Cryptanalysis of the ANSI X9.52 CBCM Mode

Eli Biham[1⋆] and Lars R. Knudsen[2⋆⋆]

[1] Computer Science Department, Technion – Israel Institute of Technology, Haifa 32000, Israel.

[2] Department of Informatics, University of Bergen, Hi-techcenter, N-5020 Bergen, Norway.

Abstract. In this paper we cryptanalyze the proposed (almost accepted) ANSI X9.52 CBCM mode. The CBCM mode is a triple-DES CBC variant which was designed against powerful attacks which control intermediate feedbacks for the benefit of the attacker. For this purpose, it uses intermediate feedbacks that the attacker cannot control, choosing them as a keyed OFB stream, independent of the plaintexts and ciphertexts. The attack we describe finds a way to use even this kind of feedback for the benefit of the attacker. It requires a single chosen ciphertext of 2^{65} blocks and 2^{58} complexity of analysis. We also describe an adaptive known-IV related-key attack which find one of three 56-bit keys requiring one known plaintext encrypted under 2^{33} different but related keys with 2^{57} complexity of analysis.

Key words. Cryptanalysis. ANSI X9.52. Modes of operation. CBCM mode. Triple-DES. Multiple Encryption.

1 Introduction

The Data Encryption Standard (DES) [14] has been the subject of intense debate and cryptanalysis. Already at the introduction of the algorithm in the seventies the DES was criticized for its short key length of 56 bits. As illustrated by Wiener [17] and by the DESCHALL [9] exhaustive search over the Internet it has become feasible for a powerful attacker to simply search exhaustively for a DES key. For a higher level of security it is therefore often recommended to use triple-DES, which multiple encrypts a plaintext three times with three different keys or to use two-key triple DES, which encrypts a plaintext with a key K_1, then decrypts with a key K_2 and finally encrypts again with key K_1. This increases the key lengths to 168 and 112 respectively. Direct application of triple-DES increases the security with respect to key-recovery attacks, but due to the short 64-bit blocksize, still allows for dictionary and ciphertext matching attacks [11, 8] with success probabilities similar as those for single-DES. Therefore, the most popular way to use triple encryption is by performing triple modes of operation. These

⋆ biham@cs.technion.ac.il, http://www.cs.technion.ac.il/~biham/.

⋆⋆ lars.knudsen@ii.uib.no, http://www.ii.uib.no/~larsr/.

modes apply three or more DES encryptions for each block and mix the data further in intermediate stages using data obtained from the previous blocks.

For several years the American National Standards Institute (ANSI) committee X9.F.1 is working on adopting a suite of triple modes of operation for triple-DES encryption [1]. One of these modes is the Triple DES Cipher Block Chaining (TCBC) mode, where the feedback block is the ciphertext block (computed by three DES encryptions). This mode is also called the *outer-CBC* mode [10]. This mode is described in Figure 1. However, this mode is vulnerable to the

