THE UNIFIED OPERATION STRUCTURE FOR SYMMETRIC-KEY ALGORITHM

Kuo-Tsang Huang[1] , Sung-Shiou Shen[2] and Jung-Hui Chiu[1]

[1]Department of Electrical Engineering, Chang Gung University, Tao-Yuan, Taiwan
d9221006@gmail.com
[2]DE LIN Institute of Technology, New Taipei City, Taiwan
shen@dlit.edu.tw

ABSTRACT

In Cloud Computing, information exchange frequently via the Internet and on-demand. Modern Internet protocols support several modes of operation to keep up with varied environments and provide the variant choice, such as SSL and IPSec support multi-mode. The different mode has the different characters. For example: CFB/OFB can be design operating without padding with bit size keystream output, CBC/CFB can self synchronize to avoid channel noise, and CFB/OFB needs encryption module only. The main emphasis is placed on the problem of case by case operation mode usage. We describe a structure for the analysis of the block operation mode combination. This unified operation structure, called UOS, combines existing in common and popular block modes of operation. UOS does multi-mode of operation with most existing popular symmetric block ciphers and do not only consist of encryption mode such as ECB, CBC, CFB and OFB, that provides confidentiality but also message authentication mode such as CBC-MAC in cryptography. It provides low-resource hardware implementation, which is proper to ubiquitous computing devices such as a sensor mote or an RFID tag. Our contribution provides a common solution for multi-mode and this is very suitable for ubiquitous computing with several resources and environments. The study indicates a better well-organized structure for symmetric block ciphers so as to improve their application scenarios.

KEYWORDS

Block Cipher, Mode of Operation, Ubiquitous, Low-Resource

1. INTRODUCTION

Symmetric-key algorithms are a class of algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. Symmetric-key encryption can use either stream ciphers or block ciphers. Block ciphers take a number of bits and encrypt them as a single unit, padding the plaintext so that it is a multiple of the block size. Blocks of 64 bits have been commonly used. The Advanced Encryption Standard (AES) algorithm approved by NIST in December 2001 uses 128-bit blocks. Many modern block ciphers have invertible functions from other functions that are themselves not invertible.

The traditional block ciphers have plaintext-ciphertext pair problem with the disadvantage of limit block region scramble. Cipher mode of operation extends the limit region and scramble to the after plaintext message. The standard modes of operation described in the literature, such as non-feedback electronic codebook (ECB) mode, cipher block chaining (CBC) mode, output feedback (OFB) mode, and cipher feedback (CFB) mode provide confidentiality. How to choose an appropriate operation mode? The different mode has the different characters. For example:

Sundarapandian et al. (Eds): CoNeCo,WiMo, NLP, CRYPSIS, ICAIT, ICDIP, ITCSE, CS & IT 07,
pp. 399–412, 2012. © CS & IT-CSCP 2012 DOI : 10.5121/csit.2012.2439

CFB/OFB can be design operating without padding with bit-based size keystream output, CBC/CFB can self sync to avoid channel noise error propagation, and CFB/OFB encryption and decryption applications need an encryption module only to reach both usages. In addition, only the forward cipher function of the block cipher algorithm is used in both encryption and decryption operations, without the need for the inverse cipher function.

A striking example of the degree to which ECB can leave plaintext data patterns in the ciphertext can be seen when ECB mode is used to encrypt a bitmap image which uses large areas of uniform colour. While the colour of each individual pixel is encrypted, the overall image may still be discerned as the pattern of identically-coloured pixels in the original remains in the encrypted version. Block cipher modes of encryption beside ECB have been suggested to remedy these drawbacks.

Modern protocols support several operation modes and ciphers to provide the variant choice. For example SSL and IPSec support multi-cipher and multi-mode [1][2][3].

2. RELATED WORKS

In cryptography, modes of operation is the procedure of enabling the repeated and secure use of a block cipher under a single key. A block cipher by itself allows encryption only of a single data block of the cipher's block length. When targeting a variable-length message, the data must first be partitioned into separate cipher blocks. Typically, the last block must also be extended to match the cipher's block length using a suitable padding scheme. A mode of operation describes the process of encrypting each of these blocks, and generally uses randomization based on an additional input value, often called an initialization vector, to allow doing so safely [4][5].

In the recent research called multi-mode, it cascades operations with the same data block[6] or in the same session [7]. The related works about Multi-mode and Multi-cipher, we explore Crypto-coprocessors and Multi-cipher cryptosystem [8][9][10][11]. Multi-cipher and multi-mode cryptosystems are widely used for hardware acceleration in modern security protocols, such as SSL and IPsec. NOP-cycle-padding algorithm (NCPA) [11] is one of those reconfigurable cryptosystems used for hardware acceleration. NOP-cycle-padding algorithm (NCPA) which enables crypto-coprocessors reconfigured with diverse encrypting bursts to be pipeline scheduled.

Crypto-coprocessor like CryptoManiac (CM) [8] processor is a flexible crypto-coprocessor which supports multiple cipher algorithms and multi-mode operations. Research [7] introduces a multi-cipher cryptosystem (MCC) which enables a cryptosystem to use multiple cipher algorithms concurrently in a session of communication. The implementation of a sample MCC is introduced in this paper using Field Programmable Gate Array (FPGA). Here refers to a multi-mode of operation, the kind of the internal structure of the cryptographic module design considerations for a specific circuit. For example, [10] is a fast pipelined multi-mode DES architecture operating in IP representation.

