Multi-level Chaos-Shift-Keying for Non-Orthogonal Multiple Access with Physical Layer Security

Walid A. Al-Hussaibi[1], Israa M. Al-Musawi[2], Falah H. Ali[3]
{alhussaibi@stu.edu.iq[1], israa.almusawii@gmail.com[2], f.h.ali@sussex.ac.uk[3]}
{[1,2]BETC, [1]BTI}, Southern Technical University, Basrah, Iraq
[3]Communications Research Group, University of Sussex, Brighton, UK

Abstract. To address the key issue of users' privacy in future wireless communications, this work presents a generalized uplink secure code-domain non-orthogonal multiple access (SCD-NOMA) based on multi-level chaos-shift-keying (MCSK) signalling over Rician propagation environment. To have cost-effective physical layer security (PLS), the proposed scheme is designed by employing chaotic drive systems at the users' side and a chaotic response system at the base station (BS) receiver. The transmitted signals are estimated efficiently at the BS through integrated maximum likelihood (ML) and chaos demodulation techniques. The efficacy of the proposed SCD-NOMA system is validated by intensive simulation results of the realized error rate, connectivity, and security gap, in comparison to the reference systems. Besides, the proposed scheme provides a huge key-space to increase the system's PLS and compact exhaustive brute-force attacks.

Keywords: code-domain NOMA; chaotic signals; physical layer security; CSK; wireless fading channels.

1 Introduction

The rapid advancement in modern technologies has initiated an incredible growth in the number of wirelessly connected devices worldwide. Therefore, new wireless networks like 5G and beyond are required to attain the critical issues of massive connectivity, reliability, security, and affordability [1]-[4]. In the same context, non-orthogonal multiple access (NOMA) is one of the attractive communication techniques that have been designed over the past years to achieve the next-generation targets by investing in power-domain NOMA (PD-NOMA) and code-domain NOMA (CD-NOMA). In such schemes, the connected users' performance outperforms the traditional orthogonal multiple access (OMA) schemes utilizing spectral efficiency and connectivity, however, at the cost of increased co-channel interference [5]-[7].

In wireless networks, the possibility of signal interception from unauthorized receivers is quite high owing to the open transmission nature [8]. Besides, the remarkable increase in the number of served users and related data traffic in the NOMA schemes may result in additional data security leakage [7]-[9]. Consequently, using the common security techniques based on cryptographic methods at the network upper layers becomes ineffective owing to cost, complexity, and power limitations [3], [4], [7]. Thus, physical layer security (PLS) emerges as a cost-effective alternative technique by utilizing the main channel features like noise, interference, diversity, and fading, to expand the realized security gap between the illegal and the legal receiver [8]-[10]. Moreover, PLS may be used jointly with other cryptography-based methods to further enhance the overall system security [4].

IMDC-IST 2021, September 07-09, Sakarya, Turkey

DOI 10.4108/eai.7-9-2021.2314409

In the literature, many PLS systems have been presented by exploiting the properties of the chaotic signal in chaos-based secure communication (CBSC) like its wideband spectrum, unpredictable operation performance, and its high sensitivity to the changes in initial conditions (ICs) [7], [9], [11]-[16]. Moreover, the parameters of the chaotic system can provide an enormous key-space that remarkably enhances the system security against eavesdroppers brute-force attacks [14]. For example, various CBSC systems based on NOMA approaches have been studied such as [9], [16] over Gaussian channels and [6], [12], [17] over fading channels with multiple-input multiple-output (MIMO) technique integrated with orthogonal frequency division multiplexing (OFDM) method [11].

The realized security gap based on the performance of bit-error-rate (BER) emerges as an efficient and practical PLS measure to evaluate the achieved PLS instead of the information theoretic-based measures such as the secrecy throughput, secrecy outage probability, and secrecy rate [3], [9]-[14], [18]. Secure communications may be achieved by expanding the realized gap between the BER performance of legal and illegitimate receivers [17]-[20]. Other important metrics are considered also like the key-space which is employed to assess the computational efforts required by an external eavesdropper to guess the secret keys correctly. Moreover, the key mismatch between the transmitter and the receiver shows the capability of the illegal receiver to correctly guess the secret keys using extensive search computations [7], [12]-[14].

