(\sqrt{k}\sigma)$ *tend to the standard normal distribution as* k *tends to infinity. In particular,*

$$\mathrm{Prob}\left(\frac{T_1 + \cdots + T_k - k\mu}{\sqrt{k}\sigma} \le x\right) \longrightarrow_{k\to\infty} \Phi(x). \tag{16}$$

for each $x \in \mathbb{R}$.
If the random variables $T_1, T_2, \ldots$ *are iid the condition* $E(|T_j|^3) < \infty$ *may be dropped, and in particular* $\sigma^2 = \sigma_T^2$
(iv) Let $u = v\mu$ *with* $v >> 1$. *Then*

$$\mathrm{Prob}\left(V_{(v\mu)} = k\right) \approx \Phi\left(\frac{v-k}{\sqrt{k}} \cdot \frac{\mu}{\sigma}\right) - \Phi\left(\frac{v-(k+1)}{\sqrt{k+1}} \cdot \frac{\mu}{\sigma}\right) \quad \textit{for } k \ge 1 \tag{17}$$

$$\mathrm{Prob}\left(V_{(v\mu)} = 0\right) \approx 1 - \Phi\left((v-1)\frac{\mu}{\sigma}\right). \tag{18}$$

The distribution of the random variable $V_{(v\mu)}$ *(or more precisely, its approximation given by (17) and (18)) depends only on the ratios* μ/σ *and* $u/\mu = v$ *but not on the absolute values of the parameters* $\mu, \sigma^2, u = v\mu$. *The mass of* $V_{(v\mu)}$ *is essentially concentrated on those* k*'s with* $k \approx v$. *Unless* k *is very small the interval*

$$J_k := \left[\frac{v-(k+1)}{\sqrt{k+1}} \cdot \frac{\mu}{\sigma}, \frac{v-k}{\sqrt{k}} \cdot \frac{\mu}{\sigma}\right) \quad \textit{has length } \approx \frac{\mu}{\sigma} \cdot \frac{v+k}{2k^{3/2}} \tag{19}$$

(v) (iid case) If the random variables $T_1, T_2, \ldots$ are iid then

$$\mathrm{Prob}(W_n \le x) = \frac{1}{\mu}\int_0^x (1 - G_T(u))\, du =: G_W(x). \tag{20}$$

(Note that if 'Prob$(W_n \le x)$' is substituted by '$\lim_{n\to\infty}$Prob$(W_n \le x)$' assertion (20) remains valid even if the sequence $(W_n)_{n\in\mathbb{N}_0}$ is not stationary.) If $G_T(\cdot)$ is continuous (or equivalently, if Prob$(T_1 = y) = 0$ *for all $y \in [0,\infty)$) then $G_W(\cdot)$ has density $g(x) := (1 - G_T(x))/\mu$.*

Proof. By Assumption 1 the random variables R_j and Y_j are stationary. Hence, (e.g.)

$$H(Y_n \mid Y_1, \ldots, Y_{n-1}) = H(Y_{n+1} \mid Y_2, \ldots, Y_n) \ge H(Y_{n+1} \mid Y_1, \ldots, Y_n),$$

and since entropy is non-negative this verifies (i). Assertions (ii), (iii) and the first assertions of (iv) follow from Lemma 1 and Lemma 2(ii) in [20]. We merely mention that (iii) applies a version of the Central Limit Theorem for dependent random variables that was proved in [12]. The remaining assertions in (iv) demand elementary but careful computations. (Note that $(\sqrt{k+1}-\sqrt{k})(\sqrt{k+1}+\sqrt{k}) = 1$ and $\sqrt{k} \approx \sqrt{k+1}$.) The remark in brackets and (20) were shown in [10] (4.10), and the last assertion of (v) follows by differentiation.

Under mild regularity assumptions on the $T_1, T_2, \ldots$ plausible heuristic arguments indicate that

$$H(Y_{n+1} \mid Y_1, \ldots, Y_n) \ge \min\{H(V_{(s-u)}(\mathrm{mod}2)) \mid u \in [0, \mu + a\sigma)\} G_W(\mu + a\sigma). \tag{21}$$

even for moderate parameter $a > 0$. We point out that for $n = 0$ or if the T_j are iid (21) is valid for any $a \ge 0$. Due to the lack of space we omit details. Theorem 1 collects the main results of this paper. Theorem 1 focuses on the entropy of the internal random numbers. Cancelling the term '(mod 2)' in (21), (24), (25) and (26) yields entropy estimates for the das random numbers. Equation (29) can be used to compute the autocovariance function and the autocorrelation function of the random variables $R_1, R_2, \ldots$.

