A Low Complexity Joint Encryption-Modulation Method for IoT Sensor Transceivers

Dai Long Hoang, Thi Hong Tran and Yasuhiko Nakashima

Graduate School of Information Science, Nara Institute of Science and Technology, Takayama 8916-5, Ikoma, Nara 630-0192, Japan; hoang.long.hg7@is.naist.jp (D.L.H.); nakashim@is.naist.jp (Y.N.)

* Correspondence: hong@is.naist.jp

Received: 2 April 2020; Accepted: 16 April 2020; Published: 19 April 2020

Abstract: Physical layer encryption (PLE) is a new research trend for securing data in communication systems. However, conventional procedures in works on PLE are of high complexity and degrade the packet error rate (PER) performance of the system. They are therefore not yet suitable for IoT sensors’ transceiver, which has limited power and computational resource. In this paper, we propose a low complexity PLE method named as joint encryption-modulation (JEM) for small transceivers such as IoT sensors. In our JEM method, data is encrypted after modulation to preserve high security. Our JEM method does not make change the constellation of the modulation after encryption; therefore, the encryption does not degrade PER performance of the system as the conventional works do. Furthermore, the encryption is performed by XOR gates and multiplexers only. It is, therefore, low complexity. Our experiment results show that the JEM method improves about 3 dB of PER performance as compared with that of conventional works. JEM method can support multiple modulation types such as BPSK, QPSK, 16-256 QAM within a small hardware cost. Compared with conventional works, JEM’s hardware resource is reduced by 87.5% in terms of FPGA synthesis and 86.5% in terms of the ASIC circuit. ASIC static power consumption of JEM is reduced by 80.6%.

Keywords: IoT transceiver; PHY circuit; physical layer encryption; hardware encryption; high order modulation; lightweight stream cipher

1. Introduction

In recent times, the concept of the Internet of Things (IoT) has become very popular and plays a crucial role in numerous applications such as smart cities, smart grid, and smart healthcare [1]. It has been demonstrated that IoT applications rely on wireless connections, which are vulnerable to eavesdropping attacks and active jammings [2]. Notably, in IoT sensor networks that require high-security such as health monitoring and military surveillance, the collected data are private and confidential. Therefore, improving the security of these connections to protect users and data from attackers is important.

In wireless communication systems, the framework of security is provided in different protocol layers and can be classified into two main approaches: information-theoretic security and computational security. The former one is executed by physical layer security (PLS) techniques at the physical (PHY) layer, and the latter is a cryptography approach that performs the encryption and decryption at different layers, such as medium access control (MAC), and PHY [3].

PLS, a well-known security approach at the PHY layer, aims to achieve information-theoretic security by exploiting channel characteristics [4,5]. PLS methods can secure the system by generating artificial noise [6–8], creating beamforming [9–11], or utilizing cooperative relay [12,13]. Although PLS brings some advantages such as flexible security level configurations, QoS guarantee, and less overhead as compared to the cryptography approach [14], its hardware implementation is complex.
It needs high complexity coding and perfect/imperfect channel state information of the receiver and eavesdroppers [3]. Therefore, PLS is not a suitable security solution for small size transceivers such as IoT sensors.

In the aspect of cryptography, most of the conventional wireless communication systems implement security encryption/decryption at the upper layers, such as the MAC layer, where attackers are able to use general-purpose microprocessor and memory to collect data for cracking the encryption key. Besides, encryption at upper layers might result in the fact that many parts of transmission data are not encrypted, e.g., the MAC header and PHY header. Such information is thus vulnerable to eavesdroppers. Researchers have recently focused attention on moving the encryption to the physical layer for improving the security of wireless connections [15–19]. For instance, encryption schemes at the PHY layer based on Polar codes, and chaotic sequences were proposed for the Orthogonal Frequency-Division Multiplexing (OFDM) system in [20,21]. Since Polar code is a high-cost encoder/decoder algorithm, it is an optional selection for a big transceiver that needs a high data rate and high reliability. Furthermore, most wireless transceivers nowadays utilize binary convolution code (BCC) encoder and Viterbi decoder as a mandatory. Therefore, a low complexity encryption method which is suitable for BCC code is needed.

Nominated as a promising solution, physical layer encryption (PLE) is considered in this work. PLE was deployed in various OFDM systems, such as constellation scrambling in the frequency domain, modulation symbols rotation [22–24], noise enhanced constellation rotation, rateless code [25], sparse code multiple access [26], subcarriers encryption [27]. The position of encryption can be placed before or after the data modulation. In case the encryption is performed after modulation, i.e., also known as phase encryption, the system is considered to be higher security because modulation type such as BPSK, QPSK, 16-256 QAM is also encrypted. However, conventional works on this method still have problems such as having high complexity for high-order modulation (64-256 QAM) and degrading packet error rate (PER) performance of the system. For that reason, PLE works in [28], and [29] only supports low complex modulation such as OQPSK.

Our main purpose in this work is to propose a new phase encryption method, named as joint encryption-modulation (JEM), that achieves two targets. Firstly, it does not degrade the PER performance of the communication system. Secondly, it must be low complexity despite system employs or not high-order modulation types (64-256 QAM). We introduce JEM as low complexity and high-performance solution so that the high-security phase encryption can be applied in IoT sensors’ transceiver.

