*Annals of Emerging Technologies in Computing (AETiC)*
*Vol. 9, No. 4, 2025*

*Research Article*

# CSK Modulation for Secure Wireless Communication Networks

**Rana H. A. Zubo[1], Walid A. Al-Hussaibi[2] and Raed Abd-Alhameed[3,4]***

[1]Northern Technical University, Iraq
r.h.a.zubo@ntu.edu.iq
[2]Southern Technical University, Iraq
alhussaibi@stu.edu.iq
[3]University of Bradford, United Kingdom
r.a.a.abd@bradford.ac.uk
[4]Al-Farqadein University College, Iraq
r.a.a.abd@bradford.ac.uk
*Correspondence: r.a.a.abd@bradford.ac.uk

Received: 23 August 2025; Accepted: 25 September 2025; Published: 1 October 2025

**Abstract: Physical layer security (PLS) has been considered as a key technology to fulfill the information confidentiality request of modern and future communication networks. Therefore, diverse chaos-based wireless communication (CBWC) systems have been developed as low complexity and cost-effective PLS approaches when compared with the upper layer secrecy protocols. In particular, chaos-shift-keying (CSK) modulation schemes have attracted significant research efforts owing to the simple signal generation techniques and enhanced secrecy. However, the practical implementation of CSK for secure data transmission over realistic CBWC channels still needs further investigation. In this paper, the application of CSK based on multiple chaotic basis functions is examined over a band-limited CBWC channel with Rayleigh fading process. Lorenz and Chua chaotic oscillator circuits are used as basis signal functions for CSK modulation at the transmit side and chaos demodulation/synchronization at the receiver end. The impact of channel bandwidth and requisites of the front-end receiver is modeled as a low pass filter process. Performance results show that chaos filtering can greatly affects the physical features of employed signals at different levels. The achieved results confirmed that inadequate filter bandwidth can remarkably distort the state-space, signature waveform, and spectral components of CSK signals in disparate extents regardless of high SNR level. For target error rate and worst-case eavesdropping secrecy, this issue has a direct impact on decreasing the error security gap of CBWC system compared with the reference CSK schemes based on a single chaotic base function, even at a high received signal-to-noise ratio. As a feasible solution to mitigate the degradation in system reliability and secrecy, it is demonstrated that the designed filter bandwidth must include the effective spectral components of utilized chaotic signals.**

**Keywords:** ***Chaotic circuits; chaotic communications; CSK; error security gap; physical layer security; wireless channels***

---

## 1. Introduction

In the last three decades and owing to the increasing demand for covert wireless services, massive research efforts and laboratory tests have been conducted on various chaos-based wireless communication (CBWC) systems for cost-effective secure data transmission [1-6]. The achieved physical layer security (PLS) in these approaches is typically based on the prominent characteristics of chaotic signals such as the noise-like spectrum, immunity to interference, and high sensitivity to initial state conditions (ISCs). The latter feature represents the main PLS advantage of employing chaotic signals rather than other existing approaches based on artificial noise or jamming signals, which are very susceptible to brute-force attacks and consumes additional power resource. Besides, it enables effective employment of chaotic secret keys at

Rana H. A. Zubo, Walid A. Al-Hussaibi and Raed Abd-Alhameed, "CSK Modulation for Secure Wireless Communication Networks", *Annals of Emerging Technologies in Computing (AETiC)*, Print ISSN: 2516-0281, Online ISSN: 2516-029X, pp. 31-41, Vol. 9, No. 4, 1 October 2025, Published by International Association for Educators and Researchers (IAER), DOI: 10.33166/AETiC.2025.04.003, Available: http://aetic.theiaer.org/archive/v9/v9n4/p3.html.

the physical layer with massive key-space to mitigate the eavesdropper's exhaustive search efforts [7-9]. On the other hand, when compared with the chaos-based PLS techniques, the conventional cryptographic-based upper layer secrecy (ULS) protocols exhibit much higher complexity and implementation cost due to vast signal processing necessities associated with high power resource depletion. Moreover, the application of ULS techniques in covert wireless communications involves huge cryptographic key generation and associated management tasks at the upper layers leading to undesired transmission link delay [2, 8, 10, 11].

For CBWCs, numerous chaos-shift-keying (CSK) modulation schemes have been designed for coherent communications to achieve the promised gains in single-user [4-5, 12-16] and multiuser scenarios [2, 17-18]. Furthermore, differential CSK (DCSK) modulation techniques are also investigated for non-coherent communication systems with reasonable performance loss by exploiting the observed features of received chaotic signals [1, 19-20]. These methods are either based on multiple chaotic basis functions [2, 19] or single chaotic system with different bifurcation parameters and/or ISCs [4, 7, 13-18]. However, simple transmission environments such as additive white Gaussian noise (AWGN) [15-16, 18-20] and static/quasi-static fading channels [13-14] are considered in the majority of presented works leading to exaggerated performance results. Therefore, valuable research efforts have considered the application of CSK/DCSK over more realistic communication channel conditions of Rayleigh fading [4, 12] for covert non-orthogonal multiple access (NOMA) systems [5, 10] and enhanced with intelligent reflecting surface techniques [1, 11]. Furthermore, composite Rician fading channel scenarios with large-scale path loss have been assumed for chaos-based secure NOMA systems in [2], [7] and 17]. However, CBWCs over band-limited channel is shown to introduce critical challenges due to low pass filter (LPF) effects from the considered transmission environment and receiver front-end requisites to boost the signal-to-noise-ratio (SNR). For instance, point-to-point CBWC systems based on single chaotic attractor have been investigated in [4, 12] to demonstrate the achieved performance results over band-limited channel of LPF process. It has been shown that inadequate filter bandwidth may cause large distortion in the state-space of chaotic attractor dynamics, alteration in the effective signal bandwidth and amplitude, high synchronisation error in coherent schemes, and noticeable degradation in error probability [4, 12]. However, the feasibility of generalized CSK based on multiple chaotic basis functions in band-limited CBWCs has not evaluated yet.

In the literature, different information-theoretic-based metrics have been used for the PLS assessment like secrecy rate, capacity, throughput, and outage probability [8-9, 11]. However, these metrics are hard to be measured in practical scenarios of non-Gaussian codes with finite lengths like chaotic codes/sequences. Therefore, the bit-error-rate (BER) performance has been considered as an important PLS measure for practical covert communication systems [13-14, 17-20]. It has been typically utilized to demonstrate the error security gap between legitimate and eavesdropping receivers, where reliable and covert communication link is achieved for larger BER gap [2, 7, 9-10]. Obviously, the error security gap can be associated with the secrecy capacity since the eavesdropper cannot extract any information (i.e. perfect secrecy) from the intercepted message when the BER performance approaches 0.5 [8].

