ISO9979/0020

ALGORITHM REGISTER ENTRY

a) ISO Entry Name — {iso standard 9979 m8 (20)}

b) Name of Algorithm — M8

c) Intended Range of Application

1. Confidentiality
2. Hash Function - as detailed in ISO 10118-2
3. Authentication - as detailed in ISO 9798
4. Data Integrity - as detailed in ISO 9797

d) Cryptographic Interface Parameters

1. Input size	64 bits
2. Output size	64 bits
3. Round number	positive integer N
4. Key length :	
Data key	64 bits
Key expansion key	256 bits
Algorithm decision key	24 * N bits
Algorithm expansion key	96 * N bits

e) Test Data

Round number	126	
Key expansion key	all 0's for 256 bits of key expansion key	
Data key	(0123 4567 89AB CDEF) hex	
Algorithm decision key	1st Round	(848B6D) hex
	2nd Round	(8489BB) hex
	3rd Round	(84B762) hex
	4th Round	(84EDA2) hex
	Iterate above numbers on and after Round	
Algorithm expansion key	(0000 0001 0000 0000 0000 0000) hex * 126	
Input data	(0000 0000 0000 0001) hex	

Intermediary (7th Round)	(C5D6 FBAD 76AB A53B) hex
Intermediary (14th Round)	(6380 4805 68DB 1895) hex
Intermediary (21st Round)	(2BFB 806E 1292 5B18) hex
Intermediary (28th Round)	(F610 6A41 88C5 8747) hex
Intermediary (56th Round)	(D3E1 66E9 C50A 10A2) hex
Output data (126th Round)	(FE4B 1622 E446 36C0) hex

f) Sponsoring Authority

Information-Technology Promotion Agency, Japan (IPA)
Bunkyo Green Court Center Office, 16F,
2-28-8 Honkomagome, Bunkyo-ku/Tokyo 113-6591, JAPAN
Tel:
+81-3-5978-7500
Fax:
+81-3-5978-7510

Registration Requested by

Hitachi, Ltd.
Omika Works

Contact for Information

Hideyuki Hara
Senior Engineer
Hitachi, Ltd.
Omika Works

ISO9979/0020

Information Systems Development Department
2-1 Omika-cho 5-chome, Hitachi-shi Ibaraki-ken,
319-1293, Japan
Tel:
+81-294-52-7333
Fax:
+81-294-53-2557

g) Date of Submission 29 January 1999
Date of Registration 19 March 1999

h) Whether the Subject of a National Standard No.

i) Patent - License Restriction

Six patents registered:
1. Japan, No. 2760799
2. Japan, No. 2798086
3. Japan, No. 2798087
4. United States Patent, No. 4,982,429
5. United States Patent, No. 5,103,479
6. United States Patent, No. 5,222,139

Eight patents applied for:

7. Japan, No. 2-295351
8. Japan, No. 9-329841
9. Japan, No. 9-329843
10. Japan, No. 9-329845
11. Japan, No. 9-329846
12. Japan, No. 10-148712
13. Japan, No. 10-221319
14. Japan, No. 10-221320

For commercial use of M8, license and fee are required.

j) References See ISO 8372 or ISO/IEC 10116 for its information on modes of operation.

k) Description of Algorithm

M8 is a symmetric block cipher algorithm based on the permutation - substitution calculation like DES. M8 is a modification of M6 (key length: 40 to 64 bits) published in 1997, so that the key length is 64 bits or more. M8 is designed to realize a high performance on a small hardware or 32-bit computers. For example, M8 with the round number N=10 exhibits the encryption speed of 32Mbps by using a dedicated hardware of 6K gates and 25MHz clock, or 208Mbps by using a C language software on PentiumII* at 266MHz.

