REPORTS
IN
INFORMATICS

ISSN 0333-3590

Block chaining modes of operation

Lars R. Knudsen

REPORT NO 207 **October 2000**

Department of Informatics

UNIVERSITY OF BERGEN

Bergen, Norway

This report has URL `http://www.ii.uib.no/publikasjoner/texrap/ps/2000-207.ps`

Reports in Informatics from Department of Informatics, University of Bergen, Norway, is available at `http://www.ii.uib.no/publikasjoner/texrap/`.

Requests for paper copies of this report can be sent to:

Department of Informatics, University of Bergen, Høyteknologisenteret,
P.O. Box 7800, N-5020 Bergen, Norway

Block chaining modes of operation

Lars R. Knudsen*
University of California at San Diego
Department of Computer Science and Engineering
9500 Gilman Drive
CA 92093 San Diego, USA

October 6, 2000

Abstract

In this paper modes of operation for block ciphers are considered. The focus is on a special class of modes, called the block chaining modes. We discuss modes with finite and infinite error propagation and propose the Accumulated Block Chaining (ABC) mode of the latter type. ABC is proposed for application for the Advanced Encryption Standard.

Key words. Block Cipher, Modes of Operation, Advanced Encryption Standard.

1 Introduction

In 1980 NBS (now NIST) published four modes of operation for block ciphers [14] with the DES [13] as a particular application in mind. The four modes are the Electronic Code Book (ECB), the Cipher Block Chaining (CBC), the Cipher FeedBack (CFB), and the Output FeedBack (OFB). For convenience the modes are described in Appendix A.

In this paper focus is on modes of operation with block chaining such as the CBC and CFB modes of operation. We propose a new mode of operation called the Accumulated Block Chaining (ABC) mode which has an infinite error propagation. Such modes are not part of the FIPS standard [14] nor of any other standards as far we are informed. However, we think they should be and shall argue in more details in this paper why such modes of operation are often preferable to modes of operation with finite error propagation.

Consider an n-bit block cipher using k-bit keys. Let $E_K(X)$ denote the encryption of plaintext block X under the key K, and let $D_K(Y)$ denote the decryption of ciphertext block Y under the key K. Let $P_1, \ldots, P_i, \ldots$ be n-bit blocks of the message or plaintext, and let $C_1, \ldots, C_i, \ldots$ be the corresponding n-bit blocks of the ciphertext.

We consider the security and properties of the block chaining modes of operation with respect to confidentiality, not for message integrity. One popular way to obtain both is to encrypt the data using a block cipher with a first key in the CBC mode, then compute the CBC-MAC of the data using a second key. Another solution is to hash the message using a collision-resistant hash function, then append the hash result to the message and encrypt the result using a block chaining mode[11, Ex. 9.84]. In both these examples, the encryption of the data is not restricted to

* On leave from the University of Bergen, Norway supported by the Norwegain Research Council.

using the CBC mode and other modes can be applied. Recently Jutla [7] showed that one can obtain message integrity together with confidentiality at the cost of $\log m$ additional encryptions for a message consisting of m blocks. In one proposal he shows how the additional encryptions can be introduced in a traditional CBC encryption scheme to obtain message integrity. We believe that Jutla's method can be applied to a wide range of block chaining modes.

In our confidentiality model, we shall assume that the block cipher is secure against known-plaintext and chosen-plaintext attacks and that the key size k is chosen such that an exhaustive key search is computationally infeasible. However regardless of the cryptographic strength of the block cipher itself modes of operation might leak information about the plaintexts when encrypting many blocks under the same key. Therefore when discussing the security of these modes, it is assumed that the attacker operates in the ciphertext-only scenario. From the point of view of the attacker the block cipher is a black box which contains an n-bit permutation chosen uniformly at random from the set of all n-bit permutations.

The encryption operation in the proposed ABC mode is defined as follows.

$$\begin{aligned} H_i &= P_i \oplus h(H_{i-1}) && (1) \\ C_i &= E_K(H_i \oplus C_{i-1}) \oplus H_{i-1}, && (2) \end{aligned}$$

where h is a mapping from n to n bits and where H_0 and C_0 are initial values. The decryption operation is

$$\begin{aligned} H_i &= D_K(C_i \oplus H_{i-1}) \oplus C_{i-1} && (3) \\ P_i &= H_i \oplus h(H_{i-1}). && (4) \end{aligned}$$

Later it is argued that choosing $h(X) = X$ or $h(X) = X^{<<1}$ (a one-bit rotation) is sufficient for most applications. With these definitions of h, H_i holds an accumulated value of the first i plaintext blocks. With $h(X) = 0$ the ABC mode equals the IGE mode of operation proposed by C. Campbell in [3] and analysed recently in [6].

The proposed technique of accumulated block chaining can be applied to any other mode of operation, including the CBC mode.

This paper is organised as follows. In §2 the requirements and properties of the considered modes of operation are discussed, where subsection 2.6 discusses why modes of operation with error propagation are sometimes preferred to modes of operation with error recovery. The design rationale of the proposed mode of operation with error propagation is presented in §3. Related work is in §4 and §5 holds our conclusions.

2 Criteria for modes of operation

We shall consider the following criteria and properties for evaluating and constructing (block chaining) modes of operation for block ciphers:

- overhead: the additional operations for the encryption or decryption operation when compared to encryption or decryption in the ECB mode.
- error recovery: the property that an error in the ith ciphertext block is inherited by only a few plaintext blocks after which the mode re-synchronises.
- error propagation: the property that an error in the ith ciphertext block is inherited by the ith and all subsequent plaintext blocks.

