OTEH
DEFENSIVE TECHNOLOGIES

6th INTERNATIONAL SCIENTIFIC CONFERENCE
ON DEFENSIVE TECHNOLOGIES

OTEH 2014

Belgrade, Serbia, 9 – 10 October 2014

ADSORPTION-DESORPTION BASED RANDOM NUMBER GENERATOR

OLGA JAKŠIĆ
IHTM – Centre of Microelectronic Technologies, University of Belgrade, Serbia olga@nanosys.ihtm.bg.ac.rs,

DRAGAN TANASKOVIĆ
IHTM – Centre of Microelectronic Technologies, University of Belgrade, Serbia dragant@nanosys.ihtm.bg.ac.rs,

DANIJELA RANDJELOVIĆ
IHTM – Centre of Microelectronic Technologies, University of Belgrade, Serbia danijela@nanosys.ihtm.bg.ac.rs,

FILIP RADOVANOVIĆ
IHTM – Centre of Microelectronic Technologies, University of Belgrade, Serbia filip@nanosys.ihtm.bg.ac.rs,

Abstract: *Data tracking and hacking is especially dangerous in modern defence forces where classified data transmission must envolve cryptographic methods for secure and reliable data coding. The more unpredictable the cipher is, the more reliable is the message. Hardware random number generator or true random number generator (TRNG) is crucial part for every telecommunication system that involves secure and confidential electronic data transfer (official state agencies, e-banking, military data networks…) because it generates random numbers from a physical process which provides statistically random noise signals, which are trully unpredictable contrary to pseudo-random number generators generated by various software algorithms. A typical hardware random noise generators employs transducer to convert random physical process (thermal noise, photoelectric effect or other quantum phenomena) to electrical signal, amplifiers and AD convertors. On the other hand, pseudo-random number generation based on methods and algorithms may be examined by statistical tests for randomnes and proove if it is cryptographically secure. We analyze the possibility to implement adsorption-based sensors noise for the creation of allgorithm for pseudo-random number generaton and also the possibility of adsorption-based hardware random generator.*

Keywords: *computer security, random number generator, noise, adsorption, desorption.*

1. INTRODUCTION

The control of an access to a message that is being transfered between different points or stored in a medium prone to physical theft is an ancient challenge with ever growing importance [1]–[3].

In todays digital world security attacs are numerous, either passive (unauthorized reading, traffic analysis, electronic surveillance) or active (modification/deletion of messages/files or denial of service). The quality of typical security services, such as authentication, access control, data confidentiality, data integrity, nonrepudiation, and availability, strongly depends on different encryption algorithms, digital signatures, and authentication protocols that are used as security mechanisms designed to detect/prevent attacs or recover data from a security attack [3].

In every security domain (information security, computer security, local network security or internet security), random numbers are essential for many of these security mechanisms, for instance for generation of secure keys for coding through encifering and decifering, or for secure personal identification. According to Bruce Schneier, Key management is the hardest part of cryptography and often the Achilles' heel of an otherwise secure system [2].

There are two classes of random number generators in use today: *pseudo-random number generators* (PRNGs) and *true random number generators* (TRNGs). PRNGs use mathematical algorithms (completely computer-generated) in order to produce a sequence of random numbers, so with the same starting point (called seed) they produce the same output and hence they are fully deterministic (but still suitable for key generation in stream cifer systems). On the other hand, TRNGs are based on a completely stochastic unpredictable physical process as a means to generate random numbers (like atmospheric noise). Both, PRNGs and TRNGs experience continous development and improvements. Some attainments of PRNGs and TRNGs are listed below.

A. PRNG (deterministic random number generator)

- built-in functions in software environments (rand() in PHP or random() in MATLAB)
- pseudo-random sequence based on Z-transform [4]

– pseudo-random bit generator based on lag time series [5]

B. TRNG (physical random number generator) [6]

– resistors' johnson noise

– Zehner diode – telegraph signal

– lasers' output phase noise optical

– q: spontaneous decay of radioactive nuclei

– detection of photons behind a beamsplitter

The fact is that some physical processes, although being truly stochastic, may not be suitable for truly random number generation because of their noise spectrum which is not entirely flat. The obtained bit sequence is then colored, which means there are slightly more 0s than 1s or vice versa, so there is a certain bias in the signal, which has to be removed. So, even physical random number generators have disadvantages, they may suffer from low bit rate, non-zero bias, correlations along the bit sequence and complex implementations.

