



(19) 대한민국특허청(KR)

(12) 등록특허공보(B1)

(45) 공고일자 2016년01월08일

(11) 등록번호 10-1583471

(24) 등록일자 2016년01월04일

(51) 국제특허분류(Int. Cl.)

G06F 7/58 (2006.01)

(21) 출원번호 10-2014-0194688

(22) 출원일자 2014년12월31일

심사청구일자 2014년12월31일

(56) 선행기술조사문헌

KR101401953 B1

JP2008197847 A

(73) 특허권자

고려대학교 산학협력단

서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)

(72) 발명자

손창환

서울특별시 마포구 와우산로 12, 810호 (상수동, 제이캐슬레지던스)

표창우

서울특별시 강남구 압구정로29길 68, 72동 901호 (압구정동, 현대아파트)

(74) 대리인

특허법인충현

전체 청구항 수 : 총 7 항

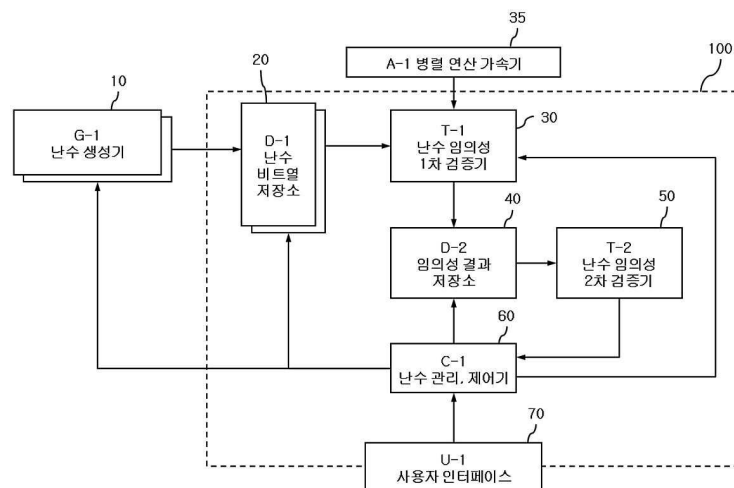
심사관 : 지정훈

(54) 발명의 명칭 임의성을 검증하는 통계적 기법을 이용하여 난수를 공급하는 장치 및 방법

(57) 요약

본 발명은 임의성을 검증하는 통계적 기법을 이용하여 난수를 공급하는 장치에 관한 것으로, 난수 생성기를 이용하여 생성된 난수 비트(bit)열을 저장하는 난수 비트열 저장소, 난수 비트열 저장소로부터 난수 비트열을 독출하여 복수 개의 임의성 검증 알고리즘에 따라 검증을 수행하고 각각의 검증 알고리즘별로 검증 결과를 산출하여 임의성 결과 저장소에 저장하는 제 1 난수 임의성 검증기, 임의성 결과 저장소로부터 각각의 알고리즘별 검증 결과를 독출하여 통계적 분포값을 산출하고 산출된 통계적 분포값이 미리 설정된 통계적 임의성을 만족하는지 여부를 검사하는 제 2 난수 임의성 검증기 및 통계적 임의성 검사 결과에 기초하여 검증된 난수를 제공하는 제어기를 포함한다.

대표도 - 도1



이 발명을 지원한 국가연구개발사업

과제고유번호 1711015820

부처명 미래창조과학부

연구관리전문기관 정보통신산업진흥원

연구사업명 2014 대학IT 연구센터육성 지원사업

연구과제명 고품질 융합 소프트웨어 개발지원 도구 연구

기 여 율 1/1

주관기관 고려대학교 산학협력단

연구기간 2014.01.01 ~ 2014.12.31

명세서

청구범위

청구항 1

적어도 하나의 프로세서(processor) 및 저장 장치를 이용하여 난수를 공급하는 장치에 있어서,

난수 생성기를 이용하여 생성된 난수 비트(bit)열을 저장하는 난수 비트열 저장소;

상기 난수 비트열 저장소로부터 난수 비트열을 독출하여 복수 개의 임의성 검증 알고리즘에 따라 검증을 수행하고, 각각의 검증 알고리즘별로 검증 결과를 산출하여 임의성 결과 저장소에 저장하는 제 1 난수 임의성 검증기;

상기 임의성 결과 저장소로부터 각각의 알고리즘별 검증 결과를 독출하여 통계적 분포값을 산출하고, 산출된 통계적 분포값이 미리 설정된 통계적 임의성을 만족하는지 여부를 검사하는 제 2 난수 임의성 검증기; 및

상기 통계적 임의성 검사 결과에 기초하여 검증된 난수를 제공하는 제어기;를 포함하는 난수 공급 장치.

청구항 2

제 1 항에 있어서,

상기 제 1 난수 임의성 검증기는,

상기 난수 비트열 저장소로부터 독출된 난수 비트열에 복수 개의 임의성 검증 알고리즘에 따라 일정 크기 단위로 검증을 수행하고, 각각의 검증 알고리즘에 대한 식별자와 산출된 검증 결과를 매칭하여 상기 임의성 결과 저장소에 저장하는 것을 특징으로 하는 난수 공급 장치.

청구항 3

제 2 항에 있어서,

상기 검증 알고리즘은,

NIST SP800-22 규격에 따른 검증 알고리즘을 포함하는 것을 특징으로 하는 난수 공급 장치.

청구항 4

제 1 항에 있어서,

상기 제 2 난수 임의성 검증기는,

상기 임의성 결과 저장소로부터 독출된 각각의 알고리즘별 검증 결과들에 대하여 유의 수준을 나타내는 임계값 이상에 해당하는 빈도의 비율을 산출하고, 산출된 비율이 미리 설정된 통계적 임의성 기준을 만족하는지 여부를 검사하는 것을 특징으로 하는 난수 공급 장치.

