XOR Encryption Versus Phase Encryption, an In-Depth Analysis

Fei Huo and Guang Gong, *Fellow, IEEE*

***Abstract*—Encryptions are used in almost all standards to ensure the confidentiality of the data. Encryptions can be and indeed are implemented in the different layers of a network protocol stack. Conventional encryption performs the bitwise XOR operation between one message bit and one key stream bit to generate one ciphertext bit. Huo *et al.* have recently proposed to provide confidentialities on the user data by performing the phase encryption on the time domain OFDM samples in LTE system. Phase encryption is performed on the modulated symbols, different from the bit level of XOR encryption, i.e., stream cipher encryption. In this paper, we extend their study. We first generalize the phase encryption to general communication systems independent of the underlying modulation scheme. Then, we formulate the mathematical models for XOR and phase encryptions. Based on our model, we compare these two encryption methods in terms of their security and encryption efficiency. We also show phase encryption can resist traffic analysis attack when implemented in the physical layer. Finally, we conduct simulations to compare the performance of these two methods in terms of their decoding symbol error rate.**

***Index Terms*—Encryption, security, wireless security.**

I. Introduction

THE security and privacy of the user's data has become increasingly more important in the past decade. People become more and more aware of the security and the privacy of their personal data. Consequently, almost all standards have incorporated security primitives to ensure that authenticity, integrality and confidentiality of the data being transmitted over the channel. For instance, LTE have incorporated stream ciphers SNOW 3G, ZUC and block cipher AES for security and authenticity protection [1].

Security primitives mentioned previously can and are implemented in different layers of the protocol stack. Each layer has its own associated advantages and drawbacks. For instance, end-to-end encryptions occur in the application layer, SSL/TLS ensures data protections in the transport layer, while IPSec protects users' data in the network layer [6]. At the lower layers, security functions are system dependent. For instance, in LTE, for evolved UMTS terrestrial radio access network (E-UTRAN), the integrality and confidentiality protections of the data contents are performed in the packet data convergence protocol (PDCP) layer or layer 3 of the E-UTRAN protocol stacks [4]. In 802.11, counter mode CBC-MAC protocol in the MAC layer provides data confidentiality, authentication as well as access control [12].

In this paper, we focus on providing the data confidentiality by encryption in the physical (PHY) layer. PHY layer is in the lowest layer of the protocol stack. The advantage of performing security functions in the PHY layer include: 1) Having the lowest impact on the network; 2) Having low latencies; 3) Introducing no overhead.

Conventional encryption, namely stream cipher encryption, makes use of bitwise exclusive OR (XOR) operation between one message bit and one key stream bit to generate one ciphertext bit. The reason for this implementation is that it is hardware efficient. In LTE, the air interface uses OFDM modulation [2]. Thus, Huo and Gong have proposed the use of phase encryption (by multiplying the real and imaginary components of time domain OFDM samples by two $\{1,-1\}$ binary key streams) at the PHY layer to provide data confidentiality protection [9]. The authors have claimed that performing phase encryption on the time domain OFDM samples creates nonlinear distortions in the frequency domain, making the decoding error rate greater than conventional XOR encryption when the adversary tries to decode without the key.

In general, phase encryption is not system dependent or rely on a specific underlying modulation scheme. In fact, phase encryption was first introduced for optical encryptions. It is based on the special property of high resolution optical materials [14], [18].

This study extends phase encryption to general wireless communication systems independent of the modulation methods. It is an expanded version of the study presented in [10]. We adopt the term *XOR-Enc* and *P-Enc* for simplicity to represent XOR encryption and phase encryption, respectively. We show P-Enc used under our context can be extended to amplitude shift keying (ASK), phase shift keying (PSK) and quadrature amplitude modulation (QAM) modulations, but not to frequency shift keying (FSK) modulation.

The contributions of this paper include:

1) We generalize P-Enc to general wireless communication systems.
2) We show the mathematical formulations of P-Enc and conventional XOR-Enc for different types of modulation.
3) We conduct theoretical analysis to compare XOR-Enc and P-Enc in terms of their security and encryption efficiency.
4) We show P-Enc at the PHY layer can prevent traffic analysis attack, which cannot be prevented with the upper layer encryptions.
5) We conduct simulations to compare the performance of XOR-Enc and P-Enc in terms of the decoding symbol error rate (SER).

Manuscript received October 1, 2014; revised December 18, 2014; accepted January 3, 2015. Date of publication January 30, 2015; date of current version August 13, 2015.

The authors are with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada (e-mail: fhuo@uwaterloo.ca; ggong@engmail.uwaterloo.ca).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TEMC.2015.2390229

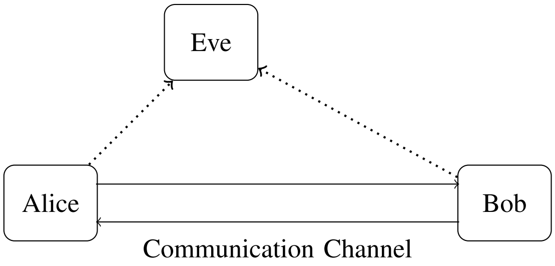


Fig. 1. Traffic analysis attack model.

The rest of the paper is organized as follows. In Section II, we give the necessary background. In Section III, we present the P-Enc scheme. In Section IV, we first present mathematical formulations for XOR-Enc and P-Enc. Then, using our mathematical formulations, we compare these two encryption methods in terms of security and encryption efficiency. In Section V, we first show how P-Enc in the PHY layer can prevent traffic analysis attack. Then, we compare XOR-Enc and P-Enc at the system level by taking into considerations of channel coding. In Section VI, we conduct simulations to compare the performance of XOR-Enc and P-Enc in terms of the decoding SER. Section VII concludes our paper.

II. Background

In this section, we first give the formal definition for traffic analysis attack. Then, we introduce conventional XOR-Enc. Finally, we present the protocol stack of E-UTRAN in LTE.

A. Traffic Analysis Attack

Traffic analysis attack is defined as the study of the external characteristics of signal communications and related materials for the purpose of obtaining information concerning the operation of a communication system [5]. This is depicted in Fig. 1.

