On the Security of Double and 2-Key Triple Modes of Operation

Helena Handschuh[1] and Bart Preneel[2⋆]

[1] Gemplus/ENST, France
helena.handschuh@gemplus.com
[2] Katholieke Universiteit Leuven, Dept. Electrical Engineering–ESAT
bart.preneel@esat.kuleuven.ac.be

Abstract. The DES has reached the end of its lifetime due to its too short key length and block length (56 and 64 bits respectively). As we are awaiting the new AES, triple (and double) encryption are the common solution. However, several authors have shown that these multiple modes are much less secure than anticipated. The general belief is that these schemes should not be used, as they are not resistant against attacks requiring 2^{64} chosen plaintexts. This paper extends the analysis by considering some more realistic attack models. It also presents an improved attack on multiple modes that contain an OFB mode and discusses practical solutions that take into account realistic constraints.

1 Introduction

Ever since the Data Encryption Standard [13] was adopted in the mid 1970s, the issue of its small key size has been raised. Nowadays a 56-bit key is clearly within the range of a dedicated exhaustive search machine [12,29]. Already in 1979, Tuchman proposed the use of triple-DES with two or three keys [25]. Double encryption was rejected quickly because Merkle and Hellman showed that a meet-in-the-middle requires 'only' 2^{57} encryptions and a memory with 2^{56} 112-bit values [24]. Later van Oorschot and Wiener came up with a more practical version of this attack, that requires 2^{72} encryptions but only 16 Gbyte [27] (other trade-offs are available). In the 1980s, triple-DES became popular; for example double length master keys were used to encrypt single length DES session keys. The best known attack on 2-key triple-DES is also by van Oorschot and Wiener [26]; it requires 2^{120-t} encryptions and 2^t known plaintexts. This shows that 2-key triple-DES may provide increased strength against brute force key search.

For encryption of more than one block, a mode of operation has to be defined different from the ECB (Electronic CodeBook) mode. The ECB mode is vulnerable to a dictionary attack, where an opponent collects ciphertexts and

⋆ F.W.O. postdoctoral researcher, sponsored by the Fund for Scientific Research, Flanders (Belgium).

L. Knudsen (Ed.): FSE'99, LNCS 1636, pp. 215–230, 1999.

corresponding plaintexts. The three other standard modes of operation are defined in FIPS 81 [14]: CBC (Cipher Block Chaining), CFB (Cipher FeedBack) and OFB (Output FeedBack). The limitation of CBC and CFB modes are the matching ciphertext attacks: after encrypting 2^{32} blocks, information starts to leak about the plaintext (see for example [18]). In the OFB mode, less information leaks, but the fact that the key stream has an expected period of 2^{63} blocks also provides some information on the plaintext. For a formal treatment of the modes of operation, see Bellare *et al.* [2].

In the early 1990s, modes for multiple encryption were analysed. The most straightforward solution is to replace DES by two-key triple-DES and to use this new block cipher in a 'standard' mode (known as 'outer-CBC' and 'outer-CFB' [16]). While for CFB and CBC mode this precludes exhaustive key search, the complexity of a matching ciphertext attack is still 2^{32} blocks, as this depends on the block length only. This motivated research on interleaved or combined modes, where the modes themselves are considered as primitives. Coppersmith analysed some early proposals for two-key triple-DES modes in [9,10]. The most straightforward solution is to iterate the CBC or CFB mode of a block cipher (known as 'inner-CBC' and 'inner-CFB'). However, Biham showed that these simple interleaved modes are vulnerable to a 2^{34} chosen ciphertext attack [4,5].

In [6], Biham systematically analyses all the double and triple 'interleaved' modes, where each layer consists of ECB, OFB, CBC, CFB and the inverses of CBC and CFB, denoted with CBC^{-1} and CFB^{-1} respectively. Note that there are 36 double encryption schemes and 216 triple encryption schemes. His main conclusion is that *"all triple modes of operation are theoretically not much more secure than a single encryption."* The most secure schemes in this class require 2^{67} chosen plaintexts or ciphertexts, 2^{75} encryptions, and 2^{66} storage (for example, scheme 208 in [6]).

Biham also proposes a small set of triple modes, where a single key stream is generated in OFB mode and exored before every encryption and after the last encryption [6]. The conjectured security is 2^{112} encryptions. He also proposes several quadruple modes with conjectured security level 2^{128} encryptions. However, at FSE'98 Wagner shows that if the attack model is changed to allow for chosen ciphertext/chosen IV attacks, the security of all but two of these modes can be reduced to 2^{56} encryptions and between 2 and 2^{32} chosen chosen-IV texts [28].

Coppersmith *et al.* propose the CBCM mode [11], which is a quadruple mode; this mode has been included in ANSI X9.52 [1]. However, Biham and Knudsen present an attack requiring 2^{65} chosen ciphertexts and memory that requires 2^{58} encryptions [7].

Many of these attacks are very intricate, but one cannot escape the conclusion that these are only 'certificational' attacks. In most environments, it is completely unthinkable to carry out a chosen plaintext or ciphertext attack with more than 2^{40} texts (e.g., on a smart card). Moreover, attacks that require a storage of 2^{56} 64-bit quantities are not feasible today. This does not imply that we do not recommend a conservative design. Our goal is to explore which sche-

mes achieve a realistic security level today. For long term security, migration to AES (Advanced Encryption Standard) will provide a solution.

