광자 도착 시간 기반 양자난수생성 및 분석

서영진, 허준
고려대학교
cherishiz@korea.ac.kr, junheo@korea.ac.kr

Quantum random number generation and analysis based on photon arrival time

Seo Young Jin, Heo Jun
Korea Univ.

요 약

본 논문은 의사난수에 비해 높은 난수성을 갖는 순수난수 중 광자 도착 시간 기반의 양자난수를 생성하는 시스템은 구현하였고, 실험을 통해 얻은 난수열을 SP800-90B를 통해 분석하였다. 구현한 양자난수의 난수생성속도는 1834.19bps이고, 분석한 난수열의 엔트로피는 평균 0.871bit로 계산되었다.

Ⅰ. 서 론

의사난수는 알고리즘을 통해 실제 난수에 근접하게 만든 난수열이다.[1] 의사난수는 알고리즘에 의해 생성되는 난수열이기 때문에, 알고리즘의 입력값과 알고리즘 동작 방식을 알고 있다면, 난수열 예측이 가능하다. 의사난수와 다르게 예측할 수 없는 랜덤한 값을 갖는 실제 난수를 진난수라고 한다. 양자난수는 진난수에 속하며, 동일한 생성방식을 구현한다고 가정해도 똑같은 난수열을 얻을 수 없다.[2]

본 논문에서는 양자난수의 생성 방식 중 광자 도착 시간 기반의 양자난수열을 생성하는 시스템을 구현하고, 생성된 난수열의 엔트로피를 분석하였다.

Ⅱ. 본론

광자 도착 시간 기반의 양자난수생성[3]은 단일광자의 생성 확률 및 소실 확률과 검출기의 검출 확률 및 데드 타임에 의해 난수열이 생성되는 방식이다. 레이저에서 생성되는 펄스는 완벽하지 않기 때문에, 정확하게 단일광자만을 생성할 수 없다. 즉, 단일광자는 생성되는 확률을 가지고 있고 이는 포아송분포를 따른다. 또한, 레이저에서 생성되는 펄스는 레이저에 도달할 때까지 일부 손실이 발생한다. 레이저에서 단일광자가 생성되어 검출기까지 도달한다면, 포아송 분포에 의해 생성된 단일광자는 검출기에 도달할 때까지 일부 손실을 거쳐 소실될 확률을 갖고 검출기에 도달하게 된다.

검출기에 도달한 펄스는 검출기에 의해 검출되게 되는데, 이때 검출기는 검출 확률을 가지고 펄스를 측정하게 된다. 즉, 80%의 검출 확률을 갖는 검출기에 10개의 펄스가 도착했다면, 확률적으로 8개의 펄스만 검출된다. 검출기의 데드 타임은 검출기가 펄스를 한번 검출한 후에 다시 펄스를 검출할 수 있도록 준비하는 시간이다. 검출기의 동작 설정에 따라 다르지만, free-running mode를 사용하는 경우, 검출기는 항상 검출을 위해 준비하고 있으며, 이때 검출 준비에 필요한 시간이 데드 타임이다. 검출기의 동작 설정 중 gate mode의 경우, 검출기는 항상 펄스 검출을 하지 않고, 미리 설정된 특정 시간에만 펄스를 검출한다. 이때, 미리 설정된 특정 시간 간격을 데드 타임 시간과 동일하게 한다면, gate mode도 free-running mode와 동일하게 동작 가능하다.

단일광자의 생성 확률 및 소실 확률과 검출기의 검출 확률 및 데드 타임에 의해 검출기에서 측정되는 펄스는 예측할 수 없는 검출 간격을 갖게 된다. 즉, 이 검출 간격에 따라 난수열을 생성하는 방식이 광자 도착 시간 기반 양자난수생성 방식이다. 예를 들어, 검출기의 데드 타임과 동일한 δ 시간 간격을 8개의 간격으로 쪼갰다고 가정하고, $\delta_1, \cdots, \delta_8$의 간격마다 $000, \cdots, 111$의 bit를 생성한다고 가정한다. 이때 검출기에서 δ_4 시간에 펄스가 검출된 경우, 검출기에서는 100의 난수열을 생성한다.

광자 도착 시간 기반의 양자난수생성을 그림으로 나타내면 그림 1과 같다.

