IET Computers & Digital Techniques

Special Issue: Hardware-Assisted Techniques for Security and Protection of Consumer Electronics

IET Journals
The Institution of Engineering and Technology

Practical realisation of a return map immune Lorenz-based chaotic stream cipher in circuitry

ISSN 1751-8601
Received on 14th March 2018
Revised 11th July 2018
Accepted on 05th September 2018
E-First on 1st October 2018
doi: 10.1049/iet-cdt.2018.5005
www.ietdl.org

Daniel Brown[1], Ava Hedayatipour[1] ✉, Md. Badruddoja Majumder[1], Garrett S. Rose[1], Nicole McFarlane[1], Donatello Materassi[1]

[1]*Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, TN 37996, USA*

✉ *E-mail: ahedaya1@vols.utk.edu*

Abstract: The authors report on the realisation of an encryption process in real-time analogue circuitry using on-the-shelf components and minimal processing power. Self-synchronisation of two similar systems through a single shared state is a unique property of the chaotic Lorenz attractor system. In this process, the single parameters of the system are modulated to mask a message before transmitting securely through a single-shared state. However, these techniques are vulnerable to the return map attack. They show that time-scaling can further obfuscate the modulation process and improve return map attack immunity and demonstrate a fabricated printed circuit board implementation of the system.

1 Introduction

The necessity of encrypting high amounts of data in real time has led to an increased interest in cryptography. Cryptography, code-breaking, and the use of ciphers are almost as old as documented human history. The frequency-analysis technique, invented in 800 A.D. was the most significant cryptanalytic advancement until World War II [1]. In the modern era, personal and financial information is communicated over cell phones, email, and file transfers. Therefore, secure and lightweight communication technique is one of the top priorities in the modern tech world.

Advancements in digital computer systems have made automatic encryption possible low cost and inexpensive. However, the same advancements have improved code cracking capabilities, and researchers around the world are heading towards quantum computing, capable of cracking the usual encryption methods. Both asymmetric and symmetric ciphers take advantage of the increased efficiency current processors [2, 3]. These techniques, requiring more computational overhead, are often troublesome to fit into the highly constrained Internet of Things devices.

Chaotic encryption, using maps or nonlinear system models, provides an alternative method for secure data communication [4, 5]. This method is based on the ability of a dynamic system to produce a sequence of numbers that are random in nature. However, this sequence of random numbers is highly dependent on the initial condition, which can be used in the decryption phase for regenerating the sequence. A slight deviation in the initial condition results in an entirely different sequence. This sensitivity to parameters and initial conditions make chaotic systems ideal for encryption and they can be used in a bit-wise manner over multiple layers [6]. In this work, we use chaotic shift keying (CSK), by employing a Lorentz system model for plain text obfuscation. Power, particularly in the age of internet of things, is at a premium, thus the ability to implement this system with substantially lowered power consumption is an advantage. The work presented in this study has been modified from [7]. The power consumption used by our developed system can be several orders of magnitude lower than the power consumption required by a microprocessor to implement a standard digital encryption technique.

This paper is organised as follows: Section 2 introduces the advantages and disadvantages of a chaotic stream cipher and introduces the option to strengthen vulnerabilities through the use of a time-scaling factor. Section 3 summarises the simulation and implementation of a CSK system using analogue circuit components. Section 4 gives the results of the fabricated system, and Section 5 discusses the results in detail. Finally, we provide some concluding remarks in Section 6.

2 Chaotic synchronisation

Chaotic systems, each with different starting initial conditions, because of the exponential divergence of the nearby trajectories of chaotic systems, may seem surprising to match. However, when the two systems are coupled, they share a single state, which is provided by the drive system and can exhibit a phenomenon known as synchronisation of chaos [8]. The second system is known as the driven system. These previous experiments showed that the success of synchronisation is limited by how well the system parameters are matched.

Since these systems can be synchronised, they can take advantage of creating encryption masks. This has been successfully used in speech applications, but the theory places severe limits on the kinds of data to be securely communicated between two systems [9]. Chaos using a Lorenz system and Chua's circuit has been used for masking of binary systems [10, 11]. CSK which utilises a chaotic Lorenz system incorporates the advantages provided by digital systems including checksum error detection and bitwise encryption.

The Lorenz-based CSK system is described by the following equation:

$$\begin{aligned} \dot{x}_1 &= \sigma(x_2 - x_2), & \dot{z}_1 &= \sigma(z_2 - z_1), \\ \dot{x}_2 &= (\beta(m) - x_3)x_1 - x_2, & \dot{z}_2 &= (\beta(m) - z_3)x_1 - z_2, \\ \dot{x}_3 &= x_1x_2 - \rho x_3, & \dot{z}_3 &= x_1z_2 - \rho z_3\,. \end{aligned} \tag{1}$$

The system states x_1, x_2, and x_3 describe the system which is performing the driving or transmitting function. The system states z_1, z_2, and z_3 describe the system which is being driven or receiving. σ is Prandtl's number. $\beta(m)$ is given by

$$\beta(m) = \begin{Bmatrix} \beta_0 & \text{if} & m = 0 \\ \beta_1 & \text{if} & m = 1 \end{Bmatrix} \tag{2}$$

and is a binary variable gain parameter which masks the binary signal m. β_0 and β_1 are different enough to mitigate noise and parameter uncertainty extraction errors, and are within some tolerance value. This tolerance limit should not affect the

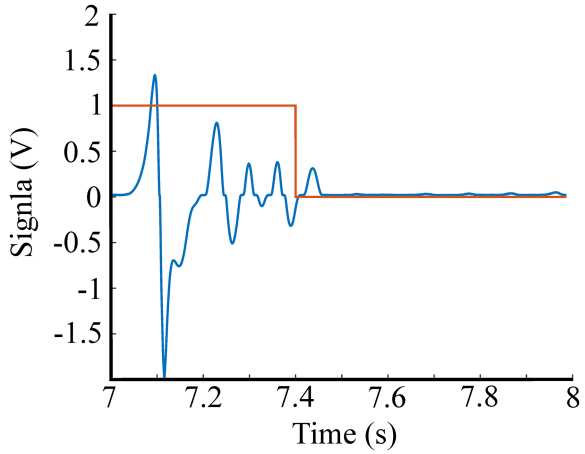


Fig. 1 *Simulation of $x_1 - z_1$ versus the message, m, for a double alternating bit space*

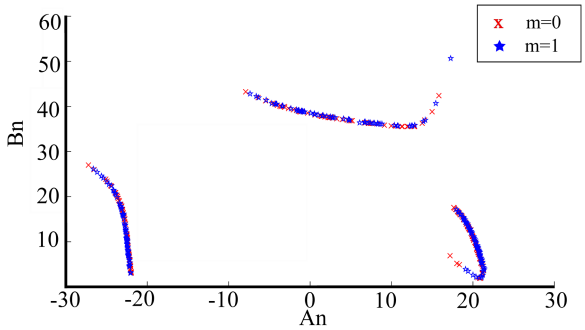


Fig. 2 *CSK RM determined using x*

transmitted state signal characteristics. The synchronisation error, Φ_{sync}, is

$$\Phi_{\text{sync}} = \begin{bmatrix} \Phi_1 \\ \Phi_2 \\ \Phi_3 \end{bmatrix}, \tag{3}$$

$$\Phi_1 = x_1 - z_1,$$
$$\Phi_2 = x_2 - z_2,$$
$$\Phi_3 = x_3 - z_3.$$

For $m = 0$, the derivatives with respect to time of the error states synchronisation are

$$\begin{aligned} \dot{\Phi}_1 &= \dot{x}_1 - \dot{z}_1 = \sigma(\Phi_2 - \Phi_1), \\ \dot{\Phi}_2 &= \dot{x}_2 - \dot{z}_2 = -(x_2 - z_2) - (x_3 - z_3)x_1 = -\Phi_3 x_1 - \Phi_2, \\ \dot{\Phi}_3 &= \dot{x}_3 - \dot{z}_3 = (x_2 - z_2)x_1 - \rho(x_3 - z_3) = \Phi_2 x_1 - \rho\Phi_3. \end{aligned} \tag{4}$$

