International Journal of Cryptology Research 5(1): 1-10 (2015)

# CFEA-Technique: Smaller Size of the Compressed Plaintext

**[1]Arif Mandangan, [2]Loh Chai Mei, [3]Chang Ee Hung and [4]Che Haziqah Che Hussin**

*[1,2,3]School of Science and Technology, Universiti Malaysia Sabah, Jalan UMS, 88400 Kota Kinabalu Sabah Malaysia,*

*[4]Preparatory Centre for Science and Technology, Universiti Malaysia Sabah, Jalan UMS, 88400 Kota Kinabalu Sabah Malaysia.*

*Email: [1]arifman@ums.edu.my, [2]christineloh_90@hotmail.com, [3]fancy_2309@hotmail.com, [4]haziqah@ ums.edu.my*

## ABSTRACT

Key distribution problem has been solve by the emergence of asymmetric cryptography. Without exchanging private key, two parties are able to communicate securely via insecure channel. As a tradeoff, the efficiency of asymmetric cryptosystems are much slower since the size of the numbers implemented are large in order to provide a good level of security. Since that, efficiency enhancement become one of the most conducted research in cryptography. We proposed a technique that we named as CFEA-technique which aims to reduce the number of plaintext and ciphertext to be encrypted and decrypted by asymmetric cryptosystems. By applying this technique, we the number of plaintext can be reduced from $k$ plaintext, where $k \in \mathbb{Z}^+$ and $k > 2$, to only 2 plaintext. Hence, instead of encrypting $k$ plaintext, now we need to encrypt only 2 compressed plaintext. Since the number of plaintext to be encrypted have been reduce, the number of ciphertext to be decrypted also become lesser. Unfortunately, even though the number of plaintext have been reduced to only 2 plaintext, the size of these compressed plaintext are become larger for large $k$. This problem will minimize the efficiency enhancement in encryption and decryption procedures. In this paper, we embed a method into the CFEA-technique in order to produce a new pair of plaintext with smaller sizes.

Keywords: RSA cryptosystem, compression, continued fraction, Euclidean algorithm.

## 1. INTRODUCTION

Internet is the main platform for communication across the globe and it has indirectly changed how we live every day. The ways we socialize, play, do our shopping and study have been changed by the emergence of the Internet. Almost everybody in this world is connected to the Internet via various mediums and devices such as smart phones, tablets, netbooks, notebooks, desktops and so on. As an open communication medium, the Internet is faced with some security problems such as confidentiality, integrity, repudiation and authentication (Farouzan, 2008). Therefore, the network security has become crucial and essential. Basically, network

security is a set of protocols that is able to minimize security attacks in order to allow us to use the Internet comfortably. The most common tool to provide network security is cryptography. Cryptography is a study about secret writing in order to provide confidentiality of which an important essence to a secured network. In cryptography, an original message is called plaintext. The transformed plaintext is called ciphertext. The transformation procedure is called encryption and a key is needed in this procedure. Decryption is the inverse of encryption and this procedure also needs a key. In symmetric cryptosystem, a common key will be shared by Alice (message sender) and Bob (message recipient) and used in encryption-decryption procedures. On the contrary, two different keys are used by Alice and Bob to communicate using asymmetric cryptosystem (Hoffstein, *et.al.,* 2008).

Due to practicality, asymmetric cryptosystem is currently the most preferred cryptosystem. To cope with today's needs, we are in dire need not only for a secured cryptosystem but also a system which is efficient enough to be embedded into small gadget. This explains why there are rigorous research in cryptography to enhance the efficiency of asymmetric cryptosystem. In (Chang and Mandangan, 2013), we introduced a technique which is able to reduce the number of plaintext from any numbers to only two plaintext. This technique is known as Compression-RSA since our first try on this technique was by embedding it into RSA cryptosystem (Rivest, *et. al.,* 1978).

After further research on this technique, it is found that this technique can be easily embedded into any asymmetric cryptosystem without major alteration on its key generation, encryption and decryption algorithms. Consequently, we renamed it as the CFEA-technique (Continued Fraction-Euclidean Algorithm). Instead of encrypting large numbers of plaintext, an asymmetric cryptosystem only needs to encrypt two plaintext to produce two ciphertext by applying this technique. By decrypting these ciphertext and then applying the inverse of CFEA-technique, we will get the actual and original plaintext without any alteration. In (Mandangan, *et. al.,* 2014), we observed that the number of original plaintext has a linear relationship with the sizes of each compressed plaintext. As the number of original plaintext increases, the sizes of the compressed plaintext $M_1$ and $M_2$ will also increase linearly.

