Physical Layer Security for Wireless Networks Based on Coset Convolutional Coding

Michael Ekonde Sone

College of Technology, University of Buea, Cameroon

***Abstract*:** This paper presents a new physical layer security for wireless networks using non-linear convolutional cryptosystem. Relevant performance metrics such as secret channel capacity and throughput are considered in the implementation. Secret channel capacity is implemented using confusion bits generated from coset convolutional coding while throughput is enhanced due to the forward error correction capability of convolutional codes. The paper establishes a method to determine wireless channel parameters for secure communication. It is shown that, the probability of correct decision of an eavesdropper is zero when appropriate values of M-PAM constellations, the number of transmitted bits, k and the signal-to-noise ratio (SNR) per bit in dB are chosen. In addition, it is shown that, the convolutional cryptosystem enhances security for the case where the eavesdropper probability of correct decision is not zero. The entire scheme applied to CDMA is ported to a Virtex 5 FPGA chip to circumvent poor key management due to additional keys used in the convolutional cryptosystem.

***Keywords*:** Non-linear convolutional cryptosystem, Programmable Gate Array, Coset coding, secret channel capacity, Field Programmable Gate Array (FPGA), Signal-to-Noise Ratio (SNR).

1. Introduction

Wireless transmission channel which is used to transmit encrypted data from an upper layer is susceptible to security threats such as eavesdropping. To circumvent this drawback, existing physical layer security techniques explore Shannon’s notion of perfect secrecy which is the theoretical basis for the information-theoretic approach [1],[2],[3]. A general setup for a wiretap channel based on perfect secrecy which guarantees both transmission errors correction and data confidentiality was proposed by Wyner [4]. In this wiretap channel, the legitimate users were assumed to have a better channel compared to the eavesdropper. In [5], the authors used a full channel state information (CSI) of the legitimate receiver which is known at the transmitter to adopt the upper bound of secret capacity. In [6], the authors used the CSI to establish a four-step procedure of security measures for assessing average secure key generation rates. However, the existing methods for implementing physical layer security under the different information-theoretic security models is expensive and requires assumptions about the communications channels that may not be accurate in practice [7],[9]. Recently, it has been recommended that [8], efficient security schemes deployed in the physical layer should involve a layered approach and the design of protocols that either combine traditional cryptographic algorithms or efficient coding methods with physical layer techniques. The traditional cryptographic algorithms or efficient coding methods will complement the information-theoretic security models in situations where the assumptions about the communication channels are not accurate. This research adopts an efficient coding method to complement information-theoretic security model. In the design of the protocol, relevant performance metrics to be considered in this research are secret channel capacity and data throughput. In [10] the forward error correction capability of non-linear convolutional was presented. Hence, this paper will present only findings on the secret channel capacity as the relevant performance metric.

In order to address the secret channel capacity metric, the scheme developed in [11] is extended to include another level of security using information-theoretic security techniques at the physical layer. This is achieved by implementing coset coding such that, different number of bits of confusion are used to transmit the data points. With the introduction of the bits of confusion, the capacity of an eavesdropper is wasted in decoding additional confusion bits instead of the message. It is shown that, the new technique could prevent an eavesdropper attack over a wireless channel if appropriate values of the M-PAM constellations, the number of bits, k per data point transmitted

and the signal-to-noise ratio (SNR) per bit in dB are chosen. For example, the probability of correct decision of an eavesdropper is zero for M=32, k=4, SNR/bit=12dB.

It should be noted that, perfect security is ensured under the afore-mentioned conditions of M-PAM constellations, the number of bits, k per data point transmitted and the signal-to-noise ratio (SNR) per bit in dB. However, if these conditions are not met due to the randomness of the wireless channel parameters or vantage position of the eavesdropper, attack is very difficult due to the additional keys used in the non-linear convolutional cryptosystem. Hence both security and throughput are enhanced using this scheme as opposed to existing schemes.

In addition, data throughput is enhanced due to the forward error correction capability of convolutional codes. The keys used for the different transitions of the convolutional cryptosystem are embedded in an FPGA at the transmitter and receiver. An FPGA implementation applied to CDMA could fit into a single FPGA. By using FPGA implementation, there is efficient key management compared to existing schemes such as AES CDMA and Rand-MIMO [2] and random key generation in MANETS [17].