3. THE UNIFIED OPERATION STRUCTURE

A block cipher by itself allows encryption only of a single data block of the cipher's block length. For a variable-length message, the data must first be partitioned into separate cipher blocks. In the simplest case, known as the electronic codebook (ECB) mode, and then each block is encrypted and decrypted independently. There are several common and popular block modes of operation like CBC, CFB , OFB, etc.

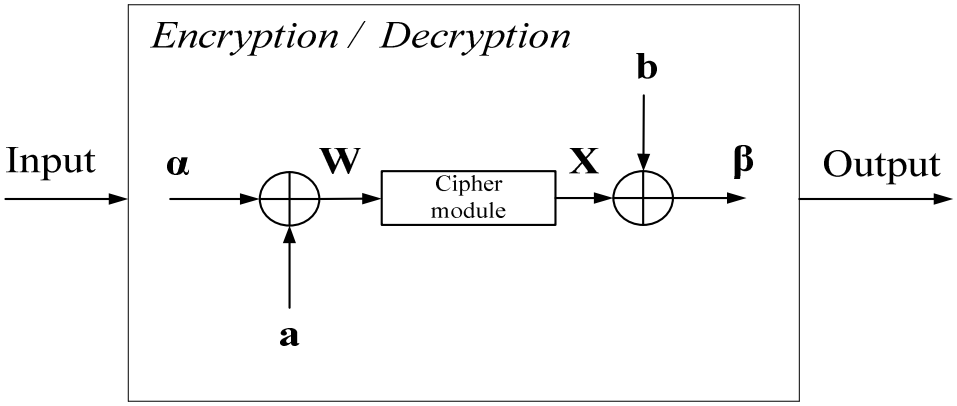
In the popular cipher block chaining (CBC) mode, for encryption to be secure the initialization vector passed along with the plaintext message must be a random or pseudo-random value, which

is added in an exclusive-or manner to the first plaintext block before it is being encrypted. The resultant ciphertext block is then used as the new initialization vector for the next plaintext block. In the cipher feedback (CFB) mode, which emulates a self-synchronizing stream cipher, the initialization vector is first encrypted and then added to the plaintext block. The output feedback (OFB) mode repeatedly encrypts the initialization vector to create a key stream for the emulation of a synchronous stream cipher.

If users want to combine one more mode to archive multi-mode performance, they must prepare several feedbacks to suit any one of the target mode needed. This is because people must hold several data for a proper feedback usage. For example, a user must prepare the current ciphertext data block feedbacks in operating the CBC mode.

How about solving the feedback problem? We use four buffers to hold the previous period, i.e. block cycle, parameters: previous input α of UOS, previous output β of UOS, previous inter-input W of cipher, previous inter-output X of a cipher. Especially in encryption, the previous output of UOS can be retrieved from ciphertext sequence, so that we do not buffer it. Therefore all the four buffers can reduce to three buffers. Because of the three buffers, we solved the feedback problem.

The W is inter-input of cipher module and the X is an inter-output of cipher module. The previous output of UOS is ciphertext in encryption used for CBC and CFB. The previous inter-output of a cipher is au output feedback used for OFB.



$$\beta = \mathrm{f}(\alpha, \mathrm{a}, \mathrm{b}) = \mathrm{E}_K(\alpha \oplus \mathrm{a}) \oplus \mathrm{b}$$

When ECB/CBC/CFB/OFB encryption
CFB/OFB decryption
CBC-MAC

$$\beta = \mathrm{f}^{-1}(\alpha, \mathrm{a}, \mathrm{b}) = \mathrm{D}_K(\alpha \oplus \mathrm{a}) \oplus \mathrm{b}$$

When ECB/CBC decryption

holding the previous period information
parameters:
α previous input of UOS
β previous output of UOS
W previous inter-iuput of cipher
X previous inter-output of cipher

Figure 1. The proposed novel multi-mode structure

Table 1. The Parameters for Proposed UOS

Operation $Mode_{App}$	Cipher module	**α**	**β**	**a**	**b**	Schematic diagram
ECB_e	$Cipher_e$	P_i	C_i	0	0	Fig 2.(a)
ECB_d	$Cipher_d$	C_i	P_i	0	0	Fig 2.(b)
CBC_e	$Cipher_e$	P_i	C_i	C_{i-1}	0	Fig 3.(a)
CBC_d	$Cipher_d$	C_i	P_i	0	C_{i-1}	Fig 3.(b)
CFB_e	$Cipher_e$	0	C_i	C_{i-1}	P_i	Fig 4.(a)
CFB_d	$Cipher_e$	0	P_i	C_{i-1}	C_i	Fig 4.(b)
OFB_e	$Cipher_e$	0	C_i	X_{i-1}	P_i	Fig 5.(a)
OFB_d	$Cipher_e$	0	P_i	X_{i-1} / W_{i-1}*	C_i	Fig 5.(b)
CBC-MAC	$Cipher_e$	P_n	*tag*	C_{n-1}	0	Fig 6.