In this paper, the practical feasibility of coherent CSK for point-to-point CBWC over band-limited Rayleigh fading channel is examined. A LPF model is considered to demonstrate the impact of limited channel bandwidth and front-end receiver filtering. The main contributions of presented work are highlighted as follows:

- A generalized CSK scheme with multiple chaotic basis functions, Lorenz chaotic system (LCS) and double-scroll chaotic system (DSCS), is considered for CBWC rather than the simple case of single analytical chaotic model in [4] and [12]. The employed signals from LCS and DSCS with different spectral characteristics and ultra-high key-space are utilized for CSK modulation at the transmit side and chaos demodulation/synchronization at the receiver end.
- The achieved outcomes reveal that insufficient bandwidth of the overall LPF process is responsible for destroying the important characteristics of utilized chaotic basis signals in varied levels. For target error rate and worst-case secrecy of unauthorized receiver with full system knowledge except the secret key (i.e. ISCs), this problem leads to decrease the error security gap of CBWC system compared with the reference binary CSK (BCSK) [2, 4] and multi-level CSK (MCSK) [7, 17] schemes that employ single chaotic function.
- As a feasible solution to mitigate the degradation in system reliability and secrecy, it is demonstrated that the designed filter bandwidth must include the effective spectral components

of utilized chaotic signals. This practical approach may lead to extend the state-of-the-art for future covert CBWCs.

## 2. System Design of CBWC

This A point-to-point (single-user) coherent CSK-based CBWC system over band-limited Rayleigh fading channel $h(t)$ with additive white Gaussian noise (AWGN) $n(t)$ is considered as shown in Fig. 1. The adopted basic covert system with chaos-based PLS is used to provide key benchmark performances for other coherent/non-coherent single-user/multiuser CBWC scenarios that employ CSK signalling of multiple basis functions. At the transmitter side, equiprobable digital data sequence $b(k)$ is modulated using CSK of chaotic basis functions from LCS and DSCS units as $s(t)$. The received signal $r(t)$ is filtered at the at the receiver end using LPF circuit as $r_f(t)$, and utilized then for signal demodulation as $\hat{s}(t)$ with the aid of channel estimation part and synchronised LCS and DSCS units. The estimated data form demodulated signal can be found at the receiver output as $\hat{b}(k)$. Descriptions of the employed LCS, DSCS, and LPF units in the designed CBWC system are presented below.

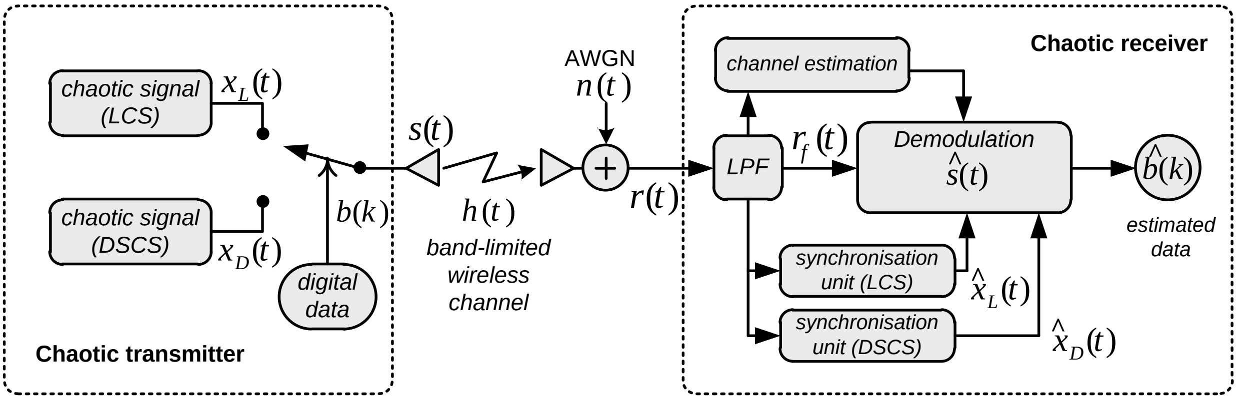


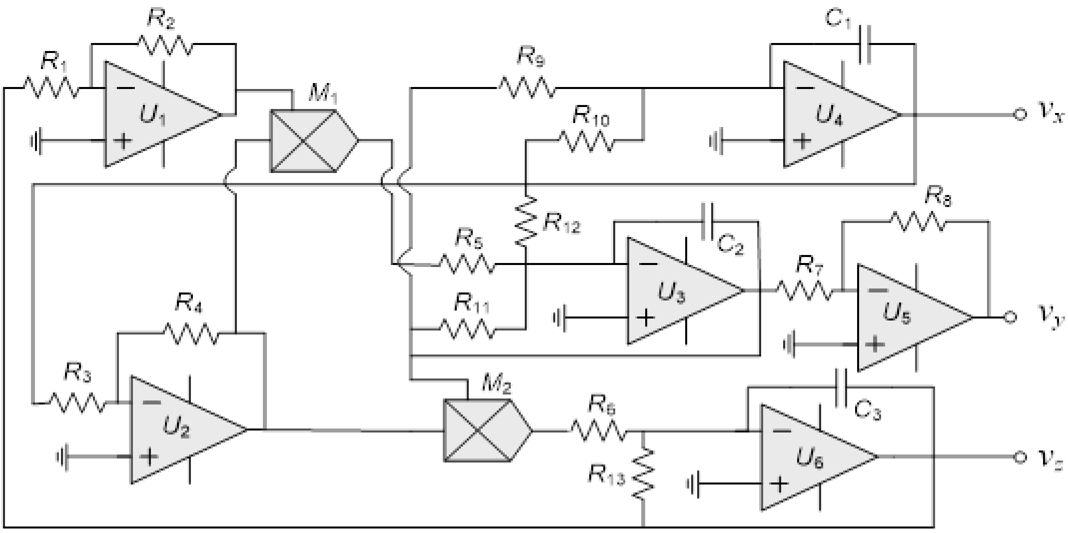

**Figure 1.** System design of secure CSK-based CBWC over band-limited Rayleigh fading channel

### 2.1. LCS Unit

The chaotic behaviour of nonlinear LCS dynamics can be described mathematically by the following three-dimensional ordinary differential equations [2, 9]:

$$\begin{cases} dv_x/dt = \sigma(v_y - v_x) \\ dv_y/dt = rv_x - v_y - v_x v_z \\ dv_z/dt = v_x v_y - m v_z \end{cases} \quad (1)$$

where $v_x$, $v_y$, and $v_z$ denote the states of LCS with chaotic attractor parameters $\sigma = 10$, $m = 2.66$, and $r = 28$. The sensitivity of this chaotic system to the utilized ISCs $\{v_{x_0}, v_{y_0}, v_{z_0}\}$ is significantly high as $\{10^{-18}, 10^{-15}, 10^{-18}\}$ allowing secrecy key-space of order $\mathcal{O}(10^{51})$ [2].




