5번 문제 답안

정답)

30라운드

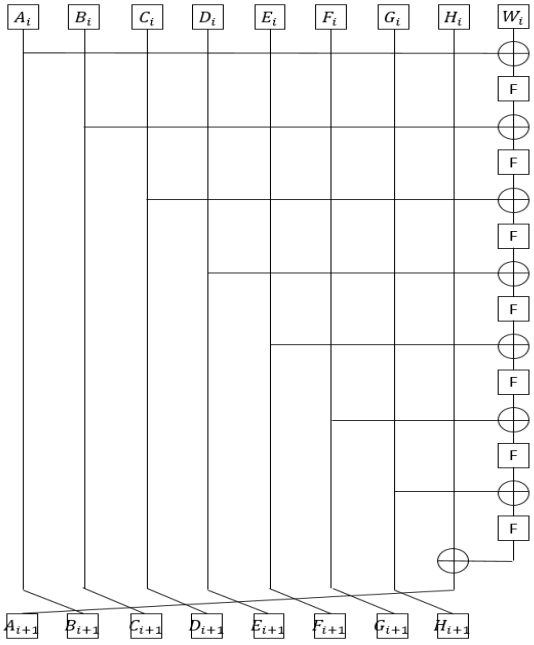
풀이)

1. 주어진 문제 파악

문제에 주어진 해시함수를 보고 임의의 256 비트값 Y에 대해, 2^{253}번의 CF 함수 연산보다 작은 계산량으로, Y를 출력값으로 갖는 CF의 어떤 768 비트 입력값 X를 찾을 수 있는 최대의 라운드 수(=L)를 구하고, Y로부터 X를 찾는 알고리즘을 기술해야 한다.

1.1 함수의 구조

입력값 : $X = (A_0, B_0, C_0, D_0, E_0, F_0, G_0, H_0, W_0, W_1, ..., W_{15})$, where $A_0, B_0, C_0, D_0, E_0, F_0, G_0, H_0, W_0, W_1, ..., W_{15}$ are 32-bits.
중간변수 : $A_i, B_i, C_i, D_i, E_i, F_i, G_i, H_i$, which are 32-bits.
라운드 수 : L
출력값 : $Y = (A_0 \oplus A_L, B_0 \oplus B_L, C_0 \oplus C_L, D_0 \oplus D_L, E_0 \oplus E_L, F_0 \oplus F_L, G_0 \oplus G_L, H_0 \oplus H_L)$



< 그림 1. i 라운드의 구조 >

$$W_i = (W_{i-3} \lll 1) \oplus (W_{i-8} \lll 1) \oplus (W_{i-14} \lll 1) \oplus W_{i-16}$$
$$\text{for } 16 \le i \le L-1$$

여기서 F 함수는 블록암호 AES의 S-box와 MDS 행렬곱이다.

5번 문제 답안

2.2 함수의 성질

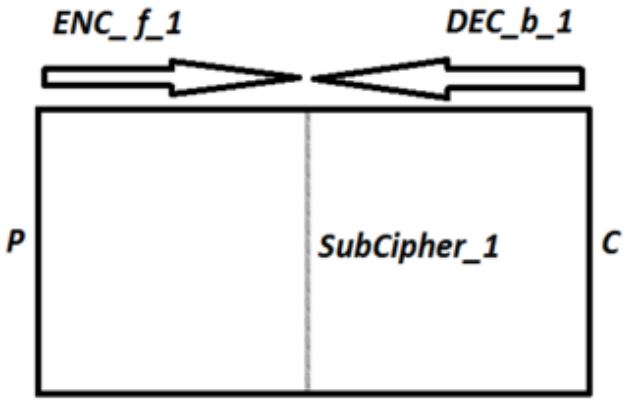
성질 1 : 이 함수는 특정한 입력이 들어오면 언제나 똑같은 과정을 거쳐서 언제나 똑같은 결과를 내놓으므로 결정론적 함수이다. 따라서 X(768-bits)에서 512-bits를 상수로 고정시키고 256-bits에 대해서 전수조사 하여도 가능한 모든 해시값을 얻을 수 있다.

성질 2 : 그림 1의 마지막 부분에서 swap이 발생한다.
따라서 $A_i, B_i, C_i, D_i, E_i, F_i, G_i = B_{i+1}, C_{i+1}, D_{i+1}, E_{i+1}, F_{i+1}, G_{i+1}, H_{i+1}$이다.

성질 3 : Round 함수에서 A_{i+1}를 계산하는 함수를 R이라 하자. $A_{i+1} = R(A_i, B_i, C_i, D_i, E_i, F_i, G_i, H_i, W_i)$이므로 $A_i, B_i, C_i, D_i, E_i, F_i, G_i, H_i, W_i, A_{i+1}$ 중 9개를 안다면 나머지 하나도 알 수 있다.

2.3 MITM(Meet In The Middle)

MITM 공격은 연산량을 개선하기 위해 중간값을 저장하여 비교하는 공격방법이다.



< 그림 2. MITM 공격의 형태 >

5번 문제 답안

3. 라운드 별 공격 방법

3.1 23라운드

2.2의 성질을 이용하여 공격이 가능하다.

Given : Y

Settings : $A_0, B_0, C_0, D_0, E_0, F_0, G_0, H_0$ fixed (IV), $W_0, W_1, W_2, W_3, W_4, W_5, W_6, W_7$ fixed

⇒ Y를 알기 때문에 $A_{23}, B_{23}, C_{23}, D_{23}, E_{23}, F_{23}, G_{23}, H_{23}$를 알 수 있다.

⇒ 2.2를 통해 다음을 알 수 있다.

