Building a block cipher mode of operation with feedback keys

Yi-Li Huang, Fang-Yie Leu, Jung-Chun Liu, Jing-Hao Yang, Chih-Wei Yu, Cheng-Chung Chu, Chao-Tung Yang
Department of Computer Science, TungHai University, Taichung ,Taiwan
{yifung, leufy, jcliu, g01350036, g99357009, cchu, ctyang}@thu.edu.tw

Abstract**—**In this paper, we propose two block cipher modes of operation (BCMO for short), named the Key Stream Protection Chain mode (KSPC for short) and Output Dual Chaining mode (ODC for short), which differ from other existing BCMOs in that in the KSPC, the ciphertext block and in the ODC, the block cipher encryption unit's output are fed back to the encryption system to be one of the inputs of the next block ciphering. We also evaluate three existing BCMOs, including the Cipher Block Chaining mode (CBC), the Propagating Cipher Block Chaining mode (PCBC) and the Output Feedback mode (OFB), and discuss the security of the these modes when they face chosen-plaintext attacks. At last, we explain why our new BCMOs' security levels are higher than those of the existing three.

Keywords**—***Cipher Block Chaining mode, Propagating Cipher Block Chaining mode, Output Feedback mode, Key Stream Protection Chain mode, OutputDual Chaining mode, Block Cipher modes of Operation, chosen-plaintext attack*

I. INTRODUCTION

Currently, some existing block cipher systems, like Data Encryption Standard (DES), Triple Data Encryption Algorithm (3DES) and Advanced Encryption Standard (AES), encrypt their data with fixed length keys, e.g., L bits long, at a time. If the plaintext is longer than L, before the encryption, it has to be divided into blocks. Each is L in length. The most serious problem of these block cipher systems is that if the key is not changed, the same plaintext block will produce the same ciphertext block. Using the BCMOs will solve this problem and upgrade the block cipher systems' security levels [1].

In the Cryptography, some BCMOs purposed by National Institute of Standards and Technology (NIST), e.g., the Cipher Block Chaining mode (CBC), the Propagating Cipher Block Chaining mode (PCBC) and the Output Feedback mode (OFB), have been widely used to cipher plaintext blocks [2]. Nowadays, different types of attacks on these BCMOs have been developed [3], meaning that the BCMOs have their own security problems. Therefore, in this paper, we purpose two BCMOs, named Key Stream Protection Chain mode (KSPC for short) and Output Dual Chaining mode (ODC for short), to solve these problems. Generally, the KSPC's ciphertext block and the output of the ODC's block cipher encryption unit as individually one of the inputs of the next block ciphering are fed back to the encryption system to increase the encryption complexity of the proposed systems.

The rest of this paper is organized as follows. Section 2 introduces three standard BCMOs proposed by NIST. The CBC, the PCBC, the OFB and our proposed KSPC and ODC are presented in Section 3. Section 4 analyzes the security of these modes and discusses how to use our BCMOs to resist chosen-plaintext attacks. Section 5 concludes this paper.

II. BLOCK CIPHER MODES OF OPERATION

The parameters used by the CBC, PCBC and OFB are defined below.

P_i : The i^{th} plaintext block to be encrypted, $1 \le i \le n$.
C_i : The i^{th} ciphertext block, $1 \le i \le n$.
Block Cipher Encryption (BCE) unit: According to [2], the standard BCE units are AES-128, AES-192, and AES-256. The function of a BCE unit is denoted by $E_K(I_P)$, in which the key K and the input I_p are used to encrypt a given plaintext block.
K: The block cipher key [2].
O_i: The output block produced by $E_K(I_P)$, $1 \le i \le n$.
IV: Initialization Vector (IV for short), a random number input to the CBC, PCBC and OFB since each of them needs an additional initial parameter.