`**Figure 2.** Schematic diagram of LCS circuit with the generated dynamical states as $v_x$, $v_y$, and $v_z$

Circuit realization of scaled versions of LCS equations have been implemented using passive components (resistors) and active devices (operational amplifiers and multipliers) to perform the linear/nonlinear mathematical operations such as summations, subtractions, integrations, and multiplications [21-23]. In this research work, a Lorenz oscillator circuit is designed to generate the chaotic dynamical states of LCS in (1) as shown in Fig. 2. The electronic circuit is implemented using six operational amplifiers (Op-Amps: $U_1 - U_6$), two multipliers ($M_1, M_2$), thirteen resistors ($R_1 - R_{13}$), three capacitors ($C_1 - C_3$), and ∓15 V biasing voltage source. The generated chaotic voltage signal $v_x$ is used to characterize $x_L(t)$ in the considered CBWC system. Table 1 summarizes the passive component values and types of utilized active devices.

**Table 1.** Summary of the adopted values and types of the utilized components for LCS circuit

| Component Name | Value/Type |
|---|---|
| $R_1 - R_8$ | 10 kΩ |
| $R_9, R_{10}$ | 100 kΩ |
| $R_{11}$ | 1 MΩ |
| $R_{12}$ | 35.7 kΩ |
| $R_{13}$ | 374 kΩ |
| $C_1 - C_3$ | 2 µF |
| Op-Amps: $U_1 - U_6$ | µA741 |
| Multipliers: $M_1$, $M_2$ | AD633 |

## 2.2. DSCS Unit

For the considered DSCS unit, the chaotic attractor of nonlinear dynamics can be represented through the following three-dimensional ordinary differential equations [4, 10]:

$$\begin{cases} dv_1/dt = [G(v_2 - v_1)/C_1] - [f(v_1)/C_1] \\ dv_2/dt = [G(v_1 - v_2)/C_2] + [i_L/C_2] \\ di_L/dt = -v_2/L \end{cases} \quad (2)$$

where $v_1$, $v_2$, and $i_L$ are the chaotic states of DSCS using $G = 0.7$, $C_1 = 1/9$, $C_2 = 1$, and $L = 1/7$. The nonlinear function $f(v_1) = m_0 v_1 + 0.5(m_1 - m_0)[|v_1 + B_P| - |v_1 - B_P|]$ can be found based on the parameters $m_0 = -0.5$, $m_1 = -0.8$, and $B_P = 1$. The achieved sensitivity of DSCS to ISCs $\{v_{1_0}, v_{2_0}, i_{L_0}\}$ is also considerably high as $10^{-16}$ for each chaotic state permitting confidentiality key-space of order $O(10^{48})$ [2].

In the literature, the DSCS can be realized using variants of Chua's circuit as in [15] and [24]. For the designed CBWC system, the schematic diagram of implemented DSCS with passive and active electronic components is shown in Fig. 3. It consists of an inductor $L$, a resistor $R = 1/G$, two capacitors ($C_1$ and $C_2$), and an equivalent circuit for the nonlinear function $f(v_1)$. The latter is configured from one Op-Amp ($U$), two general purpose diodes ($D_1$ and $D_2$), seven resistors ($R_1 - R_7$), and two DC bias voltages ($V_{\text{BIAS}} = \pm 15$V). The generated voltage signal $v_1$ is used to establish $x_D(t)$ in the considered CBWC system model (2). Table 2 presents the adopted values of utilized passive components and type of active device.

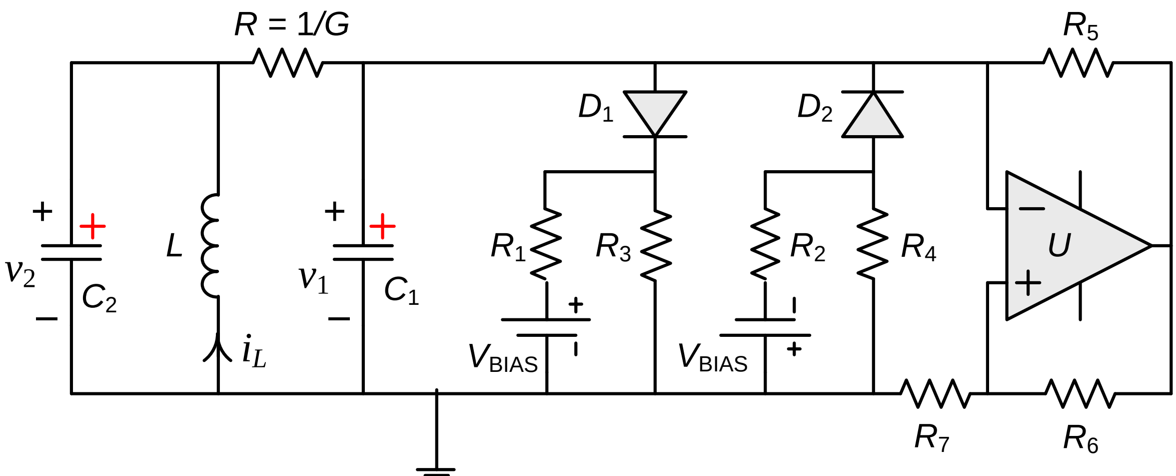



**Figure 3.** Schematic diagram of DSCS circuit with the generated dynamical states as $v_1$, $v_2$, and $i_L$

**Table 2.** Summary of the adopted values and types of the utilized components for DSCS circuit

| Component Name | Value/Type |
|---|---|
| $R = 1/G$ | 1.4 kΩ |
| $R_1$, $R_2$ | 46.2 kΩ |
| $R_3$, $R_4$ | 3.3 kΩ |
| $R_5$, $R_6$ | 0.3 kΩ |
| $R_7$ | 1.25 kΩ |
| $C_1$ | 5.5 nF |
| $C_2$ | 56 nF |
| $L$ | 8.2 mH |
| $D_1$, $D_2$ | 1N914 Silicon Diode |
| $D_1$, $D_2$ | 2 μF |
| Op-Amp: $U$ | μA741 |

### 2.3. LPF Unit

The filtering unit at the receiver is implemented using a single-pole LPF circuit with filter bandwidth (i.e. cut-off frequency) of $f_c = 1/2\pi R_f C_f$ as shown in shown in Fig. 4. This essential unit is used to improve the received SNR and enhance the signal detection process. Besides, it is used to demonstrate the filtering effects of band-limited Rayleigh fading channel [4, 10]. The schematic diagram of LPF circuit consists of a variable resistor $R_f$ used for $f_c$ tuning, two fixed resistors ($R_1$ and $R_2$), one filter capacitor $C_f$, and three Op-Amps ($U_1 - U_3$). The filter input signal $r(t)$ and output signal $r_f(t)$ are isolated from the filter section using two buffer circuits ($U_1$ and $U_2$). Table 3 summarizes the considered values of passive components and types of Op-Amp devices.

