A crypto-coding method based on punctured turbo codes for wireless communication systems

Hoang Thi Phuong Thao[1], Dinh Van Linh[2, 3*]

[1]Electric Power University, 235 Hoang Quoc Viet, Bac Tu Liem, Hanoi, Vietnam;
[2]Hanoi University of Science and Technology, 1 Dai Co Viet, Hai Ba Trung, Hanoi, Vietnam;
[3]Academy of Cryptography Techniques, 141 Chien Thang, Thanh Tri, Hanoi, Vietnam.
[*]Corresponding author: vanlinh@actvn.edu.vn
Received 29 Mar. 2025; Revised 19 May 2025; Accepted 10 Jun. 2025; Published 25 Jun. 2025.
DOI: https://doi.org/10.54939/1859-1043.j.mst.104.2025.34-40

ABSTRACT

Encryption and error correction play important roles in secure and reliable wireless communication systems. However, these two functions are performed independently in two different layers which consume a lot of resources. In this work, a crypto-coding method is proposed for these two functions in a single step to reduce the computational complexity and hardware structure. The proposed crypto-coding method is implemented by using a secret key to control the punctured block of the Turbo codes. The secret key is generated from the wireless channel characteristics of single-input single-output (SISO) systems, which ensures the randomness according to the National Institute of Standards and Technology (NIST) version 800-22REV1A. The simulations are executed through the Additive White Gaussian Noise (AWGN) and Rayleigh channels. The simulated results show that the generated keys satisfy the randomness according to the NIST standard, which is evaluated by p -values below 0.01. In addition, the proposed crypto-coding method effectively improves the error correction ability and provides the same computational complexity as the conventional Turbo codes. Meanwhile, this method does not require any extra hardware to manage and distribute secret keys.

Keywords: Crypto-coding; Turbo codes; Punctured block; BER.

1. INTRODUCTION

Crypto-coding methods are potential physical layer security methods for advanced wireless communication systems because they can perform both data encryption and error correction functions at the same time [1]. The crypto-coding methods reduce processing expenses and latency in compared with conventional systems that divide the blocks for encryption and channel coding [2]. The crypto-coding methods can be employed in several channel codes such as low-density parity check (LDPC) codes, polar codes, and Turbo codes. Although Turbo codes have a simple encoding structure, they can achieve good performance close to the Shannon limit with medium block lengths. They are widely used in Forth Generation Long-Term Evolution (4G LTE), Internet of Things, satellite, and military communication systems. Therefore, crypto-coding techniques based on Turbo codes have attracted many researchers.

The Turbo codes are channel codes proposed in 1993 [3]. The structure of the conventional Turbo codes includes two parallel recursive systematic convolutional (RSC) codes. These two RSCs are connected via an interleaved block. A punctured block is employed to choose the parity bits from RSCs.

The crypto-coding methods based on the Turbo codes can be implemented in several manners. Firstly, the authors in [4, 5] apply the Turbo codes in the stages of Advanced Encryption Standard (AES) to increase the security and reliability of the data communication and cloud computing applications. In [6], the crypto-coding methods employ hybrid encryption algorithms along with the Turbo codes to provide better security and reliability for the data storage when compared with the conventional scheme (only encryption or channel coding). The other investigations in [1, 7]

propose the AES/Data Encryption Standard (DES) blocks to generate the pseudorandom bits, and then use them to control the punctured blocks. These methods increase the confusion and diffusion of the secret key. The methods mentioned firstly increase the hardware structure because it depends on the encryption block.

In a second manner, the authors propose crypto-coding methods based on controlling the blocks of Turbo codes. The method in [8] applies the chaotic-based switch for the punctured Turbo codes. This method gives a better security level than the conventional system. However, error correction performance is slightly degraded, particularly at high switching rates. In [9], the authors propose a secure punctured, frame length, or interleaved solution by applying a secret key. The study effectively prevents several attacks, but the proposed punctured Turbo codes reduce the error correction efficiency. The method in [10] uses two controllers to adjust the bit interleaving process or the puncturing solution. This method applies the secret key generated from the wireless channel characteristics, allowing the system to be independent of a third party for key management and distribution. However, this method does not verify the randomness of the key prior to use and is limited to evaluating error correction performance over the Additive White Gaussian Noise (AWGN) channel. Moreover, the authors did not assess the computational complexity, which is a critical factor in determining the feasibility of practical implementation. The study in [11] proposes an odd-even uniform interleaving design. The methods in [10] and [11] indicate that modifications to the interleaved block can degrade the system's error correction performance. This highlights the need for caution when altering the operational principles of the interleaver.

