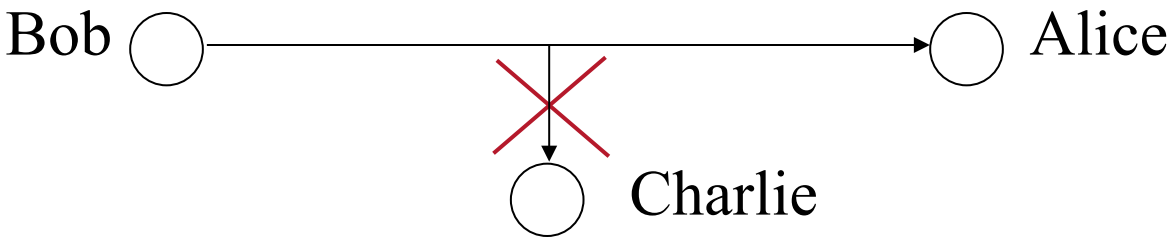
Interface of Ciphers and Authenticated Ciphers


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

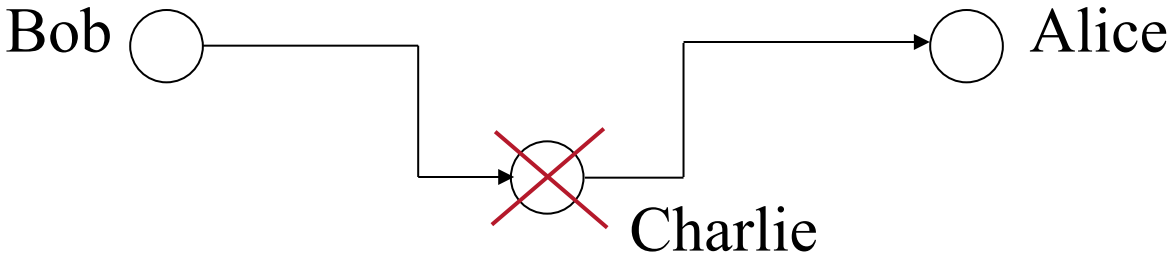

Alice:
I love you!
Bob

Basic Security Services (1)

