

(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2019년 7월 4일 (04.07.2019)



(10) 국제공개번호
WO 2019/132354 A1

(51) 국제특허분류:
H04L 9/30 (2006.01)

(21) 국제출원번호: PCT/KR2018/016014

(22) 국제출원일: 2018년 12월 17일 (17.12.2018)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2017-0183661 2017년 12월 29일 (29.12.2017) KR

(71) 출원인: 서울대학교산학협력단 (SEOUL NATIONAL UNIVERSITY R&DB FOUNDATION) [KR/KR]; 08826 서울시 관악구 관악로 1, Seoul (KR). 울산과학기술원 (UNIST(ULSAN NATIONAL INSTITUTE OF SCIENCE AND TECHNOLOGY)) [KR/KR]; 44919 울산시 울주군 언양읍 유니스트길 50, Ulsan (KR).

(72) 발명자: 이주희 (LEE, Joohee); 08826 서울시 관악구 관악로 1, Seoul (KR). 천정희 (CHEON, Junghee); 08826 서울시 관악구 관악로 1, Seoul (KR). 김두형 (KIM, Duhyeong); 08826 서울시 관악구 관악로 1, Seoul (KR). 윤아람 (YUN, Aaram); 44919 울산시 울주군 언양읍 유니스트길 50, Ulsan (KR).

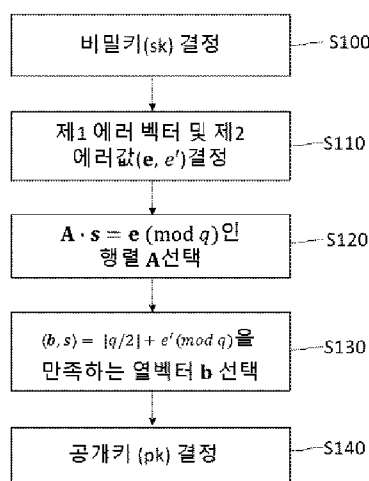
(74) 대리인: 백도현 (BACK, Dochyun); 07997 서울시 양천구 목동동로 293, 3103호, Seoul (KR).

(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 국내 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).

(54) Title: METHOD FOR GENERATING, ENCRYPTING, AND DECRYPTING PUBLIC KEY AND CRYPTOGRAPHIC KEY ON BASIS OF MODULE-WAVY AND MODULE-LWR

(54) 발명의 명칭: MODULE-WAVY와 MODULE-LWR에 기반한 공개키 암호 키 생성 및 암호복호화 방법



S100 ... Determine secret key (sk)
S110 ... Determine first error vector and second error value (e, e')
S120 ... Select matrix A satisfying $A \cdot s = e \pmod{q}$
S130 ... Select column vector b satisfying $\langle b, s \rangle = |q/2| + e' \pmod{q}$
S140 ... Determine public key (pk)

(57) Abstract: According to the present invention, a method for generating a public key and a secret key, performed by a computer, comprises: a first step of determining a secret key (s) by sampling at an arbitrary distribution on $\{-1, 0, 1\}^{nd}$; a second step of determining a first error vector (e) by sampling at $(D_{\alpha q})^d$ and determining a second error value (e') by sampling at $D_{\alpha q}^n$; a third step of selecting a randomly uniform matrix A satisfying $A \cdot s = e \pmod{q}$; a fourth step of selecting a random column vector b satisfying $\langle b, s \rangle = \text{rounded value of } q/2 + e' \pmod{q}$; and a fourth step of determining the public key (pk) as $(A \| b) \in R_q^{d \times (d+1)}$.

(57) 요약서: 본 발명에 의해, 컴퓨터가 수행하는 공개키와 비밀키 생성 방법은, 비밀키(s)를 $\{-1, 0, 1\}^{nd}$ 위의 임의의 분포에서 샘플링하여 결정하는 제1 단계와; 제1 에러 벡터(e)를 $(D_{\alpha q})^d$ 에서 샘플링하여 결정하고, 제2 에러값(e')을 $D_{\alpha q}^n$ 에서 샘플링하여 결정하는 제2 단계와; $A \cdot s = e \pmod{q}$ 를 만족하는 랜덤하게 균일한 행렬 A를 선택하는 제3 단계와; $\langle b, s \rangle = (q/2 \text{의 반올림값}) + e' \pmod{q}$ 를 만족하는 랜덤 열벡터 b를 선택하는 제4 단계와; 공개키(pk)를 $(A \| b) \in R_q^{d \times (d+1)}$ 로 결정하는 제4 단계를 포함한다.