- diffusion: how the plaintext statistics is reflected in the ciphertexts. E.g., low entropy plaintext blocks should not be reflected in the ciphertext blocks. Also, we consider the decryption modes and how the ciphertext statistics are reflected in the plaintexts.
- security: do ciphertext blocks leak information about plaintext blocks, e.g., does a birthday attack apply?

The error recovery property is sometimes referred to as a finite error propagation, and the error propagation is what is sometimes referred to as an infinite error propagation. For error propagation and error recovery also considered are the cases where a ciphertext block is lost and when an additional block is inserted by an enemy.

Most block chaining modes of operation require initial values. These values can be chosen at random for every encryption or can be fixed. Moreover, they can be sent in the clear or in encrypted form to the recipient. The properties which we discuss in this paper are independent of the initial values, and we shall not discuss these further in this paper.

2.1 Overhead

The overhead in a mode of operation is defined as the extra work needed when compared to the ECB mode of operation. Although it seems possible to construct modes of operation with strong properties by using several encryptions and/or hash function evaluations in the processing of one plaintext or ciphertext block, from a performance point of view it is preferred to keep the overhead down to a minimum. As a first design principle we will consider only modes for which the overhead is small compared to one ECB mode encryption, e.g., a few exclusive-or operations.

2.2 Error recovery

Modes with error recovery are suited for situations where a retransmission after an erroneous data transmission is not possible or regarded too expensive. In [12] the typical example is the encryption of stored data, e.g., the content of a hard disk. Using only encryption and a mode with error propagation is not recommended. A single error in an early ciphertext block will leave the rest of the hard disk garbled after decryption. Other possible applications for these modes of operation are for real-time voice, music or video transmissions. Here the possibility for a retransmission is not present.

Let us here shortly review how an error in one ciphertext block propagates in the CBC and CFB modes of operation. An error in a ciphertext block affects two plaintexts blocks. As an example, assume that ciphertext C_3 has an error and that all other ciphertext blocks are error-free, then $P_4 = D_K(C_4) \oplus C_3$ inherits the error from C_3 and $P_3 = D_K(C_3) \oplus C_2$ will be completely garbled. Here we assume that even a small change in the plaintext to the block cipher will produce a very different ciphertext. All other plaintexts will be decrypted correctly. Similarly, if a ciphertext block is lost or if an extra ciphertext block is inserted, only two plaintext blocks will be affeced. In the CFB mode with m-bit blocks an error in one ciphertext block will be inherited by $n/m + 1$ plaintext blocks.

For error recovery we use the following definition.

Definition 1 *A block cipher mode of operation has* **error recovery**, *if the decryption operation has the following form*

$$P_i = g_K(C_i, \ldots, C_{i-v}) \tag{5}$$

for some keyed function g, whose output depends on all input bits, a constant $v \geq 0$, and where C_j are some initial values for $j < 1$.

If there is an error in a ciphertext block C_i, this error will be inherited by $P_i, \ldots, P_{i+v}$ but not by any further plaintext blocks. One will not in general obtain error recovery for both the encryption operation and the decryption operation which is illustrated in §2.6.

2.3 Error propagation

Modes with error propagation are well-suited for situations where errors in transmissions are either unlikely to happen or taken care of by noncryptographic means like error-correcting codes, and/or situations where an erroneous data transmission is dealt with by a retransmission.

We shall operate with following definition for error propagation inspired by [12, page 69].

Definition 2 *A block cipher mode of operation has* **error propagation**, *if the decryption operation has the following form*

$$P_i = f_K(C_i, \ldots, C_1), \tag{6}$$

for some keyed function f, whose output depends on all input bits.

Here an error in a ciphertext block C_i affects the plaintext block P_i and all subsequent plaintext blocks P_j for $j > i$.

Matyas and Meyer gave the definition of a *general block cipher* [12]. Using our terms this is a mode of operation with error propagation for both the encryption operation and the decryption operation. In other words, this is a mode of operation where the decryption operation can be described as in Definition 2 and where the encryption operation can be described as $C_i = \tilde{f}_K(P_i, \ldots, P_1)$ for some keyed function $\tilde{f}$, whose output depends on all input bits.

Clearly, with only one pass through the blocks in the encryption mode, an error in the ith ciphertext block will not affect the decryption of the jth plaintext block for $j < i$. In this situation a general block cipher based on an n-bit block cipher is what resembles most a large sn-bit block cipher, which is one advantage of these modes of operation.

2.4 Birthday attack

The birthday attack applies to some of the standard modes of operation. When encrypting many plaintext blocks under the same key information is leaked about the plaintexts. This was noted in [8] and earlier for the CFB mode in [10]. In [4] this attack was called the *matching ciphertext attack*.

Fact 1 *Consider an n-bit block cipher used in the ECB, CBC, or CFB mode. It is assumed that the plaintext blocks are chosen at random from a uniform distribution. If s blocks are encrypted under the same key information is leaked about some plaintext blocks with a probability of $p_s = 1 - (1 - 2^{-n})^{s(s-1)/2}$. With $s = 2^{(n+1)/2}$ this probability is about 0.63.*

Proof: Consider the ECB mode. By the birthday paradox in a collection of s random n-bit blocks $C_1, ..., C_t$ there will exist a pair (i, j), s.t. $C_i = C_j$ with probability p_s. In that case the attacker immediately knows that $P_i = P_j$.

