



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2023-0162328
(43) 공개일자 2023년11월28일

(51) 국제특허분류(Int. Cl.)
H04L 9/30 (2006.01) H04L 9/00 (2022.01)
H04L 9/08 (2006.01)
(52) CPC특허분류
H04L 9/3093 (2013.01)
H04L 9/003 (2013.01)
(21) 출원번호 10-2022-0062057
(22) 출원일자 2022년05월20일
심사청구일자 2022년05월20일

(71) 출원인
국방과학연구소
대전광역시 유성구 북유성대로488번길 160 (수남동)
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
박종환
서울특별시 종로구 홍지문2길 20
우주
서울특별시 성북구 안암로 145
김종현
서울특별시 성북구 안암로 145
(74) 대리인
특허법인 광장리앤코

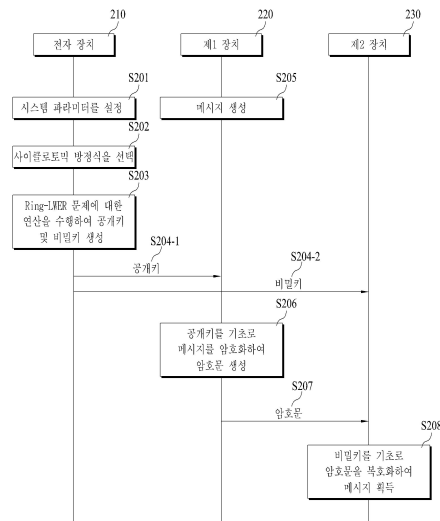
전체 청구항 수 : 총 11 항

(54) 발명의 명칭 양자 내성 공개키 암호화 방법 및 그 전자 장치와 시스템

(57) 요약

본 개시에 따르면, Ring-LWER 기반 양자 내성 공개키 암호화를 위해 전자 장치에 의해 수행되는 방법은, 적어도 하나의 시스템 파라미터를 설정하는 단계; 상기 적어도 하나의 시스템 파라미터에 기초하여 사이클로토믹 방정식을 선택하는 단계; 상기 선택된 사이클로토믹 방정식에 의해 정의되는 링을 이용하여 Ring-LWER 문제에 기반하는 공개키 및 비밀키를 생성하는 단계; 및 암호화를 수행하는 제1 장치를 위해 상기 공개키를 공개하고, 복호화를 수행하는 제2 장치에 상기 비밀키를 전송하는 단계를 포함할 수 있다.

대표도 - 도2



(52) CPC특허분류

H04L 9/0825 (2013.01)

명세서

청구범위

청구항 1

Ring-LWER(Ring-Learning With Errors and Roundings) 기반 양자 내성 공개키 암호화를 위해 전자 장치에 의해 수행되는 방법에 있어서,

적어도 하나의 시스템 파라미터를 설정하는 단계;

상기 적어도 하나의 시스템 파라미터에 기초하여 사이클로토믹 방정식을 선택하는 단계;

상기 선택된 사이클로토믹 방정식에 의해 정의되는 링을 이용하여 Ring-LWER 문제에 기반하는 공개키 및 비밀키를 생성하는 단계; 및

암호화를 수행하는 제1 장치를 위해 상기 공개키를 공개하고, 복호화를 수행하는 제2 장치에 상기 비밀키를 전송하는 단계를 포함하는, 방법.

청구항 2

제1항에 있어서,

상기 사이클로토믹 방정식을 선택하는 단계는,

상기 적어도 하나의 시스템 파라미터에 포함된 사이클로토믹 방정식의 최고 차항의 지수의 값에 기초하여, 제1 사이클로토믹 방정식 및 제2 사이클로토믹 방정식 중 하나를 선택하는 단계를 포함하는, 방법.

청구항 3

제2항에 있어서,

상기 제1 사이클로토믹 방정식은 상기 지수의 값이 2의 거듭제곱 형태인 것에 기초하여 선택되고,

상기 제2 사이클로토믹 방정식은 상기 지수의 값이 2의 거듭제곱과 3의 거듭제곱의 곱 형태인 것에 기초하여 선택되는, 방법.

청구항 4

제1항에 있어서,

상기 공개키는, 상기 링에서 랜덤으로 선택된 제1 다항식 및 상기 제1 다항식에 상기 Ring-LWER 문제를 기반으로 획득되는 제2 다항식을 포함하는, 방법.

청구항 5

제4항에 있어서,

상기 제1 장치는, 상기 전자 장치로부터 획득된 상기 공개키에 기초하여 메시지를 암호화함으로써 암호문을 생성하고 상기 제2 장치에 전송하고,

상기 제2 장치는, 상기 전자 장치로부터 수신된 상기 비밀키에 기초하여 상기 암호문을 복호화함으로써 상기 메시지를 획득하는, 방법.

청구항 6

제5항에 있어서,

상기 제1 장치는, 상기 제1 다항식에 기초하여 제1 행렬을 획득하고, 상기 제2 다항식 및 상기 메시지에 기초하여 제2 행렬을 획득함으로써, 상기 제1 행렬 및 상기 제2 행렬을 포함하는 상기 암호문을 생성하는, 방법.

청구항 7

제6항에 있어서,

상기 제1 장치는, 상기 제1 다항식에 상기 Ring-LWER 문제에 대한 연산을 수행하는 것에 기초하여 상기 제1 행렬을 획득하는, 방법.