The major contributions for this paper may be highlighted as follows:

1) A generalized uplink multiuser communications system design of secure CD-NOMA (SCD-NOMA) is presented over the environment of a realistic channel. Composite large-scale propagation and small-scale Rician fading are adopted rather than the simple Gaussian channel in [9] and [16] or the small-scale Rayleigh fading in [3], [12], and [17].
2) Multi-level chaos-shift-keying (MCSK) modulators and demodulators are used at the communication ends rather than the binary CSK in [3], [12], [16], and [17] to create an effective PLS with a large key-space advantage and higher spectral efficiency. At the receiving base station (BS), maximum likelihood (ML) and chaotic demodulation are used together for multiuser detection (MUD).
3) The realized results of the proposed SCD-NOMA are verified and compared with the reference schemes, by extensive simulations for security gap, BER, key-space metrics, and user connectivity. Moreover, the OMA gains like MIMO [8] and OFDM [11] are excluded to have a realistic performance evaluation. The realized results utilizing multiple system configurations, ICs, and chaotic sequence lengths, are attractive and show many valuable tradeoffs.

The rest of this paper is arranged as follows. In Section 2, a concise chaotic communications technical background is discussed. Section 3 shows the system design of the proposed SCD-NOMA. The designed system results and simulations are highlighted in Section 4, meanwhile, conclusions are presented in Section 5.

2 Chaotic Communications

Various modulation methods are used in CBSC such as the conventional CSK technique [12]. In this method, the involved chaotic signals can be generated from different mathematical models that reveal a nonlinear dynamical behaviour like the two-dimensional equations of the discrete-time Henon chaotic system (HCS) [6]:

$$x(n+1) = y(n) + 1 - ax^2(n)$$
$$y(n+1) = bx(n) \quad (1)$$

where n is the time instance for the chaotic attractor, $a = 1.4$, and $b = 0.3$. By using simple hardware electronic circuits or different software tools (e.g. MATLAB), the chaotic signals (x and y) of HCS can be found with high sensitivity to ICs ($\approx 10^{-15}$/state).

In CBSCs, the data can be encrypted and sent to the receiving end with high secrecy levels by using the attractive characteristics of chaotic signals. In this case, at the receiver side, it is hard to correctly decode the transmitted signals without previously knowing the parameters of the chaotic system such as the ICs, code length (β), chaotic sequence length ($\mathcal{L}$), number of chaotic states ($\mathcal{D}$), and modulation level (M). The integration of those parameters can form an essential robust key-space set $\mathcal{S} = \{\text{ICs}, \beta, \mathcal{L}, \mathcal{D}, M\}$. As a result, potential eavesdroppers using brute-force attacks will not be able to easily discover the transmitted signals owing to the need for exhaustive efforts of computations (more than 2^{100}) to scan and break the key-space $\mathcal{S}$ [13], [14]. Hence, effective PLS can be granted in CBSCs since only planned receivers with the exact system parameters are capable of decoding the transmitted data accurately.

3 System Design of SCD-NOMA

Consider a multiuser SCD-NOMA with MCSK modulation/demodulation as given in Fig. 1, in a single-cell cellular system. The proposed scheme consists of K single-antenna users communicating simultaneously with a single-antenna BS over a wireless fading propagation channel. For the MCSK units at the user's end and BS receiver, an accurate drive-response synchronization mechanism is assumed [15]. In addition, the BS is assumed to have complete channel state information (CSI) to perform efficient equal power control and MUD.

