Time-Varying Cypher Assignment Based on Secrecy Capacity

Cheng-Ying Yang[1], Jong-Shin Chen[2], Kuo-Chun Hsu[3], Jenq-Foung JF Yao[4], Min-Shiang Hwang[5,6,7]*

[1] Department of Computer Science, University of Taipei, Taiwan
[2] Dept. of Info. and Comm. Eng., Chaoyang University of Tech, Taiwan
[3] Department of Information Management, National Taipei University of Business, Taiwan
[4] Dept of Computer Science, Georgia College and State University, USA
[5] Dept. of C.S. and Info. Eng., Asia University, Taiwan
[6] Fintech and Blockchain Research Center, Asia University, Taiwan
[7] Dept. of Medical Research, University Hospital, China Medical University, Taiwan
cyang@uTaipei.edu.tw, jschen26@cyut.edu.tw, Totoro.hsu@ntub.edu.tw, jf.yao@gcsu.edu, mshwang@asia.edu.tw

Abstract

Wireless communication is a convenient but not secure transmission media. For internet application, such as E-commerce, there are a lot of private information existed. To protect the secret information inside and to set up a secure communication becomes an urgent topic. The purpose of a perfect communication system is to ensure the authentic destination could correctly and successfully receive the exact desired information from the transmitter. Also, the system with authorization and authentication could protect the transmitted information away from the eavesdroppers. Generally, the encryption scheme is applied to. Although these methods have been employed in the system for the security, those unexpected and advanced attackers have been continuously developing. Error-free cryptogram based on Shannon's theorem could provide a solution for the information security. It could be implemented with physical-layer security coding scheme. In this paper, the cypher generator is proposed with physical-layer coding scheme. The cypher format includes two parts. One is the prefixed code and the other is error-control code. The major purpose of prefixed code is the key to find the position indexing of code in the cypher. In this cypher generator, the interleaver plays a role to disturb the original data. It increases the degree of difficulty to break the cypher. With cryptanalysis, the practical example of LDPC is given. With AI technology, the advanced algorithm might be developed for cypher coding and decoding.

Keywords: Secrecy capacity, Physical-layer security, Shannon theorem, Cypher generator, Interleaver

1 Introduction

Due to wideband communication rapidly development, to access the internet service becomes convenient. A lot of internet service comes to be the part of diary life, such as APP. It makes the life easy and expedient. Although the easy life is the purpose of technology revolution, to access the wireless service is dangerous. Without an appropriate protection, the important information might be explored via the devices or the transmission. Hence, the internet security is highly requested. The major objective of secure communication ensures the de-sired information is delivered to the authentic receiver. The secure communication system gives the promising to keep the eavesdroppers away. Also, it transmits the information correctly. Conventionally, the encryption is employed for the issue of information security [1]. In the open wireless environment, it could prohibit the undesired receivers to receive the accurate information without the authorization and authentication schemes [2-3].

For the information security, it is requested to protect the information from the eavesdroppers because the eavesdroppers could receive the same data as that at the desired receiver in the wireless communications. Conventionally, the encryption, in the higher layer application, has been applied. The cypher could be transmitted in the open environment. It could not be read as a plaintext without the key. Also, with authentication and authorization, the effective access control scheme is employed in a secure system [4-6]. Based on the assumption those attackers have a limited computer resource, these security schemes could be used in the current system. However, the unexpected attacks have been developing continuously. The advanced encryption based on the complex hardware infrastructure has to promote the capacity to prohibit these attacks. Unfortunately, Internet of Things (IoT) application devices without a strong computer resource, encryption scheme is not available to apply to [7-9] combat this inconvenience, the physical-layer coding scheme might be employed for secure communications. Shannon's perfect secrecy [10] illustrates that the secure communication could be approach with a positive secrecy capacity. It could be expected the physical-layer coding scheme could provide a error-free cryptogram [11].

