Technological University Dublin
ARROW@TU Dublin

Conference papers | School of Electrical and Electronic Engineering

2017

A Hardware One-Time Pad Prototype Generator for Localising Cloud Security

Jonathan Blackledge
Technological University Dublin, jonathan.blackledge@tudublin.ie

Paul Tobin
Technological University Dublin, paul.tobin@tudublin.ie

lee Tobin
UCD, lee.tobin@ucdconnect.ie

Mick McKeever
Technological University Dublin, mick.mckeever@tudublin.ie

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

 Part of the Computer Engineering Commons

Recommended Citation

Tobin, P. et al. (2017) A Hardware One-Time Pad Prototype Generator for Localising Cloud Security , *16th European Conference on Cyber Warfare and Security (ECCWS 2017)*, University College Dublin, Dublin, June 29-30, 480-487, 2017.

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

A Hardware One-Time pad Prototype Generator for Localising Cloud Security

Paul Tobin[1], Lee Tobin[2], Michael McKeever[1] and Jonathan Blackledge[3]
[1]School of Electrical and Electronic Engineering Dublin Institute of Technology, Ireland
[2]CASL Institute Level 3, UCD Science Centre East University College, Ireland
[3]Military Technological College Sultanate of Oman
paul.tobin@dit.ie
lee.tobin@ucdconnect.ie
mick.mckeever@dit.ie
Jonathan.blackledge59@gmail.com

Abstract: In this paper, we examine a system for encrypting data before storing in the Cloud. Adopting this system gives excellent security to stored data and complete control for accessing data by the client at different locations. The motivation for developing this personal encryption came about because of poor Cloud security and doubts over the safety of public encryption algorithms which might contain backdoors. However, side-channel attacks and other unwanted third-party interventions in Cloud security, probably contribute more to the poor security record history. These factors led to the development of a prototype for personalising security locally which defeats cryptanalysis. The key distribution problem associated with random binary sequences called one-time-pads, does not exist for one-to-Cloud applications, unlike bi-directional communications where it was a big issue. The random binary sequences were generated from chaotic analogue oscillators with initial conditions from a data receiver. A JavaScript application processed the one-time pad and data using modulo two arithmetic and applied the von Neumann bias-removal algorithm to increase the overall entropy. The one-time pad binary sequences applied the fifteen tests in the National Institute of Standards and Technology statistical suite of tests to test for randomness. The one-time pads are transported between locations in a memory key device and the prototype encoder should have dimensions similar to a typical memory key device.

Keywords: one-time pad, chaotic analogue oscillators, PSpice, backdoors, von Neumann algorithm, Cloud, NIST

1. Introduction

Confidence in Cloud Security is dropping because of poor Cloud security, with many Cloud security breaches not discovered instantly (Duncan, 2016). To try and correct this problem, the European Parliament, Council, and Commission will introduce the European Union (EU) General Data Protection Regulations (GDPR, 2016) in 2018 (Tobin et al., 2017). Failure to report data breaches within 72 hours of an incident means fines of up to four percent of the company annual turnover. Figure 1 shows the number of reported attacks monthly on Cloud sites for 2014 and 2015 **(**Cyber Attacks Statistics, 2016).

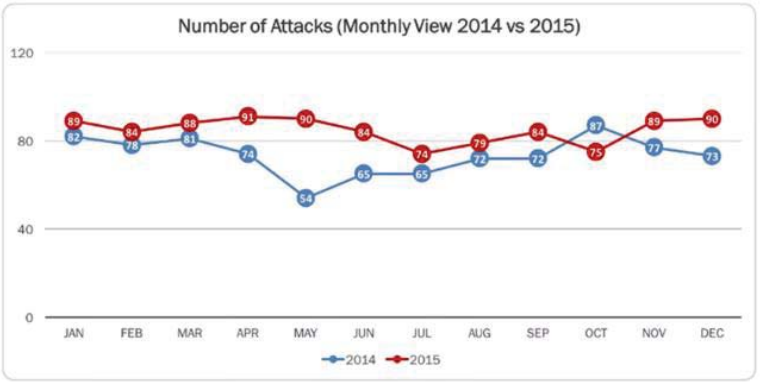

Figure 1: Cloud monthly attacks in 2014 and 2015 **(**Cyber Attacks Statistics, 2016)

