2019 암호경진대회 : 4번 문제 답안

답) $j = 10$

$Message = 0x00000000000000000000000006451cf960001020300f4b9fbd87c975860676665$

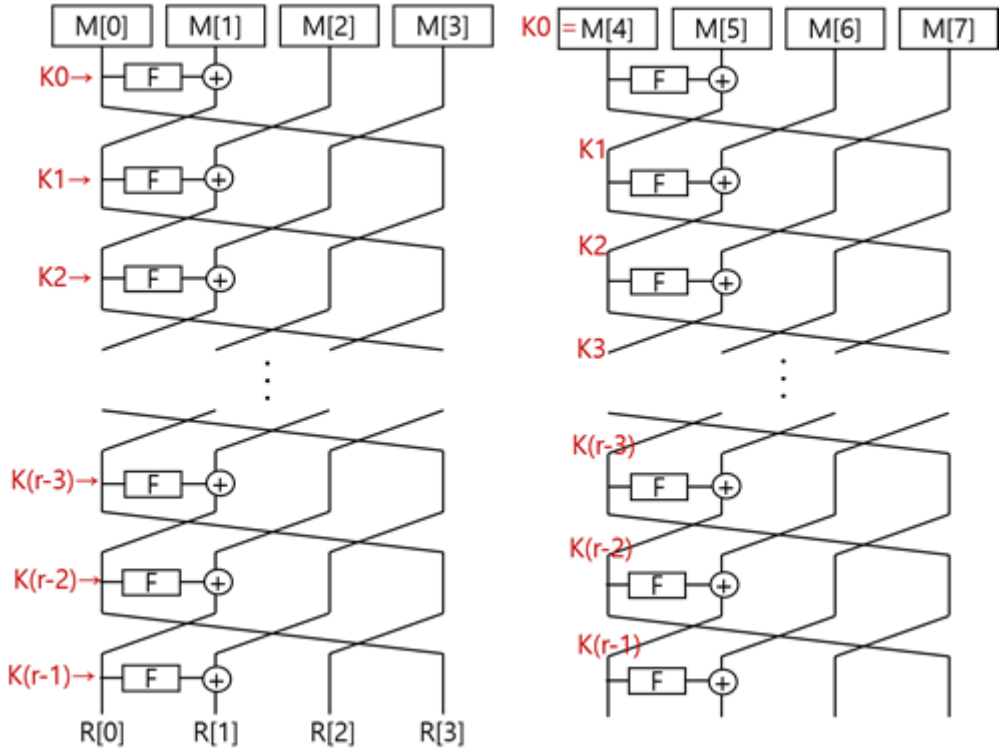
$Message' = 0xc5c5c5c500000000c5c5c5c56451cf96c5c4c7c6c5317c3e1db9529d60676665$

$Hash = 0x91149774d2b47a6ccbfab2597c512f7b$

개요 :

1. 압축함수의 구조

256비트 *Message*에 대해 r라운드 압축함수 구조는 다음과 같다.

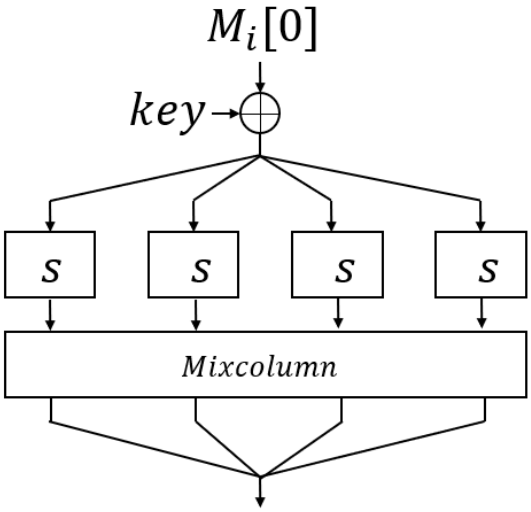


< 그림 1. 압축함수 r라운드 구조 >

입력 *Message* : 256비트 메시지 $= (M[0], M[1], \ldots, M[7])$ 크기 8의 32비트 단위벡터로 표현
출력 H : 128비트 값 = $(H[0], H[1], H[2], H[3])$ 크기 4의 32비트 단위벡터로 표현
위의 그림에서 R : 128비트 값 $= (R[0], R[1], R[2], R[3])$ 크기 4의 32비트 단위벡터로 표현
$H = R \oplus (M[0], M[1], M[2], M[3]) \oplus (M[4], M[5], M[6], M[7])$

2019 암호경진대회 : 4번 문제 답안

i라운드의 F 함수 구조는 다음과 같다.