The complete outline of the paper is as follows. In the next section, a review of non-linear convolutional cryptosystem is presented [14]. The non-linear convolutional coding is implemented by inserting product ciphers between conventional convolutional coding blocks. A methodology for the generation of additional bits of confusion using coset coding is presented in section 3. This section also presents the implementation of a new wiretap code by establishing expressions which could be used to determine the probability of correct decision of an eavesdropper based on the signal-to-noise ratio of the channel. Section 4 presents the protocol for the implementation of the new security scheme. The

FPGA-based implementation applied to CDMA using the new security scheme will be presented in section 5. Results and performance analysis of the wiretap code based on the secret channel capacity will be presented in section 6. Finally, the conclusion and future work are presented in section 7.

2. Review of Non-linear Convolutional Cryptosystem [10]

A convolutional code [13] is generated by passing the information sequence to be transmitted through a linear finite-state shift register. The shift register consists of L (k-bit) stages and n linear algebraic function generators. The n linear algebraic function generators produce the n output bits for each k-bit input sequence [13]. Such an encoder produces an (n, k, L) convolutional code. The function generators are assembled into a generator matrix [13]. The generator matrix is specified functionally by using a set of n vectors, with one vector for each of the n modulo-2 adders. Each vector has Lk dimensions and contains the connections of the encoder to the modulo-2 adder. To obtain a convolutional cryptosystem from the convolutional code, a product cipher is inserted between stages of the convolutional codes.

A simple non-linear (8, 8, 2) 2-cascaded cryptosystem shown in figure 1 which corresponds to 2^8-PAM constellation will be used to illustrate the implementation of the convolutional cryptosystem.

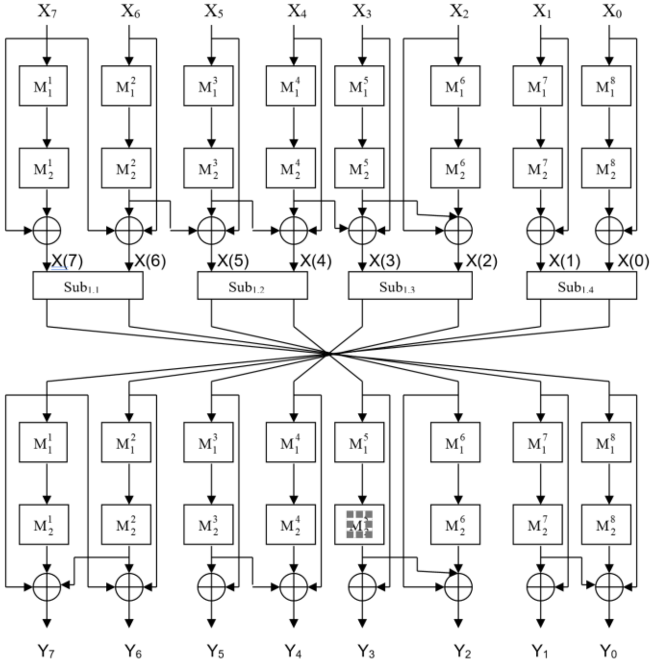


Figure 1. Initial structure of a non-linear (8,8,2) 2-cascaded cryptosystem

It is worth noting that the security level could be greatly increased by increasing the number of stages to be cascaded. In figure 1, $Sub_{1,1}$, $Sub_{1,2}$, $Sub_{1,3}$ and $Sub_{1,4}$ are S-boxes used for pairwise bit shuffling.

The specifications of the private keys used in the implementation of the (8, 8, 2) 2-cascaded cryptosystem are as follows [11], [14], [15]:

- States of each cryptosystem in the cascade given by the contents of the sub-matrices in the generator matrix.
- The next set of private keys is the transition functions, comprising 2^8 = 256 mappings. Each mapping compares the plaintext bits and present state and switches to the appropriate next state. Depending on the plaintext bits, the next state could be either of the two possible states. For the decoding process, the transition functions are similar to those for the encoder but change roles. The function which originally controls the change of states for the first stage in the encoder will instead control the change of states in the second stage of the decoder. The transition functions account for the dynamic nature of the cryptosystem.
- 2-bit S-boxes. They are used to shuffle the output of the first transducer stage of the cascade. For the (8, 8, 2) 2-cascaded scheme, four 2-bit shuffle boxes are required. The 2-bit shuffle boxes used in the scheme are displayed in table 1.

For the decoding process, the entries in the 2-bit shuffle boxes are similar to those presented in table 1, with the difference being the interchange of the inputs and the outputs for each box.

