마스킹 연구 동향

권용빈* 안규황* 권혁동* 서화정*†

*한성대학교 정보시스템공학과

dove3333@naver.com tigerk9212@gmail.com korlethean@gmail.com hwajeong84@gmail.com

Research trends in masking

Yong-Been Kwon* Kyu-Hwang An* Hyeok-Dong Kwon*

Hwa-Jeong Seo*†

*Division of information system engineering, Hansung University.

요 약

부채널분석 기술의 발달과 IOT(Internet Of Things)환경이 도래하면서, 앞으로의 암호기기에 부채널분석에 대한 대응기법의 적용은 필수불가결하다. 그 중에서도 기기에서 발생하는 전력을 이용하는 전력분석 기술과 대응기법인 마스킹(Masking)기법은 현재 활발한 연구가 진행 중이다. 본 논문에서는 이러한 마스킹기법에 대한 기존의 연구들을 분석하여 미래 연구에 대한 방향을 제시한다.

I. 서론

부채널분석 기술이란 암호기기가 작동하는 동안에 물리적으로 발생하는 전력, 전자기파, 시간을 분석하여 키와 관련된 정보 또는 키를 찾아내는 기술이다. 이전의 부채널분석에 대한 인식은 부채널분석을 시도하는 공격자가 암호기기에 가까이 접근하기 어렵다는 이유와 분석에 대한 연구 등한시되었다. 하지만 최근 분석 기구의 발달과 IOT환경에 따른 암호기기에 대한 접근성의 향상에 부채널분석 기술은 다시 활발하게 연구되고 있는 분야이다. 그 중에서도 전력분석은 대응기법이 적용되지 않은 많은 암호기기들의 키를 복원해내는데 성공한 강력한 분석법이다. 따라서 많은 암호기기들에 기본적인 대응기법을 적용하는 것이 필수적이다. 대표적인 대응기법은 마스킹기법이다. 마스킹기법은 구현 시 암호알고리즘의 특성과 암호가 사용되는 환경을 고려하여 만들어져야 한다. 본 논문에서는 마스킹기법에 대한 개념과 연구 동향을 살펴본다.

II. 전력분석

전력분석은 크게 파형을 단순하게 분석하는 기법인 SPA(Simple Power Analysis)와 여러 파형을 수집한 뒤 통계적으로 분석하는 기법인 DPA(Differential Power Analysis)로 분류된다. 일반적으로 키를 획득할 수 있는 강력한 분석 방법은 DPA이고 순서는 다음과 같다. 먼저, 전력모델을 설정한다. 기기가 전력을 소모하는 방식을 알아야한다는 것을 의미하며 주로 1의 개수를 세는 해밍웨이트(Hamming Weight)모델이나 변경되는 비트의 수를 나타내는 해밍디스턴스(Hamming Distance)모델에서 상수를 조절하여 이용한다. 다음으로 올바른 암호로 암호기기를 동작할 때 발생하는 전력파형을 수집한다. 수집된 파형은 시작점을 맞추거나 공격지점외의 부분을 제거하는 등의 전처리과정을 통해 총 DPA시간을 줄일 수 있다. 파형을 수집하고

나서는 키와의 연산을 거친 비트들의 버스내의 흐름을 고려하여 공격지점을 결정한다. 공격지점을 결정한다는 것은 그 지점에서의 비트를 예측한다는 것을 의미한다. 단순히 모든 비트를 예측하는 것은 공격에 대한 이점이 없으므로 알고리즘 구조에 맞게 좋은 공격지점을 찾는 것이 중요하다. 예를 들어 입출력 4비트 SBOX의 경우 예측 시 2^4개의 경우의 수만을 고려하기에 좋은 공격지점이 된다. 다음으로 예측된 비트와 수집한 파형을 비교한다. 이 때, 두 집합 사이의 상관관계를 계산하거나, 예측된 비트에 기반하여 파형을 두 그룹으로 나눈 뒤 관계가 있는지 판단하는 방법등을 이용한다. 결과적으로 예측된 키가 옳다는 관계가 나오면 그 키를 전체 키의 부분으로 하고 다음 부분의 비트를 분석하여 전체 키를 찾을 수 있다.

