Implementation and performance assessment of the enhanced RC5 (ERC5) algorithm based on addition-then-append key expansion technique

To cite this article: Excel B. Villanueva et al 2019 IOP Conf. Ser.: Mater. Sci. Eng. 482 012015

View the article online for updates and enhancements.
Implementation and performance assessment of the enhanced RC5 (ERC5) algorithm based on addition-then-append key expansion technique

Excel B. Villanueva¹, Bobby G. Gerardo², Ruji P. Medina¹
¹Technological Institute of the Philippines, ²West Visayas State University
¹excel.villanueva.0816@gmail.com, ²bgerardo@wvsu.edu.ph, ³ruji.medina@tip.edu.ph

Abstract. In a business, it is important to note that owners should always make sure that they give a hassle free service to their customers to attract their attention and will eventually, gain their trust and continuous patronage of their service and RFID offers a solution for this concern. Traditional way to collect payment is still in use up to this day. This paper intends to implement the use of the ERC5 algorithm in an RFID – based payment scheme for the DMMMSU-NLUC Fasfood center as an encryption algorithm for securing sensitive information. Moreover, it also intends to assess the performance of the said algorithm in terms of speed and work efficiency compared to the original algorithm. Result shows that the authors were successful in implementing ERC5 as an encryption algorithm. Result also shows that the ERC5 outperforms the classic RC5 algorithm in both speed and work efficiency category.

1. Introduction

Radio Frequency Identification, or famously known as RFID, has been part of our daily lives, may be it on our transportation, shopping or even parking. As a matter of fact, this technology has been explored for as early as in the year 1948 [1] but actually rose to fame when one of the biggest retailing company called Wal-Mart opened a new door for inventory tracking and supply chain management based on RFID when they announced the use of RFID-enable shipments in the year 2005 [2]. Since then, this technology has been an essential part of business enterprise.

One useful way to implement RFID technology is in payment systems. As a matter of fact, both government and business ventures have been eyeing on the implementation of RFID for further innovation that they could offer to their clienteles, for example cashless payments [3]. This breakthrough is evident with the use of RFID in different areas such as transportation, healthcare and other business related services.

In a business, it is important to note that owners should always make sure that they give a hassle-free service to their customers to attract their attention and will eventually gain their trust and continuous patronage of their service [4]. RFID offers this convenience to business because aside from its benefits, it also offers low cost in which can make the business owners invest in a worthwhile technology [5].

The Don Mariano Marcos Memorial State University (DMMMSU) is one of the prestigious state universities and colleges in the Philippines with Atty. Benjamin P. Sapitula as the current president. It has been founded by the late President Ferdinand Marcos on January 15, 1981 under Presidential Decree 1778 that merges 5 different schools in the entire province of La Union during that time. Since day one of the current president of the university, Atty. Sapitula, it has been his mantra to “Embrace World-class Standards,” and it is evident with the different completed and ongoing projects in the entire university. Sadly, the university still operates in semi-automated processes. For example in DMMMSU-NLUC, one
of its campus, the traditional way to collect payment for meals at the fastfood center is still in use. This means that the establishment uses pen and paper in recording their sales for the day and this may result to inaccurate data records because it is prone to human error, lost paper, etc. On the other hand, it will also cause long queue in paying for the ordered meals.

This paper intends to implement the use of the ERC5 algorithm in an RFID – based payment scheme for the DMMMSU-NLUC Fastfood center as an encryption algorithm for securing sensitive information. They would like to propose an RFID-based payment scheme for DMMMSU-NLUC Fastfood center, in which they will call DMMMSU-NLUC E-canteen System. This system is proposed to help the university embrace world-class standards through the use of current systems the world has to offer. Moreover, it also intends to assess the performance of the said algorithm in terms of speed and work efficiency compared to the original algorithm.