The structural characteristic of M8 is that each round function consists of three kinds of calculation: 32 bits circular rotation, addition in modulus 2^{32} and 32 bits exclusive OR, and the actual function of each round may be different. Key information is used as a value information that is an object of calculation and that determines the actual function of each round. As the full specification of M8 is open, it can be used for security mechanisms in open/multivendor environment.

See Appendix for detail.

*PentiumII is registered trademark of Intel Corp.

ISO 9979/0020

l) Modes of Operation

Modes of operation as defined in ISO 8372 or ISO/IEC 10116 are applicable:

1. Electronic Codebook (ECB) Mode
2. Cipher Block Chaining (CBC) Mode
3. Cipher Feedback (CFB) Mode
4. Output Feedback (OFB) Mode

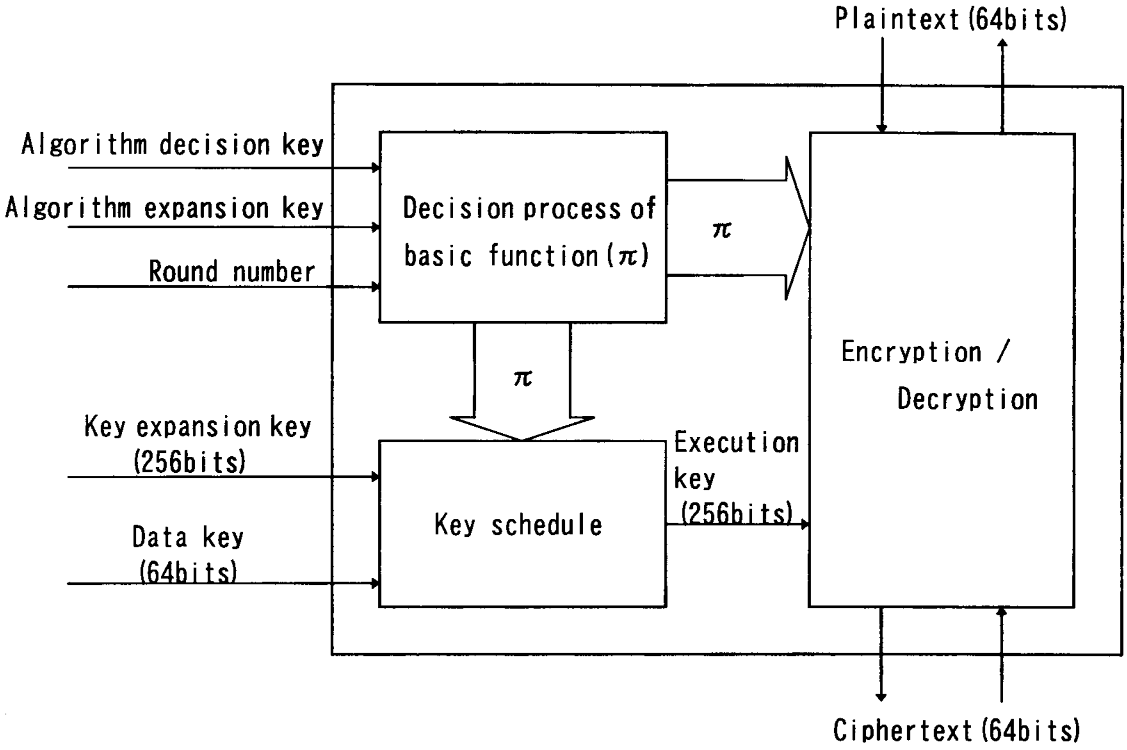
m) Other Information

In general, it is not possible to prove that an encryption algorithm and its environment are perfectly safe. However, a comparison of cryptographic strength between two encryption algorithms may help to obtain a safety measure. In M8, key information changes both numerical parameters which are calculation objects and round functions. In case that the structure of every round function is known to hostile person, it is possible to evaluate M8 by conventional cryptanalysis methods. If the structure of every round function is known, in our estimation, there is a possibility that M8 with the round number less than ten may be broken easier than DES. Therefore it is recommended that M8 be used with the round number ten or more as possible. The cryptographic strength of M8 algorithm becomes higher as the round number increases. On the other hand, the speed of M8 encryption is almost inversely proportional to the round number.

