CMOS 이미지 센서 암전류를 이용한 난수발생기

박병권[1], 박호중[2], 김용수[1], 강주성[2], 염용진[2], 문성욱[1], 한상욱[1,*]

[1]한국과학기술연구원, [2]국민대학교

*swhan@kist.re.kr

True random number generator using CMOS image sensor dark noise

Byung Kwon Park[1], Hojoong Park[2], Yong-Su Kim[1], Ju-Sung Kang[2], Yongjin Yeom[2], Sung Moon[1], and Sang-Wook Han[1]

[1]Center for Quantum Information, Korea Institute of Science and Technology (KIST)
[2]Department of Mathematics and Financial information security, Kookmin University

요 약

난수발생기는 통신, 보안, 시뮬레이션 등 다양한 분야에서 소요되는 난수를 생성하는 장치로, 최근 높은 엔트로피의 난수를 생성하기 위해 다양한 연구가 진행되고 있다. 본 논문에서는 CMOS 이미지 센서 내 암전류의 shot noise를 이용하여 높은 엔트로피의 난수를 추출하는 방법을 제안한다. 추출한 난수의 검증실험을 통해 CMOS 이미지 센서 내 암전류의 shot noise는 균일한 엔트로피를 제공할 수 있음을 보였다. 난수원에서 추출된 초기 난수는 후처리를 통해 높은 엔트로피를 가지는 난수로 출력되며 2.4Mbps 이상의 생성속도를 보였다.

Ⅰ. 서 론

난수발생기는 난수원에 따라 여러 가지 난수생성기로 분류할 수 있는데, 수학적인 결정적인 알고리즘을 이용한 pseudo random number generator (PRNG)[1], 물리적인 잡음을 이용한 physical random number generator[2], 양질의 난수를 생성하기 위해 양자적인 현상을 이용하는 quantum random number generator (QRNG)[3-6]가 있다. 시뮬레이션, 게임 등에서는 대량의 난수를 간편하게 생성하기 위해 PRNG가 많이 사용됐다. 반면에, 통신, 보안과 같은 높은 안전성이 필요한 분야에서는 양질의 난수를 생성하기 위해 physical random number generator 또는 QRNG가 함께 사용되어왔다.

QRNG는 높은 엔트로피를 가지는 난수를 생성하기 위해 광자검출시각[3], 광자수 검출[5], Bell 상태[6] 등의 양자적인 현상을 잡음원으로 이용한다. 이는 단일광자검출기가 필수적으로 소요되므로 경제적이지 못하고, 고속의 난수 생성에 무리가 있다. 단일광자검출기를 이미지 센서로 대체하여 광자의 shot noise를 잡음원으로 한 연구가 발표되었는데, 다수의 픽셀을 이용한 고속의 난수생성과 칩 형태의 경제성, 실용성으로 큰 관심을 받았다.[4] 하지만, 광원과 광 세기를 고르게 픽셀에 분포시키기 위한 부가적인 하드웨어 및 소프트웨어가 필요하다.

본 논문에서는 CMOS image sensor (CIS) 내에 흐르는 암전류의 shot noise를 이용하여 초기 난수를 추출하고 후처리를 통한 높은 엔트로피의 난수를 생성하는 방법을 제안한다. CIS는 다양한 휴대 기기에 내장되어 널리 사용되고 있으며, 암전류의 shot noise를 잡음원으로 이용하면 부가적인 하드웨어가 필요 없이 효과적으로 난수 생성이 가능하다. 잡음원에서 추출된 초기 난수, 후처리 난수를 국제표준에 기반한 엔트로피 측정을 통하여 난수원의 특성을 분석하고, 검증하였다.

Ⅱ. 본론

그림 1은 CIS를 이용한 난수발생기의 실험 셋업이다. 상용 CMOS 이미지 센서에 암상태를 구현하기 위해 렌즈캡을 이용 하였다. CIS 모듈의 이미지 데이터는 Control 보드를 통해 PC로 전송되며, PC는 CIS 모듈의 파라미터를 세팅하여 난수 생성에 최적인 상태로 조정할 수 있다. PC에서 전송된 이미지 데이터의 shot noise를 분석하고, 분석한 결과를 바탕으로 난수 추출을 진행한다. 추출된 난수는 bias, 패턴 noise와 같은 엔트로피에 악영향을 미칠 수 있는 요소가 포함되어 있으므로 후처리를 통해 이를 제거한다. 후처리를 마친 최종 난수는 국제표준 난수성 테스트를 통해 무작위성을 검증한다.