This work proposes a crypto-coding based on the punctured block of Turbo codes. To accomplish this, the punctured block is managed by a secret key generated from the wireless properties. The key generation method is referenced from our previous works [12] and [13]. The difference between this work and our previous works is that the secret keys in [12, 13] are generated based on the complex impulse response (CIR) of multiple-input multiple-output (MIMO) systems, whereas in this work, key is generated based on the CIR of single-input single-output (SISO) systems. Moreover, the key generated in [13] is used to simultaneously intervene in both the interleaved and punctured components of the Turbo code. However, in this work, the secret key is only used to intervene in the punctured block. This method is simpler than intervening in both blocks. Additionally, intervening in the interleaved block with a secret key can reduce error correction performance of SISO systems [10] and [11]. Therefore, the proposed method is suitable for SISO systems. The randomness of the key generated from CIR of SISO systems is evaluated via the National Institute of Standards and Technology (NIST) version 800-22REV1A. The performance of the proposed method is assessed by comparing its Bit Error Rate (BER) with the conventional Turbo codes and the previous works. The simulation results demonstrate that the proposed method improves BER over the conventional Turbo codes. Moreover, the computational complexity is analyzed to compare to the conventional Turbo codes. In summary, there are several contributions as below:

- The secret key is generated based on the CIR of the SISO system instead of the traditional key distribution and management methods; it satisfies the randomness according to the NIST standard. This secret key is used to control the punctured block of the Turbo codes to combine encryption and error correction in a single step.

- The proposed method ensures a low computational complexity and improves the BER performance of SISO systems.

2. PROPOSED METHOD BASED ON THE PUNCTURED TURBO CODES

In the Turbo code structure, the punctured block must be identical at both the transmitter and receiver. This work proposes the crypto-coding method by using the secret key K generated from

the CIR of the single-input single-output (SISO) to manage the punctured block. This key generation method is referenced from [12] for legitimate users. Figure 1 shows the channel model for the proposed method, where Alice and Bob are two legitimate users.

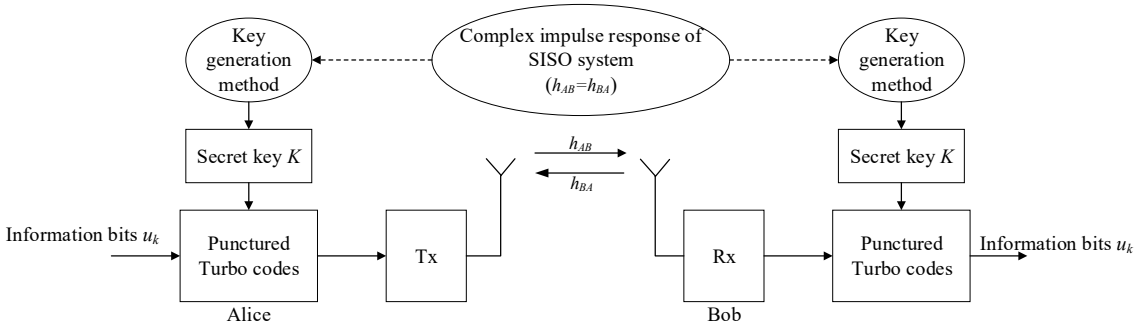

Figure 1. *The channel model for proposed method.*

In this model, Alice and Bob employ the key generation function $f(.)$ to their secret key from the complex impulse response h_{AB} and h_{BA}, respectively.

$$\begin{cases} K_{AB} = f\left(h_{AB}\right) \\ K_{BA} = f\left(h_{BA}\right) \end{cases} \tag{1}$$

Due to the reciprocal channel in time division duplexing mode with coherence time, Alice and Bob can extract the same secret key $\left(K = K_{AB} = K_{BA}\right)$, it can be called a shared secret key K. Then, Alice and Bob apply this secret key K to manage the punctured block of Turbo codes. The locations of the output bits (information bits, parity bits from RSCs) will be kept secret by the secret key K. The proposed method is shown in figure 2, and expressed by pseudocode as follows.

