

(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2015년 3월 5일 (05.03.2015)



(10) 국제공개번호
WO 2015/030553 A1

- (51) 국제특허분류:
H04L 9/30 (2006.01) H04L 9/32 (2006.01)
- (21) 국제출원번호: PCT/KR2014/008144
- (22) 국제출원일: 2014년 9월 1일 (01.09.2014)
- (25) 출원언어: 한국어
- (26) 공개언어: 한국어
- (30) 우선권정보:
10-2013-0104107 2013년 8월 30일 (30.08.2013) KR
- (71) 출원인: 고려대학교 산학협력단 (KOREA UNIVERSITY RESEARCH AND BUSINESS FOUNDATION) [KR/KR]; 136-701 서울시 성북구 안암로 145, 고려대학교 (안암동 5가), Seoul (KR).
- (72) 발명자: 김기성 (KIM, Kee Sung); 133-851 서울시 성동구 자동차시장 1길 94-15, 606호 (용답동), Seoul (KR).
정익래 (JEONG, Ik Rae); 143-904 서울시 광진구 긴고랑로 4길 53, 203호 (중곡동, 호동아파트), Seoul (KR).
박소현 (PARK, So Hyeon); 136-788 서울시 성북구 종

암로 21길 127, 104동 904호 (종암동, 현대아이파크 1차아파트), Seoul (KR).

(74) 대리인: 특허법인 엠에이피에스 (MAPS INTELLECTUAL PROPERTY LAW FIRM); 137-810 서울시 서초구 사평대로 343, 4층 (반포동, 제일약품빌딩), Seoul (KR).

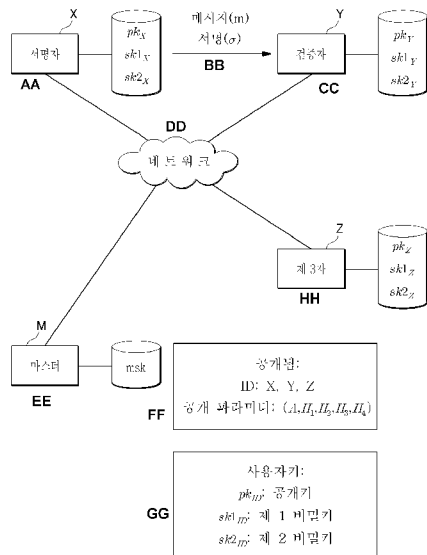
(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KZ, LA, LC, LK, LR, LS, LT, LU, LY, 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,

[다음 쪽 계속]

(54) Title: LATTICE-BASED CERTIFICATELESS SIGNATURE SYSTEM AND METHOD

(54) 발명의 명칭: 래티스 기반 인증서 비사용 서명 시스템 및 방법



AA ... Signer
BB ... Message(M), Signature(σ)
CC ... Verifier
DD ... Network
EE ... Master
FF ... Published: ID: X, Y, Z, public parameters: (A, H₁, H₂, H₃, H₄)
GG ... User key: pk_{ID}: public key, sk_{1ID}: first secret key, sk_{2ID}: second secret key
HH ... Third party

(57) Abstract: The present invention provides a digital signature system comprising: a master object for generating a first secret key by using a master key of the master object and published identification information of a user object, and then allocating the first secret key to the user object; and the user object for generating a public key of the user object and a second secret key, wherein the user object comprises: a signer object for transmitting, to a verifier object, a signature generated by using the public key, the first secret key and the second secret key of the signer object; and the verifier object for verifying the signature received from the signer object by using the published identification information of the signer object and the public key, and a trapdoor generated on the basis of the difficulty of a small integer solution (SIS) problem in a lattice is used for the generation of the master key, the first secret key and the second secret key.

(57) 요약서: 본 발명은 자신의 마스터 키 및 사용자 개체의 공개된 식별 정보를 사용하여, 제 1 비밀키를 생성하여 상기 사용자 개체에 할당하는 마스터 개체; 및 자신의 공개키 및 제 2 비밀키를 생성하는 사용자 개체;를 포함하되, 상기 사용자 개체는 상기 자신의 공개키, 제 1 비밀키, 및 제 2 비밀키를 사용하여 생성한 서명을 검증자 개체에게 전송하는 서명자 개체; 및 상기 서명자 개체로부터 수신한 서명을 상기 서명자 개체의 공개된 식별 정보, 및 공개키를 사용하여 검증하는 검증자 개체;를 포함하되, 상기 마스터 키, 제 1 비밀키, 및 상기 제 2 비밀키 생성에 래티스(lattice) 상에서의 SIS(small integer solution) 문제의 어려움에 기반하여 생성한 트랩도어(trapdoor)가 사용되는 전자 서명 시스템을 제공한다.



ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, **공개:**

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).

— 국제조사보고서와 함께 (조약 제 21 조(3))

명세서

발명의 명칭: 래티스 기반 인증서 비사용 서명 시스템 및 방법 기술분야

- [1] 본 발명은 전자 서명 시스템 및 방법에 관한 것이다.

배경기술

- [2] 전자서명 기술은 데이터에 대한 인증 및 무결성 보장 등에 사용되며 암호 분야에서 가장 널리 사용되는 기술 중 하나이다. 이러한 전자서명 기술에서 서명자는 주어진 메시지에 대해 자신의 비밀키를 사용해 서명을 생성하며, 검증자는 비밀키와 쌍을 이루는 공개키를 사용해 해당 서명의 정당성을 판단한다.
- [3] 이러한 환경에서 특정 공개키가 어떠한 사용자의 것인지를 증명하는 문제는 매우 중요하기 때문에 대부분의 환경에서는 신뢰할 수 있는 제3기관에서 발급하는 공인인증서를 통해 이러한 문제를 해결하고 있다.
- [4] 그러나 인증서 기반 전자 서명 시스템은 공인인증서 유지 관리를 위해 많은 비용을 감수해야하며, 이를 발급하는 기관은 막대한 트래픽을 처리해야 한다. 또한 인증서 자체에 대한 신뢰 문제도 가지고 있다.
- [5] 이에 따라 S. S. Al-Riyami와 K. G. Paterson가 2003년 ASIACRYPT에서 발표한 “Certificateless Public Key Cryptography”라는 제목의 논문은 인증서를 사용하지 않는 전자서명 기술을 제안하였다. 인증서를 사용하지 않으므로 전술한 여러 문제가 해결되어 종래의 인증서 기반 전자 서명 시스템보다 높은 효율성 및 안전성을 제공한다.
- [6] 한편, 서명의 안전성을 높이기 위해 기반이 되는 수학적 난제에 대한 연구도 많이 이루어졌다. 예를 들어, 이산 대수 문제의 어려움, 곱선형 함수의 어려움 등 평균적인 경우 어려운 문제(average-case hardness problems)들에서 최악의 경우에도 어려운 문제(worst-case hardness problems)로 알려진 래티스(lattice) 상에서의 SIS(small integer solution) 문제와 LWE(learning with errors) 문제의 어려움에 기반을 두는 서명 기법들로 발전하고 있다. 이러한 래티스 기반 암호화 기술은 높은 안전성뿐 아니라 연산 효율성 또한 제공한다. 특히 양자 컴퓨터 분석에 대해 내성이 있는 것으로 알려져 최근 이에 대한 연구가 크게 늘고 있다.
- [7] 따라서 래티스 기반의 암호 기술을 인증서 비사용 전자 서명 기술에 적용시킨다면, 더욱 높은 안전성과 효율성을 갖는 전자 서명 기술을 제공할 수 있을 것이다.
- [8] 전자 서명과 관련하여 한국 등록특허공보 제0369408호(발명의 명칭: "이동 통신에서의 수신자 지정 대리 서명 방법")에는 이산 대수 문제의 어려움에 기반을 둔 서명 생성 방법이 개시되어 있다.
- [9] 또한, 한국 공개특허공보 제2005-0128506호(발명의 명칭: "곱선형 사상을

이용한 한정적 검증자 서명 방법")에는 겹선형 사상을 이용한 지정된 검증자 서명 생성 방법이 개시되어 있다.

발명의 상세한 설명

기술적 과제

- [10] 본 발명은 전술한 문제를 해결하기 위한 것으로서, 그 목적은 높은 안전성 및 효율성을 갖는 전자 서명 시스템 및 방법을 제공하는 것이다.

과제 해결 수단

- [11] 상기와 같은 목적을 달성하기 위한 본 발명의 제 1 측면에 따른 전자 서명 시스템은 자신의 마스터 키 및 사용자 개체의 공개된 식별 정보를 사용하여, 제 1 비밀키를 생성하여 상기 사용자 개체에게 할당하는 마스터 개체; 및 자신의 공개키 및 제 2 비밀키를 생성하는 사용자 개체;를 포함하되, 상기 사용자 개체는 상기 자신의 공개키, 제 1 비밀키, 및 제 2 비밀키를 사용하여 생성한 서명을 검증자 개체에게 전송하는 서명자 개체; 및 상기 서명자 개체로부터 수신한 서명을 상기 서명자 개체의 공개된 식별 정보, 및 공개키를 사용하여 검증하는 검증자 개체;를 포함하되, 상기 마스터 키, 제 1 비밀키, 및 상기 제 2 비밀키 생성에 래티스(lattice) 상에서의 SIS(small integer solution) 문제의 어려움에 기반하여 생성한 트랩도어(trapdoor)가 사용되는 것을 특징으로 한다.
- [12] 상기와 같은 목적을 달성하기 위한 본 발명의 제 2 측면에 따른 전자 서명 방법은 (a) 마스터 개체가 보안 파라미터를 설정하고 자신의 마스터 키를 생성하는 단계; (b) 상기 마스터 개체가 서명자 개체 및 검증자 개체를 포함하는 사용자 개체의 공개된 식별 정보에 기초하여, 제 1 비밀키를 생성하여 상기 사용자 개체에게 할당하는 단계; (c) 상기 사용자 개체가 자신의 공개키 및 제 2 비밀키를 생성하는 단계; (d) 상기 서명자 개체가 자신의 공개키, 제 1 비밀키, 및 제 2 비밀키를 사용하여 생성한 서명을 검증자 개체에게 전송하는 단계; 및 (e) 상기 검증자 개체가 상기 서명자 개체로부터 수신한 서명을 상기 서명자 개체의 공개된 식별 정보, 및 공개키를 사용하여 검증하는 단계;를 포함하되, 상기 마스터 키, 제 1 비밀키, 및 상기 제 2 비밀키 생성에 래티스(lattice) 상에서의 SIS(small integer solution) 문제의 어려움에 기반하여 생성한 트랩도어(trapdoor)가 사용되는 것을 특징으로 한다.

발명의 효과

- [13] 본 발명은 높은 안전성 및 효율성을 갖는 전자 서명 시스템 및 방법을 제공한다.
- [14] 구체적으로, 본 발명은 인증서를 사용하지 않기 때문에 인증서 기반 전자 서명 시스템이 갖는 인증서 관리 비용 및 안전성 문제가 없으며, 공인 인증 기관을 전적으로 신뢰하지 않아도 된다.
- [15] 또한, 본 발명은 최악의 경우에도 어려운 수학적 난제인 래티스 상에서의 SIS 문제의 어려움에 기반을 두고 있으므로, 안전성이 높다.
- [16] 래티스 기반으로 설계되었기 때문에 래티스 기반 암호 시스템이 갖는 연산

효율성, 높은 안전성, 양자 컴퓨터 분석에 대한 내성의 장점을 나타낸다. 따라서 현재까지 알려진 무인증서 기반, 즉, 인증서 비사용 전자 서명 기법 중 가장 높은 안전성을 갖는다.