$V(\Phi)$ is a Lyapunov function. This function is chosen, based on [10] to demonstrate stable asymptotic synchronisation error Φ_{sync} when the message $m = 0$

$$\begin{aligned} V(\Phi) &= \frac{1}{\sigma}\Phi_1^2 + \frac{1}{\sigma}\Phi_2^2 + \frac{1}{\sigma}\Phi_3^2, \\ \dot{V}(\Phi) &= \frac{2}{\sigma}\dot{\Phi}_1\Phi_1 + \dot{\Phi}_2\Phi_2 + \dot{\Phi}_3\Phi_3 \\ &= -(\Phi_1 - \Phi_2)^2 - \Phi_1^2 - \rho\Phi_3^2. \end{aligned} \tag{5}$$

For $m = 0$, it can be seen that global asymptotic stability can be demonstrated. In (5), $V(\Phi)$ is positive definite and radially unbound. $\dot{V}(\Phi)$ is negative definite. Furthermore, it can be shown that for $m = 1$, synchronisation error's derivative with respect to time is

$$\begin{aligned} \dot{\Phi}_1 &= \sigma(\Phi_2 - \Phi_1), \\ \dot{\Phi}_2 &= \dot{x}_2 - \dot{z}_2 = (\beta_\Delta - \Phi_3)x_1 - \Phi_2, \\ \dot{\Phi}_3 &= \Phi_2 x_1 - \rho\Phi_3, \end{aligned} \tag{6}$$

where

$$\beta_\Delta = \beta_1 - \beta_0. \tag{7}$$

From (6), the coordinate at which synchronisation occurs, $\Phi_{\text{sync}} = [0 \quad 0 \quad 0]^{\text{t}}$, does not reflect a system equilibrium. This creates a mismatch in synchronisation resulting in an error relative to the message, m. This mismatch is displayed in Fig. 1.

Analogue circuits, such as resistors, capacitors, comparators, and operational amplifiers, can be used to implement mathematical functions and are often used to accomplish low-power signal processing. Thus, the dynamic chaotic encryption techniques can be implemented using electronics. CSK encryption technologies are not currently available commercially for widespread use. There has been some limited implementation in circuits; however, the CSK system is probably not secure [12].

2.1 Return map (RM) attack

There are a number of techniques that can defeat CSK encryptions methods, one of these is the RM attack. In this method, the local extrema are observed to determine the time-varying features of the system [13]. It relies on the idea that due to the symmetric nature of the Lorenz system, a dynamic RM that tends towards a one-dimensional set can be developed by examining a single state.

To achieve this, the RM from the nth local extrema (maxima and minima) of the initial or secondary state of (1), is written as $\bar{X}_n$ and $\bar{Y}_n$, respectively. A comparison of functions makes up the developed RM and is

$$\begin{aligned} A_n &= \bar{X}_n + \bar{Y}_n, \\ B_n &= \bar{X}_n - \bar{Y}_n. \end{aligned} \tag{8}$$

A plot of A_n as a function of B_n yields the three line RM. The map may be described by correlating the local extrema to the foci. The map is then determined from the output state of x and the resulting map using the CSK encryption methodology is shown in Fig. 2.

The CSK method previously described in Section 2, will always be vulnerable to the RM attack since it relies on data encryption through direct modulation of system parameters β or ρ. The CSK technique modulates the foci depending on the bit present. This leads to the RM vulnerability due to the significant distortion in the system dynamics [14].

2.2 Return time map (RTM) attack

A time-scaling encryption modulation can easily mitigate an RM attack. An RM attack can easily be defeated by performing the encryption modulation in a time-scaling factor. The time-scaling factor on maxima and the time window between maxima of the transmitted signal, RTM attacks can be used [15]. An example RTM is shown in Fig. 3, where there is a time-scaling factor that has only a switching event that occurs at bit changes. This is detected by only looking for significant changes in the transmitted state. The RTM attack is not required here, however as Fig. 3 shows, an RTM can aid when simple false switching events occur.

2.3 Time scaling CSK

CSK security vulnerabilities to RM attacks can be mitigated using a 'time-scaling function', $\lambda(x(t), m)$ to encrypt the plain-text message, $m(t)$. For any autonomous dynamical system

$$\frac{\mathrm{d}}{\mathrm{d}t}x = f(x), \tag{9}$$

where the time-scaling function is defined by

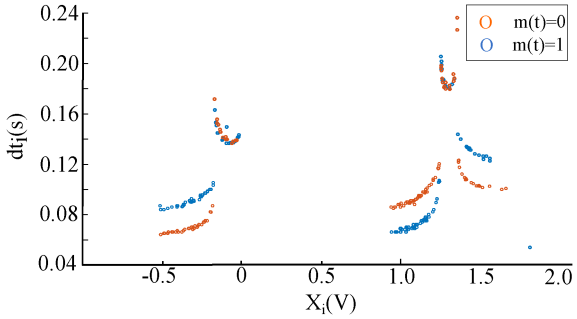


Fig. 3 *RTM calculated using TS-CSK encryption*

$$\begin{aligned} \frac{\mathrm{d}t}{\mathrm{d}\tau} &= \lambda(x), \\ \tau(t_0) &= \tau_0, \\ 0 < \lambda(x) &< \infty . \end{aligned} \tag{10}$$

It is clear that then

$$\frac{\mathrm{d}}{\mathrm{d}\tau}x = \lambda(x)f(x). \tag{11}$$

From (10) τ is strictly monotonic and increases with time t [16]. From (11), $\lambda(x)$ does not alter the phase space of x with respect to its attractors or equilibria. The trajectory of x is not distorted by the time-scaling factor. The only effect is to change the time to complete or reach a stable value [12]. The RM attack can be thwarted by encoding the message, $m(t)$, with the time-scaling factor. This occurs due to the dependence on the variation of the state phase space.