In this paper, we did some modifications on CFEA-technique so that the compressed plaintext have smaller size compared to the compressed plaintext of those produced by the early designed CFEA-technique. Before further discussion, we firstly introduced the CFEA-technique. Then, we showed the modification done to the technique and finally we presented

some examples to compare the size of plaintext produced by the old modified version of CFEA-technique.

## 2. THE CFEA-TECHNIQUE

Let the set of original plaintext as $m_1, m_2, m_3, \cdots, m_{k-1}, m_k$ where $k \in \mathbb{Z}^+$and $k > 2$. By using the CFEA-technique, these $k$ plaintext can be compressed to only 2 plaintext, denoted as $M_1, M_2$ . No matter how big the value $k$ is, the plaintext will be reduced to only 2 plaintext $M_1$ and $M_2$. The CFEA-technique is basically designed by combining two methods namely Continued Fraction and Euclidean Algorithm. CFEA is the acronym of these methods (Continued Fraction and Euclidean Algorithm).

The algorithm of CFEA-technique (Chang and Mandangan, 2013):

i. Compression procedure

Step 1: Let the set of original $k$ plaintext as

$$m_1, m_2, m_3, \cdots, m_{k-1}, m_k$$

Step 2: By using Continued Fraction method, compute the new plaintext $M_1$ and $M_2$ as follows

$$m_1 + \cfrac{1}{m_2 + \cfrac{1}{m_3 + \cfrac{1}{\vdots \\ m_{k-1} + \cfrac{1}{m_k}}}} = \frac{M_1}{M_2}$$

ii. Decompression procedure

By using Euclidean algorithm, compute the following

$$\begin{aligned} = M_2 \ q_1 \quad & + r_1 \\ = \ r_1 \ q_2 \quad & + \ r_2 \\ = \ r_2 \ q_3 \quad & + \ r_3 \\ \vdots & \\ = \ r_{k-2} \ q_{k-1} \quad & + \ r_{k-1} \\ = \ r_{k-1} \ q_k \quad & + \ r_k \end{aligned}$$

where $M_1, M_2$ are the compressed plaintext, $q_i$ is quotient and $r_i$ is remainder for $i = 1,2, \ldots, k$. From this step, we have

$$q_1, q_2, q_3, \cdots, q_{k-1}, q_k \ = \ m_1, m_2, m_3, \cdots, m_{k-1}, m_k$$

which is the set of original plaintext.

The implementation CFEA-technique in RSA cryptosystem is shown in the Figure 1.

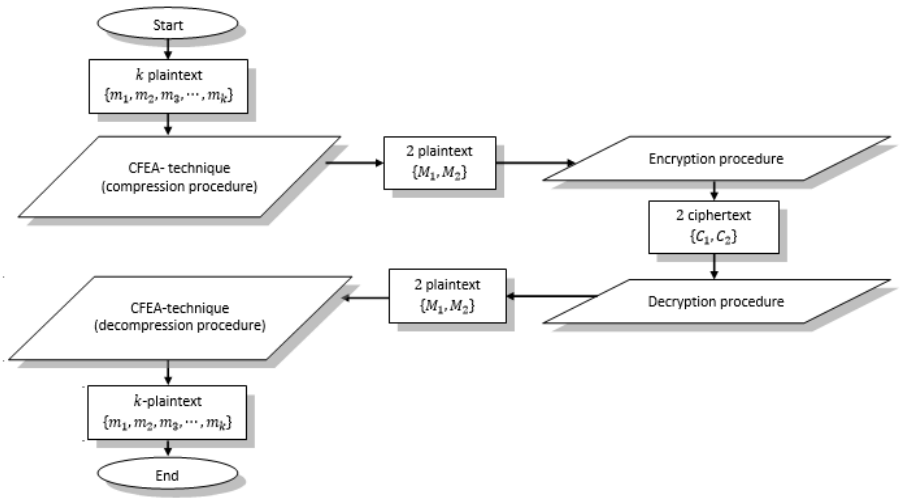


**Figure 1.** Implementation of CFEA-technique in RSA cryptosystem

**Example 1**: Let 1,4,8,6,3,7,5,9,2 be the plaintext, public key set is $N = 3079471, e = 443$ and the decryption key is $d = 62483$.

