Acta Scientific COMPUTER SCIENCES

Volume 4 Issue 11 November 2022

Research Article

# Li-Fi and BM-XOR: The Solution Based on Error Correcting Codes

**Hamada Louiza[1]*, Lorenz Pascal[1] and Djerouni Aicha[2]**

[1]*IRIMAS Institute, University of Haute Alsace, France*

[2]*LARESI Laboratory, University of Sciences and Technology of Oran, Algeria*

***Corresponding Author:** Hamada Louiza, IRIMAS Institute, University of Haute Alsace, France.

**Received:** September 29, 2022

**Published:** October 31, 2022



## Abstract

Li-Fi (Light Fidelity) is the transmission of data by visible light (VLC), an alternative to Wi-Fi (Wireless Fidelity), the idea is to set up a system with the aim of e-health in hospitals, with the health crisis of COVID, it has been obligatory at present to take in hand the patients, it is known that the electromagnetic transmission that can generate Wi-Fi can be harmful for the patients, and can even generate interference that can distort the medical report of patients, the Li-fi uses light waves for data transmission, hence the absence of interference and noise [1], which is an advantage of using Li-Fi in indoor environments. In this article, we will make an introduction to the Li-Fi system,we will present a comparison between Li-Fi and Wi-Fi, we will also talk about our system that allows to send a confidential message through the light signal of Li-Fi in full safety without that this last one is decrypted by a malicious person in the part of future works and contribution, and finally a general conclusion of this article.

**Keywords:** Li-Fi; Wi-Fi; OTP; Reed Solomon; Berlekamp-Massey; BM-XOR

## Abbreviations

BM: Berlekanp Massey; BM-XOR: Berlekamp Massey-xor; LED: Light Emitting Diode; LFSR: Linear Feedback Shifting Register; LOS: Line of Sight; Li-Fi: Light Fidelity; NLOS: Non Line of Sight; OOK: On-off Keying; OTP: One Time Pad; SNR: Signal to Noise Ratio; VLC: Visible Light Communication; Wi-Fi: Wireless Fidelity

## Introduction

Many advanced solutions and techniques [2] are envisaged in future standards (5G) to cope with the increase in connectivity while attempting to limit the cost of energy and, indirectly, the carbon impact. Another option for overcoming the issues is to apply complementary technology to radio frequencies above 300 GHz. This is the field of wireless optics.

Li-Fi allows an electronic device to connect to the Internet wirelessly [3]. A Li-Fi system will require a transceiver to transmit and receive data in order to establish a communication line between the nodes [4]. This transmitter will include a modulation technique that will allow the LED to carry data using light. The emergence of Li-Fi is intended to address current technology shortages [5,6].

In recent years, network security has become a major issue. To begin, there is the requirement to maintain data secret for that only authorized parts have access, as well as to protect data sent through the network, which may include the backup of files or/ and passwords stored on computers that are connected online, in addition to gainingaccess to computer applications and resources [7]. One of the solutions to this issue includes the requirement for users to use keys to log in to their machines, password protect important documents and automatically identify their emails. There have been numerous studies on security in a variety of areas, including physical, Medium Access Control layers, topologies, internal and external communications, co-channel interference, and many others. Although, research on security issues in light

fidelity communications has primarily been based on individual attacks [7].

## Li-Fi vs Wi-Fi

Table 1 presents a brief comparison between Li-Fi and Wi-Fi. The Li-Fi is today a significantly adapted technology to indoor environments thanks to its advantages related to the security of a computer network.

