Csci388 Wireless and Mobile Security – AES-CCMP

Xiuzhen Cheng
cheng@gwu.edu

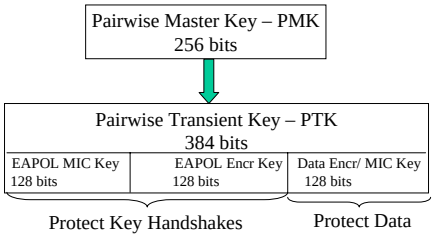
Introduction

- **CCMP stands for Counter Mode – CBC MAC Protocol**
  - CCMP defines a set of rules that use the AES block cipher for encryption and integrity protection
  - The cipher of CCMP is AES
  - The cipher of TKIP is RC4
- **The default mode for IEEE 802.11i is CCMP**
- **Provides stronger security compared to TKIP**
  - CCMP is designed from scratch, therefore ready to use best-known techniques
  - TKIP is a compromise. It uses weaker security primitives (eg. Michael) in order to accommodating existing hardware
- **Why AES?**
  - AES is secure, gone through a large amount of reviews already
  - It is export-controlled and well-understood by government agencies, and therefore easier to get export licenses

Introduction

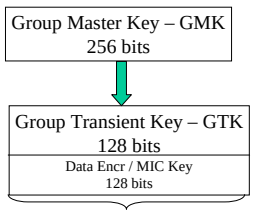
- **The decision of adopting AES in 802.11i was made earlier than the weakness of WEP had been identified**
  - It is not expected to upgrade exiting WEP hardware for the new standard due to hardware-implementation of cipher
  - TKIP is used to bridge the gap: the weakness/flaw of WEP demands an immediate solution for current systems while CCMP takes time to get ratified.
- **WEP, TKIP, and CCMP**
  - WPA/TKIP and RSN/CCMP have a lot in common: eg. Key management
  - CCMP uses one key for encryption and protection
  - The biggest difference is the encryption algorithm – how the data is encrypted/decrypted

AES Pairwise Key Hierarchy in CCMP



AES Pairwise Key Hierarchy

AES Group Key Hierarchy in CCMP



Protect Multicast/Broadcast

AES Overview

- **AES is a block cipher, with the same size for the plaintext/ciphertext**
- **It is very unlikely that any fundamental weakness will be discovered in the near future**
- **AES allows different block sizes and key sizes**
  - CCMP restricts the key size and block size to be 128 bits

Modes of Operation

- **AES has up to 16 different modes of operation (published in the NIST website), and it is still seeking for new ones**
- **ECB mode**
  - Encrypt each block independently; Padding needed; Can be done in parallel
  - Same block generates the same cipher
- **Counter mode**
  - Encrypt a counter, which is increased 1 for each block, and XOR the result with the data to produce the ciphertext
  - Decryption is exactly the same as encryption, no padding is needed
  - Parallel encryption/decryption
  - No message authentication, only encryption
  - Initial value (a nonce) of the counter and its step size need to be delivered to the receiver
  - It is possible for two blocks of identical but separate plaintexts to generate the same ciphertexts if the counter starts from 1

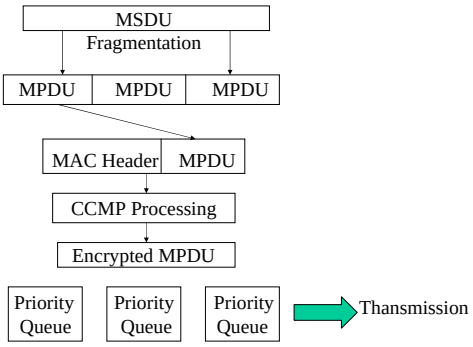
Modes of Operation

- **Counter mode + CBC MAC: CCM**
  - Created especially for IEEE 802.11i RSN
  - Invented by D. Whiting, R. Housley, and N. Ferguson in the 802.11i standard group
  - Built on top of the counter mode; uses counter mode in conjunction with a message authentication method called cipher block chaining (CBC)
  - Encrypt the first block with AES; XOR the result with the second block and then encrypt it with AES; Repeat until no block left. The result is a single block as the MIC
  - Padding is needed
  - Linking authentication and encryption
  - CCM mode allows the encryption to be performed on a subpart of the message that is authenticated by CBC-MAC
    - Header should be transmitted as plaintext but it should not be modified
  - The IVs (nonces) for the counter mode and for the CBC-MAC portion are different, leading different keys
  - Simple but can't be parallelized

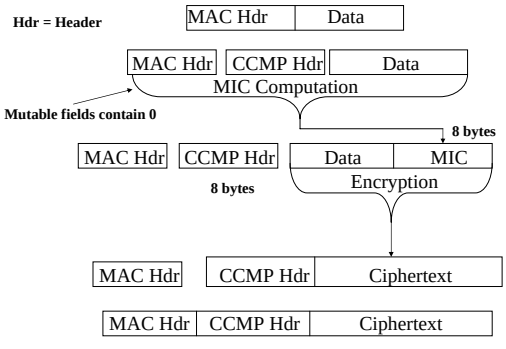
Modes of Operation

- **Offset Codebook Mode (OCB)**
  - Achieves both encryption and authentication
  - OCB is parallelizable so it can be done faster using multiple hardware blocks
  - OCB is very efficient, taking only a slightly more than the theoretical minimum encryption operations possible
  - OCB is provably secure; it is as secure as AES
- **OCB is not adopted by IEEE 802.11i**
  - It is proprietary

How CCMP is Used in RSN

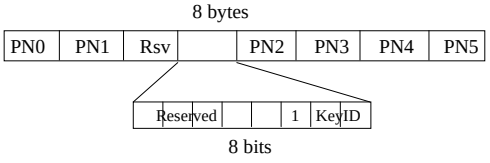


CCMP Processing

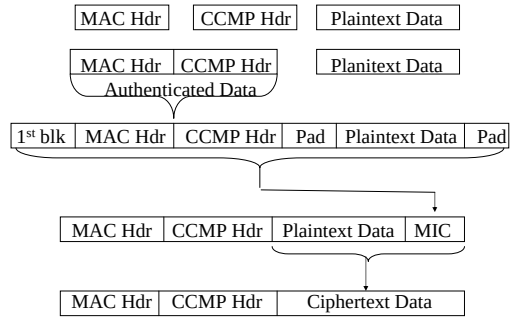


CCMP Header

- **CCMP header must be prepended to the encrypted data and transmitted in plaintext.**
- **CCMP Header contains the 48-bit packet number (PN) that provides replay protection and enables the receiver to derive the the nonce for the encryption**
- **CCMP Header also contains the KeyID field to specify which group key has been used**



CCMP Encryption



CCMP Encryption

- **First Block for MIC computation**
  - Flag fixed to 01011001, indicating that MIC field is 64-bit in length
  - Priority, SA, and PN form a unique Nonce
  - Data Length specifies the length of the plain text

Flag	Priority	Source Address	Packet Number	DLen

- **Padding for two parts, counter mode encryption works only on the plaintext and the MIC**
- **The counter for AEC Counter Mode (128 bits)**
  - Ctr starts from 1 for a frame

Flag	Priority	Source Address	Packet Number	Ctr

CCMP Decryption

- **A reverse procedure**
  - Check PN
  - Decrption
  - Check MIC
- **Counter mode AES encrypts the counter through AES, and therefore Encryption/Decryption are the same**

Question?

- **Why need the first block for MIC computation?**