We apply this time-scaling factor to a Lorenz-based chaotic system by using a function, λ (x,m), to create a time-scaling CSK (TS-CSK) encryption system. The system equations then become

$$\begin{aligned} \dot{x}_1 &= \sigma(x_2 - x_2)\lambda(x,m), \\ \dot{z}_1 &= \sigma(z_2 - z_1)\lambda(z,0), \\ \dot{x}_2 &= ((\beta(m) - x_3)x_1 - x_2)\lambda(x,m), \\ \dot{z}_2 &= ((\beta(m) - z_3)x_1 - z_2)\lambda(z,0), \\ \dot{x}_3 &= (x_1x_2 - \rho x_3)\lambda(x,m), \\ \dot{z}_3 &= (x_1z_2 - \rho z_3)\lambda(z,0), \end{aligned} \tag{12}$$

where

$$\lambda(x,m) = \begin{Bmatrix} \lambda_m & \text{if} \quad \delta_x = 0 \\ \lambda_{1-m} & \text{if} \quad \delta_x = 1 \end{Bmatrix}, \tag{13}$$

where $\delta(x)$ is the decision engine. Putting security as the paramount consideration, the decision engine should be selected such that the switching event of $\lambda(x,m)$ cannot be decoded or extracted from the signal that is being communicated. There are several options for (x), which satisfy these conditions. Materassi and Basso [12] use $\delta(x)$ such that

$$\delta(x) = \begin{Bmatrix} 0 & \dfrac{\boldsymbol{\upsilon}^{\mathrm{T}}x}{h} & \text{is even} \\ 1 & \dfrac{\boldsymbol{\upsilon}^{\mathrm{T}}x}{h} & \text{is odd} \end{Bmatrix}, \tag{14}$$

where the unitary selection vector $\boldsymbol{\upsilon}$ is

$$\Phi_{\text{sync}} = \begin{bmatrix} \upsilon_1 \\ \upsilon_2 \\ \upsilon_3 \end{bmatrix}. \tag{15}$$

However, the implementation of this decision engine gets increasingly difficult and expensive, when the oscillation rate of the Lorenz system is higher. Based on these considerations and starting with the idea of simplifying to two regions, the initial decision engine was designed

$$\delta(x) = \begin{Bmatrix} 0 & \upsilon^{\mathrm{T}}x < 0 \\ 1 & \upsilon^{\mathrm{T}}x \geq 0 \end{Bmatrix}. \tag{16}$$

The decision engine described by (14) thwarts both types of return attacks (RM and RTM) [12]. As the RM does not modify the underlying Lorenz function in correlation with the orbital foci, TS-CSK encryption mitigates the RM attack. As long as x, for the TS-CSK system of (12), is chosen so that the underlying Lorenz system is chaotic, then the system is protected from RM attacks. RTM attacks require the message, $m(t)$, to somewhat obscure the time difference between orbits. An even–odd scheme, where there is an adequate number of switching occurring between bit changes can obfuscate such that it is impossible to extract based on RTM citematerassi2008time. It must be noted that this immunity does not hold for plus-minus TS-CSK (PM TS-CSK) decision engines with a reasonable time difference between bits, instead of requiring a marginally more complicated decision engine. This is borne out of the system equations

$$\delta(x) = \begin{Bmatrix} \delta_z & x_2(t) < -\sqrt{\rho(\beta-1)} \\ 1-\delta_z & -\sqrt{\rho(\beta-1)} \leq x_2(t) < 0 \\ \delta_z & 0 < x_2(t) < \sqrt{\rho(\beta-1)} \\ 1-\delta_z & x_2(t) \geq \sqrt{\rho(\beta-1)} \end{Bmatrix}, \tag{17}$$

where

$$\delta_z = \begin{Bmatrix} 1 & x_3(t) \geq \beta - 1 \\ 0 & x_3(t) < \beta - 1 \end{Bmatrix}. \tag{18}$$

The regions of operation and switching of the equilibrium of the system are derived from this new decision engine. When the third dynamic, $x_3(t)$, crosses from one side of its equilibrium to the other the system switches. The system splits the second dynamic into four regions to increase the regions of operation. These regions are below the negative focus, between the negative focus and the origin, between the origin and the positive focus, and above the positive focus. Equations (17) and (18) describe the eight-section TS-CSK system. The synchronisation of the system, seen in (12), is again described using the same Lyapunov function as (5) and with the same error function Φ_{sync} as indicated in (3). The derivative with respect to time of Φ_{sync} when the message $m(t) = 0$ is

$$\begin{aligned} \dot{\Phi}_1 &= \sigma(\lambda_x(x_2 - x_1) - \lambda_z(z_2 - z_1)), \\ \dot{\Phi}_2 &= (\beta(\lambda_x - \lambda_z) + (\lambda_z z_3 - \lambda_x x_3))x_1 + \lambda_z z_2 - \lambda_x x_2, \\ \dot{\Phi}_3 &= (\lambda_x x_2 - \lambda_z z_2)x_1 + \rho(\lambda_z z_3 - \lambda_x x_3). \end{aligned} \tag{19}$$

The situation that occurs when the time-scaling factor of the two systems are equal is the interesting case to study. This occurs when $\lambda(x) = \lambda(z)$. When the message $m(t) = 0$, this occurs for x and z within the same region of operation. Thus, $\lambda(x) = \lambda(z)$, (19) reduces to an expression much like that of (4). The Lyapunov equation indicates the asymptotic stability of the point $\Phi_{\text{sync}} = [0 \quad 0 \quad 0]^{\mathrm{T}}$. For both systems $\lambda(x) \neq \lambda(z)$ is not always true. However, the chaotic system is cyclic. Additionally, the time-scaling factor does not change the phase space. Thus, the regions of $\lambda(x) \neq \lambda(z)$ are periodic when no synchronisation is occurring.

3 Practical system realisation

The CSK system described in the previously mentioned expression is shown in the block diagrams of the encryption transmitter (Fig. 4) and the receiver system (Fig. 5). The Gaussian noise corrupts the transmitted state x_1.