P.S. The mask means ciphers with *decryption function* especially

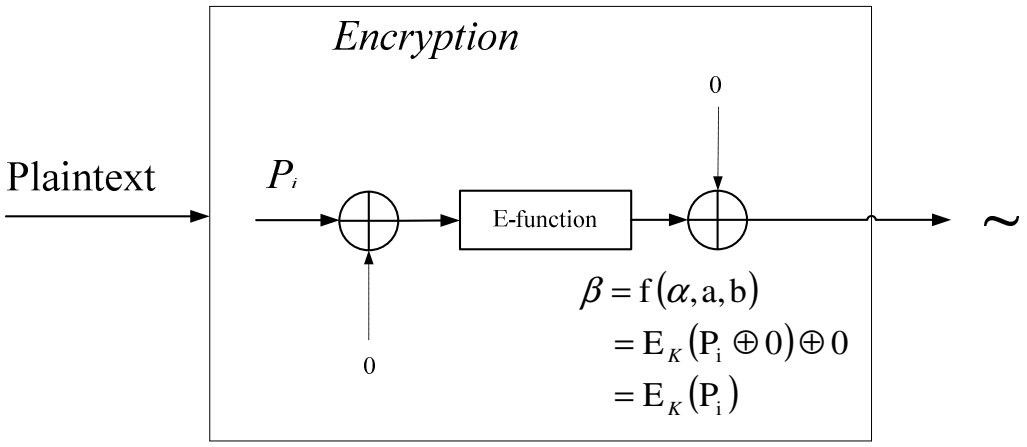
4. PARTIAL OPERATIONS WITH STANDARD

Several so-called block cipher modes of operation have been designed and specified in national recommendations such as NIST 800-38A and international standards such as ISO/IEC 10116 [4][12].

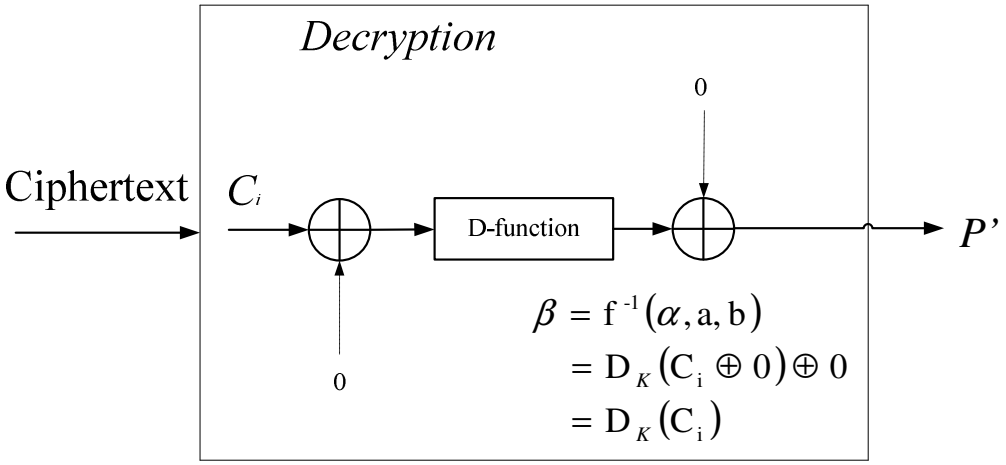
4.1. Electronic CodeBook (ECB) mode

The simplest of the encryption modes is the electronic codebook mode. The message is divided into blocks and each block is encrypted separately. The disadvantage of this method is that identical plaintext blocks are encrypted into identical ciphertext blocks; thus, it does not hide data patterns well. In some senses, it doesn't provide serious message confidentiality, and it is not recommended for use in cryptographic protocols at all.

ECB mode can also make protocols without integrity protection even more susceptible to replay attacks, since each block gets decrypted in exactly the same way. For example, the Phantasy Star Online: Blue Burst online video game uses Blowfish in ECB mode. Before the key exchange system was cracked leading to even easier methods, cheaters repeated encrypted "monster killed" message packets, each an encrypted Blowfish block, to illegitimately gain experience points quickly.