Table 1. 2-bit shuffle look-up table for encoder

$Sub_{1,1}$				
Input	00	01	10	11
Output	00	11	10	01
$Sub_{1,2}$				
Input	00	01	10	11
Output	01	00	11	10
$Sub_{1,3}$				
Input	00	01	10	11
Output	10	01	00	11
$Sub_{1,4}$				
Input	00	01	10	11
Output	11	10	01	00

- Different permutations per level of decomposition. There are eight outputs from the 2-bit shuffle boxes and eight inputs into the second transducer stage of the cascade for each channel. A permissible permutation used in this scheme is shown in table 2 [11],[15].

Table 2. Input-Output interconnect look-up-table for encoder

Input	1	2	3	4	5	6	7	8
Output	8	7	6	5	4	3	2	1

For the decoding process, the entries in the sets of permutation boxes are similar to those for the encoder, with the difference being the interchange of the inputs and the outputs.

3. Design of Coset Coding

In this section, coset coding for secrecy which is the main technique behind wiretap coding is presented. Coset coding relies on the idea that an information message is mapped to a set of codewords or coset [4]. The bit representation of the codewords in the sets result in additional bits called confusion bits which the eavesdropper sees.

3.1 Coset Coding Basics

Consider an M-PAM constellation of the form {0,1,2,- - - ,M} where M is a power of 2. The information bits will be used to locate the coset while the confusion bits are used to identify the different symbols in the constellation. To communicate one (1) information bit, the M-PAM constellation is partitioned into two cosets. In general, to communicate higher number of bits, the M-PAM constellation is appropriately partitioned into many cosets. This idea will constitute the basis for the implementation of the proposed multi-level coset coding.

The following parameters will used in the implementation of the proposed coding scheme:

- n = number of bits per data point;
- m_i = number of data points;
- M = number of constellations;
- M_L = number of cosets per level.

For $M = 2^n$ constellation points, the number of cosets, $M_L = M/2^k$ where k is the number of message or information bits transmitted. Hence, k could be computed as

$$k = \log_2 M/M_L \qquad (1)$$

The number of confusion bits per coset necessary to transmit n information bits is given as

$$L_c = n - k \qquad (2)$$

Using the expression of n we have,

$$L_c = \log_2 M - k \qquad (3)$$

(1) in (3) gives

$$L_c = \log_2 M_L \qquad (4)$$

Therefore, the number of confusion bits required, L_{ci} for m_i data points is given as

$$L_{ci} = m_i \log_2 M_L \qquad (5)$$

3.2 Design of the wiretap code

Wiretap coding model takes k bit message and maps it to an entire space of n bits such that $2^{(n-k)}$ code words correspond to each possible message. One of these code words is chosen at random and transmitted. The model is such that, the eavesdropper Eve can have full knowledge of the encoding scheme and its parameters. However, the wiretap channel's security is based on the fact that Eve uses the knowledge to decode the wrong cosets whose points are labelled by confusion bits. In the wiretap encoding scheme, Alice starts with an (n-k)-bit secret message, m to be communicated to Bob. Alice then selects one of the 2^k elements, u of the coset at random and performs the following calculation:

$$x = [m \quad u]\begin{bmatrix} G^* \\ G \end{bmatrix} \qquad (6)$$

where x is the transmitted code word over wiretap channel; G is the generator matrix for code C which is a subspace of $\{0,1\}^n$ with 2^k elements; and G* is the generator matrix for code C′ which is a complimentary subspace such that C and C′ together form the full n-dimensional space of binary numbers: $C \cup C' = \{0,1\}^n$.

Assuming noise-free main channel, Bob receives the code word x without errors and performs the following computation:

$$Hx^T = (mG^* + uG)^T = H(mG^*)^T \qquad (7)$$

where x^T is the transpose of x and H is the parity check matrix. The expression $S = H(mG^*)^T$ is the syndrome which uniquely determines the coset corresponding to message while uG is the code word and mG* is akin to noise. Eve's channel is inferior to Bob's and due to mG* she receives a corrupted version of the code word x. This assumption on Eve and her channel will be the basis for the design of the new non-linear wiretap code. Performance of the proposed non-linear convolutional coset coding scheme could be analysed in terms of the probability of correct decision for Eve. In effect, the probability of Bob and Eve making the correct decoding decision and using the assumption on Eve and her channel, try to maximize Bob's probability while minimizing the one of Eve. For classical M-PAM, the average probability of a symbol error could be expressed as [13]