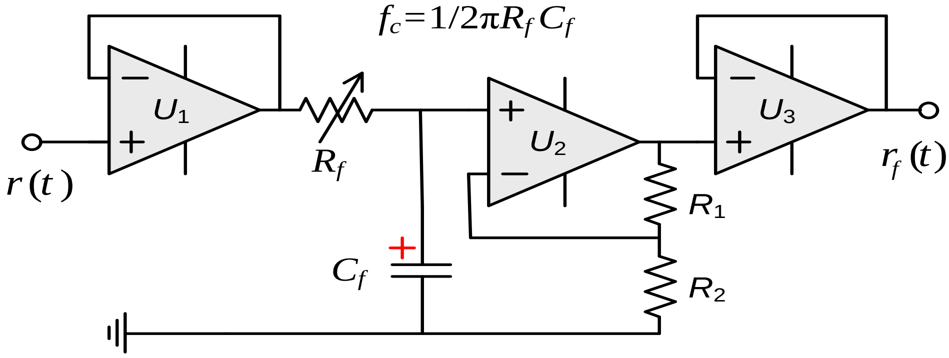



**Figure 4.** Schematic diagram of the employed single-pole LPF circuit of bandwidth $f_c$ for CBWC system

**Table 3.** Summary of the considered values and types of the utilized components for LPF circuit

| Component Name | Value/Type |
|---|---|
| $R_f$ | 10 kΩ |
| $C_f$ | 0.16 μF |
| $R_1$ | 0.58 kΩ |
| $R_2$ | 1 kΩ |
| Op-Amps: $U_1 - U_3$ | μA741 |

## 3. Signal Model of CBWC

The received signal model of designed CBWC system with PLS over fading channel $h(t)$ and AWGN $n(t)$ is given as

$$r(t) = h(t)\,\sqrt{\mathcal{P}}\,s(t) + n(t) \tag{3}$$

where $s(t)$ is the modulated chaotic signal (symbol) of time duration ($T$) and transmitted with average power $\mathcal{P}$. It modulated based on the digital data sequence $b(k)$ using BCSK of chaotic basis functions, $x_L(t)$ and $x_D(t)$, as

$$s(t) = \begin{cases} x_L(t)\,; & \text{for bit “1”} \\ x_D(t)\,; & \text{for bit “0”} \end{cases} \tag{4}$$

On the other hand, when MCSK is considered with four signalling levels (i.e. = 4 ), the modulated signal can be constructed form the utilized antipodal basis functions, $\pm x_L(t)$ and $\pm x_D(t)$, as follows

$$s(t) = \begin{cases} \{-x_L(t), -x_D(t)\}\,; & \text{for bits "00"} \\ \{-x_L(t), +x_D(t)\}\,; & \text{for bits "01"} \\ \{+x_L(t), -x_D(t)\}\,; & \text{for bits "10"} \\ \{+x_L(t), +x_D(t)\}\,; & \text{for bits "11"} \end{cases} \tag{5}$$

It should be noted that higher signalling levels ($M = 2^Q > 4$) can be implemented by employing $Q$ chaotic systems of different dynamical behaviours. For instance, MCSK with $M = 16$ can be configured using $Q = 4$ chaotic systems.

For the considered signal model, perfect channel estimation is assumed at the receiver for chaotic demodulation. Besides, LCS and DSCS units are used to provide synchronised basis functions $\hat{x}_L(t) \approx x_L(t)$ and $\hat{x}_D(t) \approx x_D(t)$ for associated correlators at the demodulator. Thus, the filtered chaotic signal $r_f(t)$ at the demodulator input is used for channel equalization through complex conjugate $h^*(t)$ as

$$\acute{r}_f(t) = h^*(t)\, r_f(t) \tag{6}$$

Estimated information data $\hat{b}(k)$ can be found then at the demodulator output using the correlator approach as presented in [3] and [19].

The achieved massive key-space of adopted CBWC system based on the sensitivity of LCS and DSCS to ISCs is of order $\mathcal{O}(10^{51} \times 10^{48} = 10^{2448}) \approx \mathcal{O}(2^{8132})$. In this case, the utilized secret keys enable ultra-robust PLS to resist the most powerful brute-force eavesdropping attacks of about $2^{100}$ computational efforts [2], [10].

### 4. Performance Evaluation and Results

Laboratory experiments based on MultiSim programming and numerical simulations using MATLAB are conducted on the designed CBWC system to show the actual performance of considered CSK schemes with ISCs of {0, 0, 0}. In the presented results, $v_x$ and $v_1$ chaotic states are derived from filtered received signal $r_f(t)$ whereas $v_z$ and $v_2$ are used from implemented LCS and DSCS units at the receiver, respectively. An average power of $\mathcal{P} = 1$ is used for the transmitted BCSK and MCSK symbols. For the BER performance, a frame of 100 symbols is transmitted over each channel realization, and the achieved outcomes are averaged over $10^6$ channel samples.

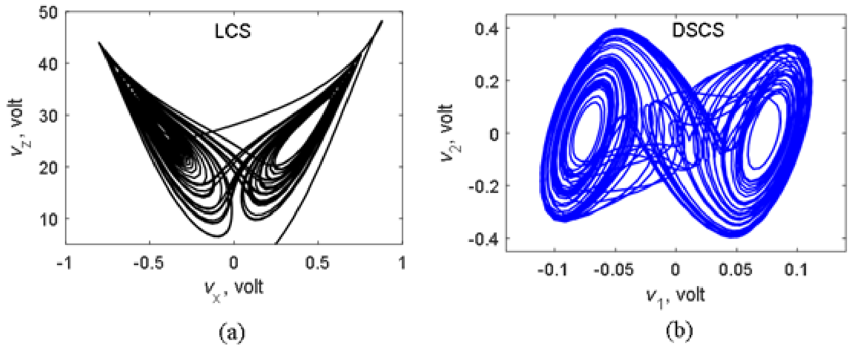



**Figure 5.** Performance of CBWC for $f_c = 10$ kHz and SNR = 35 dB: (a) Dynamical $[v_x, v_z]$ state-space of LCS; (b) Dynamical $[v_1, v_2]$ state-space of DSCS

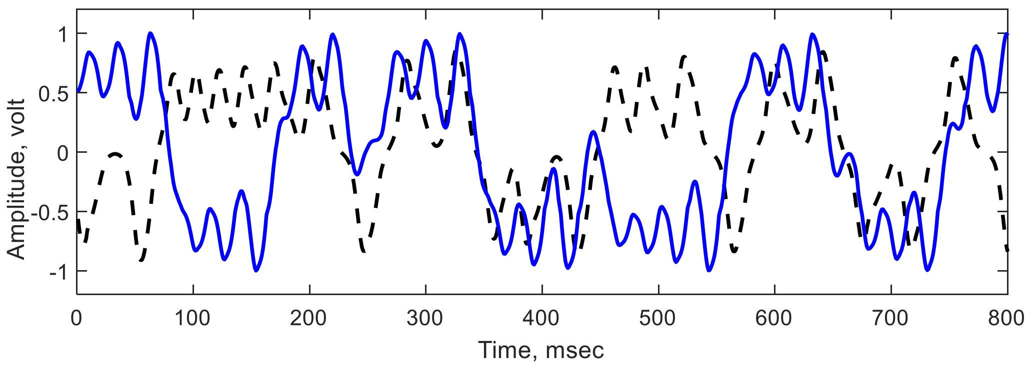



**Figure 6.** Time waveform of received chaotic signal $v_x$ from LCS compared with that of $v_1$ from DSCS. The considered CBWC system settings are $f_c = 10$ kHz and SNR = 35 dB

