5. International Data Encryption Algorithm (IDEA)

Shannon proposed composing different kinds of functions to create “mixing transformations”, which randomly distribute the meaningful messages uniformly over the set of all possible ciphertext messages. Mixing transformations could be created, for example, by applying a transformation followed by an alternating sequence of substitutions and simple linear operations.

IDEA belongs to the same class of conventional symmetric ciphers. The basic principles of IDEA have been published in 1990 by J.Massey, as an alternative to the Data encryption standard (DES).

As the DES algorithm IDEA is a block cipher with the same size of block equals to 64 bits. The length of key is 128 bits. To increase the quality of enciphering the following requirements have been satisfies within the proposed algorithm.

1. **The length of the data block is 64.** There are two basic requirements for the data block length. The first one is the complexity of the algorithm, which requires reduce the data block. The second is the statistical dependences between the data blocks, what can be reduced with increasing the length of data block. As have been proven the appropriate length of data block is 64.

2. **The length of the key.** The length of the key should be enough to eliminate so called direct attack by trying to apply all possible values of keys. The key with size 128 bits looks as a good solution for the recent and future applications.

3. **Confusion.** Dependence of the ciphertext from the plaintext and key should be complex and not obvious.

4. **Diffusion**. Each bit an open text, as well as each bit of the key should be taken into account to get each bit of the ciphertext.

5. International Data Encryption Algorithm (IDEA)

To achieve an appropriate level of the **confusion** the mixed application of the following operation on 16 bits data block have been used.

1. Bit wise XOR for two 16 bits operands, what have been denoted as $\oplus$.
2. Addition of the two integer 16 bits operands modulo 2^{16}, denoted as $\boxtimes$.
3. Multiplication of the two integer number by modulo $2^{16}+1$, where integer number should be without the signs. There is one exception for the all zero code, which have to be regarded as 2^{16}. This operation denoted as $\odot$.

For this operation next properties are true:

$$a\odot(b\boxtimes c)\neq(a\odot b)\boxtimes(a\odot c),$$

$$a\boxtimes(b\oplus c)\neq(a\boxtimes b)\oplus c.$$

All proposed operation can be easily implemented and have a low complexity.

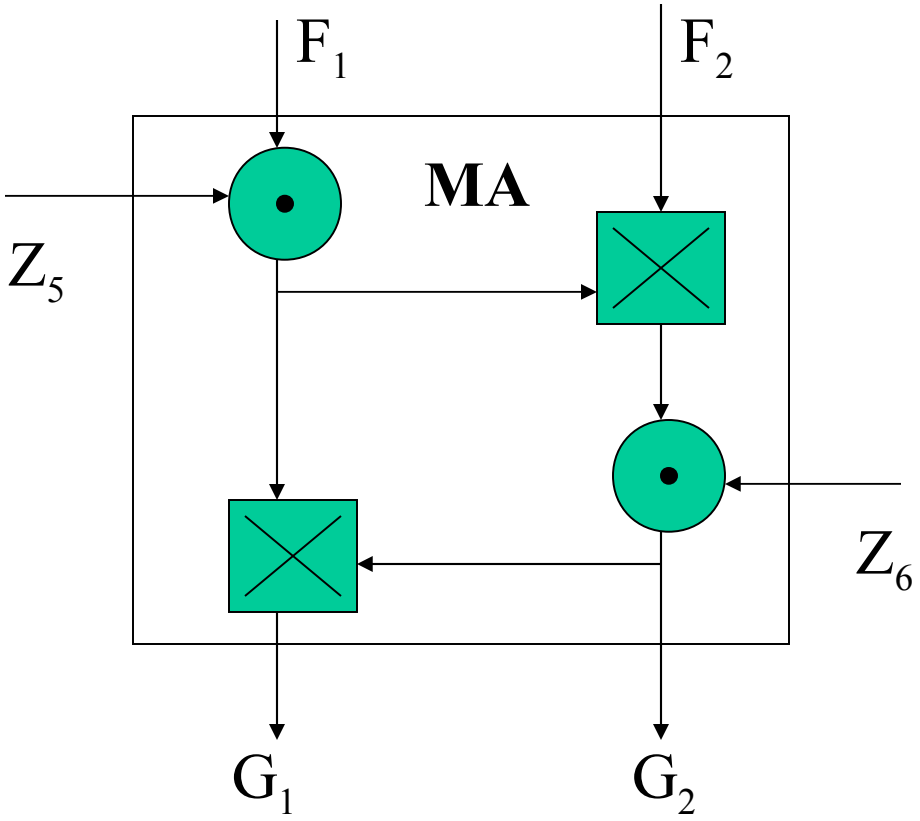
Proposed operation are shown in the following table for the case when the length of the operands equal to 2 bits.