III. 마스킹

통계를 이용한 전력분석이 가능한 이유는 키와 평문이 조합된 비트들의 흐름을 살펴 특정 지점에서의 비트가 예측가능기 때문이다. 따라서 대응기법으로서 연산이 일어나기 전에 난수를 더하여 비트를 예측할 수 없도록 만드는 기법이 마스킹기법이다. 기본적인 마스킹연산은 난수를 더하는 형태이다. 선형연산의 경우에는 더해준 난수를 모든 연산을 마친 뒤 뺌으로써 정상적인 결과를 얻을 수 있다. 하지만, 비선형 연산의 경우는 같은 방법으로 상응하는 결과를 얻을 수 없다. 그렇다고 하여 마스킹을 제거하고 비선형 연산을 한다면 예측된 부분이 노출되므로 피해야한다. 이러한 문제가 비선형연산에 있지만, 많은 암호알고리즘에서 비선형 연산을 수행하기 때문에 이러한 문제들을 고려하여야 한다.

3.1 고차마스킹 공격과 대응기법

마스킹기법이 적용된 알고리즘을 분석해내기 위한 공격들이 키를 찾아내는데 성공하였고 따라서 기존의 마스킹기법을 1차마스킹기법이라고 부르게 되었다. 1차마스킹된 알고리즘을 공격하는 방법으로 마스킹 테이블의 약점을 이용하거나 각 라운드 별로 사용하는 난수가 같다는 점을 이용하여 비트를 찾아내는 등의 방법들이 있고 이를 고차전력분석이라고 한다. 물론, 이러한 방법은 필요한 파형의 개수를 증가시키기 때문에 공격자로 하여금 더 많은 자원을 소모하게 한다. 반면, 고차전력분석을 막기 위해 마스킹 테이블을 다르게 설계하거나 각 라운드에서도 서로 다른 난수를 더하는 등 마스킹 알고리즘을 다르게 설정하는 방법을 고차마스킹기법이라고 한다. 이러한 기법 또한 암호기기가 더 많은 자원을 소모하도록 한다. 따라서 환경에 따라 적합한 수준의 마스킹기법을 적용하여야 할 것이나 공격자의 환경과 공격수준을 고려했을 때, 적어도 1차마스킹기법은 반드시 적용해야 할 것이다.

3.2 마스킹 변환

암호 알고리즘은 선형, 비선형 연산이 혼재한다. 따라서 선형 연산을 위해 마스킹된 값은 비선형 연산을 수행하기 위한 마스킹된 값으로 변환되어야 하며 이 때 마스킹 전의 값을 노출하지 않아야 한다. 이러한 변환을 위해 많은 연산을 요구한다. 특히 저전력 환경을 위한 암호알고리즘의 경우에는 보다 효율적인 변환이 요구된다.

3.3 축소마스킹

일반적으로 마스킹기법은 다양한 마스크값을 이용할수록 안전성이 증가하고 동시에 연산량 즉 자원소모량도 증가하게 된다. 따라서, 저전력 암호기기를 위한 마스킹기법으로 알고리즘 초반과 맨 마지막 부분에만 마스킹을 적용할 수 있고 이를 축소마스킹이라고 부른다.

IV. 연구동향

본 절에서는 마스킹과 관련한 최신 연구 동향을 살펴본다.

4.1 고차 분석에 안전하고 효율적인 마스킹

최근 연구에서는 하드웨어로 구현된 AES에 대해 고차마스킹으로의 확장이 가능하면서도 적은 난수 발생, 적은 저장 공간과 빠른 속도를 가지는 효율적인 마스킹을 제안하였다[1]. 1차 마스킹 구현에 대하여 가장 적은 공간을 요구

하며, 충분히 안전한 난수를 발생시키기 위한 효율적인 방법을 적용하였다.