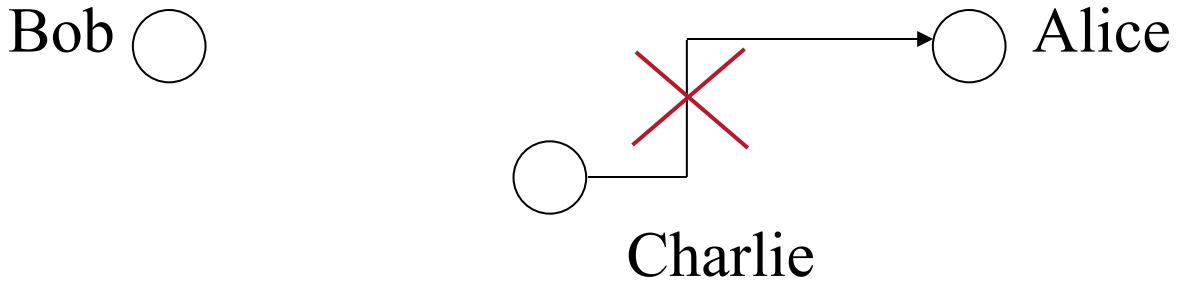
1. Confidentiality



2. Message integrity

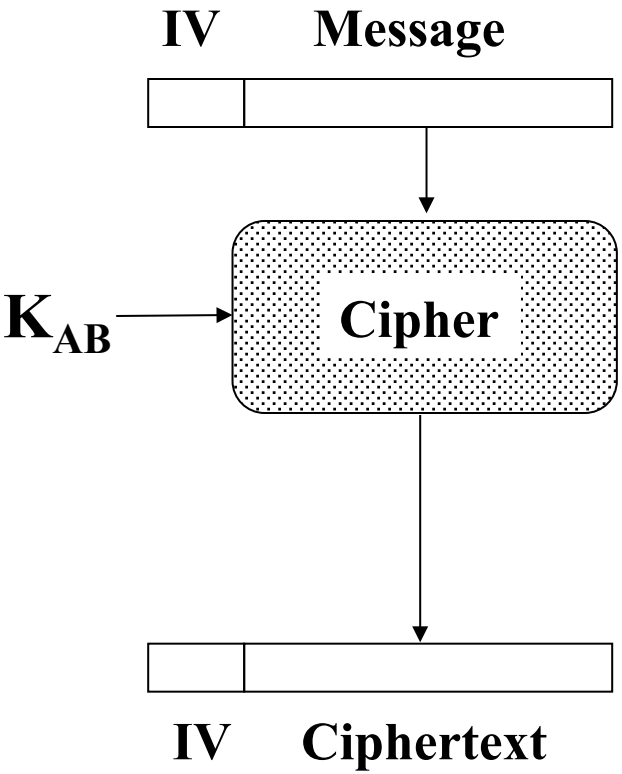


3. Message authentication

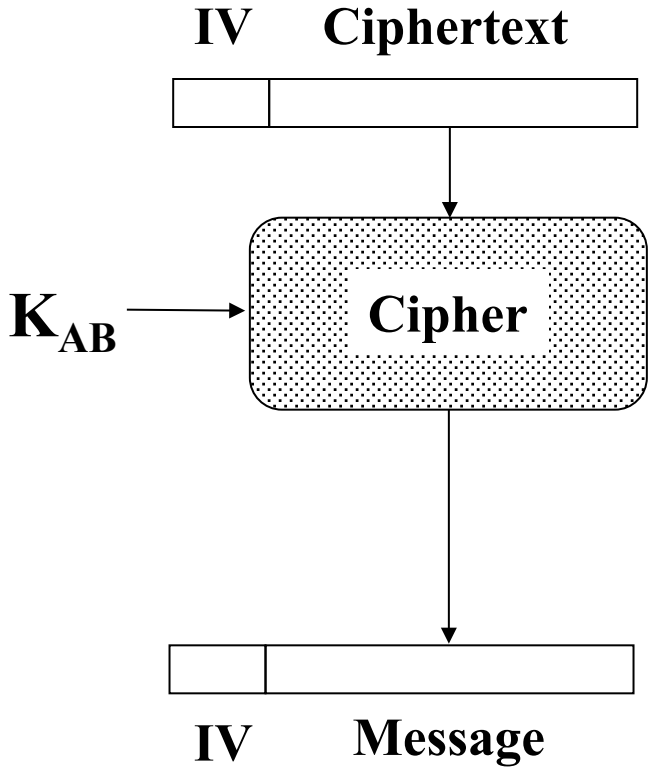


