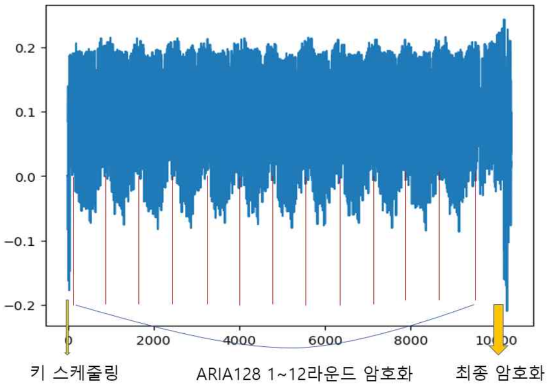
2021 암호분석경진대회			
4번 문제 풀이			
구분	일반부	팀명	HB

0. 개요

주어진 문제는 특정한 메시지가 포함된 1MB 사이즈의 그림 파일(jpg)를 ARIA128-CTR로 암호화된 answer.jpg.enc 파일에 대해 65,536번의 블록 연산에 대한 전력 소모량을 이용하여 복호화하는 문제이다. 암호화는 1번째부터 65,535번째 블록에 대해 ARIA128-CTR 암호화를 진행하고, 암호화 블록의 마지막 블록(65,536번째 블록)은 원본 블록을 사용한다.

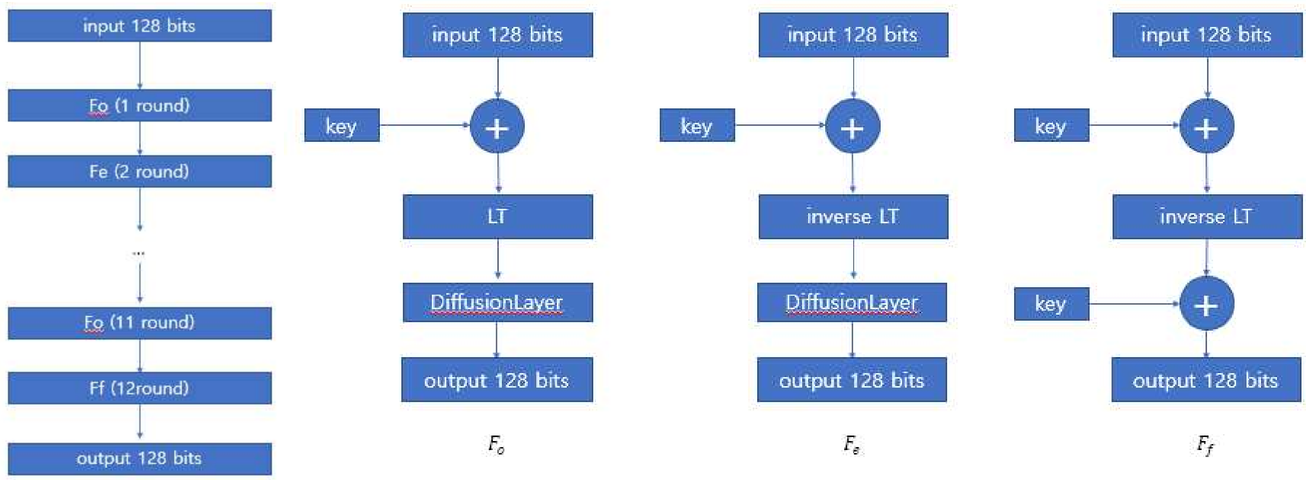
암호화에 사용된 주어진 전력 파형 이미지는 다음과 같다.



전력 파형 이미지

1. ARIA128-CTR / CPA

ARIA128은 다음과 같은 암호화 과정을 거친다.



ARIA는 블록 암호로 16bytes 블록 단위 암호화를 진행한다. 각 블록 별로, 입력 16bytes (128bits)에 대해 홀수 라운드에서는 F_o , 짝수 라운드에서는 F_e, 마지막 라운드에서는 F_f 계층을 거쳐 최종 암호화가 이루어진다. F_o 계층은 입력 128bits에 대해 라운드키와 XOR 연산 후 S-box를 활용한 치환 계층(LT)를 거쳐 확산 계층(Diffusion Layer)을 거친다. F_e 계층은 입력 128bits에 대해 라운드키와 XOR 연산 후 S-box의 inverse 결과와 치환 계층을 거치고, 확산 계층을 거친다. F_f 계층은 라운드키와 XOR 후, S-box의 inverse 결과와 치환 계층을 거친 후, 마지막 라운드 키와 XOR 한 결과를 암호화한 결과로 갖는다.

ARIA128은 총 12라운드를 거쳐 암호화가 이루어지고, 라운드키는 총 13개가 필요하다. 키 스케줄링은 초기화 과정과 키 생성 과정으로 나뉘며 다음과 같다.