A. Cipher Block Chaining (CBC)

In the encryption process of the CBC, a plaintext block P_i as shown in Fig. 1 is XORed with IV or previous ciphertext block C_{i-1}beforeit is input to $E_K(C_{i-1})$.The encryption process can be formulated as follows.

$$C_1 = E_K(P_1 \oplus IV) \tag{1}$$

$$C_i = E_K(P_i \oplus C_{i-1}),\ 2 \le i \le n \tag{2}$$

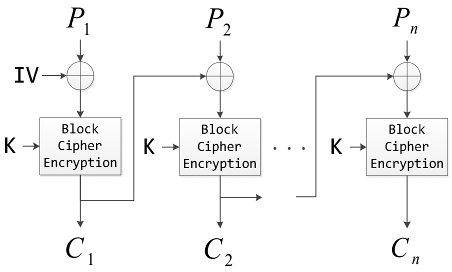

Fig.1 The CBC mode encryption

B. Propagating Cipher Block Chaining (PCBC)

As show in Fig. 2, the general rule of the PCBC's block encryption is that $P_1$is first XORed with IV. The XORed result is then input to the BCE unit to generate C_1.After that, $P_i \oplus C_i$ substitutes IV to XOR with P_{i+1}.The XORed result is then input to BCE unit to generate C_{i+1}, where $1 \le i < n$. The process can be formulated as follows.

$$C_1 = E_K(P_1 \oplus IV) \tag{3}$$

$$C_i = E_K(P_i \oplus P_{i-1} \oplus C_{i-1}) , 2 \le i \le n \tag{4}$$

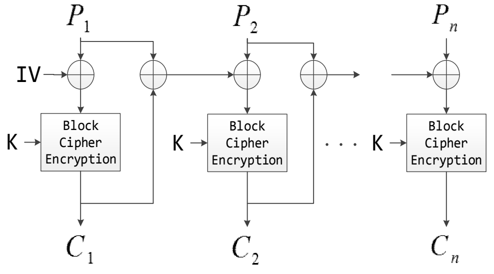

Fig. 2 The PCBC mode encryption

C. Output Feedback(OFB)

The general rule of the OFB as shown in Fig. 3 is that $E_K(C_{i-1})$ receives C_{i-1} and K as its parameters to generate O_i, which is then XORed with P_i to produce C_i, $1 \le i \le n$, where C_0 = IV. The formulas utilized to encrypt plaintext blocks of the OFB are as follows.

$$C_1 = P_1 \oplus E_K(IV) = P_1 \oplus O_1 \tag{5}$$

$$C_i = P_i \oplus E_K(O_{i-1}) = P_i \oplus O_i , 2 \le i \le n \tag{6}$$

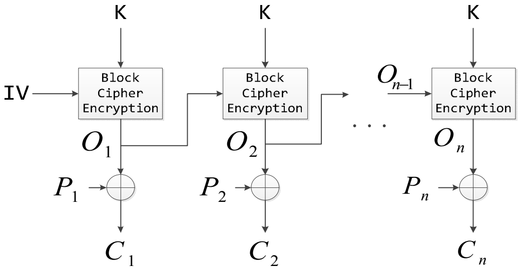

Fig. 3 The OFB mode encryption

III. THE KSPC AND ODC

In this section, we introduce the structures of the two purposed BCMOs, and describe how to use those modes to encrypt and decrypt plaintext blocks. First, we define some parameters which have not been defined above.

$D_K(I_P)$: Function of block decipher, in which the key K and an input I_P are used to decrypt a plaintext block from the corresponding ciphertext block.

$+_2$: A binary adder, which is a logical operator defined in [4].

$-_2$: The Inverse operation of $+_2$.

A. Key Stream Protection Chain (KSPC)

With the KSPC shown in Fig. 4, K is XORed with C_{i-1},$1 \le i \le n$, where C_0 = IV. The XORed result is then input to the BCE unit to encrypt P_i. One of the advantages of this mode is that every BCE unit's encryption keys are different from others when encrypting different plaintext blocks. The formulas of the KSPC are as follows.

$$C_1 = E_{K \oplus IV}(P_1) \tag{7}$$

$$C_i = E_{K \oplus C_{i-1}}(P_i) , 2 \le i \le n \tag{8}$$

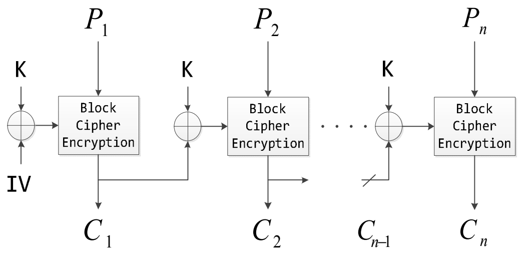

Fig. 4 The KSPC mode encryption

The decryption process as shown in Fig. 5 can be formulated as follows.