| | **Li-Fi (Light Fidelity)** | **Wi-Fi (Wireless Fidelity)** |
|---|---|---|
| Standard | IEEE 802.15.xx | IEEE 802.11.xx |
| Available spectrum | 380 THz | 300GHz |
| Operations | Li-Fi uses LED bulbs to transmit data through light. | Wi-Fi transmits the data via electromagnetic radiation with the assistance of a Wi-Fi router. |
| Bandwidth | Not limited. | Limited. |
| Topology | Point-to-point. | Point-to-multi points. |
| Electromagnetic interferences | No. | Yes |
| Density of data | Works in a very denseenviron-ment. | Works in a less dense environment due to problems related to interferences. |
| Coverage | About 10 mètres. | Approximately 32 meters (WLAN 802.11b/11g), varies depending on the transmission. |
| System composants | The lamp driver, LED bulband photo detector. | Requires the installation ofrouters, users' devices (laptops, PDAs, etc.). |
| Applications | Theaters, hospitals, airplanesplanes, offices... | Browsing the internet withusing Wi-Fi access points. |
| Security | It is safer because the wavesof light can not pass through walls and cannot be and picked up by anyoneoutside the LED lighting. | Due to the enormous scattering force of the radiowaves, anyone on the road can intercept them. |
| Cost | Low | Higher |
| Modulation | DCO-OFDM | Direct Sequence Spread Spectrum (DSSS) |
| Architecture | AttoCell | FemtoCell |

**Table 1:** An Comparison between Li-Fi and Wi-Fi.

## Li-Fi system

A Li-Fi system comprises three parts: the VLC transmitter that uses visible light wavesto send data over a wireless transmission channel.

The receiver is represented by the photodiode which transforms the light signal into an electrical signal, and finally, the transmission channel, where (02) types of propagation: direct propagation (LOS), and indirect propagation (NLOS) (Figure 1).

**Figure 1:** Li-Fi block diagram.

The continuous-time model "y = h * H(x) + w" can describe the noisy communication link (vlc), where y(t) shows the incoming signal, which is a distorted replica of the emitted signal, x(t), which is subjected to the transmitter front-non-linear end's distortion function, H(x(t)). The transmitted non-linearly distorted signal is convolved with the channel's impulse response, h(t), and contorted by additive Gaussian noise (AWGN) at the receiver, w(t), that includes shot and thermal noise. In this case, "*" stands for the linear convolution.

Because we use on-off keying (OOK) modulation for data transmission, we can express the received SNR ($SNR_{rx}$) as follows [8].

$$SNR_{rx} = \frac{(R.P_{rSignal})^2}{\sigma^2_{shot} + \sigma^2_{thermal} + (R.P_{rISI})^2}$$

Where $P_{rSignal} (= \int_0^T x(t) * h(t)dt)$ is the signal power, $P_{rISI} (= \int_T^{\infty} x(t) * h(t)dt)$ is the received power because of inter-symbol interference. A variance of the shot noise is given as $\sigma^2_{shot} = 2qi_{pc} + 2qB_{pd}RP_{bg}$ where q is the electronic charge, $i_{pc}$ denotes the photocurrent and we have $i_{pc}=RP_{LED}$, where R is the photodiode response and $P_{LED}$ is the light source power and $B_{pd}$ is the electrical bandwidth of the photodiode. In addition, the thermal noise variance is also expressed as $\sigma^2_{thermal} = \frac{}{R_F}$ where $R_F$ is the resistance [8-10].

## Materials and Methods

What we are trying to do is a two-factor authentication using the OTP protocol. The OTP is only valid for a single session or transaction. OTPs address some shortcomings associated with traditional static passwords, such as vulnerability to replay attacks. This means that if a potential intruder saves the OTP that has already been used to log into a service or perform a transaction, they cannot use it because it will no longer be valid. Humans cannot store OTPs, so they require additional technologies to be used. The user will have a one-time key which will be stored in a database; he cannot provide the same password the next time he logs in. Every time a key is generated, it will be automatically stored in a database.

In another way, our idea is to propose a reliable authentication system within hospitals, based on LED modulation. A user (transmitter) will indicate his ID and password, and the password sent by the sender will be coded thanks to the Berlekamp- Massey algorithm. This algorithmic rule is an alternative to the RS error correcting codes, which consist in the first step to construct the consecutive values of N, associate degree of linear shifting register of length L*N and $f_N$ the polynomial feedback that generates the primary N bits of the sequences. The sequences sent (coded) ought to be a multiple of the polynomial S(x) well-known earlier by the transmitter and receiver because of the generator polynomial. To get the code from the transmitted message that's identical in size because it, every message should have its proper key; we should not have two completely different messages with identical key.

