(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2020 년 1 월 9 일 (09.01.2020)

WIPO | PCT

(10) 국제공개번호
WO 2020/009265 A1

(51) 국제특허분류:
G06F 7/58 (2006.01)

(21) 국제출원번호: PCT/KR2018/008747

(22) 국제출원일: 2018 년 8 월 1 일 (01.08.2018)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2018-0077620 2018 년 7 월 4 일 (04.07.2018) KR
10-2018-0088998 2018 년 7 월 31 일 (31.07.2018) KR

(71) 출원인: 주식회사 넘버스 (**NUMBERS INC.**) [KR/KR]; 13494 경기도 성남시 분당구 대왕판교로 670, 비동 1001 호, Gyeonggi-do (KR).

(72) 발명자: 문영오 (**MOON, Young Oh**); 11353 경기도 동두천시 강변로 160, 101동 1302호, Gyeonggi-do (KR). 전성구 (**JEON, Sung Gu**); 16884 경기도 용인시 처인구 모현읍 오포로25번길 6-3, 401동 201호, Gyeonggi-do (KR).

(74) 대리인: 특허법인 다해 (**DAHAI INTERNATIONAL PATENT & LAW FIRM**); 06156 서울시 강남구 삼성로 531 고운빌딩 3층, Seoul (KR).

(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

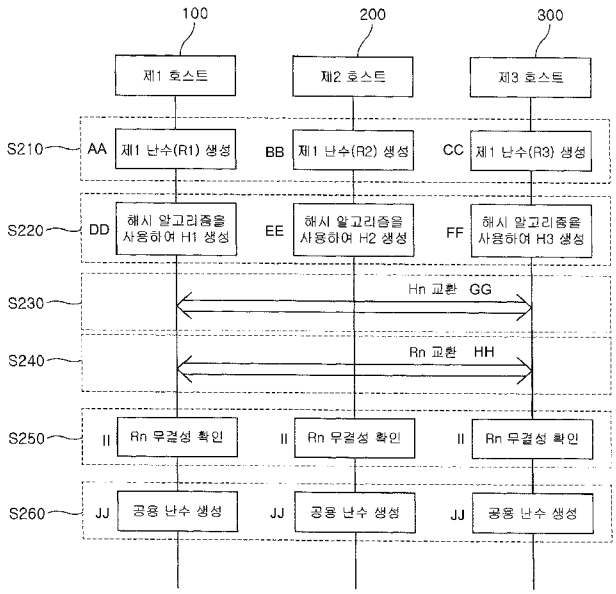
(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

공개:
— 국제조사보고서와 함께 (조약 제21조(3))

WO 2020/009265 A1

(54) Title: METHOD AND SYSTEM FOR GENERATING RANDOM NUMBERS

(54) 발명의 명칭: 난수 생성 방법 및 시스템



100 ... First host
200 ... Second host
300 ... Third host
AA ... Generate first random number (R1)
BB ... Generate first random number (R2)
CC ... Generate first random number (R3)
DD ... Generate H1 by using hash algorithm
EE ... Generate H2 by using hash algorithm
FF ... Generate H3 by using hash algorithm
GG ... Exchange Hn
HH ... Exchange Rn
II ... Verify Rn integrity
JJ ... Generate public random number

(57) Abstract: A method and system for generating random numbers are disclosed. The system for generating random numbers comprises N hosts connected with one another through a network, in which N is a natural number equal to two or greater, wherein each of the N hosts may generate and encode a private random number and then transmit the encoded private random number to (N-1) hosts, and the N hosts may decode the encoded private random numbers received from the (N-1) hosts, and then generate a public random number by using, as factors, the private random number generated by itself and the private random numbers decoded after being received from the (N-1) hosts.

(57) 요약서: 난수 생성 방법 및 시스템이 개시된다. 상기 난수 생성 시스템은, 네트워크를 통해 서로 연결된 N개의 호스트를 포함하고, N은 2 이상의 자연수이며, 상기 N개의 호스트는 각각 개별 난수를 생성 및 암호화한 후 암호화된 개별 난수를 N-1개의 호스트에게 송신하고, 상기 N개의 호스트는 각각 N-1개의 호스트로부터 수신한 암호화된 개별 난수를 복호화한 후, 자신이 생성한 개별 난수와 상기 N-1개의 호스트로부터 수신하여 복호화한 개별 난수를 인자로 사용하여 공용 난수를 생성할 수 있다.

명세서

발명의 명칭: 난수 생성 방법 및 시스템

기술분야

[1] 본 출원은 난수 생성 방법 및 시스템에 관한 것으로, 구체적으로 개별 호스트에서 생성한 난수(Private Random Number)를 암호화, 교환, 검증, 조합을 통해 예측 불가능하고 공정한 공용 난수(Public Random Number)를 생성하는 방법과 그 절차를 모두 블록체인에 기록하는 기술에 관한 것이다.

배경기술

[2] 온라인 카지노 등과 같은 온라인 게임에서 가장 문제로 제시되는 것은 기술의 투명성이며, 투명성이 문제로 제시되는 주요 이유는 난수 생성 방식(Random Number Generation; RNG)에 있다.

[3] 종래의 난수 생성 방식은 중앙화되어 있어 조작하기 쉬우며, 이에 따라 게임의 무결성과 공정성을 의심할 수 있다는 문제가 있다.

발명의 상세한 설명

기술적 과제

[4] 당해 기술분야에서는 투명하고 조작 불가능한 방식으로 난수를 생성하기 위한 방안이 요구되고 있다.

과제 해결 수단

[5] 상기 과제를 해결하기 위해서, 본 발명의 일 실시예는 해시 알고리즘을 이용한 난수 생성 방법을 제공한다.

[6] 본 발명의 일 실시예에 따른 해시 알고리즘을 이용한 난수 생성 방법은, N개의 호스트가 각각 개별 난수(Random Number) Rn을 생성하는 단계; 상기 N개의 호스트가 각각 생성한 개별 난수 Rn을 해시 알고리즘에 의해 암호화하여 Hn을 생성하는 단계; 상기 N개의 호스트가 각각 자신을 제외한 N-1개의 호스트에게 Hn을 송신하는 단계; 상기 N개의 호스트가 각각 자신을 제외한 N-1개의 호스트에게 상기 Hn의 해시값 원본에 해당하는 Rn을 송신하는 단계; 상기 N개의 호스트가 각각 N-1개의 호스트로부터 수신 받은 각각의 Hn과 Rn을 인자로 사용하는 해시 알고리즘의 결과 값을 비교하여 Rn의 무결성을 확인하는 단계; 및 상기 N개의 호스트가 각각 자신이 생성한 Rn과 자신을 제외한 N-1개의 호스트가 생성한 Rn을 인자로 사용하여 공용 난수(Public Random Number)를 생성하는 단계를 포함할 수 있다.