The realized performance of designed CBWC system is demonstrated in Figs. 5-7 for the case of $f_c$ = 10 kHz and SNR of 35 dB. In Fig. 5, it can be seen clearly that normal dynamical state-space is achieved for both LCS in the $[v_x, v_z]$ plane (Fig. 5 (*a*)) and DSCS in the $[v_1, v_2]$ plane (Fig. 5 (*b*)). Besides, undistorted received CSK signature waveforms (i.e. $v_x$ and $v_1$) are obtained in Fig. 6. This can be explained due to sufficient filter bandwidth that allows most of the effective spectral components of utilised chaotic basis signals to be exploited in CBWC system as illustrated in Fig. 7.

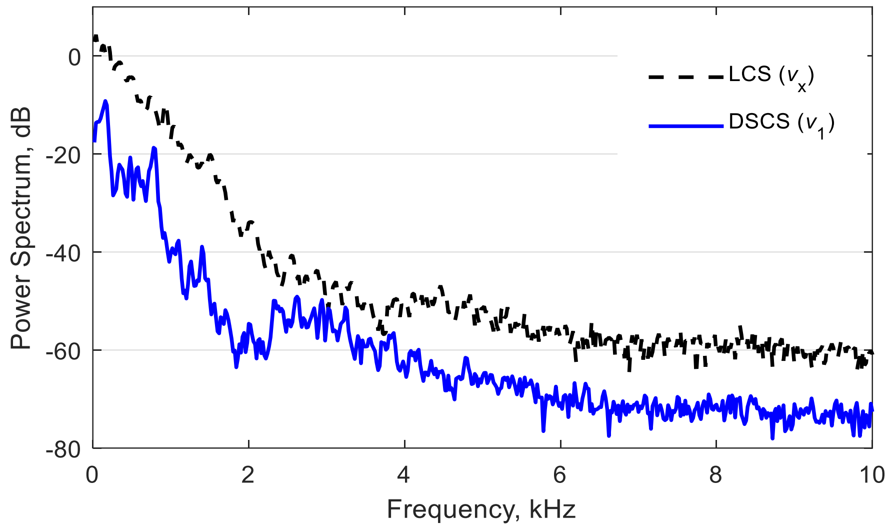



**Figure 7.** Power spectrum of received chaotic signal $v_x$ from LCS compared with that of $v_1$ from DSCS. The considered CBWC system settings are $f_c$ = 10 kHz and SNR = 35 dB

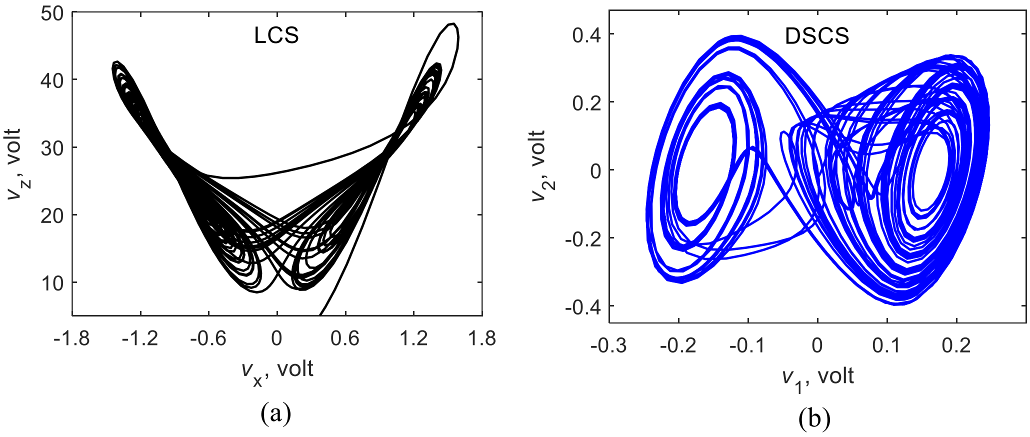



**Figure 8.** Performance of CBWC for $f_c$ = 2 kHz and SNR = 35 dB: (a) Dynamical $[v_x, v_z]$ state-space of LCS; (b) Dynamical $[v_1, v_2]$ state-space of DSCS

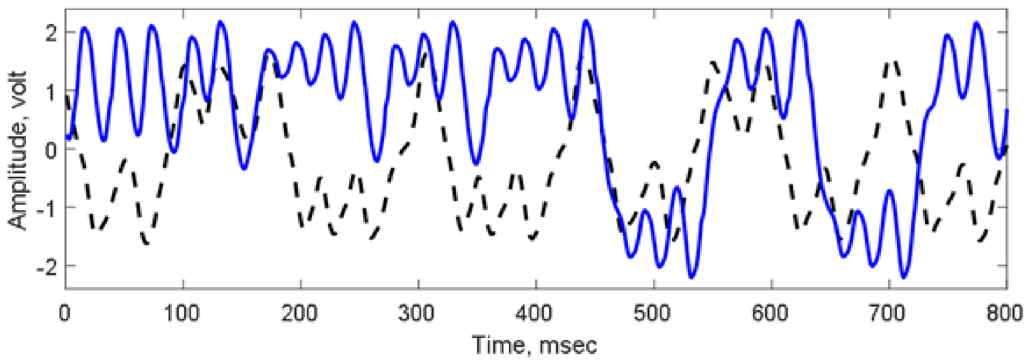



**Figure 9.** Time waveform of received chaotic signal $v_x$ from LCS (doted black line) compared with that of $v_1$ from DSCS (solid blue line). The considered CBWC system settings are $f_c$ = 2 kHz and SNR = 35 dB

On the other hand, and for the same SNR level of 35 dB, Figs. 8-10 show the obtained results for the case of LPF with $f_c$ = 2 kHz. As can be seen from Fig. 8, the dynamical state-space of LCS (Fig. 8 (*a*)) is more affected by the scarce filter bandwidth compared with that of DSCS (Fig. 8 (*b*)). The characteristics of chaotic signature waveforms in Fig. 9 are also altered in different levels since large portion of the spectral components are removed from the original transmitted signals as evident from Fig. 10. Without doubt, this high distortion on the main physical features of chaotic signals has critical impact on the essential chaos synchronisation at the receiver side of CBWC system. These important observations also coincide with those obtained in [4] and [12] where the synchronization error increased as $f_c$ decreased.