2. Review of Related Literature

In their previous paper, the authors [6] suggested a modified technique to solve one of the weaknesses of the classic RC5 algorithm, the slow encryption speed [7]. The suggested enhancement is called addition-then-append key expansion technique, a unique solution to solve the above mentioned weakness of RC5 algorithm. This enhancement is very simple as it only requires common computer operation such as adding and appending of values to produce the needed key material. This enhancement also uses 2 more blocks and an additional combination of bitwise operations.

In business, it is always wise to keep sensitive information from anyone as secret as possible, which is why implementing a security protocol is important. In RFID, securing the tag unique number is the wisest way to secure information of the users [8].

To secure the unique tag numbers in an RFID-based transactions, various researchers have explored different ways to implement security protocols in their system and even suggested different methods. To name a few, references [9] [10] both suggested the use of lightweight algorithm for authentication purposes. For example, the use of a 128-bit AES algorithm was suggested. Their approach offers a lightweight implementation of the said algorithm to RFID technology for authentication purposes. And results shows that they were able to successfully implement the said algorithm in authenticating RFID tags.

To determine the performance of an algorithm, assessment or evaluation has been a practice of various authors. For example, [11] [12] [13] [14] performed an evaluation in their own versions or enhancements in the existing algorithm and their results show that in determining the performance of an algorithm can help the author establish a concrete rebuttal or justification in their enhanced algorithm. Some of these researches also proved that their enhanced algorithm performed better than the existing algorithm. Moreover, evaluating the performance can pave a way for further improvement for a specific area in the algorithm thus opening a continuation of the research for the author themselves or other researchers.

3. Proposed Method

3.1. DMMMSU-NLUC E-canteen System

Figure 1 shows the diagram of the proposed method. As perceived in the diagram, each client or customer must scan his/her RFID-enabled card to the scanner to pay for his/her order. But it is important to note that the card should have a sufficient balance in order to avail the service, otherwise, he/she must pay in cash.

The manager can print report such as monthly and annual income of the canteen from the system. Aside from that, the clients can also request for their personal copy of their monthly or annual meal records. This feature will help both the client and manager keep tract of their meal spending and income respectively. Aside from these reports, additional feature like a notification text message will be sent to the client’s personal phone number for each successful transaction and also if the remaining balance is below the allowable amount. This will increase the security of the system because, if the transaction is
not legit or the card’s owner did not make the transaction, he/she will be notified as soon as possible and can report it to the employee or management immediately.Reloading of the card can be done in different canteen’s loading outlets.

![Figure 1. Proposed DMMMSU-NLUC e-Canteen System Diagram](image)

### 3.2. ERC5 Algorithm based on Addition-then-Append Key Expansion Technique

The authors suggested an enhancement to solve the limitation of RC5 in their previous paper [6], which is slow in encryption speed. The enhancement is called addition-then-append key expansion technique, a unique way to expand the generated source key. Moreover, it also includes 2 more blocks and bitwise operations; the 1’s complement and left & right bit rotate combination, this bitwise operation is responsible for producing a cipher text with the same size as the plaintext.

#### 3.2.1 Encryption Phase

Figure 2 shows the encryption process of the ERC5 algorithm. The algorithm comprises of several steps, which includes: (1) addition-then-append key expansion phase, (2) pre-processing of plaintext, (3) division of plaintext, and (4) block XOR-swapping. All these process will produce a cipher text with the same size as the plaintext.

- **Addition-then-append Key Expansion Phase**

  Figure 3 shows the diagram of Addition-then-append Key Expansion technique. This technique involves 3 easy steps namely: (1) random number generation, (2) addition and (3) appending of values. The goal of this technique is to remove the use of word size, array, magic constant and golden ratio in which the original algorithm uses to generate its key.

  The key expansion starts when the system generates a random number source key based from system date and time. The source key will be expanded through the 3 steps mentioned above. As perceived in figure 3, the source key will be added to any generated random number (which will be repeated twice). The algorithm will not generate the same random numbers for each two rounds, thus increasing the confusion of this phase. To produce the key material, all values from the previous steps will be appended with the original length of the source key. This key material will be needed in the next process, which is the pre-processing of the plaintext.