5. International Data Encryption Algorithm (IDEA)

X	Y	X ⊠ Y	X ⊙ Y	X ⊕ Y
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

5. International Data Encryption Algorithm (IDEA)

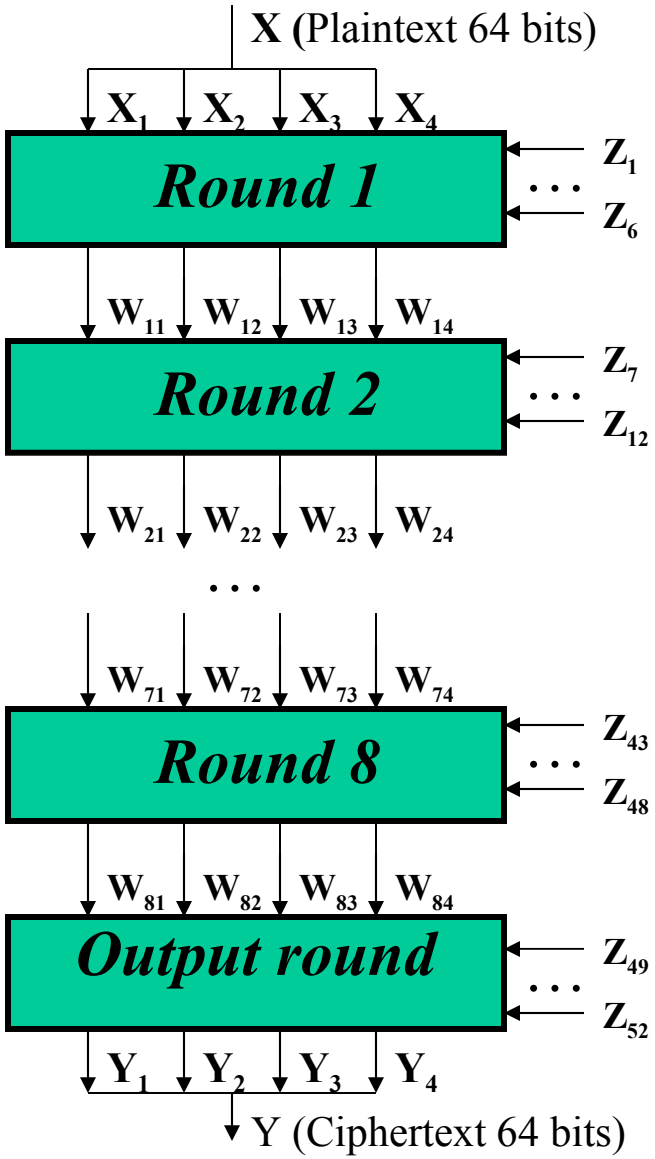
To achieve an appropriate level of the **diffusion** the main building block have been design as multiplicative-additive structure:

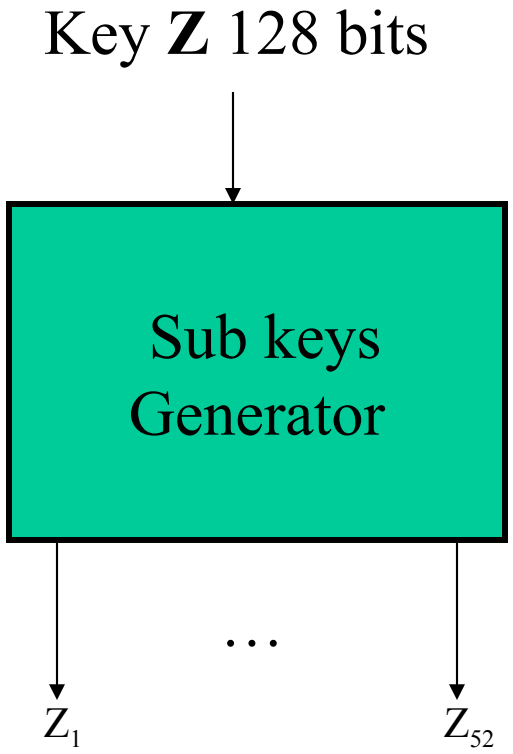


Here F_1 and F_2 are 16 bits values obtained from the plaintext; Z_5 and Z_6 are 16 bits sub keys.

