Known-IV Attacks on Triple Modes of Operation of Block Ciphers

Deukjo Hong[1], Jaechul Sung[1], Seokhie Hong[1], Wonil Lee[1], Sangjin Lee[1],
Jongin Lim[1], and Okyeon Yi[2] ⋆

[1] Center for Information Security Technologies (CIST),
Korea University, Anam Dong, Sungbuk Gu,
Seoul, Korea
{hongdj, sjames, hsh, nice, sangjin, jilim}@cist.korea.ac.kr
[2] Electronics and Telecommunications Research Institute (ETRI),
161 Gajeong-dong, Yusong-Gu, Daejon, 305-350, Korea
{oyyi@etri.re.kr}

Abstract. With chosen-IV chosen texts, David Wagner has analyzed the multiple modes of operation proposed by Eli Biham in FSE'98. However, his method is too unrealistic. We use only known-IV chosen texts to attack many triple modes of operation which are combined with cascade operations. 123 triple modes are analyzed with complexities less than E. Biham's results. Our work shows that the securities of many triple modes decrease when the initial values are exposed.

Keywords: Block cipher, mode of operation for DES, Triple DES

1 Introduction

Since the appearance of DES [7], several attacks on DES and its variants have been suggested. E. Biham and Adi Shamir introduced differential cryptanalysis of DES in 1991 and 1992 [3, 4]. Mitsuru Matsui analyzed DES with linear cryptanalysis in 1993 and 1994 [5, 6]. Differential cryptanalysis and linear cryptanalysis are the most powerful methods for attacking DES. These attacks have led many people in the cryptographic community to suggest stronger replacements for DES, which can be either new cryptosystems or new modes of operation for the DES. So triple DES instead of DES has been used and applied to the modes of operation for DES — ECB, CBC, OFB, and CFB. Triple DES is even more secure but slower than DES. This reason has led to consideration of multiple modes of operation combined from several consecutive applications of single modes. In hardware implementation, the multiple modes have an advantage that their speed is the same as of single modes because the single modes can be pipelined. In particular, the triple modes were expected to be as secure as triple DES although they have DES as a building block.

⋆ Supported by a grant of Electronics and Telecommunication Research Institute, Korea.

In 1994 and 1996, E. Biham analyzed many triple modes of operation with chosen plaintexts and chosen ciphertexts, and showed that every mode considered except the the triple ECB mode is not much more secure than single modes [1, 2]. Considering dictionary attacks or matching-ciphertext attacks, the commonly-used triple-DES-ECB mode when used with some outer chaining technique is not much more secure than any single modes. To solve this state of affairs, E. Biham proposed 9 new block modes and 2 new stream modes of operation for DES. The complexities of attacking these new modes are conjectured to be at least 2^{112}. The quadruple modes were conjectured to be more secure than any triple mode; furthermore, the complexity of attacking two of the quadruple modes was conjectured to be at least 2^{128}.

In 1998, D. Wagner analyzed E. Biham's proposals [8]. Using the chosen-IV chosen text queries he broke them with the complexities lower than what E. Biham has conjectured. His method utilizes an equation for an exhaustive search for a key or looks for a collision for a birthday attack. Since E. Biham's studies were premised on a more restrictive threat model that did not admit chosen-IV attacks, D. Wagner's results do not disprove E. Biham's conjectures but raise questions about the security of E. Biham's proposed modes.

D. Wagner's assumption of chosen-IV is too unrealistic, so we use known-IV chosen texts more practical than chosen-IV to re-analyze the triple modes which E. Biham analyzed. Our attacks take their place between E. Biham's and D. Wagner's in terms of controlling IVs. However, since for fixed IVs the birthday paradox is not available as D. Wagner, our attacks cannot break E. Biham's proposals. Our results show how much the security of each triple mode decreases when the initial value is exposed.

2 Preliminaries

In this section, we describe something to understand our attack. Note that the underlying block cipher of every mode throughout this paper is DES with 64 bit plaintext and 56 bit key.

We write $P_0, P_1, \cdots$ (or $C_0, C_1, \cdots$, respectively) for the blocks of the plaintext (or ciphertext, respectively). We number the keys $K_1, K_2, \cdots$ and the initial values $IV_1, IV_2, \cdots$ according to the order that the single-mode appears in the triple modes. The capital letters $A, B, \cdots$ are any fixed 64-bit values if no additional explanations for them are given.

D. Wagner chose initial values and plaintexts or ciphertexts to analyze the multiple modes which E. Biham has proposed. His method searches for some equations or collisions to apply to an exhaustive search or birthday attack. Since E. Biham's multiple modes are very secure, we think that it is very hard for anyone to find a proper method to break them. However the assumption that the attacker can choose the initial value is too unrealistic. The assumption of known-IV is more practical than that of chosen-IV because the initial values require integrity rather than secrecy.

When all initial values are known, every double mode is broken by a meet-in-the-middle attack. Furthermore, all except ECB|ECB, CBC|CBC $^{-1}$, CBC|OFB, CBC|CFB^{-1}, OFB|CBC^{-1}, OFB|OFB, OFB|CFB^{-1}, CF B|CBC^{-1}, CFB|OFB, CFB|CFB^{-1} are broken by only two exhaustive searches for two keys. We search equations which isolate one key or two keys to analyze any triple modes. In the initial cases, such a key value is recovered with a 2^{56} exhaustive key search and then remaining two keys are with a meet-in-the middle attack. In most of the latter cases, we can apply a meet-in-the-middle attack to the equation and then find the remaining key with the exhaustive key search.