In summary, the main contributions of this study are as follows:

- We propose a low-complexity JEM method for performing phase encryption in the PHY layer of IoT sensor transceivers.
- We provide PER and BER performance analysis of the proposed JEM method to prove that the implementation of JEM does not degrade the performance of PHY transceiver.
- We practically implement the JEM method in hardware, and we show that the complexity of JEM is low despite of the modulation types (BPSK, QPSK, 16-256 QAM).
- We choose and design a lightweight stream cipher Grain 128a to generate ciphering keys for the practical implementation of the proposed JEM method.

The rest of this paper is organized as follows. Section 2 provides the background of the physical layer encryption, related work, and the basic idea of the proposed method. Then, the algorithm of the proposed JEM method is presented in Section 3. Section 4 describes the hardware design. Section 5 provides numerical results and discussion. Finally, Section 6 is the conclusion and future work.

2. Background

In this section, we introduce PLE in the PHY transceiver model. Then, we survey recent work related to our proposed method. Finally, we present the basic idea of the proposed JEM method.
2.1. PLE in the Physical Layer Transceiver Model

Figure 1 shows a block diagram of the PHY layer of a basic wireless communication system when implementing PLE. At the transmitter, data received from the MAC layer are scrambled, encoded by Binary convolution code (BCC), interleaved, and mapped into the constellation of predefined modulation. The modulated data are then encrypted by the ciphering key generated from the “KEY GEN” block. “KEY GEN” can be any cryptography algorithm such as Grain, RC4. Because data are encrypted after modulation, both modulated data streams (in-phase part (IP) and quadrature part (QP)) must be encrypted. The processing inside the encryption determines how the ciphering key makes a change to the modulated data. At the receiver side, the decryption is executed oppositely to recover the IP and the QP of the modulated symbols. In order to decrypt data successfully, the receiver must implement the same cryptography algorithm and keep the same secret key as the transmitter does.

![Block diagram of the physical layer transceiver model.](image)

2.2. Related Works

As surveyed, some typical PLE methods have been proposed in the literature. The first one is to encrypt only the sign bit of the modulated data [30]. In this way, the encrypted data still exists on the modulation constellation. As a result, it does not degrade the BER and PER performance of the system. However, this approach remains concerned about security because it does not encrypt amplitude information of the data. Such data is available for attackers.

In [22], the authors proposed a method to encrypt both sign and amplitude information of the modulated data. To prepare for the encryption process, it firstly converts IP and QP parts of the modulated data into the corresponding amplitude, and phase components refer to Figure 2a. At the same time, the value of the ciphering key is converted into the equivalent delta phase and delta amplitude. The encryption is performed by adding or subtracting the phase and amplitude of the modulated data with the delta phase and amplitude, respectively. Finally, the encrypted phase and amplitude must be converted back to the corresponding IP and QP components. This approach is considered to be high security because it encrypts all components of the modulated data. However, it remains two main disadvantages. Firstly, the encryption is expected to degrade the PER performance of the communication system because the encrypted data no longer locates in the constellation of modulation. As a result, the receiver has more difficulty in recovering the transmitted data and thus produces more error detection. Secondly, the complexity of encryption is high and is proportional to the complexity of modulation.

In other work [28], the encryption was implemented at the PHY layer instead of at the MAC layer in the original 802.15.4 standard. Another encrypted 802.15.4 transceiver was also proposed in [29]. The hardware resource-consuming was reduced by exploiting the lightweight stream cipher Simeck 32/64. However, both works [28,29] implemented the encryption only for low complexity OQPSK modulation.

In [31], the authors presented an asymmetrical PLE scheme based on elliptic curve cryptography for wireless communications. The drawback of asymmetric cryptosystems is high computational
overhead [32]. In [33], mathematical models, design frameworks, and cryptographic primitives of PLE were developed. In this work, the constellation modulation lays on the surface of the sphere, which is different from the conventional modulation.

To deal with these drawbacks of current works, a new PLE method that is low complexity does not degrade communication performance and is able to support the state-of-the-art modulation types (BPSK, QPSK, 64-256 QAM, etc.) should be developed.

2.3. Basic Idea of the Proposed JEM Method

Most encryption methods nowadays perform XOR operation to data and ciphering key because of its low complexity. Unfortunately, if merely performing XOR operation into the modulated data, the results will no longer locate in the constellation map. For example, in the case of 16-QAM, as shown in Figure 2b, the modulated data is mapped into the IP part and QP part in which the values are −3, −1, 1, 3. If we apply XOR operation into these values, the results may jump out of the range −3, −1, 1, 3. It means that the shape of the constellation is changed. Once the transmitted data is not located in the constellation point, the receiver becomes more difficult to recover the transmitted data. Consequently, the error rate increases, and the performance of communication is reduced.

For the sake of simplicity, we prefer to use XOR operation for encrypting data. At the same time, the encryption should not degrade the performance of the system. A new idea should be proposed to guarantee that the result of XOR-operation between the modulated data and the ciphering key remains in the constellation shape. Our initial idea is to convert the values of constellation points into continuous positive integers such as 0, 1, 2, 3 (16 QAM). We then encrypt these data by XOR them with the equivalent ciphering key. The encrypted data certainly remains in the range 0, 1, 2, 3 (16 QAM). Finally, the encrypted data are converted back to values of constellation points, i.e., −3, −1, 1, 3 (16-QAM).

3. The Joint Encryption-Modulation Method

Based on the basic idea mentioned above, we propose the joint-encryption-modulation (JEM) method, as shown in Figure 3. The JEM merges the operation of mapper and encryption into one component. The encryption is divided into two stages named PRE-MAP and POST-MAP. The XOR operation is placed in between two stages to encrypt data. The detailed principle of the proposed JEM method is described as follows.

