Computers & Security (2004) **23**, 77—84

ELSEVIER

Computers & Security

www.elsevier.com/locate/cose

Biometric random number generators

J. Szczepanski[a,*,1], E. Wajnryb[a], J.M. Amigó[b], Maria V. Sanchez-Vives[c], M. Slater[d]

[a]*Institute of Fundamental Technological Research, Polish Academy of Sciences, Swietokrzyska 21, 00-49 Warsaw, Poland*
[b]*Centro de Investigación Operativa, Universidad Miguel Hernández, Elche, Spain*
[c]*Instituto de Neurociencias, Universidad Miguel Hernández-CSIC, Alicante, Spain*
[d]*Department of Computer Science, University College London, London WC1E 6BT, United Kingdom*

Received 25 April 2003; revised 27 August 2003; accepted 19 September 2003

KEYWORDS
Biometric methods;
Random number generator;
Stochastic process;
Statistical tests;
Computer communication protocols

Abstract Up to now biometric methods have been used in cryptography for authentication purposes. In this paper we propose to use biological data for generating sequences of random bits. We point out that this new approach could be particularly useful to generate seeds for pseudo-random number generators and so-called "key sessions". Our method is very simple and is based on the observation that, for typical biometric readings, the last binary digits fluctuate "randomly". We apply our method to two data sets, the first based on animal neurophysiological brain responses and the second on human galvanic skin response. For comparison we also test our approach on numerical samplings of the Ornstein—Uhlenbeck stochastic process. To verify the randomness of the sequences generated, we apply the standard suite of statistical tests (FIPS 140-2) recommended by the National Institute of Standard and Technology for studying the quality of the physical random number generators, especially those implemented in cryptographic modules. Additionally, to confirm the high cryptographic quality of the biometric generators, we also use the often recommended Maurer's universal test and the Lempel—Ziv complexity test, which estimate the entropy of the source. The results of all these verifications show that, after appropriate choice of encoding and experimental parameters, the sequences obtained exhibit excellent statistical properties, which opens the possibility of a new design technology for true random number generators. It remains a challenge to find appropriate biological phenomena characterized by easy accessibility, fast sampling rate, high accuracy of measurement and variability of sampling rate.

* Corresponding author.
E-mail address: jszczepa@ippt.gov.pl (J. Szczepanski).
[1] Also consultant of Centre of Trust and Certification CENTRAST SA.

0167-4048/04/$ - see front matter © 2004 Elsevier Ltd. All rights reserved.
doi:10.1016/S0167-4048(04)00064-1

Introduction

Biometrics is the science and technology of measuring and statistically analyzing biological data. In information technology, biometrics usually refers to techniques for measuring and analyzing human body characteristics such as fingerprints, eye retinas and irises, voice patterns, facial patterns, and hand measurements, especially for authenticating someone (Information Technology—Security Techniques, 2002; Jain et al., 1999; X9. F4 Working Group, 2001). This kind of application needs to study stationary properties uniquely determined by the attributes of each individual.

In this paper we propose the use of biometric data in quite the opposite way. Namely, we would like to explore the randomness of biometric data in order to use them (after codification in integer or bit format) as seeds for pseudo-random number generators or, directly, as random number sequences. This could be of great practical importance for generating the "key session" in the SSL, SSH, PGP or SET computer communication protocols. It would reduce also the security concerns that arise when one uses software random generators based on the system clock, the content of the input/output buffers, etc. because of their weakness against intruder's attacks.

This method can also be used during the "Key Generation Ceremony" performed in the Certification Authorities Offices (Key Management Policy and Practical Framework, 2002). In this ceremony, the seed, which is unknown to all participants and produced by a physical random number generator implemented in a cryptographic module, could be replaced by a biological random seed coming from the "key administrators". The biological data collected from each key administrator would be transformed into a bit sequence and then all these sequences could be XOR-ed into a single bit sequence. This procedure would increase the confidence of the key administrators to the Key Generation Ceremony. Biological random seeds could also be applied to key generation for electronic signatures used by subscribers.

