



Technological University Dublin
ARROW@TU Dublin

Conference papers

School of Electrical and Electronic Engineering

2017-06-21

Chaos-based Cryptography for Cloud Computing

Paul Tobin

Technological University Dublin, paul.tobin@tudublin.ie

Lee Tobin

University College Dublin, lee.tobin@ucdconnect.ie


Michael mcKeever

Technological University Dublin, mick.mckeever@tudublin.ie

Jonathan Blackledge

Technological University Dublin, jonathan.blackledge@tudublin.ie

Follow this and additional works at: <https://arrow.tudublin.ie/engscheleart>

 Part of the [Computer Engineering Commons](#), [Electrical and Electronics Commons](#), [Electronic Devices and Semiconductor Manufacturing Commons](#), and the [Other Electrical and Computer Engineering Commons](#)

Recommended Citation

Tobin, P., Tobin, L., McKeever, M. and Blackledge, J. (2016) Chaos-based Cryptography for Cloud Computing. *ISSC 2016, Ulster University, Derry, June 21–22.*

This Conference Paper is brought to you for free and open access by the School of Electrical and Electronic Engineering at ARROW@TU Dublin. It has been accepted for inclusion in Conference papers by an authorized administrator of ARROW@TU Dublin. For more information, please contact yvonne.desmond@tudublin.ie, arrow.admin@tudublin.ie, brian.widdis@tudublin.ie.



This work is licensed under a [Creative Commons Attribution-Noncommercial-Share Alike 3.0 License](https://creativecommons.org/licenses/by-nc-sa/3.0/)



Chaos-based Cryptography for Cloud Computing

P. Tobin, L. Tobin, M. Mc Keever, J. Blackledge

*School of Electrical and Electronic Engineering
Dublin Institute of Technology, Ireland*

E-mail: paul.tobin@dit.ie lee.tobin@ucdconnect.ie
mick.mckeever@dit.ie dvcresearch@ukzn.ac.za

Abstract Cloud computing and poor security issues have quadrupled over the last six years and with the alleged presence of backdoors in common encryption ciphers, has created a need for personalising the encryption process by the client. In 2007, two Microsoft employees gave a presentation “On the Possibility of a backdoor in the NIST SP800-90 Dual Elliptic Curve Pseudo Random Number Generators” and was linked in 2013 by the New York Times with notes leaked by Edward Snowden. This confirmed backdoors were placed, allegedly, in a number of encryption systems by the National Security Agency, which if true creates an urgent need for personalising the encryption process by generating locally unbreakable one-time pad ciphers. Hybrid random binary sequences from chaotic oscillators initialised by natural noise, were exported to an online Javascript application which applies a von Neumann deskewing algorithm to improve the cryptographic strength of the encryptor. The application also provides initial statistical p-test for randomness testing. Encoding the *Lenna* image by XORing it with the new cipher provided another test to observe if patterns could be observed in the encoded image. Finally, the cipher was subjected to the NIST suite of statistical tests. All designs were simulated using Orcad PSpice[®] V16.5.

Keywords — **Backdoors, one-time pads, chaos, natural noise, cryptography, Orcad PSpice, Von Neumann, NIST**

I INTRODUCTION: CLOUD COMPUTING

Protecting information from unwanted interception during transmission dates back thousands of years. During WW11 Churchill and Roosevelt communicated using a secure 1-to-1 one-time Pad (OTP) transatlantic communications system called SIGSALY. SIGSALY was developed by Bell Labs and Alan Turing and introduced a number of innovative technological systems such as transmitting speech using pulse code modulation and multi-level frequency shift keying [1]. Noise from a mercury-vapour rectifying vacuum valve was added to the voice and spread over a wide frequency band similar to direct spread spectrum communications. This 55 ton encryption system recorded unique OTPs on vinyl record which were then carefully distributed. We present a PSpice design for a 40 g electronic device for generating

OTPs for personalising data encryption prior to storage in the Cloud.