- **Plaintext Pre-processing**

  This process accepts any input from the user, be it a password or series of random numbers, and it will be converted into its hexadecimal value. At the same time, the key material, which is the result of the previous phase, the key expansion, will also be converted in its hexadecimal value. Both values will be XOR-ed to produce the plaintext. This becomes an added confusion for the enhanced algorithm because without the knowledge to the value of the key material, the input from the user cannot be easily revealed. This phase is shown in the upper portion of figure 2.

- **Plaintext Division**

  The plaintext, which is the result of the previous process, is divided into two major divisions, called left and right division. Furthermore, each major division will be divided into two more blocks, so each major blocks has its own pair of minor blocks and series of bitwise operations, which means...
that the both division does not possess the same arrangement of bitwise operations. The 2 major blocks will operate simultaneously for 12 rounds. This is shown in the middle portion of figure 2.

- **Left Division.** In this division, it will perform the combination of XOR and left & right bit rotate. This is almost the same as the original version of RC5 algorithm except that it only uses left bit rotate, wherein in the ERC5 algorithm the left & right bit rotation was used.

- **Right Division.** This division performs an additional bitwise operation along with XOR and left & right bit rotate, the 1’s complement, or NOT bitwise operation.

3.2.2 **Decryption Phase** This process is the inverse version of the encryption process. This means that the XOR swap will be performed first to place the minor blocks into its respective group. After the blocks are properly placed, the algorithm will now perform the corresponding inverse operation of each major blocks to produce the plaintext.

4. **Results and Discussions**

4.1 **Implementation of ERC5 Algorithm in DMMMSU-NLUC E-canteen System**

In developing the prototype, the authors made use of the latest version of PHP programming language, coded in a laptop with an Intel ® Core ™ i3-3217U CPU processor @ 1.80GHz (4 CPUs), ~1.8GHz with a memory size of 4096MB RAM. They also made use of a Mifare RFID reader and RFID cards for simulation purposes.

The authors were successful in implementing the ERC5 algorithm in encrypting the RFID card number in the database, as shown in Figure 4. In the prototype, once the user scans its RFID card in the reader, the system will encrypt its unique id using the ERC5 algorithm, that value will be stored in the database. The algorithm is used to protect sensitive information, such as the unique card number of the clienteles in order to prevent information thief.
4.2 Performance Evaluation of ERC5 Algorithm

For algorithm speed comparison and evaluation, two sets of class/program were used, first is for the RC5 algorithm and second for the enhanced version of the algorithm. To evaluate the encryption and decryption speed of both algorithms, the authors made use of an embedded microtime() function in PHP. They ran the program simultaneously for 10 attempts for a common user input, say a 16-bit length password. The formula used to test the difference of the speed performance between the RC5 and ERC5 is shown in equation 1, where $r$ stands for average time of the classic algorithm and $p$ stands for average time of the ERC5. The formula used for ETPE is shown in equation (1). This evaluation is used to determine the percentage of improvement on task execution [13]. The execution time average mean of the 2 algorithms was used as input data for the evaluation as shown in equation (2), wherein Latency($T_{old}$) is the average mean of the classic RC5 algorithm and the Latency($T_{new}$) is the average mean of the ERC5 algorithm.

$$\text{Performance Comparison} = \frac{(R - P)}{R} \times 100 \quad (1)$$

$$\text{ETPE (\%)} = \left(\frac{\text{Latency}(T_{old})}{\text{Latency}(T_{new})} - 1\right) \times 100 \quad (2)$$

4.2.1 Speed Performance

The encryption speed simulation results with respect to the input size and required times of the algorithm compared with the existing algorithm is shown in table 1. As shown in the table, the ERC5 algorithm beats the original algorithm by 76% with an average speed of 56.38 milliseconds (ms) while the later has an average speed of 235.05 ms. On the other hand, the same table shows the comparison between the 2 algorithms in terms of decryption speed. As perceived in the table, the ERC5 algorithm outruns the original algorithm by 42% with an average speed of 147.31 ms while the later has an average speed of 260.80 ms.