(a) Encryption application



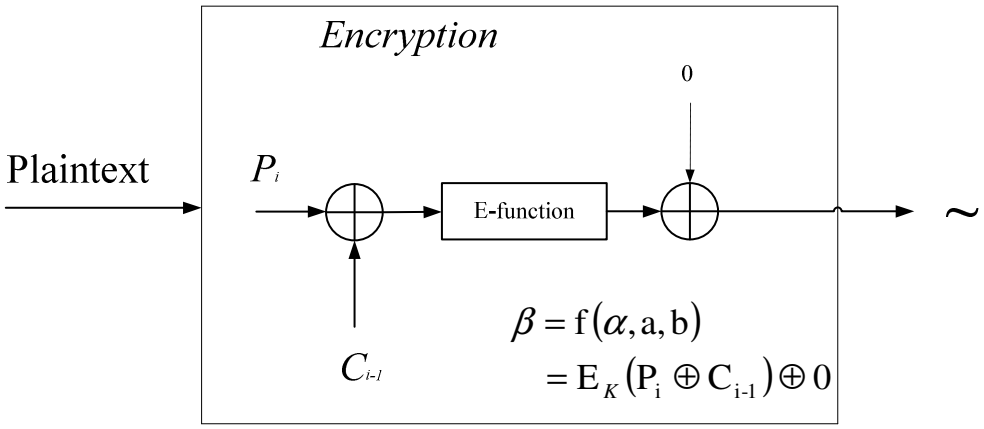
(b) Decryption application

Figure 2. Electronic CodeBook mode

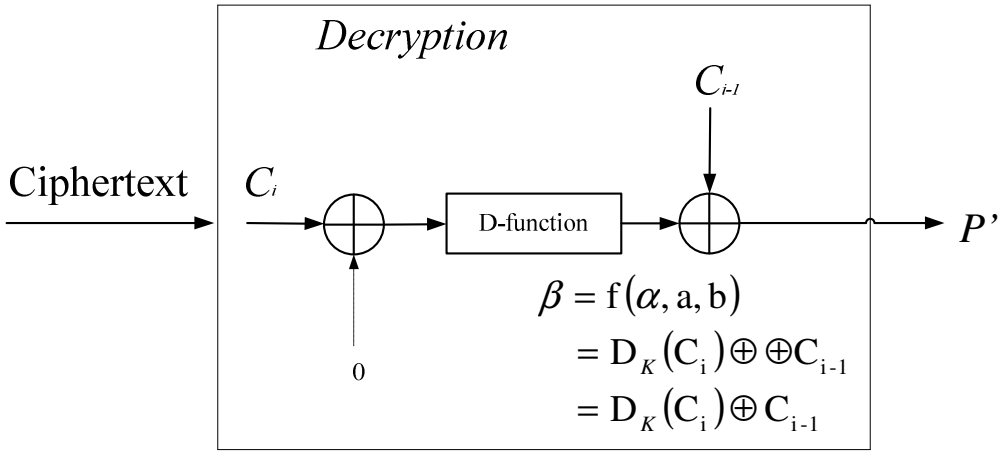
4.2. Cipher Block Chaining (CBC) mode

Cipher block chaining is a block cipher mode that provides confidentiality but not message integrity in cryptography. Cipher block chaining mode of operation was invented by IBM in 1976 [13]. In CBC mode, each block of plaintext is XORed with the previous ciphertext block before being encrypted. This way, each ciphertext block is dependent on all plaintext blocks processed up to that point. Also, to make each message unique, an initialization vector must be used in the first block.

CBC has been the most commonly used mode of operation. Its main drawbacks are that encryption is sequential (i.e., it cannot be parallelized), and that the message must be padded to a multiple of the cipher block size. One way to handle this last issue is through the method known as ciphertext stealing. Note that a one-bit change in a plaintext affects all following ciphertext blocks.



(a) Encryption application



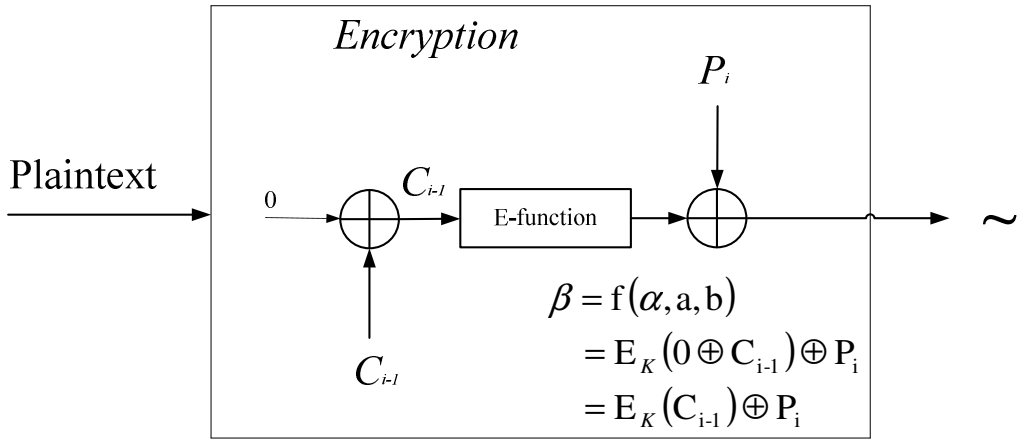
(b) Decryption application

Figure 3. Cipher Block Chaining mode

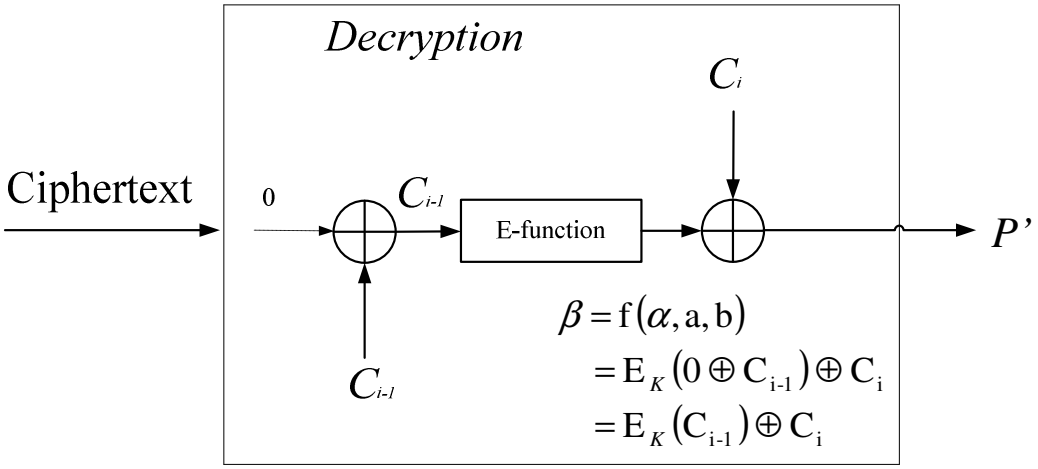
Decrypting with the incorrect previous ciphertext block causes the current block of plaintext to be corrupt but subsequent plaintext blocks will be correct. This is because a plaintext block can be recovered from two adjacent blocks of ciphertext. As a consequence, decryption can be parallelized. Note that a one-bit change to the ciphertext causes complete corruption of the corresponding block of plaintext, and inverts the corresponding bit in the following block of plaintext, but the rest of the blocks remain intact.