Our contribution. The goal of this paper is to develop a better understanding of the security of the simpler structures such as 2-key triple and double modes of operation. We show that for common applications where a known IV attack can be applied, these modes are scaringly close to being in the range of exhaustive search or at least susceptible to Merkle-Hellman's meet-in-the-middle attack [24]. We study double encryption schemes under different attack models (one of the two IV's known, and replay of IV). We also present a new attack on certain double modes (the cycle attack), that reduces the plaintext requirement from 2^{64} chosen plaintexts to about 2^{35} known plaintexts and memory, at the cost of an increased work factor for the analysis (2^{87} compared to 2^{58}); nevertheless we believe that this may be more realistic. Finally we compare some solutions for the cases where the integrity and/or secrecy of the IV's is protected. Depending on the setting, one of the following three modes is recommended : double OFB, CBC followed by CBC^{-1}, or the latter double mode masked with an OFB stream before each encryption and after the last.

The rest of the paper is organised as follows: the next section discusses the notation and the attack models for the IV's. Section 3 gives details on modes that can be broken by exhaustive search. Section 4 deals with modes that fall under the standard meet-in-the-middle attack (MITM) and Sect. 5 with modes that succumb to "narrow pipe" (the term "narrow pipe attack" is due to John Kelsey) or collision attacks. These three attacks are becoming more or less practical today because of the very low number of texts they require. In Sect. 6, we explain our new cycle attack and in Sect. 7 we compare several modes that provide a reasonable security level for current applications. Section 8 presents conclusions and open problems.

2 The Setting

In this section we introduce our notation and discuss the attack model in terms of control of the opponent over the IV.

2.1 Notation

We refer to Wagner's paper [28] for notation throughout this paper. The successive blocks of plaintext and ciphertext in every multiple mode are denoted by P_0, P_1, P_2,... and C_0, C_1, C_2,.... The standard single modes (ECB, CBC, CFB, OFB, CBC^{-1}, and CFB^{-1}) are combined to double or two-key triple modes using the notation X/Y and X/Y/Z respectively, where X,Y,Z are one of the above modes. As usual, we assume that the underlying block cipher is "ideal" in the sense that the modes are attacked by generic methods, and not by differential [8] or linear cryptanalysis [23] for instance. We will be dealing exclusively with two keys K_1 and K_2. For two-key triple modes, K_1 is the key of the first

and the last encryption components, and K_2 is the key of the middle decryption component. IV_1 and IV_2 are the initial values of the feedback and chaining modes, and for two-key triple encryption an additional IV_3 is required. Figure 1 contains an example of a 2-key triple mode.

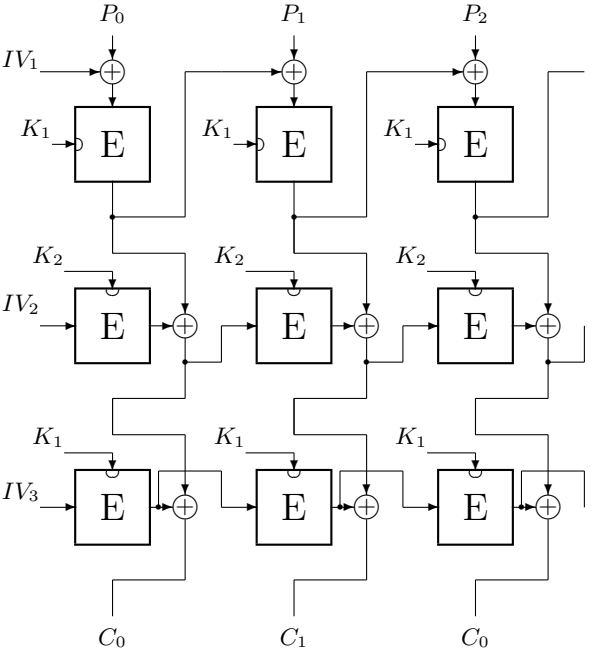

Fig. 1. The CBC/CFB/OFB mode

2.2 Models for the Initial Value

We would like to stress that Biham's attacks in [6] usually consider the initial values IV to be *unknown,* except for some of the modes that are very hard to cryptanalyse otherwise. This is the main reason why many attacks require a huge number plaintexts or ciphertexts (typically about 2^{66}). On the other hand, Wagner chose to use a security model in which the IV's may be *chosen* by the attacker. He mentions that his attacks may be converted into known IV attacks using slightly more IV's (about 2^{32}). One can also consider for certificational purposes the more artificial scenario where only one of the IV's is known.

We believe that for most applications known IV attacks are quite reasonable in the case of encryption as the IV's are chosen by the encryption box but have to be transmitted with the ciphertext in order to be decrypted by the other party. In several practical protocols the IV's are transmitted in the clear. We may also want to allow a kind of "chosen" IV attack (in a chosen ciphertext setting) in which the adversary does not know the actual value of the IV but

is able to replay the same (possibly encrypted) IV a few times with different text queries. The result of our analysis is that under such threat models, basic double or triple modes are deeply flawed.

In Sect. 7 we will also recommend schemes for scenarios where the IV's are encrypted and/or where the integrity of the IV's can be protected.

3 Divide and Conquer Strategies

In [6], Biham analyses all 36 double modes (schemes 7 to 42) under the assumption that the IV's are unknown. We are interested in a stronger attack model, and would like to find out which schemes still have a 'reasonable' security level against practical attacks. Therefore we analyse double modes for which the best known attack (with unknown IV's) requires more than 2^{64} chosen texts. Biham lists 15 such modes.

