Military Technical College
Kobry El-Kobbah,
Cairo, Egypt

9th International Conference on Electrical Engineering
ICEENG 2014

Design and Implementation of an Optimized Encryption Algorithm for Performance Enhancement Over WiMAX

By

I. Abd Elgafar** E. Abd Elwanees* A. D. Elbayoumy* H. Eldemerdash*

Abstract:

Due to the fact that encryption operations performed by any protocols increase the number of operations and also slow down the rate of data being sent or received over WiMAX network. Hence, Encryption may have negative effect on quality of services offered to the end users and the system capacity. The Performance enhancement over WiMAX network is needed by using optimized encryption algorithm, which reduces computations overheads. In this exertion, a proposed optimized encryption algorithm, which adopts AES algorithm as the encryption algorithm, is presented. In previous work [1], a customized version of the "AES" block cipher was introduced to suit proprietary data encryption applications. In this paper, a higher security level for optimized AES is proposed by adding a dynamic permutation unit of input data in every round which allowing number of round reduction possibility, improves network performance and increases diffusion propriety for each round.

Keywords:

Wireless Metropolitan Area Network (WMAN), WiMAX, Advanced Encryption Standard (AES), Dynamic Permutation Unit (DPU), Computation Overheads, Encryption, Algorithm.

---

* Egyptian Armed Forces
** AAST, Cairo, Egypt

1. Introduction

Worldwide Interoperability for Microwave Access (WiMAX) is the most widely deployed form of WMAN technology, belonging to the family of 802.16 standards. WiMAX is a very promising technology with many key features over other wireless technologies [2]. For instance, WiMAX network has the capability of working on many bands: 2.3 GHz, 2.5 GHz, etc, and provides scalability and mobility with high data rates using NLOS operation. It also provides strong security and strong QoS guaranteed services for data, voice, video, etc. However, in order for WiMAX to achieve a maturity level and become a successful technology, more research on security threats and solution to these threats need to be conducted.
By adopting the best technologies available today, the WiMAX, based on the IEEE 802.16e standard, provides strong support for authentication, key management, encryption and decryption, control and management of plain text protection and security protocol optimization. In WiMAX, most of security issues are addressed and handled in the MAC security sub-layer as described in the figure 1. The privacy sub-layer provides the Mobile Station (MS) with security capabilities and protects the Base Station (BS) from malicious attacks that may disrupt its services [3].

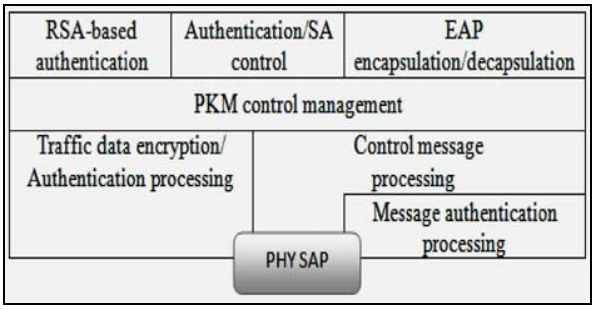

FIGURE 1: MAC SECURITY SUB-LAYER

The privacy sub-layer supports: (i) authenticate the user when the user enters in to the network, (ii) authorize the user, if the user is provisioned by the network service provider, and then (iii) provide the necessary encryption support for the key transfer and data traffic.
Encryption takes place in WiMAX network by means of Data encryption Standard (DES in CBC-Mode with 56 Bits) or Advanced Encryption Standard (AES in CCM-Mode with 128 Bits) which is widely used worldwide encryption algorithm.

This paper is organized as follows: Section 2, provides an overview of AES algorithm and its transformations. Section 3, describes the proposed optimized encryption algorithm with its components. Section 4, briefly explain methods of Optimized Encryption Algorithm Evaluation. Finally, this paper concludes with Section 5.

