A Polar Coding Scheme for Secure Data Transmission Based on 1D Chaotic-Map

T.H.M. Soliman, F.F. Yang, S. Ejaz
College of electronic and information engineering
Nanjing University of Aeronautics and Astronautics (NUAA)
Nanjing, China

***Abstract*—Combining both reliability and security in one block is very important in modern digital communications, each with a variety of sub-disciplines. In this paper, a new polar codes scheme for secure data transmission based on one dimensional chaotic map with a pre-shared secret initial condition is proposed. In this scheme we utilize the logistic map as a tool for generating binary hidden frozen bits assigned for the polar code bad channels. This strategy makes it difficult for those decoders that do not have the chaotic secret initial condition to correctly decode the information message. To increase the system security we support our scheme with hidden both frozen and information bits. This proposed scheme can provide both data secrecy and data reliability in one process to combat problems in an insecure and unreliable data channel link.**

Keywords-channel polarization; chaotic; logistic map; frozen bits; polar codes; pre-shared secret initial conditions

I. INTRODUCTION

Essential to the emergence of large-scale commercial communication networks and many military applications is the demand for reliable and secure high data rates transmission over wireless links. One of the possible methods to provide secrecy and reliability in a communication system without any increase in computational complexity is to embed security in channel coding techniques. So, merging error correction techniques and secrecy in a single block is an important aspect especially in a public and unreliable noisy channel. Polar codes, introduced by Arikan in [1] which depends in its construction on channel polarization phenomenon, are first low-complexity linear codes which provably achieve the capacity for binary discrete memoryless channels [2]. Applying polar codes for a secure communication has been done in many systems. The author of [3] depends in his secured polar codes transmission scheme on the concept that if the frozen bits in polar codes are kept secret and shared by the sender and receiver as in the conventional symmetric cryptography, it will be difficult to those who do not have the shared frozen bits to correctly decode the entire message.

Chaos is a universal phenomenon found in a wide spectrum of natural phenomena and nonlinear systems. The start of a positive relationship between chaotic systems and cryptography has been pointed out [4]. Chaotic systems present many desired cryptographic qualities such as simplicity of implementation that leads to high encryption rates, and excellent security. Chaos is characterized by the way that the dynamical system does not repeat itself, even though the system is governed by deterministic equations, meaning that their future dynamics are fully defined by its initial conditions. While the chaotic non-periodic and random characteristics are typically viewed as penalty to a system, these same features may be exploited to serve security purposes. Several schemes for applying the nonlinear dynamics of the chaotic systems to enhance the security of a communication system have been proposed [5-6]. A lot of research work on combining error correction codes and chaos in communication systems has been done [7] but the work of combining chaos with polar codes is not done yet.

Our aim in this paper is to designs new proposed efficient chaos secured polar coding scheme based on using one-dimension (1-D) chaotic map with a pre-shared secret initial condition as a chaotically pseudo random binary generator (CPRBG) to produce secured frozen bits sequence. The architecture of the proposed chaotic-polar code is based on designing a new coding scheme that possesses both the capabilities of error correction and encryption. Our main contribution in designing secured chaotic polar codes consists of two schemes. The advantages of our schemes are that it can achieve secure reliable system performances by combining the polar coding properties with chaos dynamics using chaotic logistic map without requiring classical encryption techniques.

Firstly in section II, we present the effect of hidden frozen bits on polar codes. In section III, we introduce the design of the proposed chaotic polar coding scheme explaining how we can use CPRBG to generate hidden frozen bits. This scheme can keep the probability of correct decoding low when the shared chaotic maps initial condition is unknown. Then, we extend this work further to more secured polar codes in which we can use coupled logistic maps to hide both frozen and information bits. In such scheme, the hidden process depends mainly on couple of two CPRBG(s) with frame switched output sequence. Secondly, section IV will be devoted to the comparison between the proposed system performance and different polar coding schemes. Finally, some concluding remarks are provided in Section V.