[7]

[8] 본 발명의 다른 실시예는 암호화 알고리즘을 이용한 난수 생성 방법을 제공한다.

[9] 본 발명의 다른 실시예에 따른 암호화 알고리즘을 이용한 난수 생성 방법은, N개의 호스트가 각각 개별 난수(Random Number) Rn을 생성하는 단계; 상기

N개의 호스트가 각각 생성한 개별 난수 Rn을 암호화키 Kn을 사용하는 암호화 알고리즘에 의해 암호화하여 En을 생성하는 단계; 상기 N개의 호스트가 각각 자신을 제외한 N-1개의 호스트에게 En을 송신하는 단계; 상기 N개의 호스트가 각각 자신을 제외한 N-1개의 호스트에게 상기 En의 복호화를 위한 암호화키 Kn을 송신하는 단계; 상기 N개의 호스트가 각각 N-1개의 호스트로부터 수신 받은 각각의 En을 암호화키 Kn으로 복호화하여 Rn을 획득하는 단계; 및 상기 N개의 호스트가 각각 자신이 생성한 Rn과 자신을 제외한 N-1개의 호스트가 생성한 Rn을 인자로 사용하여 공용 난수(Public Random Number)를 생성하는 단계를 포함할 수 있다.

[10]

[11] 본 발명의 또 다른 실시예는 난수 생성 시스템을 제공한다.

[12] 본 발명의 또 다른 실시예에 따른 난수 생성 시스템은, 네트워크를 통해 서로 연결된 N개의 호스트를 포함하고, N은 2 이상의 자연수이며, 상기 N개의 호스트는 각각 개별 난수를 생성 및 암호화한 후 암호화된 개별 난수를 N-1개의 호스트에게 송신하고, 상기 N개의 호스트는 각각 N-1개의 호스트로부터 수신한 암호화된 개별 난수를 복호화한 후, 자신이 생성한 개별 난수와 상기 N-1개의 호스트로부터 수신하여 복호화한 개별 난수를 인자로 사용하여 공용 난수를 생성할 수 있다.

[13]

[14] 덧붙여 상기한 과제의 해결수단은, 본 발명의 특징을 모두 열거한 것이 아니다. 본 발명의 다양한 특징과 그에 따른 장점과 효과는 아래의 구체적인 실시형태를 참조하여 보다 상세하게 이해될 수 있을 것이다.

발명의 효과

[15] 본 발명의 실시예에 따르면, 복수의 호스트가 난수 생성에 참여하기 때문에 어느 한 쪽이 유리하도록 난수를 생성하거나, 악의적인 목적을 가지고 난수를 조작하는 것이 불가능해진다.

[16] 또한, 난수 생성 과정이 모두 블록 체인에 기록되므로 언제든지 검증할 수 있게 된다.

도면의 간단한 설명

[17] 도 1은 본 발명의 실시예가 적용되는 난수 생성 시스템의 구성도이다.

[18] 도 2는 본 발명의 일 실시예에 따른 해시 알고리즘을 이용한 난수 생성 방법의 흐름도이다.

[19] 도 3은 본 발명의 다른 실시예에 따른 암호화 알고리즘을 이용한 난수 생성 방법의 흐름도이다.

[20] 도 4는 본 명세서에 개진된 하나 이상의 실시예가 구현될 수 있는 예시적인 컴퓨팅 환경을 도시하는 도면이다.

발명의 실시를 위한 최선의 형태

[21] 이하, 첨부된 도면을 참조하여 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자가 본 발명을 용이하게 실시할 수 있도록 바람직한 실시예를 상세히 설명한다. 다만, 본 발명의 바람직한 실시예를 상세하게 설명함에 있어, 관련된 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략한다. 또한, 유사한 기능 및 작용을 하는 부분에 대해서는 도면 전체에 걸쳐 동일한 부호를 사용한다.

[22] 덧붙여, 명세서 전체에서, 어떤 부분이 다른 부분과 '연결'되어 있다고 할 때, 이는 '직접적으로 연결'되어 있는 경우뿐만 아니라, 그 중간에 다른 소자를 사이에 두고 '간접적으로 연결'되어 있는 경우도 포함한다. 또한, 어떤 구성요소를 '포함'한다는 것은, 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있다는 것을 의미한다.

[23]

[24] 도 1은 본 발명의 실시예가 적용되는 난수 생성 시스템의 구성도이다.

[25] 도 1을 참조하면, 본 발명의 실시예가 적용되는 난수 생성 시스템은 N개의 호스트(예를 들어, 제1 호스트, 제2 호스트, 제3 호스트)(100, 200, 300)를 포함할 수 있다. 여기서, 호스트는 네트워크에 연결되어 있는 컴퓨팅 디바이스일 수 있으며, 호스트의 개수는 N(N>1)일 수 있다. 도 1에서는 호스트의 개수가 3개인 경우를 예를 들어 도시하나, 반드시 이로 제한되는 것은 아니다.

[26] 각각의 호스트(100, 200, 300)는 네트워크를 통해 서로 연결되어 공용 난수 생성을 위해 필요한 정보를 서로 교환할 수 있다.

[27] 각각의 호스트(100, 200, 300)는 개별 난수를 생성하여 이를 암호화한 후, 암호화된 개별 난수를 다른 호스트들에게 송신할 수 있다. 이에 따라, 각각의 호스트(100, 200, 300)는 모든 호스트에서 각각 생성되어 암호화된 개별 난수를 가지게 된다.

[28] 또한, 각각의 호스트(100, 200, 300)는 다른 호스트로부터 수신한 암호화된 개별 난수를 복호화한 후, 자신이 생성한 개별 난수와, 다른 호스트로부터 수신하여 복호화한 개별 난수들을 모두 인자(Seed)로 사용하여 공용 난수(Public Random Number)를 생성할 수 있다.

[29] 또한, 각각의 호스트(100), 200, 300)는 블록체인 기술 기반으로 난수 생성을 위해 수행하는 각 과정을 기록할 수 있다.

[30]

[31] 이하, 도 2 및 도 3을 참조하여 본 발명의 실시예에 따른 난수 생성 방법에 대해 보다 구체적으로 설명한다.

[32]

[33] 도 2는 본 발명의 일 실시예에 따른 해시 알고리즘을 이용한 난수 생성 방법의 흐름도이다. 도 2에서는 호스트의 개수가 3개인 경우를 예를 들어 도시하나, 반드시 이로 제한되는 것은 아니다.

[34] 도 2를 참조하면, 우선 N개의 모든 호스트(100, 200, 300)는 각자 개별

난수(Random Number) Rn을 생성한다(S210).

[35] 이후, N개의 모든 호스트(100, 200, 300)는 각자 생성한 개별 난수 Rn을 해시 알고리즘 hash(Rn)을 사용하여 Hn을 생성한다(S220). 여기서, 해시 알고리즘은 복호화가 불가능한 암호화 기법을 말한다. 그러나, 본 발명에서 개별 난수 Rn을 암호화하는 기법이 반드시 이로 제한되는 것은 아니며, 통상의 기술자에게 알려진 다양한 암호화 기법을 적용하여 개별 난수 Rn을 암호화할 수 있다.

