# ARCHIVE EDITION OF

# IRPS BULLETIN

Volume 18 No 3 March, 2005

Office Bearers : 2003 - 2006

Editorial

Regional Vice President's Report

Paper

New Members and Address Changes

Return to Archive Home Page

# OFFICE BEARERS : 2003 - 2006

## President:

R.H. Pratt
**Dept. of Physics**
**Univ Pittsburgh, PA**
**15260 USA**

## Secretariat:

D.A. Bradley
**School of Physics,**
**University of Exeter**
**Stocker Road**
**Exeter EX4 4QL UK**

## Treasurer:

A. Ljubicic
**Rudjer Boskovic Institute**
**Bijenicka 54**
**Zagreb 41000 Croatia**

## Chair, Advisory Board

M.J. Cooper
**Department of Physics**
**University of Warwick**
**Coventry CV4 7AL U.K.**

## Regional Vice Presidents:

***North America:***
J. Hubbell (USA)

***South and Central America:***

A. Paschoa (Brazil)

***Africa and Middle East:***

D.T.L. Jones (South Africa)

***East Europe***
L. Musilek (Czech Republic)

***F.S.U***
A.V. Korol (Russia)

***Western Europe:***

M.J. Farquharson (U. K.)

***S.E. Asia :***

S.C. Roy (India)

***Australasia :***
D.C. Creagh

## Executive Councillors:

P. Bergstrom (U.S.A.)

L. Gerward (Denmark)

J.E. Fernandez (Italy)

R.T. Mainardi (Argentina)

J. O'Meara (Canada)

K. Singh Thind (India)

D. McLean (Australia)

T. Nakamura (Japan)

| | | |
|---|---|---|
| | (Australia)<br>***North East Asia:***<br>Luo Zhengming (PR China) | |

EDITORIAL BOARD

***Editor :*** P.M. Bergstrom (U.S.A.)
***Editorial Committee :*** D.C. Creagh (Australia) S.A. McKeown (Australia)

Home Page

IRPS

# EDITORIAL

The President's column for this issue is replaced by a column from Dudley Creagh, vice-president for Australasia. This column reports progress made on two major research instruments in Australia.

Additionally, we have a column from Croatia regarding the physical realization of random numbers. The question arises "what do random numbers have to do with Radiation Physics"?

The answer lies in the increasing amount of computing power available to the average radiation physicist. This computing power has enabled the widespread application of the Monte Carlo transport method to model problems of importance in radiation physics. The statistical description of the laws of physics at the appropriate level, the quantum level, leads to the need to sample the underlying probability distributions. The sampling of these laws requires the use of large numbers of random numbers.

There are many algorithms available that provide pseudo-random numbers, a sequence of numbers usually random for all practical purposes. The article presented here uses a physical approach, measurement of the noise voltage at the terminals of a Zener diode. Beyond the interesting details of this particular generator, a solid state device, and the non-solid state heartbeat approach also discussed, this article provides a nice overview of other uses of random numbers.

***Paul Bergstrom***

Home Page | Next

REGIONAL VICE PRESIDENT'S REPORT

# NEWS FROM AUSTRALIA

## Dudley Creagh, Australasia

Exciting things are happening in Australia at present as far as science is concerned.

The Australian Synchrotron Project continues to gather momentum, with the construction of the building well under way ***(Figures 1 and 2)***, and the letting of contracts for the injection system (Danfysik), the magnets (CMS alphatech/Buckley systems), and the vacuum chambers (FMB). As well, a number of universities and instrumentalities have pledged $5 million each for the construction of beamlines. These include Melbourne and Monash Universities, the CSIRO, ANSTO, MiniFAB, and the New Zealand Government. Beamline design is progressing, and the Infra Red Beamline for which I am responsible, has made good progress in the determination of the best way of extracting the IR beam (1 to 100 microns).

A new robotic telescope has just been commissioned at the Australian National University's Siding Spring Observatory. This $9 million telescope was funded by the British philanthropist Dr Martin ("Dill") Faulkener. It has a 2m diameter mirror. Under the agreement ANU will receive 15% of experimental time and students in Australia and the UK will be able to access the facility. For further information see

http://www.faulkes-telescope.com

Recent grants by the Australian Government and industry will see further research into gravity waves and to the establishing of a Gravity Discovery Centre at Gin Gin (New South Wales).

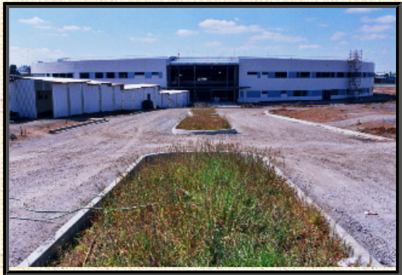


***Figure 1 :*** Entrance to the building

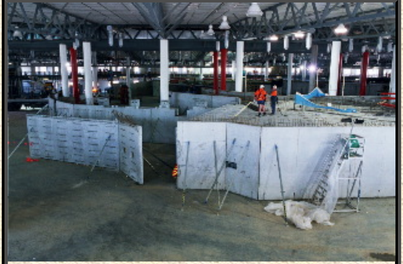


***Figure 2 :*** Shielding walls under construction

Previous Home Page Next

PAPER

# Producing Non-deterministic Random Numbers from Weakly Correlated Random Events

## Mario Stipcevic

Rudjer Boškovic Institute, Bijenicka 54, P.O.B. 180, HR-10002 Zagreb, Croatia

Email : Mario.Stipcevic@irb.hr

Non-deterministic random bits are needed in many scientific fields. Unfortunately today's computers are very limited in their ability to produce them. We present here a method for extraction of non-deterministic random binary numbers (bits) from random physics events and one practical realization of a physical generator based on it. It is shown that even if events are weakly correlated the method delivers increasingly good randomness in the limit of slow sampling. The method is also characterized by its ability to produce random bits periodically. A sample of approximately $10^9$ bits produced by the physical generator prototype is subjected to a series of well-known statistical tests showing no weaknesses.

PACS numbers: 05.40.-a, 02.50.Ng, 03.67.Dd

## 1. MOTIVATION

Today's computers are Turing machines governed by deterministic laws. It has been noticed that such machines cannot solve certain class of problems because of their inability to produce random numbers. For example, it is impossible to simulate, in every aspect, a simple radioactive decay on a deterministic machine because a computer program that would be able to do this must be able to produce a sequence of decay times which is by no means deterministic. Furthermore, a class of so called ***randomized algorithms*** can only be performed with help of a random number generator (eg. Soloway-Strassen primality test [1]). Such algorithms solve efficiently certain problems which are not known to be efficiently solvable on a deterministic Turing machine.

Consequently, a complete machine that is believed to be the ultimate universal computing machine is referred to as "Turing machine with a random number generator" or "probabilistic Turing machine" [2,3].

Since computers play an increasingly important role in modern science and life, it is also increasingly important to develop good and trustworthy random number generators.

The classical approach to generating random numbers is to approximate the non-deterministic generator of random numbers by a carefully chosen mathematical function which produces approximately random numbers. Such a function, of course, can be calculated on Turing machines.

Without loss of generality we will only consider random bit generators (RBG). The basic technique is as follows. First, one chooses at will an integer number $x_0$ (so called ***seed***) from a large set of numbers that are known to be valid seeds for a given function $f$. (Good coverage of the theory and practice of pseudo-random generators may be found in [4-12].)

