

# 现代密码学

## 第二十九讲 AES的密钥编排及伪代码

信息与软件工程学院

---

A decorative graphic consisting of ten horizontal blue lines of varying lengths, stacked vertically, is positioned in the top left corner.

## 第二十九讲 AES的密钥编排及伪代码

---

A diagram on the left side of the slide features a vertical line with two white circles. From each circle, a blue horizontal bar extends to the right, containing text. The top circle is connected to the top bar, and the bottom circle is connected to the bottom bar. The top bar contains the text 'AES的密钥编排' and the bottom bar contains 'AES的伪代码'.

AES的密钥编排

AES的伪代码

## 密钥编排

- 密钥编排指从种子密钥得到轮密钥的过程，它由密钥扩展和轮密钥选取两部分组成。其基本原则如下：
- (1) 轮密钥的比特数等于分组长度乘以轮数加1；例如要将128比特的明文经过10轮的加密，则总共需要  $(10+1) * 128 = 1408$  比特的密钥。
- (2) 种子密钥被扩展成为扩展密钥；
- (3) 轮密钥从扩展密钥中取，其中第1轮轮密钥取扩展密钥的前 $N_b$ 个字，第2轮轮密钥取接下来的 $N_b$ 个字，如此下去。

# 密钥扩展

- 扩展密钥是以4字节字为元素的一维阵列，表示为  $W[Nb * (N_r + 1)]$ ，其中前  $N_k$  个字取为种子密钥，以后每个字按递归方式定义。扩展算法根据  $N_k \leq 6$  和  $N_k > 6$  有所不同。

$w_0$	$w_1$	$w_2$	$w_3$	$w_4$	$w_5$	.....	
$k_{00}$	$k_{01}$	$k_{02}$	$k_{03}$	$k_{04}$	$k_{05}$		
$k_{10}$	$k_{11}$	$k_{12}$	$k_{13}$	$k_{14}$	$k_{15}$		
$k_{20}$	$k_{21}$	$k_{22}$	$k_{23}$	$k_{24}$	$k_{25}$		
$k_{30}$	$k_{31}$	$k_{32}$	$k_{33}$	$k_{34}$	$k_{35}$		

.....

A decorative blue horizontal bar with a series of horizontal lines is positioned to the left of the section header.

## 扩展算法 ( $N_k \leq 6$ )

---

**KeyExpansion (byteKey[4\*Nk] , W[Nb\*(Nr+1)])**

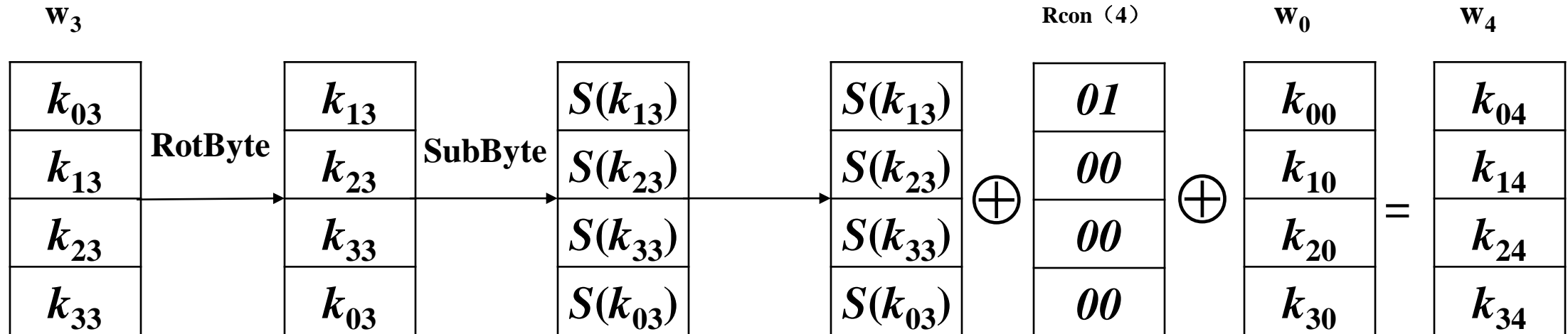
```
{  
    for (i =0; i < Nk; i ++)  
        W[i]=(Key[4* i],Key[4* i +1],Key[4* i +2],Key[4* i +3] );  
    for (i =Nk; i <Nb*(Nr+1); i ++)  
    {  
        temp=W[i-1];  
        if (i % Nk== 0)  
            temp=SubByte (RotByte (temp))^Rcon[i /Nk];  
        W[i]=W[i-Nk]^ temp;  
    }  
}
```