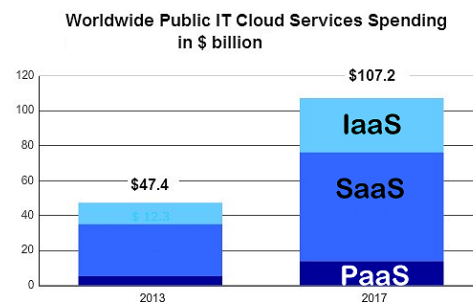


Fig. 1: Cloud computing growth.

By 2017, Global Internet protocol (IP) traffic is forecast to increase to 1.3 trillion Gigabytes. Such traffic will be subjected to ever-increasing security

attacks similar to those on the Sony server which made headline news when personal details of famous actors were divulged [3]. Dan Shumow and a Microsoft colleague, Niels Ferguson, gave a talk “On the Possibility of a backdoor in the National Institute of Standards and Technology SP800-90 Dual Elliptic Curve Pseudo Random Number Generators (ECPRNG)” [4], and in 2013 the New York Times connected this talk with classified Top Secret memos leaked by Edward Snowden [5].

This confirmed backdoors were placed, allegedly, by the National Security Agency (NSA) in a number of encryption systems as part of a decade-long covert operation undermining the integrity of user security. To address this, a system for generating unlimited unique OTPs to encrypt data locally by the end-user using systems such as OneDrive, Google Drive, Dropbox, is described. Figure 2 outlines our system which incorporates a thresholded chaotic nonlinear oscillator initialised by a natural noise to generate a OTP which is XORed with the data in an online application.

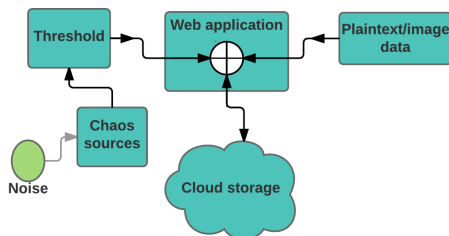


Fig. 2: System for generating OTP sequences.

The final design comprises several chaos sources but to adhere to conference maximum page guidelines, the discussion is limited to a single nonlinear Lorenz chaotic oscillator whose initial condition (IC) is a natural noise source as recommended in [6].

II CHAOS CRYPTOGRAPHY

Designing encryptors using pseudo-chaos was proposed by Claude Shannon in a 1945 paper [7] when he mentioned with great foresight, the stretching and folding mechanism associated with chaos, and is analogous to confusion and diffusion in encryption. Encoding data using chaos has grown exponentially since 2000, with many chaotic maps used in multi-algorithmic systems, encrypting data on a randomised block-by-block basis [8]. Two classes of chaotic oscillators whose ergodicity makes them suitable for encryptor generation, were considered:

- The Lorenz and Chua analogue chaotic oscillators,
- The logistic and Hénon maps digital chaotic maps, which operate in sampled time.

However, for the reasons stated previously, only the Lorenz system is considered.

a) The Lorenz chaotic oscillator

Edward Lorenz, a meteorologist became involved in chaos theory when he modelled atmospheric convection and weather patterns. The results were published in a 1963 paper [9] and probably was the first model to demonstrate chaotic behaviour which displayed a sensitivity to initial conditions (SIC). Thresholding the Lorenz oscillator signal around the fixed points, produced maximum entropy in the random binary sequences generated. The oscillator was initialised using a natural noise source and hence classified it as a hybrid pseudo-random number generator (HPRNG) [10].

Any n -th order non-linear differential equation may be expressed as coupled n first-order equations as given in equation (1). These are a reduced form of the Navier-Stokes equations and written in integral form to facilitate electronic integrator implementation.

$$\begin{aligned} x(t) &= -P \int_{t_0}^t \{x(t) - y(t)\} dt \\ y(t) &= - \int_{t_0}^t \{-Rx(t) + y(t) + x(t)z(t)\} dt \\ z(t) &= - \int_{t_0}^t \{Bz(t) - x(t)y(t)\} dt \end{aligned} \quad (1)$$

Lorenz used $B = 2.666$, $Prandtl P = 10$, $R = 28$, but slightly different values were determined experimentally using a Web application discussed later, to maximise the OTP entropy. The equations were simulated in PSpice using analogue behavioural model (ABM) parts which were replaced by integrated circuit models at a later stage [11].

b) Determining the Fixed Points

The thresholding circuit was designed by calculating the values of the fixed points (FP) at the loci centres in the Lorenz strange attractor, $v(x)$ versus $v(z)$ in Figure 3.