Random number generators (RNG) can be implemented either in hardware or in software. Random number generation performed by software utilizes a mathematical algorithm that produces a sequence of statistically independent numbers following a uniform distribution. However, this sequence is deterministic given the algorithm and the seed. While it is possible to implement a mathematical algorithm in hardware and call it a "hardware random number generator", these particular RNG clearly belong in the category of pseudo-random number generators because they require a seed and produce a deterministic sequence of numbers. True random number generation in hardware depends upon the random characteristics of some physical systems; for example lava lamps, radioactive decay of atomic nuclei, or noise from a resistor or diode. One of the most important properties of such generators is that they do not need any seed to start producing random sequences.

The number of uses of the random numbers has steadily increased over time, especially since the advent of the digital technologies. Some important examples are complex scientific and financial model simulations, modern lotteries and gambling machines, equation solving, etc. Because of computer security, there is also a growing interest in random key generation for cryptography, digital signatures and protected communication protocols. At the base of these techniques used to secure data and data transmissions lies key generation, which requires the production of secret, unguessable keys. Hence, key generation depends on an RNG to provide the necessary entropy to make the key indeterminable.

We have checked the randomness of two types of biometric data. The first one consisted of neuronal membrane voltages recorded by intracellular recordings in the primary visual cortex of a cat during series of visual stimulation. For the second we used the electrical conductances of the galvanic skin responses of humans in a virtual reality experiment. In both cases we applied a method we call 'last digit fluctuation' (see below for the description) to extract a random bit sequence from this biological data. The randomness of the generated bit sequences was then verified at a high level of significance by a variety of methods including the standard FIPS 140-2 tests (recommended by the National Institute of Standards and Technology), the Maurer universal test and the Lempel—Ziv complexity. Let us mention in this context that a third data set, the bit sequences obtained from the action potentials ("spike trains") simulated by networks of artificial neurons, did not pass the randomness tests, although such networks have been checked to simulate very well other aspects of the real neuronal activity. This serves as a control example, where simulated biological data did not have the randomness properties that we have discovered for the real biological data.

These results therefore open new possibilities of obtaining (true) random numbers by means of biological systems, to be added to the traditional ones, based on physical systems. Of course, other biologically generated data can be and will be

studied in order to confirm the results of this current study. The main advantage of this alternative in eventual implementations would be, apart from privacy (say, a better protection of the generator to externals manipulations), to provide random bits in real time in a simple and very portable way.

The last digit fluctuation method

Generally speaking, the randomness of an information source means that it outputs sequences of statistically independent symbols (also called "letters"). In other words, all sequences of a given length are equally probable. In practice, the randomness is verified at a given significance level by applying a set of appropriate statistical tests to a representative sample of sequences generated by the source. We will focus henceforth on real number sources (in practice, physical systems) and how to draw random bit sequences out of their outputs (resp. readings).

The fundamental idea of our approach to random number generation is based on the fact that for the physical measurements at noisy sources the rightmost (or least significant) digits exhibit generally random properties. Indeed, the noise present in most of the physical processes produces comparatively small disturbances of the measured quantities which, in turn, translates into a random fluctuation of the less significant digits of their exact values (i.e. after discarding those digits affected by the measurement precision). The simplest approach, which we favor and propose under the name of the last digit fluctuation method, consists in keeping only the rightmost bit of each measurement after some appropriate binary codification. Let us emphasize that it is the randomness due to quantum or thermal noise we are invoking here, and not at all the finite precision inherent to any physical measurement which, even in the absence of any kind of noise, produces a normally distributed fluctuation of the observed values around the average. The accuracy of the measurement instrument can be determined by means of non-random processes and it is, in practice, a known parameter. Of course, it is possible to apply the same method to many different types of data sets, such as tables of logarithms or even economic trend data. However, the point here is that the random digits are generated in real time in such a way that it is impossible to guess the key in advance.