3 Known-IV Attacks

We analyze 123 out of 216 triple modes. Complete knowledge of IVs is useful in breaking the triple modes which have the feedbacks driven into certain middle parts or arranged in a particular direction. However, it hardly helps the attacker who tries to find the keys of the triple modes with the feedbacks to spread forward and backward.

A meet-in-the-middle attack for double ECB mode requires two known plaintexts. Using the one plaintext, we search some key candidates such that intermediate values are equal. Despite having the wrong key, it may make intermediate values equal with the probability of 2^{-64}. We can find the right keys with a high probability by checking them for the other plaintext.

The meet-in-the-middle attacks in our work also require two equations, two chosen plaintexts, or two chosen ciphertexts. Taking this into account, we choose the plaintexts or the ciphertexts; we classify the attacks according to the choice of the texts.

3.1 *AAB*-attack

This method can break all triple modes in which the first two modes are ECB|ECB. We describe the attack of ECB|ECB|CBC^{-1} as an example. We choose the plaintexts (A, A, B) and obtain the ciphertexts (C_0, C_1, C_2). In Fig. 1, the intermediate values after the first ECB component and the second ECB component are (A', A', B') and (A'', A'', B''). Then the output of the third encryption box in the first block is equal to that in the second block. Therefore, we obtain the following equation.

$$E_{K_3}^{-1}(IV_3 \oplus C_0) = IV_3 \oplus C_0 \oplus C_1$$

So we may find K_3 by a 2^{56} exhaustive search, recognizing the right key value when the above equation holds. We expect no wrong key to survive the check with a high probability.

Finally, K_1 and K_2 can be recovered by the meet-in-the-middle attack with two plaintexts A and B. Consequently, we use 3 chosen plaintexts to break the ECB|ECB|CBC^{-1} mode, whereas E. Biham's method requires 2^{64} chosen plaintexts.

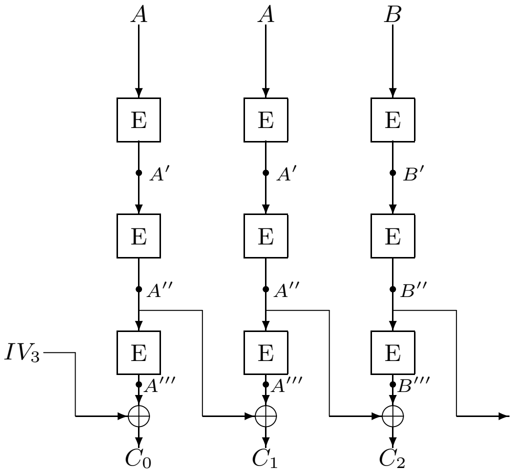

Fig. 1. Attack of ECB|ECB|CBC^{-1}

3.2 *AABB*-attack

This method can break many triple modes in which the last two modes are CBC|ECB. We describe the attack of OFB|CBC|ECB as an example. We choose the ciphertexts (A, A, B, B) and obtain the corresponding plaintexts (P_0, P_1, P_2, P_3). In Fig. 2, the intermediate values entering the second encryption boxes are (A'', A'', B'', B''), where $A' = E^{-1}_{K_3}(A), B' = E^{-1}_{K_3}(B), A'' = E^{-1}_{K_2}(A')$, and $B'' = E^{-1}_{K_2}(B')$. Therefore, we obtain the following equation for the first two blocks.

$$E_{K_1}(IV_1) \oplus E_{K_1}(E_{K_1}(IV_1)) = IV_2 \oplus P_0 \oplus P_1 \oplus E^{-1}_{K_3}(A)$$

K_1 and K_3 are founded by a meet-in-the-middle attack. The right side of the above equation is computed for each of possible key values of K_3 and the result is kept in a table. Then the left side is computed under each of possible key values of K_1 and checked whether the result appears in the table. If a pair of keys (K_1, K_3) satisfies both the above and the following equations, we conclude that they are the right keys for K_1 and K_3.

$$E_{K_1}(E_{K_1}(E_{K_1}(IV_1))) \oplus E_{K_1}(E_{K_1}(E_{K_1}(E_{K_1}(IV_1))))$$

$$= P_2 \oplus P_3 \oplus E^{-1}_{K_3}(A) \oplus E^{-1}_{K_3}(B)$$

K_2 is recovered by brute force. Consequently, we use 4 chosen ciphertexts to break the OFB|CBC|ECB mode, whereas E. Biham's method requires 2^{64} chosen ciphertexts.