1.1.1 Backdoors

Uncertainty over the presence of backdoors and a poor Cloud security record, was the prime motivation for designing and building an encryption system where the client encodes and stores sensitive data locally. Dan Shumow and Niels Ferguson proposed the dual elliptic curve pseudo random number generator might contain backdoors (Shumow and Ferguson, 2007). Such a generator has many uses such as securing the digital Bitcoin

currency (Hankerson et al., 2006) and has advantages over the Rivest, Shamir, and Adleman (RSA) encryption algorithm because it requires smaller bit sizes and is quicker to implement. Six years later, Edward Snowden alleged the National Security Agency (NSA) placed backdoors in elliptic curve cryptography (ECC) algorithms (New York Times, 2013), (New York Times, 2014). The Advanced Encryption Standard (AES) algorithm probably does not contain backdoors and is said to be secure, but one cannot be entirely sure this is true. Nevertheless, most attacks on Cloud systems are more likely due to side-channel attacks rather than backdoors, or indeed any other theoretical security weaknesses. Therefore, encoding sensitive data before storing in the Cloud, is an almost fool proof way of overcoming these security issues. Our encoding device gives control to the customer because one cannot be sure where the data is stored by the cloud service provider (CSP) on the Cloud, or what encryption exists, if any.

The prototype provides a layer of security using an unbreakable one-time pad (OTP) random binary number stream generated from chaos generators. The chaos oscillators are initialised using natural noise from a data receiver to ensure they always start from a truly random state. There are many systems for generating OTP using chaos, and in (Matthews A. J., 1989), he shows how a chaotic map algorithm can generate one-time pads. However, chaotic maps implemented on computers have certain weaknesses because of finite state arithmetic and produces random sequences which have repeating cycle lengths. For this reason, we considered chaotic sources using analogue circuit design only which have an infinite number of states. The main objection by opponents of OTP encryption concerns key distribution difficulties, but the application examples given in this paper do not require the OTP distribution to other users. Using the prototype at a different location requires transferring the OTP using "*Sneakernet*", the nomenclature when data is transferred physically and not digitally (Sneakernet). A JavaScript application was written to encode data with the OTP using an exclusive OR gate (modulo two arithmetic) which also increased the entropy of the encoding process. The application was useful at the prototype development stage for providing a single statistical p-test for investigating the effect of changing system parameters on OTP entropy.

1.1.2 Paper organisation

Section 1 is the introduction and discusses security issues. Section 2 discusses the historical use of the OTP for protecting critical conversations between heads of State during WWII, and for protecting World peace in the sixties using the infamous 'hotline'. A block diagram shows the constituent parts of the OTP encoder and explains why the prototype is a true random binary number generator. We describe two prototype applications for protecting client/patient confidentiality in Section 3. Section 4 outlines chaos cryptography and the design of the OTP generator showing how the multiplexed chaotic analogue oscillators are initiated with cosmic natural noise from a data receiver. In Section 5, we introduce the JavaScript application for interfacing data with the OTP. Section 6 describes some of the tests carried out on the prototype to ensure the OTP was random. Conclusions and future work are in Section 7.

2. Historical use of the one-time pad

Figure 2 (a) is the "hotline" popularised as a red telephone but was in fact a one-time tape (OTT) teletype machine during the Cuban missile crisis for securing peace between Kennedy and Khrushchev.

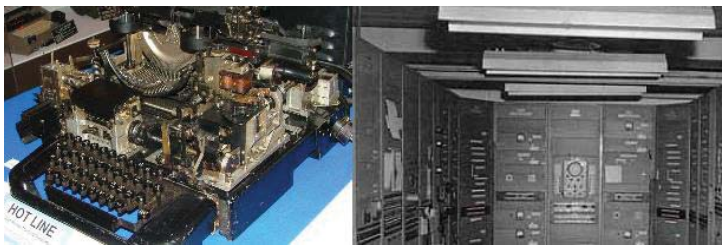

Figure 2: (a) The Washington-Moscow 'Red' telephone hotline (b) The 55-tonne SIGSALY system.

Figure 2 (b) is a picture of the SIGSALY OTP system developed by Clarke and Turin in Bell Labs which encrypted conversations between Churchill and Roosevelt during the second World War (Bennett, 1983). However, both systems had a key distribution problem and the key had to be the same size as the plaintext, but, nevertheless, these systems withstood all attacks against it. However, the prototype OTP generator discussed here does not have a distribution problem because it remains with the client who can use it at different stations.

2.1.1 The OTP prototype

Figure 3 outlines the OTP prototype for creating an additional layer of tight security before uploading data to the Cloud. There are many techniques for generating OTP from analogue and digital chaos circuits, however, sequences from digital chaos oscillators have repeatable sequence lengths because of the finite state of computer arithmetic and hence are cryptographically-poor and do not produce safe OTPs. Analogue chaotic circuit signals on the other hand, have an infinite number of states and thresholding these signals produces random binary streams with sequence lengths that do not repeat (Binder, 1986), (Álvarez, 2006), (Li et al., 2003), (Li et al., 2005). For this reason, we chose analogue chaotic circuits initialised with cosmic noise from a data receiver.