In case that the structure of the round function is unknown to the hostile persons, it must be first decided by them. However, no method has been reported to find the structure of the round function more efficiently than exhaustive search. Since there are a large number of variations of round function, we think that it is difficult to find it by exhaustive search.

In some cases, it is recommended that a trade-off between the speed and the safety margin be examined to determine the round number of M8.

APPENDIX: OUTLINE OF M8



M8 is an algorithm changeable cryptograph and both algorithm decision and expansion keys determine basic function. This basic function is used in key schedule and encryption / decryption.

Symbols

$\oplus$: bit-wise exclusive OR, +:addition in modulus 2^{32}, − : subtraction in modulus 2^{32}, rot_s: s bits left circular rotation, $\|$: concatenation of data elements,

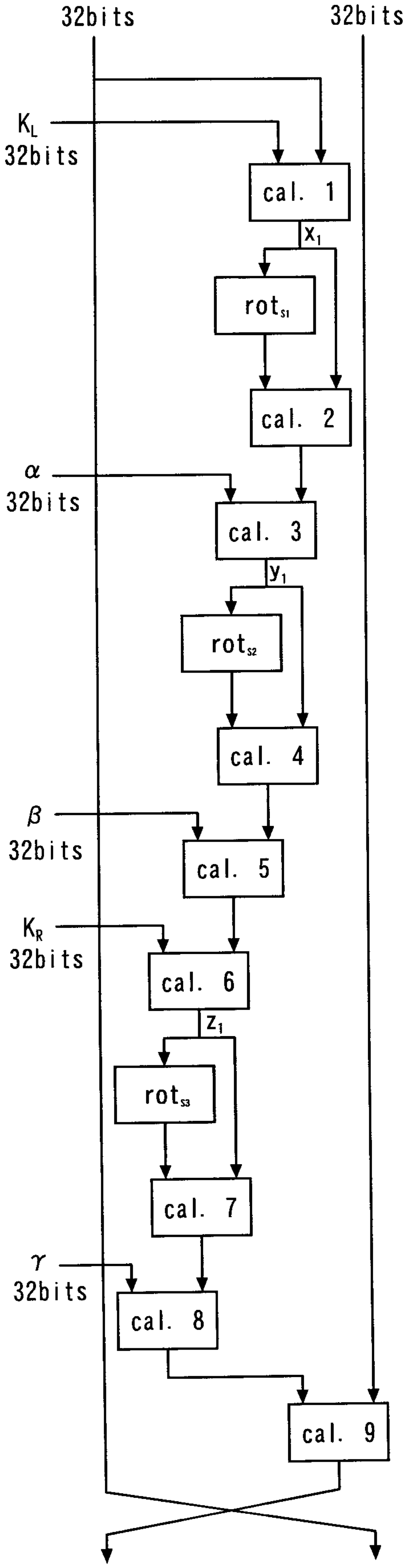
$T_{[left]}$: the string composed of the 32 leftmost bits of the block T,

$T_{[right]}$: the string composed of the 32 rightmost bits of the block T,

α, β, γ: algorithm expansion key,

K_L, K_R: Execution key

STRUCTURE OF ENCRYPTION BASIC FUNCTION(e π)



A basic function consists of three kinds of left circular rotations and nine kinds of calculations (cal. 1 to 9).
An algorithm decision key determines rotation value and kinds of calculations.

Algorithm decision key

		Calculation							Left circular rotation		
1	2	3	4	5	6	7	8	9	S1	S2	S3
9bits									5bits	5bits	5bits

Meaning of a bit of calculation 1 to 9

0: + (addition in modulus 2^{32})

1: ⊕ (bit-wise exclusive OR)

An algorithm expansion key determines α, β and γ.