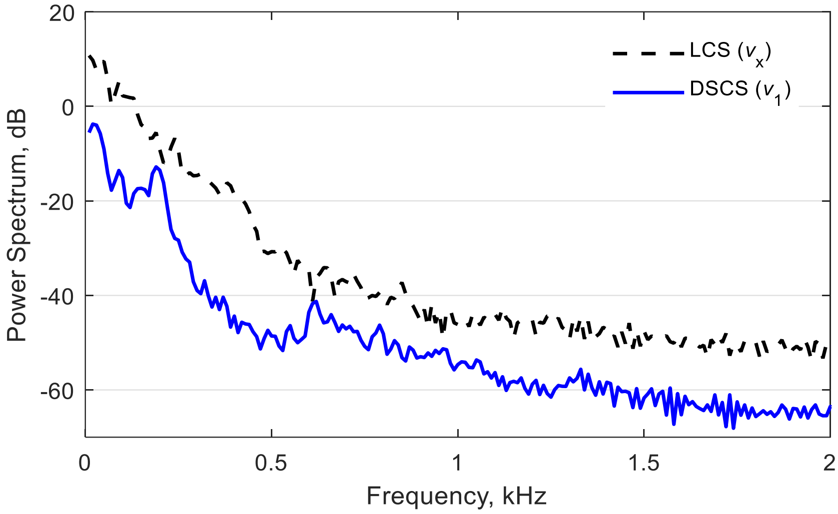



**Figure 10.** Power spectrum of received chaotic signal $v_x$ from LCS compared with that of $v_1$ from DSCS. The considered CBWC system settings are $f_c = 2$ kHz and SNR = 35 dB

In Fig. 11, the average BER performance of BCSK-based CBWC is shown as a function of $f_c$ compared with the reference BCSK that employs single chaotic function in [2] and [4] using high SNRs of 30 dB and 35 dB. It can be seen that the considered BCSK scheme of multiple chaotic basis systems performs lower than the reference BCSK over the considered range of $f_c$ and for both SNRs. Moreover, it shows higher error floor as the target BER decreases, since LCS is more sensitive to the filter process than DSCS, which affects the overall performance. For instance, when a minimum BER of $10^{-3}$ is required for target link reliability, the parameter $f_c$ for adopted BCSK with SNR of 30 dB should be more than 8.8 kHz to include most of the effective spectral components from both chaotic signals compared to 7.2 kHz for the reference scheme.

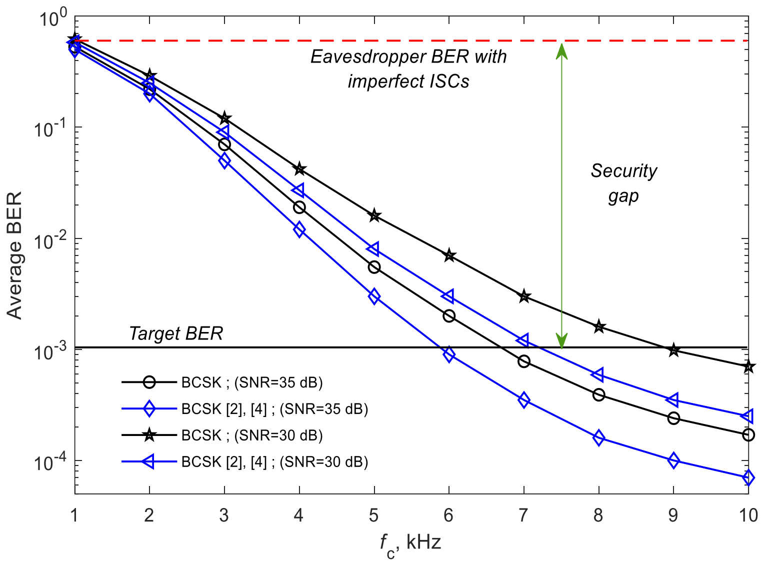



**Figure 11.** Average BER performance of BCSK-based CBWC as a function of $f_c$ in kHz compared with the reference scheme for SNRs of 30 and 35 dB

For BER-based security gap evaluation, Fig. 11 also shows the BER performance of identical eavesdropping receiver to that utilized for intended device except minor mismatch in ISCs (secret keys) of more than $10^{-15}$ (i.e. worst-case secrecy case). The serious error floor of eavesdropper (~0.5 ) demonstrates the ultra-high robustness of PLS in designed CBWC system with key-space of $O(2^{8132})$ against brute-force attacks. Considering target system BER of $10^{-3}$, it is shown that the BER security gap has direct relation with the LPF bandwidth. For instance, the realized BER results of proposed BCSK demonstrate sufficient security gap when $f_c > 6.7$ kHz and $f_c > 8.8$ kHz for SNR of 35 dB and 30 dB, respectively. Note that the reference BCSK schemes require lesser filter bandwidth to achieve same target BER as $f_c > 5.8$ kHz for 35 dB and $f_c > 7.2$ kHz for 30 dB, owing to the employment of single chaotic function. Therefore, the limited filter bandwidth has more impact on the error security gap of designed CBWC with multiple basis functions compared with reference schemes. Increasing the bandwidth of allocated channel and receiver filter may help to mitigate the obvious degradation in system error rate and BER security gap, but at cost of reduced channel capacity and increased noise level.

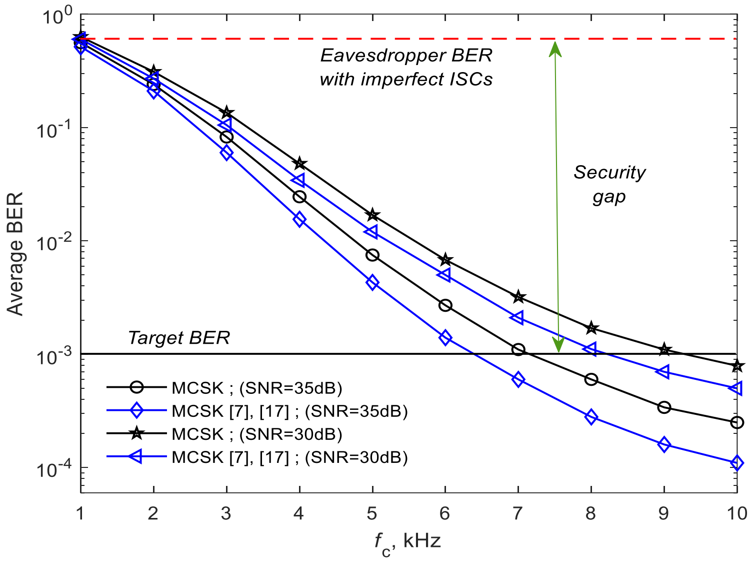



**Figure 12.** Average BER performance of MCSK-based CBWC as a function of $f_c$ in kHz compared with the reference scheme for SNRs of 30 and 35 dB