< 그림 2. F 함수의 내부 구조 >

2. 공격방법 개요 - 차분 공격

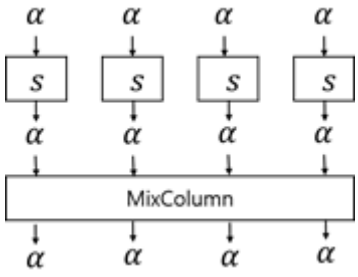
2-1. 한 종류의 차분을 이용한 공격

$Message = (m[0], m[1], \ldots, m[31])$ 크기 32의 8비트 단위벡터로 표현하자.

$i = 0, 1, \ldots, 7$에 대해 $M[i] = (m[4i], m[4i+1], m[4i+2], m[4i+3])$이다.

$j = 4i, 4i+1, 4i+2, 4i+3$에 대해 각 $m[j]$에 차분 α를 똑같이 주었을 때(α는 8비트), $Sbox$를 거쳐 차분이 변하지 않는다면, $Mixcolumn$ 과정에서도 차분이 유지된다는 것을 알 수 있다.

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} * \begin{bmatrix} \alpha \\ \alpha \\ \alpha \\ \alpha \end{bmatrix} = \begin{bmatrix} \alpha \\ \alpha \\ \alpha \\ \alpha \end{bmatrix}$$



<그림 3. F 함수에서 차분 경로 1 >

이 때, $AES\,Sbox$를 사용하므로 차분 α가 $Sbox$를 거쳐 α 차분으로 다시 나올 확률은 최대 2^{-6}이다. $Sbox$ 차분 분포표를 통해 가장 큰 확률을 가진 차분은 $\alpha = 0xc5$임을 알 수 있다. 따라서, 이 방법을 이용해 충돌쌍을 찾을 때 차분 $\alpha = 0xc5$로 고정하고 풀이하였다.

따라서 차분 $\alpha = 0xc5$일 때, $(\alpha, \alpha, \alpha, \alpha)$ 차분이 F 함수를 거쳐 다시 $(\alpha, \alpha, \alpha, \alpha)$ 차분을 나올 확률은 $(2^{-6})^4 = 2^{-24}$임을 알 수 있다.

2-1-1. 자동화 코드를 이용한 충돌쌍 찾기

우선 $(\alpha, \alpha, \alpha, \alpha)$ 차분을 간단히 α 차분이라고 하자(후자의 α는 32비트).

$Message = (M[0], M[1], ..., M[7])$에서 차분 α를 줄 수 있는 곳은 8곳이다.
따라서 2-1에서의 방법으로 공격을 할 때, 차분을 2^8가지 경우의 수로 둘 수 있다.

α 차분은 F 함수를 거쳐 다시 α 차분으로 나온다고 가정하자.

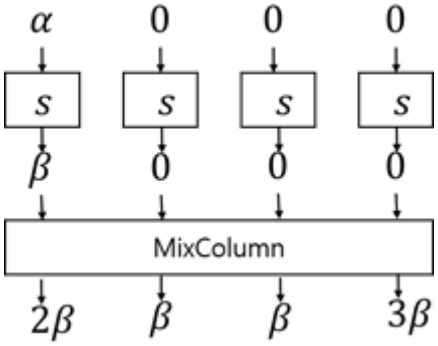
결과적으로 압축함수 값의 차분이 모두 0이 될 때를 얻어내었고, 이 때 α 차분이 F 함수에 들어가는 횟수를 세어 확률을 계산하였다.

6라운드부터 12라운드까지 각 라운드별로 이 코드를 돌려보았고 이론적으로 6, 7, 8, 10, 11, 12라운드에서 차분 경우의 수를 알 수 있었다. 10라운드까지는 2^{-24}의 확률로 충돌쌍을 찾을 수 있었으나, 11, 12라운드에서는 2^{-48}의 확률로 충돌쌍을 찾을 수 있음을 알 수 있었다.