청구항 5

제 1 항에 있어서,

상기 제 2 난수 임의성 검증기는,

상기 임의성 결과 저장소로부터 독출된 각각의 알고리즘별 검증 결과들에 대한 분포도를 산출하고, 상기 산출된 분포도의 분포 히스토그램이 미리 설정된 통계적 임의성 기준을 만족하는지 여부를 검사하는 것을 특징으로 하는 난수 공급 장치.

청구항 6

제 1 항에 있어서,

상기 난수 생성기를 통해 생성되는 난수 비트열은, 상기 제 2 난수 임의성 검증기가 요구하는 난수 공급의 수보다 상대적으로 더 많은 개수만큼 생성되는 것을 특징으로 하는 난수 공급 장치.

청구항 7

제 1 항에 있어서,

상기 제 2 난수 임의성 검증기를 통한 검사 결과 통계적 임의성을 만족하지 못한 경우, 상기 난수 비트열 저장소에 저장된 난수 비트열 중 가장 먼저 생성된 난수 비트열을 삭제하고, 삭제된 난수 비트열에 대한 검증 결과를 삭제하는 것을 특징으로 하는 난수 공급 장치.

발명의 설명

기술 분야

[0001]

본 발명은 난수 생성기를 활용한 전산 환경에 관한 기술로, 특히 난수 생성기를 사용하는 응용 프로그램 또는 전산 시스템에서 임의성을 검증함으로써 품질이 보장된 난수를 사용자 내지 시스템이 요구하는만큼 공급하는 난수 공급 장치, 방법 및 그 방법을 기록한 컴퓨터로 읽을 수 있는 기록매체에 관한 것이다.

배경 기술

[0002]

암호학적 응용에서는 이진 난수 비트열(binary random number bit sequence)을 키로 사용한다. 이진 난수의 품질은 실행되는 응용 프로그램뿐만 아니라 그 응용이 실행되는 시스템의 보안 수준을 결정하는 중요 인자로 작용한다. 예측하기 쉬운 이진 난수는 무작위 대입 공격(brute-force attack)에 의해 쉽게 해독될 수 있는 위험이 있다. 이러한 난수의 예측 가능성은 조합적 알고리즘(combinatorial algorithm)으로는 판정하기 어려우며, 통계적 방법으로 검증 가능하다.

[0003]

난수의 임의성을 통계적인 실험을 통해 검증하고자 작성된 대표적인 검증 도구로 이하의 선행기술문헌을 통해 제시되는 NIST 통계적 난수 검증 모음이 있다. 이 프로그램은 생성된 이진 난수 열을 입력값으로 하여 15 가지 검증 방법이 주는 실험값을 통해 난수의 품질을 측정한다. 특히, 통계적인 방법으로 난수의 예측 불가능한 정도인 임의성을 검증하는 방법이 활용 가능하다.

[0004]

그러나, 통계적 검증 방법들은 난수 생성기에서 생성된 일정 길이의 난수를 입력받아 난수의 품질을 측정하므로 지속적으로 난수 생성기가 품질이 좋은 난수를 발생시키는지를 보장하지는 않는다. 따라서, 암호학적 응용 분야에서 지속적으로 통계적 임의성이 보장된 난수를 공급할 수 있는 기술적 수단의 제시가 요구된다.

선행기술문헌

비특허문헌

[0005]

(비특허문헌 0001) "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications", A. Rukhin, et al. (2010, April)

발명의 내용

해결하려는 과제

[0006]

본 발명이 해결하고자 하는 기술적 과제는, 기존의 난수 공급 시스템이 난수 생성기에서 생성되는 난수 비트열의 통계적 임의성을 검증하지 않고 있다는 문제를 해소하고, 통계적 검증 방법의 경우에도 난수 공급의 관점에서 임의성이 검증된 난수의 발생을 보장하지 않는다는 한계를 극복하고자 한다.

과제의 해결 수단

[0007]

상기 기술적 과제를 해결하기 위하여, 본 발명의 일 실시예에 따른 적어도 하나의 프로세서(processor) 및 저장장치를 이용하여 난수를 공급하는 장치는, 난수 생성기를 이용하여 생성된 난수 비트(bit)열을 저장하는 난수 비트열 저장소; 상기 난수 비트열 저장소로부터 난수 비트열을 독출하여 복수 개의 임의성 검증 알고리즘에 따라 검증을 수행하고, 각각의 검증 알고리즘별로 검증 결과를 산출하여 임의성 결과 저장소에 저장하는 제 1 난수 임의성 검증기; 상기 임의성 결과 저장소로부터 각각의 알고리즘별 검증 결과를 독출하여 통계적 분포값을 산출하고, 산출된 통계적 분포값이 미리 설정된 통계적 임의성을 만족하는지 여부를 검사하는 제 2 난수 임의성

검증기; 및 상기 통계적 임의성 검사 결과에 기초하여 검증된 난수를 제공하는 제어기;를 포함한다.