We consider all of these modes under several known IV attacks and show that with a few known texts, their security drops down to the basic exhaustive search complexity of a 56-bit key.

3.1 Known IV_1 and IV_2 Attacks

Six modes are vulnerable to direct exhaustive search on each key, requiring only a handful plaintext/ciphertext pairs, about 2^{57} encryptions and no memory. These modes are: OFB/ECB, ECB/OFB, CBC^{-1}/OFB, OFB/CBC, OFB/CFB, and CFB^{-1}/OFB. Note that there are three different modes and their inverses. There is no IV on an ECB mode: we will denote this as $IV = 0$. As an example we show how to recover the two keys of the CBC^{-1}/OFB mode depicted in Fig. 2.

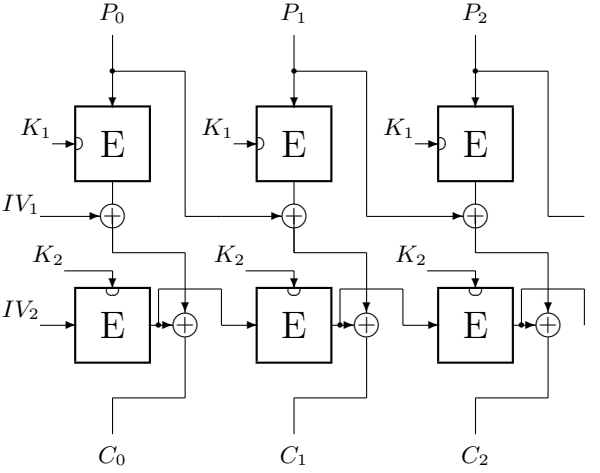

Fig. 2. The CBC^{-1}/OFB mode

The attack proceeds as follows. Choose a 3 block plaintext of the form (M, M, M) and get the corresponding ciphertext (C_0,C_1,C_2) as well as IV_2. Then

from the structure of the mode it follows that $C_1 \oplus C_2 = E^2_{K_2}(IV_2) \oplus E^3_{K_2}(IV_2)$. Therefore we can exhaustively search for the key K_2 satisfying this relation. Once this key has been found, it is straightforward to recover K_1. If more than one key pair is found, a few additional plaintext/ciphertext pairs suffice to pick the right pair.

Another example is the CFB^{-1}/OFB mode. Choose a message of the form (P_0,P_1) and encrypt it twice. Get the corresponding ciphertexts (C_0,C_1) and (C_0^*,C_1^*). The IV's will of course be different but the plaintext remains the same. Again, the relation between the two second ciphertext blocks is of the form: $C_1 \oplus C_1^* = E^2_{K_2}(IV_2) \oplus E^2_{K_2}(IV_2^*)$. Therefore we can first exhaustively search for K_2 and then for K_1.

Attacking the inverse modes requires mostly a chosen ciphertext attack where the IV's may either be chosen or just known to the attacker, depending on the context. The above modes can also be attacked under the assumption that only one of the IV's is known to the attacker. Typically, it can be shown that it suffices to know the initial value of the output feedback mode involved in every one of the six before-mentioned modes.

3.2 Replay Attacks

In this section we address a slightly different model of attack in which divide and conquer strategies may also apply. Here we assume that the attacker knows only one of the IV's, but is given the ability to replay the other IV without any knowledge of the actual value of it. In other words, one of the IV's may for instance be encrypted to offer more security. Then the ability to replay the same encrypted unknown IV together with the knowledge of the second initial value leads to an attack requiring approximately only one exhaustive key search. In some cases, it may even be enough to have the ability to replay an IV without any knowledge about its value or the second initial value. This is the case in a chosen ciphertext setting. Note that Wagner mentions that some of his chosen-IV attacks might be converted into this kind of "replay" attack [28].

As an example we describe a chosen ciphertext replay attack on the CBC/OFB mode (see Fig. 3). Assume that the attacker knows IV_1 and has the ability to replay IV_2 without having access to its actual value. From the equality of the two output feedback streams, we know that for two chosen ciphertexts (C_0, C_1) and (C_0^*, C_1^*) we have the following : $E_{K_1}(P_0 \oplus IV_1) \oplus C_0 = E_{K_1}(P_0^* \oplus IV_1^*) \oplus C_0^*$. Therefore K_1 can be found by exhaustive search. Next K_2 is recovered by $E_{K_2}(E_{K_1}(P_0 \oplus IV_1) \oplus C_0) = C_1 \oplus E_{K_1}(P_1 \oplus E_{K_1}(P_0 \oplus IV_1))$.

This type of attack applies whenever the initial value of an output feedback mode may be replayed, and sometimes even when the initial value of a cipher feedback mode is replayed.