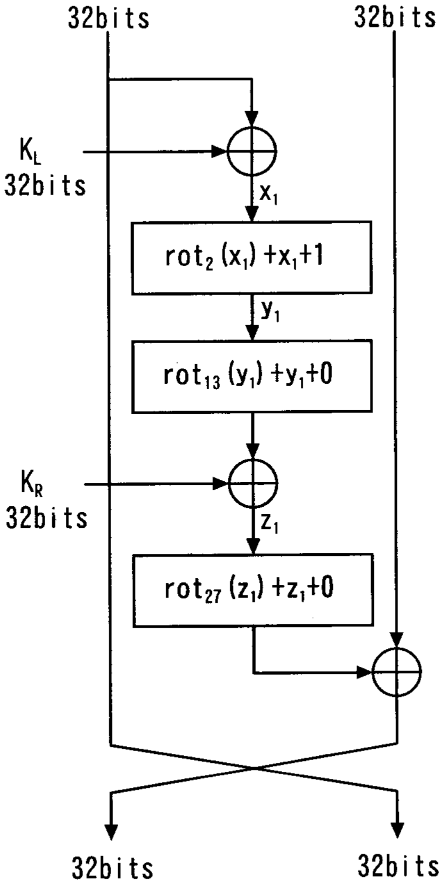
Algorithm expansion key

α	β	γ
32bits	32bits	32bits

ISO 9979 /0020

AN EXAMPLE OF ENCRYPTION BASIC FUNCTION (e π)

Basic function (e π)
(Feistel network)