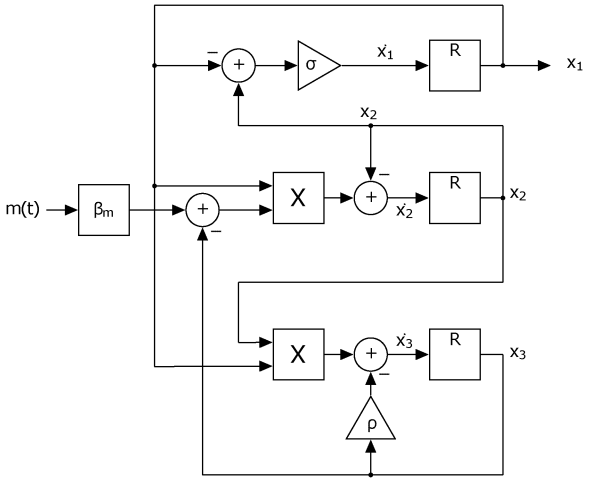


Fig. 4 *CSK transmitter system block diagram*

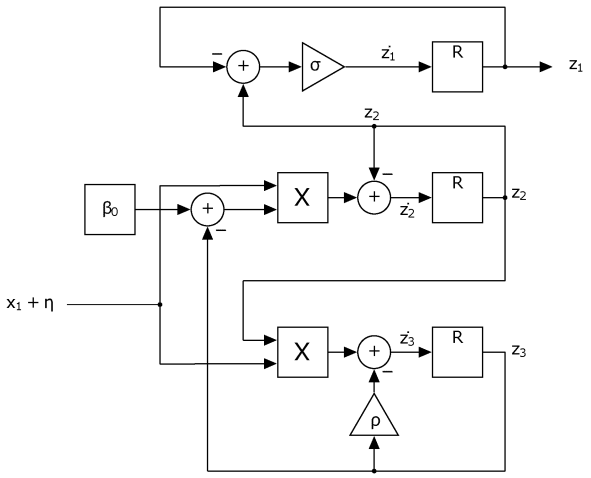


Fig. 5 *CSK receiver system block diagram*

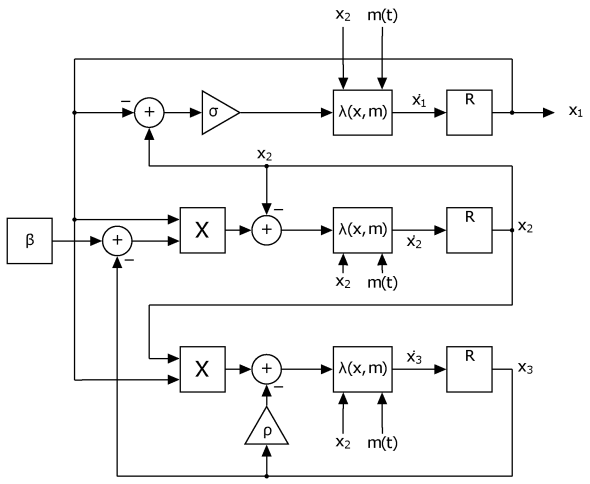


Fig. 6 *TS-CSK system transmitter*

The β_m module was implemented using a simple set of math functions. The equation used was $\beta_m = (\beta_1 - \beta_0)m(t) + \beta_0$. The message was encoded using the modulation block. Fig. 6 shows the TS-CSK Simulink block diagram of the communication system (transmitter and receiver) (Fig. 7). The TS-CSK system as implemented, compared with the CSK system has increased network complexity and components. The TS-CSK system, implemented with the analogue component is shown in Fig. 8. The function $\lambda(x,m)$ exists in both the transmitter and receiver modules. It is described in (13). The λ-modulation function is distributed inside the equations to maintain parallelism to the CSK system. This distribution also eliminates the need for increased logic gates. Thus, (12) becomes

$$\begin{aligned} \dot{q}_1 &= \sigma(\lambda(q,m)q_2 - \lambda(q,m)q_1), \\ \dot{q}_2 &= \beta g - g q_3 - \lambda(q,m)q_2, \\ \dot{q}_3 &= g q_2 - \rho\lambda(q,m)q_3, \end{aligned} \tag{20}$$

where g is chosen to be $\lambda(q,m)q_1$ or $\lambda(q,m)s$. This choice is dependent on whether the system is operating as a transmitter or receiver.

The circuits are implemented using discrete components. The operational amplifier used is an LT1057, as an excellent low noise fast amplification option and an AD633 is used as the multiplier of choice. The DG419 handles the switching tasks.

The LT1057 was configured as a differential amplifier in order to extract $\Phi_{\text{sync}} = x_1 z_1$. This is shown in Fig. 9. The amplifier output has an anti-parallel diode couple in series with it to remove synchronisation signal error. This synchronisation error (small) is due to the difference in resistor and gain values (mismatch) that occurs in the implemented transmitter and receiver systems.

3.1 Message extraction

Periodic averaging is used for message extraction. This approach uses a thresholding to make a decision. As implemented in the simulator, data is compared with $m(t)$ once a decision is made for each potential bit. This approach uses prior knowledge of the expected message frequency. Selecting a threshold level is necessary so that all bits can be extracted accurately. In the electrical bench testing, this value is experimentally varied until the best results are obtained. The periodic averaging is

$$\psi(m) = \frac{1}{T}\int_{\tau_0}^{\tau_1} \varphi(n)\text{sync}(n)\text{d}n, \tag{21}$$

$$m_\tau(t) = \begin{Bmatrix} 1 & \psi \geq \chi \\ 0 & \psi < \chi \end{Bmatrix}, \tag{22}$$

where $\varphi(n)$ is a weighting function, χ is the threshold, $\tau_0 = T(\text{floor}(t/T))$, and $\tau_1 = \tau_0 + T$. The weighting function used is

$$\varphi(n) = \begin{Bmatrix} 0.5 & n < \tau_0 + (1-\omega)\Delta\tau \\ 1 & n > \tau_0 + \omega\Delta\tau \\ 2 & \text{otherwise} \end{Bmatrix}. \tag{23}$$

The decision engine uses a series of comparators, voltage references, and logic gates to perform the λ selection. The eight-section TS-CSK decision engine circuit performs the logical operation of

$$d(x,m,t) = ((\bar{A} + B\bar{C}) \oplus D) \oplus \bar{m}(t), \tag{24}$$

where

$$\begin{aligned} A &= \begin{Bmatrix} 0 & q_2(t) < -\sqrt{\rho(\beta-1)} \\ 1 & q_2(t) \geq -\sqrt{\rho(\beta-1)} \end{Bmatrix}, \\ B &= \begin{Bmatrix} 0 & q_2(t) < 0 \\ 1 & q_2(t) > 0 \end{Bmatrix}, \\ C &= \begin{Bmatrix} 0 & q_2(t) < \sqrt{\rho(\beta-1)} \\ 1 & q_2(t) \geq \sqrt{\rho(\beta-1)} \end{Bmatrix}, \\ D &= \begin{Bmatrix} 0 & q_3(t) < \beta - 1 \\ 1 & q_3(t) \geq \beta - 1 \end{Bmatrix}. \end{aligned} \tag{25}$$

In the discrete design, an LT1011 from the Linear Technology was used as the comparator, 74HC00D series NAND chip was used to provide the four NAND gates that comprise the logic, and the 74HC266D series was chosen to perform the two XNOR

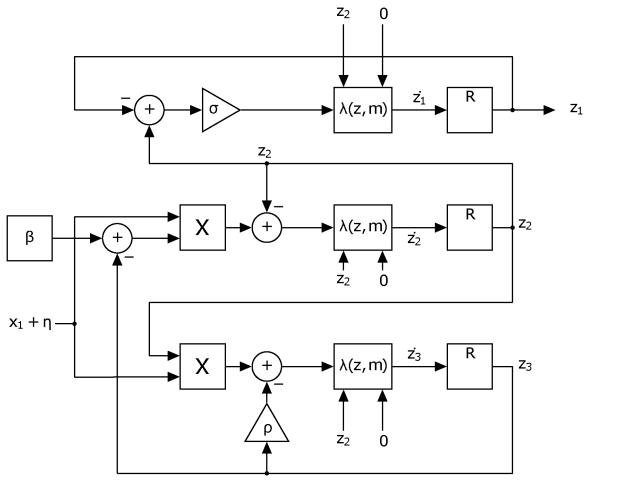


Fig. 7 *TS-CSK system receiver*

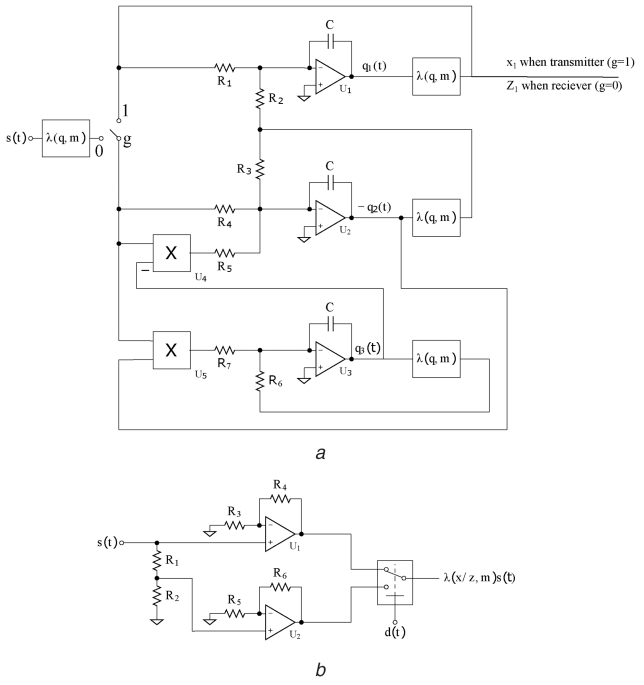


Fig. 8 *TS-CSK system*
(a) TS-CSK circuit schematic, ***(b)*** Modulator circuit schematic

