实验原理

一．IDEA算法简介

IDEA（International Data Encryption Alogrithm）是由瑞士苏黎士联邦工业大学的XueJiaLai和James L.Massey 于1991年提出的。IDEA使用128比特密钥，整个算法和DES相似，也是将明文划分成一个个64比特长的数据分组，然后经过几次迭代和一次变换，得出64比特的密文。

IDEA是将两个16比特的值映射为一个16比特的值，这些操作是：

- 半加运算，即“异或”运算，用符号“⊕”表示。所谓的半加运算，就是在进行二进制运算时只加，不进位。
- 模2^{16}的加法运算（即mod 65536），用“+”表示。
- 模2^{16}+1乘运算用符号“⊙”表示。

实际上，⊙是将两个输入的数进行乘法运算，然后再对此结果按模2^{16}+1运算得出的结果。对于这样的运算应该注意的是，参与运算的任何一个二进制数据n位，如果全是0，则用n+1位数据表示，且最高位为1，其余全为0。

为了理解以上三种操作，我们用2位的数来表示以上的三种关系，如表6-3-1所示。

表6-3-1　IDEA三种操作的关系

X		Y		X⊞Y		X⊙Y		X⊕Y	
十进制	二进制	十进制	二进制	十进制	二进制	十进制	二进制	十进制	二进制
0	00	0	00	0	00	1	01	0	00
0	00	1	01	1	01	0	00	1	01
0	00	2	10	2	10	3	11	2	10
0	00	3	11	3	11	2	10	3	11
1	01	0	00	1	01	0	00	1	01
1	01	1	01	2	10	1	01	0	00
1	01	2	10	3	11	2	10	3	11
1	01	3	11	0	00	3	11	2	10
2	10	0	00	2	10	3	11	2	10
2	10	1	01	3	11	2	10	3	11
2	10	2	10	0	00	0	00	0	00
2	10	3	11	1	01	1	01	1	01
3	11	0	00	3	11	2	10	3	11
3	11	1	01	0	00	3	11	2	10
3	11	2	10	1	01	1	01	1	01
3	11	3	11	2	10	0	00	0	00