We now describe more precisely our method. Let $\{x_i\}_{i=1}^{N}$ be the sequence of real N real numbers (measurements) produced by the source. Our goal is to convert (encode) these sequence into a new binary sequence $\{b_i\}_{i=1}^{N'}$, where $N' \leq N$. We use the estimators of the average and the standard deviation of the sequence $\{x_i\}_{i=1}^{N}$,

$$\bar{x} = \frac{1}{N}\sum_{i=1}^{N} x_i$$

$$s^2 = \frac{1}{N-1}\sum_{i=1}^{N}(x_i - \bar{x})^2$$

to eliminate the large fluctuations in the data, which improves the performance of the method. This means that we record only those measurements which are not too far from the average, e.g. $|x_i - \bar{x}| < Rs$, where R is a parameter of the order of 1. Let $\{x_i\}_{i=1}^{N'}$denote (after an eventual renumbering) the measurements which passed the previous screening. Subdivide now the interval $[\bar{x} - Rs, \bar{x} + Rs]$ into L equal subintervals numbered from 0 to $L-1$. Call l_i the subinterval containing x_i. In this way, every x_i is associated with an integer number $0 \leq l_i \leq L-1$. Finally, take $b_i = 0$ if l_i is even and $b_i = 1$ if l_i is odd. All these operations can be written in the compact formula

$$b_i = l_i \bmod 2 = \left\lfloor \frac{x_i - (\bar{x} - Rs)}{2Rs} L \right\rfloor \bmod 2$$

where symbol $\lfloor y \rfloor$ denotes the integer part of the number y. In particular, when L is the k-th power of 2, the sequence $\{b_i\}_{i=1}^{N'}$ can be obtained as the k-th bit in the binary representation of the elements of $\{l_i\}_{i=1}^{N'}$. In practice, the biological data have three or four accurate decimal digits, which suggest us to take $500 \leq L \leq 5000$ so that the resulting sequence $\{b_i\}_{i=1}^{N'}$ is closely related to the fluctuation of the last digits of the measurements.

Now our goal is to determine, for a given experiment, a pair (R, L) such that the sequences $\{b_i\}_{i=1}^{N'}$ obtained are random, i.e. they pass the suite of tests which are commonly used by the cryptographic community. Once the parameters (R, L) have been optimised for a type of biometric data, they can be generically used in practical designs of a random bit generator based on the corresponding biometric signal. The choice of the parameters R and L used in the binary encoding method we proposed determines, on the one hand, the generating rate and, on the other hand, the statistical quality of the ensuing bit sequence. A larger R means a higher generating rate, while for the parameter L the situation is a little bit more complicated. When one considers

readings with more digits, a larger L means better statistical properties. In practice, readings contain three or four fluctuating digits and one has to determine the proper L taking into account the applied parameter R. The other two parameters of the design, $(\bar{x}, s)$, which characterize the data window, can also be fixed dynamically or once and for all from an initial batch of readings.

Statistical tests to measure randomness

Various tests can be applied to a would-be random bit generator in order to detect several weaknesses the generator may have. All of them target different properties the truly random sequences are expected to exhibit and, therefore, involve the statistical analysis of a sample of output sequences. When one considers physical generators, the most commonly used suite of tests for that purpose is the FIPS 140-2 suite recommended by the National Institute of Standards and Technology (NIST). This suite consists (Menezes et al., 1996) of four tests: (i) monobit test, (ii) poker test, (iii) runs test and (iv) long run test.[2] We have used the 1/10,000 significance level, which is the one recommended for this suite. The bounds corresponding to this level can be found in FIPS PUB 140-2 (2001). However, there might be sequences that pass these tests albeit they possess very poor random attributes since the certificates of randomness can be only probabilistic, the probability of wrongly rejecting random sequences (Type I error) being given by the significance level.

In order to ensure randomness in a stronger way, some publicly available programs implement some more sophisticated tests such as Maurer's universal test (Maurer, 1990), based on compression techniques, which is able to detect any one of a very general class of possible defects a bit generator might have. To be more specific, instead of actually compressing the sequences, Maurer's test computes a statistic (basically, the average of the logarithmic distances between successive identical blocks of a predetermined length chosen from the interval [6,16]) that is related to the length of the compressed sequence. For random sequences, this statistic follows approximately a normal distribution whose mean and variance depend on the block length used in a known way (Menezes et al., 1996). Following the current wisdom, we apply Maurer's test to our sequences and, additionally, the normalized Lempel–Ziv complexity (Lempel and Ziv, 1976), which measures the generation rate of new patterns along a sequence of symbols. All these tests together provide a very comprehensive (though probabilistic) picture of the random nature of the source in question.