공개:

— 국제조사보고서와 함께 (조약 제21조(3))

명세서

발명의 명칭: MODULE-WAVY와 MODULE-LWR에 기반한 공개키 암호 키 생성 및 암호화 방법

기술분야

- [1] 본 발명은 래티스(lattice) 기반 공개키 암호화 방법에 대한 것으로서, 좀 더 구체적으로는 Module-Wavy와 Module-LWR에 기반한 공개키와 비밀키 생성 및 그러한 키를 이용한 공개키 암호화/복호화 방법에 대한 것이다.

배경기술

- [2] 암호화 방법에는 크게 대칭키 암호화 방법과 비대칭키 암호화 방법이 있다. 대칭키 암호화 방법은 암호화에 사용하는 키와 복호화에 사용하는 키가 동일하기 때문에 속도는 빠르지만 키의 분실 등이 발생하는 경우 보안성이 담보되지 않은 단점이 있다. 그러한 문제를 해결하기 위하여 등장한 것이 비대칭키 암호화 방법인데, 비대칭키 암호화 방법에 의하면 제3자에게 공개하는 공개키와, 사용자 본인만 보유하는 비밀키(개인키)를 사용하며, 암호문을 수신한 공개키로 암호화하면, 수신인은 암호문을 자신만이 가지고 있는 비밀키로 복호화할 수 있다.
- [3] 공개키 암호화 방법 중 가장 널리 사용되는 것은 RSA 방식인데 현재 연구가 활발하고 향후 등장할 예정인 양자 컴퓨터가 실용화되면 양자 컴퓨터에 의해 손쉽게 풀릴 수 있어서 그에 대한 대안이 필요한 상황이다.
- [4] 그러한 대안 중 하나로 래티스 기반 공개키 암호화 방식이 제안된 바 있는데 그 예로 최근에 NIST call for post-quantum standards를 겨냥해서 소개한 스킴인 Kyber((Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J.M., Schwabe, P., Stehlé, D.: CRYSTALS - kyber: a CCA-secure module lattice-based KEM. Cryptology ePrint Archive, Report 2017/634 (2017). <http://eprint.iacr.org/2017/634>))가 있다. 그런데 이 스킴은 암호문의 요소(component)가 두 개이기 때문에 암호문의 크기가 크고, 기존의 방식(NTRU 방식)에 비해서 속도도 느린 단점이 있다.

발명의 상세한 설명

기술적 과제

- [5] 본 발명은 그러한 종래 기술의 문제를 해결함으로써 암호문의 크기도 저감시키고 실제 적용시에 통신 부하와 통신량을 줄이며 그리고 비용도 절감할 수 있는 래티스 기반 공개키 암호화 방법을 제공하는 것을 목적으로 한다.

과제 해결 수단

- [6] 본 발명에 의해, 컴퓨터가 수행하는 공개키와 비밀키 생성 방법은, 비밀키($\mathbf{s}$)를 $\{-1, 0, 1\}^{nd}$ 위의 임의의 분포에서 샘플링하여 결정하는 제1 단계와;

제1 에러 벡터(**e**)를 $(D_{\alpha q}^n)^d$ 에서 샘플링하여 결정하고, 제2 에러값(**e'**)을

$D_{\alpha q}^n$ 에서 샘플링하여 결정하는 제2 단계와; $\mathbf{A} \cdot \mathbf{s} = \mathbf{e} \pmod{q}$ 를

만족하는 랜덤하게 균일한 행렬 **A**를 선택하는 제3 단계와;

$\langle \mathbf{b}, \mathbf{s} \rangle = \lfloor q/2 \rfloor + e' \pmod{q}$ 을 만족하는 랜덤 열벡터 **b**를 선택하는 제4 단계와; 공개키(pk)를 $(\mathbf{A} \parallel \mathbf{b}) \in R_q^{d \times (d+1)}$ 로 결정하는 제4 단계를

포함한다.

[7] 제1 단계에서 생성되는 비밀키(**s**)는 $\mathcal{HWT}_n(h_s)^d$ 에서 샘플링될 수 있다.