Set the plaintext 1,4,8,6,3,7,5,9,2 $= m_1, m_2, m_3, m_4, m_5, m_6, m_7, m_8, m_9$ . Compress the 9-plaintext 1,4,8,6,3,7,5,9,2 to produce only 2 new plaintext $M_1$ and $M_2$ as follows:

$$1 + \cfrac{1}{4 + \cfrac{1}{8 + \cfrac{1}{6 + \cfrac{1}{3 + \cfrac{1}{7 + \cfrac{1}{5 + \cfrac{1}{9 + \frac{1}{2}}}}}}}} = \frac{578559}{465616} = \frac{M_1}{M_2}$$

Encrypt the plaintext $M_1 = 578559$ and $M_2 = 465616$ as follows:

$$C_1 = 578559^{443} \bmod 3079471 = 2662637$$

$$C_2 = 465616^{443} \bmod 3079471 = 1682050$$

To recover the original plaintext, firstly we need to decrypt the ciphertext $C_1 = 2662637$ and $C_2 = 1682050$ as follows:

$$M_1 = 2662637^{62483} \bmod 3079471 = 578559$$
$$M_2 = 1682050^{62483} \bmod 3079471 = 465616$$

By using decompression procedure of the CFEA-technique, we recover the original 9-plaintext as follows:

$$\begin{array}{lcllll} 578559 & = & 465616\ 1 & + & 112943 & , q_1 = 1 \\ 465616 & = & 112943\ 4 & + & 13844 & , q_2 = 4 \\ 112943 & = & 13844\ 8 & + & 2191 & , q_3 = 8 \\ 13844 & = & 2191\ 6 & + & 698 & , q_4 = 6 \\ 2191 & = & 698\ 3 & + & 97 & , q_5 = 3 \\ 698 & = & 97\ 7 & + & 19 & , q_6 = 7 \\ 97 & = & 19\ 5 & + & 2 & , q_7 = 5 \\ 19 & = & 2\ 9 & + & 1 & , q_8 = 9 \\ 2 & = & 1\ 2 & + & 0 & , q_9 = 2 \end{array}$$

Now we have set of quotients $q_1, q_2, q_3, \cdots, q_9 = 1,4,8,6,3,7,5,9,2$ is exactly same with the set of the original plaintext $m_1, m_2, m_3, \cdots, m_9$ .

## 3. MODIFICATION ON THE CFEA-TECHNIQUE

Let the original plaintext as $m_1, m_2, m_3, \cdots, m_{k-1}, m_k$ . We set $d_1 = m_1$. Then, for all $i = 2,3, \ldots, k$ we compute

$$d_i = m_i - m_{i-1} \quad (1)$$

Now we have a new set of plaintext $d_1, d_2, d_3, \cdots, d_{k-1}, d_k$ where each of this plaintext is smaller than its corresponding original plaintext except the first plaintext where $m_1 = d_1$. That is, we have

$$d_i < m_i$$

for all $i = 2,3, \ldots, k$. This reduction leads to the production of smaller size of the compressed plaintext $M_1$ and $M_2$. To recover the original plaintext, compute

$$m_i = d_i + m_{i-1} \quad (2)$$

for all $i = 2,3, \ldots, k$.

**Example 2:** Suppose we have 9 plaintext $m = \ 1, 4, 8, 6, 3, 7, 5, 9, 2$ . Then, by applying equation (1), we have

$$
\begin{aligned}
d_1 &= m_1 = 1 \\
d_2 &= m_2 - m_1 = 4 - 1 = 3 \\
d_3 &= m_3 - m_2 = 8 - 4 = 4 \\
d_4 &= m_4 - m_3 = 6 - 8 = -2 \\
d_5 &= m_5 - m_4 = 3 - 6 = -3 \\
d_6 &= m_6 - m_5 = 7 - 3 = 4 \\
d_7 &= m_7 - m_6 = 5 - 7 = -2 \\
d_8 &= m_8 - m_7 = 9 - 5 = 4 \\
d_9 &= m_9 - m_8 = 2 - 9 = -7
\end{aligned}
$$

