Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.27, NO.3, Jun. 2017 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2017.27.3.449

양자난수발생기 Quantis의 후처리 과정에 관한 암호학적 분석*

배 민 영,† 강 주 성, 염 용 진‡
국민대학교 금융정보보안학과

Cryptographic Analysis of the Post-Processing Procedure in the Quantum Random Number Generator Quantis*

Minyoung Bae,† Ju-Sung Kang, Yongjin Yeom‡
Dept. of Financial Information Security, Kookmin University

요 약

본 논문에서는 양자난수발생기 Quantis의 후처리 과정에 대하여 암호학의 관점에서 실험을 통하여 안전성과 성능을 분석하였다. Quantis의 후처리 과정은 수학적 이론에 근거한 이진행렬-벡터 곱 연산을 통해 풀엔트로피(full-entropy)를 출력하도록 설계되었고, NIST SP 800-90B의 최소엔트로피(min-entropy) 추정 테스트를 이용하여 이를 검증하였다. 이진행렬-벡터 곱 연산에 최적화 기법을 사용함으로써 난수 생성 속도에 미치는 영향을 최소화하였음을 확인하고, NIST SP 800-90B에서 제시한 검증된 Conditioning과의 난수 출력 성능을 비교하였다. 또한, 미국 NIST와 독일 BSI의 난수발생기 표준 모델과 Quantis의 부합되는 요소와 아닌 요소를 구분하였다. Quantis를 암호학의 용도로 사용하고자할 경우, CMVP 기준에 적합하게 이용하기 위해 Quantis의 출력 데이터를 승인된 의사난수발생기의 씨드로 사용하여 출력한 난수를 사용하는 것이 적절하다고 판단된다.

ABSTRACT

In this paper, we analyze the security and performance of the Quantis Quantum random number generator in terms of cryptography through experiments. The Quantis' post-processing is designed to output full-entropy via bit-matrix-vector multiplication based on mathematical background, and we used the min-entropy estimating test of NIST SP 800-90B so as to verify whether the output is full-entropy. Quantis minimizes the effect on the random bit rate by using an optimization technique for bit-matrix-vector multiplication, and compared the performance to conditioning functions of NIST SP 800-90B by measuring the random bit rate. Also, we have distinguished what is in Quantis' post-processing to the standard model of NIST in USA and BSI in Germany, and in case of applying Quantis to cryptographic systems in accordance with the CMVP standard, it is recommended to use the output of Quantis as the seed of the approved DRBG.

Keywords: Quantum random number generator, Post-processing, Conditioning, 2-universal hashing

I. 서 론

정보보호에서 필요로 하는 이상적인 난수는 동전 던지기를 통해 얻는 수와 같이 예측불가능하고 독립적이며, 재발생이 불가능한 수이다. 암호 시스템의 암호 알고리즘이나 프로토콜 등은 난수가 이상적인

Received(03. 14. 2017), Accepted(04. 18. 2017)
* This work was supported by ICT R&D program of MSIP/IITP.[10044559, 2014-044-014-002]
* 본 논문은 2016년도 동계 학술대회에 발표한 우수논문을 개선 및 확장한 것임
† 주저자, mypear@kookmin.ac.kr
‡ 교신저자, salt@kookmin.ac.kr(Corresponding author)

난수라 가정한 후 설계되므로, 안전한 난수를 생성할 수 있는 난수발생기 사용이 필수적이다.

난수발생기는 주로 초기 씨드(Seed) 값으로부터 결정론적인 알고리즘을 통해 난수를 생성하는 의사난수발생기(Pseudo Random Number Generator; PRNG; Deterministic Random Bit Generator; DRBG)와 예측하기 어려운 물리적 현상으로부터 난수를 생성하는 진난수발생기(True Random Number Generator; TRNG)로 분류된다. PRNG의 출력 난수는 입력인 씨드에 의해 결정되기 때문에 TRNG의 출력 난수를 씨드로 사용하는 것이 일반적이다. TRNG는 아날로그 데이터인 잡음원(Noise source)을 입력으로 사용하기 위해 디지털 데이터로 바꾸는 디지털화(Digitization) 과정이 수행되고, 디지털화된 데이터의 바이어스(bias)를 줄이기 위하여 선택적으로 후처리 과정을 수행한 후 난수를 출력한다.

이상적인 난수의 출력은 난수발생기의 입력인 잡음원이 예측 불가능한 것에 의존하기 때문에, 엔트로피 소스(Entropy source)로 사용되는 잡음원의 특성파악이 중요하다. 따라서 물리적 특성의 잡음원이 가지는 바이어스를 줄이는 후처리 과정의 안전성 분석은 이상적인 난수를 출력하기 위해 반드시 고려되어야하는 사항이다.