Theorem 1. *(i)*

$$\mathrm{Prob}(R_{n+1} = k) \approx \int_0^s \mathrm{Prob}(V_{(s-u)} = k-1)\, G_W(du) \quad \textit{for } k \in \mathbb{N}_0 \tag{22}$$

$$\mathrm{Prob}(R_{n+1}(\mathrm{mod}\,2)) \approx \int_0^s \mathrm{Prob}(V_{(s-u)} \equiv k-1(\mathrm{mod}\,2))\, G_W(du) \textit{ for } k \in \{0,1\} \tag{23}$$

$$H(R_{n+1}(\mathrm{mod}\,2)) \ge H(R_{n+1}(\mathrm{mod}\,2) \mid W_n) \approx \int_0^s H(V_{(s-u)}(\mathrm{mod}\,2))\, G_W(du) \tag{24}$$

with equality for iid random variables T_j.
(ii) Substituting the integrands in (22) to (24) by Prob$(V_{(s-u)} = k-1 \mid W_0 = u)$, Prob$(V_{(s-u)} \equiv k-1(\mathrm{mod}\,2) \mid W_0 = u)$, *and* $H(V_{(s-u)}(\mathrm{mod}\,2) \mid W_0 = u)$, *resp.*,

provides equality also for the general case. For dependent T_j these conditional terms implicitly define conditions on the random variables $T_1, T_2, \ldots$ and thus on $V_{(s-u)}$.
(iii) (iid case) If the sequence $T_1, T_2, \ldots$ is iid

$$H(Y_{n+1} \mid Y_0, \ldots, Y_n) \geq \int_0^s H(V_{(s-u)} (\mathrm{mod}\, 2))\, G_W(du) \text{ for all } n \in \mathbb{N}\,. \quad (25)$$

If $G_T(\cdot)$ is continuous the right-hand side of (25) reads

$$\int_0^s H(V_{(s-u)} (\mathrm{mod}\, 2))\, \frac{1}{\mu}(1 - G_T(u))\, du. \quad (26)$$

$$(iv)\ E((R_1 + \cdots + R_j)^k) = \int_0^{js} E((V_{(js-u)} + 1)^k \mid W_0 = u)\, G_W(du) \quad (27)$$

$$\approx \int_0^{js} E((V_{(js-u)} + 1)^k)\, G_W(du) \text{ for each } k \in \mathbb{N} \quad (28)$$

with equality for iid random variables T_j. The stationarity of the R_j implies

$$E((R_1 + \ldots + R_j)^2) = jE(R_1^2) + 2\sum_{i=2}^{j}(j + 1 - i)E(R_1 R_i) \quad (29)$$

Proof. By stationarity $(R_{n+1} \mid W_n = u)$ is distributed as $(V_{(s-w_n)} + 1 \mid W_0 = u)$, and thus $(R_{n+1} (\mathrm{mod}\, 2) \mid W_n = u)$ as $(V_{(s-w_n)} + 1 (\mathrm{mod}\, 2) \mid W_0 = u)$. Formulae (22) to (24) and (ii) follow immediately from the stationarity of the random variables $R_1, R_2, \ldots$ and $W_1, W_2, \ldots$. Within this proof ν_n and $\nu_{n|y_0,\ldots,y_n}$ denote the distribution of W_n, resp. of the conditional random variable $(W_n \mid Y_0 = y_0, \ldots, Y_n = y_n)$. In this notation

$$H(Y_{n+1} \mid Y_0 = y_0, \ldots, Y_n = y_n) \geq H(Y_{n+1} \mid Y_0 = y_0, \ldots, Y_n = y_n, W_n) \quad (30)$$
$$= \int_0^\infty H(Y_{n+1} \mid Y_j = y_j, j \leq n; W_n = u)\, \nu_{n|y_0,\ldots,y_n}(du)$$