Now, we have a new set of plaintext $d = \ 1, 3, 4, -2, -3, 4, -2, 4, -7$ . To recover the original plaintext $m$, we apply equation (2) as follows

$$
\begin{aligned}
m_1 &= d_1 = 1 \\
m_2 &= d_2 + m_1 = 3 + 1 = 4 \\
m_3 &= d_3 + m_2 = 4 + 4 = 8 \\
m_4 &= d_4 + m_3 = -2 + 8 = 6 \\
m_5 &= d_5 + m_4 = -3 + 6 = 3 \\
m_6 &= d_6 + m_5 = 4 + 3 = 7 \\
m_7 &= d_7 + m_6 = -2 + 7 = 5 \\
m_8 &= d_8 + m_7 = 4 + 5 = 9 \\
m_9 &= d_9 + m_8 = -7 + 9 = 2
\end{aligned}
$$

These calculations only involve simple addition and subtraction operations which can be done in short time. For further discussion, we generate 10 sets of plaintext $m_1, m_2, m_3, \cdots, m_{k-1}, m_k$ numbered 1 to 10 where each $m_i \in \mathbb{Z}^+$ and $1 \leq m_i \leq 26$ as shown in Table 1:

| No. | Plaintext Set $m_1, m_2, m_3, \cdots, m_{k-1}, m_k$ | Compressed Plaintext $M_1, M_2$ | Number of bits | |
|---|---|---|---|---|
| | | | $M_1$ | $M_2$ |
| 1 | 18, 18, 16, 15, 4, 4, 17, 7, 13, 21 | $\frac{45721877441}{2532315448}$ | 36 | 32 |
| 2 | 5, 17, 23, 3, 10, 24, 10, 12, 21, 12 | $\frac{46351786775}{9162830549}$ | 36 | 34 |
| 3 | 8, 18, 20, 22, 24, 26, 12, 6, 8, 9 | $\frac{218991443785}{27185662929}$ | 38 | 35 |
| 4 | 13, 15, 6, 14, 14, 10, 4, 1, 6, 8 | $\frac{674599213}{51630352}$ | 30 | 26 |
| 5 | 11, 25, 12, 12, 12, 1, 14, 9, 25, 12 | $\frac{21488940092}{1946485235}$ | 35 | 31 |
| 6 | 2, 14, 16, 9, 18, 26, 3, 12, 17, 12 | $\frac{15375448123}{7423760105}$ | 34 | 33 |
| 7 | 21, 24, 3, 13, 10, 13, 19, 13, 9, 10 | $\frac{61736621036}{2934095275}$ | 36 | 32 |
| 8 | 11, 26, 1, 8, 6, 1, 13, 14, 26, 22 | $\frac{2128539531}{192851621}$ | 31 | 28 |
| 9 | 16, 11, 26, 1, 18, 23, 5, 20, 7, 20 | $\frac{30318964919}{1884265251}$ | 35 | 31 |
| 10 | 19, 12, 9, 4, 19, 5, 26, 3, 13, 20 | $\frac{17700809789}{927589530}$ | 35 | 30 |

**Table 1**: Sets of original plaintext

Furthermore, we reduce the size of each plaintext sets by using the formula given in equation (1) and get 10 corresponding sets of reduced plaintext $d_1, d_2, d_3, \cdots, d_{k-1}, d_k$ as shown in Table 2:

| No. | Reduced Plaintext Set $d_1, d_2, d_3, \cdots, d_{k-1}, d_k$ | Compressed Plaintext $D_1, D_2$ | Number of bits | |
|---|---|---|---|---|
| | | | $D_1$ | $D_2$ |
| 1 | 18, 0, -2, -1, -11, 0, 13, -10, 6, 8 | $\frac{6013}{433}$ | 13 | 9 |
| 2 | 5,12,6,-20,7,14,-14,2,9,-9 | $\frac{1644928244}{323665733}$ | 31 | 29 |
| 3 | 8,10,2,2,2,2,-14,-6,2,1 | $\frac{572041}{70657}$ | 20 | 17 |
| 4 | 13,2,-9,8,0,-4,-6,-3,5,2 | $\frac{168791}{12475}$ | 18 | 14 |
| 5 | 11,14,-13,0,0,-11,13,-5,16,-13 | $\frac{288292633}{26038413}$ | 29 | 25 |
| 6 | 2,12,2,-7,9,8,-23,9,5,-5 | $\frac{122427750}{58866559}$ | 27 | 26 |

| | | | | |
|---|---|---|---|---|
| 7 | 21,3,-21,10,-3,3,6,-6,-4,1 | $\frac{11976174}{561241}$ | 24 | 20 |
| 8 | 11,15,-25,7,-2,-5,12,1,12,-4 | $\frac{192456713}{17390385}$ | 28 | 25 |
| 9 | 16,-5,-15,-25,17,5,-18,15,-13,13 | $\frac{114843780093}{7267386437}$ | 37 | 33 |
| 10 | 19,-7,-3,-5,15,-14,21,-23,10,7 | $\frac{15466407035}{819923017}$ | 34 | 30 |

