진난수생성기에 대한 부채널 공격 및 난수성 분석 사례 조사[1)]

최낙준* 이지은** 김광조*,**

KAIST *정보보호대학원 **전산학부

Side-Channel Attack and Randomness Analysis of True Random Number Generators

Nakjun Choi* Jeeun Lee** Kwangjo Kim*,**

*Graduate School of Information Security, **School of Computing, KAIST

요 약

암호기술을 적용하는 보안 산업에서 필수적으로 사용되는 난수생성기의 결함은 보안에 직접적인 영향을 미칠 수 있으므로, 안전성을 갖춘 고성능 난수생성기를 개발하는 것이 매우 중요하다. 대부분의 진난수생성기는 물리적인 칩 형태로 존재하기 때문에 타이밍 공격 또는 오류 주입 공격 등과 같은 부채널 공격의 위험에 항상 노출될 수밖에 없으며, 실제로 난수생성기를 대상으로 유효한 부채널 공격을 성공시킨 연구들이 꾸준히 발표되고 있다. 본 논문에서는 난수생성기와 하드웨어 기반 부채널 공격들에 대해 간략히 설명하고 실제 난수생성기를 대상으로 한 부채널 공격 사례들을 소개하며, 이를 토대로 난수생성기의 부채널 공격 대응 연구의 중요성에 대해 논한다.

I. 서론

현대 사회에서 난수생성기(Random Number Generator, RNG)는 IoT, 인공지능, 데이터베이스, 정보보호 등 여러 분야에 걸쳐 매우 광범위하게 사용되고 있다. 특히 암호기술을 적용하는 보안 산업에서 필수적으로 사용되는 난수생성기의 결함은 보안에 직접적인 영향을 미칠 수 있으므로, 안전성을 갖춘 고성능 난수생성기를 개발하는 것이 매우 중요하다.

이에 따라, 물리적인 현상을 이용하여 완전한 난수를 생성하는 진난수생성기(True Random Number Generator, TRNG)의 개발이 활발하게 이루어지고 있다. 최근에는 반투명 거울을 통해 이동하는 광자, 핵붕괴 방사선원, 전자 회로의 양자 기계적 잡음 등과 같이 예측할 수 없는 양자역학적 현상을 이용하여 양자난수생성기(Quantum Random Number Generator, QRNG)의 개발이 이루어지고 있다.

하지만 대부분의 난수생성기들은 물리적인 칩 형태로 존재하기 때문에 타이밍 공격(timing attack) 또는 오류 주입 공격(fault injection attack) 등 부채널 공격의 위험에 항상 노출될 수밖에 없으며, 실제로 난수생성기를 대상으로 유효한 부채널 공격을 성공시킨 연구들이 꾸준히 발표되고 있다 [1-4]. 따라서 난수생성기의 보안성이 인정받기 위해서는 해당 난수생성기가 부채널 공격에도 안전함을 보이는 것이 매우 중요하다.

본 논문에서는 난수생성기와 하드웨어 기반 부채널 공격들에 대해 설명하고 실제 난수생성기를 대상으로 한 부채널 공격 사례들을 소개한다. 또한 이러한 공격으로 인해 난수생성기의 난수성에 어떤 변화가 있는지 비교분석하고, 이를 토대로 난수생성기의 부채널 공격 대응 연구의 중요성에 대해 논한다.

1) 이 논문은 SK Telecom Network R&D Center의 지원을 받아 수행된 연구임.

본 논문의 구성으로 Ⅱ장에서는 난수생성기와 부채널 공격에 속하는 전력 분석 공격(power analysis attack), 글리치 공격(glitch attack), 오류 주입 공격에 대해 간단하게 설명하고, Ⅲ장에서는 실제로 난수생성기를 대상으로 수행된 글리치 공격, 주파수 주입 공격(frequency injection attack), 전자기 공격(electromagnetic attack)과 같은 부채널 공격 사례들을 소개하고 그 결과를 보여준다. 마지막으로 Ⅳ장에서는 결론 및 이를 토대로 한 향후 연구 계획에 대해 논한다.