Algorithm decision key

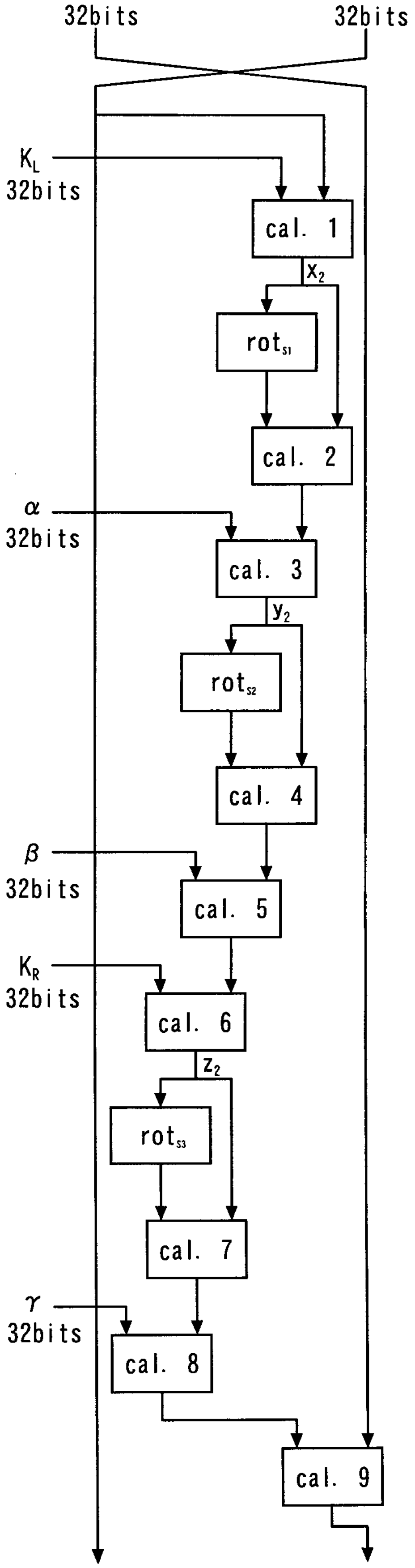
(100001001 00010 01101 11011) bin

Algorithm expansion key

(0000 0001 0000 0000 0000 0000) hex

ISO 9979 /0020

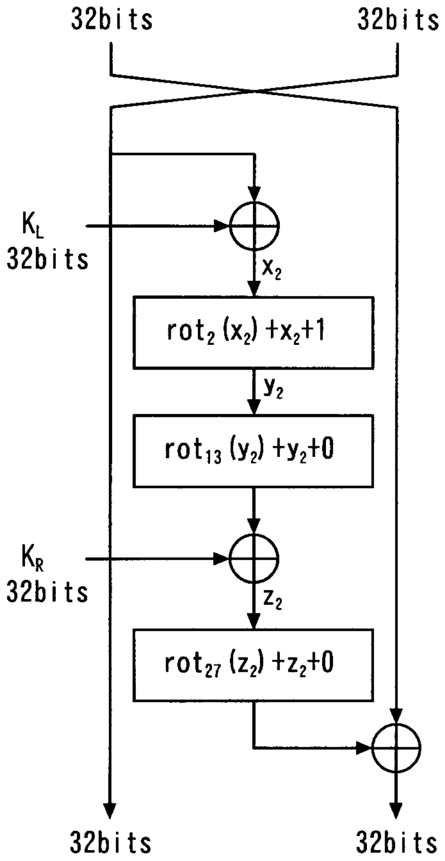
STRUCTURE OF DECRYPTION BASIC FUNCTION (d π)



Calculations 1 to 9 of decryption are identical with those of encryption.
However, only when calculation 9 of encryption is +, calculation 9 of decryption should be − (subtraction in modulus 2^{32}).

AN EXAMPLE OF DECRYPTION BASIC FUNCTION (d π)

Basic function (d π)
(Feistel network)