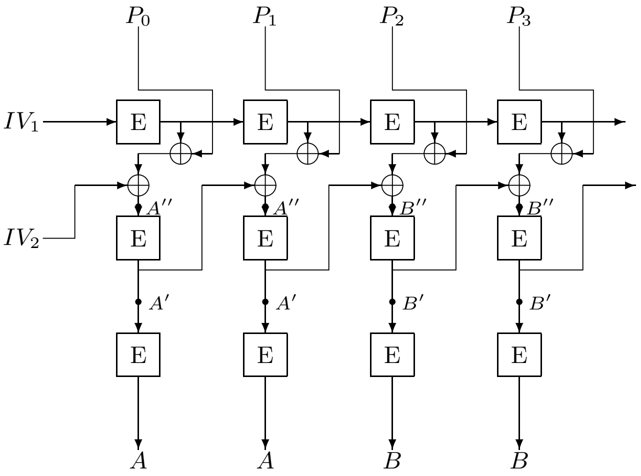

Fig. 2. Attack of OFB|CBC|ECB

3.3 *AAAB*-attack

If the last two modes are a combination of ECB, CBC, or CFB, the triple mode is vulnerable to this attack. We will describe the application of this method to the CBC|CFB|ECB. To find the keys, we choose the ciphertexts (A, A, A, B), and obtain the corresponding plaintexts (P_0, P_1, P_2, P_3). In Fig. 3, the intermediate values after the first ECB component must be of the form (?, F, F, ?). Therefore, the intermediate value entering the first encryption box in the second block is equal to that in the third block. For all the possible values of K_1, we check the following equation.

$$E_{K_1}(IV_1 \oplus P_0) \oplus E_{K_1}(E_{K_1}(IV_1 \oplus P_0) \oplus P_1) = P_1 \oplus P_2$$

Consequently, we use 4 chosen cipehrtexts to break the CBC|CFB|ECB, whereas E. Biham's method requires 2^{36} chosen ciphertexts.

3.4 *AAA*-attack

This attack can break all triple modes in which the first two mode is ECB|OFB. We describe explain the attack of the ECB|OFB|OFB mode as an example. We choose the plaintexts (A, A, A) and obtain the corresponding ciphertexts (C_0, C_1, C_2). The following equations are obtained from the fact that all of the intermediate values after the first ECB mode are equal.

$$E_{K_2}(IV_2) \oplus E_{K_2}(E_{K_2}(IV_2)) = C_0 \oplus C_1 \oplus E_{K_3}(IV_3) \oplus E_{K_3}(E_{K_3}(IV_3))$$

$$E_{K_2}(IV_2) \oplus E_{K_2}(E_{K_2}(E_{K_2}(IV_2)))$$

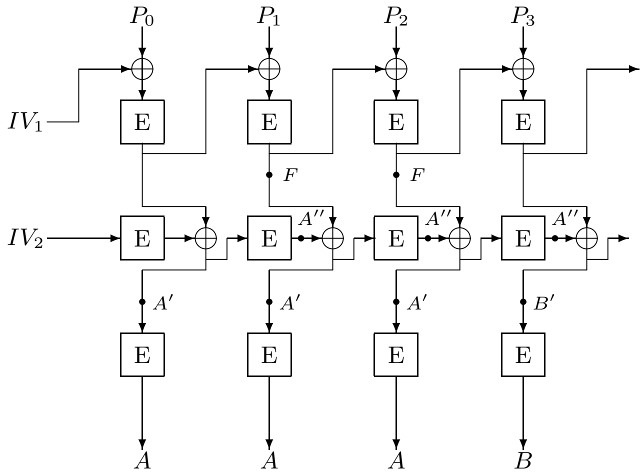

Fig. 3. Attack of CBC|CFB|ECB

$$= C_0 \oplus C_2 \oplus E_{K_3}(IV_3) \oplus E_{K_3}(E_{K_3}(E_{K_3}(IV_3)))$$

Then we can find K_2 and K_3 by a meet-in-the-middle attack. Consequently, we use 3 chosen plaintexts to break the ECB|OFB|OFB mode, whereas E. Biham's method requires 2^{65} chosen plaintexts.

3.5 *IVIVA*-attack

The main targets of this attack are the triple modes in which the last mode is CFB. We explain the attack of the OFB|CFB|CFB mode as an example. We choose the ciphertexts (IV_3, IV_3, A) and obtain the corresponding plaintexts (P_0, P_1, P_2). In Fig. 5, the intermediate values after the second CFB component must be of the form $(B, B, ?)$, where $B = IV_3 \oplus E_{K_3}(IV_3)$. Then, the intermediate value of the input to the second encryption box in the second block is equal to that in the third block. We use the following equation to find K_3 by brute force.

$$E_{K_1}(E_{K_1}(IV_1)) \oplus E_{K_1}(E_{K_1}(E_{K_1}(IV_1))) = P_1 \oplus P_2 \oplus IV_3 \oplus A$$

Consequently, we use 3 chosen ciphertexts to break the OFB|CFB|CFB mode, whereas E. Biham's method requires 2^{66} chosen cipehrtexts.

3.6 *IVIVIV*-attack

This method analyzes many triple modes in which the first mode is any single mode with a feedback and that the second mode is the OFB mode. We explain the attack of the CFB|OFB|CBC mode as a example. We choose the ciphertexts