II. 배경지식

2.1 난수생성기

난수는 정의된 범위 내에서 무작위로 선정된 수를 말한다. 난수생성기를 통해 만들어진 난수는 (1) 다음으로 어떤 난수가 생성될지 예측이 불가능해야하며(unpredictable), (2) 이전에 생성된 난수와 이후에 생성된 난수간의 상관관계가 없어야하며(uncorrelated), (3) 생성된 난수가 어느 한 쪽으로 편향되지 않아야 한다(unbiased). 하지만 실제 컴퓨터 환경에서는 난수를 결정론적인 방법으로 생성하기 때문에 완벽하게 무작위인 난수를 얻기는 어렵다. 이렇게 얻어진 난수는 진정한 의미의 난수가 아니기 때문에 의사난수(Pseudo-Random Number)라 부르며 소프트웨어에서 난수를 생성하는 코드를 의사난수생성기(Psudeo-Random Number Generator, PRNG)라 한다.

난수를 생성하기 위해 사용하는 난수생성기 중 진난수생성기는 컴퓨터 프로그램이 아닌 물리적인 현상을 이용하여, 예측할 수 없는 무작위 현상을 샘플링 함으로써 난수를 생성한다. 최근에는 양자역학적 현상의 예측할 수 없는 특성을 이용한 양자난수생성기가 개발되었고 스위스 ID Quantique사의 Quantis RNG [6], SK Telecom사의 QRNG Chip [7,8]이 대표적이다.

난수생성기를 통해 만들어진 난수는 NIST STS [12], dieharder [13]와 같은 난수성 테스트 또는 비트스트림으로 표현한 결과를 분석하여 난수성을 검증한다.

2.2 전력 분석 공격

[9]에서 처음 소개 된 전력 분석 공격은 공격 대상에 직접적인 손상 또는 변형을 가하지 않기 때문에 수동(passive) 공격 및 비침입 공격으로 분류된다. 전력 분석 공격은 크게 단순 전력 분석(Simple Power Analysis, SPA)과 차분 전력 분석(Differential Power Analysis, DPA)으로 나뉜다.

단순 전력 분석은 암호 장치의 연산 과정에서 소비되는 전력 변화를 측정 후 분석하여 비밀키 등의 유용한 정보를 얻어내는 공격 방법이고, 차분 전력 분석은 측정된 전력 소모량의 통계적 특성을 비교하여 비밀키를 추정해내는 방법이다. 전력 분석 공격을 막기 위해서는 연산에 소모되는 소비전력에 무작위성을 부여하거나 중간 값을 감추는 마스킹 기법 등이 사용되어야 한다.

2.3 글리치 공격

글리치 공격은 암호처리 프로세서가 들어있는 하드웨어 장치에 가해지는 공격이며 스마트카드가 주요 공격 대상이다 [5]. 하드웨어 장치의 회로를 분석하여 외부에서 오는 전원 또는 클록 신호에 글리치 신호를 추가하는 방법을 통해 장치에 예측할 수 없는 동작이 발생하도록 한다. 스마트카드의 경우 내부 클록이 증가하여 인증 과정이 우회되는 결과를 낳기도 한다. 글리치 공격을 막기 위해서는 하드웨어 장치가 쉽게 분석되지 않도록 회로를 불규칙하게 구성해야 한다.

2.4 오류 주입 공격

오류 주입 공격은 공격 대상에게 직접 접근하여 장치의 비정상적인 동작을 끌어내기 때문에 능동(active) 공격으로 분류된다. 주로 암호 연산 과정에서 발생하는 계산상의 오류를 이용하여 유효한 결과를 얻어내는데, 이를 위해 의도적으로 전력을 낮추거나 올리고 장치의 온도를 조절하는 cold boot 공격 [10] 등의 행위를 한다.

오류 주입 공격은 공격자가 수행할 수 있는 의도적인 행위의 선택폭이 넓고 대부분의 암호 장치에 쉽게 적용할 수 있기 때문에 널리 사용되는 부채널 공격 중 하나이다.