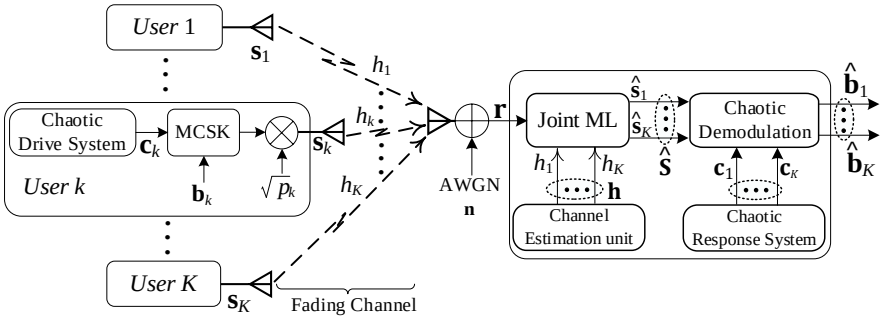

Fig. 1. General system design of SCD-NOMA over wireless fading channel environment.

3.1 Signal Model

For the considered SCD-NOMA scheme, the digital data symbol of user k is shown as $\mathbf{b}_k = [b_{k,1} \dots b_{k,U}]$ with $U = \log_2(M)$ binary bits. It has an alphabet set $\mathbf{B}_k = \left\{\mathbf{b}_k^{(1)}, \dots, \mathbf{b}_k^{(i)}, \dots, \mathbf{b}_k^{(M)}\right\}$

of size M, where $\mathbf{b}_k^{(i)} = \left[b_{k,1}^{(i)} \dots b_{k,U}^{(i)}\right]$ denotes the i^{th} possible data symbol. For each user k, a certain chaotic codebook is assigned as $\mathbf{C}_k = \left\{\mathbf{c}_k^{(1)}, \dots, \mathbf{c}_k^{(i)}, \dots, \mathbf{c}_k^{(M)}\right\}$, where $\mathbf{c}_k^{(i)} = \left[c_{k,1}^{(i)} \dots c_{k,\beta}^{(i)}\right]$ and $c_{k,j}^{(i)}$ is the j^{th} chip of i^{th} chaotic code of length $\beta \ll \mathcal{L}$. The active users utilize MCSK as $\mathbf{b}_k^{(i)} \rightarrow \mathbf{c}_k^{(i)}$ for $k = 1, \dots, K$ and $i = 1, \dots, M$. Throughout this work, is presumed that $T_{\mathbf{b}}$ the symbol duration is β times the chip duration T_c. Subsequently, user k transmitted signal is given with equal power allocation p_k as $\mathbf{s}_k = \left[s_{k,1} \dots s_{k,\beta}\right] \in \mathcal{R}^{1\times\beta}$ which represents one of the possible elements from the overall set $\mathbf{S}_k = \left\{\mathbf{s}_k^{(1)}, \dots, \mathbf{s}_k^{(i)}, \dots, \mathbf{s}_k^{(M)}\right\}$. The received composite signal at the BS $\mathbf{r} = \left[r_1 \dots r_\beta\right] \in \mathcal{C}^{1\times\beta}$ is modelled by

$$\mathbf{r} = \sum_{k=1}^{K} h_k \mathbf{s}_k + \mathbf{n} \tag{2}$$

where $\mathbf{n} = \left[n_1 \dots n_\beta\right] \in \mathcal{C}^{1\times\beta}$ stands for the vector of the AWGN with zero-mean and σ_n^2-variance coefficient, and h_k is the fading channel of user k given as [21],

$$h_k = \sqrt{\xi_k}\left[\sqrt{\frac{\mathcal{K}}{\mathcal{K}+1}}\,\bar{g}_k + \sqrt{\frac{1}{\mathcal{K}+1}}\,\breve{g}_k\right] \tag{3}$$

where $\bar{g}_k$ is a complex-valued line-of-site (LOS) coefficient, $\breve{g}_k$ is the scattered fading of zero-mean unit-variance elements and it is presumed to be fixed over the symbol duration $T_{\mathbf{b}}$, $\mathcal{K}$ is the Rician fading coefficient, and $\xi_k = \ell_k^{-\vartheta}$ stands for large-scale path loss, ℓ_k is the distance of user k from the BS, and ϑ denotes the path loss exponent.