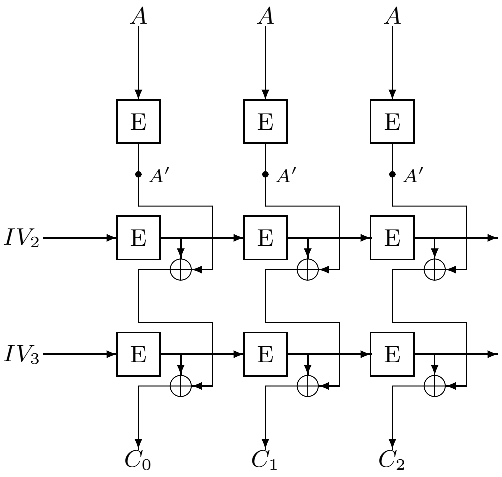

Fig. 4. Attack of ECB|OFB|OFB

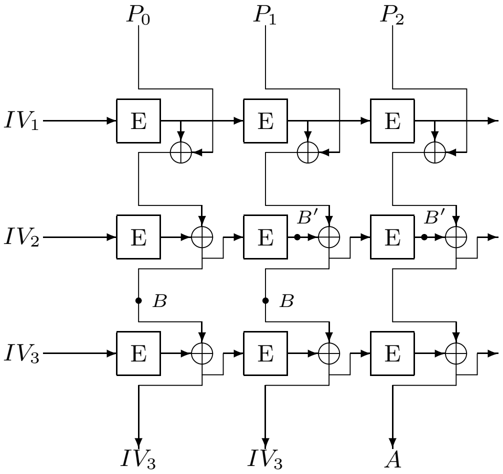

Fig. 5. Attack of OFB|CFB|CFB

(IV_3, IV_3, IV_3) and the corresponding plaintexts (P_0, P_1, P_2). In Fig. 6, all of the intermediate values after the second OFB component are equal. We obtain the following equation.

$$\begin{aligned} E_{K_1}(IV_1) \oplus P_0 \oplus E_{K_2}(IV_2) &= E_{K_1}(E_{K_1}(IV_1) \oplus P_0) \oplus P_1 \oplus E_{K_2}(E_{K_2}(IV_2)) \\ &= E_{K_1}(E_{K_1}(E_{K_1}(IV_1) \oplus P_0) \oplus P_1) \oplus P_2 \oplus E_{K_2}(E_{K_2}(E_{K_2}(IV_2))) \end{aligned}$$

Then we can find K_1 and K_2 by a meet-in-the-middle attack. Consequently, we use 3 chosen ciphertexts to break the CFB|OFB|CBC mode, whereas E. Biham's method requires 2^{66} chosen ciphertexts. Furthermore, it takes $5 \cdot 2^{56}$ encryption times with our attack until its three keys are found, whereas it takes 2^{66} encryption times with E. Biham's attack.

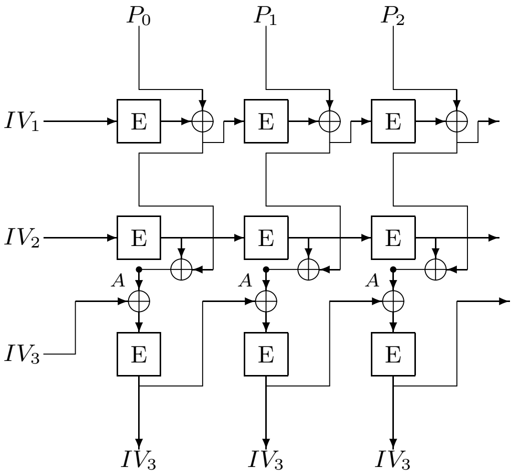

Fig. 6. Attack of CFB|OFB|CBC

3.7 *IVIVIVA*-attack

The triple CBC mode and similar modes are broken by this method. We describe the attack of the triple CBC mode as an example. We choose the ciphertexts (IV_3, IV_3, IV_3, A) and obtain the corresponding plaintexts (P_0, P_1, P_2, P_3). In Fig. 7, the intermediate values after the first CBC component must be of the form (?, $B \oplus B'$, $B \oplus B'$, ?), where $B = IV_3 \oplus E_{K_3}^{-1}(IV_3)$ and $B' = E_{K_2}^{-1}(B)$. Therefore, the second and the third blocks in the values of the input to the first encryption boxes are equal.

$$E_{K_1}(IV_1 \oplus P_0) \oplus E_{K_1}(E_{K_1}(IV_1 \oplus P_0) \oplus P_1) = P_1 \oplus P_2$$

We may find K_1 by a 2^{56} exhaustive keysearch, recognizing the right key value when the above equation holds. Consequently, we use 4 chosen ciphertexts to break the CBC|CBC|CBC mode, whereas E. Biham's method requires 2^{34} chosen ciphertexts.

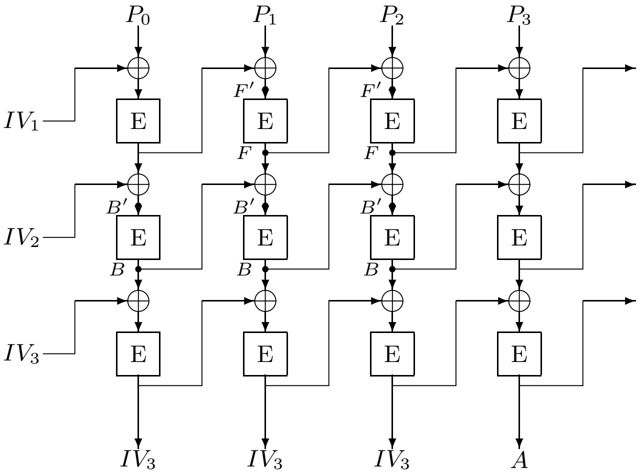

Fig. 7. Attack of CBC|CBC|CBC

3.8 *IVIVAAA*-attack

The ECB|CBC|CFB mode and the CFB|CBC|CFB mode are broken by this method. To find the keys of the ECB|CBC|CFB mode, we choose the ciphertexts (IV_3, IV_3, A, A, A) and obtain the corresponding plaintexts $(P_0, P_1, P_2, P_3, P_4)$. In Fig. 8, the intermediate values entering the second encryption boxes must be of the form $(B, B, ?, F, F)$, where $B = E_{K_2}^{-1}(E_{K_3}(IV_3) \oplus IV_3)$ and $F = E_{K_2}^{-1}(E_{K_3}(A) \oplus A)$. Therefore, for the first and the second blocks, we obtain the following equation.