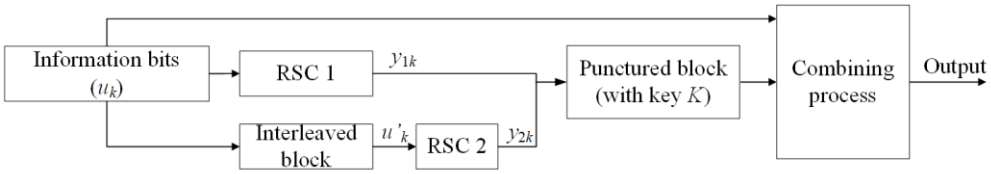

Figure 2. *Diagram of proposed method.*

Algorithm Process System (u_k)
Input: information bits u_k
Output: u_k , y_{1k}, y_{2k}
Begin
Step 1: Process input data (u_k) through interleaved block
$u'_k \leftarrow$ Interleaved block(u_k)
Step 2: Process u_k through RSC 1 to obtain the parity bits
$y_{1k} \leftarrow$ RSC1(u_k)
Step 3: Process u'_k through RSC 2 to obtain the parity bits
$y_{2k} \leftarrow$ RSC2(u'_k)
Step 4: Extracting a secret key K with a length of N bits from the wireless channel properties at the link establishment stage
Key $K \leftarrow$ The wireless channel properties
Step 5: Controlling the the punctured block by the secret key K, the locations of the output bits (u_k, y_{1k}, y_{2k}) will be arranged according to the secret key K.
Output (u_k, y_{1k}, y_{2k}) $\leftarrow D$(y_{1k}, y_{2k}, secret key K)
End

The controlling process of punctured block in step 5 is presented in pseudocode as follows.

Algorithm Process System(u_k)
Input: Secret key K_i , y_{1i} , y_{2i}
Output: $y[1:N]$
Initial: y' = ∅
Begin
For i from 1 to N **do**
If $K_i = 0$ **then**
If i is even **then**
$y'[i]$ = "Eliminating y_{1i}"
Else
$y'[i]$ = "Eliminating y_{2i}"
End If
Else
$y'[i]$ = "Reserving both y_{1i} and y_{2i}"
End If
End For
$y = y'$
End

3. SIMULATION RESULTS AND DISCUSSION

This section evaluates the proposed crypto-coding method through MATLAB simulations over two typical wireless channel models: AWGN and Rayleigh. The BER performance is compared to conventional Turbo codes and the existing methods. In addition, the effectiveness of the proposed method is also shown through computational complexity analysis.

3.1. Randomness evaluation of the secret key

At first, the 256 bit secret keys are generated from the CIR for SISO systems. The randomness of the generated keys is evaluated through p-values according to eight NIST tests [12]. The randomness test criterion requires the p-value to be greater than 0.01. Table 1 shows that all p-values are more significant than 0.01. This confirms that the generated keys satisfy the randomness requirement and are suitable for controlling the puncturing block without relying on external key management mechanisms.

Table 1. *p-values of AWGN and Rayleigh channels.*

Test	AWGN	Rayleigh	Test	AWGN	Rayleigh
Monobit	1	1	Serial 1	0.25	0.12
Block frequency	0.85	0.25	Serial 2	0.77	0.56
Runs	0.52	0.53	Approx. Entropy	1	1
Longest runs of ones	0.23	0.36	Cumulative sums	0.86	0.67
Discrete Fourier Trans.	0.39	0.45			

3.2. BER performance

The simulations were conducted over both AWGN and Rayleigh channels using binary phase-shift keying (BPSK) modulation. The Turbo encoder employed a generator matrix of [1 1 1; 1 0 1], with an input block length of 256 bits. Decoding was performed using the Log-MAP algorithm.