Once authenticated, the recipient can obtain the message that is encoded, moreover, the code to decipher the message; for the second authentication, the user can receive a cryptogram on his phone [11].

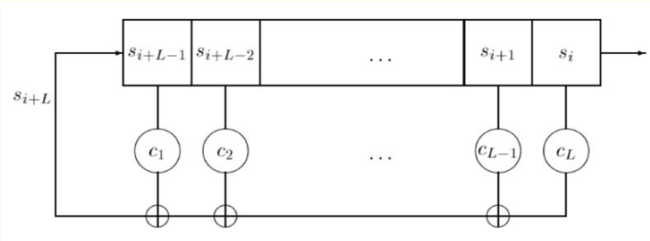


**Figure 2:** One LFSR of length L.

S(x), the generator polynomial, known in advance at the transmitter and the receiver will be written according to the sent (coded) sequences. The algorithm returns the return polynomial of the starting LFSR if N = 2L.

**Algorithm I** Berlekamp-Massey

**Input:** $s_0; s_1; \ldots; s_{N-1}$

**Output:** LFSR of length n = N/2

$f(x) = 1 + c_1x + c_2x^2 + \ldots + c_nx^n$

**Initialisation:** f(x)=1; m=-1; L=0; g(x)=1;

For N = 0 to n-1

calculer $d = s_N + \sum_{i=1}^{L} C_i S_{N-i} \bmod 2$

If d = 1 do

t(x) = f(x)

$f(x) = f(x) + g(x) * x^{N-m}$

If $2L \leq N$ then L=N+1-L, m = N, g(x)=t(x)

As already aforementioned, the target of the algorithm of BM is to seek out the minimum level of errors (L) and f(x) that ends up in all the syndromes $S_n+C_1S_{n-1}+ \ldots +C_LS_{n-L}$, at every iteration, the formula calculates the worth d. once d = zero implies that f(x), L area unit correct, we tend to rise m and continue. In case where d # 0, the formula continues to run and recalculates anytime f(x) up to d=0 [11]. The formula should conjointly scale back the quantity of "L" errors. If "L" is up to the present error range, N becomes larger than or up to 2L after that the deviation throughout

the method of iteration becomes zero. Or, the formula calculates the updated worth of L and g(x), overwrite L, and place "m equal to 1". N+1-L = L indicates the number of syndromes thatare ready to be calculated and therefore able to correct the errors and jointly manage the case where L decreases by more than one unit [11].

The name Berlekamp Massey-XOR has been assigned to our new approach, the idea of proposing this algorithm is to ensure data confidentiality and authentication of the people authorized to access the network. We modified the Berlekamp-Massey algorithm and subsequently proposed a method for encoding, decoding, and correcting the transmission errors of data sent through Li-Fi.

The modification made consists in adding a "k" variable. We use this variable to decode our sent message via the signal of light. We select "k" from prime numbers and must be different from 1.

**Algorithm II** Berlekamp Massey-XOR
**Input:** $\{s_0,s_1,\ldots,s_{N-1}\}$ a sequence of bits of N length
**Output:** LFSR of length n = N/2 (construction of f(x)) ; $f(x) = 1 + c_1x + c_2x^2 + \ldots\ldots + c_nx^n$ (to find) ; d'
**Initialization:** f(x)=1; m=-1; L=0; g(x)=1;
Read k; //k must be a prime number different from 1;
For N = 0 → n-1
  $d' = s_N + \sum_{i=1}^{L} c_i s_{N-i} \bmod k$
  If d=1 do {
    t(x) = f(x)
    g(x) = f(x)+g(x). xN-m
    If 2L ≤ N then L=N+1-L, m = N, g(x)=t(x) }
  Else If d!=0 && d!=1
    { if k mod d = 1 do {
      t(x) = f(x)
      g(x) = f(x)+g(x). xN-m
      If 2L ≤ N then L=N+1-L, m = N, g(x)=t(x) }
    }

At each iteration, the algorithm calculates the value of d', at the end of the algorithm, we will consider the sequence of different values of d' as the encryption and decryption key for each message. The key is generated from the message sent and the value of k. Each message will be the same size as this one, and a key for each message also two different messages with the same key do not exist.