: known, : brute force table, : check

A_0	B_0	C_0	D_0	E_0	F_0	G_0	H_0	W_0
A_1	B_1	C_1	D_1	E_1	F_1	G_1	H_1	W_1
A_2	B_2	C_2	D_2	E_2	F_2	G_2	H_2	W_2
A_3	B_3	C_3	D_3	E_3	F_3	G_3	H_3	W_3
A_4	B_4	C_4	D_4	E_4	F_4	G_4	H_4	W_4
A_5	B_5	C_5	D_5	E_5	F_5	G_5	H_5	W_5
A_6	B_6	C_6	D_6	E_6	F_6	G_6	H_6	W_6
A_7	B_7	C_7	D_7	E_7	F_7	G_7	H_7	W_7
A_8	B_8	C_8	D_8	E_8	F_8	G_8	H_8	W_8
A_9	B_9	C_9	D_9	E_9	F_9	G_9	H_9	W_9
A_{10}	B_{10}	C_{10}	D_{10}	E_{10}	F_{10}	G_{10}	H_{10}	W_{10}
A_{11}	B_{11}	C_{11}	D_{11}	E_{11}	F_{11}	G_{11}	H_{11}	W_{11}
A_{12}	B_{12}	C_{12}	D_{12}	E_{12}	F_{12}	G_{12}	H_{12}	W_{12}
A_{13}	B_{13}	C_{13}	D_{13}	E_{13}	F_{13}	G_{13}	H_{13}	W_{13}
A_{14}	B_{14}	C_{14}	D_{14}	E_{14}	F_{14}	G_{14}	H_{14}	W_{14}
A_{15}	B_{15}	C_{15}	D_{15}	E_{15}	F_{15}	G_{15}	H_{15}	W_{15}
A_{16}	B_{16}	C_{16}	D_{16}	E_{16}	F_{16}	G_{16}	H_{16}	W_{16}
A_{17}	B_{17}	C_{17}	D_{17}	E_{17}	F_{17}	G_{17}	H_{17}	W_{17}
A_{18}	B_{18}	C_{18}	D_{18}	E_{18}	F_{18}	G_{18}	H_{18}	W_{18}
A_{19}	B_{19}	C_{19}	D_{19}	E_{19}	F_{19}	G_{19}	H_{19}	W_{19}
A_{20}	B_{20}	C_{20}	D_{20}	E_{20}	F_{20}	G_{20}	H_{20}	W_{20}
A_{21}	B_{21}	C_{21}	D_{21}	E_{21}	F_{21}	G_{21}	H_{21}	W_{21}
A_{22}	B_{22}	C_{22}	D_{22}	E_{22}	F_{22}	G_{22}	H_{22}	W_{22}
A_{23}	B_{23}	C_{23}	D_{23}	E_{23}	F_{23}	G_{23}	H_{23}	

< 표 1. 23라운드 Settings >

5번 문제 답안

① $W_8, W_9, W_{10}, W_{11}, W_{12}, W_{13}, W_{14}$ brute force $\Rightarrow$ A_{15} table를 생성하고,

$$
\begin{aligned}
W_{16} &= (W_{13} \lll 1) \oplus (W_8 \lll 6) \oplus (W_2 \lll 11) \oplus W_0, \\
W_{17} &= (W_{14} \lll 1) \oplus (W_9 \lll 6) \oplus (W_3 \lll 11) \oplus W_1, \\
W_{18} &= (W_{15} \lll 1) \oplus (W_{10} \lll 6) \oplus (W_4 \lll 11) \oplus W_2, \\
W_{19} &= (W_{16} \lll 1) \oplus (W_{11} \lll 6) \oplus (W_5 \lll 11) \oplus W_3, \\
W_{20} &= (W_{17} \lll 1) \oplus (W_{12} \lll 6) \oplus (W_6 \lll 11) \oplus W_4, \\
W_{21} &= (W_{18} \lll 1) \oplus (W_{13} \lll 6) \oplus (W_7 \lll 11) \oplus W_5, \\
W_{22} &= (W_{19} \lll 1) \oplus (W_{14} \lll 6) \oplus (W_8 \lll 11) \oplus W_6
\end{aligned}
$$

에서 $W_{16}, W_{17}, W_{19}, W_{20}, W_{22}$ 또한 각 table에서 자동 생성된다.

A_0	B_0	C_0	D_0	E_0	F_0	G_0	H_0	W_0
A_1	B_1	C_1	D_1	E_1	F_1	G_1	H_1	W_1
A_2	B_2	C_2	D_2	E_2	F_2	G_2	H_2	W_2
A_3	B_3	C_3	D_3	E_3	F_3	G_3	H_3	W_3
A_4	B_4	C_4	D_4	E_4	F_4	G_4	H_4	W_4
A_5	B_5	C_5	D_5	E_5	F_5	G_5	H_5	W_5
A_6	B_6	C_6	D_6	E_6	F_6	G_6	H_6	W_6
A_7	B_7	C_7	D_7	E_7	F_7	G_7	H_7	W_7
A_8	B_8	C_8	D_8	E_8	F_8	G_8	H_8	W_8
A_9	B_9	C_9	D_9	E_9	F_9	G_9	H_9	W_9
A_{10}	B_{10}	C_{10}	D_{10}	E_{10}	F_{10}	G_{10}	H_{10}	W_{10}
A_{11}	B_{11}	C_{11}	D_{11}	E_{11}	F_{11}	G_{11}	H_{11}	W_{11}
A_{12}	B_{12}	C_{12}	D_{12}	E_{12}	F_{12}	G_{12}	H_{12}	W_{12}
A_{13}	B_{13}	C_{13}	D_{13}	E_{13}	F_{13}	G_{13}	H_{13}	W_{13}
A_{14}	B_{14}	C_{14}	D_{14}	E_{14}	F_{14}	G_{14}	H_{14}	W_{14}
A_{15}	B_{15}	C_{15}	D_{15}	E_{15}	F_{15}	G_{15}	H_{15}	W_{15}
A_{16}	B_{16}	C_{16}	D_{16}	E_{16}	F_{16}	G_{16}	H_{16}	W_{16}
A_{17}	B_{17}	C_{17}	D_{17}	E_{17}	F_{17}	G_{17}	H_{17}	W_{17}
A_{18}	B_{18}	C_{18}	D_{18}	E_{18}	F_{18}	G_{18}	H_{18}	W_{18}
A_{19}	B_{19}	C_{19}	D_{19}	E_{19}	F_{19}	G_{19}	H_{19}	W_{19}
A_{20}	B_{20}	C_{20}	D_{20}	E_{20}	F_{20}	G_{20}	H_{20}	W_{20}
A_{21}	B_{21}	C_{21}	D_{21}	E_{21}	F_{21}	G_{21}	H_{21}	W_{21}
A_{22}	B_{22}	C_{22}	D_{22}	E_{22}	F_{22}	G_{22}	H_{22}	W_{22}
A_{23}	B_{23}	C_{23}	D_{23}	E_{23}	F_{23}	G_{23}	H_{23}	

< 표 2. 23라운드 ① >

5번 문제 답안

② 이 때 생성된 W_{22}를 이용하여 2.2에 의해 각 table의 H_{22}를 계산할 수 있다.

