(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2021 년 11 월 4 일 (04.11.2021)

WIPO | PCT

(10) 국제공개번호
WO 2021/221243 A1

(51) 국제특허분류:
H04L 9/32 (2006.01) *H04L 9/08* (2006.01)
H04L 9/30 (2006.01) *G06F 7/552* (2006.01)

(21) 국제출원번호: PCT/KR2020/013688

(22) 국제출원일: 2020 년 10 월 7 일 (07.10.2020)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2020-0052902 2020 년 4 월 29 일 (29.04.2020) KR

(71) 출원인: 국방과학연구소 (**AGENCY FOR DEFENSE DEVELOPMENT**) [KR/KR]; 34060 대전시 유성구 북유성대로488번길 160, Daejeon (KR). 고려대학교 산학협력단 (**KOREA UNIVERSITY RESEARCH AND BUSINESS FOUNDATION**) [KR/KR]; 02841 서울시 성북구 안암로 145, Seoul (KR).

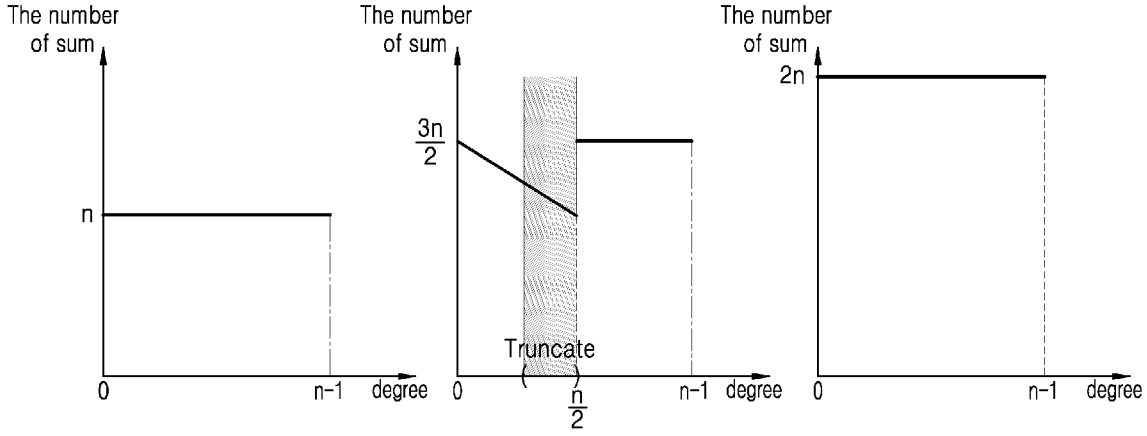
(72) 발명자: 박종환 (**PARK, Jong Hwan**); 03016 서울시 종로구 홍지문2길 20, Seoul (KR). 이광수 (**LEE, Kwang Su**); 05006 서울시 광진구 능동로 209, Seoul (KR). 박소현 (**PARK, So Hyun**); 02841 서울시 성북구 안암로 145, Seoul (KR). 우주 (**WOO, Joo**); 02841 서울시 성북구 안암로 145, Seoul (KR). 이동환 (**LEE, Dong Hwan**); 34060 대전시 유성구 북유성대로488번길 160, Daejeon (KR). 안명길 (**AHN, Myung Kil**); 34060 대전시 유성구 북유성대로488번길 160, Daejeon (KR).

(74) 대리인: 리앤목 특허법인 (**Y.P.LEE, MOCK & PARTNERS**); 06292 서울시 강남구 언주로 30길 13 대림아크로텔 12층, 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, IT, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(54) **Title:** METHOD AND SYSTEM FOR RING-LWR-BASED QUANTUM-RESISTANT SIGNATURE

(54) **발명의 명칭:** RING-LWR기반 양자내성 서명 방법 및 그 시스템



(57) **Abstract:** An embodiment of the present invention relates to a method for a ring-learning with roundings (Ring-LWR)-based quantum-resistant signature, the method comprising: a key generation step of receiving a security constant and outputting a signature key and a verification key via an operation on a ring defined by a cyclotomic equation including three terms; a signature value output step of outputting a signature value on the basis of the output signature key; and a signature verification step of calculating an operation value on the basis of the output verification key and signature value, and verifying a signature on the basis of a result of comparing the output signature value with the calculated operation value.

(57) **요약서:** 본 발명의 일 실시 예는, Ring-LWR(Ring-Learning With Roundings) 기반 양자내성 서명 방법으로서, 보안상수를 입력받고 3 개의 항으로 구성된 사이클로토믹 방정식에 의해 정의되는 링에 대한 연산으로, 서명키와 검증키를 출력하는 키생성단계; 상기 출력된 서명키를 기초로 서명값을 출력하는 서명값출력단계; 및 상기 출력된 검증키 및 서명값을 기초로 연산값을 산출하고, 상기 출력된 서명값 및 상기 산출된 연산값을 비교한 결과를 기초로 서명을 검증하는 서명검증단계;를 포함하는 Ring-LWR기반 양자내성 서명 방법을 개시한다.

[다음 쪽 계속]

WO 2021/221243 A1

(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))

명세서

발명의 명칭: RING-LWR기반 양자내성 서명 방법 및 그 시스템

기술분야

[1] 본 발명은 Ring-LWR기반 양자내성 서명 방법 및 그 시스템에 관한 것으로서, 보다 구체적으로는, 종래에 사용되어 왔던 Ring-LWE기반 양자내성 서명 방법을 개선하기 위해서 Ring-LWR을 기반으로 양자내성 서명을 수행하는 방법 및 그 시스템에 관한 것이다.

배경기술

[2] 소프트웨어의 고도화가 진행되면서, 누구나 사용하는 범용소프트웨어가 갖는 고유한 가치는 나날이 상승하는 반면, 소프트웨어가 복사, 위조되어 사용될 수 있는 위험성은 지속적으로 늘어나서, 소프트웨어 제작자들은 소프트웨어 제품에 대한 위조 및 해적행위를 방지하기 위해서 다양한 서명(signature) 또는 암호화(modulation)기법을 사용한다.

[3] 짧은 주기를 갖고 업데이트가 이루어지는 소프트웨어라서 업데이트 주기마다 제품의 진위를 판별할 수 있는 구조가 아니면, 복사된 소프트웨어도 진품 소프트웨어와 실질적인 성능 차이가 없으므로, 소프트웨어 분야에서 보안이 강화된 서명 또는 암호화 기법에 대한 요구는 날로 증대되고 있는 실정이다. 서명 또는 암호화 기법은 수학적 기교를 기반으로 하여 생성될 수 있으며, 가장 널리 사용되는 방식에는 RSA방식이 있다.

[4] 다만, RSA방식은 현재 연구가 진행되고 있는 양자 컴퓨터가 실용화되면, 양자 컴퓨터에 의해서 짧은 시간 내에 무력화될 수 있는 방식이어서, 양자 컴퓨터의 연산 체계로도 무력화시키기 어려운 서명 또는 암호화기법이 활발하게 연구되고 있으며, 이를 양자내성 서명(quantum-resistant signature) 또는 양자내성 암호화(quantum-resistant modulation)기법이라고 호칭한다.