1.1 난수발생기 및 엔트로피 소스 기준 문서

난수발생기는 암호학적으로 안전하게 사용되기 위하여 난수발생기의 구조와 입력 데이터인 엔트로피 소스 모델 등 관련 사항에 대하여 ISO/IEC 18031 국제표준[1], 독일의 BSI AIS 20/31[2], 미국의 NIST SP 800-90B[3, 4] 등에서 표준을 제시하고 있다. 이 중 잡음원에 대한 엔트로피 평가기준인 NIST SP 800-90B는 엔트로피 소스에 대한 체계적인 모델을 제시하기 위하여, 잡음원부터 후처리 과정까지 각 단계의 역할을 규정하고 있다.

2012년에 발표된 NIST SP 800-90B 첫 번째 드래프트의 엔트로피 소스 모델은 암호학적 알고리즘으로 구성된 'Conditioning'을 후처리 과정의 역할로 사용 여부를 선택할 수 있도록 포함하고, 이를 적용하였을 경우 출력 데이터의 엔트로피를 보장하여주는 조건과 이때 적용 가능한 암호학적 알고리즘 목록을 제공했다. 2016년에 발표된 두 번째 드래프트의 엔트로피 소스 모델은 [Fig. 1]과 같이 기존 모델에 후처리 과정으로 간단한 연산으로 구성된

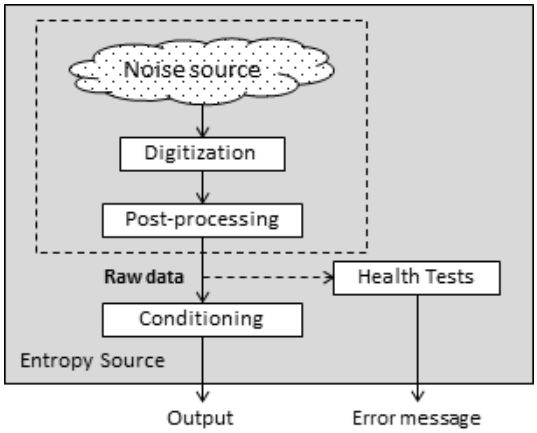

Fig. 1. NIST SP 800-90B(second draft) Entropy Source Model

'Post-processing'을 선택적으로 사용할 수 있도록 추가하였다. 'Post-processing'은 'Conditioning'과 유사한 목적으로 사용되지만, 'Post-processing'의 출력은 바이어스만 제거된 데이터로서 원시 데이터(Raw data)이므로 'Post-processing'만으로는 출력 데이터의 높은 엔트로피가 보장되지 않는다.

본 논문에서는 다른 표준 문서들과 다르게 난수발생기의 후처리 과정을 세분화하여 바라보고 있는 NIST SP 800-90B 두 번째 드래프트를 기준으로 후처리 과정을 분석하고자 한다.

1.2 양자난수발생기 Quantis[5]

상용화된 TRNG에는 양자정보의 예측불가능성을 이용하여 난수를 생성하는 양자난수발생기가 다수 존재한다. 스위스 ID Quantique 사의 'Quantis'는 단일 광자(Single photon)와 빔 스플리터(Beam splitter)를 이용하여 난수를 출력하는 난수발생기로 USB, PCI, PCI-express 인터페이스를 가진 디바이스(device)로 제공된다.

Quantis는 원시 데이터를 출력하는 경우, 4Mbps(Mega bits per second) 또는 16Mbps의 난수 출력률(Random bit rate) 성능을 가지며, 디바이스를 이용할 수 있는 라이브러리 생성 코드와 라이브러리를 사용하는 응용 프로그램을 제공하고 있어, 난수 출력 과정 및 랜덤 행렬의 생성 과정을 확인할 수 있다. 또한, 소프트웨어로 확인할 수 없는 내부 후처리 과정을 포함한 기술들에 대하여 화이트페이퍼[6,7,8]를 제공한다.

본 논문에서는 양자난수발생기 Quantis의 후처리 과정을 암호학의 관점에서 분석하고, 난수발생기 표준으로부터 검증된 후처리 방법과의 효율성 비교를 하고자 한다.

II. Quantis의 후처리 과정 분석[6,7]

Quantis는 수학적 함수인 난수 추출기(Randomness extractor)를 이용하는 디바이스 내부 후처리 과정과 소프트웨어 프로그램 상의 후처리 과정을 포함하고 있다.