## Results and Discussion

The encoding is done at the transmitter level, we encode the information sent through the signal to prevent any unauthorized user to access the confidential data.

As we have already mentioned, the objective of our study is to modify the BM algorithm for encoding and decoding operations and to propose an algorithm to correct transmission errors. We will apply the Berlekamp-Massey XOR (BM-XOR) algorithm on an example (Table 2).

We unroll BM-XOR to have the value of d'. The sequence of the various values of d' constitute the encryption and decryption key.

| N | $S_N$ | D | L | f(X) | M | g(X) |
|---|---|---|---|---|---|---|
| | | | 0 | 1 | -1 | 1 |
| 0 | 1 | 1 | 1 | 1 + X | 0 | 1 |
| 1 | 1 | 2 | 1 | 1 + X | 0 | 1 |
| 2 | 0 | 1 | 2 | $1 + X + X^2$ | 2 | 1+X |
| 3 | 0 | 1 | 2 | 1 | 2 | 1+X |
| 4 | 1 | 1 | 3 | $1 + X^2 + X3$ | 2 | 1 |

**Table 2:** Application of the BM-XOR algorithm to the binary sequence s = 11001 oflength 5 and k = 3.

The polynomial $1 + X^2 + X^3$ is the LFSR (feedback polynomial) of length 3 that generatesthe given sequence.

The encoding operation consists in the application of an XOR (or logic) among theelements of the array as follows: s ⊕ f(X) ⊕ d' (3 bits) ⊕ k: [1 1 0 0 1] ⊕ [1 0 1 1 0] ⊕

[1 0 1 0 1] ⊕ [1 1 0 0 0] = [0 0 0 1 0] ➔p(x).

The elements of the array are converted to binary:

- "s" is the message to be sent in binary: 11001 on 5 bits, all that will follow will be converted into binary on 5 bits too and according to the size of the message to besent.
- f(x) is the feedback polynomial that we will write in binary as follows: $f(x) = 1 + X^2 + X^3$ ➔ 10110.
- k is a prime number different from 1: k = 3 = 11000.
- d is the encryption key: the complexity is at this level, with BM-XOR we can have values of d' that are not in binary (0 and 1), what we will do in this case, is to convert only the values that are different from 0 and 1: d' = 12111 = 10101. As indicated, one converted (2) on three bits which gives (010), and the other bits of 1 are present it is enough just to take into account the size of the message (5 bits).

We can show that for k (decimal) = d' (in binary) i.e. if k=5 one figures d' on 5 bits the algorithm remains right.

The second step of our approach is the decoding of the information. Decoding is done at the receiver, to decode a message, once again we will apply an XOR between the encoded message p(x) and d' and k as follows: p(x) ⊕ d' (3 bits) ⊕ k : [0 0 0 1 0] ⊕ [1 0

1 0 1] ⊕ [1 1 1 0 0 0] = [0 1 1 1 1] ➔ p'(x).

We will keep the same reasoning as the encoding for the value of d'. As indicated the decrypted message p'(x) contains errors, we will proceed this time to error correction. The communication through a Li-Fi network between a transmitter and a receiver generates transmission errors, the advantage of our algorithm (BM-XOR) is to have secure communication at the level of the Li-Fi network, it allows at the same time to encrypt a message to decrypt it and to correct the transmission errors that are produced. Another advantage of the BM-XOR algorithm is the absence of redundancies in the message transmitted through the signal, unlike Reed Solomon.

Error correction is done at the receiver as well and will be done by applying an XOR betweenthe decoded message p'(x) and the feedback polynomial f(x) as follows: s = p'(x) ⊕ f(x) = [01 1 1 1] ⊕ [1 0 1 1 0] = [1 1 0 0 1].