4.3. Cipher FeedBack (CFB) mode

The cipher feedback mode is a confidentiality mode that features the feedback of successive ciphertext segments into the input blocks of the forward cipher to generate output blocks that are exclusive-ORed with the plaintext to produce the ciphertext, and vice versa.



(a) Encryption application



(b) Decryption application

Figure 4. Cipher FeedBack mode.

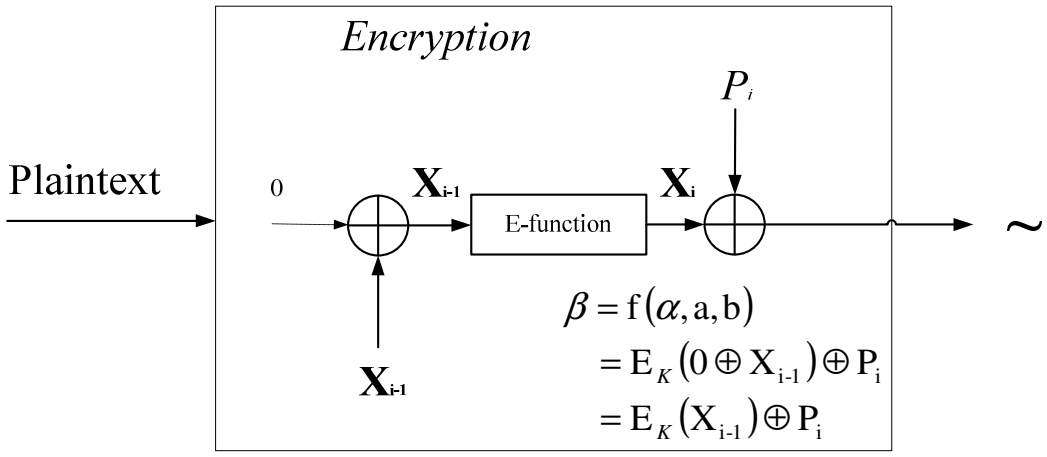
Here, a plaintext block is enciphered by being XORed to the encryption module of the previous ciphertext block. The process is repeated with the successive input blocks until a ciphertext segment is produced from every plaintext segment. In general, each successive input block is enciphered to produce an output block.

In CFB encryption, like CBC encryption, the input block to each forward cipher function depends on the result of the previous forward cipher function; therefore, multiple forward cipher operations cannot be performed in parallel. In CFB decryption, the required forward cipher operations can be performed in parallel if the input blocks are first constructed (in series) from the ciphertext [14].

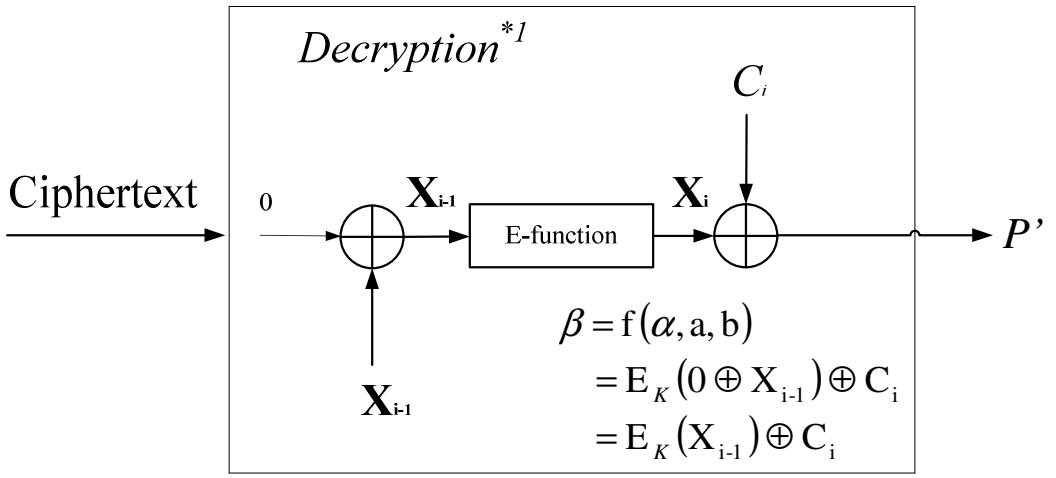
4.4. Output Feedback (OFB) Mode

One other mode among those originally suggested for use was Output Feedback Mode: this mode encrypted an initial value with DES, and then the result of the encryption was encrypted again repeatedly. The resulting values were used as a keystream to XOR with messages.