II. POLAR CODES WITH UNKNOWN FROZEN BITS

The basic construction of classical polar codes by Arikan [1] is rooted in the channel polarization effect which consists of two steps: channel combining (combine N independent channels to produce one vector channel) and channel splitting (split the vector channel back into a set of N polarized channels). For the code length N, the generator matrix GN and the binary source U_1^N = (u1, u2… uN) the codeword x is (X_1^N = U_1^N GN). By the polarization phenomenon, the mutual

information between U_1^N and the observation vector Y_1^N which obey a joint probability $W_N(y_1^N|u_1^N)2^{-N}$ is split as [8]:

$$I(U_1^N; Y_1^N) = \sum_{i=1}^{N} I\left(U_i; Y_1^N \middle| U_1^{i-1}\right) = \sum_{i=1}^{N} I(U_i; Y_1^N U_1^{i-1}) \quad (1)$$

As the block length N becomes sufficiently large and after channel polarization steps, the same independent channels will be divided into two kinds of synthesized channels with slightly different reliabilities: the good channels (noiseless channels) and the bad channels (noisy channels) where every term in the rightmost side of (1) tends to take a value near one or zero. In polar codes design, only those bad channels are assigned for fixed bits (frozen bits) and good channels are selected to transmit free bits (information bits). The baseline decoding algorithm of polar codes is the successive cancellation decoder. This decoder performs a series of interlaced step-by-step decisions in which a decision in each step heavily depends on the decisions in the previous steps [1].

As an example, each bit-channel Wi depends on the observation vector Y_1^N and the previous estimates of U_1^{i-1} $[W_i: U_i \rightarrow (Y_1^N, U_1^{i-1})]$. Generally in the polar encoder, the frozen bits are set as a zero vector or can be set as a fixed selected vector that must be known to the decoder. For the information data set u_A and the frozen bits u_{A^c}, the successive cancellation decoder can avoid errors in decoding the frozen bits part by setting $\hat{u}_{A^c} = u_{A^c}$. Due to this fact, it is difficult for the receiver to decode the information bits correctly without any knowledge about the pre-specified frozen bits [3].

III. Proposed Chaotic-Polar Coding Scheme

We can use chaotic map to generate a secured frozen bits that can be used in polar codes to increase the receiver difficulty to decode the message bits correctly. Figure 1 shows the construction block diagram of the proposed chaotic-polar codes based on 1-D logistic map. As we stated before, the chaotic system is very sensitive to its initial condition, so we can use this fact in the chaotic-polar coding scheme to increase the difficulty of the decoder to correctly decode the information bits.

To enhance the secrecy of the polar codes, we propose a scheme that utilizes a chaos binary sequence to hide both the frozen and information bits. Also, the logistic CPRBG(s) will generate a new sequence each frame depending on its initial parameter(s). Using of coupled chaotic sequence to hide the information bits imposes dependency of transmitted messages on the chaos output sequence.

Because it's widely investigation in chaos theory and simplicity in realization, logistic map has been used by many digital chaotic applications. The logistic map formula is:

$$z_{n+1} = \mu z_n(1 - z_n), 0 \leq z_n \leq 1 \text{ and } 0 \leq \mu \leq 4 \quad (2)$$

where μ is the bifurcation parameter and zn is the initial condition of the map. In this map, the next states zn+1 of the chaotic system are fully described only by its present state zn. However, only when the bifurcation parameter (μ) fall in the region $3.57 < \mu \leq 4$, the logistic map has perfect chaotic properties and the orbit diagram of the map reveals an unexpected mixture of order and chaos with periodic windows interspersed between chaotic clouds of dots. By setting the threshold at (0.5) for each logistic map output (Zn+1), the map output can be binarized by setting it to (0) if (Zn+1 < 0.5) and to (1) if (Zn+1 > 0.5). The resulting CPRBG sequences are very irregular and unpredictable (the more unpredictable, the closer to random). In this scheme, we present a CPRBG based on a couple of two chaotic logistic maps that employed to generate frame-switched chaos frozen (FSCF) binary sequence, which can provide higher security than other previous scheme. Since this sequence is generated by comparing two different chaotic orbits, it is difficult for an eavesdropper to extract information about both chaotic systems. In this proposed secured polar codes, two different 1-D logistic maps are employed and coupled together to generate binary output random sequences. As shown in fig. 1, instead of using only one chaotic map as a CPRBG to generate output sequences, random bit streams are generated by comparing the outputs of two different logistic maps Z_{n+1} and T_{n+1} with different pre-shared initial conditions as.