[8] 본 발명에 의해 컴퓨터에 의해서 수행되는, 공개키를 이용한 메시지 암호화 방법은, 공개키와 메시지($\mathbf{m} \in R_2$)를 수신하는 제1 단계와; -1,0,1 중 어느

하나의 계수를 가지는 n차 다항식 d개를 랜덤하게 추출하는 제2 단계와; 상기 다항식들 및 공개키의 일부를 연산하여 제1 값을 산출하는 제3 단계와; 상기 메시지를 공개키의 일부를 사용하여 인코딩하여 제2 값을 산출하는 제4 단계; 상기 제1 값과 제2 값을 연산하여 제3 값을 산출하는 제5 단계와; 제3값에 대해 기설정된 하위 비트를 제거하기 위한 라운딩 처리를 수행하여 암호문을 산출하는 제6 단계를 포함한다.

[9] 암호화 방법의 제2 단계는, 다항식 벡터(polynomial vector) **r**을

$\mathcal{HWT}_n(h_r)^d$ 에서 샘플링하여 결정하는 단계가 될 수 있다. 제1 값은

$\mathbf{A}^T \cdot \mathbf{r}$ 이며, 제2 값은 $\mathbf{m} \cdot \mathbf{b}$ 이며, 제3 값은 $\mathbf{A}^T \cdot \mathbf{r} + \mathbf{m} \cdot \mathbf{b}$ 으로

산출될 수 있다.

[10] 제6 단계에서 라운딩 처리된 암호문은

$\mathbf{c} = \lfloor \frac{p}{q} \cdot (\mathbf{A}^T \cdot \mathbf{r} + \mathbf{m} \cdot \mathbf{b}) \rfloor \in R_p^d$ 로 산출될 수 있다.

[11] 본 발명에 의한 복호화 방법은, 암호문(**c**)을 수신하는 제1 단계와; 다음 수학식에 의해서 복호화하는 제2 단계를 포함한다.

[12] [수학식]

[13]
$$\mathbf{m} = \left\lfloor \frac{2}{p} \cdot \langle \mathbf{c} \cdot \mathbf{s} \rangle \right\rfloor$$

발명의 효과

[14] 본 발명에 의한 암호문 **c**는 기존의 Kyber 방식과 달리 암호문이 하나의 요소(component)만을 가지고 있으며, 더욱이 $p < q$ 이기 때문에 암호문의 크기

역시 현저하게 축소된다. 따라서 기존의 래티스 기반 공개키 암호화 방식에 비하여 빠른 처리가 가능하고 암호화 통신에 있어서 통신부하 및 통신량이 현저하게 감소하여 관련 비용 역시 저감할 수 있는 효과가 제공된다.

도면의 간단한 설명

- [15] 도 1은 본 발명에 의한 공개키 및 비밀키 생성 방법의 흐름도.

발명의 실시를 위한 형태

- [16] 이하에서는 첨부 도면을 참조하여 본 발명에 대해서 자세하게 설명한다.
- [17] 본 명세서에서 수행되는 정보(데이터) 전송/수신 과정은 필요에 따라서 암호화/복호화가 적용될 수 있으며, 본 명세서 및 특허청구범위에서 정보(데이터) 전송 과정을 설명하는 표현은 별도로 언급되지 않더라도 모두 암호화/복호화하는 경우도 포함하는 것으로 해석되어야 한다. 본 명세서에서 "A로부터 B로 전송(전달)" 또는 "A가 B로부터 수신"과 같은 형태의 표현은 중간에 다른 매개체가 포함되어 전송(전달) 또는 수신되는 것도 포함하며, A로부터 B까지 직접 전송(전달) 또는 수신되는 것만을 표현하는 것은 아니다. 본 발명의 설명에 있어서 각 단계의 순서는 선행 단계가 논리적 및 시간적으로 반드시 후행 단계에 앞서서 수행되어야 하는 경우가 아니라면 각 단계의 순서는 비제한적으로 이해되어야 한다. 즉 위와 같은 예외적인 경우를 제외하고는 후행 단계로 설명된 과정이 선행 단계로 설명된 과정보다 앞서서 수행되더라도 발명의 본질에는 영향이 없으며 권리범위 역시 단계의 순서에 관계없이 정의되어야 한다. 그리고 본 명세서에서 "A 또는 B"은 A와 B 중 어느 하나를 선택적으로 가리키는 것뿐만 아니라 A와 B 모두를 포함하는 것도 의미하는 것으로 정의된다. 또한, 본 명세서에서 "포함"이라는 용어는 포함하는 것으로 나열된 요소 이외에 추가로 다른 구성요소를 더 포함하는 것도 포괄하는 의미를 가진다.
- [18] 본 명세서에서는 본 발명의 설명에 필요한 필수적인 구성요소만을 설명하며, 본 발명의 본질과 관계가 없는 구성요소는 언급하지 아니한다. 그리고 언급되는 구성요소만을 포함하는 배타적인 의미로 해석되어서는 아니되며 필수적이지 않은 특정 구성요소를 배제하거나 다른 구성요소도 포함할 수 있는 비배타적인 의미로 해석되어야 한다.
- [19] 본 발명은 전자적 연산이 가능한 컴퓨터 등의 전자적 연산 장치에 의해서 수행되며, 후술하는 본 발명의 각 단계의 수학적 연산 및 산출은 해당 연산 또는 산출을 하기 위해 공지되어 있는 코딩 방법 및/또는 본 발명에 적합하게 고안된 코딩에 의해서 컴퓨터 연산으로 구현될 수 있다.
- [20] 그리고 본 명세서에서 "값"이라 함은 스칼라값 뿐만 아니라 벡터 및 행렬도 포함하는 광의의 개념으로 정의된다.
- [21] 본 명세서에서 일반적으로 소문자 볼드체는 열벡터, 대문자는 행렬을 의미한다.

