Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**	
Title	**Clarification of the AES-CBC mode**	
Data Submitted	**2005-04-28**	
Source(s)	Sungcheol Chang Eunkyung Kim Seokheon Cho Chulsik Yoon ETRI	Voice: +82-42-860-5456 Fax: +82-42-861-1966 scchang@etri.re.kr ekkim@etri.re.kr chosh@etri.re.kr csyoon@etri.re.kr
Re:	This is a response to Sponsor Ballot 16e on P802.16e/D7.	
Abstract	The document contains suggestions on the changes in IEEE P802.16e-D7 that would clarify the AES-CBC mode.	
Purpose	The document is submitted for review by 802.16 Working Group members.	
Notice	This document has been prepared to assist IEEE 802.16. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.	
Release	The contributor grants a free, irrevocable license to the IEEE to incorporate material contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE's name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE's sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that this contribution may be made public by IEEE 802.16	
Patent Policy and Procedures	The contributor is familiar with the IEEE 802.16 Patent Policy and Procedures <http://ieee802.org/16/ipr/patents/policy.html>, including the statement "IEEE standards may include the known use of patent(s), including patent applications, provided the IEEE receives assurance from the patent holder or applicant with respect to patents essential for compliance with both mandatory and optional portions of the standard. "Early disclosure to the Working Group of patent information that might be relevant to the standard is essential to reduce the possibility for delays in the development process and increase the likelihood that the draft publication will be approved for publication. Please notify the Chair <mailto:chiar@wirelessman.org> as early as possible, in written or electronic form, if patented technology (or technology under patent application) might be incorporated into a draft standard being developed within the IEEE 802.16 Working Group. The Chair will disclose this notification via the IEEE 802.16 web site <http://ieee802.org/16/ipr/patents/notices>.	

Clarification of the AES-CBC mode

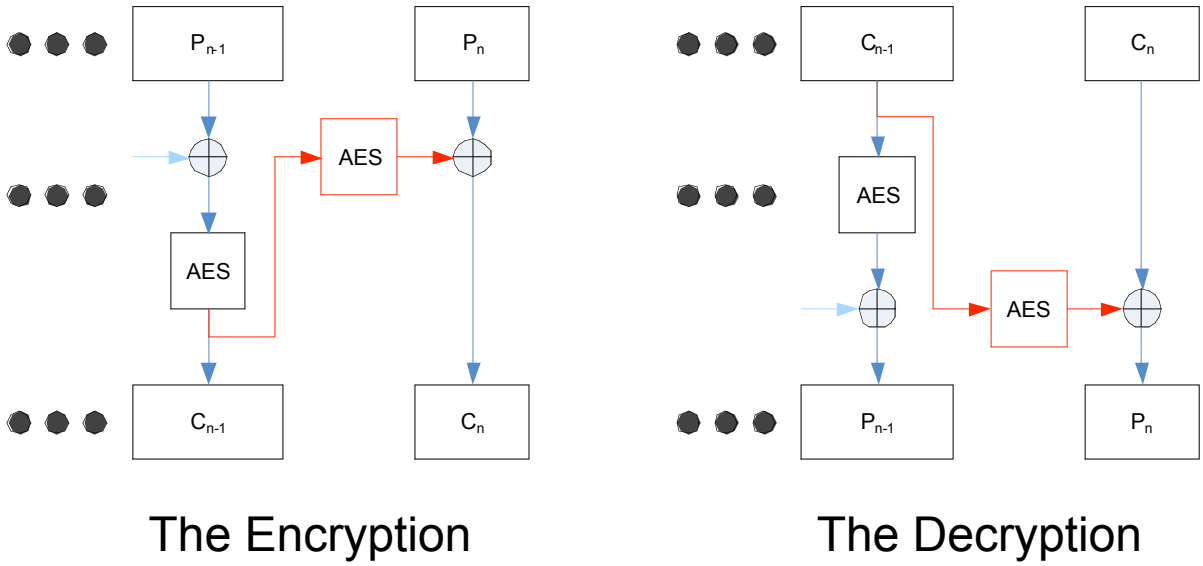
Sungcheol Chang, Eunkyung Kim, Seokheon Cho and Chulsik Yoon
ETRI

1 Problem Statements

There is no description about the problem of residual termination block processing, when the final block size is less than the cipher block size.