청구항 8

제6항에 있어서,

상기 제1 장치는, 상기 제2 다항식에 상기 Ring-LWER 문제에 대한 연산 및 트렁케이트 함수를 적용한 결과와 상기 메시지에 인코딩 함수를 적용한 결과를 더하는 것에 기초하여 상기 제2 행렬을 획득하고,

상기 트렁케이트 함수는, 입력된 다항식에서 기 결정된 조건을 만족하는 항들의 계수를 추출하는 것에 기초하여 재구성된 다항식을 출력하는 함수인, 방법.

청구항 9

제8항에 있어서,

상기 제2 장치는, 상기 제1 행렬과 상기 비밀키에 상기 트렁케이트 함수를 적용한 결과 및 상기 제2 행렬에 기초한 연산을 수행함으로써 상기 메시지를 획득하는, 방법.

청구항 10

Ring-LWER 기반 양자 내성 공개키 암호화를 위한 전자 장치에 있어서,

트랜시버;

적어도 하나의 프로그램이 저장된 메모리;

상기 트랜시버 및 상기 메모리와 연결되는 프로세서를 포함하고, 상기 프로세서는 상기 적어도 하나의 프로그램을 실행함으로써,

적어도 하나의 시스템 파라미터를 설정하고,

상기 적어도 하나의 시스템 파라미터에 기초하여 사이클로토믹 방정식을 선택하고,

상기 선택된 사이클로토믹 방정식에 의해 정의되는 링을 이용하여 Ring-LWER 문제에 대한 연산을 수행함으로써 공개키 및 비밀키를 생성하고,

암호화를 수행하는 제1 장치를 위해 상기 공개키를 공개하고, 복호화를 수행하는 제2 장치에 상기 비밀키를 전송하도록 구성되는, 전자 장치.

청구항 11

비일시적 컴퓨터 판독 가능 저장 매체로서,

상기 비일시적 컴퓨터 판독 가능 저장 매체는, 전자 장치의 프로세서에 의해 실행되는 경우, 상기 전자 장치로 하여금 Ring-LWER 기반 양자 내성 공개키 암호화를 위한 방법을 수행하도록 하는 적어도 하나의 프로그램을 저장하고, 상기 방법은,

적어도 하나의 시스템 파라미터를 설정하는 단계;

상기 적어도 하나의 시스템 파라미터에 기초하여 사이클로토믹 방정식을 선택하는 단계;

상기 선택된 사이클로토믹 방정식에 의해 정의되는 링을 이용하여 Ring-LWER 문제에 기반하는 공개키 및 비밀키를 생성하는 단계; 및

암호화를 수행하는 제1 장치를 위해 상기 공개키를 공개하고, 복호화를 수행하는 제2 장치에 상기 비밀키를 전송하는 단계를 포함하는, 비일시적 컴퓨터 판독 가능 저장 매체.

발명의 설명

기술 분야

[0001] 본 개시는 Ring-LWER(Ring-Learning with Errors and Roundings) 기반 양자 내성 공개키 암호화 방법 및 이를 위한 전자 장치 및 시스템에 관한 것이다.

배경 기술

[0002] 일반적으로 사용되는 공개키 시스템 기술은 비밀통신을 수행하고자 하는 각각의 사용자 단말이 자신의 비밀키와 공개키를 쌍으로 생성하고, 비밀통신을 수행하고자 하는 상대방 단말은 정당한 공개키를 획득해야만 통신이 이루어지도록 구성된다. 이러한 비밀통신의 보안성을 강화하기 위해 양자 컴퓨터의 연산 체계로도 무력화시키기 어려운 양자 내성 암호화(quantum-resistant encryption)기법이 개발되었다. 이러한 양자 내성 암호화 기법에 대해 다양한 연구가 진행되고 있으나, 보다 효율적인 암호화 알고리즘을 가지면서도 보안 강도가 높은 양자 내성 암호화 기술이 요구되고 있다.

발명의 내용

해결하려는 과제

[0003] 본 개시의 실시예는 상술한 문제점을 해결하기 위하여 제안된 것으로, 적어도 하나의 시스템 파라미터를 설정하고, 적어도 하나의 시스템 파라미터에 기초하여 사이클로토믹 방정식을 선택하고, 선택된 사이클로토믹 방정식에 의해 정의되는 링을 이용하여 Ring-LWER 문제에 기반하는 공개키 및 비밀키를 생성하고, 암호화를 수행하는 제1 장치를 위해 공개키를 공개하고, 복호화를 수행하는 제2 장치에 비밀키를 전송하며, 제1 장치와 제2 장치는 이러한 공개키 및 비밀키에 각각 기초하여 암호화 및 복호화를 수행하도록 하는 랜덤 분포 Ring-LWER(Ring-Learning With Errors and Roundings) 기반의 양자 내성 공개키 암호화 방법 및 이를 지원하는 전자 장치와 시스템에 관한 것이다.

[0004] 본 실시예가 이루고자 하는 기술적 과제는 상기된 바와 같은 기술적 과제들로 한정되지 않으며, 이하의 실시예들로부터 또 다른 기술적 과제들이 유추될 수 있다.

과제의 해결 수단

[0005] 일 실시예에 따르면, Ring-LWER(Ring-Learning With Errors and Roundings) 기반 양자 내성 공개키 암호화를 위해 전자 장치에 의해 수행되는 방법은, 적어도 하나의 시스템 파라미터를 설정하는 단계; 상기 적어도 하나의 시스템 파라미터에 기초하여 사이클로토믹 방정식을 선택하는 단계; 상기 선택된 사이클로토믹 방정식에 의해 정의되는 링을 이용하여 Ring-LWER 문제에 기반하는 공개키 및 비밀키를 생성하는 단계; 및 암호화를 수행하는 제1 장치를 위해 상기 공개키를 공개하고, 복호화를 수행하는 제2 장치에 상기 비밀키를 전송하는 단계를 포함할 수 있다.

