Journal of
Marine Science and Engineering

MDPI

Article

Ciphered BCH Codes for PAPR Reduction in the OFDM in Underwater Acoustic Channels

Mohsin Murad [1,2,3], Imran A. Tasadduq [3,*] and Pablo Otero [1,2]

[1] Telecommunication Engineering School, University of Malaga, 29071 Malaga, Spain; mohsin@uma.es (M.M.); pablo.otero@uma.es (P.O.)
[2] Institute of Oceanic Engineering Research, University of Malaga, 29071 Malaga, Spain
[3] Department of Computer Engineering, Umm Al-Qura University, Makkah 21955, Saudi Arabia
* Correspondence: iatasadd@alumni.uwo.ca

Abstract: We propose an effective, low complexity and multifaceted scheme for peak-to-average power ratio (PAPR) reduction in the orthogonal frequency division multiplexing (OFDM) system for underwater acoustic (UWA) channels. In UWA OFDM systems, PAPR reduction is a challenging task due to low bandwidth availability along with computational and power limitations. The proposed scheme takes advantage of XOR ciphering and generates ciphered Bose–Chaudhuri–Hocquenghem (BCH) codes that have low PAPR. This scheme is based upon an algorithm that computes several keys offline, such that when the BCH codes are XOR-ciphered with these keys, it lowers the PAPR of BCH-encoded signals. The subsequent low PAPR modified BCH codes produced using the chosen keys are used in transmission. This technique is ideal for UWA systems as it does not require additional computational power at the transceiver during live transmission. The advantage of the proposed scheme is threefold. First, it reduces the PAPR; second, since it uses BCH codes, the bit error rate (BER) of the system improves; and third, a level of encryption is introduced via XOR ciphering, enabling secure communication. Simulations were performed in a realistic UWA channel, and the results demonstrated that the proposed scheme could indeed achieve all three objectives with minimum computational power.

Keywords: underwater acoustic; PAPR; OFDM; BCH codes; XOR cipher

check for updates

Citation: Murad, M.; Tasadduq, I.A.; Otero, P. Ciphered BCH Codes for PAPR Reduction in the OFDM in Underwater Acoustic Channels. *J. Mar. Sci. Eng.* **2022**, *10*, 91. https://doi.org/10.3390/jmse10010091

Academic Editor: Weicheng Cui

Received: 1 December 2021
Accepted: 6 January 2022
Published: 10 January 2022

1. Introduction

Acoustic signals enable short, medium and long-range data transmission in the underwater channel [1]. Severe multi-path fading, variation in the speed of sound and absorption-based pathloss severely limit the communication bandwidth and make the channel complex. Moreover, the underwater acoustic (UWA) channel is wideband in nature, since the bandwidth is of the order of carrier frequency [2]. This results in a larger delay spread of the channel and causes inter-symbol interference (ISI). Since the propagation speed of sound is quite low compared to radio frequency (RF) signals, even a small motion of the transmitter and receiver in the channel causes Doppler spreading and signal shifts. This complexity of the underwater channel severely limits the transmission data-rates. Consequently, for a better utilization of the limited bandwidth and to increase the data-rate of the system, several multicarrier communication schemes have been suggested in the past two decades [3–8].

For enabling multicarrier high data-rate acoustic communication, orthogonal frequency division multiplexing (OFDM) has recently gained a great deal of attention in the UWA domain, and several research works have evaluated the performance of OFDM systems for underwater acoustic channels [2,9–11]. It is a reliable and well-studied multicarrier technique with the ability to deal with frequency selectivity of the channel and longer delay spreads [12,13]. Because of the longer duration of the OFDM symbols, it can counter the ISI caused by the severe multipath in the UWA channels. Despite its advantages, one of the foremost issues associated with OFDM is the high peak to average power ratio at the transmitter. It is a widely studied topic in the field of RF OFDM [14–18], whereas computational and bandwidth limitations render it a unique problem in the acoustic domain [19]. A large peak-to-average power ratio (PAPR) value usually results from the constructive overlapping of random symbol phases to create peaks in the time domain. The presence of non-linear power amplifiers at the transmitter side makes it mandatory to reduce the average power of the system, which causes a loss in performance. In-band distortions and spectral spreading are observed when such a signal passes through non-linear devices, such as high-power amplifiers (HPA). Thus, a high peak to average power ratio causes in-band distortions in an OFDM system and further increases the complexity of the implementation of other blocks, such as analog-to-digital (A/D) and digital-to-analog (D/A) convertors [20]. Various techniques have been suggested to reduce the PAPR of OFDM systems including: (1) signal distortion techniques, e.g., clipping and filtering, windowing, companding and peak cancellation; (2) probabilistic techniques, including partial transmit sequences (PTS), selective mapping (SL), tone injection and tone reservation; and (3) schemes based upon coding, such as linear block coding (LBC), Golay sequences and turbo coding [18].

Bose–Chaudhuri–Hocquenghem (BCH) codes have been used in communication systems for error correction to reduce bit error rates [21]. BCH codes are cyclic codes operating on a group of data bits or blocks, rather than individual bits [22]. Due to their ability to fix multiple errors and simplicity in coding and decoding implementations, they find their uses in various applications. The decoding energy consumption of BCH codes is observed to be a linear function of the number of corrected errors *t* and the length of codewords [23]. Some of the common codes used in this work and their generator polynomials generated using MATLAB's bchgenpoly() function are mentioned in Table 1.

Table 1. BCH coding parameters.

Code	*n*	*k*	*t*	Generator Polynomial
BCH (31,6)	31	6	7	1 1 0 0 1 0 1 1 0 1 1 1 1 0 1 0 1 0 0 0 1 0 0 1 1 1
BCH (31,11)	31	11	5	1 0 1 1 0 0 0 1 0 0 1 1 0 1 1 0 1 0 1 0 1
BCH (31,16)	31	16	3	1 0 0 0 1 1 1 1 1 0 1 0 1 1 1 1
BCH (63,7)	63	7	15	1 0 1 0 1 0 0 1 1 0 0 1 0 0 0 1 0 0 1 0 1 1 0 1 1 0 0 0 1 1 1 0 1 0 0 0 0 1 1 0 1 0 1 1 1 0 0 1 1 1 1 0 1 1 1 1 1
BCH (63,10)	63	10	13	1 0 0 1 1 1 0 1 0 1 1 0 0 1 0 0 1 0 0 1 1 0 0 0 1 0 1 1 0 1 0 1 0 1 1 1 0 1 0 1 0 1 0 0 0 0 0 1 1 0 1 1 0 1
BCH (63,16)	63	16	11	1 1 0 0 1 1 0 1 1 0 0 1 0 0 1 1 0 0 0 0 1 0 1 1 1 1 0 1 1 1 0 1 0 0 1 1 1 0 1 1 0 0 1 0 1 0 1 1
BCH (63,24)	63	24	7	1 1 1 1 0 1 1 0 1 0 0 1 1 0 1 0 1 1 0 0 0 0 1 0 0 0 0 0 1 0 0 1 0 0 1 0 0 0 0 1
BCH (127,8)	127	8	31	1 1 1 0 0 0 1 0 0 1 1 1 0 1 0 1 1 0 1 0 0 0 0 0 1 0 1 0 1 0 1 1 1 1 0 1 0 0 1 0 0 0 0 1 1 0 0 0 1 1 0 1 0 1 0 0 1 1 0 0 1 1 1 1 1 0 0 1 0 0 1 0 1 0 0 0 1 0 1 1 1 0 0 1 1 0 1 1 1 0 1 1 1 1 1 1 0 1 1 0 1 1 0 0 1 0 1 1 0 0 0 0 1 0 0 0 1 1 1 1
BCH (127,22)	127	22	23	1 0 1 0 0 1 1 0 1 1 1 1 1 1 1 0 0 0 0 1 1 1 0 0 0 1 0 0 0 0 0 1 0 0 1 1 1 0 1 0 0 1 0 1 0 1 0 1 0 0 1 0 1 0 0 0 1 1 1 0 1 1 0 0 1 0 0 1 0 1 1 1 0 0 1 0 1 1 0 1 1 0 0 1 1 1 1 1 1 1 0 1 0 0 1 1 1 0 0 0 1 0 0 0 1 1

Table 1. *Cont.*

Code	n	k	t	Generator Polynomial
BCH (127,36)	127	36	15	1 1 0 0 1 1 0 0 1 1 0 0 0 0 1 1 1 1 0 0 1 1 0 1 1 0 1 1 0 1 0 1 0 1 0 0 1 0 0 0 0 1 1 1 1 0 1 0 0 0 1 0 0 1 0 0 1 1 1 1 1 0 1 0 0 1 0 1 1 1 1 1 0 0 1 1 1 0 1 0 0 0 1 1 1 1 0 1 1 1 0 1
BCH (127,50)	127	50	13	1 0 1 1 0 0 1 0 0 1 0 0 1 1 0 1 0 1 0 0 1 0 1 0 1 0 1 0 1 0 0 1 1 0 1 1 0 0 1 1 0 0 0 0 0 0 0 1 0 1 0 1 0 0 0 1 0 0 0 1 1 0 1 0 0 0 0 0 1 1 0 0 0 1 0 0 0 1

The Vernam cipher was first used by Gilbert Vernam in 1917 to encrypt telegraph messaging [24]; also called the XOR cipher, its biggest advantage is that encryption and decryption are both achieved using the same operation. At the transmitter, the input data is converted into binary and divided into blocks. An XOR operation is performed for the input message data with a predefined key of the same block length. The obtained ciphertext is then transmitted, whereby the receiver performs an XOR operation for the received data with the same key to get the original message.

In this work, we use XOR ciphering on BCH codes to propose a low-complexity PAPR reduction scheme for an underwater acoustic OFDM. The proposed XOR-ciphered BCH codes not only have low PAPR, but they also provide a medium level of encryption of the transmitted data while improving the bit error rate (BER) at the same time. The main contributions of this paper are:

- A low-complexity scheme based on XOR-ciphered BCH encoded symbols for PAPR reduction in UWA OFDM systems.
- An offline vector identification technique to shortlist random key vectors that will result in the lowest possible PAPR of XOR-ciphered BCH codes.
- Evaluation of the proposed technique using a shallow underwater channel model showing PAPR as well as BER reduction.

The rest of the paper is structured as follows: Section 2 details the recent advances in the domain of PAPR reduction for underwater acoustic channels, coding techniques proposed for UWA OFDM and using coding for PAPR reduction in OFDM systems. Section 3 briefly describes the OFDM transceiver architecture, the UWA channel model and the coding technique utilized. Section 4 gives a detailed overview of the proposed PAPR reduction technique, followed by Section 5 which is devoted to the results and discussions. In the end, a short conclusion is provided in Section 6.

2. Literature Review

In this section, we detail some of the recent advances in the domain of PAPR reduction and error correcting codes for UWA OFDM systems. Various schemes to reduce PAPR on an OFDM system have been proposed for underwater channels [4,19,25–30] including partial transmit sequences (PTS), low-density parity-check (LDPC) coding, DFT precoding and companding transforms, to name a few.