[36] 이후, N개의 모든 호스트(100, 200, 300)는 자신을 제외한 나머지 N-1개의 호스트에게 Hn을 송신하여, 암호화된 개별 난수인 Hn을 서로 교환한다(S230). 예를 들어, 제1 호스트(100)는 제2 호스트(200) 및 제3 호스트(300)에게 H1을 송신하고, 제2 호스트(200)는 제1 호스트(100) 및 제3 호스트(300)에게 H2를 송신하며, 제3 호스트(300)는 제1 호스트(100) 및 제2 호스트(200)에게 H3을 송신할 수 있다. 여기서, 상대방의 개별 난수 Rn은 암호화되어 있어 해독할 수 없으며, 개별 난수 Rn은 더 이상 변경이 불가능한 상태가 된다.

[37] 이후, 도 2에서 도시되지는 않았으나, N개의 모든 호스트(100, 200, 300)는 자신을 제외한 나머지 N-1개의 호스트가 Hn을 수신하였는지 확인할 수 있다.

[38] 이후, N개의 모든 호스트(100, 200, 300)는 자신을 제외한 나머지 N-1개의 호스트에게 Hn의 해시값 원본에 해당하는 Rn을 송신하여, Rn을 서로 교환한다(S240). 예를 들어, 제1 호스트(100)는 제2 호스트(200) 및 제3 호스트(300)에게 R1을 송신하고, 제2 호스트(200)는 제1 호스트(100) 및 제3 호스트(300)에게 R2를 송신하며, 제3 호스트(300)는 제1 호스트(100) 및 제2 호스트(200)에게 R3을 송신할 수 있다.

[39] 이후, 도 2에서 도시되지는 않았으나, N개의 모든 호스트(100, 200, 300)는 자신을 제외한 나머지 N-1개의 호스트가 Rn을 수신하였는지 확인할 수 있다.

[40] 이후, N개의 모든 호스트(100, 200, 300)는 N-1개의 호스트로부터 수신 받은 각각의 Hn과 Rn을 인자로 사용하는 해시 알고리즘의 결과 값을 비교하여 Rn의 무결성을 확인한다(S250). 즉, Hn = hash(Rn) 인지 확인하여 Rn의 무결성을 확인할 수 있다.

[41] 이후, N개의 모든 호스트(100, 200, 300)는 자신이 생성한 Rn과 자신을 제외한 나머지 N-1개의 호스트가 생성한 Rn을 모두 인자(Seed)로 사용하는 공용 난수 생성 함수를 호출하여 공용 난수(Public Random Number)를 생성한다(S260).

[42] 상술한 S210 내지 S260 단계는 모두 블록체인(예를 들어, Smart Contract)에 기록되며, 누구나 검증할 수 있다.

[43] 결과적으로 N개의 모든 호스트에서 생성한 공용 난수는 예측 불가능한 공정한 난수이다. 또한, 상술한 바와 같이 모든 과정이 탈중앙화 되어 있고, 블록체인에 기록되므로 투명한 기술이다.

[44]

[45] 도 3은 본 발명의 다른 실시예에 따른 암호화 알고리즘을 이용한 난수 생성 방법의 흐름도이다. 도 3에서는 호스트의 개수가 3개인 경우를 예를 들어

도시하나, 반드시 이로 제한되는 것은 아니다.

[46] 도 3을 참조하면, 우선 N개의 모든 호스트(100, 200, 300)는 각자 개별 난수(Random Number) Rn을 생성한다(S310).

[47] 이후, N개의 모든 호스트(100, 200, 300)는 각자 생성한 개별 난수 Rn을 암호화 알고리즘 Encrypt(Kn, Rn)을 사용하여 En을 생성한다(S320). 여기서, Kn은 암호화 알고리즘에 사용되는 암호화키를 의미하며, 암호화 알고리즘은 암호화키를 사용한 암호화 알고리즘일 수 있다. 그러나, 본 발명에서 개별 난수 Rn을 암호화하는 기법이 반드시 이로 제한되는 것은 아니며, 통상의 기술자에게 알려진 다양한 암호화 기법을 적용하여 개별 난수 Rn을 암호화할 수 있다.

[48] 이후, N개의 모든 호스트(100, 200, 300)는 자신을 제외한 나머지 N-1개의 호스트에게 En을 송신하여, 암호화된 개별 난수인 En을 서로 교환한다(S330). 예를 들어, 제1 호스트(100)는 제2 호스트(200) 및 제3 호스트(300)에게 E1을 송신하고, 제2 호스트(200)는 제1 호스트(100) 및 제3 호스트(300)에게 E2를 송신하며, 제3 호스트(300)는 제1 호스트(100) 및 제2 호스트(200)에게 E3을 송신할 수 있다. 여기서, 상대방의 개별 난수 Rn은 암호화되어 있어 해독할 수 없으며, 개별 난수 Rn은 더 이상 변경이 불가능한 상태가 된다.

[49] 이후, 도 3에서 도시되지는 않았으나, N개의 모든 호스트(100, 200, 300)는 자신을 제외한 나머지 N-1개의 호스트가 En을 수신하였는지 확인할 수 있다.

[50] 이후, N개의 모든 호스트(100, 200, 300)는 자신을 제외한 나머지 N-1개의 호스트에게 En의 복호화를 위한 암호화키 Kn을 송신하여, Kn을 서로 교환한다(S340). 예를 들어, 제1 호스트(100)는 제2 호스트(200) 및 제3 호스트(300)에게 K1을 송신하고, 제2 호스트(200)는 제1 호스트(100) 및 제3 호스트(300)에게 K2를 송신하며, 제3 호스트(300)는 제1 호스트(100) 및 제2 호스트(200)에게 K3을 송신할 수 있다.

[51] 이후, 도 3에서 도시되지는 않았으나, N개의 모든 호스트(100, 200, 300)는 자신을 제외한 나머지 N-1개의 호스트가 Kn을 수신하였는지 확인할 수 있다.

[52] 이후, N개의 모든 호스트(100, 200, 300)는 N-1개의 호스트로부터 수신 받은 각각의 En을 암호화키 Kn으로 복호화하여 Rn을 획득한다(S350). 즉, Rn = Decrypt(En, Kn)가 성립한다.

[53] 이후, N개의 모든 호스트(100, 200, 300)는 자신이 생성한 Rn과 자신을 제외한 나머지 N-1개의 호스트가 생성한 Rn을 모두 인자(Seed)로 사용하는 공용 난수 생성 함수를 호출하여 공용 난수(Public Random Number)를 생성한다(S360).

[54] 상술한 S310 내지 S360 단계는 모두 블록체인(예를 들어, Smart Contract)에 기록되며, 누구나 검증할 수 있다.