The adversary conducts traffic analysis attack by intercepting the signals transmitted between Alice and Bob. Traffic analysis attack does not necessarily concern with the recovery of the data contents, but rather concern with gaining knowledge such as who are the communicating parties, what types of data/signals are being transmitted, what are the communication patterns, etc. This is a weaker attack compared to the recovery of data contents, but it may still be very serious. For instance, consider the case of a military airplane in a hostile environment, if the enemy is able to conduct traffic analysis, he may be able to deduce what action the airplane is going to take based on the communication pattern and/or the types of signals that is being transmitted.

B. XOR-Enc in a Communication System

Let $\mathbf{m}, \mathbf{k}, \mathbf{c} \in \mathbb{F}_2^N$ be messages, key streams and ciphertext, ciphertext $\mathbf{c}$ is generated by bitwise XOR operation between messages $\mathbf{m}$ and key streams $\mathbf{k}$, i.e., $\mathbf{c} = \mathbf{a} + \mathbf{b}$. This is shown in Fig. 2.

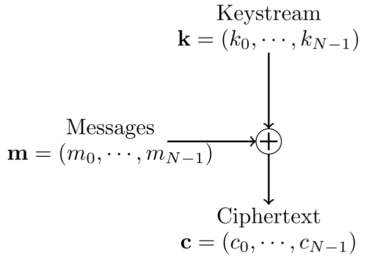

Keystream
$\mathbf{k} = (k_0, \cdots, k_{N-1})$
Messages
$\mathbf{m} = (m_0, \cdots, m_{N-1})$
Ciphertext
$\mathbf{c} = (c_0, \cdots, c_{N-1})$

Fig. 2. XOR-Enc block.

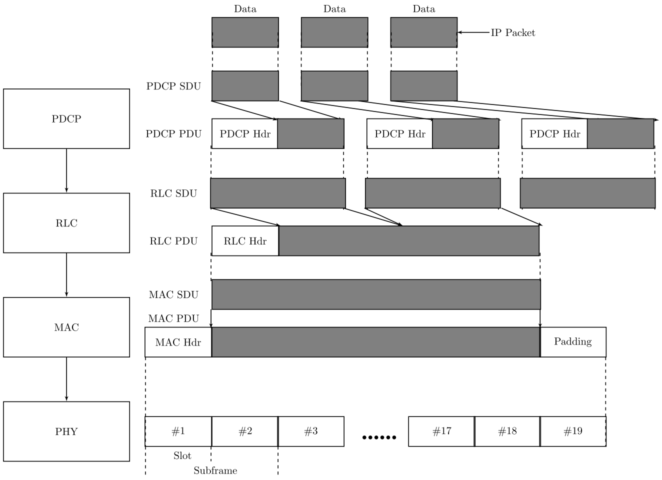


Fig. 3. E-UTRAN layered protocol stack [16].

C. LTE E-UTRAN Layered Protocol Stack

In this section, we show the layered architecture of E-UTRAN. E-UTRAN consists of base stations (termed eNB in LTE) which handles the communication between the mobiles and evolved packet core.

The protocol stack of E-UTRAN is shown in Fig. 3. For our purpose, we mainly focus on the security functionalities provided by E-UTRAN. That is from layer 3 to layer 1, or equivalently from PDCP layer to PHY layer. Data contents in the higher layers may be protected by SSL/TLS in transport layer and/or IPSec in network layer, we do not consider these as they are out of the scope of this paper.

The IP data packet passes through PDCP, RLC, MAC and finally down to PHY layer before sending into the channel for data transmission. In LTE, packets received by each layer are called service data units (SDUs), while packets at the output of a layer are called protocol data unit (PDUs). The PDU generated in a layer is formed by combing one or multiple SDUs, then adding additional information to the SDUs and prepending a header at the beginning as shown in Fig. 3. The security functions provided by E-UTRAN including the data integrality and confidentiality protections are performed in the PDCP layer prior to adding the PDCP header.

Other wireless systems including UTMS and 802.11 have similar structures as LTE. All security functions are usually performed in layer 2 or layer 3 of a protocol stack. This leaves

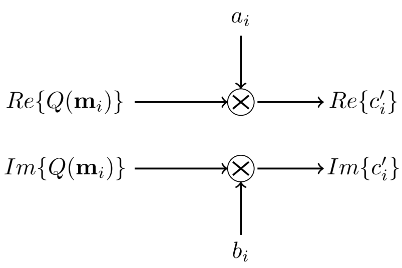


Fig. 4. P-Enc block.

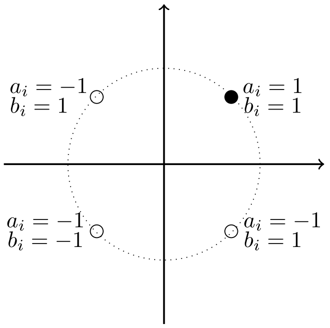


Fig. 5. Encryption illustration.

all subsequent headers and added information unprotected and vulnerable to various attacks. These unprotected headers and added information are keys to launching traffic analysis attack which we will discuss in details in Section V.

III. P-Enc in a Communication System

In this section, we present the P-Enc scheme. P-Enc is performed on the modulated symbols. Each modulated symbol contains $n = \log_2 M$ bits of message, where M is the constellation size. Thus, P-Enc would depend on the modulation method. Fig. 4 shows the general structure for P-Enc. In the figure, $Q(\mathbf{x})$ is a function that maps the message $\mathbf{x}$ to the modulated symbol. $Q(\mathbf{x})$ is generally complex valued and it is dependent on the type of the employed modulation. If $Q(\mathbf{m})$ is in general complex valued, we use two bits of key stream, one for the in-phase portion of the modulated symbol and one for the quadrature portion of the modulated symbol. If $Q(\mathbf{m})$ is real valued, then only one branch is needed. In this case, the key streams required are reduced by half.

The decryption process follows the reverse procedure. The received ciphertext is first decrypted by multiplying the real and imaginary components of the ciphertext with the keystreams $\mathbf{a}$ and $\mathbf{b}$. After that, the standard demodulation and decoding technique is used to recover the messages.

Consequently, in P-Enc, the total key streams required vary with the underlying modulation as well as the constellation size M. We will explain in details of P-Enc with different modulation schemes and use mathematical models to analyze each scheme in Section IV.