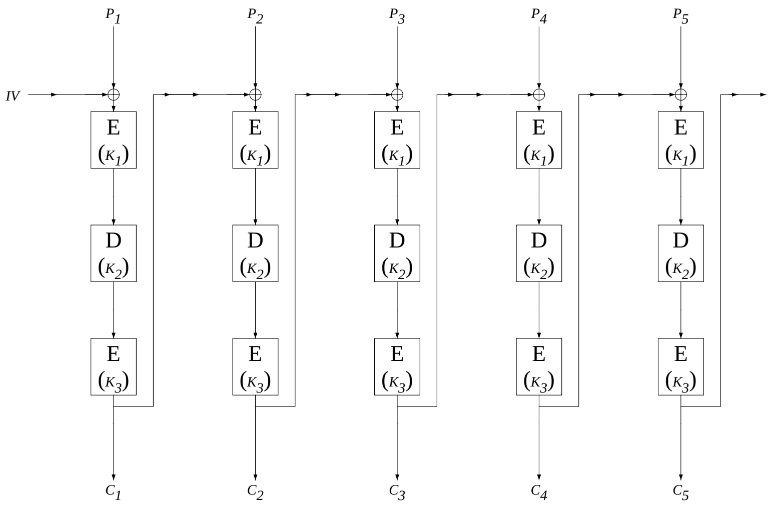


Fig. 1. The outer-CBC mode

matching ciphertext attack. Therefore it has been proposed to use triple-DES in a cipher block chaining mode with internal feedback, called the *inner-CBC* mode [10], where the feedback is applied after each single DES encryption. This mode is described in Figure 2. This mode is not vulnerable to the matching ciphertext attack, and was expected to be as secure as three-key triple-DES against key recovery attacks. As the best published attack against three-key triple-DES required 2^{112} complexity [13] it was expected that attacks against this mode require more that 2^{112} operations. (Note that recently Lucks [12] devised a new attack which slightly reduces the complexity of attacking three-key triple-DES to 2^{108}).

However, in a series of papers [2, 3, 4, 6], the first author analyzed a large number of multiple modes of operation, and in particular showed how to mount a key-recovery attack [3] against the inner-CBC mode. The complexity of this attack is considerably smaller than one would expect for triple encryption schemes,

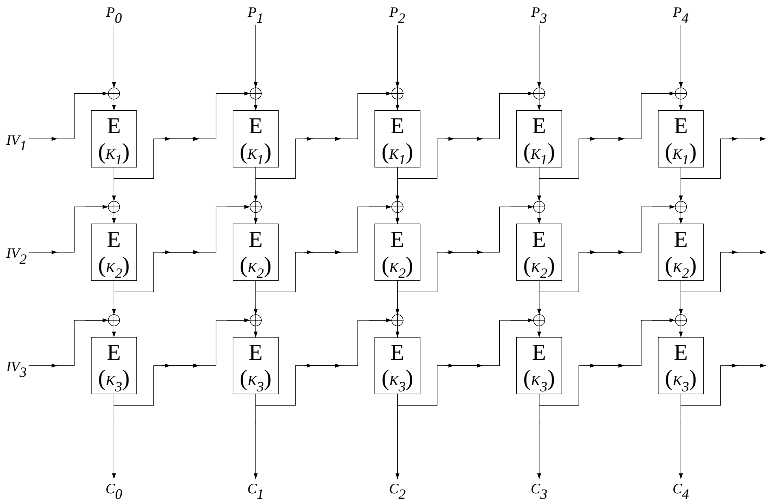


Fig. 2. The inner-CBC mode

and whose complexity is only slightly higher than the complexity of attacking single modes.

In [7, 8] Coppersmith, Johnson, and Matyas propose the *CBC with OFB Masking* (CBCM) mode of operation for triple-DES. The CBCM mode was specially designed to withstand the attacks described in [3, 5], the dictionary attack, and the matching ciphertext attack. The disadvantage of the proposal is, that it uses four DES encryptions using three different DES keys to encrypt each 64-bit plaintext block. In [7, 8] it is mentioned that the attacks in [3] that use internal feedbacks for the benefit of the attacker leave little hope for devising modes with internal feedbacks. In particular it is mentioned that the inner-CBC mode is weak due to such feedbacks, while on the other hand modes with only outer feedbacks are unsatisfactory. This motivated the design of a more complex mode which has both outer feedbacks, and internal feedbacks, but the internal feedbacks may not be controlled by the attacker, as they are the output of an OFB mode. It is claimed in [7] that the CBCM mode is immune against the kind of attacks described in [3].

Wagner analyzed an early CBCM proposal with an adaptive chosen IV chosen ciphertext attack. This attack led to the current design, in which only 2^{20} values are allowed for one of the two initial values [7, 8]. The best two attacks that the designers have sought require 2^{34} chosen ciphertexts and 2^{90} complexity of analysis respectively 2^{44} chosen ciphertexts and 2^{80} complexity of analysis.

