2018-2

Secrecy and Randomness: Encoding Cloud data Locally using a One-Time Pad

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

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

Lee Edward Tobin
University College Dublin

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

Recommended Citation

Blackledge, J. et al. (2018) Secrecy and Randomness: Encoding Cloud data Locally using a One-Time Pad, *International Journal on Advances in Security,* vol 10 no 3 & 4, 2017, http://www.iariajournals.org/security/

Secrecy and Randomness: Encoding Cloud data Locally using a One-Time Pad

Paul Tobin*, Lee Tobin†, Michael McKeever‡, and Jonathan Blackledge§
* School of Electrical and Electronic Engineering
Dublin Institute of Technology, Dublin 8, Ireland
Email: paul.tobin@dit.ie
† CASL Institute Level 3, UCD Science Centre East
University College, Belfield, Dublin 4, Ireland
Email: lee.tobin@ucdconnect.ie
‡ School of Electrical and Electronic Engineering
Dublin Institute of Technology, Dublin 8, Ireland
Email: mick.mckeever@dit.ie
§ Military Technological College
Sultanate of Oman,
Email: Jonathan.blackledge59@gmail.com

***Abstract*—There is no secrecy without randomness, and we address poor cloud security using an analogue chaotic one-time pad encryption system to achieve perfect secrecy. Local encoding returns control to the client and makes stored cloud data unreadable to an adversary. Most cloud service providers encode client data using public encryption algorithms, but ultimately businesses and organisations are responsible for encoding data locally before uploading to the Cloud. As recommended by the Cloud Security Alliance, companies employing authentication and local encryption will reduce or eliminate, EU fines for late data breach discoveries when the EU implements the new general data protection regulations in 2018. Companies failing to detect data breaches within a 72-hour limit will be fined up to four percent of their global annual turnover and estimates of several hundred billion euros could be levied in fines based on the present 146 days average EU breach discovery. The proposed localised encryption system is additional to public encryption, and obeying the rules of one-time pad encryption will mean intercepted encrypted data will be meaningless to an adversary. Furthermore, the encoder has no key distribution problem because applications for it are of "one-to-cloud" type.**

***Keywords*—*Secrecy*; *Local encryption*; *GDPR fines*; *one-time pad*; *one-to-cloud*; *key distribution problem*; *chaos*.**

I. Introduction

This paper builds on the conference paper presented at the IARIA cloud conference in Athens, Greece, February 2017, and includes new test results and concepts not included previously because of page number limitations [1]. Existing poor security of sensitive data stored in the cloud is addressed by introducing local encoding by the client. A One-Time-Pad (OTP) encryption system returns control to the client by adding an extra encoding layer of security over public encryption and makes encoded data unreadable to any adversary who gains access to a server. In May 2018, the EU introduces the General Data Protection Regulations (GDPR) which will penalise companies and organisations for late data breach discoveries more than the proposed 72-hour limit [2]. Fines up to four percent of the global annual turnover of EU and UK companies and institutions, are estimated at several hundred billion euros each year and potentially could result in some of them ceasing operation. The Cloud Security Alliance (CSA) recommends organisations should employ authentication and local encryption to protect against data breaches, and GDPR Articles 32 and 34 state why local encryption by the client will mitigate against punitive fines [3]. A two-pronged solution for inadequate cloud security and EU fines was proposed in a paper [4], where local encryption, immutable databases, and audit trail accountability, was discussed.

In this paper, we discuss further aspects of the OTP encryption system which incorporates analogue chaos oscillator sources initialised by electronic noise. For the OTP encoder, we suggest "One-To-Cloud" (OTC) applications for protecting client confidentiality, where there are no Key Distribution Problems (KDP) because the client retains the OTP key. Eliminating side-channel attacks and other less sophisticated hacking methods is not possible, irrespective of this encoding system, or that provided by the Cloud Service Providers (CSP). However, our system will make data unreadable for adversaries who do not possess the OTP key.

The paper layout is as follows: Section I introduces the concept of local encryption and OTC applications showing how it protects client data and addresses the proposed GDPR fines for late data breach discoveries. In Section II, security in the Cloud explains why local encryption will solve specific security problems. In Section III, a brief OTP history illustrates how it secured successfully, intergovernmental communications between British and American leaders in WWII, and protected world peace during the cold war period. Discussed briefly is the structure of the OTP encoder and why it is a true source of entropy.

In Section IV, modern OTP applications explain why the chaos encoder protects client confidentiality and does so with no KDP. Section V introduces chaos cryptography and describes the design of the OTP prototype comprising analogue chaos oscillators initialised with electronic noise. In Section VI, we outline a range of statistical tests carried out on the encryption prototype to ensure it meets international standards

for randomness. Conclusion and future work are given in Section VII, and the Appendix contains figures to illustrate specific points in the paper.

II. Security in the Cloud

Cloud computing has many advantages, and managing information from any location is critical for efficient business operation [5][6]. However, clients are seeing cloud server attacks reported daily in the media and is causing a drop in confidence in cloud security [7]. Furthermore, these clients do not know if their data is encrypted by the CSP, or where it is stored, but encoded data should have:

- **Integrity**: Detecting unwanted modification by an adversary,
- **Confidentiality**: Ensures authorised only users can access stored information,
- **Authentication**: Guarantees the client identity and the validity of stored data,
- **Availability**: Ensures client data can be accessed at all times, and,
- **Accountability**: An audit trail which encompasses non-repudiation, intrusion detection and prevention.

Compounding poor cloud security is the possibility of backdoors in public encryption as suggested by Shumow and Ferguson in a 2007 presentation [8][9][10]. In 2013, Edward Snowden alleged backdoors were placed in public encryption systems by the National Security Agency (NSA) [11]. That said, the Advanced Encryption Standard (AES) algorithm used in cloud security, is probably secure, but nobody knows what other weaknesses exist in public encryption. Backdoors and the threat of GDPR fines for late reporting of data breaches, strengthen our argument for an extra layer of localised security using an OTP random binary number generator.

A. Localised cloud security

Localised OTP encryption for data uploaded to the cloud Infrastructure as a Service (IaaS), addresses poor security issues. Security breaches in the Cloud are rarely discovered and reported instantly, and many months elapse before discovery [12]. Although the time for detecting these breaches has been reduced, the global average is still 146 days [3]. In May 2018, the EU GDPR will replace the Data Protection Directive 95/46/ec, where it states that mandatory breach notification must be reported within 72 hours. Companies and organisations failing to meet this will be fined up to four percent of their global annual turnover [13].

Article 32 of the regulations deals with security of personal data and states, "... controller, and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including the pseudonymization and encryption of personal data". Article 34 states for any company "... has implemented appropriate technical and organisational protection measures ... such as encryption", may avoid punitive breach fines. Apart from these two articles, the regulations cover little on encryption standards, but it appears to encourage companies to use local encryption. Interestingly, GDPR will apply to UK businesses post-Brexit.

Inadequate security in the Cloud is now a primary concern amongst cloud users because commercially-available encryption algorithms are not protecting stored data. The proposed hardware-based OTP random binary number generator encodes data locally by the client before uploading to the Cloud and makes data unreadable if intercepted. The encoder produces random binary sequences digits by thresholding the signal output from two analogue chaos oscillators, and software post-processing of the OTP binary stream ensures sequences from the interleaved chaos source are unbiased and statistically independent from each other.

III. One-Time Pad Encryption

A patent granted in 1917 for an OTP encryption system by Joseph Mauborgne and Gilbert Vernam, was not the first of its kind, however, because Dr Steven Bellovin discovered telegrams were encoded using OTPs many years before this. In an 1882 book, "Telegraphic Code to Insure Privacy and Secrecy in the Transmission of Telegrams", Frank Miller describes how OTPs could protect telegrams [14][15]. There is no record to show whether Miller, a successful banker, actually made an OTP generator prototype.

Modern encryption is not protecting sensitive data in the Cloud, as is evidenced by the fact that most of the greatest security agencies have been hacked, and so a new approach using the concept of OTP encryption is considered. Some cryptologists argue the OTP has no place in modern encryption because of the KDP and the large size of the OTP. However, we make the case that with modern electronics and specific applications, and the fact that it is unbreakable, makes the OTP a viable encryption method for protecting sensitive material in the Cloud.

A. Key distribution problem

The OTP is a symmetric encryption method that uses the same key for encoding and decoding but creates a KDP. Two solutions to this are: (i) Use the courier Sneakernet method of carrying the key between two people, or (ii) choose OTC applications which have no key sharing. The latter point is the focus of this paper where only one person is involved with no KDP. What we are not suggesting is to use the OTP for day-to-day Internet transactions, such as email, etc., but only for encoding sensitive data requiring extra security measures. The OTP is unbreakable provided it is used only once, is truly random, and is the same length as the data (plaintext). However, computer memory is inexpensive, so this latter point is no longer valid.

B. One-time pad history

Clarke and Turing worked in Bell Labs and were part of a team which created the 55-tonne SIGSALY encryption system for protecting conversations between Winston Churchill and Franklin Roosevelt between 1942-1946 [16]. Messages

encrypted with this method were wholly secure, but the system had a KDP because noise (OTP) from a vacuum tube recorded on a vinyl record was flown across the Atlantic. Another OTP application was the famous "hotline" used during the Cuban crisis by the Russian and American governments in the 60s.

Protecting information from interception by adversaries dates back many thousands of years. The WWII German four-rotor *Enigma* encoder with 10^{113} permutations, is perhaps, the most famous encryption system and would still need a year of modern computing power to decode messages. A Polish secret service cryptanalyst, Marian Rejewski, knew wiring details of the first rotor which reduced the possible permutations slightly. He passed this information to the staff in Bletchley Park to help decode German radio messages, but in reality, the German *Enigma* operators made significant operating mistakes and was a more substantial factor for decoding the messages [17][18].