2-2. 두 종류의 차분을 이용한 공격

2-2-1. 한 8비트 자리에만 차분을 준 경우

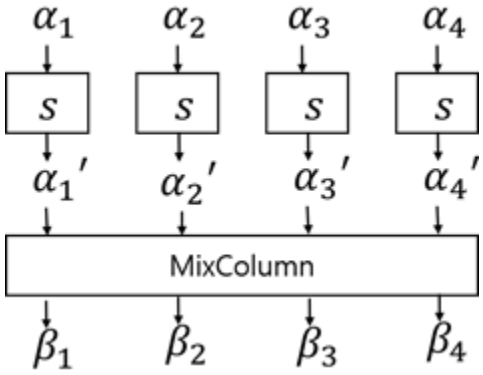
$M[i] = (m[4i], m[4i+1], m[4i+2], m[4i+3])\,(i = 0, 1, ..., 7)$에서 임의의 i에 대해 $M[i]$에 차분 $(\alpha, 0, 0, 0)$을 주었을 때, 이 차분이 $Sbox$를 거쳐 β 차분이 되었다고 하면 최종 F 함수를 거쳐 나오는 차분은 $(2\beta, \beta, \beta, 3\beta)$가 된다(각 자리는 8비트). 이 때, 다른 라운드의 F 함수로 $(\alpha, 0, 0, 0)$ 차분이 들어갔을 때, 다시 $(2\beta, \beta, \beta, 3\beta)$로 차분이 나올 확률은 차분 α가 Sbox에서 차분 β가 나올 확률과 같으므로 약 2^{-7}임을 이용하였다.



< 그림 3. F 함수에서 차분 경로 2 >

2-2-2. 네 8비트에 모두 차분을 준 경우

$M[i] = (m[4i], m[4i+1], m[4i+2], m[4i+3])(i = 0, 1, \ldots, 7)$에서 임의의 i에 대해 $M[i]$에 차분 $(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$을 주었을 때, 이 차분이 고정된 $(\beta_1, \beta_2, \beta_3, \beta_4)$로 나올 확률은, $Mixcolumn$의 역함수에 $(\beta_1, \beta_2, \beta_3, \beta_4)$를 넣었을 때 나오는 차분을 $(\alpha_1', \alpha_2', \alpha_3', \alpha_4')$라고 할 때, 각 $\alpha_k (k = 1, 2, 3, 4)$가 $Sbox$를 거쳐 $\alpha_k' (k = 1, 2, 3, 4)$로 나올 확률과 같으므로, 약 $(2^{-7})^4 = 2^{-28}$이다.



< 그림 5. F 함수에서 차분 경로 3 >

2-2-3. 자동화 코드를 이용한 충돌쌍 찾기

32비트 차분을 α, β라고 하자

$Message = (M[0], M[1], \ldots, M[7])$에서 차분 α, β를 줄 수 있는 곳은 8곳이다.

따라서 공격을 할 때, 차분을 3^8가지 경우의 수로 둘 수 있다.

α 차분은 F 함수를 지나면서 β로, β 차분은 F 함수를 지나면서 α로 나온다고 가정하자.

$\alpha \oplus \beta$가 나타나면 다음 $case$로 넘어간다고 가정하자.

결과적으로 압축함수 값의 차분이 모두 0이 될 때를 얻어내었고, 이 때 α, β 차분이 F 함수에 들어가는 횟수를 세어 확률을 계산할 수 있다.