A_0	B_0	C_0	D_0	E_0	F_0	G_0	H_0	W_0
A_1	B_1	C_1	D_1	E_1	F_1	G_1	H_1	W_1
A_2	B_2	C_2	D_2	E_2	F_2	G_2	H_2	W_2
A_3	B_3	C_3	D_3	E_3	F_3	G_3	H_3	W_3
A_4	B_4	C_4	D_4	E_4	F_4	G_4	H_4	W_4
A_5	B_5	C_5	D_5	E_5	F_5	G_5	H_5	W_5
A_6	B_6	C_6	D_6	E_6	F_6	G_6	H_6	W_6
A_7	B_7	C_7	D_7	E_7	F_7	G_7	H_7	W_7
A_8	B_8	C_8	D_8	E_8	F_8	G_8	H_8	W_8
A_9	B_9	C_9	D_9	E_9	F_9	G_9	H_9	W_9
A_{10}	B_{10}	C_{10}	D_{10}	E_{10}	F_{10}	G_{10}	H_{10}	W_{10}
A_{11}	B_{11}	C_{11}	D_{11}	E_{11}	F_{11}	G_{11}	H_{11}	W_{11}
A_{12}	B_{12}	C_{12}	D_{12}	E_{12}	F_{12}	G_{12}	H_{12}	W_{12}
A_{13}	B_{13}	C_{13}	D_{13}	E_{13}	F_{13}	G_{13}	H_{13}	W_{13}
A_{14}	B_{14}	C_{14}	D_{14}	E_{14}	F_{14}	G_{14}	H_{14}	W_{14}
A_{15}	B_{15}	C_{15}	D_{15}	E_{15}	F_{15}	G_{15}	H_{15}	W_{15}
A_{16}	B_{16}	C_{16}	D_{16}	E_{16}	F_{16}	G_{16}	H_{16}	W_{16}
A_{17}	B_{17}	C_{17}	D_{17}	E_{17}	F_{17}	G_{17}	H_{17}	W_{17}
A_{18}	B_{18}	C_{18}	D_{18}	E_{18}	F_{18}	G_{18}	H_{18}	W_{18}
A_{19}	B_{19}	C_{19}	D_{19}	E_{19}	F_{19}	G_{19}	H_{19}	W_{19}
A_{20}	B_{20}	C_{20}	D_{20}	E_{20}	F_{20}	G_{20}	H_{20}	W_{20}
A_{21}	B_{21}	C_{21}	D_{21}	E_{21}	F_{21}	G_{21}	H_{21}	W_{21}
A_{22}	B_{22}	C_{22}	D_{22}	E_{22}	F_{22}	G_{22}	H_{22}	W_{22}
A_{23}	B_{23}	C_{23}	D_{23}	E_{23}	F_{23}	G_{23}	H_{23}	

< 표 3. 23라운드 ② >

그렇게 계산된 H_{22}를 ①에서의 A_{15}의 값과 비교하여 $A_{15} = H_{22}$인 $W_8, W_9, W_{10}, W_{11}, W_{12}, W_{13}, W_{14}$ 쌍들을 찾을 수 있다.

③ 위 ②를 만족시키는 $W_8, W_9, W_{10}, W_{11}, W_{12}, W_{13}, W_{14}$ 쌍들의 각 table에서 만들어진 $W_{16}, W_{17}, W_{19}, W_{20}$이 2.2를 만족시키는지를 확인한다.

④ 위 ③을 만족시키는 $W_8, W_9, W_{10}, W_{11}, W_{12}, W_{13}, W_{14}$ 쌍들의 각 table에서 2.2를 통해 W_{15}을 알아낼 수 있고, 그 W_{15}와 그 W_{15}에 의해 생성된 W_{18}, W_{21}이 2.2를 만족시키는지를 확인한다.

5번 문제 답안

결국 $W_8, W_9, W_{10}, W_{11}, W_{12}, W_{13}, W_{14}$ 를 brute force 하면 W_{15}가 고정된다. 그리고 $W_{16}, \cdots, W_{22}$이 앞의 값들에 의해 고정된다. $W_{16}, \cdots, W_{22}$ 식이 7개이므로 $(\frac{1}{2^{32}})^7$의 확률로 만족하고 $W_8, W_9, W_{10}, W_{11}, W_{12}, W_{13}, W_{14}$ 7개를 돌리므로 $(2^{32})^7 \times (\frac{1}{2^{32}})^7 = 1$개의 쌍이 존재한다.

CF 함수 계산을 1이라 하자. CF 함수를 한 번 연산하는 데에는 ROUND 함수가 23번 사용된다. 알고리즘에서 ROUND 함수의 계산만 이용했으므로 연산량은 $(2^{32})^7$이하로 가능하다.

5번 문제 답안

3.2 29라운드

2.2 성질과 MITM 공격을 사용하여 공격이 가능하다.

Round : 29
Given : Y
Settings : $A_0, B_0, C_0, D_0, E_0, F_0, G_0, H_0$ fixed (IV), $W_0, W_1, W_2, W_3, W_4, W_5, W_6, W_7$ fixed
⇒ Y를 알기 때문에 $A_{29}, B_{29}, C_{29}, D_{29}, E_{29}, F_{29}, G_{29}, H_{29}$를 알 수 있다.
⇒ 2.2를 통해 다음을 알 수 있다.

A_0	B_0	C_0	D_0	E_0	F_0	G_0	H_0	W_0
A_1	B_1	C_1	D_1	E_1	F_1	G_1	H_1	W_1
A_2	B_2	C_2	D_2	E_2	F_2	G_2	H_2	W_2
A_3	B_3	C_3	D_3	E_3	F_3	G_3	H_3	W_3
A_4	B_4	C_4	D_4	E_4	F_4	G_4	H_4	W_4
A_5	B_5	C_5	D_5	E_5	F_5	G_5	H_5	W_5
A_6	B_6	C_6	D_6	E_6	F_6	G_6	H_6	W_6
A_7	B_7	C_7	D_7	E_7	F_7	G_7	H_7	W_7
A_8	B_8	C_8	D_8	E_8	F_8	G_8	H_8	W_8
A_9	B_9	C_9	D_9	E_9	F_9	G_9	H_9	W_9
A_{10}	B_{10}	C_{10}	D_{10}	E_{10}	F_{10}	G_{10}	H_{10}	W_{10}
A_{11}	B_{11}	C_{11}	D_{11}	E_{11}	F_{11}	G_{11}	H_{11}	W_{11}
A_{12}	B_{12}	C_{12}	D_{12}	E_{12}	F_{12}	G_{12}	H_{12}	W_{12}
A_{13}	B_{13}	C_{13}	D_{13}	E_{13}	F_{13}	G_{13}	H_{13}	W_{13}
A_{14}	B_{14}	C_{14}	D_{14}	E_{14}	F_{14}	G_{14}	H_{14}	W_{14}
A_{15}	B_{15}	C_{15}	D_{15}	E_{15}	F_{15}	G_{15}	H_{15}	W_{15}
A_{16}	B_{16}	C_{16}	D_{16}	E_{16}	F_{16}	G_{16}	H_{16}	W_{16}
A_{17}	B_{17}	C_{17}	D_{17}	E_{17}	F_{17}	G_{17}	H_{17}	W_{17}
A_{18}	B_{18}	C_{18}	D_{18}	E_{18}	F_{18}	G_{18}	H_{18}	W_{18}
A_{19}	B_{19}	C_{19}	D_{19}	E_{19}	F_{19}	G_{19}	H_{19}	W_{19}
A_{20}	B_{20}	C_{20}	D_{20}	E_{20}	F_{20}	G_{20}	H_{20}	W_{20}
A_{21}	B_{21}	C_{21}	D_{21}	E_{21}	F_{21}	G_{21}	H_{21}	W_{21}
A_{22}	B_{22}	C_{22}	D_{22}	E_{22}	F_{22}	G_{22}	H_{22}	W_{22}
A_{23}	B_{23}	C_{23}	D_{23}	E_{23}	F_{23}	G_{23}	H_{23}	W_{23}
A_{24}	B_{24}	C_{24}	D_{24}	E_{24}	F_{24}	G_{24}	H_{24}	W_{24}
A_{25}	B_{25}	C_{25}	D_{25}	E_{25}	F_{25}	G_{25}	H_{25}	W_{25}
A_{26}	B_{26}	C_{26}	D_{26}	E_{26}	F_{26}	G_{26}	H_{26}	W_{26}
A_{27}	B_{27}	C_{27}	D_{27}	E_{27}	F_{27}	G_{27}	H_{27}	W_{27}
A_{28}	B_{28}	C_{28}	D_{28}	E_{28}	F_{28}	G_{28}	H_{28}	W_{28}
A_{29}	B_{29}	C_{29}	D_{29}	E_{29}	F_{29}	G_{29}	H_{29}	

