J. Cryptology (2006) 19: 441–462
DOI: 10.1007/s00145-006-0205-3

Journal of
CRYPTOLOGY

Known-IV, Known-in-Advance-IV, and Replayed-and-Known-IV Attacks on Multiple Modes of Operation of Block Ciphers*

Deukjo Hong, Seokhie Hong, Wonil Lee, Sangjin Lee, and Jongin Lim
CIST, Korea University,
Anam-dong, Seongbuk-gu, Seoul, 136-701 Korea
{hongdj,hsh,nice,sangjin,jilim}@cist.korea.ac.kr

Jaechul Sung
Department of Mathematics, The University of Seoul,
Jeonnong-dong, Dongdaemun-gu, Seoul, 130-743 Korea
jcsung@uos.ac.kr

Okyeon Yi
Department of Mathematics, Kookmin University,
Jeongneung-dong, Seongbuk-gu, Seoul, 136-702 Korea
oyyi@kookmin.ac.kr

Communicated by Eli Biham

Received 19 February 2002 and revised 21 February 2006
Online publication 20 September 2006

Abstract. Normally, it has been believed that the initial values of cryptographic schemes do not need to be managed secretly unlike the secret keys. However, we show that multiple modes of operation of block ciphers can suffer a loss of security by the state of the initial values. We consider several attacks according to the environment of the initial values; known-IV attack, known-in-advance-IV attack, and replayed-and-known-IV attack. Our attacks on cascaded three-key triple modes of operation requires 3–7 blocks of plaintexts (or ciphertexts) and $3 \cdot 2^{56}$–$9 \cdot 2^{56}$ encryptions. We also give the attacks on multiple modes proposed by Biham.

Key words. Multiple modes of operation, Block ciphers, Known-IV attacks, Known-in-advance-IV attacks, Replayed-and-known-IV attacks, Cryptanalysis.

* This research was supported by the MIC (Ministry of Information and Communication), Korea, under the ITRC (Information Technology Research Center) support program supervised by the IITA (Institute of Information Technology Assessment).

1. Introduction

Block ciphers are widely applied throughout the cryptographic field. Modes of operation of block ciphers have been developed with two goals. The first is to give a practical and efficient application, and the other is to strengthen the security of the block cipher. As many attacks on block ciphers including differential and linear attacks [3], [6] have been developed, research on methods strengthening the security of block ciphers has become more interesting. Triple-DES has been a popular method in improving the security of DES.

Triple modes of operation were also considered as another simple method to strengthen the security of DES. Performance of some triple modes is faster in hardware than that of Triple-DES due to the fact that they can be designed to be parallelized or pipelined. Therefore, the question whether triple modes actually give any improvement of the security was raised. In [1] and [2] Biham showed that the security of all the cascaded triple modes of operation excluding the triple ECB mode is not so much stronger than any single mode even though the total size of the key of a triple mode is three times that of a single mode. He also proposed some multiple modes of operation with the conjecture that their security is much higher than that of any single mode [2].[1]

Wagner analyzed the security of all Biham's multiple modes [8]. He showed that ten modes among them do not give any improvement of the security when the attacker can choose the initial values for a small number of plaintexts or ciphertexts (up to about 2^{32}). Wagner's results do not disprove Biham's conjecture because Biham did not take the chosen-IV environment into account. However, his work shows that the security of multiple modes may depend on the management of the initial values in general.

Handschuh and Preneel adopted a little more practical condition than Wagner [4]. They suggested various attacks on the cascaded double and two-key triple modes of operation under the known-IV and the replayed-IV environments. In [5] the authors analyzed the security of all the cascaded triple modes of operation under the known-IV environment.

In this paper we refine the attacks suggested in [5]. Strictly, the attacks are classified into the *known-IV attacks*, in which the attacker knows the initial values after choosing the plaintexts or ciphertexts, and the *known-in-advance-IV attacks*, in which the attacker knows the initial values before choosing the plaintexts or ciphertexts. We also describe the *replayed-and-known-IV attacks*. We believe that many applications are not free from the assumption that the attacker can choose plaintexts or ciphertexts and replay some specified values including the initial values.

We apply known-IV, known-in-advance-IV, and replayed-and-known-IV attacks to all the cascaded triple modes of operation. Especially, the replayed-and-known-IV attacks are well applied to the triple modes which have relatively high security against the attacks introduced in [2] and [5]. Our results show that the leakage of the information of the initial values may be an important role to help the attacker find secret keys. It upsets the generally accepted idea that the initial values do not need to be kept secretly. By applying the replayed-and-known-IV attacks, we also analyze the security of the multiple modes proposed by Biham.

[1] There are two versions of [2]. Eleven multiple modes were proposed in the earlier version, but some of them were removed from the later version.

This paper is organized as follows: Section 2 introduces our notations and backgrounds. In Section 3 we describe the known-IV attacks. In Section 4 we describe the known-in-advance-IV attacks. In Section 5 we describe the replayed-and-known-IV attacks. Some concluding remarks are made in Section 6. Tables summarizing the results are given in the Appendix.

2. Preliminaries

2.1. *Notations*

We call the ith application of a single mode in a multiple mode the "ith component" or "ith layer." We assume that the underlying block cipher encrypts a 64-bit plaintext under a 56-bit key like DES. We denote an encryption of a block cipher under a key K by $E_K(\cdot)$. Similarly, we denote a decryption of a block cipher under a key K by $E_K^{-1}(\cdot)$. We consider a plaintext and a ciphertext of a mode of operation as a stream of 64-bit blocks, $P = (P_1, P_2, P_3, \ldots)$ and $C = (C_1, C_2, C_3, \ldots)$, respectively. Each plaintext (or ciphertext) has its own vector of initial values. We denote the initial value of the ith layer of a multiple mode by IV_i. Each component of a multiple mode also has its own key. We denote the key of the ith layer of a multiple mode by K_i.

2.2. *Cascaded Multiple Modes of Operation*

Cascading is the simplest method to combine single modes. We denote cascading two single modes M_1 and M_2 by $M_1|M_2$, which means that the output of M_1 is the input of M_2. We treat all the cascaded triple modes of operation made from the single modes ECB, CBC, OFB, CFB, CBC^{-1}, and CFB^{-1} (Fig. 1). Note that we consider only 64-bit OFB and CFB modes excluding other versions with shorter lengths. From now on, for simplicity and to avoid confusion, a triple mode denotes a cascaded three-key triple mode of operation if any specific description is not given.

2.3. *Security Models*

A characteristic feature of our attacks is the extremely small number of blocks of plaintexts or ciphertexts. As Handschuh and Preneel mentioned in [4], Biham's attacks in [2] usually consider the initial values to be *unknown*, except for some of the modes that are very hard to cryptanalyze otherwise. That is why Biham's many attacks require a plaintext or ciphertext stream with a huge number of blocks for searching for some weakness.

However, converting the unknown-IV environment into a known-IV or chosen-IV environment can reduce the amount of data required for the attacks. If an attacker knows or chooses the initial values, he can aggressively utilize the first block of the encryption or decryption process for his attack. We consider the following attacks as security models for the initial values:

- **Known-IV attack:** In this attack we assume that the attacker knows the initial values after choosing the plaintexts. For example, if the initial values are selected randomly by the encryption algorithm and transmitted with the ciphertext, the attacker cannot know the initial values until he chooses the plaintexts.

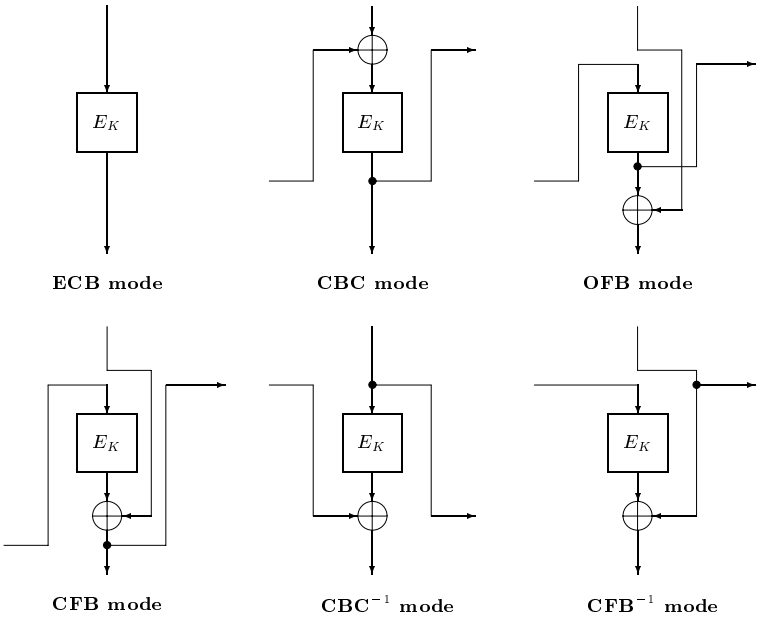

Fig. 1. Single modes of operation.

- **Known-in-advance-IV attack:** In this attack we assume that the attacker knows the initial values before choosing the plaintexts. If a mode of operation uses a counter, sequentially changed, or nonce-generated initial values, it may not be difficult for the attacker to get the initial values before choosing plaintexts. For example, the initial values of the 3GPP confidentiality scheme $f8$ and the 3GPP integrity scheme $f9$ are computed from some packet numbers and default values [9]. The initial value of the encryption mode in SSL is taken from the last block of the ciphertext of the previous session [7]. The use of frame numbers as the initial values is also very common in stream ciphers. Sometimes, the time difference between subsequent packets may allow the attacker to know initial values in advance.
- **Replayed-and-known-IV attack:** A kind of replayed-IV attack was also considered in [4]. Handschuh and Preneel claimed that the initial values can be replayed though they are unknown (e.g., though the initial values are encrypted under another key, the attacker can replay the encrypted values). In general, keeping the initial values secret requires some more actions to be appended. So, in this attack, we assume that the attacker replays the whole or some of the initial values, and knows all the initial values after choosing plaintexts. This attacker is more active than the attackers in the other security models in this paper.

If any chosen-plaintext attack on a multiple mode exists, then the corresponding chosen-ciphertext attack on its inverse mode exists. The chosen-ciphertext attack versions of the above attacks do not match with the case that the initial values are randomly selected and transmitted with the ciphertext; they only match to cases where the sender and receiver share a synchronous algorithm producing and updating initial values. Because

of such limitation, we prefer chosen-plaintext attacks to chosen-ciphertext attacks in most cases.

2.4. *DNC and MIM Attacks*

The tools which we use to give the details of our attacks are the exhaustive search and the meet-in-the-middle attack. In any type of our attacks, the point is how to divide the key space by using the information of initial values. Each component of a multiple mode has its own key. If it is possible to separate all the keys of the multiple mode, then they can be found through the exhaustive search for each key. We call this attack, the *DNC* (*Divide-aNd-Conquer*) *attack*.

We often isolate a pair of keys from the other keys and try to mount the meet-in-the-middle attack. Originally, the meet-in-the-middle attack is defined for a double encryption mode but we call any attack containing the meet-in-the-middle method, the *MIM* (*Meet-In-the-Middle*) *attack*. Usually, a DNC attack is more desirable than an MIM attack because the memory with 2^{56} cells is required for breaking the multiple mode. However, if the attacker already has such a large memory and computing power, then the time complexity is more significant.

The number of plaintext or ciphertext streams required for our attacks is one or two. We require two streams in two cases: when we use the difference of initial values, and when we replay some of the initial values and use the difference of the streams.

3. Known-IV Attacks

We describe known-IV attacks on triple modes of operation. The attacker does not know the initial values when he chooses the plaintexts. We observe that using the CBC, OFB, or CFB mode as the first layer gives resistance against our known-IV chosen-plaintext attack, and similarly that using the CBC^{-1}, OFB, or CFB^{-1} mode as the last layer gives resistance against our known-IV chosen-ciphertext attack.

3.1. *Known-IV DNC Attack*

Among our objectives the modes which are vulnerable to the known-IV DNC attacks are most insecure. It means if the attacker chooses plaintexts or ciphertexts with an intended form and then knows the initial values, he can easily find some equations to separate all the keys of the multiple mode.