C. Rules for OTP encoding

One-to-one OTP encoding systems had a KDP and operator security problems which consigned the OTP to history and was replaced by symmetric block ciphers and asymmetrical public key algorithms [19][20]. The Soviet Intelligence used OTP encryption because of its excellent record of protecting data and distributed massive quantities of OTP keys during WW11. However, human operators distributed more than two copies of the same key - a significant factor which helped the United States and British intelligence who created the *Venona* project, to break the Soviet OTP code during this period and later during the cold war period.

Encryption algorithms and devices should adhere to the Kerckhoff-Shannon Principle, *'A cryptosystem should be secure if everything about the system except the key, is public knowledge'*, or, as Claude Shannon stated, *The enemy knows the system*, now known as Shannon's maxim [21]. Thus, an encoding system should never rely on the complexity of the encoder for secrecy and should obey the encoding algorithm operating rules to remain secret.

IV. Modern One-to Cloud OTP applications

The OTP is making a comeback [22][23][24], and we propose OTC applications which have no KDP because the client carries the OTP key to decode data from the Cloud at other locations [25]. Figure 1 shows the first OTP encoder-decoding process for OTC applications which generates random binary sequences stored in an air-gapped computer (i.e., not connected to the Internet), or on a flash drive.

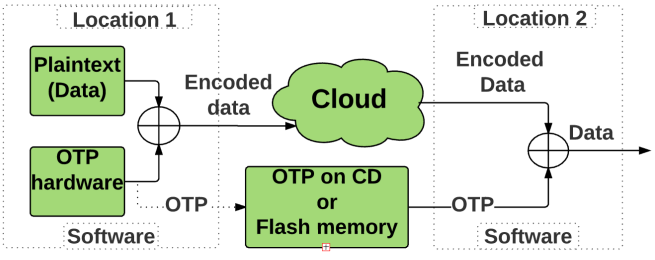

Figure 1. OTP one-to-cloud encoding application with no KDP.

The client uses software, which exclusively OR-gates the OTP from the encryptor hardware with the plaintext data at location one. At location two, software decodes the ciphertext with the key.

A. OTP encryption and randomness

Claude Shannon described the OTP as "perfect secrecy", and is information-theoretic secure and mathematically unbreakable even if using unlimited computing power. An OTP must be truly random to protect the plaintext data from ciphertext attack because an attacker cannot determine the plaintext from the ciphertext without the key. Brute-force searching the key space by an adversary will not help because all messages are equally likely.

Figure 2 shows an Exclusive OR (EXOR) logic gate (7486) which encrypts using modulo two, the message plaintext string of bits with an OTP. The message, $m \in \{0,1\}^n$ for some n, is encoded with the secret key $k \in \{0,1\}^n$ for some n, and produces an output, $E_k(m) = m \oplus k$. The encryption function E maps the secret OTP key and the plaintext message to a ciphertext, $c \in \{0,1\}^n$ for some n and is written, $c = E_k(m)$. To recover the data a decoding function, D, reverses this by mapping the key k and the ciphertext, c, back to the plaintext message, $m = D_k(c)$.

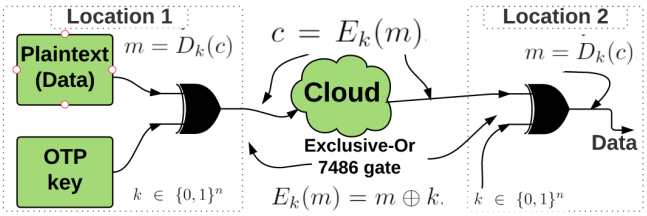

Figure 2. OTP encoding and decoding using modulo two addition.

The following OTP applications have no KDP:

- Academics uploading exam scripts for retrieval by office staff.
- Making presentations about sensitive data away at different locations.
- Medical and legal OTC applications discussed in [26] but repeated here for completeness.

Advantages of OTC applications:

- Able to download secure data at many locations,
- Eliminates transporting of sensitive unencoded documents which could be lost in transit,
- Encrypting documents locally with an OTP prevents an intruder from understanding intercepted data, and
- Avoids the punitive GDPR fines for late breach discovery.

B. Solution to the key distribution problem

The first application for solving the KDP is an OTC medical example for encoding patient medical details displayed on medical images. Transporting medical images from the hospital to the doctor via post, or given to the patient, are

insecure methods because data can be lost and compromises patient confidentiality. A better method is to encode the images and store them in the Cloud at the hospital. These can be accessed by the doctor using the OTP key given to the patient on a memory device such as a flash memory device or CD. Figure 3 shows the proposed method for storing images.

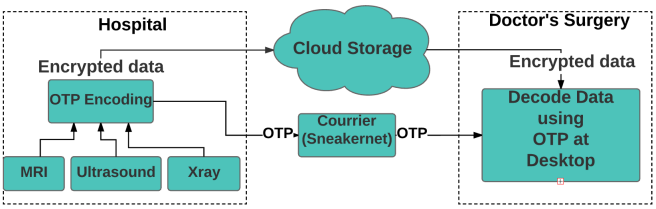

FIGURE 3. ENCODING MEDICAL IMAGES USING OTP.

Digital Imaging and Communications in Medicine (DICOM), is the international standard for distributing, processing and storing medical images, where, for example, an MRI image will display patient metadata on the image [27]. The OTP encoding system encodes the images or the metadata, to retain patient confidentiality [28]. Figure 4 for example, shows an MRI head scan image which was requested by a doctor for a patient with persistent headaches and high blood pressure. The encoded MRI image in the middle pane was processed using a JavaScript application interface written to process the OTP with the image pixel data array. The third pane is the image after processing with a deskewing algorithm described in section V.

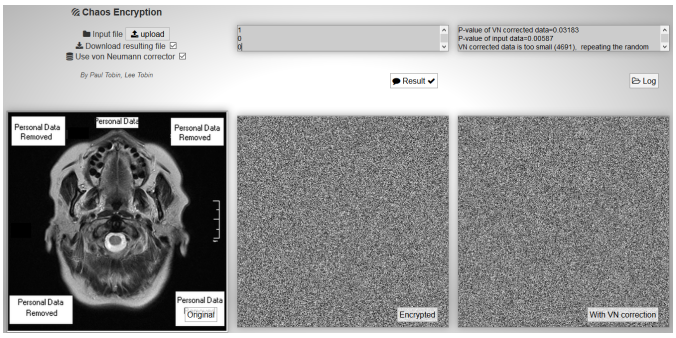

FIGURE 4. (A) DICOM MRI SCAN (B) ENCODED IMAGE (C) ENCODED IMAGE WITH VN PROCESSING.

C. The paperless court case

The second example concerns encrypting documents locally before a court case and introduces the concept of paperless litigation.The system in Figure 5 is similar to AES encoding used in [29] for protecting client confidentiality. At present, legal staff carry court case documentation to court in ring binders, and searching these files for case details in court is inefficient, slow, and insecure. Introducing a much more efficient data search mechanism in court is highly desirable and is achievable with the proposed encoder system.

Encoding data and uploading to the Cloud before a court case, creates a paperless environment, protects data and client confidentiality, and also provides an efficient document search mechanism. In court, the barrister downloads the encoded court case data to an Android device and decodes it using the OTP contained in a memory stick, which if lost, does not create any security issues requiring only a new key.

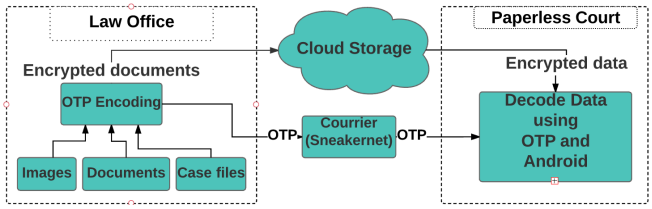

FIGURE 5. PAPERLESS LITIGATION COURTROOM USING LOCAL ENCRYPTION.

V. CHAOS CRYPTOGRAPHY

Confusion, diffusion and secrecy, are fundamental attributes of an encryption system, and comparable properties exist in chaos cryptographic systems. Claude Shannon in his 1949 paper [30], said data could be encoded by applying chaos maps in a symmetric key encryption configuration. However, Shannon's paper did not create the same interest in chaos cryptography, as did his 1945 information theory paper [31]. He discussed the relationship between chaos and cryptography and compared ergodicity and mixing in chaos to cryptographic confusion and Sensitivity to Initial Conditions (SIC) in chaos to diffusion for small changes in the key [32][33]:

"*Good mixing transformations are often formed by repeated products of two simple non-commuting operations. Hopf has shown, for example, that pastry dough can be mixed by such a sequence of operations. The dough is first rolled out into a thin slab, then folded over, then rolled, and then folded again, etc. In good mixing, transformation functions are complicated, involving all variables in a sensitive way. A small variation of any one variable changes the outputs considerably*".

Expanding on these comparisons: Any small change in the initial conditions will cause a chaos system to produce a different trajectory within a short time, similarly in cryptography, changing a small bit of the key will produce a different ciphertext. Public-key cryptography was established in 1976 by W. Diffie and M. E. Hellman, when "New Directions in Cryptography" was published showing secret communication was possible without transporting a secret key between sender and receiver [34]. Many papers published on chaos cryptography since 2000, demonstrated it was possible to encrypt data using chaotic maps in a multi-algorithmic format, arranged on a randomised block-by-block basis [35][36].