[0006] 일 실시예에 따르면, 상기 사이클로토믹 방정식을 선택하는 단계는, 상기 적어도 하나의 시스템 파라미터에 포함된 사이클로토믹 방정식의 최고 차항의 지수의 값에 기초하여, 제1 사이클로토믹 방정식 및 제2 사이클로토믹 방정식 중 하나를 선택하는 단계를 포함할 수 있다.

[0007] 일 실시예에 따르면, 상기 제1 사이클로토믹 방정식은 상기 지수의 값이 2의 거듭제곱 형태인 것에 기초하여 선택되고, 상기 제2 사이클로토믹 방정식은 상기 지수의 값이 2의 거듭제곱과 3의 거듭제곱의 곱 형태인 것에 기초하여 선택될 수 있다.

[0008] 일 실시예에 따르면, 상기 공개키는, 상기 링에서 랜덤으로 선택된 제1 다항식 및 상기 제1 다항식에 상기 Ring-LWER 문제에 기반하여 획득되는 제2 다항식을 포함할 수 있다.

[0009] 일 실시예에 따르면, 상기 제1 장치는, 상기 전자 장치로부터 획득된 상기 공개키에 기초하여 메시지를 암호화함으로써 암호문을 생성하고 상기 제2 장치에 전송하고, 상기 제2 장치는, 상기 전자 장치로부터 수신된 상기 비밀키에 기초하여 상기 암호문을 복호화함으로써 상기 메시지를 획득할 수 있다.

[0010] 일 실시예에 따르면, 상기 제1 장치는, 상기 제1 다항식에 기초하여 제1 행렬을 획득하고, 상기 제2 다항식 및 상기 메시지에 기초하여 제2 행렬을 획득함으로써, 상기 제1 행렬 및 상기 제2 행렬을 포함하는 상기 암호문을 생성할 수 있다.

[0011] 일 실시예에 따르면, 상기 제1 장치는, 상기 제1 다항식에 상기 Ring-LWER 문제에 대한 연산을 수행하는 것에

기초하여 상기 제1 행렬을 획득할 수 있다.

[0012] 일 실시예에 따르면, 상기 제1 장치는, 상기 제2 다항식에 상기 Ring-LWER 문제에 대한 연산 및 트렁케이트 함수를 적용한 결과와 상기 메시지에 인코딩 함수를 적용한 결과를 더하는 것에 기초하여 상기 제2 행렬을 획득할 수 있고, 상기 트렁케이트 함수는, 입력된 다항식에서 기 결정된 조건을 만족하는 항들의 계수를 추출하는 것에 기초하여 재구성된 다항식을 출력하는 함수일 수 있다.

[0013] 일 실시예에 따르면, 상기 제2 장치는, 상기 제1 행렬과 상기 비밀키에 상기 트렁케이트 함수를 적용한 결과 및 상기 제2 행렬에 기초한 연산을 수행함으로써 상기 메시지를 획득할 수 있다.

[0014] 일 실시예에 따르면, Ring-LWER 기반 양자 내성 공개키 암호화를 위한 전자 장치는, 트랜시버; 적어도 하나의 프로그램이 저장된 메모리; 상기 트랜시버 및 상기 메모리와 연결되는 프로세서를 포함할 수 있고, 상기 프로세서는 상기 적어도 하나의 프로그램을 실행함으로써, 적어도 하나의 시스템 파라미터를 설정하고, 상기 적어도 하나의 시스템 파라미터에 기초하여 사이클로토믹 방정식을 선택하고, 상기 선택된 사이클로토믹 방정식에 의해 정의되는 링을 이용하여 Ring-LWER 문제에 기반하는 공개키 및 비밀키를 생성하고, 암호화를 수행하는 제1 장치를 위해 상기 공개키를 공개하고, 복호화를 수행하는 제2 장치에 상기 비밀키를 전송하도록 구성될 수 있다.

[0015] 일 실시예에 따르면, 비밀시적 컴퓨터 판독 가능 저장 매체는, 전자 장치의 프로세서에 의해 실행되는 경우, 상기 전자 장치로 하여금 Ring-LWER 기반 양자 내성 공개키 암호화를 위한 방법을 수행하도록 하는 적어도 하나의 프로그램을 저장하고, 상기 방법은, 적어도 하나의 시스템 파라미터를 설정하는 단계; 상기 적어도 하나의 시스템 파라미터에 기초하여 사이클로토믹 방정식을 선택하는 단계; 상기 선택된 사이클로토믹 방정식에 의해 정의되는 링을 이용하여 Ring-LWER 문제에 기반하는 공개키 및 비밀키를 생성하는 단계; 및 암호화를 수행하는 제1 장치를 위해 상기 공개키를 공개하고, 복호화를 수행하는 제2 장치에 상기 비밀키를 전송하는 단계를 포함할 수 있다.

[0016] 기타 실시예들의 구체적인 사항은 상세한 설명 및 도면들에 포함된다.

발명의 효과

[0017] 본 개시에 따르면, 새로운 수학적 난제인 랜덤 분포 Ring-LWER 문제를 정의하고 이 문제를 기반으로 한 Ring-LWER 기반 암호화 기법을 설계함으로써 에러를 세밀하게 설정하면서도 공개키와 암호문의 크기를 최소화시켜 암호화의 효율성을 향상시킬 수 있으며, 에러를 가우시안 분포가 아닌 랜덤 분포에서 추출하므로 부채널 공격으로부터 안전한 암호화 기법을 제공할 수 있다.