We describe the attack on $\text{CFB}^{-1}|\text{ECB}|\text{OFB}$ as an example. Figure 2 depicts this attack. We choose the plaintext $P = (A, A, A, B)$ and obtained the corresponding ciphertext $C = (C_1, C_2, C_3, C_4)$. Then the output of the second component mode is of the form $(\alpha, \beta, \beta, \gamma)$ where $\alpha, \beta, \gamma \in \{0, 1\}^{64}$. These blocks can be computed from the initial value IV_3 and the ciphertext blocks as follows:

$$\beta = E_{K_3}(E_{K_3}(\text{IV}_3)) \oplus C_2, \tag{1}$$

$$\beta = E_{K_3}(E_{K_3}(E_{K_3}(\text{IV}_3))) \oplus C_3. \tag{2}$$

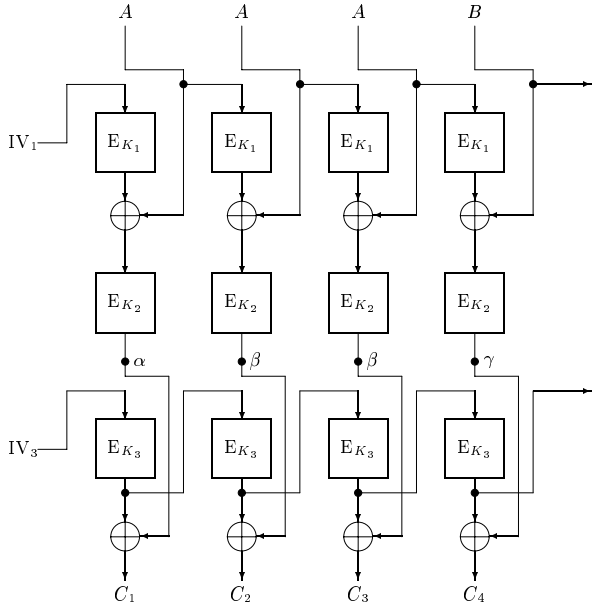

Fig. 2. Known-IV DNC attack on the CFB^{-1}|ECB|OFB mode.

These equations can be combined by cancelling β as follows:

$$E_{K_3}(E_{K_3}(\mathrm{IV}_3)) \oplus E_{K_3}(E_{K_3}(E_{K_3}(\mathrm{IV}_3))) = C_2 \oplus C_3. \tag{3}$$

Then we can exhaustively search for key K_3 to satisfy (3) among 2^{56} candidates. Then the OFB mode is peeled off from the CFB^{-1}|ECB|OFB mode. From the plaintext and the output of the second layer, the ECB mode, the following equations are obtained:

$$\beta = E_{K_2}(E_{K_1}(A) \oplus A), \tag{4}$$

$$\gamma = E_{K_2}(E_{K_1}(A) \oplus B). \tag{5}$$

We can rewrite (4) and (5) by inverting E_{K_2}:

$$E_{K_1}(A) \oplus A = E_{K_2}^{-1}(\beta), \tag{6}$$

$$E_{K_1}(A) \oplus B = E_{K_2}^{-1}(\gamma). \tag{7}$$

Equations (6) and (7) are combined by cancelling $E_{K_1}(A)$ as follows:

$$E_{K_2}^{-1}(\beta) \oplus E_{K_2}^{-1}(\gamma) = A \oplus B. \tag{8}$$

Then we can complete the attack by finding K_2 through the exhaustive search based on (8) and then searching for K_1 exhaustively. The attack requires a 4-block chosen-plaintext and $6 \cdot 2^{56}$ encryptions of the block cipher. The time complexity of Biham's attack on CFB^{-1}|ECB|OFB is similar to our result, but the amount of the data blocks required for the attack is 2^{64}, which is much larger than ours.

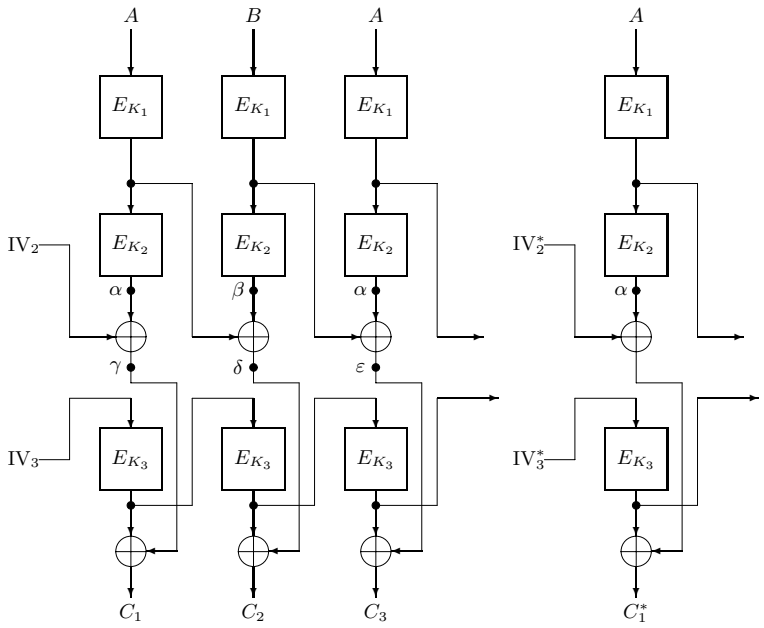

Fig. 3. Known-IV DNC attack on the ECB|CBC^{-1}|OFB mode.

Now we explain the known-IV DNC attack with two chosen-plaintexts. This is a very special attack applied only to the ECB|CBC^{-1}|OFB and ECB|CBC^{-1}|CFB^{-1} modes. We describe the attack on the ECB|CBC^{-1}|OFB mode. This attack is depicted in Fig. 3.

We choose two plaintexts $P = (A, B, A)$ and $P^* = (A)$, and obtain the ciphertexts $C = (C_1, C_2, C_3)$ and $C^* = (C_1^*)$ corresponding to the plaintexts P and P^*, respectively. Let $(\mathrm{IV}_2, \mathrm{IV}_3)$ be the initial values for the plaintext P and let $(\mathrm{IV}_2^*, \mathrm{IV}_3^*)$ be the initial values for the plaintext P^*. The outputs of the encryption boxes of the second layer for enciphering P can be denoted as (α, β, α), where α and β are distinct 64-bit values. Then the output of the encryption box of the second layer for enciphering P^* is also α, and C_1 and C_1^* are computed as follows:

$$C_1 = E_{K_3}(\mathrm{IV}_3) \oplus \mathrm{IV}_2 \oplus \alpha, \tag{9}$$

$$C_1^* = E_{K_3}(\mathrm{IV}_3^*) \oplus \mathrm{IV}_2^* \oplus \alpha. \tag{10}$$

Equations (9) and (10) can be combined by cancelling α as follows:

$$E_{K_3}(\mathrm{IV}_3) \oplus E_{K_3}(\mathrm{IV}_3^*) = C_1 \oplus C_1^* \oplus \mathrm{IV}_2 \oplus \mathrm{IV}_2^*. \tag{11}$$

K_3 is found by the exhaustive search based on (11), and so the last layer is peeled off. Then we can denote the output of the second layer for enciphering P by $(\gamma, \delta, \varepsilon)$, where γ, δ, and ε are known values. α can be computed in two different ways as follows:

$$\alpha = \mathrm{IV}_2 \oplus \gamma, \tag{12}$$

$$\alpha = E_{K_1}(B) \oplus \varepsilon. \tag{13}$$

Again, by cancelling α, we can combine (12) and (13) as follows:

$$E_{K_1}(B) = \mathrm{IV}_2 \oplus \gamma \oplus \varepsilon. \tag{14}$$

We find the correct value of K_1 by using (14) for the exhaustive search, and then the attack is completed by the exhaustive search for K_3. This attack is a little more efficient in time complexity than the attack using only one chosen plaintext, because the former requires $4 \cdot 2^{56}$ encryptions while the latter requires $5 \cdot 2^{56}$ encryptions. Similarly, the known-IV DNC attack using two chosen ciphertexts is applied to the OFB|CBC|ECB and CFB|CBC|ECB modes.

3.2. *Known-IV MIM Attack*

In this subsection we consider the known-IV MIM attack; first, we find a key using the known-IV and the chosen plaintext (or ciphertext), and then use the meet-in-the-middle method to find the other two keys.

As shown in the previous section, if we apply the DNC attack to the CFB^{-1}|ECB|OFB mode with a chosen-plaintext of the form (A, A, A, B), the time complexity is about $6 \cdot 2^{56}$ encryptions. However, if we have a memory of 2^{56} blocks, we can reduce up to $5 \cdot 2^{56}$ encryptions on breaking the CFB^{-1}|ECB|OFB mode as follows.

We choose the plaintext $P = (A, A, A)$ and obtain the corresponding ciphertext $C = (C_1, C_2, C_3)$. We can find K_3 like in Section 3.1. See Fig. 2 again, ignoring the fourth block. From the plaintext $P = (A, A, A)$ and the output of the second layer (α, β, β), the following equations are obtained:

$$\alpha = E_{K_2}(E_{K_1}(\mathrm{IV}_1) \oplus A), \tag{15}$$

$$\beta = E_{K_2}(E_{K_1}(A) \oplus A). \tag{16}$$

By inverting E_{K_2}, (15) and (16) can be transformed as follows:

$$E_{K_1}(\mathrm{IV}_1) \oplus A = E_{K_2}^{-1}(\alpha), \tag{17}$$

$$E_{K_1}(A) \oplus A = E_{K_2}^{-1}(\beta). \tag{18}$$

Note that the left sides of (17) and (18) are associated with only K_1, and the right sides of (17) and (18) are associated with only K_2. So, we can use these equations for the meet-in-the-middle attack. For each candidate of K_1, the left side of (17) is computed and the result is stored in a table. Then for each candidate of K_2 we compute the right side of (17) to look up a match with the result in the table. After finding some pairs of candidates of K_1 and K_2 to satisfy (17), we check whether they also satisfy (18) or not. Then we can get K_1 and K_2 with very high probability.

We also introduce an alternative attack which requires two chosen-plaintexts or chosen-ciphertexts. We did not find how to attack the ECB|CFB|CBC^{-1} mode with known initial values and a single plaintext stream more efficiently than Biham's attack which requires 2^{68} blocks of chosen-plaintext and 2^{66} encryptions. Here, we describe a more efficient attack on the ECB|CFB|CBC^{-1} mode in both data and time complexity than Biham's attack. Figure 4 depicts it. We choose two plaintexts $P = (A, A)$ and $P^* = (A)$. The ciphertexts $C = (C_1, C_2)$ and $C^* = (C_1^*)$ correspond to P and P^*, respectively. All the

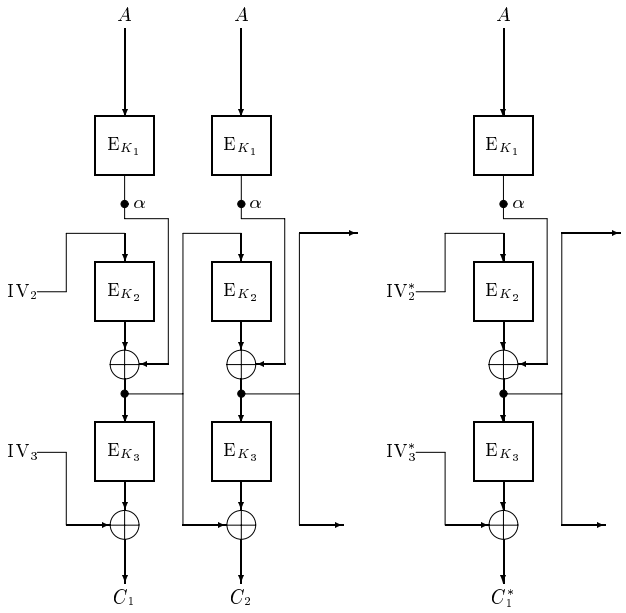

Fig. 4. Known-IV MIM attack on the ECB|CFB|CBC^{-1} mode.

output blocks of the first ECB mode for P and P^* are equal. Let $E_{K_1}(A) = \alpha$. α can be computed from initial values and ciphertexts in the following three ways:

$$\alpha = E_{K_2}(\mathrm{IV}_2) \oplus E_{K_3}^{-1}(\mathrm{IV}_3 \oplus C_1), \tag{19}$$

$$\alpha = E_{K_2}(\mathrm{IV}_2^*) \oplus E_{K_3}^{-1}(\mathrm{IV}_3^* \oplus C_1^*), \tag{20}$$

$$\alpha = E_{K_2}(E_{K_2}(\mathrm{IV}_2) \oplus E_{K_3}^{-1}(\mathrm{IV}_3 \oplus C_1)) \oplus E_{K_3}^{-1}(E_{K_3}^{-1}(\mathrm{IV}_3 \oplus C_1) \oplus C_2). \tag{21}$$

Equations (19) and (20) are combined as follows by cancelling α:

$$E_{K_2}(\mathrm{IV}_2) \oplus E_{K_2}(\mathrm{IV}_2^*) = E_{K_3}^{-1}(\mathrm{IV}_3 \oplus C_1) \oplus E_{K_3}^{-1}(\mathrm{IV}_3^* \oplus C_1^*). \tag{22}$$

Since the left side of (22) is associated with only K_2 and the right side is associated with only K_3, we can find some pairs of candidates of K_2 and K_3 through the meet-in-the-middle method based on (22). After checking for each of the pairs whether (21) is satisfied, we will have almost only one pair of K_2 and K_3. Finally, this attack is completed with the exhaustive search for K_1. Two 2-block chosen-plaintexts, $5 \cdot 2^{56}$ encryptions, and the memory with 2^{56} cells are required for this attack.