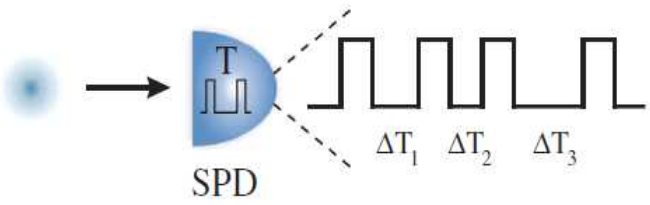

그림 1. 광자 도착 시간 기반의 양자난수생성

광자 도착 시간 기반의 양자난수생성은 검출기의 동작 설정 방식과 검출 시간 간격에 따라 설계 방식이 달라진다. 검출기의 동작 설정 방식이 free-running mode라면, 펄스 검출 시간 간격 δ가 검출기의 데드 타임에 대해 같거나 큰 δ 시간을 설정할 수 있다. 만약 δ와 데드 타임이 같다면, δ 시간 동안 검출기는 최대 1번의 펄스만 검출할 수 있을 것이다. 반대로 δ이 데드 타임보다 크다면, δ 시간 동안 검출기는 1회 이상 펄스를 검출할 수 있을 것이다. 이때, 검출로 얻어지는 난수열의 난수성은 δ이 데드 타임과 같을 경우보다 낮게 된다. 그 이유는 δ 간격에 두 개 이상의 펄스가 측정되어 난수열이 얻어지는 경우, 처음 얻은 난수열을 통해 다음 얻게

되는 난수열의 예측 확률이 높아지기 때문이다. δ 시간이 데드 타임보다 작은 경우는 δ이 데드 타임과 같은 경우와 동일한 난수성을 갖기 때문에 고려하지 않는다.

검출기의 동작 설정 방식이 gate mode인 경우, δ 시간 간격에 맞게 측정되도록 동작 시간 설정이 필요하다. 예를 들어, δ 시간 간격을 8개로 나눈다면, δ_1 시간 간격 안에 검출기가 1번 동작해야 하고, $\delta_1, \cdots, \delta_8$ 시간 간격 마다 검출기가 1번씩 동작해야 한다. 이때 동작되는 타이밍과 펄스가 검출기에 도착하는 타이밍을 맞도록 시스템을 설계해야 한다.

본 논문에서 설계한 광자 도착 시간 기반 양자난수생성기는 그림 2와 같다. 그림 2의 검출기는 free-running mode로 동작하는 검출기이며, 레이저는 100MHz로 펄스를 생성한다. 레이저의 펄스 생성 속도는 최대 100MHz이기 때문에, 검출기의 데드 타임 보다 큰 펄스 검출 시간 간격 δ을 갖도록 설계하였다.

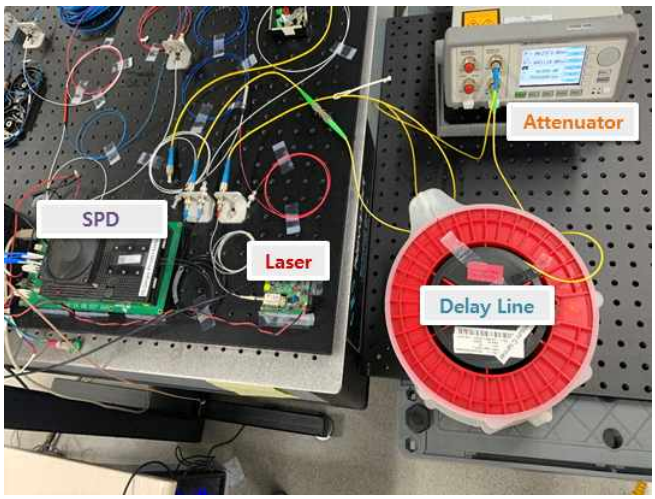

그림 2 광자 도착 시간 기반 양자난수생성기

광자 도착 시간 기반 양자난수생성기의 난수생성속도는 1834.19bps이다. 난수생성은 δ 시간을 4단계로 나누어 설계하였다. $\delta_1, \cdots, \delta_4$로 구성하였고, 펄스가 $\delta_1, \cdots, \delta_4$에 측정될 경우 각각 $00, 01, 10, 11$bit가 생성되도록 설계하였다. 레이저는 초기에 -29.5dBm의 세기로 출력하여 감쇄기를 통해 -74.5dBm로 감쇄하였다. 감쇄된 펄스는 delay line을 통해 6dBm 감쇄된다.