[55] 결과적으로 N개의 모든 호스트에서 생성한 공용 난수는 예측 불가능한 공정한 난수이다. 또한, 상술한 바와 같이 모든 과정이 탈중앙화 되어 있고, 블록체인에 기록되므로 투명한 기술이다.

[56]

[57] 도 4는 본 명세서에 개진된 하나 이상의 실시예가 구현될 수 있는 예시적인 컴퓨팅 환경을 도시하는 도면으로, 상술한 하나 이상의 실시예를 구현하도록 구성된 컴퓨팅 디바이스(1100)를 포함하는 시스템(1000)의 예시를 도시한다. 예를 들어, 컴퓨팅 디바이스(1100)는 개인 컴퓨터, 서버 컴퓨터, 핸드헬드 또는 랩탑 디바이스, 모바일 디바이스(모바일폰, PDA, 미디어 플레이어 등), 멀티프로세서 시스템, 소비자 전자기기, 미니 컴퓨터, 메인프레임 컴퓨터, 임의의 전술된 시스템 또는 디바이스를 포함하는 분산 컴퓨팅 환경 등을 포함하지만, 이것으로 한정되는 것은 아니다.

[58] 컴퓨팅 디바이스(1100)는 적어도 하나의 프로세싱 유닛(1110) 및 메모리(1120)를 포함할 수 있다. 여기서, 프로세싱 유닛(1110)은 예를 들어 중앙처리장치(CPU), 그래픽처리장치(GPU), 마이크로프로세서, 주문형 반도체(Application Specific Integrated Circuit, ASIC), Field Programmable Gate Arrays(FPGA) 등을 포함할 수 있으며, 복수의 코어를 가질 수 있다. 메모리(1120)는 휘발성 메모리(예를 들어, RAM 등), 비휘발성 메모리(예를 들어, ROM, 플래시 메모리 등) 또는 이들의 조합일 수 있다.

[59] 또한, 컴퓨팅 디바이스(1100)는 추가적인 스토리지(1130)를 포함할 수 있다. 스토리지(1130)는 자기 스토리지, 광학 스토리지 등을 포함하지만 이것으로 한정되지 않는다. 스토리지(1130)에는 본 명세서에 개진된 하나 이상의 실시예를 구현하기 위한 컴퓨터 판독 가능한 명령이 저장될 수 있고, 운영 시스템, 애플리케이션 프로그램 등을 구현하기 위한 다른 컴퓨터 판독 가능한 명령도 저장될 수 있다. 스토리지(1130)에 저장된 컴퓨터 판독 가능한 명령은 프로세싱 유닛(1110)에 의해 실행되기 위해 메모리(1120)에 로딩될 수 있다.

[60] 또한, 컴퓨팅 디바이스(1100)는 입력 디바이스(들)(1140) 및 출력 디바이스(들)(1150)을 포함할 수 있다. 여기서, 입력 디바이스(들)(1140)은 예를 들어 키보드, 마우스, 펜, 음성 입력 디바이스, 터치 입력 디바이스, 적외선 카메라, 비디오 입력 디바이스 또는 임의의 다른 입력 디바이스 등을 포함할 수 있다. 또한, 출력 디바이스(들)(1150)은 예를 들어 하나 이상의 디스플레이, 스피커, 프린터 또는 임의의 다른 출력 디바이스 등을 포함할 수 있다. 또한, 컴퓨팅 디바이스(1100)는 다른 컴퓨팅 디바이스에 구비된 입력 디바이스 또는 출력 디바이스를 입력 디바이스(들)(1140) 또는 출력 디바이스(들)(1150)로서 사용할 수도 있다.

[61] 또한, 컴퓨팅 디바이스(1100)는 컴퓨팅 디바이스(1100)가 다른 디바이스(예를 들어, 컴퓨팅 디바이스(1300))와 통신할 수 있게 하는 통신접속(들)(1160)을 포함할 수 있다. 여기서, 통신 접속(들)(1160)은 모뎀, 네트워크 인터페이스 카드(NIC), 통합 네트워크 인터페이스, 무선 주파수 송신기/수신기, 적외선 포트, USB 접속 또는 컴퓨팅 디바이스(1100)를 다른 컴퓨팅 디바이스에 접속시키기 위한 다른 인터페이스를 포함할 수 있다. 또한, 통신 접속(들)(1160)은 유선 접속 또는 무선 접속을 포함할 수 있다.

[62] 상술한 컴퓨팅 디바이스(1100)의 각 구성요소는 버스 등의 다양한 상호접속(예를 들어, 주변 구성요소 상호접속(PCI), USB, 펌웨어(IEEE 1394), 광학적 버스 구조 등)에 의해 접속될 수도 있고, 네트워크(1200)에 의해 상호접속될 수도 있다.

[63] 본 명세서에서 사용되는 "구성요소", "모듈", "시스템", "인터페이스" 등과 같은 용어들은 일반적으로 하드웨어, 하드웨어와 소프트웨어의 조합, 소프트웨어, 또는 실행중인 소프트웨어인 컴퓨터 관련 엔티티를 지칭하는 것이다. 예를 들어, 구성요소는 프로세서 상에서 실행중인 프로세스, 프로세서, 객체, 실행 가능물(executable), 실행 스레드, 프로그램 및/또는 컴퓨터일 수 있지만, 이것으로 한정되는 것은 아니다. 예를 들어, 컨트롤러 상에서 구동중인 애플리케이션 및 컨트롤러 모두가 구성요소일 수 있다. 하나 이상의 구성요소는 프로세스 및/또는 실행의 스레드 내에 존재할 수 있으며, 구성요소는 하나의 컴퓨터 상에서 로컬화될 수 있고, 둘 이상의 컴퓨터 사이에서 분산될 수도 있다.

[64]

[65] 본 발명은 전술한 실시예 및 첨부된 도면에 의해 한정되는 것이 아니다. 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 있어, 본 발명의 기술적 사상을 벗어나지 않는 범위 내에서 본 발명에 따른 구성요소를 치환, 변형 및 변경할 수 있다는 것이 명백할 것이다.

청구범위

[청구항 1] N개의 호스트가 각각 개별 난수(Random Number) Rn을 생성하는 단계;
상기 N개의 호스트가 각각 생성한 개별 난수 Rn을 해시 알고리즘에 의해 암호화하여 Hn을 생성하는 단계;
상기 N개의 호스트가 각각 자신을 제외한 N-1개의 호스트에게 Hn을 송신하는 단계;
상기 N개의 호스트가 각각 자신을 제외한 N-1개의 호스트에게 상기 Hn의 해시값 원본에 해당하는 Rn을 송신하는 단계;
상기 N개의 호스트가 각각 N-1개의 호스트로부터 수신 받은 각각의 Hn과 Rn을 인자로 사용하는 해시 알고리즘의 결과 값을 비교하여 Rn의 무결성을 확인하는 단계; 및
상기 N개의 호스트가 각각 자신이 생성한 Rn과 자신을 제외한 N-1개의 호스트가 생성한 Rn을 인자로 사용하여 공용 난수(Public Random Number)를 생성하는 단계를 포함하며,
N은 2 이상의 자연수인 난수 생성 방법.

