Interface of Ciphers and Authenticated Ciphers


Alice:
I love you!
Bob
Q W E R T Y U I O P
A S D F G H J K L return
Z X C V B N M
.?123
.?123


Alice:
I love you!
Bob

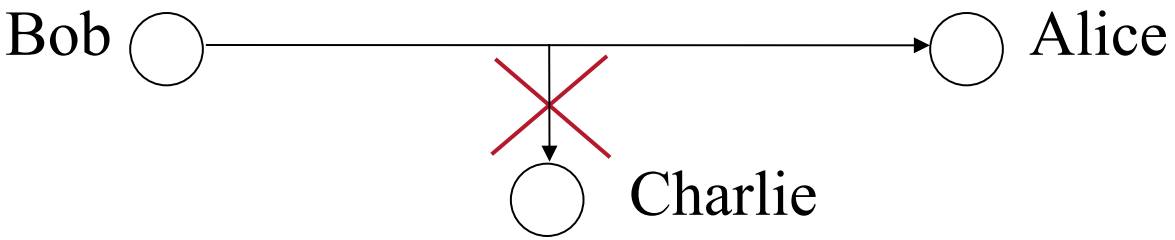




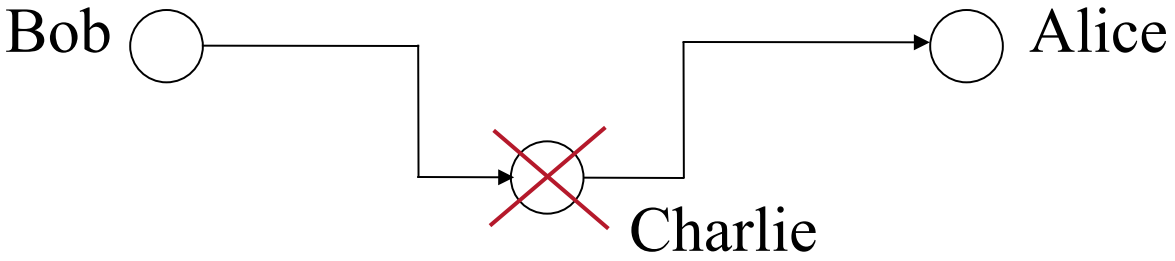
xcsdfsfgerkwerwedwkefrkgksdfsdmvasmga

Basic Security Services (1)