4. Known-in-Advance-IV Attacks

In known-in-advance-IV attacks the attacker can know the initial values before choosing plaintexts or ciphertexts. So, he can choose the plaintexts or ciphertexts containing the same blocks as the initial values. Such an ability of the attacker improves known-IV

DNC and MIM attacks, described in Section 3. For example, if the attacker for the CFB^{-1}| CFB^{-1}|CBC mode is in the known-in-advance-IV environment, he had better use the plaintext (IV$_1$,IV$_1$,A) than (A, A, A, B). Known-in-advance-IV DNC attack with (IV$_1$,IV$_1$,A) on the CFB^{-1}|CFB^{-1}|CBC mode requires three blocks of chosen-plaintext and $5 \cdot 2^{56}$ encryptions, while known-IV DNC attack with (A, A, A, B) requires four blocks of chosen-plaintext and $6 \cdot 2^{56}$ encryptions.

The multiple modes whose first layer is the CBC mode were resistant against known-IV chosen-plaintext attacks, because the feedback hides the input of the CBC mode. However, if the attacker knows the initial values before choosing the plaintexts, he can set the first block of the input of the CBC mode to be zero (or any other value) by choosing plaintext with the first block equal to IV$_1$. So, the multiple modes whose first layer is the CBC mode can be vulnerable to known-in-advance-IV attacks with two chosen-plaintexts. Similarly, the multiple modes whose last layer is the CBC^{-1} mode can be vulnerable to known-in-advance-IV attacks with two chosen-ciphertexts. Known-in-advance-IV DNC and MIM attacks with two chosen-plaintexts are introduced in the next two subsections.

4.1. *Known-in-Advance-IV DNC Attacks with Two Chosen-Plaintexts*

We describe the attack on CBC|CFB^{-1}|CBC^{-1} as an example. Figure 5 depicts this attack. We choose two plaintexts $P = (\mathrm{IV}_1, A)$ and $P^* = (\mathrm{IV}_1^*, A)$, and obtain the ciphertexts $C = (C_1, C_2)$ and $C^* = (C_1^*, C_2^*)$ corresponding to P and P^*, respectively. Then the outputs of the first CBC mode are same for P and P^*. Let the output of the first CBC mode be (α, β). The second blocks of the outputs of the second CFB^{-1} mode are

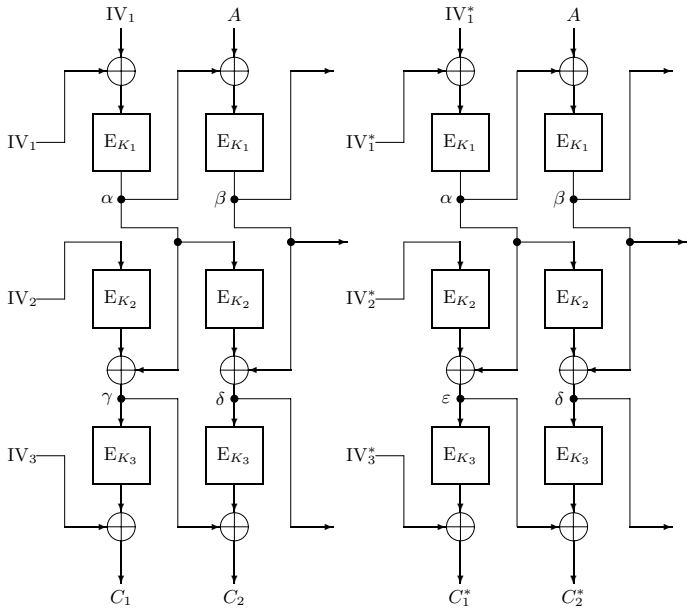

Fig. 5. Known-in-advance-IV DNC attack on the CBC|CFB^{-1}|CBC^{-1} mode.

also the same for P and P^* because both of them are computed as $E_{K_2}(\alpha) \oplus \beta$. Let the output of the second CFB^{-1} mode be (γ, δ) for P and (ε, δ) for P^*. Then δ is computed in two different ways from ciphertexts and the initial values of the last layer as follows:

$$\delta = E_{K_3}^{-1}(E_{K_3}^{-1}(\mathrm{IV}_3 \oplus C_1) \oplus C_2), \tag{23}$$

$$\delta = E_{K_3}^{-1}(E_{K_3}^{-1}(\mathrm{IV}_3 \oplus C_1^*) \oplus C_2^*). \tag{24}$$

If we invert $E_{K_3}^{-1}$,

$$E_{K_3}(\delta) = E_{K_3}^{-1}(\mathrm{IV}_3 \oplus C_1) \oplus C_2, \tag{25}$$

$$E_{K_3}(\delta) = E_{K_3}^{-1}(\mathrm{IV}_3 \oplus C_1^*) \oplus C_2^*. \tag{26}$$

By cancelling $E_{K_3}(\delta)$, we combine (25) and (26) to obtain the following equation:

$$E_{K_3}^{-1}(\mathrm{IV}_3 \oplus C_1) \oplus E_{K_3}^{-1}(\mathrm{IV}_3^* \oplus C_1^*) = C_2 \oplus C_2^*. \tag{27}$$

K_3 is found through exhaustive search based on (27). Then the last layer is removed from CBC|CFB^{-1}|CBC^{-1}. Keeping the attack, we can compute α in two different ways as follows:

$$\alpha = E_{K_2}(\mathrm{IV}_2) \oplus \gamma, \tag{28}$$

$$\alpha = E_{K_2}(\mathrm{IV}_2^*) \oplus \varepsilon. \tag{29}$$

Equations (28) and (29) can be combined to the following equation by cancelling α:

$$E_{K_2}(\mathrm{IV}_2) \oplus E_{K_2}(\mathrm{IV}_2^*) = \gamma \oplus \varepsilon. \tag{30}$$

We find K_2 through exhaustive search based on (30), and then K_1 by applying a simple exhaustive search. This attack requires two 2-block chosen-plaintexts and $5 \cdot 2^{56}$ encryptions.

4.2. *Known-in-Advance-IV MIM Attack with Two Chosen-Plaintexts*

We change the known-in-advance-IV DNC attack on CBC| CFB^{-1}|CBC^{-1} to the known-in-advance-IV MIM attack. The latter has less time complexity than the former, but requires more memory. This attack starts with the same chosen-plaintexts as Section 4.1, and K_3 is found in the same way as in Section 4.1, again. After the last layer is peeled off, we use the following equations instead of (30):

$$\gamma = E_{K_1}(0) \oplus E_{K_2}(\mathrm{IV}_2), \tag{31}$$

$$\delta = E_{K_1}(E_{K_1}(0) \oplus A) \oplus E_{K_2}(E_{K_1}(0)). \tag{32}$$

The above equations are obtained from encryption of the plaintext P. Equation (31) is changed as follows:

$$E_{K_1}(0) \oplus \gamma = E_{K_2}(\mathrm{IV}_2). \tag{33}$$

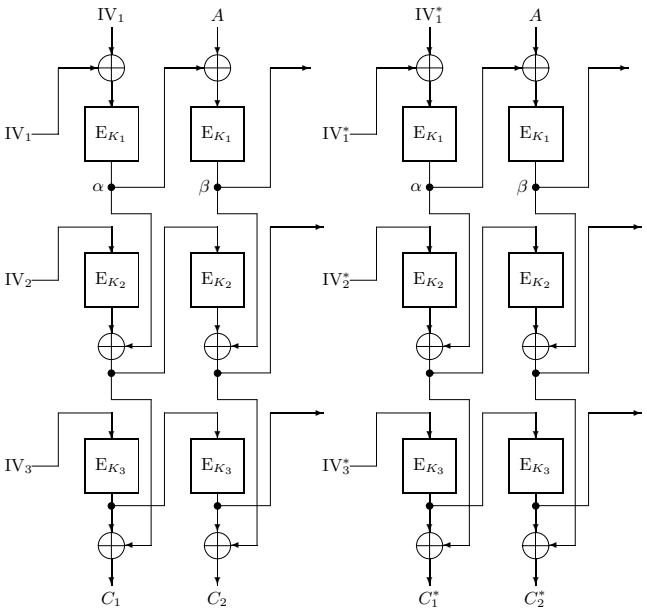

Fig. 6. Known-in-advance-IV MIM attack on the CBC|CFB|CFB mode.

Through the meet-in-the-middle method based on (33), we can find some pairs of candidates of K_1 and K_2. Equation (32) is used to determine the unique pair of K_1 and K_2 among the pairs satisfying (33). This attack requires $4 \cdot 2^{56}$ encryptions.

Likewise, known-in-advance-IV DNC attacks can be changed to known-in-advance-IV MIM attacks for many multiple modes. Moreover, known-in-advance-IV MIM attacks can be used for breaking triple modes which cannot be attacked by known-in-advance-IV DNC attacks. We describe the attack on CBC|CFB|CFB as another example of the known-in-advance-IV MIM attack with two chosen-plaintexts. It is resistant to the known-in-advance-IV DNC attack. Again, we choose two plaintexts $P = (\mathrm{IV}_1, A)$ and $P^* = (\mathrm{IV}_1^*, A)$, and obtain the ciphertexts $C = (C_1, C_2)$ and $C^* = (C_1^*, C_2^*)$ corresponding to P and P^*, respectively. Let $E_{K_1}(0) = \alpha$ and $E_{K_1}(E_{K_1}(0) \oplus A) = \beta$ as depicted in Fig. 6. Then we obtain the following equations:

$$\alpha = E_{K_2}(\mathrm{IV}_2) \oplus E_{K_3}(\mathrm{IV}_3) \oplus C_1, \tag{34}$$

$$\alpha = E_{K_2}(\mathrm{IV}_2^*) \oplus E_{K_3}(\mathrm{IV}_3^*) \oplus C_1^*, \tag{35}$$

$$\beta = E_{K_2}(E_{K_3}(\mathrm{IV}_3) \oplus C_1) \oplus E_{K_3}(C_1) \oplus C_2, \tag{36}$$

$$\beta = E_{K_2}(E_{K_3}(\mathrm{IV}_3^*) \oplus C_1^*) \oplus E_{K_3}(C_1^*) \oplus C_2^*. \tag{37}$$

We combine (34) and (35) by cancelling α, and (36) and (37) by cancelling β to the following equations:

$$E_{K_2}(\mathrm{IV}_2) \oplus E_{K_2}(\mathrm{IV}_2^*) = E_{K_3}(\mathrm{IV}_3) \oplus E_{K_3}(\mathrm{IV}_3^*) \oplus C_1 \oplus C_1^*, \tag{38}$$

$$E_{K_2}(E_{K_3}(\mathrm{IV}_3) \oplus C_1) \oplus E_{K_2}(E_{K_3}(\mathrm{IV}_3^*) \oplus C_1^*) = E_{K_3}(C_1) \oplus E_{K_3}(C_1^*) \oplus C_2 \oplus C_2^*. \quad (39)$$

Some pairs of candidates of K_2 and K_3 are found by the meet-in-the-middle method for (38). Then a unique pair of keys is determined by checking whether (39) is satisfied. Finally, we get K_1 through a simple exhaustive search. This attack requires two 2-block chosen plaintexts, $5 \cdot 2^{56}$ encryptions, and a memory of 2^{56} cells, while Biham's attack requires 2^{65} blocks of chosen-plaintext, 2^{60} encryptions, and no memory.