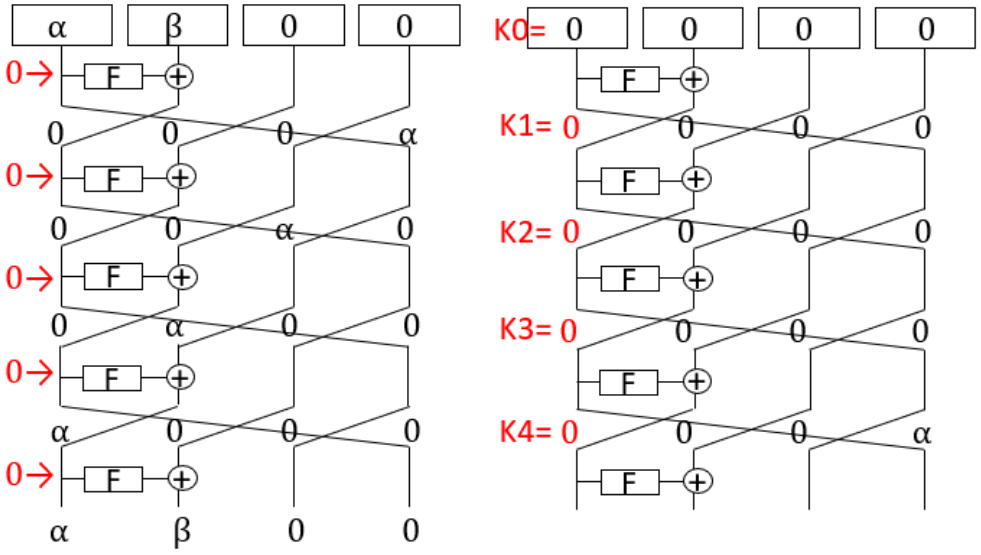
2-3. 세 종류 이상의 차분을 이용한 자동화 코드

2-1-1, 2-2-3 과 같은 방법으로 차분들을 추가시키고 가정을 추가시키며 코드를 구현할 수 있다.

2019 암호경진대회 : 4번 문제 답안

풀이)

1. 5라운드 충돌쌍



< 그림 6. 5라운드 차분 이동 >

$(M[0], M[1], M[2], M[3])$	α	β	0	0
$(M[4], M[5], M[6], M[7])$	0	0	0	0
$(R[0], R[1], R[2], R[3])$	α	β	0	0
$(H[0], H[1], H[2], H[3])$	0	0	0	0

< 표 1. 5라운드 차분 >

고정된 α차분에 대해 α차분이 F 함수를 거쳐 나오는 새로운 차분을 β라고 하면, $M[0]$에 차분 α를 주고, $M[1]$에 차분 β를 주었을 때, 첫 번째 라운드에서 차분은 상쇄된다. 이 때, α차분은 다시 5라운드에서 F 함수에 들어가는데, 이때 같은 β차분으로 나올 확률은 약 2^{-7}임을 이용하여, 평문 $M[0]$을 $0x00000000$부터 $0xff000000$까지 2^8개를 조사하여 메시지를 얻어내었다.

$Message = 0x4d000000000000000000000000000000000000000000000000000000000000000000000000$
$Hash = 0xe0cbd4952f7f0024e2f82bb7d60eedf9$
$Message' = 0x4c0000008fcaca4500000000000000000000000000000000000000000000000000000000$
$Hash' = 0xe0cbd4952f7f0024e2f82bb7d60eedf9$

따라서 $Hash = Hash'$

2019 암호경진대회 : 4번 문제 답안

2. 6라운드 충돌쌍

$(M[0], M[1], M[2], M[3])$	0	0	α	0
$(M[4], M[5], M[6], M[7])$	0	α	α	0
$(R[0], R[1], R[2], R[3])$	0	α	0	0
$(H[0], H[1], H[2], H[3])$	0	0	0	0

< 표 2. 6라운드 차분 >

확률은 2^{-24}

3. 7라운드 충돌쌍

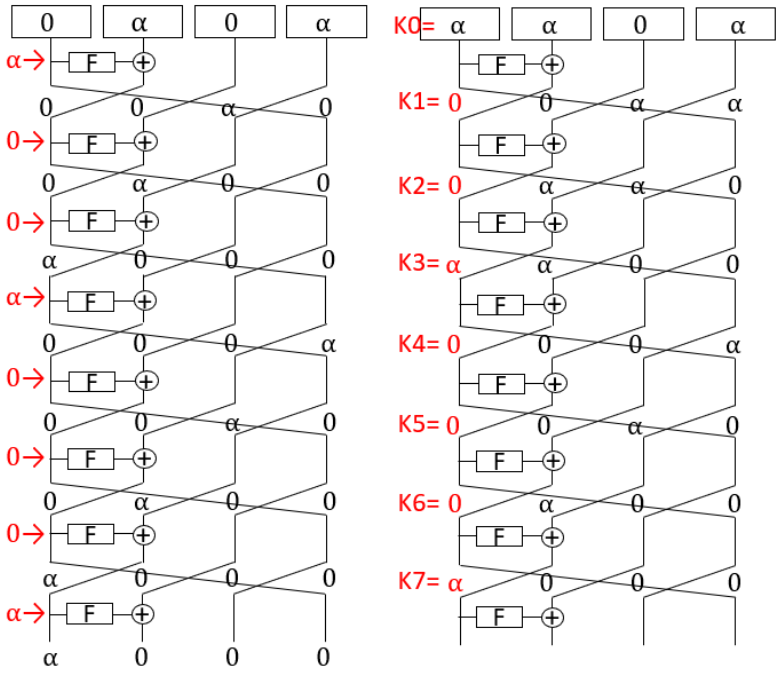
$(M[0], M[1], M[2], M[3])$	α	α	α	α
$(M[4], M[5], M[6], M[7])$	0	0	α	α
$(R[0], R[1], R[2], R[3])$	α	α	0	0
$(H[0], H[1], H[2], H[3])$	0	0	0	0