< 표 4. 29라운드 Settings >

5번 문제 답안

① $W_8, W_9, W_{10}, W_{11}, W_{12}, W_{13}, W_{14}$ brute force

⇒ A_{15} table known 이고, $W_i (16 \leqq i \leqq 28)$ 중에서 $W_{16}, W_{17}, W_{19}, W_{20}, W_{22}, W_{25}, W_{28}$이 각 table에서 자동으로 계산된다.

A_0	B_0	C_0	D_0	E_0	F_0	G_0	H_0	W_0
A_1	B_1	C_1	D_1	E_1	F_1	G_1	H_1	W_1
A_2	B_2	C_2	D_2	E_2	F_2	G_2	H_2	W_2
A_3	B_3	C_3	D_3	E_3	F_3	G_3	H_3	W_3
A_4	B_4	C_4	D_4	E_4	F_4	G_4	H_4	W_4
A_5	B_5	C_5	D_5	E_5	F_5	G_5	H_5	W_5
A_6	B_6	C_6	D_6	E_6	F_6	G_6	H_6	W_6
A_7	B_7	C_7	D_7	E_7	F_7	G_7	H_7	W_7
A_8	B_8	C_8	D_8	E_8	F_8	G_8	H_8	W_8
A_9	B_9	C_9	D_9	E_9	F_9	G_9	H_9	W_9
A_{10}	B_{10}	C_{10}	D_{10}	E_{10}	F_{10}	G_{10}	H_{10}	W_{10}
A_{11}	B_{11}	C_{11}	D_{11}	E_{11}	F_{11}	G_{11}	H_{11}	W_{11}
A_{12}	B_{12}	C_{12}	D_{12}	E_{12}	F_{12}	G_{12}	H_{12}	W_{12}
A_{13}	B_{13}	C_{13}	D_{13}	E_{13}	F_{13}	G_{13}	H_{13}	W_{13}
A_{14}	B_{14}	C_{14}	D_{14}	E_{14}	F_{14}	G_{14}	H_{14}	W_{14}
A_{15}	B_{15}	C_{15}	D_{15}	E_{15}	F_{15}	G_{15}	H_{15}	W_{15}
A_{16}	B_{16}	C_{16}	D_{16}	E_{16}	F_{16}	G_{16}	H_{16}	W_{16}
A_{17}	B_{17}	C_{17}	D_{17}	E_{17}	F_{17}	G_{17}	H_{17}	W_{17}
A_{18}	B_{18}	C_{18}	D_{18}	E_{18}	F_{18}	G_{18}	H_{18}	W_{18}
A_{19}	B_{19}	C_{19}	D_{19}	E_{19}	F_{19}	G_{19}	H_{19}	W_{19}
A_{20}	B_{20}	C_{20}	D_{20}	E_{20}	F_{20}	G_{20}	H_{20}	W_{20}
A_{21}	B_{21}	C_{21}	D_{21}	E_{21}	F_{21}	G_{21}	H_{21}	W_{21}
A_{22}	B_{22}	C_{22}	D_{22}	E_{22}	F_{22}	G_{22}	H_{22}	W_{22}
A_{23}	B_{23}	C_{23}	D_{23}	E_{23}	F_{23}	G_{23}	H_{23}	W_{23}
A_{24}	B_{24}	C_{24}	D_{24}	E_{24}	F_{24}	G_{24}	H_{24}	W_{24}
A_{25}	B_{25}	C_{25}	D_{25}	E_{25}	F_{25}	G_{25}	H_{25}	W_{25}
A_{26}	B_{26}	C_{26}	D_{26}	E_{26}	F_{26}	G_{26}	H_{26}	W_{26}
A_{27}	B_{27}	C_{27}	D_{27}	E_{27}	F_{27}	G_{27}	H_{27}	W_{27}
A_{28}	B_{28}	C_{28}	D_{28}	E_{28}	F_{28}	G_{28}	H_{28}	W_{28}
A_{29}	B_{29}	C_{29}	D_{29}	E_{29}	F_{29}	G_{29}	H_{29}	

< 표 5. 29라운드 ① >

5번 문제 답안

② $W_{22}, W_{23}, W_{24}, W_{25}, W_{26}, W_{27}, W_{28}$ brute force

⇒ H_{22} table known 이고, 자동으로 계산되는 다른 W_i $(8 \le i \le 21)$들은 없다.