2- Advanced Encryption Standard

AES stands for Advanced Encryption Standard. AES is a symmetric key encryption algorithm, which replaces the commonly used Data Encryption Standard (DES). AES provides strong encryption and was selected by NIST as a Federal Information Processing Standard in November 2001 (FIPS-197).
AES uses three key sizes: a 128, 192, or 256-bit encryption key. The initial state is the plaintext and the final state is the cipher text in the encryption. The state consists of 4 rows of bytes. As the block length is 128 bits, each row of the state contains 4 bytes. The four bytes in each column form a 32 bit word. After an initial round key addition, a round function consisting of four transformations Sub Bytes, Shift Rows, Mix Columns, and Add Round Key is applied to each data block. The standard AES Encryption and Decryption procedures shown in Figure 2. Each round performs the following four transformations:

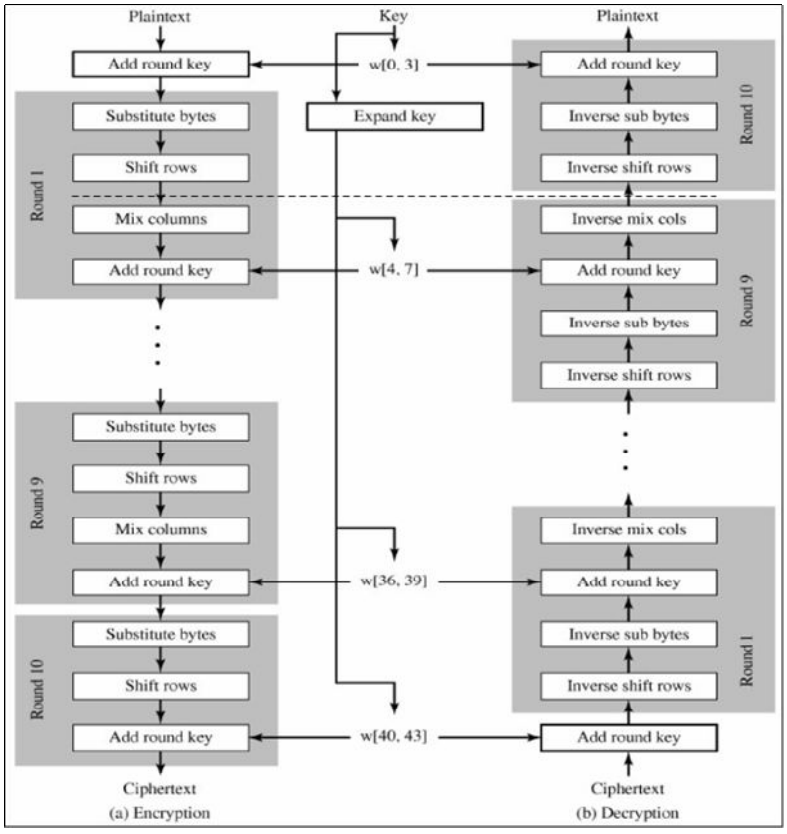

Figure 2: AES Encryption and Decryption [5].

i. Sub Byte: transforming a byte value using a nonlinear Substitution table (S-Box).
ii. Shift Row: cyclically shifting the last three rows of an array by different offsets.
iii. Mix Column: using all the columns in an array and mixing their data to produce new columns.
iv. Add Round Key: adding the corresponding round key to an array.

3- Proposed optimized encryption algorithm

An optimized encryption algorithm takes AES as the core of its structure with adopting the previous customization procedures applied on the round function transformations [7].

By using the customized version of AES the confidentiality service can be insured and proprietary data encryption applications can be suited also. The customization steps designed to cover the following three main AES cryptographic functions:

(1) S-box Generation.
(2) Mix Column Transformation.
(3) Key Expansion Function.

However, the performance enhancement over WiMAX network is still needed by the optimized encryption algorithm, which speeds up the processing time of encryption operations and minimize the number of rounds in this customized AES with adding of dynamic permutation function for each reaming rounds.
The dynamic permutation will be filling its tabs from Pseudo Random Noise Generator (PRNG), which takes RC4 stream cipher algorithm as the core of its operation. In the following subsections, the detailed information of the structure of this optimized algorithm will be discussed.