- [0008] 일 실시예에 따른 상기 난수 공급 장치에서, 상기 제 1 난수 임의성 검증기는, 상기 난수 비트열 저장소로부터 독출된 난수 비트열에 복수 개의 임의성 검증 알고리즘에 따라 일정 크기 단위로 검증을 수행하고, 각각의 검증 알고리즘에 대한 식별자와 산출된 검증 결과를 매칭하여 상기 임의성 결과 저장소에 저장할 수 있다.
- [0009] 일 실시예에 따른 상기 난수 공급 장치에서, 상기 제 2 난수 임의성 검증기는, 상기 임의성 결과 저장소로부터 독출된 각각의 알고리즘별 검증 결과들에 대하여 유의 수준을 나타내는 임계값 이상에 해당하는 빈도의 비율을 산출하고, 산출된 비율이 미리 설정된 통계적 임의성 기준을 만족하는지 여부를 검사할 수 있다.
- [0010] 또한, 일 실시예에 따른 상기 난수 공급 장치에서, 상기 제 2 난수 임의성 검증기는, 상기 임의성 결과 저장소로부터 독출된 각각의 알고리즘별 검증 결과들에 대한 분포도를 산출하고, 상기 산출된 분포도의 분포 히스토그램이 미리 설정된 통계적 임의성 기준을 만족하는지 여부를 검사할 수 있다.
- [0011] 나아가, 일 실시예에 따른 상기 난수 공급 장치에서, 상기 난수 생성기를 통해 생성되는 난수 비트열은, 상기 제 2 난수 임의성 검증기가 요구하는 난수 공급의 수보다 상대적으로 더 많은 개수만큼 생성될 수 있다.
- [0012] 한편, 일 실시예에 따른 상기 난수 공급 장치에서, 상기 제 2 난수 임의성 검증기를 통한 검사 결과 통계적 임의성을 만족하지 못한 경우, 상기 난수 비트열 저장소에 저장된 난수 비트열 중 가장 먼저 생성된 난수 비트열을 삭제하고, 삭제된 난수 비트열에 대한 검증 결과를 삭제할 수 있다.
- [0013] 나아가, 이하에서는 상기 기재된 난수 공급 장치의 각 구성요소를 제어하는 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공한다.

발명의 효과

- [0014] 본 발명의 실시예들은, 난수 생성기를 통해 생성한 난수 그대로를 시스템의 요구에 따라 공급하는 것이 아니라 통계적인 임의성을 검증한 후 검증된 난수만을 공급하며 난수 생성기에 검증 장치를 추가하여 지속적으로 임의성 검증을 수행함으로써, 그 검증 결과를 바탕으로 통계적 임의성이 보장된 난수를 지속적으로 공급하는 것이 가능하며, 결과적으로 암호학적 응용 분야에서 난수 공급에 관한 신뢰도를 향상시킬 수 있다.

도면의 간단한 설명

- [0015] 도 1은 본 발명의 일 실시예에 따른 임의성을 검증하는 통계적 기법을 이용하여 난수를 공급하는 장치를 도시한 블록도이다.
- 도 2는 본 발명의 일 실시예에 따른 도 1의 난수 공급 장치의 제 1 난수 임의성 검증기의 내부 구성을 보다 구체적으로 도시한 블록도이다.
- 도 3a 및 도 3b는 본 발명의 일 실시예에 따른 도 1의 난수 공급 장치의 제 2 난수 임의성 검증기의 내부 구성을 보다 구체적으로 도시한 블록도이다.
- 도 4는 본 발명의 일 실시예에 따른 도 1의 난수 공급 장치에서 개별 구성 요소들 간의 제어 신호 및 주요 데이터의 이동 경로를 설명하기 위한 도면이다.
- 도 5는 본 발명의 일 실시예에 따른 임의성을 검증하는 통계적 기법을 이용하여 난수를 공급하는 방법을 도시한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

- [0016] 본 발명의 실시예들을 구체적으로 설명하기에 앞서, 상기된 종래의 난수 공급 수단 내지 단순한 난수 검증 방법에 수반된 문제점을 해결하기 위해 본 발명의 실시예들이 채택하고 있는 기술적 수단을 개괄적으로 소개하도록 한다.
- [0017] 앞서 약술한 바와 같이, 통계적인 방법으로 난수의 예측 불가능 정도인 임의성을 검증하는 방법(예를 들어, NIST SP800-22, diehard 또는 TestU01 등이 있다.)이 존재하나, 이러한 통계적 검증 방법들은 난수 생성기에서 생성된 일정 길이의 난수를 입력받아서, 난수의 품질을 측정하므로 지속적으로 난수 생성기가 품질이 좋은 난수를 발생시키는지를 보장하진 않는다. 따라서, 본 발명의 실시예들이 채택하고 있는 난수 공급 장치는 지속적으로 통계적 임의성이 보장된 난수를 공급하는 다음과 같은 기술적 수단을 제안하고자 한다.