Under the assumption on the plaintext blocks using the CBC mode a match $C_i = C_j$ in s ciphertext blocks will be found with a probability of p_s. Further it follows that

$$\begin{aligned} C_i &= C_j \quad \Rightarrow \\ P_i \oplus C_{i-1} &= P_j \oplus C_{j-1} \quad \Rightarrow \\ P_i \oplus P_j &= C_{i-1} \oplus C_{j-1}. \end{aligned}$$

Thus, if the ciphertext blocks C_{i-1} and C_{j-1} are known, one can compute $P_i \oplus P_j$. The case for the CFB mode is similar to the one of the CBC mode. ■

Note that in the case of the CBC mode the previous result does not depend on whether the attacker has access to one single ciphertext consisting of s blocks, $C_1, \ldots, C_s$. The attack is applicable also in the case where an attacker has access to several or many shorter ciphertexts, $C^1, \ldots, C^t$, where each C^u consists of s_u blocks, and where $\sum_{\ell=1}^{t} s_\ell = s$.

For ease of argumentation it was assumed that the plaintext blocks are chosen uniformly at random. However as we shall argue next, the results are valid for any non-trivial/practical plaintext space. Assume that the plaintext space is redundant. For a block cipher used in the ECB mode, the probability of finding a match in two ciphertext blocks depends on the redundancy in the plaintext blocks. The more redundant the plaintexts are, the higher the probability of a match. For the attacker the worst case is when the plaintext blocks are random.
Consider the CBC mode. With a redundant plaintext space the birthday attack as outlined in Fact 1 does not directly apply. As a trivial example, if all plaintext blocks are equal, say zero, then the CBC mode reduces to the OFB mode. It is known that the OFB mode with full n-bit feed back has a cycle length of about 2^{n-1} [5]. However, it is also known that the OFB mode with r-bit feed back for $r < n$, has a cycle length of about $2^{n/2}$ [11]. Since the OFB mode with r-bit feed back is comparable to the CBC mode with a redundant plaintext space, for all nontrivial plaintext spaces the probability of success for a birthday attack will be approximately the same as that of Fact 1. Assume further that the probability distribution of the exclusive-or of pairs of plaintext blocks is nonuniform. Then as before $C_i = C_j \Rightarrow P_i \oplus P_j = C_{i-1} \oplus C_{j-1}$ and an attacker can compute $P_i \oplus P_j$. It also follows that in this case, the match $C_i = C_j$ implies that $C_{i-1} \oplus C_{j-1}$ will not be uniformly distributed. Thus with a pair of matching ciphertext blocks the plaintext statistics is reflected in the ciphertexts.

The block size for the DES is 64 bits. With $2^{32.5}$ encrypted blocks there will be a pair of matching ciphertext blocks with a probability of about 0.63. This probability is 2^{-15} when 2^{25} blocks are encrypted. The block size for the AES [15] is 128 bits. Thus, with $2^{64.5}$ blocks there will be a pair of matching ciphertext blocks with a probability of about 0.63. The probability for an information leakage is about 2^{-49} if 2^{40} blocks are encrypted and about 2^{-29} if 2^{50} blocks are encrypted.

2.5 Diffusion

If the plaintext space is redundant the distribution of the n-bit ciphertext blocks should not reflect this. Let us consider modes of operation where the encryption operation is $C_i = g_K(P_i, \ldots, P_{i-v})$. Here a low entropy plaintext space could be reflected directly in the ciphertext blocks. To illustrate this, assume that a plaintext block can take only s possible values. But then clearly any ciphertext block can take at most s^v values. If $s < 2^{n/v}$ then some n-bit values will never occur in the ciphertext blocks. One remedy is to choose v big, or to construct the mode such that each ciphertext block depends on all previous plaintext blocks as in modes of operation with error propagation, for example by including a cipher feed back.

Let us next investigate diffusion in the decryption operations. Consider modes with error recovery and $P_i = g_K(C_i, \ldots, C_{i-v})$. Here an attacker can force a plaintext block P_j to the value of a plaintext block P_i for $j \geq i + v$ by replacing $C_j, \ldots, C_{j-v}$ by $C_i, \ldots, C_{i-v}$. As an extreme case, the modes all have the following property. If all ciphertext blocks have equal values, then all plaintext blocks have equal values, except possibly for the first v blocks depending on the initial values (which may be secret).

As a concrete example, consider the CBC mode and the decryption operation $P_i = D_K(C_i) \oplus C_{i-1}$. Then an attacker can force the plaintext block P_j to the value of P_i by replacing (C_{j-1}, C_j) by (C_{i-1}, C_i). Note that although this also affects P_{j-1} and P_{i-1}, the lack of diffusion in the decryption operation allows an attacker to force certain plaintext blocks to get equal values.

These problems are not present (in general) in modes of operation with error propagation. Assume that $j > i$ then $P_i = f_K(C_i, \ldots, C_1)$ and $P_j = f_K(C_j, \ldots, C_i, \ldots, C_1)$. For a well-constructed function f an attacker will not be able to force the value of P_j to that of P_i or vice versa.

2.6 Error propagation versus error recovery

In this section we compare the modes of operation supporting error propagation and error recovery.