二．IDEA算法加密过程

1．IDEA迭代过程

IDEA加密算法采用8次迭代，如图6-3-1所示：

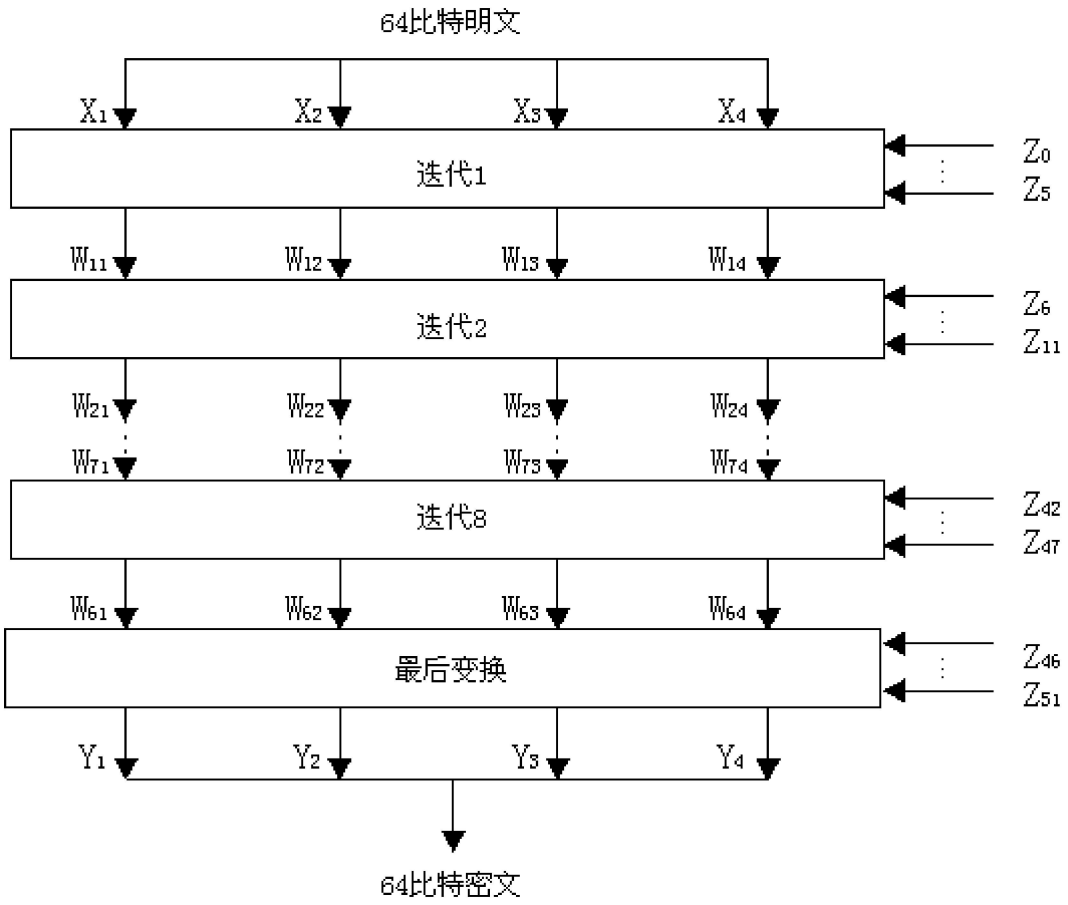

图6-3-1　8次迭代

64比特的密钥生成的数据被分成8个子块，每个子块16比特。每一次迭代过程如图6-3-2所示：

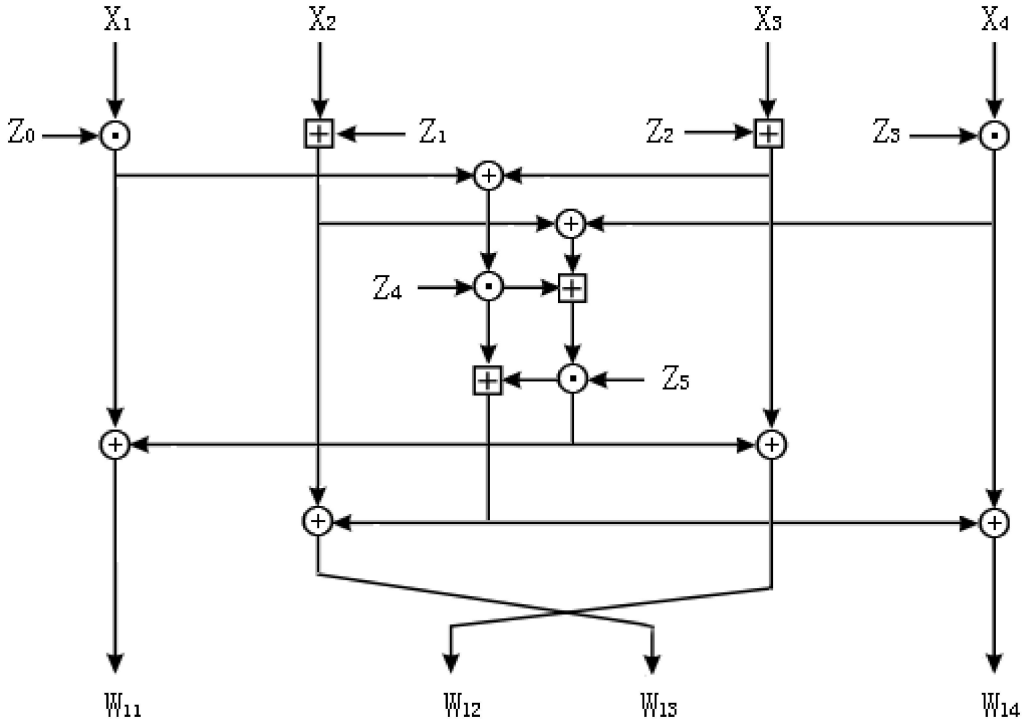

图6-3-2　单次迭代过程

「说明」 图中⊕表示异或运算；⊞表示模2^{16}的加法运算； ⊙表示模2^{16}+1的乘法运算。

X1，X2，X3和X4作为第一次迭代的输入，每轮的迭代都是4个子块以及16比特子密钥间的异或运算，模2^{16}做加法运算和模（2^{16}+1）的乘法运算。

迭代步骤如下：

（1）X1和第一个子密钥块做乘法运算。

（2）X2和第二个子密钥块做加法运算。

（3）X3和第三个子密钥块做加法运算。

（4）X4和第四个子密钥块做乘法运算。

（5）（1）和（3）的结果做异或运算。

（6）（2）和（4）的结果做异或运算。

（7）（5）的结果和第五个子密钥块做乘法运算。

（8）（6）和（7）的结果做加法运算。

（9）（8）的结果与第六个子密钥块做乘法运算。

（10）（7）和（9）的结果做加法运算。

（11）（1）和（9）的结果做异或运算。

（12）（3）和（9）的结果做异或运算。

（13）（2）和（10）的结果做异或运算。

（14）（4）和（10）的结果做异或运算。

每轮完成以上的14次运算，共进行8轮，然后进行最后的输出变换，如图6-3-3所示。经过8轮迭代运算后，W_{81}，W_{82}，W_{83}，W_{84}分别与Z_{48}，Z_{49}，Z_{50}，Z_{51}运算得到Y_1，Y_2，Y_3和Y_4。其方法如下：