- [0018] 첫째, 임의의 난수 생성기에 대해서 통계적 임의성 검증 장치를 추가함으로써, 지속적으로 통계적인 임의성이 검증되어 품질이 좋은 난수를 공급하고자 한다.
- [0019] 둘째, 제어 수단을 통해 난수 비트열의 임의성 검증 결과에 따라서 난수를 생성하고, 검증하며, 공급을 관리하고자 한다.
- [0020] 셋째, 검증 수단에 병렬 연산 가속기를 추가함으로써 향상된 검증 속도로 임의성을 검증한 후 난수를 공급하고자 한다.
- [0021] 넷째, 난수 비트열을 통계적 임의성 검증을 위한 개수보다 상대적으로 더 많이 생성한 후 미리 검증함으로써, 임의성의 검증 후 검증 결과에 따른 재생성 및 검증으로 인해 발생할 수 있는 실행 속도의 저하 문제를 감소시키고자 한다.
- [0022] 이하에서는, 도면을 참조하여 상기된 기술적 과제를 해결하기 위한 본 발명의 실시예들을 구체적으로 설명한다. 다만, 하기의 설명 및 첨부된 도면에서 본 발명의 요지를 흐릴 수 있는 공지 기능 또는 구성에 대한 상세한 설명은 생략한다. 또한, 도면 전체에 걸쳐 동일한 구성 요소들은 가능한 한 동일한 명칭 및 도면 부호로 나타내고 있음에 유의하여야 한다.
- [0023] 도 1은 본 발명의 일 실시예에 따른 임의성을 검증하는 통계적 기법을 이용하여 난수를 공급하는 장치를 도시한 블록도로서, 적어도 하나의 프로세서(processor) 및 저장 장치를 이용하여 구현 가능하다. 여기서, 프로세서는 일련의 난수의 검증 과정을 수행하여, 그 중간 산출물 내지 최종 산출물을 물리적인 저장 장치에 저장하거나 이로부터 데이터를 독출할 수 있다.
- [0024] 도 1을 참조하면, 난수 생성기(10)와 검증된 난수 공급 장치(100), 그리고 선택적으로 병렬 연산 가속기(35)가 도시되어 있다.
- [0025] 먼저, 난수 생성기(10)는 임의의 난수를 생성하여 검증된 난수 공급 장치(100)에 공급하는 구성으로서, 필요에 따라서는 검증된 난수 공급 장치(100) 내에 포함될 수도 있으나, 통상적인 난수 생성 수단 내지 알고리즘이 활용될 수도 있다. 이러한 난수 생성기(10)는 지속적으로 난수 비트를 생성하여 난수 비트열 저장소(20)에 저장하며, 비-알고리즘적 난수 발생기 및 의사 난수 발생기가 활용 가능하다.
- [0026] 난수 비트열 저장소(20)는, 난수 생성기(10)를 이용하여 생성된 난수 비트(bit)열을 저장하는 구성으로서, 상기 난수 생성기(10)를 통해 생성되는 난수 비트열은, 이후 설명할 제 2 난수 임의성 검증기(50)가 요구하는 난수 공급의 수보다 상대적으로 더 많은 개수만큼 생성되는 것이 바람직하다.
- [0027] 이러한 난수 비트열 저장소(20)는, 난수 생성기(10)에서 생성된 난수 비트열을 저장함에 있어서, 예를 들어 1,000,000 비트의 길이와 1,000개 이상의 개수를 갖는 난수 비트열을 저장할 수 있다. 특히, 난수 비트열 저장소(20)는 제 1 난수 임의성 검증기(30)에서 검증하는 크기에 따라 난수 비트열을 나누어 식별자를 부여하되, 제 1 난수 임의성 검증기(30) 및 난수 관리, 제어기(60)에서 난수 비트열을 요청할 경우, 저장된 순서대로 난수 비트열을 전달할 수 있다.
- [0028] 제 1 난수 임의성 검증기(30)는, 상기 난수 비트열 저장소(20)로부터 난수 비트열을 독출하여 복수 개의 임의성 검증 알고리즘에 따라 검증을 수행하고, 각각의 검증 알고리즘별로 검증 결과를 산출하여 임의성 결과 저장소(40)에 저장한다. 제 1 난수 임의성 검증기(30)는 난수 비트열 저장소(20)에 저장된 난수 비트열의 임의성을 일정 크기 단위로 검증하는데, 1,000,000 비트가 권장된다.
- [0029] 이러한 제 1 난수 임의성 검증기(30)는, 상기 난수 비트열 저장소(20)로부터 독출된 난수 비트열에 복수 개의 임의성 검증 알고리즘에 따라 일정 크기 단위로 검증을 수행하고, 각각의 검증 알고리즘에 대한 식별자와 산출된 검증 결과를 매칭하여 상기 임의성 결과 저장소(40)에 저장할 수 있다. 보다 구체적인 구성은 이후 도 2를 참조하여 기술하도록 한다.
- [0030] 또한, 제 1 난수 임의성 검증기(30)에서 상기 검증 알고리즘은, 난수의 임의성 검증 알고리즘을 사용할 수 있는데, 예를 들어 NIST SP800-22 규격에 따른 15 가지 검증 알고리즘을 포함하는 것이 바람직하다. 그러면, 제 1 난수 임의성 검증기(30)는 각각의 알고리즘을 사용한 검증 결과인 P-value를 계산해내어 임의성 결과 저장소(40)에 저장한다.
- [0031] 한편, 병렬 연산 가속기(35)는, 병렬 연산을 수행할 수 있는 가속기로서, 제 1 난수 임의성 검증기(30)의 보다 빠른 검증 시간을 보장하기 위해 GPGPU기술(OpenCL, CUDA 등이 활용 가능하다.)이 적용된 GPU를 사용할 수

있다.