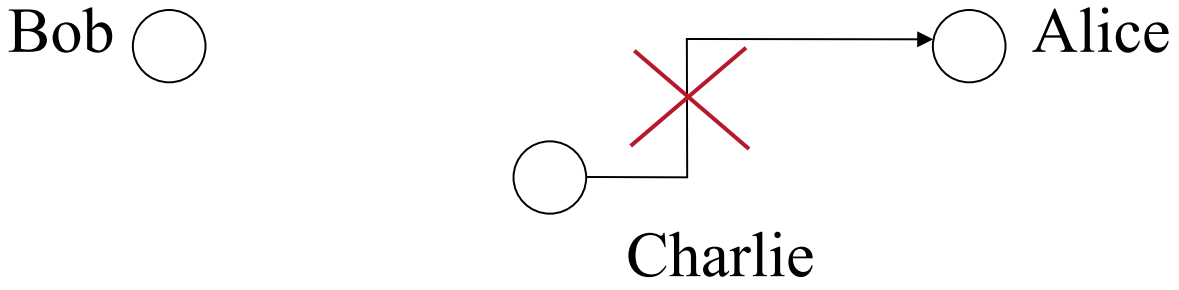
1. Confidentiality



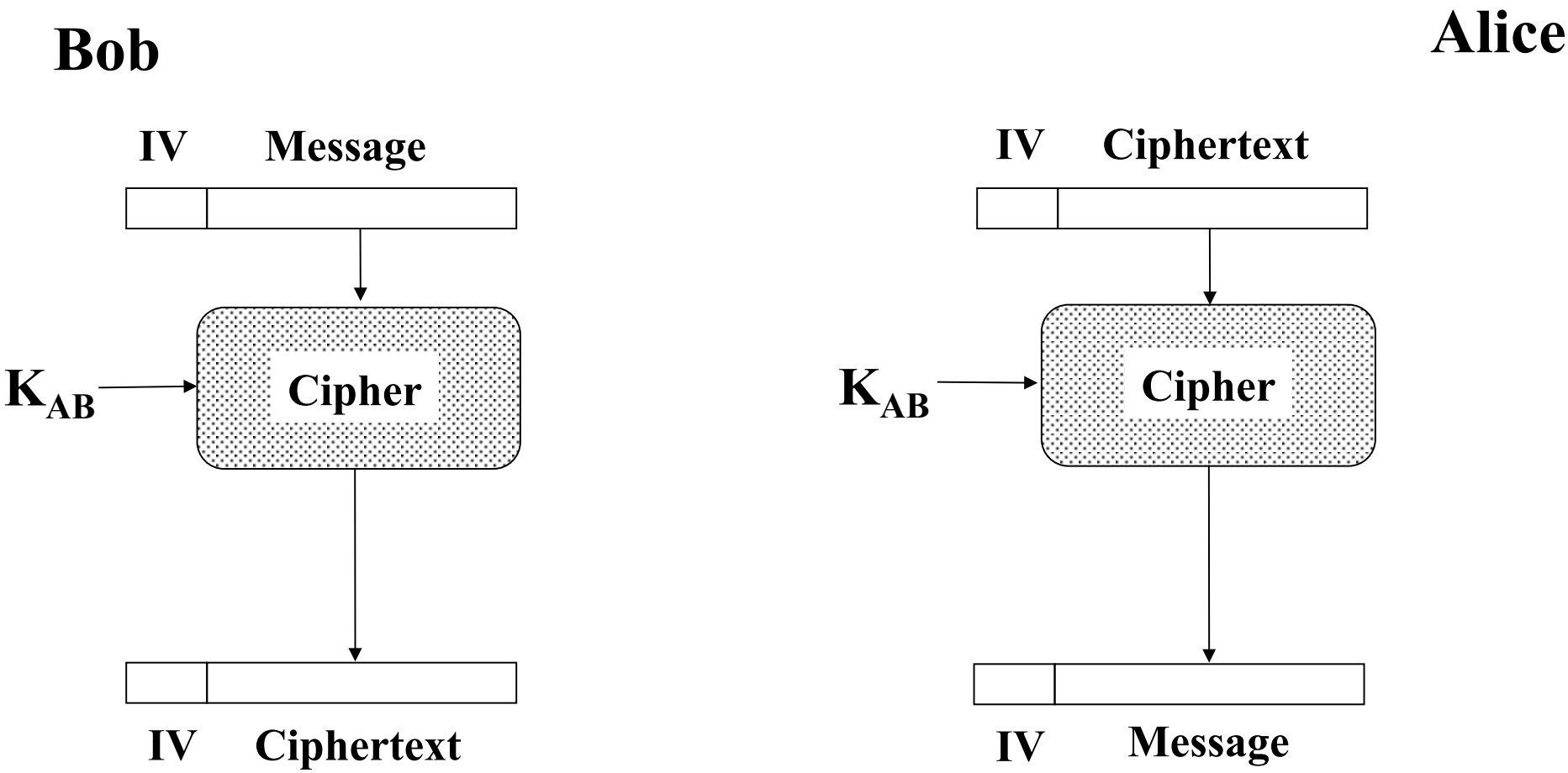
2. Message integrity



3. Message authentication



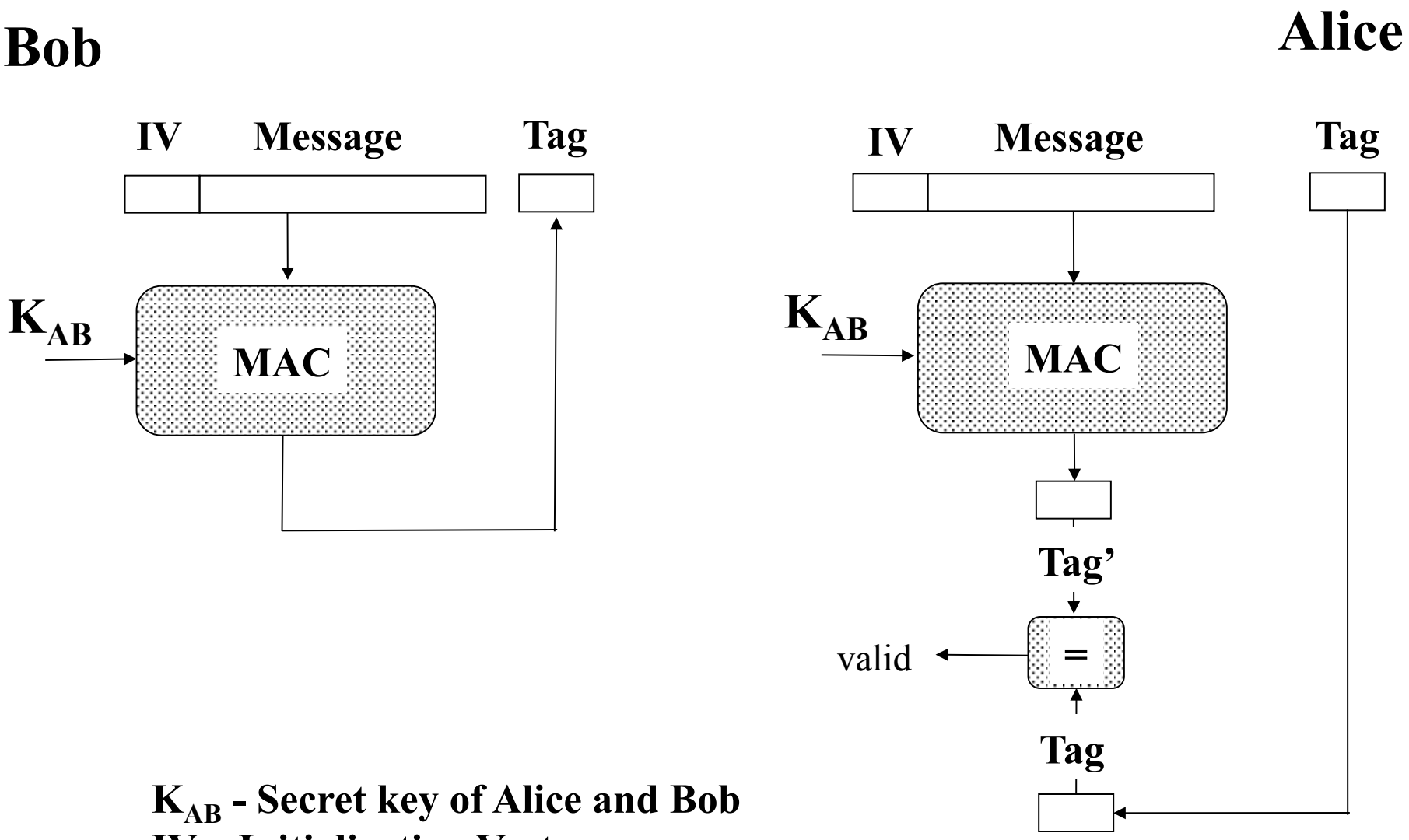
