"Random sequences generation through optical measurements by phase-shifting interferometry"

Francois, M. ; Grosges, Thomas ; Barchiesi, D. ; Erra, R. ; Cornet, Alain

ABSTRACT

The development of new techniques for producing random sequences with a high level of security is a challenging topic of research in modern cryptographies. The proposed method is based on the measurement by phase-shifting interferometry of the speckle signals of the interaction between light and structures. We show how the combination of amplitude and phase distributions (maps) under a numerical process can produce random sequences. The produced sequences satisfy all the statistical requirements of randomness and can be used in cryptographic schemes.

CITE THIS VERSION

OFFPRINT

Random sequences generation through optical measurements by phase-shifting interferometry

M. François, T. Grosjes, D. Barchiesi, R. Erra and A. Cornet

EPL, 98 (2012) 14002

Please visit the new website
www.epljournal.org
The Editorial Board invites you to submit your letters to EPL

EPL is a leading international journal publishing original, high-quality Letters in all areas of physics, ranging from condensed matter topics and interdisciplinary research to astrophysics, geophysics, plasma and fusion sciences, including those with application potential.

The high profile of the journal combined with the excellent scientific quality of the articles continue to ensure EPL is an essential resource for its worldwide audience. EPL offers authors global visibility and a great opportunity to share their work with others across the whole of the physics community.

Run by active scientists, for scientists

EPL is reviewed by scientists for scientists, to serve and support the international scientific community. The Editorial Board is a team of active research scientists with an expert understanding of the needs of both authors and researchers.
Six good reasons to publish with EPL

We want to work with you to help gain recognition for your high-quality work through worldwide visibility and high citations.

1. **Quality** – The 40+ Co-Editors, who are experts in their fields, oversee the entire peer-review process, from selection of the referees to making all final acceptance decisions.

2. **Impact Factor** – The 2010 Impact Factor is 2.753; your work will be in the right place to be cited by your peers.

3. **Speed of processing** – We aim to provide you with a quick and efficient service; the median time from acceptance to online publication is 30 days.

4. **High visibility** – All articles are free to read for 30 days from online publication date.

5. **International reach** – Over 2,000 institutions have access to EPL, enabling your work to be read by your peers in 100 countries.

6. **Open Access** – Articles are offered open access for a one-off author payment.

Details on preparing, submitting and tracking the progress of your manuscript from submission to acceptance are available on the EPL submission website [www.epletters.net](http://www.epletters.net).

If you would like further information about our author service or EPL in general, please visit [www.epljournal.org](http://www.epljournal.org) or e-mail us at info@epljournal.org.

---

**EPL is published in partnership with:**

[European Physical Society](http://www.epljournal.org)
[Italian Physical Society](http://www.epljournal.org)
[EDP Sciences](http://www.epljournal.org)
[IOP Publishing](http://www.epljournal.org)

---

“We’ve had a very positive experience with EPL, and not only on this occasion. The fact that one can identify an appropriate editor, and the editor is an active scientist in the field, makes a huge difference.”

Dr. Ivar Martinv
Los Alamos National Laboratory, USA
Visit the EPL website to read the latest articles published in cutting-edge fields of research from across the whole of physics.

Each compilation is led by its own Co-Editor, who is a leading scientist in that field, and who is responsible for overseeing the review process, selecting referees and making publication decisions for every manuscript.

- Graphene
- Liquid Crystals
- High Transition Temperature Superconductors
- Quantum Information Processing & Communication
- Biological & Soft Matter Physics
- Atomic, Molecular & Optical Physics
- Bose–Einstein Condensates & Ultracold Gases
- Metamaterials, Nanostructures & Magnetic Materials
- Mathematical Methods
- Physics of Gases, Plasmas & Electric Fields
- High Energy Nuclear Physics

If you are working on research in any of these areas, the Co-Editors would be delighted to receive your submission. Articles should be submitted via the automated manuscript system at www.epletters.net

If you would like further information about our author service or EPL in general, please visit www.epljournal.org or e-mail us at info@epljournal.org

Image: Ornamental multiplication of space-time figures of temperature transformation rules (adapted from T. S. Bíró and P. Ván 2010 EPL 89 30001; artistic impression by Frédérique Swist).
Random sequences generation through optical measurements by phase-shifting interferometry