[청구항 2] 제 1 항에 있어서,
각 단계는 블록 체인에 기록되는 난수 생성 방법.

[청구항 3] N개의 호스트가 각각 개별 난수(Random Number) Rn을 생성하는 단계;
상기 N개의 호스트가 각각 생성한 개별 난수 Rn을 암호화키 Kn을 사용하는 암호화 알고리즘에 의해 암호화하여 En을 생성하는 단계;
상기 N개의 호스트가 각각 자신을 제외한 N-1개의 호스트에게 En을 송신하는 단계;
상기 N개의 호스트가 각각 자신을 제외한 N-1개의 호스트에게 상기 En의 복호화를 위한 암호화키 Kn을 송신하는 단계;
상기 N개의 호스트가 각각 N-1개의 호스트로부터 수신 받은 각각의 En을 암호화키 Kn으로 복호화하여 Rn을 획득하는 단계; 및
상기 N개의 호스트가 각각 자신이 생성한 Rn과 자신을 제외한 N-1개의 호스트가 생성한 Rn을 인자로 사용하여 공용 난수(Public Random Number)를 생성하는 단계를 포함하며,
N은 2 이상의 자연수인 난수 생성 방법.

[청구항 4] 제 3 항에 있어서,
각 단계는 블록 체인에 기록되는 난수 생성 방법.

[청구항 5] 호스트가 제1 개별 난수를 생성하는 단계;
상기 호스트가 타 호스트로부터 상기 타 호스트에 의해 생성 및 해시 알고리즘에 의해 암호화된 제2 개별 난수를 수신하는 단계;
상기 호스트가 상기 타 호스트로부터 상기 제2 개별 난수를 수신하는 단계;

상기 호스트가 상기 암호화된 제2 개별 난수와 상기 제2 개별 난수를 인자로 사용하는 해시 알고리즘의 결과 값을 비교하여 상기 제2 개별 난수의 무결성을 확인하는 단계; 및

상기 호스트가 상기 제1 개별 난수 및 상기 제2 개별 난수를 인자로 사용하여 공용 난수를 생성하는 단계를 포함하는 난수 생성 방법.

[청구항 6] 호스트가 제1 개별 난수를 생성하는 단계;

상기 호스트가 타 호스트로부터 상기 타 호스트에 의해 생성 및 암호화 알고리즘에 의해 암호화된 제2 개별 난수를 수신하는 단계;

상기 호스트가 상기 타 호스트로부터 상기 암호화된 제2 개별 난수의 복호화를 위한 암호화키를 수신하는 단계;

상기 호스트가 상기 암호화키를 이용하여 상기 암호화된 제2 개별 난수를 복호화하는 단계; 및

상기 호스트가 상기 제1 개별 난수 및 상기 제2 개별 난수를 인자로 사용하여 공용 난수를 생성하는 단계를 포함하는 난수 생성 방법.

[청구항 7] 네트워크를 통해 서로 연결된 N개의 호스트를 포함하고, N은 2 이상의 자연수이며,

상기 N개의 호스트는 각각 개별 난수를 생성 및 암호화한 후 암호화된 개별 난수를 N-1개의 호스트에게 송신하고,

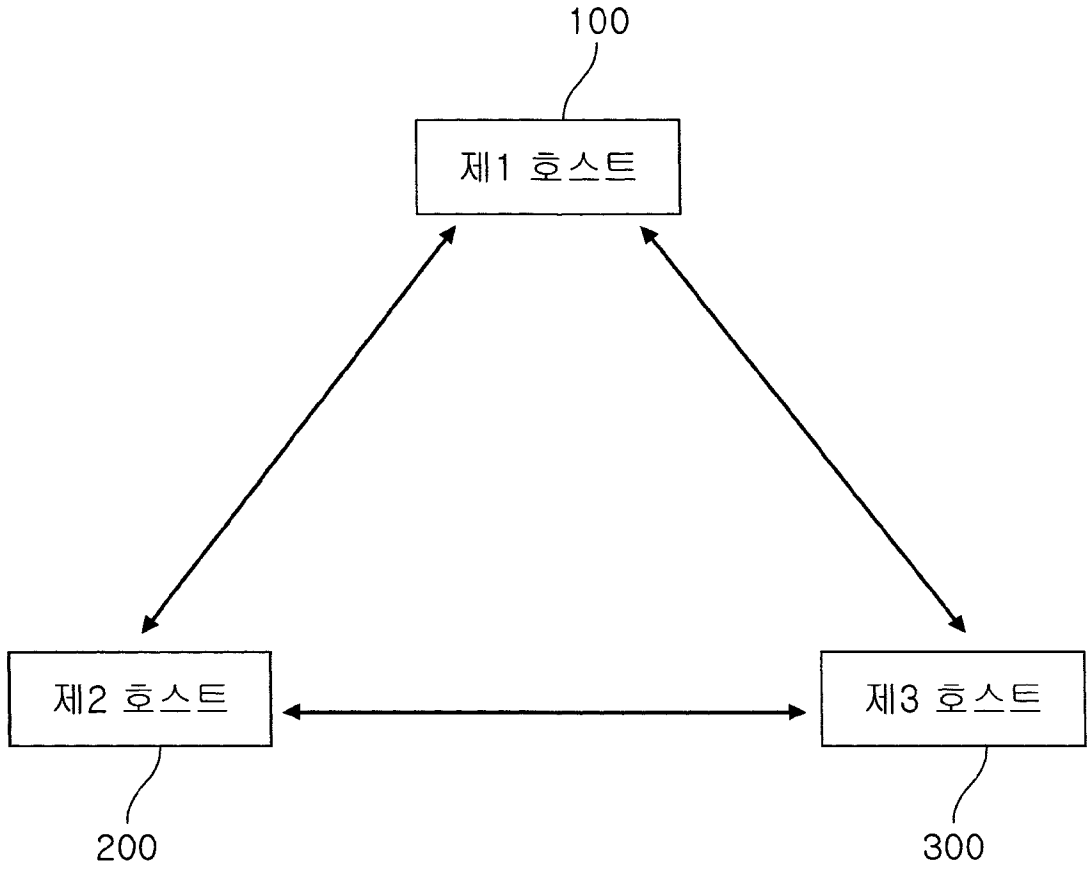
상기 N개의 호스트는 각각 N-1개의 호스트로부터 수신한 암호화된 개별 난수를 복호화한 후, 자신이 생성한 개별 난수와 상기 N-1개의 호스트로부터 수신하여 복호화한 개별 난수를 인자로 사용하여 공용 난수를 생성하는 난수 생성 시스템.

