CCM generates an encrypted keystream that is applied to input data using the XOR operation and generates an M byte MAC field in one operation. CCM and RADIO can be configured to work synchronously. CCM will encrypt in time for transmission and decrypt after receiving bytes into memory from the radio. All operations can complete within the packet RX or TX time. CCM on this device is implemented to support the Bluetooth requirements and the algorithm as defined in IETF RFC3610, and depends on the AES-128 block cipher. A description of the CCM algorithm can also be found in NIST Special Publication 800-38C. The Bluetooth specification describes the configuration of counter mode blocks and encryption blocks to implement compliant encryption for Bluetooth Low Energy.

CCM uses EasyDMA to read/write additional authenticated data, plain text and cipher text.

Two operations are supported:

- Packet encryption
- Packet decryption

All operations are done in compliance with the *Bluetooth Core Specification*, as well as IEEE 802.15.4.

8.4.1 Shared resources

The CCM shares the same AES module as the AAR and ECB peripherals. The ECB will always have the lowest priority. If an operation is aborted due to a conflict among the shared resources, an ERROR event will be generated.

Additionally, the CCM shares registers and other resources with the peripherals that have the same ID as the CCM. See Peripherals with shared ID on page 214 for more information.

8.4.2 Encryption and decryption

CCM supports both packet encryption and decryption.

The following table shows the different CCM input/output and parameters supported by the CCM module for encryption and decryption:

Parameter	Valid input	Description
M	0, 4, 6, 8, 10, 12, 14, 16	Number of bytes in the authentication field
L	2 (fixed)	Number of bytes in the length field
l(a)	0-65279	Number of bytes in additional authenticated data
l(m)	0-(65535 - M)	Number of bytes in the message to authenticate and encrypt
l(c)	0-65535	Number of bytes in the encrypted message; l(m) + M bytes
a	l(a) number of bytes	Additional authenticated data
m	l(m) number of bytes	Message to authenticate and encrypt
c	l(c) number of bytes	Encrypted message

Table 38: CCM Parameters

In addition to the parameters listed above, the CCM requires two sets of data: a 128-bit key and a 128-bit nonce. These are supplied via dedicated register interfaces: KEY.VALUE registers for the 128-bit key, and NONCE.VALUE registers for the 128-bit nonce. The 128-bit key in the KEY.VALUE registers is stored in