양자 특성 기반 칩을 활용한 엔트로피 소스 모델 수립 방법에 관한 연구

김대형 · 김주빈* · 지동화

경기과학고등학교

A Study on the Establishment of Entropy Source Model Using Quantum Characteristic-Based Chips

Dae-Hyung Kim · Jubin Kim* · Dong-Hwa Ji

Gyeonggi Science High School for the Gifted

E-mail : daehyeong1216@gmail.com / jbkmath48128@gmail.com / donghwa722@naver.com

요 약

5세대 이후의 이동통신 기술은 초고속, 초연결, 초저지연 등을 요구하고 있다. 이 중, 안전한 초연결의 기술적 요구사항을 만족하기 위해서는 IoT 서비스의 말단에 해당하는 저사양 IoT 기기들도 고사양 서버와 동일한 수준의 보안 기능을 제공할 수 있어야 한다. 이러한 보안 기능을 수행하기 위하여 암호 알고리즘에서 필요한 정도의 안전성을 가진 암호키들이 요구되고, 암호키는 보통 암호학적 난수 발생기로부터 생성된다. 이때 난수 생성을 위해서는 좋은 잡음원들이 필요한데, 저사양 기기 환경 특성상 충분한 잡음원을 확보하기 어렵기 때문에 TRNG와 같은 하드웨어 난수 발생기를 사용한다. 이 논문에서는 방사성 동위원소의 붕괴를 예측할 수 없다는 양자의 특성을 기반으로 한 칩을 사용하였으며, 이 칩이 출력하는 신호를 기반으로 이진 비트열 형태의 엔트로피 소스를 얻는 여러 방법(TRNG)을 제시하였다. 또한, 각각의 TRNG에서 출력된 값의 엔트로피에 대해 NIST SP 800-90B 테스트를 이용하여 각 방법에 대한 엔트로피 양을 비교하였다.

ABSTRACT

Mobile communication technology after 5th generation requires high speed, hyper-connection, and low latency communication. In order to meet technical requirements for secure hyper-connectivity, low-spec IoT devices that are considered the end of IoT services must also be able to provide the same level of security as high-spec servers. For the purpose of performing these security functions, it is required for cryptographic keys to have the necessary degree of stability in cryptographic algorithms. Cryptographic keys are usually generated from cryptographic random number generators. At this time, good noise sources are needed to generate random numbers, and hardware random number generators such as TRNG are used because it is difficult for the low-spec device environment to obtain sufficient noise sources. In this paper we used the chip which is based on quantum characteristics where the decay of radioactive isotopes is unpredictable, and we presented a variety of methods (TRNG) obtaining an entropy source in the form of binary-bit series. In addition, we conducted the NIST SP 800-90B test for the entropy of output values generated by each TRNG to compare the amount of entropy with each method.

키워드

Quantum Entropy Chip (QEC), True Random Number Gererator (TRNG), Entropy Source Model, Low-end Devices

Ⅰ. 서 론

저사양 기기는 고사양 기기들에 비해 낮은 성능과 적은 메모리를 가진 기기를 말한다. 따라서, 저

* corresponding author

사양 기기는 고사양 기기만큼 높은 수준의 보안성을 보장하기 어렵다. 하지만 IoT 환경에서는 말단 부분에 있는 저사양 기기에도 고사양 기기에서 전달되는 중요한 정보들이 들어가기 때문에 고사양 기기와 동일한 수준의 보안성을 보장해야 할 필요가 있다.

보안성을 위해 암호 알고리즘을 사용하는 과정에서 암호학적으로 안전한 난수를 요구하는 경우가 많다. 좋은 난수를 발생시키기 위해서는 시드값으로 사용하기 위해 엔트로피가 높은 좋은 잡음원이 필요한데, 고사양 기기에서는 비교적 좋은 잡음원을 얻기 쉽지만 저사양 기기에서는 좋은 잡음원을 얻기 어렵다. 따라서 하드웨어적으로 난수를 발생시키는 TRNG를 사용한다. TRNG는 잡음을 생성하는 부분과 이를 이진 비트열의 엔트로피 소스로 처리하는 엔트로피 소스 모델 부분으로 구성된다. 최근에는 양자의 특성을 이용해 잡음을 생성하는 칩인 QEC에 대해 많은 연구가 이루어지고 있다. 하지만, QEC에서 발생한 신호를 어떻게 처리해야 더 좋은 엔트로피 소스를 출력할 수 있을 것인가에 대해서는 아직 명확히 밝혀진 바가 없다. 따라서 본 연구에서는 방사성 동위원소가 붕괴할 때 방출하는 알파입자을 이용한 QEC를 사용하여 엔트로피 소스 모델을 여러 방식으로 설계한 뒤 수집한 엔트로피 소스의 안정성을 평가하고자 한다. 각 방식의 평가 결과는 QEC를 실제로 저사양 기기에 적용할 때 유용하게 이용될 수 있을 것으로 예상된다.