[22] 본 명세서에서 사용되는 변수 등을 아래와 같이 정의한다.

[23] n : 2의 거듭 제곱

[24] d : 양의 정수

[25] q : 양의 정수; 큰 모듈러스(large modulus)

[26] p : q 보다 작은 양의 정수; 라운딩 모듈러스(rounding modulus)

[27] $\mathbb{Z}_q = (-\frac{q}{2}, \frac{q}{2}] \cap \mathbb{Z}$; $-q/2$ 보다 크고, $q/2$ 보다 같거나 작은 정수의 집합($\mathbb{Z}_t$

)도 같은 방식으로 정의됨)

[28]
$$\mathbf{R} = \frac{\mathbb{Z}[x]}{(f(x))}$$

[29]
$$\mathbf{R}_q = \frac{\mathbb{Z}_q[x]}{(f(x))}$$

[30]
$$\mathbf{R}_t = \frac{\mathbb{Z}_t[x]}{(f(x))}$$

[31] $(f(x))$: $f(x)$ 로 생성되는 $\mathbb{Z}_q[x]$ 의 이데알(ideal)

[32] $f(x)$: n 차 다항식(예를 들어, $n = \Phi(N)$ 일 때 사이클로토믹 다항식)

[33] 링 R : 계수가 정수인 n 차 다항식의 집합

[34] 링 R 에서 연산: 모든 다항식을 연산한 후에 $f(x)$ 로 나눈 나머지를 계산

[35] 링 R_q : 계수가 $\mathbb{Z}_q$ 의 원소인 n 차 다항식의 집합

[36] 링 R_q 에서 연산: 모든 다항식을 연산한 후에 $f(x)$ 로 나누고 각 계수에 q 를 필요한 만큼 더하거나 빼서 모든 계수가 $\mathbb{Z}_q$ 에 포함되도록 함.

[37] 링 R_t : 계수가 $\mathbb{Z}_t$ 의 원소인 n 차 다항식의 집합.

[38] 링 R_t 에서 연산: 모든 다항식을 연산한 후에 $f(x)$ 로 나누고, 각 계수에 t 를 필요한 만큼 더하거나 빼서 모든 계수가 $\mathbb{Z}_t$ 에 포함되도록 함.

[39] $[r]$: 실수 r 과 가장 가까운 정수; 같은 거리의 경우 올림

[40] 같은 개수의 행을 가지는 두 개의 행렬 또는 벡터 A 와 B 에 대해서,

[41] $(A \parallel B)$ 는 행렬 A 와 B 의 다음과 같은 연접(concatenation)을 의미한다.

[42] 즉 $A \in \mathbb{Z}^{m \times n_1}$ 이고 $B \in \mathbb{Z}^{m \times n_2}$ 일 때에 A 와 B 의 연접 행렬 C 의 요소 $C_{i,j}$ 는 다음과 같이 정의된다.