The input binary data, $B = b_0b_1...b_{n-1}$, are divided into the IP part, $B_{ip} = b_0b_1...b_{m-1}$, and the QP part, $B_{qp} = b_mb_{m+1}...b_{n-1}$, where $n = 2m$ is the number of bits per modulated symbol, and $m$ is the number of bits per IP or QP part. The value of $m$ is defined in in Equation (1). In this study,
we design and evaluate the proposed JEM for the most used modulation types up to 256-QAM of the wireless communication.

\[
m = \begin{cases} 
1 & \text{if BPSK, QPSK} \\
2 & \text{if 16-QAM} \\
3 & \text{if 64-QAM} \\
4 & \text{if 256 QAM}
\end{cases}
\]  

(1)

Since the IP part and QP part are similar to each other in terms of data format, we only describe the encryption process of the IP part. The encryption of QP part is performed similarly. Note that, for BPSK, the input data only consists of the IP part. The operation of the proposed JEM for various modulation types in wireless communication is executed in the following three steps, illustrated in Figure 4:

- Step 1, PRE-MAP: The input data of IP part, denoted as \(B_{ip} = b_0b_1...b_{m-1}\), is first mapped into the continuous pre-map values \(Y_{ip} = y_0y_1...y_{m-1}\) by the following mapping rule.

\[
B_{ip} \mapsto Y_{ip}
\]

(2)

where the continuous pre-map values \(y_0y_1...y_{m-1}\) are calculated based on the input values \(b_0b_1...b_{m-1}\) and are formulated by the following equation.

\[
\begin{align*}
y_0 &= b_0 \\
y_1 &= b_0 \oplus b_1 \\
&\vdots \\
y_{m-1} &= b_0 \oplus b_1 \oplus ... \oplus b_{m-1}
\end{align*}
\]

(3)

- Step 2, ENCRYPTION: The pre-map data \(Y_{ip}\) is encrypted by a XOR-operation with the cipher keys \(K_{ip} = k_0k_1...k_{m-1}\) to obtain encrypted data \(E_{ip}\).

\[
E_{ip} = Y_{ip} \oplus K_{ip}
\]

(4)

- Step 3, POST-MAP: The encrypted data \(E_{ip}\) are then mapped to the post-map values \(Z_{ip}\) of the conventional modulation by the mapping rule in Equation (5). Since the IP part consists of \(m\) bits, there are \(2^m\) possible combinations of them. We number these combinations according to an ascending value of combination as 0, 1, ..., \(2^m - 1\).

\[
\begin{align*}
E_{ip0} &\mapsto Z_{ip0} \\
E_{ip1} &\mapsto Z_{ip1} \\
&\vdots \\
E_{ip(2^m-1)} &\mapsto Z_{ip(2^m-1)}
\end{align*}
\]

(5)

where \(Z_{ip0}, ..., Z_{ip(2^m-1)}\) are calculated as follows.

\[
\begin{align*}
Z_{ip0} &= -(2^m - 1) + 2 \times 0 \\
Z_{ip1} &= -(2^m - 1) + 2 \times 1 \\
&\vdots \\
Z_{ip(2^m-1)} &= -(2^m - 1) + 2 \times l
\end{align*}
\]

(6)

where \(l = 0, 1, ..., 2^m - 1\).

For a clear explanation of the proposed JEM, we describe in detail the operation for 16-QAM modulation in the next subsection.
Figure 3. (a) Conventional Physical layer encryption (PLE) and (b) the proposed joint encryption-modulation (JEM) method.

Figure 4. The detailed operation of the JEM method.

**JEM for 16-QAM Modulation**

For 16-QAM, we have the number of bits per IP/QP part $m = 2$. Table 1 illustrates the detailed operation of the proposed JEM. Firstly, the input data IP $B_{ip} = b_0b_1$ are mapped into $Y_{ip} = y_0y_1$ using a PRE-MAP. Then the PRE-MAP’s outputs are encrypted by a XOR-operation with the cipher key. The cipher keys $K_{ip} = k_0k_1$ may have one of the following values {00, 01, 10, 11}. In the POST-MAP, the encrypted data $E_{ip}$ are again mapped into conventional mapper values $Z_{ip}$. In which, $Z_{ip}$ may have one of the following values: $-3, -1, 1, 3$.

**Table 1. The proposed JEM for 16-QAM modulation.**

| Pre-Map In $b_0b_1b_2b_3$ | Pre-Map Out $y_0y_1y_2y_3$ | Cipher Key $k_0k_1/k_2k_3$ | Encryption Out $E_{ip}/E_{qp}$ | Post Map Out $Z_{ip}/Z_{qp}$ |
|--------------------------|-----------------------------|-----------------------------|-------------------------------|-------------------------------|
| 00                       | 00                          | 00                          | 00                            | $-3$                          |
| 01                       | 01                          | 00                          | 01                            | $-1$                          |
| 11                       | 10                          | 00                          | 10                            | 1                             |
| 10                       | 11                          | 00                          | 11                            | 3                             |
| 00                       | 00                          | 01                          | 01                            | $-1$                          |
| 01                       | 01                          | 01                          | 00                            | $-3$                          |
| 11                       | 10                          | 01                          | 11                            | 3                             |
| 10                       | 11                          | 01                          | 10                            | 1                             |
| 00                       | 00                          | 10                          | 10                            | 1                             |
| 01                       | 01                          | 10                          | 11                            | 3                             |
| 11                       | 10                          | 10                          | 00                            | $-3$                          |
| 10                       | 11                          | 10                          | 01                            | $-1$                          |
| 00                       | 00                          | 11                          | 11                            | 3                             |
| 01                       | 01                          | 11                          | 00                            | 1                             |
| 11                       | 10                          | 11                          | 01                            | $-1$                          |
| 10                       | 11                          | 11                          | 00                            | $-3$                          |

At the receiver, the decryption performs as the reversed operation of the proposed JEM. It is assumed that the legitimate receiver obtains the same secret key as the transmitter, so the same
ciphering keys are generated. In this decryption method, we apply the hard-decision decoding method. The input values of IP and QP parts first compare with the threshold values of the conventional modulation to determine the decoded output as 1 or 0. Then, by using cipher keys, they are decrypted.