This CBCM mode is part of the ANSI triple DES modes of operation proposed standard. This standard was almost accepted in September 1997, and was delayed only in order to correct some typos found in the proposal. The corrected version had to be finally accepted a few weeks later, and this attack was found just before this final vote.

In this paper we cryptanalyze the CBCM mode. In our main attack we use the internal OFB stream together with the common key K_1 of the first and last DES components for the benefit of the attacker. The attack requires one chosen ciphertext of 2^{65} blocks and 2^{58} complexity of analysis. The attack is applicable even if the initial values (IV's) are not known to (nor chosen by) the attacker. We believe that this attack uncovers a major weakness in the design of this mode, whose design took similar (chosen ciphertext) attacks into consideration, and as this mode was proposed as a replacement for modes which did not resist similar attacks.

We also show that if an attacker is able to get encryptions under several different but related keys, then one of the three keys used can be found using considerably less data. We outline a known-IV related-key known (or chosen) plaintext attack requiring only one known plaintext encrypted under 2^{33} different keys with 2^{57} complexity of analysis.

In the remaining of this paper we assume that the reader is familiar with the basic ideas of the attacks on multiple modes of operation [2, 3, 6]. As there, we describe the complexity of an attack by the number of encrypted blocks and the time of analysis required to to find the key a high probability.

In the following section we describe the CBCM mode, and in Section 3 we describe our main attack. In Section 4 we describe the related-key attack and in Section 5 we propose several possible improvements for this mode.

2 The CBCM mode

The CBCM mode is similar to the CBC mode when two-key triple-DES is used as the underlying cipher, with the following modification:

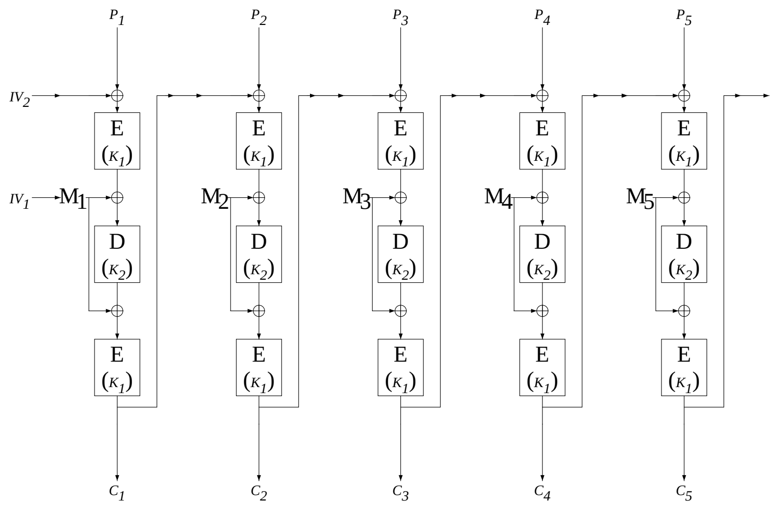
- between the first and second components, and between the second and third components, mixing with an OFB mask is applied. The same mask is used in both applications. The mask is the output of an OFB mode using a third key.

Figure 3 describes this mode, where E and D denoted encryption respectively decryption with the underlying block cipher.

3 The Attack

In this attack it is assumed that the attacker does not know any keys, key-relations nor initial values (IV's). The attacker only chooses one ciphertext stream, and receives the decrypted plaintext under the unknown key and unknown initial value.