도면의 간단한 설명

- [17] 도 1은 본 발명의 일실시예에 따른 전자 서명 시스템의 구조를 도시함.
- [18] 도 2는 도 1의 시스템의 구조를 다른 관점에서 도시함.
- [19] 도 3는 본 발명의 일실시예에 따른 전자 방법의 흐름을 도시함.
- [20] 도 4은 본 발명의 일실시예에 따른 시스템 설정 방법의 흐름을 도시함.
- [21] 도 5는 본 발명의 일실시예에 따른 제 1 비밀키 발급 방법의 흐름을 도시함.
- [22] 도 6은 본 발명의 일실시예에 따른 공개키 및 제 2 비밀키 생성 방법의 흐름을 도시함.
- [23] 도 7은 본 발명의 일실시예에 따른 서명 방법의 흐름을 도시함.
- [24] 도 8은 본 발명의 일실시예에 따른 검증 방법의 흐름을 도시함.
- [25] 도 9는 본 발명의 일실시예에 따른 트랩도어 생성 방법의 흐름을 도시함.
- [26] 도 10은 본 발명의 일실시예에 따른 트랩도어 확장 방법의 흐름을 도시함.
- [27] 도 11은 본 발명의 일실시예에 따른 가우시안 샘플링 방법의 흐름을 도시함.

발명의 실시를 위한 형태

- [28] 아래에서는 첨부한 도면을 참조하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 본 발명의 실시예를 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.
- [29] 명세서 전체에서, 어떤 부분이 다른 부분과 "연결"되어 있다고 할 때, 이는 "직접적으로 연결"되어 있는 경우뿐 아니라, 그 중간에 다른 소자를 사이에 두고 "전기적으로 연결"되어 있는 경우도 포함한다. 또한 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다.
- [30] 전술한 바와 같이 무인증서 기반인 인증서 비사용 전자 서명 시스템은 종래의 인증서 기반 전자 서명 시스템이 갖고 있는 인증서를 유지, 관리하는 비용이 크다는 문제 및 유출이나 조작 등 인증서 관련 사고가 발생한다는 문제 등을 해결하였다.
- [31] 이제까지 이러한 무인증서 기반 전자 서명 시스템은 인수 분해, 이산 대수, 페어링(pairing)을 기반으로 설계되었다. 하지만 풀기 어려워 안전하다고 여겨지던 이러한 문제들은 최근 양자 알고리즘의 발전으로 더 이상 안전성을 보장할 수 없다.

- [32] 이에 따라 양자 분석에 내성이 있는 것으로 알려진 래티스 기반 암호 시스템에 대한 관심이 점차 높아지고 있다.
- [33] 기존의 래티스 기반의 암호 시스템의 경우 안전성 증명이 결여되어 많은 문제점이 있었으나, 최근 최악의 경우(worst-case) 문제에 기반하여 증명되는 래티스 기반의 암호 시스템들이 등장하고 있다. 기존의 암호 시스템이 평균적인 경우(average-case) 문제에 기반하여 설계된 점을 비추어 볼 때 매우 높은 안전성을 제공한다는 것을 알 수 있다.
- [34] 이 뿐만 아니라 래티스 기반 암호 시스템은 종래 기법에 비해 매우 효율적이다. 인수 분해, 이산 대수, 페어링 등의 연산 복잡도는 $O(n^3)$ 이지만, 래티스에서의 연산 복잡도는 $O(n^2)$ 이다.
- [35] 따라서 본 발명은 래티스 환경에서 안전성 증명이 가능한 무인증서 기반 전자 서명 기술을 제공하고자 한다.
- [36] 도 1 및 도 2는 본 발명의 일실시예에 따른 전자 서명 시스템의 구조를 도시하고 있다.
- [37] 본 발명의 일실시예에 따른 전자 서명 시스템(10)에는 네트워크를 통해 연결된 서명자(X), 검증자(Y), 및 제3자(Z)를 포함하는 사용자와 마스터(M) 등의 개체(entity)가 참여한다.
- [38] 사용자 중, 서명자(X)는 메시지에 서명하여 검증자(Y)에게 전송하는 개체이며, 검증자(Y)는 서명자(X)로부터 수신한 서명을 검증하는 개체이다. 이때, 검증이란 전송한 바와 같이, 수신한 서명이 서명자(X)에 의해 생성된, 유효한 서명임을 확인하는 것이다.
- [39] 서명을 생성하여 전송한 서명자(X)와 서명을 수신한 검증자(Y) 이외의 다른 사용자인 제3자(Z)는 해당 서명을 검증할 수 없다.
- [40] 도면에는 각각 하나의 서명자(X), 검증자(Y), 및 제3자(Z) 개체만이 도시되어 있고, 이들이 서로 다른 개체인 것처럼 도시되어 있다. 그러나 서명자(X), 검증자(Y), 및 제3자(Z)는 모두 사용자 개체로서, 이들의 역할은 고정적이지 않으며, 전자 서명 시스템(10)에 참여하는 사용자 개체의 수에도 제한이 없을 것임을 쉽게 이해할 수 있을 것이다. 또한, 이들 각 사용자 개체는 사용자가 사용하는 기기나 소프트웨어 등의 실체를 의미할 수 있다. 이는 통용되는 개념이므로 본 명세서에서 이에 대한 명시적 기재는 생략한다. 예를 들어, 이 하 기술에서 사용자라 함은 서명자(X), 검증자(Y), 제3자(Z) 등의 사용자 개체를 나타낼 수 있다.
- [41] 전송한 바와 같이, 본 발명의 일실시예에 따른 전자 서명 시스템(10)에는 각 사용자의 제 1 비밀키를 생성하여 해당 사용자에게 배포하는 마스터(M) 개체가 참여한다. 여기에서 마스터(M)는 키 생성 기관(Key Generation Center), 인증 기관(Certification Authority) 등 다양한 이름으로 불릴 수 있으며, 전자 서명 시스템(10)이 원활하게 운영되도록 관리하는 기관들을 통칭하는 개념으로

사용하였다.

- [42] 종래의 공개키 기반 환경에서는 전술한 바와 같이, 마스터(M)가 각 사용자에게 공인 인증서를 발급해야 하지만, 본 발명의 일실시예에 따른 전자 서명 시스템(10)은 마스터(M)가 사용자(X, Y, Z)의 공개된 식별정보(ID)를 사용하여 사용자(X, Y, Z)에게 제 1 비밀키를 발급해준다. 그렇기 때문에, 전자 서명 시스템(10)은 마스터(M)와 사용자(X, Y, Z) 모두 공인 인증서를 관리할 필요가 없어, 효율적이고 안전성이 높다. 이는, 전자 서명 시스템(10)이 공인 인증서 관리에 따른 비용이나 부하가 없고, 공인 인증서 도용 등과 같은 보안 위험이 없기 때문이다. 또한 후술하는 바와 같이, 전자 서명 시스템(10)은 사용자(X, Y, Z)는 마스터(M)에게 노출되지 않는 또 다른 비밀키인 제 2 비밀키를 스스로 생성하므로, 안정성이 더욱 높다.
- [43] 종래와 달리 공인 인증서를 사용하지 않으나, 본 발명의 일실시예에 따른 전자 서명 시스템(10)은 공개키 기반 방식이다.
- [44] 공개키 기반 방식은 서로 대응되는 키 쌍을 생성하여, 이중 공개키는 암호화 또는 서명 확인용으로 사용하며, 비밀키는 복호화 또는 서명용으로 사용하는 비대칭형 암호화 또는 서명 방식이다.
- [45] 공개키 기반 방식은 해당 메시지를 보낸 사용자가 누구인가를 증명하기 위한 것이므로, 어떤 메시지에 서명할 때는 비밀키로 서명하고 대응되는 공개키로 이를 확인한다. 즉, 비밀키는 문서에 찍는 도장과 같은 기능을 한다.
- [46] 한편 전술한 바와 같이, 암호화 및 전자 서명 시스템은 특정 정보가 없으면 풀기 어려운 수학적 난제에 기반하여 구축된다. 본 발명의 일실시예에 따른 전자 서명 시스템(10)은 래티스(lattice) 상에서의 SIS(small integer solution) 문제와 LWE(learning with errors) 문제의 어려움에 기반하고 있다.
- [47] 특정 정보가 없으면 풀기 어렵다는 것은 연산이 일방향성이라는 의미이다. 일방향성은 연산은 쉬워도 연산의 역을 구하는 것은 어렵다. 그러나 특정 정보를 갖고 있는 경우에는 쉽게 역을 구할 수 있음을 나타낸다. 이러한 특정 정보를 트랩도어(trapdoor)라고 부른다.
- [48] 예를 들어, 공개키 기반 환경에서 암호화 연산은 암호화는 쉽다. 그러나 암호화 시 사용한 암호화 키에 대응하는 복호화 키가 없는 경우에는 암호화의 역변환인 복호화는 매우 어려운 일방향성 연산을 사용하여 수행된다. 즉, 암호화 시 사용한 암호화 키에 대응되는 복호화 키가 트랩도어이다. 일단 메시지를 암호화하고 나면 암호화 키가 있어도 이를 복호화할 수 없으므로, 암호화 키는 공개되어도 된다. 반면, 트랩도어 또는 복호화 키는 공개되면 안 된다. 따라서, 공개키 기반 환경에서 트랩도어를 생성하는 데 사용된 정보는 공개키로서 공개되고, 트랩도어는 비밀키로서 공개되지 않는다.
- [49] 래티스에 기반한 SIS 문제와 LWE 문제는 전술한 바와 같이 최악의 경우에서도 풀기 어려운 수학적 난제이므로, 최근 암호화 및 전자 서명 시스템에 이를 적용하려는 시도가 많이 이루어지고 있는 추세이다. 래티스는 공간에서 2개의

기저의 선형 결합을 통해 만들어지는 모든 점의 집합이다. 기저를 모르면 제3자(Z)가 어떤 점을 알아내었다고 해도 해당 점으로부터 가장 가까운 래티스 점이 어딘지 알아내는 것은 매우 어렵다는 장점이 있다. 또한, 기저를 모르면 제3자(Z)는 특정 길이 이내의 래티스 점을 찾는 것이 매우 어렵다는 장점이 있다.

[50] 따라서 본 발명의 일실시예에 따른 전자 서명 시스템(10)은 자신의 마스터 키 및 사용자 개체(X, Y, Z)의 공개된 식별 정보를 사용하여, 제 1 비밀키를 생성하여 사용자 개체(X, Y, Z)에게 할당하는 마스터 개체(M)를 포함한다. 또한, 전자 서명 시스템(10)은 자신의 공개키 및 제 2 비밀키를 생성하는 사용자 개체(X, Y, Z)를 포함한다. 그리고 전자 서명 시스템(10)은 사용자 개체(X, Y, Z)는 자신의 공개키, 제 1 비밀키, 및 제 2 비밀키를 사용하여 생성한 서명을 검증자 개체(Y)에게 전송하는 서명자 개체(X) 및 서명자 개체(X)로부터 수신한 서명을 서명자 개체(X)의 공개된 식별 정보, 및 공개키를 사용하여 검증하는 검증자 개체(Y)를 포함한다. 이때 마스터 키, 제 1 비밀키, 및 제 2 비밀키 생성에 래티스(lattice) 상에서의 SIS(small integer solution) 문제의 어려움에 기반하여 생성한 트랩도어(trapdoor)가 사용된다.

[51] 도 2에 도시되어 있는 바와 같이, 이를 위해 트랩도어 생성부(L100), 트랩도어 확장부(L200) 및 샘플링부(L300)를 포함하는 라이브러리(L)를 포함하거나 이에 연결될 수 있다. 이때, 트랩도어 생성부(L100)는 마스터(M) 및 각 사용자(A, B, C)는 균일한 분포(uniform distribution)에서 선택된 임의의 행렬로부터 생성되는 래티스의 짧은 기저(short basis)인 트랩도어를 생성할 수 있다. 또한, 트랩도어 확장부(L200)는 트랩도어의 래티스를 또 다른 래티스로 확장하고 또 다른 래티스의 짧은 기저인 확장된 트랩도어를 생성할 수 있다. 샘플링부(L300)는 트랩도어 확장부(L200), 및 트랩도어의 가우시안 분포로부터 벡터를 샘플링할 수 있다.

