Secure Transmission with Interleaver for Uplink Sparse Code Multiple Access System

Ke Lai, Lei Wen, Jing Lei, Gaojie Chen *Member, IEEE*, Pei Xiao *Senior Member, IEEE* and Amine Maaref *Senior Member, IEEE*

***Abstract*—Sparse code multiple access (SCMA) is a promising air interface candidate technique for next generation mobile networks. By introducing the *Tent map* in the Chaos theory, we propose a novel physical layer transmission scheme with codeword level interleaving at the transmitter in this letter, which is termed as interleaver based SCMA (I-SCMA). Simulation results and analysis show that I-SCMA can provide high security performance without any loss in performance and transmission rate, thus constitutes a viable solution for the next generation wireless networks to provide secure communications.**

***Index Terms*—5G; SCMA; secure transmission; interleaving.**

I. Introduction

SCMA [1] is a code domain non-orthogonal multiple access (NOMA) scheme that is considered to be a promising 5G candidate due to its excellent ability to support massive quantities of users under heavily loaded conditions.

In the possible application scenarios for SCMA, such as massive machine type of communication (mMTC), millions of nodes must be accessed. Since ubiquitous mobile devices are required to be accessed to Internet of Things (IoT) in mMTC; hence, unprecedented amount of private and sensitive data is transmitted over wireless channels in an SCMA network. From this perspective, the research on the secrecy issue of SCMA is of significant importance. Moreover, owing to the requirements such as ultra low latency and low power consumption for the IoT, it is also challenging to ensure the security in such a network.

Physical layer security (PLS) has been widely studied in recent years [2]–[5], which is regarded as a promising supplement to the cryptographic techniques. The first NOMA scheme was defined on the power domain, and its secrecy outage probability was derived in [6]. In [7], a secure transmission scheme that maximizes the minimum confidential information rate among users was proposed. In [8], we propose a secure transmission scheme for downlink SCMA system with extra phase rotations in the design of codebook, called randomized constellation rotation based SCMA (RCR-SCMA). However, in that work, extra uplink and downlink communications are necessary, and the randomized codebooks are not fully optimized, thus the secure communication is achieved by satisfying transmission rate with possible performance loss.

In this letter, we mainly focus on improving the computational complexity for the eavesdropper to recover the transmitted data, and thus achieving security for the system. In consequent, a novel physical layer secure transmission scheme with chaotic map and codeword level interleaving, which is denoted as I-SCMA, is proposed. To ensure the security, interleavers that are constructed according to the channel phase with the association of Tent map in the Chaos theory is introduced. The basic idea of I-SCMA is to amplify the randomness of limited information that can be extracted from the channel state information (CSI), and thus leading to asymmetric knowledge between the legitimate users (LUs) and eavesdropper in interleavers since they disperse the order of codewords for each LU. From this perspective, the proposed scheme can be regarded as a physical layer encryption, which is a combination of conventional ciphers and physical layer security. Therefore, the security of I-SCMA is guaranteed by the unacceptable computational complexity at the eavesdropper side.

The rest of this letter is organized as follow. Sec. II describes the system model of I-SCMA. In Sec. III, the proposed I-SCMA transmission scheme is discussed. Numerical results and conclusion are presented in Sec. IV and Sec. V, respectively.

II. Secure transmission with interleaver

The system model of I-SCMA along with the construction of interleaver are presented in this section.

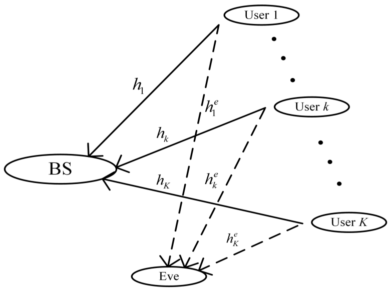

Fig. 1: Illustration of I-SCMA system with an external eavesdropper

K. Lai, L. Wen, J. Lei are with Department of Communication Engineering, College of Electronic Science and Engineering, National University of Defence technology. L. Wen is also with the Institute for Communication Systems (ICS), Home of the 5G Innovation Centre (5GIC), University of Surrey, Guildford GU2 7XH, U.K. E-mail: newton1108@126.com

G. Chen is with the Department of Engineering, University of Leicester, Leicester LE1 7RH, U.K. E-mail: gaojie.chen@leicester.ac.uk.