$$E_{K_1}(P_0) \oplus E_{K_1}(P_1) = IV_2 \oplus IV_3 \oplus E_{K_3}(IV_3)$$

By a meet-in-the middle attack, we find a few candidates of a pair of (K_1, K_3) from the above equation. If a candidate satisfies the following equation which we obtain for the fourth and fifth blocks, we are sure that it is the right value of (K_1, K_3).

$$E_{K_1}(P_3) \oplus E_{K_1}(P_4) = E_{K_3}(IV_3) \oplus E_{K_3}(A)$$

Then K_2 is recovered by an exhaustive search. Consequently, we use 5 chosen ciphertexts to break the ECB|CBC|CFB mode, whereas E. Biham's method requires 2^{34} chosen ciphertexts.

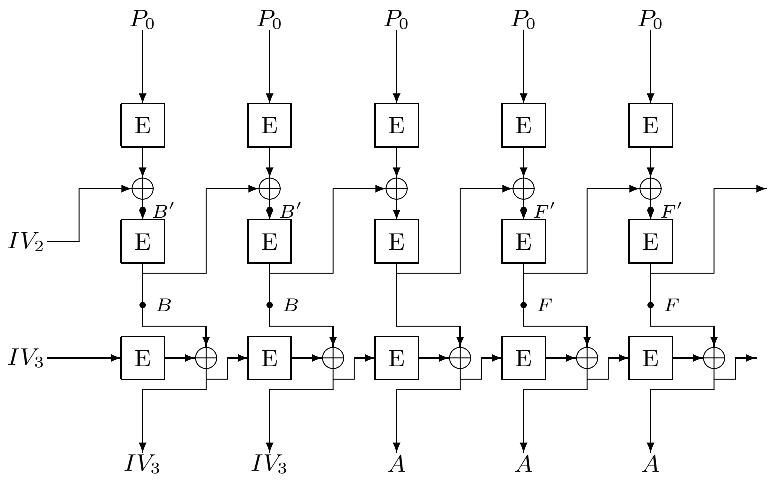

Fig. 8. Attack of ECB|CBC|CFB

3.9 *IVIVAAAB*-attack

We only apply this method to the ECB|CFB|CBC mode. To find its keys of it, we choose the ciphertexts (IV_3, IV_3, A, A, A, B) and obtain the corresponding plaintexts $(P_0, P_1, P_2, P_3, P_4, P_5)$. In Fig. 9, the intermediate values after the second CFB component must be of the form $(F, F, ?, G, G, ?)$, where $F = IV_3 \oplus E^{-1}_{K_3}(IV_3)$, and $G = A \oplus E^{-1}_{K_3}(A)$. Therefore, for the second and third blocks, we obtain the following equation.

$$E_{K_1}(P_1) \oplus E_{K_1}(P_2) = E^{-1}_{K_3}(IV_3) \oplus E^{-1}_{K_3}(A)$$

By a meet-in-the middle attack, we find a few candidates of a pair of (K_1, K_3) from the above equation. If a candidate satisfies the following equation which we obtain for the fourth and fifth blocks, we are sure that it is the right value of (K_1, K_3).

$$E_{K_1}(P_4) \oplus E_{K_1}(P_5) = E^{-1}_{K_3}(A) \oplus E^{-1}_{K_3}(B)$$

Then K_2 is recovered by an exhaustive search. Consequently, we use 6 chosen ciphertexts to break the ECB|CFB|CBC mode, whereas E. Biham's method requires 2^{34} chosen ciphertexts.

4 Conclusion

In this paper, we have presented the attacks to break many triple modes of operation with known-IV chosen plaintexts or chosen ciphertexts. Our results require fewer texts in cryptanalysis of triple modes than E. Biham's. We have