Then one calculates: $$x_1 = f(x_0) \qquad (1)$$

Iterating this as follows: $$x_{i+i} = f(x_i), \quad i = 1, 2, 3 \ldots \qquad (2)$$

results in a sequence of numbers: $x_1, x_2, x_3, \ldots$ (3)

These numbers converted to bits and put together side-by-side form a long sequence of ***pseudorandom bits***. Sometimes, in order to obtain better "randomness", not all bits from the numbers $x_i$ are used to form the sequence but only a pre-selected part (for example the most significant half).

Variants of this basic technique exists but the underlying property of all pseudo-random generators is that they ***must*** accept a seed, a form of mathematical initial state that completely determines the sequence of bits produced thereafter. The idea behind all this is that to someone who does not know the seed and/or function $f$ (or does not care about them), the sequence of bits produced appears to be random.

Pseudo-random numbers can be produced efficiently and are used a lot in simulations of stochastic processes like passage of particles through matter [16] or speeding up of calculation of exact problems such as multi-dimensional integration or primality testing [17]. This widespread use of pseudo-random numbers comes from the belief that "good" generating functions which apparently approximate true randomness quite well for most purposes of statistical simulation exist [7-9,12].

This belief is based on the assumption that those generators who passed a critical number of statistical tests and have accurately simulated some problems in the past, would pass any statistical test and would fit any further application.

A similar inductive way of thinking is in the very heart of fundaments of natural sciences, but in this case it is not more than pseudo-science. The problem is that every new application of a set of pseudo-random numbers is nothing more but yet another test, whose outcome is unknown. For generators that have passed many statistical tests and give truthful results in previous applications, we can believe that probably they are good for similar further applications. However, this is still nothing more than a belief. There is no guarantee that we are getting good results in any particular application.

This situation can be illustrated by examples of unpleasant discoveries. For example in the [13] it has been reported that some well known and otherwise good generators, when used in random walk simulation, yield obvious deviations from the theoretical expectations. Wrongful results of simulations using dignified shift register pseudo-random generators are reported in [14] for 2-D and in [15] for 3-D Ising models.

The great potential for problems in simulations based upon pseudo-random generators comes from the fact that the entropy of the whole pseudo-random sequence, no matter how long, is equal to the entropy of the seed and the description of the generating function only, which is usually not more than a few hundred bits, while a typical simulation makes use of $10^6$ - $10^{10}$ bits. This "low entropy" property is most clearly seen by noting that the optimal compression of a sequence of type (3) would result only in the seed $x_0$ and a decompression routine that equals $f$. Since $f$ is usually publicly known it does not represent a useful source of entropy, thus the only entropy left is that of the seed. And even this tiny entropy, namely the entropy of the seed, has to be provided by somebody or something that has nothing to do with the pseudo-random generator itself. Therefore the conclusion that pseudo-random generators do not generate entropy seems unavoidable.

For applications in cryptography this may be a killing property. For example provability of information-theoretic security of Quantum cryptography protocols such as BB84 [18], EPR [19] or Maurer's SKAPD protocol [20] assumes existence of generators of truly random (nondeterministic) numbers. Even much less complicated applications such as PIN or TAN number generators may not be proven secure if the numbers generated are based on a deterministic procedure. Cases are known where seeding by a low-entropy source (such as clock) led to serious compromise of the subsequent cryptographic protocol. An example is attack to the Netscape's 40 bit RC4-40 [21] challenge data and encryption keys which could be revealed in a minute or so [22]. The authors of that article suspect that 128 bit version RC4-128 would not be much harder to break either if seeding is done in a similar fashion. (This example also shows how a perfectly good cryptographic method may be ruined by a non-educated or malicious implementator.)

All these problems, both in cryptographic and in simulation applications boil down to the fact that it is hard to get truly random data form today's computing machines (usually PC's). Some ad-hoc methods exist [23-25] to extract a handful of random bits per second, but the only way to get a lot of random bits of guaranteed quality in a short time is to add a non-deterministic random bit generator to the computer, thus effectively realizing the probabilistic Turing machine.

Problem, however, is to construct a good enough generator, whose output can be for all practical purposes considered as being truly unpredictable and random. In recent years there has been a significant increase of interest and progress in this area [26-28, 33].

We describe, in this article, a theory and one practical realization of a reliable and fast random bit generator which should not be expensive to produce.

## 2. THE METHOD

Since it is obvious that only physical reality may provide true randomness, the non-deterministic RBG should be based on a repeated measurements of identical, independent physics processes and associated method for extraction of random bits from these measurements. An RBG should be characterized by the following:

1. its output can not be predicted regardless of the amount of knowledge about it (just as it would be impossible to predict outcome of flipping a fair coin by knowing exactly how it looks);
2. two identical generators may not be synchronized to produce the same sequence of bits.

The second requirement could well be regarded as the definition of a non-deterministic generator. This requirement may be reformulated so that a non-deterministic generator may not accept an initial state. This is opposite to pseudo-random generators which must accept an initial state.

Since we do not expect that the measuring of independent physics processes, that is making independent identical experiments whose outcome is random, may form any pseudo-random pattern we are left with only two problems associated with non-deterministic random bit generators. These are:

1. statistical bias, defined as:

$$\boldsymbol{b} = \boldsymbol{p}(1) - 0.5 \tag{4}$$

   where $\boldsymbol{p}(1)$ stands for probability of ones;

2. correlations among bits, among which the most important ***serial correlation coefficient*** is defined as [6]

$$a = \frac{n \sum_{i=0}^{n-1} b_i b_{(i+1) \bmod n} - \left( \sum_{i=0}^{n-1} b_i \right)^2}{n \left( \sum_{i=0}^{n-1} b_i^2 \right) - \left( \sum_{i=0}^{n-1} b_i \right)^2} \tag{5}$$

   where $\boldsymbol{b}_\mathbf{1}$, $\boldsymbol{i}$ = 0 . . . $\boldsymbol{n}$ - 1 denotes $\boldsymbol{i}$-th bit in the sequence.

Both are measures of imperfections that are inevitable in practical realizations of generators. Correlations appear if the measured physics processes (experiments) are not completely statistically independent of each other, whereas statistical bias is mainly associated with imperfections in the measuring equipment (eg. electronics). A serial correlation coefficient is a measure of the extent to which a bit (in a sequence) depends on a previous bit ([6]), and takes on a value between -1 and 1. We suppose that correlations between bits further apart (corresponding to experiments further apart in time) are smaller if not negligible. For truly random sequences of bits, of course, both statistical bias and correlations tend to zero, when the length of the sequence goes to infinity.

The method presented here solves both problems. It consists of counting events which are result of measurement of some random physical process. For example events may be a radioactive decay or tapping of rain drops on a tin roof. These events appear at random but measured for a long time they have some mean period, μ. The state of the counter is examined at regular time intervals with the period $\boldsymbol{T}$ » μ. If the counter state is found to be odd then the output from the generator is "1", otherwise it is "0". Unlike some other methods which require exponential distribution of time intervals between events [29] or sampling of an analog white noise source [30], we will show that this method, in the limit of slow sampling ($\boldsymbol{T}/\mu \to \infty$) leads to vanishing bias and correlations regardless of the distribution of the random process being measured. Therefore it may used to extract random bits from a large variety of processes.

## 3. PRACTICAL REALIZATION OF THE RANDOM BIT GENERATOR

Useful non-deterministic random bit generator built in hardware should satisfy several requirements:

1. The bit sampling method must not rely strongly on any property of the measured physical process other than its randomness, at least in some easily achievable limit;

2. The generator should withstand reasonable tolerance in components and operating conditions (eg. supply voltage, temperature, EM noise) without the need for (re)calibration or compensation;

3. Possible malfunctions during the lifetime of the generator should be foreseen and checked for at each generator restart (for example like recommended in [31]) or even continuously;

4. Sequences of bits produced by the generator should pass, with a high probability, any known statistical randomness test.