To deal with the high peaks of OFDM modulated systems, Rojo and Stojanovic [20] proposed a tone injection technique to reduce the peak to the average power of an underwater acoustic OFDM system. The tones are injected out of the normal transducer bandwidth to minimize the peaks and are added to the system just before D/A conversion. These tones are subsequently filtered out after the signal has passed through the power amplifier before transmitting the final signal. This filtering is an additional process that is required for tone suppression. Multiple techniques have been proposed by Rojo and Stojanovic for the optimal placement of the chosen tones, including a random search technique based on limited selection from a set of sequences, as an exhaustive search is not feasible. A PAPR reduction of approximately 0.5 dB to a maximum of 2.5 dB takes place based upon whether the tones have been injected above or below the useful bandwidth and how far the tones are from the useful bandwidth. The data-rate is unaffected in this scheme as there are no overheads. The authors of [31] proposed orthogonal signal division multiplexing (OSDM) for underwater acoustic communication due to its enhanced PAPR reduction performance. However, the complexity of the direct channel equalizer is quite high. An indexed modulated OFDM scheme is proposed in [32], with a PAPR improvement of up to 7 dB over traditional systems.

Historically, various implementations, such as [33–36], have explored block coding techniques to reduce the PAPR of OFDM systems for radio channels. Jones, Wilkinson, and Barton explored block coding for PAPR reduction in OFDM systems [37]. Input data is organized into blocks, and for each block a code with the lowest PAPR is chosen from a list of selected code words. However, they require exhaustive search and lookup tables incurring heavy processing costs. Tasadduq and Rao [38] analyzed the performance of a PAPR reduction technique based on linear block codes and weighting functions for an OFDM system. The codes are chosen according to the number of subcarriers used, e.g., Hamming (7,4) for an 8-subcarrier system. While the resulting coded words are not in powers of two, a redundant bit is added for easy inverse fast Fourier transform (IFFT) implementation. If the number of sub-carriers used in an OFDM system are N, we use the fundamental principles of [37,38] while employing $\mathrm{BCH}(n,k)$ codes to perform an offline exhaustive search for lower orders of k and random selection sets in the case of higher orders of k, to come up with a single key vector of $(N-1)$ bits that results in the lowest PAPR values for most of the combinations.

Carrascosa and Stojanovic employed quadrature phase shift keying (QPSK) signals encoded using BCH(64,10) in a low-complexity channel estimation technique for underwater acoustic MIMO OFDM systems [39]. Kim et al. evaluated various error correcting coding schemes for an underwater OFDM system [40]. The short-length codes evaluated were convolutional, turbo and BCH codes. Simulations using Bellhop [41] and real sea test results demonstrated that the BCH codes had the best overall error correction performance for acoustic OFDM in underwater channels.

Additive ciphers [42] work by adding a sequence of k bits to an input sequence m to obtain a ciphered sequence c. Huo and Gong [43] compared the performance of the XOR cipher and the phase cipher for an OFDM system. The encryption was performed both before channel coding and after channel coding. The XOR ciphering technique is computationally less intensive while having a similar symbol error rate to the phase cipher. Instead of a traditional first encrypt then encode technique, Gligoroski et al. evaluated the concept of cryptcoding schemes [44], whereby encryption and channel coding are integrated into a single block. The evaluated combined systems were more efficient and less complex.

In an underwater acoustic channel, frequency dependent pathloss, doppler spreading and multipath fading make it very difficult to achieve a good bit rate. Similarly, securing the transmitted data while maintaining computational simplicity is a challenge. Thus, the idea of a reliable channel coding technique, combined with a moderate level of security, that can depress the high PAPR of a UWA OFDM system is intriguing.

3. System Architecture

In this section, we briefly explain the various components of our proposed system, including the OFDM transmitter and receiver, the underwater channel model and the cipher and coding technique used.

3.1. OFDM Transceiver

An OFDM based transceiver model is demonstrated in Figure 1. The input binary stream b_i is randomly generated, having a value of 0 or 1 where $i = 0, 1, 2, \ldots$. The serial stream is then block encoded using a $\mathrm{BCH}(n,k)$ encoder.

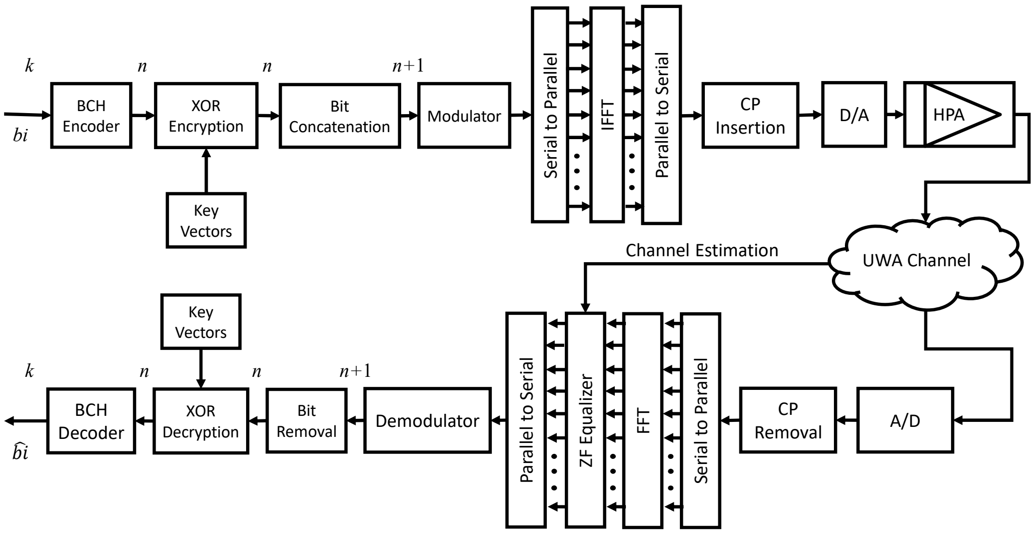


Figure 1. Proposed ciphered BCH OFDM architecture.

The output from the BCH encoder then undergoes XOR encryption. In a typical BCH(n, k) code, the value of n is a prime number, while the number of sub-carriers N in an OFDM system are in powers of two. Therefore, a single bit is appended to each of the encoded sequence. Then, the bits pass through the modulator block where MPSK, QAM or DPSK mapping takes place. Typically, the output of the modulator is a complex number. Next, the serial stream of complex numbers is converted into a parallel stream that can be represented in vector form as:

$$C_p = \left[c_{p,0}, c_{p,1}, c_{p,2}, \dots c_{p,N-1}\right]^T \tag{1}$$

where C_p is a vector of complex numbers for pth OFDM symbol and $c_{p,q}$ is the complex number for pth OFDM symbol and qth subcarrier. These signals are then converted to their discrete time–domain complex equivalents using an IFFT block of size N, and are represented as:

$$X_p = \left[x_{p,0}, x_{p,1}, \dots, x_{p,N-1}\right]^T \tag{2}$$

where X_p is a vector representing the pth OFDM symbol and $x_{p,q}$ is the qth sample of the pth OFDM symbol. A parallel to serial operation is performed and a cyclic prefix (CP) is attached at the start of the OFDM symbol by copying the tail samples of the symbol.

The discrete-time OFDM symbols are then converted into continuous-time signals using the digital to analog conversion block followed by a high-power amplifier block. The final output of the transmitter is then given by:

$$x_p(t) = \frac{1}{\sqrt{T}} \sum_{q=0}^{N-1} c_{p,q} e^{j2\pi f_q t} \tag{3}$$

where $x_p(t)$ is the continuous-time equivalent signal of the pth OFDM symbol and the duration of an OFDM symbol is T. The symbol $x(t)$ is used for the OFDM signal that has been transmitted for all the symbols. The transmitted signal then passes through the underwater acoustic channel. On the receiver, all the steps that were performed at the transmitter are performed in the reverse order. The received signal $\hat{x}(t)$, which is the degraded form of the transmitted signal, is converted back to discrete-time symbols using an analog to digital convertor. The CP is discarded and a serial to parallel operation is performed. The FFT block then produces the discrete frequency domain symbol vector given as:

$$\hat{C}_p = \left[\hat{c}_{p,0},\ \hat{c}_{p,1},\ \hat{c}_{p,2}, \dots \hat{c}_{p,N-1}\right]^T \tag{4}$$

A zero-forcing equalizer is employed, assuming the channel state information (CSI) is known. The symbols are de-mapped after parallel to serial conversion. This is followed by an XOR decryption block and, finally, BCH decoding takes place, giving the estimated binary sequence $\hat{b}_i$.

3.2. XOR Encryption

Figure 2 depicts the basic operation of an XOR encryption system [43]. The input message blocks m are bitwise XORed with the same size key k to generate encrypted data blocks c. In the proposed OFDM system, each binary plaintext/ciphertext block and key has the same size as the number of OFDM sub-carriers. However, the keys here are unique, and are determined based on the maximum PAPR reduction they can achieve when XORed with a BCH code.

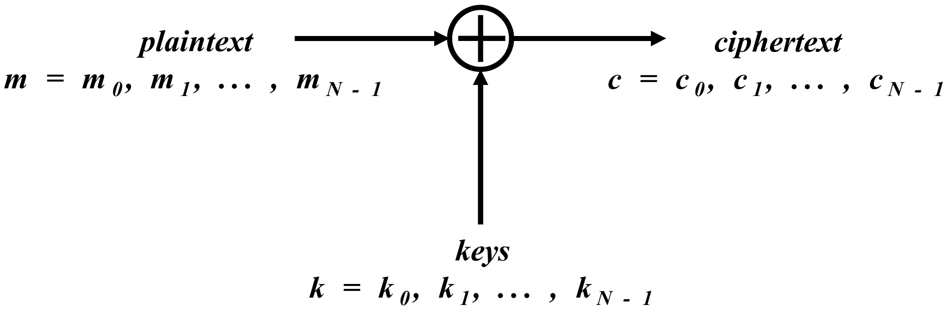

plaintext
$m = m_0, m_1, \ldots, m_{N-1}$
ciphertext
$c = c_0, c_1, \ldots, c_{N-1}$
keys
$k = k_0, k_1, \ldots, k_{N-1}$

Figure 2. XOR encryption [43].

3.3. Shallow Underwater Acoustic Channel

The system is tested using a shallow water underwater channel model [45] based on Rician fading along with absorption path loss and UWA noise [46]. Due to the doubly selective behavior of the underwater channel, acoustic signals experience both time and frequency selectivity [47]. The carrier spacing is greatly reduced [48], since the available bandwidth is of the order of several kHz over longer distances due to the presence of ambient noise as well as losses incurred because of the absorption of acoustic waves underwater [49]. In addition, the propagation velocity of sound waves in water is lower compared to terrestrial radio signals [50]. Thus, the chances of an OFDM system experiencing ICI are greatly enhanced, deteriorating the communication. Equation (5) expresses an underwater acoustic channel response [47] with L multipaths as:

$$H(t,\tau) = \sum_{\mathrm{x}=1}^{L} A_x(t)\delta(\tau - \tau_x(t)) \tag{5}$$

where $\tau_x(t)$ represents the delay coefficients, $A_p(t)$ is the amplitude of the xth multipath and $\delta(t)$ is the Dirac delta function. The delay spread for underwater acoustic channels can be anything between approximately 10 ms to 100 ms [51]. The Doppler shifts affect different subcarriers differently since the channel is wideband in nature.

Figure 3 details the channel model [45] used in this work. The transmitted signal represented by $s(t)$ passes through the absorption loss block, followed by Rician distribution-based fading and the addition of frequency-dependent ambient noise.

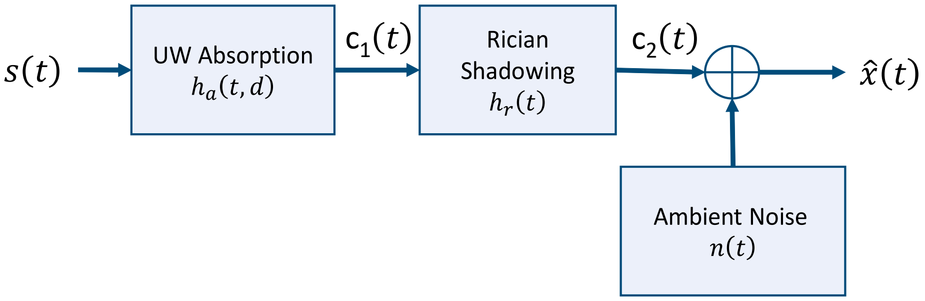


Figure 3. UWA channel model [45,52].