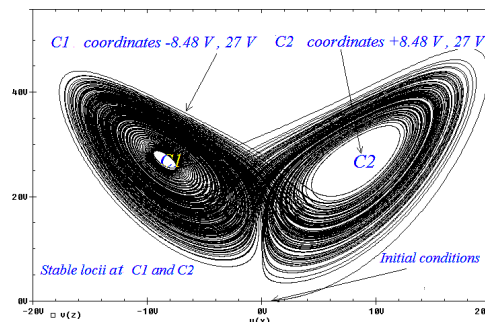


Fig. 3: Lorenz butterfly strange attractor.

To find the FP values consider the Jacobian ma-

trix:

$$\begin{pmatrix} \frac{\partial P(y-x)}{\partial x} & \frac{\partial P(y-x)}{\partial y} & \frac{\partial P(y-x)}{\partial z} \\ \frac{\partial(Rx-y-xz)}{\partial x} & \frac{\partial(Rx-y-xz)}{\partial y} & \frac{\partial(Rx-y-xz)}{\partial z} \\ \frac{\partial(xy-Bz)}{\partial x} & \frac{\partial(xy-Bz)}{\partial y} & \frac{\partial(xy-Bz)}{\partial z} \end{pmatrix} \quad (2)$$

The Lorenz model is approximately linear at the origin ($x = y = z = 0$ corresponds to stationary air masses in the original convective model), hence the Jacobian is rewritten:

$$J(0,0,0) = \begin{pmatrix} -P & P & 0 \\ R & -1 & 0 \\ 0 & 0 & -B \end{pmatrix} \quad (3)$$

The FPs were determined from the characteristic matrix ($J - \lambda I$), so, solving the characteristic polynomial yields the system eigenvalues:

$$\begin{aligned} \lambda_1 &= -B, \\ \lambda_{2,3} &= -\frac{1}{2}(P+1) \pm \frac{1}{2}\sqrt{(P+1)^2 - 4P(1-R)} \end{aligned} \quad (4)$$

The eigenvalues, -2.666, -22.8277, and +11.8277, show the system is unstable at the origin for the positive eigenvalue. The x y coordinates at each lobe centre are the FPs:

$$\left. \frac{dx}{dt} \right|_{P=10} = 10(y-x) = 0 \Rightarrow x = y \quad (5)$$

From this equality, the y equation becomes:

$$\left. \frac{dy}{dt} \right|_{x=y} = Rx - x - xz = 28x - x - xz = 0 \quad (6)$$

Substituting the value of $z = 27$ yields:

$$\left. \frac{dz}{dt} \right|_{x=y} = x^2 - Bz = 0 \Rightarrow x = \pm\sqrt{Bz} \Big|_{z=27} \quad (7)$$

The FPs at each lobe centre $C_{1,2}$ were computed as follows:

$$C_{1,2} = \{+\sqrt{B(P-1)}, -\sqrt{B(P-1)}, (R-1)\} \quad (8)$$

For the standard Lorenz parameters, the FPs were calculated as: ± 8.485 V for z equal to 27 V, as shown in Figure 3. However, scaling the equations for reasonable voltage signal ranges is necessary and changes the FP values and hence the threshold voltage values.

c) Amplitude Scaling

The Lorenz oscillator signal amplitude for the standard parameters exceeds the voltage range of electronic devices and hence scaling x , y and z by 10 was necessary. This modifies the product terms in the equations as:

$$\begin{aligned} x &= -10 \int_{t_0}^t \{x - y\} dt \\ y &= - \int_{t_0}^t \{-28x + y + 10xz\} dt \\ z &= - \int_{t_0}^t \{2.666z - 10xy\} dt \end{aligned} \quad (9)$$

Scaling thus changes the loci $C_{1,2}$ to ± 0.8485 V. The 4-quadrant AD633 multiplier IC, which has internal magnitude scaling of 0.1, realises the cross-product nonlinear terms in the Lorenz oscillator in Figure 4. To solve the equations the TL084 operational amplifier is configured as a summing inverting integrator.