$$P_e = 2\left(1 - \frac{1}{M}\right) Q\left(\frac{d_{min}}{2\sigma}\right) \qquad (8)$$

where d_{min} is defined as the minimum distance between any two data symbols in a signal constellation and σ^2 is the channel noise variance. The M-PAM minimum distance is a function of the average energy, E_{av} and M given as [13]

$$d_{min} = \sqrt{\frac{12\ E_{av}}{M^2-1}} \qquad (9)$$

Hence, using (9) in (8), the probability of correct symbol detection is given as

$$P_c = 1 - 2\left(1 - \frac{1}{M}\right) Q\left(\sqrt{\frac{12E_{av}}{(M^2-1).4\sigma^2}}\right) \qquad (10)$$

In plotting the probability of a symbol error, it is customary to use the average SNR/bit, E_{bav}/N_o as the basic parameter. Hence, using $\sigma^2 = N_o r$ where N_o is the average noise power and r is the symbol rate, (10) could be expressed in terms of the average SNR/bit, as [12]

$$P_c = 1 - 2\left(1 - \frac{1}{M}\right) Q\left(\sqrt{\frac{3(\log_2 M)E_{bav}}{(M^2-1)N_o}}\right) \qquad (11)$$

Considering the proposed wiretap channel, the probability $P_{c,b}$ of Bob's correct decision is based on the channel noise effect for the different levels of decomposition while that of Eve, $P_{c,e}$ is based on both the channel noise and the confusion bits. Hence, the probability $P_{c,b}$ of Bob's (resp. $P_{c,e}$ of Eve's) correct decision is:

$$P_{c,b} = 1 - 2\left(1 - \frac{1}{M}\right) Q\left(\sqrt{\frac{3(\log_2 M)E_{bav}}{(M^2-1)N_{ob}}}\right)$$

$$P_{c,e} = 1 - \left(2\left(1 - \frac{1}{M}\right) Q\left(\sqrt{\frac{3(\log_2 M)E_{bav}}{(M^2-1)N_o}}\right) + P_{eve}\right)$$

The P_{eve} factor in the $P_{c,e}$ expression is the probability of symbol error under the influence of the confusion bits. The aim of the design is to minimize the probability $P_{c,e}$ of Eve making a correct decision and have Bob's probability of making a correct decision close to 1.

The expression for P_{eve} could be obtained by re-defining the minimum distance, d_{min} based on wiretap coset coding. Hence the d_{min} is defined as one-half of the distance between amplitude levels of corresponding signal constellation points in adjacent cosets. For M constellation points and M_L cosets, the number of constellation points per coset, $n_o = M/M_L$. Figure 2 shows the minimum distance with respect to the number of signal constellation points per coset.

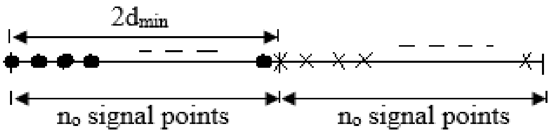


Figure 2. Minimum distance for signal points in adjacent cosets

Any signal constellation points within a coset will give the same decoded message by Bob, hence signal points less than or equal to half 2d$_{min}$ will lie in the same coset and lead to correct decision. From (10), the new d$_{min}$ based on wiretap coset coding will be

$$d_{min} = \frac{n_o}{2} \cdot \sqrt{\frac{12\ E_{av}}{M^2-1}} \tag{12}$$

Using (11) and (12), P$_{eve}$ could be given as

$$P_{eve} = 2\left(1-\frac{1}{M}\right) Q\left(\sqrt{\frac{n_o^2}{4} \cdot \frac{3(log_2 M)E_{bav}}{(M^2-1)N_o}}\right) \tag{13}$$

Using (5), n$_o$ could be written as

$$n_o = \frac{M}{2^{L_{ci}/m_i}}$$

where L$_{ci}$ is the number of confusion bits per level and m$_i$ is data points transmitted per level. Replacing n$_o$ in (13) we have

$$P_{eve} = 2\left(1-\frac{1}{M}\right) Q\left(\sqrt{\left(\frac{M}{2^{L_{ci}/m_i}}\right)^2 \cdot \frac{3(log_2 M)E_{bav}}{4\ (M^2-1)N_o}}\right) \tag{14}$$