$$F(X, Y) = \begin{cases} 1 & \text{if } Z_{n+1} > T_{n+1} \\ 0 & \text{if } Z_{n+1} \leq T_{n+1} \end{cases} \quad (3)$$

where F(X, Y) is the coupled chaos function that compares the outputs of two different chaotic logistic maps (Z_n and T_n). The coupled chaos function F(X, Y) is used to generate a series of binary chaos random vectors, (l_1, l_2. . . . l_{N-K}, l_{N-K+1}, …, l_N). This sequence is divided into two groups, the first (l_1 to l_{N-K} bits) are assigned as hidden frozen bits, while the remained (l_{N-K+1} to l_N) bits are used to secure the information.

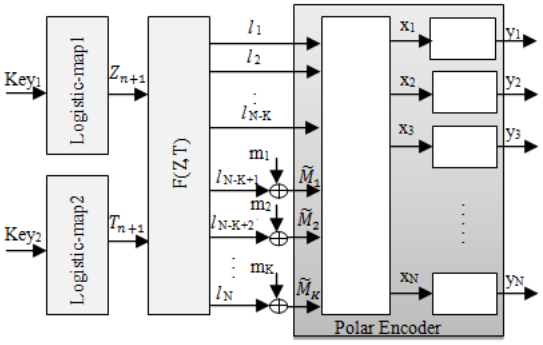

FIGURE I. THE BLOCK DIAGRAM OF THE CHAOTIC-POLAR CODES WITH COUPLED CHAOTIC HIDDEN BOTH FROZEN AND INFORMATION BITS SCHEME.

For the index set A which is a collection of indices for information data transmission and a generator matrix G, the sub-matrices G_A and $G_A{}^c$ are consisting of rows with indices in A and A^c, respectively. Then, the coding scheme can be represented as [1]:

$$x = \tilde{M} G_A + l_1^{N-K} G_{A^c} \quad (4)$$

where $\tilde{M}$ is the chaotic secured message and l_1^{N-K} is the chaos hidden frozen bits.

IV. Simulation Analysis

A. BER Analysis

For our simulation, we use polar codes over Additive White Gaussian Noise (AWGN) channel, with zero mean and

variance $\sigma^2 = N_0 / 2$, where N_0 is the noise power spectral density, the used decoding algorithm is the successive cancelation decoder and BPSK modulation. For the block length N and K be the size of information set, the code rate is R=K/N.

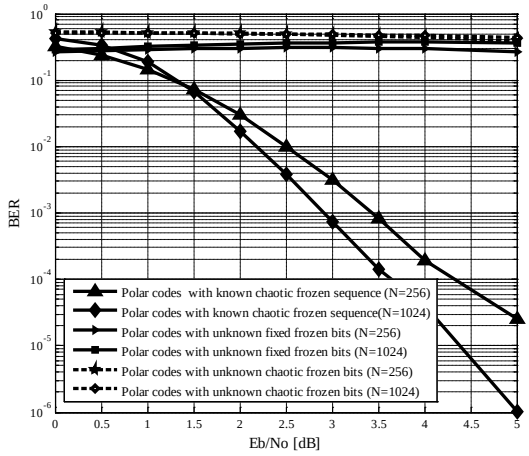

FIGURE II. BER PERFORMANCE COMPARISON BETWEEN POLAR CODES WITH UNKNOWN FIXED FROZEN BITS AND POLAR CODES WITH KNOWN/UNKNOWN CF SEQUENCE OVER AWGN CHANNEL WITH (ZN= 0.2, TN=0.25 AND μ1=3.97, $\mu_2 = 3.85$)) AT N=256 AND 1024 BITS.