[52] 다시 말해 라이브러리(L)는 래티스 상에서의 SIS 문제의 어려움에 기반하여 트랩도어를 생성, 확장, 및 사용하기 위한 기본 기능을 본 발명의 일실시예에 따른 전자 서명 시스템(10)의 각 개체(M, X, Y, Z)에 제공한다.

[53] 이들 트랩도어 생성부(L100), 트랩도어 확장부(L200), 및 샘플링부(L300)가 수행하는 동작은 도 9 내지 도 11에 도시되어 있다.

[54] 마스터(M)의 시스템 설정부(100)는 보안 파라미터를 설정하고, 일련의 해시 함수를 선택하며, 트랩도어 생성부(L100)를 사용하여 생성한 트랩도어를 자신의 비밀키인 마스터 키로 사용한다. 또한, 시스템 설정부(100)는 함께 생성된 대응 행렬을 해시 함수와 함께 공개한다.

[55] 마스터의 키 발급부(200)는 트랩도어 확장부(L200)를 사용하여 사용자의 공개된 식별 정보로부터 생성된 확장된 트랩도어를 사용자의 제 1 비밀키로 발급한다.

[56] 사용자의 키 생성부(300)는 트랩도어 생성부(L100)를 사용하여 생성한 트랩도어를 자신의 제 2 비밀키로 사용하고, 함께 생성된 대응 행렬을 자신의

공개키로 사용한다.

[57] 그러므로, 전술한 바와 같이, 사용자의 제 2 비밀키는 마스터(M)와 전혀 무관하게 사용자 자신이 생성하므로, 본 발명의 일실시예에 따른 전자 서명 시스템(10)은 마스터(M)를 전적으로 신뢰하지 않아도 되는 장점을 가진다.

[58] 사용자 중 서명자(X)는 서명부(400)를 사용하여 자신의 제 1 비밀키 및 공개키를 사용하여 제 1 서명을 생성하고, 자신의 제 2 비밀키 및 공개키를 사용하여 제 2 서명을 생성한다. 또한, 서명자(X)는 제 1 서명과 제 2 서명을 사용하여 서명을 생성하며, 이때 트랩도어 생성부(L100), 트랩도어 확장부(L200), 샘플링부(L300)를 사용한다.

[59] 서명자(X)는 제 1 비밀키의 가우시안 분포로부터 벡터를 샘플링하여 제 1 서명을 생성하며, 제 2 비밀키의 래티스를 공개키를 사용하여 확장된 래티스로 확장한다. 그리고 서명자(X)는 확장된 래티스의 짧은 기저인 확장된 트랩도어를 생성하여, 확장된 트랩도어의 가우시안 분포로부터 벡터를 샘플링하여 제 2 서명을 생성한다.

[60] 사용자 중 검증자(Y)는 검증부(500)를 사용하여 서명자(X)의 공개된 식별 정보, 및 공개키를 사용하여 제 1 서명 및 제 2 서명을 각각 검증한다. 또한, 검증자(Y)는 제 1 서명 및 제 2 서명이 모두 정당한 서명이라고 판단되었을 때 수신한 서명을 받아들이고 그렇지 않으면 기각한다.

[61] 따라서 본 발명의 일실시예에 따른 전자 서명 시스템(10)의 각 개체는 도 1의 각 개체에 연결된 키 저장소에 도식되어 있는 것과 같은 키들을 가진다.

[62] 마스터(M)는 마스터 키(msk)를 가지며, 이는 외부에 공개되어서는 안되는 비밀키이다. 반면 대응하는 행렬은 해시 함수들과 함께 공개 파라미터 (A, H_1, H_2, H_3, H_4) 로서 공개된다.

[63] 각 사용자(X, Y, Z)의 식별 정보와 공개키도 공개된다. 반면 각 사용자(X, Y, Z)의 제 1 비밀키 및 제 2 비밀키는 공개되지 않는다.

[64] 도 3는 본 발명의 일실시예에 따른 전자 방법의 흐름을 도시하고 있다.

[65] 마스터 개체(M)는 보안 파라미터를 설정하고 자신의 마스터 키를 생성한다(S100).

[66] 마스터 개체(M)는 서명자 개체(X) 및 검증자 개체(Y)를 포함하는 사용자 개체(X, Y, Z)의 공개된 식별 정보에 기초하여, 제 1 비밀키를 생성하여 사용자 개체(X, Y, Z)에게 할당한다(S200).

[67] 사용자 개체(X, Y, Z)는 자신의 공개키 및 제 2 비밀키를 생성한다(S300).

[68] 서명자 개체(X)는 자신의 공개키, 제 1 비밀키, 및 제 2 비밀키를 사용하여 생성한 서명을 검증자 개체(Y)에게 전송한다(S400).

[69] 검증자 개체(Y)는 서명자 개체(X)로부터 수신한 서명을 서명자 개체(X)의 공개된 식별 정보, 및 공개키를 사용하여 검증한다(S500).

[70] 이하 도 4 내지 도 8을 통해 각 단계를 좀더 자세히 설명한다.

[71] 도 4은 본 발명의 일실시예에 따른 시스템 설정 방법의 흐름을 도시하고 있다.

- [72] 마스터(M)는 해시 함수를 선택한다(S110).
- [73] 시스템 설정 방법은 트랩도어 생성부(L100)를 사용하여, 행렬 A 및 대응하는 트랩도어를 생성한다(S120). 트랩도어는 행렬 A에 기초하여 생성되는 래티스의 짧은 기저(short basis)이다.
- [74] 시스템 설정 방법은 공개 파라미터로 행렬 A 및 해시 함수를 출력한다(S130).
- [75] 생성된 트랩도어를 마스터 키로 사용한다(S140).
- [76] 다시 말해, 시스템 설정 단계(S100)는 시스템에서 사용할 다양한 파라미터를 정하고 키를 발급하는 기관인 마스터(M)의 마스터 키를 정하는 단계이다.
- [77] 먼저, 다음과 같은 성질을 만족하는 충돌내성 해쉬 함수(collision-resistant hash function)를 선택한다.
- [78] $H_1: \{0,1\}^* \rightarrow Z_q^{n \times m}$
- [79] $H_2: Z_q^{n \times m} \times \{0,1\}^* \times \{0,1\}^* \rightarrow Z_q^n$
- [80] $H_3: \{0,1\}^* \times Z^m \times \{0,1\}^* \times \{0,1\}^* \rightarrow Z_q^{n \times m}$
- [81] $H_4: \{0,1\}^* \times \{0,1\}^* \rightarrow Z_q^n$
- [82] 그리고 마스터(M)는 $(A \in Z_q^{n \times m}, S_A \in Z_q^{m \times m}) \leftarrow \text{GBasis}(1^n, 1^m, q)$ 을 생성하여 공개 파라미터 $param = (A, H_1, H_2, H_3, H_4)$ 와 마스터키 $msk = S_A$ 를 정한다.
- [83] 도 5는 본 발명의 일실시예에 따른 제 1 비밀키 발급 방법의 흐름을 도시하고 있다.
- [84] 마스터(M)가 사용자 ID를 입력 받는다(S210).
- [85] 사용자 ID를 해시하여 행렬 B를 산출한다(S220).
- [86] 트랩도어 확장부(L200)를 사용하여, 마스터 키를 행렬 B에 기초하여 확장한다(S230).
- [87] 확장된 마스터 키를 ID에 대한 제 1 비밀키로서 사용자(X, Y, Z)에게 전달한다(S240).
- [88] 다시 말해, 제 1 비밀키 발급 단계(S200)는 마스터(M)가 자신의 마스터 키를 이용해 주어진 ID에 대한 제 1 비밀키를 발급해주는 단계이다.
- [89] 마스터(M)는 $B \in Z_q^{n \times m} = H_1(ID)$ 을 계산하고, $S_{A||B} \in Z_q^{m \times m} \leftarrow \text{BasisDel}(A, B, S_A)$ 알고리즘을 실행한 후, $S_{A||B}$ 을 ID에 대한 제 1 비밀키로 정하고, 안전한 방법으로 해당 ID의 서명자에게 키를 전달한다.
- [90] 도 6은 본 발명의 일실시예에 따른 공개키 및 제 2 비밀키 생성 방법의 흐름을 도시하고 있다.
- [91] 후술하는 바와 같이, 사용자(X, Y, Z)는 마스터(M)와 완전히 독립적으로 자신의 공개키 및 제 2 비밀키를 생성한다. 그러므로 전술한 바와 같이 사용자(X, Y, Z)는 마스터(M)를 전적으로 신뢰하지 않아도 되며 제 2 비밀키가

마스터(M)에게 알려지지 않으므로, 본 발명의 일실시예에 따른 전자 서명 방법은 안전성이 높다.

- [92] 사용자(X, Y, Z)가 트랩도어 생성부(L100)를 사용하여, 행렬 C 및 대응하는 트랩도어를 생성한다(S310). 트랩도어는 행렬 C에 기초하여 생성되는 래티스의 짧은 기저(short basis)이다.
- [93] 행렬 C를 자신의 공개키로 사용한다(S320).
- [94] 생성된 트랩도어를 제 2 비밀키로 사용한다(S330).
- [95] 다시 말해, 공개키 및 제 2 비밀키 생성 단계(S300)는 ID에 해당하는 사용자(X, Y, Z)가 자신의 공개키와 제 2 비밀키를 생성하는 단계이다.
- [96] 사용자(X, Y, Z)는 $(C \in \mathbb{Z}_q^{n \times m}, S_C \in \mathbb{Z}_q^{m \times m}) \leftarrow \text{GBasis}(1^n, 1^m, q)$ 알고리즘을 실행한 후, C를 자신의 ID에 대한 공개키로 S_C 를 ID에 대한 제 2 비밀키로 출력한다.
- [97] 주목할 점은 전술한 바와 같이 마스터(M)는 사용자(X, Y, Z)의 제 1 비밀키는 직접 생성하였으므로 알 수 있으나, 제 2 비밀키는 사용자(X, Y, Z)가 직접 생성하였기 때문에 알 수 없다. 따라서 아무리 마스터(M)라고 해도 제 2 비밀키를 모르는 이상 서명자(X)의 서명을 생성할 수 없다. 이와 같이 본 발명의 일실시예에 따른 인증서 비사용 전자 서명 시스템(10)은 마스터(M)를 전적으로 신뢰하지 않아도 되는 장점을 가진다.
- [98] 도 7은 본 발명의 일실시예에 따른 서명 방법의 흐름을 도시하고 있다.
- [99] 서명자(X)가 메시지 m을 입력 받는다(S410).
- [100] 샘플링부(L300)를 사용하여 자신의 비밀키로부터 제 1 서명을 생성한다(S420). 이때 자신의 공개키를 메시지, 임의의 문자열과 함께 해시한 값이 사용된다.
- [101] 트랩도어 확장부(L200)를 사용하여 자신의 제 2 비밀키를 확장한다(S440).
- [102] 샘플링부(L300)를 사용하여 자신의 확장된 제 2 비밀키로부터 제 2 서명을 생성한다(S450). 이때 메시지와 또 다른 임의의 문자열을 함께 해시한 값이 사용된다.
- [103] 제 1 서명과 제 2 서명을 사용하여 서명을 생성한다(S460).
- [104] 생성한 서명을 검증자(Y)에게로 발송한다(S470).
- [105] 다시 말해, 서명 단계(S400)는 ID에 해당하는 서명자(X)가 자신의 제 1 비밀키 S_{pub} 와 제 2 비밀키 S_C 를 사용하여 주어진 메시지에 대한 서명을 생성하는 단계이다. 서명자(X)는 메시지 m에 대한 서명을 다음과 같이 생성한다.
- [106] 먼저, $\sigma_1 \in \mathbb{Z}^m \leftarrow \text{SampleD}(S_{\text{pub}}, H_2(C, m, r_1), s)$ 을 계산한다. 여기서 r_1 은 서명자(X)가 선택한 임의의 문자열이며, 파라미터 s는 SampleD 알고리즘에 쓰이는 파라미터다.
- [107] 그 후, $D \in \mathbb{Z}_q^{n \times m} = H_3(ID, \sigma_1, m, r_1)$ 을 계산하여, 자신의 제 2 비밀키 S_C 을 이용해 $S_{\text{priv}} \leftarrow \text{BasisDel}(C, D, S_C)$ 알고리즘을 실행한 후, 생성한 S_{priv} 을 사용하여

$\sigma_2 \in \mathbb{Z}^m \leftarrow \text{SampleD}(S_{\text{clID}}, H_4(m, r_2), s)$ 을 계산한다. 여기서 r_2 역시 서명자(X)가 선택한 임의의 문자열이며, 동일한 파라미터 s 를 사용한다.