For the adopted MCSK-based CBWC system with $M = 4$, Fig. 12 shows the average BER performance as a function of $f_c$ compared with the reference MCSK that utilizes single chaotic function in [7] and [17]. As can be seen, the considered MCSK of multiple chaotic basis systems performs less than the reference scheme over the range of $f_c$ and for both SNRs (30 dB and 35 dB). Besides, it shows higher error floor as the target BER decreases due to the high sensitivity of LCS to LPF compared with DSCS. For target BER of $10^{-3}$, the filter bandwidth $f_c$ for SNR of 35 dB should be more than 7.1 kHz to contain the effective spectral components from both chaotic signals compared to 6.5 kHz for the considered reference. The BER of eavesdropper with minor mismatch in ISCs (more than $10^{-15}$ ) shows severe error floor ($\sim 0.5$ ) as expected due to the massive key-space of designed CBWC system. Considering target BER of $10^{-3}$, the achieved error performance of proposed MCSK reveal sufficient security gap when $f_c > 7.1$ kHz for SNR of 35 dB and $f_c > 9.4$ kHz for SNR of 30 dB. The reference schemes with single chaotic function require less LPF bandwidth to achieve the same target BER as $f_c > 6.5$ kHz for 35 dB and $f_c > 8.3$ kHz for 30 dB. Thus, inadequate filter bandwidth utilization will lead to undesired degradation in security gap of CBWC compared with reference schemes. The achieved results represent the lower bound BER for other MCSK schemes in PLS communications.

## 5. Conclusions

In this paper, the practical feasibility of CSK modulation schemes based on multiple chaotic basis functions has been addressed for CBWC with PLS over realistic fading channel. A single-pole LPF model is used to show the impact of both band-limited channel and receiver filtering processes on the system BER and security performance. The achieved results confirmed that inadequate filter bandwidth can remarkably distort the state-space, signature waveform, and spectral components of CSK signals in disparate extents regardless of high SNR level. For target BER and worst-case eavesdropping secrecy, this issue has the influence to reduce the error security gap of CBWC system compared with the reference CSK schemes based on a single chaotic base function. The BER outcomes demonstrated lower bound benchmarks for other CSK aided CBWCs, and highlighted the accurate selection approach of LPF bandwidth to include the effective chaos spectral components and mitigate the impact of filtering process. This may enhance the practical adoption and commercialisation of secure CBWC systems in private and public wireless applications.

### CRediT Author Contribution Statement

Rana H. A. Zubo: Conceptualization, Software and Methodology, Validation, Formal Analysis, Writing—Original Draft; Walid A. Al-Hussaibi: Software and Methodology, Validation, Writing—Review & Editing, Supervision; Raed Abd-Alhameed: Validation, Formal Analysis, Supervision, Project Administration, Funding Acquisition, Writing—Review & Editing.

### Acknowledgement

This work is partially supported by the Engineering and Physical Sciences Research Council (EPSRC), UK (Grant Project Number: EP/Y035135/1), and HORIZON-MSCA-2022-SE-01-01-ID: (Project Number: 101131501), Project titled: 6G Terahertz Communications for Future Heterogeneous Wireless Network (6G-TERAFIT).

### References

[1] Xiangming Cia, Chau Yuen, Chongwen Huang, Weikai Xu and Lin Wang, "Toward chaotic secure communications: An RIS enabled M-ary differential chaos shift keying system with block interleaving", *IEEE Transactions on Communications*, ISSN: 3541-3558, Vol. 71, No. 6, pp. 3541 – 3558, 29 March 2023, Published by IEEE, DOI: 10.1109/TCOMM.2023.3262834, Available: https://ieeexplore.ieee.org/document/10086558.

[2] Israa M Al-Musawi, Walid A. Al-Hussaibi and Falah H. Ali, "Efficient secure NOMA schemes based on chaotic physical layer security for wireless networks", *IEEE Open Journal of the Communications Society*, ISSN: 2644-125X, Vol. 3, No. 1, pp. 2425 – 2443, 6 December 2022, Published by IEEE, DOI: 10.1109/OJCOMS.2022.3226883, Available: https://ieeexplore.ieee.org/abstract/document/9971720.

[3] Georges Kaddoum, "Wireless chaos-based communication systems: A comprehensive survey", *IEEE Access*, ISSN: 2169-3536, Vol. 4, No.1, pp. 2621-2648, 25 May 2016, Published by IEEE, DOI: 10.1109/ACCESS.2016.2572730, Available: https://ieeexplore.ieee.org/abstract/document/7478568.

[4] Walid Al-Hussaibi, "Effect of filtering on the synchronization and performance of chaos-based secure communication over Rayleigh fading channel", *Communications in Nonlinear Science and Numerical Simulation*, Vol. 26, no. 1-3, pp. 87-97, September 2015, Published by Elsevier, DOI: 10.1016/j.cnsns.2015.02.010, Available: https://www.sciencedirect.com/science/article/abs/pii/S1007570415000532.

[5] Alireza Mard Shoorijeh and Mahmoud Ahmadian Attari, "Chaos-Based Physical Layer Security in NOMA Systems", in *Proceedings of the 32nd International Conference on Electrical Engineering (ICEE)*, 14-16 May 2024, Tehran, Iran, ISBN:979-8-3503-7634-0, pp. 1-7, Published by IEEE, DOI: 10.1109/ICEE63041.2024.10667801, Available: https://ieeexplore.ieee.org/abstract/document/10667801.

[6] Scott Hayes, Celso Grebogi and Edward Ott, "Communicating with chaos", *Physical Review Letters*, ISSN: 1079-7114, Vol. 70, No. 20, 17 May 1993, DOI: 10.1103/PhysRevLett.70.3031, Available: https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.70.3031.

[7] Israa Al-Musawi, Walid Al-Hussaibi and Falah Ali, "Chaos-based physical layer security in NOMA networks over Rician fading channels", in *Proceedings of the IEEE International Conference on Communications Workshops (ICC Workshops)*, Montreal, QC, Canada, 14-23 June 2021, ISBN: 2694-2941, Electronic ISSN: 2694-2941, pp. 1-6, Published by IEEE, DOI: 10.1109/ICCWorkshops50388.2021.9473862, Available: https://ieeexplore.ieee.org/abstract/document/9473862.

[8] Jehad M. Hamamreh, Haji M. Furqan and Huseyin Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey", *IEEE Communications Surveys & Tutorials*, ISSN: 1553-877X, Vol. 21, No. 2, pp. 1773-1828, 25 October 2018, Published by IEEE, DOI: 10.1109/COMST.2018.2878035, Available: https://ieeexplore.ieee.org/abstract/document/8509094.

[9] Yongpeng Wu, Ashish Khisti, Chengshan Xiao, Giuseppe Caire, Kai-Kit Wong *et al.*, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead", *IEEE Journal on Selected Areas in Communications*, ISSN: 0733-8716, Vol. 36, No. 4, pp. 679-695, 11 April 2018, Published by IEEE, DOI: 10.1109/JSAC.2018.2825560, Available: https://ieeexplore.ieee.org/abstract/document/8335290.