초기화 과정 : 초기화 과정에서는 암/복호화 한 라운드를 F 함수로 하는 256 bits 3라운드 Feistal 암호를 사용하며, 마스터키 MK로부터 128bits W_0, W_1, W_2, W_3 을 생성한다.

$$KL \| KR = MK \| 0...0$$
$$W_0 = KL,\ \ W_1 = F_o(W_0, CK_1) \oplus KR$$
$$W_2 = F_e(W_1, CK_2) \oplus W_0,\ \ W_3 = F_o(W_2, CK_3) \oplus W_1$$

ARIA128에서 CK 값은 다음과 같다.

$CK_1 =$ 0x517cc1b727220a94fe13abe8fa9a6ee0

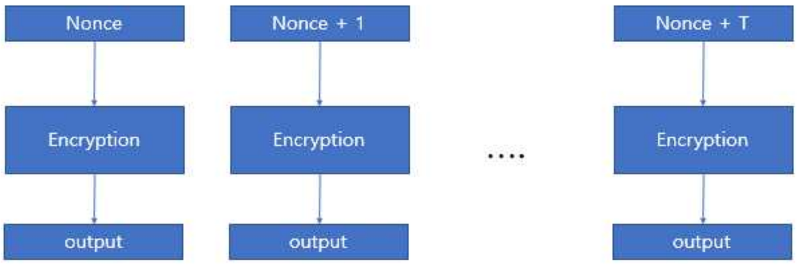
$CK_2 =$ 0x6db14acc9e21c820ff28b1d5ef5de2b0

$CK_3 =$ 0xdb92371d2126e9700324977504e8c90e

키 생성 과정 : ARIA128 암호화에 필요한 13개의 라운드 키는 다음과 같이 생성된다.

$$ek_1 = (W_0) \oplus (W_1 \gg 19),\ ek_2 = (W_1) \oplus (W_2 \gg 19)$$
$$ek_3 = (W_2) \oplus (W_3 \gg 19),\ ek_4 = (W_0 \gg 19) \oplus (W_3)$$
$$ek_5 = (W_0) \oplus (W_1 \gg 31),\ ek_6 = (W_1) \oplus (W_2 \gg 31)$$
$$ek_7 = (W_2) \oplus (W_3 \gg 31),\ ek_8 = (W_0 \gg 31) \oplus (W_3)$$
$$ek_9 = (W_0) \oplus (W_1 \ll 61),\ ek_{10} = (W_1) \oplus (W_2 \ll 61)$$
$$ek_{11} = (W_2) \oplus (W_3 \ll 61),\ ek_{12} = (W_0 \ll 61) \oplus (W_3)$$
$$ek_{13} = (W_0) \oplus (W_1 \ll 31)$$

CTR 모드는 다음과 같다.



참고 문헌을 통해 키 복구 및 초기 카운터 값 복구, 원본 이미지 복구를 실시하자. 부채널 분석은 CPA (Correlation Power Analysis)을 이용해 진행하였고, CPA에 사용되는 Peason 상관계수 식은 다음과 같다.

$$\hat{\rho}_{WH}(R) = \frac{N\sum W_i H_{i,R} - \sum W_i \sum H_{i,R}}{\sqrt{N\sum W_i^2 - (\sum W_i)^2}\sqrt{N\sum H_{i,R}^2 - (\sum H_{i,R})^2}}$$

N: 암호화에 사용된 블록 개수, W_i : i번째 전력 파형,

$H_{i,R}$: input M_i 와 reference R 사이의 Hamming weight

각 라운드의 치환 계층이 마무리되는 지점을 attack point로 잡고 전력 파형과의 상관 계수를 구하여 상관 계수의 절댓값이 가장 높은 값을 이용한다.

2. 키 복구

ARIA128-CTR에 대해 키 복구를 진행하자. 우선 주어진 전력 65536개의 파형 중 0 ~ 255번 째 파형을 이용한다. 현재 초기 카운터 값 (Nonce)를 모르는 상황이지만, 0 ~ 255번째 파형만을 이용해 부채널 분석 시, Nonce에는 최대 255가 더해지고, Nonce를 byte별로 생각했을 때 14번째 byte 값에 적용되는 15번째 byte + T의 carry는 최대 1이다.

N0	N4	N8	N12
N1	N5	N9	N13
N2	N6	N10	N14
N3	N7	N11	N15

Nonce

N0	N4	N8	N12
N1	N5	N9	N13
N2	N6	N10	N14 + carry
N3	N7	N11	N15 + T

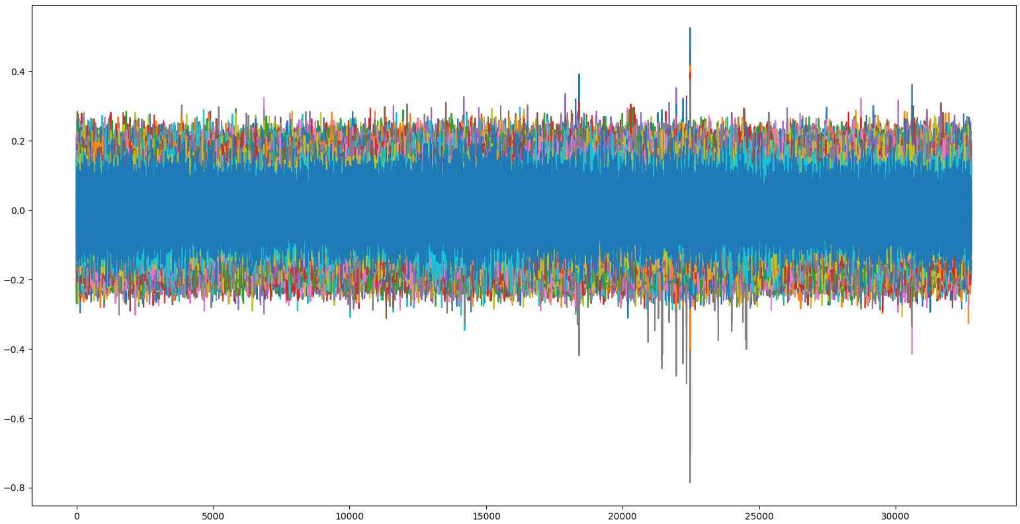
Nonce + T (T<256)