5. Replayed-and-Known-IV Attacks

Handschuh and Preneel suggested a replayed-IV attack in [4]. They assumed that the initial values can be replayed though they are unknown. For example, when the initial values are encrypted and transmitted, the attacker can replay the initial values by using the encrypted data. However, keeping the initial values secret usually needs additional tasks. So, we assume that the attacker can access and replay either all or some of the initial values. We also assume that the attacker replays the initial values only once, because we think that in practice, the attacker does not have so many chances to replay them.

All the attacks considered in this section use two plaintexts or ciphertexts. We think that the attacks on CFB|OFB|CFB^{-1} will be good examples to explain the replayed-and-known-IV DNC and MIM attacks. They are treated in the next two subsections.

5.1. *Replayed-and-Known-IV DNC Attacks*

For attacks on multiple modes, the advantage of replaying the initial values is to allow the attacker to control the intermediate values of the multiple modes in a well-controlled environment. So, in a replayed-IV environment, more aggressive attacks can be performed. The replayed-and-known-IV attacks can be applied to multiple modes which are resistant against known-IV and known-in-advance-IV attacks. Although we did not find any known-IV or known-in-advance-IV attack on the CFB|OFB|CFB^{-1} mode, we did find a replayed-and-known-IV attack. Figure 7 depicts the attack.

We replay IV_1 and IV_2 but not IV_3, and choose two plaintexts $P = (A, B)$ and $P^* = (D, F)$, where A and D are distinct. Let the ciphertexts corresponding to P and P^* be $C = (C_1, C_2)$ and $C^* = (C_1^*, C_2^*)$. In the first block of encryption processing, we find the following equations:

$$C_1 = A \oplus E_{K_1}(\mathrm{IV}_1) \oplus E_{K_2}(\mathrm{IV}_2) \oplus E_{K_3}(\mathrm{IV}_3), \quad (40)$$

$$C_1^* = D \oplus E_{K_1}(\mathrm{IV}_1) \oplus E_{K_2}(\mathrm{IV}_2) \oplus E_{K_3}(\mathrm{IV}_3^*). \quad (41)$$

Equations (40) and (41) are combined as follows, while $E_{K_1}(\mathrm{IV}_1)$ and $E_{K_2}(\mathrm{IV}_2)$ are cancelled:

$$E_{K_3}(\mathrm{IV}_3) \oplus E_{K_3}(\mathrm{IV}_3) = A \oplus D \oplus C_1 \oplus C_1^*. \quad (42)$$

Through exhaustive search for K_3 based on (42), we can peel off the last CFB^{-1} layer. Let the outputs of the second layer for P and P^* be (α, β) and (γ, δ), respectively. Then

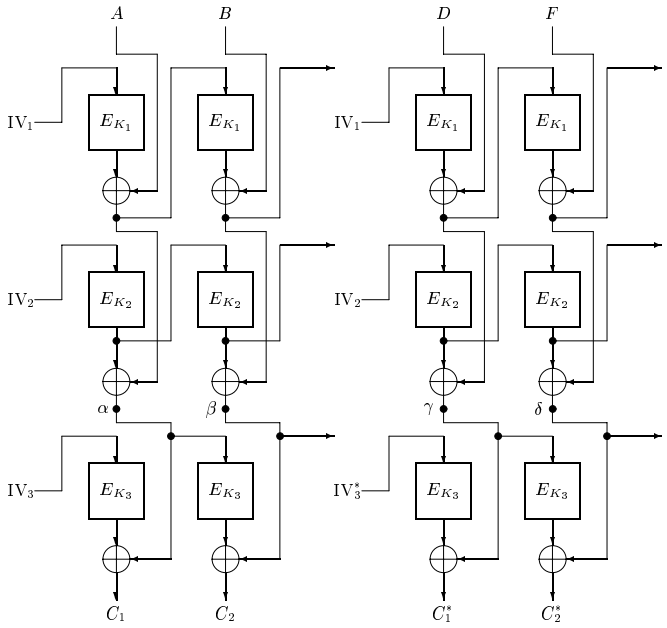

Fig. 7. Replayed-and-known-IV DNC attack on the CFB|OFB|CFB^{-1} mode.

β and δ are computed as follows:

$$\beta = E_{K_1}(E_{K_1}(\mathrm{IV}_1) \oplus A) \oplus B \oplus E_{K_2}(E_{K_2}(\mathrm{IV}_2)), \tag{43}$$

$$\delta = E_{K_1}(E_{K_1}(\mathrm{IV}_1) \oplus D) \oplus F \oplus E_{K_2}(E_{K_2}(\mathrm{IV}_2)). \tag{44}$$

We combine (43) and (44) by cancelling $E_{K_2}(E_{K_2}(\mathrm{IV}_2))$:

$$\beta \oplus \delta = E_{K_1}(E_{K_1}(\mathrm{IV}_1) \oplus A) \oplus E_{K_1}(E_{K_1}(\mathrm{IV}_1) \oplus D) \oplus B \oplus F. \tag{45}$$

Therefore, we can get the correct value of K_1 by exhaustive search based on (45), and then K_2. A total of four plaintext blocks and $6 \cdot 2^{56}$ encryptions are required for this attack.

5.2. *Replayed-and-Known-IV MIM Attacks*

The replayed-and-known-IV MIM attack on CFB|OFB|CFB^{-1} requires less data and time complexities than the replayed-and-known-IV DNC attack. Biham also adopted a kind of replayed-IV MIM attack with two plaintexts, where each plaintext has two blocks. We introduce a slightly better replayed-IV MIM attack.

We replay IV_1 and IV_2 again, but not IV_3. Then two plaintexts $P = (A, B)$ and $P^* = D$ are chosen, and the ciphertexts $C = (C_1, C_2)$ and $C^* = C_1^*$, corresponding to P and P^*, respectively, are obtained. We use the same method as in the previous section to find K_3. Let the output of the second layer for P be (α, β). From the process

encrypting (A, B) to (α, β), the following equations are obtained:

$$A \oplus E_{K_1}(\mathrm{IV}_1) = \alpha \oplus E_{K_2}(\mathrm{IV}_2), \tag{46}$$

$$B \oplus E_{K_1}(E_{K_1}(\mathrm{IV}_1) \oplus A) = \beta \oplus E_{K_2}(E_{K_2}(\mathrm{IV}_2)). \tag{47}$$

By using (46) we apply the MIM method to the first two layers, CFB|OFB, and get some pairs of (K_1, K_2) for which (46) holds. Finally, the correct values of K_1 and K_2 are obtained by checking which pair satisfies (47). This attack requires three blocks of plaintexts, $4 \cdot 2^{56}$ encryptions, and a memory with 2^{56} cells.

5.3. *Replayed-and-Known-IV MIM Attack on Biham's Multiple Modes*

Biham proposed 11 multiple modes in the earlier version of [2] by using two new operators to combine modes. One is denoted by "$\rightarrow$", which takes two modes M1 and M2, where M2 is any mode, and M1 is any stream mode (such as the OFB mode) generating a stream independent of the plaintext, and XORs the stream to the plaintext to form the ciphertext. Then M1$\rightarrow$M2 is the mode which computes the stream generated by M1, and encrypts the result under M2, resulting in a new stream, to be XORed to the plaintext. The other operator, which is denoted by "M1[M2]", where M1 is any stream mode, applies the stream mode M1 to the plaintext (e.g., XORs the plaintext and the stream of M1), applies the mode M2 to the result, and applies the same M1 on the result (e.g., XORs with the same stream of M1, without computing it again). It is easy to construct an extended operator—M1$\rightarrow$M2$\rightarrow \cdots \rightarrow$Mn and M1[M2, M3, ..., M$n$], respectively. The modes proposed by Biham are as follows. We call them "Biham mode i" for $1 \leq i \leq 11$:

1. OFB$\rightarrow$CBC$\rightarrow$CBC.
2. OFB$\rightarrow$CFB$\rightarrow$CFB.
3. OFB[CBC,CBC^{-1}].
4. OFB[CFB,CFB^{-1}].
5. OFB[CBC,CBC].
6. OFB[CFB,CFB].
7. CBC|CBC|CBC^{-1}|CBC^{-1}.
8. CFB|CFB|CFB^{-1}|CFB^{-1}.
9. OFB[CBC,CBC,CBC^{-1}].
10. OFB[CBC,CBC,CBC].
11. OFB[CFB,CFB,CFB].

He conjectured that the complexities of attacks on these triple and quadruple modes are at least 2^{112} and 2^{128}, respectively. Wagner showed that the security of ten modes of operation among them is not much more secure than single encryption if the attacker can choose the initial values with different plaintexts or ciphertexts. Independently of Wagner's results, some modes were removed from the later version of [2].

We found that our replayed-and-known-IV MIM attacks break Biham modes 1, 2, 3, 4, and 8 with less complexity than his conjecture. In view of the point that Biham also considered a kind of replayed-and-known-IV attack, in which all initial values are replayed only once and two known-plaintexts are used, for relatively strong triple

modes, our results are close to disproving the conjecture for them. Biham modes 1, 2, and 8 remained in the later version of [2]. The time complexity of our attacks on Biham modes 1, 2, 3, and 4 is better than Wagner's attacks, though our attacks need one more block and a large memory. We list the results and compare them with Biham's conjecture and Wagner's results in Section B of the Appendix.

6. Conclusions

We have considered three types of attacks on multiple modes of operation of block ciphers: known-IV attack, known-in-advance-IV attack, and replayed-and-known-IV attack. They were derived according to the environment of the initial values. Usually, it has been believed that the initial values are easily accessible by anyone, but our attacks show that a weak environment of the initial values may make some multiple modes insecure. Our attacks on cascaded three-key triple modes of operation require four blocks of data and $5 \cdot 2^{56}$ encryptions on average. Replayed-and-known-IV attacks can also be used for breaking the multiple modes proposed by Biham. We believe that our attacks can be enhanced in the environments where using more than two chosen-plaintexts (or -ciphertexts) or replaying the initial values more times are allowed.

Acknowledgements

We thank Eli Biham and the anonymous referees for useful comments and suggestions that greatly improved this paper.

Appendix

In this appendix we list our best results and compare them with Biham's results. The triple modes are listed lexicographically according to the order: ECB, CBC, CBC^{-1}, OFB, CFB, CFB^{-1}. We denote the attack type by xxx-yyy-i, where xxx $\in$ {DNC, MIM}, yyy $\in$ {KPA, CPA, CCA}, and $i \in \{1, 2, 3\}$.

We use the notation of P_1–P_2 to mean that the attacker chooses two plaintexts P_1 and P_2. KPA means the known-plaintext attack. We use KPA for the case that the attacker chooses two plaintexts AB–D or AB–DF. Since the probability that $A = D$ or $B = F$ is very low, we can almost always regard the case as the known-plaintext attack. CPA and CCA mean the chosen-plaintext and the chosen-ciphertext attacks, respectively.

The number i means the environment of the initial value. The known-IV environment is denoted by 1, the known-in-advance-IV environment is denoted by 2, and the replayed-and-known-IV environment is denoted by 3.

The column *Biham's* shows the complexities required for Biham's attacks. As in previous works [2], [8], [5], we treat three types of complexity. The first is the number of blocks of data which is chosen-plaintext or chosen-ciphertext. The second is the number of steps in the attack procedure. This is dominated of the number of encryptions required for the attack. The last is the size of the memory.