첫 번째 후처리 과정은 디바이스 내부에서 처리되는 폰노이만 방식(Von Neumann's method: Von Neumann unbiasing algorithm)으로, NIST SP 800-90B의 승인된 'Post-processing' 방식에 해당한다. 폰노이만 방식은 독립이고 연속인 이진 데이터에 대하여 적용 가능하기 때문에 양자난수발생기 후처리 과정에 사용하기 적합하지만, 결정론적이기 때문에 한계가 존재한다는 것은 잘 알려진 사실이다.

두 번째 후처리 과정은 소프트웨어 프로그램에서 처리되도록 되어있고, 폰노이만 방식이 적용된 씨드를 추가 입력으로 이용하는 난수 추출기로, 'Conditioning'에 해당하며 첫 번째 후처리 과정의 한계를 보완한다. 추가된 후처리 과정은 정보 이론인 Left-over hash lemma와 2-universal hashing에 근거[8]하고 있으며, 랜덤 행렬을 이용하여 이진행렬-벡터(Bit-matric-vector) 곱 연산을 수행하는 난수 추출기이다.

Quantis는 두 번째 후처리 과정을 효과적으로 제공하기 위하여, 소프트웨어 프로그램에서 폰노이만 방식이 적용된 데이터로 랜덤 행렬 데이터를 생성하여 파일로 저장하고, 난수 출력 요청 시마다 랜덤 행렬 데이터 파일을 입력받아 사용할 수 있도록 제공하고 있다. Quantis 후처리 과정은 안전성에 있어 이론적 근거가 충분하지만, 유니버설 해시 함수의 안전성을 충분히 확보하기 위해서는 씨드에 해당되는 랜덤 행렬 데이터가 입력 데이터인 잡음원과 독립이어야 하고 자주 갱신해주어야 한다는 조건이 필요하다. 난수발생기의 후처리 과정 운용에 있어 이를 반드시 유의해야 한다.

본 논문에서는 Quantis의 USB 디바이스와 응용프로그램 EasyQuantis, ID Quantique가 제공한 라이브러리 프로젝트, Samples C 프로젝트를 이용하여 이론적 근거를 바탕으로 설계된 Quantis의 두 번째 후처리 과정이 실제로 보장받게 되는 출력 난수의 엔트로피와, 두 번째 후처리 과정인 이진 행렬-벡터 곱 연산 속도가 최종 난수 출력 속도에 미치는 영향을 실험을 통해 분석한다. 실험에 사용된 환경은 다음과 같다.

- Windows 버전 : Windows 10 Pro
- 시스템 프로세서
  : Intel(R)Core(TM)i7-4790K CPU@4.00GHz
- 시스템 RAM : 32.0GB
- 시스템 종류
  : 64비트 운영 체제, x64 기반 프로세서
- 구동 프로그램
  : Microsoft Visual Studio Community 2015
- 프로그램 언어 : C/C++

2.1 출력 난수의 엔트로피

Quantis는 Left-over hash lemma와 2-universal hashing의 이론적 원리에 근거하여 풀엔트로피(full-entropy)인 난수를 출력하기 위하여 추출기 $Ext: \{0,1\}^n \rightarrow \{0,1\}^k$ 의 압축률을 조절하였다. 추출기의 압축률은 랜덤 행렬로 사용된 유니버설 해시 함수의 통계적 거리인 실수 $\epsilon_{hash} = \epsilon > 0$ 에 대하여 입력 데이터의 비트(bit) 당 엔트로피가 s 이상일 때, 다음 식에 의해 조절된다.

$$\frac{k}{n} = s - \frac{2\log_2\frac{1}{\epsilon}}{n} \quad \Rightarrow \quad k = sn - 2\log_2\frac{1}{\epsilon}$$

Quantis는 $\epsilon < 2^{-100}$ 로 하고, 소프트웨어 구현상 효율성 실험을 통해, 다음과 같은 두 가지 압축률의 추출기를 설계하였다.

- $s > 0.946$: (75%) $n = 1024$, $k = 768$
- $s > 0.973$: (87.5%) $n = 2048$, $k = 1792$

Quantis는 난수성에 대한 평가로 NIST SP 800-22, DIEHARD, BSI AIS20/31 등의 테스트를 시행하였고, 결과 리포트를 게시하였다[9]. 또한 충돌(Collision) 엔트로피를 이론적으로 분석하고, 이를 통해 보수적인 난수성 평가 측도로 여겨지

는 최소엔트로피(min-entropy)를 확인하였다고 명시하였다. 본 논문에서는 Quantis 상용화 당시 표준으로 게시되지 않았던 잡음원에 대한 NIST SP 800-90B 두 번째 드래프트의 통계적 최소엔트로피 추정 방법을 적용하였다. 따라서 NIST SP 800-90B의 최소엔트로피 추정 테스트는 이론적으로만 분석된 최소엔트로피를 실제 실험을 통해서 검증하는 의미를 가진다.