Case study 1: AWGN channel

Figure 3 and figure 4 show the BERs for the conventional Turbo codes and the proposed method, respectively. It can be seen that the BER values concentrate after three iterations. From the 4th iteration and the same $E_b / N_0 = 4$ dB, the BER values reach 2×10^{-6} for the conventional

Turbo codes and 10^{-6} for the proposed method, respectively. As a result, the BER of the proposed method is slightly better than that of conventional Turbo codes since the code rate changes after the punctured block is intervened.

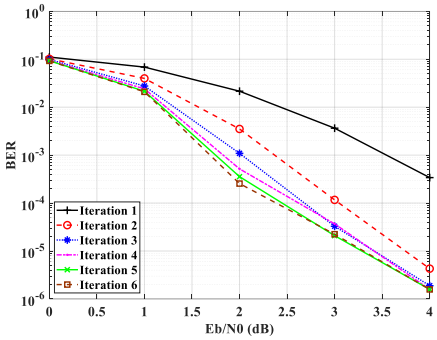

Figure 3. *The BER results for the conventional Turbo code in the AWGN channel.*

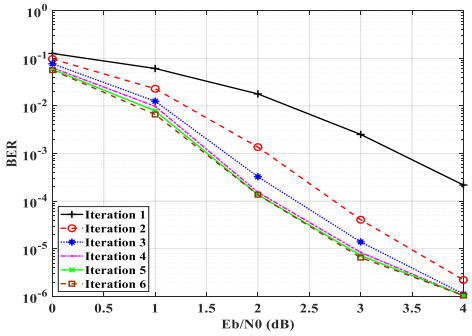

Figure 4. *The BER results for the proposed method in the AWGN channel.*

Case study 2: The Rayleigh channel

The simulation results of the Rayleigh channel are shown in figure 5 and figure 6 for the conventional Turbo codes and the proposed method, respectively. It is similar to the first case study, the conventional Turbo codes have worse BER performance than the proposed method after 6 iterations. The conventional Turbo codes and the proposed method tend to converge after three decoding iterations. In the case of the Rayleigh channel, the conventional Turbo codes obtain a BER of 10^{-3} at $E_b / N_0 = 5$ dB, while the proposed method provides a BER of approximately 10^{-4} at $E_b / N_0 = 5$ dB. In addition, comparing the corresponding figures in the two case studies, it can be seen that the BER efficiency is significantly degraded in the Rayleigh channel.

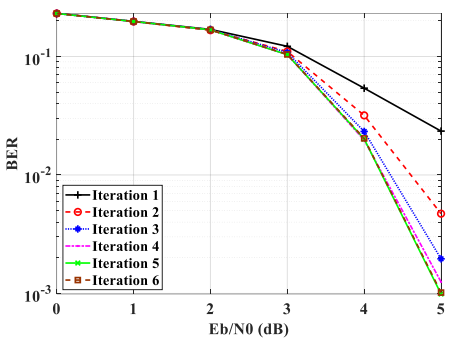

Figure 5. *The BER results for the conventional Turbo code in the Rayleigh channel.*

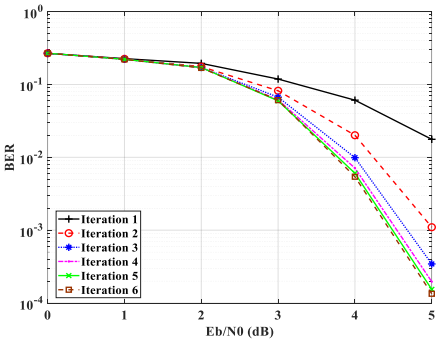

Figure 6. *The BER results for the proposed method in the Rayleigh channel.*

Overall, it can be concluded that our method enhances the error correction ability compared with the conventional Turbo codes.

Table 2 shows the comparison of the proposed method with the existing methods for the input block size of 256 bits. In [6], the authors do not provide clear channel for simulation. In this comparison, we choose the best BER performance in case of AES-ElGamal Hybrid Crypto-Coding scheme. At BER of 10^{-2}, the system obtains $E_b / N_0 = 10.5$ dB for the method in [6]. However, at BER of 10^{-2}, the method in [7] and our method provide similar E_b / N_0 with 0.75 dB for AWGN channel and 4 dB for Rayleigh channel, respectively. This demonstrates that the proposed method achieves error correction performance comparable to method in [7] and significantly outperforms method in [6].