[5] 양자내성 서명 기법 중에 알려져 있는 기법은, Ring-LWE(Ring-Learning with Errors)를 기반으로 하여, 공개키 암호와 서명을 처리하는 기법이 있다. 보다 구체적으로, Ring-LWE기반 양자내성 서명 기법에서, m, n, q는 양의 정수이고, 사이클로토믹 링 R은, 정수를 계수로 갖는 다항식 Z[X]와 사이클로토믹 다항식 $\Phi_m(X)$을 모듈러로 갖는 구조로, $Z[X]/\{\Phi_m(X)\}$의 형태를 갖는다. R_q는 $Z[X]/\{\Phi_m(X)\}$의 형태를 갖는 사이클로토믹 링이고, D_s, D_e가 R_q상의 임의의 분포라고 가정하여, 랜덤하게 선택된 다항식 $a \in R_q$, $s \in D_s$와 $e \in D_e$에 대하여, $b=a*s+e$를 계산하게 된다.

[6] 이때, (a,b)가 주어졌을 때, s를 찾는 것이 Ring-LWE 기반 기법으로 정의되며, D_s는 R_q를, D_e는 표준편차가 시그마인 가우시안 분포 GD_σ를 의미한다. Z_q에서 정의된 LWE문제는 2005년 Regev에 의해 처음 소개되었으며, 이와 동시에 Regev에 의해 처음으로 LWE기반의 공개키 암호 기법이 제안되었고, 이후,

2010년 Lyubashevsky에 링 위에서 정의된 Ring-LWE 문제가 제안되었다.

[7] Ring-LWE기법의 문제점 중 하나는 (a, b)가 주어졌을 때, s를 찾는 것이 어렵다는 점이다. Ring-LWE기법 기반 양자내성 서명 기법은, Ring-LWE 기법을 기반으로, 정당한 사용자가 갖고 있는 서명키인 s를 알고 있음을 영지식으로 증명하는 프로토콜을 사용한다. 검증키는 Ring-LWE구조로 설계하여, 서명키가 없는 정당하지 않은 사용자가 검증키로부터 서명키를 얻을 수 없고, 임의의 서명을 생성할 수 없도록 한다. Ring-LWE기반 양자내성 서명 기법의 대표적인 방법으로는, Bai와 Galbraith가 2014년에 소개한 기법이 있으며 다음과 같은 절차를 따른다.

[8] 먼저, 키를 생성하는 절차로서, 보안상수 1^{λ}를 입력받아 검증키와 서명키를 출력한다. 이어서, 서명키와 메시지 M을 입력받아 서명값을 출력한다. 마지막으로, 검증키, 메시지 M 및 서명값을 입력받아 서명을 검증한다.

[9] 위와 같은, Ring-LWE기반 양자내성 서명 기법에서는 사이클로토믹 방정식 $\Phi_m(X)$를 x^n+1로 사용한다. 해당 방정식에서 생성되는 링은 연산이 효율적이고, 곱 연산에서 발생하는 에러 전파도가 작다는 장점을 갖는다. 이때, 에러 전파도는 다항식 링의 원소인 두 다항식의 곱 연산 시, $c(x)=a(x)*b(x)=c_0+c_1x+...c_{n-1}x^{n-1}$을 구성하는 계수들 c_i가 각각 몇 개의 a_j와 b_k의 곱의 합으로 이루어져 있는지에 대한 연산으로 정의된다.

[10] 위와 같은 링에서 서명 구조가 안전하기 위해서는, 정수 n이 2의 거듭제곱 꼴이어야만 한다. 또한, 보안 강도를 높이기 위해서, 사이클로토믹 방정식의 지수 n을 증가시켜야 하는데 n이 2배 증가되면서 서명 값을 포함한 전반적인 시스템 파라미터 값이 비효율적으로 증가하게 된다. 또한, LWE기반으로 설계된 서명 구조는 키생성 과정에서, 가우시안 분포에서의 에러를 추출하여야 하므로, 키생성 과정에서 소요되는 시간이 지나치게 길어지고, 부채널 공격에 대한 취약점이 있을 수 있다.

[11] 한편, LWE기반 양자내성 서명 기법을 이용할 때, 사이클로토믹 방정식을 x^n+1으로 선택할 경우, 에러 전파도는 n이 되어, 작은 에러 전파도를 갖는다는 장점이 있으나, 지수 n이 2의 거듭제곱 형태여야 하는 조건이 생겨 시스템 파라미터를 비효율적으로 증가시키는 원인이 된다. 사이클로토믹 방정식을 $x^n+x^{n-1}+x^{n-2}...+1$가 선택될 경우, 지수 선정에 대한 자유도는 높아지더라도, 사이클로토믹 방정식을 x^n+1으로 선택할 때보다 상대적으로 에러 전파도가 커지는 문제점이 있다.

[12] 결국, LWE기반 양자내성 서명 기법에 의하면, 사이클로토믹 방정식을 어떤 식으로 채용하더라도 서로 다른 한계점을 갖고 있으므로, 양쪽의 한계점을 모두 극복할 수 있는 새로운 패러다임의 양자내성 서명 기법의 필요하다.

발명의 상세한 설명

기술적 과제

[13] 본 발명이 해결하고자 하는 기술적 과제는, 종래 방식인 Ring-LWE 기반 양자내성서명방법보다 더 적은 에러 전파도를 가지면서도 시스템 파라미터 값을 효율적으로 사용할 수 있는 Ring-LWR 기반 양자내성 서명 방법을 제공하는 데에 있다.

과제 해결 수단

[14] 상기 기술적 과제를 해결하기 위한 본 발명의 일 실시 예에 따른 방법은, Ring-LWR(Ring-Learning With Roundings)기반 양자내성 서명 방법으로서, 보안상수를 입력받고 3개의 항으로 구성된 사이클로토믹 방정식에 의해 정의되는 링에 대한 연산으로, 서명키와 검증키를 출력하는 키생성단계; 상기 출력된 서명키를 기초로 서명값을 출력하는 서명값출력단계; 및 상기 출력된 검증키 및 서명값을 기초로 연산값을 산출하고, 상기 출력된 서명값 및 상기 산출된 연산값을 비교한 결과를 기초로 서명을 검증하는 서명검증단계;를 포함한다.

[15] 상기 기술적 과제를 해결하기 위한 본 발명의 다른 일 실시 예에 따른 시스템은, Ring-LWR(Ring-Learning With Roundings)기반 양자내성 서명 시스템으로서,보안상수를 입력받고 3개의 항으로 구성된 사이클로토믹 방정식에 의해 정의되는 링에 대한 연산으로, 서명키와 검증키를 출력하는 키생성부; 상기 출력된 서명키를 기초로 서명값을 출력하는 서명값출력부; 및 상기 출력된 검증키 및 서명값을 기초로 연산값을 산출하고, 상기 출력된 서명값 및 상기 산출된 연산값을 비교한 결과를 기초로 서명을 검증하는 서명검증부;를 포함한다.

[16] 본 발명의 일 실시 예는, 상기 방법을 실행시키기 위한 프로그램을 저장하고 있는 컴퓨터 판독가능한 기록매체를 제공할 수 있다.

발명의 효과

[17] 본 발명에 따르면, 여러 보안 강도에 대해서 서명값을 비롯한 시스템 파라마터가 효율적으로 설정될 수 있다.