II. 이론적 배경

난수 발생기(random number generator, RNG)는 무한하게 난수를 발생시킬 수 있는 방법이나 이를 적용한 장치를 말한다. 이상적인 난수 발생기의 경우 다음 난수를 예측하는 것이 불가능하고, 모든 결과가 동일한 확률로 발생된다. 하지만 이런 진정한 난수를 빠른 속도로 발생시키는 방법은 아직까지 고안되지 않았고, 정해진 알고리즘을 통해서 난수를 빠르게 생성하는 방법들이 제안되었는데 이 경우에는 입력값에 따라 정해진 출력만 가능하므로 결정론적 난수 발생기, 또는 완전한 난수가 아니라는 의미에서 의사 난수 발생기(pseudorandom number generator, PRNG)라고 불린다.

한편, 의사 난수가 아닌 완전한 난수는 진난수라고 부르며, 진난수를 발생시키는 발생기를 진난수 발생기(true random number generator, TRNG)라 부른다. TRNG는 알고리즘의 방식이 아닌 물리적인 처리를 통해 하드웨어로 구현하기 때문에 무작위성을 가질 수 있다.

TRNG의 구조는 잡음원과 엔트로피 소스 모델으로 이루어진다. 잡음원은 물리적인 처리를 이용해 잡음을 생성한다. 잡음원에서 발생하는 잡음에는 열, 전기와 같은 것도 있지만 최근에는 양자의 특성을 이용한 잡음을 사용하고 있다. 양자의 경우 불확정성의 성질을 지니기 때문에 암호 체계의 물리적 구조의 취약성을 이용하여 공격하는 부채널 공격에 안전할 것으로 기대되기 때문이다. 이번 논문에선 방사성 동위원소가 붕괴하면서 방출하는 알파 입자의 감지 신호를 전달하는 QEC (quantum entropy chip)를 잡음원으로 사용한다.

엔트로피 소스 모델은 잡음원에서 생성된 잡음의 엔트로피를 수집해 디지털 값으로 출력한다. 출력되는 값은 대부분의 경우 PRNG의 초깃값으로 들어가게 된다. 이때 엔트로피의 수집 방식에 따라 결과값에서 측정되는 엔트로피 값이 달라질 수 있는데, PRNG의 경우 결정론적 알고리즘이기 때문에 그 자체로 엔트로피를 증가시킬 수 없다. 따라서 엔트로피는 잡음원과 엔트로피 소스 모델에 의해 결정되므로 전체적인 난수의 무작위성이 잡음원과 엔트로피 소스 모델에 의해 결정된다. 따라서 잡음원에서 발생하는 신호를 가장 높은 엔트로피를 갖도록 수집하는 엔트로피 소스 모델을 설계하는 것이 보안성의 측면에서 매우 중요하다.

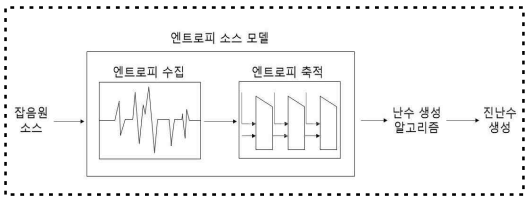

그림 1. TRNG의 구조

III. 실험 방법

전체적인 실험의 모식도는 (그림 2)와 같다. 잡음원(QEC)를 UART 통신을 이용해서 모델 기기와 연결한다. 이후, 기기에선 본 연구에서 설계한 엔트로피 소스 수집 알고리즘에 따라 UART 신호를 이진 비트열로 처리해 텍스트 파일의 형태로 저장한다. 총 1,000,000 bit가 모일때까지 실험을 진행한뒤, 이를 저장한 텍스트 파일을 PC로 옮겨서 발생한 엔트로피를 평가 방법에 따라 평가한다. 실험에 사용되는 모델 기기는 라즈베리파이4(Raspberry pi 4 Model B)이고, 평가 방법은 NIST SP 800-90B를 따른다.

엔트로피 수집 방법은 총 2가지를 설계하였다.

첫 번째 방법은 신호가 온 순간의 시간을 ms 단위로 표시한 뒤, 이를 이진수로 표현해서 뒤의 16bit를 저장하는 방법이다. 이 경우 한번 신호가 올 때마다 16bit씩 얻어내므로 빠르게 엔트로피 소스를 수집할 수 있다.