NISP SP 800-90B의 테스트는 통계적으로 의미 있는 결과를 얻기 위하여 최소 1,000,000바이트 이상의 데이터를 필요로 하고, 먼저 데이터의 통계적 특성인 IID(Independent and identically distributed) 여부를 확인한 후, IID 여부에 따라 적합한 엔트로피 추정 방법을 적용하여 최소엔트로피를 출력한다. 따라서 기준에 맞는 실험을 위하여 Quantis 디바이스로부터 원시 데이터 1,333,376바이트 10개를 추출하고, 각각에 대하여 Quantis에서 기본적으로 제공한 폰노이만 랜덤 행렬 데이터를 이용하여 두 가지 추출기를 통해 1,000,032바이트 10개, 1,166,592바이트 10개를 얻어, 총 30개 샘플에 대한 엔트로피를 추정하였다.

실험에 사용된 Quantis의 원시 데이터와 후처리 과정을 거친 데이터는 모두 IID 데이터로 확인되어 IID 최소엔트로피 추정 테스트를 진행하였다. 또한, Quantis 출력 데이터가 IID 데이터가 아닌 것으로 판단되었을 경우의 최소엔트로피를 확인해보기 위하여 Non-IID 최소엔트로피 추정 테스트도 추가로 진행해보았다. 총 30개 샘플에 대한 실험 결과를 세로축을 최소엔트로피로 설정하여 그래프로 나타내면, 각각 〔Fig. 2〕, 〔Fig. 3〕과 같다.

IID 최소엔트로피 추정 테스트 결과에서 원시 데이터와 후처리 과정을 거친 데이터의 최소엔트로피의 변동 범위가 0.994와 0.996 사이인 것으로 보아, Quantis가 설계한 추출기의 입력 데이터의 비트 당 엔트로피가 s 이상이어야 한다는 가정에 부합하고, 출력 데이터 또한 풀엔트로피로 판단하기에 충분한 결과이다.

Non-IID 최소엔트로피 추정 테스트 결과는 원시 데이터와 후처리 과정을 거친 데이터의 최소엔트로피의 변동 범위가 0.88과 0.96 사이인 것으로 확인된다. IID 데이터에 대한 Non-IID 최소엔트로피 추정 테스트 결과는 Quantis 후처리 과정의 입출력 데이터가 Non-IID 데이터로 판명되더라도 최소엔트로피는 0.9 정도로 추정될 것이라 판단할 수 있다.

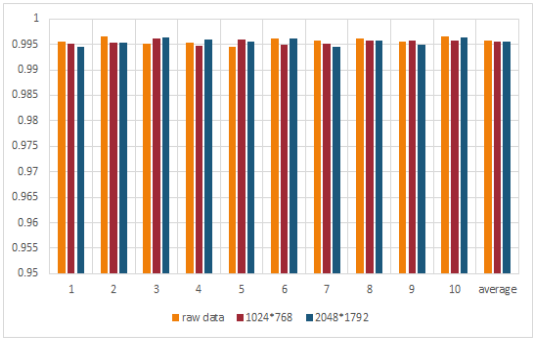

Fig. 2. Min-Entropy Estimation of IID Sources

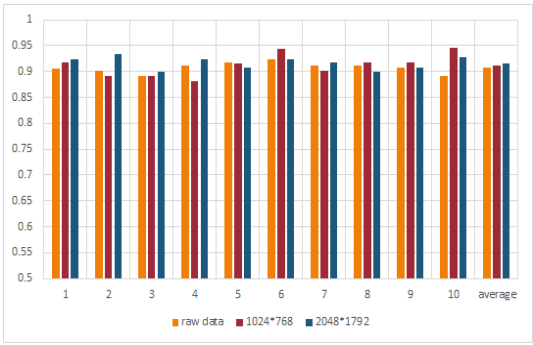

Fig. 3. Min-Entropy estimation of non-IID Sources

〔Table 1〕은 30개 샘플에 대한 실험 결과 최소엔트로피의 평균값을 정리한 것이다.