4 Meet-in-the-Middle Attack

This attack requires only a handful of plaintext/ciphertext pairs, and about 2^{57} encryptions. The simple variant needs much more memory than the attacks of the

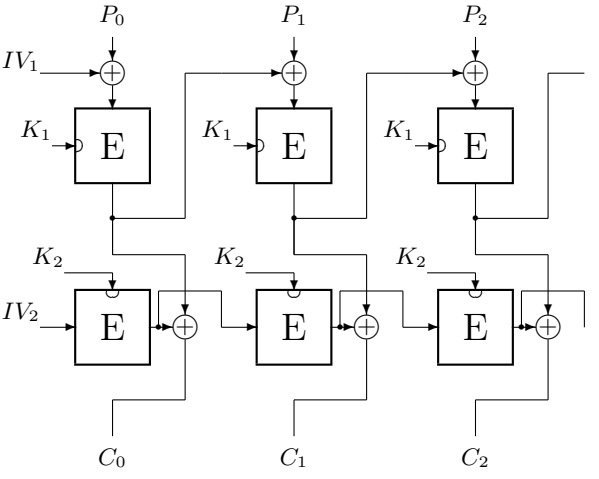

Fig. 3. The CBC/OFB mode

previous section, typically 2^{56} blocks. The latter requirement is currently hard to achieve. However, van Oorschot and Wiener show in [27] that such a standard meet-in-the-middle attack can be modified to work with a memory of 16 Gbyte, at the cost of 2^{72} encryptions; other trade-offs are possible. Their approach is based on cycle finding techniques using distinguished points. Therefore, when it comes to discussing threat models, we believe that a model in which about 2^{56} blocks have to be stored but only a few queries to the black box are needed is far more realistic than a scenario in which 2^{60} or more queries are made to the box (and possibly have to be stored anyway). We are focusing on attacks that require as few queries as possible.

4.1 Double Interleaved Modes

Again we make the assumption that both IV's are known to the attacker. It is easy to see that in this model, none of the 15 double modes can be more secure than the ECB/ECB mode. (Note that this does not hold for secret IV attacks, which are definitely more interesting from the cryptanalyst's point of view.) As explained in Sect. 3, six of these may also be attacked using exhaustive search on one key. Once again this proves that interleaved modes do not provide any additional security compared to standard encryption. In this particular setting, knowing only one of the IV's and possibly replaying it or the other one does not allow to mount a meet-in-the-middle attack.

As an example we show how an attack on CBC/CFB^{-1} proceeds (see Fig. 4). We always attack a single block message as in standard meet-in-the-middle attacks on two-key double encryption. Choose a fixed plaintext P_0 and get the corresponding ciphertext C_0. Then tabulate $E_{K_1}(IV_1 \oplus P_0) \oplus C_0$ for every possible value of the key K_1 (store the results in a hash table). Next compute every possible value of $E_{K_2}(IV_2)$ for every possible key K_2 and check for a match in

the table. The matches suggest a possible key pair. Rule out the wrong key pairs with a few additional plaintext/ciphertext pairs.

The attack is essentially the same for every other mode. Just compute one half of the key into a hash table, and lookup for a match with the other half of the key.

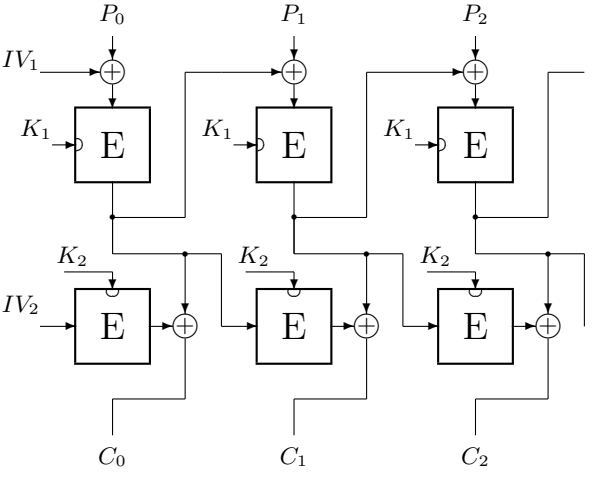

Fig. 4. The CBC/CFB^{-1} mode

4.2 Two-Key Triple Interleaved Modes

We now address the case of some two-key triple interleaved mode, which is actually the idea that motivated our research in the first place. We were wondering whether two-key triple modes are as secure as standard two-key triple ECB encryption (the best attack on this scheme is the one by van Oorschot and Wiener discussed in Sect. 1).

The result of our investigation is that under a known IV attack, no such mode using a feedback mode on its inner layer is more secure than single encryption. Indeed, whenever a feedback mode involves the middle key, a mask is applied in between the two outer layers and can be computed into a hash table, while the outer layers may be computed on their own, and the exors of the results are looked up in the table. See Fig. 1 for a picture of the CBC/CFB/OFB mode.

Query the encryption of a single plaintext block P_0, and for every possible key K_2, compute $E_{K_2}(IV_2)$ into a hash table. Next compute $E_{K_1}(P_0 \oplus IV_1) \oplus E_{K_1}(IV_3) \oplus C_0$ for every possible key K_1 and look the matches up in the hash table. Rule out the wrong key pairs with some additional plaintext/ciphertext pair as usual.

5 Narrow Pipes and Collision Attacks

In this section we focus on threat models where one of the IV's is unknown to the attacker and show that some cipher block chaining modes fall under collision or "narrow pipe" attacks. This setting may not be usual at all but the goal here is to understand which are the minimum requirements to mount a collision attack on double interleaved modes. From the structure of these modes, it is easy to see that the weakness comes from the chaining mode itself. The complexity of this kind of attack is still quite acceptable as it requires only about 2^{32} plaintext/ciphertext pairs of a few blocks each, about 2^{57} encryptions and 2^{32} memory blocks.