A. Chaos production and Dibit forming

Figure 6 presents an overview of the proposed encryption system for generating OTP random bit streams from analogue Chua and Lorenz chaos oscillators initialised by electronic noise. The random bit stream encodes data locally before storing in the Cloud [37]. OTP binary sequences were created by interleaving the two uncorrelated independent data streams from the Lorenz and Chua chaos sources to achieve alternate bit independence. Pairs of bits called *dibits*, are processed by a

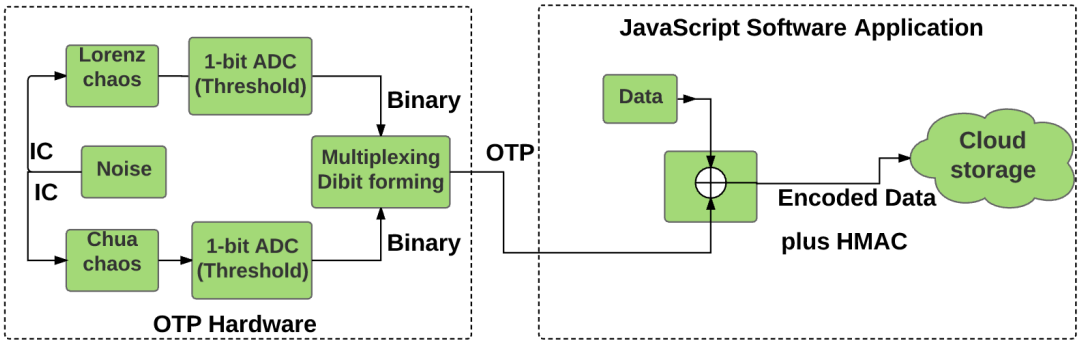

FIGURE 6. OTP RANDOM BINARY NUMBER GENERATOR WITH CHAOS SOURCES INITIALISED WITH RECEIVER NOISE. DIBIT ARE FORMED IN PREPARATION FOR THE VN ALGORITHM.

JavaScript interface through a Von Neumann (VN) algorithm. This deskewing process removes any bias that might be present and thus increases the sequence entropy. Using two uncorrelated bit streams is often overlooked, and the VN algorithm is incorrectly applied to a single data stream only.

The VN algorithm examines each dibit pair created and rejects '00' and '11' whenever they occur. Similarly, dibit '01' becomes '0' and '10' becomes '1' [38]. In this manner, the algorithm eliminates 75 percent of the data, but this just means generating more bits.

The right bottom pane in Figure 4 shows the encoded image processed with the VN but there is little discernible difference between the two encoded images because bias was not present in the OTP. Removing bias in encoded images is necessary as it makes them susceptible to cryptanalysis; otherwise, the encoded image will display patterns as shown in Figure 25 in the appendix.

B. Authentication

The Cloud Security Alliance (CSA) recommends companies add a Hash Message Authentication Code (HMAC) SHA-256 function to the encrypted data to guard against breaches and to check the integrity of the encrypted data [39]. HMAC is a unique fixed-length function derived from the plaintext and added to the ciphertext to verify the received encoded data was not changed by a third-party. The hash output ensures the clients identity is correct [40] and may be combined in several ways with the encrypted message before being sent to the Cloud.

Analogue chaos oscillator signals have infinitely many states produced from a small number of independent variables, but this is not true if created on a digital computer. Random binary sequences from analogue chaos circuits initiated with natural noise produce true random binary streams, which, in theory, will have an infinite sequence length and generate excellent keys.

Generating chaotic oscillations digitally on computers will not produce true random binary sequences because finite computer arithmetic will produce finite length sequences [41]. Similarly, random sequences from chaotic maps implemented digitally will also have repeatable sequence lengths and thus generate weaker keys [42].

Random binary streams produced from chaos sources on digital computers are called pseudo-random sequences, have a limited cycle length but are useful in many security applications.

C. The Lorenz chaos oscillator

Edward Lorenz was a meteorologist modelling weather patterns in 1963, and during one of the modelling sessions, he discovered SIC, one of the hallmarks of chaos systems. To speed up the simulation he truncated model parameters from five places of decimals to three and noticed it produced different results from a previous simulation. He simplified the original 1963 twelve equation model to three first-order coupled equations in (1) [43].

$$\begin{aligned} x &= -P\int_{t_0}^{t}\{x-y\}dt \\ y &= -\int_{t_0}^{t}\{-Rx+y+\mathbf{10}xz\}dt \\ z &= -\int_{t_0}^{t}\{Bz-\mathbf{10}xy\}dt \end{aligned} \tag{1}$$

It was necessary to scale the Lorenz second equation by ten (scale factor in bold type) to reduce signal amplitudes for electronic devices (Figure 21 Appendix). Furthermore, the equations were expressed in integral form because summing inverting integrators were used to solve the equations as shown in Figure 7. which was created and simulated using Cadence® OrCAD PSpice, v17.2.

PSpice connects parts of the circuit using net aliasing (placing names on wires) rather than actual wires, and this makes the schematic easier to read. The encoder source of randomness is supplied by analogue Lorenz and Chua chaos oscillators, both initialised by electronic noise whose ergodic properties ensure the binary streams are cryptographically-strong. Power supply decoupling components were not included in the schematic, because decoupling components are not modelled in PSpice and DC power supply lines were not shown connected directly to integrated circuits but were given alias names called POS and NEG. This simplified the circuit for easier reading.

Lorenz used B = 2.666, P = 10, R = 28 defined oscillator components: $R1$ = $R2$ = 100 kΩ, $R3$ = 36.3 kΩ, $R4$ = 10 kΩ, $R5$ = 1 MΩ, $R6$ = 10 kΩ, $R7$ = 357 kΩ, and C = 330 pF. At the testing stage, the Lorenz parameters were changed in the

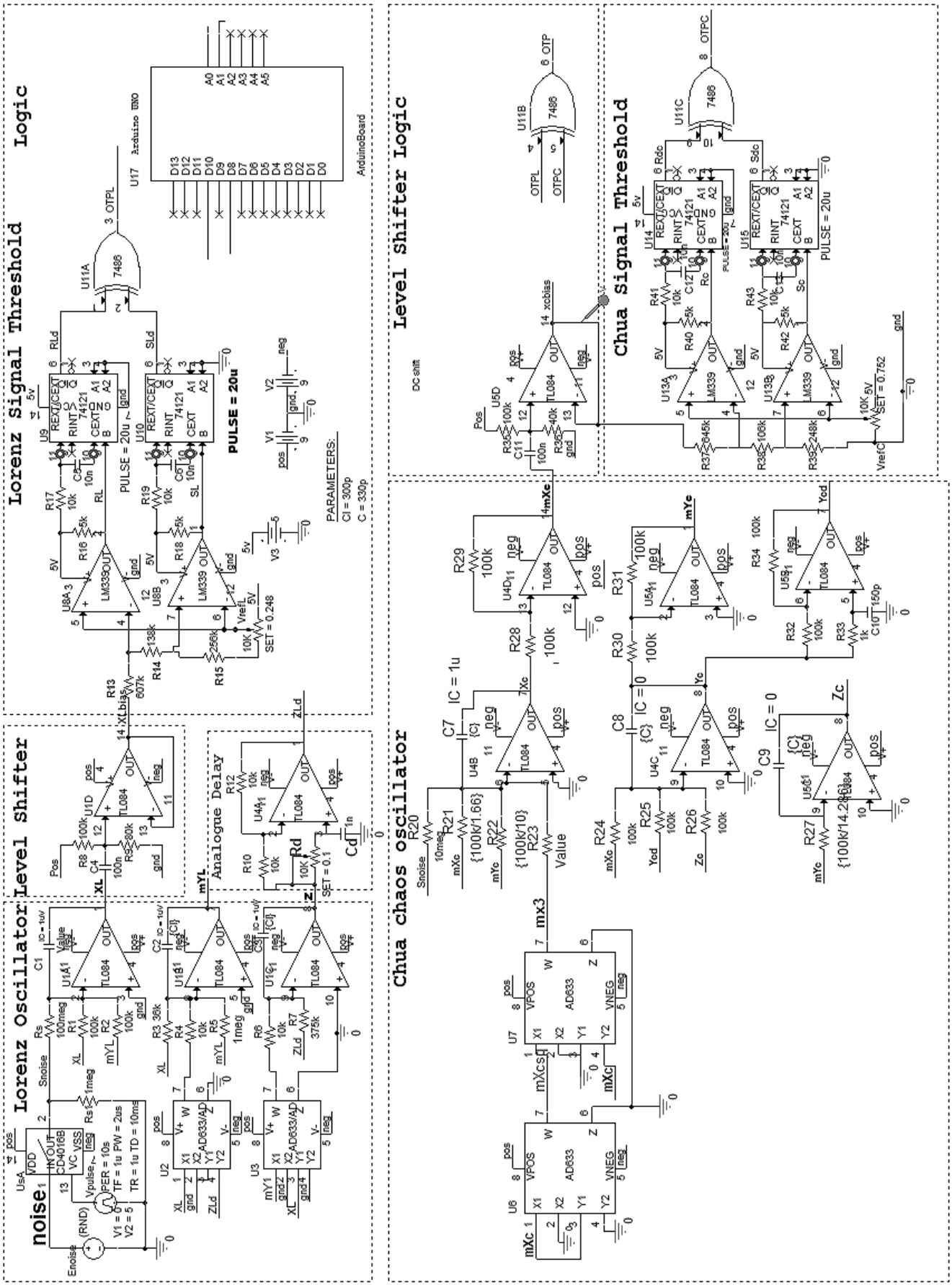

FIGURE 7. THE COMPLETE OTP CHUA-LORENZ ENCODER WITH 1-BIT ADC AND XOR LOGIC.

prototype to increase the OTP entropy as B = 2.8, P = 11, R = 27.5.

Analogue Behavioural Model (ABM) parts were used initially for summation, multiplication and integration for quicker simulation times and with fewer convergence problems (see Figure 22 in the Appendix). However, these parts were replaced with actual model parts after a successful proof-of-concept simulation, [44][45].

The four-quadrant AD633 multiplier integrated circuit (IC) implemented the nonlinear cross-product terms, xy and xz, such terms being necessary for chaos to exist. The general-purpose quad operational amplifier integrated circuits (TL084), were configured as inverting summing integrators to solve the equations.

D. Thresholding the Lorenz chaos oscillator

The OTP is a sequence of random binary numbers produced by converting the analogue chaos signal to binary. Maximum entropy binary sequences were produced by thresholding the (x) signal using a 1-bit analogue to digital converter (ADC) circuit formed from two comparators (LM339) which produced digital pulses with varying widths. It was necessary therefore to use two monostable devices to produce constant width pulses. Selecting the Fixed Points (FP) of the attractor as the suitable thresholding point on the chaos signal resulted in binary sequences with maximum sequence entropy. It was necessary to calculate the centre of these stable regions around which the trajectory of the Lorenz x signal rotates to calculate the threshold circuit values.