The attack is as follows: Choose two ciphertext block values C_1 and C_2. Request the plaintexts of *one* ciphertext stream of 2^{64} C_1's followed by 2^{64} C_2's,



M_1, M_2, ..., etc, are the output blocks of an OFB mode with IV_1 as the initial value, encrypted under the key K_3:

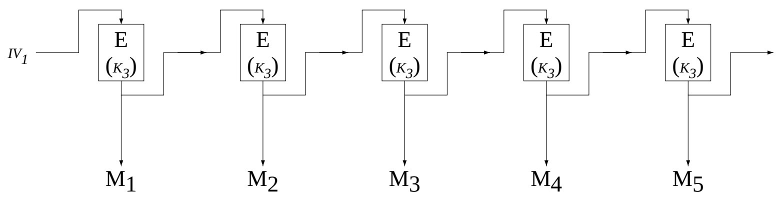


Fig. 3. The CBCM mode

under the unknown key $K = (K_1, K_2, K_3)$ (and any initial values). The period p of the OFB component can be easily identified in at most 2^{64} simple steps from the resulting plaintexts. The expected value of p is about 2^{63}. In the following description we ignore the first plaintext block, as we do not know the feedback IV_2 mixed with it. For simplicity of description we also ignore the first block with the ciphertext C_2.

Denote the plaintexts of the first p blocks (after removal of the original first block) by $P_{1,1}, \ldots, P_{1,p}$, and denote the inputs to the first DES components by $Q_{1,i} = P_{1,i} \oplus C_1$ for $i = 1, \ldots, p$. $Q_{1,i}$ is encrypted to C_1 with the OFB feedback M_i. For each i choose a corresponding block encrypted to C_2 using the same M_i, and denote its plaintext by $P_{2,i}$ (this is easy as the period p of the OFB component is known already). Denote $Q_{2,i} = P_{2,i} \oplus C_2$. This notation does not necessarily take $P_{2,1}, \ldots, P_{2,p}$ in the order they are received, but in an order easier to analyze, as for any i the same OFB block M_i is used in the computation of $P_{1,i}$ and $P_{2,i}$.

If we would now guess K_1, we can encrypt the first DES component, and decrypt the last component, and we are left with only the middle component using the key K_2 surrounded by two masks of M_i. As the masks are unknown, we cannot continue this way and find K_2 without increasing the complexity considerably. However, for this guess of K_1, we can compute the XOR of the encrypted and the decrypted results (using K_1), which equals the XORs of the input and the output of the middle DES component (if K_1 is correct).

The attack exploits that with a high probability the function $E_{K_2}(\cdot) \oplus V$ has exactly *one fixpoint* for randomly chosen V's (for example, a fixpoint of $E_{K_2}(\cdot)$ when $V = 0$). If by some chance we succeed to force this fixpoint to appear in our data, the whole triple encryption with the OFB mask reduces to something similar to double encryption with only one key K_1 (to simplify the following discussion, we describe decryption of this mode):

$$\begin{aligned} Q_{k,i} &= D_{K_1}(M_i \oplus E_{K_2}(M_i \oplus D_{K_1}(C_{k,i}))) \\ &= D_{K_1}(M_i \oplus V \oplus (M_i \oplus D_{K_1}(C_{k,i}))) \\ &= D_{K_1}(V \oplus D_{K_1}(C_{k,i})) \end{aligned}$$

and when $V = 0$

$$= D_{K_1}(D_{K_1}(C_{k,i})).$$

We use this property in our attack.

The attack is as follows:

1. Choose some arbitrary block value V.
2. Do the following steps for each candidate K' of the key K_1:
3. Compute

$$\begin{aligned} T_1(K') &= D_{K'}(V \oplus D_{K'}(C_1)) \\ T_2(K') &= D_{K'}(V \oplus D_{K'}(C_2)) \end{aligned}$$

   and search the plaintext for blocks i, j matching

$$\begin{aligned} Q_{1,i} &= T_1(K') \quad \text{and} \\ Q_{2,j} &= T_2(K'). \end{aligned}$$

4. If both matches are found compute

$$U = D_{K'}(C_1) \oplus D_{K'}(C_2)$$

   (which also necessarily equals $U = E_{K'}(Q_{1,i}) \oplus E_{K'}(Q_{2,j})$) and verify whether

$$E_{K'}(Q_{2,i}) \oplus E_{K'}(Q_{1,j}) = U$$

   (notice that the indices are exchanged!).