A. Table of Attacks on Triple Modes

Mode	Attack type	Data	Replay	Ours	Biham's
ECB|ECB|CBC	MIM-CPA-1	AAB		$3/4 \cdot 2^{56}/2^{56}$	$2^{33}/2^{58}/2^{56}$
ECB|ECB|CBC^{-1}	MIM-CPA-1	AAB		$3/3 \cdot 2^{56}/2^{56}$	$2^{64}/2^{58}/2^{56}$
ECB|ECB|OFB	MIM-CPA-1	AAB		$3/4 \cdot 2^{56}/2^{56}$	$2^{64}/2^{58}/2^{56}$
ECB|ECB|CFB	MIM-CPA-1	AAB		$3/4 \cdot 2^{56}/2^{56}$	$2^{33}/2^{58}/2^{56}$
ECB|ECB|CFB^{-1}	MIM-CPA-1	AAB		$3/4 \cdot 2^{56}/2^{56}$	$2^{64}/2^{58}/2^{56}$
ECB|CBC|CBC	DNC-CCA-1	AAA		$3/5 \cdot 2^{56}/-$	$2^{33}/2^{59}/2^{33}$
ECB|CBC|CBC^{-1}	MIM-CCA-2	$\mathrm{IV}_3 A - \mathrm{IV}_3^*$		$3/4 \cdot 2^{56}/2^{56}$	$2^{68}/2^{66}/-$
	MIM-CCA-3	AB–A	IV_3	$3/4 \cdot 2^{56}/2^{56}$	
ECB|CBC|OFB	DNC-CPA-3	ABF–ADF	IV_2	$6/5 \cdot 2^{56}/-$	$2^{65}/2^{65}/2^{65}$
ECB|CBC|CFB	DNC-CPA-3	ABF–ADF	IV_2	$6/5 \cdot 2^{56}/-$	$2^{34}/2^{59}/2^{33}$
ECB|CBC|CFB^{-1}	DNC-CPA-3	ABF–ADF	IV_2	$6/5 \cdot 2^{56}/-$	$2^{68}/2^{66}/-$
ECB|CBC^{-1}|CBC	DNC-CPA-1	AAA		$3/4 \cdot 2^{56}/-$	$5/2^{59}/-$
ECB|CBC^{-1}|CBC^{-1}	DNC-CPA-1	AAA		$3/4 \cdot 2^{56}/-$	$2^{34}/2^{59}/2^{33}$
ECB|CBC^{-1}|OFB	DNC-CPA-1	ABA–A		$4/4 \cdot 2^{56}/-$	$2^{64}/2^{58}/-$
ECB|CBC^{-1}|CFB	DNC-CPA-1	AAA		$3/4 \cdot 2^{56}/-$	$5/2^{59}/-$
ECB|CBC^{-1}|CFB^{-1}	DNC-CPA-1	ABA–A		$4/4 \cdot 2^{56}/-$	$2^{36}/2^{59}/2^{56}$
ECB|OFB|ECB	MIM-CPA-1	AAA		$3/5 \cdot 2^{56}/2^{56}$	$2^{64}/2^{58}/2^{56}$
ECB|OFB|CBC	DNC-CPA-3	AB–AD	IV_2	$4/5 \cdot 2^{56}/-$	$2^{64}/2^{58}/2^{56}$
ECB|OFB|CBC^{-1}	DNC-CPA-2	AB–DB	IV_3	$4/5 \cdot 2^{56}/-$	$2^{65}/2^{65}/-$
ECB|OFB|OFB	DNC-CPA-3	AB–AD	IV_2 or IV_3	$4/5 \cdot 2^{56}/-$	$2^{65}/2^{65}/2^{65}$
ECB|OFB|CFB	DNC-CPA-3	AB–AD	IV_2 or IV_3	$4/5 \cdot 2^{56}/-$	$2^{64}/2^{58}/2^{56}$
ECB|OFB|CFB^{-1}	DNC-CPA-3	AB–AD	IV_2 or IV_3	$4/5 \cdot 2^{56}/-$	$2^{65}/2^{65}/-$
ECB|CFB|CBC	MIM-CPA-3	AB–A	IV_2	$3/4 \cdot 2^{56}/2^{56}$	$2^{34}/2^{59}/2^{33}$
ECB|CFB|CBC^{-1}	MIM-CPA-1	AA–A		$3/5 \cdot 2^{56}/2^{56}$	$2^{68}/2^{66}/-$
ECB|CFB|OFB	DNC-CPA-3	AB–AD	IV_2	$4/5 \cdot 2^{56}/-$	$2^{65}/2^{65}/2^{65}$
ECB|CFB|CFB	MIM-CPA-3	AB–A	IV_2 or IV_3	$3/4 \cdot 2^{56}/2^{56}$	$2^{34}/2^{59}/2^{33}$
ECB|CFB|CFB^{-1}	DNC-CPA-3	AB–AD	IV_2	$4/5 \cdot 2^{56}/-$	$2^{66}/2^{66}/2^{66}$
ECB|CFB^{-1}|CBC	DNC-CPA-1	AAA		$3/5 \cdot 2^{56}/-$	$4/5 \cdot 2^{56}/-$
ECB|CFB^{-1}|CBC^{-1}	DNC-CPA-1	AAA		$3/5 \cdot 2^{56}/-$	$2^{36}/2^{59}/2^{33}$
ECB|CFB^{-1}|OFB	DNC-CPA-1	AAA		$3/6 \cdot 2^{56}/-$	$2^{64}/2^{58}/-$
ECB|CFB^{-1}|CFB	DNC-CPA-1	AAA		$3/5 \cdot 2^{56}/-$	$4/5 \cdot 2^{56}/-$
ECB|CFB^{-1}|CFB^{-1}	DNC-CPA-1	AAA		$3/6 \cdot 2^{56}/-$	$2^{34}/2^{59}/2^{33}$
CBC|ECB|ECB	MIM-CCA-1	AAB		$3/3 \cdot 2^{56}/2^{56}$	$2^{64}/2^{58}/2^{56}$
CBC|ECB|CBC	DNC-CCA-1	AAA		$3/5 \cdot 2^{56}/-$	$2^{34}/2^{59}/2^{33}$
CBC|ECB|OFB	MIM-CPA-2	$\mathrm{IV}_1 A$–IV_1^*		$3/4 \cdot 2^{56}/2^{56}$	$2^{65}/2^{65}/2^{65}$
	MIM-CPA-3	AB–A	IV_1	$3/4 \cdot 2^{56}/2^{56}$	
CBC|ECB|CFB	DNC-CCA-1	$AAAB$		$4/5 \cdot 2^{56}/-$	$2^{34}/2^{59}/2^{33}$
CBC|ECB|CFB^{-1}	MIM-CPA-2	$\mathrm{IV}_1 A$–IV_1^*		$3/4 \cdot 2^{56}/2^{56}$	$2^{68}/2^{66}/-$
	MIM-CPA-3	AB–A	IV_3	$3/4 \cdot 2^{56}/2^{56}$	
CBC|CBC|ECB	DNC-CCA-1	AAA		$3/4 \cdot 2^{56}/-$	$2^{34}/2^{59}/2^{33}$
CBC|CBC|CBC	MIM-CPA-2	$\mathrm{IV}_1 A$–$\mathrm{IV}_1^* A$		$4/5 \cdot 2^{56}/2^{56}$	$2^{34}/2^{60}/2^{33}$
CBC|CBC|CBC^{-1}	MIM-CCA-2	$\mathrm{IV}_1 A$–IV_1^*		$3/4 \cdot 2^{56}/2^{56}$	$2^{68}/2^{66}/-$
	MIM-CCA-3	AB–A	IV_3	$3/4 \cdot 2^{56}/2^{56}$	
CBC|CBC|OFB	MIM-CPA-3	AB–A	IV_1,IV_2	$3/4 \cdot 2^{56}/2^{56}$	$2^{64}/2^{59}/-$
CBC|CBC|CFB	MIM-CPA-2	$\mathrm{IV}_1 A$–$\mathrm{IV}_1^* A$		$4/5 \cdot 2^{56}/2^{56}$	$2^{34}/2^{60}/2^{33}$
CBC|CBC|CFB^{-1}	MIM-CPA-3	AB–A	IV_1,IV_2	$3/4 \cdot 2^{56}/2^{56}$	$2^{68}/2^{66}/-$
CBC|CBC^{-1}|ECB	MIM-CPA-2	$\mathrm{IV}_1 A$–IV_1^*		$3/4 \cdot 2^{56}/2^{56}$	$2^{68}/2^{66}/-$
	MIM-CPA-3	AB–A	IV_1	$3/4 \cdot 2^{56}/2^{56}$	