The set and reset pulse sequences from the two comparator outputs are superimposing on the *(x-y)* strange attractor shown in Figure 8. It can be seen how the pulse sequence trajectories line up with the two centres (The set and reset signals are shown in Figure 20 in the Appendix).

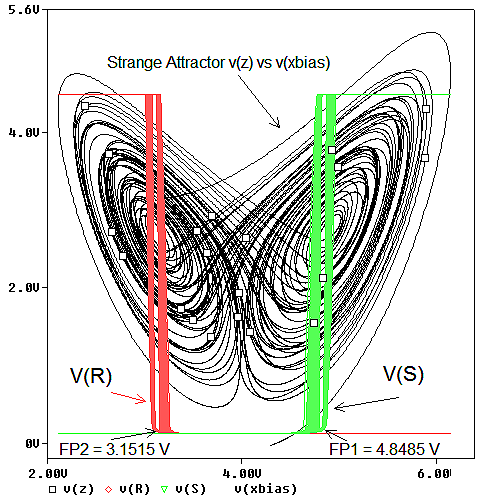

FIGURE 8. THE LORENZ STRANGE ATTRACTOR Z VS *Xbias*.

The loci centres are visited by the signal trajectory in a random fashion and the FPs of (1), where one centre loci represents a '1', when the trajectory is near that region, and a '0' for the other centre. The threshold electronic circuit is designed by determining the FPs at the centre of the strange attractor by assuming the system is approximately linear at the origin. These loci values are determined by equating to zero the first-order in (1). For example, for $x = y = z = 0$, yields $\frac{dx}{dt} = 10(y - x) = 0 \Rightarrow x = y$. Substituting this into the second equation as $\frac{dy}{dt} = 28x - x - xz = 0$, yields z = 27. Using this value, yields:

$$\frac{dz}{dt} = x^2 - Bz = 0 \Rightarrow = \pm\sqrt{B(R-1)} \qquad (2)$$

The lobe centre coordinates, $C_{1,2}$, are calculated:

$$C_{1,2} = \{+\sqrt{B(R-1)}, -\sqrt{B(R-1)}, (R-1)\} \qquad (3)$$

Substituting the standard Lorenz yielded $C_{1,2} = \{+8.48V, -8.48V, 27V\}$. It was necessary to magnitude scale the equations by ten to reduce the signal voltage amplitude suitable for electronic devices and this changed the FPs to $\pm$ 0.8485 V (see Figure 21 in the appendix). A 4 V DC bias changed the bipolar X signal to polar form and changed the upper and lower threshold levels to 3.15 V and 4.84, as shown in Figure 9.

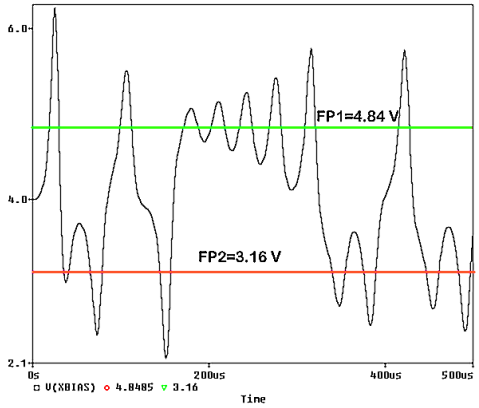

FIGURE 9. THRESHOLDS SUPERIMPOSED ON THE BIASED X SIGNAL.

Threshold component values were determined by assuming a total potentiometer value of 1 MΩ and a reference voltage of 1.24 V (Vref). Substituting these values, and the threshold values, into the following potential divider, produced values for the three resistors:

$$Vhigh = 4.84\ V = Vref\frac{R13 + R14 + R15}{R15} \qquad (4)$$

Similarly,

$$Vlow = 3.15\ V = Vref\frac{R13 + R14 + R15}{R14 + R15} \qquad (5)$$

The bias potential divider $R8$ and $R9$, shifts the x signal up by 4 V and U1 is a unity gain amplifier IC to buffer the biased signal. The threshold potentiometer values were calculated: $R13$ = 607 kΩ, $R14$ = 138 kΩ and $R15$ = 256 kΩ. The pair of LM339 comparators produce out-of-phase set and reset pulse sequences with pulses of varying widths because of the chaotic nature of the original signal. Hence, it was necessary to make the pulse widths constant using monostable

devices (74121). The new constant-width set and reset pulses from the monostable were processed in an exclusive OR gate (XOR) (7486) to generate a controlling clock stream.

This clock stream, and the reset pulse stream from the top monostable, controlled when the OTP 'ones' and 'zeroes' were stored in Arduino memory for further processing in a JavaScript application.

E. The time-delayed feedback Lorenz oscillator

Bit stream entropy was increased by adding a time delay, τ, in the feedback path of the polar z signal in the Lorenz oscillator and modified (1) to include the delay:

$$\begin{aligned} x(t) &= -11 \int_{t_0}^{t} \{x(t) - y(t)\} dt \\ y(t) &= -\int_{t_0}^{t} \{-27.5x(t) + y(t) + x(t)z(t-\tau)\} dt \\ z(t) &= -\int_{t_0}^{t} \{2.8z(t-\tau) - x(t)y(t)\} dt \end{aligned} \quad (6)$$

Adding a delay τ in the feedback path was inspired by chaotic maps such the logistic, Hénon and Lozi, which have better noise-like outputs and hence make better random number generators, but are harder to implement electronically. The normal method for introducing a delay is to use two sampling switches, i.e., a sample and hold design, but is more complex than the proposed analogue solution [46].

Figure 10 shows the analogue delay Padé approximation circuit using a passive low-pass filter. The expression for the z-transform in Digital Signal Processing (DSP), was used to obtain values for the delay [47].

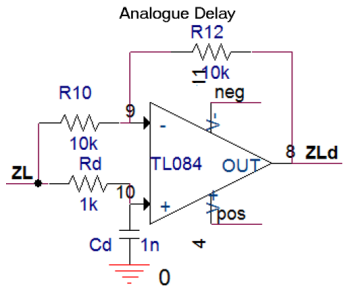

FIGURE 10. THE PADÉ DELAY CIRCUIT INCLUDED IN THE LORENZ AND CHUA OSCILLATORS.

Compare the z-transform equation to the transfer function for the analogue circuit:

$$z = e^{s\tau} = \frac{e^{s\tau/2}}{e^{-s\tau/2}} \approx \frac{1 + s\tau/2}{1 - s\tau/2} \quad (7)$$

The transfer function for the circuit in Figure 10, is:

$$\frac{V_{out}}{V_{in}} = -\frac{sCdRd}{1 + sCdRd} \quad (8)$$

This gives an expression for the analogue delay, τ, in terms of circuit component values and substituting component values gives τ = 0.5*CdRd = 0.5 us. The delay circuit is connected from the Z output via the feedback path to the input of the third integrator. Figure 11 shows the 0.5 us delay introduced to the Z signal, where Zd is the delayed signal. Chaos oscillator initial conditions were obtained from a detuned 433 MHz data FM receiver integrated circuit. Since the level of the receiver noise is random, it means an intruder cannot predict where the chaos sources start, and thus makes cryptanalysis impossible.

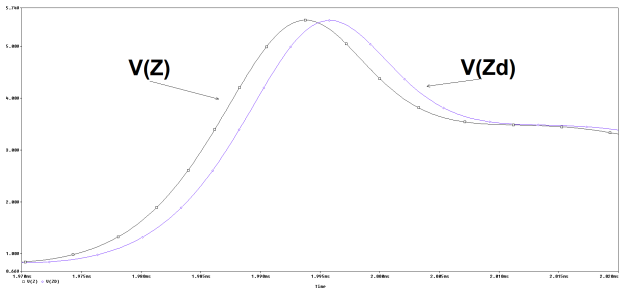

FIGURE 11. THE DELAY BETWEEN Z AND Zd IS 0.5 US

The receiver noise could be used as the primary source but external signals from an attacker, could introduce regular signals which would weaken the key.

F. The Chua chaotic oscillator

In 1983, while trying to prove the Lorenz oscillator was chaotic, Leon Chua created a new analogue chaos oscillator system defined by three first-order coupled equations as in (9). The standard Chua oscillator configuration consisted of a parallel-tuned type circuit and connected across it is a 'Chua diode'composed of segmented negative resistances achieved using operational amplifiers [48][49][50].

However, a simpler novel approach used two AD633 four-quadrant multiplier devices to implement the cubic term in (9), the term responsible for chaos [51]. An identical Padé delay to the one used in the Lorenz circuit, was also added to the y signal line to increase the signal entropy.

$$\begin{aligned} x(t) &= -\int_{t_0}^{t} \{-1.66x(t) - 10y(t) + 0.625x(t)^3\} dt \\ y(t) &= -\int_{t_0}^{t} \{-x(t) + y(t-\tau) - z(t)\} dt \\ z(t) &= -\int_{t_0}^{t} \{14.286y(t)\} dt \end{aligned} \quad (9)$$

The Chua attractor and signals in Figure 12, are similar to the Lorenz examined previously.

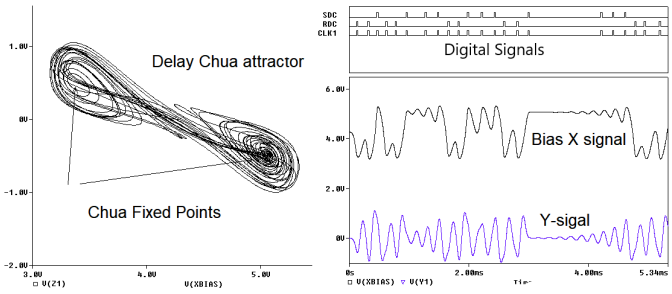

FIGURE 12. (A) THE CHUA ATTRACTOR ON THE LEFT (B) BOTTOM RIGHT PANE ARE THE ANALOGUE SIGNALS WITH THE DIGITAL SIGNALS ON TOP.