시행한 테스트가 보수적인 측정방법인 최소엔트로피에 대한 통계적 추정 테스트임을 감안할 때, 실험 결과인 엔트로피는 모두 풀엔트로피에 가까운 높은 엔트로피라고 판단할 수 있으며, 후처리에 따른 엔트로피 변동 폭은 통계적인 관점에서 차이가 없다고 판단 가능한 수치이다. 따라서 실험 결과는 Quantis 후처리 과정의 이론과 상응하는 결과를 보이며, 원시 데이터와 후처리 과정을 거친 데이터 또한 높은 엔트로피를 가지는 것을 확인하였다.

Table 1. Average Min-Entropy of the experimental data

	Raw data	1024×768	2048×1792
IID Test	0.9957	0.9954	0.9955
Non-IID Test	0.9075	0.9124	0.9162

2.2 난수의 출력 속도

Quantis의 후처리 과정으로 사용된 이진행렬-벡터 곱 연산은 처리 속도가 느리다고 알려져 있다. 따라서 Quantis에는 후처리 과정인 행렬 곱 연산 속도가 난수 출력 속도에 미치는 영향을 최소화하기 위한 구현 기법이 적용되었다. 적용된 최적화 구현 기법[10]은 행렬 데이터와 입력 데이터, 출력 데이터를 64비트 단위의 크기로 연산하고, 64비트의 각 1비트마다 배타적 논리합(exclusive or; 이하 xor; ^ 또는 ⊕로 표기)을 처리하는 과정에서 같은 기능을 하도록 'and'와 'multiplication' 등의 연산자를 사용함으로써 총 연산자 호출 횟수를 크게 줄였다.

최적화 기법의 핵심 연산 과정인 64비트 입출력의 처리 과정은 [Fig. 4]와 같고, 'parity' 배열에 적힌 숫자는 64비트인 배열의 1비트 당 인덱스를 의미한다.

[Table 2]는 [Fig. 4]의 최적화 기법이 적용된 일부 코드의 64비트 입출력 연산과, 같은 기능을 하는 일반적인(Conventional) xor를 사용한 연산 방법의 연산자 호출 횟수 비교를 나타낸 것이다.

연산자 호출 횟수 비교를 토대로 실제 후처리 과정 연산의 성능을 확인하기 위하여, Quantis 라이브러리의 최적화 기법이 적용된 후처리 과정 연산만

parity	63	62	61	60	...	3	2	1	0
parity >> 1		63	62	61	...	4	3	2	1
parity ^= parity >> 1	63	62^ 63	61^ 62	60^ 61	...	3^4	2^3	1^2	0^1
parity >> 2			63	62^ 63	...	5^6	4^5	3^4	2^3
parity ^= parity >> 2	63	62^ 63	61^ 62^ 63	60^ 61^ 62^ 63	...	3^4 ^5^ 6	2^3 ^4^ 5	1^2 ^3^ 4	0^1 ^2^ 3
parity &= 0x1111111111111111				60^ 61^ 62^ 63	...				0^1 ^2^ 3
((parity*0x1111111111111111)>>60)&1	(0^1^2^3)^(4^5^6^7)^...^(56^57^58^59)^(60^61^62^63)								

Fig. 4. The main idea of Quantis' efficient implementation

Table 2. Comparison of Operator calls

	Quantis	Conventional
xor(⊕)	2	64
shift(≫)	4	64
insert(=)	4	66
and(&)	2	1
multiplication(×)	1	0

Table 3. Speed comparison of Reading raw data and Post-processing operation (Mbps)

	1024×768	2048×1792
Quantis	101.7	54.1
Conventional	12.4	11.3

을 추출하고, 같은 기능을 하는 일반적인 행렬 곱 연산을 구현하여 10MB 데이터를 처리하는 실행 속도를 측정하여 Mbps로 나타내었다. 두 가지 압축률의 추출기에 대하여 총 10회씩 반복 시행하였고, 실험 결과에 대한 평균값은 [Table 3]과 같다.

측정 결과로 보아 일반적인 행렬 곱 연산 속도에 비해 Quantis의 이진행렬-벡터 곱 연산 속도가 8배 또는 5배 정도로 빠른 것을 확인할 수 있었다. 또한, 일반적인 방법을 사용하지 않았기 때문에 원시 데이터의 출력 속도에 비해 매우 빠르게 후처리가 가능다고 판단할 수 있다. 따라서 Quantis의 최적화한 후처리 연산 방법으로 인해 난수 생성 속도를 보장받을 수 있다.