Our experience with time series has shown us that the (normalized) Lempel–Ziv complexity is a very fast and accurate estimator of the source entropy (Amigó et al., 2004). However, unlike the Lempel–Ziv complexity version which is part of the statistical tests recommended by the NIST (2001), for the Lempel–Ziv complexity that we actually used, no rigorous method to calculate the bounds for a given significance level is known yet. In the present analysis we estimated the expectation value of the Lempel–Ziv complexity and the corresponding bounds using the Monte Carlo method for the Lahey–Fujitsu random number generator. In this test we assumed the significance level to be 0.003 (three standard deviations).

Experimental data

In our opinion, there are some desirable features that should guide the search and choice of a biometric random number generator. These are basically:

(i) sufficiently fast sampling rate,
(ii) relatively simple data acquisition,
(iii) high accuracy of measurement (at least 3–4 decimal digits),
(iv) variability of biological data for the applied sampling rate.

To give a start to our biometric approach to random bit generation, we have analyzed the two kinds of biological data which were most accessible to us: neurophysiological brain signals (NBS) and galvanic skin response (GSR). Before describing them in detail, let us point out right from the beginning that they suffer from some shortcomings, namely, NBS do not fulfil (ii), whereas GSR do not fulfil (i).

The NBS data that we used for random number generation was the neuronal membrane voltage values (in millivolts) obtained by intracellular recordings in the primary visual cortex of the cat during series of visual stimulation (Sanchez-Vives et al., 2000). These recordings were acquired at

[2] As of this writing, the requirement for the implementation of the runs test and the long run test in cryptographic modules has been temporarily suspended. Once the replacement tests are decided, the FIPS PUB 140-2 will be updated with a revision and a transition time period after which the implementation of the replacement tests will become mandatory.

a frequency of 200 Hz. Visual stimulation consisted in the succession of various stimuli on the membrane potential of cortical neurons. For this purpose, we presented a sequence of either a gray screen (0% contrast), high contrast (40–80%) optimal sinewave drifting grating presented over the whole screen, or the same drifting grating with an artificial scotoma consisting of a 4–9° (6.5° ± 1.7°, mean ± S.D.) gray square (0% contrast, same average luminance as the peripheral grating) centered over the discharge receptive field. The experimental voltage recordings gave rise, after application of the last digit fluctuation method, to a sample comprising seven binary sequences of about 360,000 bits each.

As for the GSR data, which actually are electrical conductance readings in microsiemens (μS), these were collected in the context of an experiment investigating objective responses to avatars (virtual humans) in an immersive virtual environment (Garau et al., in press). Participants spent several minutes exploring a space in which avatars reacted to their proximity in different ways. During this time, their electrodermal activity, or palmar sweating, was measured using some sensors attached to the hand. Electrodermal activity is traditionally used as a measure of arousal. Four scenarios were presented to experimental subjects in a between subject design (each subject only saw one of the scenarios). These scenarios were (a) the avatars were all static, (b) the avatars moved but did not respond to the presence of the experimental subject, (c) the avatars moved and looked at the subjects when they came within a certain distance, and (d) the avatars talked to the subjects when the subjects first entered the room and otherwise behaved as in (c). Getting these data in this way just allowed us to monitor physiological parameters continuously and subjected to a diverse range of "natural" experiences (though in a virtual environment); needless to say, a human under everyday conditions (moments of stress, relaxation, excitation, etc.) would have similar GSR. The main technical features of the GSR sensors and data acquisition are as follows. Signal input range: 0–30.0 μS; accuracy: ±5% and ±0.2 μS; maximal bandwidth: 5 Hz; and sample rate: 32 Hz. In this case, the ensuing binary sequence count amounts to 37 of approximately 45,000 bits each.