그리고 X, Y, Z를 다음과 같이 정의하자.

$X_i : input\ \ of\ \ i_{th}\ \ round$
$Y_i : LT(X_i)$
$Z_i : DL(Y_i)$
$(LT : \text{치환계층}, DL : \text{확산계층})$
$X_{i,j},\ Y_{i,j},\ Z_{i,j} : j_{th}\ byte\ \ of\ \ X_i,\ Y_i,\ Z_i$

CPA를 통해 0 ~ 255번째 파형을 이용하여 $Z_{1,15}$ 의 값을 추측할 수 있는 15bit $(b_{15}, K_{1,15,lo}, N_{15,lo})$ 를 구하면 다음과 같다. $(b_{15} = K_{1,15,hi} \oplus N_{15,hi})$, $(K_{1,15,hi}, N_{1,15,hi} = MSB\ \ of\ \ K_{1,15},\ N_{1,15})$

$Z_{1,15} = LT(K_{1,15} \oplus ((N_{15,lo} + T) \bmod 256))\ \ (T < 256)$

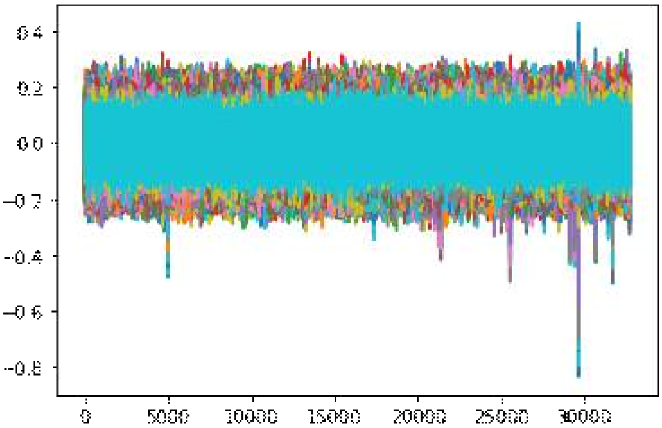


상관계수가 가장 높은 값은 22471 = 0b101011111000111 이므로

$b_{15} = 1, K_{1,15,lo} = 0b0101111, N_{15,lo} = 0b1000111$ 라 추측할 수 있다. 이를 통해 256개 블록에 대한 $Z_{1,15}$의 값을 구할 수 있고, 확산 계층을 통해 2 round에서 $Z_{1,15}$의 영향을 받는 값은 다음과 같다.

$Z_{2,1} = LT^{-1}(C_{2,1} \oplus Z_{1,15})$, $Z_{2,2} = LT^{-1}(C_{2,2} \oplus Z_{1,15})$
$Z_{2,8} = LT^{-1}(C_{2,8} \oplus Z_{1,15})$, $Z_{2,10} = LT^{-1}(C_{2,10} \oplus Z_{1,15})$
$Z_{2,15} = LT^{-1}(C_{2,15} \oplus Z_{1,15})$
$Z_{2,4} = LT^{-1}(C_{2,4} \oplus Z_{1,14} \oplus Z_{1,15})$, $Z_{2,5} = LT^{-1}(C_{2,5} \oplus Z_{1,14} \oplus Z_{1,15})$

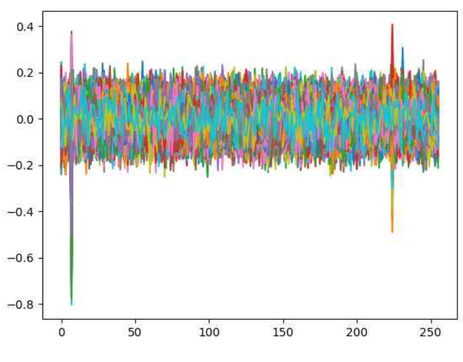
이와 같이 $C_{2,i}$ 라는 변수를 이용해 $Z_{2,i}$ 값을 나타낼 수 있고, $Z_{1,14}$ 는 초기 carry 값에 의해 결정되므로 따로 구분하자. 위와 같은 방법으로 carry에 의해 영향을 받는 $Z_{1,14}$ 를 구하기 위해 15bit $(b_{14}, K_{1,14,lo}, N_{14,lo})$를 구하자. 해당 15bit를 구하기 위해 전력 파형 65536개 중 0x0000, 0x0100, 0x0200, ..., 0xFF00 번째 파형을 이용하면 다음과 같은 15bit 값을 얻을 수 있다.