A_0	B_0	C_0	D_0	E_0	F_0	G_0	H_0	W_0
A_1	B_1	C_1	D_1	E_1	F_1	G_1	H_1	W_1
A_2	B_2	C_2	D_2	E_2	F_2	G_2	H_2	W_2
A_3	B_3	C_3	D_3	E_3	F_3	G_3	H_3	W_3
A_4	B_4	C_4	D_4	E_4	F_4	G_4	H_4	W_4
A_5	B_5	C_5	D_5	E_5	F_5	G_5	H_5	W_5
A_6	B_6	C_6	D_6	E_6	F_6	G_6	H_6	W_6
A_7	B_7	C_7	D_7	E_7	F_7	G_7	H_7	W_7
A_8	B_8	C_8	D_8	E_8	F_8	G_8	H_8	W_8
A_9	B_9	C_9	D_9	E_9	F_9	G_9	H_9	W_9
A_{10}	B_{10}	C_{10}	D_{10}	E_{10}	F_{10}	G_{10}	H_{10}	W_{10}
A_{11}	B_{11}	C_{11}	D_{11}	E_{11}	F_{11}	G_{11}	H_{11}	W_{11}
A_{12}	B_{12}	C_{12}	D_{12}	E_{12}	F_{12}	G_{12}	H_{12}	W_{12}
A_{13}	B_{13}	C_{13}	D_{13}	E_{13}	F_{13}	G_{13}	H_{13}	W_{13}
A_{14}	B_{14}	C_{14}	D_{14}	E_{14}	F_{14}	G_{14}	H_{14}	W_{14}
A_{15}	B_{15}	C_{15}	D_{15}	E_{15}	F_{15}	G_{15}	H_{15}	W_{15}
A_{16}	B_{16}	C_{16}	D_{16}	E_{16}	F_{16}	G_{16}	H_{16}	W_{16}
A_{17}	B_{17}	C_{17}	D_{17}	E_{17}	F_{17}	G_{17}	H_{17}	W_{17}
A_{18}	B_{18}	C_{18}	D_{18}	E_{18}	F_{18}	G_{18}	H_{18}	W_{18}
A_{19}	B_{19}	C_{19}	D_{19}	E_{19}	F_{19}	G_{19}	H_{19}	W_{19}
A_{20}	B_{20}	C_{20}	D_{20}	E_{20}	F_{20}	G_{20}	H_{20}	W_{20}
A_{21}	B_{21}	C_{21}	D_{21}	E_{21}	F_{21}	G_{21}	H_{21}	W_{21}
A_{22}	B_{22}	C_{22}	D_{22}	E_{22}	F_{22}	G_{22}	H_{22}	W_{22}
A_{23}	B_{23}	C_{23}	D_{23}	E_{23}	F_{23}	G_{23}	H_{23}	W_{23}
A_{24}	B_{24}	C_{24}	D_{24}	E_{24}	F_{24}	G_{24}	H_{24}	W_{24}
A_{25}	B_{25}	C_{25}	D_{25}	E_{25}	F_{25}	G_{25}	H_{25}	W_{25}
A_{26}	B_{26}	C_{26}	D_{26}	E_{26}	F_{26}	G_{26}	H_{26}	W_{26}
A_{27}	B_{27}	C_{27}	D_{27}	E_{27}	F_{27}	G_{27}	H_{27}	W_{27}
A_{28}	B_{28}	C_{28}	D_{28}	E_{28}	F_{28}	G_{28}	H_{28}	W_{28}
A_{29}	B_{29}	C_{29}	D_{29}	E_{29}	F_{29}	G_{29}	H_{29}	

< 표 6. 29라운드 ② >

5번 문제 답안

③ 각 table에서 $A_{15} = H_{22}$을 만족시키는 $W_8, W_9, W_{10}, W_{11}, W_{12}, W_{13}, W_{14}, W_{22}, W_{23}, W_{24}, W_{25}, W_{26}, W_{27}, W_{28}$ 쌍을 찾을 수 있고 그것을 하나의 table로 만들 수 있다.

A_0	B_0	C_0	D_0	E_0	F_0	G_0	H_0	W_0
A_1	B_1	C_1	D_1	E_1	F_1	G_1	H_1	W_1
A_2	B_2	C_2	D_2	E_2	F_2	G_2	H_2	W_2
A_3	B_3	C_3	D_3	E_3	F_3	G_3	H_3	W_3
A_4	B_4	C_4	D_4	E_4	F_4	G_4	H_4	W_4
A_5	B_5	C_5	D_5	E_5	F_5	G_5	H_5	W_5
A_6	B_6	C_6	D_6	E_6	F_6	G_6	H_6	W_6
A_7	B_7	C_7	D_7	E_7	F_7	G_7	H_7	W_7
A_8	B_8	C_8	D_8	E_8	F_8	G_8	H_8	W_8
A_9	B_9	C_9	D_9	E_9	F_9	G_9	H_9	W_9
A_{10}	B_{10}	C_{10}	D_{10}	E_{10}	F_{10}	G_{10}	H_{10}	W_{10}
A_{11}	B_{11}	C_{11}	D_{11}	E_{11}	F_{11}	G_{11}	H_{11}	W_{11}
A_{12}	B_{12}	C_{12}	D_{12}	E_{12}	F_{12}	G_{12}	H_{12}	W_{12}
A_{13}	B_{13}	C_{13}	D_{13}	E_{13}	F_{13}	G_{13}	H_{13}	W_{13}
A_{14}	B_{14}	C_{14}	D_{14}	E_{14}	F_{14}	G_{14}	H_{14}	W_{14}
A_{15}	B_{15}	C_{15}	D_{15}	E_{15}	F_{15}	G_{15}	H_{15}	W_{15}
A_{16}	B_{16}	C_{16}	D_{16}	E_{16}	F_{16}	G_{16}	H_{16}	W_{16}
A_{17}	B_{17}	C_{17}	D_{17}	E_{17}	F_{17}	G_{17}	H_{17}	W_{17}
A_{18}	B_{18}	C_{18}	D_{18}	E_{18}	F_{18}	G_{18}	H_{18}	W_{18}
A_{19}	B_{19}	C_{19}	D_{19}	E_{19}	F_{19}	G_{19}	H_{19}	W_{19}
A_{20}	B_{20}	C_{20}	D_{20}	E_{20}	F_{20}	G_{20}	H_{20}	W_{20}
A_{21}	B_{21}	C_{21}	D_{21}	E_{21}	F_{21}	G_{21}	H_{21}	W_{21}
A_{22}	B_{22}	C_{22}	D_{22}	E_{22}	F_{22}	G_{22}	H_{22}	W_{22}
A_{23}	B_{23}	C_{23}	D_{23}	E_{23}	F_{23}	G_{23}	H_{23}	W_{23}
A_{24}	B_{24}	C_{24}	D_{24}	E_{24}	F_{24}	G_{24}	H_{24}	W_{24}
A_{25}	B_{25}	C_{25}	D_{25}	E_{25}	F_{25}	G_{25}	H_{25}	W_{25}
A_{26}	B_{26}	C_{26}	D_{26}	E_{26}	F_{26}	G_{26}	H_{26}	W_{26}
A_{27}	B_{27}	C_{27}	D_{27}	E_{27}	F_{27}	G_{27}	H_{27}	W_{27}
A_{28}	B_{28}	C_{28}	D_{28}	E_{28}	F_{28}	G_{28}	H_{28}	W_{28}
A_{29}	B_{29}	C_{29}	D_{29}	E_{29}	F_{29}	G_{29}	H_{29}	

< 표 7. 29라운드 ③ >

④ 위 ③을 만족시키는 $W_8, W_9, W_{10}, W_{11}, W_{12}, W_{13}, W_{14}, W_{22}, W_{23}, W_{24}, W_{25}, W_{26}, W_{27}, W_{28}$ 쌍의 각 table에서 ①에서 자동으로 계산된 W_{22}, W_{25}, W_{28}가 ②에서의 W_{22}, W_{25}, W_{28}과 일치하는지를 확인한다.

5번 문제 답안

⑤ 위 ④를 만족시키는 $W_8, W_9, W_{10}, W_{11}, W_{12}, W_{13}, W_{14}, W_{22}, W_{23}, W_{24}, W_{25}, W_{26}, W_{27}, W_{28}$ 쌍의 각 table에서 ①에서 자동으로 계산된 $W_{16}, W_{17}, W_{19}, W_{20}$가 2.2 성질을 만족시키는지를 확인한다.

