Error Propagation in Various Cipher Block Modes

Karel Burda,

Brno University of Technology, Brno, Czech Republic

Summary
In this paper, we examine the problem of error propagation in various cipher block modes. We analyze the modes which are used for link encryption devices, i.e. ECB, CBC, CFB, OFB and CRT modes. The dependence between input and output error probability of the modes is derived in the paper. The results obtained can be used to choose the block cipher and its mode or to find the threshold channel error probability.

Key words:
Error propagation, cipher block mode, error probability, block cipher.

1. Introduction

Encryption devices ensure the confidentiality of the information by transforming its readable record (plaintext *P*) into an unreadable form (cryptogram *C*). In the case of link encryption devices (Fig. 1), a continuous stream *P* of plaintext bits is transformed into a continuous stream *C* of cryptogram bits in the transmitter. This transformation is called encryption. In the receiver, the inversion transformation (the so-called decryption) is performed.

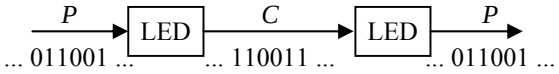

Fig. 1: Link encryption device (LED).

As a rule, the transmitter divides the continuous bit sequence *P* into blocks P_1, P_2, P_3..., which are transformed into cryptogram blocks C_1, C_2, C_3.... These blocks are sent as a continuous bit sequence to the receiver. The receiver divides the received sequence into primary blocks C_1, C_2, C_3 ... and subsequently decrypts them into the form of plaintext *P*. In this case, link encryption devices use a block cipher. The block cipher is an invertible function which assigns the blocks I_j the blocks O_j. The block length of I_j and O_j is *b* bits. This function is determined by a secret random parameter *K*, which is called the key. Formally, we write the encryption by the block cipher as $O_j = \mathrm{E}_K(I_j)$, where $j = 1, 2, 3$ ... is the ordinal number of the block. The inversion function D (i.e. decryption) is written as $I_j = \mathrm{D}_K(O_j)$.

Various types of cipher block modes are used for the encryption. The ECB, CBC, CFB, OFB and CTR [1] modes are used most frequently.

The ECB (Electronic Code Book) mode is described by the following equations, where (1) describes the encryption and (2) defines the decryption.

$$C_j = \mathrm{E}_K\left(P_j\right). \tag{1}$$

$$P_j = \mathrm{D}_K\left(C_j\right). \tag{2}$$

The CBC (Cipher Block Chaining) mode is given by the following equations, where (3) describes the encryption and (4) defines the decryption:

$$C_j = \mathrm{E}_K\left(P_j \oplus C_{j-1}\right), C_0 = IV\,, \tag{3}$$

$$P_j = \mathrm{D}_K\left(C_j\right) \oplus C_{j-1}, C_0 = IV\,, \tag{4}$$

where initialization vector *IV* is the defined block of *b* bits.

The CFB (Cipher Feedback) mode is a special mode, where segments are operated with. The segment is an *s*-bit block, where $1 \le s \le b$. The *j*-th plaintext segment or cryptogram segment is denoted $P^{\#}_j$ or $C^{\#}_j$. The CFB mode is described by the following equations, where (5) describes the encryption and (6) defines the decryption.

$$C^{\#}_j = P^{\#}_j \oplus \mathrm{MSB}_s\left(O_j\right), O_j = \mathrm{E}_K\left(I_j\right), \tag{5}$$

$$P^{\#}_j = C^{\#}_j \oplus \mathrm{MSB}_s\left(O_j\right), O_j = \mathrm{E}_K\left(I_j\right), \tag{6}$$

where $I_j = \begin{cases} IV, & j = 1, \\ \mathrm{LSB}_{b-s}\left(I_{j-1}\right) \,|\, C^{\#}_{j-1}, & j = 2,3\ldots, \end{cases}$

$\mathrm{MSB}_m(X)$ is a bit string consisting of *m* most significant bits of the bit string *X*, $\mathrm{LSB}_m(X)$ is a bit string consisting of *m* least significant bits of the bit string *X*, and $X\,|Y$ is the concatenation of two bit strings *X* and *Y*. By reason of simplicity, we suppose that $b/s = w$, where *w* is an integer.