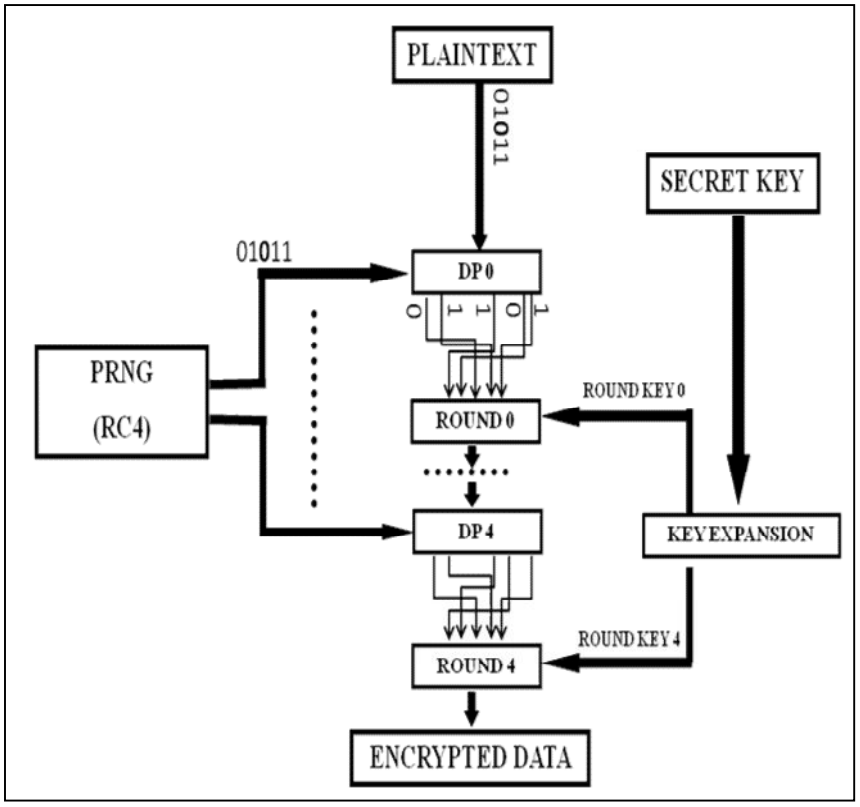

Figure 3: Optimized Encryption Algorithm Structure

3.1 Dynamic Permutation Function:

The Dynamic Permuter (DP) consists of 128 bits tapes, which will be control 128 bits data input from the previous stage by transposition cipher technique this I/P data will be have a new random locations by using the RC4 Algorithm output key which is generated by RC4 seed key 128 bits. The Dynamic permutation function can be made significantly more secure by performing more than one stage of transposition. The result is a more complex permutation that is not easily reconstructed. So after fist dynamic permutation occurred the new (DP) would takes the new output keys from RC4 Algorithm to generate the new round data with random process. Hence, this is a much less structured permutation and is much more difficult to cryptanalysis and cryptanalyst must have a knowledge of both AES encryption key and RC4 seed key to try 2^{256} all possible combinations.

3.2 Pseudo Random Noise Generator (PRNG):

PRNG adopting RC4 stream cipher as a stream random generator to control the Dynamic Permuter (DP) operation. The generated output keys from RC4 algorithm will filling the contents of DP tabs among all optimized algorithm rounds. RC4 was designed in 1987 by Ron Rivest for RSA Security. It's a variable key size stream cipher with byte-oriented operations. RC4 is probably the most widely used stream cipher. It has been widely used over the Internet and to provide confidentiality, and no known successful attacks have been published [5].
The input seed key used in initialization operation will be 128 bits and we use RC4 stream cipher algorithm as PRNG to save the used PRNG from entering dead lock state. Dead lock state is the state of continued all '0' state.

