카오스적인 랜덤 디지틀 변환에 관한 연구

Chaotic random digital transformation

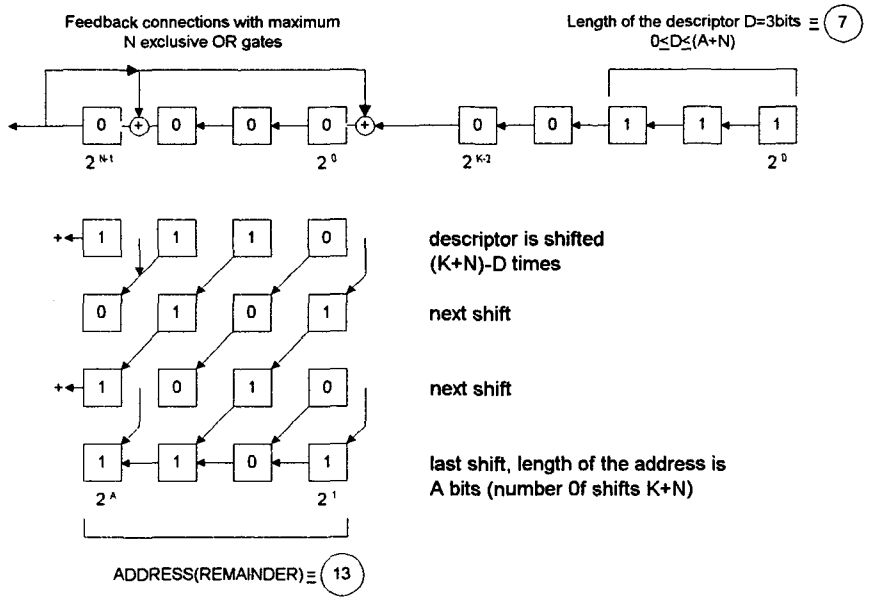
구인수* · 김환우*

* 한국원자력연구소, 충남대학교

Abstract

기존의 의사 랜덤 디지틀 변환(pseudo-random digital transformation)은 배타적 합 게이트(exclusive OR gates)를 이용한 궤환회로와 쉬프트레지스터(shift register)로 구성한다. 이와같이 기존의 변환방법은 온라인상에서 간단히 하드웨어 구성만으로도 구현이 가능한 장점 때문에 계속 이용한다. 따라서, 본 논문은 기존 의사랜덤 디지틀 변환의 하드웨어적 장점을 유지하면서 변환시 발생가능한 랜덤성의 소멸을 방지하는 혼돈적 랜덤 디지틀 변환기법에 관해 기술한다.

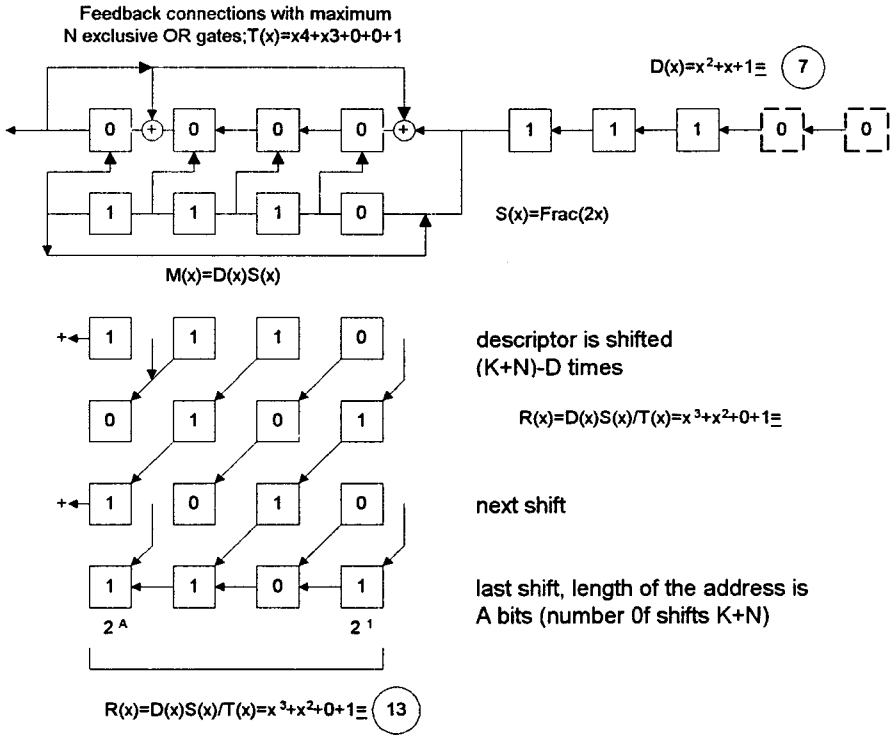
전자회로에서 회로변수의 변화를 의미하는 신호를 기술자(descriptor)라 부르는 디지틀 수(digital number)로 표현하였으며, 기존의 변환과정은 다음과 같다.



[그림 1] Generation of pseudo-random address of length A=k bits

그림 1은 기술자를 기존의 의사 랜덤변환으로 발생하는 번지를 지정하는 회로이다. 이 회로의 경우 실제 메모리 번지를 모두 지정할 수 없는 경우가 발생할 수 있다. 다시말하면, 한 주기동안 완전한 랜덤 수 발생이 되지 않을 수 있다는 것이다. 예를 들어, A1, A2, C, D 라고 명명한 기술자는 1, 2, 3, 4 라는 네 개의 실제 번지를 지정할 수 있어야 하지만, 1, 1, 3, 4라는 번지만을 지정하는 경우가 발생한다.

이와같이 불완전한 랜덤번호 발생을 완전한 랜덤번호 발생을 위해 다음 그림과 같은 카오스적인 랜덤 디지틀 변환회로를 제안한다.



[그림 2] Generation of chaotic random address of length 4 bits

그림 2의 회로에서는 결정론적 혼돈함수(deterministic chaos function)인 베이커함수(Baker's function)를 좌측 쉬프트 레지스터로 구현 가능하므로, 변환된 기술자 M(x)를 발생하기 위해 원래의 기술자 D(x)에 베이커 함수 S(x)=Frac(2x)를 곱했다.

따라서, 변환된 기술자 M(x)에 의해 혼돈적인 번지가 만들어진 것이다. 따라서, 실제 메모리의 모든 번지를 혼돈적으로 지정하므로써 지정하지 않는 번지의 존재는 없을 것이다.