P. Xiao is with the Institute for Communication Systems (ICS), Home of the 5G Innovation Centre (5GIC), University of Surrey, Guildford GU2 7XH, U.K. Emails: p.xiao@surrey.ac.uk.

A. Maaref is with the Huawei Technologies in Ottawa, ON, Canada. Emails: Amine.Maaref@huawei.com.

A. Interleaver based SCMA

As shown in Fig. 1, we consider the uplink transmissions where J single-antenna LUs transmit signal to the same base station (BS) in the presence of an eavesdropper. We assume that the eavesdropper is an external node, and the BS can distinguish it from LUs, which can be simply realized via authentication in practice. As for the SCMA transmitter, each function element is allocated to d_f users, and each user occupies d_u function elements. The encoder of I-SCMA is the same as conventional SCMA (C-SCMA), which is defined by a codebook X_j that maps $\log_2(\mathcal{C})$ binary bits to a K dimensional complex codeword $\boldsymbol{x_j}$ selected from the dedicated codebook X_j corresponding to user j, where $|X_j| = \mathcal{C}$, and $\mathcal{C}$ is the size of constellation.

At any transmission time, the received signal between single LU and BS can be expressed as

$$y_r(t) = h_r(t)x(t) + n(t), \tag{1}$$

where $x(t)$ is the transmitted signal, $h_r(t)$ is the channel gain and $n(t)$ is the additive white Gaussian noise. Without loss of generality, $h_r(t)$ can be modeled as a complex Gaussian random variable, and its polar form is $h_r(t) = |h_r(t)|e^{j\phi_r(t)}$, where $\phi_r(t) \in [0, 2\pi]$. At each transmission time instant, the BS and each LU perform channel estimation in the same coherent interval and thus they can obtain the same ϕ_r from the CSI.

In I-SCMA, b_j and $\hat{b_j}$ denote the coded information bits and candidate decoded bits of user j, respectively, where the code length is N. After encoding by the SCMA codebook mapper, there are $N/\log_2(\mathcal{C})$ codewords for each user. Subsequently, the codewords are conveyed to the interleaver π_j to scramble the sequences of codewords. Note that each user utilizes a different interleaving pattern and each data block can be encrypted with different π_j at different transmission time so that the security can be enhanced. The construction of interleaver will be demonstrated in the next subsection. After the transmitted chips are received, a de-interleaver is utilized before forward error correction (FEC) encoder. As the BS estimates the channel in the same interval of each user, it can recover the interleaving patterns utilized by LUs and further attain the original transmitted data. It should be noted that as a codeword level interleaver is applied and the detection at the receiver is codeword by codeword; hence, the received signals can be directly detected. Subsequently, the de-interleaver should be utilized to the detected bits of each user since the codewords are scrambled.

As can be observed from Fig. 1, the security of I-SCMA is based on the channel interdependence, moreover, the channel independence is amplified via Tent map for the eavesdropper while the BS can recover the data since the CSI is assumed to be unchanged within the coherent internal.