As mentioned earlier, modes of operation with error recovery are suited for situations where a retransmission after an erroneous data transmission is not possible or regarded too expensive. Let us consider the example of the encryption of stored data again. Assume that a mode with error recovery is used and that the stored data is only encrypted (e.g., no checksums nor codes are used). For concreteness, let us assume that the CBC mode is used. An error in one ciphertext block will be inherited in one plaintext block and an additional plaintext block will be garbled. Thus s bit errors in one ciphertext block will produce on the average $s + n/2$ bit errors in the plaintexts. First, the errors in the plaintext blocks cannot be detected without scanning through all data blocks, and then only if the plaintext space is sufficently redundant. One way to obtain error detection is to include a checksum or to use an error-detecting code. In a mode with error propagation this can obtained as discussed in §2.3. Second, even in case an error is detected the garbled plaintext block is lost. To overcome this problem one could use an error-correcting code on the plaintexts. However if this is practical then one should rather apply the error-correcting code on the ciphertext blocks. But then there is no longer an incentive to use a mode of operation with error recovery.

Birthday attacks similar to those of §2.4 apply to instances of both types of modes. However, as we shall see in §3 there exist modes of operation with error propagation which are (much) less vulnerable to such attacks when compared to modes with error recovery, like the CBC mode.

To sum up, the advantages of modes of operation with error propagation are: they have better diffusion properties for both the encryption and decryption operations, they are in general less vulnerable to birthday attacks, when encrypting s-block messages they resemble best a big sn-bit block cipher when only one pass through the s blocks is allowed, and there are implementational advantages as the encryption and decryption operations can be made equal.

From the definitions above it is clear that error propagation and error recovery (for a fixed value of v) are orthogonal properties. One cannot have both at the same time. However, it is possible to obtain both within one mode of operation. Consider a mode of operation X with error recovery, where $v \geq 1$. If we use the decryption mode of X for encryption, then we obtain a mode with error propagation since in this case we would have $C_i = g_K(P_i, \ldots, P_{i-v})$ and thus

$$\begin{aligned} P_i &= \tilde{f}_K(C_i, P_{i-1}, \ldots, P_{i-v}) && (7) \\ &= \tilde{f}_K(C_i, \tilde{f}_K(C_{i-1}, P_{i-2}, \ldots, P_{i-v-1}), \ldots, P_{i-v}), && (8) \end{aligned}$$

and it follows that P_i depends on all previous ciphertext blocks. However as illustrated in the previous section for such modes the plaintext statistics could be reflected in the ciphertexts. So although it is possible to have just one mode of operation to obtain both error propagation and error recovery under the definitions above, it is recommended to use different modes of operation if both properties are needed.

3 Design rationale for ABC

In this section we explain the motivation behind the proposed ABC mode of operation. The goal is to construct a mode of operation with error propagation for which the overhead, as defined earlier, is the smallest possible. Let us consider the encryption operation first and consider the encryption of the ith plaintext block P_i. We need a cipher feedback for diffusion properties. With $C_i = f_K(P_i, C_{i-1})$ one does not obtain error propagation since in this case $P_i = \tilde{f}_K(C_i, C_{i-1})$. Therefore we consider the following general encryption operation, $C_i = f_K(P_i, P_{i-1}, C_{i-1})$. If we restrict ourselves to using each input block only once, using only one (not constant) block cipher encryption and a few exclusive-or operations the possible operations are.

$$\begin{aligned} C_i &= E_K(P_i \oplus P_{i-1} \oplus C_{i-1}), && (9) \\ C_i &= E_K(P_i \oplus P_{i-1}) \oplus C_{i-1}, && (10) \\ C_i &= E_K(P_i) \oplus P_{i-1} \oplus C_{i-1}, && (11) \\ C_i &= E_K(P_i \oplus C_{i-1}) \oplus P_{i-1}, && (12) \\ C_i &= E_K(C_{i-1}) \oplus P_i \oplus P_{i-1} && (13) \end{aligned}$$

Here we have ignored the modes obtained from swapping P_i and P_{i-1}.

The modes (10) and (11) share the following property. In a ciphertext-only attack if an attacker considers the blocks $C_i \oplus C_{i-1}$ then the quantities he gets are output from modes where the encryption operation depends only on plaintext blocks. As illustrated earlier for redundant plaintext spaces such modes have diffusion problems.

Consider next the modes (9) and (13). The decryption mode of (9) is

$$\begin{aligned} P_i &= D_K(C_i) \oplus P_{i-1} \oplus C_{i-1} \\ &= D_K(C_i) \oplus D_K(C_{i-1}) \oplus P_{i-2} \oplus C_{i-2} \oplus C_{i-1} \\ &= D_K(C_i) \oplus D_K(C_{i-1}) \oplus D_K(C_{i-2}) \oplus P_{i-3} \oplus C_{i-3} \oplus C_{i-2} \oplus C_{i-1}. \end{aligned}$$

The decryption mode of (13) is

$$\begin{aligned} P_i &= E_K(C_{i-1}) \oplus C_i \oplus P_{i-1} \\ &= E_K(C_{i-1}) \oplus C_i \oplus E_K(C_{i-2}) \oplus C_{i-1} \oplus P_{i-2} \\ &= E_K(C_{i-1}) \oplus C_i \oplus E_K(C_{i-2}) \oplus C_{i-1} \oplus E_K(C_{i-3}) \oplus C_{i-2} \oplus P_{i-3} \end{aligned}$$

For both modes it follows that swapping C_{i-1} and C_{i-2} will affect only the decryption P_{i-1} and P_{i-2} but not P_i nor any subsequent plaintext blocks assuming that all other ciphertext blocks are error-free. Similarly, swapping C_i and C_{i+k}

will only affect the decryption of $P_i \ldots, P_{i+k}$. Thus, in both cases there is no error propagation.