5. International Data Encryption Algorithm (IDEA)

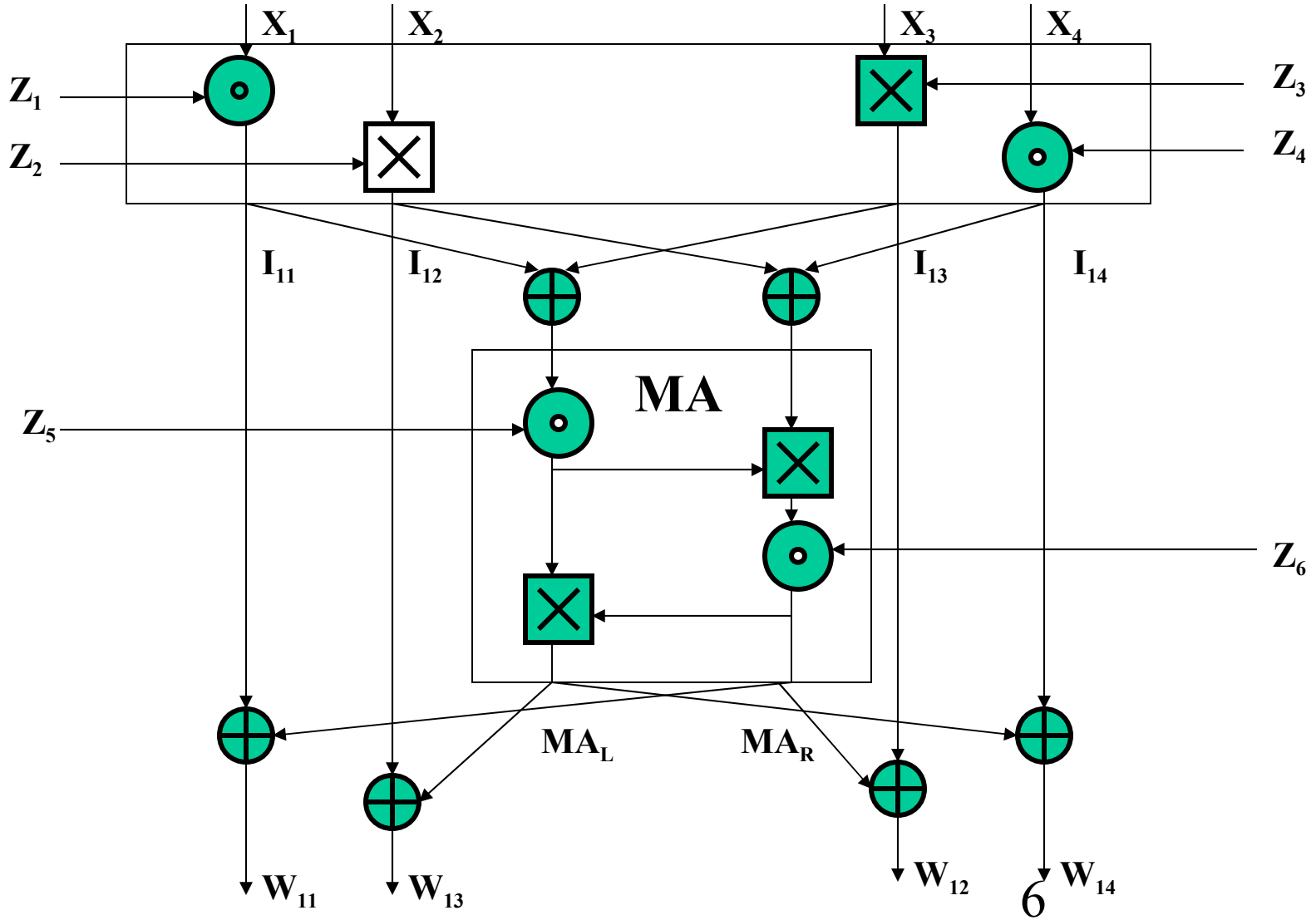
Enciphering





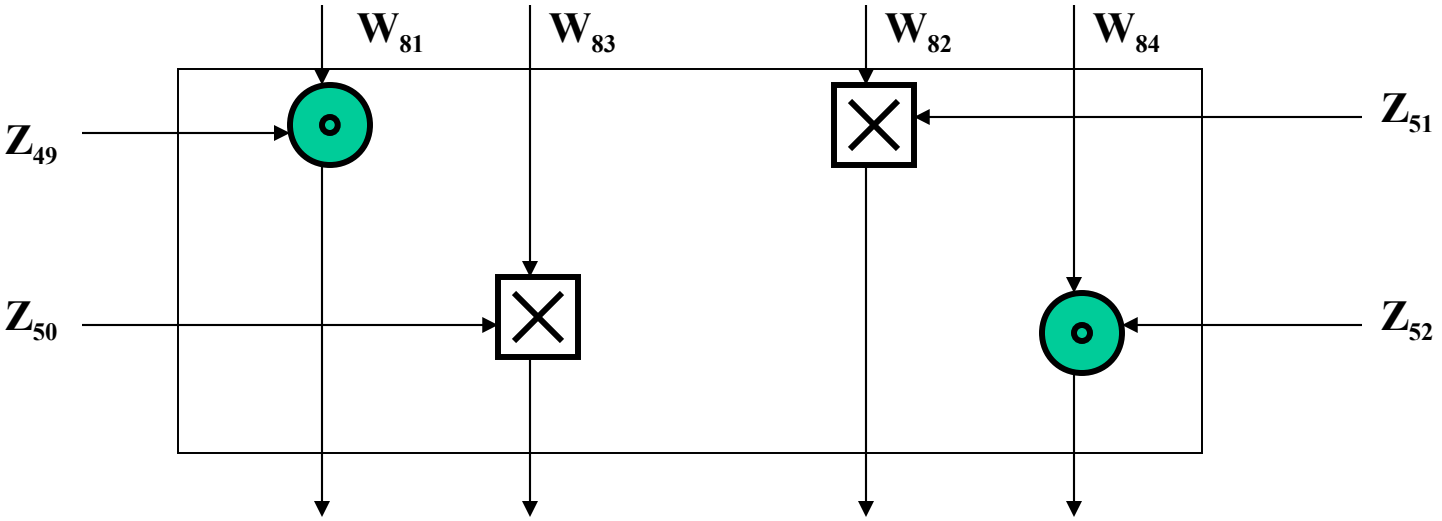
5. International Data Encryption Algorithm (IDEA)

One round for ciphering (first)



5. International Data Encryption Algorithm (IDEA)

Output round for ciphering



Sub keys calculations: The first eight sub keys $\mathbf{Z_1,Z_2,\ldots,Z_8}$ are the consecutive parts of the cryptographic key ***K***. Then ***K*** is cyclic shifted on 25 bits to the left and the next eight sub keys are generated as the copy of consecutive parts of resulted vector. This procedure have to be repeated until all 52 sub keys are generated.