B. Interleaver construction

The key principle of I-SCMA is that the π_j is derived from the CSI of each LU to BS; hence, π_j $(j \in 1, \cdots, J)$ are unique for different users. It should be noted that the interleaver in this letter has different usage with the ones of Turbo codes or interleave-division multiple-access (IDMA), it is utilized to disperse the order of SCMA codewords and thus make the detected bits unpredictable for the eavesdropper. As such, the eavesdropper cannot recover the original messages without the knowledge of interleaver, therefore, the security can be ensured. As the channels are assumed to be independently, and the Tent map can generate quasi-random sequences that are irreversible, thus π_j are independent and random. In consequent, the transmitted data can be fully scrambled by the interleaver, i.e., the eavesdropper is unable to obtain any information even though it can receive the signals transmitted by LUs since the sequences of the data is different from the original ones. It is obviously that the key of I-SCMA is the construction of π_j, which requires sufficient randomness subject to very limited information that can be used in ϕ_r.

To construct an interleaver that can satisfy our demands, we employ a Tent map in the Chaos theory [9], which can generate a random sequence with a few initial parameters. The original Tent map is expressed as follows:

$$f_\mu := \mu \min\{x, 1-x\} \tag{2}$$

For the values of the parameter $\mu \in [0, 2]$, f_μ maps the unit interval $[0, 1]$ into itself, thus defining a recurrence relation. In particular, iterating a given point x_0 in $[0, 1]$ gives rise to a sequence x_n:

$$x_{n+1} = f_\mu(x_n) = \begin{cases} \mu x_n & \text{for } x_n < \frac{1}{2} \\ \mu(1-x_n) & \text{for } x_n \geq \frac{1}{2} \end{cases} \tag{3}$$

Therefore, once the initial parameter μ and x_0 are given, a random sequence take values that range from 0 to 1 can be obtained. This is mainly due to the Tent map holds the initial parameters within the given range define a dynamical system and thus make the output from predictable to chaotic. It should be noted that such a Tent map is irreversible, i.e., the original input cannot be obtained even the generated sequence is known to the eavesdropper.

Considering the range of ϕ_r is $[0, 2\pi]$ while the range of μ and x_0 are $[0, 2]$ and $[0, 1]$, respectively; hence, a mapping from ϕ_r to μ and x_0 have to be constructed. Note that there exists numbers of such transformations and they are performed locally and silently at BS and each LU such that no signals will be radiated. Consequently, the eavesdropper cannot intercept f and g. However, due to the sensitivity of μ and x_0 in the Tent map, i.e., very minor variation of μ and x_0 can generate a totally different sequence, and the robustness of I-SCMA, f and g should have the ability to enlarge the digits of ϕ_r, which can further exploit the sensitivity of Tent map.

For the ease of implementation, we select two basic functions, which can be written as:

$$|\sin\phi_r| + |\cos\phi_r| = f : \phi_r \to \mu \tag{4}$$

and

$$\frac{1}{2}(\sin\phi_r + 1) = g : \phi_r \to x_0 \tag{5}$$

It is obviously that (4) and (5) can map ϕ_r to the range of initial parameter in (2). After the μ and x_0 are obtained, substituting them into (2) and (3) yields a sequence with certain length (equal to the number of symbols of each user).

Therefore, each value of the generated sequence corresponds to an index of the transmitted codewords. For simplicity, the construction of interleaver is given in Algorithm. 1:

```
Algorithm 1: Interleaver construction of I-SCMA
Output: Interleavers $\pi_j$
foreach transmission time do
    LUs and BS start the channel estimation process;
    LUs and BS obtain the channel phase $\phi_r(t)$ from the CSI;
    Each LU uses their $\phi_r(t)$ to calculate the initial parameters in Tent mapping according to (4) and (5);
    Each LU uses the generated $\mu$ and $x$ in last step to generate a Chaos sequence according to (3);
    Labling each block from 1 to $N/\log_2 \mathcal{C}$;
    Sorting the generated Chaos sequence and rearanging the lable of each block according to the sorted order;
    Each user generates their own interleaver $\pi_j$.
```

From the discussion above, inaccurate estimation will result in catastrophic results. However, since the digits of channel phase can be enlarged by f and g, the requiring accuracy of extracted channel phase can be decreased. Furthermore, numbers of secret key negotiation and correction techniques are reported [10].