Consider the remaining mode (12), the IGE mode, which was suggested in [3] and which is the basis for the proposed ABC mode. Encryption

$$C_i = E_K(P_i \oplus C_{i-1}) \oplus P_{i-1}. \tag{14}$$

Decryption

$$P_i = D_K(C_i \oplus P_{i-1}) \oplus C_{i-1}. \tag{15}$$

It follows that the encryption and decryption operations are equivalent, which has implementational advantages. The mode can also be seen as a combination of the CBC encryption and decryption operations.

An error in one ciphertext block propagates to the corresponding plaintext block and all subsequent plaintext blocks. Let us next analyse whether an attacker can swap, insert or delete ciphertext blocks to avoid an error propagation.

$$\begin{aligned} P_i &= D_K(C_i \oplus P_{i-1}) \oplus C_{i-1} \\ &= D_K(C_i \oplus D_K(C_{i-1} \oplus P_{i-2}) \oplus C_{i-2}) \oplus C_{i-1} \\ &= D_K(C_i \oplus D_K(C_{i-1} \oplus D_K(C_{i-2} \oplus P_{i-3}) \oplus C_{i-3}) \oplus C_{i-2}) \oplus C_{i-1}. \end{aligned}$$

The difference between the last expression and the similar expressions for the modes (9) and (13) is that here each ciphertext block appears at two different levels in a nested expression of decryptions. Moreover, any two ciphertext blocks always appear at at least two different levels. Thus, it appears to be much more difficult to manipulate ciphertext blocks and at the same time having P_i decrypt correctly. Since the encryption and decryption modes are equivalent it follows that the ith ciphertext block is a function of a complicated, nested expression of encryptions of all plaintext blocks with indices $j \leq i$. We note that although this scheme seems to enable incorporation of message integrity along with encryption, it has been shown [6] that this is not achieved in a chosen-plaintext scenario.

Next let us consider a birthday attack similar to those of §2.4 and the encryption of P_i (14). If the plaintext blocks are chosen uniformly at random a match in two ciphertext blocks does not give the attacker any immediate useful information about the plaintext blocks. But it holds that

$$P_{i-1} \oplus C_i = P_{j-1} \oplus C_j \quad \Rightarrow \tag{16}$$
$$E_K(P_i \oplus C_{i-1}) = E_K(P_j \oplus C_{j-1}) \quad \Rightarrow \tag{17}$$
$$P_i \oplus P_j = C_{i-1} \oplus C_{j-1}. \tag{18}$$

Thus, if an attacker can determine that $P_{i-1} \oplus C_i = P_{j-1} \oplus C_j$, then he can immediately also determine $P_i \oplus P_j$. However, since this depends on a match between ciphertext and plaintext blocks, the condition for this information leakage of plaintext blocks is not verifiable. If the plaintexts are chosen uniformly at random the match cannot be verified and the birthday attack will not work assuming that the attacker operates in the ciphertext-only scenario.[1] In case of a redundant plaintext space however, an attacker might succeed by scanning the ciphertext for pairs of blocks for which both $C_i \oplus C_j$ and $C_{i-1} \oplus C_{j-1}$ have a likely value of the exclusive-or of two plaintext blocks. In any case, a match $P_{i-1} \oplus C_i = P_{j-1} \oplus C_j$ can be expected to occur with probability 2^{-n} and the probability of success is in the best

[1] In [6] it is considered to use the IGE mode for message integrity, which can be achieved by appending an extra "check"-block to the message before encryption. In this scenario it was shown that the scheme is secure against existential forgery attack in a ciphertext-only attack.

case that of Fact 1. Note that in the CBC mode equal ciphertext blocks lead to the information leakage of the plaintext blocks. Here one cannot from the ciphertext blocks alone determine whether the two matches have occurred and more work is required.

One attempt to complicate the above "attacks" is to exclusive-or of one or several previous plaintext and ciphertext blocks $P_{i-1}, P_{i-2}, \ldots$ and $C_{i-1}, C_{i-2}, \ldots$ in the encryption operation either to the input of the block cipher encryption or outside of it. However, in a ciphertext-only scenario an attacker is assumed to know the ciphertext blocks so adding more of these is not going to help. When the plaintext space is very redundant, e.g., consists of English text, the problems of the birthday attack can be minimised by adding several previous plaintext blocks $P_{i-1}, P_{i-2}, \ldots$ to the encryption function. This is discussed further in the next section.

3.1 Accumulated block chaining

With a redundant plaintext space information about the plaintext blocks start to leak after the encryption of about $2^{n/2}$ blocks, cf. birthday attacks like the ones of Fact 1.