[18] 또한, 본 발명에 따르면, 링에서 정의되는 연산인 다항식 곱 연산에서 발생되는 에러 전파도를 낮추기 위한 특수 함수를 채용함으로써, 알고리즘 구현 속도를 비롯한 시스템 전체의 효율성이 현격하게 상승된다.

[19] 또한, 본 발명에 따르면, 키 생성 과정에서 가우시안 분포에서 비밀키를 생성하는 과정 자체를 생략할 수 있게 되어, 키 생성 속도가 향상되고, 부채널 공격에 대한 위험성도 감소될 수 있다.

도면의 간단한 설명

[20] 도 1은 본 발명에 따른 양자내성 서명 시스템의 일 예의 블록도이다.

[21] 도 2는 사이클로토믹 방정식에 따른 에러 전파도와 본 발명에서 적용한 트렁케이트함수 연산과의 상관관계를 도식적으로 나타내고 있는 도면이다.

[22] 도 3은 본 발명에 따른 양자내성 서명 방법의 일 예의 흐름도이다.

발명의 실시를 위한 최선의 형태

[23] 상기 기술적 과제를 해결하기 위한 본 발명의 일 실시 예에 따른 방법은, Ring-LWR(Ring-Learning With Roundings)기반 양자내성 서명 방법으로서, 보안상수를 입력받고 3개의 항으로 구성된 사이클로토믹 방정식에 의해 정의되는 링에 대한 연산으로, 서명키와 검증키를 출력하는 키생성단계; 상기 출력된 서명키를 기초로 서명값을 출력하는 서명값출력단계; 및 상기 출력된 검증키 및 서명값을 기초로 연산값을 산출하고, 상기 출력된 서명값 및 상기 산출된 연산값을 비교한 결과를 기초로 서명을 검증하는 서명검증단계;를 포함한다.

[24] 상기 방법에 있어서, 상기 사이클로토믹 방정식의 최고 차항의 차수 n은 2의 거듭제곱과 3의 거듭제곱의 곱 형태인 것을 특징으로 할 수 있다.

[25] 상기 방법에 있어서, 상기 서명값출력단계는, 기설정된 조건으로 선택된 항들의 계수만 선택적으로 추출하는 트렁케이트(truncate) 함수를 적용하여, 상기 서명값을 출력하는 것을 특징으로 할 수 있다.

[26] 상기 방법에 있어서, 상기 서명검증단계는, 기설정된 조건으로 선택된 항들의 계수만 선택적으로 추출하는 트렁케이트(truncate) 함수를 적용하여, 상기 연산값을 산출하는 것을 특징으로 할 수 있다.

[27] 상기 기술적 과제를 해결하기 위한 본 발명의 다른 일 실시 예에 따른 시스템은, Ring-LWR(Ring-Learning With Roundings)기반 양자내성 서명 시스템으로서,보안상수를 입력받고 3개의 항으로 구성된 사이클로토믹 방정식에 의해 정의되는 링에 대한 연산으로, 서명키와 검증키를 출력하는 키생성부; 상기 출력된 서명키를 기초로 서명값을 출력하는 서명값출력부; 및 상기 출력된 검증키 및 서명값을 기초로 연산값을 산출하고, 상기 출력된 서명값 및 상기 산출된 연산값을 비교한 결과를 기초로 서명을 검증하는 서명검증부;를 포함한다.

[28] 상기 시스템에 있어서, 상기 사이클로토믹 방정식의 최고 차항의 차수 n은 2의 거듭제곱과 3의 거듭제곱의 곱 형태인 것을 특징으로 할 수 있다.

[29] 상기 시스템은, 기설정된 조건으로 선택된 항들의 계수만 선택적으로 추출하는 트렁케이트(truncate)함수를 구현하는 함수연산부를 더 포함하고, 상기 서명값출력부는, 상기 트렁케이트함수를 적용하여, 상기 서명값을 출력하는 것을 특징으로 할 수 있다.

[30] 상기 시스템은, 기설정된 조건으로 선택된 항들의 계수만 선택적으로 추출하는 트렁케이트(truncate)함수를 구현하는 함수연산부를 더 포함하고, 상기 서명검증부는, 상기 트렁케이트함수를 적용하여, 상기 연산값을 산출하는 것을 특징으로 할 수 있다.

[31] 본 발명의 일 실시 예는 상기 방법을 실행시키기 위한 프로그램을 저장하고 있는 컴퓨터 판독가능한 기록매체를 제공할 수 있다.

발명의 실시를 위한 형태

[32] 본 발명은 다양한 변환을 가할 수 있고 여러 가지 실시 예를 가질 수 있는바, 특정 실시 예들을 도면에 예시하고 상세한 설명에 상세하게 설명하고자 한다. 본 발명의 효과 및 특징, 그리고 그것들을 달성하는 방법은 도면과 함께 상세하게 후술되어 있는 실시 예들을 참조하면 명확해질 것이다. 그러나 본 발명은 이하에서 개시되는 실시 예들에 한정되는 것이 아니라 다양한 형태로 구현될 수 있다.

[33] 이하, 첨부된 도면을 참조하여 본 발명의 실시 예들을 상세히 설명하기로 하며, 도면을 참조하여 설명할 때 동일하거나 대응하는 구성 요소는 동일한 도면부호를 부여하고 이에 대한 중복되는 설명은 생략하기로 한다.

[34] 이하의 실시 예에서, 제1, 제2 등의 용어는 한정적인 의미가 아니라 하나의 구성 요소를 다른 구성 요소와 구별하는 목적으로 사용되었다.

[35] 이하의 실시 예에서, 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다.

[36] 이하의 실시 예에서, 포함하다 또는 가지다 등의 용어는 명세서상에 기재된 특징, 또는 구성요소가 존재함을 의미하는 것이고, 하나 이상의 다른 특징을 또는 구성요소가 부가될 가능성을 미리 배제하는 것은 아니다.

[37] 어떤 실시 예가 달리 구현 가능한 경우에 특정한 공정 순서는 설명되는 순서와 다르게 수행될 수도 있다. 예를 들어, 연속하여 설명되는 두 공정이 실질적으로 동시에 수행될 수도 있고, 설명되는 순서와 반대의 순서로 진행될 수 있다.

[38] 설명의 편의를 위해서, 본 명세서에서 수학식 1 내지 수학식 3과 같은 표기는, 언제나 동일한 방식으로 해석하도록 한다.

[39] [수식1]

$$s1, s2 \in R$$

[40] [수식2]

$$mod(z)$$

[41] [수식3]

$$\lfloor . \rfloor$$

[42] 수학식 1은 s1, s2가 각각 R집합에 속하는 원소라는 것을 의미한다.

[43] 수학식 2는 z원소로 모듈러(modular) 연산을 수행하는 것을 의미한다.

[44] 수학식 3은 괄호 내부의 값을 반올림하는 것을 의미한다.

[45] 도 1은 본 발명에 따른 양자내성 서명 시스템의 일 예의 블록도이다.

[46] 도 1을 참조하면, 본 발명에 따른 양자내성 서명 시스템(10)은 키생성부(110), 서명값출력부(130), 서명검증부(150) 및 함수연산부(170)를 포함하는 것을 알 수

있다.