The major purpose of physical-layer coding intends not only to provide an error-control scheme in the noisy communication environment but to ensure the safety during the data transmission. Hence, according to the critical requested security, the coding scheme plays a role

*Corresponding Author: Min-Shiang Hwang; E-mail: mshwang@asia.edu.tw
DOI: https://doi.org/10.70003/160792642024092505011

of cryptographic methodology [12]. Based on Shannon's theorem, a perfect communication could be supported with a positive secrecy capacity [10]. There exists a secure communication, with a positive secrecy capacity, if the mutual information between the source station and the destination station is larger than that between the source station and the eavesdropper. The mutual information is defined as methodology the difference between the source entropy and the conditional entropy at the receiver [13]. For a positive secrecy capacity, one solution is to minimize that between the source and the eavesdroppers. The other is to maximize the mutual information between the source and the destination. The amount of entropy is described with the probability distribution of symbol at the source. Hence, to improve the entropy at the source with the code mapping is the major concern.

Physical-layer security coding scheme provides two advantages in the wireless communications. One is to approach the communication with the purpose of error control. The other is to reach the requested security level to against the eavesdroppers [14]. Although the noise interferes the desired transmitted signal, with the coding scheme, the destination could receive the correct data. Also, it benefits to promote the security capacity. How-ever, the coding scheme will add the extra parity data to the transmitted data. It suffers the bandwidth efficiency. Hence, the tradeoff between the coding rate and the secrecy capacity is an important factor to make the code mapping. This paper proposes the coding scheme for the secure communication based on the secrecy capacity. In Section 2, the secure communication system is described. Section 3 proposes the coding scheme based on the analysis of secrecy capacity. Cryptanalysis for the proposed coding scheme is given in section 4. The conclusion of this work is given in the final.

2 Secure Communications

In the communication system, the information is transmitted to the desired destination from the source destination. In the wireless environment, the information data could be received by the desired receiver and anyone including the eavesdroppers. If the information is a plaintext, everyone could read the message without any difficulty. It works as the broadcasting system. For the privacy, the information might encrypt to be a cypher and transmitted. Generally, the secure scheme employs the key to encrypt the plaintext. It transfers the information to another format and exposes in the public. With the appropriate authentication, the desired receiver could release the cypher and obtain the transmitted message, as shown in Figure 1. However, the eavesdroppers might decrypt the cypher, if the degree of security is not strict high.

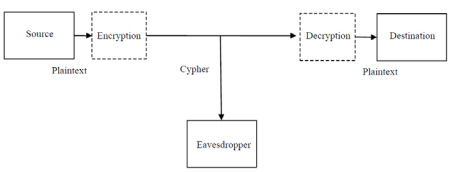

Figure 1. Encryption system

To protect the confidential information, the encryption scheme could be employed. The scheme has a transformation function (denoted as $T\{\cdot\}$) with a key K_1 to change the plaintext X to be the another format text, called cypher C. With the mathematical description

$$T_{k_1}\{X\} = C \tag{1}$$

On the reverse, the cypher could be decrypted (denoted as $D\{\cdot\}$) with a key K_2 and be recovered to be the plaintext X as

$$D_{K_2}\{C\} = X \tag{2}$$

If the key K_1 in the encryption scheme is the same scenario as the key K_2 in the decryption scheme, it is called the symmetric cryptosystem. For example, there are Transposition Cypher [15-16], Substitution Cypher [17-18] and the combination scheme [19].

On the other hand, the key K_1 is not the key K_2, the system is called asymmetric cryptosystem or two-keys cryptosystem. RSA cryptography is the famous one [20-21]. Under the error free transmission, all receivers could obtain the cypher C. However, with the private K_2, the desired destination, with the authentication, could decrypt the cypher to be plaintext X. Hence, with the authorization and the authentication schemes, access control scheme could ensure the system is secure [5-6].

In the wireless communications, from the source station, the data transmitted to the destination station are disturbed due to the noise environment. The interference comes from many natural sources, such as the thermal noise, the thermal vibrations of atoms, impulse radiation, the radiation from the earth and other warm objects, and the celestial sources. With these distortions, the destination might receive the error information. To improve the error performance of communication, error control coding scheme could be employed [22-25]. The error control coding scheme works as the transformation function [26]. It converts the information to a robust form to resist the interference. The original information, the plaintext X, could be coded as codeword by interleaving or adding extra information for the specific purpose [27]. If the coding scheme is kept confidentially, the codeword could be the cypher in the cryptology.