Hence, using (14) in the expression of P$_{c,e}$, the probability of Eve's correct decision is given as

$$P_{c,e} = 1 - \left(2\left(1-\frac{1}{M}\right)\left(\left(Q\left(\sqrt{\frac{3(log_2 M)E_{bav}}{(M^2-1)N_o}}\right) + Q\left(\sqrt{\left(\frac{M}{2^{L_{ci}/m_i}}\right)^2 \cdot \frac{3(log_2 M)E_{bav}}{4\ (M^2-1)N_o}}\right)\right)\right)\right) \tag{15}$$

4. Design of Coset Coding

The detail operations at the source and destination are as follows:

- Source:
  - ➢Step 1: Identify the M-PAM constellation used for the wireless transmission;
  - ➢Step 2: Symmetric encryption using Convolutional cryptosystem;
  - ➢Step 3: Perform coset coding to conceal ciphertext based on the number of information or message bits and the number of constellation points.
- At the destination, the entire process is reversed starting with the verification of the channel parameters for secure communication followed by symmetric decryption using convolutional cryptosystem.

Illustration

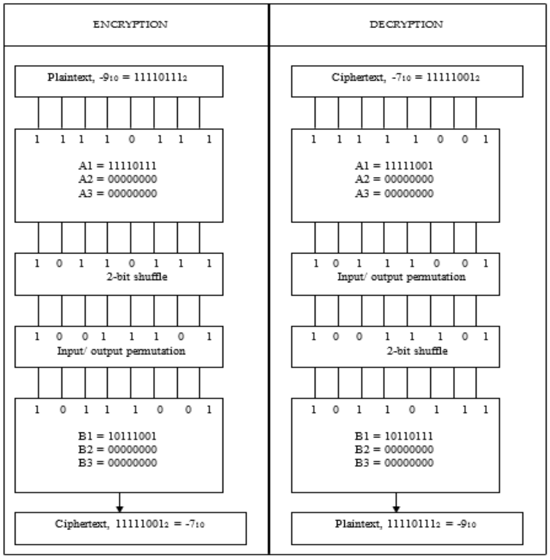
Consider a 2^8-PAM constellation used for the wireless transmission.

In figure 1, A2, A3 represent the registers M_1^2, M_2^2 for the first transducer stage while B2, B3 represent the registers M_1^1, M_2^1 for the second transducer stage during encoding. A1 and A2 are the inputs to the encoding blocks. The combinational logic based on mod-2 adder connections in figure 1 is as follows:

First state for first transducer, q$_{11}$;	Second state for first transducer, q$_{12}$;
X(7) := A1(7) ⊕ A3(7) ;	X(7) := A1(7) ⊕ A3(7) ;
X(6) := A1(7) ⊕ A1(6) ⊕ A3(6)	X(6) := A1(6) ⊕ A1(7) ⊕ A3(6)
X(5) := A1(5) ⊕ A3(5) ⊕ A3(6) ;	X(5) := A1(5) ⊕ A3(5) ;
X(4) := A1(4) ⊕ A3(4) ⊕ A3(5)	X(4) := A1(4) ⊕ A3(5) ⊕ A3(4)
X(3) := A1(3) ⊕ A3(3) ⊕ A3(4);	X(3) := A1(3) ⊕ A3(3) ;
X(2) := A1(2) ⊕ A3(2) ⊕ A3(3)	X(2) := A1(2) ⊕ A3(2) ⊕ A3(3)
X(1) := A1(1) ⊕ A3(1);	X(1) := A1(1) ⊕ A3(1) ⊕ A3(2);
X(0) := A1(0) ⊕ A3(0)	X(0) := A1(0) ⊕ A3(0) ⊕ A3(1)

Table 3 summarizes the manual computation of the encryption and decryption process of the convolutional cryptosystem for plaintext, -9$_{10}$ = 11110111$_2$ in 2s complement based on the entries of the product cipher and combinational logic of the non-linear (8,8,2) 2-cascaded convolutional transducer in figure 1.