$$P_1 = D_{K \oplus IV}(C_1) \tag{9}$$

$$P_i = D_{K \oplus C_{i-1}}(C_i) , 2 \le i \le n \tag{10}$$

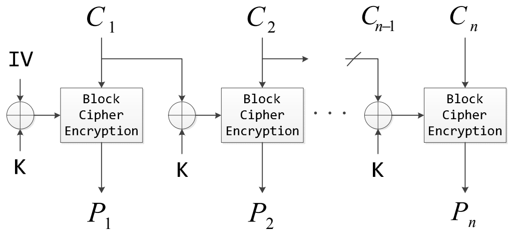

Fig. 5 The KSPC mode decryption

B. Output Dual Chaining mode (ODC)

As shown in Fig. 6, the general rule of ODC is that P_1 and K are input to the BCE unit to generate O_1, which is then binary-added with $K \oplus IV$ to generate C_1. After that, $O_1$is XORed with P_2, and the XORed result and K are input to the BCE unit to generate O_2. O_2 is then binary-added with O_1 to generate C_2. The formulas are as follows.

$$C_1 = E_K(P_1) +_2 (K \oplus IV) = O_1 +_2 (K \oplus IV) \tag{11}$$

$$C_i = E_K(O_{i-1} \oplus P_i) +_2 O_{i-1} = O_i +_2 O_{i-1} , 2 \le i \le n \tag{12}$$

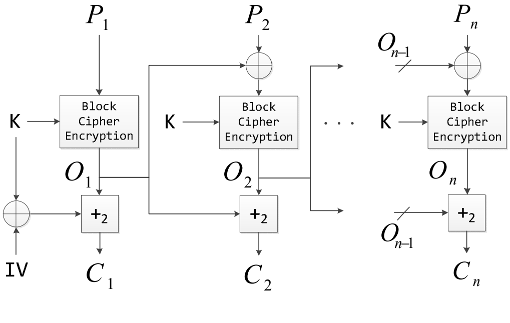

Fig. 6 The ODC mode encryption

In the decryption process of the ODC, to decrypt C_i as shown in Fig. 7, one needs O_{i-1} to calculate O_i because $O_i = C_i -_2 O_{i-1}$. After that, O_i and K are input to BCE unit. The output is then XORed with O_{i-1} to recover P_i, $1 \leq i \leq n$, where $O_0 = K \oplus IV$. P_i can be obtained by invoking the following formulas.

$$P_1 = D_K[C_1 -_2 (K \oplus IV)] = D_K(O_1) \quad (13)$$

$$P_i = D_K(C_i -_2 O_{i-1}) \oplus O_{i-1} = D_K(O_i) \oplus O_{i-1}, 2 \leq i \leq n \quad (14)$$

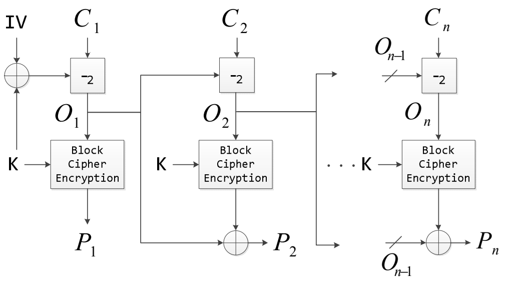

Fig. 7 The ODC mode decryption

IV. Security Analyses

The three abovementioned BCMOs, including the CBC, PCBC and OFB, have their own security risk. In fact, they do not effectively improve the security level of a block cipher. Nevertheless, if a block cipher technique is cracked, its BCE unit can also be reused by our BCMOs to reliably protect a security system. We analyze the security of the three existing BCMOs and our BCMOs in the following when each of them faces the chosen-plaintext attacks.

A. Security in the CBC

In the CBC mode, a hacker can first input n different plaintext blocks, denoted by $P = \{P_1, P_2, \ldots, P_n\}$, to obtain the corresponding ciphertext blocks $C = \{C_1, C_2, \ldots, C_n\}$. After that, the hacker can calculate the BCE unit's input, i.e., C_{i-1}□P_i (see in Fig. 1), and collect< $C_{i-1} \oplus P_i, C_i$> pairs to analyze the BCE unit's key K if n is huge.

B. Security in the PCBC

To launch a chosen-plaintext attack, the hackers can choose plaintext $P = \{P_1, P_2, \ldots, P_n\}$and input them to the BCE unit to acquire ciphertext $C = \{C_1, C_2, \ldots, C_n\}$. According to Fig. 2,they can generate a set of BCE unit's input blocks I_P = {IV, P_1□C_1, P_2□C_2, …, P_{n-1}□C_{n-1}},and then collect a huge number of <$P_{i-1} \oplus C_{i-1}, C_i$> pairs to solve K, where P_i is the i^{th} block of P and C_i is the i^{th} block of C, $1 \leq i \leq n$, and $IV = P_0 \oplus C_0$. When K is solved, the underlying system is no longer secure.