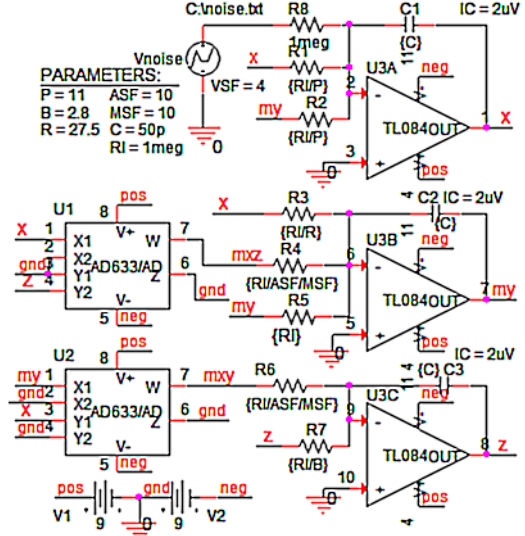


Fig. 4: Lorenz chaos oscillator circuit.

Component values, Lorenz parameters and scaling factors, are defined in a **PARAM** part to facilitate investigating parameter variation on encryptor entropy. This part then links component and parameter values to actual values using the non-numerical operator, $\{ \}$. For example, the integrator gain is $1/CR$, where R is 1 M Ω , means the P parameter is realised by reducing $R1$ and $R2$ as $\{1\text{meg}/P\}$.

The resistances between each multiplier and integrator are scaled by a magnitude scaling factor (MSF) and the 0.1 AD633 magnitude scaling factor (ASF), hence the total resistance is $\{R/ASF/MSF\}$. Final components are: $R1 = R2 = 100$ k Ω , $R3 = 36.3$ k Ω , $R4 = 10$ k Ω , $R5 = 1$ M Ω , $R6 = 10$ k Ω , $R7 = 357$ k Ω , and $C = 50$ pF. A detuned FM receiver IC natural noise source added via a large resistor, RIC , sets the initial condition.

III THRESHOLD DESIGN

The potential divider $R8$ and $R9$ in Figure 5, together with $C4$, adds 4 V DC to the bipolar x signal changing it to unipolar. The thresholding circuit comprises a resistive network, LM339 comparators and a reference voltage, $V_{ref} = 1.24$ V. The 74121 monostable produces constant width set and reset pulses, with the width time given by $0.69 \cdot C5R15$. However, these components are not modelled in PSpice and the pulse width is set as an external model parameter. The FP threshold

voltages ± 0.848 V adds to the 4 V DC shift to yield 3.15 V and 4.84 V, so that for a total resistance of 1 M Ω and $V_{ref} = 1.24$ V, the components were calculated:

$$V_{high} = 4.84 \text{ V} = V_{ref} \frac{R_{10} + R_{11} + R_{12}}{R_{12}} \quad (10)$$

This yields $R_{12} = 256$ k Ω . Similarly for R_{11} :

$$V_{low} = 3.15 \text{ V} = V_{ref} \frac{R_{10} + R_{11} + R_{12}}{R_{11} + R_{12}} \quad (11)$$

Resulting in $R_{11} = 138$ k Ω and $R_{10} = 607$ k Ω . These non-preferred values were realised in the prototype using miniature multi-turn potentiometers.

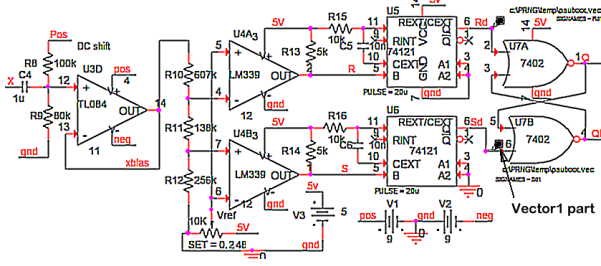


Fig. 5: Threshold circuit for producing the OTP.