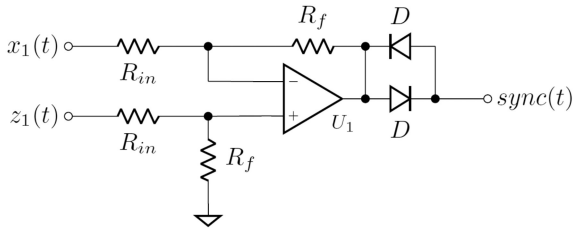


Fig. 9 *Differential amplifier in to extract output*
(a) TS-CSK circuit diagram, ***(b)*** Circuit diagram of the modulator

operations. The printed circuit board (PCB) design with surface mount devices based on the discrete circuit components is shown in Fig. 10. The resistors R14 and R15 as seen in Fig. 10*a* at the bottom centre of the board are used in coordination as a solder-able jumper selection to enable either transmitter or receiver operation. This initial board incorporates a simple decision engine that performs the decision from (12) that was changed to the decision-making circuit in Fig. 10*b* to be less vulnerable to RTM attacks.

4 System performance: simulation and experimental results

In the simulation, a bit pattern which alternates simulated the expected worst case switching behaviour. Reasonable data transmission rates and minimised transmission error in $\Phi_1 = x_1 z_1$ were ensured by choosing a suitable frequency. After choosing the circuit parameters, longer simulation runs were executed to obtain the output data. Matlab was used to calculate the RTMs for both the CSK and TS-CSK generated output data. Monte-Carlo, taking into account statistical variations, ensured the applicability and robustness of the system design. Fig. 11 shows the transmitted signal $x_1(t)$ sent in response to the encrypted message $m(t)$. Fig. 11*a* shows the Simulink model's response. Fig. 11*b* shows the experimental measurements including the actual signal $m(t)$.

Figs. 12–14 show the results of the RM attack described in Section 2. Figs. 12*a* and *b* compare the Matlab-simulated RMs for the CSK and TS-CSK systems, respectively. The difference in bit paths for the CSK system is shown in Fig. 12*a* in a zoomed in the plot. Figs. 13*a* and *b* show the SPICE-simulated RMs.

Fig. 14 shows the experimentally measured RM measured from the PCB. The eight-section TS-CSK system is compared with the CSK system, although the PM TS-CSK system demonstrates a similar RM. Alternating bit patterns at a frequency of 1 Hz for the SPICE simulation and experimental measurements were used for the RMs. No bit padding is added to any bit.

Discrete devices have value mismatches that, e.g. can range from 10 to 0.1% for resistors. The worst case parameter mismatch due to the tolerances is considered in the SPICE simulation of Fig. 15. A Monte-Carlo simulation, consisting of 300 runs, with the reference voltages set at the maximum variation from the nominal, was performed. These values are based on the manufacturer supplied data. The error $\Phi_1(t) = x_1(t) - z_1(t)$ is shown in the figure. $\Phi_1^2(t) = (x_1(t) - z_1(t))^2$ is shown in the middle figure. $m(t)$ is displayed in the bottom figure. The results of a randomly selected plain-text message encryption test are displayed in Table 1.

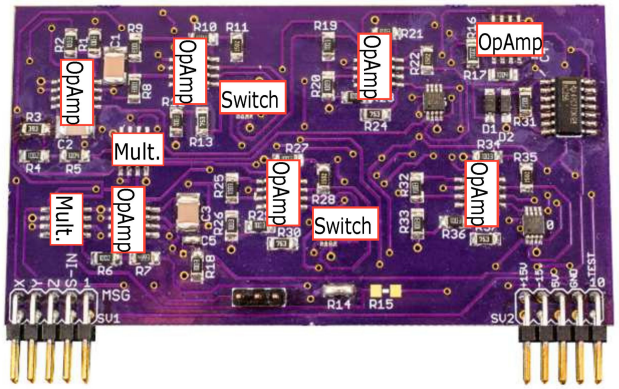
A file containing 2500 randomly generated ASCII characters from a HEX value of 0×20 to $0 \times 7E$ was used. The range is limited by bandwidth limitation through the UART between MATLAB and the message signal generator for characters higher than $0 \times 7E$. The Simulink simulation test required a bigger file. 10,000 additional characters (also randomly generated) were appended to the original 2500. The eight-section TS-CSK was limited to 1620 characters due to the length of time for a measurement. The data acquisition system used limited the ability to sequentially encrypt characters in the experimental measurement. All 12,500 characters were sequentially encrypted in the simulation. The PM TS-CSK PCB experiment took 6.5 h with a 1 Hz message frequency. The eight-section TS-CSK PCB experiment took 12 h with a 0.5 Hz message frequency. The decreased message frequency of the TS-CSK circuit is due to the reduced synchronisation.

The experimental measurements of the eight-state TS-CSK system, unlike the CSK and PM TS-CSK system, show the potential for this cryptographic method in real world implementations. The overall performance of the TS-CSK system can be broken into several sections. While security is the primary concern for any encryption system, the usefulness of the system is also important. This usability depends on functioning synchronisation, noise, and mismatch. Weak security but otherwise good performance can still be usable as weak encryption. However, strong security with real world synchronisation failure is of little use.

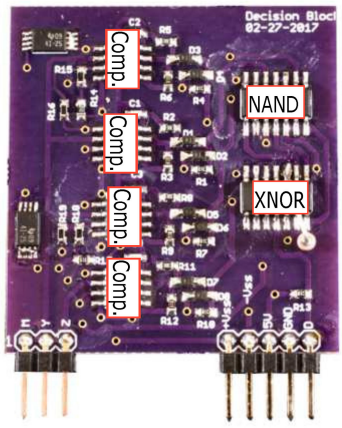
4.1 Synchronisation characteristics

The degree of synchronisation of the TS-CSK system was evaluated using simulation. A summary of the performance characteristics is summarised in Table 1. Matlab Simulink results of the eight-state TS-CSK system is shown in the first column of the table. Using the simple weighted averaging over the previously described bit periods, after the processing of 12,500 characters, no bit errors are evident. The simulated bit error rate (BER) exceeds ten parts per million.