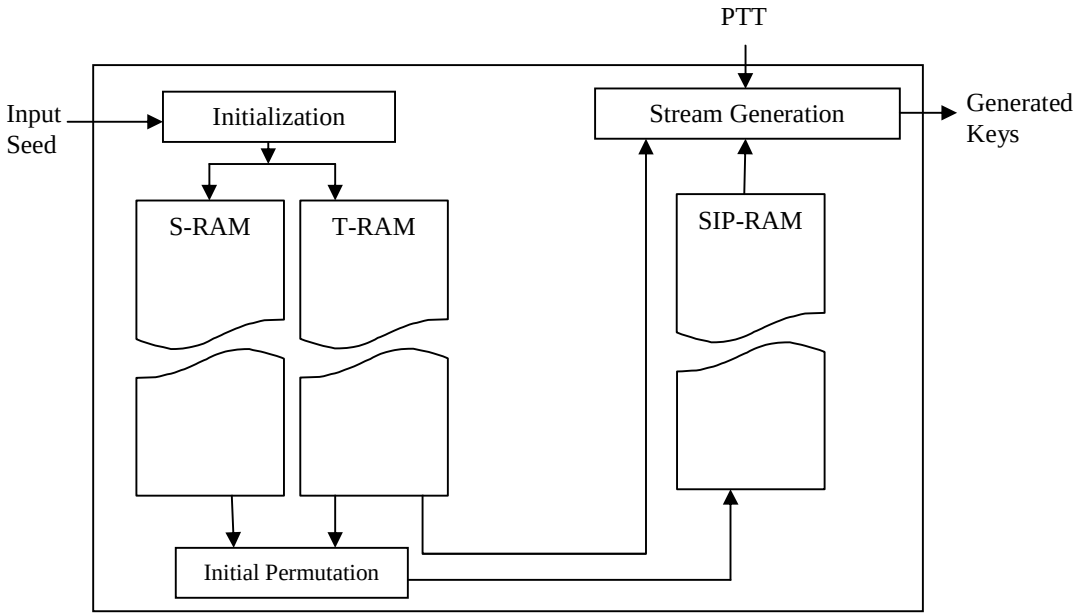

Figure 4: Optimized Encryption Algorithm Structure

3.3 Dynamic Encryption

It is intuitively clear that, the less materials a cryptanalyst have available to work on, the lower would be his chance of success. This implies that the security of encryption of a message could be enhanced, if more than one keys are employed to process a given message (in comparison to the common practice of using one single key) [6]. Dynamic encryption can be achieved by optimized encryption algorithm with two main functions, which are the followings:

1- Key dependent components such as S-Boxes [7]. At the start of the secure session, we fill the S-Boxes in optimized encryption algorithm with random contents generated from RC4 Stream cipher algorithm. Testing the contents of the new S-box is essential to insure that all required parameters of S-box in AES design are achieved by this design. For testing the S-box parameters, we used the S-box Evaluation Software Package [8], which measures the following S-box cryptographic parameters: algebraic degree (AD), non-linearity (NL), propagation criteria (PC), correlation immunity (CI), and balancedness (BL) [9].
2- Dynamic permutation function that adopts RC4 keys as PRNG which filling the contents of dynamic permutation unit is also supports dynamic encryption propriety. DP adding unpredictability principal to the optimized encryption algorithm.

3.4 Unpredictability Principal

If we use a cipher that includes a general computational process sequence, and keep all the sequence of computations of that process secret, the cryptanalyst will face a problem, which he will be unable to solve except by trying all possible combinations. It is clear that static encryption systems are deterministic and they are susceptible to cryptanalysis but dynamic encryption systems need dynamic cryptanalysis process, which is an obstacle to cryptanalysis [10]. The output controlling sequence from the RC4 to choose the DP for each round or filling the contents of S-boxes is unknown to the attacker and this provides optimized encryption algorithm with the unpredictability principal where the keys keep changed for every plaintext block and the used S-box keeps changed. Unpredictability will lead to stop cryptanalysis where the only way to break the system is by using brute force attack to try all possible combinations of the output RC4.

4- Proposed Optimized Encryption Algorithm Evaluation

4.1 Statistical Randomness Tests

An example of a successful standardization effort is the NIST selection process for the Advanced Encryption Standard; this has been a 4-year effort resulting in the publication of FIPS 197 in November 2001 [4]. For testing the algorithm output (ciphertext) based on NIST a specialized software package called "The Exhaustive Statistical Test

Package" is used. This test package exists at "The Communications and Encryption Lab" in "Science and Technology Center of Excellence (STCE)" of the Ministry of Military Production. The following Table (1) provides the conclusive results from all statistical randomness tests which were performed on 13 plaintext files with different formats (text, picture, audio and video) and the overall number of tests for the whole files are 195 tests done with result 100% scruffily tests. These tests help detecting any deviation from the assumed randomness property of ciphertexts generated by the optimized AES.

Table (1): Conclusion table for statistical randomness tests results

NO	Test	Calculated Test Statistic	Threshold	Test Final Result
1	Frequency Test	0.2647	6.5855	Passed
2	Runs Test	0.6031	6.5855	Passed
3	Serial Test	0.8658	9.2202	Passed
4	Cumulative Sums Test	0.8439	6.5855	Passed
5	Autocorrelation Test	0.0002	6.5855	Passed
6	Poker Test	123.781	166.9985	Passed
7	Maurer's Test	0.498	6.5855	Passed
8	Longest Run of Ones Test	3.6382	16.8429	Passed
9	Binary Matrix Rank Test	1.8379	9.2202	Passed
10	Lempel-Ziv Compression Test	0.631	6.5855	Passed
11	Approximate Entropy Test	10.3792	20.1209	Passed
12	Random Excursions Variant Test	0.5852	6.5855	Passed
13	NonOverlapping Template	8.5912	20.1209	Passed
14	Overlapping Template Matchings	3.5997	15.1168	Passed
15	Random Excursions Test	4.6993	15.1168	Passed