Finally, we also tested our approach against numerical samplings of the Ornstein–Uhlenbeck stochastic process (Van Kampen, 1985). The rationale for using this stochastic process as a comparison with the real biological processes is that most of the stochastic processes observed in nature are very well modelled by this process. In fact, it is the only stochastic process (up to a Galilean transformation) that is Gaussian, Markovian and stationary. Its probability and transition probability functions are given by

$$P(x,t) = \frac{1}{\sqrt{2\pi\sigma}} \exp\left[-\frac{(x-\mu)^2}{2\sigma^2}\right]$$

$$P(x_2,t_2;x_1,t_1) = \frac{1}{\sqrt{2\pi\sigma(1-\mathrm{e}^{-2(t_2-t_1)/\tau})}}$$

$$\times \exp\left[-\frac{((x_2-\mu)-(x_1-\mu)\,\mathrm{e}^{-2(t_2-t_1)/\tau})^2}{2\sigma^2(1-\mathrm{e}^{-2(t_2-t_1)/\tau})^2}\right]$$

respectively, where μ is the mean value of the stochastic variable, σ its standard deviation and τ is the relaxation time of the process. In order to be closer to the real experiments, we furthermore rounded down the numerical outputs to only three or at most four decimal digits.

Last but not least, the outputs of a numerical network of 1024 artificial Hodgkin–Huxley neurons underwent as well the above statistical scrutiny but failed and, hence, will be not considered hereafter. This negative result can be interpreted as the natural randomness being an attribute difficult to simulate numerically or, for the numerical models, as a further benchmark to be taken into account.

Results of calculations

As it was suggested in The last digit fluctuation method, we start determining the optimal encoding parameters R, L. They have the following values:

1. $R = 3.600$, $L = 3136$ for neurophysiological brain response data.
2. $R = 1.268$, $L = 560$ for galvanic skin response data.
3. $R = 0.500$, $L = 512$ for Ornstein–Uhlenbeck numerical sampling.

Table 1 summarizes the results obtained after applying the usual statistical tests described in Statistical tests to measure randomness to two samples of experimental biometric data labelled as NBS I and NBS II (for neurophysiological brain signals) and GSR (for galvanic skin response). The samples consisted of 126, 126 and 39 sequences, respectively, of 20,000 bits each, obtained after partitioning the original bit sequences (see Experimental data for details) into shorter subsequences

Table 1 Results of FIPS statistical tests

FIPS statistical tests	Source of data			
	NBS	GSR	OU	Pseudo-random
Monobit test	1	1	1	1
Poker test	1	0.976	1	1
Runs test	0.992	0.976	1	1
Long run test	1	1	1	1
Total results	0.992	0.976	1	1

The entries denote the fraction of sequences that passed the corresponding test.

of the said length, which is sufficient for the tests shown in Table 1. The column NBS comprises the results from the samples NBS I and II. The shorthand OU stands for Ornstein—Uhlenbeck and refers to the test performed using the OU process (126 numerically generated sequences). For the pseudo-random sequences (PRG) we used the Lahey—Fujitsu generator. One can see that practically all sequences satisfy the conditions required by FIPS tests.

Table 2 Results of the Maurer and Normalized Complexity tests

	Source of data			
	NBS	GSR	OU	Pseudo-random
Maurer test				
Block length = 6	1	—	1	1
Block length = 7	1	—	1	1
Block length = 8	1	—	1	1
Block length = 9	1	—	1	1
Block length = 10	1	—	1	1
Block length = 11	1	—	1	1
Normalized complexity	1	1	1	1

The entries denote the fraction of sequences that passed the corresponding Maurer test and Lempel—Ziv normalized complexity test.