[0018] 또한, 본 개시에 따르면, 사이클로토믹 방정식의 최고 차항인 지수 n 에 따라 상이한 사이클로토믹 방정식으로 생성된 링에서 연산을 정의함으로써, 지수 선택의 자유도를 높이면서 다양한 보안 강도에 대해 시스템 파라미터가 효율적으로 설정될 수 있다.

[0019] 또한, 본 개시에 따르면, 사이클로토믹 링에서 정의되는 연산인 다항식 곱 연산에서 발생하는 에러 전파도를 감소시키는 함수를 적용하여 암호화 기법을 설계함으로써, 암호문 생성 과정에서 엄밀한 파라미터 설정을 가능하게 하고 알고리즘 구현 속도를 포함한 암호화 시스템의 효율성을 향상시킬 수 있다.

[0020] 발명의 효과는 이상에서 언급한 효과로 제한되지 않으며, 언급되지 않은 또 다른 효과들은 청구범위의 기재로부터 당해 기술 분야의 통상의 기술자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

[0021] 도 1은 Ring-LWER 문제에 대한 개념도를 나타낸다.

도 2는 일 실시예에 따른 시스템의 전자 장치들에 의해 수행되는 Ring-LWER 기반 양자 내성 공개키 암호화 방법의 흐름도를 나타낸다.

도 3은 일 실시예에 따른 시스템에서 전자 장치의 블록도를 나타낸다.

도 4는 일 실시예에 따른 시스템에서 전자 장치에 의한 양자 내성 공개키 암호화를 위한 방법의 흐름도를 나타낸다.

발명을 실시하기 위한 구체적인 내용

[0022] 실시 예들에서 사용되는 용어는 본 개시에서의 기능을 고려하면서 가능한 현재 널리 사용되는 일반적인 용어들

을 선택하였으나, 이는 당 분야에 종사하는 기술자의 의도 또는 판례, 새로운 기술의 출현 등에 따라 달라질 수 있다. 또한, 특정한 경우는 출원인이 임의로 선정한 용어도 있으며, 이 경우 해당되는 설명 부분에서 상세히 그 의미를 기재할 것이다. 따라서 본 개시에서 사용되는 용어는 단순한 용어의 명칭이 아닌, 그 용어가 가지는 의미와 본 개시의 전반에 걸친 내용을 토대로 정의되어야 한다.

[0023] 명세서 전체에서 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있음을 의미한다. 또한, 명세서에 기재된 "...부", "...모듈" 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어 또는 소프트웨어로 구현되거나 하드웨어와 소프트웨어의 결합으로 구현될 수 있다.

[0024] 명세서 전체에서 기재된 "a, b, 및 c 중 적어도 하나"의 표현은, 'a 단독', 'b 단독', 'c 단독', 'a 및 b', 'a 및 c', 'b 및 c', 또는 'a,b,c 모두'를 포괄할 수 있다.

[0025] 이하에서 언급되는 "단말", "장치" 및 "전자 장치"는 네트워크를 통해 서버나 타 단말에 접속할 수 있는 컴퓨터나 휴대용 단말로 구현될 수 있다. 여기서, 컴퓨터는 예를 들어, 웹 브라우저(WEB Browser)가 탑재된 노트북, 데스크톱(desktop), 랩톱(laptop) 등을 포함하고, 휴대용 단말은 예를 들어, 휴대성과 이동성이 보장되는 무선 통신 장치로서, IMT(International Mobile Telecommunication), CDMA(Code Division Multiple Access), W-CDMA(W-Code Division Multiple Access), LTE(Long Term Evolution) 등의 통신 기반 단말, 스마트폰, 태블릿 PC 등과 같은 모든 종류의 핸드헬드(Handheld) 기반의 무선 통신 장치를 포함할 수 있다.

[0026] 아래에서는 첨부한 도면을 참고하여 본 개시의 실시 예에 대하여 본 개시가 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 개시는 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시 예에 한정되지 않는다. 이하, 도면을 참조하여 본 개시의 실시 예들이 상세히 설명된다.

[0027] 보안 통신의 성능을 향상시키기 위해 다양한 양자 내성 공개키 암호화 기법이 연구되고 있으며, 일반적으로 Ring-LWE 문제(Ring-Learning with Errors problem) 기반의 암호화 기법과 Ring-LWR 문제(Ring-Learning with Roundings problem) 기반의 암호화 기법이 고려되고 있다. 보다 구체적으로, Ring-LWE 기반 양자 내성 암호화 기법에서, m, n, q 는 양의 정수이고, 사이클로토믹 링 R 은 정수를 계수로 갖는 다항식 $\mathbb{Z}[X]$ 와 사이클로토믹 다항식 $\phi_m(X)$ 을 모듈러로 갖는 구조로, $\mathbb{Z}[X]/\langle \phi_m(X) \rangle$ 의 형태를 갖는다. R_q 는 $\mathbb{Z}_q[X]/\langle \phi_m(X) \rangle$ 의 형태를 갖는 사이클로토믹 링이고, D_s 및 D_e 는 R_q 상의 임의의 분포라고 가정하여, 랜덤하게 선택된 다항식 $a \in R_q$, $s \in D_s$ 와 $e \in D_e$ 에 대하여 $b = a \cdot s + e$ 를 계산하게 된다. 여기서 (a, b) 가 주어졌을 때, s 를 찾는 것이 Ring-LWE 기반 기법으로 정의되며, D_s 는 R_q 를, D_e 는 표준 편차가 σ 인 가우시안 분포 GD_σ 를 의미한다. $\mathbb{Z}_q$ 에서 정의된 LWE 문제는 2005년 Regev에 의해 처음 소개되었으며, 이와 동시에 Regev에 의해 처음으로 LWE 기반의 공개키 암호화 기법이 제안되었고, 이후 2010년 Lyubashevsky에 의해 링 위에서 정의된 Ring-LWE 문제가 제안되었다.