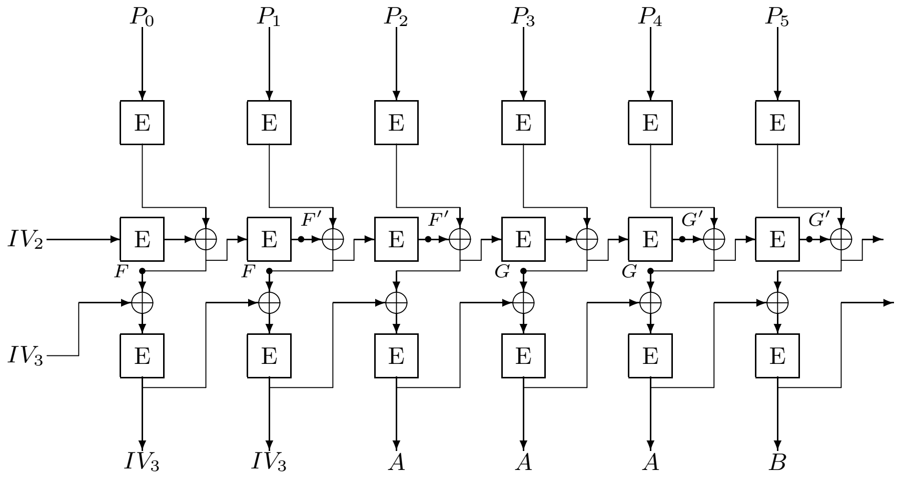

Fig. 9. Attack of ECB|CFB|CBC

analyzed 123 among 216 triple modes of operation. If the initial values are known, the triple modes which have the feedbacks driven into certain middle parts or arranged in a direction may be much weaker than under E. Biham's assumption. They are broken with about 3-4 chosen plaintexts or ciphertexts, 2^{58} encryptions, and 2^{56} memories. However, we could not find the proper method to attack the others when trying to find the keys of the triple modes which have the feedbacks to spread forward and backward. We leave the problem of such triple modes open.

References

1. E. Biham. Cryptanalysis of multiple modes of operation. *Journal of Cryptology*, 011:45–58, 1998.
2. E. Biham. Cryptanalysis of triple modes of operation. *Journal of Cryptology*, 012:161–184, 1999.
3. Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. *J. Cryptology*, 4(1):3–72, 1991.
4. Eli Biham and Adi Shamir. Differential cryptanalysis of the full 16-round DES. In E. F. Brickell, editor, *Advances in Cryptology - CRYPTO'92*, volume 740 of *Lecture Note in Computer Science*, pages 487–496. Springer-Verlag, 1993.
5. Mitsuru Matsui. Linear cryptanalysis method for DES cipher. In T. Helleseth, editor, *Advances in Cryptology - EUROCRYPT'93*, volume 765 of *Lecture Notes in Computer Science*, pages 386–397. Springer-Verlag, 1994.
6. Mitsuru Matsui. On correlation between the order of s-boxes and the strength of DES. In *Advances in Cryptology – EUROCRYPT'94*, volume 950 of *Lecture Notes in Computer Science*, pages 366–375. Springer-Verlag, 1995.

7. National Bureau of Standards. Data Encryption Standard. FIPS Pub. 46, 1977.
8. D. Wagner. Cryptanalysis of some recently-proposed multiple modes of operation. In *FSE'98*, volume 1372 of *Lecture Notes in Computer Science*, 1998.

Appendix

In this appendix we list our result. We follow Biham's notation of the complexity, which consists of three parameters: the number of plaintexts/the number of steps of the attack(the time of encryptions)/the required memory size. 'Biham' is the result in [2] corresponding to ours. We compute some E. Biham's complexities in detail when the differences between our results and them are relatively small.

Table 1. *AAB*-attack

Mode	Complexity	Biham	Inverse
ECB|ECB|CBC	$3/4 \cdot 2^{56}/2^{56}$	$2^{33}/2^{58}/2^{56}$	CBC^{-1}|ECB|ECB
ECB|ECB|CBC^{-1}	$3/3 \cdot 2^{56}/2^{56}$	$2^{64}/2^{58}/2^{56}$	CBC|ECB|ECB
ECB|ECB|OFB	$3/4 \cdot 2^{56}/2^{56}$	$2^{64}/2^{58}/2^{56}$	OFB|ECB|ECB
ECB|ECB|CFB	$3/4 \cdot 2^{56}/2^{56}$	$2^{33}/2^{58}/2^{56}$	CFB^{-1}|ECB|ECB
ECB|ECB|CFB^{-1}	$3/4 \cdot 2^{56}/2^{56}$	$2^{64}/2^{58}/2^{56}$	CFB|ECB|ECB

Table 2. *AABB*-attack

Mode	Complexity	Biham	Inverse
ECB|CBC|ECB	$4/4 \cdot 2^{56}/2^{56}$	$5/2^{59}/-$	ECB|CBC^{-1}|ECB
CBC^{-1}|CBC|ECB	$4/4 \cdot 2^{56}/2^{56}$	$5/2^{59}/-$	ECB|CBC^{-1}|CBC
CBC|CBC|ECB	$4/4 \cdot 2^{56}/2^{56}$	$2^{34}/2^{59}/2^{33}$	ECB|CBC^{-1}|CBC^{-1}
OFB|CBC|ECB	$4/4 \cdot 2^{56}/2^{56}$	$2^{64}/5 \cdot 2^{56}/-$	ECB|CBC^{-1}|OFB
CFB^{-1}|CBC|ECB	$4/4 \cdot 2^{56}/2^{56}$	$5/2^{59}/-$	ECB|CBC^{-1}|CFB
CFB|CBC|ECB	$4/4 \cdot 2^{56}/2^{56}$	$2^{36}/2^{59}/2^{33}$	ECB|CBC^{-1}|CFB^{-1}