continued

Mode	Attack type	Data	Replay	Ours	Biham's
CBC|CBC^{-1}|CBC	MIM-CPA-2	IV_1A–IV_1^*		$3/4 \cdot 2^{56}/2^{56}$	$2^{66}/2^{58}/2^{33}$
CBC|CBC^{-1}|CBC^{-1}	MIM-CPA-2	IV_1A–IV_1^*		$3/4 \cdot 2^{56}/2^{56}$	$2^{68}/2^{66}/-$
	MIM-CPA-3	AB–A	IV_1	$3/4 \cdot 2^{56}/2^{56}$	
CBC|CBC^{-1}|OFB	MIM-CPA-2	IV_1A–IV_1^*		$3/4 \cdot 2^{56}/2^{56}$	$2^{66}/2^{66}/2^{66}$
	MIM-CPA-3	AB–A	IV_1	$3/4 \cdot 2^{56}/2^{56}$	
CBC|CBC^{-1}|CFB	MIM-CPA-2	IV_1A–IV_1^*		$3/4 \cdot 2^{56}/2^{56}$	$2^{66}/2^{58}/2^{33}$
	MIM-CPA-3	AB–A	IV_1	$3/4 \cdot 2^{56}/2^{56}$	
CBC|CBC^{-1}|CFB^{-1}	MIM-CPA-2	IV_1A–IV_1^*		$3/4 \cdot 2^{56}/2^{56}$	$2^{68}/2^{58}/-$
	MIM-CPA-3	AB–A	IV_1	$3/4 \cdot 2^{56}/2^{56}$	
CBC|OFB|ECB	DNC-CCA-3	AB–DB	IV_2	$4/5 \cdot 2^{56}/-$	$2^{65}/2^{65}/-$
CBC|OFB|CBC	MIM-CPA-2	IV_1A–IV_1^*A		$4/5 \cdot 2^{56}/2^{56}$	$2^{66}/2^{66}/-$
CBC|OFB|OFB	DNC-CPA-3	AB–AD	IV_1,IV_2	$4/6 \cdot 2^{56}/-$	$2^{67}/2^{75}/2^{66}$
	DNC-CPA-3	AB–AD	IV_1,IV_3	$4/6 \cdot 2^{56}/-$	
CBC|OFB|CFB	MIM-CPA-2	IV_1A–IV_1^*A		$4/5 \cdot 2^{56}/2^{56}$	$2^{66}/2^{66}/-$
CBC|OFB|CFB^{-1}	DNC-KPA-3	AB–DF	IV_1,IV_2,IV_3	$4/6 \cdot 2^{56}/-$	$4/5 \cdot 2^{56}/2^{56}$
	DNC-CPA-3	AB–AD	IV_1,IV_2	$4/6 \cdot 2^{56}/-$	
	DNC-CPA-3	AB–AD	IV_1,IV_3	$4/6 \cdot 2^{56}/-$	
CBC|CFB|ECB	DNC-CCA-1	AAA		$3/5 \cdot 2^{56}/-$	$2^{36}/2^{59}/2^{33}$
CBC|CFB|CBC	MIM-CPA-2	IV_1A–IV_1^*A		$4/5 \cdot 2^{56}/2^{56}$	$2^{34}/2^{60}/2^{33}$
CBC|CFB|CBC^{-1}	MIM-CPA-2	IV_1A–IV_1^*A		$4/4 \cdot 2^{56}/2^{56}$	$2^{34}/2^{60}/2^{33}$
CBC|CFB|OFB	DNC-CPA-3	AB–AD	IV_1,IV_2	$4/6 \cdot 2^{56}/-$	$2^{65}/2^{60}/-$
	DNC-CPA-3	AB–AD	IV_1,IV_3	$4/6 \cdot 2^{56}/-$	
CBC|CFB|CFB	MIM-CPA-2	IV_1A–IV_1^*A		$4/5 \cdot 2^{56}/2^{56}$	$2^{34}/2^{60}/2^{33}$
CBC|CFB|CFB^{-1}	DNC-CPA-3	AB–AD	IV_1,IV_2	$4/6 \cdot 2^{56}/-$	$2^{68}/2^{58}/-$
CBC|CFB^{-1}|ECB	MIM-CPA-2	IV_1A–IV_1^*A		$4/5 \cdot 2^{56}/2^{56}$	$2^{68}/2^{68}/-$
CBC|CFB^{-1}|CBC	DNC-CPA-2	IV_1A–IV_1^*A		$4/5 \cdot 2^{56}/-$	$2^{68}/2^{58}/2^{33}$
	DNC-CPA-3	AB–AB	IV_1	$4/5 \cdot 2^{56}/-$	
CBC|CFB^{-1}|CBC^{-1}	DNC-CPA-2	IV_1A–IV_1^*A		$4/5 \cdot 2^{56}/-$	$2^{68}/2^{58}/-$
	DNC-CPA-3	AB–AB	IV_1	$4/5 \cdot 2^{56}/-$	
CBC|CFB^{-1}|OFB	DNC-CPA-2	IV_1A–IV_1^*A		$4/7 \cdot 2^{56}/-$	$2^{68}/2^{66}/2^{66}$
	DNC-CPA-3	AB–AB	IV_1	$4/7 \cdot 2^{56}/-$	
CBC|CFB^{-1}|CFB	DNC-CPA-2	IV_1A–IV_1^*A		$4/5 \cdot 2^{56}/-$	$2^{68}/2^{58}/2^{33}$
	DNC-CPA-3	AB–AB	IV_1	$4/5 \cdot 2^{56}/-$	
CBC|CFB^{-1}|CFB^{-1}	DNC-CPA-2	IV_1A–IV_1^*A		$4/7 \cdot 2^{56}/-$	$2^{68}/2^{66}/-$
	DNC-CPA-3	AB–AB	IV_1	$4/7 \cdot 2^{56}/-$	
CBC^{-1}|ECB|ECB	MIM-CCA-1	AAA		$3/4 \cdot 2^{56}/2^{56}$	$2^{33}/2^{58}/2^{56}$
CBC^{-1}|ECB|CBC	DNC-CPA-1	AAA		$3/5 \cdot 2^{56}/-$	$4/5 \cdot 2^{56}/-$
CBC^{-1}|ECB|CBC^{-1}	DNC-CPA-1	AAA		$3/5 \cdot 2^{56}/-$	$2^{34}/2^{59}/2^{33}$
CBC^{-1}|ECB|OFB	DNC-CPA-1	AAA		$3/6 \cdot 2^{56}/-$	$2^{64}/2^{58}/-$
CBC^{-1}|ECB|CFB	DNC-CPA-1	AAA		$3/5 \cdot 2^{56}/-$	$4/5 \cdot 2^{56}/-$
CBC^{-1}|ECB|CFB^{-1}	DNC-CPA-1	AAA		$3/6 \cdot 2^{56}/-$	$2^{34}/2^{59}/2^{33}$
CBC^{-1}|CBC|ECB	DNC-CPA-1	AAA		$3/4 \cdot 2^{56}/-$	$5/2^{59}/-$
CBC^{-1}|CBC|CBC	MIM-CPA-1	AAA		$3/4 \cdot 2^{56}/2^{56}$	$2^{34}/2^{59}/2^{33}$
CBC^{-1}|CBC|CBC^{-1}	MIM-CCA-2	IV_1A–IV_3^*		$3/4 \cdot 2^{56}/2^{56}$	$2^{66}/2^{58}/2^{33}$
	MIM-CCA-3	AB–A	IV_3	$3/4 \cdot 2^{56}/2^{56}$	
CBC^{-1}|CBC|OFB	MIM-CPA-3	AB–A	IV_1,IV_2	$3/4 \cdot 2^{56}/2^{56}$	$2^{65}/2^{65}/2^{65}$
CBC^{-1}|CBC|CFB	MIM-CPA-1	$AAAA$		$4/4 \cdot 2^{56}/2^{56}$	$5/5 \cdot 2^{56}/-$
CBC^{-1}|CBC|CFB^{-1}	MIM-CPA-3	AB–A	IV_1,IV_2	$3/4 \cdot 2^{56}/2^{56}$	$2^{68}/2^{58}/2^{33}$
CBC^{-1}|CBC^{-1}|ECB	DNC-CPA-1	AAA		$3/5 \cdot 2^{56}/-$	$2^{33}/2^{59}/2^{33}$
CBC^{-1}|CBC^{-1}|CBC	DNC-CPA-1	AAA		$3/5 \cdot 2^{56}/-$	$2^{34}/2^{59}/2^{33}$
CBC^{-1}|CBC^{-1}|CBC^{-1}	DNC-CPA-2	$\mathrm{IV}_1\mathrm{IV}_1\mathrm{IV}_1$		$3/4 \cdot 2^{56}/-$	$2^{34}/2^{60}/2^{33}$
CBC^{-1}|CBC^{-1}|OFB	DNC-CPA-1	AAA		$3/6 \cdot 2^{56}/-$	$2^{66}/2^{59}/-$

continued

Mode	Attack type	Data	Replay	Ours	Biham's
CBC^{-1}|CBC^{-1}|CFB	DNC-CPA-1	AAA		$3/4 \cdot 2^{56}/2^{56}$	$2^{34}/2^{59}/2^{33}$
CBC^{-1}|CBC^{-1}|CFB^{-1}	DNC-CPA-2	$IV_1IV_1IV_1$		$3/5 \cdot 2^{56}/-$	$2^{34}/2^{60}/2^{33}$
CBC^{-1}|OFB|ECB	DNC-CPA-3	AB–AD	IV_2	$4/5 \cdot 2^{56}/-$	$2^{64}/2^{58}/2^{58}$
CBC^{-1}|OFB|CBC	DNC-CPA-3	AB–AD	IV_2	$4/5 \cdot 2^{56}/-$	$2^{66}/2^{58}/-$
CBC^{-1}|OFB|CBC^{-1}	DNC-CPA-3	AB–AD	IV_2	$4/5 \cdot 2^{56}/-$	$2^{66}/2^{66}/-$
CBC^{-1}|OFB|OFB	DNC-CPA-3	AB–AD	IV_2 or IV_3	$4/5 \cdot 2^{56}/-$	$2^{65}/2^{65}/2^{65}$
CBC^{-1}|OFB|CFB	DNC-CPA-3	AB–AD	IV_2 or IV_3	$4/5 \cdot 2^{56}/-$	$2^{66}/2^{58}/-$
CBC^{-1}|OFB|CFB^{-1}	DNC-CPA-3	AB–AD	IV_2	$4/5 \cdot 2^{56}/-$	$2^{66}/2^{66}/-$
CBC^{-1}|CFB|ECB	DNC-CCA-1	AAA		$3/5 \cdot 2^{56}/-$	$4/5 \cdot 2^{56}/-$
CBC^{-1}|CFB|CBC	MIM-CPA-3	AB–A	IV_2	$3/4 \cdot 2^{56}/2^{56}$	$5/5 \cdot 2^{56}/-$
CBC^{-1}|CFB|CBC^{-1}	DNC-CPA-3	AB–AB	IV_2	$4/5 \cdot 2^{56}/-$	$2^{68}/2^{58}/2^{33}$
CBC^{-1}|CFB|OFB	MIM-KPA-3	AB–D	IV_2,IV_3	$3/4 \cdot 2^{56}/2^{56}$	$2^{65}/2^{65}/2^{65}$
	MIM-CPA-3	AB–A	IV_2 or IV_3	$3/4 \cdot 2^{56}/2^{56}$	
CBC^{-1}|CFB|CFB	MIM-CPA-3	AB–A	IV_2 or IV_3	$3/4 \cdot 2^{56}/2^{56}$	$2^{34}/2^{59}/2^{33}$
CBC^{-1}|CFB|CFB^{-1}	DNC-CPA-3	AB–AD	IV_1,IV_2	$4/5 \cdot 2^{56}/-$	$2^{66}/2^{58}/2^{33}$
CBC^{-1}|CFB^{-1}|ECB	MIM-CPA-3	AB–A	IV_2	$3/4 \cdot 2^{56}/2^{56}$	$2^{34}/2^{59}/2^{33}$
CBC^{-1}|CFB^{-1}|CBC	DNC-CPA-2	$IV_1IV_1IV_1$		$3/5 \cdot 2^{56}/-$	$5/5 \cdot 2^{56}/-$
CBC^{-1}|CFB^{-1}|CBC^{-1}	DNC-CPA-2	$IV_1IV_1IV_1$		$3/5 \cdot 2^{56}/-$	$2^{34}/2^{60}/2^{33}$
CBC^{-1}|CFB^{-1}|OFB	DNC-CPA-2	$IV_1IV_1IV_1$		$3/6 \cdot 2^{56}/-$	$2^{66}/2^{59}/-$
CBC^{-1}|CFB^{-1}|CFB	DNC-CPA-2	$IV_1IV_1IV_1$		$3/5 \cdot 2^{56}/-$	$5/5 \cdot 2^{56}/-$
CBC^{-1}|CFB^{-1}|CFB^{-1}	DNC-CPA-2	$IV_1IV_1IV_1$		$3/6 \cdot 2^{56}/-$	$2^{34}/2^{60}/2^{33}$
OFB|ECB|ECB	MIM-CCA-1	AAB		$3/4 \cdot 2^{56}/2^{56}$	$2^{64}/2^{58}/2^{56}$
OFB|ECB|CBC	DNC-CCA-1	AAA		$3/6 \cdot 2^{56}/-$	$2^{64}/2^{58}/-$
OFB|ECB|CBC^{-1}	MIM-CCA-2	IV_3A–IV_3^*		$3/4 \cdot 2^{56}/2^{56}$	$2^{65}/2^{65}/2^{65}$
	MIM-CCA-3	AB–A	IV_3	$3/4 \cdot 2^{56}/2^{56}$	
OFB|ECB|OFB	DNC-CPA-3	AB–AD	IV_1 or IV_3	$4/5 \cdot 2^{56}/-$	$2^{65}/2^{65}/2^{64}$
OFB|ECB|CFB	DNC-CCA-1	$AAAB$		$4/6 \cdot 2^{56}/-$	$2^{64}/2^{58}/-$
OFB|ECB|CFB^{-1}	DNC-CPA-3	AB–AD	IV_1 or IV_3	$4/5 \cdot 2^{56}/-$	$2^{65}/2^{65}/2^{65}$
OFB|CBC|ECB	DNC-CCA-1	ABA–A		$4/4 \cdot 2^{56}/-$	$2^{64}/2^{58}/-$
OFB|CBC|CBC	DNC-CCA-1	AAA		$3/6 \cdot 2^{56}/-$	$2^{66}/2^{59}/-$
OFB|CBC|CBC^{-1}	MIM-CCA-2	IV_3A–IV_3^*		$3/4 \cdot 2^{56}/2^{56}$	$2^{66}/2^{66}/2^{66}$
	MIM-CCA-3	AB–A	IV_3	$3/4 \cdot 2^{56}/2^{56}$	
OFB|CBC|OFB	DNC-CPA-3	AB–AD	IV_1,IV_2	$4/5 \cdot 2^{56}/-$	$2^{66}/2^{66}/2^{66}$
OFB|CBC|CFB	DNC-CCA-2	$IV_3IV_3IV_3$		$3/5 \cdot 2^{56}/-$	$2^{66}/2^{59}/-$
OFB|CBC|CFB^{-1}	DNC-CPA-3	AB–AD	IV_1,IV_2	$4/5 \cdot 2^{56}/-$	$2^{66}/2^{66}/2^{66}$
OFB|CBC^{-1}|ECB	MIM-CPA-3	AB–A	IV_1	$3/4 \cdot 2^{56}/2^{56}$	$2^{65}/2^{65}/2^{65}$
OFB|CBC^{-1}|CBC	MIM-CPA-3	AB–A	IV_1	$3/4 \cdot 2^{56}/2^{56}$	$2^{65}/2^{65}/2^{65}$
OFB|CBC^{-1}|CBC^{-1}	MIM-CPA-3	AB–A	IV_1	$3/4 \cdot 2^{56}/2^{56}$	$2^{64}/2^{59}/-$
	MIM-CPA-3	AB–A	IV_2,IV_3	$3/4 \cdot 2^{56}/2^{56}$	
OFB|CBC^{-1}|OFB	MIM-CPA-3	AB–A	IV_1	$3/4 \cdot 2^{56}/2^{56}$	$2^{66}/2^{66}/2^{66}$
OFB|CBC^{-1}|CFB	MIM-CPA-3	AB–A	IV_1	$3/4 \cdot 2^{56}/2^{56}$	$2^{65}/2^{65}/2^{65}$
OFB|CBC^{-1}|CFB^{-1}	MIM-CPA-3	AB–A	IV_1	$3/4 \cdot 2^{56}/2^{56}$	$2^{65}/2^{60}/-$
OFB|OFB|ECB	DNC-CCA-3	AB–AD	IV_2 or IV_3	$4/5 \cdot 2^{56}/-$	$2^{65}/2^{65}/2^{65}$
OFB|OFB|CBC	DNC-CCA-3	AB–AD	IV_2 or IV_3	$4/5 \cdot 2^{56}/-$	$2^{65}/2^{65}/2^{65}$
OFB|OFB|CBC^{-1}	MIM-KPA-3	AB–D	IV_2,IV_3	$3/4 \cdot 2^{56}/2^{56}$	$2^{67}/2^{75}/2^{66}$
OFB|OFB|OFB	MIM-KPA-3	AB–D	IV_1,IV_2	$3/4 \cdot 2^{56}/2^{56}$	$2^{67}/2^{75}/2^{66}$
	MIM-KPA-3	AB–D	IV_1,IV_3	$3/4 \cdot 2^{56}/2^{56}$	
	MIM-KPA-3	AB–D	IV_2,IV_3	$3/4 \cdot 2^{56}/2^{56}$	
OFB|OFB|CFB	DNC-CCA-3	AB–AD	IV_2	$4/7 \cdot 2^{56}/-$	$2^{65}/2^{65}/2^{65}$
OFB|OFB|CFB^{-1}	DNC-KPA-3	AB–DF	IV_1,IV_3	$4/6 \cdot 2^{56}/-$	$2^{67}/2^{75}/2^{66}$
	DNC-KPA-3	AB–DF	IV_2,IV_3	$4/6 \cdot 2^{56}/-$	
OFB|CFB|ECB	DNC-CCA-1	AAA		$3/6 \cdot 2^{56}/-$	$2^{64}/2^{58}/-$