[47] 본 발명에 따른 양자내성 서명 시스템(10)은 기존에 알려진 Ring-LWE기반 양자내성 서명 기법을 개선하기 위한 Ring-LWR기반 양자내성 서명 기법을 구현할 수 있다. 여기서, Ring-LWR(Ring-Learning with Roundings)은 a*s 연산 값에 작은 범위의 에러 e를 더하는 과정을 필수적으로 포함하는 Ring-LWE대신, 라운딩 함수인 $[.]_p:Z_q \rightarrow Z_p$를 이용하여, $(a,b=[a*s]_p)$가 주어졌을 때, s를 찾는 문제로 정의되며, 가우시안 분포에서 에러를 뽑는 과정이 생략되어, 키생성 시간이 줄어들고 공개키의 크기가 Z_q에서 Z_p로 감소하는 장점이 있다.

[48] 키생성부(110)는 보안상수를 입력으로 받아서, 3개의 항으로 구성된 사이클로토믹 방정식에 의해 정의되는 링에 대한 연산으로 서명키와 검증키를 출력한다.

[49] 키생성부(110)가 입력값으로 받는 보안상수는 1^{λ}이고, 검증키는 vk이며, 서명는 sk이다. 본 발명에 따른 양자내성 서명 시스템(10)에서 전반적으로 사용되는 파라미터는 n, l, q, p, Ds, B, d, h, L_s 및 L_E가 포함되고, 이러한 파라미터들은 기존의 Ring-LWR기법에서 사용되는 파라미터와 동일한 범주에 속한다. 즉, n, l, B, h, d와 모듈러스(modulus) q, p는 모두 양의 정수이고, l은 1보다 크거나 같고 n/2보다 작거나 같은 특징을 갖는다. 또한, q와 p는 2의 거듭제곱 형태이며, p는 q보다 작다. 또한, n은 2의 거듭제곱과 3의 거듭제곱의 곱 형태가 된다.

[50] 키생성부(110)에서 사용되는 사이클로토믹 방정식은 3개의 항으로 구성된다.

[51] [수식4]

$$x^n - x^{n/2} + 1$$

[52] 수학식 4는 키생성부(110)에서 사용되는 사이클로토믹 방정식의 일 예를 나타낸 식이다. 수학식 4는 3개의 항을 갖는 3항식으로서, 본 발명은 3개의 항으로 구성된 사이클로토믹 방정식을 링의 모듈러 연산으로 사용함으로써, 지수 n을 선정하는데에 있어서 높은 자유도가 보장되면서도 상대적으로 에러 전파도도 작은 특징을 갖는다. 또한, 수학식 4를 사이클로토믹 방정식으로 사용할 경우, 보안강도를 올리기 위해서, n이 2의 거듭제곱과 3의 거듭제곱의 곱 형태이면 족하다. 예를 들어, 본 발명에서 수학식 4를 사이클로토믹 방정식으로 채택할 경우, n은 512, 648, 768, 864, 972, 1024 등이 될 수 있다.

[53] 키생성부(110)는 사이클로토믹 3항식에 대한 연산으로서, 다항식 a를 R_q에서 무작위로 선택하고, 다항식 s를 분포 D_s에서 선택한다. 여기서, R_q란 사이클로토믹 방정식에 의한 링을 의미하고, 링(Ring)이란 기설정된 계수를 가지는 다항식의 집합으로서, 원소들 사이에 덧셈과 곱셈이 정의되어 있으며, 덧셈과 곱셈에 대해서 닫혀 있는 집합을 의미한다. 일 예로서, 3개의 항으로 구성된 사이클로토믹 방정식 $x^n-x^{n/2}+1$으로 생성되는 링은 $Z_q[X]/(x^n-x^{n/2}+1)$이다.

[54] 또한, 키생성부(110)는 다항식 t를 계산하며, 다항식 t는 수학식 5를 통해 계산될 수 있다.

[55] [수식5]

$$t = \frac{p}{q}(a \cdot s)$$

[56] 다항식 a, s, t가 각각 결정되었으면, 키생성부(110)는 검증키 vk와 서명키 sk를 출력하게 되며, 출력되는 검증키와 서명키는 수학식 6 및 수학식 7에 의해 결정된다.

[57] [수식6]

$$vk = (a, t)$$

[58] [수식7]

$$sk = s$$

[59] 서명값출력부(130)는 키생성부(110)에서 출력된 서명키를 기초로 서명값을 출력한다.

[60] 일 예로서, 서명값출력부(130)는 서명키 sk와 메시지 M을 입력으로 받아, 서명값 (z, c)를 출력한다. 서명값출력부(130)는 다항식 y를 D_y=[-B, B]에서 무작위로 선택하고, 수학식 8을 이용하여 v를 계산한다.

[61] [수식8]

$$v = a \cdot y (mod\ q)$$

[62] 서명값출력부(130)는 수학식 8을 통해 계산된 v를 트렁케이트(truncate)함수에 입력하여 vtrun을 계산한다. 여기서, 트렁케이트(truncate)함수는 기설정된 조건으로 선택된 항들의 계수만 선택적으로 추출하는 함수로서, 3항식으로 구성된 사이클로토믹 방정식으로 생성되는 링의 에러 전파도를 줄이기 위해 적용되는 함수이다.

[63] 본 발명처럼 Ring-LWR을 기반으로 양자내성 서명 기법을 구현하는 경우, 앞서 설명한 것과 같이 시스템 파라미터가 효율적으로 설정되는 장점은 있으나, 수학식 5나 수학식 8과 같이 곱 연산이 반복적으로 이루어지면서 에러 전파도가 커지게 되는데, 트렁케이트 함수가 적용됨으로써, 에러 전파도도 적절하게 낮아지게 된다.

[64] 트렁케이트함수는 입력된 방정식의 계수 가운데

$$\frac{n}{2} - 1$$

차항 이하의 1개 항에 대한 계수만 선별적으로 추출할 수 있으며, 트렁케이트함수의 연산에 의해 3항식 x^n-$x^{n/2}$+1의 에러 전파도가 가장 작은

영역이 되어서, 링 연산에서 발생되는 에러의 크기가 효율적으로 제한된다.

[65] 트렁케이트함수가 동작하는 일 예는 다음과 같다.

[66] 먼저, 트렁케이트함수는 입력값으로 방정식 $a=a_0+a_1x+...+a_{n-1}x^{n-1}$와 n/2보다 작거나 같은 정수 l을 받는다. 이어서, 트렁케이드함수는 방정식 a로부터 계수 집합 $(a_{n/2-l}, a_{n/2-l+1}, ..., a_{n/2-1})$을 추출하고, 추출된 계수들로 방정식을 생성하여 출력한다. 수학식 9는 트렁케이트함수에 의해 추출되는 방정식의 일 예이다.

[67] [수식9]

$$Trun(a,l) = a_{\frac{n}{2}-l}x^{\frac{n}{2}-l} + a_{\frac{n}{2}-l+1}x^{\frac{n}{2}-l+1} + \cdots + a_{\frac{n}{2}-1}x^{\frac{n}{2}-1}$$

[68] 택적 일 실시 예로서, 서명값출력부(130)는 트렁케이트함수 연산을 함수연산부(170)라고 하는 별도의 모듈에서 수행되도록 제어할 수도 있다. 함수연산부(170)는 서명값출력부(130)로부터 방정식 a과 정수 l을 전달받아서 함수를 수행하고, 결과값을 서명값출력부(130)에 리턴할 수 있다.