If the T_j are iid for all $n \in \mathbb{N}$ the vector $(T_{z_n+1}, T_{z_{n+1}+2}, \ldots)$ is distributed as $(T_1, T_2, \ldots)$, regardless of u and the history $y_0, \ldots, y_n$. In particular, since $H(Y_{n+1} \mid \cdot) = H(Y_{n+1} - Y_n (\mathrm{mod}\, 2) \mid \cdot) = H(R_{n+1} (\mathrm{mod}\, 2) \mid \cdot)$ the integrand of the right-hand side of (30) only depends on u. More precisely, for any $y_0, \ldots, y_n$ the integrand equals $H(V_{(s-u)} + 1 (\mathrm{mod}\, 2)) = H(V_{(s-u)} (\mathrm{mod}\, 2))$. Altogether

$$\begin{aligned} & H(Y_{n+1} \mid Y_0, \ldots, Y_n, W_n) \\ = & \sum_{y_0,\ldots,y_n \in \{0,1\}} \mathrm{Prob}(Y_0 = y_0, \ldots, Y_n = y_n) \int_0^\infty H(V_{(s-u)} (\mathrm{mod}\, 2))\, \nu_{n|y_1,\ldots,y_n}(du) \\ = & \int_0^\infty H(V_{(s-u)} (\mathrm{mod}\, 2))\, \nu_n(du) = \int_0^s H(V_{(s-u)} (\mathrm{mod}\, 2))\, G_W(du) \end{aligned}$$

in the iid case. The last equation follows from the fact that $\text{Prob}(W_{n+1} > s) = 1 - G_W(s) \approx 0$ since $s >> \mu$. This proves (25), and (26) follows immediately from Lemma 2(v). The sum $R_1 + \cdots + R_n = Z_n - Z_0$ is distributed as $V_{(ns-W_0)} + 1$, which proves (27). For iid T_j the history (expressed by W_0) is irrelevant, yielding (28). The stationarity of the T_j finally yields (29).

Remark 4. (i) (robustness) Formulae (24), (25) and (26) (with and without '(mod 2)') provide entropy estimators for the das random numbers and the internal random numbers that seem to be robust against at least moderate deviations of the distribution of the random variables $T_1, T_2, \ldots$. In fact, by (17) and (18) the entropy $H(V_{(s-u)})$ essentially depends on the ratios $(s-u)/\mu$ and μ/σ. The density $(1 - G_T(\cdot))/\mu$ in (26) is monotonically decreasing, which additionally supports robustness.
(ii) (approximation errors) Theorem 1 tacitly applies the normal approximations (17) and (18). For large ratios s/μ this should not cause serious problems unless very small 'entropy defects' $\epsilon := 1 - H(Y_{n+1} \mid Y_1, \ldots, Y_n)$ shall be verified (cf. Sect. 5); for small ratios s/μ one should be careful anyway. The convergence rate of the central limit theorem and thus the meaning of 'small' depends on the distribution of the random variables $T_1, T_2, \ldots$. Fortunately, for the conditional entropy $H(Y_{n+1} \mid Y_1, \ldots, Y_n)$ the sum $\sum_{k \equiv 0(\bmod 2)} \text{Prob}(V_{(s-u)} = k)$ is relevant so that one may expect that approximation errors in Lemma 2(iv) cancel out each other to a large extent.

To be on the safe side (especially for very small ϵ) one may study the approximation errors in (17) and / or in $H(V_{(s-u)} (\bmod 2))$ for the relevant distribution. For this purpose stochastic simulations may be applied where pseudo-random numbers t_j are generated according to the distribution of the random variables $T_1, T_2, \ldots$. A similar approach can be followed with experimental data from measurements (cf. (iii)). If the T_j are independent one may operate with Fourier transforms. Concerning (17) it seems to be reasonable to concentrate on integers k in a vicinity of s/μ, resp. for $(s-u)/\mu$ with small u.
(iii) Theorem 1 considers the stationary distribution of the random variables W_j but it can also be adjusted to experimental data in a straight-forward way. To apply (22), (23), (24), (25) and (28) one uses a sequence of measured time spans $t_1, t_2, \ldots$ between consecutive 0-1-crossings to obtain an empirical distribution for the stationary distribution of $W_1, W_2, \ldots$ (tacitly assuming ergodicity). The formulae are then applied with this empirical distribution in place of G_W. For Theorem 1(ii) and (27) (relevant for dependent T_j's) the procedure is similar but more costly since only subsequences of $t_1, t_2, \ldots$ can be used to obtain the conditional distributions $(\cdot \mid u)$. Of course, in this empirical approach statistical deviations add to the approximation errors mentioned in (ii).