Table 2. *The comparison E_b/N_0 of the proposed method with the existing methods at BER=10^{-2}.*

Channel	E_b / N_0 of [6] (dB)	E_b / N_0 of [7] (dB)	E_b / N_0 of Our method (dB)
AWGN channel	10.5	0.75	0.75
Rayleigh channel	10.5	3.75	3.75

3.3. Computational complexity

To evaluate the computational complexity, we assume that the input of the Turbo encoder and decoder is N bits. Based on the rule of the proposed puncturing mechanism, the Turbo encoder produces qN number of bits (with $2 < q < 3$). As a result, the computational complexity of the puncturing mechanism will be:

$$\mathrm{O}_{puncturing} = \mathrm{O}(rN) = \mathrm{O}(N) \tag{2}$$

Other components of Turbo codes like RSCs and interleaver remain unchanged, thus the computational complexity of RSCs and interleaver are $\mathrm{O}(N)$. The total computational complexity of Turbo encoder is the sum of computational complexities of RSCs, interleaver, and puncturer. It can be calculated as:

$$\begin{aligned} \mathrm{O}_{proposed\_method} &= \mathrm{O}_{RSC1} + \mathrm{O}_{RSC2} + \mathrm{O}_{interleaver} + \mathrm{O}_{puncturing} \\ &= \mathrm{O}(N) + \mathrm{O}(N) + \mathrm{O}(N) + \mathrm{O}(N) = \mathrm{O}(N) \end{aligned} \tag{3}$$

Consequently, the computational of the proposed method is the same as the conventional Turbo codes.

Moreover, the Turbo decoding process of the proposed method uses the log-MAP, thus the computational complexity of decoding process in this method will be $\mathrm{O}\left(n_{iter}.N.2^M\right)$, where n_{iter} denotes the number of iterations and 2^M is the constraint length of the code. Consequently, the computational complexity of the decoding process of the proposed method is comparable to the conventional Turbo code.

4. CONCLUSIONS

This research develops a crypto-coding method based on controlling the punctured block of the Turbo codes by a secret key. The secret key is extracted from the wireless channel properties that ensure the degree of randomness according to the required NIST tests. By using this method, the positions of the parity and information bits are hidden at the output of the punctured block. Only users who know the exact secret key can successfully decode/decrypt. The simulation results demonstrate that the proposed method outperforms the conventional Turbo codes in terms of BER efficiency. The BER values of the proposed method can reach a BER of 10^{-6} at E_b / N_0 of 4 dB for the AWGN and a BER of 10^{-4} at E_b / N_0 of 5 dB for the Rayleigh channel, respectively. In addition, the computational complexity of the proposed method is the same as the conventional Turbo codes. In future work, the proposed method will be implemented in hardware structure to check the feasibility of the proposed method.

REFERENCES

[1]. D. Van Linh and V. Van Yem, *"A turbo-based encryption and coding scheme for multiple-input multiple-output orthogonal frequency division multiplexing wireless communication systems affected by Doppler frequency offset,"* IET Commun., (2023), doi: 10.1049/cmu2.12568.

[2]. D. Van Linh, V. Van Yem, and H. T. T. Phuong, *"Crypto-coding technique based on polar code and secret key generated from wireless channel characteristics for wireless communication systems,"* PLoS One, pp. 1–20, (2025), doi: 10.1371/journal.pone.0318110.