3.2 Receiver Design

Signal estimation is carried out jointly at the BS using the optimal ML receiver and chaotic demodulator. For the considered MCSK, there is a set of $\Omega = M^K$ probable elements for transmitted signals as $\mathbb{S} = \left\{\mathbf{S}^{(1)}, \dots, \mathbf{S}^{(l)}, \dots, \mathbf{S}^{(\Omega)}\right\}$, where $\mathbf{S}^{(l)} = \left[\mathbf{s}_1^{(l)} \dots \mathbf{s}_k^{(l)} \dots \mathbf{s}_K^{(l)}\right]^{\mathrm{T}}$, and $\mathbf{s}_k^{(l)}$ is the l^{th} likely transmitted signal vector from user k. Therefore, MUD can be performed as

$$\hat{\mathbf{S}} = [\hat{\mathbf{s}}_1 \dots \hat{\mathbf{s}}_k \dots \hat{\mathbf{s}}_K]^{\mathrm{T}} = \arg\min_{\mathbf{S}^{(l)}\in\mathbb{S}} \left\|\mathbf{r} - \mathbf{h}\mathbf{S}^{(l)}\right\|^2 \tag{4}$$

where $\|.\|$ represents the Euclidean vector norm. The output of estimated signals can be sent then to the chaotic modulator to find the detected data as $\hat{\mathbf{b}}_k = \left[\hat{b}_{k,1} \dots \hat{b}_{k,U}\right]$ for $k = 1, \dots, K$.

4 Results and Security Evaluations

In this section, simulation experiments are accomplished to demonstrate the SCD-NOMA system performance by terms of the realized security gap, BER, and the users' connectivity for any considered OMA resource dimension. The effects of parameter β and mismatch of the secret keys on the BER performance are also studied. The Key-space analysis is shown to validate the SCD-NOMA improved resistance to fight the brute-force attacks from potential unauthorized receiver devices. The considered parameters for simulations are: cellular network radius of

300 m; $\vartheta = 4$; $K = 2, 3,$ and 4; $\mathcal{L} = 10^4$; $M = 4$; $\beta = 50$; and the ICs utilized in the chaotic drive/response systems are $\{x_0 = 0.0, y_0 = 0.0\}$. The legal BS employs perfect ICs meanwhile the illegitimate receiver device owns inaccurate secret keys (ICs) of 10^{-15} accuracy. The BER outcomes are compared for fairness with the reference system of quadrature phase-shift keying NOMA (QPSK-NOMA) and averaged over 10^6 channels.

4.1 BER Performance and Achieved Security Gap

In **Figure 2**, the BER curves of the 2-user scheme as a function of the signal-to-noise ratio (SNR) are given considering different Rician factors. The presented results of all scenarios show that the legal receiving end achieves a substantial performance gain for all connected users in comparison to the 2-user QPSK-NOMA reference owing to the extra code diversity. For example, at BER target of 10^{-5} the BERs of SCD-NOMA outperform the references by 21 dB, 27.5 dB, and 26 dB when $\mathcal{K} = 0$, $\mathcal{K}$ =4, and $\mathcal{K}$ =8, respectively. Moreover, it is clear that with the increase of $\mathcal{K}$ from $\mathcal{K} = 0$ to $\mathcal{K} = 8$, the attained security gap also significantly increases. It is noted that the unauthorized receiver BERs reveals an obvious error floor due to imperfect ICs.