M. François¹, T. Grosges¹(a), D. Barchiesi¹, R. Erra² and A. Cornet³

¹ Project Group for Automatic Mesh Generation and Advanced Methods, Gamma3 Project (UTT-INRIA), University of Technology of Troyes, France - 12 rue Marie Curie, BP 2060, 10010 Troyes Cedex, France, EU
² Network & Information Security, Ecole Supérieure d’Informatique, Electronique, Automatique (ESIEA) 9 rue Vésale, 75005 Paris, France, EU
³ Nanoscopic Physics, Institute of Condensed Matter and Nanosciences, Catholic University of Louvain 2 Chemin du Cyclotron, 1348 Louvain-la-Neuve, Belgium, EU

received 6 December 2011; accepted in final form 6 March 2012
published online 10 April 2012

PACS 42.25.Hz – Interference
PACS 42.30.Va – Image forming and processing
PACS 89.20.-a – Interdisciplinary applications of physics

Abstract – The development of new techniques for producing random sequences with a high level of security is a challenging topic of research in modern cryptography. The proposed method is based on the measurement by phase-shifting interferometry of the speckle signals of the interaction between light and structures. We show how the combination of amplitude and phase distributions (maps) under a numerical process can produce random sequences. The produced sequences satisfy all the statistical requirements of randomness and can be used in cryptographic schemes.

Introduction. – The generation of (pseudo-)random numbers plays a critical role in several applications. Sequences of random numbers have been widely used in many domains, such as statistical mechanics, numerical simulations, gaming industry or cryptography [1]. In practice, the generation of random numbers is an open problem and the production of sequences with randomness properties continues to be investigated. The randomness quality of the sequence is decisive in the choice of their applications. Two main categories of generators can be considered: software and physical generators. For the software generators, the produced sequences are the so-called pseudo-random numbers and the generator is defined as an algorithm enabling to generate sequences of numbers with properties of randomness [2–4]. From a single seed, these generators will always produce the same sequence of numbers. To avoid the problem of determinism, physics random processes are often used for the generation such as quantum noise [5–7], chaotic signals [8,9] laser noise [10] or speckle phenomenon [11–14]. Random phenomena such as photon noise or thermal noise in resistors have been used as physical entropy sources for the generation of truly random bits [15–17]. The thermal noise is the only parameter of integrated circuits that is truly random because an integrated circuit is specially designed to be deterministic in nature. Such non-deterministic generators are often slow during the number generation due to the mechanisms for extracting bits from the physical procedures. The speckle was used to produce a large amount of binary sequences with interesting statistical properties of space and time independence, such as weak correlation between produced sequences [12,18]. Nevertheless, the only weak correlation between produced sequences is not sufficient to ensure a cryptographic randomness quality of the binary sequence. Indeed, speckle images do not always satisfy the basic statistical tests of randomness for cryptographic applications. In the case of generators using broadband optical noise, the randomness properties of the output can be significantly improved by constructing the XOR between each produced signal [19]. Here we propose to improve the randomness quality of speckle for a non-random object by using interferometric detection and by xoring the amplitude and phase.

Optical-field measurements as source of pseudo-random generator. – The selected physical phenomenon used as basis of a random number generator is the well-known speckle phenomenon [20,21]. The speckle comes from diffusers illuminated in coherent light that spontaneously scatter optical waves of random amplitude
and phase, and therefore introduce a random aspect [11–13]. This randomness depends on many parameters such as the nature and the characteristics of the diffuser (surface or volume diffusion, surface roughness and geometry), illumination source and the sensitivity to the detector. In this paper, a method of generating sequences of random numbers based on speckle measurements by phase-shifting interferometry (PSI) [22–24] is proposed. Here, the phase-shifting interferometer corresponds to a Mach-Zehnder interferometer since the diffuser object lies in one arm of the interferometer [21,25,26]. This phase shifting is one of the techniques to extract the phase and the amplitude of the speckle. Such a measurement method is well known and permits to reconstruct the image of the amplitude of the speckle. Such a measurement method is introduced for several decades in optical testing [27]. Such a method owns advantage of a rapid measurement [28]. The collected data are the amplitude and the phase of the light scattered by the object through a CDD camera which digitally captures the interference patterns. The measurement of amplitude and phase maps \(A(x,y)\) and \(\phi(x,y)\) is combined in a numerical process to construct a random sequence. The used experimental setup for PSI recording is displayed in fig. 1. A laser source at wavelength \(\lambda\) provides an illumination and a reference beam. The reference beam is spatially shifted by a phase modulator (phase modulator \(\alpha_1\) on the upper arm in fig. 1) and both beams recombined in front of a camera. Four shifted images (at \(\alpha_1+0, \alpha_1+\pi/2, \alpha_1+\pi, \alpha_1+3\pi/2\)) are used in order to calculate the amplitude and phase maps. The second phase modulator (\(\alpha_2\) on the down arm in fig. 1) and the rotation of the object (\(\theta\) around the y-axis for any diffusely complex object) is only added in order to increase the total number of images that can be generated and to increase the space of parameters. The construction of the random sequence is achieved in three steps:

1) Measurement of amplitude \(A(x,y)\) and phase \(\phi(x,y)\) of the signal. From the amplitude and phase, the complex map function \(F(x,y)\) is computed:

\[
F(x,y) = A(x,y) \exp(2\pi \phi(x,y)).
\] (1)

The vector \(\mathbf{N}\) normal to the complex map \(F(x,y)\) is then computed:

\[
\mathbf{N} = \nabla F(x,y) = (\partial_x F(x,y), \partial_y F(x,y), -1).
\] (2)

2) The second step consists in computing the intensity of \(|F|^2\) and \(|\mathbf{N}|^2\) to produce two new maps \(I_F(n)\) and \(I_N(n)\), with \(n\) the length of the sequence (i.e. \(n\) is corresponding to the number of pixels of the image). The elements of maps \(I_F(n)\) and \(I_N(n)\) are real numbers and all these elements are reduced between 0 and 1. Two new maps are constructed from \(I_F(n)\) and \(I_N(n)\) and are given by

\[
X_F(n) = \text{Int}[\beta_1 |I_F(n)|] \mod S,
\] (3)

\[
X_N(n) = \text{Int}[\beta_2 |I_N(n)|] \mod S,
\] (4)

where \(\beta_1\), \(\beta_2\) and \(S\) are fixed integers (e.g., \(\beta_1 = \beta_2 = 10^7\) and \(S = 256\)). A large value of \(\beta\) allows to take into account a large number of digits to increase the sensitivity between two nearby optical data. The two maps \(X_F(n)\) and \(X_N(n)\) only produce directly random-like images (i.e., images that seem to be random in appearance but not necessarily satisfying cryptographic randomness requirements).

3) The last step consists in applying a binary XOR operator by matching \(X_F(n)\) and \(X_N(n)\) to produce a new map \(\Psi(n)\):

\[
\Psi(n) = X_F(n) \oplus X_N(n).
\] (5)

Such a matching benefits from the differences between \(I_F(n)\) and \(I_N(n)\) (i.e., \(I_F(n)\) can exhibit strong variations whenever \(I_N(n)\) is smoother). That comes from the mixing of orthogonal functions.

The produced sequence \(\Psi(n)\) has a high level of randomness and can be used efficiently. It is important to note that the numerical treatment is a deterministic process. To ensure the cryptographic quality of the output, the sequence \(\Psi(n)\) is evaluated through statistical NIST tests suite for cryptographic applications (National Institute of Standards and Technology). This statistical package of fifteen tests was developped to quantify and to evaluate the randomness of (arbitrarily long) binary sequences produced by either hardware- or software-based cryptographic random or pseudo-random number generators [29]. For each statistical test, a set of \(p_{\text{value}}\)’s is produced and is compared to a fixed significance level \(\delta = 0.01\) (i.e., only 1% of the sequences are expected to fail). Therefore, a sequence passes a statistical test for \(p_{\text{value}} > \delta\) and fails otherwise.
Random sequences generation for phase-shifting interferometry

Table 1: Results of the NIST tests for the produced sequences $X_F(n)$ and $\Psi(n)$.