Confidentiality
Ciphers

Bob



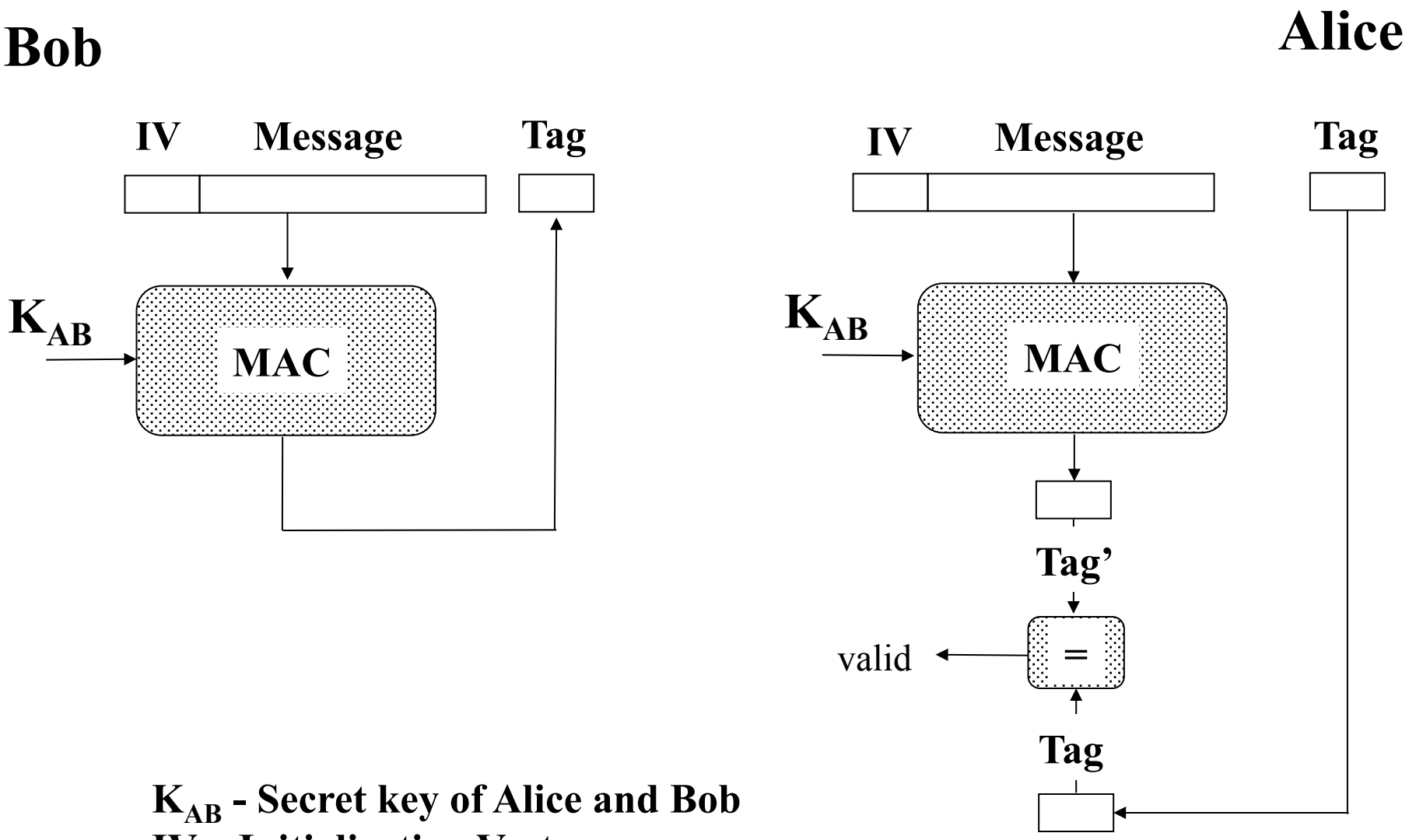
Alice



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

Authentication