The acoustic pathloss in an underwater channel is a result of the absorption and geometric spreading of the acoustic signals. Thus, the obtained channel transfer function $H_a(f,d)$ [53,54] can be written as:

$$H_a(f,d) = A_d e^{-\gamma(f)d} \tag{6}$$

where A_d is the scaling constant, d represents the transmitter–receiver separation in meters and $\gamma(f)$ is the propagation constant, which is complex. The signal $c_1(t)$, shown in Figure 3, is then computed as the convolution of the inverse Fourier transform of the transfer function and the transmitted signal $s(t)$.

$$c_1(t) = h_a(t,d) \otimes s(t) \tag{7}$$

It is evident from experimental data fitting models that the fading observed in a sound signal in an underwater channel can be modelled using a Rician distribution [55–57]. The parameters used in this work are: $k = 2.0$; $m = 0.4$ [56]. The signal $c_2(t)$ becomes:

$$c_2(t) = h_r(t) \otimes c_1(t) + n(t) \tag{8}$$

where $n(t)$ represents the additive channel noise and $h_r(t)$ represents the inverse Fourier transform of transfer function [58]. Figure 4 shows an instance of the delay profile used in this work and the average path gains.

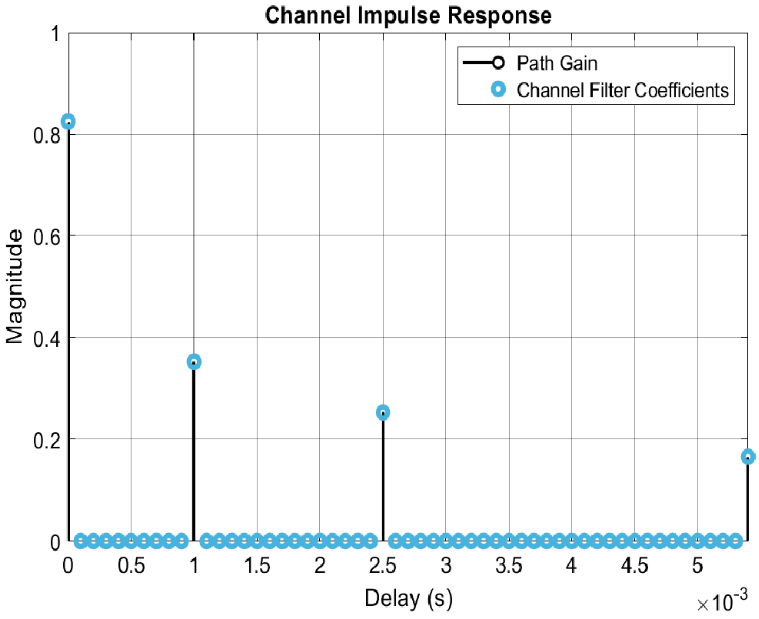


Figure 4. Channel impulse response sample.

For an underwater channel, the ambient noise is a combination of various frequency dependent noises, and major noise sources include thermal noise, shipping activity, noise from turbulence and wave noise [59]. Additionally, from the noise equation, it is evident that the noise is location dependent. Furthermore, the amplitude is higher at the low and high ends of the spectrum and at its minimum at the frequency of 60 kHz [60].

3.4. Peak to Average Power Ratio

PAPR refers to the ratio between the peak power and average power of the system. OFDM adds a PAPR of $10 \log K$ dB to the original PAPR of the system, where K is the number of subcarriers used. The PAPR of an OFDM system [61] is calculated as:

$$\text{PAPR (dB)} = 10 \log_{10} \frac{max[|x_n|^2]}{E[|x_n|^2]} \tag{9}$$

where x_n is the discrete time domain OFDM signal, $max\ [|x_n|^2]$ is the peak signal power and $E[|x_n|^2]$ is the average signal power. The PAPR performance is usually evaluated using a complementary cumulative distribution function (CCDF). A CCDF is a plot that shows the probability of exceeding a certain value of PAPR. Additionally, in this work, we use "PAPR gain" to evaluate the effectiveness of a certain ciphered BCH code. We define "PAPR gain" as the amount of reduction in PAPR compared with the maximum possible PAPR of an OFDM signal. The maximum possible PAPR of an OFDM signal with N subcarriers is given by $10 \log_{10} N$.

4. Proposed Technique

We propose a ciphered BCH (C-BCH)-encoded OFDM scheme that uses predetermined keys to obtain the lowest possible PAPR for an N sub-carrier system. It may be noted that the proposed key selection algorithm is offline and several keys that would produce low PAPR are determined for each code. These key vectors are then used in the live system to produce ciphered codes for reducing the PAPR, as depicted in Figure 5, improving the error performance and providing secure communication. Since the key vectors are obtained in advance using a computer, real time calculations for determining low PAPR combinations are not needed at the transmitter. The only overhead is an XOR operation; however, this operation also adds a level of encryption to the system.

The n value of the BCH(n,k) encoder is selected based on the number of bits required in one OFDM symbol. For example, for an OFDM system with 64 subcarriers and binary phase-shift keying (BPSK) modulation, BCH$(63,k)$ would be selected. BCH$(63,k)$ would also be used for an OFDM system that has 32 subcarriers and quadrature phase-shift keying (QPSK) modulation since in this case, one OFDM symbol will have 64 bits as well. The value of k is based on the desired error and PAPR performances. It is known that the lower the code rate (k/n), the better the error performance. Additionally, such lower code rates can also translate to higher PAPR gains using the proposed algorithm—as will be shown in Section 5. Hence, a BCH$(63,10)$ code will give a better error performance as well as better PAPR gain than a BCH$(63,45)$ code.

Algorithm 1 summarizes the steps for determining the best key vectors for an N sub-carrier BPSK-OFDM scheme and works as follows. A BCH(n,k) encoder is chosen based upon the value of N, such that $n = N - 1$. Since the value of k is a design parameter, it is chosen based on the desired error performance and required PAPR gain. If the value of k is reasonably small, such that all possible k-bit words can be generated, then N_R, i.e., the number of k-bit words to be generated, is given by 2^k. If the value of k is large enough, such that it is computationally impractical to generate all possible k-bit words, then N_R is chosen to be an arbitrarily large number. After generating N_R number of k-bit words, the words are encoded using the chosen BCH(n,k) encoder. Next, N_w number of n-bit key vectors are randomly generated. The value of N_w is chosen based upon trial and error, and will be described in detail in Section 5.

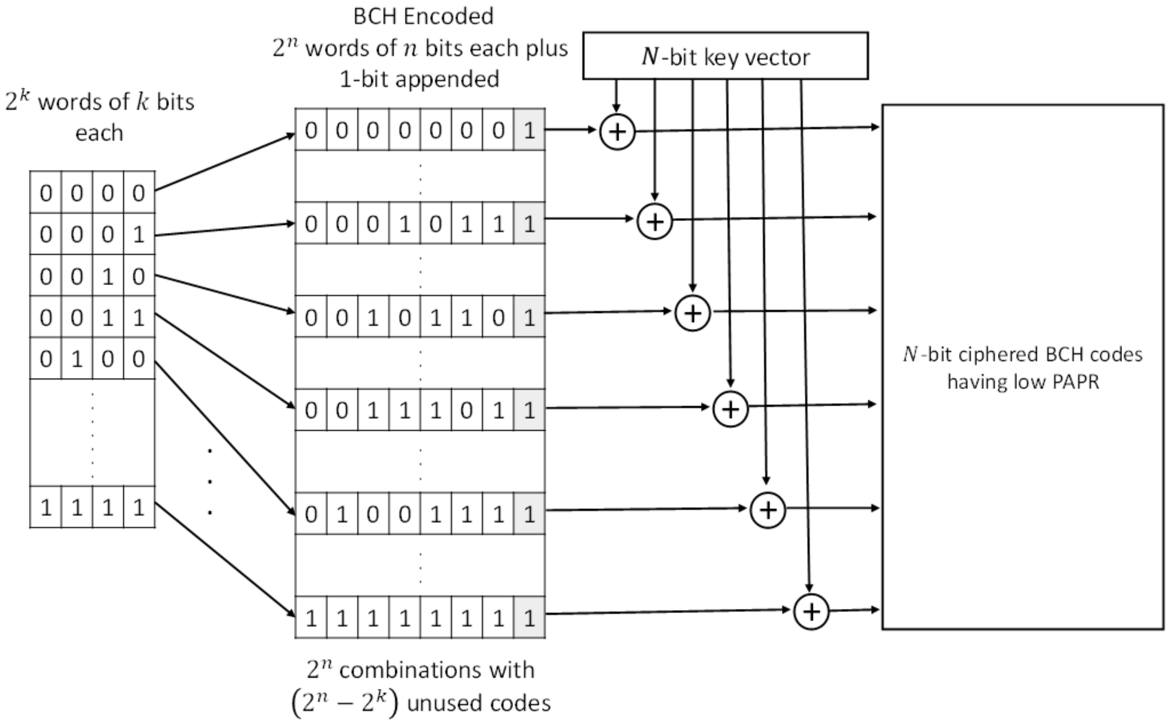

2^k words of k bits each
0 0 0 0
0 0 0 1
0 0 1 0
0 0 1 1
0 1 0 0
1 1 1 1
BCH Encoded 2^n words of n bits each plus 1-bit appended
0 0 0 0 0 0 0 1
0 0 0 1 0 1 1 1
0 0 1 0 1 1 0 1
0 0 1 1 1 0 1 1
0 1 0 0 1 1 1 1
1 1 1 1 1 1 1 1
2^n combinations with $(2^n - 2^k)$ unused codes
N-bit key vector
N-bit ciphered BCH codes having low PAPR

Figure 5. An example of the generation of ciphered BCH(n,k) codes for an 8 subcarrier OFDM system with $k = 4,\ n = 7$.

One key vector is chosen from the set of N_w key vectors and all the BCH-encoded words that were generated in the previous step are XORed with this key vector, resulting in a new set of BCH codes called “ciphered BCH codes”. The PAPR of each of these ciphered codes is computed and the maximum value is stored. Then, the next key vector is chosen from the set of N_w key vectors and the process of producing ciphered codes, determining their PAPRs and storing the maximum PAPR is repeated until all N_w key vectors are exhausted. This results in N_w values of maximum PAPRs along with their corresponding key vectors. Finally, the minimum value from the stored maximum PAPRs is selected along with its corresponding key vector. Since there will be multiple instances of minimum PAPRs and their corresponding key vectors, several key vectors are selected for later use in the live system. The number of key vectors to be selected is a design parameter that depends upon the desired level of security. The higher the level of desired security, the more the number of key vectors selected. The selected key vectors are then used in the live system in a round-robin fashion to perform the XOR operation as shown in Figure 2. The set of selected key vectors are shared with the receiver before switching the system to live operation. However, in the proposed system, side information is not required to be transmitted to the receiver.

A single bit (either 0 or 1) is appended to each of the encoded symbols to make them N-bits long. This step is necessary for two reasons. First, higher PAPR gains are possible only when the number of bits in the encoded sequence are equal to the number of bits in one OFDM symbol.