The BER of the simple PM TS-CSK is shown in column two of the table. The BER decreases to 800 parts per million. The final

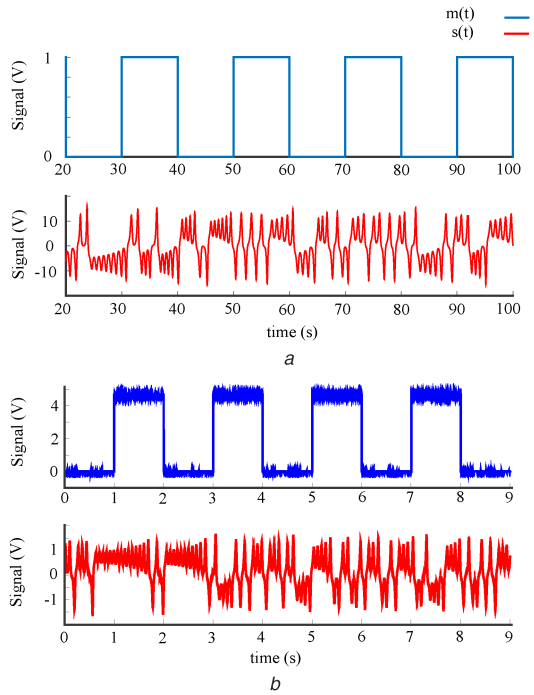


a



b

Fig. 10 *Physical implementation on PCB of*
(a) TS-CSK system, ***(b)*** Decision engine



a

b

Fig. 11 *Transmitted signal $x_1(t)$ versus the message $m(t)$*
(a) Simulation capture, ***(b)*** Actual capture

column shows 2000 parts per million BER (0.3% BER) for the eight-state TS-CSK system.

Based on these performance characteristics, the PM TS-CSK performs adequately. The addition of parity checking does not severely degrade the accuracy or rate of the transmitted data. Four times the number of errors is seen in the eight-state TS-CSK system. In both systems, the use of the optimised threshold results in the PM TS-CSK system missing the lows and the eight-section TS-CSK system missing the highs.

For the PM TS-CSK system, when some of the bits go high, the size of the error in synchronisation is a very small percentage of the error for the other bit changes. Thus, for the optimum BER, there is an asymmetric bit miss rate.

In a few instances, the eight-state TS-CSK system showed a limited change in magnitude as the bits go from 0 to 1 (Fig. 16). This characteristic allowed the eight-state TS-CSK approach to exhibiting low- to high-bit changes that were impossible to isolate from the synchronised background. While the system is in the non-synchronising state, the bit frequency increases (Fig. 16).

4.2 Noise characteristics

Noise is a fundamental limit on any system performance and may be due to the noise inherent to the system parameters or external environmental noise. The signal-to-noise ratio is <40 dB. This results in the exceedingly superior BER to fall to a complete loss of all the low bits. Based on Cisco recommendation, for voice applications, the signal to noise ratio should be 25 dB. For data networks and wireless transmissions, the signal-to-noise ratio should be 20 dB [17]. For the TS-CSK system to be utilised commercially, the minimum signal to noise needs to be decreased.

4.3 Effects of mismatch and variation

All electronic components have variation due to the imprecise nature of their fabrication process. This results in these components having a nominal value plus or minus some tolerance. These tolerances have a statistical pattern, and Monte-Carlo simulations can be used to determine how these deviations affect a system. In this work, we focus on the resistors and capacitor tolerances. Due to the use of feedback, the other discrete components effect of variation on the system is minimised. Spice was used to simulate the eight-section TS-CSK system using the nominal values. Based on simulations, the use of 'high accuracy' components should allow for synchronisation to occur. However, this was not borne out experimentally. The synchronisation mismatch in the fabricated eight-section TS-CSK system was severely diminished. Figs. 15 and 16 show the results using worst case tolerances (maximum deviation from nominal). This result was verified experimentally.

Much of this synchronisation error is due to the mismatch in the Zener diodes used for voltage regulation. Each transmitter system and receiver system have their own decision engine board. The original crossing point is the same for both the upper and lower foci. The selected Zener diodes have a $\pm 1\%$ tolerance. This causes the third state foci set point to vary. The solder-less breadboard used to fabricate the system also contributes to the synchronisation error. Two breadboards were made for this system. One was used in the experiments reported in this work. However, the second board failed. Further experiments are required to determine the reason for the failure. One possible reason is that this breadboard, which had been used in previous circuits' experiments, had traces which were no longer electrically viable. A digital multimeter was used to verify all voltages and component values.

4.4 System response to vulnerabilities

The susceptibility of the chaotic encryption scheme was evaluated using the system return and RTMs against standard cryptanalysis methods.

4.4.1 Cipher text attacks: Digital encryption methods and ciphers are subject to a number of attacks. Not all attacks apply to the TS-CSK system. We perform a brief examination of those that do apply to the TS-CSK system.

4.4.2 Ciphertext-only attack: RM and RTM are ciphertext-only attacks. An encryption method is entirely insecure if vulnerable to this type of attack [18]. The PM TS-CSK and CSK systems are vulnerable to RTM and RM attacks. Other ciphertext-only attacks

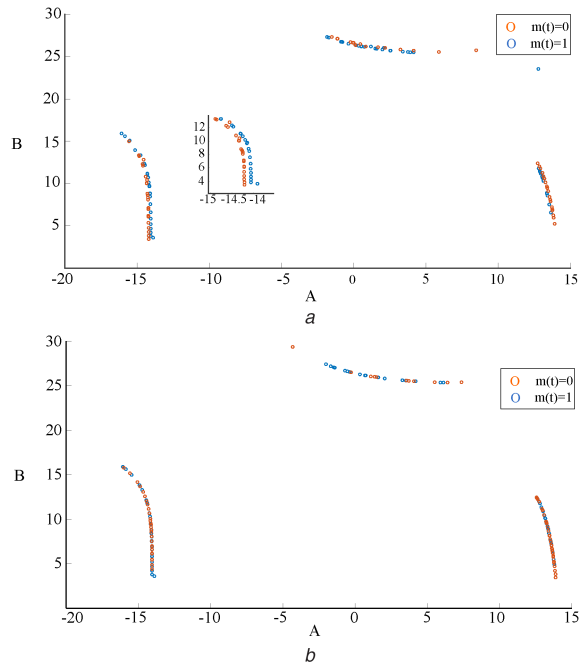


Fig. 12 *Simulink simulation of system RMs*
(a) CSK system simulink, ***(b)*** TS-CSK system simulink

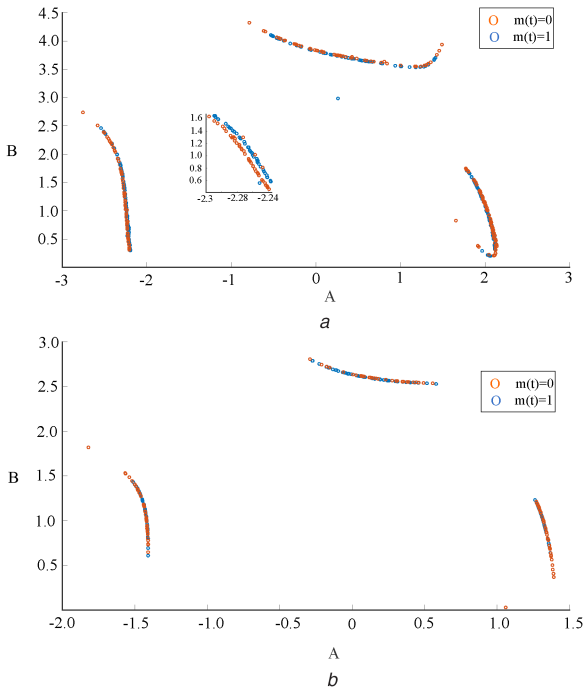


Fig. 13 *SPICE simulation of implemented circuit RMs*
(a) CSK system SPICE, ***(b)*** TS-CSK system SPICE