Example: An illustration of P-Enc of a QPSK modulated symbol is shown in Fig. 5. Let the solid dot represent the modulated but unencrypted symbol, after the encryption, the resulting encrypted symbol could lie on any of the four dots depending on the value of the in-phase (real) and quadrature (imaginary) component of the key stream as shown in the figure.

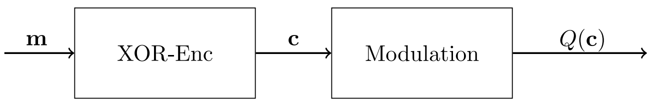


Fig. 6. XOR-Enc in a communication system.

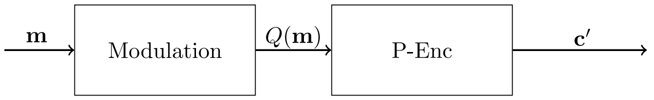


Fig. 7. P-Enc in a communication system.

IV. XOR-Enc and P-Enc Comparisons

In wireless communications, carrier modulation is often used. These carriers, namely, sinusoidal signals have three parameters: amplitude, frequency and phase. Transmitted messages are modulated using one or multiple of these parameters. Consequently, the most three common modulation methods are ASK, FSK and PSK [19].

In this section, we first give a high level overview of XOR-Enc and P-Enc used in a wireless communication system. Then, we break down into modulation specific scenarios. We will discuss a total of four modulation methods. In addition to the three aforementioned modulation methods, we also add QAM, which is a combination of ASK and PSK modulations. We use mathematical models to illustrate the difference between XOR-Enc and P-Enc in these modulated communication systems. We further analyze and compare the two encryption methods in terms of their security and encryption efficiency. We define the encryption efficiency to be the ratio of the ciphertext bits to the required key stream bits, the higher the ratio, the higher the encryption efficiency.

A. Overview of XOR-Enc and P-Enc in a Communication System

In this section, we omit channel coding, source coding and other baseband functions, we focus only on the modulation and encryption blocks. We will discuss XOR-Enc and P-Enc on a system level by taking into considerations of channel coding in Section V.

XOR-Enc and P-Enc in a communication system are illustrated in Figs. 6 and 7, respectively. In these two figures, $\mathbf{m}$ is the message, again $Q(\mathbf{x})$ is a function that maps the message $\mathbf{x}$ to the modulated symbol. $\mathbf{c}$ and $\mathbf{c}'$ are the resulting modulated ciphertext symbols for XOR-Enc and P-Enc, respectively.

By comparing Figs. 6 and 7, we see the order of encryption and modulation is reversed between XOR-Enc and P-Enc. XOR-Enc takes place prior to the modulation. Consequently, XOR-Enc is independent of the modulation methods. On the other hand, P-Enc takes place after the modulation, the required key stream size depends on the underlying modulation scheme as well as the constellation size.

B. Mathematical Formulations of XOR-Enc and P-Enc With Different Types of Modulation

In an M-ary modulated communication system, as discussed earlier, each modulated symbol contains $n = \log_2 M$ bits of message.

For XOR-Enc, the incoming message bits are first bitwise XORed with the key stream bits. Then the resulting ciphertext $\mathbf{c}$ is then divided into multiples of n-bit tuples, i.e., $\mathbf{c}_i \in \mathbb{F}_2^n$, where $i = 1, 2, \ldots$. The modulation is performed on each encrypted n-bit tuple.

On the other hand, for P-Enc, the message bits are first divided into multiples of n-bit tuples, then modulation is performed on these n-bit tuples. Ciphertext is subsequently generated by multiplying each of the in-phase and quadrature portion of the modulated symbol with one binary valued $\{1, -1\}$ key keystream bit.

In this section, we use mathematical formulations to illustrate XOR-Enc and P-Enc using different passband modulations. Based on our model, we further analyze and compare XOR-Enc and P-Enc in terms of security and encryption efficiency.

1) ASK Modulation: Let f_c be the carrier frequency, $p(t)$ be the pulse shape and denote the amplitude spacing to be $2a$, then the M-ary ASK modulated passband signal $s(t)$ at time t has the form

$$s(t) = Ap(t)\cos(2\pi f_c t), 0 \le t \le T$$

where $A = -(M-1)a, -(M-3)a, \ldots, (M-3)a, (M-1)a$.

Let $Q_{\mathrm{ASK}}(\mathbf{x}_i)$ be a function that maps ith symbol $\mathbf{x}_i$ to one of the M amplitudes using ASK modulation, $\mathbf{k}_i$ and k_i' represent key streams used for encrypting ith symbol in XOR-Enc and P-Enc, respectively, then we can model the ith modulated ciphertext symbol c_i and c_i' with XOR-Enc and P-Enc, respectively, by

$$c_i(t) = Q_{\mathrm{ASK}}(\mathbf{m}_i + \mathbf{k}_i)p(t)\cos(2\pi f_c t) \tag{1}$$

$$c_i'(t) = k_i' Q_{\mathrm{ASK}}(\mathbf{m}_i)p(t)\cos(2\pi f_c t). \tag{2}$$

Here, $0 \le t \le T$, $\mathbf{m}_i, \mathbf{k}_i \in \mathbb{F}_2^n$ and k_i' is binary valued between 1 and -1.

Comparing (1) and (2), we observe in XOR-Enc, ciphertext $\mathbf{m}_i + \mathbf{k}_i$ takes on the same space as message $\mathbf{m}_i$. Therefore, the modulated ciphertext symbol could lie on any one of the valid signal constellations. However, this is not the case for P-Enc. Encryption in P-Enc is achieved by changing the sign of the amplitude of the modulated message symbol. The magnitude of the amplitude remains unchanged. Another interpretation of this is that the encryption is performed by a potential phase shift of 0 or π between the modulated message and ciphertext symbols.

From (1) and (2), we observe that with XOR-Enc, if message $\mathbf{m}$ contains k symbols (nk bits), then the total key stream size is nk bits. This number reduces to k bits using P-Enc. Equivalently, the encryption efficiency for XOR-Enc and P-Enc are 1 and n, respectively. The minimum value of $n = 1$ for binary ASK modulation. Consequently, P-Enc would always require smaller or equal amount of key streams for M-ary ASK modulated systems. In general, the key stream size is reduced by a factor of n using P-Enc compared to XOR-Enc in an ASK-modulated communication system.