Table 3. *AAAB*-attack

Mode	Complexity	Biham	Inverse
ECB|CBC|CBC	$4/4 \cdot 2^{56}/2^{56}$	$2^{33}/2^{59}/2^{33}$	CBC^{-1}|CBC^{-1}|ECB
CBC^{-1}|CBC|ECB	$4/4 \cdot 2^{56}/2^{56}$	$5/2^{59}/-$	ECB|CBC^{-1}|CBC
CBC|CBC|ECB	$4/4 \cdot 2^{56}/2^{56}$	$2^{34}/2^{59}/2^{33}$	ECB|CBC^{-1}|CBC^{-1}
CFB^{-1}|CBC|ECB	$4/4 \cdot 2^{56}/2^{56}$	$5/2^{59}/-$	ECB|CBC^{-1}|CFB
CBC^{-1}|CFB|ECB	$4/4 \cdot 2^{56}/2^{56}$	$4/5 \cdot 2^{56}/-$	ECB|CFB^{-1}|CBC
CBC|CFB|ECB	$4/4 \cdot 2^{56}/2^{56}$	$2^{36}/2^{59}/2^{33}$	ECB|CFB^{-1}|CBC^{-1}
OFB|CFB|ECB	$4/5 \cdot 2^{56}/2^{56}$	$2^{64}/5 \cdot 2^{56}/-$	ECB|CFB^{-1}|OFB
CFB^{-1}|CFB|ECB	$4/4 \cdot 2^{56}/2^{56}$	$4/5 \cdot 2^{56}/-$	ECB|CFB^{-1}|CFB
CFB|CFB|ECB	$4/5 \cdot 2^{56}/2^{56}$	$2^{34}/2^{59}/2^{33}$	ECB|CFB^{-1}|CFB^{-1}
CBC^{-1}|CBC|CBC	$4/4 \cdot 2^{56}/2^{56}$	$2^{34}/2^{59}/2^{33}$	CBC^{-1}|CBC^{-1}|CBC
OFB|CBC|CBC	$4/5 \cdot 2^{56}/2^{56}$	$2^{66}/2^{59}/-$	CBC^{-1}|CBC^{-1}|OFB
CFB^{-1}|CBC|CBC	$4/4 \cdot 2^{56}/2^{56}$	$2^{34}/2^{59}/2^{33}$	CBC^{-1}|CBC^{-1}|CFB

Table 4. *AAA*-attack

Mode	Complexity	Biham	Inverse
ECB|OFB|ECB	$3/5 \cdot 2^{56}/2^{56}$	$2^{64}/5 \cdot 2^{56}/2^{56}$	itself
ECB|OFB|CBC	$3/5 \cdot 2^{56}/2^{56}$	$2^{64}/5 \cdot 2^{56}/2^{56}$	CBC^{-1}|OFB|ECB
ECB|OFB|CBC^{-1}	$3/5 \cdot 2^{56}/2^{56}$	$2^{65}/2^{65}/-$	CBC|OFB|ECB
ECB|OFB|OFB	$3/5 \cdot 2^{56}/2^{56}$	$2^{65}/2^{65}/2^{65}$	OFB|OFB|ECB
ECB|OFB|CFB	$3/5 \cdot 2^{56}/2^{56}$	$2^{64}/5 \cdot 2^{56}/2^{56}$	CFB^{-1}|OFB|ECB
ECB|OFB|CFB^{-1}	$3/5 \cdot 2^{56}/2^{56}$	$2^{65}/2^{65}/-$	CFB|OFB|ECB

Table 5. *IVIVA*-attack

Mode	Complexity	Biham	Inverse
ECB|CFB|CFB	$3/4 \cdot 2^{56}/2^{56}$	$2^{34}/2^{59}/2^{33}$	CFB^{-1}|CFB^{-1}|ECB
CBC|ECB|CBC	$3/3 \cdot 2^{56}/2^{56}$	$2^{34}/2^{59}/2^{33}$	CBC^{-1}|ECB|CBC^{-1}
CBC|ECB|CFB	$3/3 \cdot 2^{56}/2^{56}$	$2^{34}/2^{59}/2^{33}$	CFB^{-1}|ECB|CBC^{-1}
OFB|ECB|CBC	$3/4 \cdot 2^{56}/2^{56}$	$2^{64}/5 \cdot 2^{56}/-$	CBC^{-1}|ECB|OFB
CBC^{-1}|ECB|CBC	$3/4 \cdot 2^{56}/2^{56}$	$4/5 \cdot 2^{56}/-$	itself
CBC^{-1}|ECB|CFB	$3/4 \cdot 2^{56}/2^{56}$	$4/5 \cdot 2^{56}/-$	CFB^{-1}|ECB|CBC
CFB|ECB|CBC	$3/4 \cdot 2^{56}/2^{56}$	$2^{34}/2^{59}/2^{33}$	CBC^{-1}|ECB|CFB^{-1}
CBC^{-1}|CFB|CFB	$3/4 \cdot 2^{56}/2^{56}$	$2^{34}/2^{59}/2^{33}$	CFB^{-1}|CFB^{-1}|CBC
OFB|ECB|CFB	$3/4 \cdot 2^{56}/2^{56}$	$2^{64}/5 \cdot 2^{56}/-$	CFB^{-1}|ECB|OFB
OFB|CFB|CFB	$3/5 \cdot 2^{56}/2^{56}$	$2^{66}/2^{59}/-$	CFB^{-1}|CFB^{-1}|OFB
CFB|ECB|CFB	$3/4 \cdot 2^{56}/2^{56}$	$2^{34}/2^{59}/2^{33}$	CFB^{-1}|ECB|CFB^{-1}
CFB|CFB|CFB	$3/5 \cdot 2^{56}/2^{56}$	$2^{34}/2^{60}/2^{33}$	CFB^{-1}|CFB^{-1}|CFB^{-1}
CFB^{-1}|CFB|CFB	$3/4 \cdot 2^{56}/2^{56}$	$2^{34}/2^{59}/2^{33}$	CFB^{-1}|CFB^{-1}|CFB
CFB^{-1}|ECB|CFB	$3/4 \cdot 2^{56}/2^{56}$	$4/5 \cdot 2^{56}/-$	itself