<table>
<thead>
<tr>
<th>Test Name</th>
<th>$X_F(n)$</th>
<th>$\Psi(n)$</th>
<th>p-value</th>
<th>Result</th>
<th>p-value</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td>0.000000</td>
<td>0.896687</td>
<td>Fail</td>
<td>Pass</td>
<td>0.434157</td>
<td>Pass</td>
</tr>
<tr>
<td>Block-frequency</td>
<td>0.000000</td>
<td>0.727251</td>
<td>Fail</td>
<td>Pass</td>
<td>0.845361</td>
<td>Pass</td>
</tr>
<tr>
<td>Cumulative sums (1)</td>
<td>0.000000</td>
<td>0.879970</td>
<td>Fail</td>
<td>Pass</td>
<td>0.879970</td>
<td>Pass</td>
</tr>
<tr>
<td>Cumulative sums (2)</td>
<td>0.000000</td>
<td>0.724534</td>
<td>Fail</td>
<td>Pass</td>
<td>0.724534</td>
<td>Pass</td>
</tr>
<tr>
<td>Runs</td>
<td>0.000000</td>
<td>0.845361</td>
<td>Fail</td>
<td>Pass</td>
<td>0.845361</td>
<td>Pass</td>
</tr>
<tr>
<td>Longest run</td>
<td>0.000000</td>
<td>0.879970</td>
<td>Fail</td>
<td>Pass</td>
<td>0.879970</td>
<td>Pass</td>
</tr>
<tr>
<td>Rank</td>
<td>0.586378</td>
<td>0.649170</td>
<td>Pass</td>
<td>Pass</td>
<td>0.649170</td>
<td>Pass</td>
</tr>
<tr>
<td>FFT</td>
<td>0.000000</td>
<td>0.980367</td>
<td>Fail</td>
<td>Pass</td>
<td>0.980367</td>
<td>Pass</td>
</tr>
<tr>
<td>Non-overlapping</td>
<td>0.000000</td>
<td>0.106920</td>
<td>Fail</td>
<td>Pass</td>
<td>0.106920</td>
<td>Pass</td>
</tr>
<tr>
<td>Overlapping</td>
<td>0.078439</td>
<td>0.239421</td>
<td>Pass</td>
<td>Pass</td>
<td>0.239421</td>
<td>Pass</td>
</tr>
<tr>
<td>Universal</td>
<td>0.000000</td>
<td>0.950283</td>
<td>Fail</td>
<td>Pass</td>
<td>0.950283</td>
<td>Pass</td>
</tr>
<tr>
<td>Approximate entropy</td>
<td>0.000000</td>
<td>0.707145</td>
<td>Fail</td>
<td>Pass</td>
<td>0.707145</td>
<td>Pass</td>
</tr>
<tr>
<td>Random Excursions</td>
<td>Not applicable</td>
<td>0.068471</td>
<td>Fail</td>
<td>Pass</td>
<td>0.068471</td>
<td>Pass</td>
</tr>
<tr>
<td>Random E-variant</td>
<td>Not applicable</td>
<td>0.048876</td>
<td>Fail</td>
<td>Pass</td>
<td>0.048876</td>
<td>Pass</td>
</tr>
<tr>
<td>Serial (1)</td>
<td>0.000000</td>
<td>0.733731</td>
<td>Fail</td>
<td>Pass</td>
<td>0.733731</td>
<td>Pass</td>
</tr>
<tr>
<td>Serial (2)</td>
<td>0.000000</td>
<td>0.511406</td>
<td>Fail</td>
<td>Pass</td>
<td>0.511406</td>
<td>Pass</td>
</tr>
<tr>
<td>Linear complexity</td>
<td>0.391863</td>
<td>0.948597</td>
<td>Pass</td>
<td>Pass</td>
<td>0.948597</td>
<td>Pass</td>
</tr>
</tbody>
</table>

Fig. 2: Optical maps for amplitude (a) and phase (b) of the diffusely object with double slit, measured by phase-shifting interferometry.

Fig. 3: The computed sequences $X_F(n)$ (a) and $X_N(n)$ (b) from interferometric maps. These maps appear like random images, but do not pass the statistical NIST tests.