We show how this attack works on the CFB/CBC^{-1} mode (see Fig. 5) when IV_1 is not known to the attacker. Randomly encrypt plaintexts of the form (P_0, P_1, M) where M is kept constant, and store the ciphertexts and associated IV_2 values. After about 2^{32} trials, a collision occurs on the exor value of the second block of the first encryption layer. This collision propagates through the cipher feedback of the first layer as well as through the plaintext chaining of the second layer to all the following ciphertext blocks. Therefore such a collision has most probably occurred when a collision is found on the third ciphertext block. Now write the equality of the colliding samples as:

$$D_{K_2}(C_0 \oplus IV_2) \oplus C_1 = D_{K_2}(C_0^* \oplus IV_2^*) \oplus C_1^*$$

and exhaustively search for the right key K_2. Once K_2 is found, find the first key by exhaustive search using the equation:

$$M \oplus D_{K_2}(C_2 \oplus D_{K_2}(C_1 \oplus D_{K_2}(C_0 \oplus IV_2))) = E_{K_1}(D_{K_2}(C_1 \oplus D_{K_2}(C_0 \oplus IV_2))) \ .$$

This technique applies to several modes making use of the CBC or CFB mode.

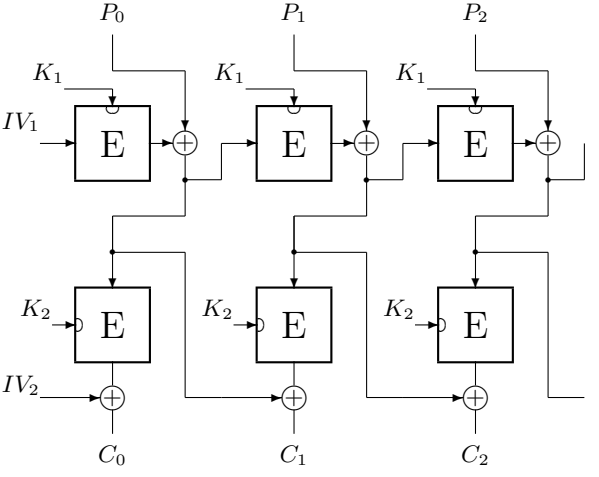

Fig. 5. The CFB/CBC^{-1} mode

6 Cycle Attacks

This attack is actually the dual of the narrow pipe attack. In this case we guess one of the keys (say, K_2) and peel off the corresponding layer. What remains is the output of an OFB-mode, which is in some sense a narrow pipe (64 bits). However, in this case, it is very *unlikely* that a collision will occur in a sequence of 2^{35} blocks (because the feedback function in OFB-mode is a permutation rather than an injective mapping). If a collision is observed, we know that our guess for the key K_2 was wrong. We will show that this attack requires about 2^{35} plaintext blocks, 2^{87} encryptions, and 2^{35} memory blocks (or 256 Gbyte).

This attack applies to the following double modes: CBC^{-1}/OFB, OFB/CBC, CFB^{-1}/OFB, and OFB/CFB, even if the IV's are unknown; it represents a different trade-off than the attack by Biham (2^{64} chosen plaintexts, 2^{58} encryptions). The attack also applies to CBC/OFB, OFB/CBC^{-1}, CFB/OFB, and OFB/CFB^{-1} if one of the IV's is known. If the mode of which the IV is known is not the OFB mode, then one has to choose the plaintext to be constant (for example, all zeroes after the 2nd block) in order to make the mode behave like the OFB mode.

Consider for example the OFB/CBC mode (see Fig. 6). The attack proceeds as follows. Collect a plaintext containing $\ell = 2^{34.7}$ blocks and the corresponding ciphertext. Guess K_2, and peel off the CBC mode. One can now compute a sequence of ℓ blocks that should be the output of the OFB mode. Therefore, if the guess for K_2 was correct, one does not expect to see a collision (the probability that a random starting point lies on an OFB cycle shorter than ℓ blocks is given by $\ell/2^{64}$, which is negligible in our case;[1] see for example Flajolet and Odlyzko [15]). If the guess for K_2 was wrong, the effect is that one obtains a random sequence of blocks, that contains with high probability a collision. For $\ell \approx \sqrt{2^n}$, this probability is given by $1 - \exp(-\lambda)$ with $\lambda = \ell^2/2^{n+1}$; for $\ell = 2^{34.7}$ and $n = 64$, this is equal to $1 - e^{-21.11} \approx 1 - 6.8 \cdot 10^{-10}$. (Note that the number of collisions is Poisson distributed with parameter λ given by the above expression.) On average, the collision will occur after $\sqrt{\pi/2} \cdot 2^{n/2}$ blocks [15]. If a wrong value of K_2 does not result in a collision (an event with probability $\exp(-\lambda)$), one has to try all values for K_1. The work factor of this attack is given by

$$\left(1 - exp\left[-\frac{\ell^2}{2^{n+1}}\right]\right)\sqrt{\frac{\pi}{2}} \cdot 2^{n/2} \cdot 2^{k-1} + exp\left[-\frac{\ell^2}{2^{n+1}}\right](\ell + 2^k)2^{k-1} + \ell + 2^{k-1} \quad .$$

The first term is the expected work factor to eliminate guesses for K_2 that result in a collision. The second term corresponds to the guesses for K_2 for which no collision occurs, which implies that an exhaustive search for K_1 is required. The last two terms correspond to the expected effort for the correct value of K_2; they are negligible compared to the first two terms. The second term decreases with ℓ, and becomes negligible with respect to the first one if $\ell \geq 2^{34.7}$. The total

[1] Such a short cycle is easy to detect.

work factor is then approximately equal to

$$\sqrt{\frac{\pi}{8}} \cdot 2^{k+n/2} \approx 2^{87.3} \ .$$

At first sight, one might think that this attack also applies to the ECB/OFB and OFB/ECB modes. However, in this case a wrong key guess K_2^* means that we encrypt the OFB sequence in double DES (with the correct key K_2 and the wrong key guess K_2^* respectively). A double-DES encryption in ECB mode does not create collisions, which implies that it is not possible to distinguish between wrong and correct guesses.