Remark 5. In [4] a design of a physical RNG is investigated that also exploits the switchings of a comparator. The amplified noise is also modelled as a stationary stochastic process, and the autocorrelation function of the random numbers are computed. We mention that unlike the present paper reference [4] yet considers idealized assumptions (Gaussian white noise etc.), which clearly simplify analysis. [4] exploits the number of comparator switchings within fixed time periods

for an online test (cf. Sect. 6). For an introduction into the field of stationary stochastic processes we refer the interested reader e.g. to [24].

5 Practical Experiments

As pointed out in Remark 3 relations (9) to (11) fit to various RNG designs. The distribution of the random variables T_j and thus of R_j and Y_j depend on the particular design but also on the concrete implementation. To get 'real' das random numbers we performed measurements on a prototype of a particular physical RNG (cf. Fig. 2 and Acknowledgement) for which the design left from the first flip-flop coincides with the generic design discussed in Section 3.

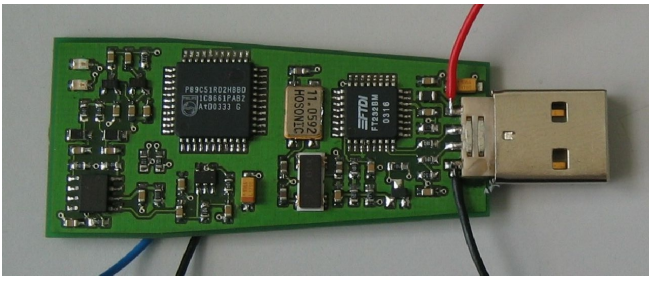

Fig. 2. RNG prototype used for measurements

Maximum-Likelihood tests indicate that the one-dimensional empirical distribution of the times between consecutive 0-1-crossings can be well approximated by a Gamma distribution with shape parameter 3.0949 and rate 0.0240. In Fig. 3 the circles show the percentiles of the empirical distribution, and the curve shows the percentile of Gamma distribution with the indicated parameters.

We applied Theorem 1 (more precisely, (25) and (28) and (29)) to a set of $\approx 620\,000$ measured time spans $t_1, t_2, \ldots$ between consecutive 0-1-crossings to obtain Table 1 (cf. Remark 4(iii)). We estimated $\mu = E(T_1)$ by $\widetilde{\mu} = 128.85ns$ and $\mathrm{Var}(T_1)$ by $\widetilde{\sigma}_T^2 = 5314.0$. The estimates for the autocovariances $\mathrm{cov}(T_j, T_{j+\tau}) = E(T_j T_{j+\tau}) - E(T_j)E(T_{j+\tau})$ were -2.08, -10.08, 5.56, 3.80 and -1.18 for the shift parameters $\tau = 1, \ldots, 5$. Compared to $\widetilde{\sigma}_T^2$ these values are very small, and experiments with various measurement sets support the conjecture that the true autocovariances are essentially 0. We point out that also contingency tests did not contradict the hypothesis that the random variables T_j and T_{j+1} are independent (97 from 99 tests on significance level 0.01 were passed).

The correlation coefficient of random variables X and Y is given by $\mathrm{corr}(X, Y) = \mathrm{cov}(X, Y)/\sqrt{\mathrm{Var}(X)\mathrm{Var}(Y)}$. We applied Theorem 1 directly to the experimental data and to their Gamma approximation (Table 1). Especially for the small clock lengths $s = 7.497\widetilde{\mu}$ and $s = 9.996\widetilde{\mu}$ the exact conditional entropy $H(Y_{n+1} \mid Y_1, \ldots, Y_n)$ might differ somewhat from the estimates in Table 1