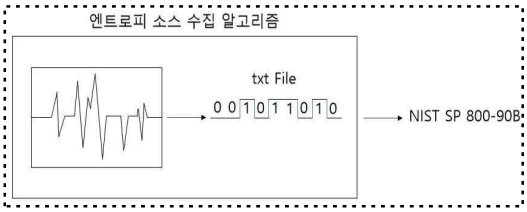

그림 2. 실험의 모식도

두 번째 방법은 특정 단위 시간을 정한 뒤, 단위 시간 동안 신호가 온 경우 1, 오지 않은 경우 0으로 하여 처리하는 것이다. 이때, 특정 단위 시간은 30ms로 정하였는데, 미리 10초동안 신호가 오는 횟수를 측정한 뒤 이 결과를 통해 단위 시간동안 신호가 올 확률과 안 올 확률이 같도록 단위 시간을 설정했다. 두 번째 방법의 경우엔 1bit당 무조건 30ms의 시간이 걸리므로 평균적으로 첫 번째 방법에 비해 16배 느리다. 또한, 환경에 따라 단위 시간이 달라질 수 있기 때문에 매번 단위 시간을 설정해주어야 한다는 단점이 있다.

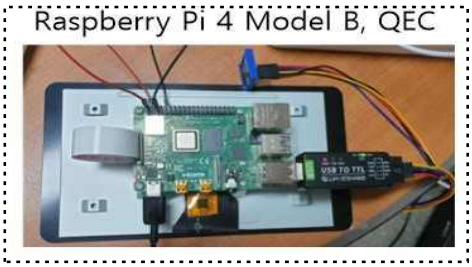

그림 3. 엔트로피 소스 수집 환경

수집한 엔트로피는 NIST SP 800-90B에 따라 평가한다[1]. NIST SP 800-90B는 IID특성을 가진 데이터에 대한 IID Test와 그렇지 않은 데이터에 대한 Non-IID Test가 존재한다. 본 연구에서는 IID 특성을 만족하지 못하는 것으로 나타났기 때문에, Non-IID Test로 평가를 진행하였다.

Non-IID Test의 경우 총 10가지의 엔트로피 추정과정을 거친다. 그 뒤, 10가지의 엔트로피 추정값 중 가장 작은 값을 엔트로피 소스에 대한 최종 추정값으로 결정한다. 10가지 방법에 대한 자세한 내용은 참고문헌의 내용을 통해 확인할 수 있다.

테스트는 NIST에서 제공하는 구현 코드를 이용하여 진행하였다[2]. 실험환경은 다음과 같다.

- Windows 버전 : Windows 10 Home
- 시스템 프로세서 : Intel(R)Core(TM)i5-1135G7@2.40GHz
- 시스템 RAM : 8.0GB
- 시스템 종류 : 64비트 운영 체제

Ⅳ. 실험 결과

NIST SP 800-90B를 이용한 엔트로피 평가 결과는 다음과 같다. 각 방법당 총 3번에 걸쳐 수집한 엔트로피 소스에 대한 실험 결과의 평균값을 구하였다.

표 1. 엔트로피 평가 결과의 평균값

	방법 1	방법 2
Non-IID Test	0.735781	0.772973

Ⅴ. 결 론

NIST SP 800-90B의 테스트 결과 방법 2로 얻은 엔트로피가 방법 1로 얻은 엔트로피에 비해 높은 것으로 나타났다. 하지만, 방법 2와 방법 1의 수집 시간이 16배 차이가 나기 때문에 걸리는 시간에 비해 엔트로피의 양의 차이는 적은 것을 알 수 있었다.

한편, 다른 참고문헌에 비해 엔트로피 값이 작게 나타났다. 그 이유는 우리가 엔트로피를 수집한 방법 자체에 문제가 있거나, NIST SP 800-90B에 테스트를 하기 위해 사용한 데이터의 양이 적었기 때문으로 추측된다. 따라서 추후 더욱 다양한 엔트로피 수집 방법을 사용하고, 더 많은 양의 엔트로피 수집하여 연구를 보완할 계획이다.

Acknowledgement

본 논문은 경기과학고등학교 2021년도 R&E 및 한국과학창의재단 창의 R&E 연구사업의 지원을 받았습니다.

References

[1] M.S. Turan, E. Barker, J. Kelsey, K.A. McKay, M.L. Baish and M. Boyle, “Recommendation for the Entropy Sources Used for Random Bit Generation,” NIST SP 800-90B(second DRAFT), Jan. 2016

[2] The SP800-90B_EntropyAssessment C++package implements the min-entropy assessment methods included in Special Publication 800-90B. [Internet]. Available : https://github.com/usnistgov/SP800-90B_EntropyAssessment.