According to Shannon Theorem [10], a perfect communication could be existed based on the positive secrecy capacity. Hence, based on the physical layer coding scheme, it could support the secure and error-free transmission. The secure communications could be depicted in Figure 2.

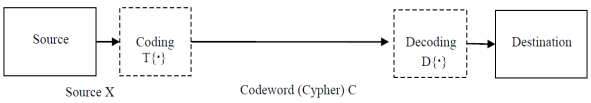

Figure 2. Secure communication system

At the source station, the total information I_X is

$$I_X = \sum_i \log_2 \frac{1}{p(x_i)} \tag{3}$$

where $p(x_i)$ represents the probability of symbol x_i in the source X. With physical layer coding, the source X transfer the symbol x_i to the codeword c_i, as shown in Figure 3. The length of source symbol x_i and that of codeword c_i are denoted as $|x_i|$ and $|c_i|$, respectively. The ratio of $|x_i| / |c_i|$, R, is the coding rate, representing the bandwidth efficiency.

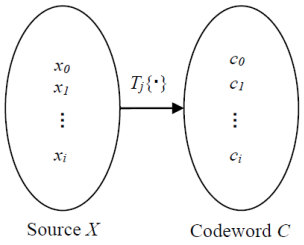

Figure 3. Code assignment codebook j

Under the fixed codebook j, the information I_C of codeword C is

$$I_C = \sum_i \log_2 \frac{1}{p(c_i)} \tag{4}$$

If the probability $p(c_i)$ is inherited from $p(x_i)$, the information I_X at the source station is equal to the information I_C. It meets the minimum requirement for perfect communication, i.e.

$$C_S = I_C - I_X \geq 0 \tag{5}$$

where C_S is defined as secrecy capacity. The interleaving code and one-time pad code are the examples with the coding rate equal to 1. For the interleaving code, the secret key to decrypt the cypher (codeword) could be the transposition table. On the other hand, this interleaving code could resist the burst error due to the impulse radiation interference.

To increase the secrecy capacity C_s, it could increase the valid codewords for the source. In Figure 3, the source x_i is coded with the codebook j. While the codeword space increases, the information of codeword will increase if the multiple codeword assignment is available [4]. Hence, for each source symbol x_i, the cyber assignment could be illustrated in Figure 4.

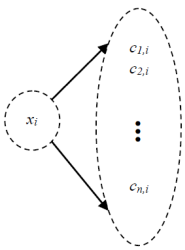

Figure 4. Multiple codeword assignment

Multiple codeword assignment could be the solution to increase the information of codeword if the codewords generated with uniform distribution. After adding the independent prefixed code c_j to the codeword c_i, if the code c_j is dependent to c_i, the probability of the valid codeword c_{ji} is

$$p(c_{ji}) = p(c_j) \cdot p(c_i) \tag{6}$$

For the information of the codeword C', after extending the code space, could be derived to

$$\begin{aligned} I_{C'} &= \sum_{j=1}^{n} \sum_i \log_2 \frac{1}{p(c_{ji})} \\ &= \sum_{j=1}^{n} \sum_i \log_2 \frac{1}{p(c_j)p(c_i)} \\ &= \sum_{j=1}^{n} \sum_i \left(\log_2 \frac{1}{p(c_j)} + \log_2 \frac{1}{p(c_i)} \right) \\ &= \sum_{j=1}^{n} \log_2 \frac{1}{p(c_j)} + \sum_i \left(\log_2 \frac{1}{p(c_i)} \right) \\ &= \sum_{j=1}^{n} \log_2 \frac{1}{p(c_j)} + I_C \\ &> I_C \end{aligned} \tag{7}$$

The improved secrecy capacity Cs' becomes

$$\begin{aligned} C_S' &= I_{C'} - I_X \\ &> I_C - I_X = C_S \\ &> 0 \end{aligned} \tag{8}$$

With adding the prefixed code c_j to the original codewords c_i, although decreasing the coding rate and decreasing the bandwidth efficiency, it provides a positive secrecy capacity for the system and approaches a perfect communication.