There are numerous tests that have been developed to verify the obtained sequence randomness for cryptographic purposes. The first battery of statistical tests for measuring the quality of a random number generator that has been developed by George Marsaglia (an american mathematician and computer scientist who established the lattice structure of linear congruential generators [7]) under name diehard battery of tests [8] is no longer being maintained. Tests from the Statistical Test Suite (STS) developed by the National Institute for Standards and Technology (NIST) [9] became then the state of the art in tests for randomness. Further development has been done in that field in the context of cluster analysis, online testing, tetsting of symetric ciphers and hash functions [10] or real time statistics and new test suits have been developed, like dieharder test suite [11] but none of them is fully applicable for all optical domain. New optical random signal generators or tests for optical random /sequences are yet to be seen.

Our intention here is to investigate the possibility to use the adsorption-desorption process as a means for pseudo random number generation or true random number generation in electrical or optical domain.

In the text that follows, the stochastic nature of the adsorption-desorption process will be adressed first. Then, the algorithms for the generation of pseudo random sequence will be proposed and tested. At the end, we analyze an adsorption based optical random signal generator.

2. THE STOCHASTIC NATURE OF AN ADSORPTION-DESORPTION PROCESS

Adsorption-desorption process is a surface phenomena [12–15]. It takes place on a boundary between two chemical phases (gas-solid, liquid-solid, gas-liquid). Stochasically moving particles from one phase approach the boundary surface, stay on the surface for a speciffic residential time and leave the surface afterwards, stochastically moving in the first phase and being able to come to the boundary surface again after some time. In time, in a stable system (constant pressure, temperature), the process reaches an equilibrium where adsorption and desorption take place uninterruptedly but he surface coverage remains constant: the number of adsorbed particles per time unit equals the number of desorbed particles per time unit. The stoichiometric equation for this process is [16]–[18]

$$A_f + A_g \underset{k_d}{\overset{k_a}{\rightleftarrows}} A_a \tag{1}$$

It sais that a particle in a gas phase (in case of an adsorption on a gas-solid interface) A_g and a free adsorption place on the solid surface A_f reversibly form an adsorbed particle A_a with an adsorption rate k_a and desorption rate k_d.

Comings and leavings are stochastical events, but the kinetics of the process can be treated in a deterministic way at a macroscopic level. The deterministic equation that corresponds to a stoichiometric one in (1) and governs the monolayer adsorption in a closed system (where the overal number of particles remains constant over time) is [19]

$$\frac{dN_a}{dt} = k_a\left(N_0 - N_a\right)\left(M - N_a\right) - k_d N_a \tag{2}$$

M is the number of adsorption sites on the solid surface, N_a is the instantaneous number of adsorbed particles, M-N_a is the instantaneous number of free adsorption sites on the surface, N_0 is the overall number of particles in the system and N_0-N_a is the number of particles in a gas phase.

The adsorption-process as a stochastic phenomena has been studied. The analytical analysis of equilibrium dynamics of fluctuations in adsorption-desorption process is given in [20], [21]. The analytical analysis of kinetics of fluctuations in adsorption-desorption process is given in [22]–[24].

Here we propose the stochastic simulation algorithm suitable for numerical interpretation of the time evolution of the number of adsorbed particles N_a. The algorithm relies on the use of a built in random number generator for simple distributions of chosen programming language. The times between arrivals have an exponential distribution with varying mean. The mean time between arrivals equals the reciprocial of adsorption rate, *i.e.* $1/k_a(N_0$-$N_a)(M$-$N_a)$, according to (2). Likewise, the mean time between departures equals the reciprocial of adsorption rate, *i.e.* $1/k_dN_a$.

The algorithm for the simulation of the process can be summarized as follows:

1. Initialize N_a to zero.
2. First transition is adsorption:

– generate t_1 from exponential distribution with parameter that equals the reciprocial of the initial adsorption rate: $1/k_aN_0M$.

– set $N_a(t_1)$ to 1.

3. If $N_a(t_i)$=0, adsorption is possible only, so:

– generate τ_a from exponential distribution with parameter that equals the reciprocial of the instantaneous adsorption rate: $1/k_aN_0M$.