[3]. C. Berrou, A. Glavieux, and P. Thitimajshima, *"Near SHANNON limit error-correcting coding and encoding: Turbo-codes,"* IEEE Int. Conf. Commun., no. 1, pp. 1064–1070, (1993).
[4]. D. Kuswanto and A. Rachmad, *"Combination Scheme of Aes Encryption and Error Correction Turbo Code for Cryptography of Cloud Storage,"* in International Conference on Science and Technology (IICST 2018), no. January, pp. 720–724, (2018), doi: 10.2991/icst-18.2018.146.
[5]. D. Kuswanto, *"Performances Combination Schemes AES-Turbo Code Based-on Keys Length,"* IOP Conf. Ser. Mater. Sci. Eng., vol. 1125, no. 1, p. 012047, (2021).
[6]. T. J. Jeyaprabha and G. Sumathi, *"A pragmatic study on hybrid-crypto-coding schemes for secure data access,"* J. Internet Technol., vol. 22, no. 2, pp. 371–384, (2021).
[7]. D. Van Linh and V. Van Yem, *"A Novel Scheme for Joint Error Control and Dynamic Security Coding Using Puncturing Mechanism,"* J. Commun., vol. 17, no. 11, pp. 948–955, (2022), doi: 10.12720/jcm.17.11.948-955.
[8]. T. H. M. Soliman, F. Yang, and S. Ejaz, *"A proposed chaotic-switched turbo coding design and its application for half-duplex relay channel,"* Discret. Dyn. Nat. Soc., vol. 2015, (2015).
[9]. D. Abbasi-Moghadam and V. T. Vakili, *"Enhanced secure error correction code schemes in time reversal UWB systems,"* Wirel. Pers. Commun., vol. 64, no. 2, pp. 403–423, (2012), doi: 10.1007/s11277-010-0206-2.
[10]. T. H. T. Nguyen and J. P. Barbot, *"Joint error control and dynamic security coding,"* Int. Conf. Adv. Technol. Commun., pp. 285–290, (2013).
[11]. K. S. Arkoudogiannis and C. E. Dimakis, *"Performance analysis of the odd-even uniform interleaver for turbo codes,"* IET Commun., vol. 13, no. 16, pp. 2469–2477, (2019), doi: 10.1049/iet-com.2018.6250.
[12]. D. Van Linh and V. Van Yem, *"Key Generation Technique Based on Channel Characteristics for MIMO-OFDM Wireless Communication Systems,"* IEEE Access, vol. 11, no. January, pp. 7309–7319, (2023), doi: 10.1109/ACCESS.2023.3238573.
[13]. D. Van Linh, H. T. P. Thao, and V. Van Yem, *"A Hybrid of Encryption and Error Correction Method for Multiple-Input Multiple-Output Wireless Communication Systems,"* Int. J. Commun. Networks Distrib. Syst., vol. 30, no. 1, (2024), doi: 10.1504/ijcnds.2024.10061300.

TÓM TẮT

Một phương pháp mã hóa mã hóa dữ liệu và mã hóa kênh trên cùng một bước (Crypto-coding) dựa trên mã kênh Turbo cho hệ thống thông tin vô tuyến

Mã hóa dữ liệu và sửa lỗi kênh truyền là hai chức năng quan trọng trong hệ thống bảo mật thông tin vô tuyến. Tuy nhiên, hai chức năng này đang thực hiện độc lập ở hai lớp khác nhau làm tiêu tốn tài nguyên thiết bị. Trong nghiên cứu này, phương pháp mã mật và mã hóa kênh trên cùng một bước (Crypto-coding) được đề xuất để giảm độ phức tạp và cấu trúc phần cứng. Phương pháp crypto-coding này được thực hiện bằng cách sử dụng khóa bí mật để can thiệp khối mã Turbo bị thủng. Khóa bí mật được sinh ra từ các đặc tính kênh truyền vô tuyến đảm bảo được độ ngẫu nhiên theo tiêu chuẩn của Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST) phiên bản 800-22REV1A. Các mô phỏng được thực hiện qua kênh nhiễu Gauss trắng cộng (AWGN) và kênh Rayleigh. Kết quả mô phỏng và phân tích cho thấy phương pháp mã mật và mã hóa kênh trên cùng một bước đề xuất có hiệu quả cao trong việc cải thiện khả năng sửa lỗi và đạt được độ phức tạp tính toán tương đương mã Turbo truyền thống. Ngoài ra, phương pháp này không yêu cầu phần cứng bổ sung để quản lý và phân phối khóa bí mật.

Từ khoá: Mã hóa dữ liệu và mã hóa kênh; Mã Turbo; Khối đâm thủng; BER; Độ phức tạp tính toán.