3 Proposed Coding Scheme

For a perfect communication system, a positive secrecy capacity is required. Hence, the theoretical error-free cryptogram could be constructed based on the previous derivation. The source symbol x_i could be multiple assigned to those valid codewords c_{ji}. With appending the prefixed code, the physical-layer security coding scheme (code assignment) is proposed.

Two parts of code in the proposed cypher, in Eq. (6), one is for the prefixed code c_j and the other is the original codeword c_i. The proposed format concatenates these two parts as shown in Figure 5.

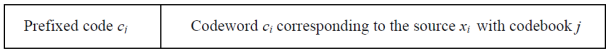

Figure 5. Cypher format

The prefixed code c_j is used to represent the information of j, to decode the received codeword with codebook j.

It works as the first key to decrypt the cypher. In order to maximize the secrecy capacity in Eq. (8) with increasing the numbers of prefixed code, the prefixed code c_j could be kept as iid (Independent and identically distributed). Figure 6 shows the logarithm of secrecy capacity with the increasing j.

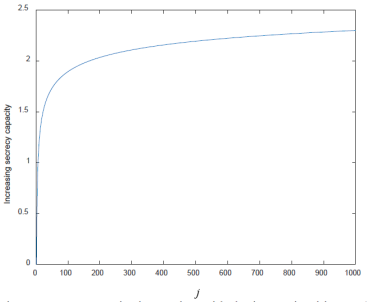

Figure 6. Secrecy capacity increasing with the increasing j in Eq. (8)

For the practical application, the length of prefixed code could is denoted as $\lceil \log_2 j \rceil$, the closed integer that is larger or equal to the $\log_2 j$. In Figure 6, while j is larger than 200, the increasing secrecy capacity could not have a significant difference.

The second part in the proposed cypher format is the code assignment scheme. The assignment scheme could work as the second key to decrypt the cypher. It could apply the error control coding scheme, such as Iterleaving code, eck code, Reed Soleman code, Convolutional code, Turbo code, Low-density parity-check code, Polar code [22-28].

There are two schemes are proposed in this work. Both schemes adopt the transposition method to disturb the code.

(1) Interleaving after channel encoder

Since there are j prefixed code, there are j codebook existed. Although these codebooks could be kept as the same one, it does not affect the secrecy capacity. However, in order to disturb the degree of randmon, it proposes the different codebook corresponding to each different prefixed code. If there are i valid codewords in the codebook, with the tansposition method, there are $i!$ permutation to assign the codebook. For example, the shift transposition scheme, the oder of the codeword assignment (codebook) depends on the position shift, shown in Table 1.

Table 1. Codebook corresponding to the prefixed code

	The source X				
	x_1	x_2	•••	x_{i-1}	x_i
Codebook 1	c_1	c_2	•••	c_{i-1}	c_i
Codebook 2	c_2	c_3	•••	c_i	c_1
⋮	⋮	⋮	⋮	⋮	⋮
Codebook j	c_j	c_{j+1}	•••	c_{j-2}	c_{j-1}

As the mentioned above, the prefixed code c_j is kept as iid. The order of codebook j is random and has the statistical property of independence. Hence,

$$\mathrm{E}\{c_{j_1} \cdot c_{j_2}\} = \begin{cases} 0, & if \quad c_{j_1} \neq c_{j_2} \\ 1, & if \quad c_{j_1} = c_{j_2} \end{cases} \tag{9}$$

It illustrates the cypher could be decrypted with the exact prefixed code first. The cypher generator is depicted in Figure 7.

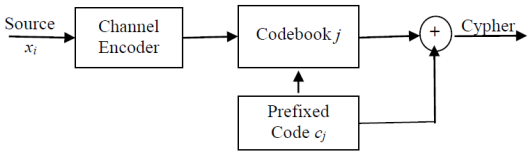

Figure 7. Cyber generator with concatenation of prefixed code and the corresponding assigned code

(2) Interleaving before channel encoder

Since the channel encoder could generate the corresponding codeword according to the input source, with the transposition, the source x_i could be exchanged to be another source x_k, the generated codeword is c_k. Hence, the transposition table is the key for the cypher. If the length of source x_i is $| x_i | = l$, there are there are l! permutation to transpose the input source. The pseudo-random interleaver [29] could maximumly generate 2^n-1 different numbers if there are n-stage register. For example, the structure of the interleaver with 3-stage shift registers as shown in Figure 8.

