



SDI Review Form 1.6

PART 1:

Journal Name:	<u>British Journal of Mathematics & Computer Science</u>
Manuscript Number:	2013_BJMCS_5252
Title of the Manuscript:	Transform of various Random Noises in sequences of proved random numbers
Type of the Article	Research Paper

General guideline for Peer Review process is available in this link:

(<http://www.sciencedomain.org/page.php?id=sdi-general-editorial-policy#Peer-Review-Guideline>)

- This form has total 7 parts. Kindly note that you should use all the parts of this review form.



SDI Review Form 1.6

PART 2: Review Comments

	Reviewer's comment	Author's comment (if agreed with reviewer, correct the manuscript and highlight that part in the manuscript. It is mandatory that authors should write his/her feedback here)
<u>Compulsory</u> REVISION comments	0. The whole paper looks like an automatic translation from another language (apparently French). It should be substantially improved because many sentences have no meaning (or very unfitting one) as written and one has to figure out what the authors meant by it. 1. In the first sentence of the Abstract authors mention "sequences of numbers proven random". However, regarding notion of "provably random sequences of numbers" I would note that there is no such object, simply because there is no definition of random sequence of numbers, as noted in Sect 3.4). Authors should concentrate on some known problem with the initial random sequence and show that their extraction procedure does improve it without spoiling any other property of random numbers. 2. It is well known that IID numbers cannot be obtained by pseudo-random generators and therefore the first sentence in Sect. 1.1 is wrong. 3. Words of language are not random but contain complex correlations and are not of maximal entropy. therefore sentence "... a text is a noise randomly chosen." (bottom of Sect 6.1) simply	In phrase 1 of the summary I replace "In a previous paper, we have shown how to obtain sequences of numbers proved random." by "In a previous paper, we have shown how to obtain sequences of numbers proved random : these sequences can be regarded as a sample of IID sequences of random variables." In phrase 1 of section 1.1 "To have IID random numbers" is replaced by "To have IID random or pseudo-random numbers" At the end of section 6.1, I add in the footnote of "This is especially true for texts: a text is a noise randomly chosen : footnote : It is not surprising...." "This is especially true for texts: a text is a noise randomly chosen : footnote : We mean that text can be regarded as a realization of some sequences of random variables. It is not surprising...." In section 6.4, new pages 17-18, I add " Indeed, a way in order to understand what we want to mean when we say



SDI Review Form 1.6

	does not hold. 4. Authors have failed to give a clear description of the extraction procedure and dependence of its parameters (e.g. compression ratio) on initial sequence. Please write a section with detailed description that could be understood by a reader averagely skilled in the art. 5. A fundamental problem with the authors' approach is that they substitute the (non existing) definition of randomness by requirement that a sequence obeys some distribution which is a very weak criterion of randomness. Just an example imagine a sequence of 8-bit binary sequential numbers 0,...,255. this sequence is perfectly uniformly distributed and yet it is not random. There are many technical imperfections that are uncorrectable by the reader, such as in the beginning of Sect 1.2 where a-prime and b-prime are never defined! The authors' reasoning throughout the paper is at places very shaky and follows the rule of thumb, for example where they use undefined terms like "not too large", "very random" etc. By virtue of that, in hardly any instance the word "proof" is completely appropriate. Furthermore, some of the "proofs" rely heavily on previous work of the author(s) which extends over 600 pages of text of similar quality.	"noises not too deterministic" is to compare with min-entropy : $H_1(X) = \min_x \log \frac{1}{P_f(X=x)}$ Indeed, by Shaltiel (2011), if $H_1(X) \geq qN$, T_q cannot be an 0-extractor : i.e. a necessary condition in order that $T_q(Y_{1; \dots; Y_N})$ is IID is that $P_f(Y_{1; \dots; Y_N}) = \frac{1}{2^{qN}}$ for all $m(1; \dots; N) \geq 2^{qN}$. If it is not case, we say "the noise y_n is too deterministic". For example, assume $m = O(4^{-1036})$, $q = 33$ and $N_0 = 105$. Then, if y_n is not too deterministic, $P_f(Y_{1; \dots; Y_N}) = \frac{1}{2^{qN}}$ where $\frac{1}{2^{qN}} = \frac{1}{2^{33 \cdot 105}}$. Then, if $H_1(X) \geq qN$, $\frac{1}{2^{qN}} = \frac{1}{2^{33 \cdot 105}}$. Then, there exists $(1; \dots; N_0)$
--	--	---



SDI Review Form 1.6

	This paper substantially lags behind the state of the art of the research of similar kind (for example references 23, 31 and 34 called out in the paper).	) such that $Pf(Y_{-1}; \dots; Y_{-N}) = (_0 1; \dots; _0N)$ $g = O(533N_)$. Of course, in this case, there is a very big breakdown of randomness and one can say that Y_{-N} is very deterministic. " We replace section 8.1 " 8.1 Description of the method We are interested in the choice of parameters in the building of IID sequences. Then, we consider the case of sequences of noises y_{0n} $2 f0; 1; \dots; m \square 1g, n = 1; 2; \dots; N0$. We set $y_n = y_{0n} + rand0(n)] = m$ where $rand0(n)$ is pseudo random generator. Then, by applying Remark 4.3, we shall impose that r $N3$ $0 q2q$ m $_1 = N0 :$ Remark that this condition is less good than the condition used when one impose
--	---	---



SDI Review Form 1.6

		that the Lipschitz coefficients K_0 are small : $(m)K_0N_02q$ $m_{-10} \leq 3$. " by " 8.1 Choice of parameters We are interested in the choice of parameters in the building of IID sequences. Then, we consider the case of sequences of noises y_0^n $2 \leq n \leq m$; $n = 1, 2, \dots, N_0$. We set $y_n =$ 1 y_0^n $+ \text{rand}_0(n) \cdot m$ where $\text{rand}_0(n)$ is pseudo random generator. Then, by applying Remark 4.3, we shall impose that r N_3 $0 \leq q \leq 2q$ m $m_{-1} = N_0$: Remark that this condition is less good than the condition used when one impose that the Lipschitz coefficients K_0 are small : $(m)K_0N_02q$ $m_{-10} \leq 3$. " For reviewer 1, here is my comment I corrected the paper according remarks
--	--	--



SDI Review Form 1.6

		1,2,3,4. Now, some comments are not true : Thus, a comment is " A fundamental problem with the authors' approach is that they substitute the (non existing) de_nition of randomness by requirement that a sequence obeys some distribution which is a very weak criterion of randomness. Just an example imagine a sequence of 8-bit binary sequential numbers 0,,255. this sequence is perfectly uniformly distributed and yet it is not random." He has not understood that I do not use unidimensional distribution, but multidimensional distribution : the example does not hold in dimension N. Other example "there are many technical imperfections that are uncorrectable by the reader, such as in the beginning of Sect 1.2 where a-prime and b-prime are never de_ned!" : I use a very classical notation which is very known.
--	--	--



SDI Review Form 1.6

Minor REVISION comments		
Optional/General comments		