– set t_i=$t_{i\text{-}1}$+τ_a

– set $N_a(t_i)$= $N_a(t_{i\text{-}1})$+1.

4. Otherwise, generate both times: τ_a from exponential distribution with parameter that equals the reciprocial of the instantaneous adsorption rate: 1/k_a(N_0-N_a)(M-N_a) and τ_d from exponential distribution with parameter that equals the reciprocial of the instantaneous desorption rate: 1/k_aN_a. Then test which transition is more likely to occure

– If minimal free path time of all particles in a gas phase is less than minimal residential time of all adsorbed particles then set t_i=$t_{i\text{-}1}$+τ_a and $N_a(t_i)$= $N_a(t_{i\text{-}1})$+1

– Otherwise set t_i=$t_{i\text{-}1}$+τ_d and $N_a(t_i)$= $N_a(t_{i\text{-}1})$-1

5. Return to step 3.

Figure 1 shows time evolutions of the number of adsorbed particles according to analytical deterministic model (2) and according to proposed stochastic simulation algorithm for a hypothetical process with exemplary values for rate constants, number of adsorption sites on the surface and overall number of particles in the system. Rate constants of adsorption-desorption process can be controlled by system parameters (such as pressure, temperature...) and they both vary in a broad span [25]. For instance, in case of oxygene adsorption on gold, at room temperature, under pressure of 50 kPa, in a reaction chamber of a 3 dm^3, the adsorption rate constant is $8.18{\cdot}10^{-27}$, and the desorption rate constant is 118.21. With ease (by change in pressure or temperature in technologically feasible limits) the rate constants change of several orders of magnitude can be obtained and the new response has new kinetics and new equilibrium dynamics (new response time and new stationary surface coverage.

Generally, every adsorption process has the same shape of time evolution of the number of adsorbed particles, regardless of the initial parameters (the proposed algorithm can be adapted for any initial value, different from zero, which is unlikely even in deep space, it usually is some former stationary value). It is the shape of exponential growth with distinguishable response time and equilibrium value of stationary surface coverage. Far from equilibrium (at the beginning of the process) the fluctuations are the most visible, but they are omnipresent in time and space.

Figure 2 shows the deterministic solution for and stochastic simulations of the number of adsorbed particles during the transition period for the same system (surface of gold, 625 adsorption sites, 652222 gas particles in a gas phase at the beginning, adsorption rate constant 8.18 10^{-27} 1/moleculesec, desorption rate constant 1.182 1/sec). Further focusing on that part of the evolution curve would clearly show that the adsorption is a descreete process that exhibits very fast transitions. That is extreemly important for physical realization and key management in many cryptographic applications.

Figure 3 shows simulated number of adsorbed particles in equilibrium for that system with an important difference: streight line does not represent the deterministic solution but the adsorption limit - the maximal possible number of adsorbed particles and that is the overall number of adsorption centres on the surface.

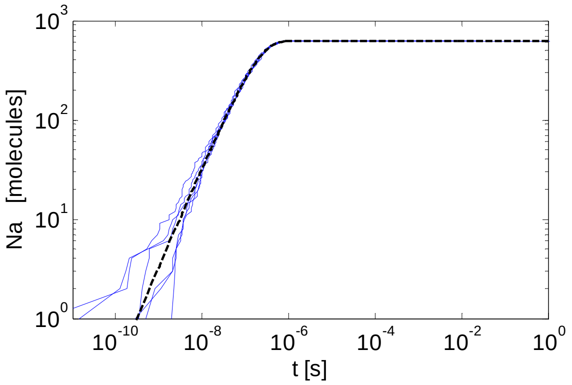

Figure 1: Time evolutions of the number of adsorbed particles on the golden surface with 625 adsorption sites in a system with overall 652222 initial gas particles, adsorption rate constant being 8.18 10^{-27} 1/moleculesec, desorption rate constant being 1.182 1/sec: analytical deterministic solution (black dashed line) and stochastic simulation algorithm (blue zig-zag lines)