4. Hardware Design

After completing simulation and evaluating BER and PER performances of the proposed JEM, we designed the hardware to analyze the hardware complexity and to prove that our proposed JEM can be practically implemented. The hardware of the proposed JEM supports a variety of modulation types, such as BPSK, QPSK, 16-QAM, 64-QAM, and 256-QAM. In this paper, we show in detail the hardware implementation of encryption. There may be several ways to design the decryption at the receiver side. The explanation of the hardware design of decryption is out of the scope of this paper. We only show the implementation result to prove its practical feasibility.

4.1. Overview Hardware Architecture of JEM Method

Figure 5 presents the overview hardware architecture of the JEM encryption and decryption process. It consists of three blocks, i.e., encryption, decryption, and stream cipher Grain 128a. The input data is encrypted in the encryption block using cipher keys generated by the Grain 128a block. Similarly, the decryption block decrypts the encrypted data produced by the encryption block. For the sake of comparison, we also designed the hardware of the conventional encryption and decryption method in [22] and conventional mapper and demapper to compare with our encryption and decryption. Based on the results of [34] and our experience in hardware implementation, we chose 18 bits as the fixed point for data representation, which does not affect the performance of the system and benefits the hardware implementation.

To achieve low complexity, in addition to utilizing the proposed JEM, the lightweight keystream generator also plays an important role.

4.2. Lightweight Keystream Generator

The encryption and decryption processes need keystreams generated by cipher algorithms. There are two types of ciphers known as block-cipher and stream-cipher. In this design, we chose a stream cipher rather than a block cipher due to following reasons.

- Block ciphers have high complexity and consume large power consumption [28]. They are, therefore, not suitable for IoT sensor transceivers.
- Block ciphers are sensitive to burst error because an error in one symbol may cause the corruption of an entire block.

There are many types of stream ciphers, such as RC4, Grain 128a, A5, Mickey, Trivium. Although RC4 is one of the most widely used stream ciphers, it uses much more hardware resources and consumes more power than the others do [29]. In this work, we chose stream cipher Grain 128a because it is lightweight and more suitable for IoT sensors. We developed the hardware for both
RC4 and Grain 128a stream cipher for comparison and finally choose Grain 128a for implementation. The details of Grain 128a can be found in [35]. Further, we designed the Grain 128a hardware to generate 8-bit keystreams per clock cycle to encrypt and decrypt the IP and QP parts.

As shown in Table 2, the slices look-up tables (LUTs) of Grain 128a is less than half of RC4’s slice LUTs. In addition, the static power and area of Grain 128a is also about half of the designed RC4 version.

Table 2. Hardware area and power consumption of RC4 and Grain 128a stream ciphers

| Implemented Design | Clocks | Slice Registers | Slice LUTs | Static Power (mW) | Area (µm²) |
|--------------------|--------|-----------------|------------|-------------------|------------|
| GRAIN 128a         | 256    | 2195            | 2715       | 1.53              | 188,175    |
| Designed RC4       | 256    | 2213            | 7954       | 3.25              | 344,461    |
| RC4 [28]           | 256    | 2478            | 7064       | 163.43            | -          |

4.3. JEM’s Encryption and Decryption

Figure 6a shows the overview hardware architecture of JEM’s encryption. It consists of a PRE-MAP block, POST-MAP block, and XOR-encryption. The PRE-MAP block converts input data into continuous positive values. Then the POST-MAP block maps data into the corresponding values of modulation constellation. PRE-MAP and POST-MAP are designed so that they support multiple modulation types such as BPSK, QPSK, 16-256 QAM. Figure 6b shows hardware implementation inside PRE-MAP and POST-MAP. Because their functions are to map input data into predefined output data, we only need multiplexers to perform the work. No complexity calculation unit is required. Therefore, they consume significantly low hardware resources. Moreover, the encryption between PRE-MAP and POST-MAP employs only XOR gates, which is just a low complexity logic gate.

**Figure 6.** (a) Hardware architecture of the JEM encryption; (b) the pre-map and post-map architecture.
Figure 7a shows the overview hardware architecture of JEM decryption at the receiver side. It consists of a Gain block, joint demapper-decryption, and a MUX block. In this regard, the gain block is responsible for recovering any decrease in the amplitude of the input data by multiplying with a corresponding gain constant of each modulation type, as illustrated in Figure 7b. The joint demapper-decryption supports different modulation types. In this block, we use several binary fix-point comparators to compare the input data with the threshold values to determine the output values. Then, depending on the value of the cipher key, the decrypted output data is decided.

Figure 7. (a) Hardware architecture of the decryption; (b) gain block architecture.

5. Numerical Results and Evaluation

In this section, we show and analyze the performance simulation and hardware implementation results of the proposed JEM method.