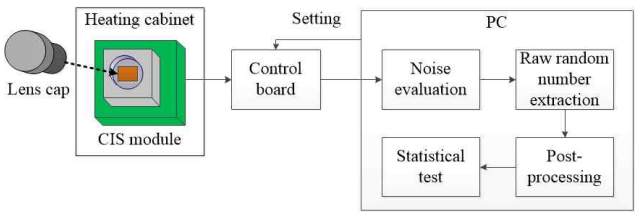

그림 1. CMOS 이미지 센서의 암전류를 이용한 난수발생기의 실험 셋업

그림 2는 CIS 내 암전류의 분포를 나타낸다. CIS의 analog digital converter (ADC)의 해상도로 인해 하나의 전자를 분별할 수 없으므로 shot noise의 Poisson 분포보다 큰 히스토그램을 보인다. 실험에서 3개의 암전류의 전자가 더해진 shot noise 분포를 확인할 수 있었다. Min entropy에 의해 실험에서 사용된 CIS 내 암전류의 분포는 하나의 sample 당 2bit를 추출할 수 있다. 암전류가 많아지면 shot noise의 분포는 넓어지며, 추출 가능한 난수도 비례하게 증가한다. 그림 3은 CIS 암전류의 전자수에 따른 shot noise 분포와 추출 가능한 난수를 나타낸다. 실험에서 CIS 모듈의 온도조절을 통해 암전류를 증가시켜 주었다.

초기 난수는 bias와 패턴 noise로 인해 엔트로피의 감소가 있을 수 있는데, 이를 후처리하여 엔트로피를 증가시킨다. 표 1은 초기 난수와 후처리 된 최종 난수의 엔트로피 측정결과를 보여준다. 한 sample 당 1Mbit의 난수가 사용되었다. CIS 내 암전류의 shot noise는 0.7의 엔트로피가 균일하게 측정되었으며, 이는 난수 생성에 적합한 잡음원 임을 보여준다. 표

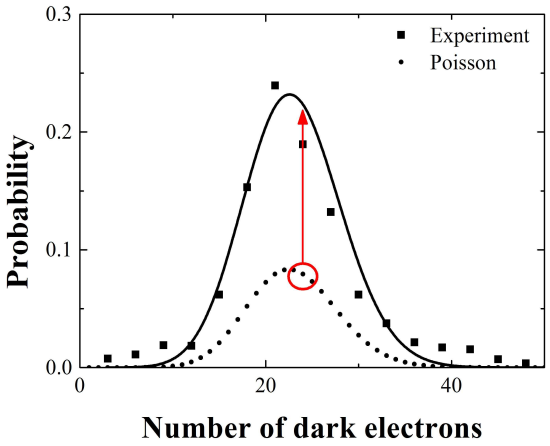

그림 2. CIS 내부 암전류의 shot noise 분포

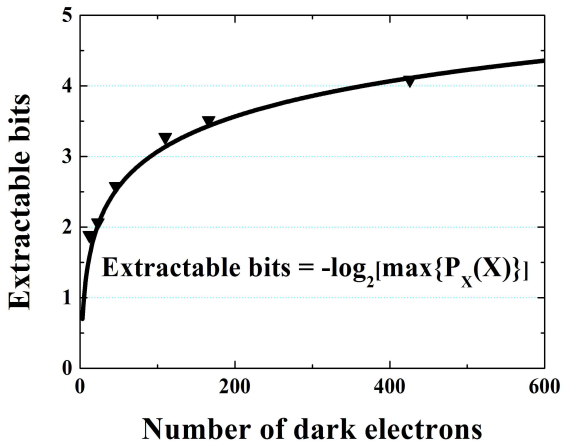

그림 3. CIS 내부 암전류의 shot noise 분포

표 1. 초기 난수와 후처리 된 최종 난수의 엔트로피 측정결과

	Raw data	Hankel matrix	HMAC
Sample 1	0.70251	0.99620	0.99591
Sample 2	0.69850	0.99966	0.99506
Sample 3	0.71113	0.99572	0.99548
Sample 4	0.70079	0.99624	0.99594
Sample 5	0.70538	0.99548	0.99594
Avg.	0.70366	0.99666	0.99567