Second, to facilitate the efficient computation of the FFT algorithm, the number of sub-carriers in an OFDM system are kept in powers of two. There are three options for appending the extra bit to the ciphered BCH code. One option is to add this bit arbitrarily. This will make the total encoded bits equal to N and will save computational power. However, the added bit will not be used and will be wasted. The second option is to utilize this bit for channel estimation. This may marginally increase the computational complexity of the system; however, it can improve the error performance of the system. The third option is to use this bit to obtain further gains in PAPR. However, to determine whether appending a bit 0 or a bit 1 provides more gains in PAPR, the PAPR will have to be computed twice for each OFDM symbol: once while appending a binary 1 and again while appending a binary 0. Our observation is that the computational power required in the third option far outweighs the gain obtained in PAPR.

Algorithm 1 Key Vector Selection

```
1. Initialize $N_w,\ N_R,\ j = 0$
2. Repeat $N_R$ times
   a. Generate a $k$-bit binary sequence $R_j$
   b. Encode $R_j$ using BCH($n$, $k$) and generate encoded sequence $E_j$
   c. $j = j + 1$
3. $i = 0$
4. Repeat $N_w$ times
   a. Randomly generate an $n$-bit key vector $k_i$
   b. $j = 0$
   c. Repeat $N_R$ times
      $C_j = k_i \oplus E_j$
      $\text{PAPR}_j = \text{PAPR}\left\{C_j\right\}$
      $j = j + 1$
   d. $\text{PAPR}^i_{max} = \max_{\forall j} \text{PAPR}_j$
   e. $i = i + 1$
5. $\text{PAPR}_{min} = \min_{\forall i} \text{PAPR}^i_{max}$
6. $l = \arg\{\min_{\forall i} \text{PAPR}^i_{max}\}$
7. $Key_{best} = k_l$
```

Hence, out of the three options, the second option is the most feasible. Table 2 lists some of the key vectors computed for several BCH codes using the proposed algorithm. For each BCH code, we use four key vectors and use them in rotation after every subcarrier block. The vectors and their rotation orders are known at the receiver side; thus, the data is encrypted and only a receiver with the knowledge of the key vectors used will be able to decipher the received information.

Table 2. Keys selected and gains achieved.

Code	No. of Symbols	No. of Vectors	Key Vectors (Hex)	Gain over BCH (dB)
BCH (31,6)	All 2^k	900×10^3	0DA1BDB0	7.6588
		10×10^3	5813A4C0	7.4783
		50×10^3	7C2157D4	7.4397
		100×10^3	243ADB40	7.6109
BCH (31,11)	All 2^k	30×10^3	0C912BDC	4.9975
		30×10^3	31CF7963	4.9975
		30×10^3	45EE06B4	4.9975
		30×10^3	03BC0550	4.9975
BCH (31,16)	All 2^k	10×10^3	778D14A4	3.2545
		10×10^3	6E9E5E56	3.2545
		2500	37D46C5D	3.2545
		2500	4599D87C	3.2545
BCH (63,7)	All 2^k	20×10^3	31DC0A4E92769604	9.8923
		50×10^3	64F1EA51AFD4CF7E	9.7317
		50×10^3	344DDD2044A4BEAC	9.8782
		50×10^3	2924410DE70648C3	9.8218
BCH (63,10)	All 2^k	10×10^3	3AB7480E3466653B	8.5194
		10×10^3	25FD2809A8DA12B5	8.5194
		20×10^3	571232A7E4372046	8.5194
		10×10^3	17AC03EFE0B5814D	8.5194

Table 2. *Cont.*

Code	No. of Symbols	No. of Vectors	Key Vectors (Hex)	Gain over BCH (dB)
BCH (63,16)	All 2^k	1000	4CEF656704A38285	6.0206
		1000	6E892F8204C475FE	6.0206
		1000	4CA8A16F750B7891	6.5812
		1000	47C2E8C0DD58608D	6.0206
BCH (63,24)	Random 2^{18}	6000	1BD6BEB858D9AF8D	1.4927
		500	42B4DF5FA1F308A0	1.5664
		1000	3D4DBDC2F65C0AEC	1.0067
		400	33B03FB68BC55EF3	1.4927
BCH (127,8)	Random 2^{20}	100	3938BBED30C10407F8AB226D735D56AC	11.6499
		100	2E5678670CCF3D50F32840268A11AB4E	11.7250
		500	3D430D3A3A137AA36128FD9AF05C4853	11.5146
		100	195AE63DC2718151B55338F761F95625	11.7058
BCH (127,22)	Random 2^{20}	300	455EA099475B134A14C375EA9CBF8018	7.8241
		1000	1F27F92B1A3EEE260B89073BCDC4854B	8.5194
		1000	6ED23998D6EDA9D4939D85F76738753B	8.5194
		100	7C72213050301219B2ECEC77FF2C0EC3	8.1648
BCH (127,36)	Random 2^{20}	100	51874DF0E5A3550DEFA7C12EADDE812E	1.8035
		100	372AC8B3BD34F81FCE3A58193396A821	1.7430
		100	0B9D9E7FC5D042409B3A77AA4A0E8370	1.5278
		100	1D23FAA5C239438B4E9D917118A172E2	1.8035
BCH (127,50)	Random 2^{20}	100	6B9372C81B6A95C4BE47BC9F543F5ADB	0.9485
		100	0E6950513B228A58D4809AC1AF7CA5A0	0.6437
		100	77E4C718EA54FC99141B0983B1055CE6	0.9485
		100	3C13DC982F9922E6EC58AEF7AB35CB0D	0.8899

5. Simulation Setup and Results

We implemented an OFDM transceiver model in MATLAB 2019b together with a UW channel realization. Table 3 shows the configurations for the transceiver used in our simulations, whereas Table 4 shows the UW channel parameters used. We present the PAPR performance as well as the BER performance of the proposed algorithm in the following two subsections.

Table 3. Transceiver parameters.

Symbol	Quantity
No. of subcarriers	32, 64, 128
Mapping	BPSK
FFT size	32, 64, 128
CP length	N/4
Equalizer	Zero Forcing
Bandwidth	10 kHz

Table 4. Channel parameters.

Symbol	Quantity
TX–RX distance	500, 1500 m
Depth	10 m
Max doppler shift	10 Hz
Gain vector	$[0; -1.5; -2.5; -2]$ dB
Tau vector	$[0; 1; 2.5; 7]$ ms
Atmospheric pressure	1.01325×10^5 Pa
Salinity	35 parts/1000
Density	10^3 Kg/m^3
Water temperature	25 °C

5.1. PAPR Performance

In this work, "gain in PAPR" refers to reduction in maximum possible PAPR, and the maximum possible PAPR for an OFDM system with N number of subcarriers is given by

$10 \log_{10} N$. We simulated three OFDM systems with 32, 64 and 128 subcarriers. Ciphered $\mathrm{BCH}(31,\ k)$ codes and the associated keys were used for the 32-subarrier system, ciphered $\mathrm{BCH}(63,\ k)$ and the associated keys for the 64-subcarrier system and ciphered BCH(127, k) and the associated keys for the 128-subcarrier system. Although, for large values of k, a large number of possible keys are randomly generated, it was observed that using a very large pool of randomly generated keys did not produce a key that would give any appreciable gain in PAPR. In other words, a small subset of randomly generated keys is enough to provide the most appropriate keys that provide a substantial gain in PAPR. One such example is shown in Figure 6, where increasing the pool of random keys only provides a marginal improvement in PAPR, and a 6 dB gain is possible using a key obtained from a set of 50 randomly generated keys.

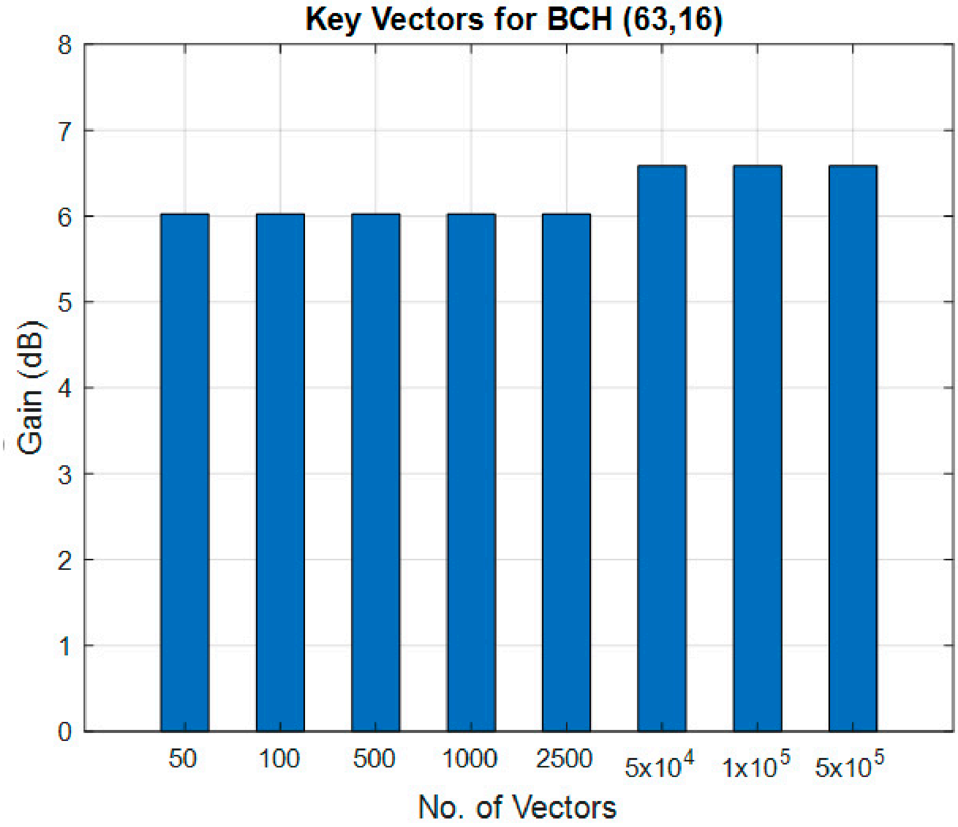


Figure 6. Possible PAPR gain from the most appropriate key obtained from a set of multiple random keys.

Figure 7 shows the gain in maximum PAPR for the three types of ciphered BCH codes used in this work. It should be noted that the smaller the value of k, the greater the gain in PAPR. For a 32-subcarrier OFDM system, the maximum gain obtained was approximately 8 dB for a ciphered BCH(31,6) OFDM system. The maximum possible PAPR for an uncoded 32-subcarrier OFDM system was 15.05 dB; this means that the maximum PAPR of the proposed system never exceeded 7.05 dB. For a 64-subcarrier OFDM system, the maximum gain obtained was approximately 10 dB for a ciphered $\mathrm{BCH}(63, 7)$ OFDM system, which means that the maximum PAPR of the proposed system never exceeded 8.06 dB. Similarly, for a 128-subcarrier OFDM system, the maximum gain obtained was approximately 12 dB for a ciphered $\mathrm{BCH}(127, 8)$ OFDM system.