$Y_1 = Z_{48} \odot W_{81}$　　$Y_3 = Z_{50} \boxplus W_{82}$

$Y_2 = Z_{49} \boxplus W_{83}$　　$Y_4 = Z_{51} \odot W_{84}$

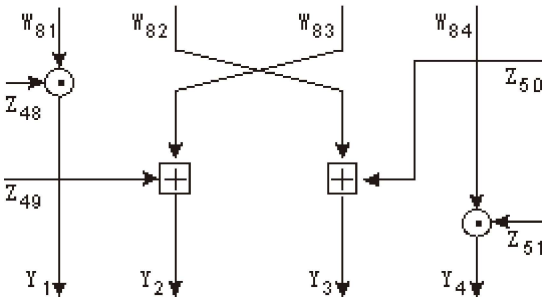

图6-3-3　8轮迭代变换后的输出变换

2．IDEA密钥生成过程

在图6-3-3中可以看出，在加密过程中共有52个子密钥块参与运算，每个块长16比特。这52个密钥块是由128比特密钥产生的，我们将这52个密钥块记为Z0，Z1……，Z51。最初的8个子密钥Z0，Z1，……，Z7是直接来自用户输入，Z0是用户输入密钥的前16比特；Z1是用户输入密钥的第二个16比特，Z7是用户输入密钥的最后16比特。这样从Z0到Z7的密钥共计长度为128比特。

IDEA每一轮迭代使用6个子密钥，每个子密钥有16位，这意味着在一轮迭代中，密钥中只有96位被使用。最初的6个连续的子密钥（Z0到Z5）直接用于第一轮迭代，然后128位的密钥要循环左移25位，之后再取密钥的前96位作为下一轮的6个子密钥。以此类推，直到8轮迭代全部完成。

3．IDEA解密算法与其加密的关系

IDEA的解密处理和其加密处理基本相同，只是解密处理输入的是密文，选择的密钥不大相同，但也有一定的联系。它与加密密钥的关系如下。

解密过程的第i轮前四个密钥是与加密过程中的第（10-i）轮的相同，最后置换作为第9轮。解密过程的第1和第4轮是对应加密处理过程第1轮和第4轮的模（$2^{16}+1$）乘运算，解密过程中的第2轮和第3轮对应与加密过程中的第3轮和第2轮的模2^{16}的加运算。

在前8轮运算中，解密的第i轮的最后两个子密钥块等于加密过程中的第9-i轮的最后两个子密钥块。每一轮的加密和解密的子密钥关系如表6-3-2所示。

表6-3-2　加密和解密的子密钥关系

加解密轮次	每轮的加密密钥	原始密钥对应的位
第一轮	$Z_0Z_1Z_2Z_3Z_4Z_5$	$Z_{48}^{-1}-Z_{49}-Z_{50}Z_{51}^{-1}Z_{46}Z_{47}$
第二轮	$Z_6Z_7Z_8Z_9Z_{10}Z_{11}$	$Z_{42}^{-1}-Z_{44}-Z_{43}Z_{45}^{-1}Z_{40}Z_{41}$
第三轮	$Z_{12}Z_{13}Z_{14}Z_{15}Z_{16}Z_{17}$	$Z_{36}^{-1}-Z_{38}-Z_{37}Z_{39}^{-1}Z_{34}Z_{35}$
第四轮	$Z_{28}Z_{19}Z_{20}Z_{21}Z_{22}Z_{23}$	$Z_{30}^{-1}-Z_{32}-Z_{31}Z_{33}^{-1}Z_{28}Z_{29}$
第五轮	$Z_{34}Z_{25}Z_{26}Z_{27}Z_{28}Z_{29}$	$Z_{24}^{-1}-Z_{26}-Z_{25}Z_{27}^{-1}Z_{22}Z_{23}$
第六轮	$Z_{30}Z_{31}Z_{32}Z_{33}Z_{34}Z_{35}$	$Z_{18}^{-1}Z_{20}-Z_{19}Z_{21}^{-1}Z_{18}Z_{17}$
第七轮	$Z_{46}Z_{37}Z_{38}Z_{39}Z_{40}Z_{41}$	$Z_{12}^{-1}Z_{14}-Z_{13}Z_{15}^{-1}Z_{10}Z_{11}$
第八轮	$Z_{42}Z_{43}Z_{44}Z_{45}Z_{46}Z_{47}$	$Z_6^{-1}-Z_8-Z_7Z_9^{-1}Z_4Z_5$
最后的置换	$Z_{48}Z_{49}Z_{50}Z_{51}$	$Z_0^{-1}-Z_1-Z_2Z_3^{-1}$

以上Z_j与Z_j^{-1}及$-Z_j$与Z_j的关系为：

- $Z_j \odot Z_j^{-1} = 1$
- $-Z_j \boxplus Z_j = 0$