If the ***K*** can be denoted as Z[1…128] then the first sub keys for all eight rounds are Z_1=Z[1…16], Z_7=Z[94…112], Z_{13}=Z[90…105], Z_{19}=Z[83…98], Z_{25}=Z[76…91], Z_{31}=Z[44…59], Z_{37}=Z[34…52], Z_{43}=Z[30…45].

5. International Data Encryption Algorithm (IDEA)

Sub keys for ciphering

Round	Notation	Equivalent
#1	$Z_1Z_2Z_3Z_4Z_5Z_6$	Z[1…96]
#2	$Z_7Z_8Z_9Z_{10}Z_{11}Z_{12}$	Z[97…128;26…89]
#3	$Z_{13}Z_{14}Z_{15}Z_{16}Z_{17}Z_{18}$	Z[90…128;1…25;51…82]
#4	$Z_{19}Z_{20}Z_{21}Z_{22}Z_{23}Z_{24}$	Z[83…128;1…50]
#5	$Z_{25}Z_{26}Z_{27}Z_{28}Z_{29}Z_{30}$	Z[76…128;1…43]
#6	$Z_{31}Z_{32}Z_{33}Z_{34}Z_{35}Z_{36}$	Z[44…75;101…128;1…36]
#7	$Z_{37}Z_{38}Z_{39}Z_{40}Z_{41}Z_{42}$	Z[37…100;126…128;1…29]
#8	$Z_{43}Z_{44}Z_{45}Z_{46}Z_{47}Z_{48}$	Z[30…125]
Output round	$Z_{49}Z_{50}Z_{51}Z_{52}$	Z[23…86]