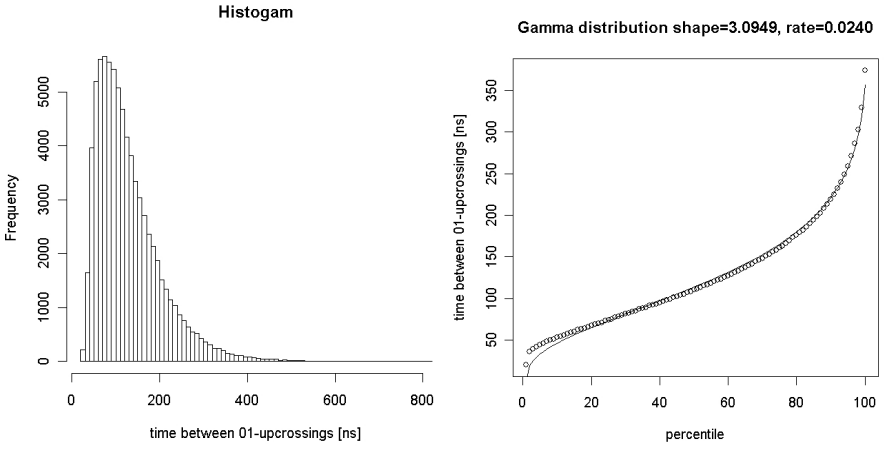

Fig. 3. Empirical distribution of the time between 0-1 crossings: histogram and percentiles

(cf. Remark 4(ii)). Table 1 suggest that the true conditional entropies should be indeed very close to 1, especially for $s = 15.017\widetilde{\mu}$, which gives an output of slightly more than 500 kBit internal random numbers per second. For a k-fold convolution (let's say for $k \in \{10, \ldots, 20\}$) of a gamma distribution with the above-mentioned parameters the normal approximation and thus approximation (17) should be pretty good. Numerical experiments indicate that for $s = 15.017\widetilde{\mu}$ the entropy defect $\epsilon = 1 - H(Y_{n+1} \mid Y_1, \ldots, Y_n)$ (cf. Remark 4) should be smaller than (at least) $< 10^{-4}$. Smaller bounds seem to be realistic but (in our opinion) deserve more elaborate analysis.

It is easy to see that the random variables R_n and R_{n+1} are negatively correlated: A 'large' value r_n (resp., a small value r_n) is an indicator that w_n is also large (resp., that w_n is small), and thus r_{n+1} is likely to be small (resp., r_{n+1} to be large). Apart from the autocorrelation coefficients $\mathrm{corr}(R_1, R_2)$ and $\mathrm{corr}(R_1, R_3)$ the results obtained by the direct application of Theorem 1 to the experimental data and to their Gamma approximation are essentially equal. To obtain the autocorrelation coefficients we had to apply (28) and (29) iteratively. In particular since the terms $E(R_j^2)$ dominate estimation errors clearly propagate to the autocorrelation coefficients. The results for the Gamma approximation are more reasonable since $|\mathrm{corr}(R_1, R_3)|$ is considerably smaller than $|\mathrm{corr}(R_1, R_2)|$ and both values decrease for larger s, what was expected. Increasing the sample size should also yield better results for the direct use of the experimental data.

6 Online Tests

The conditional entropies $H(R_{n+1} \mid R_0, \ldots, R_n)$ and $H(Y_{n+1} \mid Y_0, \ldots, Y_n)$ are closely related to the entropy of the random variables $V_{(s-u)}$ and $V_{(s-u)}(\bmod 2)$, respectively. If the ratio $(s-u)/\mu$ is not too small $H(V_{(s-u)})$ essentially depends

Table 1. Experimental Results

	$s = 7.497\widetilde{\mu}$	$s = 9.996\widetilde{\mu}$	$s = 9.996\widetilde{\mu}$ (Gamma approx.)	$s = 15.017\widetilde{\mu}$	$s = 15.017\widetilde{\mu}$ (Gamma approx.)
$E(R_1)$	7.493	9.994	9.996	15.014	15.017
$\mathrm{Var}(R_1)$	2.701	3.502	3.519	5.107	5.141
$\mathrm{corr}(R_1, R_2)$	−0.034	−0.034	−0.041	−0.011	−0.028
$\mathrm{corr}(R_1, R_3)$	0.022	0.010	0.0001	0.019	0.00009
$H(R_{n+1} \mid R_1, \ldots, R_n)$	2.631	2.850	2.858	3.155	3.163
$H(Y_{n+1} \mid Y_1, \ldots, Y_n)$	0.99990	1.00000	0.99999	1.00000	1.00000

only on the ratios μ/σ and $(s-u)/\mu$ (17). Moreover, 'small' arguments u provide the essential contribution to the integrals from Theorem 1. Hence it is natural (and effective) to estimate the process parameters $\mu = E(T_j)$ and the generalized variance σ^2 of $T_1, T_2, \ldots$ while the RNG is in operation. Unfortunately, this required an internal clock with high resolution, which may be too costly for many applications.