In the generator described here physical processes in a Zener diode serve as a source of randomness. The noise voltage at terminals of the diode is "measured" by a special electronic circuit at regular time intervals. Each measurement results in a random bit.

The circuit presented in ***Fig.1*** follows the method of operation described in the previous section. It consists of the following five blocks:

1. A source of electric noise;

2. A DC decoupling capacitor C;

3. A circuit for digitizing the noise voltage consisting of a comparator controlled with a rough automatic zero-bias correction circuitry;

4. A counting circuit (JK flip-flop);

5. A sampling circuit which delivers a bit upon an external request.

It is a well known fact that a Zener diode operating in a reverse polarity and the current strength near the knee, can serve as a noise generator. For example, a 6.8 Volt commercial Zener diode can produce a noise fluctuation of an amplitude of 30 to 50 mV (peak to peak) with a mean frequency of zero crossings of the order of 10 MHz [32].

It is also well known that a Zener diode with a knee voltage of less than 6.2 V operates mainly in the quantum mechanical (tunneling) regime, while the diodes with the knee above that operate mainly in the micro plasma regime [32]. Both regimes have ideal properties of unpredictability needed for a truly random noise voltage source.

The generator functions in the following way. Noisy voltage from the Zener diode is AC decoupled from the digitizing stage which consists of a comparator COMP controlled with a rough automatic zero-bias feedback control. The capacitor $C$ in the series with the output resistance $R$ of the noise source and the effective input resistance $R_i$ of the comparator forms a major contribution to an unwanted "memory" $t_e = C(R + R_i)$. If physical events are not completely independent of each other there will be another persistence ***ôp*** giving rise to the total memory: $t = t_e + t_p$. Luckily, this "memory" effect dies off exponentially with the time distance between the two variations, thus one can conclude that any two variations that are distant enough in time may be considered as statistically independent. Whenever this applies, our method is valid, as will be explained later.

Nevertheless, the "memory" of the circuit limits frequency bandwidth of the noise and sets an absolute upper limit to the bit extraction rate from the generator, which limit is independent of the latter bit extraction method.

Voltage variations across the diode are shown in the ***Fig. 2a***. The negative input of the comparator COMP is connected to a suitable DC reference voltage $V_r$. Between the two inputs of the comparator (positive and negative) a small DC "offset" voltage can be induced by virtue of the resistor $R_i$ and the control current $I_c$ that flows through it. As the result, the positive input of the comparator "sees" the sum of the offset voltage and the noise voltage. Whenever the sum exceeds the reference voltage $V_r$ the output of the comparator goes into the high logical state "1", whereas when the sum goes below the $V_r$ the output goes into the low logical state "0". This is illustrated in the ***Fig.2b***.

By setting the control current $I_c$ to a precise value it is possible to obtain that the output of the comparator COMP spends on average the same amount of time in both states "0" and "1". This behaviour effectively solves the requirement 2.

Already here, at the output of the comparator COMP, there is an approximately equal chance that the state is at logical "0" or at logical "1", i.e. the bias of the sampled output would be close to zero. However, due to technical reasons it is quite difficult to keep the bias below 1/1000 for long term and even this would be not possible without some fine-tuning. Tuning the bias consumes a lot of time (due to its statistical nature) and would therefore be unfavourable for a mass production of the generator.

The present method for extracting random bits eliminates the need to tune the bias to zero value, and actually allows to achieve bias as low as desired, without the need to do any modifications to the circuit.

Event counting is the crucial point of the method. Namely, the JK-type flip-flop ***(Fig. 1)*** performs a continued counting of the events, but keeps track only whether the count is even or odd. The result of the counting appears at the output Q of the JK flip-flop ***( Fig. 2c)*** and represents a new random bit sequence with highly suppressed bias and serial correlation.

To understand how this works it is important to keep in mind that the output Q of the JK flip-flop shall be sampled periodically in time, with the period ***T (Fig. 2d)***. This is a condition for good operation of this generator. The sampling is done by the D-type flip-flop.

In the pure quantum mechanical regime of the Zener diode, intervals between neighbouring voltage breakdowns **D**$t_k$ follow the Exponential distribution. Mixing of the quantum mechanical model with the plasma noise, noise sources other than a Zener diode or other models including effective memory and/or filtering of the noise signal prior to digitization, may lead to more centered distributions such as Poisson or even Uniform-like distribution. The power of this method lies in the fact that the knowledge of the actual distribution of the time intervals between neighbouring voltage breakdowns is irrelevant. It can be shown [33] that under the assumptions ***a)*** that the shape of the distribution stays stable over a period of time substantially larger than the sampling period ***T***, and ***b***) that the voltage breakdowns distant in time are negligibly correlated, both conditions 4 and 5 are fulfilled in the limit of slow enough sampling, more precisely when both of the following is satisfied: $T/\mu \rightarrow \infty$ and $T/\tau \rightarrow \infty$ respectively.

It is important to understand that the output Q of the JK flip-flop always produces "1" after "0" and "0" after "1", therefore its output is not random at all. However a duration of zeros and ones varies randomly (***Fig. 2c***) and periodic sampling of the said output by the D-type flip-flop provides a good quality random bits, in the limit of slow sampling (***T*** » µ and ***T*** »**t** ).

## 4. THE PROTOTYPE

We have constructed a prototype based on the block-diagram in ***Fig. 1*** using a Zener diode standard analog chips and CMOS logic. Bits were produced at 300 kbit/sec. We built four identical circuits and fed their outputs to a PC computer, thus obtaining a total of 1.2 Mbit/sec. Thanks to such a high speed we were able to easily produce long sequences of bits for the subsequent testing. The sequences of bits produced by the physical generator were tested by three batteries of statistical tests: Walker's ENT [34], Marsaglia's DIEHARD [35] and NIST's Statistical Test Suite [36].

The ENT consists of battery of standard tests: entropy, Chi-square, mean value, Monte Carlo pi value test and the serial correlation test. These tests may be evaluated for short sequences thus making possible a fast check of the prototype in the development stage. The most important of them are the mean value and the serial correlation test because they best grasp problems in hardware. The mean value addresses the inequality between number of ones and zeros which is very hard to keep close to zero with imperfect hardware. Non zero serial correlation reflects existence of a short-term memory in the system, as explained in the section 3. Indeed, at the development stage of the prototype a slight consistent bias (positive, of the order of $10^{-4}$ ) has been noticed on all four gadgets which was attributed to the fact that comparator had quite a different rise time from the fall time at its output. This was corrected by taking another comparator after which the bias became undetectable.

Once the generator was debugged and ENT tests passed well, we proceeded by generating long sequences (approx. $10^8$ bits) needed by the DIEHARD, probably the toughest battery of tests known today. Table I shows a typical result of testing of $8\times10^7$ bits (10 megabyte) of random data obtained from the generator.

According to Marsaglia [35] the sequence has failed a test if the p-value of that test is very close to 1 ($p > 0.999999$), otherwise the sequence has passed the test. There are 15 different tests in the DIEHARD, but some are run more than once with different parameters (eg. binary rank test) or on independent parts of the sequence under test (eg. count the 1's). Results in the Table I indicate a random sequence that has passed all the tests.

It is interesting to note that efforts to standardize requirements for random bit generators for use with cryptographic software have been taken, notably the recommendations of NIST [31]. A sequence of $10^9$ bits divided in 100 equally long pieces (files) has been subjected to the NIST's battery of randomness tests, version sts-1.50 [36]. We used the recommended test parameters. Results are summarized in the Table II.