생성된 난수열은 NIST의 SP800-90B에서 제시한 난수성 검증 방식으로 엔트로피를 계산할 수 있다.[2] 난수열의 난수성 검증 방식은 초기에 반복 카운트 검증(repetition count test), 조정 비율 검증(adaptive proportion test)으로 구성된 헬스 테스트(Health test)를 통하여 그 적절성을 검증한다. SP800-90B에서 승인된 검증방법 및 추가로 사용자가 정의한 헬스 테스트를 통과하면, 선택적으로 컨디셔닝을 통과시킨 수열의 IID(Independent and Identically Distributed) 유무를 검증한다. 컨디셔닝은 FIPS180 또는 FIPS202에 정의된 HMAC, SP800-38에서 정의되고 블록 암호화에 활용되는 CMAC, CBC-MAC, 해시함수 등을 활용한다. 이후 IID를 판단하기 위하여, Permutation 검증 도구와 Chi-Square 검증 도구를 활용한다. 최종적으로 IID 혹은 Non-IID 결정에 따라 다양한 엔트로피 측정방법으로 엔트로피를 측정한다.

Permutation test와 Chi-Square test를 통과한 난수열은 IID로 판단하고, IID인 난수열의 엔트로피는 'Most Common Value Estimate'로 계산할 수 있다. Most Common Value Estimate의 계산 과정은 다음과 같다.

1. 입력 데이터에서 가장 많은 빈도로 발생하는 x에 대하여 비율 p를 구한다.
2. upper bound p_u를 다음과 같은 방식으로 구한다.

$$p_u = \min\left(1, p + 2.576\sqrt{\frac{p(1-p)}{L}}\right)$$

여기서 L은 입력 데이터의 길이이다.

3. 추정 최소 엔트로피는 $-\log_2(p_u)$이다.

Permutation test와 Chi-Square test를 통과하지 못한 난수열은 Non-IID로 판단하고, Non-IID인 난수열의 엔트로피는 'Most Common Value Estimate', 'Collision Estimate', 'Markov Estimate', 'Compression Estimate'를 통해 각각 엔트로피를 계산하고 그중에서 minimum을 난수열의 엔트로피로 추정한다. 추정된 엔트로피는 높을수록 난수성이 좋음을 의미한다.

본 논문에서 설계한 광자 도착 시간 기반 양자난수생성기를 통해 생성한 양자난수열의 엔트로피는 평균 0.871bit로 계산되었다. 엔트로피는 1bit 기준으로 계산되었으며, 총 10회 난수열 생성을 통해 평균값으로 계산되었다. 광자 도착 시간 기반 양자난수생성은 양자 난수 생성방식 중 광자 분산 기반 양자난수생성방식보다 엔트로피가 낮다. 그 이유는 광자 도착 시간 기반 양자난수생성은 레이저의 단일광자 생성이 포아송 분포를 따르기 때문에, 난수성이 낮다. 또한, 난수생성확률이 단일광자의 생성확률과 소실확률 및 검출기의 검출 확률과 데드 타임에 주요하기 때문에 Uniform 분포를 따르지 않는다. 이에 반해, 광자 분산 기반 양자난수생성방식은 빔분리기를 통해 온전히 Uniform 분포를 따르는 난수생성확률 갖기 때문에 난수성이 높다.[4]

Ⅲ. 결론

본 논문에서는 광자 도착 시간 기반 양자난수생성기를 설계하고 난수열을 생성하였다. 생성된 난수열의 난수생성속도는 레이저의 100MHz 펄스 생성속도에서 1834.19bps로 측정되었다. 생성된 난수열의 엔트로피 계산을 위해서, NIST의 SP800-90B를 이용하여 계산하였다. 난수열의 엔트로피는 1bit 기준에서 0.871bit로 계산되었다.

ACKNOWLEDGMENT

이 성과는 2021년도 정부(과학기술정보통신부, 교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No.2019R1A2C2010061, 한국연구재단-2019-글로벌박사양성사업)

참 고 문 헌

[1] Barker, E. et al. "Recommendation for key Management" NIST Special Publication 800-57, July, 2012.

[2] Sonmez Turan, M. et al. "Recommendation for the Entropy Sources Used for Random Bit Generation," NIST Special Publication 800-90B, Jan, 2018.

[3] Ma, X et al. "Quantum random number generation," Npj Quantum Inf 2 16021, 2016.

[4] 박주윤, 이종현, 서영진, 허준, "무선 레이저 송수신기를 이용한 양자난수생성 및 분석," 한국통신학회 하계학술대회, 2019.