- [108] 최종적으로 전자 서명은 $\sigma = (ID, C, m, \sigma_1, \sigma_2, r_1, r_2)$ 으로 구성된다.
- [109] 도 8은 본 발명의 일실시예에 따른 검증 방법의 흐름을 도시하고 있다.
- [110] 검증자(Y)가 서명자(X)의 서명을 입력 받는다(S510).
- [111] 서명자의 ID 및 공개키를 사용하여 제 1 서명에 대해 도시되어 있는 바와 같은 기 지정된 조건을 만족하는지 판단한다(S520).
- [112] 서명자의 ID 및 공개키를 사용하여 제 1 서명에 대해 도시되어 있는 바와 같은 기 지정된 조건을 만족하는지 판단한다(S530).
- [113] 제 1 서명 조건 및 제 2 서명 조건을 모두 만족할 경우 서명은 검증되며, 하나라도 만족하지 못할 경우 서명은 기각된다(S540).
- [114] 다시 말해, 검증 단계(S500)는 ID에 해당하는 서명자(X)가 보내온 서명을 검증자(Y)가 검증하는 단계이다.
- [115] 주어진 서명 $\sigma = (ID, m, \sigma_1, \sigma_2, r_1, r_2, C)$ 은 다음과 같은 조건을 만족할 때 정당하다.
- [116] $\sigma_1 \neq 0, \|\sigma_1\| \leq s\sqrt{2m}$ 그리고 $[A \| H_1(ID)]\sigma_1 = H_2(C, m, r_1)$
- [117] $\sigma_2 \neq 0, \|\sigma_2\| \leq s\sqrt{2m}$ 그리고 $[C \| H_3(ID, \sigma_1, m, r_1)]\sigma_2 = H_4(m, r_2)$
- [118] 이하 도 9 내지 도 11을 통해 본 발명의 일실시예에 따른 전자 서명 방법이 키 발급 및 서명에 사용하기 위해 래티스 상에서의 SIS 문제의 어려움에 기반하여 트랩도어를 생성, 확장, 및 샘플링하는 방법을 구체적으로 설명한다.
- [119] 본 발명은 m 차원의 풀-랭크(full-rank) 정수 래티스를 사용하며, 이것은 유한개의 지수(finite index)를 가지는 $\mathbb{Z}^m$ 의 이산 가산 서브그룹(discrete additive subgroup)이다. 즉, 몫군(quotient group) $\mathbb{Z}^m/\Lambda$ 이 유한하다.
- [120] 하나의 래티스 $\Lambda \subseteq \mathbb{Z}^m$ 은 m 개의 선형 독립 기저(basis) 벡터 $B = \{b_1, \dots, b_m\} \subset \mathbb{Z}^m$ 의 모든 정수 선형 결합의 집합과 동일하게 정의된다.
- [121] $\Lambda = L(B) = \left\{ Bc = \sum_{i \in \{1, \dots, m\}} c_i b_i : c \in \mathbb{Z}^m \right\}$
- [122] 여기서 $m \geq 2$ 경우, 동일한 래티스를 생성하는 기저들은 무수히 많다.
- [123] 본 발명은 다음과 같은 정수 래티스의 특정한 형태를 사용한다. 여기서 $n \geq 1$ 과 $q \geq 2$ 는 정수이며, 차원 n 은 본 발명에서 사용되는 시큐리티 파라미터이고, 모든 다른 파라미터들은 n 의 함수들로 내포되었다고 가정한다. 여기서 m 차원 하드 래티스는 패리티 검사 행렬(parity check matrix) $A \in \mathbb{Z}_q^{n \times m}$ 에 의해 생성되며, 다음과 같이 정의된다.

- [124] $\Lambda^\perp(A) = \left\{ x \in \mathbb{Z}^m : Ax = \sum_{j \in \{1, \dots, m\}} x_j \cdot a_j = 0 \in \mathbb{Z}_q^n \right\} \subseteq \mathbb{Z}^m$
- [125] 어떤 y 에 대해서, 패리티 검사 행렬 $A \in \mathbb{Z}_q^{n \times m}$ 에 의해 생성되는 코셋(coset)은 다음과 같이 정의된다.
- [126] $\Lambda_y^\perp(A) = \{ x \in \mathbb{Z}^m : Ax = y \in \mathbb{Z}_q^n \}$
- [127] 어떤 고정된 상수 $C > 1$ 과 어떤 $m \geq Cn \lg q$ 에 대해, 균등하게 랜덤 한(uniformly random) $A \in \mathbb{Z}_q^{n \times m}$ 의 열 벡터는 $\mathbb{Z}_q^n$ 상의 모두를 ($2^{-\Omega(n)} = \text{negl}(n)$ 확률을 제외하고) 생성할 수 있다. 따라서 본 발명은 균등하게 랜덤 한 A 를 사용한다.
- [128] 본 발명이 기반하는 하드 래티스의 (short integer solution) 문제는 평균적인 경우에 어려운 문제(average-case hardness problems)에 속해있으며, Miklos Ajtai는 이 문제를 최악의 경우에 어려운 문제(worst-case hardness problems)로 커넥션(connection)하는 방법을 발견하였다.
- [129] 래티스의 SIS 문제는 (l_2 norm에서의) $SIS_{q,\beta}$ 문제는 어떤 $m = \text{poly}(n)$ 에 대해 균등하게 랜덤한 행렬 $A \in \mathbb{Z}_q^{n \times m}$ 을 입력으로 받아 $\|v\|_2 \leq \beta$ 와 $Av = 0 \in \mathbb{Z}_q^n$ (즉, $v \in \Lambda^\perp(A)$)을 만족하는 영이 아닌(nonzero) 정수 벡터 $v \in \mathbb{Z}^m$ 를 찾는 것으로 정의된다.
- [130] 도 9는 본 발명의 일실시예에 따른 트랩도어 생성 방법의 흐름을 도시하고 있다.
- [131] 보안 파라미터를 입력 받는다(SL110).
- [132] 균등한 분포에서 임의의 행렬을 선택한다(SL120).
- [133] 행렬로부터 래티스를 생성한다(SL130).
- [134] 래티스의 짧은 기저를 산출한다(SL140).
- [135] 산출된 짧은 기저를 트랩도어로서 행렬과 함께 출력한다(SL150).
- [136] 다시 말해, 트랩도어 생성부(L100)는 균등한 분포에서 임의로 선택된 매트릭스 $A \in \mathbb{Z}_q^{n \times m}$ 와 이러한 매트릭스로 생성되는 래티스 $\Lambda^\perp(A)$ 의 짧은 기저 S 를 생성하는 알고리즘 $(A \in \mathbb{Z}_q^{n \times m}, S \in \mathbb{Z}_q^{m \times m}) \leftarrow \text{GBasis}(1^n, 1^m, q)$ 을 제공한다.
- [137] 임의의 래티스의 짧은 기저를 찾는 문제는 결국 SIS 문제이기 때문에 알고리즘 $\text{GBasis}(1^n, 1^m, q)$ 은 임의의 래티스와 그것의 트랩도어(SIS 문제에 대한) 즉, 짧은 기저를 생성하게 된다.
- [138] 이때 파라미터들은 $m = O(n \log q)$ 을 만족하며, 기저 s 의 길이는 $\|\tilde{s}\| = O(\sqrt{n \log q})$ 만큼 짧다.
- [139] 도 10은 본 발명의 일실시예에 따른 트랩도어 확장 방법의 흐름을 도시하고 있다.

- [140] 래티스를 나타내는 행렬, 즉, 래티스를 생성하는 행렬 및 래티스의 짧은 기저를 입력 받는다(SL210).
- [141] 균등한 분포에서 임의의 행렬을 선택한다(SL220).
- [142] 확장된 래티스를 생성한다(SL230).
- [143] 확장된 래티스의 짧은 기저를 산출한다(SL240).
- [144] 산출된 짧은 기저를 확장된 트랩도어로 출력한다(SL250).
- [145] 다시 말해, 트랩도어 확장부(L200)는 래티스의 짧은 기저를 위임하는 알고리즘을 제공한다.
- [146] 래티스 $\Lambda^\perp(A)$ 와 그것의 짧은 기저 $S_A, B \in \mathbb{Z}_q^{n \times m}$ 를 입력값으로 하는 알고리즘 $BasisDel(A, B, S_A)$ 은 출력값으로 래티스 $\Lambda^\perp(A \| B)$ 와 그것의 짧은 기저 $S_{A \| B}$ 을 출력한다.
- [147] 도 11은 본 발명의 일실시예에 따른 가우시안 샘플링 방법의 흐름을 도시하고 있다.
- [148] 래티스의 짧은 기저, 샘플링 입력값, 샘플링 파라미터를 입력받는다(SL310).
- [149] 가우시안 분포를 생성한다(SL320).
- [150] 분포로부터 벡터를 샘플링한다(SL330).
- [151] 벡터를 출력한다(SL340).
- [152] 다시 말해, 샘플링부(L300)는 래티스의 가우시안 분포로부터 벡터를 샘플링하는 알고리즘을 제공한다.
- [153] 어떤 $s > 0$ 과 차원 $m \geq 1$ 에 대해, 가우시안 함수(Gaussian function) $\rho_s: \mathbb{R}^m \rightarrow (0, 1]$ 는 $\rho_s(x) = \exp(-\pi \|x\|^2 / s^2)$ 으로 정의된다.
- [154] 어떤 코셋에 대해, 코셋 상의 (중심이 0인) 이산 가우시안 분포(discrete Gaussian distribution) $D_{\Lambda_y^\perp(A), s}$ 는 각각의 $x \in \Lambda_y^\perp(A)$ 에서 $\rho_s(x)$ 에 비례하는 확률을 가진다.
- [155] 래티스에서의 가우시안 분포와 관련되는 성질을 살펴보면 다음과 같다. 여기에서 S 는 어떤 $A \in \mathbb{Z}_q^{n \times m}$ 에 대한 $\Lambda^\perp(A)$ 의 기저를 말하며, $s \geq \| \tilde{S} \| \cdot \omega(\sqrt{\log n})$ 이다.
- [156] $\Pr_{x \leftarrow D_{\Lambda_y^\perp(A), s}} [\|x\| > s \cdot \sqrt{m}] \leq \text{negl}(n)$
- [157] $\Pr_{x \leftarrow D_{\Lambda_y^\perp(A), s}} [x=0] \leq \text{negl}(n)$
- [158] 이에 따라 $\text{SampleD}(S, y, s)$ 은 $\text{negl}(n)$ 통계적인 거리를 가지는 $D_{\Lambda_y^\perp(A), s}$ 로부터 샘플링을 할 수 있다.
- [159] 전술한 바와 같이, 가우시안 샘플링은 서명자(X)가 자신의 비밀키, 즉 확장된 트랩도어에서 서명에 사용할 래티스 벡터를 추출하기 위해 사용한다.
- [160] 본 발명의 일실시예는 컴퓨터에 의해 실행되는 프로그램 모듈과 같은 컴퓨터에

의해 실행가능한 명령어를 포함하는 기록 매체의 형태로도 구현될 수 있다. 컴퓨터 판독 가능 매체는 컴퓨터에 의해 액세스될 수 있는 임의의 가용 매체일 수 있고, 휘발성 및 비휘발성 매체, 분리형 및 비분리형 매체를 모두 포함한다. 또한, 컴퓨터 판독가능 매체는 컴퓨터 저장 매체 및 통신 매체를 모두 포함할 수 있다. 컴퓨터 저장 매체는 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터와 같은 정보의 저장을 위한 임의의 방법 또는 기술로 구현된 휘발성 및 비휘발성, 분리형 및 비분리형 매체를 모두 포함한다. 통신 매체는 전형적으로 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈, 또는 반송파와 같은 변조된 데이터 신호의 기타 데이터, 또는 기타 전송 메커니즘을 포함하며, 임의의 정보 전달 매체를 포함한다.

