GNU Radio를 이용한 소프트웨어적 전력분석 방안

김태용*, 이훈재*

*동서대학교

Software Power Analysis Countermeasure using GNU Radio Antenna

Tae Yong Kim*, Hoon-Jae Lee*

*Dongseo University

E-mail : tykimw2k@dongseo.ac.kr

요 약

일반적인 전력분석 공격을 위해서는 고가의 측정 장비들을 이용하여야만 하고, 장시간의 연산수행을 통해 원하는 값을 탐색하여야만 하는 문제가 있다. 본 연구에서는 소프트웨어에 기반하여 무선통신 시스템을 용이하게 구축할 수 있는 GNU Radio를 이용하여 신호 추정에 요구되는 신호처리 과정을 효율적으로 수행할 수 있는 방안을 연구하고, 그 활용 범위를 확인하고자 한다.

ABSTRACT

General Power Analysis Attack has been investigated by high cost measurement tools and required long term computation process to estimate secrete key. In this paper, effective signal processing technique will be considered by using GNU Radio which can be used to be telecommunication system easily.

키워드

암호시스템, 전력분석공격, 마스터키, GNU Radio

Ⅰ. 서 론

P. Kocher[1] 등이 제안한 전력분석 방법은 보안장치가 암호 알고리즘을 실행하는 동안에 소모하는 전력신호를 관찰하여 암호장치에서 연산되는 비밀키를 추정하기 위한 방법이다. 비밀키를 추정하는 대표적인 방법[1-2]은 DPA(Differential Power Analysis), SPA(Simple Power Analysis)으로 분류되며 암호 알고리즘의 연산이 이미 알려져 있고, 알려진 값과 숨겨진 값을 입력받아 연산을 실행하는 시점에서 전력분석을 하여 숨겨진 비밀키를 추출할 수 있다.

Stefan[3] 등은 단거리 통신범위에서 주로 사용하는 코드리스 전화기 시스템 DECT (Digital Enhanced Cordless Telecommunications)에 대한 보안 취약점 분석과 함께 인증 알고리즘에 적용된 암호키 추출을 위한 효과적인 공격수단에 대한 방법을 제안하였다.

박영구 연구팀은 AES-128 블록 암호알고리즘이 탑재된 8비트 연산을 하는 스마트카드에 대하여 전력분석공격을 어렵게 하는 조건을 적용한 비밀 중간키를 이용한 소프트웨어적 방어대책을 제안하였다[4].

본 연구에서는 소프트웨어에 기반하여 무선통신 시스템을 용이하게 구축할 수 있는 GNU Radio[5]를 이용하여 전력분석 공격에 필요한 전력샘플링 과정을 포함하여 신호 추정에 요구되는 신호처리 과정을 자동화 시킬 수 있는 효율적인 방안을 연구하고, 그 활용 범위를 확인하고자 한다.

Ⅱ. GNU Radio 기반 전력분석 방안

GNU Radio[5]는 1998년에 시작된 GNU의 정규 프로젝트로서 소프트웨어에 기반한 무선 통신 시스템을 연구하고 제작하기 위한 툴킷이다. 이것은 USRP(Universal Software Radio Peripheral)

또는 HackRF와 같은 범용 무선장치를 이용하여 강력한 신호처리 소프트웨어를 통하여 다양한 분야의 응용이 가능하다.

전력분석공격은 알고 있는 값과 마스터키로부터 생성된 숨겨진 값을 입력받아 연산하는 시점에 이루어진다. 따라서 암호연산 결과 값과 연산 중에 측정된 전력신호의 상관도를 분석함으로써 숨겨진 값을 탐색할 수 있고, 탐색된 이 값을 통해 마스터키를 추정할 수 있다.

그러나 그림 1에서와 같이 통상적인 전력분석 공격을 위한 고가의 측정 장비들(고분해능을 가진 디지털 오실로스코프, 정밀 프로브 등)을 이용하여야만 하고, 다량의 전력샘플 채집과 장시간의 연산수행을 통해 원하는 값을 탐색하여야만 하는 문제가 있다.

그림 1. 전력분석 장치

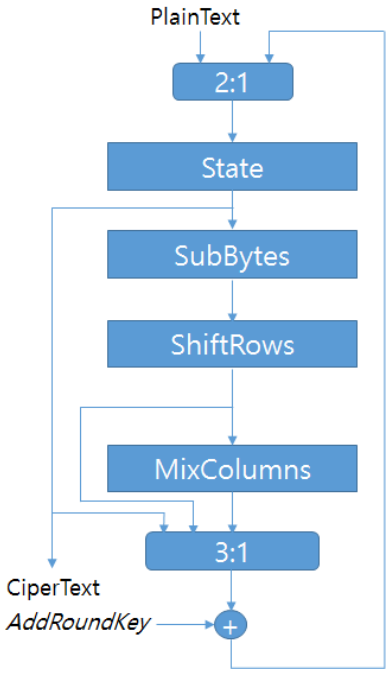

그림 2. AES 암호연산 과정

III. 전력분석 시스템의 구축

암호장치에서 그림 2와 같은 암호화 연산을 수행하는 과정에서 첫 번째 라운드의 SubBytes() 함수의 출력 값 생성 시점에 맞춰 공격한다고 가정한다. 이때 전력분석에 필요한 전력수집은 HackRF 또는 USRP와 같은 범용 무선장치를 이용하여 디지털 오실로스코프 대신에 활용 가능하다. 이후 GNU Radio를 이용하여 전력분석 공격에 따른 알고리즘은 다음과 같은 절차를 통하여 신호처리를 하여 추정된 전력신호와 측정된 전력신호간의 상관도 분석 등을 수행하여 비밀키를 추정할 수 있다.

- Step 1: 범용 무선장치를 이용하여 전력신호 수집을 위한 인터페이스 설정
- Step2: GNU Radio에서 범용 무선장치 인터페이스를 통해 전력신호(power traces)를 수집하고 큐에 저장
- Step 3: 큐에 저장된 전력신호를 구간 단위로 임의의 추정 키를 대입 연산하여 SBOX에 대입하여 출력 값을 도출
- Step 4: 도출된 값을 토대로 SPA 또는 신호 상관도를 계산하여 추정키를 계산하고 전체 키를 얻을 수 있을 때까지 Step 2로 되돌아가서 이 과정을 반복
- Step 5: 최종 키 수열을 획득

IV. 결 론

통상적으로 이용되는 전력분석 공격 시스템 구축에 요구되는 계측 시스템을 범용 무선장치와 GNU Radio 소프트웨어를 이용하여 전력분석 공격 시스템을 용이하게 구축 가능할 것으로 보인다.

참고문헌

[1] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," Advances in Cryptology, CRYPTO'99, LNCS 1666, pp. 388-397, 1999.

[2] J. Jaffe, "Introduction to differential power analysis," Presented at ECRYPT Summer school on Cryptographic Hardware, Side Channel and Fault Analysis. 2006.

[3] Stefan Lucks, Andreas Schuler, Erik Tews, Ralf-Philipp Weinmann, and Matthias Wenzel, "Attacks on the DECT Authentication Mechanisms," LNCS 5473, pp. 48 - 65, 2009.

[4] 박영구, 김형락, 이훈재, 한덕찬, 박의영, "비밀 중간키를 이용한 소프트웨어적 전력분석공격 방어대책," 한국정보통신학회논문지 Vol. 17, No. 12, pp.2883-2890, 2013.

[5] GNU Radio site. http://gnuradio.org/.