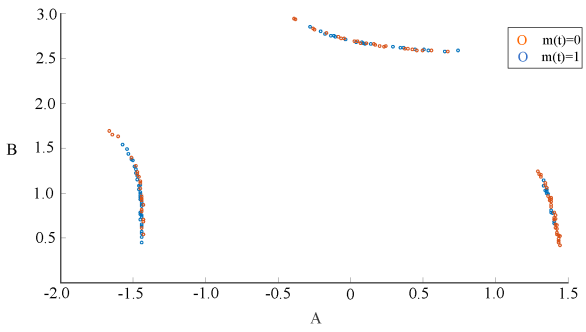


Fig. 14 *Experimentally derived RM of fabricated TS-CSK system*

attempt to determine from the transmitted state the foci point locations. The CSK system also falls to this type of attack [19]. Foci evaluation can only give a ratio function to the attacker [19]. $x_1(t)$ and $x_2(t)$ states are the only foci that can be determined from the two possible transmission states of the Lorenz system. Thus, the only relation that can be drawn from the determined c_i, x_C, is

$$x_C = \pm\sqrt{\rho(\beta-1)}\,. \tag{26}$$

This equation is very useful if either the ρ or β parameters change. However, the TS-CSK system does not show this characteristic. The potential possibilities for the key-space are reduced. However, $\lambda(x, m)$ is part of the key space. This partially mitigates the key space issues.

4.4.3 Known-plain-text and chosen-plain-text attacks: The developed discrete circuit components based CSK system is not vulnerable to the insertion of known plain text messages. Only the orbitals or orbital speed regimes for CSK and TS-CSK system are affected. Repeated cipher text applies when the initial conditions of the system can be guaranteed. This does not work for a realised network of discrete components without prior knowledge of how the Lorenz system was implemented. Furthermore, extremely accurate measurements of the state values are required.

4.4.4 Parameter sweeping: In the brute force attack approach to compromising the CSK or TS-CSK encryption, a receiver with the same system topology is created. With a sample of sweeping parameters of the cipher text, synchronisation can be achieved for a single instance. Similar to the RM and RTM attacks, the hidden bit change structure can be determined from the synchronisation. Thus, two unique possibilities can be determined. However, this assumes the key space is not too large and an accurately reproducible sample is achievable.

The TS-CSK has a larger key space and is secure against the RM attack. Sufficiently hidden switching events can remove vulnerability to the RTM attacks. The key space of the Lorenz system is increased by the parameters 0 and 1. The size of the key space is

k_L = the available key space of the Lorenz system
k_S = the available key space of the time scaling system
k_T = the number of decision engines immune to TS and TS-CSK

$$k_{FULL} = k_L k_S k_T\,.$$

Bit extraction will still be successful if k_L has a range of possibilities for each key that will still allow synchronisation to occur. k_L will be finite if the synchronisation has a maximum speed and a range of values exist for which the circuit can sufficiently operate. k_S is limited by the system's bandwidth response and power spectral density spread. k_T is limited by methodologies that lead to RTM immunity. It is also limited by methods which require a practical implementation method.

5 Real world implementation considerations

The TS-CSK system developed in this work is promising for successfully encrypting current real world communication systems. However, there are a number of practical considerations before the system can be deployed. These issues include the method by which the bits are extracted, the signal to noise ratio, and causes of error in synchronisation. Thus, a number of enhancements and optimisations need to be made to the system.

5.1 Synchronisation improvement

The sender/receiver systems realised using discrete analogue circuits could be improved to enhance synchronisation. This would significantly increase the encryption applications where the TS-CSK system could be used. There are a number of areas where the

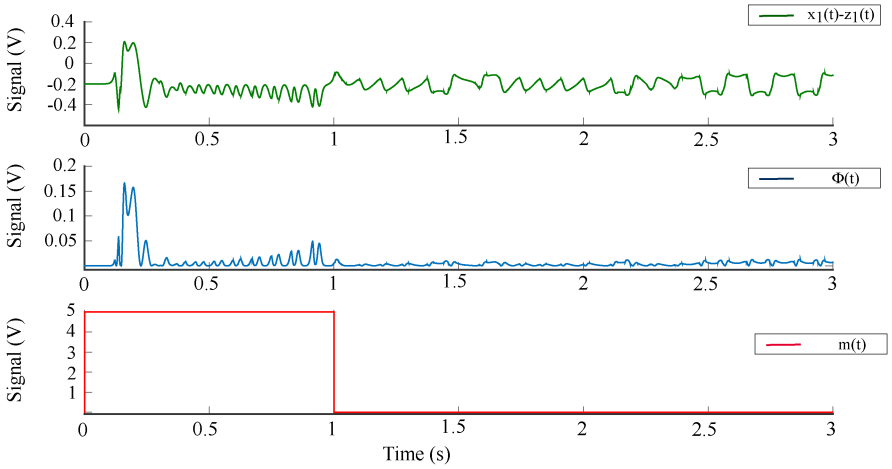


Fig. 15 *Effect of noise and parameter (resistor, capacitor values) mismatch on the signals*

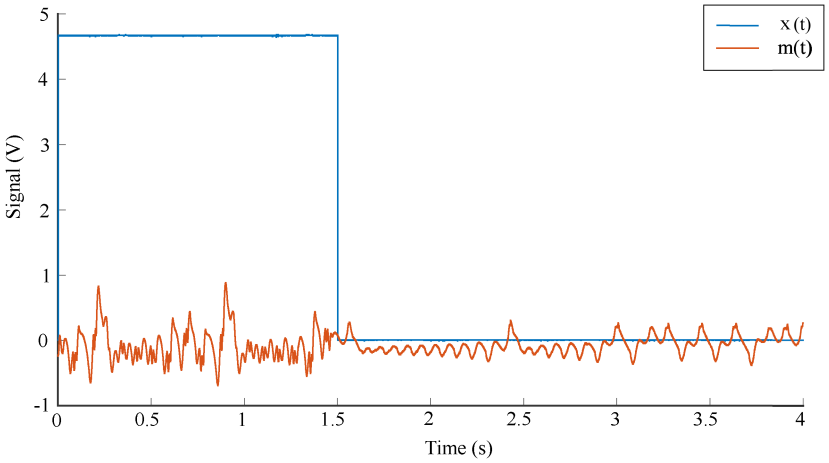


Fig. 16 *Synchronisation error as a function of the scaled message, m(t), of the eight-section TS-CSK system*

system could be further optimised. These include the implementation of the analogue circuits, the methodology used for extracting the bits, and the methods used for switching decisions.

5.2 Improvements in the analogue realisation

Future work can include a number of enhancements to the analogue realisation of the TS-CSK system. Mismatch in the voltages used as references caused a mismatch in synchronisation. An improved voltage source with greater resolution and the ability to be tuned would give increased accuracy and closer matching between the mirrored switching reference points. The addition of the ability to be tuned will add further control over any differences due to the mismatch in the device or experimental environmental differences that can occur in real applications.