If the adversary performs random guessing on the received ciphertext symbols, then his successful probability for recovering message $\mathbf{m}$ with XOR-Enc $P_{\text{suc,ASK-XOR}}$ and P-Enc $P_{\text{suc, ASK}-P}$ are, respectively

$$P_{\text{suc, ASK}-\text{XOR}} = \frac{1}{2^{nk}}$$

$$P_{\text{suc, ASK}-P} = \frac{1}{2^k}.$$

2) PSK Modulation: Let f_c be the carrier frequency, θ be the message symbol represented in phase, then the M-ary PSK-modulated passband signal $s(t)$ has the form

$$s(t) = \cos\left(2\pi f_c t + \theta\frac{2\pi}{M}\right), 0 \le t \le T$$

where $\theta = 0, 1, \ldots, (M-1)$.

Now, let $Q_{\mathrm{PSK}}(\mathbf{x}_i)$ be a function that maps ith symbol $\mathbf{x}_i$ to one of the M phases, again $\mathbf{k}_i$ and k_i' denote key streams used for encrypting ith symbol in XOR-Enc and P-Enc, respectively, and $g(\mathbf{m}_i, k_i')$ be the phase shift of ith symbol using P-Enc with key stream k_i', then we can model the ith modulated ciphertext symbol c_i and c_i' with XOR-Enc and P-Enc, respectively, by

$$c_i(t) = \cos\left(2\pi f_c t + Q_{\mathrm{PSK}}(\mathbf{m}_i + \mathbf{k}_i)\frac{2\pi}{M}\right) \tag{3}$$

$$c_i'(t) = \cos\left(2\pi f_c t + Q_{\mathrm{PSK}}(\mathbf{m}_i)\frac{2\pi}{M} + g(\mathbf{m}_i, k_i')\right). \tag{4}$$

Here, $0 \le t \le T$, $\mathbf{m}_i, \mathbf{k}_i \in \mathbb{F}_2^n$, and k_i' is an integer between 0 and 3. k_i' can be generated using two bits of key stream.

Comparing (3) and (4), we observe in XOR-Enc, similar to ASK modulation, ciphertext $\mathbf{m}_i + \mathbf{k}_i$ takes on the same space as message $\mathbf{m}_i$. Therefore, the phase offset between the modulated message and ciphertext symbols is $\frac{2\pi l}{M}$, where $l = 1, \ldots, M-1$.

Recall that P-Enc is performed by multiplying each of real and quadrature components of the modulated symbol by a $\{-1, 1\}$ valued key stream, then the modulated ciphertext symbol using P-Enc only takes on four phase values which lies in four different quadrants and it is determined by the four key streams. Without loss of generality, we denote the phase that lies in the first quadrant as p_0, then the other three phase values are $\pi - p_0$, $\pi + p_0$ and $2\pi - p_0$.

Remark: If the M-ary PSK signal constellation is not symmetrical along the x-axis and y-axis, as it is the case when M is odd, then there exists an attack. When M is odd, the signal constellation is symmetrical only along the x-axis. Therefore, only two out of all four phases of the modulated ciphertext symbol lie in the valid signal constellation, the adversary can identify and remove those that are not belong to the signal constellation. Therefore, the searching space is reduced by half. This attack only exists when M is odd. In practise, $n = \log_2 M$, or $M = 2^n$. In this case, M is always even and all four phases of the modulated ciphertext lie in the valid signal constellation. Therefore, this attack is not applicable in practise.

In general, n is an integer greater than or equal to 2. Thus, in terms of required key stream size, if message $\mathbf{m}$ contains k symbols, then the total required key stream size is nk for XOR-Enc. This number becomes $2k$ for P-Enc. Equivalently, the encryption efficiency for XOR-Enc and P-Enc are 1 and $\frac{n}{2}$, respectively. The required key streams for P-Enc would always be smaller than or equal to that of XOR-Enc. In general, the key stream size is reduced by a factor of $\frac{2}{n}$ using P-Enc compared to XOR-Enc in a PSK-modulated communication system.

Remark: If Binary PSK (BPSK) modulation is used, then $n = 1$ and the modulated symbol only contains only the in-phase signal (real valued). This is identical to binary ASK. Thus, we only perform encryption on the real part of the modulated symbol. Consequently, the number of key streams required for XOR-Enc and P-Enc are still identical. In conclusion, P-Enc would always require smaller or equal amount of key streams for PSK-modulated systems.

If the adversary performs random guessing on the received ciphertext symbols, excluding the BPSK case, then his successful probability for recovering message $\mathbf{m}$ with XOR-Enc $P_{\mathrm{suc,PSK-XOR}}$ and P-Enc $P_{\mathrm{suc,PSK}-P}$ are, respectively

$$P_{\text{suc,PSK-XOR}} = \frac{1}{2^{nk}}$$
$$P_{\text{suc,PSK}-P} = \frac{1}{2^{2k}}.$$

If BPSK modulation is used, $P_{\text{suc,BSPK-XOR}}$ has the same form as ASK modulation, namely

$$P_{\text{suc,BSPK}-P} = \frac{1}{2^{k}}.$$

3) QAM Modulation: Let f_c be the carrier frequency, A_l be the symbol amplitude and θ_l be the phase, then the M-ary QAM-modulated passband signal $s(t)$ has the form

$$s(t) = A_l \cos(2\pi f_c t + \theta_l), 0 \leq t \leq T$$

where $l = 1, 2, \ldots, M$. Unlike ASK and PSK modulations where the modulation is performed either on the amplitude or the phase, QAM modulates message using both the amplitude and phase. Note that the values of amplitude A_l and phase θ_l depend on the type of the employed QAM.

