Submit to: Workshop on Cryptology and Information Security

Dynamic Triple-DES

Chu-Hsing Lin*, Yi-Shiung Yeh** and Chen-Yu Lee**

**Department of Computer Science and Information Engineering,*
Tunghai University, 407 Taichung, Taiwan, ROC
TEL: 04-23590121 ext. 3287 FAX: 04-23591567

E-mail: chlin@mail.thu.edu.tw

***Institute of Computer Science and Information Engineering,*
National Chiao Tung University, 300 Hsinchu, Taiwan, ROC
TEL: 03-5712121 ext. 54713 FAX: 03-5724176
E-mail: ysyeh@csie.nctu.edu.tw

Correspondence Address:

Dr. Chu-Hsing Lin

Department of Computer Science and Information Engineering,
Box 809, Tunghai University, 407 Taichung, Taiwan
E-mail : chlin@mail.thu.edu.tw
TEL: 04-23590121 ext. 3287
FAX: 04-23591567

Keywords: Triple-DES, Block ciphers, Differential cryptanalysis, S-Box.

Dynamic Triple-DES

Chu-Hsing Lin*, Yi-Shiung Yeh** and Chen-Yu Lee**

**Department of Computer Science and Information Engineering,*
Tunghai University, 407 Taichung, Taiwan, ROC

E-mail: chlin@mail.thu.edu.tw

***Institute of Computer Science and Information Engineering,*
National Chiao Tung University, 300 Hsinchu, Taiwan, ROC
E-mail: ysyeh@csie.nctu.edu.tw

Abstract

In this article, we propose a variant of Triple-DES, called dynamic Triple-DES, in which permutations are used to make S-Boxes key dependent. By keeping the permutation information in secret, the new version of Triple-DES is more secure.

Keywords: Triple-DES, Block ciphers, Differential cryptanalysis, S-Box.

1. Introduction

Triple-DES [1], shown in Figure 1, was published and adopted as a federal standard in FIPS 46-3. In 1997, NIST called for AES proposals [2] and finally published the FIPS 197 as a federal standard in November 2001. In the past, various cryptanalytic methods against Triple-DES have been proposed. In addition to the brute-force attack [3], the differential attack [3], the chosen plaintext attack [4], and the known plaintext attack [5] also threaten Triple-DES although they are not yet awful to break it.

In 1990, Biham and Shamir proposed a new technique of cryptanalysis [6] indicated as the differential attack. It is a statistical attack against DES-like cryptosystems and it is more efficient than the brute force attacks. This method works mainly on attacking block ciphers. By using this method, a cryptanalyst looks at the differences of plaintext pairs and that of ciphertext pairs. Especially, the attacker examines ciphertext pairs whose plaintexts have particular difference conditions. There exists a high probability that certain plaintext difference will result in certain ciphertext difference. A difference pattern with high probability will be useful for the deduction of some key bits. The knack is by inputting the plaintext pairs with required difference into the enciphering algorithm to get the corresponding ciphertexts, and then some key values will be suggested according to the ciphertexts and the difference pattern. A best guess of the difference pattern will suggest some key values; on the other hand, a bad guess may suggest incorrect key values. Accordingly, with certain difference patterns, the probabilities to the possible keys are assigned. Eventually, the most probable key is located when enough number of plaintext pairs has been analyzed. Differential cryptanalysis requires more than 10^{52} operations to attack Triple-DES during analysis [3].

One reason of the vulnerability of Triple-DES (and DES-like cryptosystems) to attacks is the use of fixed and public S-boxes. This feature profits an attacker for cryptanalysis. This inspires us to propose a method to strengthen Triple-DES against attacks by rearranging the order of S-boxes dynamically. However, the similar method can be applied to various block ciphers.

In this paper, we propose a variant, called a dynamic Triple-DES, which withstands the aforementioned cryptanalytic approaches. In the dynamic Triple-DES, S-boxes are variable, dependent on keys and thus it can resist the attacks.