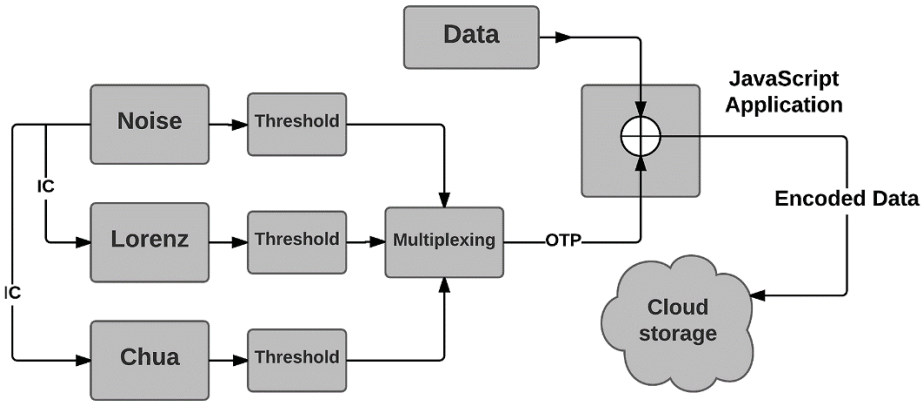

Figure 3: System overview of OTP prototype

The prototype generates unbreakable OTP cyphers from deterministic analogue chaos sources initialised with noise from a 433 MHz data FM receiver integrated circuit. According to (Salih, 2015), (Ergün et al., 2011), (Schneier, 1996), this qualifies the design as a true random generator. The receiver noise supplies a different initial condition (IC) each time a OTP is generated. However, for simulation only, the initialization source was an RND generator part introduced in the latest Orcad® Cadence® PSpice V 17.2. In a previous paper (Tobin et al., 2016), we showed how the *x*-signal of the Lorenz oscillator, when thresholded correctly, generated random binary sequences which were stored in an Arduino memory shield. In this paper, the Chua oscillator is the second chaos source.

3. Applications for the OTP prototype

There are advantages to using this system in court; for example, a Barrister involved in a legal case normally carries armfuls of documents to court and runs the risk of losing material in transit. This procedure raises questions about loss of client confidentiality. The second advantage concerns the searching process; searching for facts in these paper documents is grossly inefficient compared to an electronic search. The solution is to encode and upload all pertinent documents to the Cloud. The first paperless litigation case appeared in June 2015 in an appeal case of Lanigan v Barry, in the Supreme Court in Dublin, Ireland. This electronic system called eCourt, developed by eCúirt Teoranta™ (ecourt, 2015), used Android tablets which contained previously scanned documents pertinent to the case in hand. This paperless litigation removed the need for carrying folders of papers and provided a better search mechanism. Of course, the legal team could lose the tablets and this is where encoding and uploading document is a better and safer option. The *Four* Courts, the primary legal court centre in Dublin, currently does not have WIFI but this will change. The Court of Justice of the European Union (CJEU), created a CURIA application for smartphones and tablets for accessing data in real time for free in court (CJEU, 2016). The Supreme Court Justice in England, Lord Kerr, initiated paperless litigation by introducing Cloud computing technology in a commercial dispute of Berezovsky v Abramovich in the UK, 2012. Real-time searching for relevant transcripts and documents during a case is a more efficient process over existing methods.

3.1.1 Securing legal data in the Cloud

There are many potential applications for our OTP system for protecting data placed in the Cloud, but the following legal application allows real-time access to case data in court. Is encrypting data before storing in the Cloud necessary? The AES algorithm probably does not contain backdoors and is very secure. Nevertheless, data is compromised daily through other means such as side-channel attacks even with AES encryption. Some Cloud

service providers (CSP), do not encrypt the data thus making our system desirable. What the OTP encoder does is to make the intercepted Cloud data meaningless and cannot be decoded without the OTP. Applying the encoder to very sensitive data gives greater confidence to the client and eliminates the need for transporting documents between office and court to prevent loss of case information and protects customer confidentiality. Figure 4 outlines the process whereby sensitive legal documents or images are encoded locally before storing in the Cloud. There is no key distribution problem in this situation since the OTP is not transmitted but carried by the legal team who will use it to download the relevant case documents from the Cloud in court.