- [0032] 임의성 결과 저장소(40)는, 제 1 난수 임의성 검증기(30)에서 검증 알고리즘별로 생성된 임의성 검증 결과(P-value)를 저장하는데, 난수 비트열 저장소(20)와 동일한 부여하여 검증 결과(P-value)를 저장하는 것이 바람직하다.
- [0033] 제 2 난수 임의성 검증기(50)는, 상기 임의성 결과 저장소(40)로부터 각각의 알고리즘별 검증 결과를 독출하여 통계적 분포값을 산출하고, 산출된 통계적 분포값이 미리 설정된 통계적 임의성을 만족하는지 여부를 검사한다. 제 2 난수 임의성 검증기(50)는 난수 비트열에 대한 검증 결과를 일정 개수 단위로 검증하는데, 1,000개 단위가 권장된다.
- [0034] 이러한 2차 검증은 각 알고리즘별 검증 결과의 통계적 분포 값이 유의 수준을 만족하는지를 확인하기 위함이며, 예를 들어 'NIST SP800-22' 규격의 "P.4-2, P4-3, 4.2.1 proportion of sequences Passing a Test, 4.2.2 uniform distribution of P-values" 부분을 참조하여 구현 가능하다. 이러한 제 2 난수 임의성 검증기(50)는, 크게 두 가지 방식으로 2차 검증을 수행할 수 있다.
- [0035] 첫째, 제 2 난수 임의성 검증기(50)는, 상기 임의성 결과 저장소(40)로부터 독출된 각각의 알고리즘별 검증 결과들에 대하여 유의 수준을 나타내는 임계값 이상에 해당하는 빈도의 비율을 산출하고, 산출된 비율이 미리 설정된 통계적 임의성 기준을 만족하는지 여부를 검사할 수 있다. 보다 구체적인 구성은 이후 도 3a를 참조하여 기술하도록 한다.
- [0036] 둘째, 제 2 난수 임의성 검증기(50)는, 상기 임의성 결과 저장소(40)로부터 독출된 각각의 알고리즘별 검증 결과들에 대한 분포도를 산출하고, 상기 산출된 분포도의 분포 히스토그램이 미리 설정된 통계적 임의성 기준을 만족하는지 여부를 검사할 수 있다. 보다 구체적인 구성은 이후 도 3b를 참조하여 기술하도록 한다.
- [0037] 난수 관리, 제어기(60)는, 난수의 생성 및 저장, 임의성 검증 과정을 제어하는 역할을 수행하며, 상기 제 2 난수 임의성 검증기(50)를 통해 출력되는 통계적 임의성 검사 결과에 기초하여 검증된 난수를 요청자(예를 들어, 사용자 또는 난수 요청 시스템이 될 수 있다.)에게 제공한다.
- [0038] 사용자 인터페이스(70)는, 사용자로부터 요청을 입력받아 난수 관리, 제어기(60)에게 난수 전달을 요청할 수도 있다. 나아가, 사용자 인터페이스(70)는 현재 난수의 임의성 검증 결과를 요청하여 사용자에게 제공함으로써 사용자로 하여금 그 결과를 볼 수 있도록 유도한다.
- [0039] 한편, 제 2 난수 임의성 검증기(50)를 통한 검사 결과 통계적 임의성을 만족하지 못한 경우, 상기 난수 비트열 저장소(20)에 저장된 난수 비트열 중 가장 먼저 생성된 난수 비트열을 삭제하고, 삭제된 난수 비트열에 대한 검증 결과를 삭제하는 것이 바람직하다. 이러한 일련의 난수 비트열 생성 과정과 검증 과정은 공급의 측면에서 관리될 필요가 있으며, 이후 도 5를 참조하여 전체적인 흐름을 재차 구체적으로 설명하도록 한다.
- [0040] 도 2는 본 발명의 일 실시예에 따른 도 1의 난수 공급 장치의 제 1 난수 임의성 검증기의 내부 구성을 보다 구체적으로 도시한 블록도로서, 통계적 임의성 검증 방법을 구현한 기술적 수단에 해당한다.
- [0041] 이러한 제 1 난수 임의성 검증기(30)는, 앞서 소개한 바와 같이 난수 비트열 저장소(20)에 저장된 난수 비트열을 입력받아, 각 알고리즘별(31)로 알고리즘의 검증 결과인 P-value(32)를 출력하여 임의성 결과 저장소(40)에 저장한다. 이때, 검증 결과인 P-value(32)는 난수 비트열과 검증 방법에 따른 식별자를 적용함으로써 구분하여 임의성 결과 저장소(40)에 저장하는 것이 바람직하다.
- [0042] 도 3a 및 도 3b는 본 발명의 일 실시예에 따른 도 1의 난수 공급 장치의 제 2 난수 임의성 검증기(50)의 내부 구성을 보다 구체적으로 도시한 블록도이다.
- [0043] 도 3a는 유의 수준 통과 비율을 검증하는 방법을 제시하고 있다. 도 3a를 참조하면, k번째 검증 알고리즘에 대해서 모든 난수 비트열에 대한 결과 P-value인 $P(j,k)$ 값들(32)이 유의수준 값 α (51)를 넘는 비율(52)이 통계적 임의성을 만족하는지 여부를 확인(53)하여 그 결과를 난수 관리, 제어기(60)에 전달한다. 구현의 관점에서 이러한 검증 방식은, 예를 들어 'NIST SP800-22' 규격의 "P.4-2, 4.2.1 proportion of sequences Passing a Test" 부분을 참조하여 활용하는 것이 가능하다.
- [0044] 도 3b는 분포도를 검증하는 방법을 제시하고 있다. 도 3b를 참조하면, k번째 검증 알고리즘에 대해서 모든 난수 비트열에 대한 결과 P-value인 $P(j,k)$ 값들(32)의 분포도를 확인한다. 일정한 개수의 범위 구간, 예를 들어 10개 범위($C0:0.0 \sim 0.1$ 미만, $C1:0.1 \sim 0.2$ 미만 ... $C9:0.9 \sim 1.0$ 이하로 설정될 수 있다.)에 해당하는 $P(j,$

k)값의 분포 히스토그램을 통해서 적합성 검증(55)을 수행한 후, 미리 설정된 통계적 임의성을 만족하는지 여부를 확인(56)하여 그 결과를 난수 관리, 제어기(60)에 전달한다.