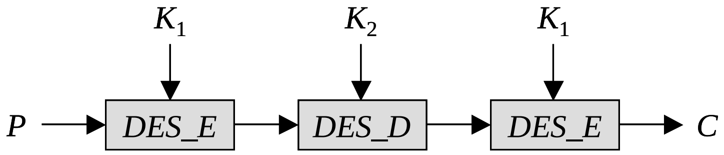

Figure1. Triple-DES

2. Dynamic Triple-DES

Triple-DES is encrypt-decrypt-encrypt (EDE) mode [10] and each DES has 16 rounds, which have eight constant S-boxes, each of them is a mapping from {0,...,63} to {0,...,15}, or indicated as the function S: [0..63]→[0..15], used in a fixed order. The fixed and public feature is convenient for cryptanalysis. To remedy the situation, more flexible use of S-boxes is needed. The change is to rearrange the order of S-boxes in the succeeding rounds. In detail, let a permutation (a bijective function) p:[1..8]→[1..8] be used to construct the new order. Then the i^{th} S-box in the j^{th} round will be equal to the $p(i)^{th}$ S-box in the $(j\text{-}1)^{th}$ round. For example, suppose that the S-boxes sequence in the previous one round is indicated as $S_1S_2S_3S_4S_5S_6S_7S_8$ and the given permutation is (3,2,7,8,1,4,6,5). Then the S-boxes sequence in the following round will be $S_3S_2S_7S_8S_1S_4S_6S_5$.

By keeping the permutation information in secret, the exact use of S-boxes is not explicit. This increases the difficulty of differential cryptanalysis. The secret permutation can be derived from additional key values. In the case, the key length of Dynamic Triple-DES (D3DES) may be extended to 136 bits in which 24 bits are used to indicate the secret permutation.

3. Practical Considerations

For the simple way, the whole data of S-boxes can be retained in two dimensions array with size 8×64. Note that to maintain an S-box, it needs a table of 64 words, each word with length of 4 bits. Without loss of generality, let the table be M[1..8,1..64] and the initial S-boxes sequence be $S_1S_2S_3S_4S_5S_6S_7S_8$. Then the k^{th} word (4-bit) of S_i is placed in the entry of $M[i, k]$. While applying a permutation function p on the S-boxes, the S-boxes sequence of the first round in an encryption process will become $S_{p(1)}S_{p(2)}S_{p(3)}S_{p(4)}S_{p(5)}S_{p(6)}S_{p(7)}S_{p(8)}$. That is, the value of the k^{th} word of the i^{th} S-box is placed in the entry of $M[p(i), k]$. Generally, the S-boxes sequence of the j^{th} round will become $S_{p^j(1)}$ $S_{p^j\,(2)}$ $S_{p^j\,(3)}$ $S_{p^j\,(4)}$ $S_{p^j\,(5)}$ $S_{p^j\,(6)}$ $S_{p^j\,(7)}$ $S_{p^j\,(8)}$, where $p^j_{(i)}$ indicates that the permutation p is composed j times with itself or symbolically $p(p(...p(p(i))...))$. It is obvious that the value of the k^{th} word of the i^{th} S-box in the j^{th} round can be found in the entry $M[p^j_{(i)}, k]$.

According to the above description, we know that a word in any S-box can be easily accessed from the table retaining the S-boxes while a permutation function is enforced to the S-boxes. Comparing to original Triple-DES, the extra cost for dynamic Triple-DES is that for the permutations. This never exceeds 16 times of nested mapping because of the 16 rounds of each DES structure. Since the permutation can be implemented very efficiently, which will be discussed later. Thus the efficiency of the proposed new algorithm is the same as that of Triple-DES.

While decrypting, on the other hand, the same 16 S-boxes sequences in the encryption/decryption process will be used, but with the sequences order reversed. This does not increase the computational complexity.

4. Security Analysis

Triple-DES is not susceptible to the meet-in-the-middle attack [8], but Merkle and Hellman developed a chosen-plaintext attack [4] requiring 2^{56} operations and 2^{56} words of memory. In 1998, Oorschot and Wiener converted above scheme to a known-plaintext attack [5]. The attack still requires a running time on $2^{120-log_2 n}$ operations and *n* words of memory, where *n* is the number of plaintext-ciphertext pairs. They are not very practical, but are weaknesses.

The probability of a cryptanalysis for D3DES focuses on all the sequences of the permutation on 8 S-boxes, that is, 40320 (= 8!) possible cases. According to the investigation of Matsui [7], with the differential cryptanalysis which derived by tracing the spread of differential values in each round. Although the situation in the research of Matsui, which permutes the order of S-boxes just once, it is not exactly the same as our proposed scheme. Thus, a block cipher with weaker S-boxes sequence for differential cryptanalysis, such as DES, can be modified to be more secure against it.

The above chosen-plaintext and known-plaintext attacks require numerous amount plaintext and ciphertext pairs, which are pre-computed in the situation that all the sequence of S-box are the same in each round, to analyze the possible key pairs. But it is impossible for a key-owner to provide the huge information.