TABLE I. NIST RESULTS FOR THE COMPLETE OTP ENCODER (SHORT LENGTH OTP).

Statistical Test	*P-value natural noise*	*P-value Lorenz and Chua (XOR)*	*Pass/Fail*
Frequency	P = 0.4122	P = 0.6123	Pass
Block frequency	P = 0.1161	P = 0.1008	Pass
Runs	P = 0.7846	P = 0.0557	Pass
Block Longest Run Ones	P = 0.5388	P = 0.5850	Pass
Binary Matrix Rank	P = 0.7138	P = 0.4370	Pass
D Fourier Transform	P = 0.5206	P = 0.6840	Pass
Overlapping Template Match	P = 0.7729	P = 0.97144	Pass
Linear Complexity	P = 0.952	P = 0.4699	Pass
Serial	(P1 = 0.1971 P2 = 0.544)	(P1 = 0.0831 P2 = 0.487)	Pass
Approximate Entropy	P = 0.1143	P = 0.0603	Pass
Cumulative Sums	P = 0.4444	P = 0.6753	Pass

TABLE II. NIST RESULTS FOR THE COMPLETE ENCODER (LONG LENGTH OTP).

Random Excursion Test	χ^2 *test*	*P-value test*	*Pass/Fail*
(x =-4)	χ^2 = 3.7052	P = 0.5925	Pass
(x =-3)	χ^2 = 5.0654	P = 0.4079	Pass
(x =-2)	χ^2 = 2.1114	P = 0.8335	Pass
(x =-1)	χ^2 = 0.7659	P = 0.9791	Pass
(x = 1)	χ^2 = 1.5392	P = 0.9084	Pass
(x = 2)	χ^2 = 0.5213	P = 0.9913	Pass
(x = 3)	χ^2 = 2.2011	P = 0.8206	Pass
(x = 4)	χ^2 = 11.649	P = 0.0399	Pass

Random Excursion Variant Test	*Total visits*	*P-value*	*Pass/Fail*
(x =-9)	Total visits = 362	P = 0.0388	Pass
(x =-8)	Total visits = 412	P = 0.0645	Pass
(x =-7)	Total visits = 413	P = 0.0479	Pass
(x =-6)	Total visits = 445	P = 0.0591	Pass
(x =-5)	Total visits = 504	P = 0.1208	Pass
(x =-4)	Total visits = 525	P = 0.1228	Pass
(x =-3)	Total visits = 547	P = 0.1192	Pass
(x =-2)	Total visits = 596	P = 0.2144	Pass
(x =-1)	Total visits = 658	P = 0.6435	Pass
(x = 1)	Total visits = 673	P = 0.9565	Pass
(x = 2)	Total visits = 692	P = 0.7893	Pass
(x = 3)	Total visits = 669	P = 0.9417	Pass
(x = 4)	Total visits = 614	P = 0.5303	Pass
(x = 5)	Total visits = 620	P = 0.6178	Pass
(x = 6)	Total visits = 663	P = 0.9215	Pass
(x = 7)	Total visits = 754	P = 0.5509	Pass
(x = 8)	Total visits = 851	P = 0.2161	Pass
(x = 9)	Total visits = 899	P = 0.1392	Pass
(x = 9)	Total visits = 899	P = 0.1392	Pass

VI. TESTING THE RANDOMNESS OF THE ONE-TIME-PAD

It is impossible to say if a binary stream is random, but statistical tests such as the National Institute of Standards and Technology (NIST) suite of fifteen statistical tests (revised in 2010), can evaluate the cryptographic strength of the OTP random number sequences (see Figure 26).

These NIST Statistical null hypothesis tests examine the binary random bit stream to ascertain if the null hypothesis is verified and entails exploring the p-values to see if they are more significant than the significance level, 0.01 to 1. The test also checks the numbers produced are uniformly distributed in the interval 0:1 [52][53][54].

The NIST suite contains parameter tests to evaluate long sequences of several million bits and non-parameter tests for short sequences of 1000 bits. Table I shows NIST results for short sequences for the encoder. Included in the first column, for comparison purposes, are results from binary sequences obtained from [55]. The NIST test results for long binary sequences of several million bits are in Table II [56][57].

A. Additional randomness tests

Additional tests evaluated the entropy of the OTP for correct certification:

- Autocorrelation,
- Power Spectral Density (PSD),
- Shannon entropy,
- Kolmogorov Sinai entropy and Algorithmic Complexity,
- Histogram distribution,
- Probability Distribution Function test,
- Lyapunov exponent test, and
- Averaging test

B. Autocorrelation Test

For truly random bit sequences, the autocorrelation function test should display a Kronecker delta function over time. A display showing other correlation peaks means the stream is not truly random. The auto-correlation function for a digital sequence is the cross-correlation of a signal, $x(t)$ with a

delayed version of itself, which, for intervals of rΔt, is:

$$[R_{xx}(r\Delta t) = \frac{1}{N-r}\sum_{n=0}^{N-r} x(n)x(n+r\Delta t) \qquad (10)$$

Polar binary sequences meaning positive w.r.t. zero, will display a triangular shaped autocorrelation function rather than an impulse. Hence, it is prudent to subtract the mean from the series to obtain the correct impulse response shown in Figure 13 (Appendix Figure 23).

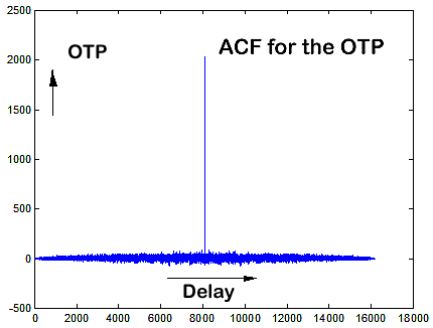

FIGURE 13. (A) THE OTP AUTOCORRELATION PLOT

C. Power Spectral Density

Spectral attacks by an adversary are possible if the Power Spectral Density (PSD) for a key is not uniform. The PSD is obtained from the absolute value of the square of the magnitude of the Fast Fourier Transform (FFT). Alternatively, apply the Wiener-Khinchine theorem to the FFT of the auto-correlation function.

$$S_x f = \lim_{T\to\infty} E\left\{\frac{1}{2T}\left|\int_{-T}^{T} x(t)e^{-j2\pi ft}dt\right|^2\right\} \qquad (11)$$

Figure 14 displays Histogram and Power Spectral Density plots of the Lena bitmap image encoded by an OTP in an XOR gate. The PSD and histogram are uniform and no bias lines are in the encoded picture. The decoded Lena image in the bottom pane shows no visible degradation. Test suites such as the ENT, TestU01, CryptX, Diehard, are similar to the NIST test suite, but NIST is considered the most comprehensive [58]. Figure 26 in the appendix shows the NIST test application software used for testing the OTP binary sequence.

D. Entropy and Information

Entropy quantifies the randomness of a cipher and Shannon and Szilard showed how information and unpredictability are connected. The French Carnot family named entropy as the portion of energy which cannot do useful work in a system [59], and the German physicist, Rudolf Clausius, defined entropy S as the ratio of the heat in a system Q to its temperature T as $S = \frac{Q}{T}$. Ludwig Boltzmann formed his kinetic theory of gases and said in any closed system entropy will always increase and is a measure of the dispersal of energy

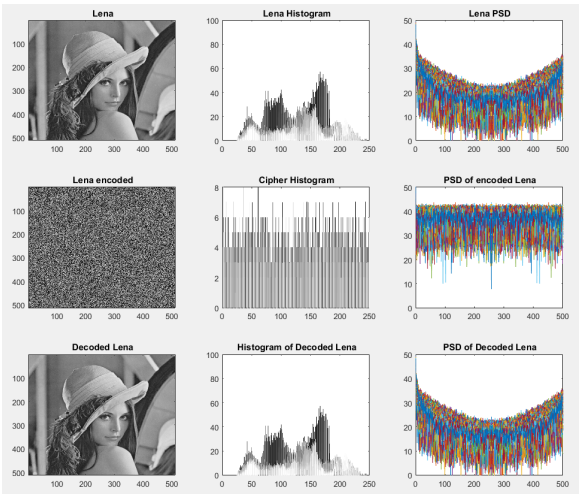

FIGURE 14. (A) THE LENA IMAGE (B) HISTOGRAM OF UNENCODED IMAGE (C) POWER SPECTRAL DENSITY OF UNENCODED IMAGE.

$S = k_B \log W$ with k_B = 1.3806x10^{-23} Joules/K. Here, W is the equiprobable number of microstates with the same dimension as entropy. According to Boltzmann's hypothesis, a logarithmic relationship exists between entropy, phase space volume, k_B, and the macroscopic and microscopic states of gas [60].

A famous thought experiment by James Clerk Maxwell called Maxwell's Demon, created a paradox [61] on the entropy of gas particles in a closed system. Szilard described a sealed box containing hot and cold gas particles and a gate operated by a devil who could separate the hot and cold gas particles without expending energy.

Leo Szilard proposed a solution by associating information with entropy, because each time the demon operated the gate he collected information. Szilard argued the information balanced the overall entropy and solved the paradox. In Szilard's doctoral dissertation (1922), and a companion paper 1929 [62], he stated there was an increase of $klog2$ units of entropy in any measurement. Later, Shannon and Kolmogorov independently argued the case for a link between information and entropy.