5. If the verification succeeds, the key K_1 is probably K'. If it fails, try the next candidate.
6. If verification fails for all candidates, choose another V, and repeat the analysis.

Figure 4 gives some details, where we assume for the purpose of illustration that

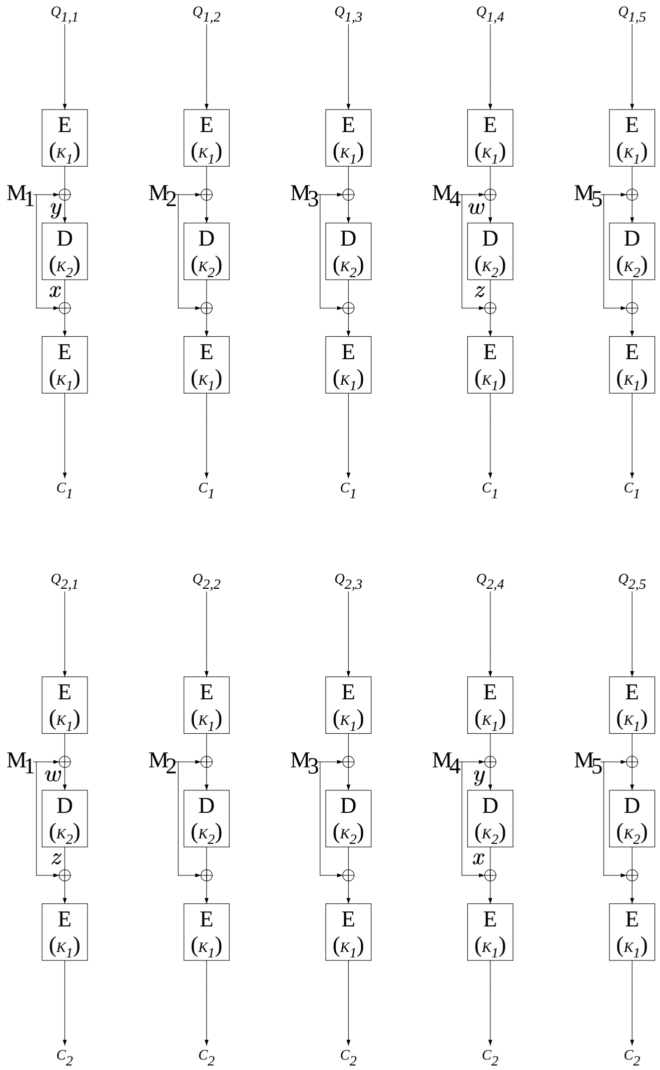


Fig. 4. Some intermediate details of the attack

$i = 1$ and $j = 4$, that the fixpoint is $x = E_{K_2}(x) \oplus V = y \oplus V$, and that $z = x \oplus M_i \oplus M_j$.

Let us explain why the attack works. Assume that $K' = K_1$ and that $E_{K_2}(\cdot) \oplus V$ has one fixpoint. Assume further that $Q_{1,i} = T_1(K') = D_{K'}(V \oplus D_{K'}(C_1))$ and $Q_{2,j} = T_2(K') = D_{K'}(V \oplus D_{K'}(C_2))$. Thus, we can assume that the output of the decryption step with K_2 equals the fixpoint in both cases. Therefore, $D_{K'}(C_1) \oplus D_{K'}(C_2) = M_i \oplus M_j = U$. Consider the encryptions of $Q_{1,j}$ and $Q_{2,i}$. We know that the OFB blocks used are M_j respectively M_i and the outputs of the decryption step with K_2 are $D_{K'}(C_1) \oplus M_j$ respectively $D_{K'}(C_2) \oplus M_i$. But since the latter two are equal, it must hold that the inputs to the decryption step with K_2 are equal. Thus, it must hold that $E_{K'}(Q_{2,i}) \oplus E_{K'}(Q_{1,j}) = M_i \oplus M_j = U$. Clearly, this test fails with a very high probability if $K' \neq K_1$.