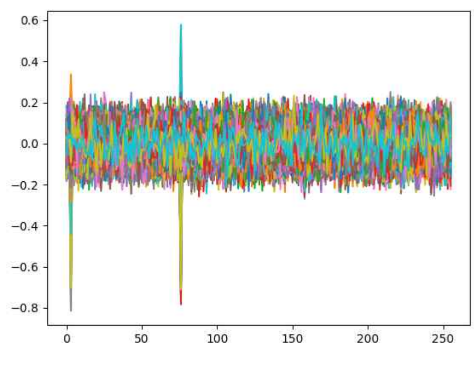


해당 결과는 29646 = 0b111001111001110 이므로 $b_{14} = 1, K_{1,14,lo} = 0b1100111, N_{14,lo} = 0b1001110$ 이다.
이를 이용해 다음과 같은 case를 나눌 수 있다. $(K_{1,14}, N_{14}, K_{1,15}, N_{15}$ 순$)$

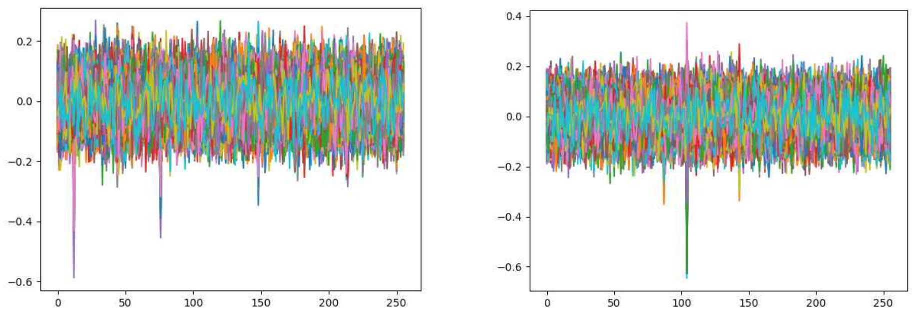
case1 = (0b01100111, 0b11001110, 0b00101111, 0b11000111)
case2 = (0b01100111, 0b11001110, 0b10101111, 0b01000111)
case3 = (0b11100111, 0b01001110, 0b00101111, 0b11000111)
case4 = (0b11100111, 0b01001110, 0b10101111, 0b01000111)

0 ~ 255번째 파형과 CPA를 이용해 $C_{2,1}, C_{2,2}, C_{2,8}, C_{2,10}, C_{2,15}, C_{2,4}, C_{2,5}$ 값을 case 별로 구하자. $K_{1,14}, N_{14}$ 의 MSB가 바뀌어도 $K_{1,14} \oplus (N_{14} + carry)$는 동일한 값을 갖기 때문에 case1과 case3에서는 동일한 $C_{2,i}$ 를 갖고, case2와 case4에서는 동일한 $C_{2,i}$ 를 갖는다.
case1, case3 일 때 상관계수가 가장 높은 $C_{2,i}$는 다음과 같다. (1byte hex로 표현)
$C_{2,1} = 07$, $C_{2,2} = 03, 4C$, $C_{2,8} = 63$, $C_{2,10} = 03, 4C$, $C_{2,15} = 0F$, $C_{2,4} = 0C$, $C_{2,5} = 68$





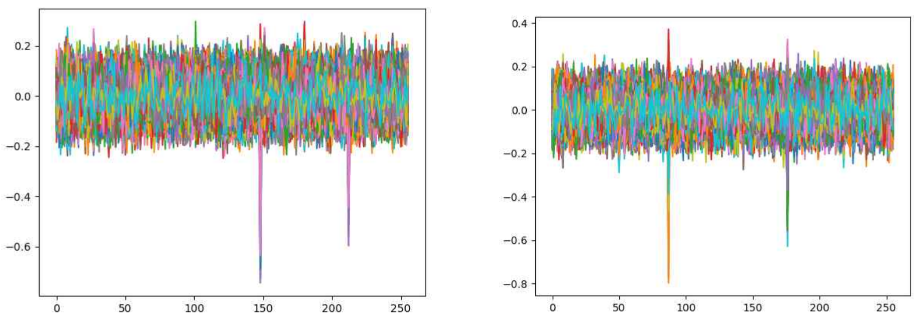
(예) $C_{2,1}$ = 0x07 $C_{2,2}$ = 0x03, 0x4C



(예) $C_{2,4}$ = 0x0C $C_{2,5}$ = 0x68

case2, case4 일 때 상관계수가 가장 높은 $C_{2,i}$는 다음과 같다. (1byte hex로 표현)

$C_{2,1}=07$, $C_{2,2}=03,4C$, $C_{2,8}=63$, $C_{2,10}=03,4C$, $C_{2,15}=0F$, $C_{2,4}=94$, $C_{2,5}=57$



(예) $C_{2,4}$ = 0x94 $C_{2,5}$ = 0x57

$C_{2,2}, C_{2,10}$ 의 경우 모든 case에서 03과 4C일 가능성이 있으므로 각 case 별로 총 4개의 경우가 생긴다.

