Building an Initialization Cipher Block with Two-Dimensional Operation and Random Parameters

Yi-Li Huang[1], Fang-Yie Leu[1], Ilsun You[2], Jing-Hao Yang[1]

1: Department of Computer Science, TungHai University, Taiwan
{yifung, leufy, g01350036}@thu.edu.tw
2: School of Information Science, Korean Bible University, South Korea
ilsunu@gmail.com

Abstract. In recent years, parallel computing capabilities have been more powerful than before. Consequently some block cipher standards, such as DES used to protect important electronic messages, have been cracked in the past years. Also due to the rapid development of hardware processing speeds, 3DES and AES may someday be solved by brute-force attacks. Basically, the common characteristics of these block cipher standards are that each time, when a standard is invoked, the same parent key is used to generate subkeys. The subkeys are then utilized in the standard's encryption rounds to encrypt data. In fact, the variability of the key values is quite limited. Generally, producing random parameters to encrypt data is an effective method to improve the security of ciphertext. But how to ensure the security level of using and delivering these random parameters and how to avoid information leakage have been a challenge. So in this paper, we propose a novel random parameter protection approach, called the Initialization Cipher Block Method(ICBM for short), which protects random parameters by using a two-dimensional operation and employs random parameters to change the value of a fixed parent key for block ciphering, thus lowering the security risk of a block cipher algorithm. Security analysis demonstrates that the ICBM effectively improve the security level of a protected system. Of course, this also safely protect our homeland, particularly when it is applied to our governmental document delivery systems.

***Keywords*:** Cryptography, Block Cipher, random parameter, Two-Dimensional Operation, ICBM

1 Introduction

In recent years, due to the rapid development of different network technologies, many government offices, private companies, banks, etc. for environmental protection purpose send electronic documents, rather than paper documents, to people or customers to save paper consumption, of course also reducing the resource consumption for our homelands. With this achievement, information on the contrary is easily spread, delivered and obtained. Today, the Internet has been the biggest information pool, from which users can access different kinds of required data. However, when people enjoy the Internet access, attackers may also steal private information through the Internet for a variety of purposes. Currently, new attacks have been developed quickly and new

adfa, p. 1, 2014.

vulnerabilities have been discovered frequently. So it is hard for us to completely protect private information by using IDS, IPS and firewall. Then how to use cryptographic techniques to protect such information has been a very serious and urgent issue.

In the field of data encryption, block cipher is one of the most common method to protect electronic documents from being known to hackers. The most famous and widely used block cipher standards are the Data Encryption Standard (DES)[1], Triple Data Encryption Standard (3DES)[2] and Advanced Encryption Standard(AES)[3] published by National Institute of Standards and Technology (NIST). However, in 1997, DES message has been broken for the first time in public. And in 1999, the security key of DES has been broken[4]. Due to the rapid advance of hardware speed and parallel computing, securely protecting this type of fixed-key cryptography has been a technical challenge[5]. Now the block cipher standards still used in many ways to protect personal privacy and confidential information. We hope to enhance their security levels without significantly changing their original structures.

Therefore, in this study, we propose a random number protection approach, named Initialization Cipher Block Method (ICBM for short), which strengthens the security of the block cipher standards by adding random parameters, which are themselves unpredictable, to them. Security analysis shows that the random parameters as security keys can effectively rise the security level of a system since only the user who has the legitimate keys can solve those messages protected by these random parameters.

The rest of this paper is organized as follows. Section 2 introduces the most popular block cipher standards. Section 3describesthe proposed method. The security of Initialization Cipher Block Method is analyzed in Section 4.Section5concludes this paper and outlines our future studies.

2 Related Work

In this section, we individually introduce DES, 3DES and AES.

2.1 DES and 3DES

DES algorithm was first developed between 1973 and 1974 by International Business Machines Corporation (IBM). This proposal was then accepted and published by National Bureau of Standards (NBS), the predecessor of National Institute of Standards and Technology (NIST). It is now one of the data encryption standards. Generally, its security key is used to customize the transformation from ciphertext to plaintext, i.e., only the user who has current key can solve the ciphertext. The original length of a key is 64 bits. But only 56 bits are used to encrypt data. Other 8 bits, employed to check data parity, are abandoned after encrypting data. Due to short key length, nowadays DES is no longer a secure block cipher standard.

The 3DES is then proposed to solve the short-key problem by repeating DES operations three times, as three phases, to complete its data encryption and decryption. Because users can choose different keys for each phase each time when 3DES is invoked, the length of a key is then $168(= 56 \times 3)$ bits.

