컴퓨터공학과 20211507 김동건

LCG, MT 이외의 난수 생성 방식에 관하여 3가지 이상 열거하고 설명하시오.

첫 번째 방식으로는 폰 노이만이 제시한 중앙제곱법이 있다. 중앙제곱법은 구현이 굉장히 쉽다는 특징이 있다. 먼저, 임의의 seed를 정하고 이를 제곱한다. 제곱한 결과의 중앙 부분을 새 난수로 사용한다. 예를들어 기존 시드값이 7432라면 7432를 제곱한 55234624의 중앙인 2346이 새로운 시드가 된다. 그 다음은 2346을 제곱한 5507716의 중앙인 0771이 새로운 시드가 된다. 중앙제곱법은 이러한 방식으로 난수를 생성한다. 중앙제곱법은 위 설명에서 보면 알겠지만, 구현이 매우 간단하다는 특징이 있다. 다만, 현대에는 잘 쓰이지 않는데, 주기가 짧다는 특징이 있기 때문이다. 그럼에도 불구하고 중앙제곱법을 이용하면 굉장히 빠른 속도로 난수를 생성할 수 있고, 구현이 매우 간단하다는 장점이 있기 때문에 고품질의 난수가 필요하지 않다면 사용을 고려해볼 수 있다.

두 번째 방식으로는 XOR시프트 방식이 있다. 이는 비트연산 중 XOR연산과 비트시프트 연산을 사용하는 난수 생성 방식이다. 가장 기본적인 형태의 XOR시프트 방식은 다음과 같이 진행된다. seed, a, b, c가 있다면 먼저, seed에 (seed << a)를 XOR한다. 다음으로 seed에 (seed >> b)를 XOR한다. 마지막으로, seed에 (seed << c)를 XOR한다. 과정을 보면 알겠지만 a, b, c의 값을 어떻게 정하느냐에 따라 난수 생성기의 특성이 정해지기 때문에 적절한 값을 잘 정해주어야 한다. XOR연산과 비트시프트 연산은 비트 연산이라 매우 빠르기 때문에 난수 생성이 매우 빠르다는 장점이 있다. 그러나 단순한 구조로 인해 상태 공간이 제한적이고, a, b, c값을 잘 정해주지 않는다면 주기가 길지 않은 경우가 있을 수 있다. 또, 난수 품질 테스트 중 통과하지 못하는 테스트들이 있다. 이러한 단점들을 보완한 XOR Shift+, XOR WOW 등의 XOR시프트 변종 난수 생성방식들이 나와있다.

세 번째 방식으로는 TRNG가 있다. 이는 True Random Number Generator의 약자이다. 이는 예측이 거의 불가능하고, 난수들이 편항되지 않는 특징이 있다. 이러한 특징을 가질 수 있는 이유는 통계적으로 무작위 시그널을 만들어 내는 물리적 현상에서 엔트로피를 수집하여 난수를 생성하기 때문이다. 다른 난수 생성들은 이론적으로 완벽한 난수를 만들어 내지 않지만, TRNG는 물리적 현상을 통해 난수를 생성하기 때문에 이론적으로 예측할 수 없는 무작위한 난수를 만들어 낸다. 잡음, 광자 간섭, 방사능 붕괴 등에서 수집하곤 한다. 이 중 가장 일반적인 방식은 잡음 기반 방식이다. 잡음 기반 방식은 회로에서 발생하는 열의 잡음, 진폭 잡음 등 전자 장치들의 잡음을 통해 난수를 생성한다. 열의 잡음, 진폭 잡음 등은 불규칙성을 갖기 때문에 이를 이용하여 난수를 생성하는 것이다. 그렇지만, 속도가 느리다는 단점이 있다. 물리적 환경을 측정하여야 하기 때문에 많은 난수를 단기간에 생성하는 데에는 적절하지 못한 경우가 많다. 또한, 물리적 환경을 측정하기 위한 하드웨어가 필요하다는 단점이 있다. 또, 측정과 관련하여 환경과 품질 관리가 필요하다는 단점이 있다. 그럼에도 불구하고 생성하는 난수의 품질이 좋기 때문에 보안이 중요한 곳에서 많이 쓰이고 있다.