- [43]
$$c_{i,j} = \begin{cases} a_{i,j} & 1 \leq j \leq n_1 \\ b_{i,(j-n_1)} & n_1 < j \leq n_1 + n_2 \end{cases}$$
- [44] $x \leftarrow D$: 분포 D 에 따라 x 를 샘플링하는 것. 분포 D 가 유한 집합일 때에는 균일한 샘플링이 된다.
- [45] D_σ : 이산 가우시안 분포(discrete Gaussian distribution); 정수 x 에 대해서 $\exp\left(-\frac{\pi x^2}{\sigma^2}\right)$ 에 비례하는 확률을 나타내는 확률 분포. σ 가 아주 작지 않은 경우에는 D_σ 의 분산(variance)은 $\sigma^2/2\pi$ 에 아주 근접한다.
- [46] 0 이상 n 이하인 정수 h 에 대해서, 분포 $\mathcal{HWT}_n(h)$ 는 $\{-1, 0, 1\}^n$ 에서 0이 아닌 원소의 개수가 h 개인 벡터를 균등하게 샘플링하는 분포이다.
- [47] 1보다 크거나 같은 정수 n 에 대해서, D^n 은 분포 D 를 따르는 n 개의 독립 랜덤 변수들(independent and identically distributed random variables)의 곱을 나타낸다.
- [48] 본 발명의 기초가 되는 Module-LWR 문제는 Alperin-Sheriff, Jacob, and Daniel Apon. "Dimension-Preserving Reductions from LWE to LWR." IACR Cryptology ePrint Archive report 2016/589. (2016). <http://eprint.iacr.org/2016/589>에 공개되어 있다. 또다른 기초인 Module-Wavy 문제는 본 발명의 발명자들에 의해서 다음과 같이 정의된다.
- [49] R^d 의 원소인 비밀 다항식 s 에 대해서 에러 다항식 e 를 $D_{\alpha q}^n$ 에서 샘플링하고, $\langle a, s \rangle_q = e \text{ in } R_q$ 를 만족하는 $a \in R_q^d$ 를 균등하고 랜덤하게 선택하고 a 의 분포를 $A_{n,d,q,\alpha}^{MWavy}(s)$ 로 표시할 때, Module-Wavy 문제는 s 를 D 에서 샘플링 했을 때, $A_{n,d,q,\alpha}^{MWavy}(s)$ 와, R_q^d 상의 균등 분포를 구별하는 문제이다.
- [50] 다음으로는 본 발명에 의한 공개키 암호화 및 복호화 방법에 있어서 사용되는 공개키와 비밀키 생성 방법에 대해서 설명한다.
- [51] 키 생성에 앞서서 먼저 보안 인수(security parameter) λ 를 정하고 그에 기초하여 앞서 정의한 변수 n, p, q, d 를 결정하고, 추가적인 변수로 양의 정수 h_s 및 h_r 과 에러 파라미터 α 를 다음과 같이 결정한다. 보안 인수 λ 는 암호 스킴(scheme)이 얼마나 안전한지를 나타내는 척도로서 예를 들어 128이 될 수 있다.

- [52] $h_s < n$
- [53] $h_r < n$
- [54] $0 < \alpha < 1$
- [55] 먼저 다음과 같이 다항식 열벡터 $\mathbf{s}$ 를 샘플링하여 결정한다(단계 S100)
- [56] $\mathbf{s} \leftarrow \mathcal{HWT}_n(h_s)^d$
- [57] 열벡터 $\mathbf{s}$ 의 다항식은 0, -1, +1 의 계수를 가지며, 후술하는 바와 같이 비밀키로 결정된다.
- [58] 이어서 제1 에리 벡터($\mathbf{e}$)와 제2 에리값(e')을 다음과 같이 샘플링하여 결정한다(단계 S110)
- [59] $\mathbf{e} \leftarrow (D_{\alpha q}^n)^d$
- [60] $e' \leftarrow D_{\alpha q}^n$
- [61] 그리고 $\mathbf{A} \cdot \mathbf{s} = \mathbf{e} \pmod{q}$ 를 만족하는 행렬 $\mathbf{A} \in R_q^{d \times d}$ 을 랜덤하고 균일하게(uniformly at random) 선택한다(단계 S120).
- [62] 다음으로는 다음 관계를 만족하는 랜덤 열벡터 $\mathbf{b}$ 를 선택한다(단계 S130)
- [63] $\langle \mathbf{b}, \mathbf{s} \rangle = \lfloor q/2 \rfloor + e' \pmod{q}$
- [64] $\lfloor q/2 \rfloor$ 는 $q/2$ 의 내림값을 의미한다.
- [65] 이러한 과정을 거쳐서 결정되거나 선택된 행렬과 벡터를 이용하여 본 발명에 의한 공개키와 비밀키를 다음과 같이 생성한다(단계 S140).
- [66] 공개키(pk) = $(\mathbf{A} \parallel \mathbf{b}) \in R_q^{d \times (d+1)}$
- [67] 비밀키(sk) = $\mathbf{s}$
- [68] 이와 같이 공개키와 비밀키를 생성한 후에 메시지를 암호화하고 복호화하는 과정에 대해서 설명한다.
- [69] 공개키를 소유한 자는 메시지($\mathbf{m} \in R_2$)를 입력받는다. 즉 메시지 $\mathbf{m}$ 은 각 계수가 $\mathbb{Z}_2$ 의 원소인 n 차 다항식으로 표시된다.
- [70] 0, -1, +1 의 계수를 가지는 다항식 열벡터 $\mathbf{r}$ 을 다음과 같이 샘플링하여 결정한다.
- [71] $\mathbf{r} \leftarrow \mathcal{HWT}_n(h_r)^d$
- [72] 위에서 설명한 샘플링에서 $\mathcal{HWT}_n(h_s)^d$ 와 $\mathcal{HWT}_n(h_r)^d$ 는 $\{-1, 0, 1\}^{nd}$ 상의 임의의 분포, 즉 -1, 0, 1의 계수를 가지는 n 차 다항식 d 개를