- [161] 본 발명의 방법 및 시스템은 특정 실시예와 관련하여 설명되었지만, 그것들의 구성 요소 또는 동작의 일부 또는 전부는 범용 하드웨어 아키텍처를 갖는 컴퓨터 시스템을 사용하여 구현될 수 있다. 본 발명의 일실시예의 하나 이상의 구성 요소 또는 동작을 실시하기 위하여 사용될 수 있는 컴퓨터 시스템 아키텍처의 일례를 설명하면, 하드웨어 시스템은 프로세서, 캐쉬, 메모리 및 상술한 기능에 관련된 하나 이상의 소프트웨어 어플리케이션 및 드라이버를 포함할 수 있다.
- [162] 전술한 본 발명의 설명은 예시를 위한 것이며, 본 발명이 속하는 기술분야의 통상의 지식을 가진 자는 본 발명의 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 쉽게 변형이 가능하다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다. 예를 들어, 단일형으로 설명되어 있는 각 구성 요소는 분산되어 실시될 수도 있으며, 마찬가지로 분산된 것으로 설명되어 있는 구성 요소들도 결합된 형태로 실시될 수 있다.
- [163] 본 발명의 범위는 상기 상세한 설명보다는 후술하는 특허청구범위에 의하여 나타내어지며, 특허청구범위의 의미 및 범위 그리고 그 균등 개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

청구범위

[청구항 1]

전자 서명 시스템에 있어서,
 자신의 마스터 키 및 사용자 개체의 공개된 식별 정보를 사용하여,
 제 1 비밀키를 생성하여 상기 사용자 개체에게 할당하는 마스터
 개체; 및
 자신의 공개키 및 제 2 비밀키를 생성하는 사용자 개체;를
 포함하되,
 상기 사용자 개체는
 상기 자신의 공개키, 제 1 비밀키, 및 제 2 비밀키를 사용하여
 생성한 서명을 검증자 개체에게 전송하는 서명자 개체; 및
 상기 서명자 개체로부터 수신한 서명을 상기 서명자 개체의
 공개된 식별 정보, 및 공개키를 사용하여 검증하는 검증자 개체;를
 포함하되,
 상기 마스터 키, 제 1 비밀키, 및 상기 제 2 비밀키 생성에
 래티스(lattice) 상에서의 SIS(small integer solution) 문제의
 어려움에 기반하여 생성한 트랩도어(trapdoor)가 사용되는 전자
 서명 시스템.

[청구항 2]

제 1 항에 있어서,
 상기 마스터 개체는
 균일한 분포(uniform distribution)에서 선택된 임의의 행렬로부터
 생성되는 래티스의 짧은 기저(short basis)인 트랩도어를 생성하여,
 상기 트랩도어를 자신의 비밀키인 마스터 키로 사용하고, 상기
 임의의 행렬을 공개하는 전자 서명 시스템.

[청구항 3]

제 1 항에 있어서,
 상기 마스터 키의 래티스를 상기 사용자 개체의 공개된 식별
 정보를 사용하여 확장된 래티스로 확장하고 상기 확장된 래티스의
 짧은 기저인 확장된 트랩도어를 생성하여,
 상기 확장된 트랩도어를 상기 사용자 개체의 제 1 비밀키로
 발급하는 전자 서명 시스템.

[청구항 4]

제 1 항에 있어서,
 상기 사용자 개체는
 균일한 분포에서 선택된 임의의 행렬로부터 생성되는 래티스의
 짧은 기저인 트랩도어를 생성하여,
 상기 트랩도어를 자신의 제 2 비밀키로 사용하고, 상기 임의의
 행렬을 자신의 공개키로 사용하는 전자 서명 시스템.

[청구항 5]

제 1 항에 있어서,
 상기 사용자 개체는

자신의 제 1 비밀키 및 공개키를 사용하여 제 1 서명을 생성하고, 자신의 제 2 비밀키 및 공개키를 사용하여 제 2 서명을 생성하여, 상기 제 1 서명과 제 2 서명을 사용하여 상기 서명을 생성하는 전자 서명 시스템.

[청구항 6]

제 5 항에 있어서,

상기 사용자 개체는

상기 제 1 비밀키의 가우시안 분포로부터 벡터를 샘플링하여 상기 제 1 서명을 생성하는 전자 서명 시스템.

[청구항 7]

제 5 항에 있어서,

상기 사용자 개체는

상기 제 2 비밀키의 래티스를 상기 공개키를 사용하여 확장된 래티스로 확장하고 상기 확장된 래티스의 짧은 기저인 확장된 트랩도어를 생성하여,

상기 확장된 트랩도어의 가우시안 분포로부터 벡터를 샘플링하여 상기 제 2 서명을 생성하는 전자 서명 시스템.

[청구항 8]

전자 서명 방법에 있어서,

(a) 마스터 개체가 보안 파라미터를 설정하고 자신의 마스터 키를 생성하는 단계;

(b) 상기 마스터 개체가 서명자 개체 및 검증자 개체를 포함하는 사용자 개체의 공개된 식별 정보에 기초하여, 제 1 비밀키를 생성하여 상기 사용자 개체에게 할당하는 단계;

(c) 상기 사용자 개체가 자신의 공개키 및 제 2 비밀키를 생성하는 단계;

(d) 상기 서명자 개체가 자신의 공개키, 제 1 비밀키, 및 제 2 비밀키를 사용하여 생성한 서명을 검증자 개체에게 전송하는 단계; 및

(e) 상기 검증자 개체가 상기 서명자 개체로부터 수신한 서명을 상기 서명자 개체의 공개된 식별 정보, 및 공개키를 사용하여 검증하는 단계;를 포함하되,

상기 마스터 키, 제 1 비밀키, 및 상기 제 2 비밀키 생성에 래티스(lattice) 상에서의 SIS(small integer solution) 문제의 어려움에 기반하여 생성한 트랩도어(trapdoor)가 사용되는 전자 서명 방법.

[청구항 9]

제 8 항에 있어서,

상기 (a) 단계는

균일한 분포(uniform distribution)에서 선택된 임의의 행렬로부터 생성되는 래티스의 짧은 기저(short basis)인 트랩도어를 생성하여, 상기 트랩도어를 상기 마스터 개체의 비밀키인 마스터 키로

[청구항 10]

사용하고, 상기 임의의 행렬은 공개되는 전자 서명 방법.

제 8 항에 있어서,

상기 (b) 단계는

상기 마스터 키의 래티스를 상기 사용자 개체의 공개된 식별 정보를 사용하여 확장된 래티스로 확장하고 상기 확장된 래티스의 짧은 기저인 확장된 트랩도어를 생성하여,
상기 확장된 트랩도어를 상기 사용자 개체의 제 1 비밀키로 발급하는 전자 서명 방법.

[청구항 11]

제 8 항에 있어서,

상기 (c) 단계는

균일한 분포에서 선택된 임의의 행렬로부터 생성되는 래티스의 짧은 기저인 트랩도어를 생성하여

상기 트랩도어를 상기 사용자 개체의 제 2 비밀키로 사용하고,
상기 임의의 행렬을 상기 사용자 개체의 공개키로 사용하는 전자 서명 방법.

[청구항 12]