The attack also applies to eight 2-key triple modes with OFB in the middle, where the first mode is CBC^{-1}, CFB^{-1}, or ECB and the last mode is CBC, CFB, or ECB (the only exception is the ECB/OFB/ECB mode). If the corresponding IV is known, the OFB mode is also allowed for the first or last encryption, the CBC^{-1} and CFB^{-1} are allowed for the last encryption, and CBC and CFB are allowed for the first encryption.

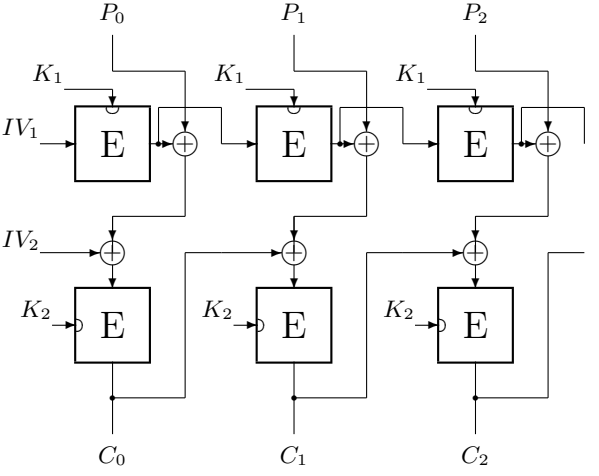

Fig. 6. The OFB/CBC mode

7 What's Left for Common Applications?

In this section we first summarise our results. Subsequently we look at which pragmatic solutions are available to designers who want a short-term solution with an acceptable security level.

7.1 Summarising Our Results

The results of the previous sections are summarised in Table 1. We will denote divide and conquer attacks as DIV&C, replay attacks as RPL, meet-in-the-middle

attacks as MITM, collision attacks as COLL, and cycle attacks as CYCLE. We consider different known IV cases, as well as the case where no IV is known. The associated complexities are the following (known or chosen plaintexts/off-line computations/memory requirements):

- Divide and conquer or Replay attacks: $4/2^{57}/-$;
- Meet-in-the-middle attacks: $4/2^{57}/2^{56}$, $4/2^{66}/2^{40}$, or $4/2^{72}/2^{34}$;
- Collision attacks: $2^{32}/2^{57}/2^{32}$ (chosen plaintexts);
- Cycle attacks: $2^{35}/2^{87}/2^{35}$ (1 single plaintext, sometimes chosen; see Sect. 6).

Table 1 shows how vulnerable double modes can become if the attacker obtains information about the initial values or can manipulate these. We would like to stress that this is the case in many applications and that designers should make the right choices having these numbers in mind.

Table 1. Double modes under known/unknown IV attacks

Mode	Known IV_1 and IV_2	Known IV_1	Known IV_2	Unknown IV's
ECB/OFB	–	–	DIV&C	RPL
OFB/ECB	–	DIV&C	–	RPL
CBC/CBC^{-1}	MITM	COLL	COLL	
CBC/OFB	MITM	CYCLE / RPL	CYCLE	
CBC/CFB^{-1}	MITM	COLL / RPL	COLL	
CBC^{-1}/OFB	DIV&C	CYCLE / RPL	DIV&C	CYCLE / RPL
OFB/CBC	DIV&C	DIV&C	CYCLE / RPL	CYCLE / RPL
OFB/CBC^{-1}	MITM	CYCLE	CYCLE	
OFB/OFB	MITM	CYCLE / RPL	CYCLE / RPL	
OFB/CFB	DIV&C	DIV&C	CYCLE / RPL	CYCLE / RPL
OFB/CFB^{-1}	MITM	CYCLE / RPL	CYCLE / RPL	
CFB/CBC^{-1}	MITM	COLL	COLL / RPL	
CFB/OFB	MITM	CYCLE / RPL	CYCLE / RPL	RPL
CFB/CFB^{-1}	MITM	COLL / RPL	COLL / RPL	
CFB^{-1}/OFB	DIV&C	CYCLE / RPL	DIV&C	CYCLE / RPL

7.2 Discussion

An important question is: which solutions remain with a reasonable security level that require only two keys? This implies that we are not worried about attacks that require more than 2^{50} chosen plaintexts or ciphertexts, or that require a work factor of 2^{100} or more. The choice of these numbers is rather arbitrary; note however that it is easy to prevent attackers from having access to more than 2^{50} plaintext/ciphertext pairs by changing the keys more frequently, or by taking the system out of service early. However, once encrypted data is made public,

an opponent can record it and wait 20 or 30 years (or even more) before he attempts to decipher it. We also assume that the keys are generated or derived in such a way that related key attacks are precluded [3].