각각 $\mathcal{HWT}_n(h_s)$ 와 $\mathcal{HWT}_n(h_r)$ 에서 랜덤하게 추출하는 과정으로 볼 수 있다.

[73] 이 다항식들과 공개키의 일부를 연산하여 제1 값을 산출하고, 메시지를 공개키 일부를 사용하여 인코딩한 제2 값을 산출한 후에, 제1 값과 제2 값을 연산하여 제3 값을 산출한다.

[74] 제1 값은 예를 들어, $A^T \cdot r$ 가 될 수 있고, 제2 값은 $m \cdot b$ 가 될 수 있으며, 제3 값은, 제1 값과 제2 값의 합인 $A^T \cdot r + m \cdot b$ 가 될 수 있다.

[75] 이 제3 값에 대해서 기설정된 하위 비트를 제거하기 위한 라운딩(rounding) 처리를 수행하기 위해 제3 값에 p/q를 곱해서 다음과 같이 암호문을 산출한다.

[76]
$$c = \left\lfloor \frac{p}{q} \cdot (A^T \cdot r + m \cdot b) \right\rfloor \in R_p^d$$

[77] R_p^d 는, 각각의 계수가 $\mathbb{Z}_p$ 에 포함되어 있는 n차 다항식 d개의 튜플(tuple)을 원소로 갖는 링을 의미한다.

[78] 본 발명에 의한 암호문 c 는 기존의 Kyber 방식과 달리 암호문이 하나의 요소(component)만을 가지고 있으며, 더욱이 $p < q$ 이기 때문에 암호문의 크기 역시 현저하게 축소된다. 따라서 기존의 래티스 기반 공개키 암호화 방식에 비하여 빠른 처리가 가능하고 암호화 통신에 있어서 통신부하 및 통신량이 현저하게 감소하여 관련 비용 역시 저감할 수 있는 효과가 제공된다.

[79] 본 발명에 의한 암호문 c 는 다음과 같이 복호화될 수 있다.

[80]
$$m = \left\lfloor \frac{2}{p} \cdot \langle c \cdot s \rangle \right\rfloor$$

[81] 이상 첨부 도면을 참고하여 본 발명에 대해서 설명하였지만 본 발명의 권리범위는 후술하는 특허청구범위에 의해 결정되며 전술한 실시예 및/또는 도면에 제한되는 것으로 해석되어서는 아니된다. 그리고 특허청구범위에 기재된 발명의, 당업자에게 자명한 개량, 변경 및 수정도 본 발명의 권리범위에 포함된다는 점이 명백하게 이해되어야 한다.