III. Analysis and discussion

A. Decrypted complexity of I-SCMA

The decryption complexity for an eavesdropper is a vital secrecy performance metric. From the previous discussion, if the eavesdroppers intend to intercept the data by guessing the interleavers of each user, then the complexity equals to $J \cdot (N/\log_2(\mathcal{C}))!$. Note that $\log_2(\mathcal{C})$ equals to 2 and 4 typically. Consequently, the search space S can be approximated as:

$$S = J \cdot (N/\log_2(\mathcal{C}))! \approx 10^{n\cdot(\ln n - 1)}, \tag{6}$$

where $n = N/\log_2(\mathcal{C})$. As can be observed from (6), even if the code length N is moderate, the computational complexity is certainly unaffordable for the eavesdroppers.

In contrast to enumerate the interleavers as a random attacker with brute force attack, another attacker model considered in this letter, called intelligent attacker [11] is able to estimate the CSI with certain accuracy. However, they still encounter the following difficulties: (i) According to the feature of Tent map in the Chaos theory, the generated sequences are very sensitive to the initial parameters μ and x_0. As reported in [9], the variation of 10 digits after decimal point can even generate totally different sequences. Therefore, the intelligent attacker should have the ability to approximate the CSI with extremely high accuracy. (ii) The mappings from channel phase ϕ_r to μ and x_0 are diverse, and the mapping f and g are unknown to the eavesdroppers; hence, it is impossible for the eavesdropper to intercept the initial parameter that used to generate the interleavers even though it can guess the channel phase with low margin. (iii) The interleavers can be changed over a period time as the CSI is time-varying, which can further enhance the security of I-SCMA.

TABLE I: Searching space comparison per frame

Order Scheme	4-point	16-point
Conventional SCMA	$nC \cdot (\frac{360}{\epsilon})$	$nC \cdot (\frac{360}{\epsilon})$
RCR-SCMA	$4nC \cdot (\frac{360}{\epsilon})^4 \binom{8}{2}^2$	$4nC \cdot (\frac{360}{\epsilon})^2 \binom{4}{2}^2$
I-SCMA	$JC \cdot n!$	$JC \cdot n!$

Therefore, the eavesdropper cannot recover the interleavers to intercept the transmitted data as BS do even the CSI can be estimated with certain accuracy since the pilots are broadcasted

To demonstrate the advantages of I-SCMA, we also compare the decryption complexity of RCR-SCMA and C-SCMA with I-SCMA by using brute force searching. In Table. I, the frame length equals to the code length N, C is the complexity of MPA to detect a data block, ϵ denotes the step size of searching for a correct codebook. As reported in [8], the security cannot be enhanced by further reducing ϵ and thus I-SCMA can achieve a better secrecy performance than C-SCMA and RCR-SCMA in terms of decryption complexity.

B. Entropy Analysis of Post-processing Attack

Aiming at evaluating the performance of the post-processing attacker (PPA) [11], we analyze the entropy of the received signal at the PPA side (H_{PPA}), and make comparison to the entropy of transmitted messages (H_T).

We assume that each user is independent as the codewords are interleaved to be uncorrelated, according to the definition of entropy, for a message with N bits, H_T equals to N. Considering various sizes of codebook in C-SCMA, as for a PPA, the codebook size should be judged at first; hence, the calculation of the entropy is:

$$H_{PPA} = -\frac{1}{K}\sum_{K}\frac{N}{\log_2 \mathcal{C}_k}\sum_{k=1}^{K}\sum_{i=1}^{I_k}\left(\frac{1}{KI_k}\right)\cdot\log_2\left(\frac{1}{KI_k}\right) \tag{7}$$

where K is the possible codebook size that the LUs can use; $\mathcal{C}_k$ is the size of kth candidate codebook; I_k is the number of all possible interleavers. For simplicity and considering the worse scenario, we assume that the codebook size is known to the eavesdropper, then (7) degenerates to:

$$H_{PPA} = -\frac{N}{\log_2 \mathcal{C}}\sum_{I_k}\left(\frac{1}{I_k}\right)\cdot\log_2\left(\frac{1}{I_k}\right) = \frac{N}{\log_2 \mathcal{C}}\cdot\log_2(I_k) \tag{8}$$