[0028] 한편, Ring-LWR 기반 양자 내성 암호화 기법은 Ring-LWE 문제의 변형인 Ring-LWR 문제를 이용하는 것으로, Ring-LWR 문제는 $a \cdot s$ 연산 값에 작은 범위의 에러 e 를 더하는 과정 대신 라운딩 함수인 $[\cdot]_p : \mathbb{Z}_q \rightarrow \mathbb{Z}_p$ 와 $[\cdot]_t : \mathbb{Z}_p \rightarrow \mathbb{Z}_t$ 를 이용한다. 이 때, 라운딩 함수는 $[x]_p = \lfloor \frac{p}{q} \cdot x \rfloor$, $[x]_t = \lfloor \frac{t}{p} \cdot x \rfloor$ 와 같이 연산되며, $\lfloor \cdot \rfloor$ 는 가장 가까운 정수를 나타내는 반올림 함수이다. Ring-LWR 문제는 $(a, b = [a \cdot s]_p)$ 가 주어졌을 때 s 를 찾는 문제로 정의된다. Ring-LWR 문제는 2012년 Peikert 등에 의해 처음 소개된 LWR 문제에서 확장된 것이며, 가우시안 분포에서 에러를 추출하는 과정이 없어 공개키 암호화 및 서명 기법에서 사용될 때, 키 생성 시간이 감소되고 공개키의 크기가 $\mathbb{Z}_q$ 에서 $\mathbb{Z}_p$ 로 감소될 수 있다.

[0029] 이러한 Ring-LWR 문제가 어렵다는 Ring-LWR 가정, 즉 (a, b) 가 주어졌을 때 s 를 찾는 것이 어렵다는 가정을 기반으로 하여 Ring-LWR 공개키 암호화 기법이 설계될 수 있다. 구체적으로, 비밀키 s 를 알고 있는 정당한 사용자만이 Ring-LWR 구조로 설계된 공개키 b 를 이용하여 암호화된 암호문 C 를 복호화하여 평문을 획득할 수 있다. 반

면, 비밀키가 없는 정당하지 않은 사용자는 공개키로부터 비밀키를 얻을 수 없고, 임의의 암호문을 복호화할 수 없다. Ring-LWR 기반 공개키 암호화 기법의 대표적인 방법으로는 2018년 Bhattacharya 등에 의해 소개된 기법이 있으며, 이는 다음과 같은 절차를 따른다.

[0030] 먼저, 키를 생성하는 단계로서, 보안 상수 λ 를 입력 받고, 설정된 시스템 파라미터에 기초하여 공개키 pk 및 비밀키 sk가 출력된다. 구체적으로 다항식 a 가 R_q 에서 랜덤하게 선택되고, 다항식 s 가 분포 D_s 에서 선택되며, 다항식 $b = [(a \cdot s)]_p$ 가 계산된다. 이에 따라 공개키 $pk = (a, b)$ 와 비밀키 $sk = s$ 가 출력된다.

[0031] 다음으로, 암호화를 수행하는 단계로서, 공개키 pk 및 ℓ 비트의 메시지 m 을 입력 받아 암호문 (C_1, C_2) 가 출력된다. 구체적으로, 다항식 r 이 분포 D_s 에서 선택되고, 다항식 $c_1 = [(a \cdot r)]_p$ 및 다항식 $c_2 = [(b \cdot r)]_t + E(m)$ 가 계산된다. 여기서 $E(m)$ 은 ℓ 비트의 메시지 m 을 입력으로 하여 R_t 에서의 다항식 원소를 출력하는 인코딩 함수를 나타낸다. 다항식 C_1 및 C_2 가 계산되면, 암호문 (C_1, C_2) 이 출력될 수 있다.

[0032] 다음으로, 복호화를 수행하는 단계로서, 비밀키 sk 및 암호문 (C_1, C_2) 를 입력 받아 메시지 m 이 출력된다. 구체적으로, 비밀키 및 암호문이 입력되면 $\frac{p}{t}C_2 - C_1 \cdot s$ 의 값이 계산되고, 계산된 값을 디코딩 함수 D에 입력하여 메시지 m 이 출력될 수 있다.

[0033] Ring-LWE 문제에서는, 에러를 특정 범위에서 직접 추출하여 $a \cdot s$ 에 더해주기 때문에 세밀한 에러 추출이 가능하고 이를 통해 모듈러 q 의 크기가 감소될 수 있다. 그러나 $b = a \cdot s + e$ 가 모듈러 q 에서 계산되기 때문에 공개키 및 암호문의 크기가 크다는 문제가 존재한다. 한편, Ring-LWR 문제는 에러를 직접 추출하지 않고 $a \cdot s$ 의 하위 비트를 자르는 방식으로 계산되기 때문에, 공개키 및 암호문이 q 보다 작은 모듈러스 p 에서 계산되어 획득되므로, 작은 크기를 갖는다는 장점이 있지만, 에러가 결정적으로 발생하며 비트 단위의 추가에 의해 세밀한 에러 추출이 불가능하다는 문제를 갖는다.