청구범위

- [청구항 1] 컴퓨터에 의해서 수행되는 공개키와 비밀키 생성 방법에 있어서,
비밀키(**s**)를 $\{-1, 0, 1\}^{nd}$ 위의 임의의 분포에서 샘플링하여 결정하는
제1 단계와,
제1 에러 벡터(**e**)를 $(D_{\alpha q}^n)^d$ 에서 샘플링하여 결정하고, 제2
에러값(**e'**)을 $D_{\alpha q}^n$ 에서 샘플링하여 결정하는 제2 단계와,
 $\mathbf{A} \cdot \mathbf{s} = \mathbf{e} \pmod{q}$ 를 만족하는 랜덤하게 균일한 행렬 **A**을 선택하는
제3 단계와,
 $\langle \mathbf{b}, \mathbf{s} \rangle = \lfloor q/2 \rfloor + e' \pmod{q}$ 을 만족하는 랜덤 열벡터 **b**를
선택하는 제4 단계와,
공개키(pk)를 $(\mathbf{A} \parallel \mathbf{b}) \in R_q^{d \times (d+1)}$ 로 결정하는 제4 단계를
포함하는,
공개키와 비밀키 생성 방법.
- [청구항 2] 청구항 1에 있어서,
제1 단계에서 생성되는 비밀키(**s**)는 $\mathcal{HWT}_n(h_s)^d$ 에서 샘플링되는,
공개키와 비밀키 생성 방법.
- [청구항 3] 컴퓨터에 의해 수행되는, 청구항 2의 공개키와 비밀키 생성 방법에
의해서 생성된 공개키를 이용한 메시지 암호화 방법에 있어서,
공개키와 메시지($\mathbf{m} \in R_2$)를 수신하는 제1 단계와,
-1,0,1 중 어느 하나의 계수를 가지는 n차 다항식 d개를 랜덤하게 추출하는
제2 단계와,
상기 다항식들 및 공개키의 일부를 연산하여 제1 값을 산출하는 제3
단계와,
상기 메시지를 공개키의 일부를 사용하여 인코딩하여 제2 값을 산출하는
제4 단계;
상기 제1 값과 제2 값을 연산하여 제3 값을 산출하는 제5 단계와,
제3값에 대해 기설정된 하위 비트를 제거하기 위한 라운딩 처리를
수행하여, 암호문을 산출하는 제6 단계를 포함하는,
암호화 방법.
- [청구항 4] 청구항 3에 있어서,
제2 단계는, 다항식 벡터(polynomial vector) **r** 을 $\mathcal{HWT}_n(h_r)^d$ 에서
샘플링하여 결정하는 단계이며,

제1 값은 $A^T \cdot \mathbf{r}$ 이며, 제2 값은 $m \cdot \mathbf{b}$ 이며, 제3 값은

$A^T \cdot \mathbf{r} + m \cdot \mathbf{b}$ 이며,

제6 단계에서 라운딩 처리된 암호문은

$$\mathbf{c} = \left\lfloor \frac{p}{q} \cdot (A^T \cdot \mathbf{r} + m \cdot \mathbf{b}) \right\rfloor \in R_p^d \quad \text{로 산출되는,}$$

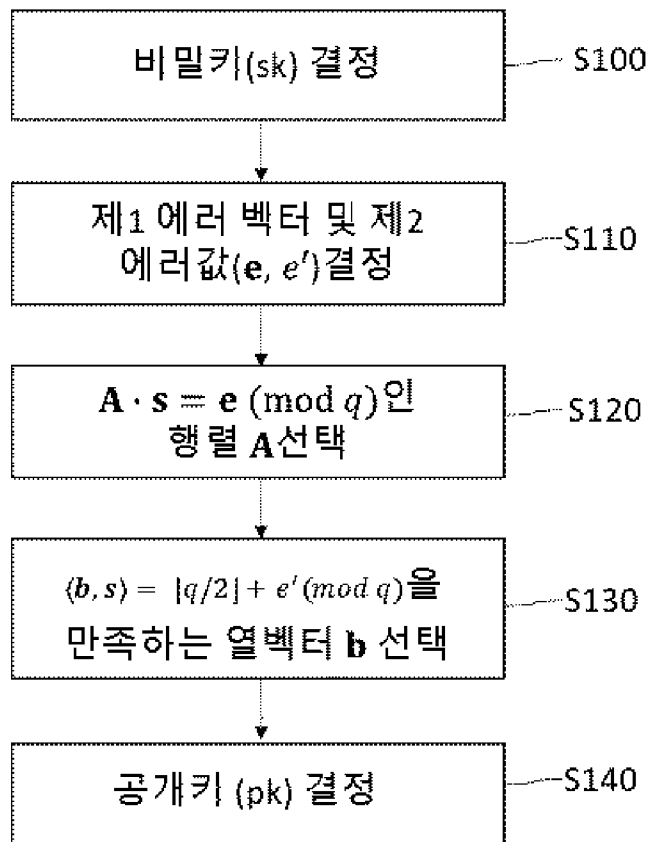
공개키 암호화 방법.

[청구항 5] 컴퓨터에 의해 수행되는, 청구항 2 또는 청구항 3에 의해 암호화된 암호문을 복호화하는 방법에 있어서,
암호문($\mathbf{c}$)을 수신하는 제1 단계와,
다음 수학식에 의해서 복호화하는 제2 단계를 포함하는,
복호화 방법.