4.2 Proof of Optimized Encryption Algorithm Security

1- Security Type:

When evaluating the security of our designed architecture according to Kerckhoffs' Principle, it is clear that the cryptanalyst knows everything about the encryption algorithms and the PRNG generates the controlling sequence, except the algorithms secret keys and the PRNG controlling sequence. Therefore, proposed optimized encryption algorithm will be computationally secure by increasing security level by 16!

Where: The enhanced security level for just five rounds = $(16!)^5 \approx 4 * 10^{66} \approx 2^{221}$. Which means it cannot be broken with the current computer technology within limited time and computational resources.

2- Resist to Linear crypt analysis:

Increasing known plain/cipher text pairs:

For 10 rounds No. of P/C text pairs = 2^{179}

For 5 rounds No. of P/C text pairs = 2^{32}

So all possibilities for using just 5 rounds ≈ (2^{32})* (2^{221}) ≈ 2^{253} > 2^{179} which is infeasible to try by the attacker.

3- Complexity:

The complexity of the system is measured in how many trials the attacker will do to get the right RC4 input to the optimized algorithm. For one plaintext block, the attacker needs to try 2 ^ 128 trials to get the right combination. For P number of plaintext blocks, the attacker needs to try (2 ^ 128) ^ P trials to get the right combination.

3- Reduce the computation overheads by using just five rounds.

We choose to implement this optimized algorithm because it has the lowest design size, the highest speed and the highest security level.

4- Reconfigurable/Dynamic Algorithm.

5- Free of Trapdoor Algorithms.

5- Conclusion

This paper discussed an efficient design of an optimized encryption algorithm based on AES, which already used in WiMAX networks. The performance enhancement over WiMAX is achieved by using high-speed algorithm with reduced number of encryption rounds, which positively affected the processing speed and decreased its delays. The security evaluation and measurements is being analyzed for proposed algorithm, which achieved a higher security level by adding dynamic permutation function based on dynamic security methodology.

References:

[1] Ashraf D. Elbayoumy, Haitham Eldemerdash, "Design and Implementation of Multi-Rate Encryption Unit Based on Customized AES", International Journal of Video & Image Processing and Network Security IJVIPNS-IJENS Vol: 11 No: 06, December 2011.

[2] Rakesh Kumar Jha, Dr Upena D Dalal, "A Journey on WiMAX and its Security Issues", International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 1 (4), 2010.

[3] Kahya Noudjoud, Debbah Adel and Nacira Ghoualmi, "WiMAX Security – A Formal Analysis using Scyther tool", International Conference on Computational Techniques and Artificial Intelligence ICCTAI, Penang, Malaysia, 2012.

[4] FIPS 197 "Advanced Encryption Standard (AES)," Federal Information Processing Standard (FIPS), Publication 197, National Institute of Standards and Technology, US Departmen of Commerce, Washington D.C., November 26, 2001.

[5] William Stallings, "Cryptography and Network Security Principles and Practices", Fourth Edition, 2005.

[6] Bo Dömstedt, Jesper Jansson, "The Theory of Dynamic Encryption, a New Approach to Cryptography", Department of Computer Science, Lund University, Sweden.

[7] N. Hamdy, K. Shehata, H. Eldemerdash. “Design and Implementation of Encryption Unit Based on Customized AES Algorithm” IJVIPNS International Journal of Video & Image Processing and Network Security, Vol: 11 No: 01, February 2011.

[8] Adham Elhosary, Evaluation software package on platform Linux Ubuntu, Kernel 2.6.32-25 used in "Wireless Computer Communication Network”, a Ph.D. Dissertation, MTC, 2013.

[9] Claude Carlet, "Boolean Functions for Cryptography and Error Correcting Codes”, University of Paris, France, 2008.

[10] M. H. Megahed, D. Makrakis, H. Mouftah, C. Adams, “Spread Spectrum Encryption Architecture SSEA: A New Encryption Architecture for Post Quantum Computing Design and Analysis”, 15th International Conference on Aerospace Sciences & Aviation Technology (ASAT-15), MTC, Cairo, Egypt, 2013.