E. Shannon Entropy

Claude Shannon discussed the relationship between entropy and information in his 1949 paper [30] and related this to the randomness of a signal. Shannon defined entropy as a measure of the amount of information to determine precisely a system state from among all possible states. Thus, the *Shannon information content* in binary digits, or '*bits*', for an outcome, *x*, for a random sequence, *X*, with *n* outcomes, $x_1, x_2 ..... x_n$, is $h(x) = \ln \frac{1}{p(x_i)}$. A measure of uncertainty for a string of length *n*, is the *average Shannon entropy*:

$$H(x) = -\sum_{i=1}^{n} p(x_i) \ln p(x_i)\ bits \qquad (12)$$

The probability that an event x_i occurs from the number of states *n*, is $p(x_i)$, with each state having a probability between 0 and 1. The log of the probability yields 0 to negative infinity, but because entropy is positive a negative sign in (12) is

introduced. Boltzmann and Shannon entropy equations have opposite signs and a scaling factor, *-kln*2. Shannon entropy sorts objects into *N* bins of size n_i and measures the amount of information required to determine precisely a system state from all possible states. The higher the entropy of a signal, the greater the amount of information and is, therefore, a measure of signal unpredictability or randomness.

F. Kolmogorov entropy and Algorithmic Complexity

The Russian mathematician, Andrei Kolmogorov suggested in 1959, a modified form of the Shannon entropy, as did Y.Sinai in the same year, hence it is known as the Kolmogorov-Sinai (KS) entropy and is an essential metric for testing the randomness of a chaotic series. For example, KS entropy is zero for a regular series, finite for a chaotic series, but infinite for a random signal [18]. Shannon and KS entropy represents the rate at which information is created and defines when a time series is chaotic.

From an observer's resolution, the partition is, $\beta = \{X_1, X_2, ..., X_m\}$, and examining the system state, x, the observer determines only the fact that $x \in X_i$ and can reconstruct the symbolic trajectory $\alpha_n = \{s_{m_1}, s_{m_2}, \ldots, s_{m_n}\}$ corresponding to the regions visited. The entropy of a trajectory α_n, with respect to the partition β, is given by

$$H_n^\beta = -\sum_{\alpha_n} \Pr(\alpha_n) \log_{|\mathcal{A}|} \Pr(\alpha_n) \tag{13}$$

where $\Pr(\alpha_n)$ is the probability of occurrence of the substring, α_n. The conditional entropy of the $(n+1)$-th symbol provided the previous n symbols are known, is defined as:

$$h_n^\beta = h_{n+1|n}^\beta = \begin{cases} H_{n+1}^\beta - H_n^\beta, & n \geq 1 \\ H_1^\beta, & n = 1 \end{cases} \tag{14}$$

The entropy for a partition, β, is given by

$$h^\beta = \lim_{n\to\infty} h_n^\beta = \lim_{n\to\infty} \frac{1}{n} H_n^\beta$$

The KS entropy of a chaotic system is the supremum over all possible partitions.

$$h_{KS} = \sup_\beta h^\beta \tag{15}$$

The KS entropy is zero for regular systems, finite and positive for a deterministic chaos, but infinite for a random process. It is related to the Lyapunov exponents by $h_{KS} = \sum_{1\leq d\leq D} \lambda_d$, and proportional to the time horizon T on which the system is predictable. An important metric in cryptography which also measure randomness is the Kolmogorov Complexity (KC) created simultaneously by Kolmogorov and Ray Solmonoff but essentially is the Shannon entropy. KC specifies the minimum length to which a binary string of bits may be compressed (a truly random sequence is incompressible) [63]. A positive KS entropy is proof of chaotic behaviour and randomness and related to algorithmic complexity, where the system is ergodic. We may relate complexity and entropy as "cause and effect"- the more complex a system is, the more unpredictable its behaviour is and results in higher entropy. Complexity is considered the size of an "internal program" that generates a binary sequence, whereas entropy is computed from the probability distribution of that sequence.

G. Probability Distribution Function-Histograms

A Probability Distribution Function (PDF) is defined as a function from strings $\mathcal{L} = \{\alpha_j\}$, to nonnegative real numbers, i.e., $\Pr : \mathcal{L} \to [0, 1]$, such that $\sum_{\alpha\in\mathcal{L}} \Pr(\alpha) = 1$. A string α is truly random if, for any substring $\beta_n, \gamma_n \in \alpha$, $0 > n > length(\alpha)$ $\Pr(\beta_n) = \Pr(\gamma_n)$. We cannot predict any digit in a truly random string, i.e., for any symbol $s_i \in \alpha$, the conditional probability $\Pr(s_i|s_{i-1}, s_{i-2}, \ldots) = \Pr(s_i)$. A knowledge of a previous state has no effect on the probability of a successful prediction of the next state.

H. Lyapunov Exponential

The Lyapunov Exponent (LE) quantifies how chaotic trajectory orbits diverge with time and must be positive for the function to generate chaotic trajectories within a few iterations. The LE measures how fast two chaotic paths separate from each other, i.e., predicting the behaviour of a chaotic system in time. However, this measure has the disadvantage in that it does not consider the resolution under which the system is observed, unlike KS entropy [64][65]. Entropy and LE's in a chaotic system are approximately equal, and Pesin's theorem relates KS as the sum of positive LE's.

I. The average entropy test

Averaging the Lorenz *x* signal is a novel and quick test for assessing how parameter variation changes the randomness of the binary stream. A truly random signal should oscillate close to zero, but if it displays more positive than negative excursions around the zero axis, then the signal is biased. Figure 15 shows four plots for each value of *C5* and demonstrates how the delay changes the average value of the Lorenz *X* signal.

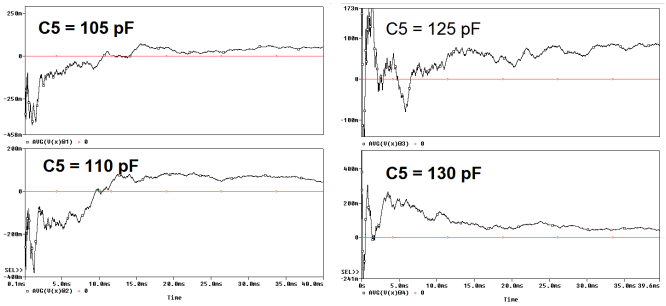

FIGURE 15. EFFECT OF C5 ON THE *X* SIGNAL ENTROPY.

The delay is changed by varying *Cd* or *Rd*, and observing the value which brought the average signal closest to the zero axis. In the prototype, the resistance, *Rd* was chosen as the variable parameter as it was the easier option. Averaging a non-random sequence of alternating ones and zeroes would also be plotted closest to the zero axis but the method is useful nevertheless for assessing the presence of bias. A positive start-up transient part can be observed in the average of *x* in Figure

16 and means the stream is biased. This necessitated rejecting the start-up transient region by the software. Figure 17 and Figure 18 show the effect of changing Lorenz parameters on the average value.

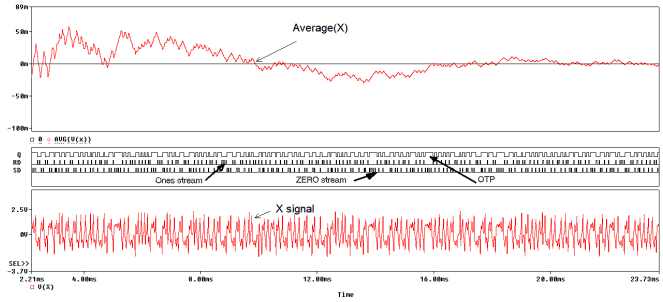

FIGURE 16. AVERAGE x FOR 0.5 US DELAY

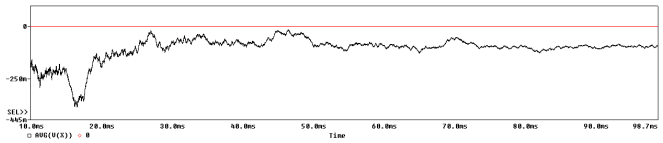

FIGURE 17. AVERAGE x FOR P = 11

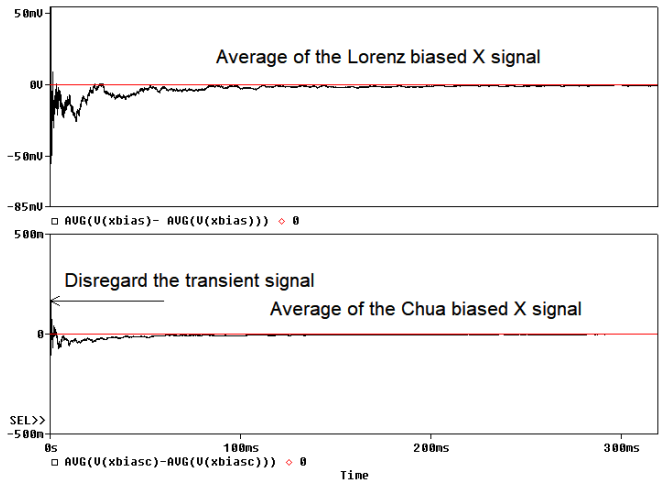

FIGURE 18. AVERAGE x FOR LORENZ AND CHUA PARAMETERS.

VII. CONCLUSION AND FUTURE WORK

Inadequate Cloud security for sensitive data stored in the Cloud was addressed by creating an extra layer of localised encoding using a truly random binary number OTP generator to return control to the client. Local encryption could reduce or eliminate, fines against companies and organisations who fail to meet the 72-hour breach deadline notification as outlined in the 2018 GDPR legislation. The proposed OTP encoder generates binary sequences from analogue chaos signals having an infinite number of states and overcome the difficulties associated with a digital implementation of an OTP which uses finite-state arithmetic and not truly random.

An analogue delay was added to the feedback paths of the Lorenz and Chua analogue oscillators to increase the OTP entropy in a novel way. Chaos sources initialised by noise from a data receiver generated truly random unlimited amounts of unbreakable binary sequences that passed the NIST statistical suite of tests. A novel testing method was developed to investigate the effect of specific parameter variation on entropy. This simple, quick test involved observing the signal average and selected the parameter which caused the average to oscillate close to the zero time axis. A JavaScript application post-processed the OTP sequences by applying a VN algorithm which maximised the sequence entropy and then combined it with the plaintext data.