Table 3. Manual computation for encryption/ decryption



5. FPGA-Based Implementation of New Scheme Applied to CDMA

Considering a (8, 8, 2) non-linear cryptosystem which corresponds to a 256-PAM constellation for illustrative purposes, the mapping process will involve M = 2^8 =256 orthogonal waveforms. Using the dynamic range of [-128, 126] , a set of M = 2^8 = 256 orthogonal waveforms is required to completely represent all the integers or symbols. Based on this, the corresponding Hadamard matrix obtained from the procedure elaborated in [23] is as follows:

$$H_{256} = H_{128} \otimes H_{128}$$
$$= \begin{pmatrix} H_{128} & H_{128} \\ H_{128} & \overline{H}_{128} \end{pmatrix}$$

The H$_{256}$ matrix is a large matrix comprising of 256 rows and 256. The Hadamard matrix results into a multi–dimensional array. Multi–dimensional arrays are arrays with more than one index. Multi–dimensional arrays are not allowed for hardware synthesis. One way around this is to declare two one–dimensional array types. This approach is easier to use and more representative of actual hardware. The VHDL code used to declare the two one–dimensional array types are shown in figure 3 [16].

```
  Subtype Depth_Typ is Integer range 0 to 255;
 Subtype Width_Typ is Integer range 255 downto 0;
 Subtype Data_Typ is Bit_vector (Width_Typ);
Type Memory_Typ is array (Depth_Typ) of Data_Typ;
```

Figure 3. VHDL code for synthesizable 256 x 256 Hadamard matrix

The other operations in the hardware Walsh function generator implementation are trivial since they involve modulo–2 addition with built–in operators in VHDL code to handle such operations.

Using the synthesis tools and the libraries associated with the Xilinx platforms (**Xilinx-ISE**), the architecture was synthesizable. The summary of the synthesis result generated by synthesis tool simulator using the newly developed package is slightly different from the results presented in [15] due to the additional security at the physical layer.

The device utilization summary is as follows:

- Number of slices: 12431 out of 89088 14%
- Number of slice Flip flops: 180 out of 178176 0%
- Number of 4 input LUTs: 10452 out of 178176 6%
- Number of bonded IOBs: 340 out of 960 35%
- IOB Flip flops: 16

With respect to the place and route operation, the total REAL time to Router completion was 28mins 9secs and the total REAL time to place and route (PAR) completion was 29mins 22secs. The entire PAR operation required a peak memory usage of 681 MB. In addition, from the report, it was seen that 20124 out of 30651 have pin delays less than 1.00ns given a percentage of 65.6%.

6. Results and Discussions

In this section, results obtained from probability of correct decision expressions established in section 3 will be presented. In addition, cryptanalysis will be performed if conditions of secure transmission are not met due to the randomness of the wireless channel parameters or vantage position of the eavesdropper.

6.1 Results and Performance Analysis

Using (11), the probability of Bob's correct decision for different M-PAM constellations is shown in figure 4. Bob's probability of correct decision is maximum for a signal-to-noise ratio per bit, E_{bav}/N_o of 10dB for M = 4. For higher values of M-PAM constellations, the SNR/bit increases for the maximum probability value, $P_{b,c,max} = 1$ to be attained.

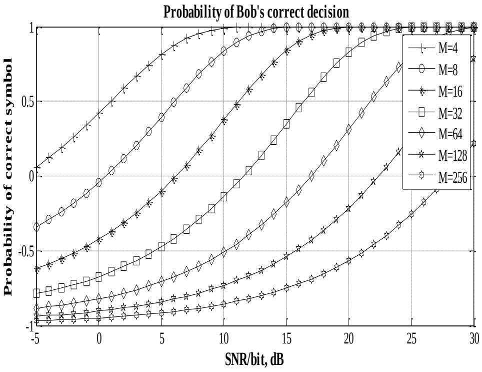


Figure 4. Probability of Bob's correct decision

The probability, $P_{c,e}$ of Eve's correct decision is directly related to the block number of samples transmitted and the number of bits per sample.

Table 4 shows the generated number of confusion bits for different M-PAM constellations using k = 2 and k = 4 information bits to transmit message sample points.

Table 4. Number of confusion bits generated

M constellations	No. of confusion bits, L_{ci} for k =4	No. of confusion bits, L_{ci} for k =2
256	32	48
128	24	40
64	16	32
32	8	24
16	-	16
8	-	8
4	-	-

(15) will be used to establish the probability of Eve's correct decision for different information bits, k required to identify a coset. Figure 5 and figure 6 show the probability of Eve to correctly decode a message symbol at decomposition level 1 for k = 4 and k = 2 respectively for the different M-PAM constellations.