$$C_{2,2}\,,\,C_{2,10} = (03,03),(03,4C),(4C,03),(4C,4C)$$

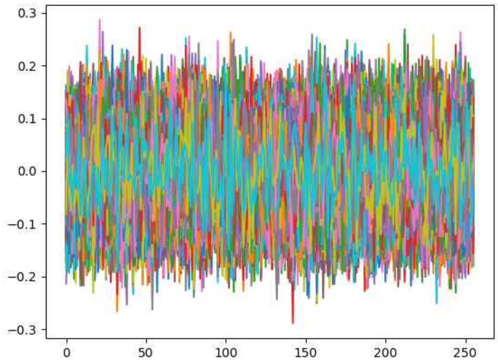
총 16가지 case에 대해 3 round의 $Z_{3,i}$ 값을 attack point로 잡자. ARIA의 확산함수에 의해 위에서 구한 $C_{2,1}, C_{2,2}, C_{2,8}, C_{2,10}, C_{2,15}, C_{2,4}, C_{2,5}$ 을 이용하면 $Z_{3,i}, C_{3,i}$ 에 해당하는 값을 구할 수 있다.

$$Z_{3,0}=LT(C_{3,0}\oplus Z_{2,4}\oplus Z_{2,8}),\ Z_{3,1}=LT(C_{3,1}\oplus Z_{2,2}\oplus Z_{2,5}\oplus Z_{2,8}\oplus Z_{2,15})$$
$$Z_{3,2}=LT(C_{3,2}\oplus Z_{2,1}\oplus Z_{2,4}\oplus Z_{2,10}\oplus Z_{2,15}),\ Z_{3,3}=LT(C_{3,3}\oplus Z_{2,5}\oplus Z_{2,10})$$
$$Z_{3,4}=LT(C_{3,4}\oplus Z_{2,2}\oplus Z_{2,5}\oplus Z_{2,8}\oplus Z_{2,15}),\ Z_{3,5}=LT(C_{3,5}\oplus Z_{2,1}\oplus Z_{2,4}\oplus Z_{2,10}\oplus Z_{2,15})$$
$$Z_{3,6}=LT(C_{3,6}\oplus Z_{2,2}\oplus Z_{2,10}),\ Z_{3,7}=LT(C_{3,7}\oplus Z_{2,1}\oplus Z_{2,8})$$
$$Z_{3,8}=LT(C_{3,8}\oplus Z_{2,1}\oplus Z_{2,4}\oplus Z_{2,10}\oplus Z_{2,15}),\ Z_{3,9}=LT(C_{3,9}\oplus Z_{2,1}\oplus Z_{2,5})$$
$$Z_{3,10}=LT(C_{3,10}\oplus Z_{2,2}\oplus Z_{2,5}\oplus Z_{2,8}\oplus Z_{2,15}),\ Z_{3,11}=LT(C_{3,11}\oplus Z_{2,2}\oplus Z_{2,4})$$
$$Z_{3,12}=LT(C_{3,12}\oplus Z_{2,1}\oplus Z_{2,2}),\ Z_{3,13}=LT(C_{3,13}\oplus Z_{2,8}\oplus Z_{2,10})$$
$$Z_{3,14}=LT(C_{3,14}\oplus Z_{2,4}\oplus Z_{2,5}),\ Z_{3,15}=LT(C_{3,15}\oplus Z_{2,1}\oplus Z_{2,2}\oplus Z_{2,4}\oplus Z_{2,5}\oplus Z_{2,8}\oplus Z_{2,10}\oplus Z_{2,15})$$

또한 위와 마찬가지로 case1, case3에서 동일한 $C_{2,i}$, case2, case4에서 동일한 $C_{2,i}$를 가지므로 같은 원리로 case1, case3에서 동일한 $C_{3,i}$, case2, case4에서 동일한 $C_{3,i}$를 가짐을 알 수 있다. 0 ~ 255번째 파형과 CPA를 이용해 $C_{3,i}$를 구하자.

① case1, case3

case1과 case3 일 때, $C_{2,2}, C_{2,10}$ 4가지 경우에 대해 $C_{3,0}$ 는 다음과 같다.

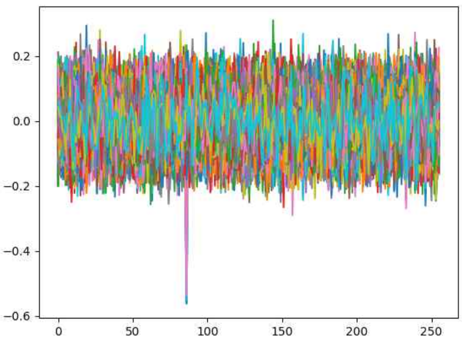


그러므로 case1, case3 일 때는 $C_{3,i}$ 를 구할 수 없다.