4.2.2 Execution Time Performance Evaluation (ETPE)

Table 2 shows the execution time performance efficiency results. It is notable that the ERC5 is more efficient in both encryption and decryption than the classic RC5 algorithm with a percentage of 316.90 and 77.04 respectively. This means that there is a big improvement when it comes to work efficiency in ERC5 algorithm as compared to the classic RC5 algorithm.

| Speed | RC5         | ERC5         | Difference |
|-------|-------------|--------------|------------|
| Encryption | 235.05 ms   | 56.38 ms     | 75.73%     |
| Decryption | 260.80 ms   | 147.31 ms    | 42.05%     |

| Latency | Mean | ETPE (%) |
|---------|------|----------|
| Encryption (Told) | 235.05 ms | 56.38 ms | 316.90 |
| Decryption (Tnew) | 260.80 ms | 147.31 ms | 77.04 |

5. Conclusion and Future Works

The authors were successful in implementing the ERC5 algorithm in an RFID-based payment scheme for DMMMSU-NLUC Fastfood center in which they called DMMMSU-NLUC e-Canteen System. Additionally, they were able to provide solution to replace the manual procedure of the said establishment. Moreover, the authors evaluated the performance of both the classic rc5 algorithm and
the ERC5 in terms of its speed and work efficiency. Experimental shows that in both category, the ERC5 algorithm positively outruns the existing algorithm.

For future work, the authors intend to evaluate the security level of the ERC5 algorithm with the use of avalanche effect. Furthermore, the prototype used in this study will undergo usability testing to finalize its design and other system features according to the preference of the end-user.

References
[1] Landt J 2005 The history of RFID IEEE Potentials vol 24 no 4 pp 8-11
[2] Weinstein R 2005 RFID: A Technical overview and its application to the enterprise IEEE Computer Society vol 7 no 3 pp 27-38
[3] Lokshina I and Thompson W 2013 Analysis of design requirements for electronic tags from business viewpoint IEEE 16th Int. Symp. on Wireless Personal Multimedia Communication pp 1-6
[4] Caya MV, Losaria NF, Manzano MJ, Tan HK and Pellegrino RV 2017 Cashless transaction for resort club amenities using RFID technology IEEE 9th Int. Conf. on Humanoid, Nanotechnology Information Technology, Communication and Control, Environment and Management pp 1-5
[5] Weis SA 2007 RFID (Radio Frequency Indentification): principles and applications System vol 2 no 3 pp 1-23
[6] Villanueva EB, Medina RP and Gerardo BD 2018 An enhanced RC5 (ERC5) algorithm based in simple random number key expansion technique IEEE Symp. on Computer Applications and Industrial Electronics (ISCAIE) pp 134-8
[7] Bhanot R and Hans R 2015 A review and comparative analysis of various encryption algorithms Int. J. of Security and Its Application vol 9 no 4 pp 289-306
[8] Juels A 2006 RFID Security and privacy: a research survey IEEE J. on Selected Areas in Communications vol 24 no 2 pp 381-94
[9] Feldhofer M, Dominikus S and Wolkerstofer J 2004 Strong authentication for RFID systems using the AES algorithm Springer vol 3156 pp 357-70
[10] Juels A and Weis S 2005 Authenticating pervasive devices with human protocols Springer vol 3621 pp 293-308
[11] Hong L, Wan Y and Jain A 1998 Fingerprint image enhancement: algorithm and performance evaluation IEEE Transactions on Pattern Analysis and Machine Intelligence vol 20 no 8
[12] Jamel T 2016 Performance evaluation of the fast euclidean direction search algorithm for adaptive beamforming applications Int. Conf. on Multidisciplinary in IT and Communication Science and Applications pp 1-6
[13] Wenceslao F 2015 Performance efficiency of modified AES algorithm using multiple S-boxes Int. J. of New Computer Architectures and Their Applications vol 5 no 1 pp 1-9
[14] Zheng X 2016 Research on performance evaluation method based on neural network algorithm IEEE Int. Conf. on Smart City and Systems Engineering pp 524-6