For the first chaotic polar coding scheme simulation, fig. 2 compares the BER performances between polar codes of rate *R=1/2* and *N* = 256, 1024 with known CF sequence, with unknown fixed frozen bits and polar codes with only unknown chaotic-frozen (CF) sequence. For polar system with unknown fixed frozen bits, the frozen bits will be arbitrary selected and will be unknown by the classical polar successive cancelation decoder. With the use of chaotic-polar codes with coupled initial conditions (z_n*=0.2*, T_n*=0.25*) and bifurcation parameter ($\mu_1 = 3.97$ and $\mu_2 = 3.85$), only decoder that has the pre-shared secret initial conditions has the ability to decode the transmitted data. Also, we can see clearly that the BER performance of the CF sequence polar codes is worse than that of the polar codes with unknown fixed frozen bits. It means that the use of coupled logistic maps increase the decoder difficulty to decode the transmitted message correctly besides its advantages of being infinite, aperiodic and not correlated binary generator. Another advantage of the chaotic-polar codes scheme is that during the chaotic mapping only a few parameters (pre-shared secret initial condition) are needed being transferred from transmitter to receiver.

Figure 3 displays the BER performances of the polar codes with (known/unknown) FSCF bits compared with the previous different polar coding systems. In the simulation we use the same polar codes system parameters in first scheme and the logistic maps initial condition is set at the same value (z_n*=0.2*, T_n*=0.25*) while the bifurcation parameter (μ) changes each frame with a very little value but we will keep it lying in chaotic area as, ($3.57 < \mu \leq 4$). Figure 3 depicts that for chaotic-polar coding with FSCF bits; it is more difficult for the decoder to decode the transmitted data. Compared with the all three models, polar coding with FSCF is most secured polar coding scheme.

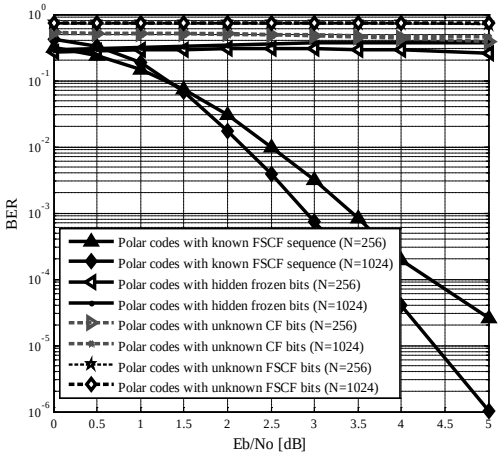

FIGURE III. BER COMPARISON BETWEEN POLAR CODES WITH UNKNOWN FIXED FROZEN BITS, POLAR CODES WITH KNOWN/UNKNOWN CF SEQUENCE AND POLAR CODES WITH KNOWN/UNKNOWN FSCF SEQUENCE OVER AWGN CHANNEL WITH (ZN=0.2, TN=0.25 AND μ=CHANGED) AT N=256 AND 1024 BITS.

B. Security Analysis

In our chaotic-polar coding scheme, we make use of the coupled CPRBG as a kernel for the generation of a random bit stream. This bit-stream is used to hide and secure both frozen and information bits. The use of coupled CPRBG possesses excellent statistical and cryptographic properties. Normally when an intruder finds some information about the used chaotic map from their orbits, he might use such information to lessen the complexity of its pre-shared secret initial condition. With the use of coupled chaotic maps, the cryptanalysis of chaotic ciphers will be more difficult as the chaos output sequence depends on many different chaotic orbits. Hence, for decoders that have no knowledge about the frozen sequence, they need to decode both frozen and information bits, thus the block error probability for both (N, K, A) code and code with the frozen set u_{A^c} are bounded respectively as.