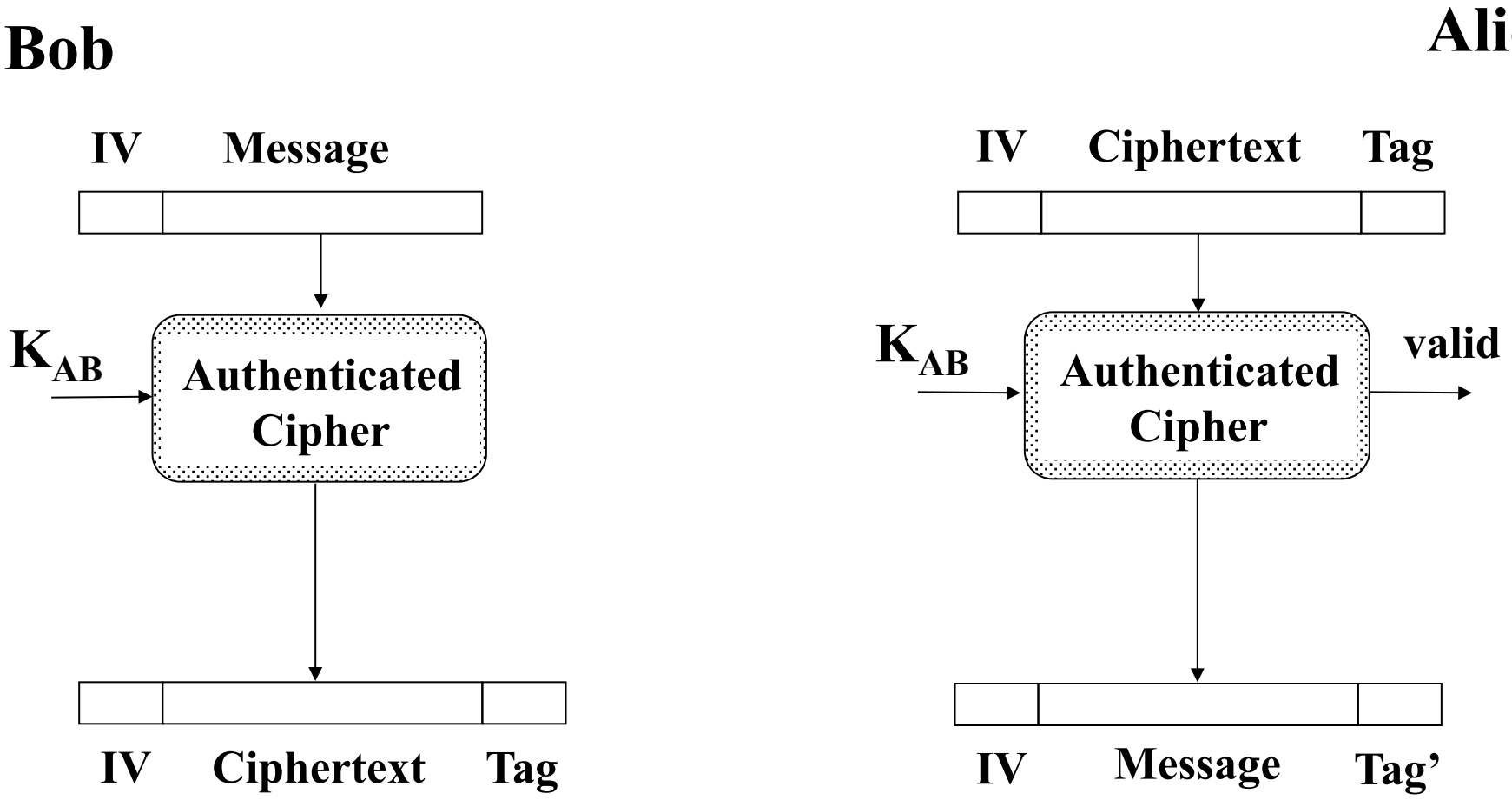
Message Authentication Code - MAC



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

Confidentiality & Authentication