제 8 항에 있어서,

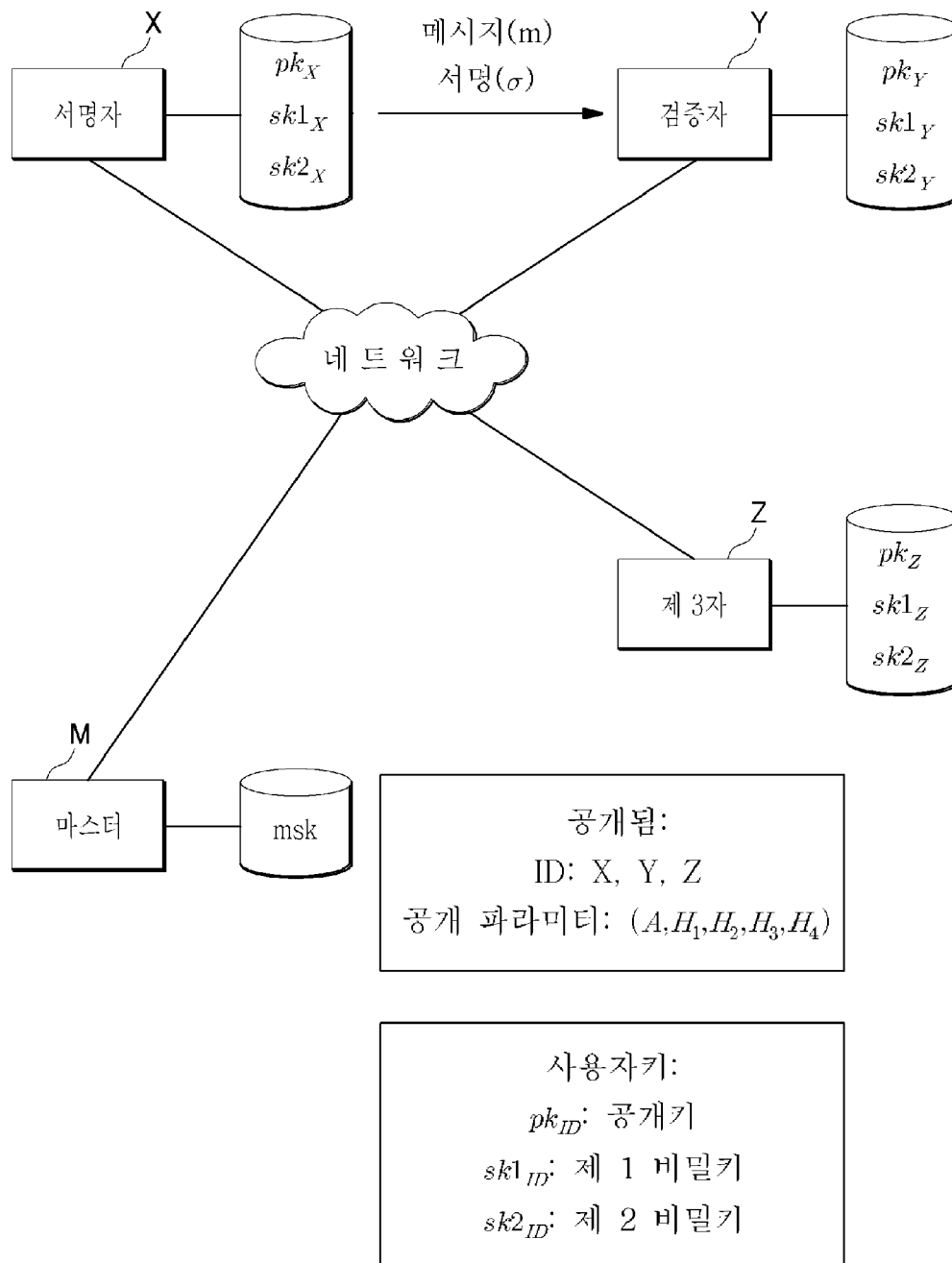
상기 (d) 단계는

상기 서명자 개체의 제 1 비밀키 및 공개키를 사용하여, 상기 제 1 비밀키의 가우시안 분포로부터 벡터를 샘플링하여 제 1 서명을 생성하고,

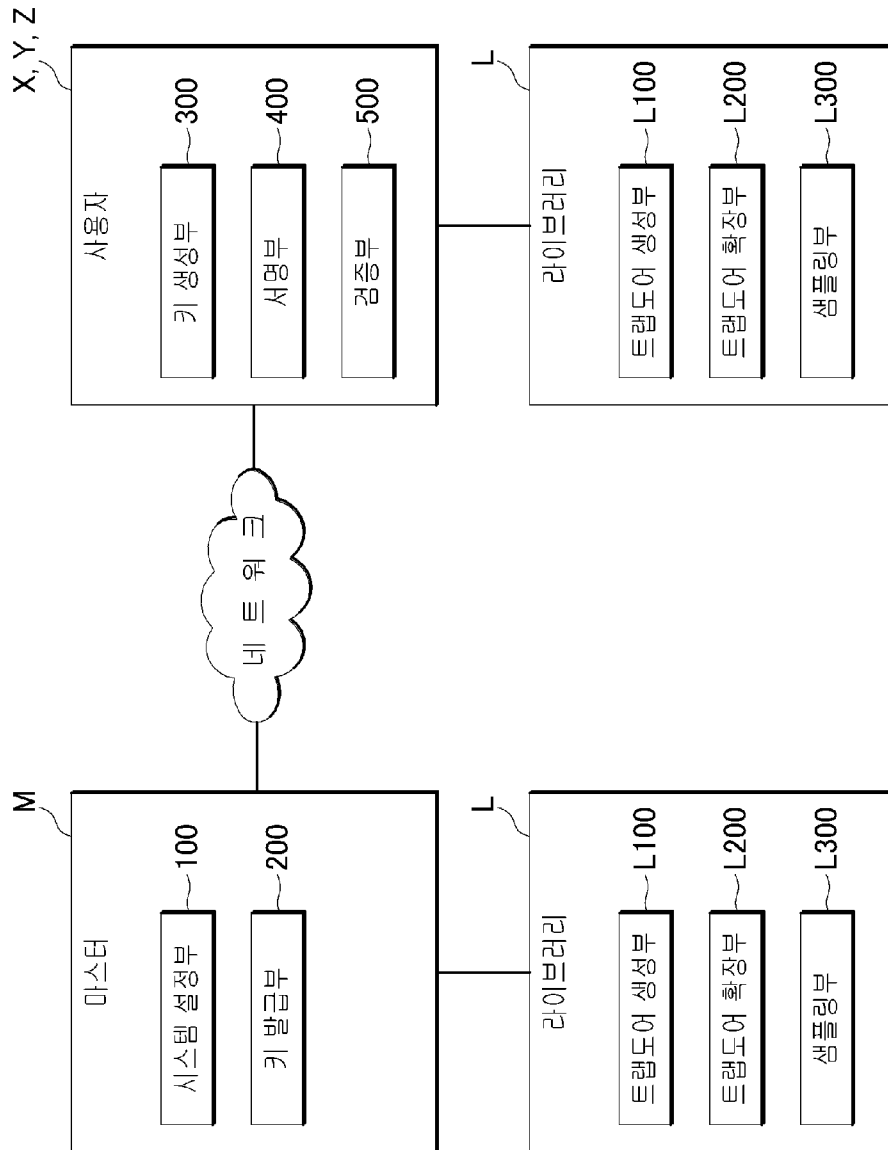
상기 서명자 개체의 제 2 비밀키 및 공개키를 사용하여, 상기 제 2 비밀키의 래티스를 상기 공개키를 사용하여 확장된 래티스로 확장하고 상기 확장된 래티스의 짧은 기저인 확장된 트랩도어를 생성하여, 상기 확장된 트랩도어의 가우시안 분포로부터 벡터를 샘플링하여 제 2 서명을 생성하여,

상기 제 1 서명과 제 2 서명을 사용하여 상기 서명을 생성하는 전자 서명 방법.

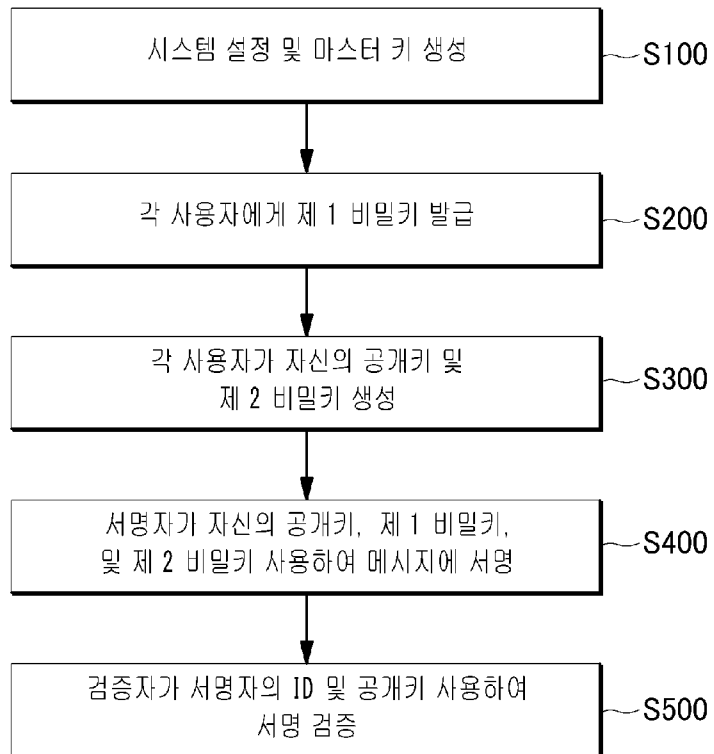
[Fig. 1]



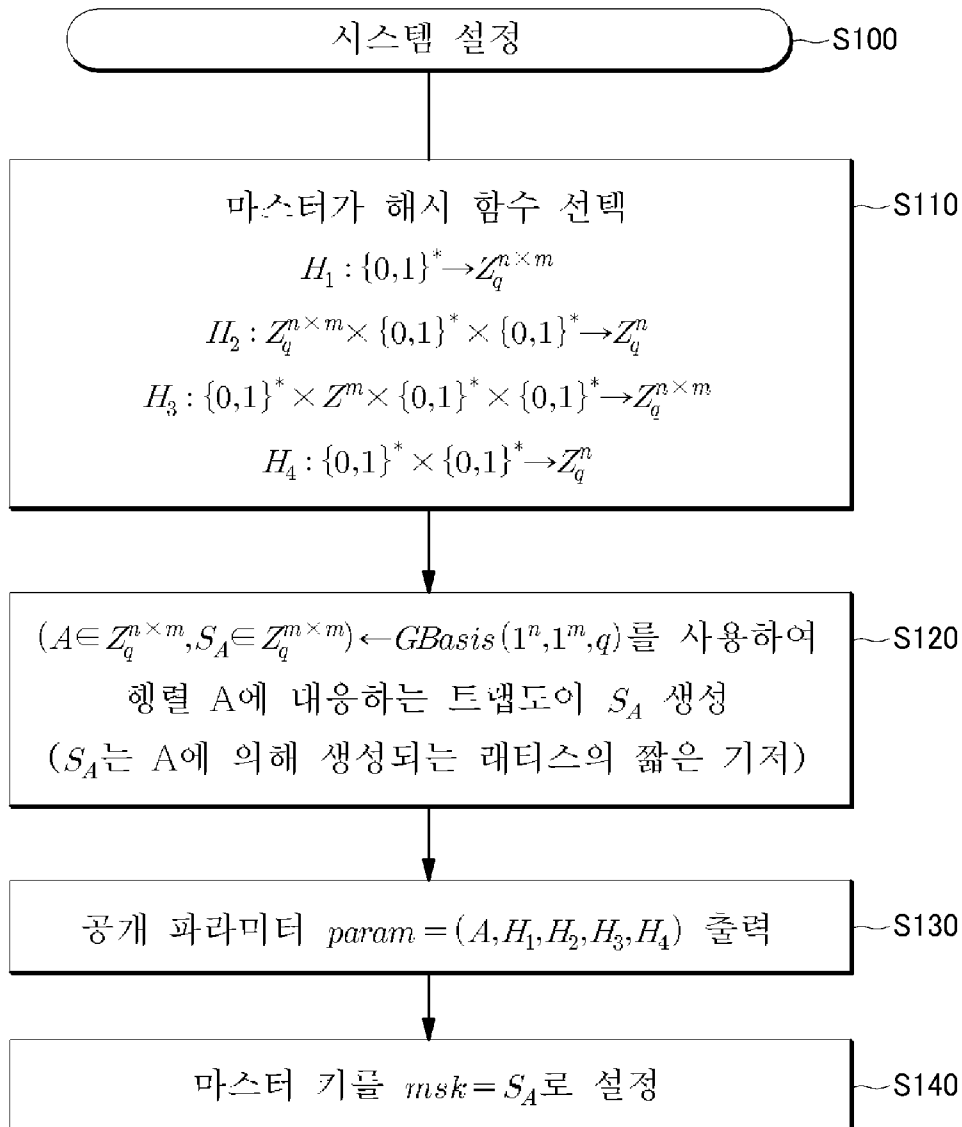
[Fig. 2]



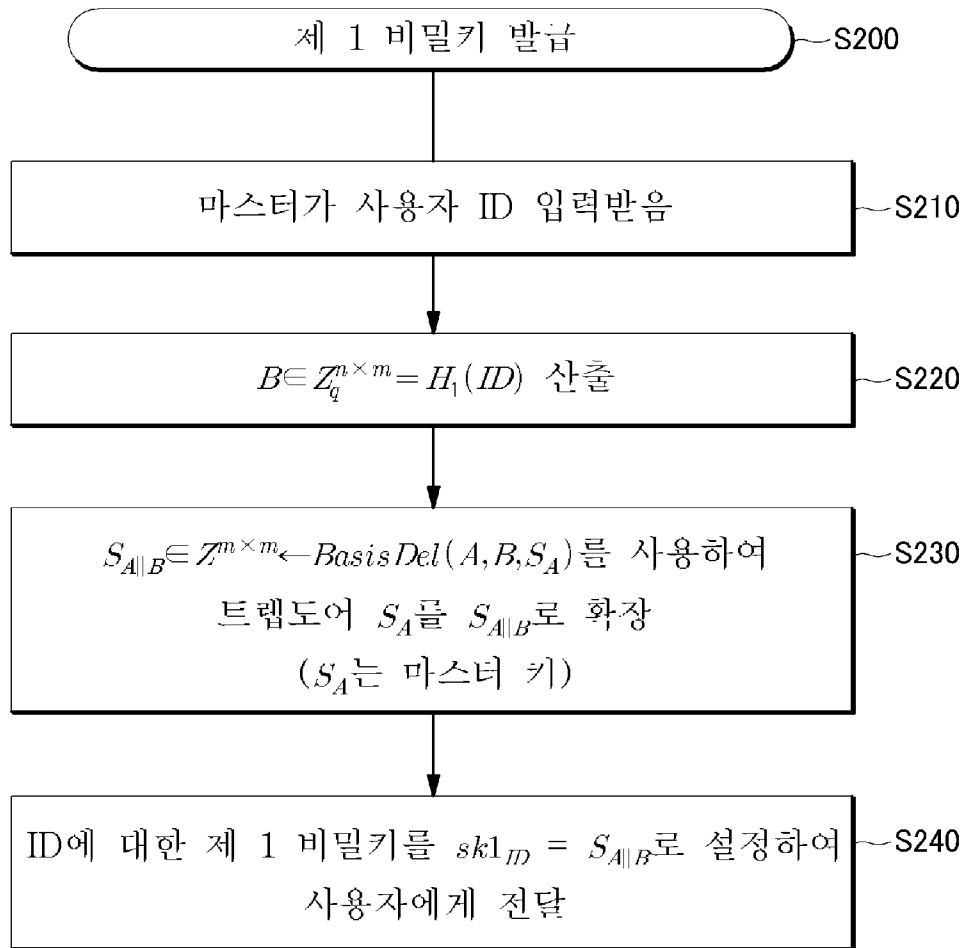
[Fig. 3]