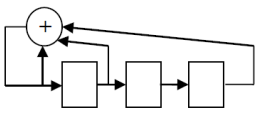

Figure 8. The position generator with 3-stage shift registers

There are 7 different random number generated recyclable. For the initial state 010, the position generator could transpose the data position from $x_i = (d_1, d_2, d_3, d_4, d_5, d_6, d_7)$ to $\hat{x}_i = (d_2, d_5, d_6, d_7, d_3, d_1, d_4)$. According to the transposed source $\hat{x}_i$, the channel generate the codeword corresponding to $\hat{x}_i$. Hence the cypher encoder could be depicted in Figure 9.

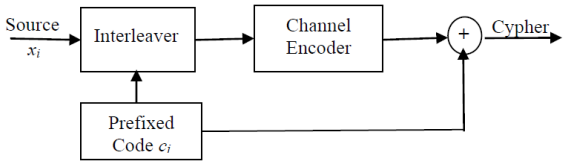

Figure 9. Cyber generator with concatenation of prefixed code and the codeword generated with the interleaved source

Even though the codewords are same, without the same prefixed code, the source is not exactly correct. It could provide a private communication with a high degree of secrecy. Besides, the length of the source, | xi | is less or equal to the length of codeword, | c_i |. For the hardware

implementation, the second opposed cypher generator might be efficient to save the memory.

4 Cryptanalysis

The proposed cypher generator has two parts, the prefixed code and the codeword by error control coding. For the codewords, if the length of souce, $| x_i | = l$, and the length of codeword, $| c_i | = m$, there should be 2^l valid codewords among the 2^m. If m is large, it is exactly difficult to find the corresponding source. For Inter Range Instrumentation Group (IRIG) standards example [29], LDPC has l =4096 or 1024 with coding rate, R, 1/2, 2/3, 4/5. Among the huge number of codespace, it is hardly to recover the source.

However, generally, the codeword is encoded by channel coding with systematic coding scheme. The codeword contains the original source directly. Hence, it could be recovered if the format of the codeword is know. To disguise the default because of systematic encoder, the interleaver has been proposed in this work. Without the exact interleaving information, it is hardly to discover the valid codeword because there are m! permutation among the received code. For example, LDPC has a minimum codeword length 1280. Hence, exhaustive attack has a high difficulty to break this codeword with the interleaving scheme added.

For the first part of the proposed cypher, it is the prefixed code. The benefit of prefixed code not only increases the degree of randomness but increases the secrecy capacity. Specially, in Eq. (9), the statistical property among the different prefixed code is uncorrelated and is independent to the codewords. The information of prefixed code could not be found with the found codeword. The statistical property ensures the only accurate prefixed code could spread the contents of cypher. In pratical, the fixed code could be generated with pseudo-random generator.

5 Conclusion

The issue of information security is highly requested in Internet applications. Without a strong computing resource such as IoT, physical layer coding scheme might provide the optimal solution for the security. In this work, it intends to improve the security capacity in the system. With increasing the length of prefixed code, it shows the enhanced performance. Hence, the method of multiple codeword assignment could effectively improve the secrecy capacity. However, the increasing secrecy capacity could not have a significant difference under the critical condition. Besides, in the cypher generator, the interleaver plays an important role to disturb the data structure. Usually, the channel coding scheme generates the systematic codeword, the source will be revealed without transposition. The indexing of data position is the major key to recover the original data. This work proposes the cypher generator structure based on multiple codeword assignment scheme. For the research on multiple codeword assignment, AI algorithm might apply to. The advanced algorithm could be developed for cypher coding and decoding.

Acknowledgement

This work was supported by the Ministry of Science and Technology, Taiwan, under grants MOST 111-2221-E-845-003- and NSTC 113-2221-E-845 -005 -MY2.

References

[1] W. Easttom, *Modern cryptography: applied mathematics for encryption and information security*, Springer Nature, 2022.

[2] L. Cao, Y. Zhang, M. Liang, S. Cao, An Improved User Identity Authentication Protocol for Multi-Gateway Wireless Sensor Networks, *International Journal of Network Security*, Vol. 24, No. 4, pp. 713-726, July, 2022.