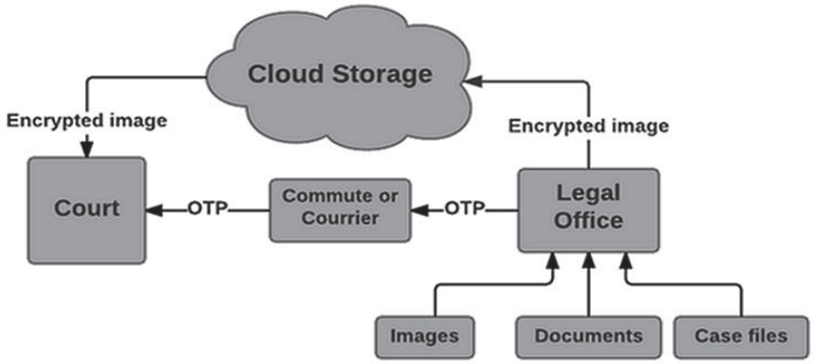

Figure 4: Encoding legal images using OTP

3.1.2 Encrypting medical scans

Figure 5 shows an example of protecting patient confidentiality by encoding medical images, or the personal meta information contained in them. For example, a patient who needs an MRI scan attends the local hospital for a head scan as part of an investigation into the cause of persistent headaches.

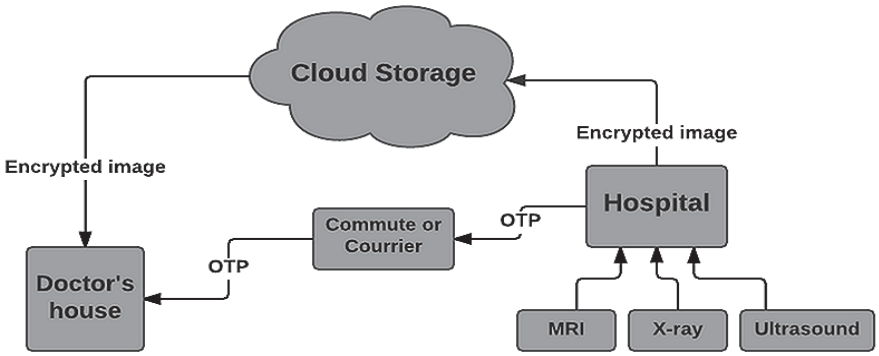

Figure 5: Medical images are encoding application

The images contain personal information and are sent by post on a CD, or given to the patient directly for the doctor's attention. Neither method is secure and could result in loss of data in transit. Digital Imaging and Communications in Medicine (DICOM) is the de facto standard for storing, distributing and processing, medical images (Blackledge et al., 2014), (Jees, 2016). DICOM images contain patient personal information, which if lost in transit, would constitute a serious breach of patient confidentiality. A safer method is to encode the scanned image locally and store them in the Cloud. Alternatively, one could encrypt the header metadata only which would reduce the size of the OTP considerably. The staff gives the new OTP to the patient so the doctor can download and decode the images from the Cloud at his surgery.

4. Chaos cryptography

Claude Shannon's 1949 paper (Shannon, 1949), proposed chaotic digital maps for encrypting data using symmetric key encryption, and since then, the area of chaos cryptography has grown considerably. Our OTP generator prototype uses modified Lorenz and Chua chaotic oscillators to generate the random binary stream. In this paper, we considered only the Chua generator and introduced a novel method to increase the entropy by adding an analogue delay to one of the outputs fed back to the input. The following first-order coupled equations were created by Leon Chua in 1983 when he was trying to prove the Lorenz oscillator was chaotic:

$$\frac{dx}{dt} = 2.7x(t) + 2.4y(t) - 3.925x(t)^3 \Rightarrow -x = -\int (2.7x(t) + 2.4y(t) - 3.925x^3)dt$$

$$\frac{dy}{dt} = 4.16x(t) - y(t-\tau) + 7.083z(t) \Rightarrow -y = -\int (4.16x(t) - y(t-\tau) + 7.083z(t))dt$$

$$\frac{dz}{dt} = -2.099y(t) \Rightarrow z = -\int (2.099y(t))dt$$

The delay tau in the second equation was added to represent the delay and the equations are expressed in integral form when designing the electronic integrators in the prototype. The Chua oscillator is commonly implemented using a type of parallel tuned circuit across which a 'Chua diode' comprising a segmented negative resistance characteristic, is connected to the tuned circuit to provide energy and nonlinearity to initiate chaos. A comprehensive paper on the Chua circuit is (Kennedy, 2013). However, a different approach using four-quadrant AD633 multiplier devices was used to model the nonlinear cubic term. Figure 6 (a) shows the Chua chaotic oscillator in analogue behavioural model (ABM) form to realise these equations using the latest Cadence® Orcad® PSpice V17.2. ABM parts are useful for initial proof-of-concept and for simulating long runs to avoid convergence errors that may occur periodically using real device models. The ABM integrators have a negative gain to solve the equations but these were replaced subsequently with model parts of a TL084 integrated circuit connected as a summing inverting integrator (Tobin, 2007).