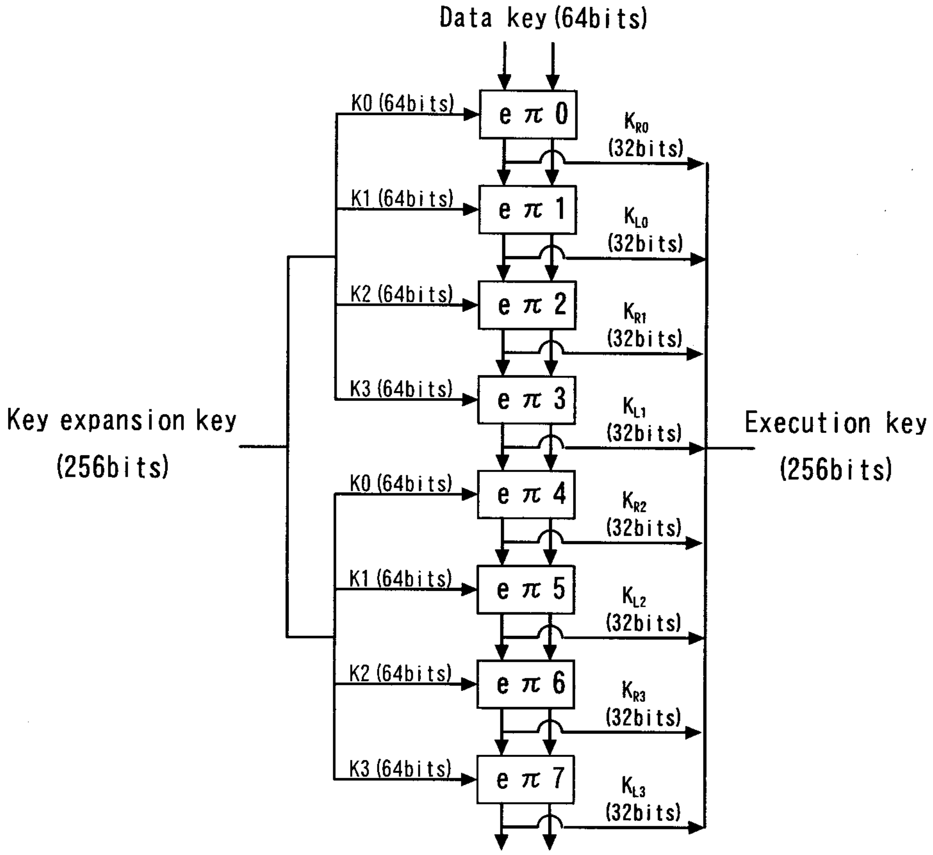
Algorithm decision key

(100001001 00010 01101 11011) bin

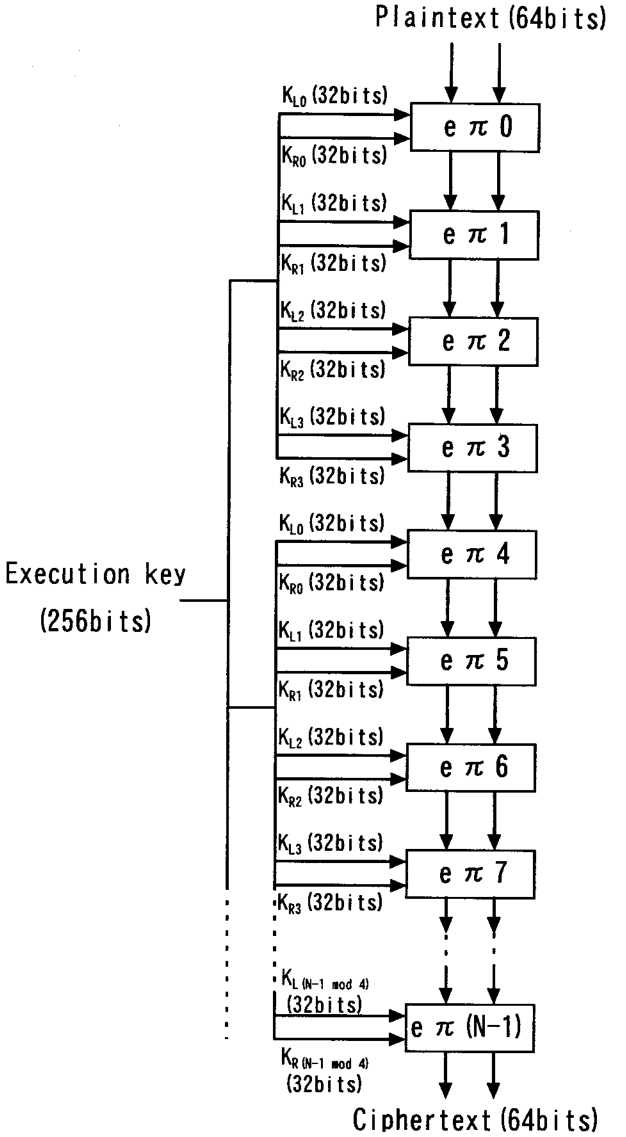
Algorithm expansion key

(0000 0001 0000 0000 0000 0000) hex

KEY SCHEDULE



ENCRYPTION



e π 0～(N-1) :each round function

of Basic Function (e π d π) $a_6 = $ e π 6 $S_2(a_5)$

ISO 9979/0020.

Decision Process of Basic Function(e π, d π)

Let A_K be the algorithm decision key.

$A_K=A_{K3} \| A_{K2} \| A_{K1} \| A_{K0}$

Let X_K be the algorithm expansion key.

$X_K=\alpha \| \beta \| \gamma$

Where α, β, γ are 32-bit data blocks.

In this section, we define two basic functions (e π, d π) in case of as follows:

A_{K3}= (100001001) bin,

A_{K2}=S1, A_{K1}=S2, A_{K0}=S3

1. e π

Let T be the input to e π.

Let K_L, K_R be the execution key.