⑥ 위 ⑤를 만족시키는 $W_8, W_9, W_{10}, W_{11}, W_{12}, W_{13}, W_{14}, W_{22}, W_{23}, W_{24}, W_{25}, W_{26}, W_{27}, W_{28}$ 쌍의 각 table에서 2.2 성질을 통해 W_{15}을 알아낼 수 있고, 그 W_{15}에 의해 생성된 $W_{23}, W_{24}, W_{26}, W_{27}$이 table의 $W_{23}, W_{24}, W_{26}, W_{27}$과 일치하는지를 확인한다.

⑦ 위 ⑥을 만족시키는 $W_8, W_9, W_{10}, W_{11}, W_{12}, W_{13}, W_{14}, W_{22}, W_{23}, W_{24}, W_{25}, W_{26}, W_{27}, W_{28}$ 쌍의 각 table에서 2.2 성질을 통해 알게 된 W_{15}와 그 W_{15}에 의해 생성된 W_{18}, W_{21}들이 2.2 성질을 만족시키는지를 확인한다.

각각을 brute force한 table을 비교하는 과정에서 W_{15}가 고정된다. 그리고 $W_{16}, \cdots, W_{28}$ 이 앞의 값에 의해 고정된다. $W_{16}, \cdots, W_{28}$ 13개의 식이 있으므로 $(\frac{1}{2^{32}})^{13}$의 확률로 만족하고 brute force를 7개씩 두 번을 돌리므로 $(2^{32})^{14} \times (\frac{1}{2^{32}})^{13} = 2^{32}$개의 쌍이 존재한다.

CF 함수 계산을 1이라 하자. CF 함수를 한 번 연산하는 데에는 ROUND 함수가 29번 사용된다. 알고리즘에서 ROUND 함수의 계산만 이용했으므로 연산량은 $2^*(2^{32})^7 = 2^{225}$이하로 가능하다.

5번 문제 답안

3.3 30라운드

Round : 30
Given : Y
Settings : $A_0, B_0, C_0, D_0, E_0, F_0, G_0, H_0$ fixed (IV), $W_0, W_1, W_2, W_3, W_4, W_5, W_6, W_7$ fixed
⇒ Y를 알기 때문에 $A_{30}, B_{30}, C_{30}, D_{30}, E_{30}, F_{30}, G_{30}, H_{30}$을 알 수 있다.
⇒ 2.2 성질을 통해 다음을 알 수 있다.

A_0	B_0	C_0	D_0	E_0	F_0	G_0	H_0	W_0
A_1	B_1	C_1	D_1	E_1	F_1	G_1	H_1	W_1
A_2	B_2	C_2	D_2	E_2	F_2	G_2	H_2	W_2
A_3	B_3	C_3	D_3	E_3	F_3	G_3	H_3	W_3
A_4	B_4	C_4	D_4	E_4	F_4	G_4	H_4	W_4
A_5	B_5	C_5	D_5	E_5	F_5	G_5	H_5	W_5
A_6	B_6	C_6	D_6	E_6	F_6	G_6	H_6	W_6
A_7	B_7	C_7	D_7	E_7	F_7	G_7	H_7	W_7
A_8	B_8	C_8	D_8	E_8	F_8	G_8	H_8	W_8
A_9	B_9	C_9	D_9	E_9	F_9	G_9	H_9	W_9
A_{10}	B_{10}	C_{10}	D_{10}	E_{10}	F_{10}	G_{10}	H_{10}	W_{10}
A_{11}	B_{11}	C_{11}	D_{11}	E_{11}	F_{11}	G_{11}	H_{11}	W_{11}
A_{12}	B_{12}	C_{12}	D_{12}	E_{12}	F_{12}	G_{12}	H_{12}	W_{12}
A_{13}	B_{13}	C_{13}	D_{13}	E_{13}	F_{13}	G_{13}	H_{13}	W_{13}
A_{14}	B_{14}	C_{14}	D_{14}	E_{14}	F_{14}	G_{14}	H_{14}	W_{14}
A_{15}	B_{15}	C_{15}	D_{15}	E_{15}	F_{15}	G_{15}	H_{15}	W_{15}
A_{16}	B_{16}	C_{16}	D_{16}	E_{16}	F_{16}	G_{16}	H_{16}	W_{16}
A_{17}	B_{17}	C_{17}	D_{17}	E_{17}	F_{17}	G_{17}	H_{17}	W_{17}
A_{18}	B_{18}	C_{18}	D_{18}	E_{18}	F_{18}	G_{18}	H_{18}	W_{18}
A_{19}	B_{19}	C_{19}	D_{19}	E_{19}	F_{19}	G_{19}	H_{19}	W_{19}
A_{20}	B_{20}	C_{20}	D_{20}	E_{20}	F_{20}	G_{20}	H_{20}	W_{20}
A_{21}	B_{21}	C_{21}	D_{21}	E_{21}	F_{21}	G_{21}	H_{21}	W_{21}
A_{22}	B_{22}	C_{22}	D_{22}	E_{22}	F_{22}	G_{22}	H_{22}	W_{22}
A_{23}	B_{23}	C_{23}	D_{23}	E_{23}	F_{23}	G_{23}	H_{23}	W_{23}
A_{24}	B_{24}	C_{24}	D_{24}	E_{24}	F_{24}	G_{24}	H_{24}	W_{24}
A_{25}	B_{25}	C_{25}	D_{25}	E_{25}	F_{25}	G_{25}	H_{25}	W_{25}
A_{26}	B_{26}	C_{26}	D_{26}	E_{26}	F_{26}	G_{26}	H_{26}	W_{26}
A_{27}	B_{27}	C_{27}	D_{27}	E_{27}	F_{27}	G_{27}	H_{27}	W_{27}
A_{28}	B_{28}	C_{28}	D_{28}	E_{28}	F_{28}	G_{28}	H_{28}	W_{28}
A_{29}	B_{29}	C_{29}	D_{29}	E_{29}	F_{29}	G_{29}	H_{29}	W_{29}
A_{30}	B_{30}	C_{30}	D_{30}	E_{30}	F_{30}	G_{30}	H_{30}	

< 표 8. 30라운드 Settings >

5번 문제 답안

① $W_8, W_9, W_{10}, W_{11}, W_{12}, W_{13}, W_{14}$ brute force

⇒ A_{15} table known 이고, $W_i (16 \leq i \leq 29)$ 중에서 $W_{16}, W_{17}, W_{19}, W_{20}, W_{22}, W_{25}, W_{28}$이 각 table에서 자동으로 계산된다.