Now, let $Q_{\mathrm{QAM}}(\mathbf{x}_i)$ be a function that maps ith symbol $\mathbf{x}_i$ to one of the M symbols using QAM modulation which contains a amplitude of $|Q_{\mathrm{QAM}}(\mathbf{x}_i)|$ and a phase of $\angle Q_{\mathrm{QAM}}(\mathbf{x}_i)$, let $\mathbf{k}_i$ and k_i' represent key streams used for encrypting ith symbol in XOR-Enc and P-Enc, respectively, and $g(\mathbf{m}_i, k_i')$ be the phase shift of ith symbol using P-Enc with key stream k_i', then we can model the ith modulated ciphertext symbol c_i and c_i' with XOR-Enc and P-Enc, respectively, by

$$\begin{aligned} c_i(t) = {} & |Q_{\mathrm{QAM}}(\mathbf{m}_i + \mathbf{k}_i)| \cos(2\pi f_c t + \\ & \angle Q_{\mathrm{QAM}}(\mathbf{m}_i + \mathbf{k}_i)) \end{aligned} \tag{5}$$
$$\begin{aligned} c_i'(t) = {} & |Q_{\mathrm{QAM}}(\mathbf{m}_i)| \cos(2\pi f_c t + \angle Q_{\mathrm{QAM}}(\mathbf{m}_i) + \\ & g(\mathbf{m}_i, k_i')). \end{aligned} \tag{6}$$

Here $0 \leq t \leq T$, $\mathbf{m}_i, \mathbf{k}_i \in \mathbb{F}_2^n$, and k_i' is an integer between 0 and 3. k_i' can be generated using two bits of key stream.

Comparing (5) and (6), we see for XOR-Enc, the modulated ciphertext symbol space is identical to the modulated message symbol space. Therefore, the modulated ciphertext symbol could be lie on any one of the valid signal constellations.

However, encryption using P-Enc is achieved by only changing the phase of the modulated message symbol, the amplitude remains unchanged. For P-Enc in QAM modulation, modulated ciphertext symbol also takes on four phase values and these four phase values are identical to PSK modulation. Using the same notation as PSK modulation, these four phase values are p_0, $\pi - p_0$, $\pi + p_0$ and $2\pi - p_0$.

Remark: Note that for M-ary QAM, signal constellation is always symmetrical along the x-axis and y-axis. The modulated ciphertext symbols of all four phases are also a valid modulated message symbol. Therefore, the attack described previously for PSK modulation is not applicable here.

In terms of required key stream size, if the message $\mathbf{m}$ contains k symbols, then for XOR-Enc, the total key stream size is nk. This number becomes $2k$ for P-Enc. Equivalently, the encryption efficiency for XOR-Enc and P-Enc are 1 and $\frac{n}{2}$, respectively. In general, the key stream size is reduced by a factor of $\frac{2}{n}$ using P-Enc compared to XOR-Enc in a QAM-modulated communication system.

If the adversary performs random guessing on the received ciphertext symbols, then his successful probability for recovering message $\mathbf{m}$ with XOR-Enc $P_{\text{suc,QAM-XOR}}$ and P-Enc $P_{\text{suc,QAM}-P}$ are identical to the PSK case, namely

$$P_{\mathrm{suc,QAM-XOR}} = \frac{1}{2^{nk}}$$
$$P_{\text{suc,QAM}-P} = \frac{1}{2^{2k}}.$$

4) FSK Modulation: P-Enc used under our context cannot be applied to FSK modulation. The reason is that the message bearer is the carrier itself. Therefore, applying P-Enc on the modulated symbol with the key stream will not hide the information. The fact that there has been a signal transmitted on that carrier is still revealed to the adversary. Thus, he can demodulate and decode the symbol back to the message bits.

5) Summary: In the previous section, we have shown the mathematical formulations for XOR-Enc and P-Enc using three passband modulations, namely, ASK, PSK and QAM modulations. Since XOR-Enc is performed prior to the modulation, we observe the required key stream size for XOR-Enc is independent of the modulation methods. However this is not the case with P-Enc. The required key streams depend on the modulated symbols as P-Enc is performed after the modulation. In the case of ASK modulation where the modulated symbol is real valued, only one key stream bit is required to encrypted one modulated symbol. In PSK and QAM modulations, the modulated symbol is in general complex valued. Therefore, two key stream bits are required to encrypt one modulated symbol. One bit for the in-phase component and one bit for the quadrature component of the modulated symbol. The only exception is BPSK modulation. Modulated BPSK symbol is also real valued. Therefore, only one bit key stream is needed for encryption. Finally, we have concluded P-Enc cannot be applied to FSK-modulated system.

TABLE I
RANDOM GUESSING SUCCESSFUL PROBABILITY COMPARISONS BETWEEN XOR-ENC AND P-ENC

Modulations	XOR-Enc	P-Enc
ASK	$P_{\rm suc} = \frac{1}{2^{nk}}$	$P_{\rm suc} = \frac{1}{2^{k}}$
PSK	$P_{\rm suc} = \frac{1}{2^{nk}}$	$P_{\rm suc} = \frac{1}{2^{2k}}$
QAM	$P_{\rm suc} = \frac{1}{2^{nk}}$	$P_{\rm suc} = \frac{1}{2^{2k}}$

In terms of security, if the adversary adopts the random guessing approach, then his successful probability for ASK, PSK and QAM modulations are summarized and listed in Table I.

From this table, we observe that XOR-Enc has a lower random successful random guessing probability than P-Enc. This is expected due to the increased key stream size. However, if the number of transmitted symbols k are sufficiently large, i.e., $k \geq 128$, then from the random guessing point of view, the reduced key size do not compromise the security of the underlying communication system.

V. PERFORMANCE ANALYSIS BETWEEN XOR-ENC AND P-ENC

In this section, we first explain how PHY layer P-Enc can prevent traffic analysis attack. Then, we compare P-Enc and XOR-Enc at the system level by taking into account the effect of channel coding.

A. PHY Layer P-Enc for Combating Traffic Analysis Attack

As it has been mentioned in Section II, the security functionalities of LTE E-UTRAN are implemented in the PDCP layer. The confidentiality of message contents is kept secure at this layer. Layer headers and other information which are added afterwards are not encrypted. They can be easily captured, and consequently revealed in plaintext to the adversary. This includes the PDCP, RLC, MAC headers and MAC control elements along with the optional padding in the MAC layer. Please refer to Fig. 3 for details.

For instance, in the MAC layer, an MAC PDU contains an MAC header, zero or more MAC control elements, zero or more MAC SDUs and optional paddings. One MAC header is consisted of one or multiple MAC PDU subheaders, each subheader corresponds to an MAC SDU, which contains the length of SDU in bytes and the value of LCID used to differentiate the logic channels for uplink and downlink. The control elements include instructions such as timing advance command, contention resolution identity and/or power headroom, etc [3]. The MAC header, control elements and paddings are not protected as they are sent in plaintext over the wireless channel. Thus, the adversary can conduct traffic analysis and recover these relevant information.