< 표 3. 7라운드 차분 >

확률은 2^{-24}

2019 암호경진대회 : 4번 문제 답안

4. 8라운드 충돌쌍



< 그림 7. 8라운드 차분 이동 >

$(M[0], M[1], M[2], M[3])$	0	α	0	α
$(M[4], M[5], M[6], M[7])$	α	α	0	α
$(R[0], R[1], R[2], R[3])$	α	0	0	0
$(H[0], H[1], H[2], H[3])$	0	0	0	0

< 표 4. 8라운드 차분 >

키 스케줄에서 α차분이 F 함수를 거쳐 다시 α차분으로 나와야하는 라운드는 1, 4라운드이다. 이는 $M[4]$를 1라운드에서 α차분이 나오도록 고정시키고, 4라운드 함숫값을 계산하여 α차분이 α차분으로 나오도록 $M[7]$을 고정시킬 수 있다. 마찬가지로, 평문 라운드에서는 1번째 라운드에서만 F 함수에 α차분이 들어가게 되는데 이도 $M[0]$를 위와 같은 방법으로 계산하여 메시지를 구할 수 있다.

$Message = 0x00000000000000000000000006451cf960001020300f4b9fbd87c975860676665$

$Hash = 0x50dbe29e1357025326682d1aec4aa329$

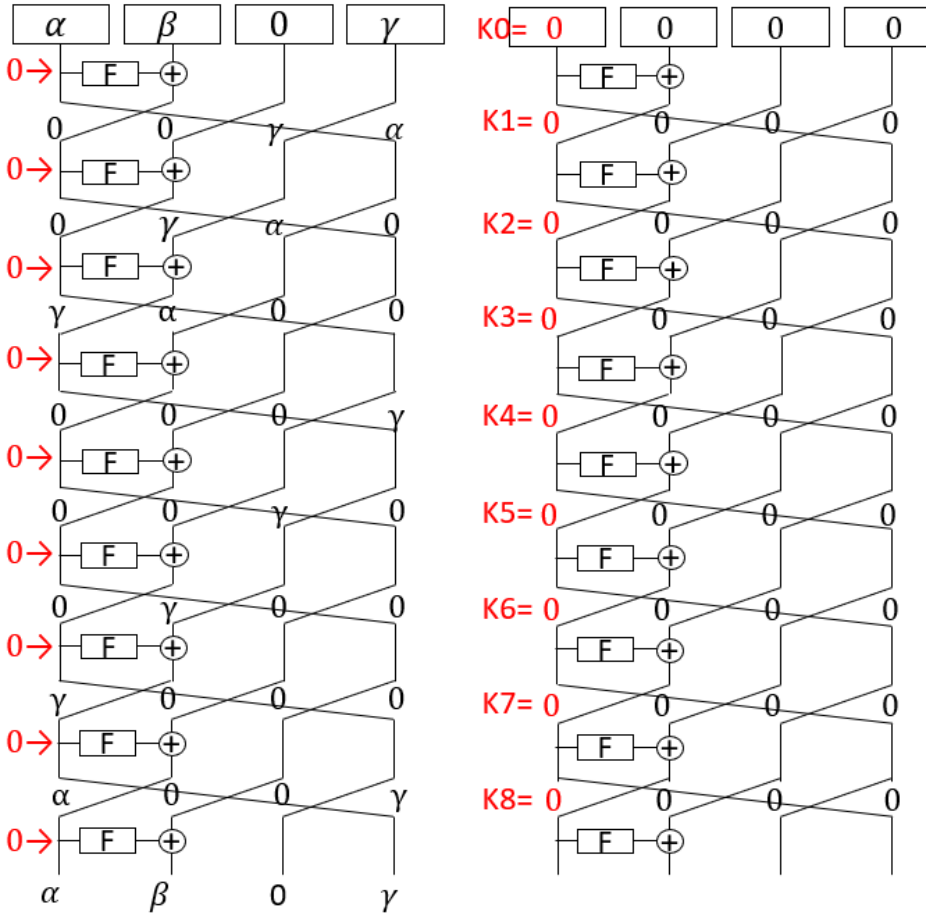
$Message' = 0x00010203c5c5c5c500000000c5c5c5c5c5c4c7c6c5c5c5c500000000a1f55327$