- [0045] 도 4는 본 발명의 일 실시예에 따른 도 1의 난수 공급 장치에서 개별 구성 요소들 간의 제어 신호 및 주요 데이터의 이동 경로를 설명하기 위한 도면으로서, 실선으로 표시된 선은 데이터의 흐름을 나타내며, 점선으로 표시된 선은 제어의 흐름을 나타낸 것이다. 여기서는 데이터의 흐름을 중심으로 데이터 그 자체의 특성만을 약술하도록 한다.
- [0046] (1) 난수 비트열(E-1)은, 난수 생성기(10)에서 발생한 난수 비트열이다.
- [0047] (2) 난수 비트열 모음(E-2)은, 1차 검증에 필요한 길이의 난수 비트열로서, 1,000,000 비트가 권장된다.
- [0048] (3) 1차 검증 결과(E-3)는, 1차 검증에서 난수 비트열 1개에 대한 각 검증 알고리즘의 결과를 나타내는 것으로, 0.0에서 1.0 사이의 P-value 값을 가진다.
- [0049] (4) 검증 결과 모음(E-4)은, 임의성 검증 알고리즘별로 일정한 개수의 난수 비트열의 P-value 모음을 나타내는 것으로, 각각의 검증별로 1,000개가 권장된다.
- [0050] (5) 2차 검증 결과(E-5)는, 임의성 검증 알고리즘별로 통계적인 방법으로 임의성을 검증한 결과를 나타내는 것으로, P-value의 빈도와 분포에 따라 임의성의 높고 낮음을 판단할 수 있다.
- [0051] 도 5는 본 발명의 일 실시예에 따른 임의성을 검증하는 통계적 기법을 이용하여 난수를 공급하는 방법을 도시한 흐름도이다.
- [0052] S510 단계에서는, 난수 생성기(10)를 통해 난수 비트열 1개를 생성하여 난수 비트열 저장소(20)에 저장하는데, 1,000,000 비트가 권장된다.
- [0053] S520 단계에서는, 제 1 난수 임의성 검증기(30)를 통해 난수 비트열 1개에 대한 임의성을 검증하여 임의성 결과 저장소(40)에 검증 알고리즘별 P-value를 저장한다.
- [0054] 그런 다음, S525 단계를 통해 비트열의 개수가 충분한지 여부를 검사한 후, 조건이 충족될 경우 S530 단계로 진행하고, 조건이 충족되지 못한 경우 S510 단계로 되돌아가 비트열의 생성을 반복한다.
- [0055] S530 단계에서는, 제 2 난수 임의성 검증기(50)를 통해 검증 알고리즘별 P-value에 대한 2차 임의성 검증을 수행하고, 난수 관리, 제어기(60)에 그 결과를 전달하여 2차 검증 결과를 확인한다.
- [0056] 이제, S535 단계를 통해 미리 설정된 임의성이 충분하다고 판단된 경우 S540 단계로 진행하며, 그렇지 못한 경우 S550 단계로 진행한다.
- [0057] S540 단계에서는, 임의성이 충족되었다는 전제 하에, 난수 관리, 제어기(60)를 통해 난수를 공급할 준비를 완료하며, 사용자 인터페이스(70)를 통해 난수 공급 준비가 완료되었음을 알린다.
- [0058] 반면, S550 단계에서는, 임의성이 충족되지 못하였으므로, 난수 비트열 저장소(20)에 저장된 난수 비트열 중에서 가장 먼저 생성된 난수 비트열을 삭제하고, 임의성 결과 저장소(40)에 저장된 검증 결과 중 앞서 삭제된 난수 비트열에 대한 검증 결과 또한 삭제한 후, S510 단계로 진행하여 새로운 난수 비트열을 생성하게 된다.
- [0059] S560 단계에서는, 사용자 인터페이스(70)를 통해 사용자로부터 난수 비트열을 요청받을 수 있으며, S570 단계에서 난수 관리, 제어기(60)를 통해 난수 비트열 저장소(20)에 요청한 비트 개수를 전달한다. 또한, S570 단계에서 난수 비트열 저장소(20)는 사용자 인터페이스(70)를 통해 사용자에게 난수 비트열을 전달한 후 해당 난수 비트열을 삭제한다.
- [0060] 이제, S575 단계에서는, 난수 비트열 재생성이 필요한지 여부를 검사한 후, 그 결과에 따라 S510 단계로 진행하여 추가적인 난수 비트열을 생성하거나, S540 단계로 진행하여 단지 난수 재생성 없이 난수 공급이 준비되었음을 알린 후 대기할 수 있다.
- [0061] 이상에서, 도 5의 일련의 연산 과정을 각각 '난수 생성', '난수 검증' 및 '난수 공급'의 관점에서 정리하면 다음과 같다.
- [0062] (1) '난수 생성-검증' 과정
- [0063] - 1 단계: 길이가 1,000,000 비트인 난수 비트열을 생성한다.