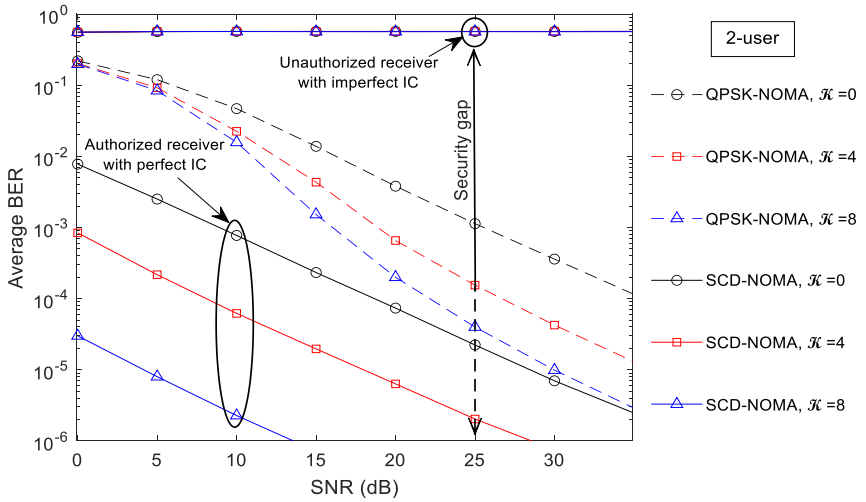

Fig. 2. Average BER of 2-user SCD-NOMA using $\beta = 50$ and different Rician factors of $\mathcal{K} = 0, \mathcal{K} = 4$, and $\mathcal{K} = 8$.

Figures 3 and **4** show the BERs of 3 and 4-user schemes, respectively as a function of SNR considering different Rician factors. The BERs of the authorized receiver for all Rician factor scenarios display a significant performance compared to the benchmark references over the entire SNR range. Moreover, the best performance among all considered scenarios with a remarkable security gap is noticed when $\mathcal{K} = 0$. The BERs of the illegal receiver for those cases also achieve an error floor over the whole range of SNR. A summary for the attained gains in dB is presented in **Table 1** considering target BER of 10^{-5}. As it can be seen the 4-user realizes a huge dB gain and for all Rician factors compared to the reference systems.

Table 1. SNR gain for the considered scenarios at target BER of 10^{-5} compared with the considered reference systems.

Rician Factor	2-user scenario	3-user scenario	4-user scenario
$\mathcal{K} = 0$	21 dB	36.2 dB	45.7 dB
$\mathcal{K} = 4$	27.5 dB	28.4 dB	44.6 dB
$\mathcal{K} = 8$	26 dB	31 dB	45.8 dB

4.2 Effect of code length and User Connectivity

Figure 5, shows the BER curves of 2, 3, and 4-user schemes as a function of the code length β for two SNR values of 15 dB, 25 dB, and $\mathcal{K} = 0$ Rician factor. It is noticed that the increased values of β have a direct influence on enhancing the BER performance and the level of PLS, however, at the cost of an increased receiver complexity. Moreover, the increased level of β has no impact on data rate degrading compared to the OMA systems since $T_{\mathbf{b}} = \beta T_c$. On the other hand, the unauthorized receiver BERs with imperfect ICs also reveal an obvious error floor over the entire range of β. The obtained results are based on a very tiny difference in the ICs of about 10^{-15}. So, the choice of the appropriate parameters for SCD-NOMA allows cost-effective information security with robust error rate performance.

The user connectivity effect on the performance of the SCD-NOMA system can also be noticed from **Figure 5** where the BER performance shows very close results as K increased from 2 to 4. This is a remarkable finding since the BERs are demonstrating high robustness to the number of users increase in contrast to the considered reference of QPSK-NOMA. Therefore, the nonorthogonal users who can be served reliably in this scenario are only limited by the target BER. However, the complexity of BS receiver will be increased as K increased resulting in ML search effort of $\mathcal{O}(M^K)$. This provides a significant tradeoff between the achieved BER performance, user connectivity, and the required SNRs.

4.3 Effect of Secret Key Mismatch

In **Figure 6,** the secret key mismatch effect on the BER system performance is illustrated as a function of the sensitivity to ICs (10^{-x}) considering 2, 3, and 4-user schemes with $\mathcal{K} = 0$ and two SNRs values of 15 dB and 25 dB. It may be noticed that all configurations' signals reveal a clear error floor up to 10^{-16} accuracy. Moreover, the BER performance of all served users can achieve a reliable link at BER target of 10^{-3} when ultra-high sensitivity levels of $\leq 10^{-16}$ is used.