Note that the attack still works if there is more than one fixpoint for $E_{K_2}(\cdot) \oplus V$. In this case the number of pairs in step 4 above increases slightly for the correct value of K'.

Once the key K_1 is found, K_2 can be found. Choose a random value a and assume it is decrypted in the second DES component (using key K_2) for one of the encryptions the attacker has already. Since the period p is expected to be 2^{63} this will be the case with probability one half. Compute $b = a \oplus D_{K_2}(a)$ for all values of K_2 and check if $b = E_{K_1}(Q_{1,i}) \oplus D_{K_1}(C_1)$ for some i. Note that K_1 is known at this stage. For every candidate of the key K_2 compute $M_i = E_{K_1}(Q_{1,i}) \oplus a$. Since the period of the OFB stream is known we find the encryption in the second collection of p plaintexts where M_i was used, and test whether $Q_{2,i} = D_{K_1}(M_i \oplus E_{K_2}(M_i \oplus D_{K_1}(C_{2,i})))$. This test leaves only very few possible values of the key K_2. If the attack fails, choose another value for a and repeat the attack. Once the keys K_1 and K_2 are found, K_3 can be found using the same data as before. The main idea is to find M_i and M_{i+1} for some value of i and then search exhaustively for the value of K_3 using $M_{i+1} = E_{K_3}(M_i)$. Simply choose 2^{33} random values a_i, $i = 1, \ldots, 2^{33}$ and compute $b_i = a_i \oplus D_{K_2}(a_i)$ (now K_2 is known). From the collection of plaintexts and the knowledge of the key K_1 find i and j such that a_i and a_j are used in the computation of two consecutive ciphertext blocks, and derive the likely candidates for M_i and M_{i+1}.

The complexity of the attack is as follows.

1. 2^{57} encryptions for each chosen value of V.
2. About 2^{65} chosen ciphertext blocks.
3. The attack (as described) finds the correct value of the key K_1 for about 16% of the values of V, which is the estimated probability that the function $E_{K_2}(\cdot) \oplus V$ has at least one fixpoint (63%) and that it occurs in both cycles of expected length 2^{63} (one half for each).
4. Higher probabilities of success can be reached by repeating the attack with several V's, and by increasing the number of chosen ciphertexts slightly: choosing three different C_1, C_2, C_3 increases the probability of finding *two* fixpoints in the three streams to one half (rather than one quarter), in which case the attack succeeds for 32% of the V's, and choosing four different C_1, C_2, C_3, C_4 increases the probability of finding *two* fixpoints in the four

streams to 13/16, in which case the attack succeeds in 51% of the V's.

5. The total time complexity of analysis is expected to be about 2^{58} using 2^{65} chosen ciphertext blocks.

4 A Related-Key Attack

In this section we show that the CBCM mode is vulnerable to a *known-IV related-key attack*, where an attacker is able to get encryptions under several different unknown but related keys. Our attack finds the value of the key K_3 using 2^{33} blocks and has 2^{57} complexity of analysis. One design principle of CBCM mode is that it should not be possible for an attacker to control the M_is, in other words, it should be impossible to find the value of K_3. In the following, let $E_{K_1,K_2,K_3}(IV_1, IV_2, P_1, \ldots, P_n)$ denote the encryption of plaintext blocks $P_1, ..., P_n$ in the CBCM mode and let $C_1, ..., C_n$ denote the corresponding ciphertext blocks. Decryption $D_{K_1,K_2,K_3}(\cdot)$ is defined correspondingly.