According to the NIST analysis program, the minimum pass rate for each statistical test with the exception of the random excursion (variant) test is approximately 0.9602 whereas the minimum pass rate for the random excursion (variant) test is approximately 0.9527. Taking this into account we conclude that all 16 tests were passed with excellent marks. Passing all three batteries of tests shows that this generator conforms also to the general requirement 4 stated in the section 3.

As one more check of the sampling method itself bits were generated from a cardiogram data of a healthy patient. A record of 1190 consequent heartbeats was made in course of an ergometric stress test. During the test patient is required to walk on a treadmill whose speed varies according to a standardized procedure. Test lasts approximately 12 minutes. The times at which main heartbeat peaks occur were considered as physical "events". Taking $T/\mu \approx 5$ we obtained a sequence of 216 bits using our method. Results of ENT test shown in the Table III indicate excellent randomness. This demonstrates the power of the method which is able to extract good random bits form a sequence of heartbeats which are nearly periodic but have only a slight random jitter.

The conclusion is that heartbeat timings may very well be used as a base for a non-deterministic random generator !

## 5. CONCLUSION

A method for extraction of non-deterministic random bits from random physics processes (such as nuclei decay or noise voltage variations) is presented. The method is characterized by the fact that it ensures a good quality random bits in an easily obtainable limit, that is the limit of slow sampling, regardless of the distribution of times between adjacent processes. A physical random bit generator which makes use of the method and Zener diode noise was built and successfully tested.

The generator is shown to conform to general requirements for non-deterministic generators stated in section 3. A sample of approximately $10^9$ bits produced by the physical generator prototype is subjected to a series of well-known statistical tests showing no weaknesses.

## 6. ACKNOWLEDGEMENTS

[1] R. Soloway, V. Strassen, A fast Monte-Carlo test for primality. SIAM J. Comput., 6(1976)84-85

[2] M.A. Nielsen, I.L. Chuang, Quantum Computation and Quantum Information, (Cambridge University Press, Cambridge, 2000) p. 2.

[3] Wikipedia, the free encyclopedia, Internet URL: http://www.wikipedia.org/wiki/Probabilistic Turing Machine

[4] M. J. Atallah, Algorithms and Theory of Computation Handbook, (CRC Press LLC, Boca Raton, 1998) p. 29.

[5] W. H. Press, B. P. Flannery, S. A. Teukolsky, W. T. Vetterling, Numerical Recipes in C: The Art of Scienti.c Computing, (Cambridge University Press, New York, 1992)

[6] D. E. Knuth, The art of computer programming, Vol. 2, Third edition, (Addison-Wesley, Reading, 1997)

[7] M. Luescher, Comp. Phys. Comm, 79(1994) 100.

[8] F. James, Comp. Phys. Comm. 79(1994) 111.

[9] P. Hellekalek, Mathematics & Computers in Simulation 46(1998) 485.

[10] W. E. Sharp, C. Bays, Computers and Geosciences, 18(1992) 79.

[11] A.J. Miller, P. Mars, Mathematics and Computers in Simulation, 19(1997) 198

[12] G. Marsaglia, Statistics & Probability Letters, 9(1990) 345.

[13] A. Proykova, How to improve a random number generator, Comp. Phys. Comm. 124(2000)125-131

[14] A.M. Ferrenberg, D.P.Landau, Y.J.Wong, Phys. Rev. Lett. 69(1992)3382

[15] P. Grassberger, Phys. Lett. A 181(1993)43 14

[16] S. Agostinelli et. al, Nucl. Instr. and Meth. A 506(2003) 250.

[17] M. O. Rabin, J. Number Th. 12(1980) 128.

[18] C. H. Bennet, G. Brassard, Quantum cryptography: Public key distribution and coin tossing, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, (IEEE, New York, 1984) p. 175.

[19] A. K. Ekert, Quantum Cryptography Based on Bell's Theorem, Phys. Rev. Lett. 67 (1991) 661-663

[20] U. Maurer, IEEE Transactions on Information Theory, 39 (1993) 733.

[21] R. L. Rivest, The RC4 Encryption Algorithm, RSA Data Security Inc., Mar. 12, 1992.

[22] I. Goldberg, D. Wagner, Dr. Dobb's, January 1996

[23] D. Davis, R. Ihaka, P. Fenstermacher, Cryptographic Randomness from Air Turbulence in Disk Drives in: Lecture Notes in Computer Science Advances in Cryptology - Crypto '94, Springer Verlag, Berlin, 1984) p. 839.

[24] D. Eastlake, S. Crocker, J. Schiller, Randomness Recommendations for Security, Internet RFC 1750, December 1994.

[25] T. Ts'o, private communication. See also Linux man page urandom(4) and source code of Linux kernel ver. 2.4.18, .le random.c

[26] Internet URL: http://random.com.hr/products/random/hg32 .html

[27] A Fast and Compact Quantum Random Number Generator, T. Jennewein et. al., arXiv:quantph/9912118v1

[28] Internet URL: http://www.idquantique.ch/

[29] C. H. Vincent, J. Phys. E 3(1970) 594.

[30] V. Bagini, M. Bucci, A design of Reliable True Random Number Generator for Cryptographic Applications, in: Proceedings of CHES'99 Workshop, (Springer Verlag, Berlin ,2000) p. 204.

[31] Security Requirements for Cryptographic Modules, Federal Information Processing Standards Publication 140-1, (FIPS, Gaithersburg, 1994)

[32] P. I. Somlo, Electronics Letters, 11 (1975) 290.

[33] M. Stipcevic, Fast nondeterministic random bit generator based on weakly correlated physical events, Rev. Sci. Instr. 75(2004)4442-4449

[34] ENT - A Pseudorandom Number Sequence Test Program, J. Walker, Internet URL: http://www.fourmilab.ch/random/

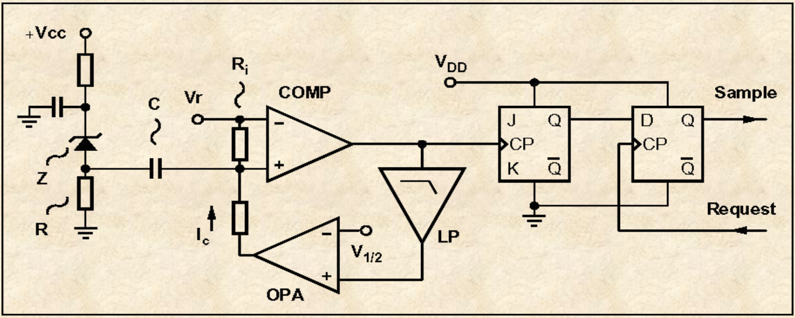
[35] DIEHARD battery of stringent randomness tests (various articles and software), G. Marsaglia, Internet URL: http://stat.fsu.edu/~geo/diehard.html, also available on CDROM online

[36] A. Rukhin et. al., A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, NIST Special Publication, (NIST, Gaithersburg, 2001)

---

## FIGURES and TABLES :

***Fig. 1 :*** Schematic diagram of the non-deterministic random bit generator



* * * * * *

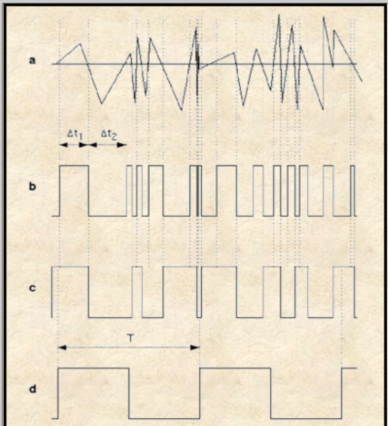


***Fig 2 :***

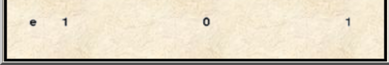
Signals at different points of the hardware generator :

a) analog diode noise,

b) output of the comparator COMP,

c) output Q of the JK flip-flop,

d) final output of the generator (D flip-flop)