원시 데이터의 출력 속도가 4Mbps인 USB 디바이스와 응용프로그램 EasyQuantis를 이용하여 (1)후처리를 사용하지 않는 경우, (2)후처리를 사용하는 경우, (3)디바이스를 이용하지 않고, 후처리만

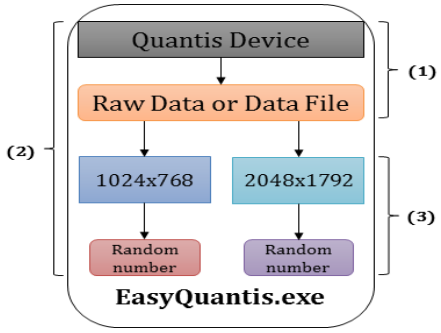

Fig. 5. Speed testing target

Table 4. Result of Speed test by EasyQuantis application (Mbps)

	1024×768	2048×1792
(1)	3.9	
(2)	1.5	
(3)	32.8	17.6

을 이용하여 난수를 출력하는 속도를 Mbps로 측정해보았다. 측정 대상을 도식화하면 [Fig. 5]와 같고, 측정 결과의 평균 속도는 [Table 4]와 같다.

실험은 후처리 과정인 두 가지 압축률의 추출기 모두 진행되었으나, 압축률에 따른 속도의 차이는 없었다. 반면, 두 추출기 모두 후처리 과정을 사용함으로 인한 난수 출력 속도의 현저한 감소를 확인하였다. 이 결과는 이진행렬-벡터 곱 연산 분석을 통해 후처리 과정 연산 속도가 매우 빠르기 때문에 난수 출력 속도에 큰 영향을 보이지 않을 것이라는 결과와 매우 상이하다. 따라서 Quantis는 후처리 연산 과정 자체가 난수 출력 속도에 미치는 영향은 거의 없으나, 후처리 연산을 위해 부가적으로 소모되는 처리량의 비중이 매우 크다고 판단된다.

III. 난수발생기 표준 모델과의 비교

3.1 표준 난수발생기와의 구조 비교

NIST SP 800-90B와 BSI AIS 31에서는 후처리 방법으로 비트 간 독립인 데이터에 대해 사용 가능한 폰노이만 방식, 선형 필터링 방법(Linear filtering method) 등의 방식을 승인된 방법으로 권고하고 있다. 따라서 Quantis 디바이스 내부에서 제공하는 후처리 과정인 폰노이만 방식은 NIST SP 800-90B의 승인된 'Post-processing' 방식에 포함되어 표준에 부합한다.

Quantis는 두 번째 후처리인 난수 추출기의 이론적 근거에 부합하도록 디바이스에서 출력하는 원시 데이터의 비트 당 엔트로피가 0.946 또는 0.973 이상이 되도록 디바이스 성능을 모니터링하고 있다고 명시하였다. 이는 [Fig. 1]에서 표기된 NIST SP 800-90B의 건전성(Health) 테스트와 BSI AIS 31의 완전 붕괴(Total failure) 테스트를 시행하여 엔트로피 소스의 유효성을 모니터링 하는 것과 비교되는 항목이다.

한편 Quantis 소프트웨어 프로그램에서 처리되는 후처리 과정인 이진행렬-벡터 곱 연산은 NIST SP 800-90B의 'Conditioning'에 해당하는 요소이지만 검증된 방식에는 포함되지 않는다. 3.2절에서는 검증된 'Conditioning' 방식과 Quantis의 이진행렬-벡터 곱 연산의 성능을 비교하였다.

3.2 승인된 후처리 과정과의 성능 비교

NIST SP 800-90B는 검증된 'Conditioning' 함수의 입력 데이터 크기가 출력 데이터 크기의 2배 이상이면 풀엔트로피 데이터를 출력하고, 그렇지 않다면 풀엔트로피의 0.85배인 데이터를 출력함을 보장하고 있다. 또한, 검증되지 않은 'Conditioning' 함수는 출력 데이터의 추정 엔트로피의 0.85배를 보장받는다. 검증된 'Conditioning' 방식은 다음과 같다.

- HMAC : FIPS 198-1[11]
- CMAC : NIST SP 800-38B[12]
- CBC-MAC : NIST SP 800-90B
- Hash_df : NIST SP 800-90A[13]
- Block_Cipher_df : NIST SP 800-90A
- Hash Function

본 논문에서는 Quantis의 이진행렬-벡터 곱 연산과 검증된 함수 중 Hash Function을 제외하고 모두 처리 속도를 측정하였다. 함수들을 공정한 성능 비교를 위하여 실험에 필요한 내부 함수는 오픈 소스 라이브러리인 boringSSL의 코드를 사용하였고, 다음과 같은 조건에서 진행되었다.