[69] 이하에서는, 서명값출력부(130)에 대해서 이어서 설명하기로 한다.

[70] 서명값출력부(130)는 트렁케이트함수의 연산결과인 v_{trun}을 파라미터 m과 함께 해시함수에 입력하여 서명값을 구성하는 c를 계산한다.

[71] [수식10]

$$c = H([v_{trun}]_d, m)$$

[72] 수학식 10은 서명값출력부(130)가 서명값 c를 계산하기 위해 사용하는 수학식의 일 예이다. 바람직한 결과를 유도하기 위해서, 트렁케이트함수의 연산결과인 v_{trun} 에서 최하 d비트를 잘라내는 결과인 $[v_{trun}]_d$가 해시함수에 입력되며, d값에 대해서는 키생성부(110)에 대한 설명에서 시스템 파라미터 중 하나라고 설명한 바 있다.

[73] 서명값출력부(130)는 c가 계산되면, 수학식 11를 통해 z를 계산하며, 수학식 12에 따른 조건이 성립되면, 모든 연산을 초기화하고, 키생성부(110)에서 검증키와 서명키를 출력하는 과정부터 새로 시작하도록 제어한다.

[74] [수식11]

$$z = y + s \cdot c$$

[75] [수식12]

$$||[z]||_\infty > B - L_s$$

[76] 서명값출력부(130)는 수학식 12에 따른 조건이 성립되지 않으면, 수학식 13을 통해 w를 계산한다.

[77] [수식13]

$$w = a \cdot z - \frac{q}{p}(t \cdot c)(mod\ \ q)$$

[78] 수학식 13은 w를 계산하기 위한 식으로서, 수학식 13을 구성하는 a, z, p, q, t, c 및 q는 시스템 파라미터로서 미리 정해져 있거나, 이전 연산과정을 통해서 산출된다는 것은 이미 설명한 바 있다.

[79] 서명값출력부(130)는 w가 산출되면, 트렁케이트함수를 다시 호출하여, 산출된 w를 정수 l과 함께 입력하고 w_{trun}을 산출한다 서명값출력부(130)는 수학식 14 또는 수학식 15에 따른 조건이 성립되면, 모든 연산을 초기화하고, 키생성부(110)에서 검증키와 서명키를 출력하는 과정부터 새로 시작하도록 제어한다.

[80] [수식14]

$$||[w]_{2^d}||_{\infty} > 2^{d-1} - L_E$$

[81] [수식15]

$$[w_{trun}]_d \neq [v_{trun}]_d$$

[82] 서명값출력부(130)는 수학식 14 및 수학식 15에 따른 조건이 모두 성립되지 않으면, 서명값 (z, c)을 출력한다.

[83] 서명검증부(150)는 키생성부(110)에서 출력된 검증키 vk와 서명값출력부(130)에서 출력된 서명값(z, c)을 기초로 연산값을 산출하고, 서명값 및 연산값을 비교한 결과를 기초로 서명을 검증한다.

[84] 구체적으로, 서명검증부(150)는 수학식 16을 통해서 w'를 계산하고, 산출된 w'을 트렁케이트함수에 입력하여, w_{trun}을 계산한다. 이 과정에서 서명검증부(150)는 서명값출력부(130)와 마찬가지로 함수연산부(170)에 방정식과 정수 l을 전달하고, 트렁케이트함수를 연산한 결과값을 리턴받을 수도 있다.

[85] [수식16]

$$w' = a \cdot z - \frac{q}{p}(t \cdot c)(mod\ \ q)$$

[86] 수학식 16는 수학식 13과 전체적인 형태는 유사하고, 수학식 13은 서명단계에서 사용되는 식이고, 수학식 16은 서명을 검증하는 단계에서

사용되는 식이므로, 올바른 서명이 입력된다면, 수학식 16 및 수학식 13는 실질적으로 동일한 식이 된다.

[87] 이어서, 서명검증부(150)는 산출된 w_{trun} 및 m을 수학식 10과 같이, 해시 함수에 입력하여 c'을 계산하고, 서명값을 구성하는 c와 연산값을 구성하는 c'을 비교하여 검증한다. 서명검증부(150)는 서명값을 구성하는 c와 연산값을 구성하는 c'가 동일하고, 수학식 17에 따른 조건이 성립되면 검증이 된 것으로 간주한다.

[88] [수식17]

$$||z||_{\infty} > B - L_s$$

[89] 반면, 서명검증부(150)는 수학식 17에 따른 조건이 성립되지 않으면, 서명값을 구성하는 c와 연산값을 구성하는 c'이 동일한 것과 상관없이, 서명에 따른 검증이 통과되지 않은 것으로 간주한다. 수학식 17에서 B는 서명과정에서 다항식 y가 선택될 수 있는 범위 중 가장 큰 값, L_s는 시스템 파라미터로 정해지는 값이라는 것은 이미 설명한 바 있다.

[90] 함수연산부(170)는 서명값출력부(130) 및 서명검증부(150)로부터 방정식과 정수를 전달받아서, 트렁케이트 연산을 수행하고, 수행한 결과를 서명값출력부(130) 또는 서명검증부(150)에 반환하는 기능을 수행한다. 함수연산부(170)는 트렁케이트연산을 하기 위한 모듈이므로, 도 1에 기재된 것과 다르게, 실시 예에 따라서, 함수연산부(170)는 서명값출력부(130) 및 서명검증부(150) 내부에 각각 포함되는 형태로 구현될 수도 있다.

[91] 도 2는 사이클로토믹 방정식에 따른 에러 전파도와 본 발명에서 적용한 트렁케이트함수 연산과의 상관관계를 도식적으로 나타내고 있는 도면이다.

[92] 보다 구체적으로, 도 2는 총 3개의 그래프를 동일선상에서 비교하고 있으며, 사이클로토믹 방정식가 어떤 식으로 설정되었지에 따라서 시스템은 도 2에 도시된 세 가지 그래프 중 어느 하나와 동일한 에러 전파도를 가질 수 있다.

[93] 먼저, 도 2의 가장 좌측의 그래프는 사이클로토믹 방정식을 x^n+1로 설정하고, Ring-LWE기반으로 양자내성 서명 기법을 구현했을 때의 에러전파도를 나타낸 것이다. 도 2를 참조하면, 가장 좌측의 그래프에서는, 0에서 n-1차수까지 걸쳐서 The number of sum이 n으로 고정되어 있는 것을 알 수 있다.

[94] 이어서, 도 2의 가장 우측의 그래프는 사이클로토믹 방정식을 $x^n+x^{n-1}+...+1$로 설정하고, Ring-LWE기반으로 양자내성 서명 기법을 구현했을 때의 에러전파도를 나타낸 것이다. 도 2를 참조하면, 가장 우측의 그래프에서는, 0에서 n-1차수까지 걸쳐서 The number of sum이 2n으로 고정되어 있는 것을 알 수 있으며, 배경기술에서 설명한 것과 같이, 사이클로토믹 방정식을 $x^n+x^{n-1}+...+1$로 설정할 경우, 지수 선정에 대한 자유도가 높아지지만, 에러 전파도가 2n이 되는 것을 알 수 있다.

[95] 마지막으로, 도 2의 중앙에 위치한 그래프는 사이클로토믹 방정식을 3항식으로 설정하고, Ring-LWR기반으로 양자내성 서명 기법을 구현했을 때의 에러전파도를 나타낸 것이다.