[0034] 또한, 전술한 바와 같은 대부분의 Ring-LWE 기반 암호화 기법 및 Ring-LWR 기반 암호화 기법은 사이클로토믹 방정식 $\phi_m(X)$ 를 $x^n + 1$ 로 사용한다. 해당 방정식에서 생성되는 링은 연산이 효율적이고 곱 연산에서 발생하는 에러 전파도가 작다는 장점을 갖는다. 여기서, 에러 전파도는 복호화 오류에 영향을 미치는 파라미터로서 에러 전파도가 커질수록 복호화 오류 확률이 증가하게 된다. 다항식 링의 원소인 두 다항식의 곱 연산 시, $c(x) = a(x) \cdot b(x) = c_0 + c_1x + \dots + c_{n-1}x^{n-1}$ 을 구성하는 계수들 c_i 가 각각 몇 개의 a_j 와 b_k 의 곱의 합으로 이루어져 있는지에 대한 연산으로 정의된다. 그러나 해당 링에서의 암호화 기법이 안전하기 위해서는 정수 n 이 2의 거듭제곱 꼴이어야 한다는 제한 조건이 만족되어야 한다. 보안 강도를 높이기 위해서는 사이클로토믹 방정식의 지수 n 을 증가시켜야 하는데, 이러한 제한 조건 하에서는 n 이 2배로 증가되면 암호문 값을 포함한 전반적인 시스템 파라미터 값이 비효율적으로 증가한다는 문제가 있다. 따라서 Ring-LWE 문제와 Ring-LWR 문제의 장점을 모두 가지면서도 부채널 공격으로부터 안전하고, 시스템 파라미터를 효율적으로 설정할 수 있도록 지수 n 의 자유도가 높은 사이클로토믹 방정식을 이용하면서 에러 전파도의 증가를 최소화시킬 수 있는 방안이 요구될 수 있다.

[0035] 이를 위해, 본 발명은 도 1의 개념도에 도시된 바와 같은 래티스 기반의 새로운 수학적 난제인 랜덤 분포 Ring-LWER 문제에 기반한 양자 내성 암호화 방법을 제안한다. 본 개시에서 제안되는 양자 내성 암호화를 수행하기 위해 이용되는 Ring-LWER 문제, 사이클로토믹 방정식 및 트렁케이트(truncate) 함수가 아래에서 상세히 설명된다.

[0036] Ring-LWER 문제

[0037] m, n, q 는 양의 정수이고, 사이클로토믹 링 R 은 정수를 계수로 가지는 다항식 $\mathbb{Z}[X]$ 와 사이클로토믹 다항식 $\phi_m(X)$ 을 모듈러로 갖는 구조로서 $\mathbb{Z}[X]/\langle \phi_m(X) \rangle$ 의 형태를 갖는다. R_q 는 $\mathbb{Z}_q[X]/\langle \phi_m(X) \rangle$ 의 형태를 갖는 사이클로토믹 링이고, D_s 는 R_q 상의 임의의 분포이며, D_e 는 Ring-LWE 문제와는 달리 R_q 상의 랜덤 분포라고 가

정된다. 이때, 랜덤하게 선택된 다항식 $a \in R_q$, $s \in D_s$ 와 $e \in D_e$ 에 대하여 $b = [a \cdot s + e]_p$ 를 계산한다. 여기서 (a, b)가 주어졌을 때, s를 찾는 것이 Ring-LWE 문제라고 정의될 수 있다. 즉, Ring-LWE 문제는, 다항식 a 및 s의 연산 결과 as(110)에 랜덤 분포에서 추출된 에러 e(120)를 더하여 as + e (130)를 획득하고, 라운드 함수를 적용하여(140), 그 결과로 획득된 다항식(150)에서 s를 찾는 것을 의미할 수 있다.

[0038] 사이클로토믹 방정식

[0039] 일반적인 Ring-LWE 기반 공개키 암호화 기법에서, 사이클로토믹 방정식으로 방정식 $x^n + 1$ 및 방정식 $x^n + x^{n-1} + \dots + x + 1$ 이 사용된다. 방정식 $x^n + 1$ 을 링의 모듈러 연산으로 사용하는 경우, 에러 전파도가 n이 되므로 에러 전파도가 작은 값을 가진다는 장점이 있지만, 지수 n이 2의 거듭제곱 형태여야 한다는 제한 조건이 발생하게 된다(예: n = 512, 1024, 2048 등). 이러한 제한 조건은 시스템 파라미터를 비효율적으로 증가시킨다는 문제점이 있다. 한편 방정식 $x^n + x^{n-1} + \dots + x + 1$ 을 링의 모듈러 연산으로 사용하는 경우, 지수 n의 선택에 대한 자유도가 높아진다는 장점이 있지만, 에러 전파도가 2n이 되므로 에러 전파도가 큰 값을 가진다는 문제점이 있다.

[0040] 따라서, 본 개시의 일 실시예에 따른 Ring-LWE 기반 양자 내성 암호화 기법에서는, 지수 n이 2의 거듭제곱 형태일 경우에는 방정식 $x^n + 1$ 을 사이클로토믹 방정식으로 사용하고, 그 외의 지수에 대해서는 지수 n의 선택에 대한 자유도가 높고 에러 전파도가 작은 새로운 방정식 $x^n - x^{n/2} + 1$ 을 사이클로토믹 방정식으로 사용한다. 이와 같은 방정식 $x^n - x^{n/2} + 1$ 에 의해 생성되는 링은 방정식 $x^n + 1$ 로 생성되는 링의 에러 전파도보다는 크고 방정식 $x^n + x^{n-1} + \dots + x + 1$ 로 생성되는 링의 에러 전파도보다는 작은 에러 전파도 값을 가진다. 또한, 방정식 $x^n - x^{n/2} + 1$ 에서는 지수 n이 2의 거듭제곱과 3의 거듭제곱의 곱 형태이면 되므로(예: n = 648, 768, 864, 972 등), 지수 n의 선택의 자유도를 향상시킬 수 있다. 더불어, 방정식 $x^n - x^{n/2} + 1$ 에 의해 생성되는 링을 기반으로 하는 연산에서 발생하는 에러전파도를 방정식 $x^n + 1$ 로 생성되는 링의 에러 전파도보다 작게 만들기 위해 아래의 트렁케이트 함수를 사용한다.