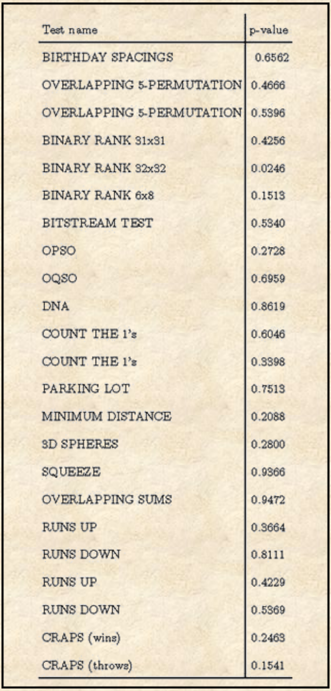


| | | | |
|---|---|---|---|
| e | 1 | 0 | 1 |

* * * * * *

## TABLE I

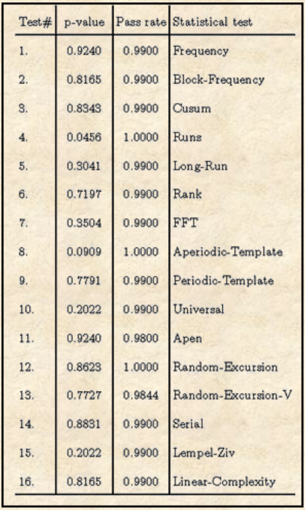
Typical result of the DIEHARD tests for the hardware non-deterministic generator



| Test name | p-value |
|---|---|
| BIRTHDAY SPACINGS | 0.6562 |
| OVERLAPPING 5-PERMUTATION | 0.4666 |
| OVERLAPPING 5-PERMUTATION | 0.5396 |
| BINARY RANK 31x31 | 0.4256 |
| BINARY RANK 32x32 | 0.0246 |
| BINARY RANK 6x8 | 0.1513 |
| BITSTREAM TEST | 0.5340 |
| OPSO | 0.2728 |
| OQSO | 0.6959 |
| DNA | 0.8619 |
| COUNT THE 1's | 0.6046 |
| COUNT THE 1's | 0.3398 |
| PARKING LOT | 0.7513 |
| MINIMUM DISTANCE | 0.2088 |
| 3D SPHERES | 0.2800 |
| SQUEEZE | 0.9366 |
| OVERLAPPING SUMS | 0.9472 |
| RUNS UP | 0.3664 |
| RUNS DOWN | 0.8111 |
| RUNS UP | 0.4229 |
| RUNS DOWN | 0.5369 |
| CRAPS (wins) | 0.2463 |
| CRAPS (throws) | 0.1541 |

## TABLE II

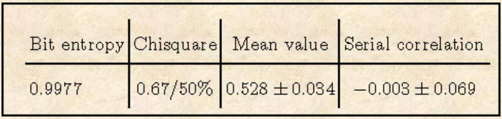
Test of randomness extracted from heartbeats



| Test# | p-value | Pass rate | Statistical test |
|---|---|---|---|
| 1. | 0.9240 | 0.9900 | Frequency |
| 2. | 0.8165 | 0.9900 | Block-Frequency |
| 3. | 0.8343 | 0.9900 | Cusum |
| 4. | 0.0456 | 1.0000 | Runs |
| 5. | 0.3041 | 0.9900 | Long-Run |
| 6. | 0.7197 | 0.9900 | Rank |
| 7. | 0.3504 | 0.9900 | FFT |
| 8. | 0.0909 | 1.0000 | Aperiodic-Template |
| 9. | 0.7791 | 0.9900 | Periodic-Template |
| 10. | 0.2022 | 0.9900 | Universal |
| 11. | 0.9240 | 0.9800 | Apen |
| 12. | 0.8623 | 1.0000 | Random-Excursion |
| 13. | 0.7727 | 0.9844 | Random-Excursion-V |
| 14. | 0.8831 | 0.9900 | Serial |
| 15. | 0.2022 | 0.9900 | Lempel-Ziv |
| 16. | 0.8165 | 0.9900 | Linear-Complexity |

## TABLE III

Test of randomness extracted from heartbeats



| Bit entropy | Chisquare | Mean value | Serial correlation |
|---|---|---|---|
| 0.9977 | 0.67/50% | $0.528 \pm 0.034$ | $-0.003 \pm 0.069$ |

Previous | Home Page | Next

# NEW MEMBERS and ADDRESS CHANGES

## *Welcome to New Members :*

| | |
|---|---|
| Dr Jouni Uusi-Simola Finland | Dr. Hedi Kharrati Tunisia |

New Members' addresses are listed in the Contact Members' Details (click on country next to name)

| | |
|---|---|
| Previous | Home Page |

# Austria

| | |
|---|---|
| Dr Roberto Capote Noy | International Atomic Energy Agency<br>Nuclear Data Section<br>P.O. Box 100<br>Wagramerstrasse 5<br>Vienna A-1400<br>AUSTRIA<br><br>*Email* : R.CapoteNoy@iaea.org |

# Croatia

| | |
|---|---|
| Dr. Ines Krajcar Bronic | Radiocarbon and Tritium Laboratory<br>Department of Physics<br>Rudjer Boskovic Institute<br>P.O. Box 1016,   Bijenicka 54<br>10001  Zagreb<br>CROATIA<br><br>*email:* krajcar@rudjer.irb.hr |
| Mr. Kresimir Jakovcic | Rudjer Boskovic Institute<br>Bijenicka 54<br>10000  Zagreb<br>CROATIA |
| Dr. Ivana Jelovica | Faculty of Philosophy<br>Omladinska 14<br>51000 Rijeka<br>CROATIA |

| | |
|---|---|
| Dr. Zoran Kaliman | Faculty of Philosophy<br>Omladinska 14<br>51000 Rijeka<br>CROATIA<br>*email:* kaliman@mapef.pefri.hr |
| Dr. Milica Krcmar | Rudjer Boskovic Institute<br>Bijenicka 54<br>Zagreb 41001<br>CROATIA<br>*email :* mkrcmar@rudjer.irb.hr |
| Mr. Zvonko Krecak | Rudjer Boskovic Institute<br>P.O. Box 1016<br>Zagreb 41001<br>CROATIA<br>*email :* krecak@rudjer.irb.hr |
| Dr. Ante Ljubicic | Rudjer Boskovic Institute<br>Bijenicka 54<br>Zagreb 41000<br>CROATIA |
| Dr. Vladimir Lokner | Hazardous Waste Management Agency<br>10000 Zagreb<br>Savska 41 IV<br>CROATIA<br>*email:* vladimir.lokner@apo.tel.hr |
| Dr. (Mrs) Saveta Milajanic | Rudjer Boskovic Institute<br>Bijenicka c. 54<br>10000 Zagreb<br>CROATIA<br>*email:* saveta@rudjer.irb.hr |

| | |
|---|---|
| Dr. Bogomil Obelic | Rudjer Boskovic Institute<br>P.O. Box 1016<br>Zagreb 41001<br>CROATIA<br>*email :* obelic@rudjer.irb.hr |
| Dr. Nada Orlic | Faculty of Philosophy<br>University of Rijeka<br>Omladinska 14<br>Rijeka 51000<br>CROATIA |

