CCMP (cryptography)

From Wikipedia, the free encyclopedia

[Jump to navigation](https://en.wikipedia.org/wiki/CCMP_(cryptography)#mw-head)[Jump to search](https://en.wikipedia.org/wiki/CCMP_(cryptography)#searchInput)

**Counter Mode Cipher Block Chaining Message Authentication Code Protocol** (**Counter Mode CBC-MAC Protocol**) or **CCM mode Protocol** (**CCMP**) is an [encryption](https://en.wikipedia.org/wiki/Encryption) [protocol](https://en.wikipedia.org/wiki/Security_protocol) designed for [Wireless LAN](https://en.wikipedia.org/wiki/Wireless_LAN) products that implements the standards of the [IEEE 802.11i](https://en.wikipedia.org/wiki/IEEE_802.11i) amendment to the original [IEEE 802.11](https://en.wikipedia.org/wiki/IEEE_802.11) standard. CCMP is an enhanced data cryptographic encapsulation mechanism designed for data confidentiality and based upon the Counter Mode with CBC-MAC ([CCM mode](https://en.wikipedia.org/wiki/CCM_mode)) of the [Advanced Encryption Standard](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard) (AES) standard.[[1]](https://en.wikipedia.org/wiki/CCMP_(cryptography)#cite_note-802.11_2007-1) It was created to address the vulnerabilities presented by [Wired Equivalent Privacy](https://en.wikipedia.org/wiki/Wired_Equivalent_Privacy) (WEP), a dated, insecure protocol.[[1]](https://en.wikipedia.org/wiki/CCMP_(cryptography)#cite_note-802.11_2007-1)



**Contents**

* [1Technical details](https://en.wikipedia.org/wiki/CCMP_(cryptography)#Technical_details)
* [2Security](https://en.wikipedia.org/wiki/CCMP_(cryptography)#Security)
  + [2.1Known attacks](https://en.wikipedia.org/wiki/CCMP_(cryptography)#Known_attacks)
* [3References](https://en.wikipedia.org/wiki/CCMP_(cryptography)#References)

Technical details[[edit](https://en.wikipedia.org/w/index.php?title=CCMP_(cryptography)&action=edit&section=1)]

|  |  |
| --- | --- |
|  | This article **may be too technical for most readers to understand**. Please [help improve it](https://en.wikipedia.org/w/index.php?title=CCMP_(cryptography)&action=edit) to [make it understandable to non-experts](https://en.wikipedia.org/wiki/Wikipedia:Make_technical_articles_understandable), without removing the technical details. *(February 2018) (*[*Learn how and when to remove this template message*](https://en.wikipedia.org/wiki/Help:Maintenance_template_removal)*)* |

CCMP uses [CCM](https://en.wikipedia.org/wiki/CCM_mode) that combines [CTR mode](https://en.wikipedia.org/wiki/Block_cipher_modes_of_operation#Counter_.28CTR.29) for data confidentiality and CBC-MAC for authentication and integrity. CCM protects the integrity of both the [MPDU](https://en.wikipedia.org/wiki/MAC_protocol_data_unit) data field and selected portions of the IEEE 802.11 MPDU header. CCMP is based on AES processing and uses a 128-bit key and a 128-bit block size. CCMP uses CCM with the following two parameters:

* M = 8; indicating that the MIC is 8 [octets](https://en.wikipedia.org/wiki/Octet_(computing)) (eight bytes).
* L = 2; indicating that the Length field is 2 octets.