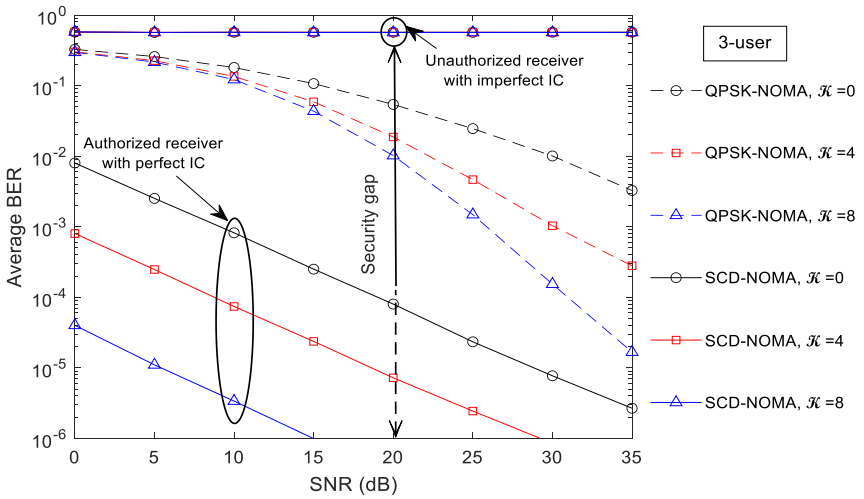

Fig. 3. Average BER of 3-user SCD-NOMA using $\beta = 50$ and different Rician factors of $\mathcal{K} = 0, \mathcal{K} = 4$, and $\mathcal{K} = 8$.

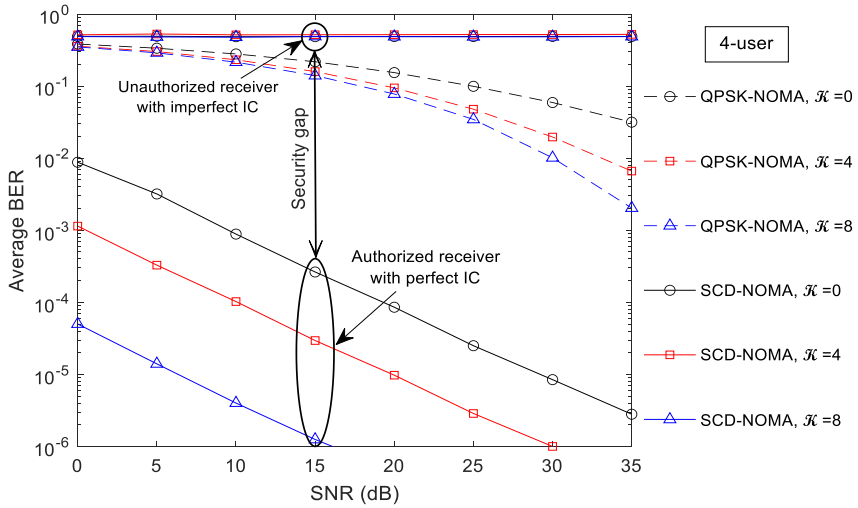

Fig. 4. Average BER of 4-user SCD-NOMA using $\beta = 50$ and different Rician factors of $\mathcal{K} = 0, \mathcal{K} = 4$, and $\mathcal{K} = 8$.

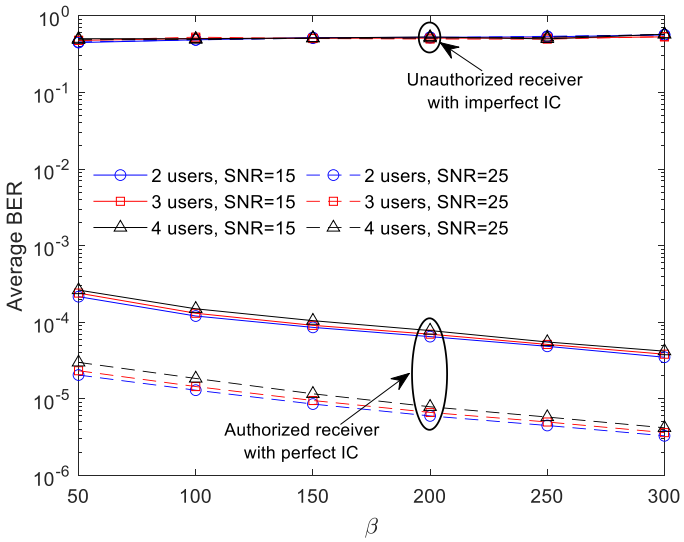

Fig. 5. Average BER performance of 2, 3, and 4-user SCD-NOMA as a function of β using $\mathcal{K} = 0$.