The OFB (Output Feedback) mode is given by following equations, where (7) describes the encryption and (8) defines the decryption:

$$C_j = P_j \oplus O_j, O_j = \mathrm{E}_K\left(O_{j-1}\right), O_0 = IV\,. \tag{7}$$

$$P_j = C_j \oplus O_j, O_j = \mathrm{E}_K\left(O_{j-1}\right), O_0 = IV\,. \tag{8}$$

Manuscript received November 5, 2006.
Manuscript revised November 25, 2006.

The CTR (Counter) mode is described by the following equations, where (9) describes the encryption and (10) defines the decryption.

$$C_j = P_j \oplus O_j, O_j = \mathrm{E}_K(T_j), \quad (9)$$

$$P_j = C_j \oplus O_j, O_j = \mathrm{E}_K(T_j), \quad (10)$$

where T_j is the defined block of b bits.

A bit error is the substitution of a '0' bit for a '1' bit, or vice versa. These errors originate in the transmission channel as a consequence of interference and noise. We denote p_e the bit error probability in the channel. Then, the probability p_e is simultaneously the bit error probability in the cryptogram. Errors in the cryptogram produce errors in the decrypted plaintext. This phenomenon is called error propagation. We denote P_e the bit error probability in the decrypted plaintext. The probabilities p_e and P_e will, for brevity, be referred to as input and output error probabilities, respectively.

The effect of the error bit $c_{i,j}$ or $c^{\#}_{i,j}$ in the block $C_j = (c_{1,j}, c_{2,j}, ..., c_{b,j})$ or $C^{\#}_j = (c^{\#}_{1,j}, c^{\#}_{2,j}, ..., c^{\#}_{s,j})$ on the appearance of errors in the plaintext for individual modes is summarised in the following Table (in accordance with [1]).

Table 1: The effect of bit errors for cipher block modes

Mode	**Effect of Bit Errors in C_j or $C^{\#}_j$**
ECB	RBE in P_j
CBC	RBE in P_j SBE in P_{j+1}
CFB	SBE in $P^{\#}_j$ RBE in $P^{\#}_{j+1}, P^{\#}_{j+2}, ... P^{\#}_{j+w}$
OFB	SBE in P_j
CTR	SBE in P_j

In the Table, SBE (specific bit errors) means that an individual error bit $c_{i,j}$ or $c^{\#}_{i,j}$ produces in the appropriate plaintext block $P_j = (p_{1,j}, p_{2,j}, ..., p_{b,j})$ or $P^{\#}_j = (p^{\#}_{1,j}, p^{\#}_{2,j}, ..., p^{\#}_{s,j})$ an individual error bit $p_{i,j}$ or $p^{\#}_{i,j}$. In other words, bit errors in the plaintext occur in the same bit positions as the bit errors in the cryptogram.

The abbreviation RBE (random bit errors) means that an individual error bit $c_{i,j}$ or $c^{\#}_{i,j}$ affects randomly all bits in the plaintext block P_j or in the segments $P^{\#}_{j+1}, P^{\#}_{j+2}, ... P^{\#}_{j+w}$. In this case, each bit from P_j or $P^{\#}_{j+1}, P^{\#}_{j+2}, ... P^{\#}_{j+w}$ is correct with probability 1/2 or incorrect with the same probability.

In OFB and CTR modes only the SBE type of error propagation can occur. For these modes, each error bit $c_{i,j}$ of the cryptogram causes only one incorrect bit $p_{i,j}$ of the plaintext and thus the output error probability P_e is the same as the input error probability:

$$P_e = p_e. \quad (11)$$

In the case of the other modes (i.e. ECB, CBC and CFB), the RBE type of error appears, which causes that the number of errors in the plaintext is greater than the number of errors in the cryptogram. Thus, it holds in these modes that $P_e > p_e$, whereas a high value of output error probability P_e can disable any information transmission. The effect of error propagation is well known and explained (e.g. in [2] or [3]) but no exact dependence of the output error probability P_e on the input error probability p_e for ECB, CBC and CFB modes has come to be known. The knowledge of this dependence can be useful for the choice of the block cipher or for the choice of the channel from the viewpoint of its error probability. Deriving the above dependence is the aim of this paper.

2. Model

In the following derivation, we assume a binary symmetric channel with the bit error probability $p_e \in \langle 0, 1/2 \rangle$. In this case, the probability $P(x)$ that there are x error bits out of b received bits, is given by the formula:

$$P(x) = \binom{b}{x} \cdot p_e^x \cdot (1 - p_e)^{b-x}, x = 0,1,2,\ldots,b. \quad (12)$$

Then, it holds for the probability P_0, that b bits are correct:

$$P_0 = (1 - p_e)^b, \quad (13)$$

and for the probability Q_0, that at least one bit is incorrect:

$$Q_0 = 1 - P_0 = 1 - (1 - p_e)^b. \quad (14)$$

We call P_0 the correct block probability and Q_0 the incorrect block probability.