5. International Data Encryption Algorithm (IDEA)

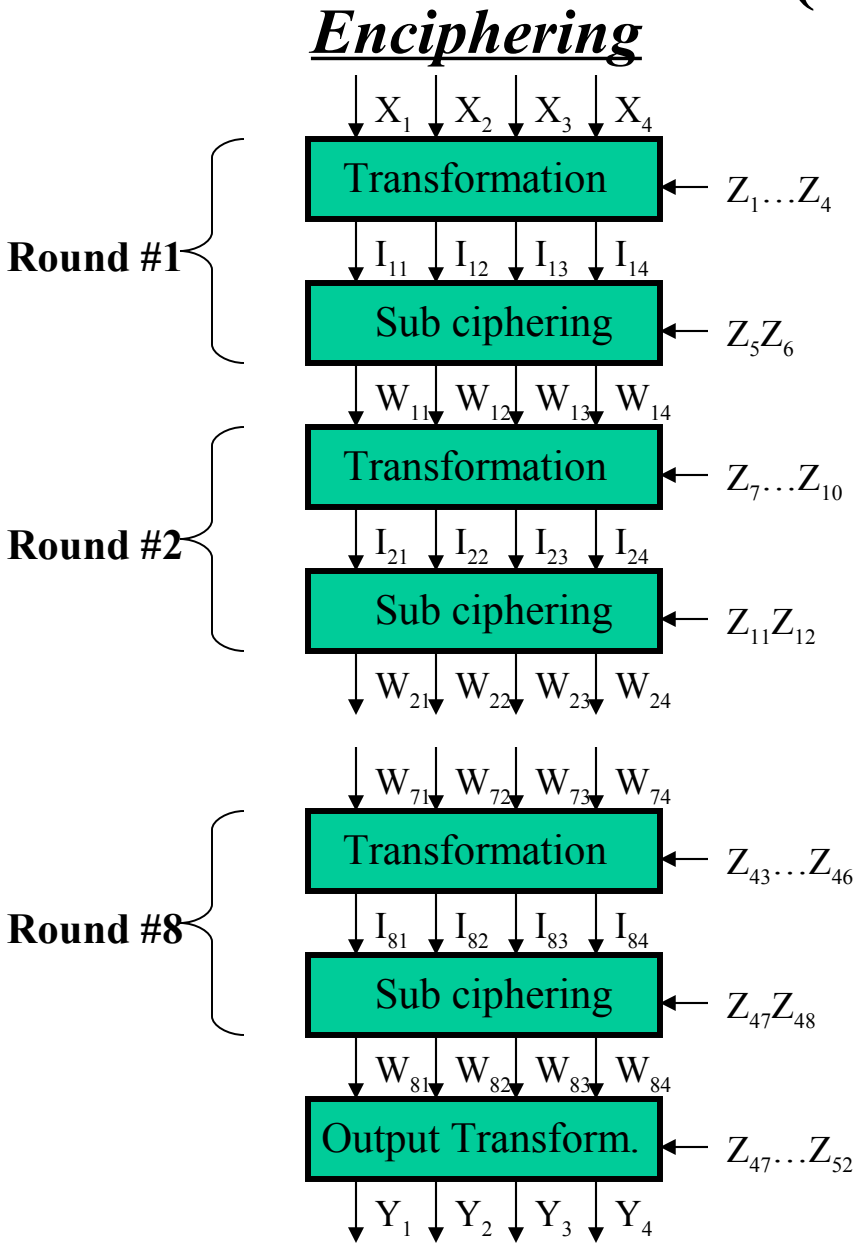
Sub keys for deciphering

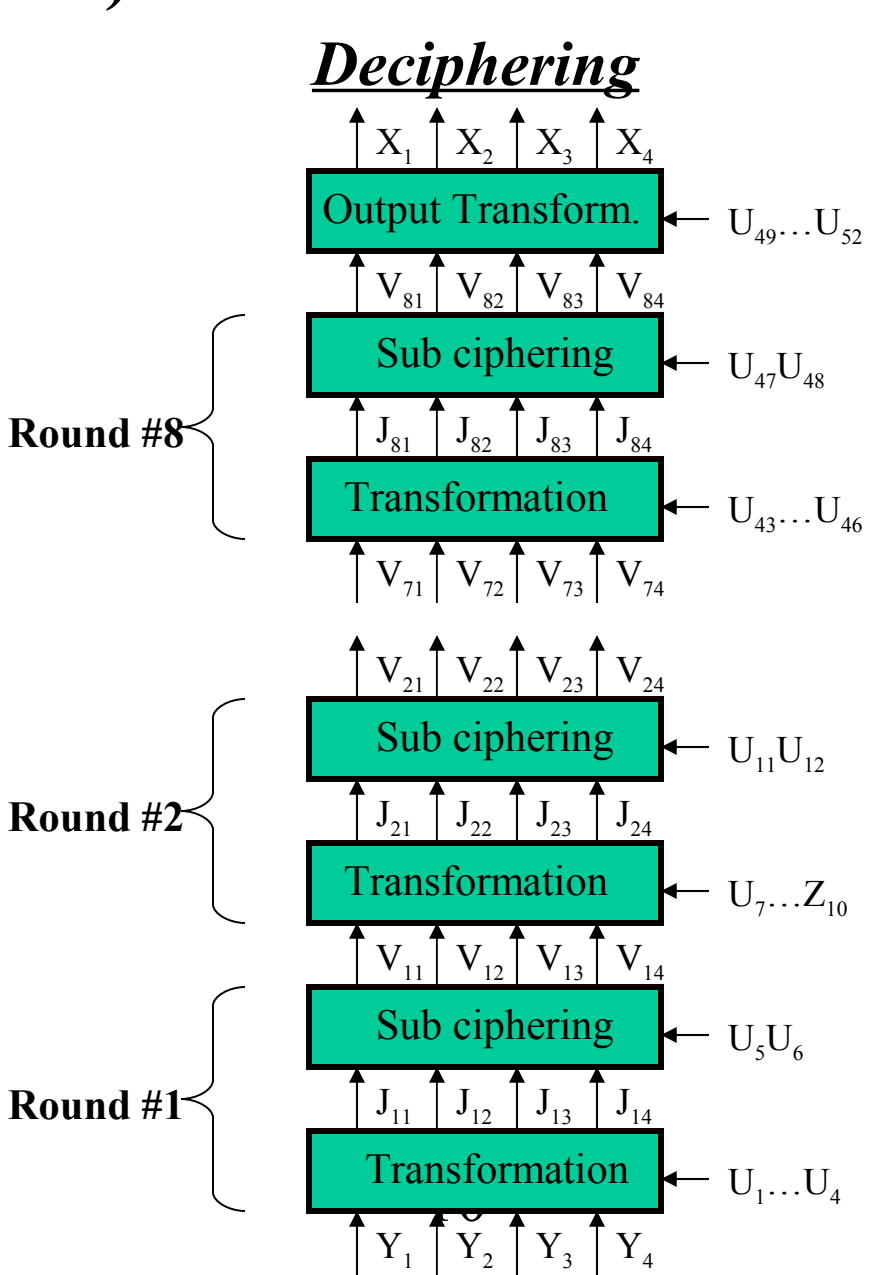
Round	Notation	Equivalent
#1	$U_1U_2U_3U_4U_5U_6$	$Z_{49}^{-1},-Z_{50},-Z_{51}, Z_{52}^{-1},Z_{47},Z_{48}$
#2	$U_7U_8U_9U_{10}U_{11}U_{12}$	$Z_{43}^{-1},-Z_{45},-Z_{44}, Z_{46}^{-1},Z_{41},Z_{42}$
#3	$U_{13}U_{14}U_{15}U_{16}U_{17}U_{18}$	$Z_{37}^{-1},-Z_{39},-Z_{38}, Z_{40}^{-1},Z_{35},Z_{36}$
#4	$U_{19}U_{20}U_{21}U_{22}U_{23}U_{24}$	$Z_{31}^{-1},-Z_{33},-Z_{32}, Z_{34}^{-1},Z_{29},Z_{30}$
#5	$U_{25}U_{26}U_{27}U_{28}U_{29}U_{30}$	$Z_{25}^{-1},-Z_{27},-Z_{26}, Z_{28}^{-1},Z_{23},Z_{24}$
#6	$U_{31}U_{32}U_{33}U_{34}U_{35}U_{36}$	$Z_{19}^{-1},-Z_{21},-Z_{20}, Z_{22}^{-1},Z_{17},Z_{18}$
#7	$U_{37}U_{38}U_{39}U_{40}U_{41}U_{42}$	$Z_{13}^{-1},-Z_{15},-Z_{14}, Z_{16}^{-1},Z_{11},Z_{12}$
#8	$U_{43}U_{44}U_{45}U_{46}U_{47}U_{48}$	$Z_7^{-1},-Z_9,-Z_8, Z_{10}^{-1},Z_5,Z_6$
Output round	$U_{49}U_{50}U_{51}U_{52}$	$Z_1^{-1},-Z_2,-Z_3, Z_4^{-1}$