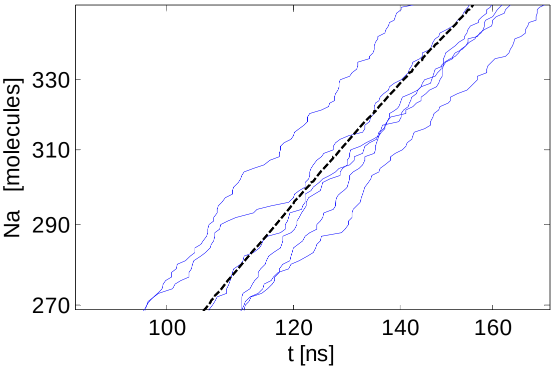

Figure 2: The number of adsorbed particles during the transition period (golden surface with 625 adsorption sites, initially 652222 gas particles in a system, adsorption rate constant 8.18 10^{-27}/moleculesec, desorption rate constant 1.182 1/sec): deterministic solution (black dashed line) and stochastic simulation (blue zig-zag lines)

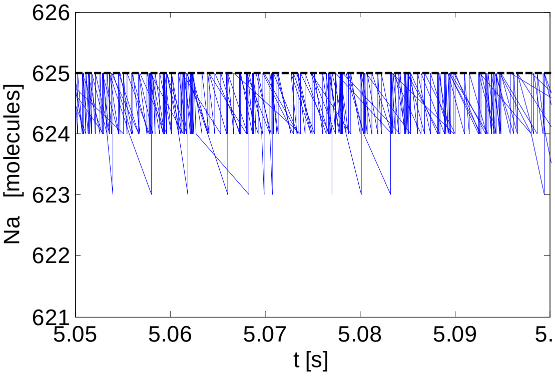

Figure 3: The simulated number of adsorbed particles in equilibrium (surface of gold, 625 adsorption sites, 652222 particles in a system, adsorption rate constant 8.18 10^{-27} 1/moleculesec, desorption rate constant 1.182 1/sec): blue zig-zag lines and adsorption limit (black dashed line)

Equilibrium fluctuations of the number of adsorbed molecules are fluctuations around some stationary value and that value can never reach M (the maximal number of adsorption centres on the surface). In equilibrium, surface is never fully occupied during monolayer adsorption, but the fact is that equilibrium surface coverage can be influenced by technological and environmental conditions (surface area, pressure, temperature). That is important for issues such as seting of the threshold level and debiasing of a signal in practical applications.

Read-out signal from the surface where adsorption takes place depends on the sensing mechanism. Adsorption based sensing relies on various mechanisms. For instance, adsorption induced mass fluctuations of micro resonators cause frequency fluctuations and we have read-out in electrical domain. On the other hand, adsorption based sensors famous for their speed and sensitivity are plasmonic sensors and they have optical read-out which may be important for working in all optical domain.

The purpose of this work the investigation of the possibility that the adsorption-desorption process may be a good basis for pseudo random number generation or true random number generation in electrical, but also in optical domain. In the text that follows we sugest and analyze different algorithms and solutions.

3. STOCHASTIC SIMULATION ALGORITHM AND RANDOM NUMBER GENERATION

There are many pseudo random number generators in a digital world, they can be used as built-in functions, incorporated in a programming language, or they can be designed according to a custom designed algorithm. The fact is that the quality of the generated random sequence may vary, depending on the application: the quality depends strongly on the combination of programming language, operating system, and functions used in the programming code.

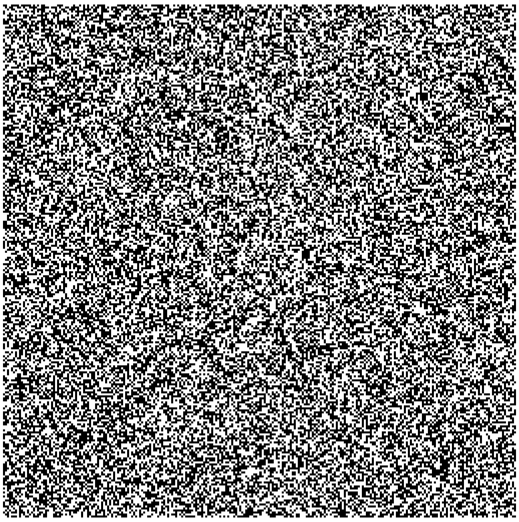

Figure 4: Bitmap generated by the true random number generator at http://www.random.org

Randomness and Integrity Services Ltd, organization that runs free and paid online services based on true random number generation (games, gambling, random number based lists, strings, maps, web tools and education) at http://www.random.org, published open bitmap generated by the TRNG (Figure 4) that can be used for simple visual analysis evaluation test of bitmaps obtained by PRNGs. Figure 5 shows their example for the importance of specifying the complete environment where the PRNGs have been tested: bitmap generated by Bo Allens code based on PHPs rand(), written on Microsoft Windows platform. Allens algorithm, the same code passsed tests and did not show patterns in simple visual analysis in a Linux environment or with the use of mt_rand() function instead of rand().