5.1. Simulation Results

Our simulation model follows the IEEE 802.11ah wireless communication network, which is suitable for IoT applications. Table 3 shows some important parameters used in the simulation. We simulated the system for high order modulations such as 16-QAM, 64-QAM, and 256-QAM. It is assumed that the channel was corrupted by the additive white Gaussian noise (AWGN). The transfer data is random, with 100 bytes per packet. The simulation was run 10,000 times.

Figures 8 and 9 show the BER and PER performance of the system for four cases: with the proposed encryption, with no encryption, using the conventional encryption method in [22], and with
an unexpected user who does not obtain the correct key at the receiver side (an eavesdropper). From these figures, we can make the following observations.

Table 3. Simulation parameters based on IEEE 802.11ah.

| Simulation parameters | Value                     |
|----------------------|---------------------------|
| Simulator            | IEEE 802.11ah             |
| Number of iterations | $10^4$                    |
| Number of spacial streams in TXxRX | $1 \times 1$               |
| Channel type         | AWGN                      |
| Channel estimation   | Ideal                     |
| Modulation types     | 16, 64, 256-QAM           |
| Code rate            | 3/4                       |
| Transfer data type   | Random                    |

Firstly, the proposed JEM has nearly the same BER and PER performances as the unencrypted system for all modulation types (16-QAM, 64-QAM, and 256-QAM). This means that the proposed JEM does not degrade the BER or PER performance. The reason is that the proposed JEM does not change the constellation of modulated symbols. Consequently, it does not affect the error correction performance of the system. Secondly, these figures also show that the conventional method in [22] degrades the BER and PER performances about 3 dB as compared with the proposed JEM at the observation point of $BER = 10^{-3}$ and $PER = 10^{-3}$. This result confirms our statement in Section 2. The main reason for BER and PER performance degradation of [22] is that the encrypted data of [22] (which is transmitted to the receiver) do not locate on the constellation points anymore. The transmitted data is thus more sensitive to noise and interference during transmission. In addition, the receiver has more difficulty in recovering the transmitted data, which originally does not locate on the constellation. Error detection rate increases and BER/PER performance degrades.

![Figure 8. BER performance of 802.11ah with 16-QAM, 64-QAM, and 256-QAM using AWGN channel.](image)
Finally, the figures show that an unexpected user, who does not have the correct key, has approximately 50% BER, and 100% PER. Note that a bit has value either 0 or 1; the 50% of BER is a random bit error rate detection in case the receiver has no information about the transmitter. It does not mean that the receiver of unexpected users can detect the transmitted data. PER = 100% shows that the unexpected user completely not be able to recover the transmitted data. It means the proposed JEM method successfully protects data from an unexpected user who does not own the correct private key.

5.2. Implementation Results

The hardware circuits mentioned in this work were designed by Verilog hardware description language and verified by using the ModelSim simulation tool. FPGA synthesis was performed with Intel Quartus II using a Cyclone IVE EP4CE115F29C7 device. The ASIC synthesis was executed at 16 MHz frequency by Synopsys’ Design Compiler using VDEC’s Rohm 180 nm technology library.

In theory, we need only 2 XOR gates and 2N multiplexers to implement JEM encoder at the transmitter side of the system supporting N types of modulation. For example, the IEEE 802.11ah system supports five types of modulation (BPSK, QPSK, 16QAM, 64QAM, and 256 QAM) that will need two XOR gates and ten multiplexers for JEM encryption. On the other hand, the complexity of JEM decryption will depend on the decryption algorithm used. In this research, we have successfully developed JEM decryption to recover the encrypted data. However, the detailed explanation of JEM decryption as well as analyzing its complexity are out of the scope of this paper.

It is worth noting that the system employing our JEM method does not need to implement Mapper at the transmitter side and Demapper at the receiver side as the conventional work has. That is because Mapper and Demapper have been merged into JEM encryption and JEM decryption, respectively. For the sake of fairness, we compare JEM encryption with the combination of conventional encryption in [22] and Mapper. We compare JEM decryption with the combination of conventional decryption in [22] and Demapper. We synthesized hardware circuits in both hardware platforms FPGA and ASIC. FPGA synthesis results are shown in Table 4, and ASIC synthesis results are shown in Table 5. Based on these results, the merits of the JEM method are exposed as follows.
Table 4. FPGA Synthesis Results: Cyclone IVE EP4CE115F29C7 @16MHz.

| Implemented Design | Encryption (Proposed) (+Mapper) | Conven. Encryption (Only) | Conven. Encryption [22] (+Mapper) | Decryption (Proposed) (+Demapper) | Conven. Decryption (Only) | Conven. Decryption [22] (+Demapper) |
|--------------------|---------------------------------|--------------------------|---------------------------------|---------------------------------|--------------------------|---------------------------------|
| Slice registers    | 51                              | 34                       | 1326                            | 90                              | 54                       | 1352                            |
| Slice LUTs         | 229                             | 139                      | 3516                            | 713                             | 629                      | 4016                            |

Table 5. ASIC implementation results: VDEC’s Rohm 180 nm technology @16MHz

| Implemented Design | Encryption (Proposed) (+Mapper) | Conven. Encryption (Only) | Conven. Encryption [22] (+Mapper) | Decryption (Proposed) (+Demapper) | Conven. Decryption (Only) | Conven. Decryption [22] (+Demapper) |
|--------------------|---------------------------------|--------------------------|---------------------------------|---------------------------------|--------------------------|---------------------------------|
| Area ($\mu$m$^2$)   | 9,902                           | 6,899                    | 436,942                         | 124,372                         | 116,628                  | 548,767                         |
| Power(mW)           | 0.09                            | 0.08                     | 3.62                            | 1.63                            | 1.55                     | 5.23                            |