The encryption process of 3DES does not really repeat DES encryption process. In the second phase, it decrypts the data, and in the third, it encrypts the data again. In other words, an integral 3DES encryption uses DES encryption-decryption-encryption process and its decryption employs DES decryption-encryption-decryption process. If

the three keys utilized in the three phases of encryption and decryption are the same, 3DES is indeed a DES.

2.2 AES

AES algorithm was published by NIST in 2001 to substitute for the DES. Its block size is 128 bits. But the key length can be 128, 192 or 256 bits. Generally, a longer key can raise a system's security level.AES operation needs a 4×4matrix, in which an element is 8 bits long. Due to allowing different key lengths, the encryption / decryption algorithms will repeat 10, 12 or 14 rounds and each round includes 4 steps, except the last round. The 4 steps are as follows.

Step 1: AddRoundKey. When an encryption round starts, AES generates a round key by invoking the Rijndael key schedule[3], and the key is then XORed with the underlying plaintext block.

Step 2: SubByte. In this step, an element of the 4*4 matrix is moved to its designated position according to the content of the Rijndael S-box, which provides the matrix with a nonlinear transformation.

Step 3 ShiftRow. In this step, row i left shifts i bytes, i = 0, 1, 2, 3.

Step 4: MixColumns. In a column, the 4 bytes from bottom to top are treated as the coefficients of the 1, X, X^2 and X^3 in a $GF(2^8)$ polynomial. The column is first multiplied with $3X^3 + X^2 + X + 2$and moduloed by $X^4 + 1$.

3 Initialization Cipher Block Method (ICBM)

In the ICBM, there is a cipher block generated before the system starts encrypting data. The main function of this cipher block is protecting those random parameters used to encrypt the parent key. Of course, the length of the cipher block is changed if the lengths of the given key is different.

3.1 Parameters and Functions definition

In the following, we first define the parameters and functions used by the ICBM:

K: The key of block ciphering. Its length can be changed to meet the key length of the standard being concerned.

S-box: The S-box utilized when collaborating with DES or AES.

K_{01}: The first transient key generated by substituting for the bytes of K, following the content of S-box.

K_{02}: The second transient key generated by XORing K with K_{01}.

RND: The random parameter, the length of which is determined by the length of K. There are many methods to generate RND, e.g., invoking a random number generation function or using the One Time Password(OTP) system provided by a programming language, like Java/C++.

$+_2$: A binary adder, which is a logical operator defined in [6].

$-_2$: The inverse operation of$+_2$ [6].

K': The system key calculated by binary-adding RND and K_{02} for substituting for K to encrypt / decrypt data blocks.

ICB: Initialization Cipher Block, which when delivered is placed at the position in front of ciphertext.

3.2 Encryption process of ICBM

Step 1.K is the parent key of block ciphering, i.e., 56 bits for DES, and 128, 192 or 256 bits for AES. After K is input, the proposed system will calculate the corresponding value, following the content of the S-box of the selected block cipher standard, and then generate the first transient key K_{01}.

Step 2. Calculating the second transient key K_{02} by XORing K_{01} with K.

Step 3. Generating RND by using the example method mentioned above and then encrypting it with K_{01} and K_{02} to generate two outputs. One is K' which substitutes for K in the following encryption and decryption processes. The other is ICB which is output with the ciphertext and as stated above, is placed at the position in front of the ciphertext. In decryption process, the ICB needs to be decrypted first to obtain the random parameter RND for the following decryption, i.e.,

$$K' = RND +_2 K_{02} \quad (1)$$

$$ICB = RND +_2 K_{01} \quad (2)$$

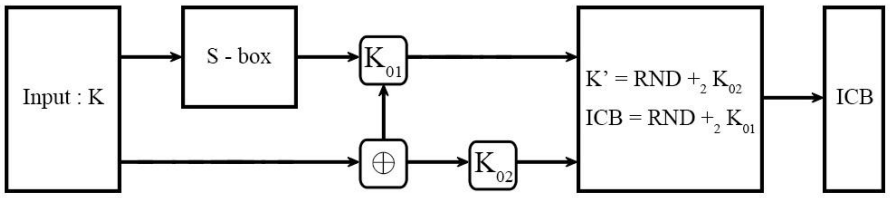

Fig. 1 Generation process of ICB

3.3 Decryption process of ICBM

Step 1. As shown in Fig. 1, the first transient key $K_{01}$is obtained by substituting the bytes of K, following the content of DES / AES S-box.