Results and discussion. – For the experiment, a semi-transparent diffusely object including a double slit (here an unpolished glass plate) is considered and illuminated by a helium-neon lasers at wavelength $\lambda = 633$ nm and illuminating power $P_W$ varying from 0.5 mW to 35 mW. The detected signals are collected by the CCD camera (with output analog-to-digital converted by 16 bits), the amplitude and phase are computed and are corresponding to maps of size $501 \times 501$ (i.e., $n = 251001$). These amplitude and phase are shown in fig. 2. The two sequences obtained during the processing (i.e., $X_F(n)$ and $X_N(n)$, see fig. 3) are used to produce the final sequence $\Psi(n)$. These sequences seem to be random, but they do not always pass the NIST tests (see fig. 3(a) and table 1 for $X_F(n)$ sequence). The produced sequence $\Psi(n)$ (see fig. 4) is analyzed through the NIST tests and the results are presented in table 1. For the tests “Non-overlapping”, “Random Excursions” and “Random E-variant”, the smallest $p$-value’s of all corresponding subtests are presented. The tests “Random Excursions” and “Random E-variant” can be applied only when a minimum number of cycle in a cumulative sum random walk can be determined. Therefore, these tests are not applicable for an insufficient number of cycles in the sequence [29]. We can note that the tests fail for the $X_F(n)$ sequence. This contrasts with the $\Psi(n)$ sequence which passes successfully all the NIST tests. Such a sequence can be considered as good candidate for the random binary sequence. Moreover, one of the important aspects in the generation of random numbers is the sensitivity related to the initial conditions. Here, for nearby values of the parameters (e.g., the initial laser power $P_W$, the phase modulations $\alpha_1$, $\alpha_2$), the gain $G$ of the detector (i.e. associated with the initial laser power and the sensitivity of the camera), or the complexity of the object and its orientation $\theta$), the constructed sequences are completely different. As
an example, the discrepancy between two different angles for the orientation of the object $\theta$ and $\theta'$ is $\Delta \theta = \theta - \theta' = \lambda/(2\pi L)$, where $L$ is the size of the object [30]. The phase-shifting discrepancies $\Delta \alpha_1 = \alpha_1 - \alpha_1'$ and $\Delta \alpha_2 = \alpha_2 - \alpha_2'$ are given by the resolution of the CCD camera. In practice, the value $\Delta \theta \approx 2.0 \times 10^{-3}$ rad is sufficient to ensure the decorrelation between the measured optical maps. To illustrate the sensitivity to the parameters, we produce two new sequences $\Psi_2(n)$ and $\Psi_3(n)$ obtained by only small modifications of the initial complex map $F$. The modification consists in modifying the phase value of the reference beam $\delta \phi_2$ or $\delta \phi_3$. $\Phi \rightarrow \Phi + \delta \phi$. $F_2(x,y) = A_2(x,y) \exp(j2\pi(\Phi(x,y) + \delta \phi_2))$, with $\delta \phi_2 = 2.0 \times 10^{-3}$ rad and $F_3(x,y) = A_3(x,y) \exp(j2\pi(\Phi(x,y) + \delta \phi_3))$, with $\delta \phi_3 = 2.0 \times 10^{-2}$ rad. If the cryptosystem is sensitive to the parameter value then the produced outputs $\Psi_2$ and $\Psi_3$ should pass the NIST tests and should also be very different from $\Psi$ and not correlated. The correlation between the produced sequences are analysed globally by computing the correlation coefficients of each pair of sequences [31]. Taking the two sequences $\Psi = [\Psi(1), \ldots, \Psi(m)]$ and $\Phi = [\Phi(1), \ldots, \Phi(m)]$, we have

$$C_{xy} = \frac{\sum_{i=1}^{m} (\Psi(i) - \overline{\Psi})(\Phi(i) - \overline{\Phi})}{\left[\sum_{i=1}^{m} (\Psi(i) - \overline{\Psi})^2\right]^{1/2} \cdot \left[\sum_{i=1}^{m} (\Phi(i) - \overline{\Phi})^2\right]^{1/2}}, \quad (6)$$

where $\overline{\Psi} = \sum_{i=1}^{m} \Psi(i)/m$ and $\overline{\Phi} = \sum_{i=1}^{m} \Phi(i)/m$ are the mean values of $\Psi$ and $\Phi$, respectively. The correlation coefficients between these three produced sequences are reported in table 2. The produced sequences $\Psi$, $\Psi_2$ and $\Psi_3$ are very different for near $F$-map distributions (i.e., sensitivity to the initial parameters) and only a very weak correlation is detected. With such discrepancies in the object orientation, phase modulations, detector gain $G$ and input initial laser power $P_W$, the values of real parameters encoded on only 12 bits (i.e., limiting the significant digits relatively to a 64 bits encoded real number), the total number of generable pseudo-random sequences is around $2^{12} \times 2^{12} \times 2^{12} = 2^{48}$. Assuming that the time for the acquisition data is about $150 \text{ ms}$ per parameter set $\{P_W, \theta, \alpha_1, \alpha_2\}$ (the time for the numerical treatment being neglected), an attacker will take in average $1338826$ years to test all the sequences. Therefore, due to the physical time to data acquisition, storage and treatment, the cryptosystem can be considered as secure against exhaustive attacks. Such a system assures high sensitivity to the initial conditions and provides binary sequences of high quality and large space of parameters.

**Conclusion.** – We presented a phase-shifting interferometry digital holography random number generator speckle based on the measurement of the complex wavefront at the plane of the camera. The method combines the amplitude and phase maps under a numerical process to produce a sequence with a high level of randomness. This procedure takes advantage of speckle, interferometric measurement and numerical XOR. All these steps are necessary to construct a robust algorithm passing all statistical tests for cryptographic applications. The proposed method improves speckle-based methods without the constraint of using a random object, assures a weak correlation between the produced sequences and can be used in several applications in cryptography. The advantage of this system is that the method is simple and that the choice of the object remains free even if the object can be as imaginative as possible.

***

The authors thank the Centre de Calcul Intensif ROMEO2 for computational facilities, the Région Champagne-Ardennes and the Conseil Régional de l’Aube for financial supports.

**REFERENCES**