$$P_e(N,K,A) \leq \sum_{i \in A} Z\left(W_N^{(i)}\right) \quad (5)$$

$$P_e(N,K,A,u_{A^c}) \leq \sum_{i \in A} Z\left(W_N^{(i)}\right) \quad (6)$$

For the froze set u_{A^c}, it is proved in [2] that, for a given binary DMC W and a set of frozen indices A^c, the average block error probability $P_e(A^c)$ is bounded as.

$$\max_{i \in A} \frac{1}{2}\left(1 - \sqrt{1 - Z\left(W_N^{(i)}\right)^2}\right) \leq P_e(A^c) \leq \sum_{i \in A} Z\left(W_N^{(i)}\right) (7)$$

Hence, the average block error probability $P_e(A^c)$ boundary can be rewritten as.

$$\max_{i \in A}\left(\frac{1}{2} - \varepsilon\right) \leq P_e(A^c) \leq \sum_{i \in A} Z\left(W_N^{(i)}\right) \quad (8)$$

Hence, for better system security characteristics with higher block error rate, the value of $Z\left(W_N^{(i)}\right)$ will be maximum and very close to "1" that leads to ε will be very small and very near to "0" and the error probability will be high. Hence,

decoders that don't have the pre-shared secret initial condition have no ability to decode the transmitted data correctly.

V. CONCLUSION

In this paper we have presented a combination of polar coding design with chaotic dynamics. It is established that without any knowledge of the pre-specified frozen bits for the proposed chaotic polar coding scheme, the decoder has no ability to correctly decode the transmitted information bits. Also we proved that generating hidden frozen bits by coupled CPRBG increases the difficulty of the decoder to decode transmitted bits correctly and the system BER becomes worse. Moreover we can increase the security by adjusting the CPRBG output to change chaotically each frame. By designing of secured polar codes with coupled chaotic hidden both frozen and information bits, we can enhance the decoding difficulty and the system secrecy but with increasing of the pre-share secret initial conditions.

REFERENCES

[1] E. Arıkan, "Channel Polarization: A Method for Constructing Capacity-Achieving Codes for Symmetric Binary-Input Memoryless Channels," IEEE Trans. Inf. Theory, vol. 55, no. 7, pp. 3051–3073, Jul. 2009.

[2] S. B. Korada and R. Urbanke, "Polar codes are optimal for lossy source coding," IEEE Trans. Inf. Theory, vol. 56, no. 4, pp. 1751–1768, Apr. 2010.

[3] Young-Sik Kim, Jong-Hwan Kim, and Sang-Hyo Kim, "A Secure Information Transmission Scheme With a Secret Key Based on Polar Coding," IEEE Comm. Letters, vol. 18, No. 6, Jun. 2014.

[4] F. Dachselt and W. Schwarz, "Chaos and cryptography," IEEE Trans. Circuits Syst. I, Fundam. Theory Appl., vol. 48, no. 12, pp. 1498–1509, Dec. 2001.

[5] X. Yongxiang, C. K. Tse, and F. C. M. Lau, "Performance of differential chaos-shift-keying digital communication systems over a multipath fading channel with delay spread," IEEE Trans. Circuits Syst. II, Exp. Briefs, vol. 51, no. 12, pp. 680–684, Dec. 2004.

[6] R. Bose and S. Pathak, "A novel compression and encryption scheme using variable model arithmetic coding and coupled chaotic system," IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 53, no. 4, pp. 848–857, Apr. 2006.

[7] Francisco J., Alexandre Wagemakers and Miguel A. F., "Chaos-Based Turbo Systems in Fading Channels," IEEE Trans. Circuits Syst., vol. 61, No. 2, Feb. 2014.

[8] Kai Niu, Kai Chen, Jiaru Lin, and Q. T. Zhang, "Polar Codes: Primary Concepts and Practical Decoding Algorithms," IEEE Comm. Magazine, Jul. 2014.