By applying the Stirling's approximation, (7) can be further written as:

$$H_{PPA} \approx \left(\frac{N}{\log_2 \mathcal{C}}\right)^2 \cdot \log_2\left(\frac{\sqrt{2\pi}}{e}\left(\frac{N}{\log_2 \mathcal{C}}\right)^{\frac{3}{2}}\right) \tag{9}$$

Note that $\frac{\sqrt{2\pi}}{e} \approx 1$, therefore,

$$H_{PPA} \approx \frac{3}{2}\left(\frac{N}{\log_2 \mathcal{C}}\right)^2 \cdot \log_2\left(\frac{N}{\log_2 \mathcal{C}}\right) \tag{10}$$

In general, $N \gg \mathcal{C}$, thus (10), $H_{PPA} \gg H_T$, which indicates that the entropy of secret keys is larger than plaintext; hence, the proposed I-SCMA can reach the perfect secrecy for PPA.

TABLE II: BER PERFORMANCE OF EAVESDROPPER UNDER CERTAIN ESTIMATED ACCURACY $\sigma^2 = 0.04$

Scheme \ E_b/N_0	5 dB	6 dB	7dB	8dB	9dB
BER	0.4970	0.4968	0.4982	0.4967	0.4977
SER	0.7454	0.7454	0.7461	0.7452	0.7455

IV. SIMULATION RESULTS AND DISCUSSION

The simulation results and security analysis of the I-SCMA are discussed in this section.

As noted in [8], [12], the error rate performance can be used to assess the secrecy performance of a system, thus we evaluate the error rate performance from the perspective of LUs and eavesdropper, respectively, to demonstrate the validity of the proposed scheme.

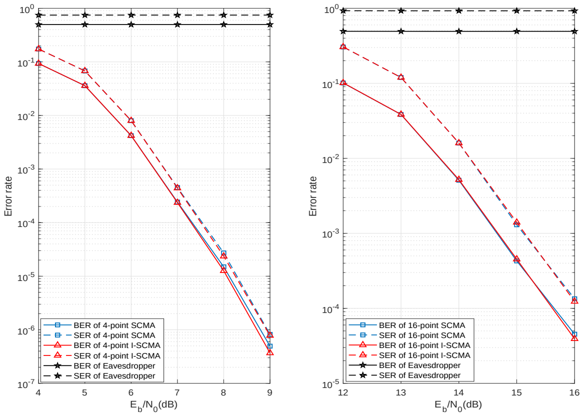

Fig. 2: Error rate performance comparison of legitimate users and an eavesdropper for I-SCMA

Average error rate comparisons of each user for 4-point, 16-point I-SCMA and C-SCMA are shown in Fig. 2 (simulation parameters $K = 4$; $J = 6$; $d_f = 3$; $d_u = 2$; $\max(N_{iter}) = 6$; $\lambda = 150\%$; $N = 256$ and code rate $r = 0.5$). As can be seen from the figures, the performance of I-SCMA is slightly better than C-SCMA especially in the high SNR region, which indicates that I-SCMA will not suffer from performance loss compare to the existing secure transmission for SCMA in [8]. This is mainly because the interleavers disperse the coded sequences so that the adjacent blocks are approximately uncorrelated. Furthermore, it is clear that eavesdroppers cannot obtain any information as they cannot estimate ϕ_r with very high accuracy and the mappers are unknown to them. Note that the symbol error rate (SER) of I-SCMA for eavesdroppers approximate to 0.75 and 0.94 for 4-point and 16-point I-SCMA, respectively, which follows from the fact that each symbol can be wrongly detected with probability:

$$\Pr\{x_i \neq x\} = \frac{\mathcal{C} - 1}{\mathcal{C}} \tag{11}$$

In Table. II, the error rate performance of LUs under the condition that the eavesdropper can approximate the CSI with low error margin is presented. We assume that the estimated ϕ_r of eavesdropper follows the distribution $\tilde{\phi_r} \sim \mathcal{N}(\phi_r, \sigma^2)$. As can be observed from the table, although the eavesdropper can estimate the CSI with certain accuracy, the BER and SER performance of the eavesdropper is still too high to detect the correct transmitted information, which follows from the fact that the Tent map is very sensitive to the input value. Note that the results of 16-point I-SCMA are similar to 4-point I-SCMA.

By combining the higher layers cryptography, the eavesdropper would have to guess both the key and the random interleavers introduced by the CSI, which leads to a significant increase in the search space when performing cryptanalysis. The proposed I-SCMA is a viable solution for secure transmissions in an SCMA network.

V. CONCLUSION

In this letter, we propose a novel secure transmission scheme for uplink SCMA system, which is called I-SCMA. As indicated by the simulation results and analysis, I-SCMA can achieve a good secrecy performance without any performance loss. Furthermore, I-SCMA does not impose any overhead in terms of extra uplink and downlink communications compared to the existing physical layer security transmission schemes. In conclusion, our scheme serves as a valuable supplement to conventional cryptographic technologies.

REFERENCES

[1] H. Nikopour and H. Baligh, "Sparse code multiple access," in *in Proc. IEEE 24th Int. Symp. Pers. Indoor Mobile Radio Commun. (PIMRC)*, Sep. 2013, pp. 332–336.

[2] J. Qiao, H. Zhang, X. Zhou, and D. Yuan, "Joint beamforming and time switching design for secrecy rate maximization in wireless-powered FD relay systems," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 1, pp. 567–579, Jan 2018.

[3] J. Qiao, H. Zhang, F. Zhao, and D. Yuan, "Secure transmission and self-energy recycling with partial eavesdropper CSI," *IEEE Journal on Selected Areas in Communications*, 2018.

[4] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Dual antenna selection in secure cognitive radio networks," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 10, pp. 7993–8002, Dec 2015.

[5] G. Chen, J. Coon, and M. D. Renzo, "Secrecy outage analysis for downlink transmissions in the presence of randomly located eavesdroppers," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 5, pp. 1195 – 1206, Jan 2017.

[6] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and L. Hanzo, "Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks," *IEEE Transactions on Wireless Communications*, vol. 16, no. 3, pp. 1656–1672, Jan. 2017.

[7] B. He, A. Liu, N. Yang, and V. K. N. Lau, "On the design of secure non-orthogonal multiple access systems," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 10, pp. 2196 – 2206, Jul. 2016.

[8] K. Lai, J. Lei, L. Wen, G. Chen, W. Li, and P. Xiao, "Secure transmission with randomized constellation rotation for downlink sparse code multiple access system," *IEEE Access*, vol. 6, pp. 5049–5063, Feb. 2018.

[9] P. Collet and J. P. Eckmann, *Iterated Maps on the Interval as Dynamical Systems*. Boston, MA, USA.: Birkhuser Boston, 1980.

[10] Y. Liu, H. H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Communications Surveys and Tutorials*, vol. 19, no. 1, pp. 347–376, Aug. 2016.

[11] S. Althunibat, V. Sucasas, and J. Rodriguez, "A physical-layer security scheme by phase-based adaptive modulation," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 11, pp. 9931–9942, Aug 2017.

[12] I. M. Kim, B. H. Kim, and J. K. Ahn, "BER-based physical layer security with finite codelength: Combining strong converse and error amplification," *IEEE Transactions on Communications*, vol. 64, no. 9, pp. 3844–3857, Jul. 2016.