[96] 도 2를 참조하면, 가장 중앙에 위치한 그래프에서는, 차수가 0일 때의 에러 전파도가 3n/2으로서, 가장 좌측의 그래프의 값보다 더 높지만, 차수가 올라가면서 점차 감소하는 모습이 관측되는데, 본 발명에서는 서명값을 출력하고 서명을 검증하는 단계에서 트렁케이트함수까지 적용하여, 에러 전파도가 3n/2보다 훨씬 낮은 부분만 추출하는 구성을 추가적으로 채용함으로써, 에러 전파도를 획기적으로 감소시켰다.

[97] 도 3은 본 발명에 따른 양자내성 서명 방법의 일 예의 흐름도이다.

[98] 도 3에 따른 방법은 도 1에서 설명한 양자내성 서명 시스템(10)에 의해서 구현될 수 있으므로, 이하에서는, 도 1을 참조하여 설명하기로 하고, 도 1에서 설명한 내용과 중복되는 설명은 생략하기로 한다.

[99] 키생성부(110)는 3개의 항으로 구성된 사이클로토믹 방정식에 의해 정의되는 링에 대한 연산으로 서명키와 검증키를 출력한다(S310).

[100] 서명값출력부(130)는 서명키를 기초로 서명값을 출력한다(S320).

[101] 서명검증부(150)는 검증키와 서명값을 기초로 연산값을 산출한다(S330).

[102] 서명검증부(150)는 서명값과 연산값이 동일한지 비교하고(S340), 서명값과 연산값이 동일하면 정상적인 서명이라고 간주하고, 서명값과 연산값이 동일하지 않으면, 정상적인 서명이 아니라고 간주할 수 있다(S350).

[103] 일 실시 예로서, 단계 S350에서, 서명값과 연산값이 동일하더라도, 수학식 17에 따른 조건이 성립되지 않으면, 정상적인 서명이 아니라고 간주할 수 있다는 것은 이미 설명한 바 있다.

[104] 본 발명에 따르면, 여러 보안 강도에 대해서 서명값을 비롯한 시스템 파라마터가 효율적으로 설정될 수 있다.

[105] 또한, 본 발명에 따르면, 링에서 정의되는 연산인 다항식 곱 연산에서 발생되는 에러 전파도를 낮추기 위한 특수 함수를 채용함으로써, 알고리즘 구현 속도를 비롯한 시스템 전체의 효율성이 현격하게 상승된다. 특히, 본 발명은 트렁케이트 함수를 적용하여, 오차 범위를 엄밀하게 설정할 수 있게 되고, 서명 생성 알고리즘에서 반복 수행되는 횟수를 줄일 수 있다.

[106] 또한, 본 발명은, 기존의 Ring-LWE 기반으로 설계되던 서명의 구조를 Ring-LWR기반으로 설계함으로써, 비밀키의 크기를 반으로 줄이고, 공개키의 크기도 Z_q에서 Z_p로 줄임과 동시에, 키생성 과정에서 가우시안 분포에서 비밀키를 생성하는 과정 자체를 생략할 수 있게 되어, 키 생성 속도가 향상되고, 부채널 공격에 대한 위험성도 감소될 수 있다.

[107] 이상 설명된 본 발명에 따른 실시 예는 컴퓨터 상에서 다양한 구성요소를 통하여 실행될 수 있는 컴퓨터 프로그램의 형태로 구현될 수 있으며, 이와 같은 컴퓨터 프로그램은 컴퓨터로 판독 가능한 매체에 기록될 수 있다. 이때, 매체는

하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM 및 DVD와 같은 광기록 매체, 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical medium), 및 ROM, RAM, 플래시 메모리 등과 같은, 프로그램 명령어를 저장하고 실행하도록 특별히 구성된 하드웨어 장치를 포함할 수 있다.

[108] 한편, 상기 컴퓨터 프로그램은 본 발명을 위하여 특별히 설계되고 구성된 것이거나 컴퓨터 소프트웨어 분야의 당업자에게 공지되어 사용 가능한 것일 수 있다. 컴퓨터 프로그램의 예에는, 컴파일러에 의하여 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용하여 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드도 포함될 수 있다.

[109] 본 발명에서 설명하는 특정 실행들은 일 실시 예들로서, 어떠한 방법으로도 본 발명의 범위를 한정하는 것은 아니다. 명세서의 간결함을 위하여, 종래 전자적인 구성들, 제어 시스템들, 소프트웨어, 상기 시스템들의 다른 기능적인 측면들의 기재는 생략될 수 있다. 또한, 도면에 도시된 구성 요소들 간의 선들의 연결 또는 연결 부재들은 기능적인 연결 및/또는 물리적 또는 회로적 연결들을 예시적으로 나타낸 것으로서, 실제 장치에서는 대체 가능하거나 추가의 다양한 기능적인 연결, 물리적인 연결, 또는 회로 연결들로서 나타내어질 수 있다. 또한, "필수적인", "중요하게" 등과 같이 구체적인 언급이 없다면 본 발명의 적용을 위하여 반드시 필요한 구성 요소가 아닐 수 있다.

[110] 본 발명의 명세서(특히 특허청구범위에서)에서 "상기"의 용어 및 이와 유사한 지시 용어의 사용은 단수 및 복수 모두에 해당하는 것일 수 있다. 또한, 본 발명에서 범위(range)를 기재한 경우 상기 범위에 속하는 개별적인 값을 적용한 발명을 포함하는 것으로서(이에 반하는 기재가 없다면), 발명의 상세한 설명에 상기 범위를 구성하는 각 개별적인 값을 기재한 것과 같다. 마지막으로, 본 발명에 따른 방법을 구성하는 단계들에 대하여 명백하게 순서를 기재하거나 반하는 기재가 없다면, 상기 단계들은 적당한 순서로 행해질 수 있다. 반드시 상기 단계들의 기재 순서에 따라 본 발명이 한정되는 것은 아니다. 본 발명에서 모든 예들 또는 예시적인 용어(예들 들어, 등등)의 사용은 단순히 본 발명을 상세히 설명하기 위한 것으로서 특허청구범위에 의해 한정되지 않는 이상 상기 예들 또는 예시적인 용어로 인해 본 발명의 범위가 한정되는 것은 아니다. 또한, 당업자는 다양한 수정, 조합 및 변경이 부가된 특허청구범위 또는 그 균등물의 범주 내에서 설계 조건 및 팩터에 따라 구성될 수 있음을 알 수 있다.

청구범위

[청구항 1] Ring-LWR(Ring-Learning With Roundings)기반 양자내성 서명 방법으로서,
보안상수를 입력받고 3개의 항으로 구성된 사이클로토믹 방정식에 의해 정의되는 링에 대한 연산으로, 서명키와 검증키를 출력하는 키생성단계;
상기 출력된 서명키를 기초로 서명값을 출력하는 서명값출력단계; 및
상기 출력된 검증키 및 서명값을 기초로 연산값을 산출하고, 상기 출력된 서명값 및 상기 산출된 연산값을 비교한 결과를 기초로 서명을 검증하는 서명검증단계;를 포함하는 Ring-LWR기반 양자내성 서명 방법.