A_0	B_0	C_0	D_0	E_0	F_0	G_0	H_0	W_0
A_1	B_1	C_1	D_1	E_1	F_1	G_1	H_1	W_1
A_2	B_2	C_2	D_2	E_2	F_2	G_2	H_2	W_2
A_3	B_3	C_3	D_3	E_3	F_3	G_3	H_3	W_3
A_4	B_4	C_4	D_4	E_4	F_4	G_4	H_4	W_4
A_5	B_5	C_5	D_5	E_5	F_5	G_5	H_5	W_5
A_6	B_6	C_6	D_6	E_6	F_6	G_6	H_6	W_6
A_7	B_7	C_7	D_7	E_7	F_7	G_7	H_7	W_7
A_8	B_8	C_8	D_8	E_8	F_8	G_8	H_8	W_8
A_9	B_9	C_9	D_9	E_9	F_9	G_9	H_9	W_9
A_{10}	B_{10}	C_{10}	D_{10}	E_{10}	F_{10}	G_{10}	H_{10}	W_{10}
A_{11}	B_{11}	C_{11}	D_{11}	E_{11}	F_{11}	G_{11}	H_{11}	W_{11}
A_{12}	B_{12}	C_{12}	D_{12}	E_{12}	F_{12}	G_{12}	H_{12}	W_{12}
A_{13}	B_{13}	C_{13}	D_{13}	E_{13}	F_{13}	G_{13}	H_{13}	W_{13}
A_{14}	B_{14}	C_{14}	D_{14}	E_{14}	F_{14}	G_{14}	H_{14}	W_{14}
A_{15}	B_{15}	C_{15}	D_{15}	E_{15}	F_{15}	G_{15}	H_{15}	W_{15}
A_{16}	B_{16}	C_{16}	D_{16}	E_{16}	F_{16}	G_{16}	H_{16}	W_{16}
A_{17}	B_{17}	C_{17}	D_{17}	E_{17}	F_{17}	G_{17}	H_{17}	W_{17}
A_{18}	B_{18}	C_{18}	D_{18}	E_{18}	F_{18}	G_{18}	H_{18}	W_{18}
A_{19}	B_{19}	C_{19}	D_{19}	E_{19}	F_{19}	G_{19}	H_{19}	W_{19}
A_{20}	B_{20}	C_{20}	D_{20}	E_{20}	F_{20}	G_{20}	H_{20}	W_{20}
A_{21}	B_{21}	C_{21}	D_{21}	E_{21}	F_{21}	G_{21}	H_{21}	W_{21}
A_{22}	B_{22}	C_{22}	D_{22}	E_{22}	F_{22}	G_{22}	H_{22}	W_{22}
A_{23}	B_{23}	C_{23}	D_{23}	E_{23}	F_{23}	G_{23}	H_{23}	W_{23}
A_{24}	B_{24}	C_{24}	D_{24}	E_{24}	F_{24}	G_{24}	H_{24}	W_{24}
A_{25}	B_{25}	C_{25}	D_{25}	E_{25}	F_{25}	G_{25}	H_{25}	W_{25}
A_{26}	B_{26}	C_{26}	D_{26}	E_{26}	F_{26}	G_{26}	H_{26}	W_{26}
A_{27}	B_{27}	C_{27}	D_{27}	E_{27}	F_{27}	G_{27}	H_{27}	W_{27}
A_{28}	B_{28}	C_{28}	D_{28}	E_{28}	F_{28}	G_{28}	H_{28}	W_{28}
A_{29}	B_{29}	C_{29}	D_{29}	E_{29}	F_{29}	G_{29}	H_{29}	W_{29}
A_{30}	B_{30}	C_{30}	D_{30}	E_{30}	F_{30}	G_{30}	H_{30}	

< 표 9. 30라운드 ① >

5번 문제 답안

② $W_{23}, W_{24}, W_{25}, W_{26}, W_{27}, W_{28}, W_{29}$ brute force

⇒ H_{23} table known 이고, 자동으로 계산되는 다른 W_i $(8 \le i \le 22)$들은 없다.

A_0	B_0	C_0	D_0	E_0	F_0	G_0	H_0	W_0
A_1	B_1	C_1	D_1	E_1	F_1	G_1	H_1	W_1
A_2	B_2	C_2	D_2	E_2	F_2	G_2	H_2	W_2
A_3	B_3	C_3	D_3	E_3	F_3	G_3	H_3	W_3
A_4	B_4	C_4	D_4	E_4	F_4	G_4	H_4	W_4
A_5	B_5	C_5	D_5	E_5	F_5	G_5	H_5	W_5
A_6	B_6	C_6	D_6	E_6	F_6	G_6	H_6	W_6
A_7	B_7	C_7	D_7	E_7	F_7	G_7	H_7	W_7
A_8	B_8	C_8	D_8	E_8	F_8	G_8	H_8	W_8
A_9	B_9	C_9	D_9	E_9	F_9	G_9	H_9	W_9
A_{10}	B_{10}	C_{10}	D_{10}	E_{10}	F_{10}	G_{10}	H_{10}	W_{10}
A_{11}	B_{11}	C_{11}	D_{11}	E_{11}	F_{11}	G_{11}	H_{11}	W_{11}
A_{12}	B_{12}	C_{12}	D_{12}	E_{12}	F_{12}	G_{12}	H_{12}	W_{12}
A_{13}	B_{13}	C_{13}	D_{13}	E_{13}	F_{13}	G_{13}	H_{13}	W_{13}
A_{14}	B_{14}	C_{14}	D_{14}	E_{14}	F_{14}	G_{14}	H_{14}	W_{14}
A_{15}	B_{15}	C_{15}	D_{15}	E_{15}	F_{15}	G_{15}	H_{15}	W_{15}
A_{16}	B_{16}	C_{16}	D_{16}	E_{16}	F_{16}	G_{16}	H_{16}	W_{16}
A_{17}	B_{17}	C_{17}	D_{17}	E_{17}	F_{17}	G_{17}	H_{17}	W_{17}
A_{18}	B_{18}	C_{18}	D_{18}	E_{18}	F_{18}	G_{18}	H_{18}	W_{18}
A_{19}	B_{19}	C_{19}	D_{19}	E_{19}	F_{19}	G_{19}	H_{19}	W_{19}
A_{20}	B_{20}	C_{20}	D_{20}	E_{20}	F_{20}	G_{20}	H_{20}	W_{20}
A_{21}	B_{21}	C_{21}	D_{21}	E_{21}	F_{21}	G_{21}	H_{21}	W_{21}
A_{22}	B_{22}	C_{22}	D_{22}	E_{22}	F_{22}	G_{22}	H_{22}	W_{22}
A_{23}	B_{23}	C_{23}	D_{23}	E_{23}	F_{23}	G_{23}	H_{23}	W_{23}
A_{24}	B_{24}	C_{24}	D_{24}	E_{24}	F_{24}	G_{24}	H_{24}	W_{24}
A_{25}	B_{25}	C_{25}	D_{25}	E_{25}	F_{25}	G_{25}	H_{25}	W_{25}
A_{26}	B_{26}	C_{26}	D_{26}	E_{26}	F_{26}	G_{26}	H_{26}	W_{26}
A_{27}	B_{27}	C_{27}	D_{27}	E_{27}	F_{27}	G_{27}	H_{27}	W_{27}
A_{28}	B_{28}	C_{28}	D_{28}	E_{28}	F_{28}	G_{28}	H_{28}	W_{28}
A_{29}	B_{29}	C_{29}	D_{29}	E_{29}	F_{29}	G_{29}	H_{29}	W_{29}
A_{30}	B_{30}	C_{30}	D_{30}	E_{30}	F_{30}	G_{30}	H_{30}	

< 표 10. 30라운드 ② >

5번 문제 답안

③ 위 ①에서 얻은 table에서 계산된 W_{25}, W_{28}와 ②에서의 $W_{23}, W_{24}, W_{25}, W_{26}, W_{27}, W_{28}, W_{29}$ table의 W_{25}, W_{28}이 일치하는지 확인하여, 일치하는 $W_8, W_9, W_{10}, W_{11}, W_{12}, W_{13}, W_{14}$, $W_{23}, W_{24}, W_{25}, W_{26}, W_{27}, W_{28}, W_{29}$ 쌍을 찾을 수 있고 그것을 하나의 table로 만들 수 있다.