---

# 扩展算法 ( $N_k \leq 6$ ) (续)

$w_0$	$w_1$	$w_2$	$w_3$	$w_4$	$w_5$	.....	
$k_{00}$	$k_{01}$	$k_{02}$	$k_{03}$	$k_{04}$	$k_{05}$		
$k_{10}$	$k_{11}$	$k_{12}$	$k_{13}$	$k_{14}$	$k_{15}$		
$k_{20}$	$k_{21}$	$k_{22}$	$k_{23}$	$k_{24}$	$k_{25}$		
$k_{30}$	$k_{31}$	$k_{32}$	$k_{33}$	$k_{34}$	$k_{35}$		

.....



# 扩展算法 ( $N_k \leq 6$ ) (续)

$w_0$	$w_1$	$w_2$	$w_3$	$w_4$	$w_5$	.....	
$k_{00}$	$k_{01}$	$k_{02}$	$k_{03}$	$k_{04}$	$k_{05}$		
$k_{10}$	$k_{11}$	$k_{12}$	$k_{13}$	$k_{14}$	$k_{15}$		
$k_{20}$	$k_{21}$	$k_{22}$	$k_{23}$	$k_{24}$	$k_{25}$		
$k_{30}$	$k_{31}$	$k_{32}$	$k_{33}$	$k_{34}$	$k_{35}$		

.....

$$\begin{array}{|c|} \hline w_1 \\ \hline k_{01} \\ \hline k_{11} \\ \hline k_{21} \\ \hline k_{31} \\ \hline \end{array} \oplus \begin{array}{|c|} \hline w_4 \\ \hline k_{04} \\ \hline k_{14} \\ \hline k_{24} \\ \hline k_{34} \\ \hline \end{array} = \begin{array}{|c|} \hline w_5 \\ \hline k_{05} \\ \hline k_{15} \\ \hline k_{25} \\ \hline k_{35} \\ \hline \end{array}$$

## 扩展算法 ( $N_k > 6$ )

**KeyExpansion (byte Key[4\*Nk] , W[Nb\*(Nr+1)])**

```
{  
    for (i=0; i < Nk; i ++)  
        W[i]=(Key[4* i], Key[4* i +1], Key[4* i +2], Key[4* i +3] );  
    for (i =Nk; i <Nb*(Nr+1); i ++)  
    {  
        temp=W[i -1];  
        if (i % Nk== 0)  
            temp=SubByte (RotByte (temp))^Rcon[i /Nk];  
        else if (i % Nk==4)  
            temp=SubByte (temp);  
        W[i]=W[i - Nk]^ temp;  
    }  
}
```

$N_k > 6$  与  $N_k \leq 6$  的密钥扩展算法的区别在于：当  $i-4$  为  $N_k$  的整数倍时，须先将前一个字  $W[i-1]$  经过 SubByte 变换