continued

Mode	Attack type	Data	Replay	Ours	Biham's
OFB|CFB|CBC	DNC-CCA-2	$IV_3IV_3IV_3$		$3/6 \cdot 2^{56}/-$	$2^{66}/2^{59}/-$
OFB|CFB|CBC^{-1}	MIM-KPA-3	AB–D	IV_1,IV_2	$3/4 \cdot 2^{56}/2^{56}$	$2^{66}/2^{66}/2^{66}$
OFB|CFB|OFB	DNC-KPA-3	AB–DF	IV_1,IV_2	$4/5 \cdot 2^{56}/-$	$2^{66}/2^{66}/2^{66}$
OFB|CFB|CFB	DNC-CCA-2	IV_3IV_3A		$3/6 \cdot 2^{56}/-$	$2^{66}/2^{59}/-$
OFB|CFB|CFB^{-1}	DNC-KPA-3	AB–DF	IV_1,IV_2	$4/5 \cdot 2^{56}/-$	$2^{66}/2^{66}/2^{66}$
OFB|CFB^{-1}|ECB	DNC-KPA-3	AB–DF	IV_1,IV_2	$4/6 \cdot 2^{56}/-$	$2^{65}/2^{65}/2^{65}$
OFB|CFB^{-1}|CBC	DNC-CPA-3	AB–AB	IV_1	$4/5 \cdot 2^{56}/-$	$2^{65}/2^{65}/2^{65}$
OFB|CFB^{-1}|CBC^{-1}	DNC-CPA-3	AB–AD	IV_1	$4/5 \cdot 2^{56}/-$	$2^{65}/2^{60}/-$
OFB|CFB^{-1}|OFB	DNC-KPA-3	AB–DF	IV_2,IV_3	$4/5 \cdot 2^{56}/-$	$2^{66}/2^{66}/2^{66}$
OFB|CFB^{-1}|CFB	DNC-CPA-3	AB–AB	IV_1	$4/5 \cdot 2^{56}/-$	$2^{65}/2^{65}/2^{65}$
OFB|CFB^{-1}|CFB^{-1}	DNC-CPA-3	AB–AB	IV_1	$4/7 \cdot 2^{56}/-$	$2^{64}/2^{59}/-$
CFB|ECB|ECB	MIM-CCA-1	AAB		$3/4 \cdot 2^{56}/2^{56}$	$2^{64}/2^{58}/2^{56}$
CFB|ECB|CBC	DNC-CCA-1	AAA		$3/6 \cdot 2^{56}/-$	$2^{34}/2^{58}/2^{33}$
CFB|ECB|CBC^{-1}	MIM-CCA-2	IV_3A–IV_3^*		$3/4 \cdot 2^{56}/2^{56}$	$2^{68}/2^{66}/-$
	MIM-CCA-3	AB–A	IV_3	$3/4 \cdot 2^{56}/2^{56}$	
CFB|ECB|OFB	DNC-CPA-3	AB–AD	IV_1	$4/5 \cdot 2^{56}/-$	$2^{65}/2^{65}/2^{65}$
CFB|ECB|CFB	DNC-CCA-2	IV_3IV_3A		$3/5 \cdot 2^{56}/-$	$2^{34}/2^{59}/2^{33}$
CFB|ECB|CFB^{-1}	DNC-CPA-3	AB–AD	IV_1	$4/5 \cdot 2^{56}/-$	$2^{68}/2^{66}/-$
CFB|CBC|ECB	DNC-CCA-1	ABA–A		$4/4 \cdot 2^{56}/-$	$2^{36}/2^{59}/2^{33}$
CFB|CBC|CBC	DNC-CCA-2	$IV_3IV_3IV_3$		$3/5 \cdot 2^{56}/-$	$2^{34}/2^{60}/2^{33}$
CFB|CBC|CBC^{-1}	MIM-CCA-2	IV_3A–IV_3^*		$3/4 \cdot 2^{56}/2^{56}$	$2^{68}/2^{58}/-$
	MIM-CCA-3	AB–A	IV_3	$3/4 \cdot 2^{56}/2^{56}$	
CFB|CBC|OFB	DNC-CPA-3	AB–AD	IV_1,IV_2	$4/5 \cdot 2^{56}/-$	$2^{65}/2^{60}/-$
CFB|CBC|CFB	DNC-CCA-2	$IV_3IV_3IV_3$		$3/5 \cdot 2^{56}/-$	$2^{34}/2^{60}/2^{33}$
CFB|CBC|CFB^{-1}	DNC-CPA-3	AB–AD	IV_1,IV_2	$4/5 \cdot 2^{56}/-$	$2^{68}/2^{58}/-$
CFB|CBC^{-1}|ECB	MIM-CPA-3	AB–A	IV_1	$3/4 \cdot 2^{56}/2^{56}$	$2^{68}/2^{66}/-$
CFB|CBC^{-1}|CBC	MIM-CPA-3	AB–A	IV_1	$3/4 \cdot 2^{56}/2^{56}$	$2^{68}/2^{58}/2^{33}$
CFB|CBC^{-1}|CBC^{-1}	MIM-CPA-3	AB–A	IV_1	$3/4 \cdot 2^{56}/2^{56}$	$2^{68}/2^{66}/-$
CFB|CBC^{-1}|OFB	MIM-CPA-3	AB–A	IV_1	$3/4 \cdot 2^{56}/2^{56}$	$2^{66}/2^{66}/2^{66}$
CFB|CBC^{-1}|CFB	MIM-CPA-3	AB–A	IV_1	$3/4 \cdot 2^{56}/2^{56}$	$2^{68}/2^{58}/2^{33}$
CFB|CBC^{-1}|CFB^{-1}	MIM-CPA-3	AB–A	IV_1	$3/4 \cdot 2^{56}/2^{56}$	$2^{68}/2^{58}/-$
CFB|OFB|ECB	DNC-CCA-3	AB–AD	IV_1 or IV_2	$4/5 \cdot 2^{56}/-$	$2^{65}/2^{65}/-$
CFB|OFB|CBC	DNC-CCA-3	AB–AD	IV_2	$4/5 \cdot 2^{56}/-$	$2^{66}/2^{66}/-$
CFB|OFB|CBC^{-1}	DNC-KPA-3	AB–DF	IV_1,IV_2,IV_3	$4/6 \cdot 2^{56}/-$	$4/5 \cdot 2^{56}/2^{56}$
CFB|OFB|OFB	DNC-KPA-3	AB–DF	IV_1,IV_2	$4/6 \cdot 2^{56}/-$	$2^{67}/2^{75}/2^{66}$
	DNC-KPA-3	AB–DF	IV_1,IV_3	$4/6 \cdot 2^{56}/-$	
CFB|OFB|CFB	DNC-CCA-3	AB–AD	IV_2	$4/7 \cdot 2^{56}/-$	$2^{66}/2^{66}/-$
CFB|OFB|CFB^{-1}	DNC-KPA-3	AB–DF	IV_1,IV_2	$4/6 \cdot 2^{56}/-$	$4/5 \cdot 2^{56}/2^{56}$
	DNC-KPA-3	AB–DF	IV_2,IV_3	$4/6 \cdot 2^{56}/-$	
CFB|CFB|ECB	DNC-CCA-1	AAA		$3/6 \cdot 2^{56}/-$	$2^{34}/2^{59}/2^{33}$
CFB|CFB|CBC	DNC-CCA-2	$IV_3IV_3IV_3$		$3/6 \cdot 2^{56}/-$	$2^{34}/2^{60}/2^{33}$
CFB|CFB|CBC^{-1}	MIM-CPA-3	AB–AB	IV_1	$4/5 \cdot 2^{56}/2^{56}$	$2^{68}/2^{66}/-$
CFB|CFB|OFB	DNC-CPA-3	AB–AD	IV_1,IV_3	$4/6 \cdot 2^{56}/-$	$2^{64}/2^{59}/-$
CFB|CFB|CFB	DNC-CCA-2	IV_3IV_3A		$3/6 \cdot 2^{56}/-$	$2^{34}/2^{60}/2^{33}$
CFB|CFB|CFB^{-1}	MIM-KPA-3	AB–D	IV_1,IV_2	$3/4 \cdot 2^{56}/2^{56}$	$2^{68}/2^{66}/-$
	MIM-KPA-3	AB–D	IV_1,IV_3	$3/4 \cdot 2^{56}/2^{56}$	
	MIM-KPA-3	AB–D	IV_2,IV_3	$3/4 \cdot 2^{56}/2^{56}$	
CFB|CFB^{-1}|ECB	DNC-CPA-3	AB–AB	IV_1	$4/5 \cdot 2^{56}/-$	$2^{66}/2^{66}/2^{66}$
CFB|CFB^{-1}|CBC	DNC-CPA-3	AB–AB	IV_1	$4/5 \cdot 2^{56}/-$	$2^{66}/2^{58}/2^{33}$
CFB|CFB^{-1}|CBC^{-1}	DNC-CPA-3	AB–AB	IV_1	$4/5 \cdot 2^{56}/-$	$2^{68}/2^{58}/-$
CFB|CFB^{-1}|OFB	DNC-KPA-3	AB–DF	IV_2,IV_3	$4/5 \cdot 2^{56}/-$	$2^{68}/2^{66}/2^{66}$