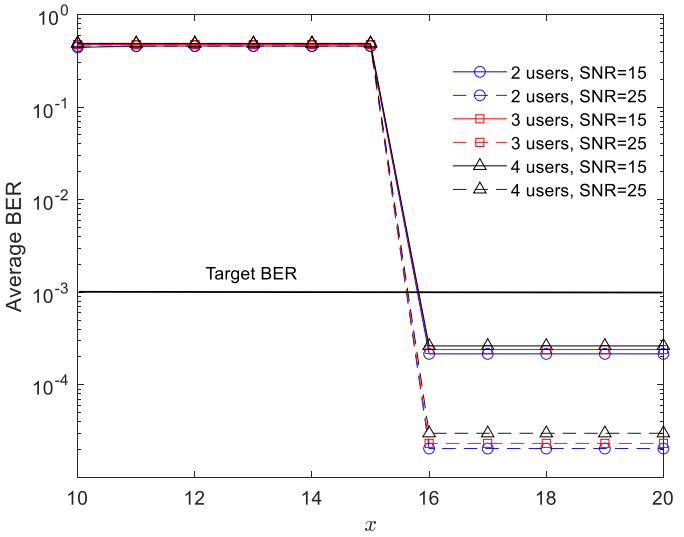

Fig. 6. Average BER performance of 2, 3, and 4-user SCD-NOMA as a function of the sensitivity to ICs (10^{-x}) using $\beta = 50$ and Rician factor of $\mathcal{K} = 0$.

4.4 Key-Space

The SCD-NOMA system's robustness against possible brute-force attacks may be estimated according to the attained key-space. Many essential parameters are considered in the designed system that can efficiently provide powerful secret keys with a key-space set $\mathcal{S} = \{K, \beta, \mathcal{L}, \mathcal{D}, M, \text{ICs}\}$. For example in HCS, the employed ICs with $10^{-16}/\text{state}$ accuracy will attain a key-space of $10^{2\times16} = 10^{32}$. Moreover, when any of the K-served users employ different chaotic codes of length β from any $\mathcal{D}$-state chaotic system, the realized key-space will be increased to $K \times M \times \beta \times \mathcal{L} \times \mathcal{D}$ times. For example, the key-space for PLS will be of order $\mathcal{O}(10^8 \times 10^{32} = 10^{40}) \approx \mathcal{O}(2^{133})$, which is larger than the bound limit of 2^{100} in [14].

5 Conclusion

An efficient uplink system design for SCD-NOMA is presented in this work over Rician channel environments with large-scale and small-scale fading. At the users' sides, a general MCSK system has been used while ML and chaos demodulation have been employed for MUD at the receiving BS. The realized security gap and BER result considering different SCD-NOMA scenarios have confirmed the effectiveness of the proposed scheme in comparison to the QPSK-NOMA reference with many appealing tradeoffs. Furthermore, a massive key-space of order $\mathcal{O}(2^{133})$ is attained to fight the intensive brute-force attacks. The designed system robustness may lead to possible future integration with the existing OMA techniques for modern secure wireless communications.

References

[1] Makki B., Chitti K., Behravan A., Alouini M.S.: A Survey of NOMA: Current Status and Open Research Challenges. IEEE Open Journal of Communications Society. Vol. 1, 179-189 (2020)

[2] Khan L., Yaqoob I., Imran M., Han Z., Hong C.: 6G Wireless Systems: A Vision, Architectural Elements, and Future Directions. IEEE Access. Vol. 8, 147029-147044 (2020)

[3]Almusawi I., Al-Hussaibi W., Tahir Y.: Wireless Nonorthogonal Chaotic Communications: Opportunities, Challenges, and Future Directions. IMDC-SDSP. Antalya, Turkey (2020)

[4] Hamamreh J., Furqan H., Arslan H.: Classifications and Applications of Physical Layer Security Techniques for Confidentiality: A Comprehensive Survey. IEEE Communications Surveys & Tutorials. Vol. 21, 2, 1773-1828 (2019)