We distinguish between four cases:

- if the IV's are encrypted and their integrity is protected by a MAC (which also should prevent replay), we recommend to use the simple OFB/OFB mode (scheme 28 in [6]). The best known attack described in [6] has complexity $2^{65}/2^{65}/2^{64}$; such an attack is not realistic in many environments. Note also that chosen-IV attacks are precluded by the use of the MAC algorithm. This mode provides no error propagation; if the authenticity of the information is a concern, it is recommended to calculate a MAC over the IV's and over the plaintext.

  As a MAC algorithm, MacDES could be used [20]; this algorithm extends the well known CBC-MAC with double-DES in the first and last encryption (but with different but related keys for the 2nd encryption). MacDES seems to provide high security at relatively low cost; forgery attacks are not feasible if the number of plaintexts encrypted with a single key is reduced to 2^{32} (or a little less), and the best known key recovery attack requires 2^{65} chosen text-MAC pairs, 2^{90} encryptions, 2^{55} MAC verifications, and 2^{37} bytes memory.

  Wagner discusses the use of encrypted and authenticated IV's and argues that *"adding this much complexity to the system may begin to test the limits of one's comfort zone,"* [28]. However, our point of view is that the currently known attacks on multiple modes tend to be very complex as well; moreover, MAC algorithms are probably better understood than encryption modes. It is of course important to apply appropriate key separation techniques (this may require additional evaluation).
- If the IV's are encrypted but their integrity is not protected by a MAC, we recommend to use the CBC/CBC^{-1} mode (scheme 15 in [6]). The best known attack described in [6] has complexity $2^{68}/2^{66}/2^{66}$. This mode seems to provide better security against IV replay attacks than the previous one. In order to simplify the scheme, one can choose $IV_1 = IV_2$.
- We do not recommend a double mode where the IV's are not encrypted but their integrity is protected. If follows from Table 1 that all these scheme succumb to a meet-in-the-middle attack that requires only a few plaintext/ciphertext pairs. For this case, we suggest the OFB[CBC,CBC^{-1}] mode proposed by Biham [6]; this notation means that one first applies the OFB mode, then CBC, then OFB (with the same key stream), then CBC^{-1} and finally OFB (again with the same key stream). Wagner asserts that his chosen-IV attacks do not apply to this scheme [28]. Our preliminary evaluation suggests that the security level of this mode is still sufficiently high even if the same key is used for the CBC and CBC^{-1} encryption.
- If the IV's are not encrypted and their integrity is not protected by a MAC, one could also use the previous scheme; however, we do not recommend this solution.

We understand that making such recommendations is a little risky; indeed, there are certificational attacks on these schemes (except for the last one), and in the past years significant progress has been made in the cryptanalysis of multiple modes. On the other hand, we believe that it is important to point out to the research community (and to practitioners) that for some of the schemes, we are not aware of any realistic attacks.

We also recall a number of other schemes that can serve as "reference points" (note that the major motivation for introducing new modes was precisely to avoid the drawbacks of the first two of them):

- 2-key triple-DES in outer-CBC mode: the main attacks here are a matching ciphertext attack and the van Oorschot-Wiener attack [26] with the following parameters: $2^t/2^{120-t}/2^t$.
- DESX in CBC mode [17]: the matching ciphertext attack applies as well; the security bound is $2^t/2^{119-t}/2^t$. A disadvantage is that this solution has a smaller margin to shortcut attacks (differential and linear cryptanalysis) than all double or triple modes.
- DEAL-128 in CBC mode [19]: this is certainly an interesting alternative. The best known attack on this cipher is $2^{70}/2^{121}/2^{67}$, where the texts are chosen plaintexts. A small disadvantage is the slow key schedule (6 DES encryptions). We believe that further research is necessary on this solution, as DEAL is a new block cipher rather than a mode (see also [22]).

Table 2 compares the efficiency of the solutions proposed. The security level corresponds to the best attack known. For DESX this is the security bound proved, but if the underlying block cipher is DES, shortcut attacks apply with a lower complexity (differential [8] and linear cryptanalysis [23]). If the IV's are encrypted, this requires 3 encryptions per IV (2-key triple encryption), except for DESX, where IV is encrypted using DESX. For the OFB/OFB scheme, it is assumed that the MAC algorithm is applied to both the IV's and the plaintext; this implies that this variant also provides guarantees on the message integrity. If the MAC is applied only to the IV's, the number of encryptions drops to $2t + 10$. Note that for the CBC/CBC^{-1} scheme a single IV is used. The MAC algorithm used is MacDES [20]; it requires $t + 2$ encryptions and requires that $t \geq 2$.

8 Conclusions and Open Problems

We have analysed the security of double and 2-key triple modes under the assumption that information on the IV's is available. Under this model, most of these schemes are practically insecure. This extends the work of Biham who has shown that these modes are theoretically insecure when the IV's are secret. We have also introduced a new attack, the cycle attack, that reduces the plaintext requirement for certain double and triple modes (at the cost of an increased number of off-line encryptions).