[청구항 8] 제 7 항에 있어서,

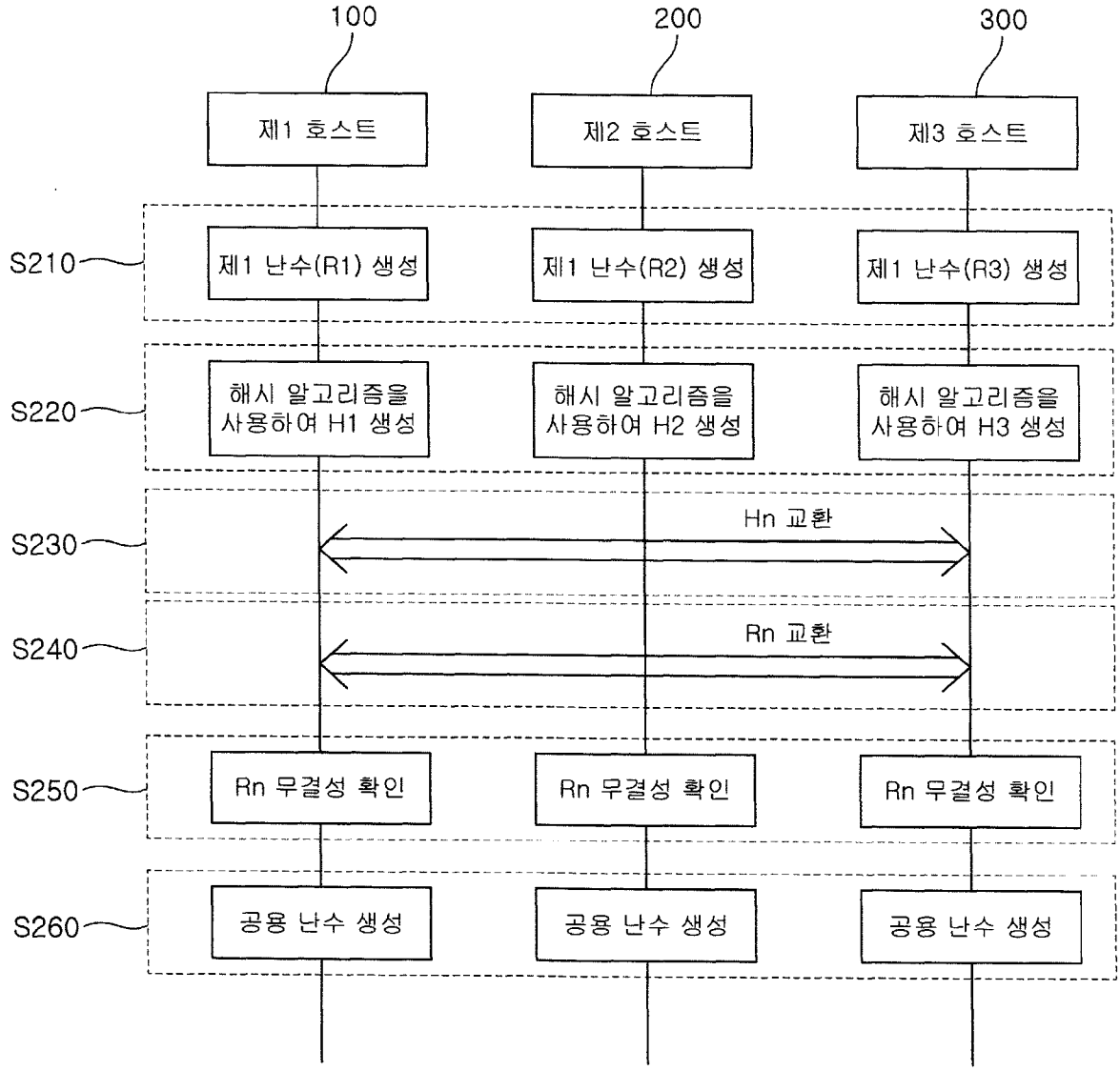
상기 N개의 호스트는 각각 상기 공용 난수를 생성하기 위해 수행하는 각 과정을 블록체인 기술 기반으로 기록하는 난수 생성 시스템.

WO 2020/009265 PCT/KR2018/008747

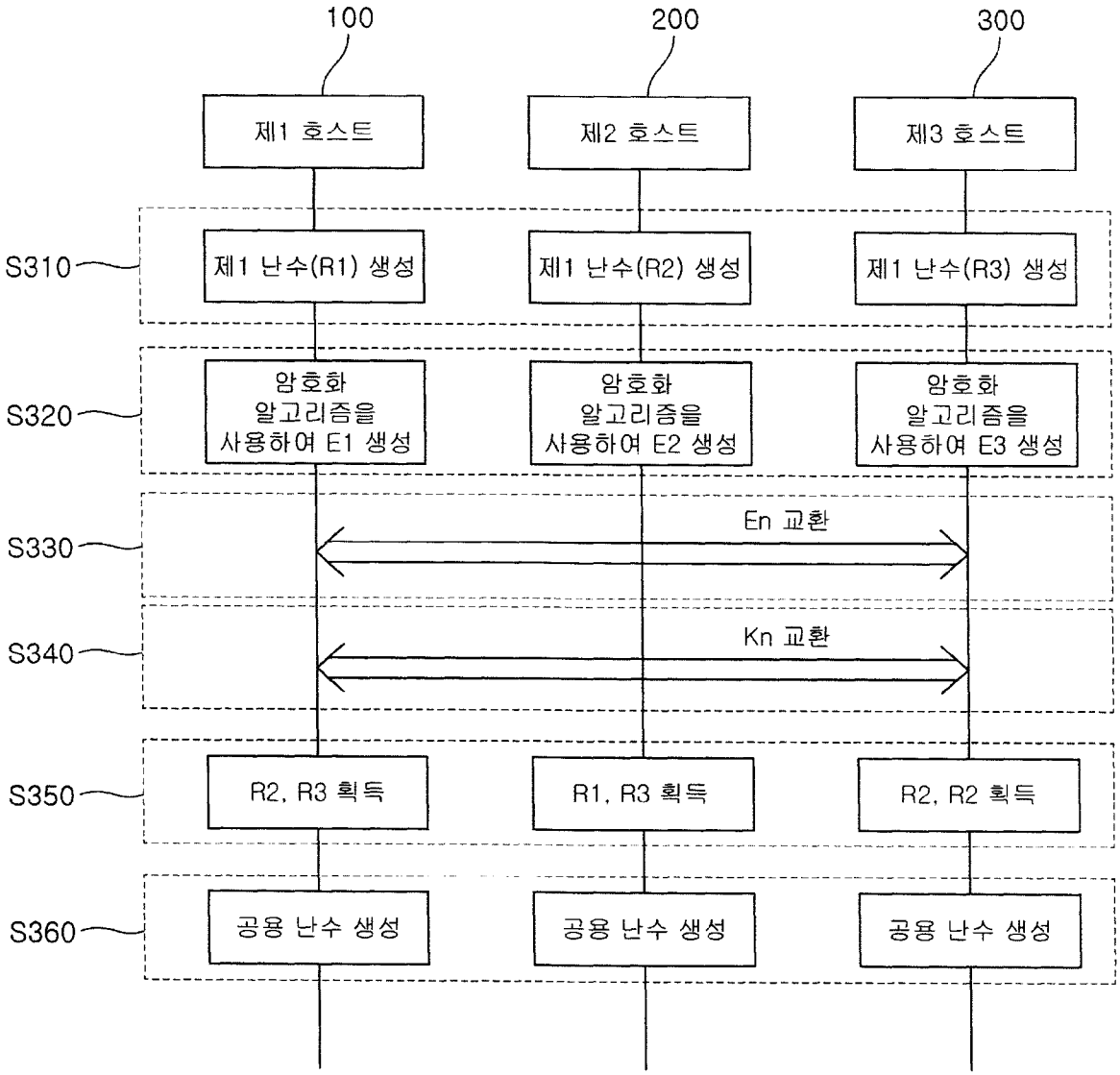
[도1]