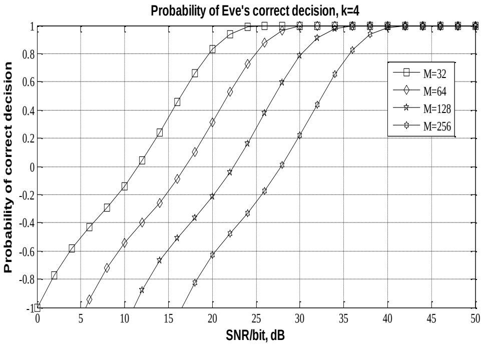


Figure 5. Probability of Eve's correct decision for k=4

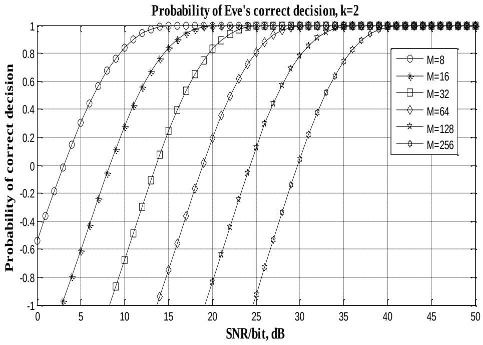


Figure 6. Probability of Eve's correct decision for k=2

In figure 5, simulation is not possible for lower values of constellation such as M = 4, 8 or 16 since with k = 4 information bits there is no possibility of generating confusion bits. From figure 5 and figure 6, it is shown that, the minimized value of Eve's probability of correct decision, $P_{c,e}$ is affected slightly by the number of information bits, k since it is approximately 13dB for M = 32 for k = 2 and k = 4. In addition, to minimize $P_{c,e}$ the SNR/bit increases with the constellations, M. Finally, the scheme is not suitable if the main channel and the wiretap or eavesdropper's channel has the same high SNR/ bit above 20dB.

6.2 Cryptanalysis

Figure 5 and figure 6 show bounds of perfect secrecy from the eavesdropper. This region corresponds to values of $P_{c,e} = 0$ for different values of k bits and M constellations. However, for regions where $0 < P_{c,e} < 1$, the new physical security scheme offers additional security compared to the existing scheme in [11]. For example in figure 5, for k = 4 and M = 32, there is a 20% probability of correct decision which implies an 80% increase in the security level. It was shown in [11] that, the number of steps, S required for a partial key exposure attack on N-cascaded stage convolutional cryptosystem is given as

$$S = \left\{\left[p.\left[\frac{q.2^k}{p-k-1} * \frac{q.2^k}{p} * \frac{k!}{p} * \frac{1}{p} * \left(\frac{k}{2}\right)^2 * 2^2\right]\right]^N\right\} \qquad (16)$$

where p = number of blocks of input data; q = number of states in the convolutional transducer.

The additional number of steps, S_2 required due to the percentage increase in the eavesdropper wrong decision is given as

$$S_1 = S. (1 + (1 – P_{c,e})) \qquad (17)$$

where $P_{c,e}$ is the expression in (15).

Hence, the total number of steps, S_T required for a partial key attack on the new layered security scheme at the physical layer is given as

$$S_T = \left(1 + (1 - P_{c,e})\right).\left\{\left[p.\left[\frac{q.2^k}{p-k-1} * \frac{q.2^k}{p} * \frac{k!}{p} * \frac{1}{p} * \left(\frac{k}{2}\right)^2 * 2^2\right]\right]^N\right\} \qquad (18)$$

(18) and (16) will used to compare the new physical security scheme and the existing scheme in [11] as shown in table 5.

Table 5. Number of steps required to break the 2-cascaded transducer

Operand key length	Existing security scheme [10]	New physical security scheme
16-bit	$2.1\text{x}10^{57}$	$9.4\text{x}10^{61}$
32-bit	$1.4\text{x}10^{57}$	$6.2\text{x}10^{61}$
64-bit	$1.5\text{x}10^{62}$	$6.7\text{x}10^{66}$
128-bit	$6.1\text{x}10^{71}$	$2.7\text{x}10^{76}$
256-bit	$9.87\text{x}10^{87}$	$4.4\text{x}10^{92}$
512-bit	$2.68\text{x}10^{112}$	$1.2\text{x}10^{117}$

The values of the number of steps required for the physical layer security scheme were computed for M = 256, k =2 and SNR/bit = 32dB and (1 – $P_{c,e}$) = 0.8 from figure 4. A close inspection of the values displayed in table 5 shows that there is a slight increase in the number of steps required to break the new physical security scheme compared to the scheme in [11].