표 2. 초기 난수와 후처리 된 최종 난수의 NIST 난수 테스트 결과

Test	Raw data	Hankel Matrix	HMAC
Frequency	Fail	Pass	Pass
Block frequency	Fail	Pass	Pass
Cumulative sums	Fail	Pass	Pass
Runs	Fail	Pass	Pass
Longest run	Fail	Pass	Pass
Rank	Pass	Pass	Pass
FFT	Pass	Pass	Pass
Non-overlapping template	Fail	Pass	Pass
Approximate entropy	Fail	Pass	Pass
Serial	Fail	Pass	Pass
Linear complexity	Fail	Pass	Pass

2는 NIST의 난수 국제표준 테스트 결과를 나타낸다. 후처리 된 최종 난수는 11종류의 난수 테스트를 모두 통과하였다.

Ⅲ. 결론

CMIS 이미지 센서 내 암전류의 shot noise를 잡음원으로 하는 난수를 생성하고 국제 표준에 기반하여 검증하였다. 초기 난수는 균일한 엔트로피가 안정적으로 측정되어 적합한 난수원 임을 알 수 있었고, 후처리를 마친 최종 난수는 국제 표준 테스트를 모두 통과하였다. 이미지 센서의 픽셀 어레이를 이용하여 최대 2.4Mbps의 속도로 난수 생성이 가능하다. CMOS 이미지 센서 내 암전류를 이용하면 부가적인 하드웨어 없이 소프트웨어 업데이트만으로 난수 생성이 가능하므로 휴대용 기기에 효율적으로 적용할 수 있을 것이라 기대된다.

ACKNOWLEDGMENT

This work was supported by the KIST program (2E30620) and the Institute for Information and Communications Technology Promotion (2020-0-00972).

참 고 문 헌

[1] M. Matsumoto and T. Nishimura, “Mersenne Twister: A 623-dimensionally equidistributed uniform pseudorandom number generator,” ACM Trans. Modeling and Computer Simulation, 8, pp.3-30, Jan. 1998.

[2] A. Uchida, K. Amano, M. Inoue, K. Hirano, S. Naito, H. Someya, I. Oowada, T. Kurashige, M. Shiki, S. Yoshimori, K. Yoshimura, and P. Davis, “Fast physical random bit generation with chaotic semiconductor lasers,” Nat. Photonics, 2, pp. 728-732, Nov. 2008.

[3] J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields, “A high speed, postprocessing free, quantum random number generator,” Appl. Phys. Lett., 93, pp. 031109-1-031109-3, Jul. 2008.

[4] B. Sanguinetti, A. Martin, H. Zbinden, and N. Gisin, “Quantum Random Number Generation on a Mobile Phone,” Phys. Rev. X, 4, 031056-1-031056-6, Sep. 2014.

[5] M. J. Applegate, O. Thomas, J. F. Dynes, Z. L. Yuan, D. A. Ritchie, and A. J. Shields, “Efficient and robust quantum random number generation by photon number detection,” Appl. Phys. Lett., 107, pp. 071106-1-071106-5, Aug. 2015.

[6] Y. Liu, X. Yuan, M.-H. Li, W. Zhang, Q. Zhao, J. Zhong, Y. Cao, Y.-H. Li, L.-K. Chen, H. Li, T. Peng, Y.-A. Chen, C.-Z. Peng, S.-C. Shi, Z. Wang, L. You, X. Ma, J. Fan, Q. Zhang, and J.-W. Pan, “High-Speed Device-Independent Quantum Random Number Generation without a Detection Loophole,” Phys. Rev. Lett., 120, pp. 010503-1-010503-6, Jan. 2018.