Moreover, we want to emphasize that MAC header in 802.11 contain MAC address of the transmitting and receiving devices [12]. By conducting traffic analysis, the identities of the two communicating parties are immediately revealed!

Traffic analysis attack can be prevented by employing encryption functions in the lowest (PHY) layer in the network protocol stack. That is if the data contents are encrypted just before the transmission, with no additional unprotected information being added, then the adversary cannot gain any useful information by analyzing the intercepted signals. This is exactly the case with PHY layer P-Enc. From Fig. 4, we observe that the encryption is taking place immediately prior to the DAC conversion and radio transmission, no additional unprotected information are added which would result in the information leakage.

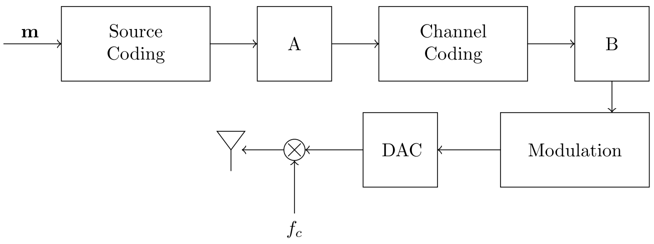


Fig. 8. PHY layer XOR-Enc in a communication system.

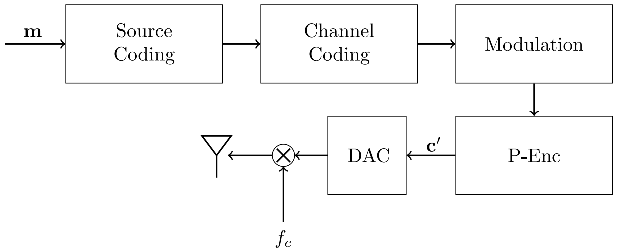


Fig. 9. PHY layer P-Enc in a communication system.

Remark: Note that XOR-Enc in the PHY layer would also prevent traffic analysis attack if there is no additional unprotected information being added to the packets before the transmission. Therefore, both XOR-Enc and P-Enc can thwart traffic analysis attack when performed at the PHY layer.

B. Comparison Between P-Enc and XOR-Enc

In the previous section, we have only considered encryption and modulation blocks for XOR-Enc and P-Enc. In this section, we analyze and compare XOR-Enc and P-Enc in terms of the efficiency and the security at the system level by taking into considerations of channel coding.

The system level XOR-Enc and P-Enc are shown in Figs. 8 and 9, respectively. On a system level, P-Enc still take place after immediately after the modulation block, while XOR-Enc can take place in one of two places, either in block A or block B as shown in Fig. 8, both are prior the modulation block. We now discuss these two cases separately.

1) Encryption Before Channel Coding: The encryption is taking place inside block A. Most communication systems adopt this order for conducting encryption and channel coding. The reason being channel coding introduces redundancies, the resulting codewords are expanded in length from the original message. For instance, the channel coding in LTE has specified different coding rates [2]. Suppose turbo code with a rate of $\frac{1}{3}$ is used, the length of the message is increased by a factor of 3 due to channel coding. Therefore, performing encryptions after the channel coding would triple the amount of required key streams. Thus, the encryption efficiency is reduced.

However, depending on the modulation rate, P-Enc may still have a higher encryption efficiency than XOR-Enc even if the encryption efficiency is reduced due to channel coding. This occurs when modulation and coding rates are high. For example, in the 802.11ac standard, when 256 QAM modulation and $\frac{5}{6}$ channel coding rate is employed [12], six key stream bits are required to encrypt one modulated message symbol using XOR-Enc. On an average, this number is reduced to $\frac{12}{5}$ bits with P-Enc. In this case, P-Enc still holds an advantage over XOR-Enc in terms of encryption efficiency.

2) Encryption After Channel Coding: The encryption is taking place inside block B. This can occur when the source coding and the channel coding are jointly encoded and decoded [8]. In this case, both XOR-Enc and P-Enc are performed after channel coding. Therefore, the channel coding would not have an impact on the encryption efficiency as it did in the previous case. Consequently, P-Enc would always have an equal or higher encryption efficiency than XOR-Enc. In the worst case, the two encryption schemes would result in the identical required key stream size. For higher rate modulations, i.e., $n > 2$, P-Enc would always require less key streams which results in a higher encryption efficiency.

In terms of security, from the random guessing point of view, if the same amount of key streams are used, then the security level is identical between P-Enc and XOR-Enc. If P-Enc uses less key streams as it is the case with high modulation and channel coding rate, then the efficacy is increased at the expense of some reduced security level. On the other hand, if the P-Enc uses more key streams as it is the case with lower modulation and channel coding rate, then the security level is increased at the expense of reduced encryption efficiency. Overall, there exists a tradeoff between the security level and the encryption efficiency.

VI. Simulation Results

In this section, we conduct simulations in MATLAB to compare P-Enc and XOR-Enc. Our simulations include three modulation schemes. They are ASK, PSK and QAM modulations. Moreover, in the simulation, we assume the channel is corrupted by the additive white Gaussian noise (AWGN). For each modulation, we compare the decoding SER as a function signal to noise ratio (SNR). In addition, we have selected three constellation sizes, $M = 2$, $M = 4$ and $M = 16$. Therefore, each modulated symbol contains $n = 1$, $n = 2$ and $n = 4$ bits, respectively. Finally, SER is computed over the average of 100 trials, each trial contains 10^5 modulated symbols for each modulation type.