4.2 효율적인 마스킹 변환

LEA는 저전력 환경을 위해 설계된 블록 암호 알고리즘이다. 특징으로 Addition, Rotation, XOR연산으로 이루어진 ARX구조를 가진다는 점이다. 이렇게 선형 연산과 비선형 연산이 섞여있는 구조는 마스킹변환이 필요하다. 마스킹 변환 시 반드시 고려해야할 점은 원래의 값이 노출되지 않아야 한다는 점과 저전력 환경을 감안하여 연산량을 줄이고 연산속도를 빠르게 해야한다는 점이다. 마스킹변환에는 산술 마스킹된 값을 불 마스킹된 값으로 변환하는 AtoB(Arithmetic-to-Boolean)과 그 반대인 BtoA(Boolean-to-Arithmetic)이 있다. 일반적으로 BtoA기법은 Goubin이 제안한 기법을 이용하며 연산량이 적어 효율적이다. 하지만 AtoB 연산의 경우 연산량이 많아 사전 계산된 테이블을 이용하는 C-T기법이나 Debraize기법을 LEA에 적용하는 연구가 있었다[3]. 최근 연구에서는 기존 LEA에 적용된 C-T기법에서 C-테이블을 만들지 않고 알고리즘 상에서 발생한 캐리를 바로 덧셈하는 방법으로 처리하여 필요한 메모리의 수를 절반으로 줄인 마스킹 최소 단위 8기준 2^8바이트를 저장할 메모리만을 필요하도록 하였고. 동시에 처리 속도를 향상시키기 위해 반복문 내 바이트 단위 연산을 반복문 밖에서 워드 단위로 연산하여 효율적인 연산이 가능케 하였다. 그 결과 이전까지 가장 빠르다고 알려진 C-T기법 보다도 17%정도의 속도 향상과 C-T기법과 Debraize기법이 요구하는 메모리의 절반인 256바이트의 메모리만을 요구하는 효율적인 LEA 마스킹 기법을 제안하였다[2].

4.3 축소마스킹에 대한 공격

SIMON 암호 알고리즘은 저전력 환경에 적합한 블록 암호 알고리즘이다. 따라서 효율적인 마스킹을 위해 축소마스킹을 적용할 수 있는데 이 경우 알고리즘 중반에 해당하는 비트들의 해밍웨이트를 알 수 있다. 이 해밍웨이트 값이 특정 값을 만족하는 평문을 찾아 차분 공격을 진행한다. 차분 특성을 만족하는 횟수가 많은 예측키의 비트 중 차분의 영향을 받는 비트만을 옳은 키의 비트의 일부로 하여 전체키를 복구하였다. 많은 라운드를 마스킹 할수록 더 많은 평문이 필요하지만 10라운드 이내로 마스킹이 적용된 SIMON 알고리즘은 취약함이 발표되었다[3].

V. 결론

마스킹기법은 각 암호 알고리즘의 특성에 맞게 다양하게 구현될 수 있다. 따라서 암호 알고리즘을 잘 분석한다면 적은 연산으로도 강력한 암호 강도를 보장할 수 있다. 최근 연구들은 저전력 환경에 적합하도록 효율적인 마스킹기법을 제안하면서 부채널분석에 대한 충분한 안전성을 가지는지 검증하고 있다. 전력분석에 대한 연구가 활발하게 일어나고 저전력 환경이 중요해지는 만큼 대응기법인 마스킹기법을 암호 알고리즘을 고려하여 효율적이고 안전하게 설계하는 것이 중요하다.

[참고문헌]

[1] H. Gross, S. Hangard and T. Korak, An efficient side-channel protected AES implementation with arbitrary protection order, *Cryptographers' Track at the RSA Conference*, pp. 95-112, February, 2017

[2] E. Park, S. Oh and J. Ha, Masking-Based Block Cipher LEA Resistant to Side Channel Attacks, *Journal of The Korea Institute of Information Security & Cryptology* 27(5), pp. 1023-1032, October, 2017.

[3] J. Kim, K. Hong, S. Kim, J. Cho and J. Kim, Side Channel Attacks on SIMON Family with Reduced Masked Rounds, *Journal of The Korea Institute of Information Security & Cryptology* 27(4), pp. 923-941, August, 2017.