Triple-DES is the EDE mode, thus the dynamic S-box in Triple-DES can be considered in different situations: whether the sequences are round dependent or round independent, and the sequences in encryption and decryption parts are the same or not. In round dependent, each round uses the same permutation; while in round independent, each round uses different permutations. First, we consider the situation that the sequences in encryption and decryption parts are the same. If the permutation is round dependent, there are 40320 choices. Otherwise, we use different permutations in each round, that resulting in $(40320)^{16} \approx 4.88 \times 10^{73}$ choices with 496 (= 112 + 384) bits key, where 384 = 24 (bits/round) × 16 (round). Secondly, as needed, the sequences may be different in encryption and decryption parts. Under this situation, there are $(40320)^{2} \approx 1.63 \times 10^{9}$ possible choices for round dependent and $(40320)^{32} \approx 2.38 \times 10^{147}$ possible choices for round independent, respectively. The required key sizes for these two cases are extended to 160 (= 112 + 24 × 2) and 880 (=112 + 24 × 16 × 2) bits, respectively. Figure 2 shows the possible choices in each type of D3DES.

We use the 8 S-Boxes of Triple-DES but their orders for D3DES are changing. The order of 8 S-Boxes in each round of D3DES is unknown. We know that differential cryptanalysis works only on the knowing composition of the S-Boxes [9]. If the S-Boxes are key-dependent, then differential cryptanalysis is much harder. Therefore, differential attack on D3DES is much difficult than on Triple-DES. Since the order of S-Boxes on each round of D3DES are unknown, then we can not give the requirement of the number of chosen-plaintexts or known-plaintexts or DES operations during differential analysis on D3DES.

Choices	**E = D**	**E ≠ D**
Round dependent	**40320**	**1.63×10^{9}**
Round independent	**4.88×10^{73}**	**2.38×10^{147}**

Figure 2. Possible choices in each type

5. Conclusions

D3DES may provide greater resistance to differential attacks than the original Triple-DES. By applying permutation functions on the sequences of S-boxes such that their orders are variable in the succeeding rounds, the use of S-boxes become more confused. However, the permutation information should be kept secret and is better to derived from additional key material, otherwise the confusion effect no more exists and even favors to cryptanalysis. Some block ciphers use implement-dependent (non-fixed) S-boxes, such as GOST [11] to be Dynamic-GOST [12]. The feature favors them to resist linear attacks. On the other hand, since the order of S-Boxes in each round of D3DES is unknown, we believe that differential attack on D3DES is much more difficult than on Triple-DES. However, the same vantage is not held when the contents of the S-boxes are open to the public or known by the adversary. In the situation, the dynamic S-boxes scheme may be applied to strengthen their security.

References

[1] *Federal Information Processing Standard Publication* 46-3, “Data Encryption Standard (DES),” October 25, 1999. http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

[2] *Federal Information Processing Standard Publication* 197, “Announcing the Advanced Encryption Standard (AES),” November 26, 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[3] D. Coppersmith, "The Data Encryption Standard (DES) and its strength against attacks," *IBM Journal of Research and Development*, vol. 38 no. 3, May 1994, pp. 243-250.

[4] R. Merkle, and M. Hellman, “On the Security of Multiple Encryption,” *Communications of the ACM*, vol. 24, November 1981, pp. 465-167.

[5] P. Oorschot, and M. Wiener, “A Known-plaintext Attack on Two-Key Triple encryption,” *Proceedings of EUROCRYPT ’90*, Springer-Verlag, 1990.

[6] E. Biham and A. Shamir, “Differential Cryptanalysis of DES-like Cryptosystems,” *Proceedings of CRYPTO’90*, Springer-Verlag, 1991, pp. 2-21.

[7] M. Matsui, “On Correlation Between the Order of S-boxes and the Strength of DES,” *Proceedings of EUROCRYPT’94*, Springer-Verlag, 1995, pp. 366-375.

[8] W. Diffie, and M. Hellman, “Exhaustive Cryptanalysis of the NBS Data Encryption Standard,” Computer, vol. 10, no. 6, June 1977, pp. 7484.

[9] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C 2nd edition*, John Wiley & Sons, Inc., 1996.

[10] ANSI X9.17, “American National Standard for Financial Institution Key Management,” American Bankers Association, 1995.

[11] B. Schneier, “The GOST Encryption Algorithm,” *Dr. Dobb’s Journal*, vol.20, no.1. January 1995, pp.123-124.

[12] Y. S. Yen, C. H. Lin, and C. C. Wang, “Dynhamic GOST,” *Journal of Information Science and Engineering*, vol. 16, 2000, pp. 857-861.