# Czech Republic

| | |
|---|---|
| Dr. Tomas Cechak | Czech Technical<br>University in Prague<br>Faculty of Nuclear<br>Sciences and<br>Physical Engineering<br>Brehova 7<br>Prague 1 11519<br>CZECH REPUBLIC<br>*email* cechak@br.fjfi.cvut.cz |
| Prof. Jaroslar Kluson | Czech Technical University in<br>Prague<br>Faculty of Nuclear Sciences and<br>Physical Engineering<br>Brehova 7<br>Prague 1 11519<br>CZECH REPUBLIC<br>*email* kluson@br.fjfi.cvut.cz |

| | |
|---|---|
| Dr. Ladislav Musilek | Faculty of Nuclear Sciences and<br>Physical Engineering<br>Brehova 7,<br>Praha 1 115 19<br>CZECHOSLOVAKIA<br><br>*email:* musilek@br.fjfi.cvut.cz |
| Dr. Miroslav Pardy | Department of Theoretical Physics<br>and Astrophysics<br>Masaryk University<br>Kotlarska 2 BRNO 61137<br>CZECH REPUBLIC<br><br>*email:* pamir@physics.muni.cz |

# Denmark

| | |
|---|---|
| Prof. Leif I. Gerward | Physics Department<br>Bldg. 307,<br>Technical University of Denmark<br>Kgs. Lyngby DK- 2800<br>DENMARK<br><br>*email:* gerward@fysik.dtu.dk |
| Dr. Per Hedemann Jensen | Head of Section<br>Applied Health Physics<br>Danish Decommissioning<br>Building 214<br>Riso National Laboratory<br>Roskilde DK- 4000<br>DENMARK<br><br>*email:* p.hedemann@dekom.dk |

| | |
|---|---|
| Dr. Bente Lauridsen | AHF-214<br>Riso National Laboratory<br>Roskilde DK- 4000<br>DENMARK<br>*email:* bente.lauridsen@dekom.dk |

## Finland

| | |
|---|---|
| Dr. Servo Kasi | Kajavankatu 6 B 45<br>FIN-04230 Kerava<br>FINLAND<br>*email:* servo.kasi@helsinki.fi |
| Dr. Jouni Uusi-Simola | HUSLAB<br>Department of Nuclear Medicine<br>P.O. Box 340<br>FIN-00029 HUS<br>FINLAND |

## France

| | |
|---|---|
| Dr. Monique Jung | Laboratoire PHASE<br>23, rue du Loess<br>B.P. 20 67037 Strasbourg-Cedex 2<br>FRANCE<br>*email:* Monique.jung@phase.c-strasbourg.fr |

| | |
|---|---|
| Dr. Cecile Malgrange | Lab de Mineralogie-Cristallographie<br>Universite Paris 6<br>4 place Jussieu<br>F-75252 Paris    Cedex 5<br>FRANCE<br>*email :* cecile.malgrange@lmcp.jussieu.fr |

## Germany

| | |
|---|---|
| Mr Nadir O. Hashim | FB-7 Physik<br>University Siegen<br>Emy-noether-Campus<br>Walter Flex Str. 3<br>D-57068<br>GERMANY<br>*email:* hashim@hep.physik.uni-siegen.de |
| Professor Syed M. Qaim | Research Centre<br>Institute of Nuclear Chemistry<br>D-52425<br>Juelich<br>GERMANY |
| Dr. Maria S.A. Zankl | GSF-Forschugszentrum fur Umwelt<br>und Gesundhelt<br>Institut fur Strahlenschutz<br>Ingolstadter Landstr 1<br>85764 Neuherberg<br>GERMANY<br>*email:* zankl@gsf.de |

# Gibraltar

Dr. John Pardo

32 Ross House
Red Sands Road
GIBRALTAR

*email :* tribunal@gibnet.gi

# Greece

Prof. Ioannis Kandarakis

Technological Educational Institute
Department of Medical Instruments
Technology
Ionising Radiation Laboratory
Agiou Spyridonos
12210-Aigaleo
Athens
GREECE

*email:* kandarakis@teiath.gr

# Hungary

Prof. Guyla J. Csikai

4010 Debrecen-10
Pf. 1105
HUNGARY

*email :* csikai@delfin.klte.hu

# Italy

| | |
|---|---|
| Dr. Jorge E. Fernandez | Laboratorio di Ingegneria Nucleare<br>di Montecuccolino<br>Universita di Bologna<br>via dei Colli 16<br>I-40136<br>ITALY<br>*email :* jorge.fernandez@mail.ing.unibo.it |

# Portugal

| | |
|---|---|
| Mr Joao A.S. Barata | Universidade da Beira<br>Interior<br>Department of Fisica<br>Rua marues 2 Avilae<br>Bolama<br>P-60201-001<br>Covilha<br>PORTUGAL |
| Professor Carlos A.N. Conde | Department of Physics<br>Universidade de Coimbra<br>Coimbra<br>P- 3004-156<br>PORTUGAL |
| Professor Margarida Costa | Departmento de Fisica<br>Universidade de Coimbra<br>Coimbra 3004-156<br>PORTUGAL<br>*email:* guida@pollux.fis.uc.pt |

| | |
|---|---|
| Professor Isabel Lopes | Departmento de Fisica<br>Universidade de Coimbra<br>Coimbra 3004-156<br>PORTUGAL<br>*email:* isabel@lipc.fis.uc.pt |
| Prof. A.P. de Leao Policarpo | Departmento de Fisica<br>Universidade de Coimbra<br>3004-156 Coimbra<br>PORTUGAL<br>*email:* policarpo@lipc.fis.uc.pt |
| Dr. L. M. Tavora | ESTG,<br>Inst. Politécnico de Leiria,<br>Morro do Lena - Alto do Vieiro<br>2411-901 Leiria<br>PORTUGAL<br>*email:* lmtavora@estg.ipleiria.pt |

## Romania

| | |
|---|---|
| Dr. Dan M. Timus | National Institute for Laser, Plasma and Radiation Physics<br>Electron Accelerators Department<br>PO Box MG-36<br>Bucharest R-76900<br>ROMANIA<br>*email :* dante@alpha2.infim.ro<br>timusmdan@yahoo.co.uk<br>timusdan@netscape.net |

# Russia

| | |
|---|---|
| Dr. Andrei V Korol | Department of Physics<br>St Petersburg State Maritime Technical University<br>101 Leninski Prospect<br>198262 St Petersburg<br>RUSSIA |
| Dr. Dmitry A. Kovalev | Usacheve Str., 35, b/1<br>Moscow 119048<br>RUSSIA |
| Dr. Konstantin Kozlovskii | Moscow State Engineering Physics Institute<br>31 Kashimskoe Sh.<br>Moscow 115409<br>RUSSIA |
| Dr. Alexander Shikanov | Federal Nuclear Geophysics and Geochemist Center (FNGGC)<br>140 100 Ramenskoe<br>Neftegazosjimka<br>RUSSIA |
| Dr. Eugene A. Shikanov | Usacheve Str., 35, b/1<br>Moscow 119048<br>RUSSIA |
| Prof. Victor L. Sukhorukov | Rostov State University of Transport Communication<br>N. Opolcheniya Square 2<br>Rostov-na-Donu 344038<br>RUSSIA<br>*email:* vls@AAAnet.ru |

| | |
|---|---|
| Dr. Alexander S. Tsybin | Department of Solid State Physics<br>Moscow Engineering Physics Institute<br>(State University)<br>Kashirskoe Shosse 31<br>Moscow 115405<br>RUSSIA<br><br>*email:* tsybin@tpark.ru |