Confidentiality
Ciphers



K_{AB} - Secret key of Alice and Bob
IV – Initialization Vector

Authentication

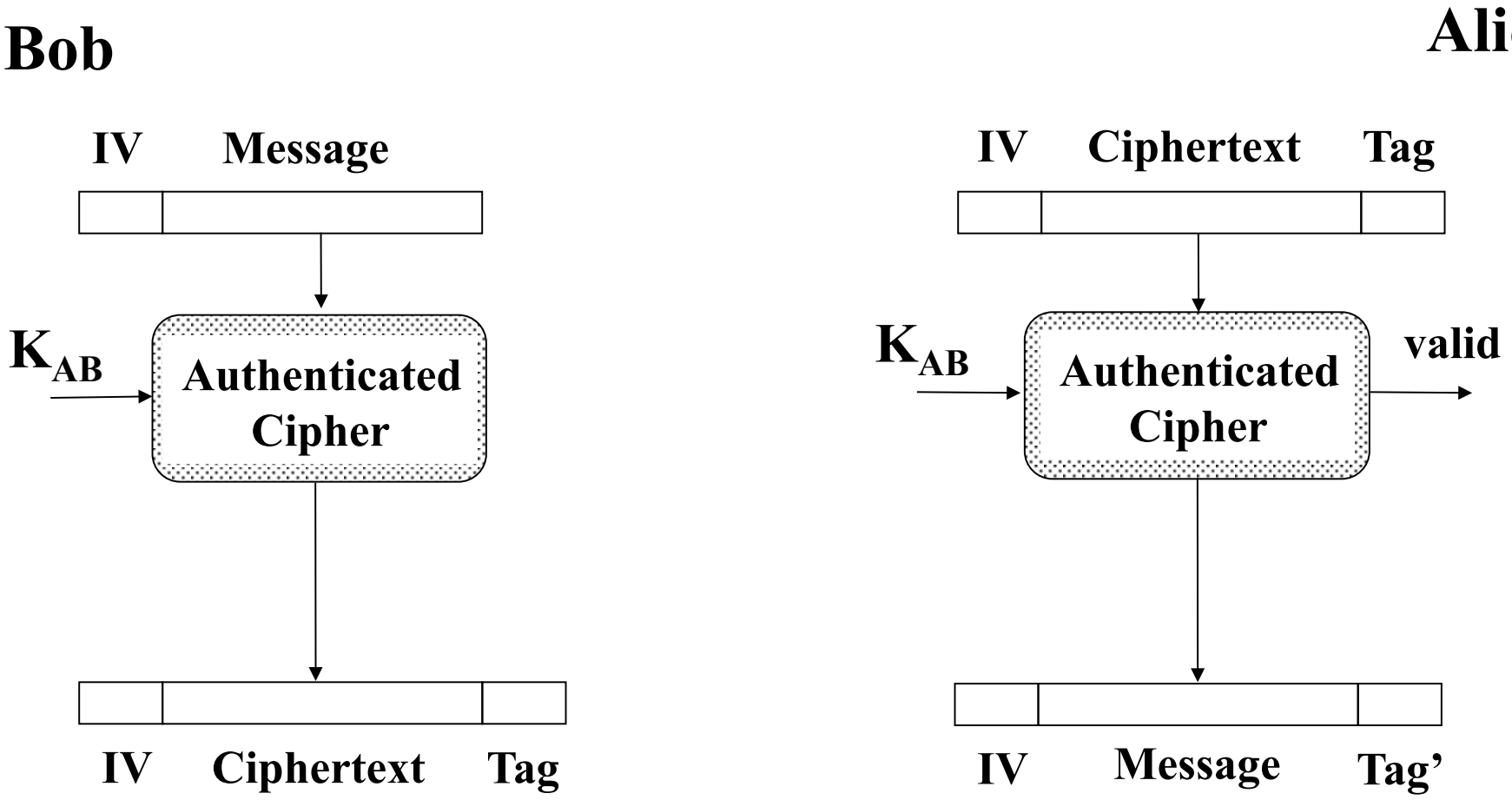
Message Authentication Code - MAC