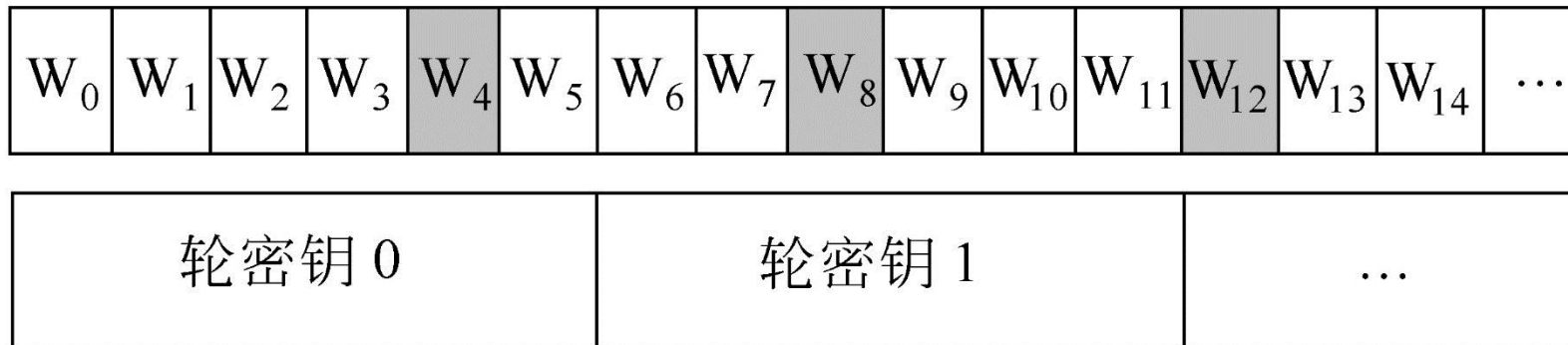


## 轮常数

- 以上两个算法中， $\mathbf{Rcon}[i/Nk]$  为轮常数，其值与 $Nk$ 无关，定义为（字节用十六进制表示，同时理解为 $\mathbf{GF}(2^8)$ 上的元素）：
  - $\mathbf{Rcon}[i] = (\mathbf{RC}[i], '00', '00', '00')$
  - 其中 $\mathbf{RC}[i]$  是 $\mathbf{GF}(2^8)$  中值为 $x^{i-1}$ 的元素，因此
    - $\mathbf{RC}[1] = 1$  (即 '01')
    - $\mathbf{RC}[i] = x$  (即 '02')  $\cdot \mathbf{RC}[i-1] = x^{i-1}$

## 轮密钥选取

- 轮密钥 $i$ （即第 $i$ 个轮密钥）由轮密钥缓冲字 $W[Nb * i]$ 到 $W[Nb * (i+1)]$ 给出，如图所示。



$N_b=6$ 且 $N_k=4$ 时的密钥扩展与轮密钥选取

A decorative graphic consisting of several horizontal blue lines of varying lengths, stacked vertically, is positioned in the top left corner.

## 第二十九讲 AES的密钥编排及伪代码

---

A diagram on the left side of the slide shows two white circles connected by a vertical line. From the top circle, a line extends upwards and to the left. From the bottom circle, a line extends downwards and to the left. Each circle is partially overlapped by a blue rectangular box containing text.

AES的密钥编排

AES的伪代码

A decorative blue horizontal bar with a series of horizontal lines is positioned on the left side of the slide.

# AES加密过程的伪代码

---

**Cipher(byte in[4\*Nb], byte out[4\*Nb], word w[Nb\*Nr+1])**

**begin**

**byte state[4,Nb]**

**state = in**

**AddRoundKey(state, w[0, Nb-1])**

**for round = 1 step 1 to Nr-1**

**SubBytes(state)**

**ShiftRows(state)**

**MixColumns(state)**

**AddRoundKey(state, w[round\*Nb, (round+1)\*Nb-1])**

**end for**

**SubBytes(state)**

**ShiftRows(state)**

**AddRoundKey(state, w[Nr\*Nb, (Nr+1)\*Nb-1])**

**Out = state**

---

**end**

A decorative blue horizontal bar with a series of horizontal lines is positioned on the left side of the slide.

# AES解密过程的伪代码

---

**InvCipher(byte in[4\*Nb], byte out[4\*Nb], word w[Nb\*Nr+1])**

**begin**

**byte state[4,Nb]**

**state = in**

**AddRoundKey(state, w[Nr\*Nb, (Nr+1)\*Nb-1])**

**for round = Nr-1 step -1 downto 1**

**InvShiftRows(state)**

**InvSubBytes(state)**

**AddRoundKey(state, w[round\*Nb, (round+1)\*Nb-1])**

**InvMixColumns(state)**

**end for**

**SubBytes(state)**

**ShiftRows(state)**

**AddRoundKey(state, w[0, Nb-1])**

**Out = state**

---

**end**

A decorative blue horizontal bar with white horizontal stripes is positioned to the left of the title.

# AES密钥编排算法的伪代码

---

```
KeyExpansion (byte key[4*Nk] , word w[Nb*(Nr+1)], Nk)
begin
    word temp
    i=0
    while (i<Nk)
        w[i]=word(Key[4* i], Key[4* i +1], Key[4* i +2], Key[4* i +3] )
        i=i+1
    end while
    i=Nk
    while(i<Nb*(Nr+1))
        temp=W[i-1]
        if (I mod Nk= =0)
            temp=SubByte (RotByte (temp)) xor Rcon[i /Nk]
        else if (Nk>6 and i mod Nk = 4)
            temp=SubWord(temp)
        end if
        w[i]=w[i-Nk ] xor temp
    end while
end
```



感谢聆听!

xynie@uestc.edu.cn