A CCMP [Medium Access Control Protocol Data Unit](https://en.wikipedia.org/wiki/MAC_protocol_data_unit) (MPDU) comprises five sections. The first is the MAC header which contains the destination and source address of the data packet. The second is the CCMP header which is composed of 8 octets and consists of the packet number (PN), the Ext IV, and the key ID. The packet number is a 48-bit number stored across 6 octets. The PN codes are the first two and last four octets of the CCMP header and are incremented for each subsequent packet. Between the PN codes are a reserved octet and a Key ID octet. The Key ID octet contains the Ext IV (bit 5), Key ID (bits 6–7), and a reserved subfields (bits 0–4). CCMP uses these values to encrypt the data unit and the MIC. The third section is the data unit which is the data being sent in the packet. The fourth is the [message integrity code](https://en.wikipedia.org/wiki/Message_authentication_code) (MIC) which protects the integrity and authenticity of the packet. Finally, the fifth is the [frame check sequence](https://en.wikipedia.org/wiki/Frame_check_sequence) (FCS) which is used for error detection and correction. Of these sections only the data unit and MIC are encrypted.[[1]](https://en.wikipedia.org/wiki/CCMP_(cryptography)#cite_note-802.11_2007-1)

Security[[edit](https://en.wikipedia.org/w/index.php?title=CCMP_(cryptography)&action=edit&section=2)]

CCMP is the standard encryption protocol for use with the [Wi-Fi Protected Access II](https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access_II) (WPA2) standard and is much more secure than the [Wired Equivalent Privacy](https://en.wikipedia.org/wiki/Wired_Equivalent_Privacy) (WEP) protocol and [Temporal Key Integrity Protocol](https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol) (TKIP) of [Wi-Fi Protected Access](https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access) (WPA). CCMP provides the following security services:[[2]](https://en.wikipedia.org/wiki/CCMP_(cryptography)#cite_note-2)

* Data confidentiality; ensures only authorized parties can access the information
* Authentication; provides proof of genuineness of the user
* Access control in conjunction with layer management

Because CCMP is a block cipher mode using a 128-bit key, it is secure against attacks to the 264 steps of operation. Generic [meet-in-the-middle attacks](https://en.wikipedia.org/wiki/Meet-in-the-middle_attack) do exist and can be used to limit the theoretical strength of the key to 2*n*∕2 (where *n* is the number of bits in the key) operations needed.[[3]](https://en.wikipedia.org/wiki/CCMP_(cryptography)#cite_note-3)

**Known attacks**[[edit](https://en.wikipedia.org/w/index.php?title=CCMP_(cryptography)&action=edit&section=3)]

*Main article:*[*Advanced Encryption Standard § Known attacks*](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#Known_attacks)

References[[edit](https://en.wikipedia.org/w/index.php?title=CCMP_(cryptography)&action=edit&section=4)]

* 1. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/CCMP_(cryptography)#cite_ref-802.11_2007_1-0) [***b***](https://en.wikipedia.org/wiki/CCMP_(cryptography)#cite_ref-802.11_2007_1-1) [***c***](https://en.wikipedia.org/wiki/CCMP_(cryptography)#cite_ref-802.11_2007_1-2) *Cole, Terry (12 June 2007).*[*"IEEE Std 802.11-2007"*](http://standards.ieee.org/getieee802/download/802.11-2007.pdf)*(PDF). New York, New York: The Institute of Electrical and Electronics Engineers, Inc. Retrieved 11 April 2011.*
  2. [**^**](https://en.wikipedia.org/wiki/CCMP_(cryptography)#cite_ref-2) *Ciampa, Mark (2009). Security Guide To Network Security Fundamentals (3 ed.). Boston, MA: Course Technology. pp. 205, 380, 381.*[*ISBN*](https://en.wikipedia.org/wiki/ISBN_(identifier))[*1-4283-4066-1*](https://en.wikipedia.org/wiki/Special:BookSources/1-4283-4066-1)*.*
  3. [**^**](https://en.wikipedia.org/wiki/CCMP_(cryptography)#cite_ref-3) *Whiting, Doug; R. Housley; N. Ferguson (September 2003).*[*"Counter with CBC-MAC (CCM)"*](http://tools.ietf.org/html/rfc3610)*. The Internet Society. Retrieved 11 April 2011.*