Step 2. Calculating the second transient key K_{02} by XORing $K_{01}$with K.

Step 3. After the generation of K_{01} and K_{02}, RND and K' can be obtained by invoking the following formulas.

$$RND = ICB -_2 K_{01} \quad (3)$$

$$K' = RND +_2 K_{02} \quad (4)$$

4 Security Analysis

This section will describe the security of the Two-Dimensional Operation and Initialization Cipher Block Method.

4.1 Security of the Two-Dimensional Operation

Generally, the field of electronic cryptography only uses XOR($\oplus$) to encrypt / decrypt data because it is a fast and simple operation. If plaintext A and a key B are of the same length n, the probability of cracking A $\oplus$ Bis $\frac{1}{2^n}$, which is also the cost of cracking a key by using a brute-force method.

In this study, we utilized another logic operator, the Binary Adder($+_2$), to enhance the complexities of the encryption / decryption processes of the ICBM. The security level of $+_2$ is the same as that of XOR [6]. If a key Y of m bits in length is employed to encrypt plaintext X of also m bits long, the probability of cracking X $+_2$ Yis $\frac{1}{2^m}$ [7].

4.2 Security of Initialization Cipher Block Method

In the ICBM, we assume that (1) the system key K is X bits in length where X is determined by the block cipher standard invoked, i.e., a key is 56 bits for DES, 56 to 168 bits for 3DES and 128 to 256 bits for AES;(2) there is a random parameter RND which is also X bits long;(3) the attacker has invalidly acquired ICB with the goal of obtaining K.

In section 3.2, the ICB is calculated by adding K_{01} and RND with $+_2$.To crack K, the attacker needs to solve current pair of $\langle RND, K_{01} \rangle$by using the invalidly acquired ICB and the anti-operator$-_2$.Thecracking probability P of using a brute-force method is $\frac{1}{2^X}$.

In the cracking process, the values of all parameters are guessed by the attacker, except ICB. Even users use a fixed K to encrypt their data, and K_{01} and K_{02} are parameters of a specific length, it is hard for the attacker to solve K since K is encrypted by RND and RND is unknown to the attacker. The security level of this method is higher than that of only expanding the length of a key due to the unpredictability of RND.RND is different each time when it is generated for a session.

5 Conclusions and Future Studies

In this paper, we propose the ICBM which employs random parameters to increase the unpredictability of the generated ICB. This is a special design for encrypting keys before plaintext is encrypted. So it can be widely applied to different block cipher standards, like DES, 3DES and AES. What we need to do is adjusting the length of RND to meet the key length of employed standard.

ICBM only uses the basic operators, like $\oplus$,$+_2$and $-_2$, and one S-box. Its consumption time is short. In the future, we will apply this concept to block cipher algorithms and design an encryption system which has the characteristics of higher randomness, security and processing speed than those of the ICBM. We would also like to derive the reliability model and performance models for the ICBM and the newly designed system mentioned so that users can predict their reliability and performance before using them. These constitute our future studies.

Acknowledgements:

This research was partially supported by TungHai University on GREENs project, and National Science Council, Taiwan, grants NSC 100-2221-E-029-018 and 101-2221-E-029-003-MY3. This research was also in part supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT & Future Planning (2014R1A1A1005915).

6 Reference

1. FIPS Publication 46-3, Data Encryption Standard (DES), U.S. DoC/NIST, October 25, 1999.
2. National Institute of Standards and Technology, NIST Special Publication 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Reversion 1.1, January 2012.
3. FIPS Publication 197, Advanced Encryption Standard (AES), U.S. DoC/NIST, November 26, 2001.
4. http://en.wikipedia.org/wiki/Data_Encryption_Standard
5. NIST Special Publication 800-57 Recommendation for Key Management — Part 1: General (Revised), March 2007.
6. K. C. Wei, Y. L. Huang, and F. Y. Leu, "A Secure Communication over Wireless Environments by Using a Data Connection Core," Computers and Mathematics with Applications, in press.
7. Y.L. Huang, F.Y. Leu, and C.R. Dai, "A Secure Data Encryption Method by Employing a Feedback Encryption Mechanism and Three-Dimensional Operation," Multidisciplinary Research and Practice for Information Systems, Lecture Notes in Computer Science Volume 7465, 2012, pp. 578-592.