[10] Israa Almusawi, Walid Al-Hussaibi, Yassen Tahir and Falah Ali, "Chaos-based secure power-domain NOMA for wireless applications", In *Proceedings of the 2020 23rd International Symposium on Wireless Personal Multimedia Communications (WPMC)*, 19-26 October 2020, Okayama, Japan, ISBN:978-1-7281-8296-4, Published by IEEE, DOI: 10.1109/WPMC50192.2020.9309502, Available: https://ieeexplore.ieee.org/abstract/document/9309502.

[11] Lu Lv, Qingqing Wu, Zan Li, Zhiguo Ding, Naofal Al-Dhahir and Jian Chen, "Covert communication in intelligent reflecting surface-assisted NOMA systems: Design, analysis, and optimization", *IEEE Transactions on Wireless Communications*, ISSN: 1536-1276, Vol. 21, No. 3, pp. 1735-1750, 27 August 2021, Published by IEEE, DOI: 10.1109/TWC.2021.3106346, Available: https://ieeexplore.ieee.org/abstract/document/9524501.

[12] Walid Al-Hussaibi, Jaafar Alsmael and Mustafa Türkmen, "On the chaos synchronization in CBSC systems over realistic wireless channels", in *Proceedings of the 2019 16th International Multi-Conference on Systems, Signals & Devices (SSD)*, 21-24 March 2019, Istanbul, Turkey, ISBN:978-1-7281-1820-8, pp. 642-647, Published by IEEE, DOI: 10.1109/SSD.2019.8893267, Available: https://ieeexplore.ieee.org/abstract/document/8893267.

[13] Ebrahim Soujeri, Georges Kaddoum and Marijan Herceg, "Design of an initial condition-index chaos shift keying modulation", *Electronics Letters*, ISSN: 1350-911X, Vol. 54, No. 7 , pp. 447-449, 1 April 2018, Published by Wiley, DOI: 10.1049/el.2018.0119, Available: https://ietresearch.onlinelibrary.wiley.com/doi/full/10.1049/el.2018.0119.

[14] B. Jovic, "Chaos-based BPSK communication system", *Electronics Letters*, ISSN: 1350-911X, Vol. 51, No. 8, pp. 630-632, 1 April 2015, Published by Wiley, DOI: 10.1049/el.2015.0638, Available: https://ietresearch.onlinelibrary.wiley.com/doi/full/10.1049/el.2015.0638.

[15] J. Liu, , Y. X. Wu, J. H. Xiao and Y. H. Zhang, "Multi-state chaos-shift-keying modulation system using feedback synchronising Chua's circuit", *Electronics Letters*, ISSN: 1350-911X, Vol. 32, No. 8, pp. 714-715, 11 April 1996, Published by IET, DOI: 10.1049/el:19960485, Available: https://digital-library.theiet.org/doi/abs/10.1049/el%3A19960485.

[16] Herve Dedieu, Michael Peter Kennedy and Martin Hasler, "Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits", *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, ISSN: 1057-7130, Vol. 40, No. 10, pp. 634-642, 31 October 1993, Published by IEEE, DOI: 10.1109/82.246164, Available: https://ieeexplore.ieee.org/abstract/document/246164.

[17] Walid A. Al-Hussaibi, Israa M. Al-Musawi and Falah H. Ali, "Multi-level Chaos-Shift-Keying for Non-Orthogonal Multiple Access with Physical Layer Security", In *Proceedings of the 2nd International Multi-Disciplinary Conference Theme: Integrated Sciences and Technologies (IMDC-IST '21)*, Sakarya, Turkey, 7-9 September 2021, Published by EAI, DOI: 10.4108/eai.7-9-2021.2314409, Available: https://eudl.eu/doi/10.4108/eai.7-9-2021.2314409.

[18] W. M. Tam, F. C. M. Lau, Chi Kong Tse and M. M. Yip, "An approach to calculating the bit-error rate of a coherent chaos-shift-keying digital communication system under a noisy multiuser environment", *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, ISSN: 1057-7122, Vol. 49, No. 2, pp. 210-223, 28 February 2002, Published by IEEE, DOI: 10.1109/81.983868, Available: https://ieeexplore.ieee.org/abstract/document/983868.

[19] W. M. Tam, Francis CM Lau and Chi K. Tse, "Analysis of bit error rates for multiple access CSK and DCSK communication systems", *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, ISSN: 1057-7122, Vol. 50, No. 5, pp. 702-707, 31 May 2003, Published by IEEE, DOI: 10.1109/TCSI.2003.811018, Available: https://ieeexplore.ieee.org/abstract/document/1203833.

[20] F. C. M. Lau, M. M. Yip, Chi Kong Tse and S. F. Hau, "A multiple-access technique for differential chaos-shift keying", IEEE *Transactions on Circuits and Systems I: Fundamental Theory and Applications*, ISSN: 1057-7122, Vol. 49, No. 1, pp. 96-104, 31 January, 2002, Published by IEEE, DOI: 10.1109/81.974883, Available: https://ieeexplore.ieee.org/abstract/document/974883.

[21] Juan Liu, Xuefeng Cheng and Ping Zhou, "Circuit Implementation Synchronization between Two Modified Fractional-Order Lorenz Chaotic Systems via a Linear Resistor and Fractional-Order Capacitor in Parallel Coupling", *Mathematical Problems in Engineering*, ISSN:1563-5147, Vol. No. 1, pp. 1-8, 19 August 2021, Published by Wiley, DOI: 10.1155/2021/6771261, Available: https://onlinelibrary.wiley.com/doi/pdf/10.1155/2021/6771261.

*[22]* Jonathan N. Blakely, Michael B. Eskridge and Ned J. Corron, "A simple Lorenz circuit and its radio frequency implementation", *Chaos: An Interdisciplinary Journal of Nonlinear Science*, ISSN 1089-7682, Vol. 17, No. 2, June 2007, DOI: 10.1063/1.2723641, Available: https://pubs.aip.org/aip/cha/article-abstract/17/2/023112/934378/A-simple-Lorenz-circuit-and-its-radio-frequency.

[23] Kevin M. Cuomo and Alan V. Oppenheim, "Circuit implementation of synchronized chaos with applications to communications", *Physical Review Letters*, ISSN 1079-7114, Vol. 71, No. 1, p. 65, 5 July, 1993, Published by American Physical Society, DOI: 10.1103/PhysRevLett.71.65, Available: https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.71.65.

[24] L. Gámez-Guzmán, C. Cruz-Hernández, R. M. López-Gutiérrez and E. E. García-Guerrero, "Synchronization of Chua's circuits with multi-scroll attractors: application to communication", *Communications in Nonlinear Science and Numerical Simulation*, Vol. 14, No. 6, pp. 2765-2775, June 2009, Published by Elsevier, DOI: 10.1016/j.cnsns.2008.10.009, Available: https://www.sciencedirect.com/science/article/abs/pii/S1007570408003298.