5.2.1. Low FPGA Resource

Table 4 shows that the amount of slice LUTs of JEM encryption is just about 6.5% (229 versus 3516) of that of the conventional work. The amount of slice LUTs of JEM decryption is about 17.8% (713 versus 4016) of that of conventional work. Similarly, the number of registers of JEM encryption and JEM decryption are respectively about 3.8% and 6.7% of those of the conventional work. Overall, the total LUTs of JEM encryption and decryption is just 12.5% of that of conventional encryption and decryption. It means that the JEM method helps to reduce FPGA hardware resources by 87.5%. Our proposed JEM method consumes low FPGA hardware resources.

5.2.2. Small Area

Table 5 shows that ASIC areas of JEM encryption and JEM decryption are respectively about 2.2% (9902 $\mu$m$^2$ versus 43,6942 $\mu$m$^2$) and 22.7% (124,372 $\mu$m$^2$ versus 116,628 $\mu$m$^2$) of that of the conventional work. In total, ASIC area of JEM method (encryption + decryption) is about 13.5% of that of conventional work in [22]. It means that the JEM method helps to reduce ASIC hardware cost by 86.5%.

5.2.3. Low Power Consumption

Table 5 also shows that the JEM method requires less static power consumption than that of the conventional work. In detail, power consumptions of JEM encryption and JEM decryption are respectively 2.5% (0.09 mW versus 3.62 mW) and 31% (1.63 mW versus 5.32 mW) of those of the conventional work in [22]. The total power consumption of the JEM method is 19.4% of that of conventional work. It means that power consumption is reduced by 80.6%.

Due to the significant reduction in FPGA hardware resource, ASIC area, and ASIC power consumption, the proposed JEM method is a candidate for employing phase encryption in the PHY layer of IoT sensors’ transceiver.

5.3. Security Analysis

Security of JEM is guaranteed because it is a type of phase encryption and it encrypts all bits of the transmitted data. Readers refer to [27–29] for the detail analysis and evidence on security of phase encryption. In this work, we propose JEM as a low complexity method that is able to encrypt all bits of modulated data using the existing ciphering key. The strength of security over several types of attacks (Brute force search, etc.) is not affected by JEM method itself but depends on the algorithms that generate the ciphering key. Any cipher algorithms such as Grain 128a, RC4, advanced encryption standard (AES), etc., can be applied for JEM method. The selection of cipher algorithms for JEM method is a trade-off between security requirement and circuit complexity.
In our prototype work, we select Grain 128a stream cipher algorithm to generate ciphering key for JEM method. Security of Grain 128a has been proved in [35]. Security of our combined JEM and Grain 128a encryption is analyzed through many aspects as follows.

5.3.1. Brute Force Search Attack

In brute force search, all possible combinations of encrypted data have to be collected and analyzed by an exhaustive search operation. Grain 128a has a 128-bit secret key. Therefore, there are $2^{128}$ alternative values of ciphering key. Let say system employs 256-QAM modulation, there are 256 possible symbols are encrypted by ciphering keys. It means that the brute force search engine must collect and analyze $256 \times 2^{128}$ possible combinations of encrypted data to be able to successfully decrypt a data frame. For such huge number of combinations, it is difficult enough for brute force search attack. System is considered to be sufficient secure according to current standard [36].

5.3.2. Traffic Analysis Attack

As a phase encryption, JEM method encrypts not only the transmitted information but also PHY preamble. Consequently, the adversary (or attackers) can not precisely detect the timing of the data transmission due to the difficulties of identifying and synchronizing valid frames. In other words, the proposed JEM method has sufficient resistivity against traffic analysis attacks.

5.3.3. Confidentiality

In the worse case that the eavesdropper successfully decrypts a valid frame by using brute force search, the system still preserves its confidentiality because the entire correct data (from many data frames) can not be recovered without a correct secret key.

5.3.4. Integrity

Thanks to the encryption provided at the PHY layer, all the upper layers’ headers (includes MAC header) are encrypted. Consequently, the system can easily detect whether the source address or the data has been unexpectedly modified or changed during the transmission or not. In short, the system with JEM method achieves better integrity.

5.3.5. Confusion of the Constellations

Confusion of the constellations is an essential factor of the security of the physical layer encryption. JEM method encrypts information relates to types of modulations (BPSK, QPSK, 16-QAM, or 256-QAM, etc.). The adversary (or attackers, eavesdroppers) are thus confused on what the shape of constellation being used. Their attack methods become less efficient.

6. Conclusions

In this study, we have proposed a low complexity join-encryption-modulation (JEM) method for performing phase encryption at the PHY layer of IoT sensors’ transceiver. The BER/PER performance simulation has been conducted. The results have shown that the JEM method does not degrade BER/PER performance of the PHY system, while the BER/PER performance degradation caused by conventional work is about 3 dB. We have also developed hardware circuits of the JEM method and conventional method and synthesized the circuits on two hardware platforms FPGA and ASIC. The results have shown that our proposed JEM method can support multiple modulation types. Hardware resource of the JEM method is only about 12.5% (FPGA resource), or 13.5% (ASIC area) of that of the conventional work. ASIC static power consumption of JEM is about 19.4% of that of conventional work. Because of such a remarkable reduction of hardware complexity, the proposed JEM is a candidate for employing high-security phase encryption at the PHY layer of IoT sensors’ transceiver.
However, it could be seen that the hardware resource of our developed JEM decryption is still high. Further research for reducing the hardware complexity of JEM decryption is needed. Our future work is to find algorithm and low complexity hardware circuit to decrypt JEM encryption. In addition, our plan is to develop the IEEE 802.11ah PHY transceiver that implements JEM encryption and decryption.