- [0064] - 2 단계: 난수 비트열 1개에 대한 1차 임의성을 검증하여 P-value를 수집한다.
- [0065] - 3 단계: 이상의 1-2단계를 병렬 수행할 수도 있다.
- [0066] - 4 단계: 1,000개의 난수 비트열의 1차 검증 결과인 P-value를 2차 검증한다.
- [0067] - 5 단계: 만약 통계적 임의성이 충분하면 공급 대기 및 공급 요청 시 이후의 7 단계를 수행할 수 있다.
- [0068] - 6 단계: 만약 통계적 임의성이 불충분이면 먼저 생성된 순으로 일정 개수의 난수 비트열을 폐기한 후 1 단계에서부터 각 과정을 반복한다.
- [0069] (2) '난수 공급' 과정
- [0070] - 7 단계: 요청된 비트 수만큼 난수를 공급하되, 먼저 생성된 난수 비트열 순으로 난수 비트열 저장소로부터 난수 비트열을 독출하여 공급한 후 해당 난수 비트열을 제거한다.
- [0071] - 8 단계: 사용된 난수 비트열 개수만큼 난수 비트열을 생성하되, 1 단계에서부터 각 과정을 반복한다.
- [0072] 이상과 같은 난수 비트열의 생성 과정은 단지 요구된 1,000개에 대해서만 수행하는 것이 아니라, 난수 생성기가 생성하는 품질에 따라 일정 길이의 버퍼를 두어 미리 생성하는 것이 바람직하다.
- [0073] 한편, 구현의 관점에서 본 발명의 실시예들이 채택하고 있는 임의성 검증 비트 수(난수 비트열 길이를 의미한다.)와 난수 비트열의 개수는, NIST의 권장에 따라 각각 1,000,000 비트 이상, 1,000개를 검증하는 것이 바람직하나, 본 발명의 실시예들이 구현되는 환경에 적합하도록 선택될 수 있으며, 상기 예시된 개수에 제한되지 않는다.
- [0074] 또한, 이러한 임의성 검증 비트 수 및 난수 비트열 개수는 난수 관리, 제어기에 의해 제어될 수 있는데, 난수 비트열은 단지 요구되는 개수, 예를 들어 1,000개만을 생성하는 것이 아니라, 난수 생성기가 생성하는 품질에 따라 일정 길이의 버퍼를 두어 미리 생성하는 것이 바람직하다. 보다 구체적인 예로서, 평균 재생성 개수가 10개인 경우, 난수 생성기는 최초에 1,010개의 난수 비트열을 생성하여 1차 검증을 수행하고, 이후 난수를 공급하는 경우 생성된 뒤의 10개를 하나씩 차례대로 사용하여 2차 검증을 수행할 수 있다.
- [0075] 상기된 본 발명의 실시예들은, 난수 생성기를 통해 생성한 난수 그대로를 시스템의 요구에 따라 공급하는 것이 아니라 통계적인 임의성을 검증한 후 검증된 난수만을 공급하며 난수 생성기에 검증 장치를 추가하여 지속적으로 임의성 검증을 수행함으로써, 그 검증 결과를 바탕으로 통계적 임의성이 보장된 난수를 지속적으로 공급하는 것이 가능하며, 결과적으로 암호학적 응용 분야에서 난수 공급에 관한 신뢰도를 향상시킬 수 있다. 나아가, 병렬 연산 가속기를 사용하여 고속으로 검증을 수행할 수 있으므로 빠른 난수 검증 및 공급 속도를 가진다.
- [0076] 한편, 본 발명의 실시예들에서 난수 공급 장치의 각 구성요소를 제어하는 일련의 연산 방법은 컴퓨터로 읽을 수 있는 기록 매체에 컴퓨터가 읽을 수 있는 코드로 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록 매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다.
- [0077] 컴퓨터가 읽을 수 있는 기록 매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광 데이터 저장장치 등이 있으며, 또한 캐리어 웨이브(예를 들어 인터넷을 통한 전송)의 형태로 구현하는 것을 포함한다. 또한, 컴퓨터가 읽을 수 있는 기록 매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산 방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다. 그리고 본 발명을 구현하기 위한 기능적인(functional) 프로그램, 코드 및 코드 세그먼트들은 본 발명이 속하는 기술 분야의 프로그래머들에 의하여 용이하게 추론될 수 있다.
- [0078] 이상에서 본 발명에 대하여 그 다양한 실시예들을 중심으로 살펴보았다. 본 발명에 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

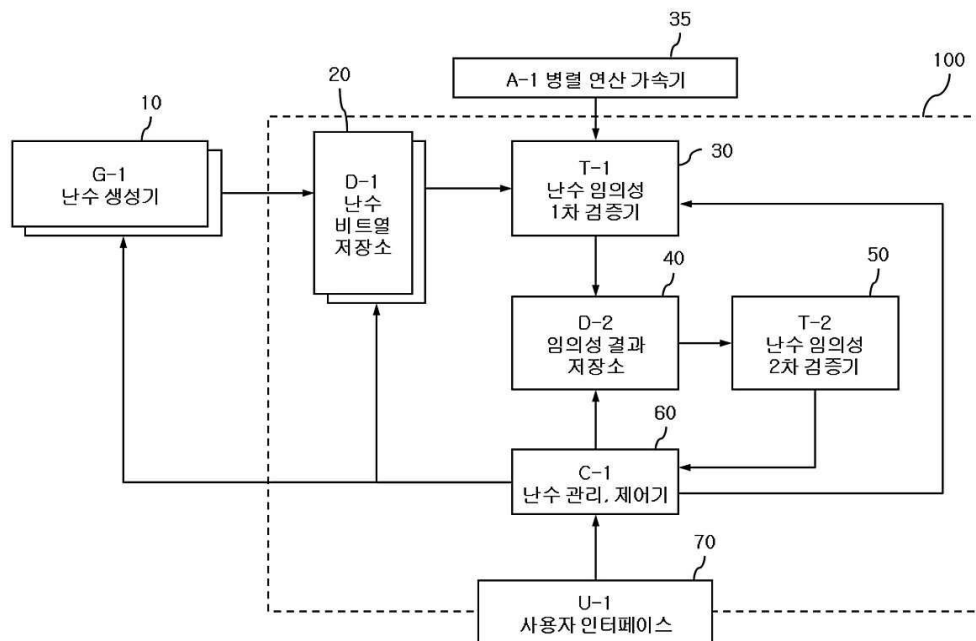
부호의 설명

- [0079] 10 : 난수 생성기
- 100 : 검증된 난수 공급 장치

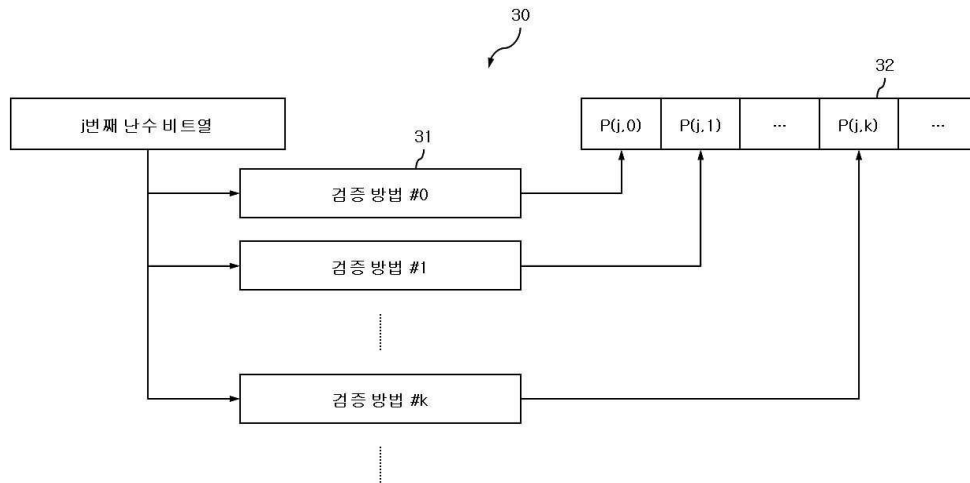
- 20 : 난수 비트열 저장소
- 30 : 제 1 난수 임의성 검증기
- 35 : 병렬 연산 가속기
- 40 : 임의성 결과 저장소
- 50 : 제 2 난수 임의성 검증기
- 60 : 난수 관리 및 제어기
- 70 : 사용자 인터페이스