As mentioned in the previous section one can minimise this problem by adding more plaintext blocks to the encryption functions. This can be done generally as follows. Define a series of "hash values" $H_i = P_i \oplus h(H_{i-1})$ where H_0 is an initial value, e.g., $H_0 = 0$, and where h is an (arbitrary) n to n bit mapping. Then if the output of h depends on (all of) its input, the value H_i holds an accumulated value of the first i plaintext blocks. Let us assume that $h(X) = X$ and defer further discussions on h till later. Let $P_i = g_K(C_i, \ldots, C_{i-v})$ be the decryption operation for a mode of operation with error recovery. Then we define the decryption operation for the accumulated block variant as follows

$$\begin{aligned} H_i &= g_K(C_i, \ldots, C_{i-v}) && (19) \\ P_i &= H_i \oplus h(H_{i-1}). && (20) \end{aligned}$$

Clearly the encryption function is well-defined for this scheme if the original encryption function is, as we shall illustrate very soon. The resulting scheme retains the error recovery property, since

$$\begin{aligned} P_i &= H_i \oplus h(H_{i-1}) && (21) \\ &= g_K(C_i, \ldots, C_{i-v}) \oplus h(g_K(C_{i-1}, \ldots, C_{i-v-1})). && (22) \end{aligned}$$

Thus, if the original scheme has error recovery after v blocks the accumulated block version has error recovery after $v+1$ blocks.

A similar approach can be applied to modes of operation with error propagation. Let us illustrate this method by applying it to the IGE mode (14), the result of which is what we call the ABC mode. The encryption operation in this case is

$$\begin{aligned} H_i &= P_i \oplus h(H_{i-1}) && (23) \\ C_i &= E_K(H_i \oplus C_{i-1}) \oplus H_{i-1}, && (24) \end{aligned}$$

where h is as above. The decryption function is

$$\begin{aligned} H_i &= D_K(C_i \oplus H_{i-1}) \oplus C_{i-1} && (25) \\ P_i &= H_i \oplus h(H_{i-1}). && (26) \end{aligned}$$

Before we discuss the implications of the birthday attack let us shortly define the probability distribution of sums of plaintext blocks.

Let $0, \ldots, 2^{n-1}$ be the possible values of one n-bit plaintext block, and let $\{p_i\}$ be the probability distribution on these, such that $p_i = \Pr(P^1 = i)$, where P^1 is a random variable representing one plaintext block. Let P^2 be a random variable representing the exclusive-or of two plaintext blocks, and let P^k be a random variable representing the exclusive-or of k plaintext blocks. Then the probability distribution of P^k is $\{p_i^{(k)}\}$, where

$$p_i^{(k)} = \Pr(P^k = i) = \sum_j p_j^{(k-1)} p_{j \oplus i}.$$

It follows that the distribution $\{p_i^{(k)}\}$ is less nonuniform for increasing values of k. More precisely, the distance from the uniform distribution $\sum_{i=0}^{2^n-1}(p_i^{(k)} - 1/2^n)^2$ does not increase for increasing k.

Let us next consider the birthday attack on the ABC mode. The condition for this attack is that the attacker can find blocks such that $P_{i-1} \oplus C_i = P_{j-1} \oplus C_j$. In case of a redundant plaintext space an attacker might be able to verify that this match has occurred, cf. earlier. Using the accumulated block technique an attacker must determine whether a match of the form $H_{i-1} \oplus C_i = H_{j-1} \oplus C_j$ has occurred. The point we want to make is that for a typical plaintext space, e.g. natural English, expressions of the form $P_i \oplus \cdots \oplus P_j$ will look random for increasing values of $j - i$. For the ABC mode it means that the required match in the birthday attack will be hard (or impossible) to determine.

Consider the CBC mode with the accumulated block operation. With h chosen as before, one gets $H_i = P_i \oplus H_{i-1}$ and $C_i = E_K(H_i \oplus C_{i-1})$. It follows that an attacker can still verify the condition of the birthday attack, which as before is a match in two ciphertext blocks, however what he obtains is the value of an exclusive-or sum of possibly many plaintext blocks. Let us assume that an attacker has found two matching ciphertext blocks, C_i and C_j, in the blocks resulting from one long plaintext consisting of $2^{(n+1)/2}$ blocks encrypted using the CBC mode with accumulated block chaining. Then the expected value[2] of $j - i$ is about $2^{(n+1)/2}/3$. Together with a block size of, say, $n = 64$ or larger, this would mean that the obtained expressions are useless to an attacker.

To illustrate this we computed the distribution of the 7-bit ASCII characters in the LaTeX representation of this document (or more correctly, the version prior to this version!). Then we computed the distance to the uniform distribution for P^k, more concretely, with the definition $d^k = \sum_{i=0}^{2^n-1}(p_i^{(k)} - 1/2^n)^2$, we computed and found $d^1 \simeq 0.04$, $d^2 \simeq 0.007$, $d^4 \simeq 10^{-3}$, $d^8 \simeq 10^{-4}$, $d^{16} \simeq 10^{-5}$, $d^{32} \simeq 10^{-8}$, and $d^{64} \simeq 10^{-14}$. For comparison we encrypted the text using the block cipher Serpent[2] in the ABC mode of operation, and computed the corresponding numbers. They were $d^1 \simeq 10^{-5}$ and $d^2 \simeq 10^{-9}$. This illustrates that the distribution of the exclusive-ors of k ASCII characters from this text very rapidly converges to the uniform distribution.

For typical English text this is supported by the following. It has been argued that a one-time pad scheme using as key the exclusive-or of four texts consisting of typical English characters appears to be unbreakable [11, Fact 7.59], which was also noted by Shannon [16].