[0041] 트렁케이트 함수

[0042] 본 개시의 일 실시예에 따른 Ring-LWE 기반 양자 내성 암호화 기법에서는, 사이클로토믹 방정식 $x^n + 1$ 및 $x^n - x^{n/2} + 1$ 로 각각 생성되는 링 $\mathbb{Z}_q[X]/\langle x^n + 1 \rangle$ 및 $\mathbb{Z}_q[X]/\langle x^n - x^{n/2} + 1 \rangle$ 에서의 에러 전파도를 더욱 감소시키기 위해 트렁케이트 함수가 사용될 수 있다. 트렁케이트 함수는 주어진 방정식 계수 중에서 $\frac{n}{2} - 1$ 차 항 이하의 ℓ 개 항에 대한 계수만 선택적으로 추출할 수 있다. 트렁케이트 함수의 연산에 의해 3항식 $x^n - x^{n/2} + 1$ 에러 전파도가 가장 작은 영역이 되므로, 링 연산에서 발생하는 에러의 크기가 효율적으로 제한될 수 있다. 일 실시예에 따르면, 트렁케이트 함수는 방정식 $a = a_0 + a_1x + \dots + a_{n-1}x^{n-1}$ 과 n/2보다 작거나 같은 정수 ℓ 을 입력 받을 수 있다. 이어서, 트렁케이트 함수는 방정식 a 로부터 계수 집합 $(a_{\frac{n}{2}-1}, \dots, a_{\frac{n}{2}-\ell})$ 을 추출하고, 추출된 계수들로 방정식을 생성하여 출력할 수 있다. 트렁케이트 함수에 의해 추출되는 방정식의 일 예는 아래 수학식 1과 같다.

[0043] [수학식 1]

$$\text{Trunc}(a, \ell) = \frac{a_{\frac{n}{2}-\ell} + a_{\frac{n}{2}-\ell+1}x + \dots + a_{\frac{n}{2}-1}x^{\ell-1}}$$

[0045] 이하 도 2 내지 도 4를 통해, Ring-LWE 기반의 양자 내성 공개키 암호화 방법이 상세히 설명된다.