The results of the Maurer and normalized complexity tests applied to the same data are presented in Table 2 but, because Maurer's test requires very long sequences to perform well, it could only be applied to the original (360,000 bit

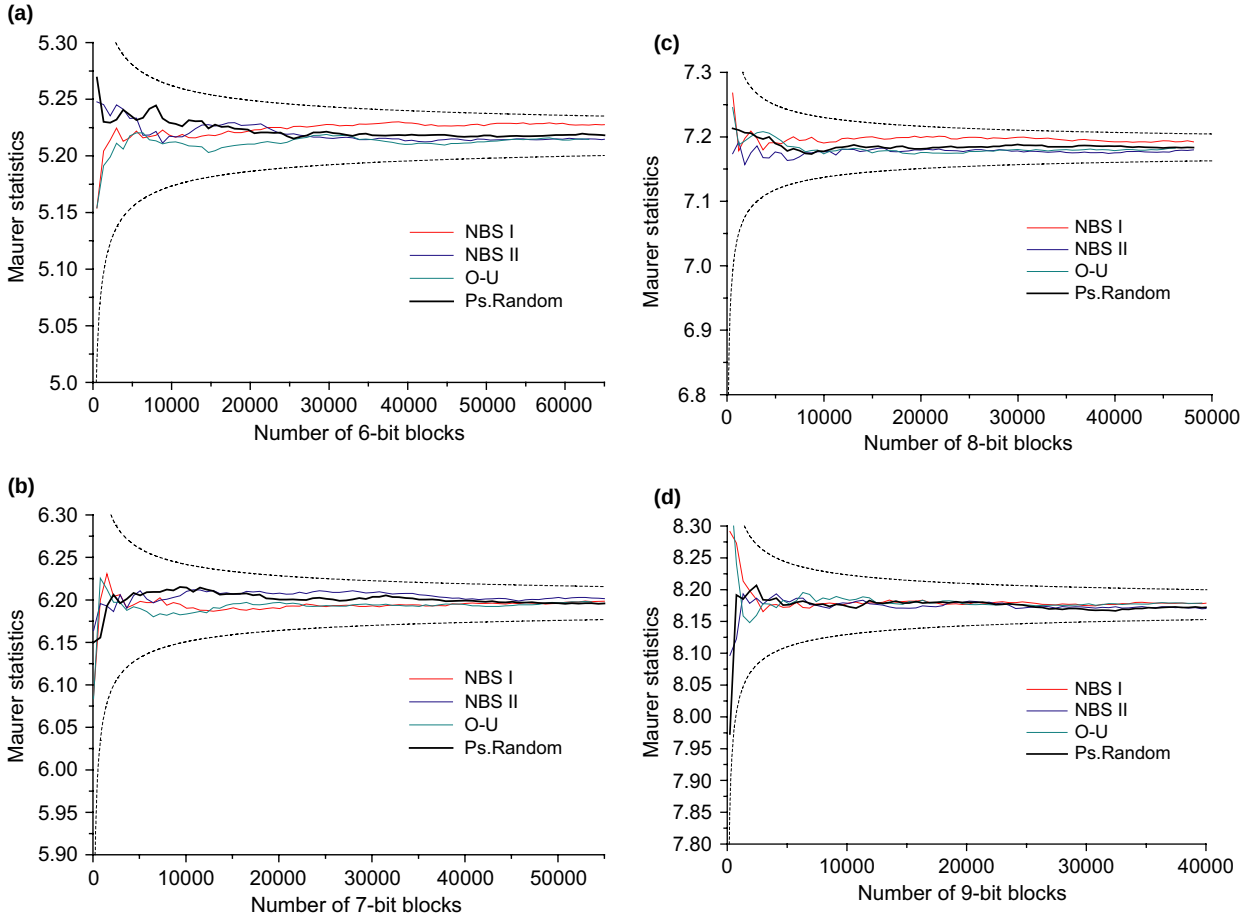

Figure 1 Plots of Maurer's test statistics versus the number of blocks for blocks of lengths 6—9.