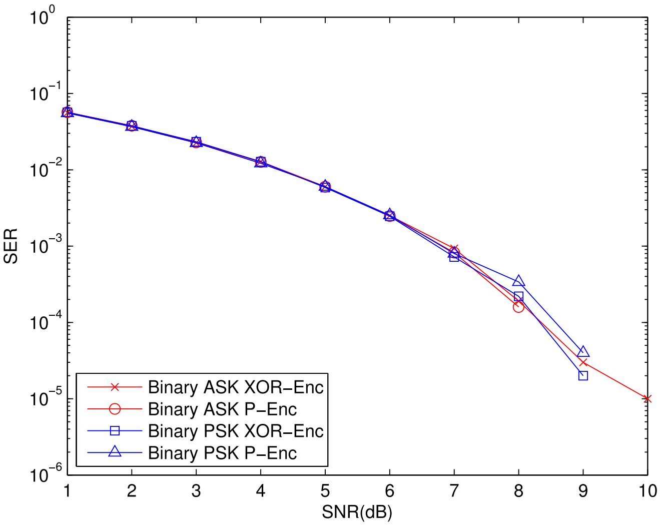


Fig. 10. SER versus SNR for $M = 2$.

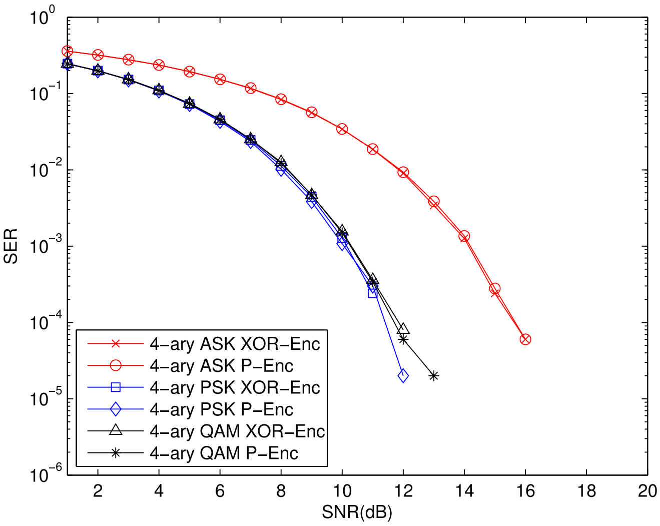


Fig. 11. SER versus SNR for $M = 4$.

The SER plot as a function of SNR for $M = 2$ is shown in Fig. 10. We have plotted for ASK and PSK modulations. When $M = 2$, the signal constellation between ASK and PSK modulations are identical. Thus, their decoding SER is expected to be identical. This is precisely the case as shown in the figure. Moreover, we can observe the SER between P-Enc and XOR-Enc is approximately the same, indicating their performances are comparable.

The SER plot as a function of SNR for $M = 4$ is shown in Fig. 11. When $M = 4$, the signal constellation between PSK and QAM modulations are identical. Thus, their decoding SER is expected to be identical. This has precisely been reflected in the figure. Moreover, with identical average transmitted power, 4PSK should have a lower SER than 4ASK. This has also been observed in the figure. Finally, we observe in all three modulations, the SER between P-Enc and XOR-Enc is approximately the same.

The SER plot as a function of SNR for $M = 16$ is shown in Fig. 12. We observe between the three modulations, QAM modulation has the lowest SER, followed by PSK modulation, ASK modulation has the worst SER. This agrees with the theory [19]. Once again, the SER between P-Enc and XOR-Enc is approximately the same.

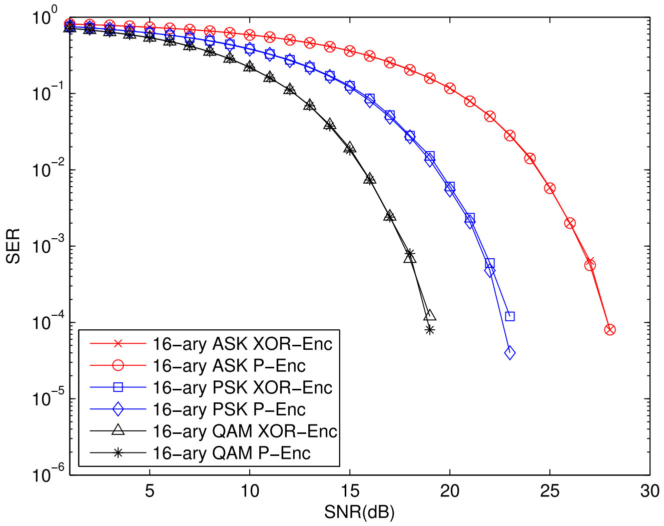


Fig. 12. SER versus SNR for $M = 16$.

TABLE II
XOR-ENC AND P-ENC COMPARISONS

	XOR-Enc	P-Enc
Key Stream Size	nk	k or $2k$
Resistance to Traffic Analysis	Yes	Yes
SER	$P_{e,\text{XOR−Enc}} = P_{e,P\text{ −Enc}}$	

From these plots, we have observed the performance of P-Enc is almost identical to that of XOR-Enc. In fact, this is theoretically true if the channel is AWGN. The reason is in XOR-Enc, the decoder first demodulate each encrypted symbol, then it performs the decoding. Each message symbol can be recovered provided the corresponding demodulated ciphertext symbol is correct. Therefore, SER in XOR-Enc is only dependent on the SNR ratio. In P-Enc, the decoder first decrypts the received symbol, then it performs the decoding. Each received ciphertext symbol is decrypted by multiplying a $\{1, -1\}$ valued keystream. Therefore, the decrypted symbol is the sum of the message symbol and noise modeled by a zero mean Gaussian random variable. Since a Gaussian random variable is symmetrical along the axis and this Gaussian random variable has a mean of 0, by multiplying 1 or -1 will not change the mean and the variance of the noise. Therefore, the SER for P-Enc is determined by the exact same SNR as XOR-Enc. Consequently, their overall performance is expected to be identical.

VII. Conclusion and Future Study

In this paper, we have extended the use of P-Enc to general communication systems. This include ASK, PSK and QAM modulated systems but not FSK modulated system. Then we have formulated mathematical models in order to analyze and compare XOR-Enc and P-Enc. Using the mathematical formulations, we compared the security and encryption efficiency between these two encryption methods. We also showed P-Enc at the PHY layer can resist traffic analysis attack. Moreover, we compared XOR-Enc and P-Enc at the system level when taking into considerations of channel coding. Finally, we conducted two simulations to compare the performance of XOR-Enc and P-Enc in terms of the decoding SER.