② case2, case4

case2와 case4 일 때, $C_{2,2}, C_{2,10}$ = 76, 3 일 때 올바른 $C_{3,i}$ 를 구할 수 있다. 이 때 $C_{3,i}$ 는 다음과 같다. (1byte hex로 표현)

$$C_{3,0},\ C_{3,1},\ C_{3,2},\ C_{3,3} = FC,\ BB,\ B7,\ 10$$
$$C_{3,4},\ C_{3,5},\ C_{3,6},\ C_{3,7} = FB,\ 75,\ 45,\ 16$$
$$C_{3,8},\ C_{3,9},\ C_{3,10},\ C_{3,11} = B0,\ DA,\ 35,\ C2$$
$$C_{3,12},\ C_{3,13},\ C_{3,14},\ C_{3,15} = 4F,\ 17,\ 0A,\ 56$$

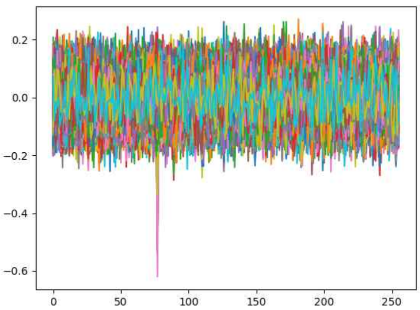


(예) $C_{3,15}$ = 0x56

이제 $C_{3,0}, \cdots, C_{3,15}$ 를 알고 있으므로 $Z_{3,0}, \cdots, Z_{3,15}$ 를 구할 수 있고, 4 round key를 마찬가지로 0 ~ 255번째 파형과 CPA를 이용해 구할 수 있다. 4 round key는 다음과 같다.

K_4 = [77, 163, 72, 107, 244, 46, 27, 228, 214, 0, 254, 225, 238, 222, 221, 22] (dec)

= [4D, A3, 48, 6B, F4, 2E, 1B, E4, D6, 00, FE, E1, EE, DE, DD, 16] (hex)



(예) $K_{4,0}$ = 0x4D

이제 키스케줄링을 통해 마스터키 (MK)를 구하자. ARIA128에서 $W_0 = MK$ 이고,

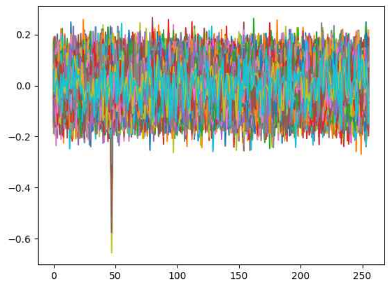
$K_4 = (W_0 \ggg 19) \oplus W_3$, $K_5 = W_0 \oplus (W_1 \ggg 31)$, $K_6 = W_1 \oplus (W_2 \ggg 31)$, $K_7 = W_2 \oplus (W_3 \ggg 31)$ 이므로 $W_0 \oplus (W_0 \ggg 112) = (K_7 \ggg 62) \oplus (K_6 \ggg 31) \oplus K_5 \oplus (K_4 \ggg 93)$ 이 됨을 알 수 있다.

그러므로 5,6,7 round key K_5, K_6, K_7를 CPA로 구하면 다음과 같다.

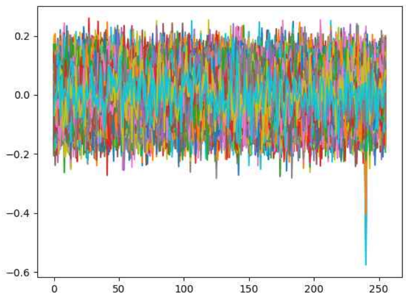
K_5 = [47, 222, 7, 107, 7, 88, 12, 143, 254, 133, 176, 137, 5, 45, 73, 93] (dec)
 = [2F, DE, 07, 6B, 07, 58, 0C, 8F, FE, 85, B0, 89, 05, 2D, 49, 5D] (hex)

K_6 = [240, 36, 143, 167, 94, 143, 223, 224, 133, 104, 73, 151, 182, 245, 193, 161] (dec)
 = [F0, 24, 8F, A7, 5E, 8F, DF, E0, 85, 68, 49, 97, B6, F5, C1, A1] (hex)

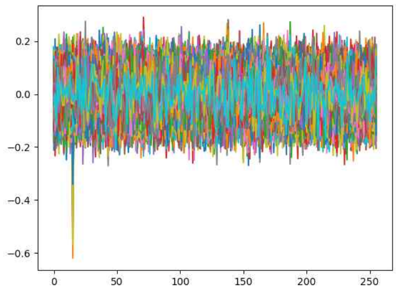
K_7 = [15, 25, 120, 122, 155, 250, 230, 78, 190, 81, 213, 132, 81, 2, 248, 179] (dec)
 = [0F, 19, 78, 7A, 9B, FA, E6, 4E, BE, 51, D5, 84, 51, 02, F8, B3] (hex)