Alternatively, one may check the process parameters μ and σ^2 indirectly, namely by estimating the mean value $\mu_R := E(R_j)$ and the generalized variance σ_R^2 of the stationary sequence $R_1, R_2, \ldots$. In a first step intervals I_μ and I_{σ^2} should be specified which contain 'suitable' values of the process parameters μ and σ^2. By Theorem 1(iv) one computes sets I_{μ_R} and $I_{\sigma_R^2}$ that contain μ_R and σ_R^2 if μ and σ^2 are contained in I_μ and I_{σ^2}. It seems to be reasonable if the online tests consider the mean and maybe also the generalized variance of $R_1, R_2, \ldots$. Generically,

- Estimate μ_R: Compute the arithmetic mean $\mathrm{av}(r_1, \ldots, r_m) := (r_1 + \cdots + r_m)/m$.
- Estimate σ_R^2 or a related parameter from das random numbers $r_{m+1}, \ldots, r_{m+M}$.

The respective test fails if the estimator lies outside a particular regions. Such basis tests may directly serve as online tests, or they can be integrated into a more sophisticated procedure that covers the tasks of the tot test, self test and online test. Due to lack of space we cannot deepen this aspect here but refer the interested reader to [18], [22], Sect. 6, or [13], Example 7. In any case the probability for a failure of a single test must be determined to specify appropriate test rules.

The distribution of $\mathrm{av}(R_1, \ldots, R_m)$ can be computed with (22) with upper integration boundary ms in place of s. The second basis test should be tailored to the distribution of the random variables R_j, which is determined by the RNG. The generalized variance σ_R^2 can be estimated directly, or a relevant set of covariances $\mathrm{cov}(R_n, R_{n+k})$ may be estimated. A precise computation of the failure probability, i.e. that the test value lies outside a specified set, is more complicated than for the arithmetic mean. This may be done on basis of theoretical considerations, or by stochastic simulations (with pseudorandom numbers $\widetilde{t}_1, \widetilde{t}_2, \ldots$ that are generated according to the specified distribution of the random variables T_j), or on basis of measurement series. We point out that under

suitable circumstances the second type of online test may be dropped, e.g. when within the class of distributions that contains the true distribution of $R_1, R_2, \ldots$ ($\rightarrow$ stochastic model) the generalized variance σ^2 is a function of μ.

7 Final Remarks

We addressed general requirements that should be considered in security evaluations of physical RNGs. We formulated and analyzed a stochastic model that describes the stochastic behaviour of a particular RNG design that exploits two noisy diodes. Interestingly, this stochastic model also fits to other designs, which makes its understanding important. Theorem 1 collects the main results of this paper, which allow to establish tight lower bounds for the entropy per internal random random number. We applied our results to a particular physical RNG, and we briefly touched the field of online tests.

Acknowledgement. The authors would like to thank Frank Bergmann, who courteously provided the RNG prototype, and Joachim Schüth for performing measurements.