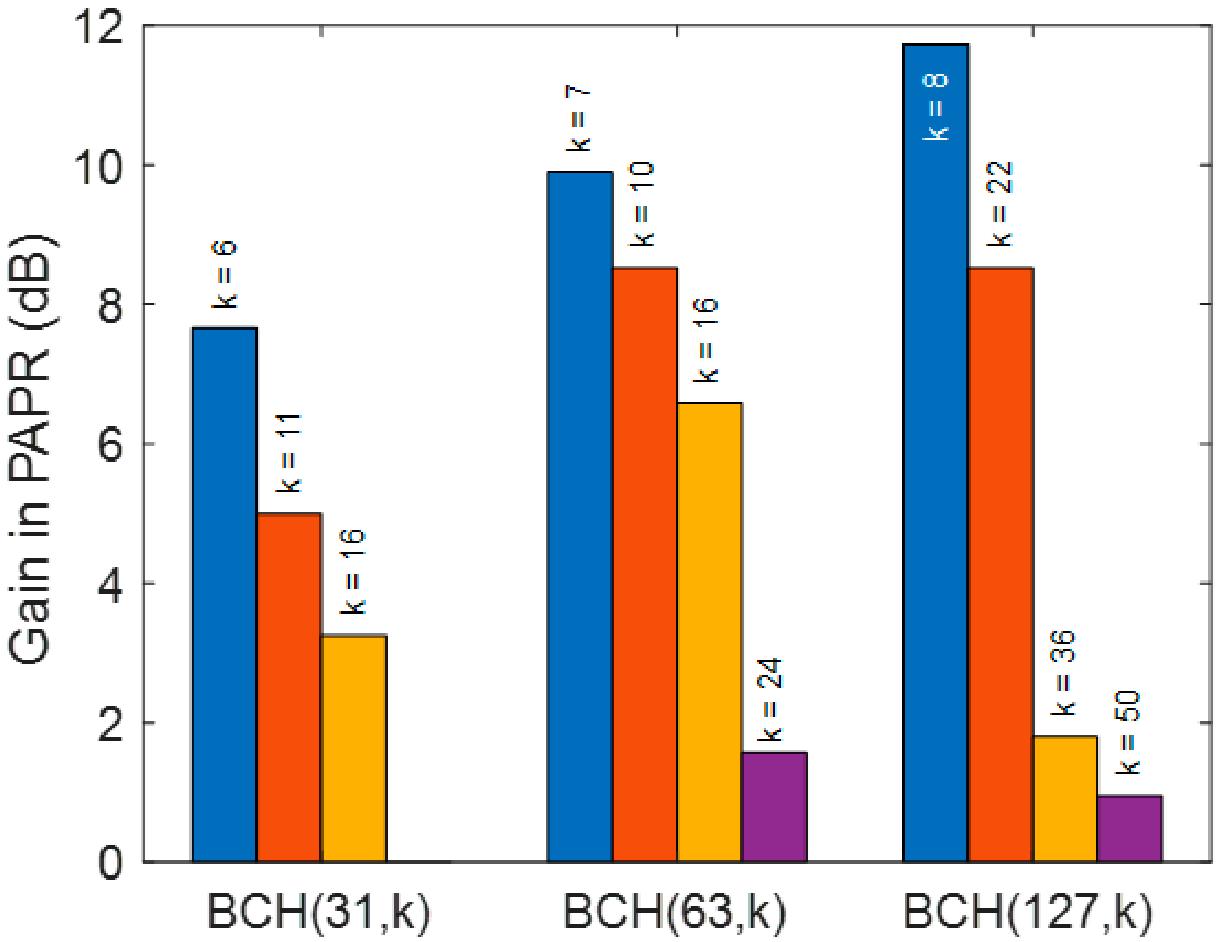


Figure 7. Gain in maximum PAPR as a function of various ciphered BCH codes.

Figure 8 compares the PAPR performances of the proposed 32-subcarrier OFDM systems with uncoded and BCH-encoded OFDM systems using CCDF plots. Figure 8a,c,e compare the PAPR performances of ciphered BCH$(31, k)$ with those of uncoded systems, while Figure 8b,d,f compare the PAPR performances of ciphered BCH(31, k) with those of BCH$(31, k)$ encoded systems. For the sake of illustration, Figure 8a shows the gain achieved in PAPR as an example for a 32-subcarrier system. As shown in Figure 7, the PAPR performance of the ciphered BCH$(31, 6)$ system was much superior to that of an uncoded OFDM system, as the PAPR of proposed system never exceeded about 7.5 dB. As shown in Figure 8b, when comparing the PAPR performance of a ciphered BCH$(31, 6)$ with that of conventional BCH$(31, 6)$ system, it was observed that the PAPR of a conventional BCH(31,6)-encoded system remained high with a high probability, unlike the uncoded OFDM system. A similar phenomenon is observed in Figure 8d. As would be expected, the PAPR performance of ciphered BCH codes for higher values of k was not at par with the systems where the value of k was small, as shown in Figure 8e,f. This is because when the code rate k/n becomes large, there are fewer number of possible key vectors that will produce low PAPR sequences. Hence, there does not exist a key vector that would give the same gain in PAPR as is given by the key vector when the code rate is low.

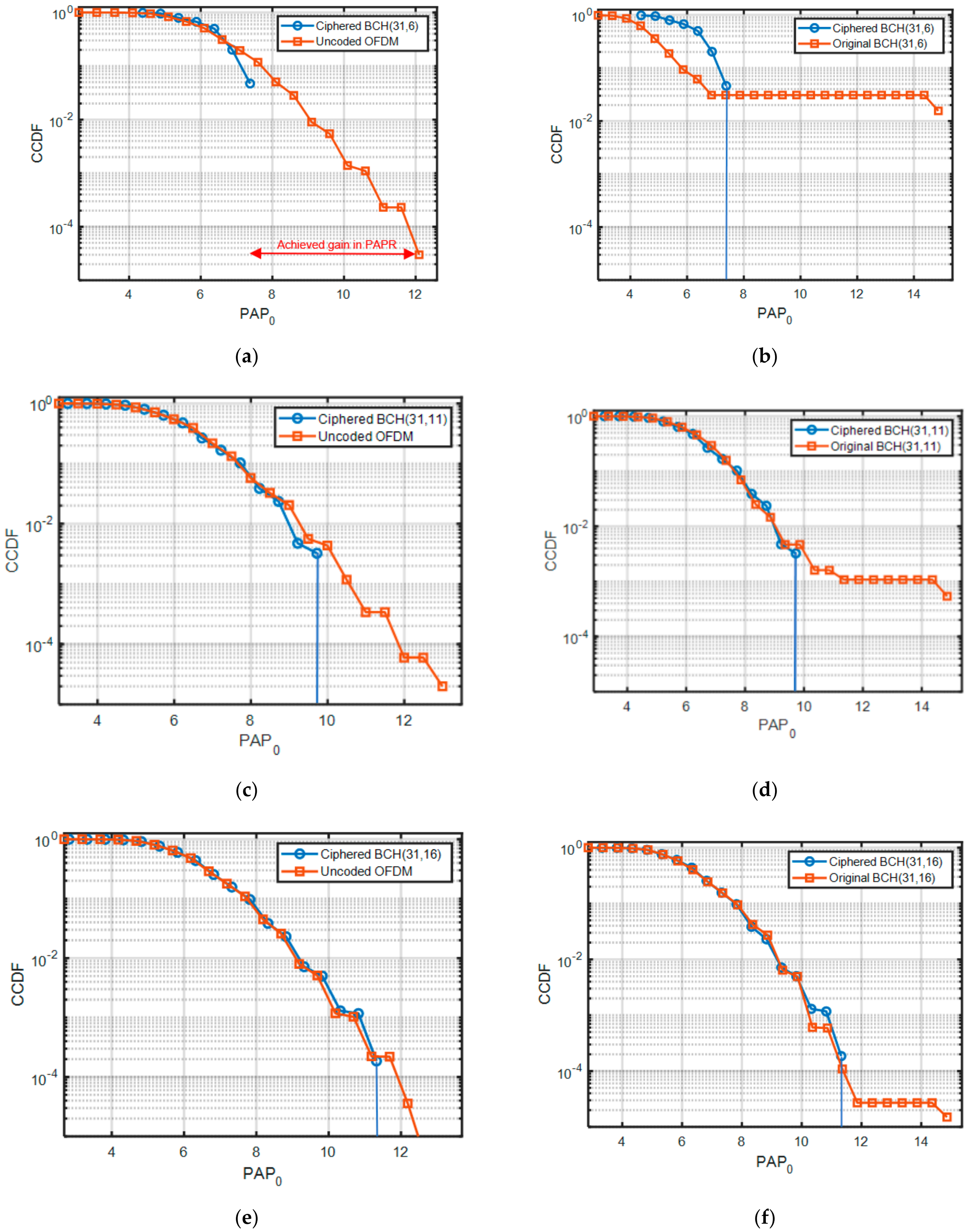
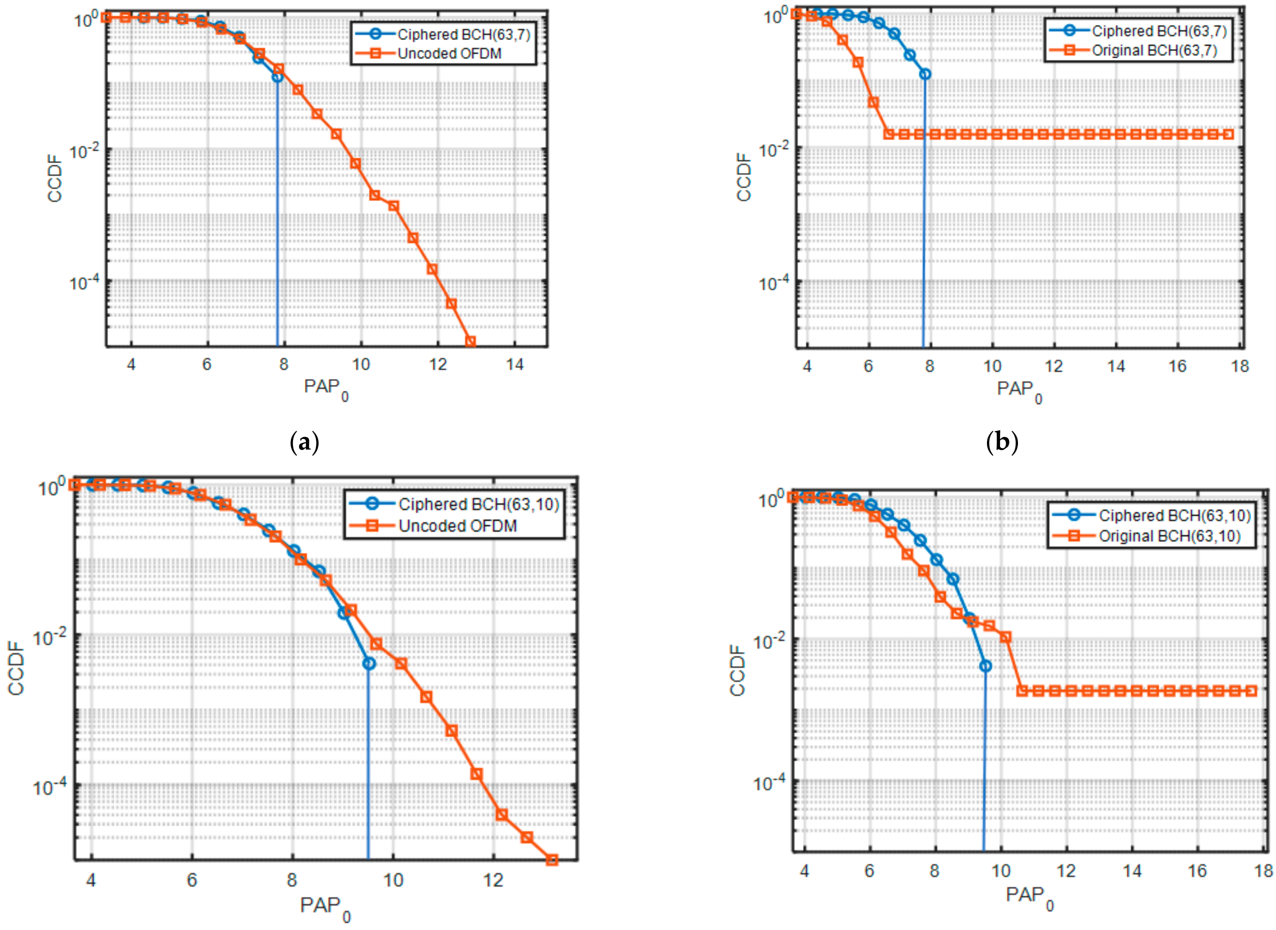


Figure 8. PAPR performance of the proposed technique for ciphered BCH(31,*k*) systems. (**a**) Ciphered BCH(31,6) vs uncoded OFDM, (**b**) Ciphered BCH(31,6) vs original BCH(31,6), (**c**) Ciphered BCH(31,11) vs uncoded OFDM, (**d**) Ciphered BCH(31,11) vs original BCH(31,11), (**e**) Ciphered BCH(31,16) vs uncoded OFDM and (**f**) Ciphered BCH(31,16) vs original BCH(31,16).