도면

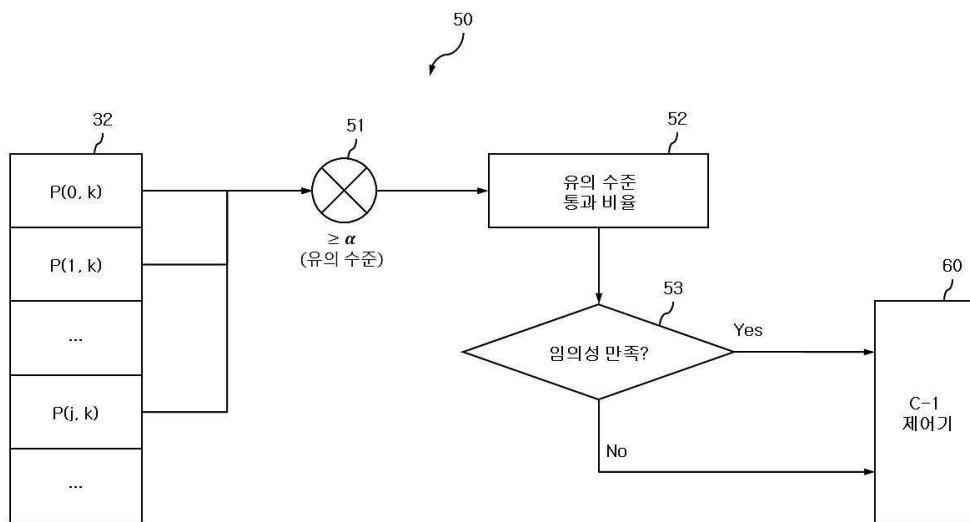
도면1



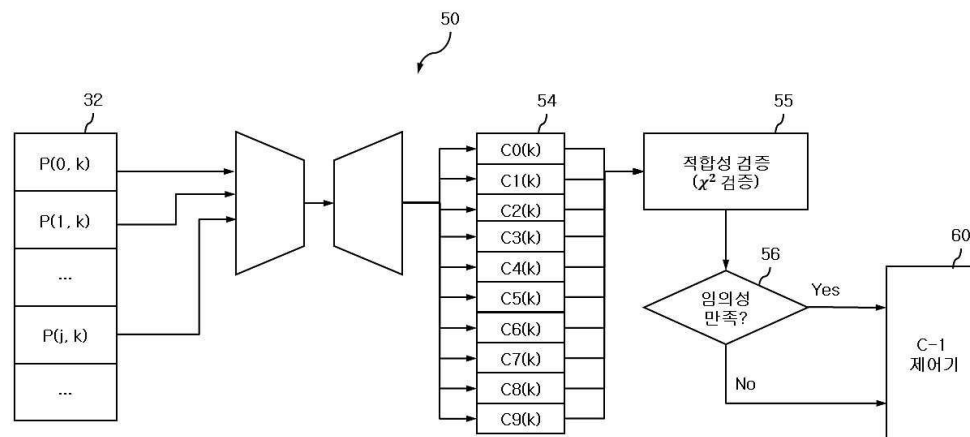
도면2



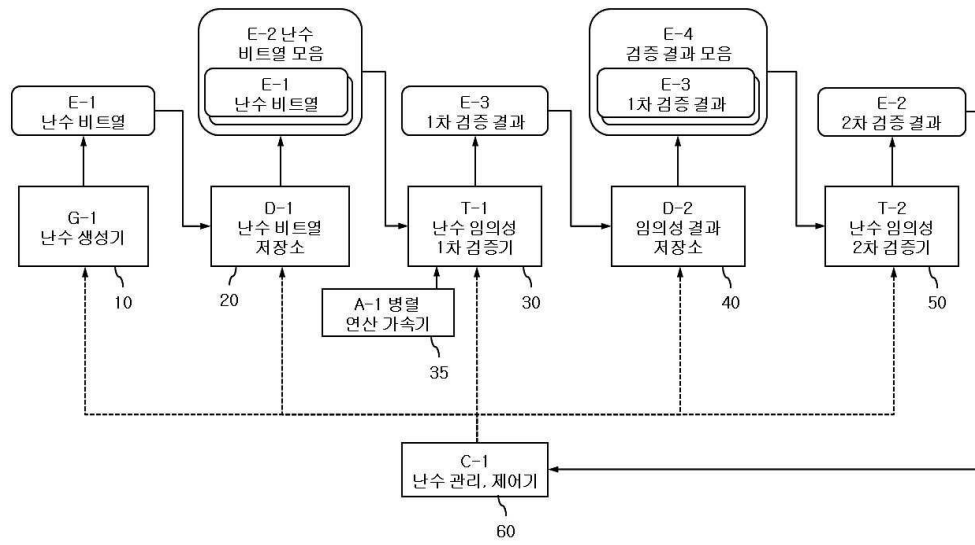
도면3a



도면3b



도면4



도면5