- 내부 해시 함수 : SHA-256[14]
- 내부 블록 암호 : AES-256[15]
- 테스트에 사용된 입력 데이터 크기 : 10MB

실험에 사용된 검증된 'Conditioning' 함수는 입력 데이터의 크기가 출력 데이터의 크기의 2배 이상일 때 풀엔트로피를 출력할 수 있으므로, 압축률을 모두 50%로 고정하여 사용한다. Quantis의 후처

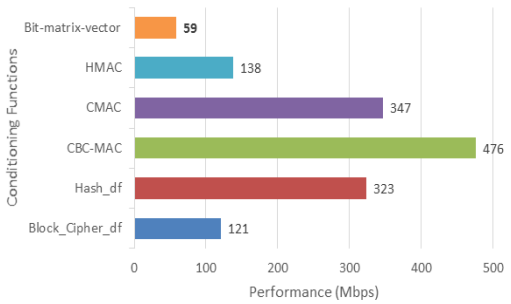

Fig. 6. Performance comparison with vetted conditioning functions

리 과정은 풀엔트로피를 출력하는 압축률과 관련한 조건이 입력 데이터의 비트 당 엔트로피이므로 실험에는 75% 압축률의 추출기를 선택하여 성능을 측정한다. 실험은 총 10회 반복 시행하였고, 실험 결과인 처리 속도의 평균값을 Mbps로 나타내면 〔Fig. 5〕와 같다.

실험 결과를 통해 승인된 Conditioning 함수 중 가장 성능이 좋은 함수는 난수 출력률이 476Mbps인 CBC-MAC이고, 가장 성능이 나쁜 함수는 121Mbps인 Block_Cipher_df임을 알 수 있었다. Quantis가 후처리 과정으로 사용한 유니버설 해시 함수 연산인 이진행렬-벡터 곱은 이론적 근거로 인해 안전성이 보장받지만, 난수 출력률이 59Mbps로 승인된 Conditioning 함수에 비해 2~8배 느리다는 것을 확인하였다.

3.3 Quantis의 암호학적 활용을 위한 방안

실험 결과를 통해 Quantis의 후처리 과정이 설계 이론에 상응하기 때문에 이론에 근거한 풀엔트로피를 출력한다고 판단할 수 있다. 그러나 Quantis를 암호학적으로 활용하기 위해서는 표준에 근거한 안전성을 보장받을 필요가 있다.

미국의 NIST와 캐나다의 CSEC가 공동으로 운영하는 암호모듈 검증제도(Cryptographic Module Validation Program; CMVP)〔16〕는 난수발생기의 활용 시 엔트로피가 높은 씨드와 NIST SP 800-90A에서 정의된 결정론적 난수 발생 알고리즘을 이용하도록 정의하였다. 이때, CMVP는 엔트로피가 높은 씨드임을 확인하기 위해 NIST SP 800-90B의 엔트로피 추정 테스트를 이용할 것을 강력히 권고하고 있다. 따라서 Quantis의 암호학적 활용을 위해 다음의 방안을 제안한다.

Quantis의 후처리 과정을 이용한 출력 데이터는 NIST SP 800-90B의 엔트로피 추정 테스트를 통해 풀엔트로피임을 확인하였고, 검증된 'Conditioning' 함수에 포함되지는 않으므로 출력 데이터의 표준에 근거한 비트 당 엔트로피를 0.85로 판단할 수 있다. 이 결과에 의해 Quantis의 출력 데이터는 NIST SP 800-90B DRBG의 씨드로 사용가능하다. 따라서 Quantis의 출력 데이터는 DRBG와 함께 사용할 경우 암호학적으로 활용하기에 적합하다.

IV. 결 론

본 논문에서는 양자난수발생기 Quantis가 잡음원의 바이어스를 줄이는 과정인 후처리 과정에 대하여 암호학적으로 분석하였다. Quantis의 후처리 과정은 이론 근거와 실험을 통해 출력 데이터의 엔트로피가 풀엔트로피를 가지고, 행렬 곱 연산에 최적화 기법을 적용하여 난수 출력 속도에 미치는 영향을 최소화하였음을 확인하였다.

Quantis의 후처리 과정은 NIST SP 800-90B의 표준 엔트로피 소스 모델과 비교하였을 때, 승인된 'Post-processing' 방식과 건전성 테스트를 시행하고 있어 표준 모델에 부합함을 확인하였으나, 'Conditioning'에 해당하는 유니버설 해시 함수의 사용은 검증된 방식이 아니며, 안전성을 충분히 얻기 위한 조건들을 조절하는 정책이 명확하지 않는다고 판단하였다. 또한 Quantis의 후처리 과정의 난수 출력 속도는 59Mbps로 검증된 Conditioning 함수 중 가장 성능이 좋은 CBC-MAC에 비해 8배 느렸다.