$Hash' = 0x50dbe29e1357025326682d1aec4aa329$

따라서 $Hash = Hash'$

2019 암호경진대회 : 4번 문제 답안

5. 9라운드 충돌쌍



< 그림 8. 9라운드 차분 이동 >

$(M[0], M[1], M[2], M[3])$	α	β	0	γ
$(M[4], M[5], M[6], M[7])$	0	0	0	0
$(R[0], R[1], R[2], R[3])$	α	β	0	γ
$(H[0], H[1], H[2], H[3])$	0	0	0	0

< 표 5. 9라운드 차분 >

2019 암호경진대회 : 4번 문제 답안

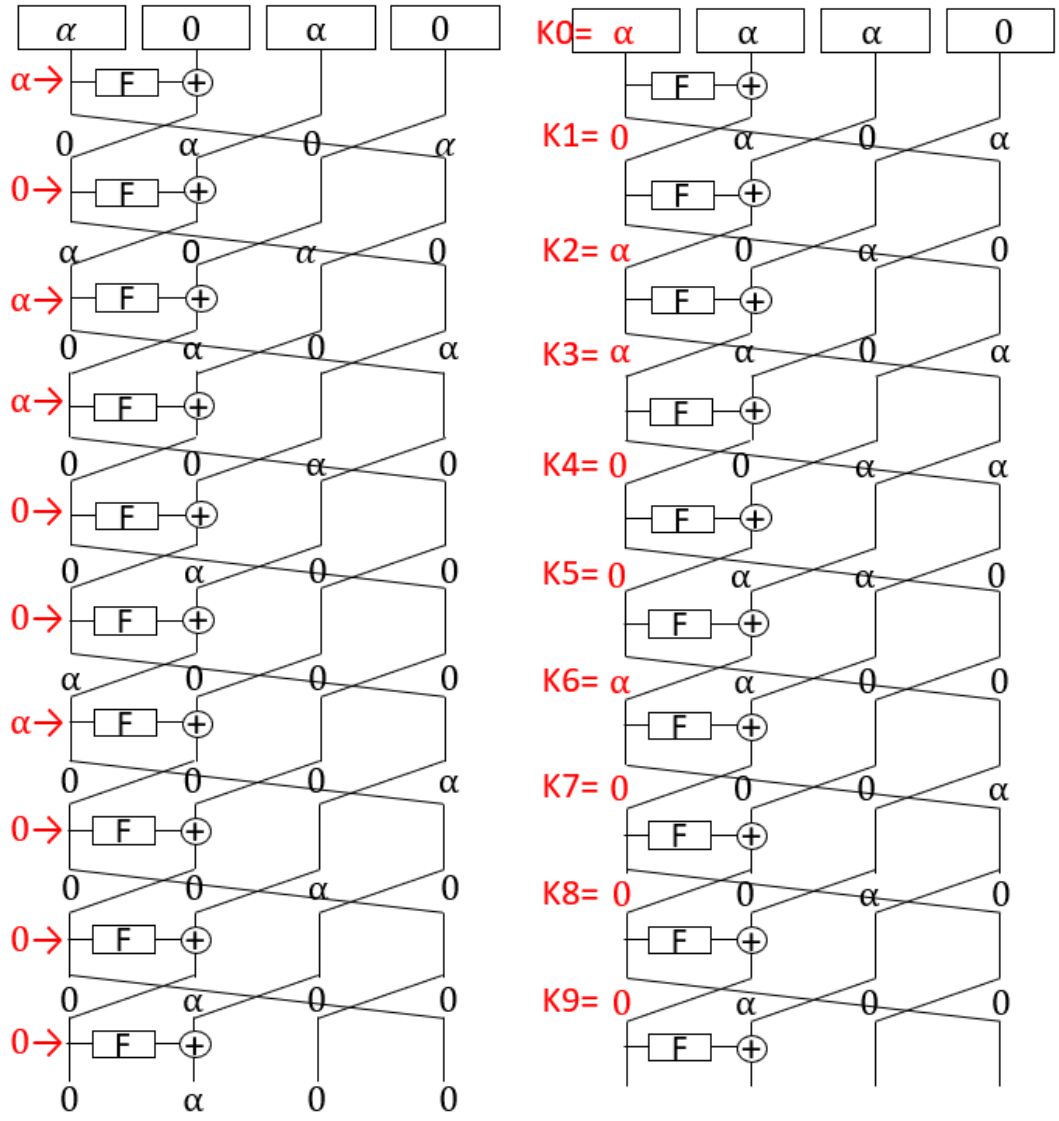
$M[4], M[5], M[6], M[7]$의 차분은 0이라 하자.