We assume that the encryption/decryption by the block cipher is a pseudorandom function, i.e. any modification of the input block causes random changes of all bits in the output block. The probability P_h that the output bit changes its value as a consequence of modifying the input block is called the bit inversion probability. We assume that P_h = 1/2. In the end, we assume that the transmitter and receiver operate synchronously, the transmission is without any bit slips and possible blocks IV or T_j are correct at both ends of the communication.

At first, we will solve the output error probability for the ECB mode. In this mode, $P_j = \mathrm{D}_K(C_j)$. Therefore, the bit p_{ij} is incorrect only in the case when the block C_j is incorrect and simultaneously the bit p_{ij} is inverted. The incorrect block probability is Q_0 and the bit inversion probability is P_h. Then, the output error probability P_e is equal to:

$$P_e = P_h \cdot Q_0 = \frac{1}{2} \cdot \left[1 - (1 - p_e)^b\right] \quad (15)$$

In the CBC mode, $P_j = U_j \oplus C_{j-1}$, where $U_j = D_K(C_j)$. The bit p_{ij} is incorrect in the following cases:

a) the bit $c_{i,(j-1)}$ is incorrect and the block C_j is correct,
b) the bit $c_{i,(j-1)}$ is incorrect, the block C_j is incorrect and the bit $u_{i,j}$ is not inverted,
c) the bit $c_{i,(j-1)}$ is correct but the block C_j is incorrect and the bit $u_{i,j}$ is inverted.

The probability of the error bit $c_{i,(j-1)}$ is equal to p_e and the probability of the correct block C_j is P_0. Thus, the situation a) occurs with the probability $P_{a)} = p_e \cdot P_0$. The probability of the incorrect block C_j is equal to Q_0 and the probability that the bit $u_{i,j}$ is not inverted, amounts to $(1\text{-}P_h)$. Then, the probability of the situation b) is equal to the quantity $P_{b)} = p_e \cdot Q_0 \cdot (1\text{-}P_h)$. The probability of the correct bit $c_{i,(j-1)}$ is equal to the value $(1\text{-}p_e)$, the probability of the incorrect block C_j is equal to Q_0 and the probability that the bit $u_{i,j}$ is inverted, amounts to P_h. Then, the probability of the situation c) is equal to the quantity $P_{c)} = (1\text{-}p_e) \cdot P_h \cdot Q_0$. Thus the resultant output error probability P_e for the CBC mode is given by this equation:

$$P_e = P_{a)} + P_{b)} + P_{c)} = p_e \cdot P_0 + \frac{1}{2} \cdot Q_0 = \\ = p_e \cdot (1 - p_e)^b + \frac{1}{2} \cdot \left[1 - (1 - p_e)^b\right]. \quad (16)$$

The CFB mode decryption is defined by specification (6). In this case, the bit p_{ij} is incorrect in the following situations:

a) the bit $c^{\#}_{i,j}$ is incorrect and the block I_j is correct,
b) the bit $c^{\#}_{i,j}$ is incorrect, the block I_j is incorrect and the bit $o_{i,j}$ is not inverted,
c) the bit $c^{\#}_{i,j}$ is correct, the block I_j is incorrect and the bit $o_{i,j}$ is inverted.

The probability of the incorrect bit $c^{\#}_{i,j}$ is equal to p_e and the probability of the correct block I_j (i.e. b correct previous bits of the cryptogram) amounts to P_0. Thus the situation a) occurs with the probability $P_{a)} = p_e \cdot P_0$. The probability of the incorrect block I_j is equal to Q_0 and the probability that the bit $o_{i,j}$ is not inverted, amounts to $(1\text{-}P_h)$. Then, the probability of the situation b) is equal to the quantity $P_{b)} = p_e \cdot Q_0 \cdot (1\text{-}P_h)$. The probability of the correct bit $c^{\#}_{i,j}$ is equal to the quantity $(1\text{-}p_e)$, the probability of the incorrect block I_j is equal to Q_0 and the probability of the non-inverted bit $o_{i,j}$ amounts to P_h. Then, the probability of the situation c) is equal to the quantity $P_{c)} = (1\text{-}p_e) \cdot P_h \cdot Q_0$. Consequently, the overall output error probability P_e is equal to:

$$P_e = P_{a)} + P_{b)} + P_{c)} = p_e \cdot P_0 + \frac{1}{2} \cdot Q_0 = \\ = p_e \cdot (1 - p_e)^b + \frac{1}{2} \cdot \left[1 - (1 - p_e)^b\right]. \quad (17)$$