K_{AB} - Secret key of Alice and Bob
IV – Initialization Vector

Confidentiality & Authentication

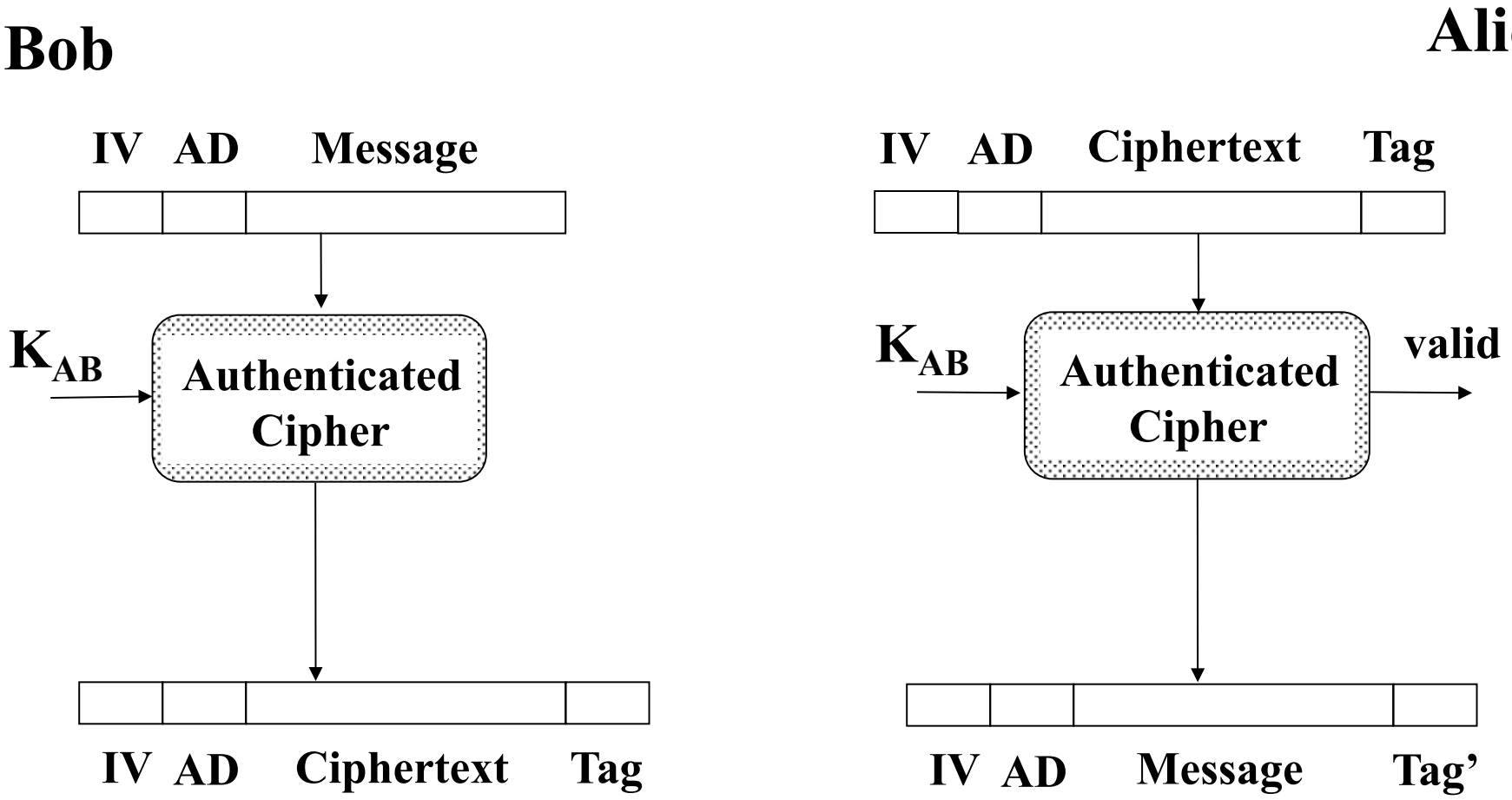
Authenticated Ciphers