[청구항 2] 제1항에 있어서,
상기 사이클로토믹 방정식의 최고 차항의 차수 n은 2의 거듭제곱과 3의 거듭제곱의 곱 형태인 것을 특징으로 하는, Ring-LWR기반 양자내성 서명 방법.

[청구항 3] 제1항에 있어서,
상기 서명값출력단계는,
기설정된 조건으로 선택된 항들의 계수만 선택적으로 추출하는 트렁케이트(truncate) 함수를 적용하여, 상기 서명값을 출력하는 것을 특징으로 하는, Ring-LWR기반 양자내성 서명 방법.

[청구항 4] 제1항에 있어서,
상기 서명검증단계는,
기설정된 조건으로 선택된 항들의 계수만 선택적으로 추출하는 트렁케이트(truncate) 함수를 적용하여, 상기 연산값을 산출하는 것을 특징으로 하는, Ring-LWR기반 양자내성 서명 방법.

[청구항 5] 제1항에 따른 방법을 실행시키기 위한 프로그램을 저장하고 있는 컴퓨터 판독가능한 기록매체.

[청구항 6] Ring-LWR(Ring-Learning With Roundings)기반 양자내성 서명 시스템으로서,
보안상수를 입력받고 3개의 항으로 구성된 사이클로토믹 방정식에 의해 정의되는 링에 대한 연산으로, 서명키와 검증키를 출력하는 키생성부;
상기 출력된 서명키를 기초로 서명값을 출력하는 서명값출력부; 및
상기 출력된 검증키 및 서명값을 기초로 연산값을 산출하고, 상기 출력된 서명값 및 상기 산출된 연산값을 비교한 결과를 기초로 서명을 검증하는 서명검증부;를 포함하는 Ring-LWR기반 양자내성 서명 시스템.

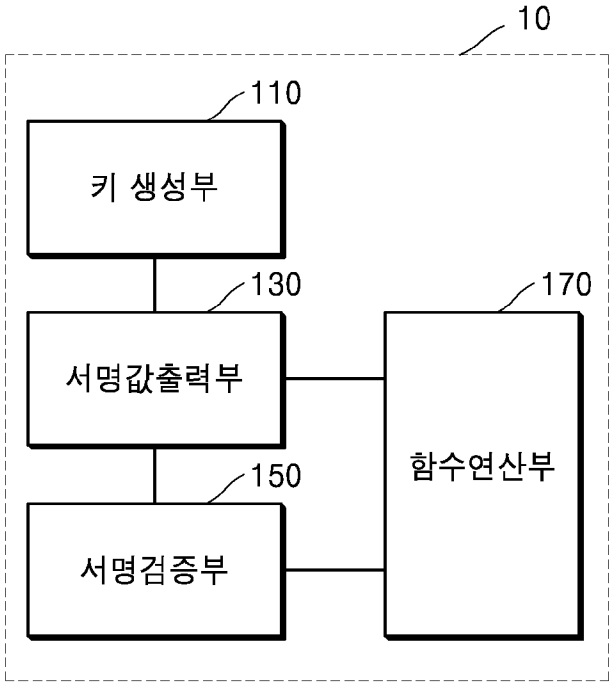
[청구항 7] 제6항에 있어서,
상기 사이클로토믹 방정식의 최고 차항의 차수 n은 2의 거듭제곱과 3의 거듭제곱의 곱 형태인 것을 특징으로 하는, Ring-LWR기반 양자내성 서명 시스템.

[청구항 8] 제6항에 있어서,

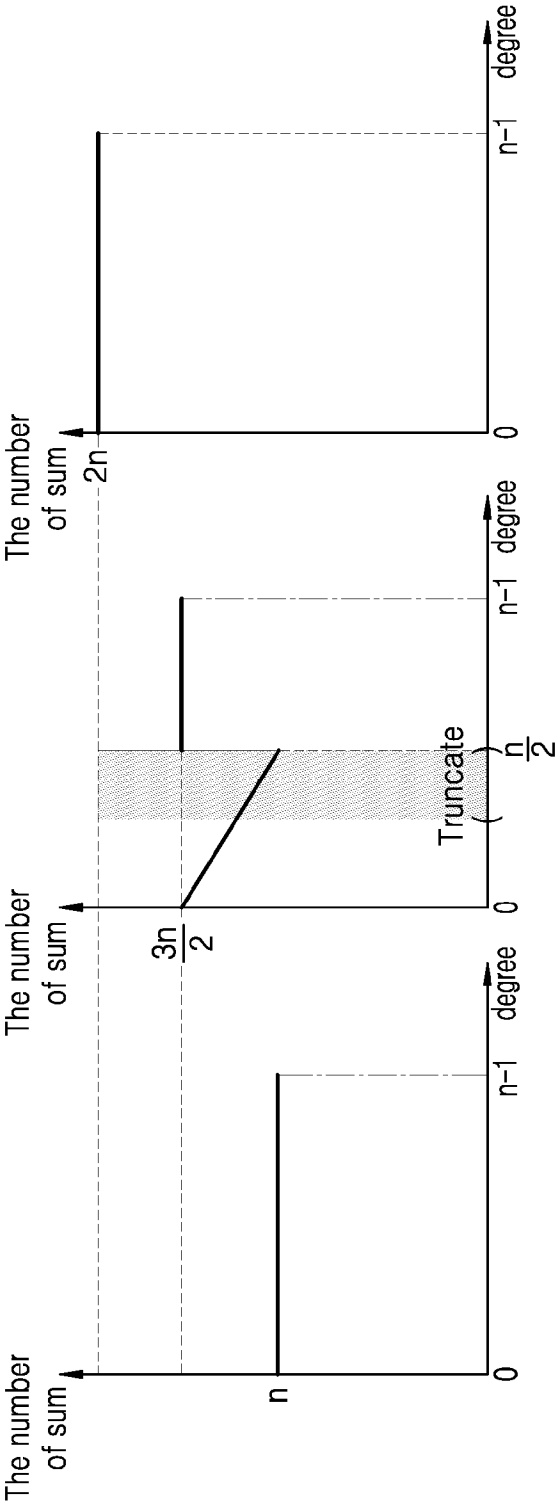
상기 시스템은,
기설정된 조건으로 선택된 항들의 계수만 선택적으로 추출하는 트렁케이트(truncate)함수를 구현하는 함수연산부를 더 포함하고,
상기 서명값출력부는,
상기 트렁케이트함수를 적용하여, 상기 서명값을 출력하는 것을 특징으로 하는, Ring-LWR기반 양자내성 서명 시스템.

[청구항 9] 제6항에 있어서,
상기 시스템은,
기설정된 조건으로 선택된 항들의 계수만 선택적으로 추출하는 트렁케이트(truncate)함수를 구현하는 함수연산부를 더 포함하고,
상기 서명검증부는,
상기 트렁케이트함수를 적용하여, 상기 연산값을 산출하는 것을 특징으로 하는, Ring-LWR기반 양자내성 서명 시스템.