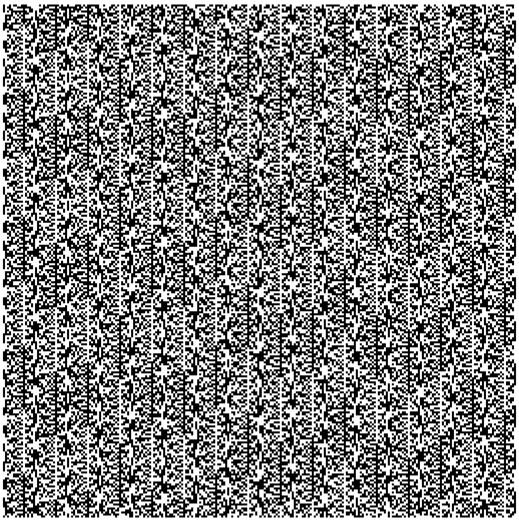

Figure 5: Bitmap generated by Bo Allens code based on PHPs rand(), written on Microsoft Windows platform, published open at http://www.random.org/analysis

The algorithms we proposed were implemented in MATLAB R2012a environment, on Microsoft Windows64 platform.

The first algorithm we propose for PRNG stream bit or digit (cifers 0-9) generation. It is based on the algorithm for the simulation of the adsorption-desorption process from previous section, with following speciffics:

- generation of time sequence is ommited,
- random number of adsorbed molecules is transformed into random bits by modulus after division with 2, mod(,2) function,
- mod(,10) was for transformation into random digits
- for sample of m values exponentialy distributed around mean value lambda the following expression is used

sample = -lambda* log(1-rand(sample_size,1))

- final sequence of random numbers is then scaled into bit image by using imagesc(,,) for the purpose of simple visual analysis

The second algorithm we propose for PRNG generation is based on a snapshot of the real time animation of a process. It is organized as follows:

1. Initialize constants and parameters for surface dimension and process simulation
2. calculate instantaneous adsorption and desorption rates (ads and des)
3. If instantaneous number of adsorbed particles N_a is zero, adsorption should take place,
4. Otherwise,

   a. if N_a equals M, desorption should hapen
   b. otherwise test
      i. If minimal free path time of all particles in a gas phase is less than minimal residential time of all adsorbed particles then opt for adsorption
      ii. otherwise opt for desorption
5. In case of adsorption, choose random row and colon among all instantaneous free adsorption sites and set pausing time to a number from exponential distribution with reciprocial instantaneous adsorption rate as parameter lambda
6. In case of desorption, choose random row and colon among all instantaneous occupied adsorption sites and set pausing time to a number from exponential distribution with reciprocial instantaneous desorption rate as parameter lambda
7. pause for that time and show the image of instantaneous coverage on the surface
8. return to step 2
9. At any moment during that loop save bitmap image

4. RESULTS

The obtained bitmap images were first examined by simple visual analysis and then by two different test suits. The first test suite provided John Walker, founder of Autodesk, Inc. and co-author of AutoCAD at Fourmilab Switzerland page http://www.fourmilab.ch/random/. It performs diehard test, NIST test and ENT test (which besides other tests, measures entropy). The second test suite named Java Random Test suite provided Zur Aougav, under open source software licence at http://jrandtest.sourceforge.net/. It includes general statistical tests, NIST and DIEHARD tests.