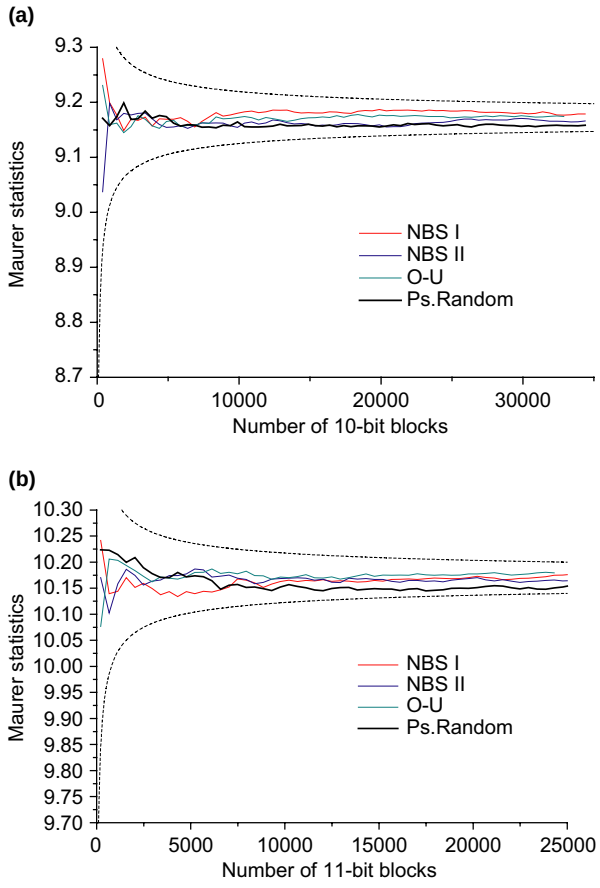

Figure 2 Plots of Maurer's test statistics versus the number of blocks for blocks of lengths 10 and 11. Observe that, in this case, the biological random sequences perform even better than the Lahey—Fujitsu benchmark.

long) NBS sequences. The GSR data are at the moment too short due to the experimental restrictions. The column NBS comprises the results from the samples NBS I and II.

Since Maurer's test is particularly recommended by many authors and institutions (ALGO, 2001), we additionally present the graphs of the value of Maurer's statistics plotted versus the number of blocks of a given length (Figs. 1 and 2).

It is worthy of notice that the "biological" curves lie very well between the predetermined bounds (NIST, 2001) for the significance level 0.01. One can even see that, for the longer blocks, biological data behave even better than the Lahey—Fujitsu benchmark.

Conclusions

We proposed a new method of generating random sequences based on biological phenomena and specified two of them which we have extensively analyzed. The crucial fact in implementations of our method is the use of biological systems that allow a simple data acquisition and provide a profuse sampling of readings with at least four fluctuating accurate digits. In this paper we showed that our method works very well for the two biological phenomena considered, namely, brain signals and galvanic skin responses, providing some clear evidence in support of our approach. Let us underline again that the use of a virtual environment in obtaining the latter responds only to a methodological convenience; similar data had been obtained in a real environment. It turns out that, applying a very natural encoding method, we are able to obtain random bit sequences that pass in almost 100% of the cases both the commonly recommended FIPS statistical tests and the more sophisticated Maurer and Lempel—Ziv complexity tests. Interestingly enough, neuronal signals generated artificially failed to produce random bit sequences.

Other biometric signals that we consider interesting to be checked for randomness are EEG (electroencephalogram) and EMG (electromyogram). Both of them can be obtained with non-invasive techniques with the only requirement of an adequate amplifier. Further candidates to biometric random number generators include blood volume pulse and similar easy-to-get measurements that, even when regular on the surface, may contain randomness in their internal structure. Any of these possibilities might be very important from the point of view of the implementation of our algorithms for generating random bit sequences via biometric methods. The practical introduction of such technology will need extensive scrutiny and verification procedures.

Acknowledgements

Partially supported by Polish—Spanish Scientific Cooperation Program (PAS-CSIC), grant 20/2001-2002. M. Garau collaborated in the GSR experiments. The support to J.S. by Polish Scientific Committee grant 8T11D02019 is kindly acknowledged.

References

Algorithms Group (ALGO). Algorithms and parameters for secure electronic signatures. European Electronic Signature Standardization Initiative Steering Group, v. 2.1; October 19, 2001.

Amigó JM, Szczepanski J, Wajnryb E, Sanchez-Vives MV. Estimating the entropy rate of spike trains via Lempel—Ziv complexity. Neural Computation 2004;16(3).