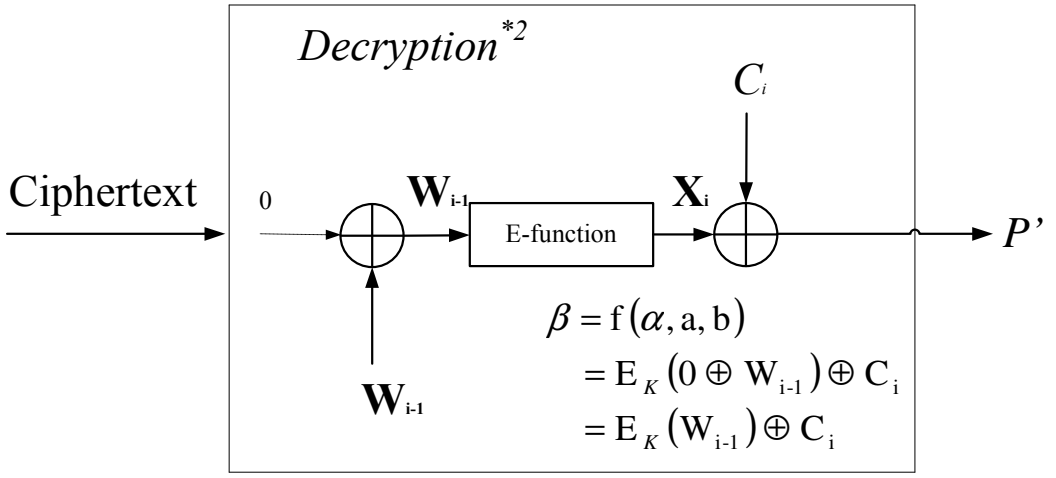
The Output Feedback (OFB) mode is a confidentiality mode that features the iteration of the forward cipher on an IV to generate a sequence of output blocks that are exclusive-ORed with the plaintext to produce the ciphertext, and vice versa. The OFB mode requires that the IV is a nonce, i.e., the IV must be unique for each execution of the mode under the given key; In OFB encryption, the IV is transformed by the forward cipher function to produce the first output block. The first output block is exclusive-ORed with the first plaintext block to produce the first ciphertext block. The forward cipher function is then invoked on the first output block to produce the second output block. The second output block is exclusive-ORed with the second plaintext block to produce the second ciphertext block, and the forward cipher function is invoked on the second output block to produce the third output block. Thus, the successive output blocks are produced by applying the forward cipher function to the previous output blocks, and the output blocks are exclusive-ORed with the corresponding plaintext blocks to produce the ciphertext blocks.



(a) Encryption application



*1: When previous mode change is OFB or CFB



*2: When previous mode change is ECB or CBC

(b) Decryption application

Figure 5. Output FeedBack mode

In OFB decryption, the IV is transformed by the forward cipher function to produce the first output block. The first output block is exclusive-ORed with the first ciphertext block to recover the first plaintext block. The first output block is then transformed by the forward cipher function to produce the second output block. The second output block is exclusive-ORed with the second ciphertext block to produce the second plaintext block, and the second output block is also transformed by the forward cipher function to produce the third output block. Thus, the successive output blocks are produced by applying the forward cipher function to the previous output blocks, and the output blocks are exclusive-ORed with the corresponding ciphertext blocks to recover the plaintext blocks.

4.5. Cipher Block Chaining Message Authentication Code (CBC-MAC)

A cipher block chaining message authentication code (CBC-MAC) is a technique for constructing a message authentication code from a block cipher. The message is encrypted with some block cipher algorithm in CBC mode to create a chain of blocks such that each block depends on the proper encryption of the previous block. This interdependence ensures that a change to any of the plaintext bits will cause the final encrypted block to change in a way that cannot be predicted or counteracted without knowing the key to the block cipher.

To calculate the CBC-MAC of message one encrypts in CBC mode with zero initialization vector. The following figure sketches the computation of the CBC-MAC of a message comprising $P_1||P_2||P_3|..||P_n$ using a secret key K and a block cipher E():

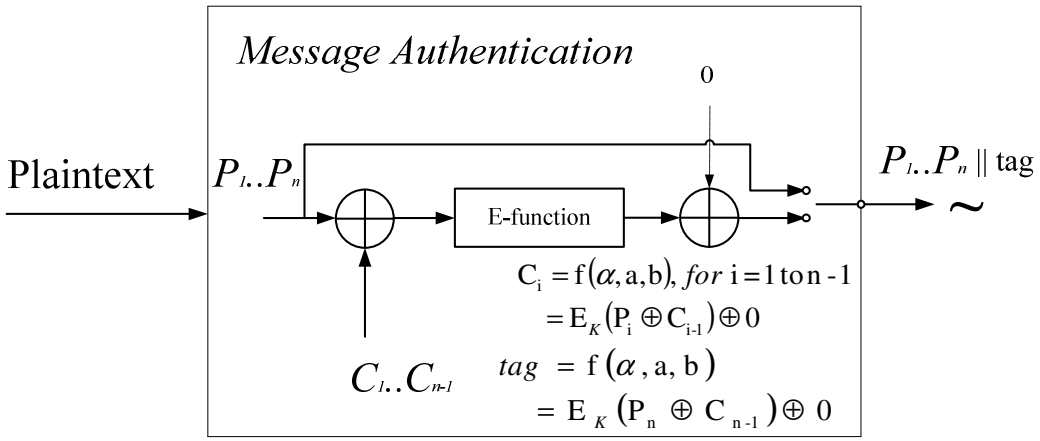


Figure 6. Cipher Block Chaining Message Authentication Code.

The simple CBC-MAC operation uses CBC encryption, just CBC-MAC outputs of UOS are the through passed plaintext block from the first divided message block to the end. A tag only goes behind the whole message with C_n as the message authentication code, i.e. an integrity check value.

5. Mode Selecting Scheme and Operating Simulation

We design three schemes for mode selecting, and then using the second scheme, normal change, to perform an operating simulation in this chapter.

5.1. Mode Selecting Schemes

We define that current mode exchange depends on the two choice bits of last plaintext. For example, if the choice bits are 01_2, then we choose the current mode exchange to CBC mode. Therefore 00_2 means ECB, 01_2 means CBC, 10_2 means CFB and 11_2 means OFB choice.