Then, the intermediates x_1, y_1 and z_1 are calculated as:

$x_1 = T_{[left]} \oplus K_L$

$y_1 = rot_{S1}(x_1)+x_1+\alpha$

$z_1 = (rot_{S2}(y_1)+y_1+\beta) \oplus K_R$

The output of e π is obtained:

e π $K_L K_R(T) = (T_{[right]} \oplus (rot_{S3}(z_1)+z_1+\gamma)) \| T_{[left]}$

2. d π

Let T be the input to d π.

Let K_L, K_R be the execution key.

Then, the intermediates x_2, y_2 and z_2 are calculated as:

$x_2 = T_{[right]} \oplus K_L$

$y_2 = rot_{S1}(x_2)+x_2+\alpha$

$z_2 = (rot_{S2}(y_2)+y_2+\beta) \oplus K_R$

The output of d π is obtained:

d π $K_L K_R(T) = T_{[right]} \| (T_{[left]} \oplus (rot_{S3}(z_2)+z_2+\gamma))$

Key Schedule

Let D_k be the data key.

Let S_k be the key expansion key.

$S_k = S_3 \| S_2 \| S_1 \| S_0$

Where S_0, S_1, S_2, S_3 are 64-bit data blocks.

The execution key E_k is obtained:

a_0 = e π 0 $S_0(D_k)$

$E_{R0} = a_{0[left]}$

a_1 = e π 1 $S_1(a_0)$

$E_{L0} = a_{1[left]}$

a_2 = e π 2 $S_2(a_1)$

$E_{R1} = a_{2[left]}$

a_3 = e π 3 $S_3(a_2)$

$E_{L1} = a_{3[left]}$

a_4 = e π 4 $S_0(a_3)$

$E_{R2} = a_{4[left]}$

a_5 = e π 5 $S_1(a_4)$

$E_{L2} = a_{5[left]}$

a_6 = e π 6 $S_2(a_5)$

$E_{R3} = a_{6[left]}$

a_7 = e π 7 $S_3(a_6)$

$E_{L3} = a_{7[left]}$

$E_k = E_{L3} \| E_{R3} \| E_{L2} \| E_{R2} \| \cdots \| E_{R0}$

Encryption

Let round number be positive integer N.

Let E_k be the execution key.

$E_k = E_{L3} \| E_{R3} \| E_{L2} \| E_{R2} \| \cdots \| E_{R0}$

Let P be the plaintext.

Then, the ciphertext C is obtained as follows:

$$
\begin{aligned}
C = {} & e\pi\,(N-1)\,E_{L(N-1 \bmod 4)}, E_{R(N-1 \bmod 4)} \cdot \\
& e\pi\,(N-2)\,E_{L(N-2 \bmod 4)}, E_{R(N-2 \bmod 4)} \cdot \\
& \cdots \cdot \\
& e\pi\,4E_{L0}, E_{R0} \cdot \\
& e\pi\,3E_{L3}, E_{R3} \cdot \\
& e\pi\,2E_{L2}, E_{R2} \cdot \\
& e\pi\,1E_{L1}, E_{R1} \cdot \\
& e\pi\,0E_{L0}, E_{R0}\,(P)
\end{aligned}
$$

Decryption

Let C be the ciphertext.

Then, the plaintext P is obtained as follows:

$$
\begin{aligned}
P = {} & d\pi\,0E_{L0}, E_{R0} \cdot \\
& d\pi\,1E_{L1}, E_{R1} \cdot \\
& d\pi\,2E_{L2}, E_{R2} \cdot \\
& d\pi\,3E_{L3}, E_{R3} \cdot \\
& d\pi\,4E_{L0}, E_{R0} \cdot \\
& \cdots \cdot \\
& d\pi\,(N-2)\,E_{L(N-2 \bmod 4)}, E_{R(N-2 \bmod 4)} \cdot \\
& d\pi\,(N-1)\,E_{L(N-1 \bmod 4)}, E_{R(N-1 \bmod 4)}\,(C)
\end{aligned}
$$