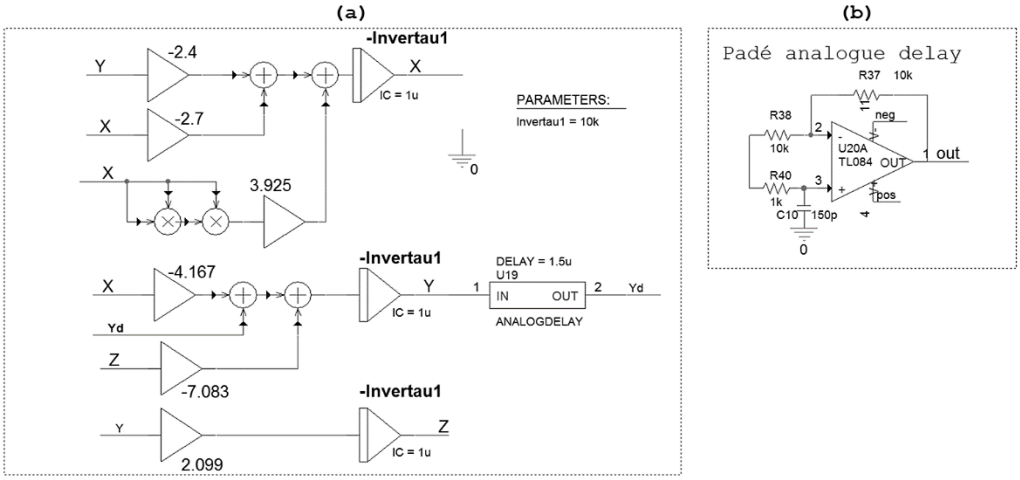

Figure 6: (a) The Chua chaotic oscillator in ABM form (b) A Padé operational amplifier delay tau = 0.5R40C10 S

The analogue delay in Figure 6 (a) shows a customised analogue delay part which contains a correctly-terminated transmission line buffered at input and output. However, in the prototype, this ABM part was replaced with the Padé delay circuit shown in Figure 6 (b) was connected as in Figure 7 to maximise the OTP entropy.

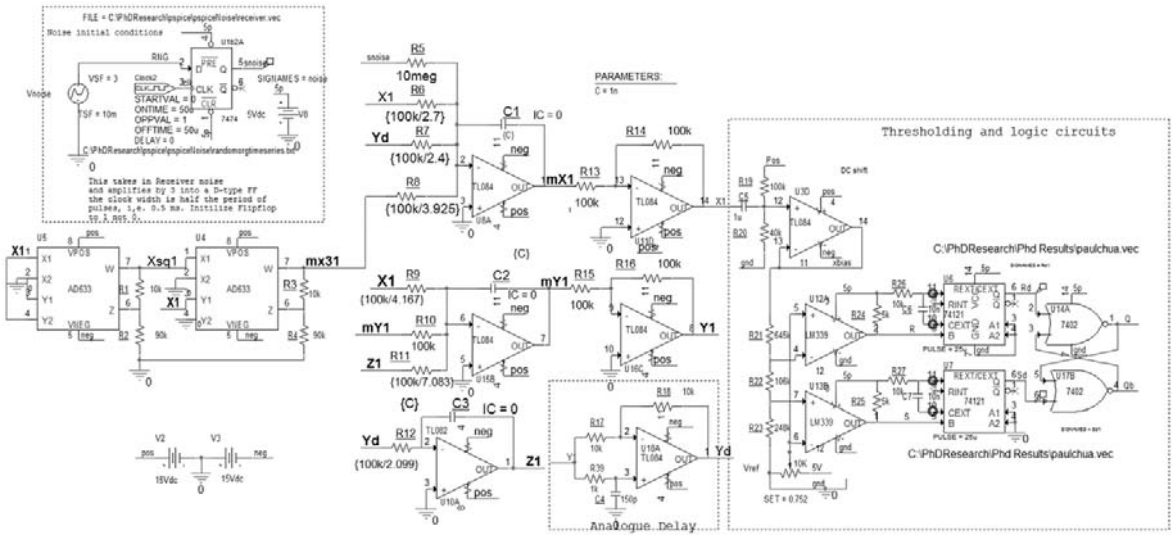

Figure 7: Chua oscillator with threshold circuit and logic

4.1.1 Thresholding the chaos signal

The trajectory of the Chua chaos signal will trace out a path that encompasses the two fixed points (FP) for the Chua system as shown in the strange attractor in Figure 8 (a). Each FP corresponds to a '1' and'0', hence it was necessary to calculate the FPs to determine the comparator input voltage levels and hence calculate the threshold circuit component values. The FP values were obtained by setting the rates of change for each equation to zero and solving for the system variables. The threshold circuit also biases the *x* signal to a unipolar format. However, the width of the V(S) set and V(R) reset pulse widths from the comparator outputs are not constant because of the chaotic nature of the signals. Hence, 74121 monostable devices are required to correct this and produce constant width pulses as shown in the top right pane in Figure 8 (b).