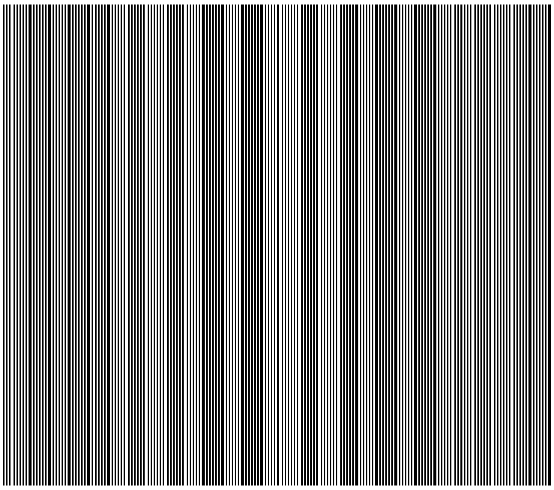

Figure 6: Bitmap generated by bit stream PRNG algorithm

The bit stream PRNG algorithm did not pass any test (Figure 6). The digit stream PRNG algorithm did not pass simple visual test (Figure 7), but with modifications (after filtration) it could pass some of tests in John Walkers and Zur Aougavs test suits. The algorithm for PRNG generation based on a snapshot of the real time animation of an adsorption-desorption process proved superior through all tests.

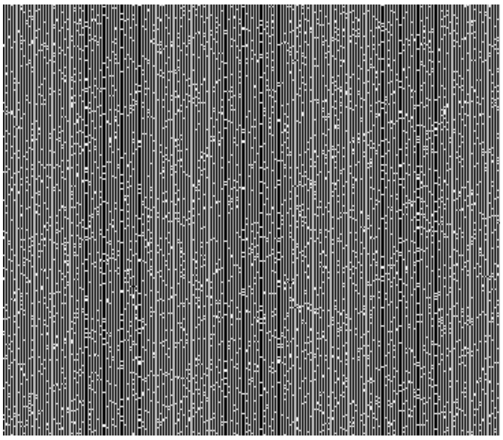

Figure 7: Bitmap generated by digit stream PRNG algorithm

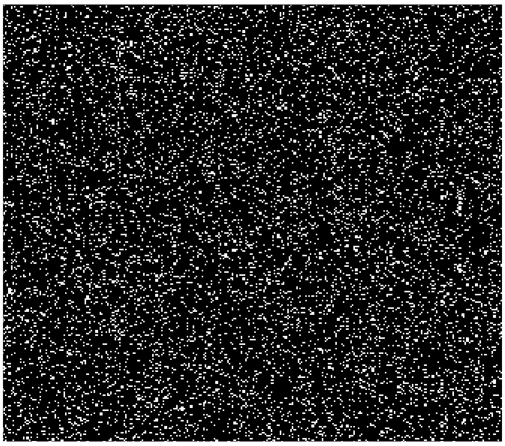

Figure 8: Bitmap generated by the algorithm for PRNG generation based on a snapshot of the real time animation of an adsorption-desorption process

Stochastic simulation of the process and real time animation indicate that future steps could be made in the direction of developing the true hardware adsorption based random number generator.

5. CONCLUSION

Adsorption-desorption process as a means for data encryption has been analyzed. For the first time the stochastic simulation of asdsorbtion-desorption process has been done. The simulation is in accordance with analytical expression for the mean number of adsorbed particles in a monolayer on a homogeneous surface.

Three algorithms have been proposed for generation of pseudo random numbers and tested in three different ways: through simple visual analysis and two different test suits (John Walkers and Zur Aougavs test suite) each of which encorporates standard NIST test suite and diehard tests among other statistical tests.

The investigation showed that the development of the true hardware adsorption based random number generator could be feasible and beneficial for optical data treansmission and networking.

ACKNOWLEDGMENT

This work has been funded by Serbian Ministry of Education, Science and Technological Development within the framework of the project TR 32008.

REFERENCES

[1] D.R.Stinson, Cryptography:Theory and Practice, Third Edition. Chapman and Hall/CRC, 2001, p. 616.

[2] B.Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons, Inc, 1996.

[3] W.Stallings, Cryptography and Network Security: Principles and Practice. Prentice Hall, 1998, p. 569.

[4] S. B. SADKHAN and R. K. SALIH, “Determination of complexity of pseudo-random sequence based on Z-transform,” Atti della Fond. Giorgio Ronchi, p. 165.

[5] M.García-Martínez and E. Campos-Cantón, “Pseudo-random bit generator based on lag time series,” Int. J. Mod. Phys. C, vol. 25, no. 04, p. 1350105, Apr. 2014.