C. Security in the OFB

For the OFB, we analyze its security based on two cases, i.e., the IV can and cannot be chosen by the users/hackers.

1) An attack on IV that can be chosen: If IV can be chosen,hackers can input an IV the same as the one selected by the normal userto the BCE unit to acquire O_1. As shown in Fig. 3, the output block $O_i$is only determined by K or O_{i-1}, where $1 \leq i \leq n$. Then the hackers can collect a set of output blocks$O = \{O_1, O_2, \ldots, O_n\}$ corresponding to this IV, and then acquirethe user's plaintext block P_i from an illegally intercepted C_i since $P_i = C_i \oplus O_i$ without requiring to break the key K of the BCE unit.

2) Attack on IV that cannot be chosen: If IV cannot to be chosen, the security level of the OFB will be higher.But it has a security problem on chosen-plaintext attack. The hackers can first input n plaintext blocks, denoted by $P = \{P_1, P_2, \ldots, P_n\}$, to acquire ciphertext blocks $C = \{C_1, C_2, \ldots, C_n\}$. After that, they can calculate a set of output blocks $O = \{O_1, O_2, \ldots, O_n\}$, since $O_i = P_i \oplus C_i, 1 \leq i \leq n$, and collect a huge number of <O_{i-1}, O_i> pairs to analyze the key K of the BCE unit. After that, its security level will be low.

D. Security in KSPC

In the KSPC, the BCE unit's key changes for each P_i, i=1,2,…n. So if hackers choose their own plaintext P to acquire ciphertext C, K is still hard to be analyzed because C_i varies when i is different. But the serious problem is that if IV can be controlled by the hacker, as shown in Fig. 4,they can select a fixed IV and input many different plaintext blocks, e.g., P_1, to acquire their ciphertext block $C_1$and collect a huge number of different <P_1, C_1> pairs to analyze IV ⊕ K. Therefore, we design the ODC mode to solve this problem.

E. Security in ODC

Fig. 6 shows the ODC mode Encryption, no matter whether IV can be chosen or not, if the hackers wish to analyze the block cipher encryption component of the ODC, they need to collect a set of BCE unit's outputs $O = \{O_1, O_2, \ldots, O_n\}$ to acquire a huge number of <$P_i \oplus O_{i-1}, O_i$> pairs, where $1 \leq i \leq n$. Even a large number of chosen plaintext blocks is used to collect ciphertext blocks, the BCE unit's output O_i is protected by $K \oplus IV$ when i = 0 or by $O_{i-1}$when i > 1.

V. ConclusionS

In this paper, we describe some standard BCMOs, and try to crack these modes by chosen-plaintext attacks. In fact, these modes in common have their security drawbacks, through which their BCE unit's data can be easily collected. We improve this by generating key stream and by protecting the output of the block cipher encryption component to achieve the goal of strengthening block ciphering.

In the future, we would like to increase the difficulty of collecting block cipher's data to avoid the hackers from analyzing the keys, and purpose other BCMOs with the security the same as or higher than those of the KSPC and ODC mode.

Acknowledgements: This research was partially supported by TungHai University on GREENs project, and National Science Council, Taiwan, grants NSC 100-2221-E-029-018 and 101-2221-E-029-003-MY3.

REFERENCES

[1] W. Stallings, Cryptography and Network Security: Principles and Practice, Fifth Edition, Publisher: Prentice Hall, January, 2010.

[2] National Institute of Standards and Technology, NIST Special Publication 800-38A, Recommendation for Block Cipher Modes of Operation Methods and Techniques, December, 2001.

[3] H. Hudde, "Building Stream Ciphers from Block Ciphers and their Security," Seminararbeit Ruhr-Universität Bochum, February, 2009. http://imperia.rz.rub.de:9085/imperia/md/content/seminare/itsws08_09/hudde.pdf

[4] Y.F. Huang, F.Y. Leu, C.H. Chiu and I.L. Lin, "Improving Security Levels of IEEE802.16e Authentication by Involving Diffie-Hellman PKDS," Journal of Universal Computer Science, vol. 17, no.6, March 2011, pp. 891-911.