However, it must be noted that although there is not an appreciable gain in PAPR for the higher-rate ciphered BCH codes, their PAPR performances are still much better than the conventional BCH codes. As a result, the bit error rate performance is significantly improved without any deterioration in PAPR performance.

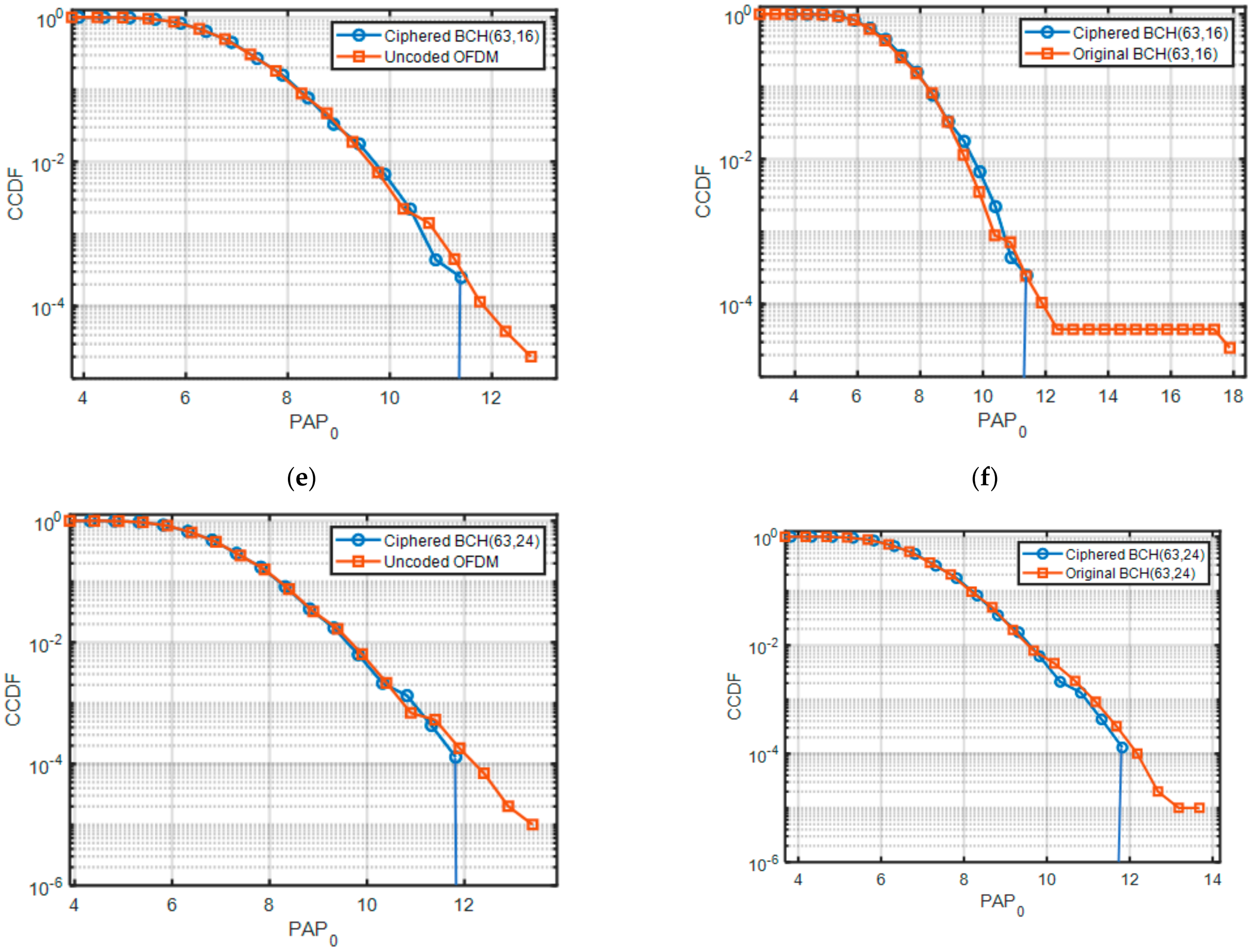
Figure 9 compares the PAPR performances of the proposed 64-subcarrier OFDM systems with uncoded and BCH-encoded OFDM systems using CCDF plots. Figure 9a,c,e compare the PAPR performances of ciphered BCH$(63, k)$ systems with those of uncoded systems, while Figure 9b,d,f compare the PAPR performances of ciphered BCH$(63, k)$ systems with those of BCH$(63, k)$ encoded systems. As shown in Figure 9a, the PAPR performance of the ciphered BCH$(31, 6)$ system was much superior to that of an uncoded OFDM system as it never exceeded about 8 dB, while that of uncoded scheme increased to about 13 dB. As shown in Figure 9b, when comparing the PAPR performance of the ciphered BCH$(63, 10)$ with that of the conventional BCH$(63, 10)$ system, it was observed that the PAPR of the conventional BCH$(63, 10)$ encoded system remained high with a high probability, unlike the uncoded OFDM system—a phenomenon that was also observed in the case of the 32-subcarrier system. A similar phenomenon is observed in Figure 9d. In this case also, the PAPR performance of the ciphered BCH codes for higher values of k was not at par with the systems where the value of k was small, as shown in Figure 9e,h.



(**a**) (**b**)

(**c**) (**d**)

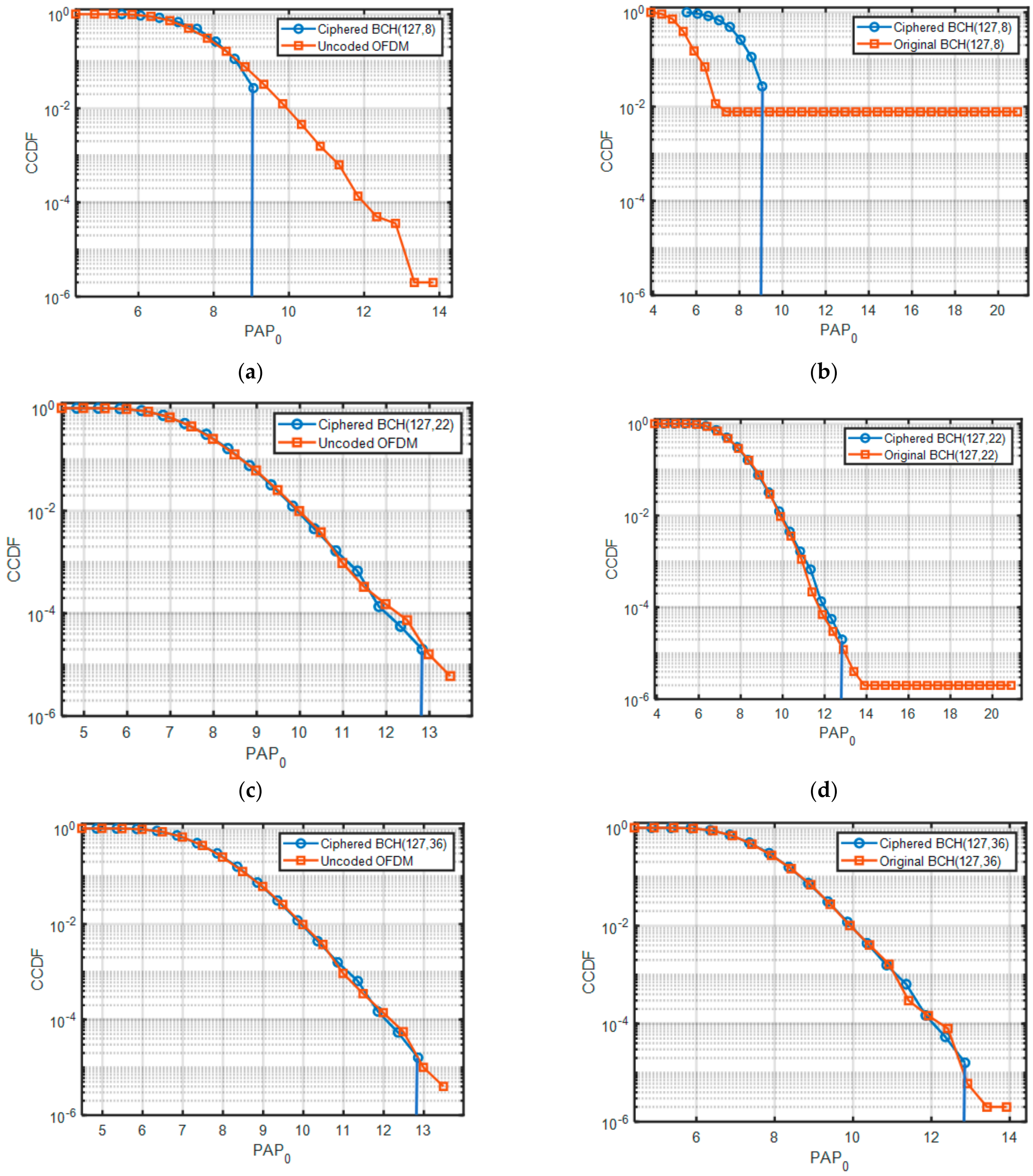
Figure 9. *Cont.*



(**e**) (**f**) (**g**) (**h**)

Figure 9. PAPR performance of the proposed technique for ciphered BCH(63,*k*) systems. (**a**) Ciphered BCH(63,7) vs uncoded OFDM, (**b**) Ciphered BCH(63,7) vs original BCH(63,7), (**c**) Ciphered BCH(63,10) vs uncoded OFDM, (**d**) Ciphered BCH(63,10) vs original BCH(63,10), (**e**) Ciphered BCH(63,16) vs uncoded, (**f**) Ciphered BCH(63,16) vs original BCH(63,16), (**g**) Ciphered BCH(63,24) vs uncodedand (**h**) Ciphered BCH(63,24) vs original BCH(63,24).

The PAPR performances of the 128-subcarrier OFDM systems are shown in Figure 10. It was observed that the PAPR performance of the proposed system was significantly better than the uncoded and BCH encoded OFDM systems for ciphered BCH$(127, 8)$ codes—as is shown in Figure 10a,b. However, for other codes, we did not observe an appreciable reduction in PAPR. The reason for this is the relatively large value of k. When the value of k is 22, 36 and 50, the space of possible key vectors becomes very large as the number of possible key vectors are 2^{22}, 2^{36} and 2^{50}, respectively. Hence, the problem of finding the best key vector becomes intractable.