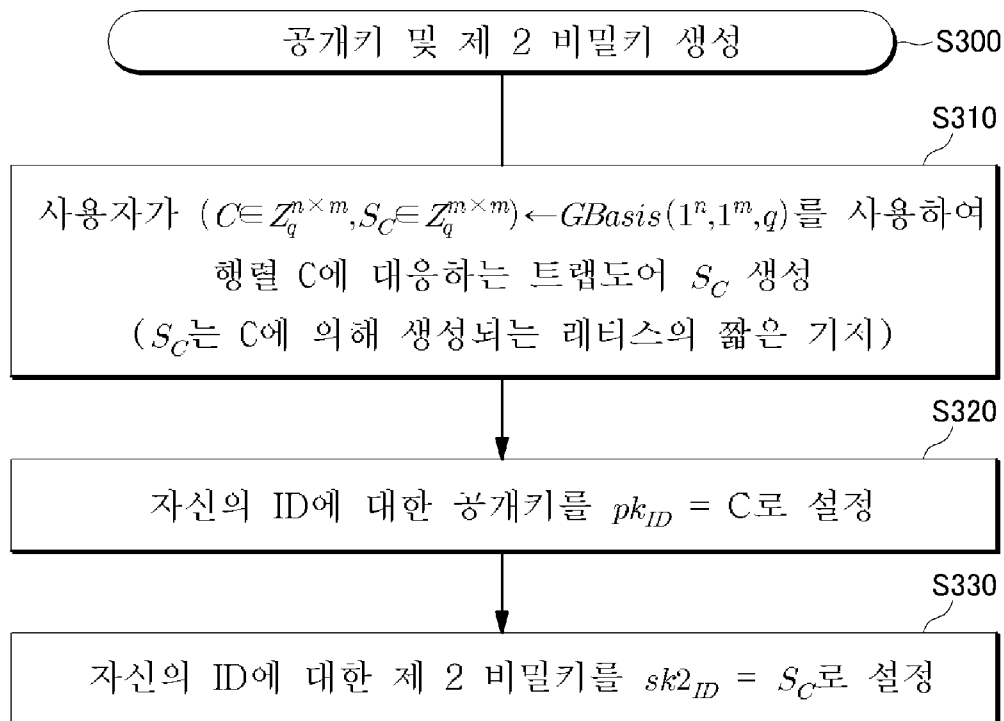
[Fig. 4]



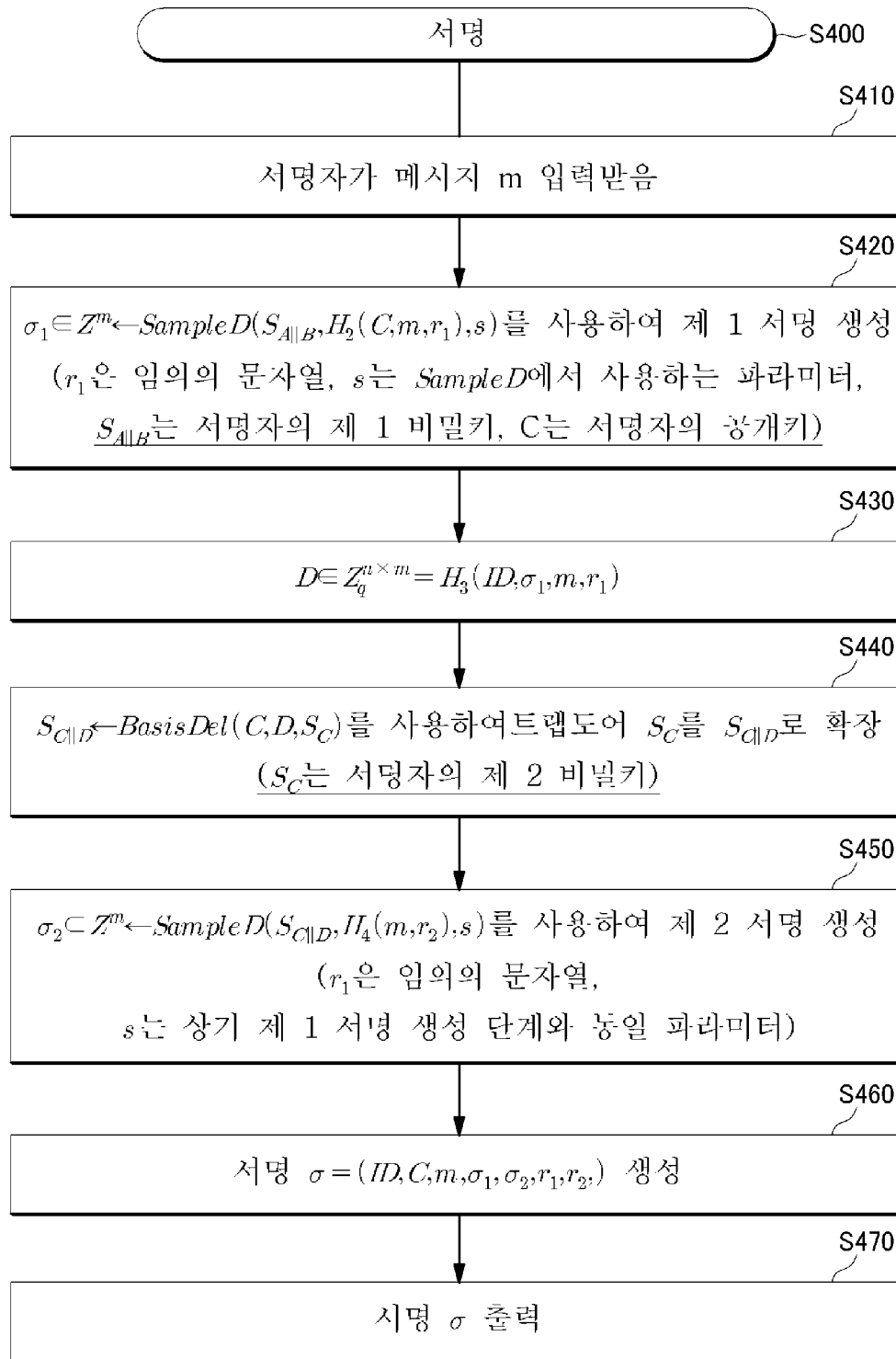
[Fig. 5]



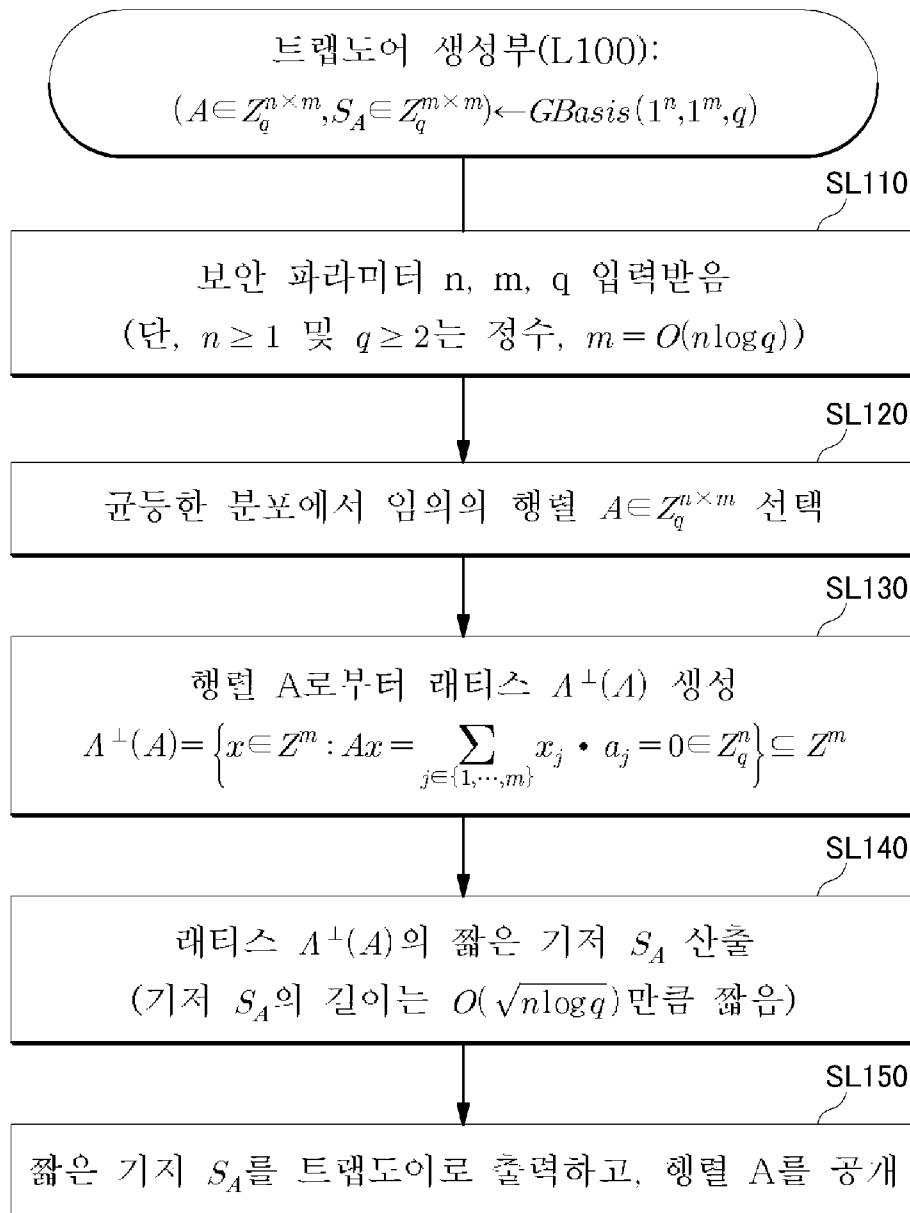
[Fig. 6]