[3] Y. C. Lu, M. S. Hwang, A Cryptographic Key Generation Scheme without a Trusted Third Party for Access Control in Multilevel Wireless Sensor Networks, *International Journal of Network Security*, Vol. 24, No. 5, pp. 959-964, September, 2022.

[4] C. Y. Yang, J. S. Chen, J. F. J. Yao, M. S. Hwang, A Study on Cypher Assignment Based on Secrecy Capacity, *International Journal of Network Security*, Vol. 26, No. 2, pp. 167-172, March, 2024.

[5] H. T. Pan, S. F. Chiou, C.-Y. Yang, M. S. Hwang, An Improved Key Agreement Authentication Scheme Based on an Anonymous Password, International *Journal of Electrical and Electronic Engineering & Telecommunications*, Vol. 9, No. 3, pp. 199-205, May, 2020.

[6] S. K. Sood, A. K. Sarje, K. Singh, Inverse cookie-based virtual password authentication protocol, *International Journal of Network Security*, Vol. 13, No. 2, pp. 98-108, September, 2011.

[7] L. Liu, Y. Jia, Z. Cao, A Note on One Lightweight Authenticated Key Agreement for Fog-enabled IoT Deployment, *International Journal of Network Security*, Vol. 26, No. 2, pp. 252-256, March, 2024.

[8] S. S. Qureshi, J. He, N. Zhu, M. Jia, S. Qureshi, F. Ullah, A. Nazir, A. Wajahat, A New Deep Learning Paradigm for IoT Security: Expanding Beyond Traditional DDoS Detection, *International Journal of Network Security*, Vol. 26, No. 3, pp. 349-360, May, 2024.

[9] Z. Cao, J. Zhu, L. Liu, Analysis of One Multifactor Authenticated Key Agreement Scheme for Industrial IoT, *International Journal of Network Security*, Vol. 26, No. 4, pp. 605-609, July, 2024.

[10] C. E. Shannon, Communication theory of secrecy systems, *The Bell System Technical Journal*, Vol. 28, No. 4, pp. 656-715, October, 1949.

[11] M. Bloch, J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*, Cambridge, 2011.

[12] Y. Zou, Physical-Layer Security for Spectrum Sharing Systems, *IEEE Transactions on Wireless*