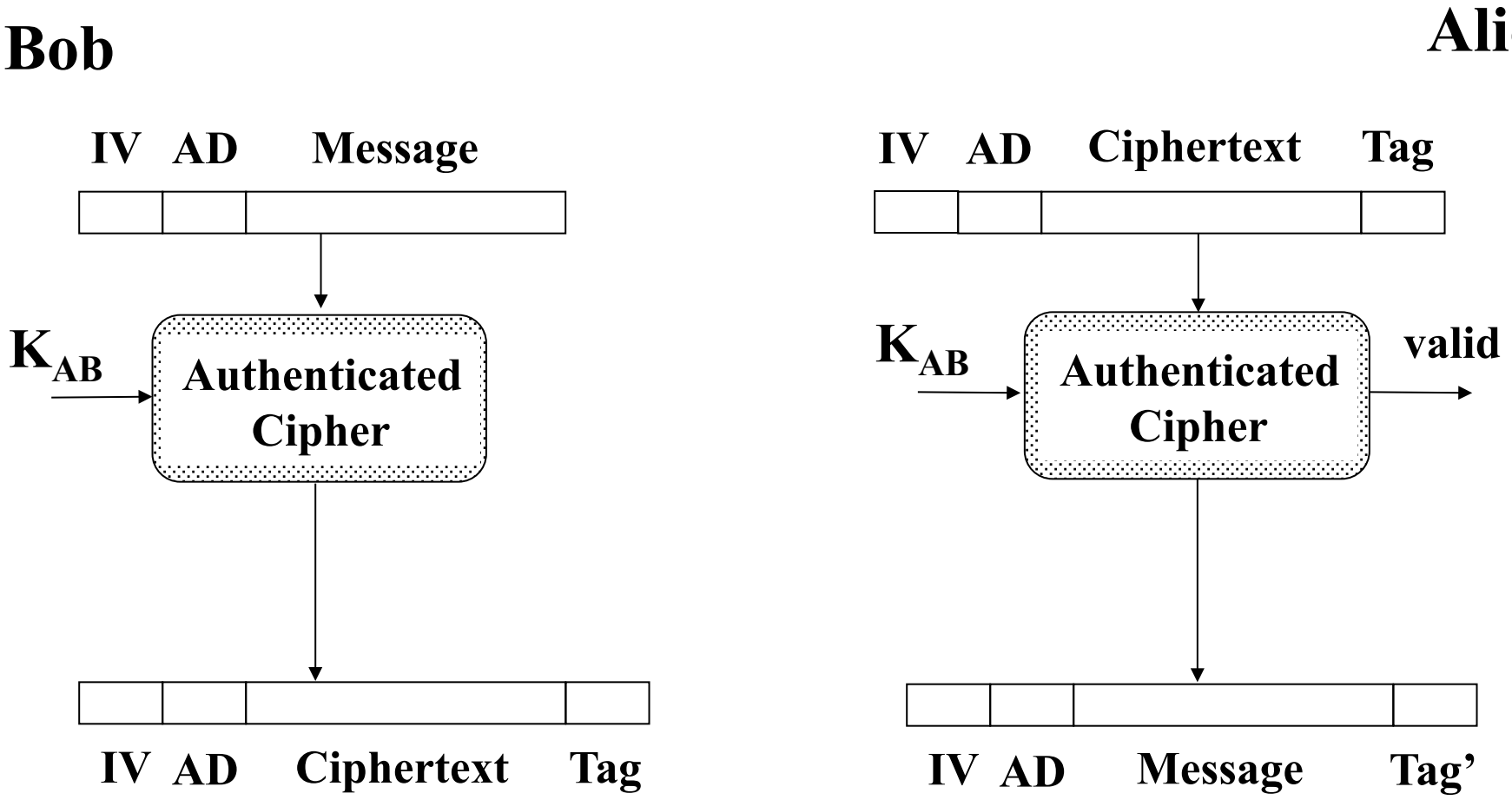
Authenticated Ciphers



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

Two Types of Ciphers

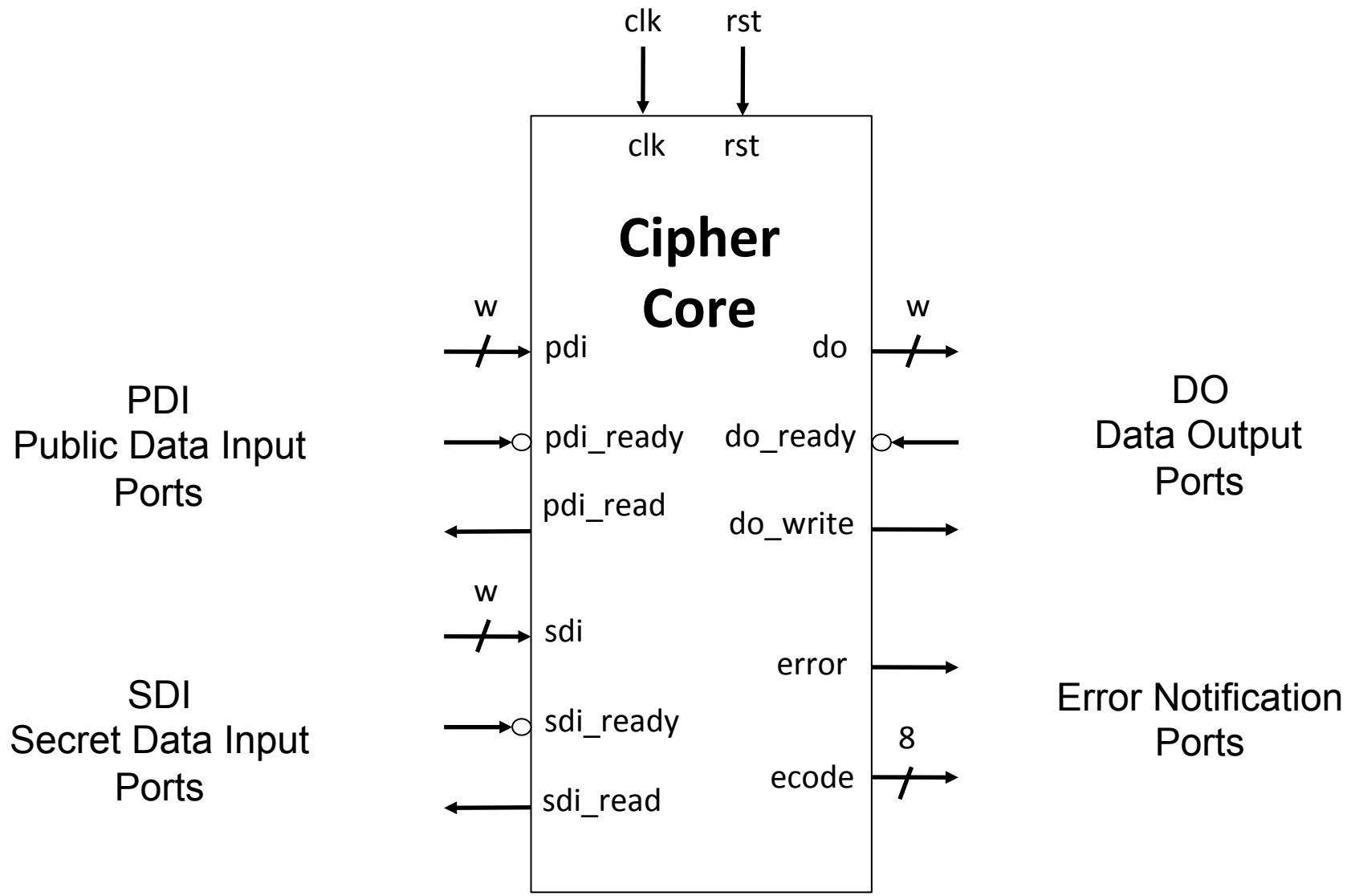
Ciphers:

- XTS-AES
- Salsa20/12
- KASUMI
- CLEFIA
- Rabbit
- SNOW 3G
- HIGHT
- SEED-128
- MISTY1
- Camellia

Authenticated Ciphers:

- AES-GCM
- AES-OCB3
- AES-OCB
- AES-CCM
- AES-EAX
- Grain-128a

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

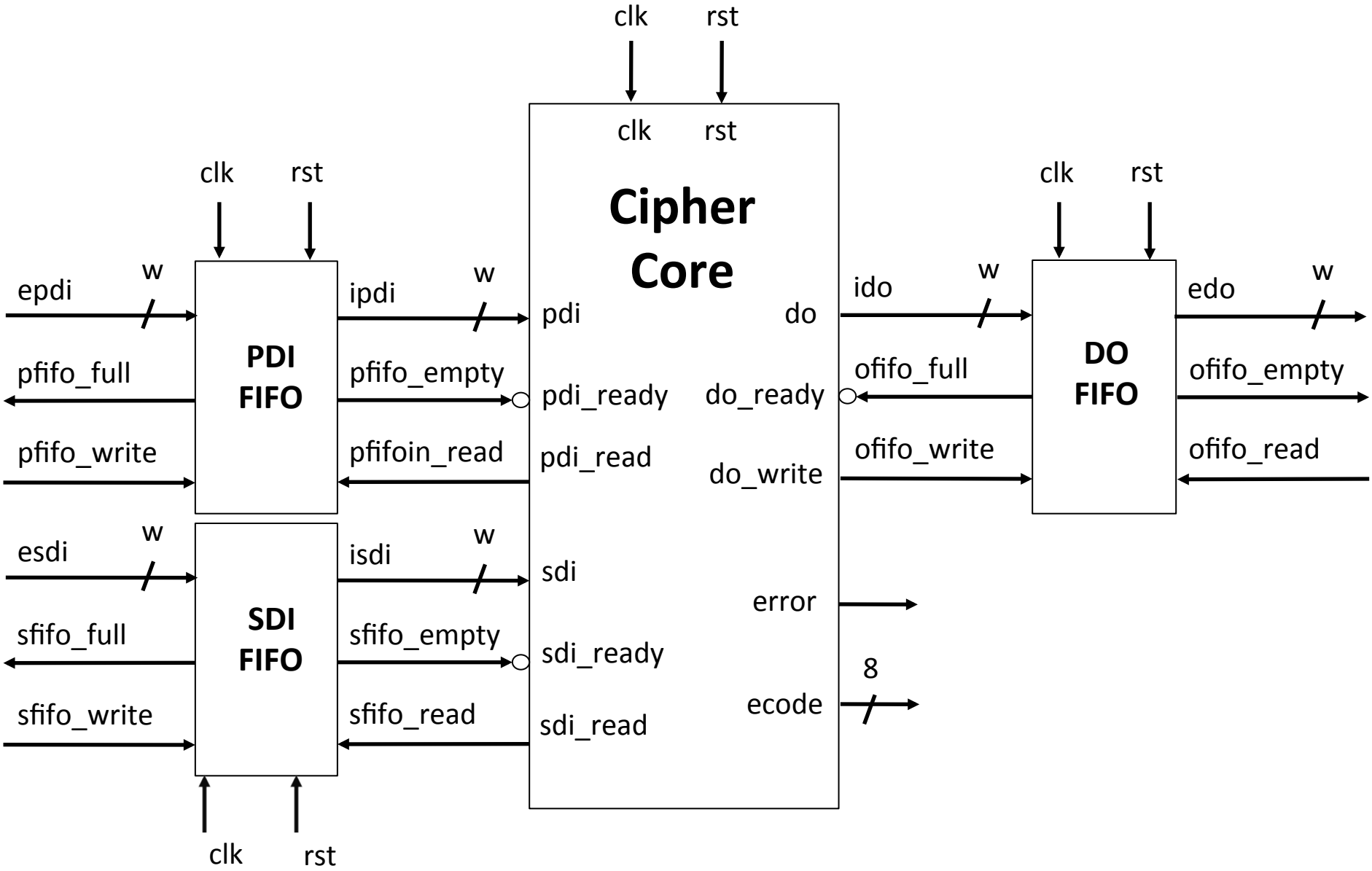
Decryption:

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

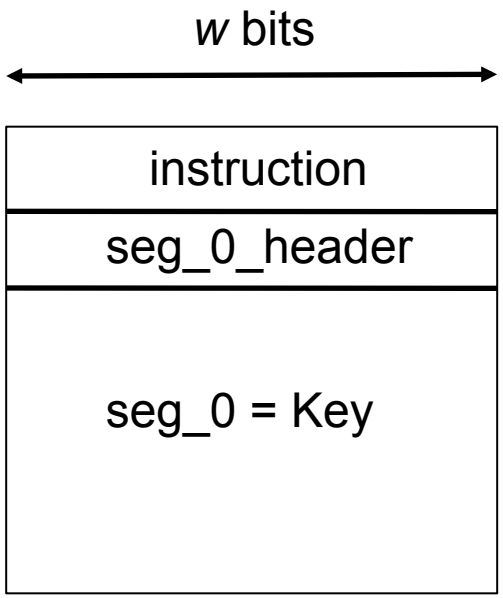
Secret Data Input:

- Key - K

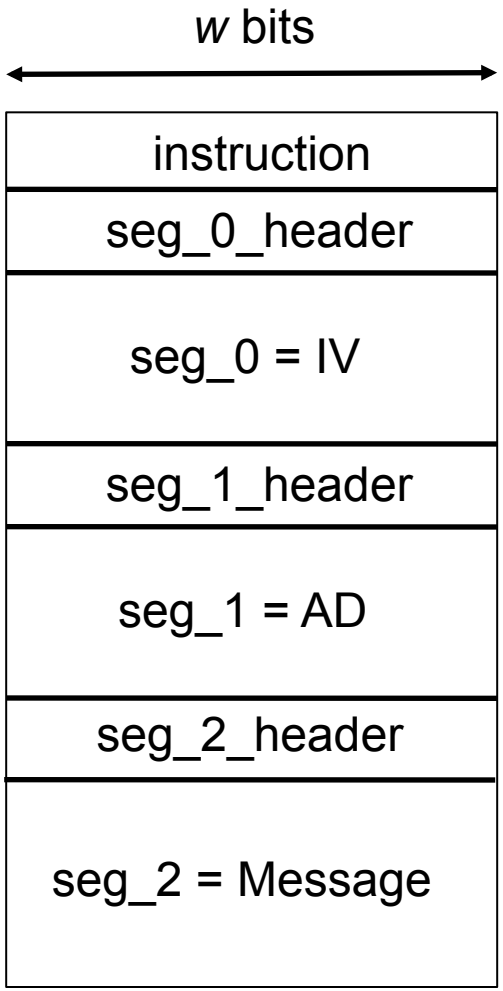
Typical External Circuit



Format of Secret Data Input

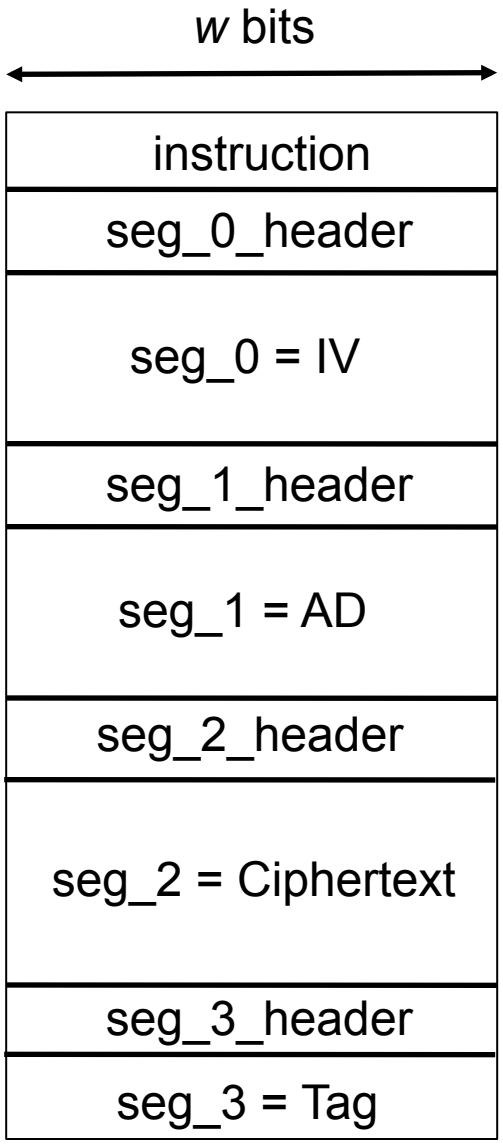


Format of Public Data Input
Authenticated Cipher - Encryption

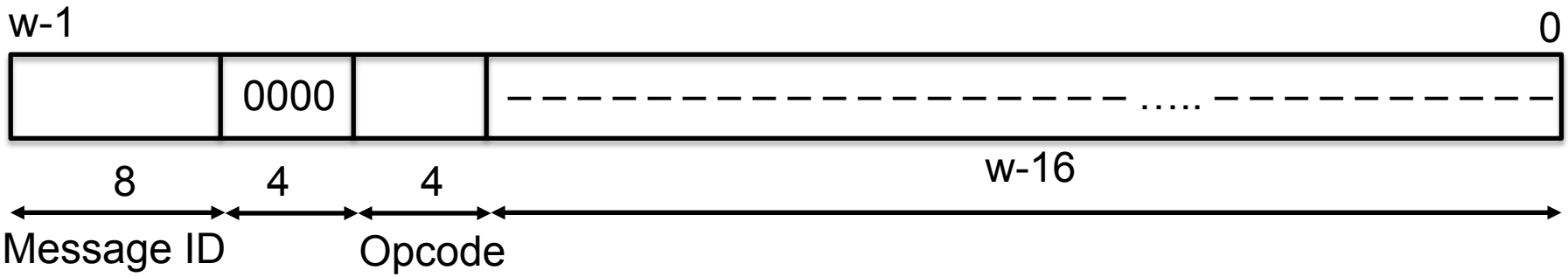


Format of Data Output

Authenticated Cipher - Encryption

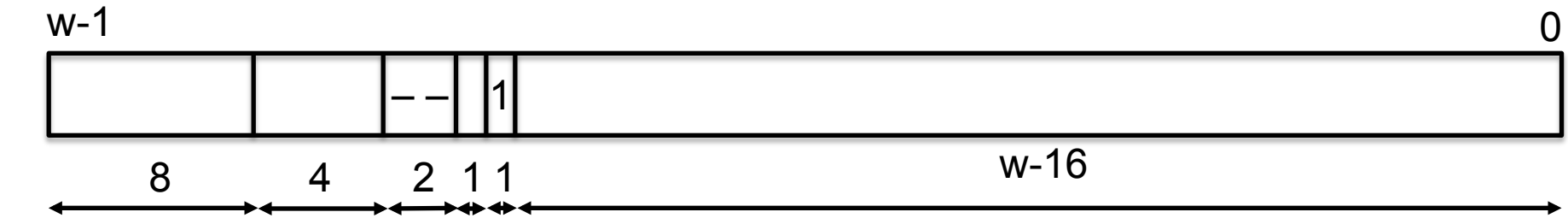


Instruction



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

Segment Header



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

LS = 1 if the last segment of input
0 otherwise

Error Codes

ecode output

0 – No error
1 – Unsupported opcode
2 – Uninitialized key
3 – Unsupported key length
4 – Unsupported IV length
5 – Unsupported tag length
6 – Segments out of sequence (e.g., Message before IV)
7 – Segment type incompatible with opcode (e.g., AD for Encryption)
8 – Invalid Tag