$M[3]$자리에 차분 γ를 고정시킨다. 이 때, 차분 γ는 한 바이트에만 준다. 이 차분은 4라운드까지 그대로 내려와 F 함수를 거쳐 α 차분으로 나온다고 하자. 이 α차분을 $M[0]$ 자리에 주게 되면, 4라운드 F 함수를 거쳐 나온 차분은 결과적으로 상쇄되어 0이 됨을 알 수 있다. 또한, $M[0]$ 자리에 부여한 α차분이 F함수를 거쳐 β차분이 된다고 할 때, 마찬가지 방법으로 $M[1]$자리에 β차분을 주게 되면 결과적으로 상쇄되어 차분이 0이 된다. 이는 평문을 고정시켜 얻어낼 수 있으므로 확률이 붙지 않는다.

이 때, 8라운드에서 γ 차분은 F 함수에 들어가게 되는데, 이때 F 함수를 거쳐 아까와 같은 α차분이 나올 확률은 약 2^{-7}이 된다. 여기서 발생한 α차분은 9라운드에서 다시 F 함수로 들어가게 되는데, 이때 β차분으로 나올 확률은 약 2^{-28}이므로, 9라운드의 결과값의 차분이 $(\alpha, \beta, 0, \gamma)$이 될 확률은 약 2^{-35}이 됨을 알 수 있다.

2019 암호경진대회 : 4번 문제 답안

6. 10라운드 충돌쌍



< 그림 9. 10라운드 차분 이동 >

$(M[0], M[1], M[2], M[3])$	α	0	α	0
$(M[4], M[5], M[6], M[7])$	α	α	α	0
$(R[0], R[1], R[2], R[3])$	0	α	0	0
$(H[0], H[1], H[2], H[3])$	0	0	0	0

< 표 6. 10라운드 차분 >

2019 암호경진대회 : 4번 문제 답안

키 스케줄에서 α차분이 F 함수를 거쳐 다시 α차분으로 나와야하는 라운드는 1, 3, 4, 6라운드이고 평문 라운드에서는 4번째 라운드이다. 이 때 키 스케줄의 1, 3, 4 라운드는 각각 $M[4], M[6], M[7]$을 고정시키고, 평문 4번째 라운드에서도 $M[3]$을 고정시켜 α차분이 다시 F 함수를 거쳐 α차분으로 나오도록 할 수 있다.

따라서 확률이 적용되는 부분은 키 스케줄의 6라운드 부분이다. 위의 2-1에서 구했듯이 α차분이 F 함수를 거쳐 다시 α차분으로 나올 확률은 2^{-24}이었음으로, $M[5]$를 $0x00000000$부터 $0xffffffff$까지 2^{32}가지 조사하여 메시지를 찾아내었다.

$Message = 0x000102030000000000000000000000000001020300000000000000000643096e2$
$Hash = 0x91149774d2b47a6ccbfab2597c512f7b$
$Message' = 0xxc5c5c5c500000000c5c5c5c56451cf96c5c4c7c6c5317c3e1db9529d60676665$
$Hash' = 0x91149774d2b47a6ccbfab2597c512f7b$

따라서 $Hash = Hash'$

7. 11라운드 충돌쌍

$(M[0], M[1], M[2], M[3])$	0	α	0	α
$(M[4], M[5], M[6], M[7])$	0	0	α	α
$(R[0], R[1], R[2], R[3])$	0	α	α	0
$(H[0], H[1], H[2], H[3])$	0	0	0	0

< 표 7. 11라운드 차분 >

확률은 2^{-48}

8. 12라운드 충돌쌍

$(M[0], M[1], M[2], M[3])$	α	0	0	0
$(M[4], M[5], M[6], M[7])$	α	α	0	0
$(R[0], R[1], R[2], R[3])$	0	α	0	0
$(H[0], H[1], H[2], H[3])$	0	0	0	0

< 표 8. 12라운드 차분 >

확률은 2^{-48}