(예) $K_{5,0}$ = 0x2F

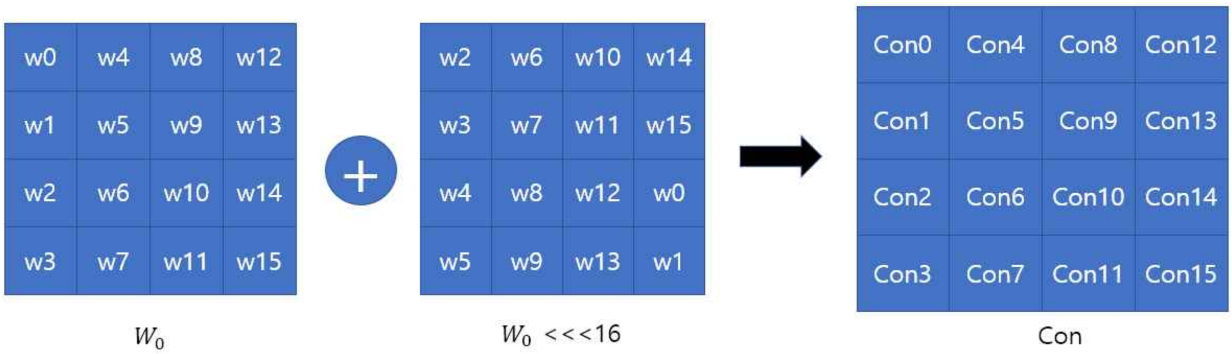


$K_{6,0}$ = 0xF0



$K_{7,0}$ = 0x0F

$Con = (K_7 \ggg 62) \oplus (K_6 \ggg 31) \oplus K_5 \oplus (K_4 \ggg 93)$라 하자. $W_0 \ggg 112 = W_0 \lll 16$ 이므로 다음을 알 수 있다. ($w_0,\ldots,w_{15}$: W_0의 byte 별 값, $con_0,\ldots,con_{15}$: Con의 byte 별 값)

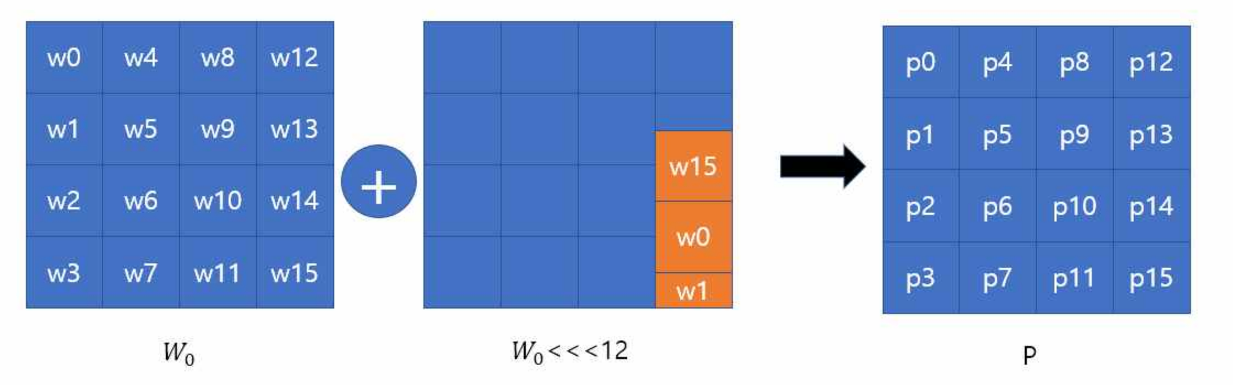


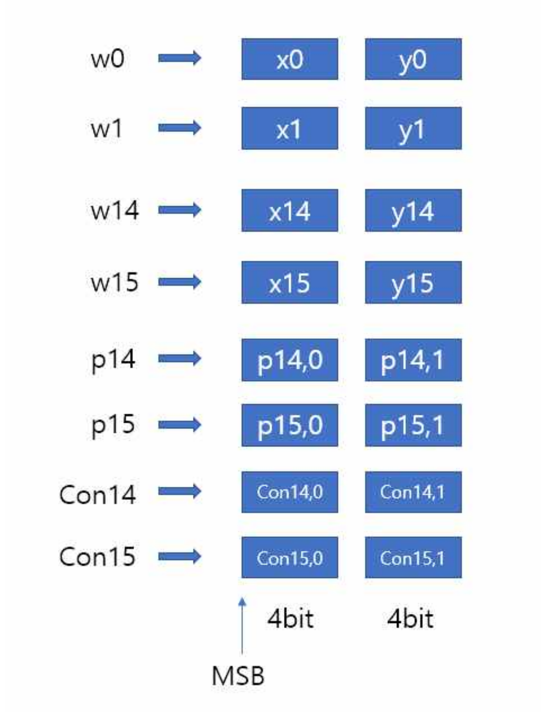
(식 1)

또한 case2, case4에서 1 round key K_1의 일부를 알고 있고, P를 아래와 같이 잡자.

$$K_1 = W_0 \oplus (W_1 \ggg 19) = W_0 \oplus (K_5 \lll 12) \oplus (W_0 \lll 12)$$
$$W_0 \oplus (W_0 \lll 12) = K_1 \oplus (K_5 \lll 12) = P$$

case2와 case4에서 K_1의 일부인 $K_{1,14}$, $K_{1,15}$ 를 알고 있으므로 위 관계와 다음의 세팅을 통해 아래와 같은 식을 잡을 수 있다.