FIPS PUB 140-2, Federal Information Processing Standards Publications. Security requirements for cryptographic modules; May 25, 2001.
Garau M, Slater M, Pertaub DP, Sasse MA, Razzaque S. The response of people to avatars in an immersive virtual environments. Presence: Teleoperators and Virtual Environments, in press.
Information Technology—Security Techniques. Officer's contribution on ISO/IEC JTC 1/SC 27's role in the standardization of Biometrics; August 30, 2002.
Jain A, Bolle R, Pankanti S. Biometrics, personal identification in a networked society. Norwell, Massachusetts: Kluwer Academic Publishers; 1999. p. 20—34.
Key Management Policy and Practical Framework. KPMG consulting inc. report; January 2002.
Lempel A, Ziv J. On the complexity of an individual sequences. IEEE Trans Inform Theory 1976;IT-22:75—88.
Maurer U. A universal statistical test for random bit generators. Advances in cryptology. CRYPTO '90; 1990. p. 409—20.
Menezes AJ, van Oorshot PC, Vanstone SA. Handbook of applied cryptography. Amsterdam: CRC Press; 1996.
NIST Special Publication 800-22. A statistical test suite for random and number generators for cryptographic applications; May 15, 2001.
Sanchez-Vives MV, Nowak LG, McCormick DA. Membrane mechanisms underlying contrast adaptation in cat area 17 in vivo. J Neurosci 2000;20:4267—85.
Van Kampen NG. Stochastic processes in physics and chemistry. Amsterdam: North Holland; 1985.
X9. F4 Working Group, ANSI/ASC X9.84. Biometric information management and security; April 2001.

Janusz Szczepanski received the M.Sc. degree in mathematics from Warsaw University in 1979 and the Ph.D. degree in applied mathematics from the Polish Academy of Sciences in 1985. He is a researcher at the Institute of Fundamental Technological Research (Polish Academy of Science) in Warsaw and also a consultant on cryptography with the Polish Certification Authority (Root) for Public Key Infrastructure (Centre of Trust and Certification CENTRAST SA). He received the Polish Academy of Sciences Award in 1989 and in 1992 Kosciuszko Foundation Fellowship (NY) for research visit in Snowbird Research Center (USA). In 2000 and 2003 he was Visiting Scientist at the Miguel Hernández University (Spain). His research interests include cryptography, information theory and application of dynamical systems and stochastic processes to biological systems.

Eligiusz Wajnryb received the M.Sc. degree in theoretical physics in 1978 and the Ph.D. degree in statistical physics in 1983 from the University of Warsaw. He was a postdoctoral fellow at the University of Minnesota (1992—1994) and at RWTH Aachen (1999—2001). He is Associate Professor at the Institute of Fundamental Technological Research in Warsaw. Currently he is on leave in the Mechanical Engineering Department of Yale University. His research interests include numerical methods in fluid dynamics, hydrodynamic interactions and application of stochastic processes to biological systems.

José M. Amigó received the Ph.D. degree in theoretical physics from the University of Göttingen (Germany) in 1987. He was a postdoctoral fellow at the National Aerospace Laboratory in Tokyo (1989—1990) and a system analyst with an aerospace company in Madrid (1991—1997). Currently he is Associate Professor of Applied Mathematics at the Miguel Hernández University and researcher at the Operations Research Centre of this university in Elche.

Maria V. Sanchez-Vives received the M.D. and Ph.D. degrees in neuroscience from the University of Alicante in 1992. Postdoctoral fellow in neurobiology at Rockefeller University (1993—1994) and Yale University (1995—1999), she is currently Associate Professor of Physiology at the Miguel Hernández University and a researcher on neurophysiology at its Institute of Neuroscience (also belonging to the Spanish Board of Scientific Research CSIC) in San Juan de Alicante.

Mel Slater (D.Sc. from the University of London, 2000) is Professor in the Department of Computer Science, University College London, where he leads the Virtual Environments and Computer Graphics research group. He was Visiting Professor at UC Berkeley in 1991—1992, and Visiting Scientist at the MIT Research Laboratory of Electronics in 1998.