[수학식]

$$m = \left\lfloor \frac{2}{p} \cdot \langle \mathbf{c} \cdot \mathbf{s} \rangle \right\rfloor$$

[도1]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2018/016014

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/30(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 9/08

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, LWR, public key

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	COSTACHE, Anamaria et al., "Homomorphic Encryption without Gaussian Noise", Cryptology ePrint Archive: Report 2017/163, Version: 20170223:140236, 23 February 2017 See pages 2, 6-7.	1-2
A		3-5
Y	CHASE, Melissa et al., "Security of Homomorphic Encryption", Homomorphic Encryption Standardization Workshop, 13-14 July 2017 See section 4.	1-2
A	CHEON, Jung Hee et al., "A Practical Post-Quantum Public-Key Cryptosystem Based on spLWE", Cryptology ePrint Archive: Report 2016/1055, Version: 20161121:021856, 21 November 2016 See sections 2.2-3.4.	1-5
A	BISHOP, Allison et al., "New Circular Security Counterexamples from Decision Linear and Learning with Errors", Cryptology ePrint Archive: Report 2015/715, Version: 20151201:020914, 01 December 2015 See section 3.	1-5
A	US 2015-0033033 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 29 January 2015 See paragraphs [0068]-[0081].	1-5



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

08 MARCH 2019 (08.03.2019)

Date of mailing of the international search report

08 MARCH 2019 (08.03.2019)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
Government Complex Daejeon Building 4, 189, Cheongsu-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/KR2018/016014

Patent document cited in search report	Publication date	Patent family member	Publication date
US 2015-0033033 A1	29/01/2015	CN 102822816 A	12/12/2012
		CN 102822816 B	20/01/2016
		DE 112011100327 T5	20/12/2012
		GB 2492698 A	09/01/2013
		GB 2492698 B	27/12/2017
		JP 2013-524277 A	17/06/2013
		JP 5812300 B2	11/11/2015
		US 2011-0243320 A1	06/10/2011
		US 8861716 B2	14/10/2014
		US 9252954 B2	02/02/2016
		WO 2011-123418 A1	06/10/2011

A. 발명이 속하는 기술분류(국제특허분류(IPC))

H04L 9/30(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

H04L 9/30; H04L 9/08

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, LWR, 공개키

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
Y	ANAMARIA COSTACHE 등, `Homomorphic Encryption without Gaussian Noise`, Cryptology ePrint Archive: Report 2017/163, Version: 20170223:140236, 2017.02.23 페이지 2, 6-7 참조.	1-2
A		3-5
Y	MELISSA CHASE 등, `Security of Homomorphic Encryption`, Homomorphic Encryption Standardization Workshop, 2017.07.13-14 섹션 4 참조.	1-2
A	JUNG HEE CHEON 등, `A Practical Post-Quantum Public-Key Cryptosystem Based on spLWE`, Cryptology ePrint Archive: Report 2016/1055, Version: 20161121:021856, 2016.11.21 섹션 2.2-3.4 참조.	1-5
A	ALLISON BISHOP 등, `New Circular Security Counterexamples from Decision Linear and Learning with Errors`, Cryptology ePrint Archive: Report 2015/715, Version: 20151201:020914, 2015.12.01 섹션 3 참조.	1-5
A	US 2015-0033033 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 2015.01.29 단락 [0068]-[0081] 참조.	1-5

☐ 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

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

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

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

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

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

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

“&” 동일한 대응특허문헌에 속하는 문헌

“P” 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

국제조사의 실제 완료일

2019년 03월 08일 (08.03.2019)

국제조사보고서 발송일

2019년 03월 08일 (08.03.2019)

ISA/KR의 명칭 및 우편주소



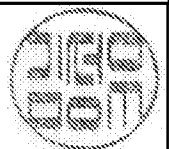
대한민국 특허청
(35208) 대전광역시 서구 청사로 189,
4동 (둔산동, 정부대전청사)

팩스 번호 +82-42-481-8578

심사관

김성우

전화번호 +82-42-481-3348



국제조사보고서에서
인용된 특허문헌

공개일

대응특허문헌

공개일

US 2015-0033033 A1

2015/01/29

CN 102822816 A

2012/12/12

CN 102822816 B

2016/01/20

DE 112011100327 T5

2012/12/20

GB 2492698 A

2013/01/09

GB 2492698 B

2017/12/27

JP 2013-524277 A

2013/06/17

JP 5812300 B2

2015/11/11

US 2011-0243320 A1

2011/10/06

US 8861716 B2

2014/10/14

US 9252954 B2

2016/02/02

WO 2011-123418 A1

2011/10/06