The effect of inherent noise sources of the system can also be reduced. The realised circuits, both the dynamic system and the decision engine, are implemented on a PCB. The implemented PCB has ground planes to provide some noise immunity. However, there are interconnections between boards which utilised breadboards. Breadboards are notoriously noisy and not as robust as PCBs or integrated circuits. Thus, a PCB using sockets with lowered parasitics can be used for providing the power and measurement connections. The power supply used in this work is a computer power supply, which does not conform to the low noise, low ripple requirements of the system. A custom power supply on PCB would mitigate much of the uncertainty with using a commercial computer power supply.

Table 1 BERs

	Simulation	Experimental (P&M)	Experimental (eight-state)
high misses	0	0	38
high bits	47,964	9658	6234
low misses	0	16	0
low bits	52,036	10,342	6726
total misses	0	16	38
total bits	10,000	000	12,960
miss rate	$< 1 \times 10^{-5}$	$< 8 \times 10^{-4}$	$< 8 \times 10^{-3}$

5.3 Bit extraction

This work uses a simple periodic averaging methodology to perform bit extraction. However, this methodology can be heavily influenced by the degree of noise and mismatch in synchronisation. Bit extraction becomes more challenging with decreasing difference between synchronous bits and non-synchronous bits. Peak detection, which averages all the maximum within an area that is above a predefined threshold can be more suitable for bit extraction. A running tally can provide an additional weighting factor and could be used for extraction from synchronisation signals such as that of Fig. 16.

Pattern recognition or machine learning algorithms could be used to develop alternative bit extraction methodologies. The use of these algorithms is limited by the fact that the intended technology application should not be heavily dependent on significant amounts of software processing. The error due to the synchronisation mismatch rather than a non-synchronous bit is an area of further improvement. Different sources of error may exhibit varying power spectral densities. Exploiting this possibility would imply using various filtering options, which could lead to more simplified bit extraction.

This work sought to limit the requirement of analogue-to-digital converter (ADC) devices due to the increased power budget and increased system size. Thus, we use a reduced BER switching

criterion rather than the simpler, but, reduced security two-state PM TS-CSK switching criteria. A potential enhancement to the system involves performing a linear adjustment function set to one or more states which are then compared with the ground reference (origin). Two decisions which do not rely on external voltage references and provides a four-region switching plane are

$$\alpha_0 = \begin{Bmatrix} 0 & x_2 \geq x_1 \\ 1 & x_2 < x_1 \end{Bmatrix}, \quad \alpha_1 = \begin{Bmatrix} 0 & x_2 \geq 0 \\ 1 & x_2 < 0 \end{Bmatrix}. \tag{27}$$

Comparing x_2 or x_1 with x_3, (27) could further be expanded in some manner to double the number of generated regions. Additionally, these regions would not need external references.

6 Conclusion

In this study, the theory underlying an RM immune chaotic stream cipher based on a Lorenz system is presented and realised in a fabricated PCB using discrete circuit components. All component choices can function using a ±12 V DC power supply and consume a minimal amount of processing power to obtain the cipher text. The power consumption is several orders of magnitude lower than the power consumption required by a microprocessor to implement a standard digital encryption technique. This work has shown that while the simulation results show proper synchronisation of the eight-section TS-CSK system, the actual circuits depend on voltage references for the decision engine and as such may not provide adequate results. Thus, future research paths include using an ADC switching scheme relying on a likewise mismatched voltage source pair, further investigation of Frequency Modulation broadcast capability in both an analogue form and a Digital Signal Processing processed digital form, and adjusting components, such as the capacitor, sizes and matching to increase speed and accuracy.

7 Acknowledgments

The authors would like to thank Md. Sakib Hasan from the University of Tennessee, Knoxville for insightful and helpful discussions.

8 References

[1] Pincock, S.: '*Codebreaker: the history of codes and ciphers*' (Walker & Company, New York City, USA, 2006)

[2] Rivest, R.L., Shamir, A., Adleman, L.: 'A method for obtaining digital signatures and public-key cryptosystems', *Commun. ACM*, 1978, **21**, (2), pp. 120–126

[3] Daemen, J., Rijmen, V.: '*The design of Rijndael: AES-the advanced encryption standard*' (Springer Science & Business Media, Berlin, Germany, 2013)

[4] Makris, G., Antoniou, I.: 'Cryptography with chaos'. Proc. 5th Chaotic Modeling and Simulation Int. Conf., Athens, Greece, 2012, pp. 12–15

[5] Liu, J.M., Tsimring, L.S.: '*Digital communications using chaos and nonlinear dynamics*' (Springer Science & Business Media, Berlin, Germany, 2006)

[6] Lu, J., Wu, X., Lü, J.: 'Synchronization of a unified chaotic system and the application in secure communication', *Phys. Lett. A*, 2002, **305**, (6), pp. 365–370

[7] Brown, D.: 'A practical realization of a return map immune Lorenz based chaotic stream cipher in circuitry'. MS thesis, University of Tennessee, 2017

[8] Pecora, L.M., Carroll, T.L.: 'Synchronization of chaotic systems', *Chaos: Interdiscip. J. Nonlinear Sci.*, 2015, **25**, (9), p. 097611

[9] Oppenheim, A.V., Wornell, G.W., Isabelle, S.H., *et al.*: 'Signal processing in the context of chaotic signals'. 1992 IEEE Int. Conf. on Acoustics, Speech, and Signal Processing (ICASSP-92), Physical review letters, vol. 4, 1992, pp. 117–120

[10] Cuomo, K.M., Oppenheim, A.V.: 'Circuit implementation of synchronized chaos with applications to communications', *Phys. Rev. Lett.*, 1993, **71**, (1), p. 65

[11] Dedieu, H., Kennedy, M.P., Hasler, M.: 'Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits', *IEEE Trans. Circuits Syst. II, Analog Digit. Signal Process.*, 1993, **40**, (10), pp. 634–642

[12] Materassi, D., Basso, M.: 'Time scaling of chaotic systems: application to secure communications', *Int. J. Bifurcation Chaos*, 2008, **18**, (02), pp. 567–575

[13] Pérez, G., Cerdeira, H.A.: 'Extracting messages masked by chaos', *Phys. Rev. Lett.*, 1995, **74**, (11), p. 1970

[14] Yang, T., Yang, L.B., Yang, C.M.: 'Cryptanalyzing chaotic secure communications using return maps', *Phys. Lett. A*, 1998, **245**, (6), pp. 495–510

[15] Candaten, M., Rinaldi, S.: 'Peak-to-peak dynamics: a critical survey', *Int. J. Bifurcation Chaos*, 2000, **10**, (08), pp. 1805–1819

[16] Sampei, M., Furuta, K.: 'On time scaling for nonlinear systems: application to linearization', *IEEE Trans. Autom. Control*, 1986, **31**, (5), pp. 459–462

[17] Meraki: 'Wireless fundamentals: signal-to-noise ratio (SNR) and wireless signal strength'. Available at https://documentationmerakicom, accessed July 2018

[18] Menezes, A.J., Van Oorschot, P.C., Vanstone, S.A.: '*Handbook of applied cryptography*' (CRC Press, Florida, United States, 1996)

[19] Orue, A.B., Fernandez, V., Alvarez, G., *et al.*: 'Determination of the parameters for a Lorenz system and application to break the security of two-channel chaotic cryptosystems', *Phys. Lett. A*, 2008, **372**, (34), pp. 5588–5592