**Table 2**: Sets of reduced plaintext

For comparison purpose, consider the following graph:

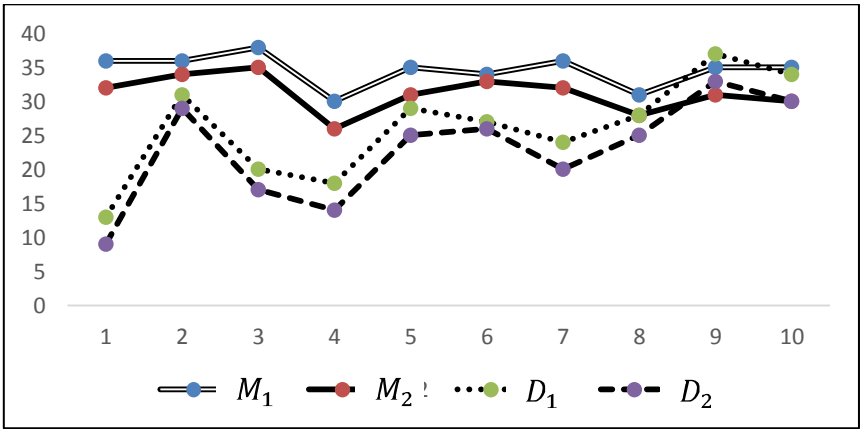


**Figure 2**: Comparison of compressed plaintext between sets of original and reduced plaintext

We can observe that the size of compressed plaintext of the reduced plaintext sets are smaller than the size of compressed plaintext of the original plaintext sets. This is because we implement the proposed formula in equation (1). We expect that encrypting $D_1$ and $D_2$ will be faster than encrypting $M_1$ and $M_2$ due to their smaller size.

## 4. CONCLUSION AND DISCUSSION

Some modifications on the CFEA-technique were done in this paper. We reduced the size of the compressed plaintext $M_1$ and $M_2$ to smaller size in order to enhance the performance of encryption and decryption procedures. Some experiments could be done in further research to find the actual percentage of the size reduction of the compressed plaintext especially

when we deal with large numbers of original plaintext. Also, we did several attempts to embed the modified CFEA-technique into other asymmetric cryptosystems such as ElGamal and Elliptic Curve Cryptography.

## 5. ACKNOWLEDGMENTS

We would like to thank Universiti Malaysia Sabah for supporting our participation in CRYPTOLOGY 2014. This research is supported by *Research Acculturation Grant Scheme* (*RAGS*) RAG0001-SG-2012 MOHE (Malaysia).

## REFERENCES

Bach, E. and Shallit, J. 1996. Algorithmic Number Theory, Vol.1: Efficient Algorithms. Cambridge, MA:MIT Press

Chang, E. H. and Mandangan, A. 2013. Compression-RSA: New approach of encryption and decryption method. *AIP Conference Proceeding 1522, American Institute of Physics*: 50-54.

Farouzan, B. A. 2008. *Introduction to Cryptography and Network Security*, New York: McGraw-Hill Companies: 20-28.

Hoffstein, J. , Pipher, J. and Silverman, J. H. 2008. *An Introduction to Mathematical Cryptography,* New York*:* Springer Science +Bussiness Media, 37-39.

Mandangan, A., Loh, C. M., Chang, E. H. and Hussin, C. H. C. 2014. Compression-RSA Technique: A More Efficient Encryption-Decryption Procedure. AIP Conference Proceedings 1602, 50;doi:10.1063/1.4882465

Mandangan, A., Lee, S. Y., Chang, E. H., and Che Hussin, C. H. 2014. ElGamal Cryptosystem with Embedded Compression-Crypto Technique. AIP Conference Proceedings 1635, 455; doi: 10.1063/1.4903621

Rivest R. L., Shamir, A. and Adleman, L. 1978. A Method for Obtaining Digital Signature and Public Key Cryptosystem, *Commun. ACM21*:120-126.

Shannon, C. E. 1948. A Mathematical Theory of Communication. Bell System Technical Journal, 28(4): 656-715

Verma, S. and Gark, D. 2011. Improvement in RSA Cryptosystem. Journal of Advances in Information Technology, 2(3): 146-151