K_{AB} - Secret key of Alice and Bob
IV – Initialization Vector

Confidentiality & Authentication

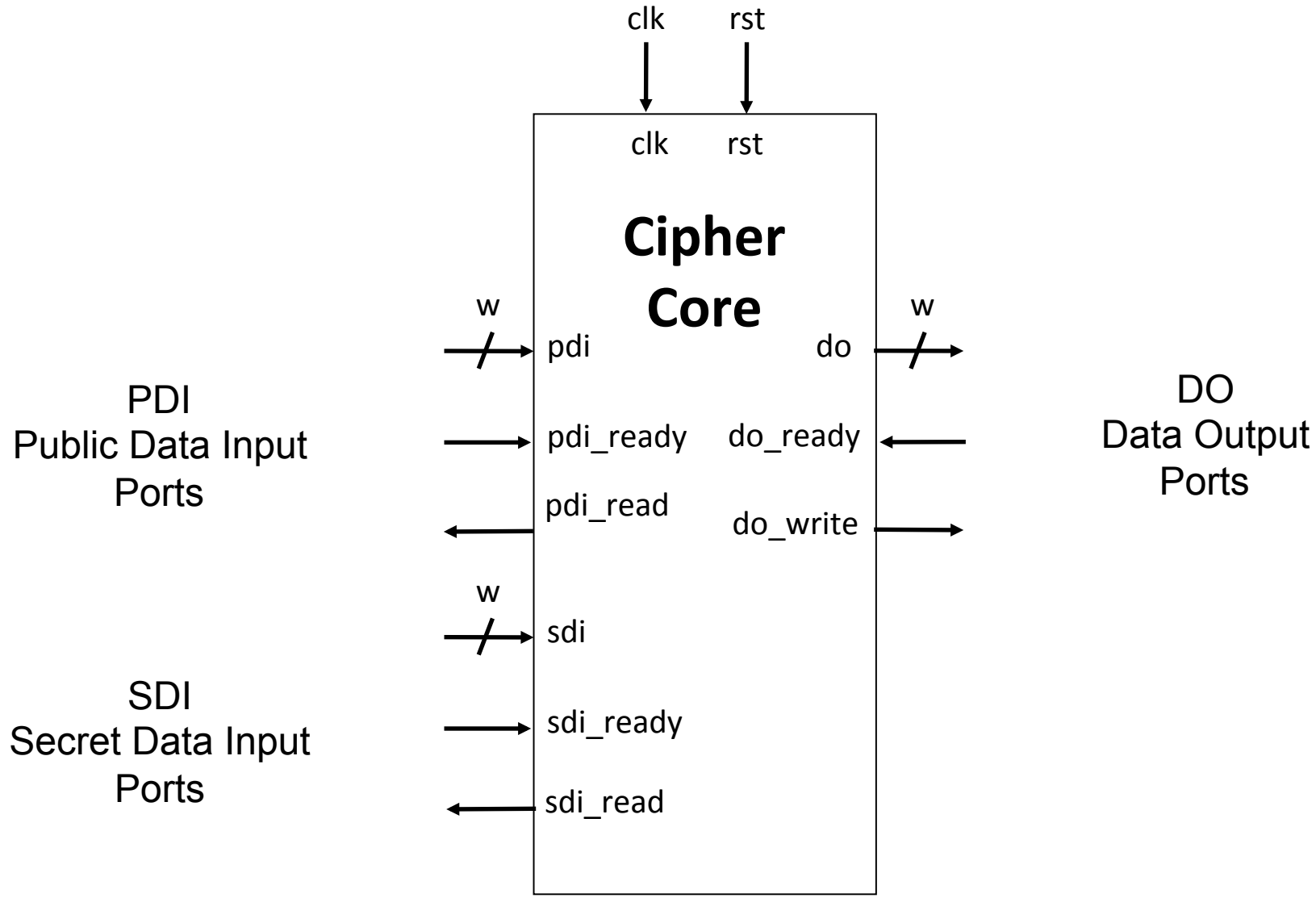
Authenticated Ciphers with Associated Data



