2019 암호경진대회

5번 문제 : 부채널 분석

부채널 분석(Side-Channel Analysis) 또는 부채널 공격(Side-Channel Attack)이란 과거 암호 해독 기법과는 달리 암호 연산 수행 시 장비에서 발생되는 전력 또는 전자파와 같은 정보를 이용해 비밀키를 찾는 방법이다. 일반적으로 시간공격 (TA, Timing Attack), 전자기누출공격 (EMA, ElectroMagnetic emission Attack) 그리고 전력분석공격 (PA, Power analysis Attack) 등으로 나눌 수 있으며, 수집한 전력 또는 전자파의 일반적인 특성 또는 통계적인 분석 기법을 활용한다. 특히, 전력분석 공격은 하드웨어에서 '0', '1'을 처리하는 소비되는 전력이 서로 다르다는 점을 이용하여, 장비에서 암호 알고리즘이 실행되는 동안의 소비 전력을 분석해 비밀키에 대한 정보를 얻어 내는 방법이다. 이는 단순 전력 분석(SPA, Simple Power Analysis), 차분 전력 분석(DPA, Differential Power Analysis)[1] 및 상관 전력 분석(CPA, Correlation Power Analysis)[2] 등으로 나뉜다.

▣ 참고 사항

1) http://opensca.sourceforge.net/ 에서 부채널 분석을 시행 할 수 있는 matlab 기반의 오픈 소스 및 부채널 분석 관련 내용을 확인 할 수 있다.
2) 각 문제를 풀기위한 정보(소비 전력 파형 등)는 아래의 url을 통해 다운로드 가능하다.
   - 소비 전력 파형, 평문, 암호문
   https://drive.google.com/open?id=1mhTSYE0-kn789wrdv_AXwi-cpoIjN4XY
   - 참고문헌
   https://drive.google.com/open?id=1GhTC3D2BfhFf1kTCkXuqOO7ZUDYaTecR
   ※ 문제는 압축 파일(.zip)로 존재하며, 소비 전력 정보, 평문, 암호문 정보가 포함되어 있다.

▣ File Information

HEADER 정보 (총 20 Bytes)

8 Bytes : CONTEST0 * 헤더의 처음을 의미
4 Bytes : 파형 수 **(리틀 엔디언)**
4 Bytes : 파형의 포인트 수 **(리틀 엔디언)**
4 Bytes : END! * 헤더의 끝을 의미

이후 바이트들은 각 포인트에 대한 정보로 한 포인트의 정보가 **FLOAT 형**으로 저장되어 있다.

제공되는 정보는 **8비트 기반 소프트웨어로 구현된 암호 알고리즘**이 Atmel XMEGA128 8-bit Microcontroller에서 동작 할 때 **소비되는 전력**을 수집한 결과이다. **1회 암호화 연산이 수행되는 부분을 대상**으로 수집하였다.

파일명	설명
Contest_SCA_problem.trace	**동일한 암호화키** 및 **서로 다른 평문**을 이용하여 암호 알고리즘이 **500번 시행된** 소비 전력 정보 (binary 파일)
Contest_SCA_problem_plain.txt	알고리즘 시행에 사용된 평문 정보 (hex값)
Contest_SCA_problem_cipher.txt	암호문 정보 (hex값)

제공되는 동일한 비밀키로 500개의 서로 다른 평문을 암호화 하는 과정에 수집된 소비 전력 및 사용된 평문, 암호문 정보를 이용하여 **암호 알고리즘 구조** 및 암호 알고리즘 동작 시 사용된 **비밀키**를 찾으시오.

[참고] 암호는 64비트 데이터 입출력, 64비트 비밀 키를 사용하는 비공개 블록 암호이다. 라운드 키 생성 함수는 따로 존재하지 않으며, 64비트 비밀 키를 32비트씩 끊어서 라운드 키로 반복 사용한다. (홀수 라운드 키 : 비밀 키 상위 32비트, 짝수 라운드 키 : 비밀 키 하위 32비트)

입출력 데이터 크기	비밀 키 크기	라운드 수
64비트	64비트	비공개

비밀 키 (64비트)	홀수 라운드 키 (32비트)	짝수 라운드 키 (32비트)
$K = (K_0 \parallel K_1)$	K_0	K_1