[2] To see this, assume that there is one collision, $x_i = x_j$ in a collection of s random blocks, $x_1, \ldots, x_s$. Then the expected distance $j - i$ can be calculated as follows. Note that there are $S = \binom{s}{2}$ pairs of blocks, which are equally likely to be the pair in the collision. Also, there are $s - 1$ pairs of distance one, $s - 2$ pairs of distance 2, and $s - \ell$ pairs of distance ℓ. Thus, the expected distance of the blocks in the collision is $1/S \sum_{\ell=1}^{s-1} \ell(s - \ell) = (s+1)/3$.

3.1.1 On the choice of the function h

Note that since the function h is never inverted it can be chosen arbitrarily. However, we shall argue that choosing $h(X) = X$ or $h(X) = X^{<<1}$ is sufficient for most applications. In the latter case the input is bitwise rotated one position to the left. With h the identity function it was shown above that for the CBC mode a pair of matching ciphertext blocks enables an attacker to compute the exclusive-or sum of several plaintext blocks. With a "non-degenerate" plaintext space such a sum will give the attacker very little information. As an example of a "degenerate" plaintext space, consider the case where natural English is encoded in (standard) ASCII, then characters are likely bytes where the most significant bit in every byte is a zero bit. Therefore, in an exclusive-or sum of several plaintext blocks the most significant bits of all bytes will also be zero bits. This does not affect the probability of success of the birthday attack, but as illustrated in §2.4 using the CBC mode, a pair of matching ciphertext blocks, e.g., $C_i = C_j$, yields a correlation between the ciphertext blocks C_{i-1} and C_{j-1}. With this plaintext space one could choose $h(X) = X^{<<1}$. Then one gets $H_i = P_i \oplus (P_{i-1})^{<<1} \oplus (P_{i-2})^{<<2} \oplus \cdots \oplus (P_{i-s})^{<<s} \oplus \cdots$. Hence, H_i will not inherit the structure of the plaintext characters. In practical implementations an n-bit text is implemented as n/m m-bit words. In this case the one-bit rotation can be implemented as one-bit rotations for every m-bit word, i.e., if $X = X_1, \ldots, X_{n/m}$ then $h(X) = X_1^{<<1}, \ldots, X_{n/m}^{<<1}$.

As as final observation consider the decryption operation of the CBC mode with accumulated block chaining. One gets $P_i = D_K(C_i) \oplus C_{i-1} \oplus h(D_K(C_{i-1}) \oplus C_{i-2})$. With $h(X) = X$ it follows that an attacker can force the value $P_i = 0$ by choosing equal values for the blocks C_{i-2}, C_{i-1}, C_i. For the CBC mode (without accumulated block chaining), a similar approach would mean that the attacker forces P_i and P_{i-1} to the same but unknown value. Forcing $P_i = 0$ might be considered more serious than forcing $P_i = P_{i-1}$, however this advantage can be effectively eliminated by choosing $h(X) = X^{<<1}$.

3.2 Further variants

In this section we list some other possible modes of operation with error propagation, where we have restricted ourselves to modes where the encryption and decryption operations are equivalent. Consider first general encryption operation $C_i = f_K(P_i, P_{i-1}, C_{i-1})$ from §3. If we allow for using each input block more than once the following variant is possible.

$$C_i = E_K(P_i \oplus P_{i-1} \oplus C_{i-1}) \oplus P_{i-1} \oplus C_{i-1}, \tag{27}$$
$$P_i = D_K(C_i \oplus C_{i-1} \oplus P_{i-1}) \oplus C_{i-1} \oplus P_{i-1}. \tag{28}$$

If we further extend the model to encryption operations with additional plaintext and ciphertext blocks $C_i = f_K(P_i, P_{i-1}, P_{i-2}, C_{i-1}, C_{i-2})$, the following variant is possible.

$$C_i = E_K(P_i \oplus P_{i-1} \oplus C_{i-2}) \oplus P_{i-2} \oplus C_{i-1}, \tag{29}$$
$$P_i = D_K(C_i \oplus C_{i-1} \oplus P_{i-2}) \oplus C_{i-2} \oplus P_{i-1}. \tag{30}$$

These modes have properties similar to those of (12) and better diffusion properties in the case of a redundant plaintext space, and could be used instead of the accumulated block chaining technique of the ABC mode.

4 Related work

The mode of (9) is also known under the name of PCBC, see [11, 9.91][9, 12]. The mode of (12) was proposed as early as 1977 by Carl Campbell at the first National Bureau of Standards Conference on Computer Security and the Data Encryption Standard [3, 6]. Campbell referred to the mode as the "Infinite Garble Extension" mode, from which the name IGE was derived in [6]. In [6] the IGE mode is analysed in various security models.

5 Concluding remarks

In this paper modes of operation with block chaining were investigated. It was argued that there are scenarios where modes of operation with (infinite) error propagation have several advantages over modes of operation with error recovery and it is our opinion that the former have been somewhat overlooked in the past. Modes of operation with error propagation in general, and the Accumulated Block Chaining (ABC) mode of operation in particular are proposed for application for the DES and the Advanced Encryption Standard (AES).

Acknowledgments

The author wishes to thank Virgil Gligor, Håvard Raddum, Paul Van Oorschot and David Wagner for many helpful comments.

References

[1] ISO/IEC 10116. Information processing – modes of operation for an n-bit block cipher algorithm. ISO/IEC, 1991.