Each proposed change mechanism is using 2 bits choice related from the last block plaintext message before current block operating. The mode change depends on 2-bit choice S, i.e. S_0S_1.

5.1.1. Easy Change Scheme

Easy change is using 2 bits plaintext from the previous block plaintext message before current block operating. We define that current mode exchange depends on the msb./lsb./middle two bits of last plaintext. The mode change is depended on partial 2-bits message.

$$S=(S_0S1)=filter(P_{i-1})$$
$$=MSB^{2\text{-}bit}(P_{i-1})\ or\ LSB^{2\text{-}bit}(P_{i-1})\ or\ MID^{2\text{-}bit}(P_{i-1}) \quad (1)$$

5.1.2. Normal Change Scheme

This scheme uses two parity check bits, one is from all odd positions sequence and the other is from all even positions sequence. It can make a simple related effect. If changing any one bit then infecting effect the current block and behind operating.

$$S=(S_0S_1)$$
$$S_0=f^{odd}(P_{i-1})=Parity\ (P_{i-1}{}^{odd})$$
$$S_1=f^{even}(P_{i-1})=Parity\ (P_{i-1}{}^{even}) \quad (2)$$

5.1.3. Hash Change Scheme

We improve the normal change by hash functions to instead of parity check functions. This brings hard scrambled performance but an extra cost of the resource.

$$S=(S_0S1)=f(Pi\text{-}1)=hash^{2\text{-}bit}(Pi\text{-}1)$$
$$=LSB^{2\text{-}bit}(\ MD5(Pi\text{-}1)\ )or\ LSB^{2\text{-}bit}(\ SHA\text{-}1(Pi\text{-}1)\ ) \quad (3)$$

5.2. Operating Simulation

According to the low-resource environment, we suggest using the easy change scheme in cloud computing. Here we perform an operating simulation with the easy change scheme in the following. The detail descriptions of one-by-one steps are in the appendix.

Table 2. The Parameters for UOS Simulation

Cipher: AES
Key: 12121212121212123434343434343434
IVs: 00000000000000000000000000000000
Plaintext: 00000000000000000000000000000010 00000000000000000000000000000011 00000000000000000000000000000001 11111111111111111111111111111111 ……
Ciphertext: 1F8300022FAD7840E51D265C9A1B663F 8EC78F4182557DEE3461681A3061D901 644A48DCC8CB017482399212A5164471 4B095F7288862F4FD4D8F7BFDD18131B ……

7. CONCLUSIONS

In this paper, a novel structure, called unified operation structure (UOS), is proposed. The technique uses possible options to satisfy any next one of all feedbacks so that UOS can perform several modes of operation. It is easier to provide multi modes of operation and suit for any kinds of block ciphers. We design three schemes for mode selecting and then use the normal change scheme to perform an operating simulation according to the low-resource environment in Cloud Computing. Our contribution reduces the cost of resource for multi mode implementation and support continuous mode change application. It provides low-resource hardware implementation of a common solution for multi-mode. It is proper to ubiquitous computing devices such as a sensor mote or an RFID tag.