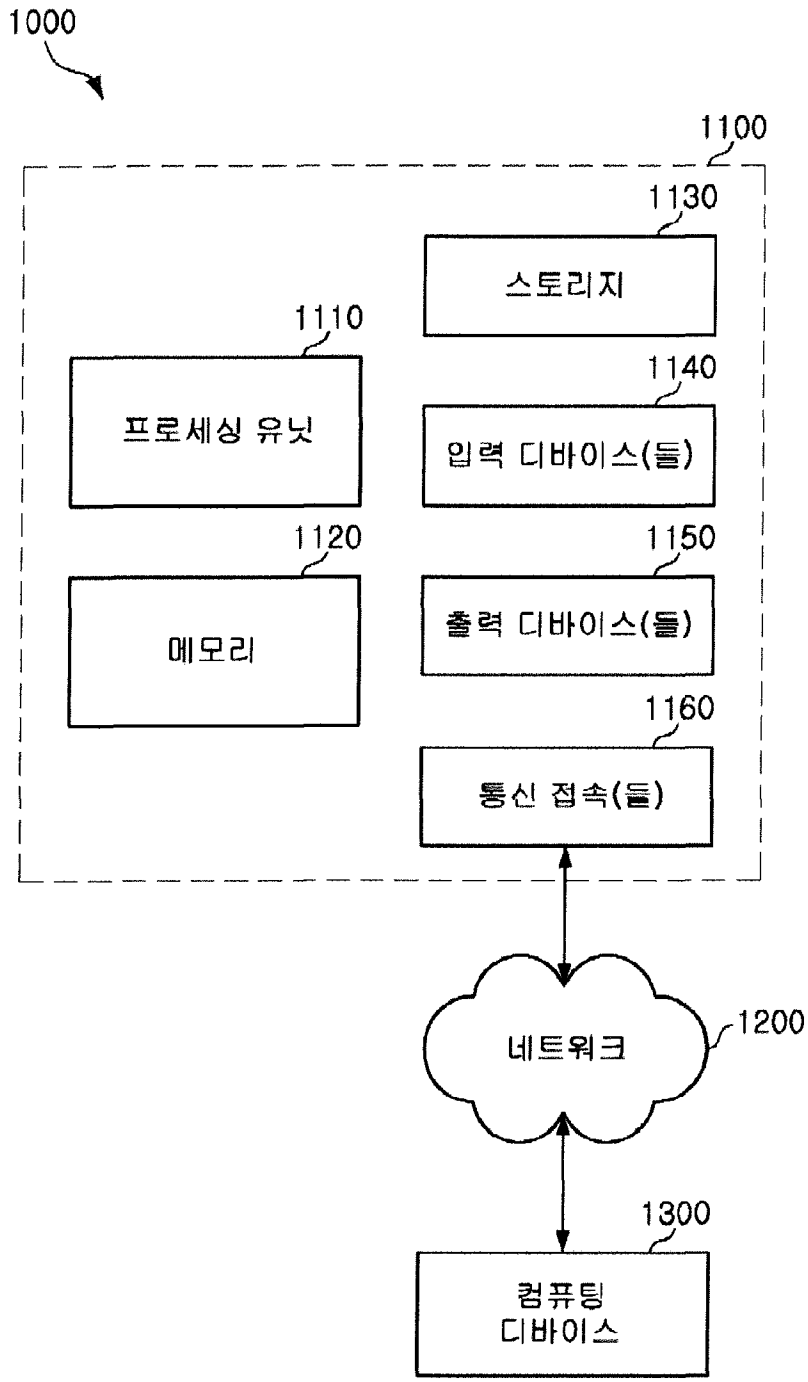
[도2]


100
200
300
제1 호스트
제2 호스트
제3 호스트
S210
제1 난수(R1) 생성
제1 난수(R2) 생성
제1 난수(R3) 생성
S220
해시 알고리즘을 사용하여 H1 생성
해시 알고리즘을 사용하여 H2 생성
해시 알고리즘을 사용하여 H3 생성
S230
Hn 교환
S240
Rn 교환
S250
Rn 무결성 확인
Rn 무결성 확인
Rn 무결성 확인
S260
공용 난수 생성
공용 난수 생성
공용 난수 생성

[도3]


100
200
300
제1 호스트
제2 호스트
제3 호스트
S310
제1 난수(R1) 생성
제1 난수(R2) 생성
제1 난수(R3) 생성
S320
암호화 알고리즘을 사용하여 E1 생성
암호화 알고리즘을 사용하여 E2 생성
암호화 알고리즘을 사용하여 E3 생성
S330
En 교환
S340
Kn 교환
S350
R2, R3 획득
R1, R3 획득
R2, R2 획득
S360
공용 난수 생성
공용 난수 생성
공용 난수 생성

[도4]


1000
1100
1130
스토리지
1110
프로세싱 유닛
1140
입력 디바이스(들)
1120
메모리
1150
출력 디바이스(들)
1160
통신 접속(들)
네트워크
1200
1300
컴퓨팅
디바이스

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2018/008747

A. CLASSIFICATION OF SUBJECT MATTER

G06F 7/58(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F 7/58; G06F 1/02; G06F 17/30; H04L 9/22