We can see that equations (16) and (17) are the same. It follows that the output error probability P_e is the same for both of the modes. Thus the CBC and CFB modes are equivalent from the viewpoint of error propagation. From equality (17), it is also evident that the output error probability of the CFB mode does not depend on the length s of segments.

3. Discussion

The dependence of the output error probability P_e on the input error probability p_e of the CBC and CFB modes for the block lengths b = 64, 128 and 256 bits is depicted in Fig. 2. It is evident from this figure that the output error probability grows with increasing length of blocks.

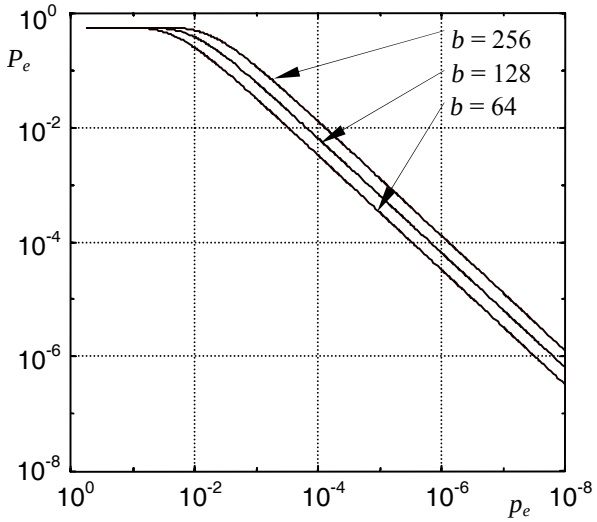

Fig. 2: The dependence of the output error probability P_e on the input error probability p_e of the CBC and CFB modes for the block lengths b = 64, 128 and 256 bits.

The dependence of the output error probability P_e on the input error probability p_e for all modes discussed (i.e. for ECB, CBC, CFB and CTR modes) is depicted in Fig. 3. The block length b amounts to 128 bits in this case. It follows from the Figure that the OFB and CTR modes are optimal from the viewpoint of error propagation. The worst modes are the CBC and CFB modes. The ECB mode is slightly better than the last mentioned modes (by the value $p_e \cdot P_0$) but this improvement is practically negligible for large block lengths b.

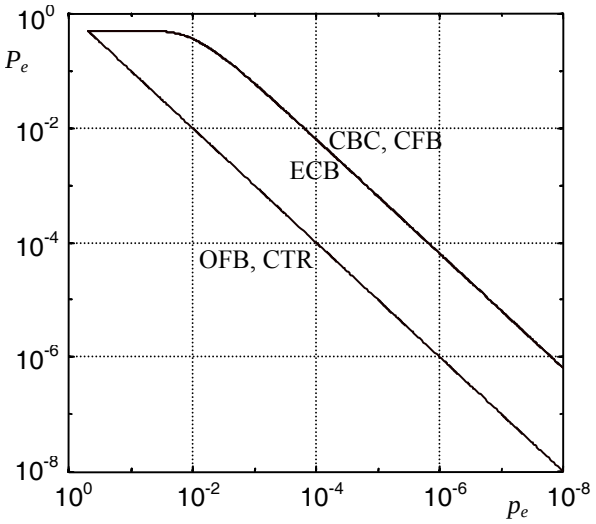

Fig. 3: The dependence of the output error probability P_e on the input error probability p_e of the ECB, CBC, CFB and CTR modes for the block length b = 128 bits.

The dependence of the error propagation ratio R_e on the input error probability p_e of the CBC and CFB modes for the block lengths b = 64, 128 and 256 bits is depicted in Fig. 4.