## Slovenia

| | |
|---|---|
| Dr. Matjaz Korun | Jozef Stefan Institute<br>Jamova 39<br>Ljubljana 1000<br>SLOVENIA<br><br>*email:* matjaz.korun@ijs.si |

## Spain

| | |
|---|---|
| Prof. Pedro Coll Buti | Universidao Politecnica de Catalunya<br>Department de Fisica i Enginyeria Nuclear<br>C/Avenida Diagonal 647<br>Barcelona 08028<br>SPAIN |

| | |
|---|---|
| Dr. Fernando Legarda | Universidad del Pais Vasco<br>Departamento de Ingenieria Nuclear<br>Mecanica de Fluidos<br>E.T.S. Ingenieros Industriales<br>Alameda de Urquijo s/n<br>48013 Bilbao<br>SPAIN<br><br>*email:* inpleibf@bi.ehu.es |

## Sweden

| | |
|---|---|
| Professor Klas Malmqvist | Department of Nuclear Physics<br>University of Stockholm-Karolinsk Inst<br>Lund Institute of Technology<br>Lund University<br>PO Box 128<br>Lund 22100<br>SWEDEN |

## U.K.

| | |
|---|---|
| Ms Layla Mohammed Ali | School of Physics<br>University of Exeter<br>Stocker Road<br>EX4 4QL<br>U.K. |

| | |
|---|---|
| Dr. David A. Bradley | School of Physics<br>University of Exeter<br>Stocker Road<br>Exeter EX4 4QL<br>U.K.<br>*email:* d.a.bradley@exeter.ac.uk |
| Professor Malcolm J. Cooper | Department of Physics<br>University of Warwick<br>Coventry CV4 7AL<br>U.K.<br>*email:* m.j.cooper@warwick.ac.uk |
| Dr. M. J. Farquharson | Department of Radiography<br>City University<br>Rutland Place<br>Charterhouse Square<br>London EC1 M6PA<br>U.K.<br>*email:* M.J.Farquharson@city.ac.uk |
| Ms. Kalotina Geraki | Department of Radiography<br>City University<br>Rutland Place<br>Charterhouse Square<br>London EC1M 6PA<br>U.K.<br>*email:* k.geraki@city.ac.uk |
| Dr. Walter B. Gilboy | Physics Department<br>University of Surrey<br>Guildford<br>Surrey GU2 5XH<br>U.K.<br>*email:* w.gilboy@surrey.ac.uk |

| | |
|---|---|
| Dr. Christopher C. Goddard | BNFL Environmental Services<br>Berkeley Centre<br>Berkeley<br>Gloucestershire GL13 9PB<br>U.K.<br>*email:* goddard@myrealbox.com |
| Dr. Stuart Green | Department of Medical Physics<br>and Bioengineering<br>Queen Elizabeth Medical Centre<br>Birmingham B15 2TH<br>U.K.<br>*email:* Stuart.Green@uhb.nhs.uk |
| Dr. Richard Hugtenburg | School of Physics and Astronomy<br>University of Birmingham<br>Birmingham B15 2TT<br>U.K.<br>*email:* r.p.hugtenburg@bham.ac.uk |
| Dr. Russell D. Luggar | Department of Physics<br>University of Surrey<br>Guildford Surrey GU2 5XH<br>U.K.<br>*email:* r.luggar@surrey.ac.uk |

| | |
|---|---|
| Ms. Elaine Ryan | Department of Radiography<br>School of Allied Health<br>Sciences<br>City University<br>Northampton Square<br>London EC1V OHB<br>U.K.<br><br>*email:* e.ryan@city.ac.uk |
| Dr. D. N. Timms | School of Environmental<br>and Earth<br>Sciences<br>Burnaby Building<br>Portsmouth University<br>Portsmouth PO1 3QL<br>U.K.<br><br>*email:* david.timms@port.ac.uk |

## Uzbekistan

| | |
|---|---|
| Dr. Alexander Rakov | Phonon Scientific Indudstrial<br>Association<br>S.Yusupov. St. 50<br>Tashkent 700054<br>UZBEKISTAN |

# Botswana

| | |
|---|---|
| Dr. V.R.K. Murty | Department of Physics<br>University of Botswana<br>Post Bag 0022<br>Gaborone<br>BOTSWANA<br><br>*e-mail :*<br>murtyvrk@mopipi.ub.bw |

# Egypt

| | |
|---|---|
| Professor Nassef Comsan | Nuclear Research Centre<br>Atomic Energy Authority<br>Cairo<br>EGYPT<br><br>*email:* rucycle@rusys.eg.net |
| Dr. Abdel Megid Mamoon | C/- Egyptian Atomic Energy Authority<br>Ahmed al Zmer St<br>Nasr City<br>Cairo<br>EGYPT |

# Ghana

| | |
|---|---|
| Mr. Benjamin Nyarko | Ghana Atomic Energy Commission<br>P.O. Box LG 80<br>Legon-Accra<br>REPUBLIC OF GHANA<br><br>*email:* bjbnyarko@yahoo.co.uk |

# Kenya

| | |
|---|---|
| Mr Michael J Mangala | University of Nairobi<br>Institute of Nuclear Science<br>G.P.O. Box 30197<br>Nairobi<br>KENYA |
| Dr. Amidu Mustapha | Department of Physics<br>University of Nairobi<br>PO Box 30197<br>Nairobi<br>KENYA<br><br>*e-mail :* amustapha@uonbi.ac.ke |
| Dr Indra V S Rathore | Physics Department<br>Kenyata University<br>P.O. Box 43844<br>Nairobi<br>KENYA |

# Libya

| | |
|---|---|
| Dr. Ayad Miftah Shahout | AL-KHOMS<br>P.O. Box 40099<br>LIBYA<br><br>*Email :* shahout@hotmail.com |

# Morocco

| | |
|---|---|
| Professor L Erradi | Faculty of Sciences<br>Department of Physics<br>B.P. 1014<br>Rabat<br>MOROCCO<br><br>*Email :* erradi@hotmail.com |
| Professor Hassane Erramli | Faculty of Sciences<br>Department of Physics<br>B.P. 2390 - 4000<br>Marrakech<br>MOROCCO |
| Professor Jillali Ghassoun | University of Cadi Ayyad<br>Faculty of Science<br>Semlalia<br>Department of Physics BP 2390<br>Marrakech 40000<br>MOROCCO |

| | |
|---|---|
| Professor Fouad Lahlou | Faculte des Sciences<br>Dhar Mehraz<br>BP 1796 (Atlas)<br>Fes<br>MOROCCO<br><br>*email:* flahlou@yahoo.com |

## Namibia

| | |
|---|---|
| Professor J. A. Oyedele | Department of Physics<br>University of Namibia<br>Private Bag 13301<br>Windhoek<br>NAMIBIA<br><br>*email:* oyedelej@unam.na |