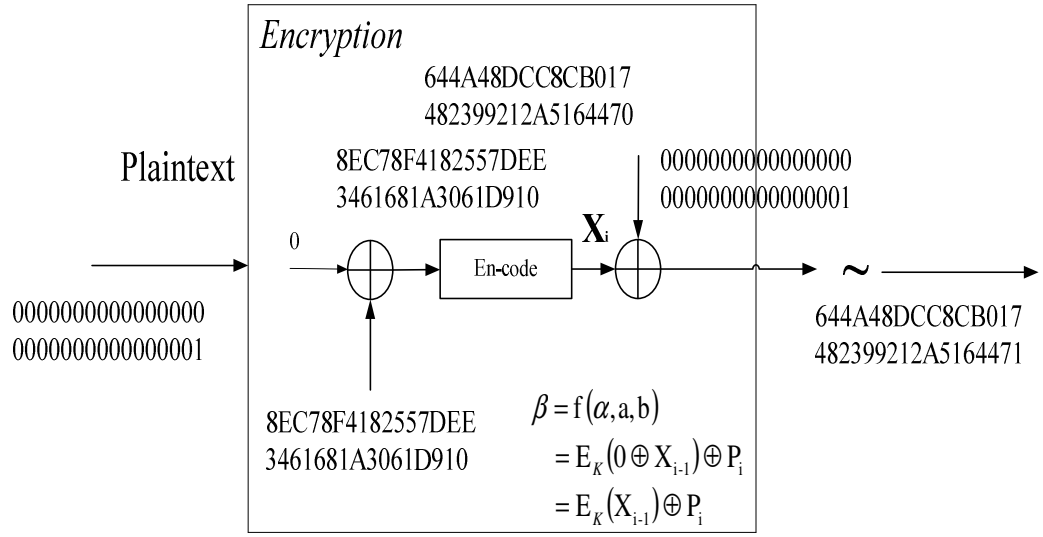
REFERENCES

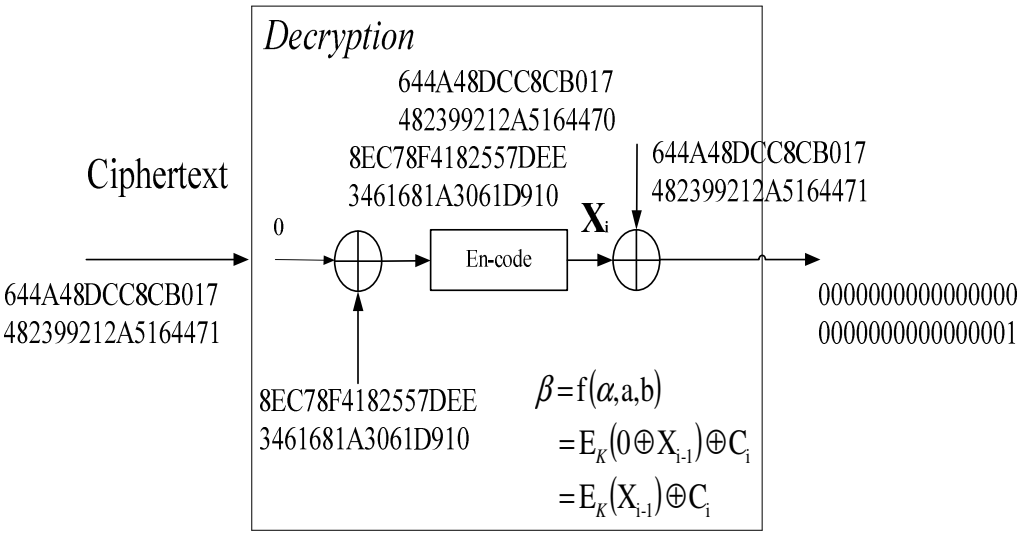
[1] IPSec Working Group. http://www.ietf.org/html.charters/ipseccharter.html
[2] OpenSSL. http://etutorials.org/Programming/secure+programming/Chapter+5.+Symmetric+Encryption/5.17+Performing+Block+Cipher+Setup+for+CBC+CFB+OFB+and+ECB+Modes+in+OpenSSL/
[3] SSL 3.0 Specification. http://wp.netscape.com/eng/ssl3/
[4] National Institute of Standards and Technology (NIST), NIST. gov - Computer Security Division - Computer Security Resource Center, "Recommendation of block cipher security methods and Techniques," NIST SP800-38.
[5] Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone (1996). *Handbook of Applied Cryptography*. CRC Press. ISBN 0-8493-8523-7.
[6] E. Biham, (1998) "Cryptanalysis of multiple modes of operation," *J. Cryptology*, Vol. 11, No. 1, pp. 45-58.
[7] Chung-Ping Young, Yen-Bor Lin & Chung-Chu Chia, (2009) "Software and Hardware Design of a Multi-cipher Cryptosystem," *Proc. IEEE TENCON 2009*, Singapore.
[8] Lisa Wu, Chris Weaver, and Todd Austin, (2001) "CryptoManiac: A Fast Flexible Architecture for Secure Communication," *Proc. IEEE Int. Symp. Comput. Archit.*, pp. 110–119.
[9] S. Laovs, A. Priftis, P. Kitsos, and O. Koufopavlou, (2003) "Reconfigurable crypto process design of encryption algorithms operation modes methods and FPGA integration," *Proc. IEEE Int. Conf. MWSCAS*, pp. 811–814.
[10] S. Guilley, P. Hoogvorst, and R. Pacalet, (2007) "A Fast Pipelined Multi-Mode DES Architecture Operating in IP Representation," *The VLSI Journal*, Vol. 40, No. 4, pp.479-489.
[11] Young, C.-P., (2008) "NCPA: A Scheduling Algorithm for Multi-cipher and Multi-mode Reconfigurable Cryptosystem," *Proc. IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing*), Harbin, China.
[12] International Organization for Standardization (ISO), "Information Technology-Security Techniques-Modes of Operation for. an n-bit Block Cipher," ISO/IEC 10116, 1997.
[13] William F. Ehrsam, Carl H. W. Meyer, John L. Smith, Walter L. Tuchman, (1976) "Message verification and transmission error detection by block chaining," US Patent 4074066.
[14] H. M. Heys, (2003) "Analysis of the Statistical Cipher Feedback Mode of Block Ciphers," *IEEE Transactions on Compuiters,* Vol. 52, No. 1.

APPENDIX A

Simulation case of sector 5.2, especially marking OFB and then CBC.
People can download the simulation program to verify the results.
(http://dl.dropbox.com/u/54967925/UOS_Win32.exe or
http://dl.dropbox.com/u/54967925/UOS_x64.exe, it is suitable for OS: Windows 2000/XP Pro./Vista/7 but not Windows XP Home Edition)

A.(1) OFB Encryption and Decryption Applications


Encryption
644A48DCC8CB017
482399212A5164470
Plaintext
8EC78F4182557DEE
3461681A3061D910
0000000000000000
0000000000000001
Xi
0
En-code
~
0000000000000000
0000000000000001
644A48DCC8CB017
482399212A5164471
8EC78F4182557DEE
3461681A3061D910
β = f(α,a,b)
= E_K(0 ⊕ X_i-1) ⊕ P_i
= E_K(X_i-1) ⊕ P_i


Decryption
644A48DCC8CB017
482399212A5164470
Ciphertext
8EC78F4182557DEE
3461681A3061D910
644A48DCC8CB017
482399212A5164471
Xi
0
En-code
644A48DCC8CB017
482399212A5164471
0000000000000000
0000000000000001
8EC78F4182557DEE
3461681A3061D910
β = f(α,a,b)
= E_K(0 ⊕ X_i-1) ⊕ C_i
= E_K(X_i-1) ⊕ C_i

A. (2) CBC Encryption and Decryption Applications