References

1. AIS 20: Functionality Classes and Evaluation Methodology for Deterministic Random Number Generators. Version 1 (02.12.1999) (mandatory if a German IT security certificate is applied for; English translation) (1999), `www.bsi.bund.de/zertifiz/zert/interpr/ais20e.pdf`
2. AIS 31: Functionality Classes and Evaluation Methodology for Physical Random Number Generators. Version 1 (25.09.2001) (mandatory if a German IT security certificate is applied for; English translation) (2001), `www.bsi.bund.de/zertifiz/zert/interpr/ais31e.pdf`
3. ANSI X9.82, Random Number Generation (Draft Version)
4. Bagini, V., Bucci, M.: A Design of Reliable True Number Generators for Cryptographic Applications. In: Koç, Ç.K., Paar, C. (eds.) CHES 1999. LNCS, vol. 1717, pp. 204–218. Springer, Berlin (1999)
5. Bucci, M., Germani, L., Luzzi, R., Trifiletti, A., Varanonuovo, M.: A High-Speed Oscillator-Based Truly Random Number Source for Cryptographic Applications. IEEE Trans. Computers 52, 403–409 (2003)
6. Bucci, M., Lucci, R.: Design of Testable Random Bit Generators. In: Rao, J.R., Sunar, B. (eds.) CHES 2005. LNCS, vol. 3659, pp. 147–156. Springer, Berlin (2005)
7. Bock, H., Bucci, M., Luzzi, R.: An Offset-Compensated Oscillator-Based Random Bit Source for Security Applications. In: Joye, M., Quisquater, J.-J. (eds.) CHES 2004. LNCS, vol. 3156, pp. 268–281. Springer, Berlin (2004)
8. Dichtl, M.: How to Predict the Output of a Hardware Random Number Generator. In: Walter, C.D., Koç, Ç.K., Paar, C. (eds.) CHES 2003. LNCS, vol. 2779, pp. 181–188. Springer, Berlin (2003)
9. Dichtl, M., Golic, J.: High-Speed True Random Number Generation with Logic Gates Only. In: Paillier, P., Verbauwhede, I. (eds.) CHES 2007. LNCS, vol. 4727, pp. 45–62. Springer, Berlin (2007)

10. Feller, W.: An Introduction to Probability Theory and Its Application, vol. 2. Wiley, New York (1965)
11. ISO / IEC 18031 Random Bit Generation (November 2005)
12. Hoeffding, W., Robbins, H.: The Central Limit Theorem for Dependent Random Variables. Duke Math. J. 15, 773–780 (1948)
13. Killmann, W., Schindler, W.: A Proposal for: Functionality Classes and Evaluation Methodology for True (Physical) Random Number Generators. Version 3.1, 25.09.2001, mathematical-technical reference of [2] (English translation) (2001), www.bsi.bund.de/zertifiz/zert/interpr/trngk31e.pdf
14. Marsaglia, G.: Diehard (Test Suite for Random Number Generators), www.stat.fsu.edu/~geo/diehard.html
15. Pliam, J.O.: The Disparity Between the Work and the Entropy in Cryptology (01.02.1999), eprint.iacr.org/complete/
16. Rukhin, A., et al.: A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST Special Publication 800–22 with revisions dated (15.05.2001), csrc.nist.gov/rng/SP800-22b.pdf
17. Schindler, W.: Functionality Classes and Evaluation Methodology for Deterministic Random Number Generators. Version 2.0, 02.12.1999, mathematical-technical reference of [1] (English translation) (1999), www.bsi.bund.de/zertifiz/zert/interpr/ais20e.pdf
18. Schindler, W.: Efficient Online Tests for True Random Number Generators. In: Koç, Ç.K., Naccache, D., Paar, C. (eds.) CHES 2001. LNCS, vol. 2162, pp. 103–117. Springer, Heidelberg (2001)
19. Schindler, W., Killmann, W.: Evaluation Criteria for True (Physical) Random Number Generators Used in Cryptographic Applications. In: Kaliski Jr., B.S., Koç, Ç.K., Paar, C. (eds.) CHES 2002. LNCS, vol. 2523, pp. 431–449. Springer, Heidelberg (2003)
20. Schindler, W.: A Stochastical Model and Its Analysis for a Physical Random Number Generator Presented at CHES 2002. In: Paterson, K.G. (ed.) Cryptography and Coding 2003. LNCS, vol. 2898, pp. 276–289. Springer, Heidelberg (2003)
21. Schindler, W.: Random Number Generators for Cryptographic Applications. In: Koç, Ç.K. (ed.) Cryptographic Engineering. Signals and Communication Theory. Springer, Berlin (to appear)
22. Schindler, W.: Evaluation Criteria for Physical Random Number Generators. In: Koç, Ç.K. (ed.) Cryptographic Engineering. Signals and Communication Theory. Springer, Berlin (to appear)
23. Tkacik, T.: A Hardware Random Number Generator. In: Kaliski Jr., B.S., Koç, Ç.K., Paar, C. (eds.) CHES 2002. LNCS, vol. 2523, pp. 450–453. Springer, Heidelberg (2003)
24. Yaglom, A.M.: Correlation Theory of Stationary and Related Random Functions. Springer Series in Statistics, vol. 1. Springer, New York (1987)