III. 부채널 공격 사례

3.1 글리치 공격

스펜인의 Honorio 연구팀은 self-timed ring 기반 진난수생성기에 전력 글리치 공격, 클록 글리치 공격을 수행하였으며 이로 인해 편향된 난수들을 발생 시킬 수 있음을 증명하였다 [1].

원활한 전력 글리치 공격을 위해 진난수생성기의 기본 전력을 1.2V에서 0.7V로 하향한 뒤 전력 글리치를 주입하는 시간을 늘려가며 실험을 진행하였다. [그림 1]의 (a)는 기존 진난수생성기의 난수 출력을 비트스트림으로 표현한 결과이고 (b)와 (c)는 각각 62.5μs, 187.5μs 동안 전력 글리치 신호를 주입한 결과이다 [1]. 주입 시간이 길어질수록 난수성이 감소하는 모습을 통해 공격의 유효성을 확인 할 수 있다.

또한 클록 글리치 공격을 위해 기존 20MHz의 클록 신호 대신 40MHz의 클록 신호를 주입하였고 이를 통해 진난수생성기의 출력 난수를 완전히 통제 가능하다는 것을 실제로 증명하였다.

3.2 주파수 주입 공격

2009년 Markettos 링 발진기(ring oscillator) 기반의 진난수생성기의 주파수 주입 공격 방법을 발표 하였다 [2]. 스마트카드 또는 보안 마이크로 컨트롤러의 전원 공급 장치에 사인파 신호를 주입하여 의도적으로 링 발진기의 동작 조건을 수정하고 편향된 출력 신호를 얻어내는 결과를 보여주었다. 난수성의 감소를 비교 및 분석하기 위하여, 사인파 신호 주입 이후 시행된 난수성 검증 결과를 [표 1]에 정리하였다 [2]. NIST STS 통과율은 약 15%, dieharder 테스트는 약 32% 수준으로 하락하는 결과를 통해 주파수 주입 공격의 유효성을 확인하였다.

[표 1] 난수성 검증 결과

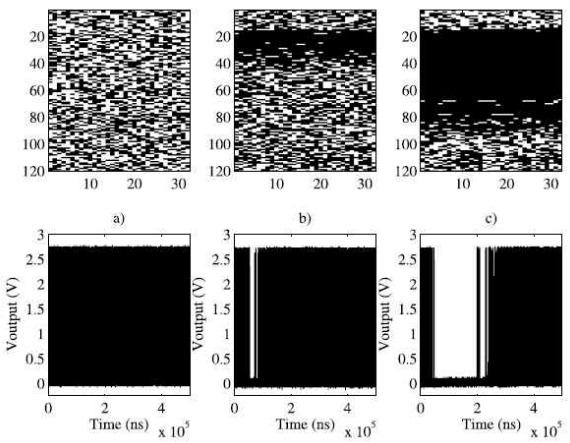
NIST	Pass			Fail
No injection	187			1
Injection	28			160
Dieharder	**Pass**	**Poor**	**Weak**	**Fail**
No injection	86	6	6	9
Injection	28	16	5	58

3.3 전자기 공격

2012년 [2]에서 수행된 주파수 주입 공격을 개선한 전자기 공격이 발표되었다 [11]. 일반적으로 전자기 공격은 암호화 장치에서 방출되는 전자기의 특성을 분석하는 비침입 공격이다. 하지만 [2]에서는 프로브를 이용하여 전자기를 직접 암호화 장치에 주입하는 능동 공격의 형태를 보여준다. [2]와 마찬가지로 링 발진기 기반의 진난수생성기에 공격을 수행하였으며, 전원 패드에 직접 신호를 주입할 필요가 없는 향상된 공격 방법이다.

[그림 2]는 진난수생성기의 출력 난수를 비트스트림으로 표현한 결과이다 [11]. 강한 전자기가 주입될수록 난수성이 감소하는 모습을 관측할 수 있고 이를 통해 공격의 유효성을 확인할 수 있다.