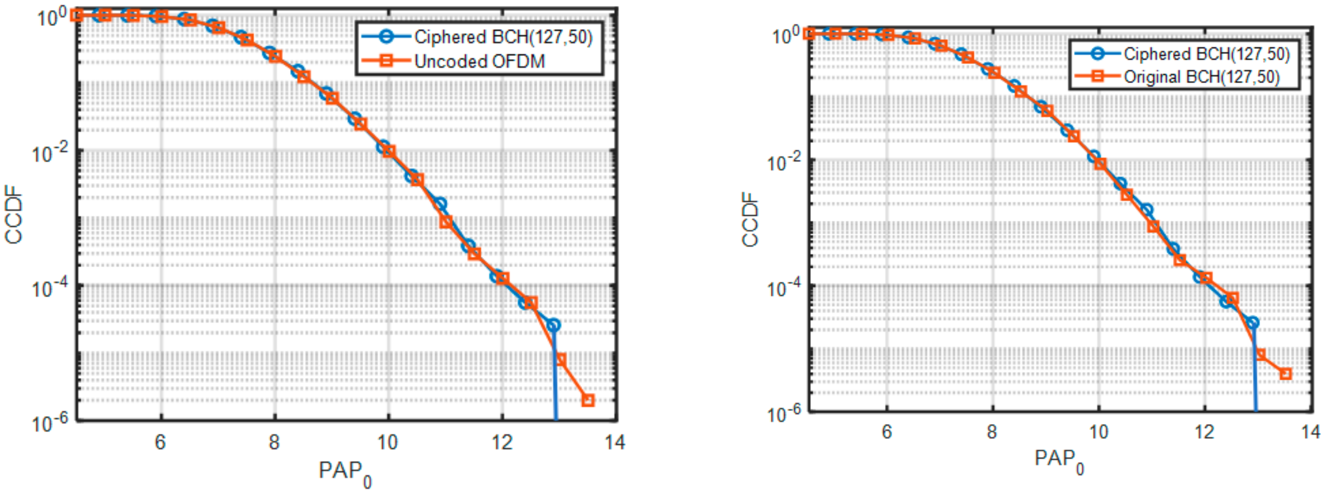


(**a**) (**b**)

(**c**) (**d**)

(**e**) (**f**)

Figure 10. *Cont.*

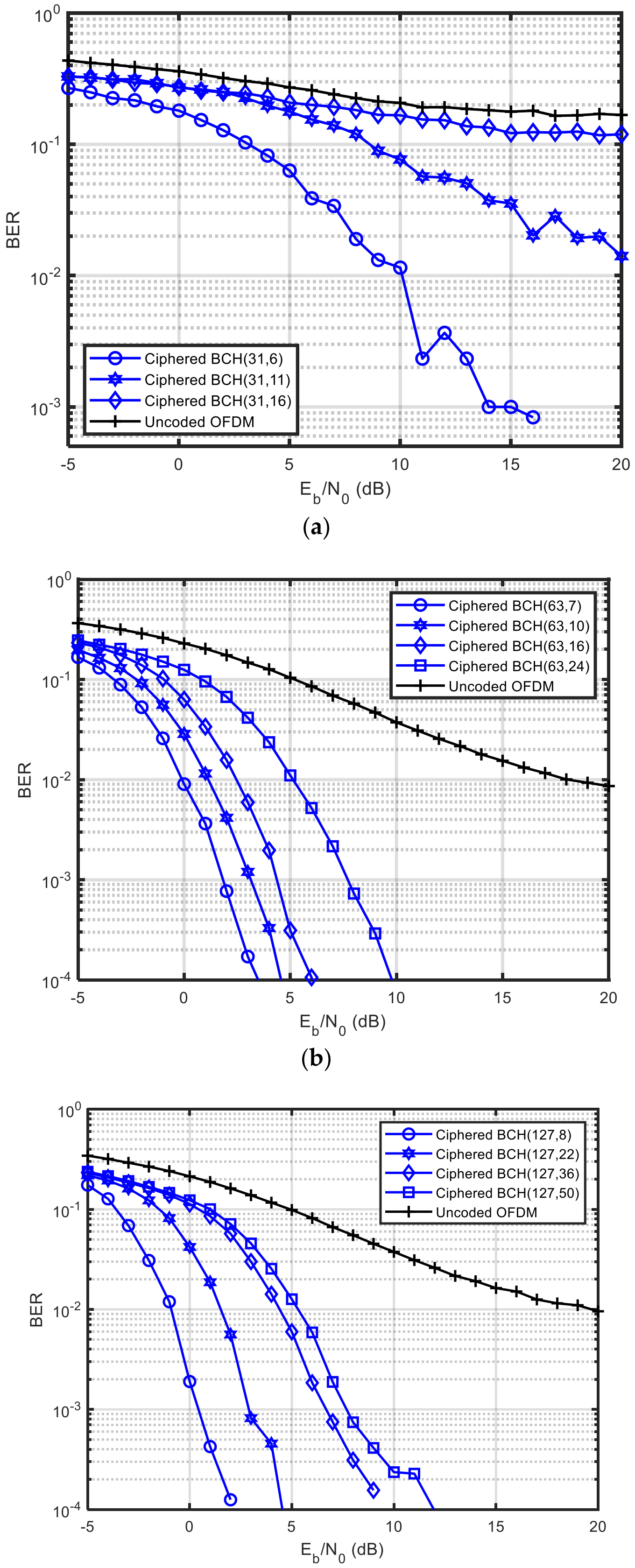


(**g**) (**h**)

Figure 10. PAPR performance of the proposed technique for ciphered BCH(127,*k*) systems. (**a**) Ciphered BCH(127,8) vs uncoded OFDM, (**b**) Ciphered BCH(127,8) vs original BCH(127,8), (**c**) Ciphered BCH(127,22) vs uncoded OFDM, (**d**) Ciphered BCH(127,22) vs original BCH(127,22), (**e**) Ciphered BCH(127,36) vs uncoded, (**f**) Ciphered BCH(127,36) vs original BCH(127,36), (**g**) Ciphered BCH(127,50) vs uncoded and (**h**) Ciphered BCH(127,50) vs original BCH(127,50).

5.2. BER Performance

In this section, we demonstrate the BER performance of the proposed ciphered BCH codes and show that the error correcting capability of the original BCH codes remains preserved for the proposed system. Figure 11 compares the BER performance of the proposed system against the ordinary uncoded OFDM for a transmitter–receiver distance of 1500 m. It was observed that all the ciphered BCH codes improved the BER performance of the OFDM system, as would be expected. It is pertinent to mention that the BER results for ciphered BCH codes having the lowest *k* values showed significant improvement; however, the overhead is too high, and these codes are ideal for scenarios where a very reliable transmission of low data-rate information is required. The channel state information was assumed to be known and used in the zero-forcing equalizer. For BCH$(31, k)$, the lowest BER values were associated with $k = 6$. For the same codes, we did not report *k* values higher than 16, as there was a very insignificant improvement in BER performance and PAPR reduction due to the lack of unused combinations at higher *k* values. This holds true for BCH$(63, k)$ and BCH$(127, k)$ as well.



(**a**)

(**b**)

(**c**)

Figure 11. BER performance of C-BCH(31,*k*), C-BCH(63,*k*) and C-BCH(127,*k*), (**a**) explanation, (**b**) explanation and (**c**) explanation.

6. Conclusions

We proposed a low complexity PAPR reduction technique for an underwater acoustic OFDM transceiver. It consists of multiple pre-determined cipher keys, generated using a high-end PC, that are used for XOR ciphering of the BCH-encoded and decoded data at the OFDM transmitter and receiver, respectively. Our findings suggest that while reducing PAPR, the ciphered BCH technique improves the BER performance of the system using channel coding. It is observed that a higher PAPR reduction and a lower BER is achieved when lower code rate BCH codes are used. Using multiple keys, known to both the transmitter and receiver, a level of encryption is achieved as an added advantage. Given the power and processing limitations of the underwater acoustic nodes, the proposed technique is easy to implement and reduces the computational complexity of the transceiver, as most of the processing for the key vector search is performed offline. The most appropriate keys generated are stored in both the transmitter and receiver and are used for ciphering purposes and to reduce the PAPR of the OFDM signal.

Author Contributions: M.M. and I.A.T. conceived the idea and designed the system. M.M. and I.A.T. implemented the model, ran the simulations and wrote the manuscript. P.O. conceived and designed the UWA channel model used and contributed to the discussion section. I.A.T. and P.O. reviewed the final version of the manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by a grant from the Spanish Ministry of Science and Innovation in the framework of the project "NAUTILUS: Swarms of underwater autonomous vehicles guided by artificial intelligence: its time has come" (PID2020-112502RB / AEI / 10.13039/501100011033).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors express their gratitude to the Escuela Técnica Superior de Ingeniería de Telecomunicación and the Instituto de Ingeniería Oceánica, Universidad de Málaga, Málaga, Spain. We would also like to thank College of Computer and Information Systems, Umm Al-Qura University, Makkah, Saudi Arabia.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Akyildiz, I.F.; Pompili, D.; Melodia, T. Challenges for Efficient Communication in Underwater Acoustic Sensor Networks. *ACM SIGBED Rev.* **2004**, *1*, 3–8. [CrossRef]
2. Stojanovic, M. Low Complexity OFDM Detector for Underwater Acoustic Channels. In *Proceedings of the OCEANS 2006, Boston, MA, USA, 18–21 September 2006*; IEEE: Piscataway, NJ, USA, 2006.
3. Stojanovic, M. Performance Analysis of Filtered Multitone Modulation Systems for Underwater Communication. In Proceedings of the OCEANS 2009, Biloxi, MS, USA, 26–29 October 2009.
4. Huang, J.; Zhou, S.; Willett, P. Nonbinary Ldpc Coding for Multicarrier Underwater Acoustic Communication. *IEEE J. Sel. Areas Commun.* **2008**, *26*, 1684–1696. [CrossRef]
5. Li, B.; Zhou, S.; Stojanovic, M.; Freitag, L.; Willet, P. Multicarrier Communication over Underwater Acoustic Channels with Nonuniform Doppler Shifts. *IEEE J. Ocean. Eng.* **2008**, *33*, 198–209.
6. Hwang, S.-J.; Schniter, P. Efficient Multicarrier Communication for Highly Spread Underwater Acoustic Channels. *IEEE J. Sel. Areas Commun.* **2008**, *26*, 1674–1683. [CrossRef]
7. Amini, P.; Chen, R.R.; Farhang-Boroujeny, B. Filterbank Multicarrier Communications for Underwater Acoustic Channels. *IEEE J. Ocean. Eng.* **2014**, *40*, 115–130. [CrossRef]
8. Zhu, P.; Xu, X.; Tu, X.; Chen, Y.; Tao, Y. Anti-Multipath Orthogonal Chirp Division Multiplexing for Underwater Acoustic Communication. *IEEE Access* **2020**, *8*, 13305–13314. [CrossRef]
9. Mason, S.; Anstett, R.; Anicette, N.; Zhou, S. A Broadband Underwater Acoustic Modem Implementation Using Coherent Ofdm. In Proceedings of the National Conference for Undergraduate Research (NCUR) 2007, San Rafael, CA, USA, 12–14 April 2007.
10. Wang, X.; Wang, X.; Jiang, R.; Wang, W.; Chen, Q.; Wang, X. Channel Modelling and Estimation for Shallow Underwater Acoustic Ofdm Communication Via Simulation Platform. *Appl. Sci.* **2019**, *9*, 447. [CrossRef]