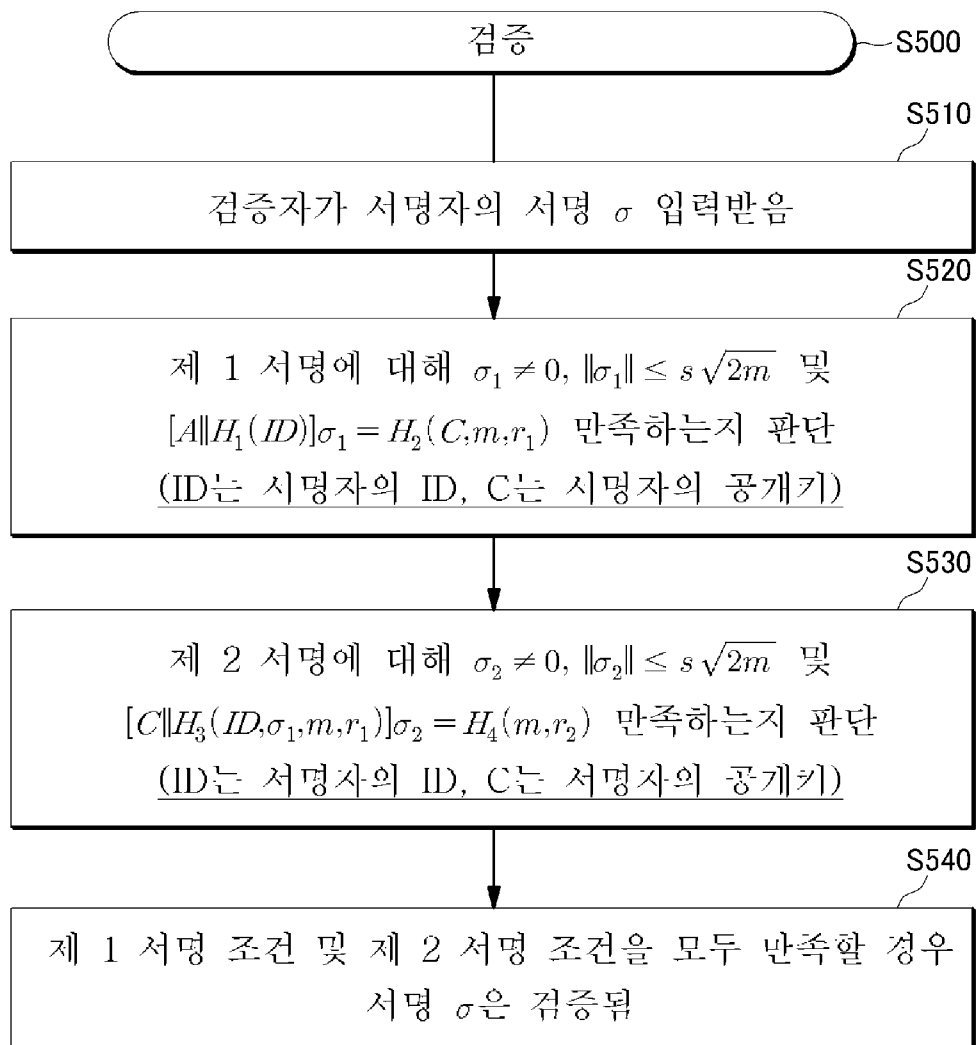
[Fig. 7]



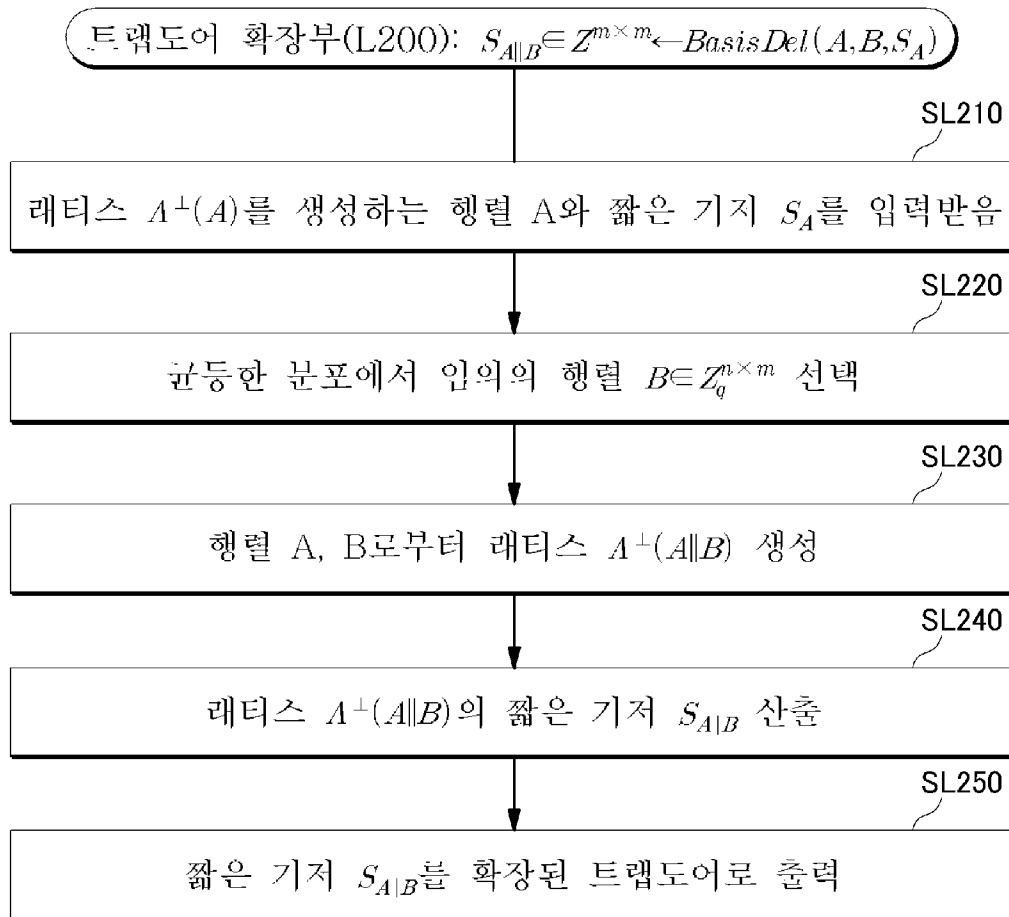
[Fig. 8]



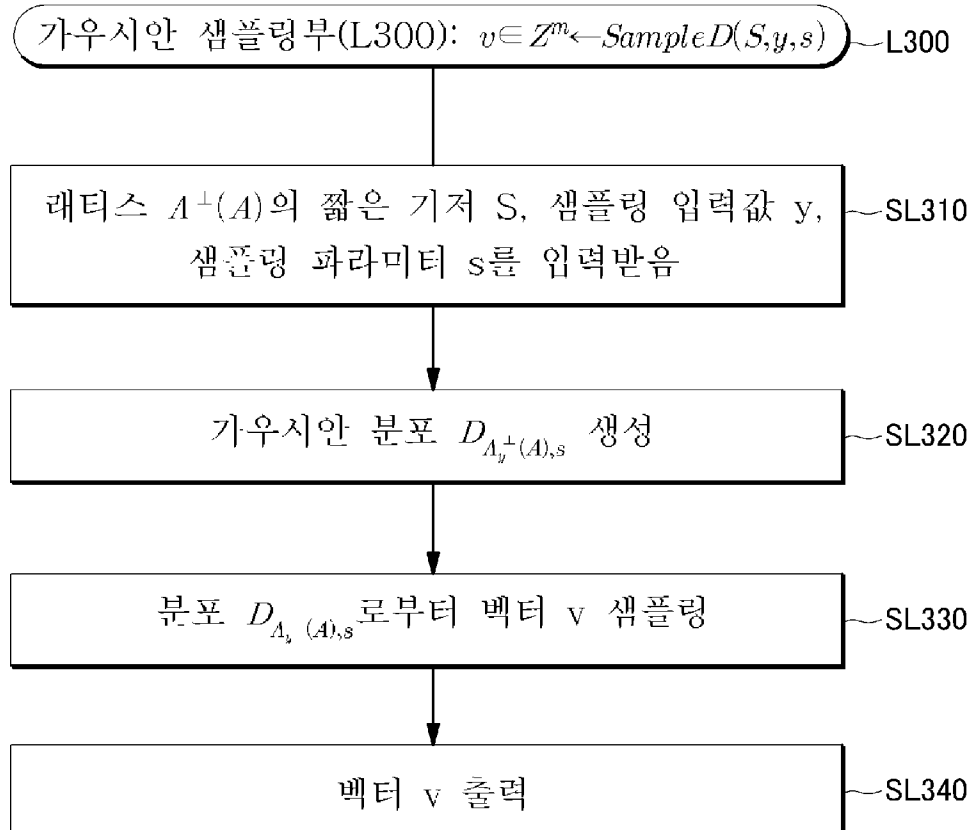
[Fig. 9]



[Fig. 10]



[Fig. 11]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2014/008144**A. CLASSIFICATION OF SUBJECT MATTER****H04L 9/30(2006.01)i, H04L 9/32(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 9/30; H04L 9/14; H04L 9/32; H04L 9/00; G06F 21/60

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: "lattice, public key, secret key, signature, master key, verification, trapdoor"

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KR 10-2013-0085491 A (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE) 30 July 2013 See abstract, claims 1-3 and figures 1-2.	1-12
A	US 2007-0165843 A1 (LAUTER et al.) 19 July 2007 See abstract, claims 6-19 and figures 1-4.	1-12
A	KR 10-2012-0071884 A (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE et al.) 03 July 2012 See abstract, claims 1-11 and figures 1-2.	1-12
A	US 7237116 B1 (DWORK et al.) 26 June 2007 See abstract, claims 1-7 and figures 1-3.	1-12



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

"I" 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

28 OCTOBER 2014 (28.10.2014)

Date of mailing of the international search report

01 DECEMBER 2014 (01.12.2014)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
Government Complex-Daejeon, 189 Seonsa-ro, Daejeon 302-701,
Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/KR2014/008144

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-2013-0085491 A	30/07/2013	US 2013-0148803 A1	13/06/2013
US 2007-0165843 A1	19/07/2007	US 8180047 B2	15/05/2012
KR 10-2012-0071884 A	03/07/2012	US 2012-0166808 A1	28/06/2012
US 7237116 B1	26/06/2007	NONE	

A. 발명이 속하는 기술분류(국제특허분류(IPC)) H04L 9/30(2006.01)i, H04L 9/32(2006.01)i		
B. 조사된 분야 조사된 최소문헌(국제특허분류를 기재) H04L 9/30; H04L 9/14; H04L 9/32; H04L 9/00; G06F 21/60 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: "래티스, 공개키, 비밀키, 서명, 마스터키, 검증, 트랩도어"		
C. 관련 문헌		
카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
A	KR 10-2013-0085491 A (한국전자통신연구원) 2013.07.30 요약, 청구항 1-3 및 도면 1-2 참조.	1-12
A	US 2007-0165843 A1 (LAUTER et al.) 2007.07.19 요약, 청구항 6-19 및 도면 1-4 참조.	1-12
A	KR 10-2012-0071884 A (한국전자통신연구원 외 1명) 2012.07.03 요약, 청구항 1-11 및 도면 1-2 참조.	1-12
A	US 7237116 B1 (DWORK et al.) 2007.06.26 요약, 청구항 1-7 및 도면 1-3 참조.	1-12
☐ 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 2014년 10월 28일 (28.10.2014)		국제조사보고서 발송일 2014년 12월 01일 (01.12.2014)
ISA/KR의 명칭 및 우편주소  대한민국 특허청 (302-701) 대전광역시 서구 청사로 189, 4동 (둔산동, 정부대전청사) 팩스 번호 +82-42-472-7140		심사관 홍기완 전화번호 +82-42-481-5662 

국제조사보고서
대응특허에 관한 정보

국제출원번호

PCT/KR2014/008144

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2013-0085491 A	2013/07/30	US 2013-0148803 A1	2013/06/13
US 2007-0165843 A1	2007/07/19	US 8180047 B2	2012/05/15
KR 10-2012-0071884 A	2012/07/03	US 2012-0166808 A1	2012/06/28
US 7237116 B1	2007/06/26	없음	