The first variant of the attack is a *known plaintext attack* and is as follows: the attacker gets the encryptions of about 2^{33} messages, each consisting of a single, fixed plaintext block P for 2^{33} different values of the key K_3. That is, the attacker obtains

$$C(i) = E_{K_1,K_2,K_3 \oplus a(i)}(IV_1(i), IV_2, P)$$

for $i = 1, \ldots, 2^{33}$, where the $a(i)$s are known to the attacker and where $a(i) \neq a(j)$ for $i \neq j$. The values of $IV_1(i)$ can be arbitrary and may vary, as long as they are known to the attacker. With a high probability the attacker finds $C(i) = C(j)$ for some $i \neq j$, and expects that this comes from coinciding masking values used in the encryptions, i.e., that $M_1(i) = M_1(j)$, where $M_1(i) = E_{K_3 \oplus a(i)}(IV_1(i))$ and $M_1(j) = E_{K_3 \oplus a(j)}(IV_1(j))$. This can be confirmed by checking if equal ciphertexts are obtained for the two keys with the same initial values for a plaintext $P' \neq P$. The attacker then searches exhaustively for K_3, that is, he solves the equation

$$E_{K_3 \oplus a(i)}(IV_1(i)) = E_{K_3 \oplus a(j)}(IV_1(j))$$

for K_3, which can be done in at most 2^{57} encryptions. The attack is independent of the values of $IV_1(i)$, as long as they are known. Therefore, restricting the possible values of IV_1 does not help to avoid the attack. Note, that in [7, 8] it is suggested that the initial values are sent in the clear and thus known to an attacker.

The second variant of the attack is a *chosen ciphertext attack*, which works even if the values of IV_2 vary and are unknown. The attacker now gets $P_1(i)$ and $P_2(i)$ from $D_{K_1,K_2,K_3 \oplus a(i)}(IV_1(i), IV_2(i), C_1, C_2)$ for $i = 1, \ldots, 2^{33}$, that is, the decryptions of a ciphertext consisting of two fixed blocks C_1 and C_2. Now he looks for a match $P_2(i) = P_2(j)$ and proceeds similarly as before.

The situation is simpler after K_3 is found. It is clear that the resulting (double encryption) scheme is not stronger than a two-key triple encryption scheme with respect to key-recovery attacks. In fact it is possible to find the values of K_1 and

K_2 using less data than the best known attack on two-key triple encryption [15]. Use K_3 to compute M_i, $1 \leq i \leq 2s$, such that for almost every 64-bit value U there exist M_i and M_j, where $i \leq s$ and $s < j \leq 2s$, such that $U = M_i \oplus M_j$. Store each such distinct value of U in a table together with the indices i, j. With $s \simeq 2^{35}$ it is possible to construct 2^{69} such values of U, which result in almost all possible 64-bit values. Subsequently, choose an additional chosen ciphertext consisting of s identical blocks C_1 followed by s identical blocks C_2. For all values k of K_1 compute $U = D_k(C_1) \oplus D_k(C_2)$. Since K_3 is assumed to be known at this stage it is possible for the attacker to find a pair M_i and M_j such that $U = M_i \oplus M_j$, where M_i was used to decrypt C_1 and M_j was used to decrypt C_2. Let P_i and P_j denote the two corresponding plaintext blocks. If $E_k(P_i \oplus C_1) \oplus E_k(P_j \oplus C_2) = U$, k is a possible value of K_1. The attack is repeated a few times to get a unique value of K_1. Once K_1 is found, it is straightforward to find K_2 by an exhaustive key search. Although this part of the attack requires the memory to store up to 2^{64} values, the chosen text requirements are small, and in particular, crucially smaller than similar attacks on the TCBC mode of operation.

5 Possible Improvements of the CBCM Mode

Our main attack exploits both the internal OFB feedbacks and the use of the same key K_1 in the first and last DES components. As noted in [7, 8] it is not advisable to use two different OFB feedbacks instead of one. In [6] some modes are cryptanalyzed just when the OFB components are different, and these attacks do not hold when the OFB streams are the same.

The attack can be thwarted by introducing a third OFB component, which will mix into the ciphertext. This is also similar to the modes proposed in [5] and [6]. Changing the key of the last DES component to a fourth key K_4 is also expected to thwart our main attack.

The related key attack can be thwarted by introducing a key schedule, which derives the four DES keys needed from two or three user-selected keys, such that changing one or several of the user-selected keys changes several of the four DES keys with a high probability.