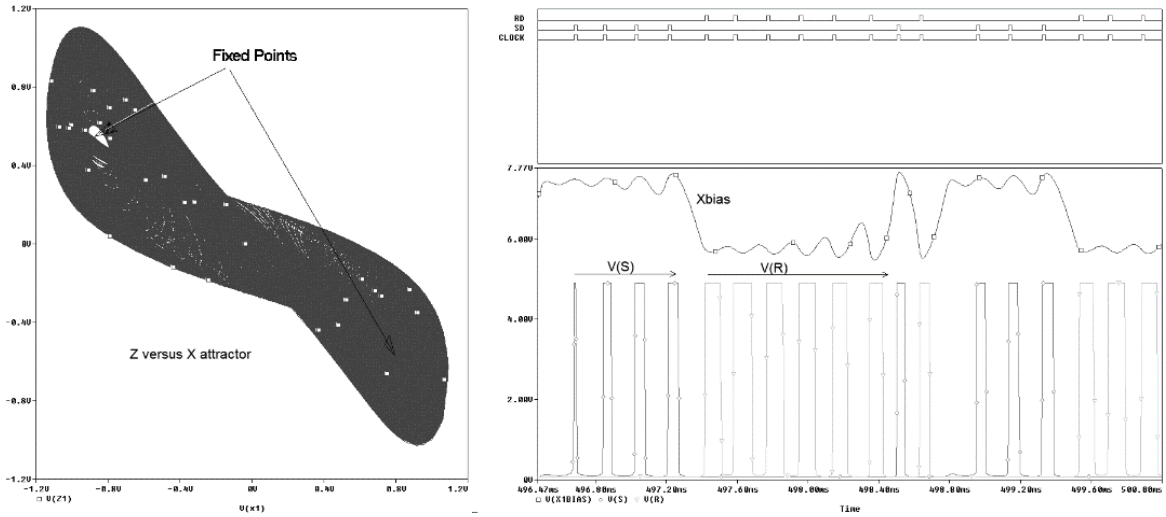

Figure 8: (a) Chua strange attractor (b) Digital signals on top and analogue signals on the bottom

The 'ones' are written to an Arduino shield from the monostable reset output, and the clock signal determines when the 'zeroes' occur. This writing procedure is different to that used during simulation, where the OTP was written to a text file using vector parts attached to the set and reset lines as shown and processed in the JavaScript application. A detuned 433 MHz FM receiver integrated circuit produced cosmic noise sampled at regular intervals for the initial conditions of the two chaos sources. The output level of the noise is random even though it is sampled at regular intervals and initialises the chaos sources with a different value each time. Thus, the output cannot be predicted or reproduced by a third party and ensures the OTP will be completely random.

5. JavaScript interface application

The JavaScript application in Figure 9 reads the OTP data from the vector1 PSpice parts and carries out modulo two arithmetic between it and the pixel array data from the bitmap medical image (Tobinapp, 2016). However, in the prototype, the JavaScript application will read the text file stored in the Arduino shield. An MRI scan of the brain is shown in the left pane, with the middle pane showing the encoded image with no von Neumann (vN) deskewing algorithm (removes any bias in the OTP) applied to the OTP. The bottom right pane shows the encoded image after deskewing the data using a vN deskewing algorithm. The other top panels are self-explanatory and can be explored using the link in the reference section, if interested. The application writes the encoded image to a text file for randomness testing. Bias in the OTP must be avoided to defeat cryptanalysis so the OTP must be totally random and the same length as the picture. Bias present in the OTP will show up as patterns in the encoded image, so the vN) algorithm de-skews the bit stream rejecting 00 and 11 dibit pairs, and converts 01 and 10 dibit pairs to 0 and 1, respectively (vonNeumann, 1951). The algorithm is inefficient as 75 percent of the data is thrown away. Another essential requirement, often over-looked when using this algorithm, is that the dibit stream should be from two uncorrelated data streams. Multiplexing two independent chaotic data streams from the prototype achieve alternating bit independence.

6. Randomness testing

The cryptographic strength of the prototype was tested using the NIST suite of tests (revised in 2010-SP800-22) (Ruk et al., 2001). The NIST suite is the international choice for random binary sequence testing to obtain a certification of randomness. The 15 tests comprise non-parameter tests for small OTP stream lengths and parameter tests for much larger sequences containing several million bits.