continued

Mode	Attack type	Data	Replay	Ours	Biham's
CFB|CFB^{-1}|CFB	DNC-CPA-3	AB–AB	IV_1	$4/5 \cdot 2^{56}/-$	$2^{66}/2^{58}/2^{33}$
CFB|CFB^{-1}|CFB^{-1}	DNC-CPA-3	AB–AB	IV_1	$4/7 \cdot 2^{56}/-$	$2^{66}/2^{58}/2^{33}$
CFB^{-1}|ECB|ECB	MIM-CCA-1	AAB		$3/4 \cdot 2^{56}/2^{56}$	$2^{33}/2^{58}/2^{56}$
CFB^{-1}|ECB|CBC	DNC-CCA-1	AAA		$3/5 \cdot 2^{56}/-$	$4/5 \cdot 2^{56}/-$
CFB^{-1}|ECB|CBC^{-1}	DNC-CPA-1	$AAAB$		$4/5 \cdot 2^{56}/-$	$2^{34}/2^{59}/2^{33}$
CFB^{-1}|ECB|OFB	DNC-CPA-1	$AAAB$		$4/6 \cdot 2^{56}/-$	$2^{64}/2^{58}/-$
CFB^{-1}|ECB|CFB^{-1}	DNC-CPA-2	$\mathrm{IV}_1\mathrm{IV}_1A$		$3/5 \cdot 2^{56}/-$	$2^{34}/2^{59}/2^{33}$
CFB^{-1}|CBC|ECB	DNC-CCA-1	AAA		$3/4 \cdot 2^{56}/-$	$5/5 \cdot 2^{56}/-$
CFB^{-1}|CBC|CBC	DNC-CCA-1	AAA		$3/4 \cdot 2^{56}/-$	$2^{34}/2^{59}/2^{33}$
CFB^{-1}|CBC|CBC^{-1}	MIM-CCA-2	IV_3A–IV_3^*		$3/4 \cdot 2^{56}/2^{56}$	$2^{66}/2^{58}/2^{33}$
	MIM-CCA-3	AB–A	IV_3	$3/4 \cdot 2^{56}/2^{56}$	
CFB^{-1}|CBC|OFB	DNC-CPA-3	AB–AD	IV_1,IV_2	$4/5 \cdot 2^{56}/-$	$2^{65}/2^{65}/2^{65}$
CFB^{-1}|CBC|CFB	DNC-CCA-2	$\mathrm{IV}_3\mathrm{IV}_3\mathrm{IV}_3$		$3/4 \cdot 2^{56}/-$	$5/5 \cdot 2^{56}/-$
CFB^{-1}|CBC|CFB^{-1}	DNC-CPA-3	AB–AD	IV_1,IV_2	$4/5 \cdot 2^{56}/-$	$2^{68}/2^{58}/2^{33}$
CFB^{-1}|CBC^{-1}|ECB	MIM-CPA-2	$\mathrm{IV}_1\mathrm{IV}_1AAA$		$5/4 \cdot 2^{56}/2^{56}$	$2^{34}/2^{59}/2^{33}$
CFB^{-1}|CBC^{-1}|CBC	DNC-CPA-1	$AAAA$		$4/5 \cdot 2^{56}/-$	$5/5 \cdot 2^{56}/-$
CFB^{-1}|CBC^{-1}|CBC^{-1}	DNC-CPA-2	$\mathrm{IV}_1\mathrm{IV}_1\mathrm{IV}_1$		$3/4 \cdot 2^{56}/-$	$2^{34}/2^{60}/2^{33}$
CFB^{-1}|CBC^{-1}|OFB	DNC-CPA-2	$\mathrm{IV}_1\mathrm{IV}_1\mathrm{IV}_1$		$3/5 \cdot 2^{56}/-$	$2^{66}/2^{59}/-$
CFB^{-1}|CBC^{-1}|CFB	DNC-CPA-2	$\mathrm{IV}_1\mathrm{IV}_1\mathrm{IV}_1$		$3/4 \cdot 2^{56}/-$	$5/5 \cdot 2^{56}/-$
CFB^{-1}|CBC^{-1}|CFB^{-1}	DNC-CPA-2	$\mathrm{IV}_1\mathrm{IV}_1\mathrm{IV}_1$		$3/5 \cdot 2^{56}/-$	$2^{34}/2^{60}/2^{33}$
CFB^{-1}|OFB|ECB	DNC-CCA-3	AB–AD	IV_1 or IV_2	$4/5 \cdot 2^{56}/-$	$2^{64}/2^{58}/2^{56}$
CFB^{-1}|OFB|CBC	DNC-CPA-3	AB–AD	IV_2	$4/5 \cdot 2^{56}/-$	$2^{66}/2^{58}/-$
CFB^{-1}|OFB|CBC^{-1}	DNC-CPA-3	AB–AD	IV_2	$4/7 \cdot 2^{56}/-$	$2^{66}/2^{66}/-$
CFB^{-1}|OFB|OFB	DNC-CPA-3	AB–AD	IV_2	$4/7 \cdot 2^{56}/-$	$2^{65}/2^{65}/2^{65}$
CFB^{-1}|OFB|CFB	DNC-CPA-3	AB–AD	IV_2	$4/5 \cdot 2^{56}/-$	$2^{66}/2^{58}/-$
CFB^{-1}|OFB|CFB^{-1}	DNC-CPA-3	AB–AD	IV_2	$4/7 \cdot 2^{56}/-$	$2^{66}/2^{66}/-$
CFB^{-1}|CFB|ECB	DNC-CCA-1	AAA		$3/5 \cdot 2^{56}/-$	$4/5 \cdot 2^{56}/-$
CFB^{-1}|CFB|CBC	DNC-CCA-2	$\mathrm{IV}_3\mathrm{IV}_3\mathrm{IV}_3$		$3/5 \cdot 2^{56}/-$	$5/5 \cdot 2^{56}/-$
CFB^{-1}|CFB|CBC^{-1}	MIM-KPA-3	AB–D	IV_1,IV_2	$3/4 \cdot 2^{56}/2^{56}$	$2^{68}/2^{58}/2^{33}$
CFB^{-1}|CFB|OFB	DNC-CPA-3	AB–AD	IV_1,IV_3	$4/6 \cdot 2^{56}/-$	$2^{65}/2^{65}/2^{65}$
CFB^{-1}|CFB|CFB	DNC-CCA-2	$\mathrm{IV}_3\mathrm{IV}_3A$		$3/5 \cdot 2^{56}/-$	$2^{34}/2^{59}/2^{33}$
CFB^{-1}|CFB|CFB^{-1}	MIM-KPA-3	AB–D	IV_1,IV_2	$3/4 \cdot 2^{56}/2^{56}$	$2^{66}/2^{58}/2^{33}$
	MIM-KPA-3	AB–D	IV_1,IV_3	$3/4 \cdot 2^{56}/2^{56}$	
	MIM-KPA-3	AB–D	IV_2,IV_3	$3/4 \cdot 2^{56}/2^{56}$	
CFB^{-1}|CFB^{-1}|ECB	DNC-CPA-2	$\mathrm{IV}_1\mathrm{IV}_1A$		$3/5 \cdot 2^{56}/-$	$2^{34}/2^{59}/2^{33}$
CFB^{-1}|CFB^{-1}|CBC	DNC-CPA-2	$\mathrm{IV}_1\mathrm{IV}_1A$		$3/5 \cdot 2^{56}/-$	$2^{34}/2^{59}/2^{33}$
CFB^{-1}|CFB^{-1}|CBC^{-1}	DNC-CPA-2	$\mathrm{IV}_1\mathrm{IV}_1\mathrm{IV}_1$		$3/5 \cdot 2^{56}/-$	$2^{34}/2^{59}/2^{33}$
CFB^{-1}|CFB^{-1}|OFB	DNC-CPA-2	$\mathrm{IV}_1\mathrm{IV}_1A$		$3/6 \cdot 2^{56}/-$	$2^{66}/2^{59}/-$
CFB^{-1}|CFB^{-1}|CFB	DNC-CPA-2	$\mathrm{IV}_1\mathrm{IV}_1A$		$3/5 \cdot 2^{56}/-$	$2^{34}/2^{59}/2^{33}$
CFB^{-1}|CFB^{-1}|CFB^{-1}	DNC-CPA-2	$\mathrm{IV}_1\mathrm{IV}_1A$		$3/6 \cdot 2^{56}/-$	$2^{34}/2^{60}/2^{33}$

B. Table of Attacks on Biham modes

This table lists the results of the replayed-and-known-IV MIM attacks on Biham modes 1, 2, 3, 4, and 8. The column *Biham's* shows Biham's conjecture of the security of the multiple modes against conventional unknown-IV attacks. The column *Wagner's* shows the complexities required for Wagner's chosen-IV attacks.

Mode	Attack type	Data	Replay	Ours	Biham's	Wagner's
OFB→CBC→CBC	MIM-KPA-3	AB–D	IV_1,IV_2	$3/4 \cdot 2^{56}/2^{56}$	2^{112}	$2/5 \cdot 2^{56}/-$
OFB→CFB→CFB	MIM-KPA-3	AB–D	IV_1,IV_2	$3/4 \cdot 2^{56}/2^{56}$	2^{112}	$2/5 \cdot 2^{56}/-$
	MIM-KPA-3	AB–D	IV_1,IV_3			
	MIM-KPA-3	AB–D	IV_2,IV_3			
OFB[CFB,CFB]	MIM-KPA-3	AB–D	IV_1,IV_2	$3/4 \cdot 2^{56}/2^{56}$	2^{112}	$2/5 \cdot 2^{56}/-$
	MIM-KPA-3	AB–D	IV_1,IV_3			
	MIM-KPA-3	AB–D	IV_2,IV_3			
OFB[CFB,CFB^{-1}]	MIM-KPA-3	AB–D	IV_1,IV_2	$3/4 \cdot 2^{56}/2^{56}$	2^{112}	$2/5 \cdot 2^{56}/-$
	MIM-KPA-3	AB–D	IV_1,IV_3			
	MIM-KPA-3	AB–D	IV_2,IV_3			
CFB|CFB|CFB^{-1}|CFB^{-1}	MIM-CPA-3	AB–AD	IV_1,IV_2	$4/8 \cdot 2^{56}/2^{56}$	2^{128}	$3/7 \cdot 2^{56}/-$
	MIM-CPA-3	AB–AD	IV_1,IV_2			

C. Improvement of Biham's Results

We found some better results of conventional unknown-IV attacks on the ECB| ECB|CBC, ECB|ECB|CFB, CBC^{-1}|ECB|ECB, and CFB^{-1}|ECB|ECB modes than Biham's results. The following table lists the results. Since the environment of the initial value is clear as "unknown", we drop i in the field of *Attack Type* and do not use another notation to denote the unknown-IV environment

Mode	Attack type	Data	Our complexity	Biham's complexity
ECB|ECB|CBC	MIM-CPA	$ABBD$	$4/2^{58}/2^{56}$	$2^{33}/2^{58}/2^{56}$
ECB|ECB|CFB	MIM-CPA	$ABBD$		
CBC^{-1}|ECB|ECB	MIM-CCA	$ABBD$		
CFB^{-1}|ECB|ECB	MIM-CCA	$ABBD$		

References

[1] E. Biham, Cryptanalysis of Multiple Modes of Operation, *Journal of Cryptology*, Vol. 11, No. 1, pp. 45–58, 1998. *Advances in Cryptology – Proceedings of ASIACRYPT* '94, LNCS 917, pp. 278–292, Springer-Verlag, Berlin, 1994.

[2] E. Biham, Cryptanalysis of Triple Modes of Operation, *Journal of Cryptology*, Vol. 12, No. 3, pp. 161–184, 1999. Technion Technical Report CS0885, 1996.

[3] E. Biham and A. Shamir, *Differential Cryptanalysis of the Data Standard*, Springer-Verlag, New York, 1993.

[4] H. Handschuh and B. Preneel, On the Security of Double and 2-Key Triple Modes of Operation, *Proceedings of FSE* '99, LNCS 1636, pp. 215–230, Springer-Verlag, Berlin, 1999.

[5] D. Hong, J. Sung, S. Hong, W. Lee, S. Lee, J. Lim, and O. Yi, Known-IV Attacks on Triple Modes of Operation of Block Ciphers, *Advances in Cryptology – Proceedings of ASIACRYPT* 2001, LNCS 2248, pp. 208–221, Springer-Verlag, Berlin, 2001.

[6] M. Matsui, Linear Cryptanalysis Method for DES Cipher, *Advances in Cryptology – Proceedings of EUROCRYPT* '93, LNCS 765, pp. 386–397, Springer-Verlag, Berlin, 1994.

[7] SSL 3.0 Specification, an Internet draft dated November 1996, available at http://wp.netscape.com/eng/ssl3/draft302.txt.

[8] D. Wagner, Cryptanalysis of Some Recently-Proposed Multiple Modes of Operation, *Proceedings of FSE* '98, LNCS 1372, pp. 254–269, Springer-Verlag, Berlin, 1998.

[9] 3GPP Specification, available at http://www.3gpp.org/specs/specs.htm.