2021 암호분석경진대회

4번 문제 : 부채널분석

특정 메시지가 포함되어 있는 1MB 사이즈의 그림파일(JPG)을 ARIA128-CTR로 다음 그림과 같이 암호화하여 answer.jpg.enc 파일을 생성하였다. 하지만, 파일 암호화 과정에서 수행되는 65,536(=1MB/16B) 번의 ARIA 단위 블록 연산에 대한 전력 소모량이 공격자에게 누출되었고, 이 65,536개의 전력소비 파형은 각각 10,340개의 시점으로 구성되어 있었다.

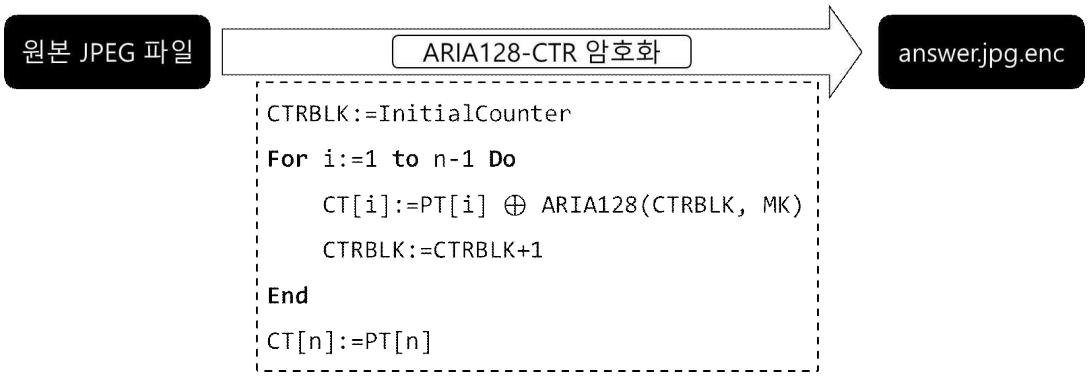

그림 1【 JPG 파일 암호화 방식 】

누출된 전력소비 파형으로부터 마스터키(MK)와 초기 카운터값(InitialCounter)을 복구하고, 암호화된 원본 JPG 파일을 복호화하여 내부의 메시지를 제출하시오.

▣ 참고 사항

1) 누출된 전력 소비 파형 traces-aria128ctr.bin 파일은 10,340 시점을 가진 65,536개의 파형으로 구성되어져 있으며 파일은 다음과 같이 구성되어져 있다.
   - unsigned int(4바이트), Little endian : 파형의 전체 개수 → 00 00 01 00 (65,536)
   - unsigned int(4바이트), Little endian : 각 파형의 시점 개수 → 64 28 00 00 (10,340)
   - 65,536개의 파형이 첫 번째 파형부터 순차적으로 저장되어 있으며, 파형의 각 시점은 float(4바이트) 형태로 저장되어 있음
   - 파일경로 : 전력파형 파일경로 (비밀번호: cryptocontest2021)

2) 참고문헌 :
   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

3) 평가 참고사항
   - 부채널분석에 사용한 파형의 수와 분석 복잡도
   - 마스터키 복구 여부
   - 초기 카운터값 복구 여부
   - 메시지 복구 여부