Furthermore, computing the initial values IV_1 and IV_2 as the result of a keyed-hash function of the transmitted "IV" (for example using the three keys K_1, K_2, K_3 used in the CBCM mode) rather than sending them in the clear, inhibits their knowledge by the attacker, and thus protect against the related key attack and against Wagner's attacks on the CBCM mode. Recently Wagner devised many known-IV and chosen-IV attacks [16] against the modes of operation described in [5]. These attacks share the basic property of our related key attack that it works only if the attacker knows the initial values, or can affect them in a specified way, and thus they are also thwarted by choosing the initial values as the result of a keyed-hash function of the transmitted "IV". As this protecting technique is very simple and very effective against known-IV and chosen-IV attacks, which usually have a relatively small complexity, we recommend using it in all the modes of operation. On the other hand, this technique does not protect against all kinds of attacks. In particular, our main attack and the attacks described in [3, 6] are not affected, as they require only one stream of ciphertext, and do not assume any special property of the initial values.

Acknowledgments

The first author was supported by the fund for the promotion of research at the Technion.

References

1. ANSI draft X9.52, *Triple Data Encryption Algorithm Modes of Operation*, Revision 6.0, May 1996.
2. Eli Biham, *On Modes of Operation (Abstract)*, proceedings of Fast Software Encryption, Cambridge, Lecture Notes in Computer Science, pp. 116–120, 1993.
3. Eli Biham, *Cryptanalysis of Multiple Modes of Operation*, Lecture Notes in Computer Science, Advances in Cryptology, proceedings of ASIACRYPT'94, pp. 278–292, 1994.
4. Eli Biham, *How to Forge DES-Encrypted Messages in 2^{28} Steps*, technical reports CS884, Technion, August 1996.
5. Eli Biham, *Cryptanalysis of Triple Modes of Operation*, technical reports CS885, Technion, August 1996. This is a preliminary version of [6].
6. Eli Biham, *Cryptanalysis of Triple Modes of Operation*, Journal of Cryptology, to appear.
7. Don Coppersmith, Don B. Johnson, Stephen M. Matyas, *Triple DES Cipher Block Chaining with Output Feedback Masking*, submitted to ANSI, 1995.
8. D. Coppersmith, D. B. Johnson, S. M. Matyas, *A Proposed Mode for Triple-DES Encryption*, IBM Journal of Research and Development, Vol. 40, No. 2, pp. 253–262, March 1996.
9. The DESCHALL home page, `http://www.frii.com/~rcv/deschall.htm`.
10. B. S. Kaliski and M. J. B. Robshaw. *Multiple encryption: Weighing security and performance.* Dr. Dobbs Journal, pp. 123–127, January 1996.
11. L.R. Knudsen. *Block Ciphers – Analysis, Design and Applications.* PhD thesis, Aarhus University, Denmark, 1994.
12. Stefan Lucks, *Attacking Triple Encryption*, proceedings of Fast Software Encryption, Paris, Lecture Notes in Computer Science, 1998.
13. R. C. Merkle, M. E. Hellman, *On the Security of Multiple Encryption*, Communications of the ACM, Vol. 24, No. 7, pp. 465–467, July 1981.
14. National Bureau of Standards, *Data Encryption Standard*, U.S. Department of Commerce, FIPS pub. 46, January 1977.
15. Paul C. van Oorschot, Michael J. Wiener, *A known-plaintext attack on two-key triple encryption*, Advances in Cryptology, proceedings of EUROCRYPT'90, LNCS 473, pp. 318–325, 1990.
16. David Wagner, *Cryptanalysis of Some Multiple Modes of Operation*, proceedings of Fast Software Encryption, Paris, Lecture Notes in Computer Science, 1998.

17. Michael J. Wiener, *Efficient DES Key Search*, technical report TR-244, School of Computer Science, Carleton University, Ottawa, Canada, May 1994. Presented at the Rump session of CRYPTO'93, August 1993.