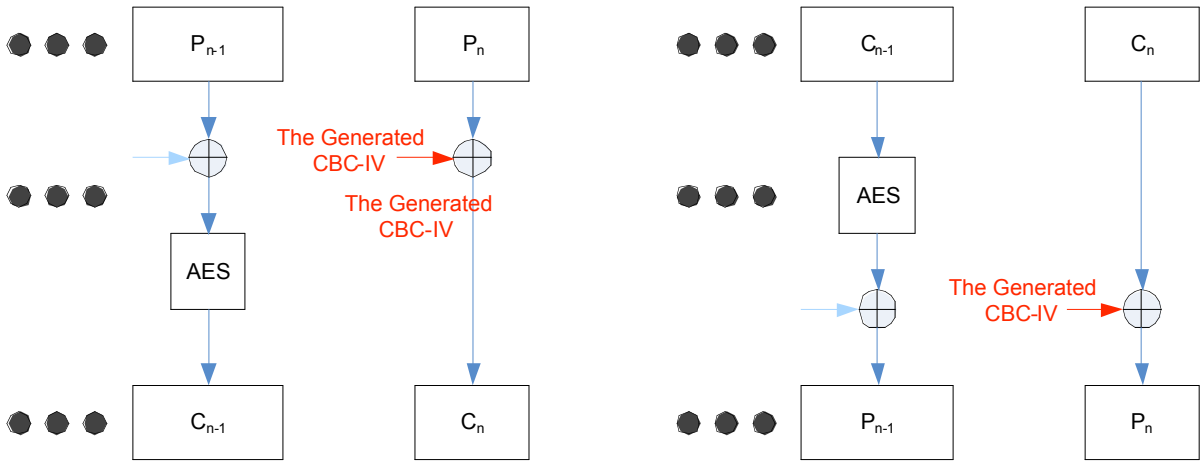
2 Overview of Proposed Solution

2.1 Remedy 1: Similar method to the DES-CBC mode



The Encryption The Decryption

2.2 Remedy 2: Using the generated CBC-IV



The Encryption The Decryption

3 Proposed changes to IEEE 802.16e/D7

3.1 Remedy 1: Similar method to the DES-CBC mode

[Modify text in subclause 7.8.4.3:]

7.8.4.3 Data encryption with AES in CBC mode

If the data encryption algorithm identifier in the cryptographic suite of an SA equals 0x03, data connections associated with that SA shall use the CBC mode of the US Advanced Encryption Standard algorithm [NIST Special Publication 800-~~38C~~38A, FIPS 197] to encrypt the MAC PDU payloads.

Residual termination block processing shall be used to encrypt the final block of plaintext when the final block is less than the cipher block size. Given a final block having n bits, where n is less than the cipher block size, the next-to-last ciphertext block shall be AES encrypted for the second time, using the electronic code book (ECB) mode, and the most significant n bits of the result are XORed with the final n bits of the payload to generate the short final cipher block. In order for the receiver to decrypt the short final cipher block, the receiver AES encrypts the next-to-last ciphertext block, using the ECB mode, and XORs the most significant n bits with the short final cipher block in order to recover the short final plaintext block. This encryption procedure is depicted in Figure 9.4 of Schneier [B42].

In the special case when the payload portion of the MAC PDU is less than the cipher block size, the most significant n bits of the generated CBC-IV, corresponding to the number of bits of the payload, shall be XORed with the *n* bits of the payload to generate the short cipher block.

3.2 Remedy 2: Using the generated CBC-IV

[Modify text in subclause 7.8.4.3:]

7.8.4.3 Data encryption with AES in CBC mode

If the data encryption algorithm identifier in the cryptographic suite of an SA equals 0x03, data connections associated with that SA shall use the CBC mode of the US Advanced Encryption Standard algorithm [NIST Special Publication 800-~~38C~~38A, FIPS 197] to encrypt the MAC PDU payloads.

Residual termination block processing shall be used to encrypt the final block of plaintext when the final block is less than the cipher block size. Given a final block having n bits, where n is less than the cipher block size, the most significant n bits of the generated CBC-IV, shall be XORed with the *n* bits of the final block plaintext to generate the short cipher block. In order for the receiver to decrypt the short final cipher block, the receiver XORs the most significant n bits of the generated CBC-IV with the short final cipher block in order to recover the short final plaintext block. In the case when the payload portion of the MAC PDU is less than the cipher block size, the residual termination block processing shall be applied.