A prototype printed circuit board (PCB) was tested for randomness, but future work is being planned to implement the final encoder on a Programmable System-on-Chip (PSoC) family of microcontroller integrated circuits [66]. Other planned work involves localised encryption for devices used to protect local devices used in the Internet of Things (IoT), which is growing at a fast pace and has very little security at present.

ACKNOWLEDGEMENT

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

APPENDIX

Figure 19 shows noise voltage initial conditions produce a different trajectory in the strange attractor for each noise level. This mechanism makes cryptanalysis difficult because the random nature of electronic noise produces a different value each time it is sampled.

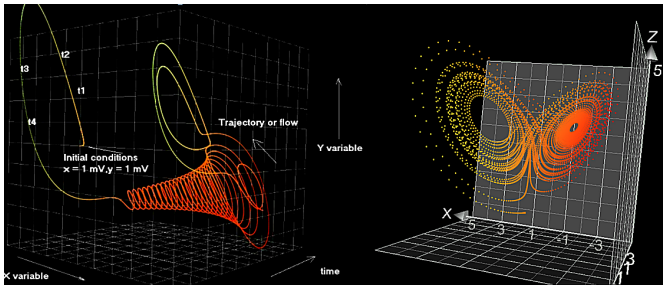

FIGURE 19. A 30D LORENZ ATTRACTOR INITIALISED BY NOISE.

Figure 20 plots a Poincaré section placed through the FPs of the attractor.

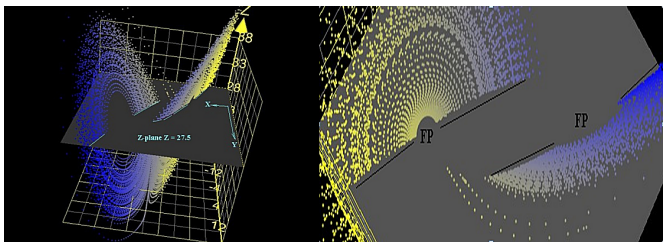

FIGURE 20. 3-D PLOT OF LORENZ ATTRACTOR.

Scaling Lorenz signals is necessary because the amplitude of the unscaled z signal shown in Figure 21 is too large at 45 V for normal electronic operation electronic implementation.

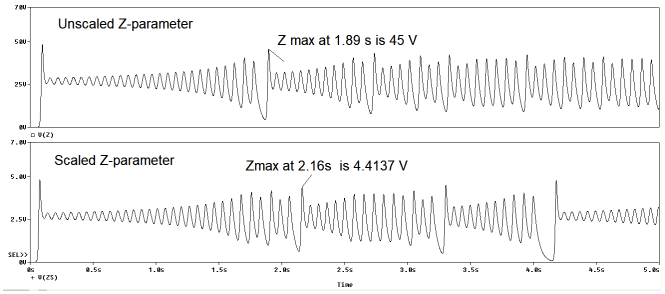

FIGURE 21. THE SCALED THE LORENZ Z SIGNAL IS IN THE LOWER PANE.

The ABM Chua circuit in Figure 22 allowed concepts to be simulated quickly and without the convergence problems of model integrated circuits. The nonlinear Chua chaos parameters are different to the previous values used. The ABM SUM, MULT, INTEG, and GAIN parts implement mathematical arithmetical functions, with a PARAM part to define any variables used.

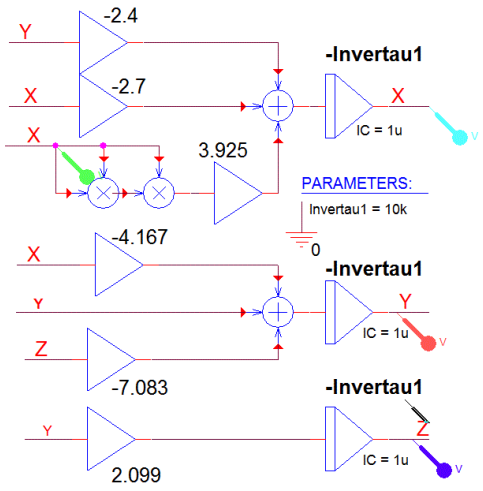

FIGURE 22. A CHUA ABM CHAOS OSCILLATOR

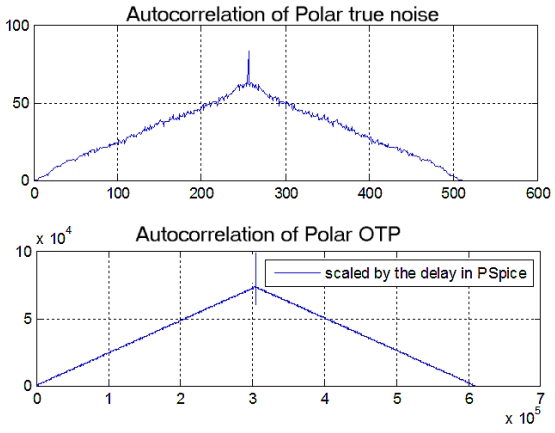

FIGURE 23. AN AUTOCORRELATION PLOT OF A POLAR NOISE SIGNAL.

The autocorrelation plots for noise and the OTP in Figure 23 shows an impulse on a triangle which is caused by the DC of a polar OTP.

Removing the average DC will display the classic impulse autocorrelation shaped response. Figure 24 shows the Lorenz out-of-phase set and reset signal pulses from the LM339 comparator and have different widths at each sampling time but are made to have a constant width using the monostable devices. External resistor-capacitor components connected to the monostable set the width of the binary pulses to a constant value. The process of producing binary signals from an analogue source is a 1-bit ADC.

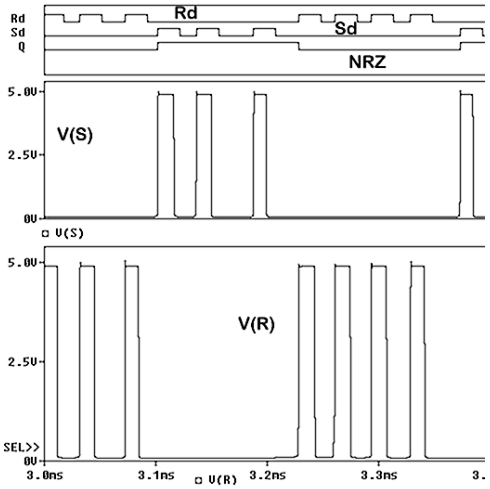

FIGURE 24. OUTPUT SET AND RESET SIGNALS FROM THE COMPARATOR.

Figure 25 illustrates how bias in the random string shows up as regular patterns in the encoded picture. This should never be allowed as any bias reduces the robustness of the OTP against attacks.

FIGURE 25. BIAS IN THE ENCODED PICTURE.

Figure 26 shows the application used to evaluate the randomness of the OTP. The parameterised tests need certain parameters inputted, as shown in the parameter boxes on the right-hand-side.

REFERENCES

[1] P. Tobin, L. Tobin, M. McKeever, and J. Blackledge, "On the Development of a One-Time Pad Generator for Personalising Cloud Security," Cloud Comput. 2017 Eighth Int. Conf. Cloud Comput. GRIDs, Virtualization, 2017, pp. 1–6.

[2] Accessed 08.12.2017. [Online]. Available: https://www.privacy-regulation.eu/en/32.htm

[3] J. P. Albrecht, "How the gdpr will change the world," Eur. Data Prot. L. Rev., vol. 2, 2016, p. 287.

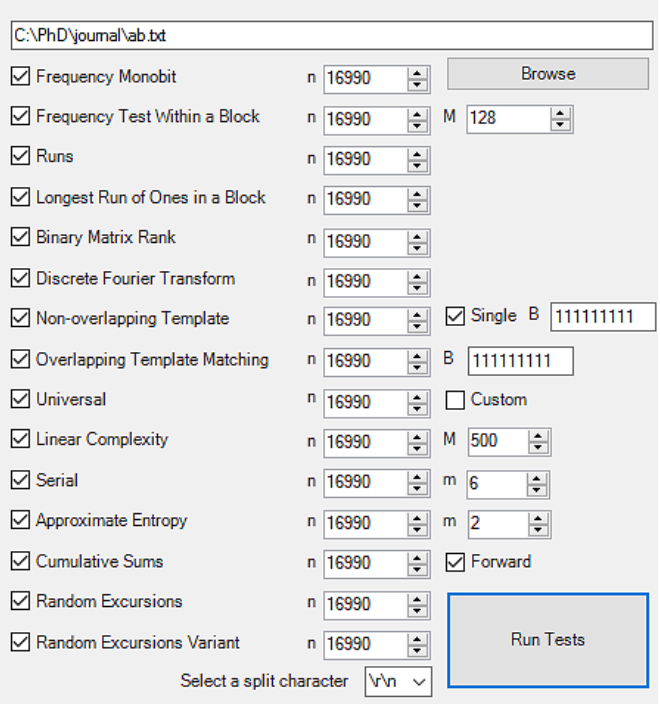

FIGURE 26. APPLICATION FOR NIST TESTING.

[4] P. Tobin, B. Duncan, M. McKeever, J. Blackledge, and M. Whittington, "UK Financial Institutions Stand to Lose Billions in GDPR Fines: How can They Mitigate This?" Cloud Comput. 2017 Eighth Int. Conf. Cloud Comput. GRIDs, Virtualization, 2017, pp. 1–6.

[5] A. Aich, A. Sen, and S. R. Dash, "A survey on cloud environment security risk and remedy," Proc. - 1st Int. Conf. Comput. Intell. Networks, CINE 2015, 2015, pp. 192–193.

[6] L. Badger, T. Grance, R. Patt-Corner, and J. Voas, "Draft cloud computing synopsis and recommendations," NIST special publication, vol. 800, 2011, p. 146.

[7] Accessed 09.12.2017. [Online]. Available: https://www.theguardian.com/media-network/media-network-blog/2014/feb/18/cloud-computing-nsa-privacy-breaches-crisis-confidence

[8] D. Shumow and N. Ferguson, "On the possibility of a back door in the nist sp800-90 dual ec prng," in Proc. Crypto, vol. 7, 2007.