The constant width monostable set and reset pulses displayed in Figure 6 are combined by the NOR gates forming an SR latch giving a non-return-to zero (NRZ) format to the OTP. The set and reset pulses never overlap and is a property exploited in the software algorithm in the next section. Figure 7 shows the upper and lower threshold

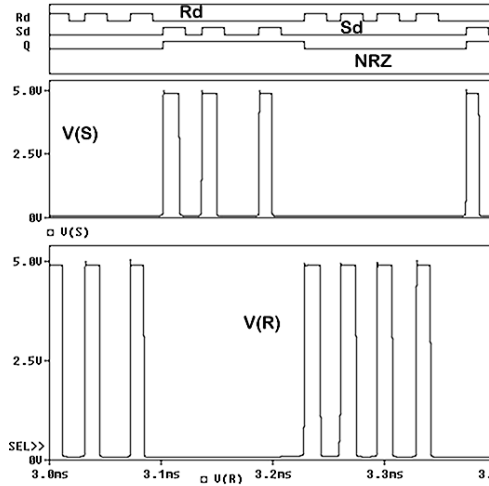


Fig. 6: (a) Monostable signals (b) Set pulse (c) Reset pulse.

voltages superimposed on the x signal.

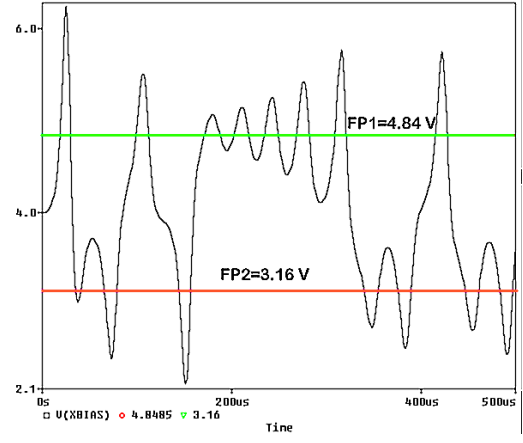


Fig. 7: Threshold voltages at 3.15 V and 4.84 V.

The butterfly strange attractor in Figure 8 shows the set and reset pulse trajectories superimposed at the loci thus correlating with the previous figure. The monostable pulses cannot be superimposed on the attractor.

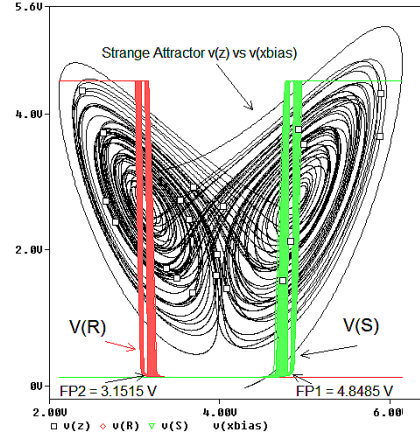


Fig. 8: Butterfly attractor with set and reset pulse trajectories.

IV EXPORTING DATA FROM PSpice

Exporting PSpice analogue signals using copy and paste, works for analogue signals but not for digital data. Instead, binary signals were exported in a text file using PSpice Vector1 parts which specify the directory location and file name. Assigning the same file name to each vector1 parts attached to the monostable set and reset output lines, automatically combines the two outputs forming a dibit pair in a column vector. Table 1 is part of a vector1 text file from PSpice and shows header rows, and time-voltage vectors. The PSpice time vector is not increasing monotonically and shows transitions only.

The Javascript application ignores the time vector column and an algorithm concatenates the set

* Created by PSpice	Sd Rd (dibit)
28.22us	10
36.7767us	00
59.2285us	01
69.2285us	00

Table 1: Example of Vector1 output text file.

and reset bit streams forming the OTP. The first bit of the second column is the set pulse and the second bit is the reset pulse. The goal was to ignore the temporal information and remove the dibit 00 and 11 pairs- states that should never happen. This leaves 10 or 01, of which the first bit is processed to combine the two data streams into a single OTP column stream as displayed in Figure 9. In this example, the final OTP, when XORed with the pixel array data from the test bitmap image, *Lenna*, produced the encoded image as shown. A single statistical p-test is also displayed and gives an initial indication of randomness in the OTP.