Figures 3 and 4 is a simulations of the error rate on bits (BER) vs Eb/N0, according to Reed Solomon and BM-XOR, we have an error rate much lower than the error rate of RS,see the constant for certain codes (63,47), this presents an advantage of more for the use of BM-XOR.

**Figure 3:** Performance of the Reed Solomon code.

**Figure 4:** BM-XOR code performance. (a) BM-XOR(15,13); (b) BM-XOR(63,47) and BM- XOR(15,11).

A two-factor authentication architecture/scenario has also been proposed (Figure 5).

**Figure 5:** Two-factor authentication scenario.

In the first time, the customer sends a request of authentication (1); then he sends the MAC address of his machine + MDP generated superimposed to a coded light signal emitted by this one (2); the server will decode/demodulate the received signal to recover the MAC address and the password of the customer (3); then the server will check if the MAC address belongs to this network (4) and sends in its turn a SMS which contains a secret code for the 2nd authentication (5). The client will retrieve the secret code and enter it (6) to succeed in the authentication (7).

## Conclusion

This article presents a novel approach combining OTP and Li-Fi which consists of securing our system safer, especially in light of the worldwide medical crisis. Our focusis to develop our idea in all hospitals in France and to have a positive result for our approach.

The advantage of the BM-XOR algorithm is the non-existence of redundancies that can generate RS, we can choose codes up to $2^b$=N and/or K. We note RS(N,K), with N is the bits number of the code-word that represents the message received with error and K is the bits number of the information word which represents the message received without error. For these two parameters, we will define two other variables: m which defines the length of the symbols with $2^{m-1}$ = N; and t is the maximum number of correctable symbols $2^t$ = N-K.

A few technical limitations must be addressed in order to realize the full potential ofVLC technology; channel models for VLC are limited, particularly for outdoor non-line ofsight (NLOS) environments; and channel models and platforms for VLC are actively researched [12]. Another challenge that the lighting industry must help with is the networking of light sources and upgrading current infrastructure to support communication.

## Bibliography

1. Hamada L., and Lorenz P. "Li-Fi: A Revolution in Wireless Networking for Smart Communication Through Illumination". *Acta Scientific Computer Sciences* 3.10 (2021): 53-58.

2. Wang CX., *et al*. "Cellular architecture and key technologies for 5G wireless communication networks". *IEEE Communications Magazine* 2.52 (2014): 122-130.

3. Ayyash M., *et al*. "Coexistence of WiFi and LiFi toward 5G: Concepts, opportunities, and challenges". *IEEE Communications Magazine* 2.54 (2016): 64-71.

4. Ramadhani E and Mahardika GP. "The Technology of LiFi: A brief Introduction". IOP Publishing, ICITDA (2017).

5. Lorenz P and Hamada L. "LiFi Towards 5G: Concepts, Challenges, Applications in Telemedicine". EasyChair Preprints, August (2020).

6. Haas H. "LiFi is a paradigm-shifting 5G technology". *Reviews in Physics* 3 (2017): 26-31.

7. Farrel A. "The Internet and Its Protocols: A Comparative Approach". Morgan Kaufmann Publishers In (2004): Chapter 14, 677-681.

8. Kim S and Jung S-Y. "Modified Reed-Muller Coding Scheme Made from the Bent Function for Dimmable Visible Light Communications". *IEEE Photonics Technology Letters* 1.25 (2013).

9. Dimitrov S., *et al*. "On the SIR of a Cellular Infrared Optical Wireless System for an Aircraft". *IEEE Journal on Selected Areas in Communications* 9.27 (2009): 1623-1638.

10. Haas H., *et al*. "Introduction to indoor networking concepts and challenges in LiFi". *IEEE/OSA Journal of Optical Communications and Networking* 2.12 (2020): A190- A203.

11. https://en.wikipedia.org/wiki/Berlekamp-Massey-algorithm

12. Z Zhang., *et al*. "Physical layer security in light-fidelity systems". *Philosophical Transactions of the Royal Society A* 378 (2020): 20190193.