2020 암호분석경진대회

5번 문제 : 해시 함수

임의의 256비트값 Y에 대해, 2^{253}번의 CF함수 연산 보다 작은 계산량으로, Y를 출력 값으로 갖는 CF의 어떤 768비트 입력값 X를 찾을 수 있는 최대의 라운드 수(=L)를 구하고, Y로부터 X를 찾는 알고리즘을 기술하시오.

문제에서 함수 CF는 768비트 입력값에 대하여 256비트 출력 값을 생성한다.

CF 함수 구조

#입력값: $X = (A_0, B_0, C_0, D_0, E_0, F_0, G_0, H_0, W_0, W_1, \ldots, W_{15})$,
where $A_0, B_0, C_0, D_0, E_0, F_0, G_0, H_0, W_0, W_1, \ldots, W_{15}$ are 32-bit.
#중간변수: $A_i, B_i, C_i, D_i, E_i, F_i, G_i, H_i$, which are 32-bit.
#라운드 수: L
#출력값: $Y = (A_0 \oplus A_L, B_0 \oplus B_L, C_0 \oplus C_L, D_0 \oplus D_L, E_0 \oplus E_L, F_0 \oplus F_L, G_0 \oplus G_L, H_0 \oplus H_L)$
For i = 16 to L-1:
$W_i = (W_{i-3} \lll 1) \oplus (W_{i-8} \lll 6) \oplus (W_{i-14} \lll 11) \oplus W_{i-16}$
For i = 0 to L-1:
$(A_{i+1}, B_{i+1}, C_{i+1}, D_{i+1}, E_{i+1}, F_{i+1}, G_{i+1}, H_{i+1}) = \text{Round}(A_i, B_i, C_i, D_i, E_i, F_i, G_i, H_i, W_i)$

CF 함수 구조 설명에 포함된 Round는 다음과 같은 구조를 가진 함수이다.

i 번째 Round 함수 구조

#입력값: $(A_i, B_i, C_i, D_i, E_i, F_i, G_i, H_i, W_i)$
#중간변수: T which is 32-bit
#출력값: $(A_{i+1}, B_{i+1}, C_{i+1}, D_{i+1}, E_{i+1}, F_{i+1}, G_{i+1}, H_{i+1})$
$T = (W_i[0], W_i[1], W_i[2], W_i[3])$
$T = \text{MDS}(S(T[0] \oplus A_i[0]), S(T[1] \oplus A_i[1]), S(T[2] \oplus A_i[2]), S(T[3] \oplus A_i[3]))$
$T = \text{MDS}(S(T[0] \oplus B_i[0]), S(T[1] \oplus B_i[1]), S(T[2] \oplus B_i[2]), S(T[3] \oplus B_i[3]))$
$T = \text{MDS}(S(T[0] \oplus C_i[0]), S(T[1] \oplus C_i[1]), S(T[2] \oplus C_i[2]), S(T[3] \oplus C_i[3]))$
$T = \text{MDS}(S(T[0] \oplus D_i[0]), S(T[1] \oplus D_i[1]), S(T[2] \oplus D_i[2]), S(T[3] \oplus D_i[3]))$
$T = \text{MDS}(S(T[0] \oplus E_i[0]), S(T[1] \oplus E_i[1]), S(T[2] \oplus E_i[2]), S(T[3] \oplus E_i[3]))$
$T = \text{MDS}(S(T[0] \oplus F_i[0]), S(T[1] \oplus F_i[1]), S(T[2] \oplus F_i[2]), S(T[3] \oplus F_i[3]))$
$T = \text{MDS}(S(T[0] \oplus G_i[0]), S(T[1] \oplus G_i[1]), S(T[2] \oplus G_i[2]), S(T[3] \oplus G_i[3]))$
$(A_{i+1}, B_{i+1}, C_{i+1}, D_{i+1}, E_{i+1}, F_{i+1}, G_{i+1}, H_{i+1}) = (H_i \oplus T, A_i, B_i, C_i, D_i, E_i, F_i, G_i)$

위 함수 구조 기술에서 사용된 기호 및 연산은 다음과 같이 설명된다.

기호 및 연산 설명

① $\oplus$: 비트별 배타적 논리합 (Bitwise eXclusive OR)
② $\lll$ n : n비트 Left Rotation
③ S() : 블록암호 AES의 S-box (참고문헌: FIPS 197)
④ MDS() : 블록암호 AES의 MDS 행렬곱 (참고문헌: FIPS 197)
⑤ T = (T[0],T[1],T[2],T[3]) : 4개의 8비트값 T[0], T[1], T[2], T[3]을 32비트로 이어 붙여 T에 저장하는 연산
⑥ (T[0],T[1],T[2],T[3]) = T : 32비트값 T를 4개의 8비트값 T[0], T[1], T[2], T[3]으로 분할하는 연산