Quantis의 암호학적 활용의 관점에서 본 논문의 실험과 분석을 통해 NIST SP 800-90A에서 승인된 DRBG의 입력 씨드로 NIST SP 800-90B에 근거하여 비트 당 엔트로피 0.85를 줄 수 있으므로, CMVP가 암호학적 난수발생기 사용을 위해 제시한 기준을 충족시킬 수 있다. 따라서 Quantis는 출력 데이터를 DRBG와 함께 이용한다면 표준에 근거한 안정성을 보장받으며 활용할 수 있다.

References

〔1〕 "Information technology – Security techniques – Random bit generation," ISO/IEC 18031, Nov. 2011.

〔2〕 W. Killmann and W. Schindler, "A proposal for: Functionality classes for random number generators," BSI AIS 20 / AIS 31, Sep. 2011.

〔3〕 E. Barker and J. Kelsey, "Recommendation for the Entropy Sources Used for Random Bit Generation," NIST SP 800-90B, Aug. 2012.

〔4〕 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.

〔5〕 ID Quantique SA, ID Quantique White Paper - Random Number Generation using Quantum Physics, ID Quantique SA, Apr. 2010.

〔6〕 ID Quantique SA, ID Quantique White Paper - Randomness Extraction for the Quantis True Random Number Generation, ID Quantique SA, Sep. 2012.

〔7〕 M. Troyer and R. Renner, ID Quantique Technical Paper on Randomness Extractor - A randomness extractor for the Quantis device, ID Quantique SA, Sep. 2012.

〔8〕 R. Impagliazzo, L.A. Levin, and M. Luby. "Pseudo-random generation from one-way functions (extended abstract)." In Proceedings of the Twenty-First Annual ACM Symposium on Theory of Computing, May 1989.

〔9〕 ID Quantique SA, Quantis Certifications, ID Quantique SA, Apr. 2016.

〔10〕 D. Frauchiger, R. Renner, and M. Troyer, "True randomness from realistic quantum devices," arXiv preprint arXiv:1311.4547v1, Nov. 2013.

〔11〕 NIST, "The Keyed-Hash Message Authentication Code (HMAC)," FIPS PUB 198-1, Jul. 2008.

〔12〕 M. Dworkin, "Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication," NIST SP 800-38B, May 2005.

〔13〕 E. Barker and J. Kelsey, "Recommendation for Random Number Generation Using Deterministic Random Bit Generators," NIST SP 800-90A (Revision 1), Jun. 2015.

〔14〕 NIST, "Secure Hash Standard (SHS)," FIPS PUB 180-4, Mar. 2012.

〔15〕 NIST, "Advanced Encryption Standard (AES)," FIPS PUB 197, Nov. 2001.

〔16〕 NIST, "Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program," FIPS PUB 140-2 IG, Jun. 2017.

〈저자소개〉

배 민 영 (Minyoung Bae) 학생회원
2016년 2월: 국민대학교 수학과 학사
2016년 3월~현재: 국민대학교 일반대학원 금융정보보안학과 석사과정
〈관심분야〉 정보보호, 암호이론 및 구현, 인증시스템

강 주 성 (Ju-Sung Kang) 종신회원
1989년 2월: 고려대학교 수학과 학사
1991년 2월: 고려대학교 일반대학원 수학과 석사
1996년 2월: 고려대학교 일반대학원 수학과 박사
1997년~2004년: 한국전자통신연구원 선임연구원/팀장
2001년~2002년, 2010년: 벨기에 루벤대학 COSIC 방문 연구원
2004년~현재: 국민대학교 수학과 교수
2013년~현재: 국민대학교 BK21+ 미래 금융정보보안 인력양성사업단 교수
〈관심분야〉 암호이론, 정보보안 프로토콜, 안전성 분석 및 평가

염 용 진 (Yongjin Yeom) 종신회원
1991년 2월: 서울대학교 수학과 학사
1994년 2월: 서울대학교 수학과 석사
1999년 2월: 서울대학교 수학과 박사
2000년 4월~2012년 2월: ETRI 부설연구소 책임연구원/팀장
2006년 12월~2007년 12월: Columbia 대학교 방문 연구원
2012년 3월~현재: 국민대학교 수학과 부교수
2013년~현재: 국민대학교 BK21+ 미래 금융정보보안 인력양성사업단 교수
〈관심분야〉 암호구현 및 분석, 보안시스템 평가