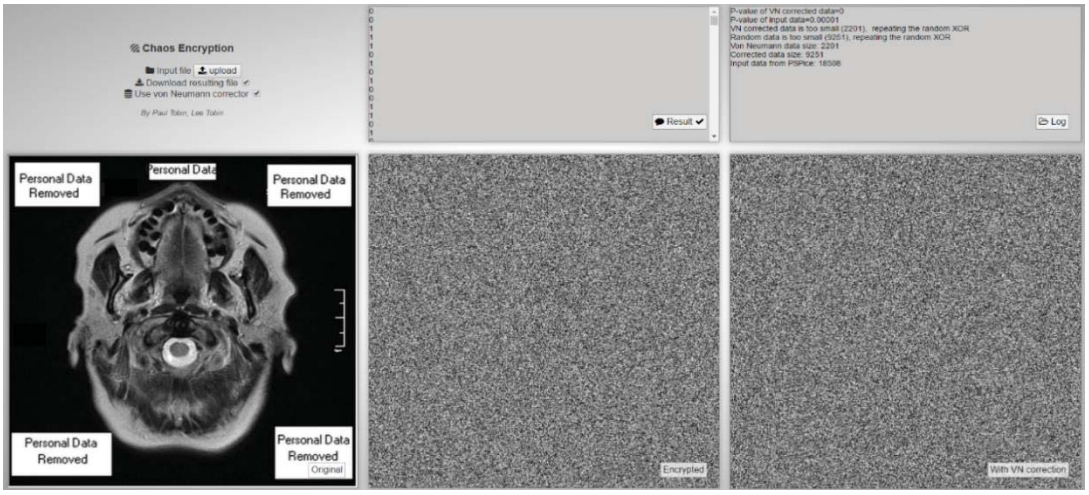

Figure 9: A JavaScript interface for processing the OTP

Table 1 shows the results for the simulated Chua OTP generator sequence tests and the Chua prototype. For maximum Shannon entropy, the OTP should also display a uniform power spectral density (PSD), and the chaos oscillators should operate in a chaotic region to produce positive Lyapunov exponents (LE) (Blackledge et al., 2013). Shannon's entropy essentially is the Kolmogorov complexity (KC) which specifies the minimum length to which a string of binary digits may be compressed (Tobin, Blackledge, 2014), but a truly random OTP should be incompressible.

Table 1: NIST results for noise, simulation, and prototype

Statistical Test	Cosmic noise	Simulation	Chua prototype	Result
Frequency test	P = 0.3961	P = 0.503	P = 0.433	Pass
Block frequency	P = 0.4466	P = 0.216	P = 0.403	Pass
Runs	P = 0.1621	P = 0.508	P = 0.493	Pass
Block Longest Run Ones	P = 0.9131	P = 0.490	P = 0.513	Pass
Binary Matrix Rank	P = 0.6966	P = 0.333	P = 0.430	Pass
D Fourier Transform	P = 0.2142	P = 0.216	P = 0.350	Pass
Non-overlap Tp Match	P = 0.5485	NA	NA	NA
Overlapping Tp Match	P = 0.7729	P = 0.002	P = 0.080	Pass
Universal	NA	NA	NA	NA
Linear Complexity	P = 0.9525	P = 0.263	P = 0.330	Pass
Serial	P1=0.3249 P2= 0.1893	P1=0.197 P2= 0.544	P1 = 0.490 P2 = 0.509	Pass
Approximate Entropy	P = 0.5385	P = 0.201	P = 0.320	Pass
Cumulative Sums	P = 0.5351	P = 0.563	P = 0.530	Pass
Random Excursion	NA	P = 0.203	P = 0.187	Pass
Random Excursion VAR	NA	P = 0.216	P = 0.210	Pass

7. In conclusion

Our OTP random number generator provides an additional layer of security locally and personalising the encryption process by the client makes the data unreadable if intercepted. The generator comprises analogue chaos sources initialised from a novel cosmic natural noise source to create unlimited amounts of unbreakable OTPs which pass the NIST statistical tests for randomness. Several novel features were introduced in this encoder design to increase the overall entropy and the effect of parameter variation on random bit stream entropy was investigated using an online JavaScript application. This application also added a von Neumann algorithm to the bit stream to maximise the OTP entropy. Two, one-to-Cloud examples explained how the OTP could securing data stored in the Cloud and highlighted why there are no key distribution problems. Future work for this prototype involves solving key distribution problems when bi-directional communication is involved.

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

Álvarez, G. and Li, S. (2006) “Some basic cryptographic requirements for chaos-based cryptosystems”, Int. J. Bifurcat. Chaos 16(8), pp. 2129–2151.

Barker, E. K. and Kelsey, (2016) “Recommendation for the Entropy Sources Used for Random Bit Generation (draft)”, NIST SP800-90B.

Bennett W. R, (1983) “SIGSALY IEEE Transactions on Communications”, 31.1.

Binder, P. M. and Jensen, R.V (1986) “Simulating chaotic behavior with finite-state machines”, Physical Review A 34(5), pp. 4460–4463.