Table 2. Summary of properties of several schemes when encrypting a t-block plaintext

mode	encrypt IV's	authenticate IV's	number of encryptions	security
OFB/OFB	yes	yes	$3t+10$	$2^{65}/2^{65}/2^{64}$
CBC/CBC^{-1}	yes	no	$2t+3$	$2^{68}/2^{66}/2^{66}$
OFB[CBC/CBC^{-1}]	no	yes	$3t+5$	$2/2^{112}/-$
2-key triple-DES outer-CBC	yes	no	$3t+3$	$2^t/2^{120-t}/2^t$ 2^{32} Match. Ciph.
DESX in CBC	yes	no	$t+1$	$2^t/2^{119-t}/2^t$ 2^{32} Match. Ciph.
DEAL in CBC	yes	no	$3t+3$	$2^{70}/2^{121}/2^{67}$

We have also compared the security level and performance of a number of alternatives that offer a reasonable security level against attacks that require less than 2^{40} known or chosen texts. Some of these schemes seem to provide a simple solution that is easy to analyse, but we caution the reader against too much optimism. We leave it as an open problem to improve the attacks on the schemes listed in Table 2.

References

1. ANSI draft X9.52, *"Triple Data Encryption Algorithm Modes of Operation," Revision 6.0,* 1996.
2. M. Bellare, A. Desai, E. Jokipii, P. Rogaway, "A concrete security treatment of symmetric encryption: Analysis of the DES modes of operation," *Proceedings of the 38th Symposium on Foundations of Computer Science*, IEEE, 1997.
3. E. Biham, "New types of cryptanalytic attacks using related keys," *EUROCRYPT'93, LNCS 765,* Springer-Verlag, 1994, pp. 398–409.
4. E. Biham, "On modes of operation," *Fast Software Encryption'93, LNCS 809,* Springer-Verlag, 1994, pp. 116–120.
5. E. Biham, "Cryptanalysis of multiple modes of operation," *ASIACRYPT'94, LNCS 917,* Springer-Verlag, 1994, pp. 278–292.
6. E. Biham, "Cryptanalysis of triple-modes of operation," *Technion Technical Report CS0885,* 1996.
7. E. Biham, L. R. Knudsen, "Cryptanalysis of the ANSI X9.52 CBCM mode," *EUROCRYPT'98, LNCS 1403,* Springer-Verlag, 1998, pp. 100–111.
8. E. Biham, A. Shamir, *"Differential Cryptanalysis of the Data Encryption Standard,"* Springer-Verlag, 1993.
9. D. Coppersmith, "A chosen-ciphertext attack on triple-DES modes," 1994.
10. D. Coppersmith, "A chosen-plaintext attack on 2-key inner triple DES CBC/EDE," 1995.
11. 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, 1996, pp. 253–262.

12. The Electronic Frontier Foundation, *"Cracking DES. Secrets of Encryption Research, Wiretap Politics & Chip Design,"* O'Reilly, May 1998.
13. FIPS 46, *"Data Encryption Standard,"* US Department of Commerce, National Bureau of Standards, 1977 (revised as FIPS 46–1:1988; FIPS 46–2:1993).
14. FIPS 81, *"DES Modes of Operation,"* US Department of Commerce, National Bureau of Standards, 1980.
15. P. Flajolet, A. M. Odlyzko, "Random mapping statistics," *EUROCRYPT'89, LNCS 434,* Springer-Verlag, 1990, pp. 329–354.
16. B. S. Kaliski, M.J.B. Robshaw, "Multiple encryption: Weighing security and performance," *Dr. Dobb's Journal*, January 1996, pp. 123–127.
17. J. Kilian, P. Rogaway, "How to protect DES against exhaustive key search, *CRYPTO'96, LNCS 1109,* Springer-Verlag, 1996, pp. 252–267.
18. L. R. Knudsen, *"Block Ciphers – Analysis, Design and Applications,"* PhD thesis, Aarhus University, Denmark, 1994.
19. L. R. Knudsen, *"DEAL: a 128-bit block cipher,"* AES submission, 1998.
20. L. Knudsen, B. Preneel, "MacDES: MAC algorithm based on DES," *Electronics Letters*, Vol. 34, No. 9, 1998, pp. 871–873,
21. S. Lucks, "Attacking triple encryption," *Fast Software Encryption'98, LNCS 1372,* Springer-Verlag, 1998, pp. 239–253.
22. S. Lucks, "On the security of the 128-bit block cipher DEAL," *Fast Software Encryption, LNCS*, L.R. Knudsen, Ed., Springer-Verlag, 1999.
23. M. Matsui, "Linear cryptanalysis method for DES cipher," *EUROCRYPT'93, LNCS 765,* Springer-Verlag, 1993, pp. 386–397.
24. R. C. Merkle, M. E. Hellman, "On the security of multiple encryption," *Communications of the ACM,* Vol. 24, No. 7, 1981, pp. 465–467.
25. W. Tuchman, "Hellman presents no shortcut solutions to the DES," *Spectrum*, Vol. 16, 1979, pp. 40–41.
26. P. C. van Oorschot, M. J. Wiener, "A known-plaintext attack on two-key triple encryption," *EUROCRYPT'90, LNCS 473,* 1990, pp. 318–325.
27. P. C. van Oorschot, M. J. Wiener, "Improving implementable meet-in-the-middle attacks by orders of magnitude," *CRYPTO'96, LNCS 1109*, 1996, pp. 229–236.
28. D. Wagner, "Cryptanalysis of some recently-proposed multiple modes of operation," *Fast Software Encryption'98, LNCS 1372,* Springer-Verlag, 1998, pp. 254–269.
29. M.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 and reprinted in W. Stallings, *Practical Cryptography for Data Internetworks,* IEEE Computer Society Press, 1996, pp. 31–79.