Table 6. *IVIVIV*-attack

Mode	Complexity	Biham	Inverse
CBC|OFB|CBC	$3/5 \cdot 2^{56}/2^{56}$	$2^{66}/2^{66}/-$	CBC^{-1}|OFB|CBC^{-1}
CBC|OFB|CFB	$3/5 \cdot 2^{56}/2^{56}$	$2^{66}/2^{66}/-$	CFB^{-1}|OFB|CBC^{-1}
CBC^{-1}|OFB|CBC	$3/5 \cdot 2^{56}/2^{56}$	$2^{66}/5 \cdot 2^{56}/-$	itself
OFB|OFB|CBC	$3/5 \cdot 2^{56}/2^{56}$	$2^{65}/2^{65}/2^{65}$	CBC^{-1}|OFB|OFB
CBC^{-1}|OFB|CFB	$3/5 \cdot 2^{56}/2^{56}$	$2^{66}/5 \cdot 2^{56}/-$	CFB^{-1}|OFB|CBC
CFB|OFB|CBC	$3/5 \cdot 2^{56}/2^{56}$	$2^{66}/2^{66}/-$	CBC^{-1}|OFB|CFB^{-1}
OFB|OFB|CFB	$3/5 \cdot 2^{56}/2^{56}$	$2^{65}/2^{65}/2^{65}$	CFB^{-1}|OFB|OFB
CFB|OFB|CFB	$3/5 \cdot 2^{56}/2^{56}$	$2^{66}/2^{66}/-$	CFB^{-1}|OFB|CFB^{-1}
CFB^{-1}|OFB|CFB	$3/5 \cdot 2^{56}/2^{56}$	$2^{66}/5 \cdot 2^{56}/-$	itself

Table 7. *IVIVIVA*-attack

Mode	Complexity	Biham	Inverse
CBC|CBC|CBC	$4/4 \cdot 2^{56}/2^{56}$	$2^{34}/2^{60}/2^{33}$	CBC^{-1}|CBC^{-1}|CBC^{-1}
CBC|CBC|CFB	$4/4 \cdot 2^{56}/2^{56}$	$2^{34}/2^{60}/2^{33}$	CFB^{-1}|CBC^{-1}|CBC^{-1}
CBC|CFB|CBC	$4/4 \cdot 2^{56}/2^{56}$	$2^{34}/2^{60}/2^{33}$	CBC^{-1}|CFB^{-1}|CBC^{-1}
CBC|CFB|CFB	$4/4 \cdot 2^{56}/2^{56}$	$2^{34}/2^{60}/2^{33}$	CFB^{-1}|CFB^{-1}|CBC^{-1}
CBC^{-1}|CBC|CFB	$4/4 \cdot 2^{56}/2^{56}$	$5/5 \cdot 2^{56}/2^{56}$	CFB^{-1}|CBC^{-1}|CBC
CFB|CBC|CBC	$4/4 \cdot 2^{56}/2^{56}$	$2^{34}/2^{60}/2^{33}$	CBC^{-1}|CBC^{-1}|CFB^{-1}
CBC^{-1}|CFB|CBC	$4/4 \cdot 2^{56}/2^{56}$	$5/5 \cdot 2^{56}/-$	CBC^{-1}|CFB^{-1}|CBC
OFB|CFB|CBC	$4/5 \cdot 2^{56}/2^{56}$	$2^{66}/2^{59}/-$	CBC^{-1}|CFB^{-1}|OFB
CFB^{-1}|CFB|CBC	$4/4 \cdot 2^{56}/2^{56}$	$5/5 \cdot 2^{56}/-$	CBC^{-1}|CFB^{-1}|CFB
CFB|CFB|CBC	$4/4 \cdot 2^{56}/2^{56}$	$2^{34}/2^{60}/2^{33}$	CBC^{-1}|CFB^{-1}|CFB^{-1}
OFB|CBC|CFB	$4/5 \cdot 2^{56}/2^{56}$	$2^{66}/2^{59}/-$	CFB^{-1}|CBC^{-1}|OFB
CFB^{-1}|CBC|CFB	$4/4 \cdot 2^{56}/2^{56}$	$5/5 \cdot 2^{56}/-$	CFB^{-1}|CBC^{-1}|CFB

Table 8. *IVIVAAA*-attack

Mode	Complexity	Biham	Inverse
ECB|CBC|CFB	$5/4 \cdot 2^{56}/2^{56}$	$2^{34}/2^{59}/2^{33}$	CFB^{-1}|CBC^{-1}|ECB
CFB|CBC|CFB	$5/4 \cdot 2^{56}/2^{56}$	$2^{34}/2^{60}/2^{33}$	CFB^{-1}|CBC^{-1}|CFB^{-1}

Table 9. *IVIVAAAB*-attack

Mode	Complexity	Biham	Inverse
CBC|CFB|CBC	$6/5 \cdot 2^{56}/2^{56}$	$2^{34}/2^{59}/2^{33}$	CBC^{-1}|CFB^{-1}|ECB