Author Contributions: Conceptualization, D.L.H., and T.H.T.; methodology, D.L.H., and T.H.T.; software, T.H.T. and D.L.H.; validation, D.L.H, T.H.T., and Y.N.; writing—original draft preparation, D.L.H.; writing—review and editing, D.L.H., T.H.T., Y.N.; supervision, T.H.T., Y.N. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by JSPS KAKENHI Grant Number JP16K18105.

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

Abbreviations
The following abbreviations are used in this manuscript:

| Abbreviation | Description                                      |
|--------------|--------------------------------------------------|
| ASIC         | Application-specific Integrated Circuit          |
| AWGN         | Additive White Gaussian Noise                    |
| BCC          | Binary Convolution Coding                        |
| BER          | Bit Error Rate                                   |
| BPSK         | Binary Phase Shift Keying                        |
| CMOS         | Complementary Metal-Oxide-Semiconductor          |
| FPGA         | Field Programmable Gate Arrays                   |
| IoT          | Internet of Things                               |
| IP           | In-phase Part                                    |
| LUT          | Lookup Table                                     |
| MAC          | Media Access Control                             |
| OFDM         | Orthogonal Frequency Division Multiplexing       |
| OQPSK        | Offset Quadrature Phase-Shift Keying             |
| PER          | Packet Error Rate                                |
| PLE          | Physical Layer Encryption                        |
| PLS          | Physical Layer Security                          |
| PHY          | Physical                                        |
| QAM          | Quadrature Amplitude Modulation                  |
| QP           | Quadrature Part                                  |
| QPSK         | Quadrature Phase Shift Keying                    |
| VDEC         | VLSI Design and Education Center                 |

References
1. Stankovic, J.A. Research Directions for the Internet of Things. *IEEE Internet Things J.* 2014, 1, 3–9. [CrossRef]
2. Zhang, J.; Duong, T.Q.; Woods, R.; Marshall, A. Securing Wireless Communications of the Internet of Things from the Physical Layer, An Overview. *Entropy* 2017, 19, 420. [CrossRef]
3. Zou, Y.; Zhu, J.; Wang, X.; Hanzo, L. A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends. *Proc. IEEE* 2016, 104, 1727–1765. [CrossRef]
4. Mukherjee, A.; Fakoorian, S.A.A.; Huang, J.; Swindlehurst, A.L. Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey. *IEEE Commun. Surv. Tutor.* 2014, 16, 1550–1573. [CrossRef]
5. Bloch, M.; Barros, J. *Physical-Layer Security: From Information Theory to Security Engineering*; Cambridge University Press: Cambridge, UK, 2011.
6. Goel, S.; Negi, R. Guaranteeing Secrecy using Artificial Noise. *IEEE Trans. Wirel. Commun.* 2008, 7, 2180–2189. [CrossRef]
7. Zhou, X.; McKay, M.R. Secure Transmission With Artificial Noise Over Fading Channels: Achievable Rate and Optimal Power Allocation. *IEEE Trans. Veh. Technol.* 2010, 59, 3831–3842. [CrossRef]
8. Liao, W.; Chang, T.; Ma, W.; Chi, C. QoS-Based Transmit Beamforming in the Presence of Eavesdroppers: An Optimized Artificial-Noise-Aided Approach. *IEEE Trans. Signal Process.* 2011, 59, 1202–1216. [CrossRef]
9. Mukherjee, A.; Swindlehurst, A.L. Robust Beamforming for Security in MIMO Wiretap Channels with Imperfect CSI. *IEEE Trans. Signal Process.* 2011, 59, 351–361. [CrossRef]

10. Khisti, A.; Wornell, G.W. Secure Transmission With Multiple Antennas I: The MISOME Wiretap Channel. *IEEE Trans. Inf. Theory* 2010, 56, 3088–3104. [CrossRef]

11. Romero-Zurita, N.; Mclernon, D.; Ghogho, M. Physical layer security by robust masked beamforming and protected zone optimisation. *IET Commun.* 2014, 8, 1248–1257. [CrossRef]

12. Dong, L.; Han, Z.; Petropulu, A.P.; Poor, H.V. Improving Wireless Physical Layer Security via Cooperating Relays. *IEEE Trans. Signal Process.* 2010, 58, 1879–1888. [CrossRef]

13. Rodriguez, L.J.; Tran, N.H.; Duong, T.Q.; Le-Ngoc, T.; Elkashlan, M.; Shetty, S. Physical layer security in wireless cooperative relay networks: State of the art and beyond. *IEEE Commun. Mag.* 2015, 53, 32–39. [CrossRef]

14. Sun, L.; Du, Q. A Review of Physical Layer Security Techniques for Internet of Things: Challenges and Solutions. *Entropy* 2018, 20, 730. [CrossRef]

15. Khan, M.A.; Asim, M.; Jeoti, V.; Manzoor, R.S. On secure OFDM system: Chaos based constellation scrambling. In Proceedings of the 2007 International Conference on Intelligent and Advanced Systems, Kuala Lumpur, Malaysia, 25–28 November 2007; pp. 484–488.