A_0	B_0	C_0	D_0	E_0	F_0	G_0	H_0	W_0
A_1	B_1	C_1	D_1	E_1	F_1	G_1	H_1	W_1
A_2	B_2	C_2	D_2	E_2	F_2	G_2	H_2	W_2
A_3	B_3	C_3	D_3	E_3	F_3	G_3	H_3	W_3
A_4	B_4	C_4	D_4	E_4	F_4	G_4	H_4	W_4
A_5	B_5	C_5	D_5	E_5	F_5	G_5	H_5	W_5
A_6	B_6	C_6	D_6	E_6	F_6	G_6	H_6	W_6
A_7	B_7	C_7	D_7	E_7	F_7	G_7	H_7	W_7
A_8	B_8	C_8	D_8	E_8	F_8	G_8	H_8	W_8
A_9	B_9	C_9	D_9	E_9	F_9	G_9	H_9	W_9
A_{10}	B_{10}	C_{10}	D_{10}	E_{10}	F_{10}	G_{10}	H_{10}	W_{10}
A_{11}	B_{11}	C_{11}	D_{11}	E_{11}	F_{11}	G_{11}	H_{11}	W_{11}
A_{12}	B_{12}	C_{12}	D_{12}	E_{12}	F_{12}	G_{12}	H_{12}	W_{12}
A_{13}	B_{13}	C_{13}	D_{13}	E_{13}	F_{13}	G_{13}	H_{13}	W_{13}
A_{14}	B_{14}	C_{14}	D_{14}	E_{14}	F_{14}	G_{14}	H_{14}	W_{14}
A_{15}	B_{15}	C_{15}	D_{15}	E_{15}	F_{15}	G_{15}	H_{15}	W_{15}
A_{16}	B_{16}	C_{16}	D_{16}	E_{16}	F_{16}	G_{16}	H_{16}	W_{16}
A_{17}	B_{17}	C_{17}	D_{17}	E_{17}	F_{17}	G_{17}	H_{17}	W_{17}
A_{18}	B_{18}	C_{18}	D_{18}	E_{18}	F_{18}	G_{18}	H_{18}	W_{18}
A_{19}	B_{19}	C_{19}	D_{19}	E_{19}	F_{19}	G_{19}	H_{19}	W_{19}
A_{20}	B_{20}	C_{20}	D_{20}	E_{20}	F_{20}	G_{20}	H_{20}	W_{20}
A_{21}	B_{21}	C_{21}	D_{21}	E_{21}	F_{21}	G_{21}	H_{21}	W_{21}
A_{22}	B_{22}	C_{22}	D_{22}	E_{22}	F_{22}	G_{22}	H_{22}	W_{22}
A_{23}	B_{23}	C_{23}	D_{23}	E_{23}	F_{23}	G_{23}	H_{23}	W_{23}
A_{24}	B_{24}	C_{24}	D_{24}	E_{24}	F_{24}	G_{24}	H_{24}	W_{24}
A_{25}	B_{25}	C_{25}	D_{25}	E_{25}	F_{25}	G_{25}	H_{25}	W_{25}
A_{26}	B_{26}	C_{26}	D_{26}	E_{26}	F_{26}	G_{26}	H_{26}	W_{26}
A_{27}	B_{27}	C_{27}	D_{27}	E_{27}	F_{27}	G_{27}	H_{27}	W_{27}
A_{28}	B_{28}	C_{28}	D_{28}	E_{28}	F_{28}	G_{28}	H_{28}	W_{28}
A_{29}	B_{29}	C_{29}	D_{29}	E_{29}	F_{29}	G_{29}	H_{29}	W_{29}
A_{30}	B_{30}	C_{30}	D_{30}	E_{30}	F_{30}	G_{30}	H_{30}	

< 표 11. 30라운드 ③ >

5번 문제 답안

④ 위 ③을 만족시키는 $W_8, W_9, W_{10}, W_{11}, W_{12}, W_{13}, W_{14}, W_{23}, W_{24}, W_{25}, W_{26}, W_{27}, W_{28}, W_{29}$ 쌍의 각 table에서 ①에서 자동으로 계산된 $W_{16}, W_{17}, W_{19}, W_{20}, W_{22}$가 2.2 성질을 만족시키는지를 확인한다.

⑤ 위 ④를 만족시키는 $W_8, W_9, W_{10}, W_{11}, W_{12}, W_{13}, W_{14}, W_{23}, W_{24}, W_{25}, W_{26}, W_{27}, W_{28}, W_{29}$ 쌍의 각 table에서 2.2 성질을 통해 W_{15}을 알아낼 수 있고, 그 W_{15}에 의해 생성된 $W_{23}, W_{24}, W_{26}, W_{27}, W_{29}$가 table의 $W_{23}, W_{24}, W_{26}, W_{27}, W_{29}$와 일치하는지를 확인한다.

⑥ 위 ⑤를 만족시키는 $W_8, W_9, W_{10}, W_{11}, W_{12}, W_{13}, W_{14}, W_{23}, W_{24}, W_{25}, W_{26}, W_{27}, W_{28}, W_{29}$ 쌍의 각 table에서 2.2를 통해 알게 된 W_{15}와 그 W_{15}에 의해 생성된 W_{18}, W_{21}들이 2.2 성질을 만족시키는지를 확인한다.

각 brute force한 table을 비교하는 과정에서 W_{15}가 고정된다. 그리고 $W_{16}, \cdots, W_{29}$ 이 앞의 값에 의해 고정된다. $W_{16}, \cdots, W_{29}$ 14개의 식이 있으므로 $(\frac{1}{2^{32}})^{14}$의 확률로 만족하고 brute force를 7개씩 두 번을 돌리므로 $(2^{32})^{14} \times (\frac{1}{2^{32}})^{14} = 1$개의 쌍이 존재한다.

CF 함수 계산을 1이라 하자. CF 함수를 한 번 연산하는 데에는 ROUND 함수가 30번 사용된다. 알고리즘에서 ROUND 함수의 계산만 이용했으므로 연산량은 $2^*(2^{32})^7 = 2^{225}$이하로 가능하다.