[6] M.Fürst, H.Weier, S.Nauerth, D.G.Marangon, C. Kurtsiefer, and H. Weinfurter, “High speed optical quantum random number generation,” Opt. Express, vol. 18, no. 12, pp. 13029–13037, Jun. 2010.

[7] G.Marsaglia, “Random Numbers Fall Mainly in the Planes,” Proc. Natl. Acad. Sci. U. S. A., vol. 61, no. 1, pp. 25–28 CR – Copyright &#169; 1968 National Academy, Sep. 1968.

[8] “The Marsaglia Random Number CDROM including the Diehard Battery of Tests.” [Online]. Available: http://www.stat.fsu.edu/pub/diehard/. [Accessed: 15-Aug-2014].

[9] L.E.Bassham, A.L. Rukhin, J.Soto, J.R.Nechvatal, M. E.Smid, S.D. Leigh, M.Levenson, M.Vangel, N.A.Heckert, and D.L.Banks, “A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications,” NIST SP - 800-22rev1, p. 131, 2010.

[10] E.Filiol, “A New Statistical Testing for Symmetric Ciphers and Hash Functions,” in Proc. Information and Communications Security 2002, 2002, vol. 2513, pp. 342–353.

[11] R.G.Brown, “Dieharder: A Random Number Test Suite.” [Online]. Available: http://www.phy.duke.edu/~rgb/General/dieharder.php. [Accessed: 15-Aug-2014].

[12] D.D.Do, Adsorption Analysis: Equilibria and Kinetics, vol. 2. London: Imperial College Press, 1998.

[13] J.H.DeBoer, “The Dynamical Character of Adsorption,” Soil Science, vol. 76, no. 2. p. 166, 1953.

[14] W.J.Thomas and B. Crittenden, Adsorption Technology and Design, no. April. Elsevier Science & Technology Books, 1998, p. 271.

[15] V.J.Inglezakis and S. G. Poulopoulos, Adsorption, Ion Exchange and Catalysis: Design of Operations and Environmental Applications, Tom 3. Elsevier, 2006, p. 614.

[16] Y.Liu and L. Shen, “From Langmuir kinetics to first- and second-order rate equations for adsorption.,” Langmuir, vol. 24, no. 20, pp. 11625–30, Oct. 2008.

[17] J.G.Van Alsten, “Self-Assembled Monolayers on Engineering Metals□: Structure , Derivatization , and Utility,” Langmuir, vol. 15, no. 19, pp. 7605–7614, 1999.

[18] I.Langmuir, “The adsorption og gases on plane surfaces of glas, mica and platinum,” ?, pp. 1361–1403, 1918.

[19] L.Kolar-Anić, Ž. Čupić, V. Vukojević, and S. Anić, The dynamics of nonlinear processes. Belgrade: Faculty of Physical Chemistry, 2011.

[20] O.Jakšić, Z. Jakšić, and J. Matović, “Adsorption–desorption noise in plasmonic chemical/biological sensors for multiple analyte environment,” Microsyst. Technol., vol. 16, no. 5, pp. 735–743, Feb. 2010.

[21] Z.Djurić, O. Jakšić, and D. Randjelović, “Adsorption–desorption noise in micromechanical resonant structures,” Sensors Actuators A Phys., vol. 96, no. 2–3, pp. 244–251, Feb. 2002.

[22] D.A.McQuarrie, “Stochastic Approach to Chemical Kinetics,” J. Appl. Probab., vol. 4, no. 3, pp. 413–478, 1967.

[23] O.M.Jakšić, Z.S.Jakšić, Ž.D.Čupić, D.V.Randjelović, and L.Z. Kolar-Anić, “Fluctuations in transient response of adsorption-based plasmonic sensors,” Sensors Actuators B Chem., vol. 190, pp. 419–428, 2014.

[24] I.Oppenheim, K.E.Shuler, and G.H.Weiss, Stochastic processes in chemical physics: The master equation. London: MIT Press, 1977.

[25] O.M. Jakšić, D.VRandjelović, Z.S.Jakšić, Ž.D.Čupić, and L.Z.Kolar-Anić, “Plasmonic sensors in multi-analyte environment: Rate constants and transient analysis,” Chem. Eng. Res. Des., vol. 92, pp. 91–101, 2014.