Blackledge, J. and Ptitsyn, N. (2011) “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), pp. 78-87.

Blackledge, J., Bezobrazov, S., Tobin, P. and F. Zamora (2013) “Cryptography using Evolutionary Computing”, (IET ISSC13 LYIT Letterkenny), pp. 1-6.

Blackledge, J., Al-Rawi, A. and Tobin, P. (2013) “Stegacryption of DICOM Metadata”, In Irish Signals and Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014). 25th IET June, pp. 304-309. Chicago.

Cyber Attacks Statistics", *HACKMAGEDDON*, (2016) [Online]. Available: http://www.hackmageddon.com/2016/01/11/2015-cyber-attacks-statistics/.

Duncan, B. and Whittington, M., (2016) “Enhancing Cloud Security and Privacy: The Power and the Weakness of the Audit Trail”, Conference on CLOUD COMPUTING, pp. 119-144.

ecourt [Online]. Available: http://www.ecourt.ie/

CJEU [Online]. Available: https://europa.eu/european-union/about-eu/institutions-bodies/court-justice_en

Ergün, S. Güler, U. and Asada, K. (2011) “A High-Speed IC Truly Random Number Generator Based on Chaotic Sampling of Regular Waveform”, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E94 A, 1, pp. 180-190.

GDPR [Online]. Available: http://www.allenovery.com/SiteCollection\newline Documents/Radical changes to European data protection legislation.pdf.

Hankerson, D. Menezes, A.J and S. Vanstone (2006) “Guide to elliptic curve cryptography”, Springer Science and Business Media.

Jees, P. and Diya, T. “Medical Image Protection in Cloud System”, matrix, V2, 2016, pp. 3.

Li, S. et al, (2003) “On the security of a chaotic encryption scheme: problems with computerized chaos”, Comput. Phys. Commun. 153(1), pp. 52–58.

Li, S., G. Chen and X. Mou, (2005) “On the dynamical degradation of digital piecewise linear chaotic maps”, Int. Journ. Bifurcat. Chaos 15(10), pp. 3119–3151.

Matthews A. J. (1989) “On the derivation of a chaotic encryption algorithm”, Cryptologia, XIII(1): pp. 29-42 1989.

New York Times, (2013) “Secret Documents Reveal N.S.A. Campaign Against Encryption”.

New York Times, (2014) [Online]. Available: https://www.nytimes.com/2014/12/15/opinion/aaron-sorkin-journalists-shouldnt-help-the-sony-hackers.html?_r=0

Random.org, (2013) “True Random Number Service”, [Online]. Available: http://www.random.org,

Ruk, A. et al (2001) “A statistical test suite for the validation of random number generators and pseudo-random number generators for cryptographic applications”, NIST, http://csrc.nist.gov/rng/rng2.html.

Salih, E. (2015) “Security analysis of a chaos-based random number generator for applications in cryptography”, 15th International Symposium on Communications and Information Technologies (ISCIT), IEEE, pp. 319-322.

Schneier, B. (1996) “Applied Cryptography second edition”, John Wiley and Sons.

Shannon, C.E. (1949) ``Communication Theory of Secrecy Systems'', Bell Technical Journal, vol.28-4, pp. 656–715.

Shumow, D. and Ferguson, N. (2007) “On the possibility of a backdoor in the NIST SP800-90 Dual Ec Prng”, CRYPTO 2007 Rump Session, http://rump2007.cr.yp.to/15-shumow.pdf, August.

Sneakernet [Online]. Available: https://en.wikipedia.org/wiki/Sneakernet

TobinApp, Available: https://github.com/leetobin/ChaosEncrypt

Tobin, P., Tobin, L., McKeever, M. and Blackledge, J., (2017) “On the Development of a One-Time Pad Generator for Personalising Cloud Security”. *CLOUD COMPUTING 2017*, p.83.

Tobin, P., Tobin, L., McKeever, M. and Blackledge, J. (2016) “Chaos-based Cryptography for Cloud Computing”, 27th ISSC conference Ulster University, Londonderry, June 21-22, doi: 10.1109, pp. 1-6.

Tobin, P. (2007) “PSpice for Circuit Theory and Electronic Devices”, Synthesis Lectures on Digital Circuits and Systems, www.morganclaypool.com, ISBN:1598291564, pp. 127.

Tobin, P. (2007) “PSpice for Digital Communications” Engineering, Synthesis Lectures on Digital Circuits and Systems, www.morganclaypool.com, ISBN:1598291629, pp. 97.

Tobin, P., Blackledge, J. (2014) “Entropy, Information, Landauer's Limit and Moore's Law”, (IET ISSC14 UL, Limerick), pp. 1-6.

von Neumann, J. (1951) “Various techniques used in connection with random digits”, Applied Math Series, 12, pp. 36–38.