[9] D. Hankerson, A. J. Menezes, and S. Vanstone, Guide to elliptic curve cryptography. Springer ScienceandBusiness Media, 2006.

[10] J. Huergo, "Nist removes cryptography algorithm from random number generator recommendations," NIST announcement, April, 2007.

[11] N. Perlroth, J. Larson, and S. Shane, "Nsa able to foil basic safeguards of privacy on web," The New York Times, vol. 5, 2013.

[12] B. Duncan and M. Whittington, "Enhancing cloud security and privacy: The power and the weakness of the audit trail," Cloud Comput, 2016, pp. 125–130.

[13] W. Blackmer, "Gdpr: Getting ready for the new eu general data protection regulation," Information Law Group, InfoLawGroup LLP, Retrieved, vol. 22, no. 08, 2016, p. 2016.

[14] S. M. Bellovin, "Frank miller: Inventor of the one-time pad," Cryptologia, vol. 35, no. 3, 2011, pp. 203–222.

[15] ——, "Vernam, mauborgne, and friedman: The one-time pad and the index of coincidence," Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 9100, 2016, pp. 40–66.

[16] W. R. Bennett, "Secret Telephony as a Historical Example of Spread-Spectrum Communication," IEEE Trans. Commun., vol. 31, no. 1, 1983, pp. 98–104.

[17] O. Hoare, "Enigma: Codebreaking and the second world war," The True Story through Contemporary Documents, introduced and selected by Oliver Hoare. UK Public Record Office, Richmond, Surrey, 2002.

[18] J. M. Blackledge, Cryptography and Steganography: New Algorithms and Applications. Center for Advanced Studies Warsaw University of Technology, 2011.

[19] D. Rijmenants, "Is one-time pad history," Cipher maschines and cryptology, vol. 5, 2011.

[20] D,Rijmenants, "The complete guide to secure communications with the one time pad cipher," Cipher Machines & Cryptology, 2010.

[21] S. Mrdovic and B. Perunicic, "Kerckhoffs' principle for intrusion detection," in Telecommunications Network Strategy and Planning Symposium, 2008. Networks 2008. The 13th International. IEEE, 2008, pp. 1–8.

[22] B. ShreeJain, S. Chandrakar, and S. Tiwari, "An innovative approach for implementation of one-time pads," International Journal of Computer Applications, vol. 89, no. 13, 2014, pp. 35–37.

[23] G. Upadhyay and M. J. Nene, "One Time Pad Generation Using Quantum Superposition States," no. 1, 2016, pp. 1882–1886.

[24] M. Borowski and M. Lesniewicz, "Modern usage of old one-time pad," Communications and Information Systems Conference (MCC), 2012 Military, 2012, pp. 1–5.

[25] M. Borowski, "The infinite source of random sequences for classified cryptographic systems," in 2016 International Conference on Military Communications and Information Systems, ICMCIS 2016, 2016.

[26] P. Tobin, L. Tobin, M. Mc Keever, and J. Blackledge, "Chaos-based cryptography for cloud computing," 2016 27th Irish Signals and Systems Conference, ISSC 2016, 2016.

[27] P. Jees and T. Diya, "Medical image protection in cloud system," matrix, vol. 2, 2016, p. 3.

[28] J. Blackledge, A. Al-Rawi, and P. Tobin, "Stegacryption of DICOM Metadata," Irish Signals Syst. Conf. 2014 2014 China-irel. Int. Conf. Inf. Commun. Technol. (ISSC 2014/CIICT 2014). 25th IET, 2014, pp. 304–309.

[29] F. A. Mohsin, R. R. Mostafa, and H. M. El Bakry, "Design of information system for facilitating litigation procedures," International Journal of Computer Engineering and Information Technology, vol. 6, no. 1, 2015, pp. 107–112.

[30] C. E. Shannon, "Communication theory of secrecy systems," Bell Labs Technical Journal, vol. 28, no. 4, 1949, pp. 656–715.

[31] C.E, Shannon, "A mathematical theory of communication," ACM SIGMOBILE Mobile Computing and Communications Review, vol. 5, no. 1, 2001, pp. 3–55.

[32] C. Pellicer-Lostao and R. Lopez-Ruiz, "Notions of chaotic cryptography: Sketch of a chaos based cryptosystem," arXiv preprint arXiv:1203.4134, 2012.

[33] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," International Journal of Bifurcation and Chaos, vol. 16, no. 08, 2006, pp. 2129–2151.

[34] W. Diffie and M. Hellman, "New directions in cryptography," IEEE transactions on Information Theory, vol. 22, no. 6, 1976, pp. 644–654.

[35] J. M. Blackledge, "On the Applications of Deterministic Chaos for Encrypting Data on the Cloud," in Third Int. Conf. Evol. Internet, 2011, pp. 78–87.

[36] V. Patidar, N. Pareek, and K. Sud, "A new substitution–diffusion based image cipher using chaotic standard and logistic maps," Communications in Nonlinear Science and Numerical Simulation, vol. 14, no. 7, 2009, pp. 3056–3075.

[37] E. B. Barker and J. M. Kelsey, Recommendation for the Entropy Sources Used for Random Bit Generator. US Department of Commerce, National Institute of Standards and Technology, 2012.

[38] J. Van Neuman, "Various techniques used in connection with random digits, collected works, 765–770," 1963.

[39] E. B. Barker and A. Roginsky, "Recommendation for Cryptographic Key Generation," NIST Spec. Publ. 800-133, 2012, pp. 1–26.

[40] S. Bruce, "Applied cryptography: protocols, algorithms, and source code in c," John WileyandSons, Inc., New York, 1996.

[41] P. M. Binder and R. V. Jensen, "Simulating chaotic behavior with finite-state machines," Physical Review A, vol. 34, no. 5, 1986, p. 4460.

[42] S. Li, X. Mou, Y. Cai, Z. Ji, and J. Zhang, "On the security of a chaotic encryption scheme: problems with computerized chaos in finite computing precision," Computer physics communications, vol. 153, no. 1, 2003, pp. 52–58.

[43] E. N. Lorenz, "Deterministic nonperiodic flow," Journal of the atmospheric sciences, vol. 20, no. 2, 1963, pp. 130–141.

[44] P. Tobin, PSpice for Digital Communications Engineering. Morgan & Claypool Publishers, 2007, vol. 2, no. 1.

[45] Tobin, Paul, PSpice for circuit theory and electronic devices. Morgan & Claypool Publishers, 2007, vol. 2, no. 1.

[46] M. Lakshmanan and D. V. Senthilkumar, Dynamics of nonlinear time-delay systems. Springer Science & Business Media, 2011.

[47] P. Tobin, "Pspice for digital signal processing," Synthesis Lectures On Digital Circuits and Systems, vol. 2, no. 1, 2007, pp. 1–142.

[48] M. P. Kennedy, "Three steps to chaos. i. evolution," IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, vol. 40, no. 10, 1993, pp. 640–656.
[49] ——, "Robust op amp realization of chua's circuit," Frequenz, vol. 46, no. 3-4, 1992, pp. 66–80.
[50] P. Kennedy, "Genealogy of chuas circuit," Chaos, CNN, Memristors and Beyond: A Festschrift for Leon Chua With DVD-ROM, composed by Eleonora Bilotta, 2013, pp. 3–24.
[51] R. Kiliç, A practical guide for studying Chua's circuits. World Scientific, 2010, vol. 71.
[52] P. M. Alcover, A. Guillamón, and M. d. C. Ruiz, "A new randomness test for bit sequences," Informatica, vol. 24, no. 3, 2013, pp. 339–356.
[53] J. M. Bahi, X. Fang, C. Guyeux, and Q. Wang, "Ramdomness quality of CI chaotic generators. Application to Internet security," Science (80-.)., 2010.
[54] K. Hamano, F. Sato, and H. Yamamoto, "A new randomness test based on linear complexity profile," IEICE Trans. Fundam. Electron. Commun. Comput. Sci., vol. E92-A, no. 1, 2009, pp. 166–172.
[55] M. Haahr, "Random. org: True random number service," School of Computer Science and Statistics, Trinity College, Dublin, Ireland. Website (http://www. random. org). Accessed, vol. 10, 2010.
[56] F. D. K. Corporation, "The Evaluation of Randomness of RPG100 by Using NIST and DIEHARD Tests," Test, 2003, pp. 1–6.
[57] D. A. Cristina and B. R. Eugen, "A new method to improve cryptographic properties of chaotic discrete dynamical systems," in Internet Technology And Secured Transactions, 2012 International Conference for. IEEE, 2012, pp. 60–65.
[58] A. NIST, "Statistical test suite for the validation of random number generators and pseudo random number generators for cryptographic applications," Special Publication, 2001, pp. 800–22.
[59] J. Boyling, "Carnot engines and the principle of increase of entropy," International Journal of Theoretical Physics, vol. 7, no. 4, 1973, pp. 291–299.
[60] R. Frigg and C. Werndl, "A guide for the perplexed," Probabilities in physics, 2, p. 115.
[61] P. Tobin and J. Blackledge, "Entropy, information, landauer's limit and moore's law," in 25th IET Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014).
[62] L. Szilard, "On the Decrease of Entropy in a Thermodynamics System by the intervention of intelligent beings," Zeitschrift für Physik, vol. 53, 1929, pp. 840–856.
[63] R. Landauer, "Irreversibility and heat generation in the computing process," IBM journal of research and development, vol. 5, no. 3, 1961, pp. 183–191.
[64] R. Wackerbauer, A. Witt, H. Atmanspacher, J. Kurths, and H. Scheingraber, "A comparative classification of complexity measures," Chaos, Solitons & Fractals, vol. 4, no. 1, 1994, pp. 133–173.
[65] K. Pawelzik and H. Schuster, "Generalized dimensions and entropies from a measured time series," Physical Review A, vol. 35, no. 1, 1987, p. 481.
[66] R. Ashby, Designer's guide to the Cypress PSoC. Newnes, 2005.