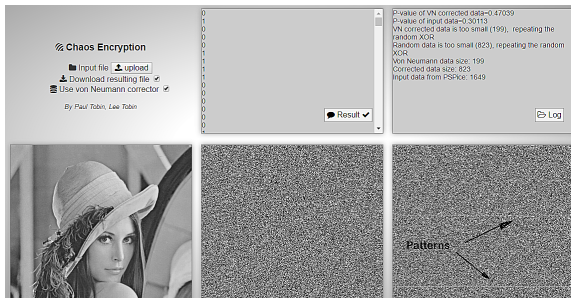


Fig. 9: Online application for processing the Vector1 OTP.

A biased OTP demonstrated undesirable patterns in the encrypted image. Another feature applied the Von Neumann de-skewing algorithm to pairs of data (dibit) but rejected all 00 and 11 dibit pairs [12]. This removes bias from the bit stream which would produce lines in the encrypted image but the algorithm is inefficient and removes 75 percent of data in the process. The VN algorithm should be applied to two uncorrelated data streams but this is addressed in the final circuit by XORing two chaos independent data streams from Lorenz and Chua oscillators. However, for this paper only the Lorenz data was exported from the application as a text file.

V TESTING THE ONE-TIME-PAD

The cryptographic strength of the OTP was evaluated by the National Institute of Standards and Technology (NIST) suite of tests [13]. These tests comprise parameter and non-parameter tests but the OTPs from simulation were limited to non-parameter tests because it was not practical to run the parameter tests which require several million bits in length. Table 2 shows the OTP passed those

tests for file sizes less than one million bits. The online software p-test shows the results of changing the Lorenz system parameters on the cipher entropy and it was found that $B = 2.8$, $P = 11$, and $R = 27.5$ produced maximum entropy in the OTP.

Nist Tests	Result
Frequency test	P=0.503
Block Frequency	P= 0.116
Runs	P=0.508
Block Long Run Ones	P=0.490
Binary Matrix Rank	P=0.333
D Fourier Transform	P=0.216
Non-overlap Tp Match	P=0.370
Overlapping Tp Match	P=0.002
Universal	P= NA
Linear Complexity	P=0.263
Serial	P1=0.1971 P2=0.544
Approximate Entropy	P=0.201
Cumulative Sums	P=0.563
Random Excursions	P=NA
Random Excursion Variant	P=NA

Table 2: NIST p-test results for OTP.

The OTP was also subjected to an autocorrelation test which displayed a single Kronecker delta function as in Figure 10 showing no statistical bias [14].

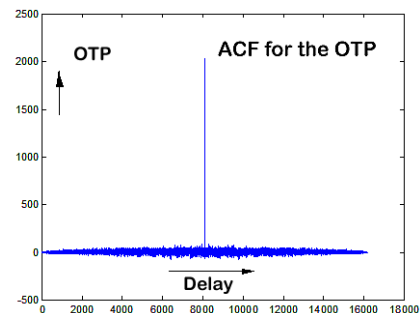


Fig. 10: OTP autocorrelation test result.

The OTP should have several desirable quantities such as infinite uniform power spectral density (PSD) plot, with a positive Lyapunov exponents (LE) which ensures the non-linear oscillator operates in the chaotic region [15]. Another measure of randomness is the Shannon entropy, which essentially is the Kolmogorov complexity (KC) created simultaneously by Andrey Kolmogorov and Ray Solomonoff. This measure specifies the minimum length to which a string of binary digits can be compressed [16]. For certain phase space conditions, Brudno's theorem states that the Kolmogorov-Sinai entropy (KSE) is the algorithmic complexity

(AC) over all the trajectories [17] and Pesin's theorem relates to the KSE by summing the positive LEs.

VI CONCLUSION

Poor security in cloud computing is growing exponentially and our solution was to personalise the encryption process using OTPs. Ultimately, this solution gives greater control and complete confidence to the end user security because the OTP is the only proven unbreakable cipher provided it is used only once. This condition is met however as a new OTP is generated each time new data is uploaded to the cloud. Designing encryptor circuits for chaos cryptography is made considerably easier and more time efficient, by simulating in the first instance, all aspects of the design procedure [18] and the resultant HPRNG circuit produces OTPs that passes the NIST international randomness tests.