K_{AB} - Secret key of Alice and Bob

IV – Initialization Vector, AD – Associated Data

Cipher Core Interface



Ciphers

Public Data Inputs:

Encryption:

- Initialization Vector - IV
- Message - M

Decryption:

- Initialization Vector - IV
- Ciphertext - C

Data Outputs:

Encryption:

- Initialization Vector - IV
- Ciphertext - C

Decryption:

- Initialization Vector - IV
- Message - M

Secret Data Input:

- Key - K

Authenticated Ciphers

Public Data Inputs:

Encryption:

- Initialization Vector - IV
- Associated Data - AD
- Message - M

Decryption:

- Initialization Vector - IV
- Associated Data - AD
- Ciphertext - C
- Tag - T

Data Outputs:

Encryption:

- Initialization Vector - IV
- Associated Data - AD
- Ciphertext - C
- Tag - T

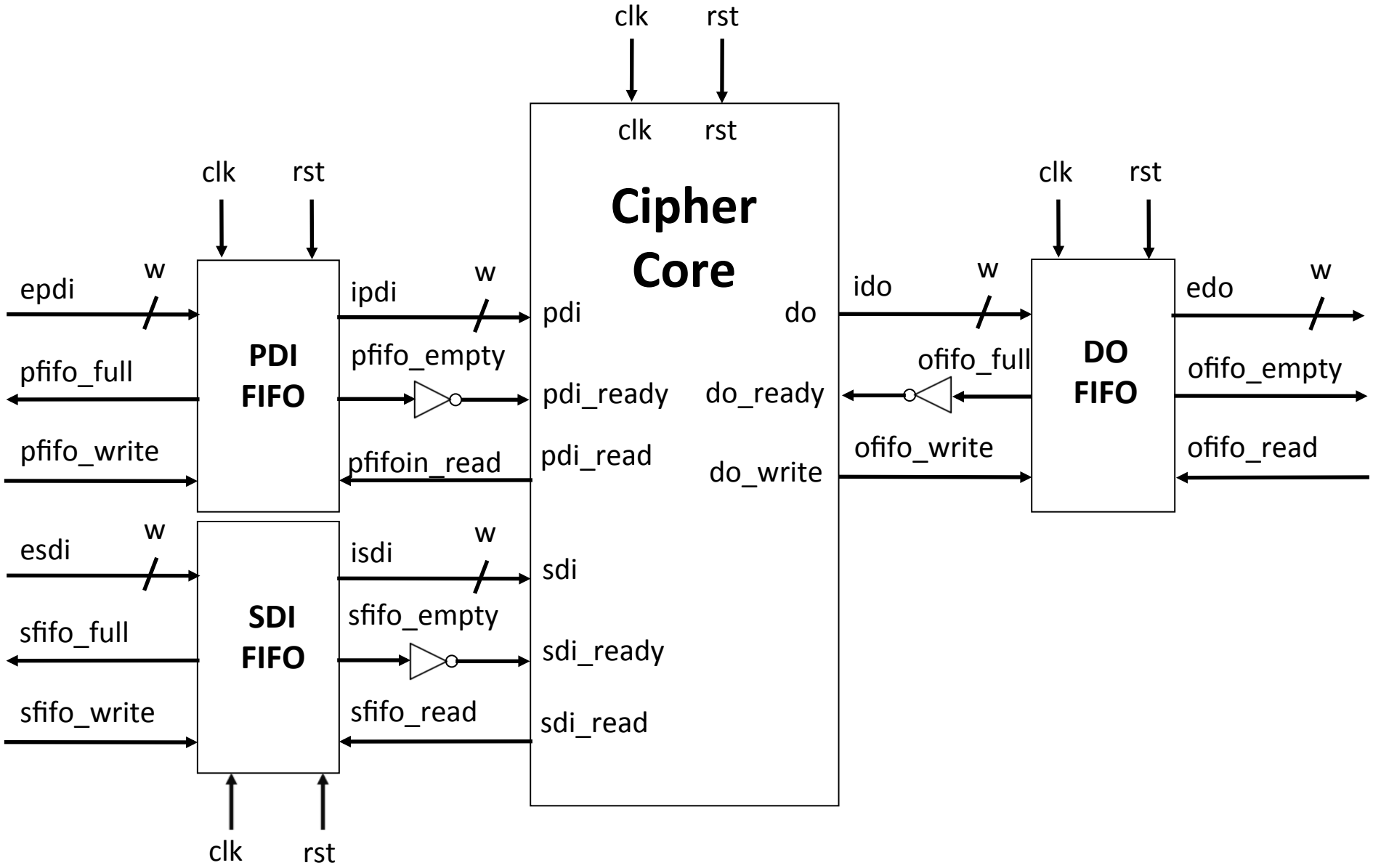
Decryption:

- Initialization Vector - IV
- Associated Data - AD
- Message - M
- Tag - T

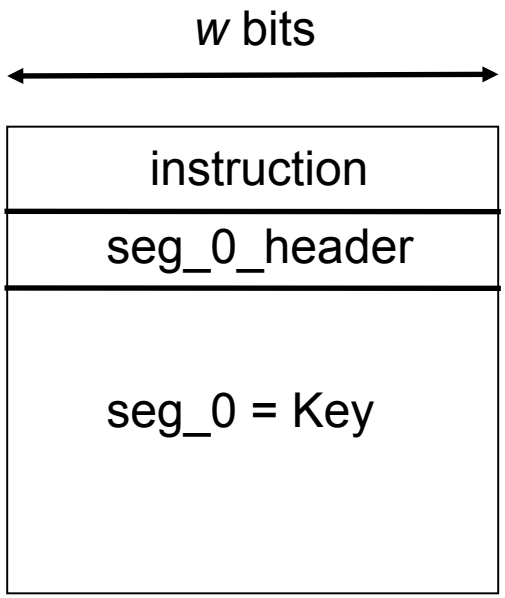
Secret Data Input:

- Key - K

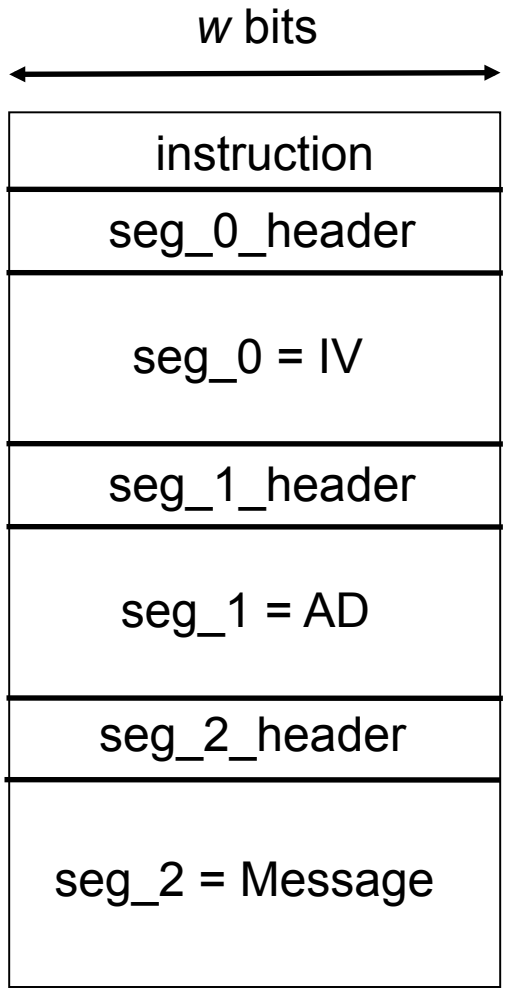
Typical External Circuit



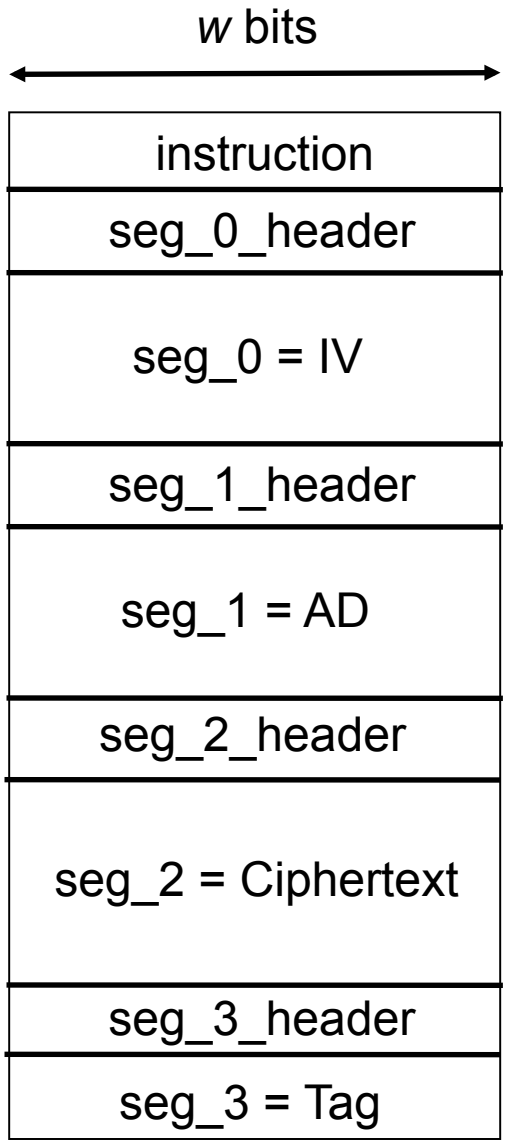
Format of Secret Data Input



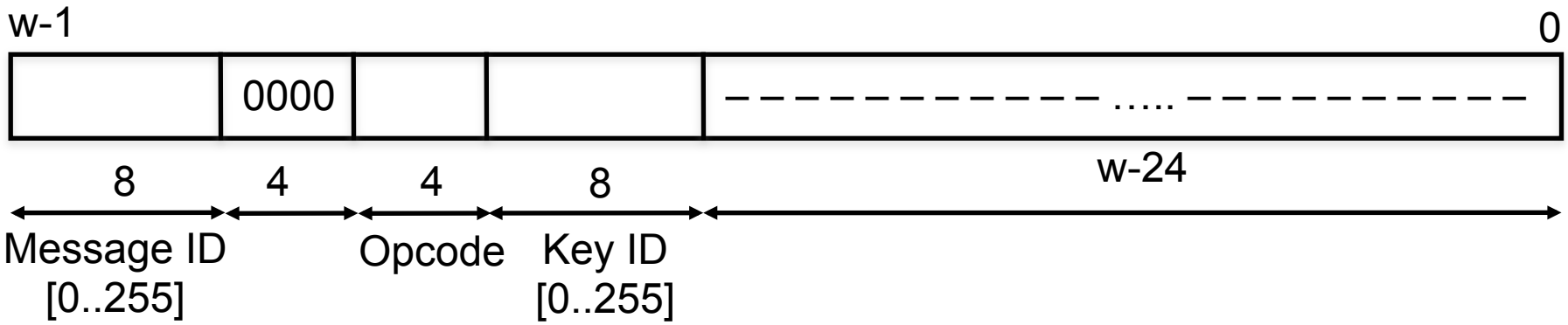
Format of Public Data Input
Authenticated Cipher - Encryption



Format of Data Output
Authenticated Cipher - Encryption

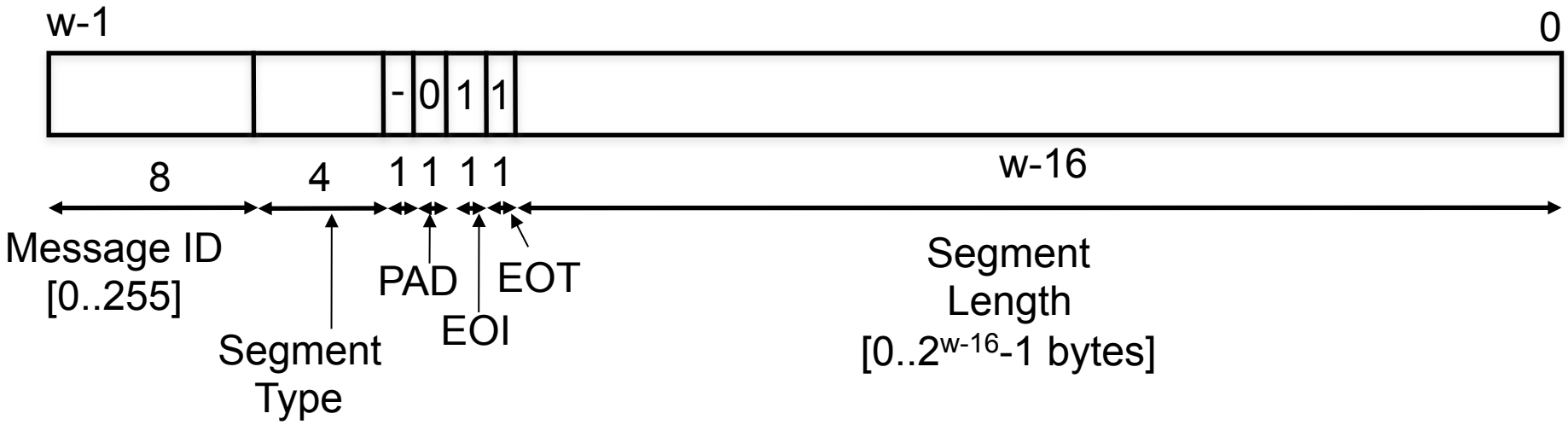


Instruction



0000 – Encryption
0001 – Decryption
0010 – Authenticated Encryption
0011 – Authenticated Decryption
0100 – Load Key
0101 – Activate Key

Segment Header



0000 – Reserved
0001 – Initialization Vector
0010 – Associated Data
0011 – Message
0100 – Ciphertext
0101 – Tag
0110 – Key

PAD = 1 if the input data segment contains padding
0 otherwise

EOI = 1 if the last segment of input
0 otherwise

EOT = 1 if the last segment of its type
0 otherwise