[5] Islam S., Avazov N., Dobre O., Kwak K.: Power-Domain Non-Orthogonal Multiple Access (NOMA) in 5G Systems: Potentials and Challenges. IEEE Communications Surveys & Tutorials. Vol. 19, 2, 721-742 (2017)

[6] Almusawi I., Al-Hussaibi W., Tahir Y.: Chaos-Based NOMA for Secure Wireless Communications over Rayleigh Fading Channels. IMDC-SDSP. Antalya, Turkey (2020)

[7] Al-Musawi I., Al-Hussaibi W., Tahir Y. H., Ali F.: Chaos-Based Physical Layer Security in NOMA Networks over Rician fading Channels. Accepted in IEEE ICC'2021. Canada, (2021)

[8] Xiao K., Gong L., Kadoch M.: Opportunistic Multicast NOMA with Security Concerns in a 5G Massive MIMO System. IEEE Communications Magazine. Vol. 56, 3, 91-95 (2018)

[9] Okamoto E., Horiike N., Yamamoto T.: Sparse chaos code multiple access scheme achieving larger capacity and physical layer security. 2017 20th International Symposium on Wireless Personal Multimedia Communications (WPMC). 604-610, (2017)

[10] Cao K., Wang B., Ding H., Lv L., Tian J., Gong F.: On the Security Enhancement of Uplink NOMA Systems With Jammer Selection. IEEE Trans. Commun. Vol. 68, 9, 5747-5763 (2020)

[11] Masuda Y., Okamoto E., Yamamoto T.: Low Complexity Decoding of Downlink Chaos NOMA Scheme with Physical Layer Security. 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC). 1-6, Las Vegas, NV, USA (2020)
[12] Al-Musawi I., Al-Hussaibi W., Tahir Y. H., Ali F.: Chaos-Based Secure Power-Domain NOMA for Wireless Applications. 2020 23rd International Symposium on Wireless Personal Multimedia Communications (WPMC). 1-6, Okayama, Japan (2020)
[13]Elfiqi A., Khallaf H., Hegazy S., Elsonbaty A., Shalaby H., Obayya S.: Chaotic Polarization-Assisted *L*DPSK-MPPM Modulation for Free-Space Optical Communications. IEEE Transactions on Wireless Communications. Vol. 18, 9, 4225-4237 (2019)
[14] Bi M., Fu X., Zhou X., Zhang L., Yang G., Yang X., Xiao S., Hu W.: A Key Space Enhanced Chaotic Encryption Scheme for Physical Layer Security in OFDM-PON. IEEE Photonics Journal. Vol. 9, 1, 1-10 (2017)
[15] Al-Hussaibi W.: 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, 1-3, 87-97 (2015)
[16] Tam W., Lau F., Tse C.: Analysis of bit error rates for multiple access CSK and DCSK communication systems. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications. Vol. 50, 5, 702-707 (2003)
[17]Lau Y., Jusak J., Hussain Z.: Blind Adaptive Multiuser Detection for Chaos CDMA Communication. IEEE TENCON 2005. 1-5, Melbourne, Australia (2005)
[18] Hamamreh J., Basar E., Arslan H.: OFDM-Subcarrier Index Selection for Enhancing Security and Reliability of 5G URLLC Services. IEEE Access. Vol. 5, 25863-25875 (2017)
[19] Hamamreh J., Arslan H.: Secure Orthogonal Transform Division Multiplexing (OTDM) Waveform for 5G and Beyond. IEEE Communications Letters. Vol. 21, 5, 1191-1194 (2017)
[20] Christopher R., Borah D.: Physical Layer Security for Weak User in MISO NOMA Using Directional Modulation (NOMAD). IEEE Communications Letters. Vol. 24, 5, 956-960 (2020)
[21] Sanguinetti L., Kammoun A., Debbah M.: Theoretical Performance Limits of Massive MIMO With Uncorrelated Rician Fading Channels. IEEE Trans. Commun. Vol. 67, 3, 1939-1955 (2019)