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models: IPC as above
Japanese utility models and applications for utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & Keywords: random, number, generator, encrypt, decrypt, host, server, compare, hash, verification, integrity, and similar terms.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6253223 B1 (SPRUNK, Eric J.) 26 June 2001 See column 3, lines 45-56; claims 1, 13; and figure 1.	6
Y		5
A		1-4,7-8
Y	US 2009-0240717 A1 (MIMATSU, Yasuyuki) 24 September 2009 See paragraph [0065]; and figure 4A.	5
A	US 2010-0121896 A1 (ORAM, Thomas K.) 13 May 2010 See paragraphs [0018]-[0031]; and figures 1-3.	1-8
A	US 6628786 B1 (DOLE, Bryn) 30 September 2003 See column 5, line 43-column 7, line 33; and figures 1-4.	1-8
A	US 2014-0136583 A1 (ELWHA LLC, A LIMITED LIABILITY CORPORATION OF THE STATE OF DELAWARE) 15 May 2014 See paragraphs [0044]-[0065]; and figures 1A-5B.	1-8

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
27 MARCH 2019 (27.03.2019)	**27 MARCH 2019 (27.03.2019)**

Name and mailing address of the ISA/KR
Korean Intellectual Property Office
Government Complex Daejeon Building 4, 189, Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea
Facsimile No. +82-42-481-8578

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2018/008747

Patent document cited in search report	Publication date	Patent family member	Publication date
US 6253223 B1	26/06/2001	AU 2000-73290 A1	28/12/2000
		AU 2000-73290 B2	06/11/2003
		AU 7329000 A	28/12/2000
		AU 767265 B2	06/11/2003
		CA 2372996 A1	14/12/2000
		CN 1159633 C	28/07/2004
		CN 1354848 A	19/06/2002
		EP 1190294 A1	27/03/2002
		JP 2003-501736 A	14/01/2003
		KR 10-2002-0008849 A	31/01/2002
		WO 00-75761 A1	14/12/2000
US 2009-0240717 A1	24/09/2009	EP 2104040 A2	23/09/2009
		EP 2104040 A3	29/09/2010
		JP 2009-230741 A	08/10/2009
US 2010-0121896 A1	13/05/2010	CA 2743622 A1	20/05/2010
		CA 2743622 C	06/06/2017
		EP 2366143 A1	21/09/2011
		MX 2011005121 A	03/08/2011
		US 9552191 B2	24/01/2017
		WO 2010-056806 A1	20/05/2010
US 6628786 B1	30/09/2003	None	
US 2014-0136583 A1	15/05/2014	US 2014-0136754 A1	15/05/2014
		US 2014-0136755 A1	15/05/2014
		US 2014-0136903 A1	15/05/2014
		US 2014-0136915 A1	15/05/2014
		US 2014-0137119 A1	15/05/2014
		US 2014-0137271 A1	15/05/2014
		US 2014-0208041 A1	24/07/2014
		US 2016-0028544 A1	28/01/2016
		US 8925098 B2	30/12/2014
		US 8966310 B2	24/02/2015
		US 8996951 B2	31/03/2015
		US 9026719 B2	05/05/2015
		US 9323499 B2	26/04/2016
		US 9442854 B2	13/09/2016
		US 9582465 B2	28/02/2017

국 제 조 사 보 고 서

국제출원번호
PCT/KR2018/008747

A. 발명이 속하는 기술분류(국제특허분류(IPC))

G06F 7/58(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)
G06F 7/58; G06F 1/02; G06F 17/30; H04L 9/22

조사된 기술분야에 속하는 최소문헌 이외의 문헌
한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC
일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))
eKOMPASS(특허청 내부 검색시스템) & 키워드: random, number, generator, encrypt, decrypt, host, server, compare, hash, verification, integrity, 및 유사 용어.

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
X	US 6253223 B1 (SPRUNK, ERIC J.) 2001.06.26 컬럼 3, 라인 45-56; 청구항 1, 13; 및 도면 1 참조.	6
Y		5
A		1-4,7-8
Y	US 2009-0240717 A1 (MIMATSU, YASUYUKI) 2009.09.24 단락 [0065]; 및 도면 4A 참조.	5
A	US 2010-0121896 A1 (ORAM, THOMAS K.) 2010.05.13 단락 [0018]-[0031]; 및 도면 1-3 참조.	1-8
A	US 6628786 B1 (DOLE, BRYN) 2003.09.30 컬럼 5, 라인 43 - 컬럼 7, 라인 33; 및 도면 1-4 참조.	1-8
A	US 2014-0136583 A1 (ELWHA LLC, A LIMITED LIABILITY CORPORATION OF THE STATE OF DELAWARE) 2014.05.15 단락 [0044]-[0065]; 및 도면 1A-5B 참조.	1-8

☐ 추가 문헌이 C(계속)에 기재되어 있습니다.

☒ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

"A" 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌

"E" 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌

"L" 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

"O" 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

"P" 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

"T" 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

"X" 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

"Y" 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

"&" 동일한 대응특허문헌에 속하는 문헌

국제조사의 실제 완료일	국제조사보고서 발송일
2019년 03월 27일 (27.03.2019)	2019년 03월 27일 (27.03.2019)

ISA/KR의 명칭 및 우편주소
대한민국 특허청
(35208) 대전광역시 서구 청사로 189,
4동 (둔산동, 정부대전청사)
팩스 번호 +82-42-481-8578

심사관
변성철
전화번호 +82-42-481-8262

국제조사보고서
대응특허에 관한 정보

국제출원번호
PCT/KR2018/008747

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
US 6253223 B1	2001/06/26	AU 2000-73290 A1	2000/12/28
		AU 2000-73290 B2	2003/11/06
		AU 7329000 A	2000/12/28
		AU 767265 B2	2003/11/06
		CA 2372996 A1	2000/12/14
		CN 1159633 C	2004/07/28
		CN 1354848 A	2002/06/19
		EP 1190294 A1	2002/03/27
		JP 2003-501736 A	2003/01/14
		KR 10-2002-0008849 A	2002/01/31
		WO 00-75761 A1	2000/12/14
US 2009-0240717 A1	2009/09/24	EP 2104040 A2	2009/09/23
		EP 2104040 A3	2010/09/29
		JP 2009-230741 A	2009/10/08
US 2010-0121896 A1	2010/05/13	CA 2743622 A1	2010/05/20
		CA 2743622 C	2017/06/06
		EP 2366143 A1	2011/09/21
		MX 2011005121 A	2011/08/03
		US 9552191 B2	2017/01/24
		WO 2010-056806 A1	2010/05/20
US 6628786 B1	2003/09/30	없음	
US 2014-0136583 A1	2014/05/15	US 2014-0136754 A1	2014/05/15
		US 2014-0136755 A1	2014/05/15
		US 2014-0136903 A1	2014/05/15
		US 2014-0136915 A1	2014/05/15
		US 2014-0137119 A1	2014/05/15
		US 2014-0137271 A1	2014/05/15
		US 2014-0208041 A1	2014/07/24
		US 2016-0028544 A1	2016/01/28
		US 8925098 B2	2014/12/30
		US 8966310 B2	2015/02/24
		US 8996951 B2	2015/03/31
		US 9026719 B2	2015/05/05
		US 9323499 B2	2016/04/26
		US 9442854 B2	2016/09/13
		US 9582465 B2	2017/02/28