Communications, Vol. 16, No. 2, pp. 1319-1329, February, 2017.
[13] M. Stamp, *Information Security: Principles and Practice*, 2nd ed., Wiley, 2011.
[14] M. Khoo, T. A. Wood, C. Manzie, I. Shames, *Exploiting structure in the bottleneck assignment problem*, August, 2020. https://arxiv.org/abs/2008.10804
[15] B. Al-Kasasbeh, A novel secure transposition cipher technique using arbitrary zigzag patterns, *International Journal of Advanced Computer Science and Applications*, Vol. 13, No. 1, pp. 269-276, 2022. DOI:10.14569/IJACSA.2022.0130133
[16] B. Thakkar, B. Thankachan, A multilevel approach of transposition ciphers for data security over cloud, *GIS Science Journal*, Vol. 8, No. 5, pp. 1732-1738, May, 2021.
[17] M. Dharshini, K. Gayathri, S. R. Devi, B. Gopalakrishnan, Refined Imbricate Cryptography with addition of Polygram Substitution Cipher Method: an enhanced tool for security, *Journal of Physics: Conference Series*, Vol. 1767, No. 1, Article No. 012048, 2021.
[18] J. Chen, L. Chen, Y. Zhou, Cryptanalysis of image ciphers with permutation-substitution network and chaos, *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 31, No. 6, pp. 2494-2508, June, 2020.
[19] V. N. Shruthy, V. Maheswari, hybrid combination of substitution and transposition ciphers for efficient encryption using graph labeling, *Turkic World Mathematical Society Journal of Applied and Engineering Mathematics*, Vol. 11, pp. 154-163, 2021
[20] R. Imam, Q. M. Areeb, A. Alturki, F. Anwer, Systematic and critical review of rsa based public key cryptographic schemes: Past and present status, *IEEE Access*, Vol. 9, pp. 155949-155976, November, 2021.
[21] T. S. Obaid, Study a public key in RSA algorithm, *European Journal of Engineering and Technology Research*, Vol. 5, No. 4, pp. 395-398, April, 2020.
[22] S. Lin, D. J. Costello, Jr., *Error Control Coding*, 2nd ed., Pearson, 2004.
[23] V. Bioglio, C. Condo, I. Land, Design of polar codes in 5G new radio, *IEEE Communications Surveys & Tutorials*, Vol. 23, No. 1, pp. 29-40, Firstquarter, 2020.
[24] R. Gallager, Low-density parity-check codes, *IRE Transactions on information theory*, Vol. 8, No. 1, pp. 21-28, January, 1962.
[25] J. Hao, S. T. Xia, K. W. Shum, B. Chen, F. W. Fu, Y. Yang, Bounds and constructions of locally repairable codes: parity-check matrix approach, *IEEE Transactions on Information Theory*, Vol. 66, No. 12, pp. 7465-7474, December, 2020.
[26] J. Ballé, P. A. Chou, D. Minnen, S. Singh, N. Johnston, E. Agustsson, S. J. Hwang, G. Toderici, Nonlinear transform coding, *IEEE Journal of Selected Topics in Signal Processing*, Vol. 15, No. 2, pp. 339-353, February, 2020.
[27] X. Li, J. A. Ritcey, Bit-interleaved coded modulation with iterative decoding, *Proceedings of 1999 IEEE International Conference on Communications*, Vol. 2, Vancouver, BC, 1999, pp. 858-863.
[28] D. Hui, S. Sandberg, Y. Blankenship, M. Andersson, L. Grosjean, Channel Coding in 5G New Radio: A Tutorial Overview and Performance Comparison with 4G LTE, *IEEE Vehicular Technology Magazine*, Vol. 13, No. 4, pp. 60-69, December, 2018.
[29] B. R. Rau, Pseudo-randomly interleaved memory, *Proceedings of the 18th Annual International Symposium on Computer Architecture*, Toronto, Ontario, Canada, 1991, pp. 74-83.

Biographies

Cheng-Ying Yang received the M.S. degree in Electronic Engineering from Monmouth University, New Jersey, in 1991, and Ph.D. degree from The University of Toledo, Ohio, in 1999. He is a member of IEEE Satellite & Space Communication Society. Currently, he is employed as a Professor at The University of Taipei, Taiwan. His research interests are performance analysis of digital communication systems, signal processing, and computer security.

Jong-Shin Chen was born in 1972. He received the B.S. and Ph.D. degrees in computer science from Feng Chia University, Taiwan, in 1996 and 2003, respectively. Currently, he is an associate professor in the Department of Information and Communication Engineering, ChaoYang University of Technology, Taiwan. His research interests include big-data mining, capacity planning, and wireless networking.

Kuo-Chun Hsu graduated from the Department of Transportation and Communication Management Science at National Cheng Kung University with a master's degree and a doctorate. His main research expertise includes information security management, e-learning, system simulation, and intelligent systems. He has long served as the director of the university's information center and has chaired several information security projects for the Ministry of Education.

Jenq-Foung JF Yao is a professor of computer science and data science at Georgia College & State University. With over 30 research papers published, his work focuses on machine learning and data mining, shaping the future of computer and data science education and professionals.

Min-Shiang Hwang received M.S. in industrial engineering from National Tsing Hua University, Taiwan in 1988, and a Ph.D. degree in computer and information science from National Chiao Tung University, Taiwan, in 1995. He was a professor and Chairman of the Department of Management Information Systems, NCHU, during 2003-2009. He was also a visiting professor at the University of California (UC), Riverside, and UC. Davis (USA) during 2009-2010. He was a distinguished professor of the Department of Management Information Systems, NCHU, during 2007-2011. He obtained the 1997, 1998, 1999, 2000, and 2001 Excellent Research Award of National Science Council (Taiwan). Dr. Hwang was a dean of the College of Computer Science, Asia University (AU), Taichung, Taiwan. He is currently a chair professor with the Department of Computer Science and Information Engineering, AU. His current research interests include cryptography, Steganography, and mobile computing. Dr. Hwang has published over 300+ articles on the above research fields in international journals.