## Nigeria

| | |
|---|---|
| Dr. Emmanuel H. Agba | Department of Physics<br>Faculty of Science<br>Benue State University<br>PMB 102 119<br>Makurdi<br>NIGERIA<br><br>*email :* hemenagba@yahoo.com |

| | |
|---|---|
| Dr. Nneoyi Egbe | Radiography Department<br>College of Medical Science<br>University of Calabar<br>PMB 1115<br>Calabar 540001<br>NIGERIA<br>*email :* nneoyiegbe@yahoo.com |
| Dr. Taofeeq Ige | National Hospital (Medical Physics)<br>PMB 425<br>Garki Ablja<br>NIGERIA<br>*email:* taofeeqige@yahoo.com |
| Dr. Samuel O Inyang | Department of Physics<br>University of Calabar<br>Calabar 540001<br>Cross River State<br>NIGERIA<br>*email :* inyangso@yahoo.com |
| Dr. Sunday A. Jonah | Centre for Energy<br>Research and Training<br>Ahmadu Bello University<br>PMB 1014<br>Zaria<br>NIGERIA<br>*email:* jonahsa2001@yahoo.com |

| | |
|---|---|
| Dr. Christopher Mayaki | Centre for Energy Research and Training<br>Ahmadu Bello University<br>PMB 1014<br>Zaria<br>NIGERIA<br>*email:* chris_mayaki04@yahoo.com |
| Dr. Folorunso O. Ogundare | Department of Physics<br>University of Ibadan<br>Ibadan<br>NIGERIA |
| Dr. Olusola I. Okunade | Centre for Energy Research and Training<br>Ahmadu Bello University<br>PMB 1014<br>Zaria<br>NIGERIA |

## Saudi Arabia

| | |
|---|---|
| Dr. Osama Fageeha | Environmental Protection Department<br>Aramaco<br>PO Box 12526 31311<br>SAUDI ARABIA |

# South Africa

| | |
|---|---|
| Ms Mary Assiamah | Schonland Research Institute<br>University of the Witwatersrand<br>Private Bag 3<br>Wits 2050<br>SOUTH AFRICA<br>*email:* assiamah@src.wits.ac |
| Mr. Samuel S. S. Bakhane | iThemba Labs<br>P.O. Box 722<br>Somerset West 7129<br>SOUTH AFRICA |
| Dr Dobroslana Budka | iThemba Labs<br>P.O. Box 722<br>Somerset West 7129<br>SOUTH AFRICA<br>*email:* dobrusiabudka@tlabs.ac.za |
| Professor Andy Buffler | Department of Physics<br>University of Cape Town<br>Rondebusch 7701<br>SOUTH AFRICA<br>*email:* abuffler@science.uct.ac.za |
| Dr Mohamed E.M. Eisa | iThemba Labs<br>P.O. Box 722<br>Somerset West 7129<br>SOUTH AFRICA<br>*email:* memeisa@yahoo.com |

| | |
|---|---|
| Dr. Egbert E. R. Hering | Department of Medical Physics<br>Groote Schuur Hospital<br>Observatory 7925<br>SOUTH AFRICA |
| Dr. Dan T. Jones | iThemba LABS<br>(Laboratory for Accelerator Based Sciences)<br>P O Box 722<br>Somerset West 7129<br>SOUTH AFRICA<br><br>*email:* jones@tlabs.ac.za |
| Prof. Rex J. Keddy | Dept. of Medical Physics<br>University of the Witwatersrand<br>Private Bag 3<br>Powits<br>Johannesburg 2050<br>SOUTH AFRICA<br><br>*email:* mwrexilm@mweb.co.za<br>keddy@sic.wits.ac.za |
| Dr. Steven S. Maage | iThemba Labs<br>P.O. Box 722<br>Somerset West 7129<br>SOUTH AFRICA<br><br>*email:* maagest@nac.ac.za |
| Dr. Given G.K. Mabala | 827 Khatello Street<br>Molapo<br>P.O. Moroka 1860<br>SOUTH AFRICA |

| | |
|---|---|
| Mr Johan A. Mars | iThemba Labs<br>P.O. Box 722<br>Somerset West 7129<br>SOUTH AFRICA |
| Mr R. D. Mavunda | Health Physics Service<br>Schonland Research Institute<br>for Nuclear Sciences<br>University of the Witwatersrand<br>Private Bag 3, Wits 2050<br>Johannesburg<br>SOUTH AFRICA |
| Mr Mandlenkosi Msimange | iThemba Labs<br>P.O. Box 722<br>Somerset West 7129<br>SOUTH AFRICA<br>*email:* m_msimanga@hotmail.com |
| Mr Tshepp Ntsoane | iThemba Labs<br>Materials Research Group<br>P.O. Box 722<br>Somerset West 7129<br>SOUTH AFRICA |
| Dr Carlos A. Pineda-Vargas | iThemba Labs<br>P.O. Box 722<br>Somerset West 7129<br>SOUTH AFRICA |
| Dr Gabriel G. Pitsoane | iThemba Labs<br>P.O. Box 722<br>Somerset West 7129<br>SOUTH AFRICA |

| | |
|---|---|
| Dr Wojciech J. Przybylowicz | iThemba Labs<br>P.O. Box 722<br>Somerset West 7129<br>SOUTH AFRICA |
| Dr Jolanta M. Mesjasz-Przybylowicz<br><br>< | iThemba Labs<br>P.O. Box 722<br>Somerset West 7129<br>SOUTH AFRICA |
| Mr. Johann van Rooyen | iThemba LABS<br>(Laboratory for Accelerator Based Sciences)<br>P O Box 722<br>Somerset West 7129<br>SOUTH AFRICA<br><br>*email:* johanvr@nac.ac.za |
| Dr Thulaganyo P. Sechogela | iThemba LABS<br>(Laboratory for Accelerator Based Sciences)<br>P O Box 722<br>Somerset West 7129<br>SOUTH AFRICA |
| Ms Patience P. Segonyane | IBA and SEM<br>Radiation Utilization Group<br>Necsa<br>Pretoria<br>SOUTH AFRICA<br><br>*email:* sps@necsa.co.za |
| Professor John F. Sharpey-Schafer | iThemba LABS<br>(Laboratory for Accelerator Based Sciences)<br>P O Box 722<br>Somerset West 7129<br>SOUTH AFRICA |

| | |
|---|---|
| Dr. Julyan J.E. Symons | iThemba Labs<br>P.O. Box 722<br>Somerset West 7129<br>SOUTH AFRICA<br>*email:* symons@tlabs.ac.za |
| Dr. Chris Theron | iThemba Labs<br>P.O. Box 722<br>Somerset West 7129<br>SOUTH AFRICA<br>*email:* ctheron@tlabs.ac.za |
| Dr. Grzegorz J. Tylko | iThemba Labs<br>P.O. Box 722<br>Somerset West 7129<br>SOUTH AFRICA |
| Mr. Dawid de Villiers | Department of Physics<br>Stellenbosch University<br>Stellenbosch<br>SOUTH AFRICA<br>*email:* dawid@sun.ac.za |

## Syria

| | |
|---|---|
| Dr. Ibrahim Othman | Atomic Energy Commission<br>P.O. Box 6091<br>Damascus<br>SYRIA<br>*email:* aecs@mail.sy |

# Tunisia

| | |
|---|---|
| Dr. Hedi Kharrati | Ecole Supérieure de la Santé<br>5000 Monastir<br>TUNISIA |

# Turkey

| | |
|---|---|
| Dr. Ahmet Cengiz | Uludag University<br>Faculty of Science and Literature<br>Department of Physics<br>Gorukle<br>Bursa 16059<br>TURKEY |
| Dr. Orhan Gurler | Uludag University<br>Fen Edebiyat Foikultesi<br>Fizik Bolumu Forukle Kampusu<br>16059 Bursa<br>TURKEY |
| Dr. Arzu Kurtoglu | Istanbul Technical University<br>Institute for Nuclear Energy<br>Ayazaga Campus<br>80626 Maslak<br>Istanbul<br>TURKEY |
| Dr. Sezai Yalcin | Gaza University<br>Kastamona Egitim Fakultesi<br>Kastamona 37200<br>TURKEY |