[2] R.J. Anderson, E. Biham, and L.R. Knudsen. SERPENT - a 128-bit block cipher. A candidate for the Advanced Encryption Standard. Documentation available at `http://www.ii.uib.no/ larsr/serpent`.

[3] C. Campbell. Design and specification of cryptographic capabilities. In D. Branstad, editor, *National Bureau of Standards Special Publications*, pages 54–66. U.S. Department of Commerce, February 1978.

[4] D. Coppersmith, D.B. Johnson, and S.M. Matyas. Triple DES cipher block chaining with output feedback masking. Technical Report RC 20591, IBM, October 1996. Presented at the rump session of CRYPTO'96.

[5] D.W. Davies and W.L. Price. *Security for Computer Networks*. John Wiley & Sons, 1989.

[6] V. D. Gligor and P. Donescu. On message integrity in symmetric encryption. September 26 2000. Draft document.

[7] C.S. Jutla. Encryption modes with almost free message integrity. Available at `http://eprint.iacr.org/2000/039`.

[8] L.R. Knudsen. *Block Ciphers – Analysis, Design and Applications*. PhD thesis, Aarhus University, Denmark, 1994.

[9] J. T. Kohl. The use of encryption in Kerberos for network authentication (invited). In Gilles Brassard, editor, *Advances in Cryptology - Crypto '89*, pages 35–43, Berlin, 1989. Springer-Verlag. Lecture Notes in Computer Science Volume 435.

[10] U. M. Maurer. New approaches to the design of self-synchronizing stream ciphers. In Donald W. Davies, editor, *Advances in Cryptology - EuroCrypt '91*, pages 458–471, Berlin, 1991. Springer-Verlag. Lecture Notes in Computer Science Volume 547.

[11] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1997.

[12] C. Meyer and Matyas. *A new direction in Computer Data Security*. John Wiley & Sons, 1982.

[13] National Bureau of Standards. Data encryption standard. Federal Information Processing Standard (FIPS), Publication 46, National Bureau of Standards, U.S. Department of Commerce, Washington D.C., January 1977.

[14] National Bureau of Standards. DES modes of operation. Federal Information Processing Standard (FIPS), Publication 81, National Bureau of Standards, U.S. Department of Commerce, Washington D.C., December 1980.

[15] National Institute of Standards and Technology. Advanced encryption algorithm (AES) development effort. `http://www.nist.gov/aes`.

[16] C.E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28:656–715, 1949.

A FIPS-81

In 1980 a list of four modes of operation for the DES was published [14]. These four modes can be used with any block cipher. In the following let $E_K(\cdot)$ be the permutation induced by using the block cipher E of block length n with the key K and let $P_1, P_2, ..., P_i, ...$ be the blocks of plaintexts to be encrypted. The four modes are

- **Electronic Code Book (ECB)** The native mode, where one block at a time is encrypted independently of the encryptions of other blocks. Encryption

  $$C_i = E_K(P_i)$$

  Decryption

  $$P_i = E_K(C_i)$$

- **Cipher Block Chaining (CBC)** The chaining mode, where the encryption of a block depends on the encryptions of previous blocks. Encryption

  $$C_i = E_K(P_i \oplus C_{i-1})$$

  Decryption

  $$P_i = D_K(C_i) \oplus C_{i-1}$$

  where C_0 is a chosen initial value.

- **Cipher Feedback (CFB)** The first stream mode, where one m-bit character at a time is encrypted. Encryption

  $$\begin{aligned} C_i &= P_i \oplus \mathrm{MSB}_m(E_K(X_i)) \\ X_{i+1} &= \mathrm{LSB}_{n-m}(X_i) \| C_i \end{aligned}$$

  Decryption

  $$\begin{aligned} P_i &= C_i \oplus \mathrm{MSB}_m(E_K(X_i)) \\ X_{i+1} &= \mathrm{LSB}_{n-m}(X_i) \| C_i \end{aligned}$$

  where X_1 is an initial value, $\|$ denotes concatenation of blocks, MSB_s and LSB_s denote the s most and least significant bits respectively. Here m can be any number between 1 and the block length of the cipher. If the plaintext consists of characters $m = 7$ or $m = 8$ is usually the well-chosen parameter.

  In the ISO-variant [1] of this scheme the encryption operation is defined $P_i = C_i \oplus \mathrm{MSB}_{\tilde{m}}(E_K(X_i))$, where $\tilde{m} \leq m$. This allows for encryption of blocks which has a length different from the length of the feed back variable.

- **Output Feedback (OFB)** The second stream mode, where the stream bits are not dependent on the previous plaintexts, i.e. only the stream bits are fed back, not the ciphertext as in CFB mode. Encryption

  $$\begin{aligned} C_i &= P_i \oplus \mathrm{MSB}_m(E_K(X_i)) \\ X_{i+1} &= \mathrm{LSB}_{n-m}(X_i) \| \mathrm{MSB}_m(E_K(X_i)) \end{aligned}$$

  Decryption

  $$\begin{aligned} P_i &= C_i \oplus \mathrm{MSB}_m(E_K(X_i)) \\ X_{i+1} &= \mathrm{LSB}_{n-m}(X_i) \| \mathrm{MSB}_m(E_K(X_i)) \end{aligned}$$

  where X_1 is an initial value.

In the ISO-variant [1] of this scheme the feed back operation is $X_{i+1} = E_K(X_i)$ which is more secure [11, page 232].