The advantage of P-Enc include the potentially reduced keystream size. Reducing the required keystreams imply saving power and dissipating less electromagnetic fields. This is very important in power constrained devices such as mobiles. Moreover, side channel attacks in the literature which rely on the measurement of power [15] and electromagnetic fields [11] becomes more difficult to realize. The disadvantage of P-Enc is that the hardware implementation is different from XOR-Enc and it may incur a higher hardware complexity cost. The reason is XOR operation can be efficiently implemented in hardware. However, for P-Enc, multiplier is needed.

The overall comparisons between XOR-Enc and P-Enc is summarized and listed in Table II. In general, P-Enc provides an alternative to XOR-Enc.

For future study, we would like to consider the following problems: 1) IEEE in August 2008 has issued an standard to compare different datasets using the feature selective validation technique [7], [13], [17], we would like to apply this technique to further compare and validate our P-Enc versus XOR-Enc results. 2) We have reasoned one impact of P-Enc on EMC is saving power and dissipating less electromagnetic fields. Since P-Enc has not been studied extensively, we would like pose the question that what other impacts would P-Enc have on EMC?

References

[1] *Evolved Universal Terrestrial Radio Access (E-UTRA): Security Architecture*, 3GPP TS 33.401 v11.7.0, 2013.

[2] *Evolved Universal Terrestrial Radio Access (E-UTRA): Physical Channels and Modulation*, 3GPP TS 36.211 v11.4.0, 2013.

[3] *Medium Access Control (MAC) Protocol Specification*, 3GPP TS 36.321 v11.3.0, 2013.

[4] *Evolved Universal Terrestrial Radio Access (E-UTRA): Packet Data Convergence Protocol (PDCP) Specification*, 3GPP TS 36.323 v11.2.0, 2013.

[5] L. D. Callimahos, "Introduction to traffic analysis," Declassified by NSA, 2008.

[6] L. Chen and G. Gong, *Communication System Security.* Boca Raton, FL, USA: CRC Press, 2012.

[7] A. P. Duffy, A. J. M. Martin, A. Orlandi, G. Antonini, T. M. Benson, and M. S. Woolfson, "Feature selective validation (FSV) for validation of computational electromagnetics (CEM). Part I—The FSV method," *IEEE Trans. Electromagn. Compat.*, vol. 48, no. 3, pp. 449–459, Aug. 2006.

[8] M. Fresia, F. Perez-Cruz, H. V. Poor, and S. Verdu, "Joint source and channel coding," *IEEE Signal Process. Mag.*, vol. 27, no. 6, pp. 1053–5888, Nov. 2010.

[9] F. Huo and G. Gong, "A new efficient physical layer OFDM encryption scheme," in *Proc. IEEE INFOCOM*, Apr. 2014, pp. 1024–1032.

[10] F. Huo and G. Gong, "Physical layer phase encryption for combating the traffic analysis attack," in *Proc. IEEE Int. Symp. Electromagn. Compat.*, Aug. 2014, pp. 604–608.

[11] M. Hutter, S. Mangard, and M. Feldhofer, "Power and EM attacks on passive 13.56 MHz RFID devices," in *Proc. Int. Workshop Cryptographic Hardware Embedded Syst.,* 2007, pp. 320–333.

[12] *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Std 802.11ac, 2013.

[13] *IEEE Standard for Validation of Computational Electromagnetics Computer Modelling and Simulations*, IEEE Std 1597, 2008.

[14] B. Javidi, "Noise performance of double-phase encryption compared to XOR encryption," *Opt. Eng.*, vol. 38, no. 1, pp. 9–19, Jan. 1999.

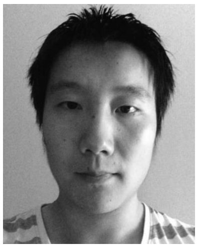
[15] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. 19th Annu. Int. Cryptology Conf. Adv. Cryptology*, 1999, pp. 388–397.

[16] LTE tutorial. (2014). [Online]. Available: http://www.tutorialspoint.com/lte/lte_layers_data_flow.htm

[17] A. Orlandi, A. P. Duffy, B. Archambeault, G. Antonini, D. E. Coleby, and S. Connor, "Feature selective validation (FSV) for validation of computational electromagnetics (CEM). Part II—Assessment of FSV performance," *IEEE Trans. Electromagn. Compat.*, vol. 48, no. 3, pp. 460–467, Aug. 2006.

[18] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Opt. Lett.*, vol. 20, no. 7, pp. 767–769, 1995.

[19] F. Xiong, *Digital Modulation Techniques.* Norwood, MA, USA: Artech House, 2006.



Fei Huo received the B.A.Sc., M.A.Sc., and Ph.D. degrees from the University of Waterloo, Waterloo, ON, Canada, in 2009, 2011, and 2014, respectively.

His research interests include sequences design, application and physical layer security for wireless communication systems.

Guang Gong (M'00–SM'07–F'14) received the B.S. degree in mathematics from Xichang Normal College, Xichang, China in 1981, the M.S. degree in applied mathematics from Xidian University, Xian, China in 1985, and the Ph.D. degree in electrical engineering from the University of Electronic Science and Technology of China (UESTC), Chengdu, China in 1990, and a Postdoctoral Fellowship from the Fondazione Ugo Bordoni, Rome, Italy.

She was promoted to an Associate Professor at the University of Electrical Science and Technology of China, Chengdu, China. During 1995–1998, she worked with several internationally recognized, outstanding coding experts and cryptographers, including S. W. Golomb, at the University of Southern California. She joined the University of Waterloo, Waterloo, ON, Canada, in 1998, as an Associate Professor in the Department of Electrical and Computer Engineering in September 2000. She has been a Full Professor since 2004. Her research interests include the areas of sequence design, cryptography, and communication security. She has authored or coauthored more than 250 technical papers and two books. She serves/served as an Associate Editor for several journals, and served on a number of technical program committees and conferences as cochairs or committee members.

Dr. Gong has received several awards including the Best Paper Award from the Chinese Institute of Electronics in 1984, Outstanding Doctorate Faculty Award of Sichuan Province, China, in 1991, the Premiers Research Excellence Award, Ontario, Canada, in 2001, NSERC Discovery Accelerator Supplement Award, 2009, Canada, and Ontario Research Fund—Research Excellence Award, 2010, Canada, Best Paper Award of IEEE ICC 2012.