16. Zhang, L.; Xin, X.; Liu, B.; Wang, Y. Secure OFDM-PON Based on Chaos Scrambling. *IEEE Photonics Technol. Lett.* 2011, 23, 998–1000. [CrossRef]

17. Li, H.; Wang, X.; Hou, W. Secure Transmission in OFDM Systems by Using Time Domain Scrambling. In Proceedings of the 2013 IEEE 77th Vehicular Technology Conference (VTC Spring), Dresden, Germany, 2–5 June 2013; pp. 1–5.

18. Reilly, D.; Kanter, G.S. Noise-enhanced encryption for physical layer security in an OFDM radio. In Proceedings of the 2009 IEEE Radio and Wireless Symposium, San Diego, CA, USA, 18–22 January 2009; pp. 344–347.

19. Ma, R.; Dai, L.; Wang, Z.; Wang, J. Secure communication in TDS-OFDM system using constellation rotation and noise insertion. *IEEE Trans. Consum. Electron.* 2010, 56, 1328–1332. [CrossRef]

20. Lu, X.; Lei, J.; Li, W.; Lai, K.; Pan, Z. Physical Layer Encryption Algorithm Based on Polar Codes and Chaotic Sequences. *IEEE Access* 2019, 7, 4380–4390. [CrossRef]

21. Lu, X.; Shi, Y.; Li, W.; Lei, J.; Pan, Z. A Joint Physical Layer Encryption and PAPR Reduction Scheme Based on Polar Codes and Chaotic Sequences in OFDM System. *IEEE Access* 2019, 7, 73036–73045. [CrossRef]

22. Kloos., M. Method and Apparatus for Encryption of over-the-Air Communications in a Wireless Communication System. U.S. Patent US7693284B2, 28 September 2010

23. Dzung, D. Data Encryption on the Physical Layer of a Data Transmission System. U.S. Patent No 7,752,430, 6 July 2010.

24. Hoang, D.L.; Tran, T.H.; Nakashima, Y. Hardware Implementation of CORDIC Based Physical Layer Phase Decryption for IEEE 802.11Ah. In Proceedings of the 7th International Conference on Communications and Broadband Networking, Nagoya, Japan, 12 April 2019; ICCBN 2019. pp. 17–21.

25. Huang, Y.; Li, W.; Lei, J. Concatenated physical layer encryption scheme based on rateless codes. *IET Commun.* 2018, 12, 1491–1497. [CrossRef]

26. Lai, K.; Lei, J.; Wen, L.; Chen, G.; Li, W.; Xiao, P. Secure Transmission With Randomized Constellation Rotation for Downlink Sparse Code Multiple Access System. *IEEE Access* 2018, 6, 5049–5063. [CrossRef]

27. Zhang, J.; Marshall, A.; Woods, R.; Duong, T.Q. Design of an OFDM Physical Layer Encryption Scheme. *IEEE Trans. Veh. Technol.* 2017, 66, 2114–2127. [CrossRef]

28. Nain, A.K.; Bandaru, J.; Zubair, M.A.; Pachamuthu, R. A Secure Phase-Encrypted IEEE 802.15.4 Transceiver Design. *IEEE Trans. Comput.* 2017, 66, 1421–1427. [CrossRef]

29. Bhoyar, P.; Dhok, S.; Deshmukh, R. Hardware implementation of secure and lightweight Simeck32/64 cipher for IEEE 802.15.4 transceiver. *AELI Int. J. Electron. Commun.* 2018, 90, 147–154. [CrossRef]

30. Hoang, D.L.; Hong Tran, T.; Nakashima, Y. Performance Evaluation of 802.11ah Physical Layer Phase Encryption for IoT Applications. In Proceedings of the 2018 International Conference on Advanced Technologies for Communications (ATC), Ho Chi Minh City, Vietnam, 18–20 October 2018; pp. 84–88.

31. Li, W.; Mclernon, D.; Wong, K.; Wang, S.; Lei, J.; Zaidi, S.A.R. Asymmetric Physical Layer Encryption for Wireless Communications. *IEEE Access* 2019, 7, 46959–46967. [CrossRef]

32. Zhang, Z.; Cho, M.C.Y.; Wang, C.; Hsu, C.; Chen, C.; Shieh, S. IoT Security: Ongoing Challenges and Research Opportunities. In Proceedings of the 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications, Matsue, Japan, 17–19 November 2014; pp. 230–234.
33. Li, W.; McIlrnon, D.; Lei, J.; Ghogho, M.; Zaidi, S.A.R.; Hui, H. Cryptographic Primitives and Design Frameworks of Physical Layer Encryption for Wireless Communications. *IEEE Access* **2019**, *7*, 63660–63673. [CrossRef]

34. Ferdian, R.; Hou, Y.; Okada, M. A Low-Complexity Hardware Implementation of Compressed Sensing-Based Channel Estimation for ISDB-T System. *IEEE Trans. Broadcast.* **2017**, *63*, 92–102. [CrossRef]

35. Ågren, M.; Hell, M.; Johansson, T.; Meier, W. Grain-128a: A new version of Grain-128 with optional authentication. *IJWMC* **2011**, *5*, 48–59. [CrossRef]

36. Stalling, Q. Classical encryption techniques. In *Cryptography and Network Security: Principle and Practice*, 5th ed.; Prentice Hall: Englewood Cliffs, NJ, USA, 2011; Chapter 2; pp. 35–38.