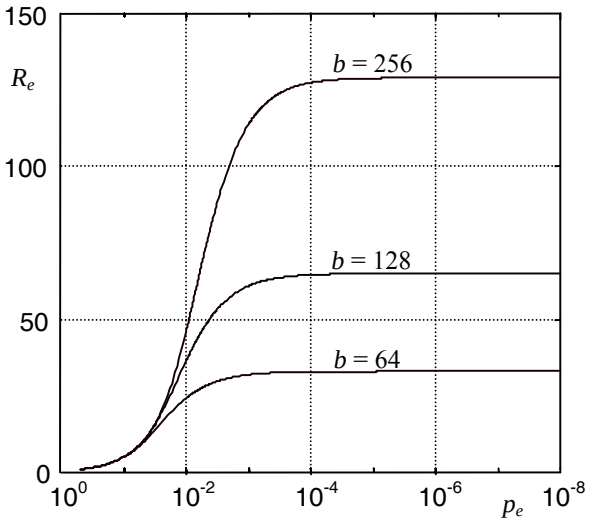

Fig. 4: The dependence of the error propagation ratio R_e on the input error probability p_e of the CBC and CFB modes for the block lengths b = 64, 128 and 256 bits.

We express the measure of error propagation by the ratio of the output to input error probability. This error propagation ratio R_e is given by:

$$R_e = \frac{P_e}{p_e}. \tag{18}$$

It is evident from this Figure that the error propagation rate is always equal to 1 for p_e = 1/2. On the contrary, the error propagation rate R_e approaches the limit value (1+b/2) for $p_e \to 0$. It follows from this dependence that the output error probability P_e increases with increasing block length b.

The dependence of the error propagation rate R_e on the input error probability p_e for all the modes discussed (i.e. for ECB, CBC, CFB, OFB and CTR modes) and for the block length b = 128 bits is depicted in Fig. 5. We can see that the lowest value of R_e (i.e. 1) is for the OFB and CTR modes. This value is a constant and does not depend on the input error probability p_e. The error propagation rate R_e of the ECB mode is slightly lower than R_e of the CBC and CFB modes and the limit value of this rate is equal to b/2 for $p_e \to 0$.

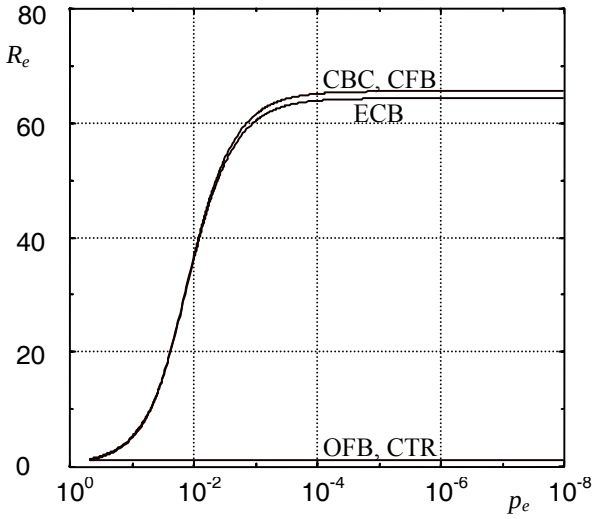

Fig. 5: The dependence of the error propagation rate R_e on the input error probability p_e of the ECB, CBC, CFB and CTR modes for the block length b = 128 bits.

4. Conclusions

In this paper, the output error probability P_e for the ECB, CBC, CFB, OFB and CTR modes is examined. The dependence P_e on the input error probability p_e is derived for all the modes discussed. The output error probability P_e can be also expressed by the formula $P_e = R_e \cdot p_e$, where R_e is the error propagation rate. The error propagation rate R_e = 1 for the OFB and CTR modes. For $p_e \to 0$, the error propagation rate R_e approaches the value (1+b/2) for the CBC and CFB modes and the value (b/2) for the ECB mode. The results obtained can be used to choose the block cipher and its mode or to find the threshold channel error probability.

References

[1] Dworkin, M.: Recommendation for block cipher modes of operation. [NIST Special Publication 800-38A]. National Institute of Standards and Technology, Gaithersburg 2001.
[2] Schneier, B.: Applied cryptography. John Wiley & Sons, New York 1996.
[3] Menezes, A. J. - Oorschot, P. C. - Vanstone S. A.: Handbook of applied cryptography. CRC Press, Boca Raton 1997.

Karel Burda received the M.S. and Ph.D. degrees in Electrical Engineering from the Liptovsky Mikulas Military Academy in 1981 and 1988, respectively. During 1988-2004, he was a lecturer at two military academies. At present, he lectures at Brno University of Technology. His current research interests include the security of information systems and cryptology.