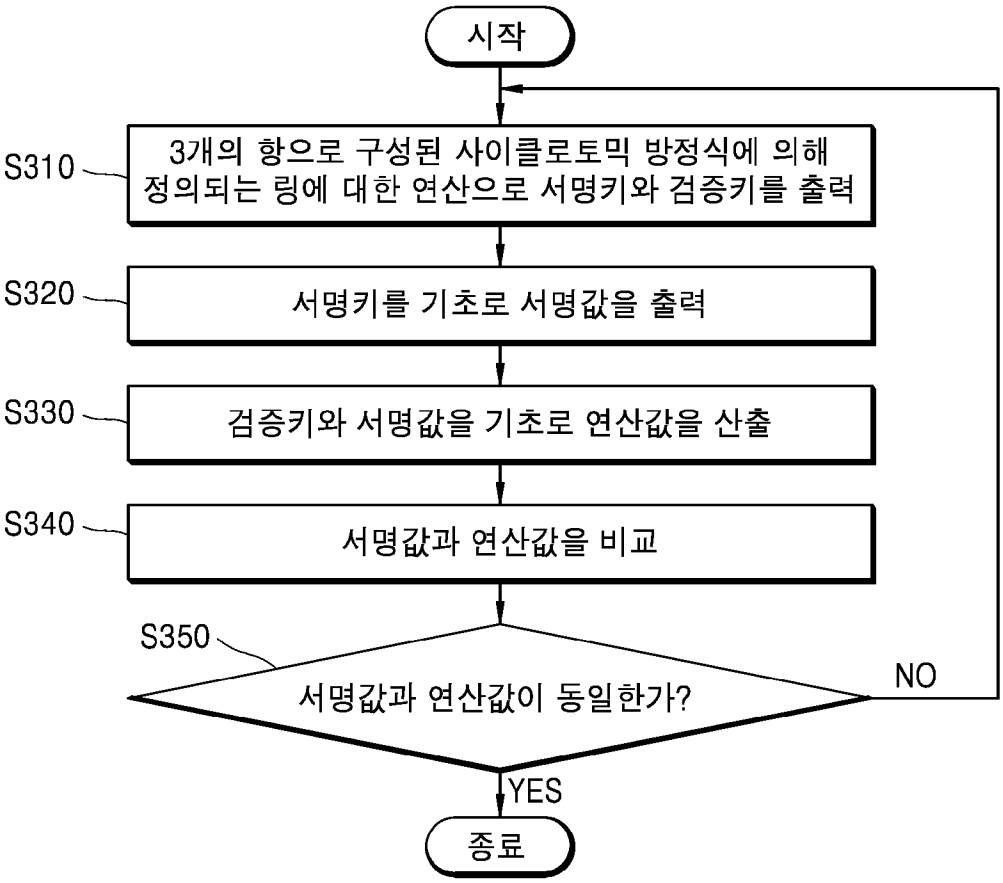
[도1]



[도2]


The number of sum
2n
0
n−1 degree
The number of sum
3n/2
Truncate
n/2
0
n−1 degree
The number of sum
n
0
n−1 degree

[도3]


시작
S310
3개의 항으로 구성된 사이클로토믹 방정식에 의해 정의되는 링에 대한 연산으로 서명키와 검증키를 출력
S320
서명키를 기초로 서명값을 출력
S330
검증키와 서명값을 기초로 연산값을 산출
S340
서명값과 연산값을 비교
S350
서명값과 연산값이 동일한가?
NO
YES
종료

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2020/013688

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32(2006.01)i; **H04L 9/30**(2006.01)i; **H04L 9/08**(2006.01)i; **G06F 7/552**(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)

H04L 9/32(2006.01); H04L 9/08(2006.01); H04L 9/14(2006.01); H04L 9/30(2006.01)

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: Ring-LWR(Ring-Learning With Roundings), 양자내성 서명(quantum-resistant signature), 트렁케이트(truncate), 사이클로토믹(cyclotomic)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	LEE, Joohee et al. RLizard: Post-Quantum Key Encapsulation Mechanism for IoT Devices. In: IEEE Access. 03 December 2018, pp. 2080-2091. See section II.	1-9
A	KR 10-2012-0071884 A (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE et al.) 03 July 2012 (2012-07-03) See paragraphs [0076]-[0087]; claim 1; and figure 2.	1-9
A	US 9698986 B1 (ISARA CORPORATION) 04 July 2017 (2017-07-04) See column 11, line 38 – column 14, line 26; claim 1; and figure 3.	1-9
A	CHOI, Piljoo et al. Fast and Power-Analysis Resistant Ring Lizard Crypto-Processor Based on the Sparse Ternary Property. In: IEEE Access. 16 July 2019, pp. 98684-98693. See section III.	1-9
A	AN, Hyeongcheol et al. QChain: Quantum-resistant and Decentralized PKI using Blockchain. In: 2018 Symposium on Cryptography and Information Security. 23 January 2018, pp. 1-8. See section 4.	1-9

☐ 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
"D" document cited by the applicant in the international application
"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
21 January 2021	**22 January 2021**

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

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2020/013688

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
KR 10-2012-0071884 A	03 July 2012	US 2012-0166808 A1	28 June 2012
US 9698986 B1	04 July 2017	US 10103886 B1	16 October 2018

국 제 조 사 보 고 서

국제출원번호
PCT/KR2020/013688

A. 발명이 속하는 기술분류(국제특허분류(IPC))

H04L 9/32(2006.01)i; **H04L 9/30**(2006.01)i; **H04L 9/08**(2006.01)i; **G06F 7/552**(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

H04L 9/32(2006.01); H04L 9/08(2006.01); H04L 9/14(2006.01); H04L 9/30(2006.01)

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: Ring-LWR(Ring-Learning With Roundings), 양자내성 서명(quantum-resistant signature), 트렁케이트(truncate), 사이클로토믹(cyclotomic)

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
A	JOOHEE LEE 등. RLizard: Post-Quantum Key Encapsulation Mechanism for IoT Devices. In: IEEE Access. 2018.12.03, 페이지 2080-2091. 섹션 II	1-9
A	KR 10-2012-0071884 A (한국전자통신연구원 등) 2012.07.03 단락 [0076]-[0087]; 청구항 1; 및 도면 2	1-9
A	US 9698986 B1 (ISARA CORPORATION) 2017.07.04 컬럼 11, 라인 38 – 컬럼 14, 라인 26; 청구항 1; 및 도면 3	1-9
A	PILJOO CHOI 등. Fast and Power-Analysis Resistant Ring Lizard Crypto-Processor Based on the Sparse Ternary Property. In: IEEE Access. 2019.07.16, 페이지 98684-98693. 섹션 III	1-9
A	HYEONGCHEOL AN 등. QChain: Quantum-resistant and Decentralized PKI using Blockchain. In: 2018 Symposium on Cryptography and Information Security. 2018.01.23, 페이지 1-8. 섹션 4	1-9

☐ 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
"D" 본 국제출원에서 출원인이 인용한 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
2021년01월21일(21.01.2021)	**2021년01월22일(22.01.2021)**

ISA/KR의 명칭 및 우편주소	심사관
대한민국 특허청 **(35208) 대전광역시 서구 청사로 189, 4동 (둔산동, 정부대전청사)**	**양정록**
팩스 번호 **+82-42-481-8578**	전화번호 **+82-42-481-5709**

국 제 조 사 보 고 서
대응특허에 관한 정보

국제출원번호
PCT/KR2020/013688

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2012-0071884 A	2012/07/03	US 2012-0166808 A1	2012/06/28
US 9698986 B1	2017/07/04	US 10103886 B1	2018/10/16