또한 비트스트림을 조작하여 특정한 문장이 나타나도록 하는 등 추가적인 실험을 통해 진난수생성기의 난수를 완전히 통제할 수 있음을



[그림 1] 전력 글리치 공격의 결과

[그림 2] 전자기 공격의 결과

성공적으로 증명하였다. 공격자는 이러한 공격들을 통하여 난수의 정확한 값을 취하고 암호화 알고리즘 구현의 비밀 키 정보를 손쉽게 추출할 수 있기 때문에 진난수생성기의 부채널 공격 안전성을 높이기 위한 연구가 활발히 이루어져야 한다.

IV. 결론 및 향후 연구

본 논문에서는 현대 사회에서 필수로 사용되고 있는 난수생성기에 대해 간략히 설명하고 하드웨어 기반 부채널 공격의 종류 및 적용 가능성에 대해 언급하였다. 또한 난수생성기를 대상으로 한 부채널 공격의 실제 공격 사례들을 소개함으로써 난수생성기의 부채널 공격 대응 연구의 중요성을 강조하였다.

2002년, 스위스 ID Quantique사에서 세계최초로 양자난수생성기를 출시한 이후 진정한 무작위성을 가진 난수를 생성하기 위한 연구가 계속되어 왔다. 최근에는 대한민국의 EYL사가 방사성동위원소 반감기를 이용한 초소형 양자난수생성기 칩을 개발하고 [14], SK Telecom사가 세계최소형 양자난수생성기 칩을 개발하는 등 현재까지도 양자역학적 특성을 이용한 난수생성기의 연구가 활발히 이루어지고 있다. 이에 따라 향후 연구로는 현재 상용 또는 개발 중인 양자 난수생성기에 널리 알려진 전력분석 공격, 글리치 공격, 오류 주입 공격 등의 부채널 공격을 수행한 후 각 장치들의 안전성을 비교 및 분석 하고자 한다.

[참고문헌]

[1] H. Martin, T. Korak, M.E. San, M. Hutter, Fault attacks on STRNGs: Impact of glitches, temperature, and underpowering on randomness, *IEEE transactions on information forensics and security*, 10(2), 266-277. 2015.

[2] A.T. Markettos, S.W. Moore, The frequency injection attack on ring-oscillator-based true random number generators, Springer, Cryptographic *Hardware and Embedded Systems-CHES 2009*, 317-331. 2009.

[3] P. Bayon, L. Bossuet, A. Aubert, V. Fischer, Electromagnetic analysis on ring oscillator-based true random number generators, *Circuits and Systems (ISCAS), 2013 IEEE International Symposium on,* 1954-1957. 2013.

[4] https://hal-ujm.archives-ouvertes.fr/file/index/docid/833822/filename/2013_APEMC_Bayon.pdf

[5] Glitch attack, https://www.pcmag.com/encyclopedia/term/43805/glitch-attack

[6] Quantis RNG, https://www.idquantique.com/random-number-generation/products/quantis-random-number-generator

[7] SK Telecom QRNG Chip, https://www.globalskt.com/home/info/2108

[8] Quantis QRNG Chip, https://www.idquantique.com/random-number-generation/products/quantis-qrng-chip

[9] Power analysis attack, http://softknow.com/up2/file/20130930/20130930141438_0781.pdf

[10] J.A. Halderman, S.D. Schoen, N. Heninger, W. Clarkson, W. Paul, J.A. Calandrino, A.J. Feldman, J. Appelbaum, E.W. Felten, Lest we remember: cold-boot attacks on encryption keys, *Communications of the ACM*, 52(5), 91-98. 2009.

[11] P. Bayon, L. Bossuet, A. Aubert, V. Fischer, F. Poucheret, B. Robisson, P. Maurine, Contactless electromagnetic active attack on ring oscillator based true random number generator, Springer, *International Workshop on Constructive Side-Channel Analysis and Secure Design*, 151-166. 2012.

[12] NIST STS, https://csrc.nist.gov/publications/detail/sp/800-22/rev-1a/final

[13] dieharder, https://webhome.phy.duke.edu/~rgb/General/dieharder.php

[14] EYL QRNG, http://www.eylpartners.com/index.php/quantum-random-number-generator