단일광자 검출기의 dark count를 이용한 난수생성 방법

박주윤, 문현승, 김범일, 허준

고려대학교

{pjy1343,hsmoon1104,bik0118,junheo}@korea.ac.kr

요 약

본 논문은 단일광자를 검출하기 위하여 사용되는 단일광자 검출기의 특성을 이용하여 난수 혹은 난수의 seed value를 생성하는 방법에 대하여 소개한다. 단일광자 검출기는 미세한 입력신호를 검출하기 위하여 매우 예민하게 동작이 되는 avalanche photodiode를 사용하는데, 이 때 원하지 않는 열잡음 등에 의하여 외부 입력이 존재하지 않을 때도 입력 신호로 오인하여 검출신호를 생성하는 dark count 문제가 발생한다. dark count 생성을 정규분포로 모사하는 과정과 정규분포 모델을 이용하여 난수를 생성하는 방법을 소개한다.

Ⅰ. 서 론

난수는 크게 두 가지로 나눠지는데 하나가 의사난수이고 나머지 하나가 진난수이다. 의사난수는 가능성은 낮으나 예측가능한 위험성이 존재하므로 예측이 불가능하다고 알려진 진난수가 주목받고 있다. 본 논문에서는 free-running하는 단일광자 검출기를 이용하여 난수를 생성하는 방법을 소개한다.

Ⅱ. 본론

Avalanche photodiode(APD)를 사용하는 단일광자 검출기는 실제로 검출기로 빛이 들어오지 않아도 검출신호를 출력하는 dark count 현상이 존재한다. 제안하는 방법은 정해진 검출시간을 미리 정해진 시간 간격으로 나누어서, 각 구간에서 발생하는 dark count의 수를 바탕으로 난수를 생성하는 것이다.

Dark count rate이 p인 단일광자 검출기가 있고 동일한 시간 간격마다 n개의 검출기 trigger 신호가 검출기에 인가된다면 해당 시간에 dark count가 검출되는 사건의 random variable은 이항분포 $x_i \sim B(n,p)$를 따르고 n이 충분히 크다면 random variable x_i의 합인 $X=\sum_{i=1}^{n} x_i$는 정규분포 $X \sim N(np, np(1-p))$를 따른다. 예를 들어 $n=100, p=0.1$인 경우 100번의 검출을 시도하는 동안 dark count 사건이 발생하는 횟수의 합 X는 정규분포 $N(10,9)$를 따른다. 따라서 X의 확률 분포는 다음과 같다.

$$p(X)=\begin{cases}0.2525 & X<8\\ 0.2475 & 8 \le X<10\\ 0.2475 & 10 \le X<12\\ 0.2525 & 12 \le X\end{cases} \quad (1)$$

그림 1과 같이 X의 값에 해당하는 구역에 bit를 할당한다면 정해진 횟수인 100회 동안 2개의 임의의 bit를 얻을 수 있다. 100MHz로 trigger 신호가 입력되는 단일광자 검출기를 가정한다면 1초를 기준으로 10^8번의 시행횟수가 되고 정해진 간격인 100으로 각 구간을 보면 10^6개의 구간이 만들어진다. 한 구간에 2개의 bit가 생성되므로 난수의 생성속도는 2MHz가 된다.

보다 현실적인 단일광자 검출기를 고려하여 $p=1.7\times10^{-6}$라고 하고 [1], $n=5\times10^6$, 단일광자 검출기의 동작속도 100MHz라 가정하면 40b/s의 난수생성속도를 구할 수 있다.

Bit를 할당하는 구간을 몇 개로 나누냐에 따라서도 난수 생성속도가 크게 달라질 수 있는데, 예를들어 각 구간의 발생 확률을 1/8로 나오게 기준점을 설정한다면 매 구간마다 3개의 bit를 얻을 수 있으므로 앞에서와 같은 조건에서 60b/s의 난수생성 속도를 얻을 수 있게된다.

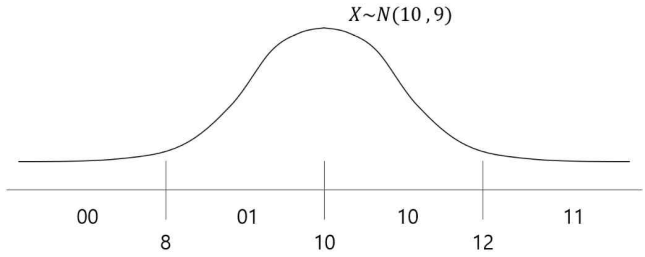

그림 1 $n=100, p=0.1$인 경우 bit할당을 위한 기준선 예시

Dark count는 주로 원하지 않는 열잡음에 의해 검출기가 발생되는 것이기 때문에 언제 어느 정도의 열잡음이 발생하여 단일광자 검출기가 검출신호를 발생할지 예측할 수 없고, 그렇기 때문에 제안하는 방법으로 생성하는 난수는 진난수일 것으로 예상할 수 있다.

Ⅲ. 결론

본 논문에서는 단일광자 검출기를 사용하면 피할 수 없는 문제인 dark count를 이용하여 난수를 생성하는 방법을 소개하였다. 이항분포를 따르는 dark count 발생 사건이 시행횟수가 충분히 클 때 정규분포로 근사되는 것을 이용하여 원하는 구간을 나누고 해당 구간에 bit를 할당하였다. free-running하는 단일광자 검출기에서 버려지는 dark count 정보를 활용할 수 있고 사용하는 검출기의 dark count rate만 알고 있다면 모델링 및 구현이 어렵지 않기 때문에 의미가 있다고 생각된다.

ACKNOWLEDGMENT

본 연구는 2019년도 한국과학기술정보연구원(KISTI) 주요사업 과제로 수행한 것입니다.

참 고 문 헌

[1] C. Gobby, Z. L. Yuan, and A. J. Shields, Appl. Phys. Lett. 84,3762 2004