$$x_{14} \oplus y_{15} = p_{14,0},\ y_{14} \oplus x_0 = p_{14,1},\ x_{15} \oplus y_0 = p_{15,0},\ y_{15} \oplus x_1 = p_{15,1}$$
$$x_{14} \oplus x_0 = con_{14,0},\ y_{14} \oplus y_0 = con_{14,1},\ x_{15} \oplus x_1 = con_{15,0},\ y_{15} \oplus y_1 = con_{15,1}$$

(식 2)

(식 1)을 통해 W_0를 구하는 것은 w0와 w1을 구하면 됨을 알 수 있다. 또한 (식 2)를 통해 다음을 얻을 수 있다.

$$(x_{14} \oplus y_{15}) \oplus (y_{15} \oplus x_1) = x_{14} \oplus x_1 = p_{14,0} \oplus p_{15,1}$$
$$\Rightarrow (x_0 \oplus x_{14}) \oplus (x_{14} \oplus x_1) = x_0 \oplus x_1 = con_{14,0} \oplus p_{14,0} \oplus p_{15,1}$$

(식 3)

case2와 case4에 따라 $p_{14,0}, p_{15,1}$을 알 수 있으므로 4bits x_0 에 따라 연쇄적으로 y_0, x_1, y_1 을 구할 수 있고, 이를 통해 w_0, w_1 을 구할 수 있으므로 $W_0 = MK$ 를 구할 수 있다.

case2와 case4 각각에 x_0 = 0 ~ 15를 대입하여 나온 결과를 1 round key와 비교하였을 때 옳은 결과는 case4일 때, x_0=6 일 때이다.

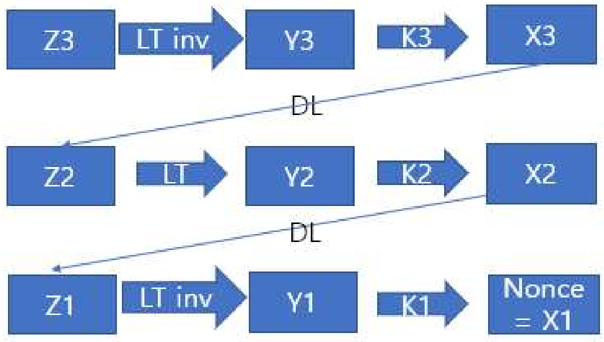
따라서 $W_0 = MK$ = [99, 114, 121, 112, 116, 111, 103, 114, 97, 112, 104, 121, 110, 105, 99, 101] (dec)

= [63, 72, 79, 70, 74, 6F, 67, 72, 61, 70, 68, 79, 6E, 69, 63, 65] (hex)

= 0x63727970746F6772617068796E696365 이다. (아스키코드로 변환 시 cryptographynice)

3. 초기 카운터 값 복구

마스터 키를 구했으므로 첫 번째 블록 (T=0 인 블록)에 대해 3라운드까지 암호화가 된 $Z_{3,i}$ 를 구할 수 있으므로 역추적하면 카운터 값 (Nonce)를 구할 수 있다. (LT : 치환 계층, DL : 확산 계층)



ARIA에서 확산 계층에 사용되는 행렬의 경우 역행렬과 동일한 행렬이므로 기존의 확산 계층을 이용하면 된다. 이를 통해 구한 초기 카운터 값은

Nonce = [67, 82, 89, 80, 84, 79, 73, 83, 70, 85, 78, 84, 72, 73, 78, 71] (dec)

= [43, 52, 59, 50, 54, 4F, 49, 53, 46, 55, 4E, 54, 48, 49, 4E, 47] (hex)

= 0x43525950544F495346554E5448494E47 이다. (아스키코드로 변환 시 CRYPTOISFUNTHING)

4. 메시지 복구

마스터 키와 초기 카운터 값을 구했으므로 기존 이미지를 복구할 수 있다. 복구된 이미지 answer.jpg는 다음과 같다.

(포함된 메시지 : 내년에는 더 어려운 문제로 만나요 ~~~ !!!)

5. 결과

부채널분석에 사용한 파형의 수는 0 ~ 255번째 파형과 0x0000, 0x0100, ..., 0xFF00 번째 파형을 사용하였으므로 총 512개의 파형을 사용하였다. (0번째 파형 중복)

또한 분석복잡도는 처음 15bit 2가지를 구할 때 $O(2^{15})$, $C_{2,i}, C_{3,i}, K_4, K_5, K_6, K_7$ 를 구할 때 $O(2^8)$ 의 복잡도가 사용되었다.

마스터 키와 초기 카운터 값은 아래와 같다.

MK = 0x63727970746F6772617068796E696365 (cryptographynice)

Nonce = 0x43525950544F495346554E5448494E47 (CRYPTOISFUNTHING)

참고자료

1. A First-Order DPA Attack Against AES in Counter Mode with Unknown Initial Counter, CHES 2007
2. Recovering the CTR_DRBG state in 256 traces, TCHES 2020
3. ARIA specification : https://seed.kisa.or.kr/kisa/Board/19/detailView.do