7. Conclusion

In this paper, a new physical layer security technique for wireless transmission is proposed. The rationale in designing the new scheme is to establish parameters for secure wireless transmission parameter and to complement existing security if the appropriate parameters are not tenable due to channel randomness. The new physical layer security is implemented using coset non-linear convolutional coding. Coset coding introduces additional confusion bits, which eliminates eavesdropping. The results of this research establishes bounds based on the parameters of a fading channel such as the M-PAM constellations, the number of bits per data point transmitted and the signal-to-noise ratio (SNR) per bit in dB for the probability of correct decision of the eavesdropper to be zero. However, due to the randomness of the wireless channel, if the appropriate parameters to prevent eavesdropping are not obtainable, results in this research show that, attack is difficult since the product ciphers used in the non-linear convolutional cryptosystem increases the cryptographic complexity. The entire scheme was implemented in a Virtex-5 FPGA and applied to CDMA signal to circumvent the key management drawback associated with symmetric cryptographic schemes.

Future work will associate the new physical layer security with CBC-X for the transmission of packets at the link layer in order to provide for security services such as authentication and data integrity in addition to confidentiality. The new security scheme will also be applied to Wireless Mesh Networks (WMN) and Cooperative networks.

References

[1] A. Khisti, G. W. Wornell, “Secure Transmission with Multiple Antennas: The MIMOME Wiretap Channel,” IEEE Trans. Inform. Theory, vol. 56, pp. 3088–3104, 2010

[2] F. Oggier, B. Hassibi, “The Secrecy Capacity of the MIMO Wiretap Channel,” IEEE Int’l. Symp. Info. Theory, pp. 524–28, 2008.

[3] S. Leung-Yan-Cheong, M. Hellman, “The Gaussian WireTap Channel,” *IEEE Trans. Info Theory*, pp. 451–56, 1978.

[4] A. D. Wyner, “The Wire-Tap Channel,” Bell System Technical Journal, vol. 54, issue 8, pp. 1355–1387, 1975.

[5] M. Bloch *et al.*, “Wireless Information-Theoretic Security,” *IEEE Trans. Info. Theory*, pp. 2515–34, 2008.

[6] J. Barros, M. R. D. Rodrigues, “Secrecy Capacity of Wireless Channels,” *IEEE Int’l. Symp. Info. Theory*, pp. 356–60, 2006.

[7] J. Barros, M. R. D. Rodigues, “Secrecy Capacity of Wireless Channels,” Proc. IEEE International Symposium on Information Theory, pp. 356-360, 2006.

[8] S. Yi-Sheng, S. Y. Cheng, H. Wu, S. H. Huang, H. Chen, “Physical Layer Security in Wireless Networks: A Tutorial”, IEEE Wireless Communications, pp 66-74, 2011.

[9] Y.Liang, H.V.Poor and S.Shamai, “Secure Communication Over Fading Channels,” IEEE Trans. Inf. Theory, 54, pp. 2470-2492, 2008.

[10] M. E. Sone, “A New Cross-Layer FPGA-Based Security Scheme for Wireless Networks” In IntechOpen, Online First, DOI: 10.5772/intechopen.82390, 2018.

[11] M .E. Sone, “Efficient Key Management Scheme To Enhance Security-Throughput Trade-Off Performance In Wireless Networks,” in Proc. Science and Information Conference (SAI), London, UK, pp. 1249 – 1256, 2015.

[12] S. Kambala, R. Vaidyanathaswami, A. Thangaraj, “Implementation of Physical Layer Key Distribution using Software Defined Radios,” in Defence Science Journal, Vol. 63, No. 1, pp. 6-14, 2013.

[13] J. Proakis and M. Salehi, “Communication Systems Engineering,” in Prentice Hall, 2nd Ed, 2001.

[14] N. N. Ningo and M. E. Sone, “Efficient key management FPGA-based cryptosystem using the RNS and iterative coding,” Int. J. Information and Communication Technology, Vol. 2, No. 4, pp. 302 – 322, 2010.

[15] M. E. Sone and N. N. Ningo, “A Simple FPGA-based Wireless Transmitter/ receiver Convolutional Cryptosystem,” International Journal of Computers and Applications, Vol. 33, No. 2, pp. 137-143, 2011.

[16] B. Cohen, “VHDL coding styles and methodologies,” Kluwer Academic Publishers, 2nd ed., 2001.

[17] Amiruddin, A. A. P. Ratna, R. F. Sari, “New Key Generation and Encryption Algorithms for Privacy Preservation in Mobile Ad Hoc Networks,” International Journal of Communication Networks and Information Security (IJCNIS) vol. Vol. 9, No. 3, p. 376-385, 2017.