2021 암호분석경진대회

5번 문제 : 해시 함수

아래와 같은 해시함수에 대해, 동일한 해시 값을 가지는 서로 다른 메시지 쌍(충돌쌍)을 제시하시오. (작은 공격복잡도로 충돌쌍을 찾는 경우 가산점 부여)

※ 제출물:
공격 기법을 간략하게 설명, 충돌쌍 공격에 필요한 공격복잡도 제시, 충돌쌍 공격 알고리즘의 pseudo code 작성, 동일한 해시 값을 가지는 서로 다른 메시지 쌍 제시

<용어 정의>

- $X^{0,1,\cdots,l-1}$: X가 $32\times l$-bit 길이의 데이터일 때, $X=X^0\|X^1\|\cdots\|X^{l-1}=X^{0,1,\cdots,l-1}$
- CV_{n-1}: n번째 compression 함수에 입력되는 128-bit 연쇄변수(Chaining Variable), $n=1,2,\cdots$.
- M_{n-1}: n번째 compression 함수에 입력되는 256-bit 메시지 블록, $n=1,2,\cdots$.
- $Midori64(Data,Key)$: 64-bit $Data$를 블록암호 Midori64 (https://eprint.iacr.org/2015/1142.pdf)에서 128-bit Key로 암호화한 64-bit 암호문

블록암호 Midori64를 기반으로 설계되어 128-bit 해시 값을 출력하는 해시함수는 다음과 같이 작동한다.

Midori64 기반 해시함수 정의

입력: 256-bit의 배수 길이의 메시지 $M=M_0\|M_1\|\cdots\|M_{m-1}$

출력: 128-bit 해시 값 CV_m

$IV=CV_0=CV_0^{0,1,2,3}=0x88888888888888889999999999999999;$
$For\ \ i=0\sim m-1:$
$\quad CV_{i+1}=Compression(CV_i,M_i);$
return CV_m

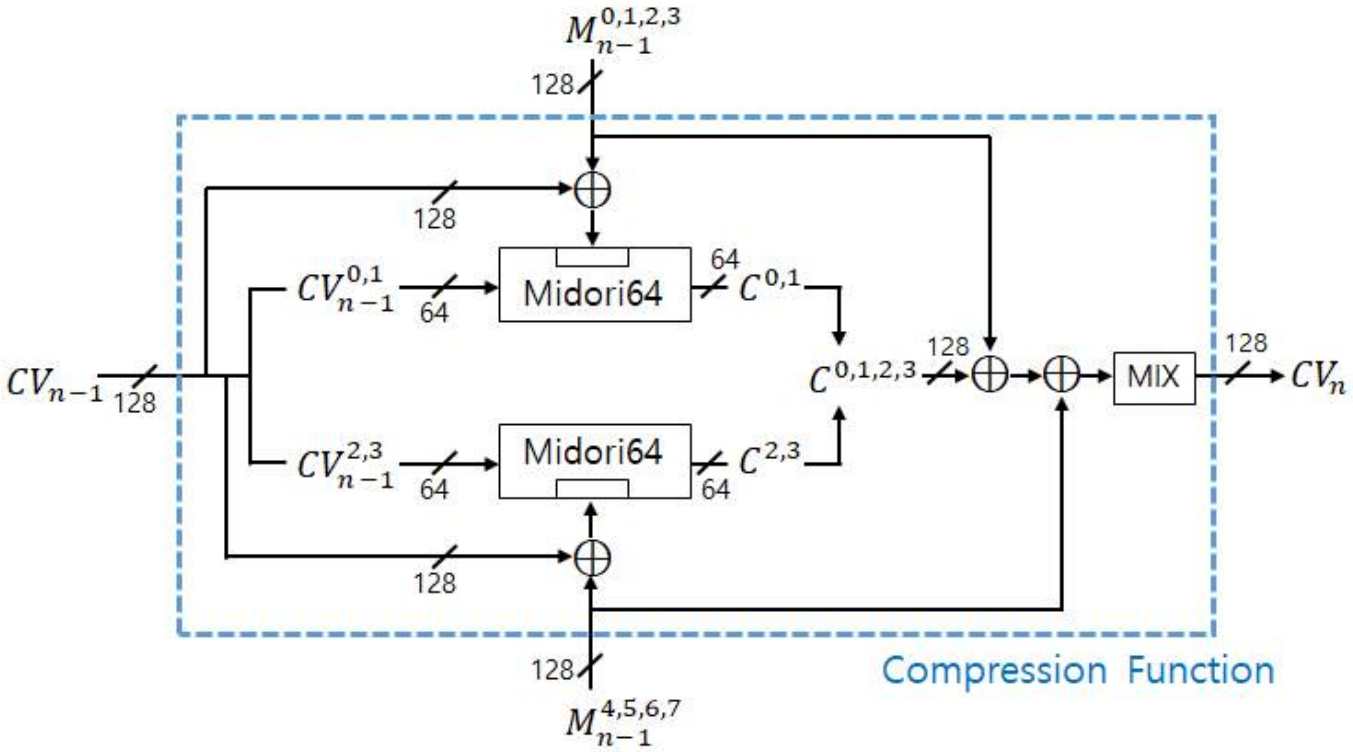
$Compression$ 함수 정의

입력: 128-bit 길이의 연쇄변수 CV_{n-1}, 256-bit의 길이의 메시지 블록 M_{n-1}

출력: 128-bit 연쇄변수 CV_n

$C^{0,1}=Midori64(CV_{n-1}^{0,1},M_{n-1}^{0,1,2,3}\oplus CV_{n-1});$
$C^{2,3}=Midori64(CV_{n-1}^{2,3},M_{n-1}^{4,5,6,7}\oplus CV_{n-1});$
$C^{0,1,2,3}=C^{0,1}\|C^{2,3};$
$C^{0,1,2,3}=C^{0,1,2,3}\oplus M_{n-1}^{0,1,2,3}\oplus M_{n-1}^{4,5,6,7};$
$CV_n=C^0\|C^3\|C^2\|C^1=MIX(C^{0,1,2,3});$
return CV_n

아래 그림은 Midori64 기반으로 설계된 블록암호 기반 해시함수의 n번째 compression 함수의 도식도이다.



Test Vector 1

$M = M_0$ = 0x0000000000000000000000000000000000000000000000000000000000000000

해시 값: 0xca712515a15b5dbf5357d91d7b6bbd14

Test Vector 2

$M = M_0 \| M_1$

M_0 = 0x0000000000000000000000000000000000000000000000000000000000000000

M_1 = 0x0000000000000000000000000000000000000000000000000000000000000000

해시 값: 0x823e590925d042b24d74e29d61bb207d

Test Vector 3

$M = M_0$ = 0x000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f

해시 값: 0xe4cfa3b8a55c123d449ec93801c3095e