$$Z_j^{-1} \odot Z_j = 1 \ \textbf{mod}\ (2^{16}+1);$$

$$-Z_j \boxtimes Z_j = 0 \ \textbf{mod}\ 2^{16}.$$

5. International Data Encryption Algorithm (IDEA)





5. International Data Encryption Algorithm (IDEA)

Let us consider the last boxes on the Enciphering and Deciphering procedures:

For Enciphering $Y_1=W_{81}\odot Z_{49}$, $Y_2=W_{83}\boxtimes Z_{50}$, $Y_3=W_{82}\boxtimes Z_{51}$, $Y_4=W_{84}\odot Z_{52}$,

For Deciphering $J_{11}=Y_1\odot U_1$, $J_{12}=Y_2\boxtimes U_2$, $J_{13}=Y_2\boxtimes U_3$, $J_{14}=Y_4\odot U_4$, after substitution of the real value of the sub keys we'll get

$$J_{11}=Y_1\odot Z_{49}^{-1}=W_{81}\odot Z_{49}\odot Z_{49}^{-1}=W_{81}$$

$$J_{12}=Y_2\boxtimes {}^{-}Z_{50}=W_{83}\boxtimes Z_{50}\boxtimes {}^{-}Z_{50}=W_{83}$$

$$J_{13}=Y_3\boxtimes {}^{-}Z_{51}=W_{82}\boxtimes Z_{51}\boxtimes {}^{-}Z_{51}=W_{82}$$

$$J_{14}=Y_4\odot Z_{52}^{-1}=W_{84}\odot Z_{52}\odot Z_{52}^{-1}=W_{84}$$

So, the result of the first stage of deciphering is the same as the values before the last stage of enciphering. Now let's consider the next boxes according to the last slide.

$$W_{81}=I_{81}\oplus MA_R(I_{81}\oplus I_{83}, I_{82}\oplus I_{84}),$$

$$W_{82}=I_{81}\oplus MA_R(I_{81}\oplus I_{83}, I_{82}\oplus I_{84}),$$

$$W_{83}=I_{81}\oplus MA_L(I_{81}\oplus I_{83}, I_{82}\oplus I_{84}),$$

$$W_{84}=I_{81}\oplus MA_L(I_{81}\oplus I_{83}, I_{82}\oplus I_{84}),$$

Here $MA_R(A,B)$ means the right output value for MA, as well as $MA_L(A,B)$ – left value.

5. International Data Encryption Algorithm (IDEA)

The next box according to deciphering procedure allow to calculate the value of $V_{11}, V_{12}, V_{13}, V_{14}$, Then

$$V_{11} = J_{11} \oplus MA_R(J_{11} \oplus J_{13}, J_{12} \oplus J_{14}) =$$

$$= W_{81} \oplus MA_R(W_{81} \oplus W_{83}, W_{82} \oplus W_{84}) =$$

$$= I_{81} \oplus MA_R(I_{81} \oplus I_{83}, I_{82} \oplus I_{84}) \oplus MA_R[(I_{81} \oplus MA_R(I_{81} \oplus I_{83}, I_{82} \oplus I_{84}) \oplus I_{83} \oplus MA_R(I_{81} \oplus I_{83}, I_{82} \oplus I_{84}),\ I_{82} \oplus MA_L(I_{81} \oplus I_{83}, I_{82} \oplus I_{84}) \oplus I_{84} \oplus MA_L(I_{81} \oplus I_{83}, I_{82} \oplus I_{84})] =$$

$$= I_{81} \oplus MA_R(I_{81} \oplus I_{83}, I_{82} \oplus I_{84}) \oplus MA_R(I_{81} \oplus I_{83}, I_{82} \oplus I_{84}) =$$

$$= I_{81}$$

The same way it is easy to show that $V_{12} = I_{12}$, $V_{13} = I_{13}$ and $V_{14} = I_{14}$