11. Yonggang, W. Underwater Acoustic Channel Estimation for Pilot Based Ofdm. In Proceedings of the 2011 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC), Xi'an, China, 14–16 September 2011.
12. Li, B.; Huang, J.; Zhou, S.; Ball, K.; Stojanovic, M.; Freitag, L.; Willett, P. Mimo-Ofdm for High-Rate Underwater Acoustic Communications. *IEEE J. Ocean. Eng.* **2009**, *34*, 634–644.
13. Stojanovic, M. Ofdm for Underwater Acoustic Communications: Adaptive Synchronization and Sparse Channel Estimation. In Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing 2008 (ICASSP 2008), Las Vegas, NV, USA, 31 March–4 April 2008.
14. Han, S.H.; Lee, J.H. Papr Reduction of Ofdm Signals Using a Reduced Complexity Pts Technique. *IEEE Signal Process. Lett.* **2004**, *11*, 887–890. [CrossRef]
15. Jiang, T.; Yang, Y.; Song, Y.-H. Exponential Companding Technique for Papr Reduction in Ofdm Systems. *IEEE Trans. Broadcast.* **2005**, *51*, 244–248. [CrossRef]
16. Jiang, Y. New Companding Transform for Papr Reduction in Ofdm. *IEEE Commun. Lett.* **2010**, *14*, 282–284. [CrossRef]
17. Wong, K.T.; Wang, B.; Chen, J.-C. Ofdm Papr Reduction by Switching Null Subcarriers and Data-Subcarriers. *Electron. Lett.* **2011**, *47*, 62–63. [CrossRef]
18. Rahmatallah, Y.; Mohan, S. Peak-to-Average Power Ratio Reduction in Ofdm Systems: A Survey and Taxonomy. *IEEE Commun. Surv. Tutor.* **2013**, *15*, 1567–1592. [CrossRef]
19. Rojo, G.; Stojanovic, M. Peak-to-Average Power Ratio (Par) Reduction for Acoustic Ofdm Systems. In Proceedings of the OCEANS 2009, Biloxi, MS, USA, 26–29 October 2009.
20. Jawhar, Y.A.; Audah, L.; Taher, M.A.; Ramli, K.N.; Shah, N.S.M.; Musa, M.; Ahmed, M.S. A Review of Partial Transmit Sequence for Papr Reduction in the Ofdm Systems. *IEEE Access* **2019**, *7*, 18021–18041. [CrossRef]
21. Hanzo, L.; Steele, R.; Fortune, P.-M. A Subband Coding, Bch Coding, and 16-Qam System for Mobile Radio Speech Communications. *IEEE Trans. Veh. Technol.* **1990**, *39*, 327–339. [CrossRef]
22. Krasikov, I.; Litsyn, S. On Spectra of Bch Codes. *IEEE Trans. Inf. Theory* **1995**, *41*, 786–788. [CrossRef]
23. Kashani, Z.H.; Shiva, M. Bch Coding and Multi-Hop Communication in Wireless Sensor Networks. In Proceedings of the 2006 IFIP International Conference on Wireless and Optical Communications Networks, Bangalore, India, 11–13 April 2006.
24. Nagaraj, N.; Vaidya, V.; Vaidya, P.G. Re-Visiting the One-Time Pad. *arXiv* **2005**, arXiv:cs/0508079.
25. Kumar, P.; Kumar, P. Performance Evaluation of Dft-Spread Ofdm and Dct-Spread Ofdm for Underwater Acoustic Communication. In Proceedings of the 2012 IEEE Vehicular Technology Conference (VTC Fall), Quebec City, QC, Canada, 3–6 September 2012.
26. Wu, J.; Qiao, G.; Qi, X. The Research on Improved Companding Transformation for Reducing Papr in Underwater Acoustic Ofdm Communication System. *Discret. Dyn. Nat. Soc.* **2016**, *2016*, 3167483. [CrossRef]
27. Tao, J. Dft-Precoded Mimo Ofdm Underwater Acoustic Communications. *IEEE J. Ocean. Eng.* **2017**, *43*, 805–819. [CrossRef]
28. Gomathi, R.M.; Manickam, J.M.L. Papr Reduction Technique Using Combined Dct and Ldpc Based Ofdm System for Underwater Acoustic Communication. *ARPN J. Eng. Appl. Sci.* **2016**, *11*, 4424–4430.
29. Abd El-galil, M.S.; Soliman, N.F.; Abdalla, M.I.; Elaskily, M.A.; Abd El-Samie, F.E. Tanhr Nonlinear Companding Scheme for Uwa System. *Int. J. Electron. Lett.* **2020**, 1–7. [CrossRef]
30. Xing, S.; Qiao, G.; Ma, L. A Blind Side Information Detection Method for Partial Transmitted Sequence Peak-to-Average Power Reduction Scheme in Ofdm Underwater Acoustic Communication System. *IEEE Access* **2018**, *6*, 24128–24136. [CrossRef]
31. Han, J.; Ma, S.; Wang, Y.; Leus, G. Low-Complexity Equalization of Mimo-Osdm. *IEEE Trans. Veh. Technol.* **2019**, *69*, 2301–2305. [CrossRef]
32. Qasem, Z.A.; Leftah, H.A.; Sun, H.; Qi, J.; Esmaiel, H. X-Transform Time-Domain Synchronous Im-Ofdm-Ss for Underwater Acoustic Communication. *IEEE Syst. J.* **2021**, 1–12. [CrossRef]
33. Jiang, T.; Zhu, G.; Zheng, J. Block Coding Scheme for Reducing Papr in Ofdm Systems with Large Number of Subcarriers. *J. Electron.* **2004**, *21*, 482–489.
34. Jiang, T.; Zhu, G. Complement Block Coding for Reduction in Peak-to-Average Power Ratio of Ofdm Signals. *IEEE Commun. Mag.* **2005**, *43*, S17–S22. [CrossRef]
35. Ghassemi, A.; Gulliver, T.A. Papr Reduction of Ofdm Using Pts and Error-Correcting Code Subblocking-Transactions Papers. *IEEE Trans. Wirel. Commun.* **2010**, *9*, 980–989. [CrossRef]
36. Yang, K.; Chang, S.-I. Peak-to-Average Power Control in Ofdm Using Standard Arrays of Linear Block Codes. *IEEE Commun. Lett.* **2003**, *7*, 174–176. [CrossRef]
37. Jones, A.E.; Wilkinson, T.A.; Barton, S.K. Block Coding Scheme for Reduction of Peak to Mean Envelope Power Ratio of Multicarrier Transmission Schemes. *Electron. Lett.* **1994**, *30*, 2098–2099. [CrossRef]
38. Tasadduq, I.A.; Rao, R.K. Weighted Ofdm with Block Codes for Wireless Communication. In Proceedings of the 2001 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (IEEE Cat. No. 01CH37233), Victoria, BC, Canada, 26–28 August 2001.
39. Carrascosa, P.C.; Stojanovic, M. Adaptive Channel Estimation and Data Detection for Underwater Acoustic Mimo–Ofdm Systems. *IEEE J. Ocean. Eng.* **2010**, *35*, 635–646. [CrossRef]
40. Kim, J.; Cho, Y.-H.; Ko, H.; Im, T. Performance Comparison of Short-Length Error-Correcting Codes in an Underwater Ofdm Systems. In Proceedings of the 2019 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Korea, 16–18 October 2019.

41. Porter, M. Bellhop Code. Available online: http://oalib.hlsresearch.com/AcousticsToolbox/ (accessed on 1 December 2021).
42. Tutte, W.T. Fish and I. In *Coding Theory and Cryptography*; Springer: Berlin, Germany, 2000; pp. 9–17.
43. Huo, F.; Gong, G. Xor Encryption Versus Phase Encryption, an in-Depth Analysis. *IEEE Trans. Electromagn. Compat.* **2015**, *57*, 903–911. [CrossRef]
44. Gligoroski, D.; Knapskog, S.J.; Andova, S. Cryptcoding-Encryption and Error-Correction Coding in a Single Step. In Proceedings of the International Conference on Security and Management, Las Vegas, NV, USA, 26–29 June 2006.
45. Murad, M.; Tasadduq, I.A.; Otero, P.; Poncela, J. Flexible Ofdm Transceiver for Underwater Acoustic Channel: Modeling, Implementation and Parameter Tuning. *Wirel. Pers. Commun.* **2020**, *116*, 1423–1441. [CrossRef]
46. Tasadduq, I.A.; Murad, M.; Otero, P. Cpm-Ofdm Performance over Underwater Acoustic Channels. *J. Mar. Sci. Eng.* **2021**, *9*, 1104. [CrossRef]
47. Liu, C.; Zakharov, Y.V.; Chen, T. Doubly Selective Underwater Acoustic Channel Model for a Moving Transmitter/Receiver. *IEEE Trans. Veh. Technol.* **2012**, *61*, 938–950.
48. Wang, X.; Wang, J.; He, L.; Song, J. Doubly Selective Underwater Acoustic Channel Estimation with Basis Expansion Model. In Proceedings of the 2017 IEEE International Conference on Communications (ICC), Paris, France, 21–25 May 2017.
49. Bocus, M.J.; Agrafiotis, D.; Doufexi, A. Underwater Acoustic Video Transmission Using Mimo-Fbmc. In Proceedings of the 2018 OCEANS-MTS/IEEE Kobe Techno-Oceans (OTO), Kobe, Japan, 28–31 May 2018.
50. Stojanovic, M. Underwater Acoustic Communications: Design Considerations on the Physical Layer. In Proceedings of the 5th Annual Conference on Wireless on Demand Network Systems and Services, Garmisch-Partenkirchen, Germany, 23–25 January 2008.
51. Wan, L. Underwater Acoustic Ofdm: Algorithm Design, Dsp Implementation, and Field Performance. Ph.D. Thesis, University of Connecticut, Mansfield, CT, USA, 2014.
52. Murad, M.; Tasadduq, I.A.; Otero, P. Towards Multicarrier Waveforms Beyond Ofdm: Performance Analysis of Gfdm Modulation for Underwater Acoustic Channels. *IEEE Access* **2020**, *8*, 222782–222799. [CrossRef]
53. Morse, P.M.; Ingard, K.U. *Theoretical Acoustics*; Princeton University Press: Princeton, NJ, USA, 1986.
54. Otero, P. *Fundamentos de Propagación de Ondas*; Universidad de Malaga: Malaga, Spain, 2015.
55. Kulhandjian, H.; Melodia, T. Modeling Underwater Acoustic Channels in Short-Range Shallow Water Environments. In Proceedings of the International Conference on Underwater Networks & Systems, Rome, Italy, 12–14 November 2014.
56. Ruiz-Vega, F.; Clemente, M.C.; Otero, P.; Paris, J.F. Ricean Shadowed Statistical Characterization of Shallow Water Acoustic Channels for Wireless Communications. *arXiv* **2011**, arXiv:1112.4410.
57. Radosevic, A.; Proakis, J.G.; Stojanovic, M. Statistical Characterization and Capacity of Shallow Water Acoustic Channels. In Proceedings of the OCEANS 2009—EUROPE, Bremen, Germany, 11–14 May 2009.
58. Jeruchim, M.; Balaban, P.; Shanmugan, K.S. *Simulation of Communication Systems*, 2nd ed.; Kluwer Academic/Plenum: New York, NY, USA, 2000.
59. Stojanovic, M. On the Relationship between Capacity and Distance in an Underwater Acoustic Communication Channel. *ACM SIGMOBILE Mob. Comput. Commun. Rev.* **2007**, *11*, 34–43. [CrossRef]
60. Hebbar, R.P.; Poddar, P.G. Generalized Frequency Division Multiplexing–Based Acoustic Communication for Underwater Systems. *Int. J. Commun. Syst.* **2020**, *33*, e4292. [CrossRef]
61. Hasan, M.M. VLM Precoded SLM Technique for PAPR Reduction in OFDM Systems. *Wirel. Pers. Commun.* **2013**, *73*, 791–801. [CrossRef]