The Javascript application software encrypted data with the OTP from a text file exported from PSpice. The application added a von Neumann algorithm to improve cipher entropy and provided a single statistical test for investigating the effect of parameter variation on randomness (Software is available at [19]). A prototype circuit was produced after submitting the conference paper and matched all the simulation results. It is expected that the final PCB circuit using several chaos sources initialised by a natural noise source, will pass all the NIST randomness tests.

ACKNOWLEDGEMENTS

The authors are grateful to Professor Michael Conlon and Dr Marek Rebow, Dublin Institute of Technology, for arranging the author's collaborative research programme.

REFERENCES

- [1] Bennett W., *Secret telephony as a historical example of spread-spectrum communication*, IEEE Transactions on Communications, vol. 31, no. 1, pp. 98104, 1983.
- [2] [Online]. Available: <http://softwarestrategiesblog.com/tag/cloud-computing-forecasts/>.
- [3] <http://www.nytimes.com/opinion/aaron-sorkin-journalists-shouldn-t-help-the-sony-hackers.html>, 2014.
- [4] Shumow D., Niels Ferguson N., *On the possibility of a back door in the NIST SP800-90 Dual Ec Prng.*, CRYPTO Rump Session, August 2007. [Online]. Available at: <http://rump2007.cr.yt.to/15-shumow.pdf>.
- [5] The New York Times, *Secret Documents Reveal N.S.A. Campaign Against Encryption*, 2013.
- [6] Barker E., Kelsey K., *Recommendation for the Entropy Sources Used for Random Bit Generation (draft)* NIST SP800-90B, August 2016.
- [7] Shannon, C.E., 1949, *Communication Theory of Secrecy Systems*, Bell Technical Journal, vol.28-4, 1949, pp. 656 715.
- [8] Blackledge J., *Cryptography and Steganography: New Algorithms and Applications*, Centre for Advanced Studies Text-books, Warsaw University of Technology, ISBN: 978-83-61993-05-6, 2012.
- [9] Lorenz E., *Chaos and Strange Attractors: The Lorenz Equations* pp. 532-538, 1963.
- [10] Cuomo, K. M., Oppenheim A. V. Strogatz S. H. *Synchronization of Lorenz-based Chaotic circuits with Applications to Communications* IEEE Trans. Circuit Syst., II: Analog Digital Signal Process. 40, 626 1999.
- [11] Tobin P., *PSpice for Digital Communications Engineering* <http://www.morganclaypool.com/action/doSearch?AllField=tobin&x=0&y=0&SeriesKey=> ISBN:1598291629, 2007.
- [12] von Neumann J., *Various techniques used in connection with random digits* Applied Math Series, 12:3638, 1951.
- [13] Rukhin, A., et al., *A statistical test suite for random and pseudorandom number generators for cryptographic applications*. Booz-Allen and Hamilton Inc Mclean Va, 2001.
- [14] Blackledge J., Ptitsyn N., *On the Applications of Deterministic Chaos for Encrypting Data on the Cloud* (Third International Conference on the Evolving Internet IARIA Luxembourg) (ISBN: 978-1-61208-008-6 78-87), 2011.
- [15] Blackledge J., Bezobrazov S., Tobin P. and Zamora F., *Cryptography using Evolutionary Computing* (IET ISSC13 LYIT Letterkenny), 2013.
- [16] Tobin P., Blackledge J., *Entropy, Information, Landauer's Limit and Moore's Law* (IET ISSC14 UL, Limerick), 2014 .
- [17] Frigg R., *In what sense is the KSE a measure for chaotic behaviour?* (London School of Economics May), 2003.
- [18] Tobin P., *PSpice for Circuit Theory and Electronic Devices* <http://www.morganclaypool.com/action/doSearch?>

AllField=tobin&x=0&y=0&SeriesKey=
ISBN:1598291564, 2007.

[19] [Online]. Available: [http://jork.
byethost7.com/chaosencrypt/](http://jork.byethost7.com/chaosencrypt/)