- [0046] 도 2는 일 실시예에 따른 시스템의 전자 장치들에 의해 수행되는 Ring-LWER 기반 양자 내성 공개키 암호화를 위한 방법의 흐름도를 나타낸다. 일 실시예에 따르면, 시스템은 전자 장치(210), 제1 장치(220) 및 제2 장치(230)를 포함할 수 있고, 도 2는 전자 장치(210), 제1 장치(220) 및 제2 장치(230)에 의해 수행되는 Ring-LWER 기반 양자 내성 공개키 암호화 방법을 예시한다. 일 실시예에 따르면, 전자 장치(210)는 공개키 및 비밀키를 생성하는 키 생성 서버일 수 있고, 제1 장치(220)는 제2 장치(230)에 메시지를 송신하고자 하는 송신 장치일 수 있으며, 제2 장치(230)는 제1 장치(220)가 송신한 메시지를 수신하는 수신 장치일 수 있다.
- [0047] 도 2를 참조하면, 제1 장치(220) 및 제2 장치(230)는 전자 장치(210)가 생성한 공개키 및 비밀키를 이용하여 메시지를 암호화 및 복호화함으로써 서로 간에 통신을 수행할 수 있다.
- [0048] 전자 장치(210)는 공개키 및 비밀키 생성에 이용하기 위한 적어도 하나의 시스템 파라미터를 설정할 수 있다 (S201). 일 실시예에 따른 시스템에서, 시스템 파라미터 n , ℓ , q , p , t , D_s , D_e 가 설정되어 시스템 전반에서 사용될 수 있다. 여기서, n 및 ℓ 은 $1 \leq \ell \leq \frac{n}{2}$ 을 만족하는 양의 정수이다. 보다 구체적으로, 사이클로토믹 방정식 $x^n + 1$ 이 사용되는 경우, n 은 2의 거듭제곱 형태인 양의 정수이고, 사이클로토믹 방정식 $x^n - x^{n/2} + 1$ 이 사용되는 경우, n 은 2의 거듭제곱과 3의 거듭제곱의 곱 형태인 양의 정수일 수 있다. 또한, 모듈러스 q , p , t 는 모두 2의 거듭제곱 형태인 양의 정수이며, $t < p < q$ 를 만족한다. 또한, D_s 는 R_q 상의 임의의 분포이며, D_e 는 R_q 상의 랜덤 분포일 수 있다. 한편, 도 2에 도시되지는 않았으나, 제1 장치(220) 및 제2 장치(230)는 전자 장치(210)로부터 시스템 파라미터에 대한 정보를 획득하여, 암호화 및 복호화를 수행하는 데 시스템 파라미터를 이용할 수 있다.
- [0049] 일 실시예에서, 전자 장치(210)는 설정된 시스템 파라미터에 기초하여 사이클로토믹 방정식을 선택할 수 있다 (S202). 보다 구체적으로, 시스템 파라미터에서 n 이 2의 거듭제곱 형태인 경우, 전자 장치(210)는 사이클로토믹 방정식 $x^n + 1$ 을 선택하고 해당 방정식에 의해 정의되는 사이클로토믹 링 $R_q = \mathbb{Z}_q[X]/\langle x^n + 1 \rangle$ 를 획득할 수 있다. 시스템 파라미터에서 n 이 2의 거듭제곱과 3의 거듭제곱의 곱 형태인 경우, 전자 장치(210)는 사이클로토믹 방정식 $x^n - x^{n/2} + 1$ 을 선택하고 해당 방정식에 의해 정의되는 사이클로토믹 링 $R_q = \mathbb{Z}_q[X]/\langle x^n - x^{n/2} + 1 \rangle$ 를 획득할 수 있다.
- [0050] 일 실시예에서, 전자 장치(210)는 Ring-LWER 문제에 대한 연산을 수행하여 공개키 및 비밀키를 생성할 수 있다. 즉, 전자 장치(210)는 보안 상수 1^λ 를 입력 받고 Ring-LWER 문제를 계산함으로써 공개키 pk 및 비밀키 sk를 생성할 수 있다. 보다 구체적으로, 전자 장치(210)는 R_q 에서 다항식 a 를 랜덤하게 선택하고, 분포 D_s 에서 다항식 s 를 선택하며, 에러를 나타내는 다항식 e 를 분포 D_e 에서 선택할 수 있다. 이어서, 전자 장치(210)는 다항식 $b = [a \cdot s + e]_p$ 를 계산하여, 공개키 $pk = (a, b)$ 및 비밀키 $sk = s$ 를 생성할 수 있다. 일 실시예에 따르면, 공개키 pk 및 비밀키 sk는 제2 장치(230)를 위한 키 쌍을 이루며, 공개키 pk는 제2 장치(230)에 메시지를 송신하려는 장치들(예: 제1 장치(220))이 메시지를 암호화하는 것에 이용되고, 비밀키 sk는 이들 장치로부터 메시지를 수신한 제2 장치(230)가 메시지를 복호화하는 것에 이용될 수 있다.
- [0051] 일 실시예에서, 전자 장치(210)는 생성된 공개키 $pk = (a, b)$ 를 공개하며(S204-1), 이에 따라 제1 장치(220)는 제2 장치로 송신할 메시지를 암호화하기 위해 전자 장치(210)로부터 공개키 pk를 획득할 수 있다. 또한, 전자 장치(210)는 생성된 비밀키 $sk = s$ 를 제2 장치(230)에 전송할 수 있다.
- [0052] 일 실시예에서, 제1 장치(220)는 메시지를 생성하고(S205), 전자 장치(210)로부터 획득된 공개키를 기초로 메시지를 암호화하여 암호문을 생성할 수 있다(S206). 일 실시예에서, 메시지는 제1 장치(220)로부터 제2 장치(230)에 전송될 메시지일 수 있다. 일 실시예에서, 제1 장치(220)는 공개키 pk 및 ℓ 비트의 메시지 m 에 기초하여 암호문 (C_1, C_2) 를 생성할 수 있으며, 구체적인 생성 과정은 아래에서 설명될 수 있다.
- [0053] 먼저, 제1 장치(220)는 분포 D_s 에서 다항식 r 을 선택하고, D_e 에서 e_1 및 e_2 를 추출할 수 있다. 전자 장치(220)는 선택한 다항식 r , 추출한 에러 e_1 및 e_2 , 시스템 파라미터, 획득한 공개키 $pk = (a, b)$ 및 생성한 메시지 m 에

기초하여 아래의 수학식 2 및 수학식 3과 같이 행렬 C_1 및 C_2 를 계산할 수 있다.

[0054] [수학식 2]

$$C_1 = [a \cdot r + e_1]_p$$

[0056] [수학식 3]

$$C_2 = Trunc([b \cdot r + e_2]_t, \ell) + E(m)$$

[0058] 여기서 $E(m)$ 은 ℓ 비트의 메시지 m 을 입력으로 하여 Z_t^ℓ 에서의 원소를 출력하는 인코딩 함수를 나타낸다. 또한,

$Trunc([b \cdot r + e_2]_t, \ell)$ 는 방정식 $[b \cdot r + e_2]_t$ 및 ℓ 을 입력으로 하여, 방정식 $[b \cdot r + e_2]_t$ 중 $\frac{n}{2} - \ell$ 번째 항에서 $\frac{n}{2} - 1$ 번째 항까지의 계수로 재구성된 방정식을 출력하는 트렁케이트 함수를 나타낸다. 이와 같이 제1 장치(220)는 암호문 (C_1 , C_2)를 생성하고, 생성된 암호문을 제2 장치(230)에 전송할 수 있다(S206).

[0059] 일 실시예에서, 제2 장치(230)는 비밀키를 기초로 암호문을 복호화하여 메시지를 획득할 수 있다. 즉, 제2 장치(230)는 전자 장치(210)로부터 수신한 비밀키 sk 를 이용하여 제1 장치(220)로부터 수신한 암호문 (C_1 , C_2)을 복호화함으로써 메시지 m 을 생성할 수 있다. 먼저, 제2 장치(230)는 시스템 파라미터, 비밀키 $sk = s$ 및 암호문 (C_1 , C_2)에 기초하여 아래의 수학식 4와 같이 다항식 V 를 계산할 수 있다.

[0060] [수학식 4]

$$V = \frac{p}{t} C_2 - Trunc(C_1 \cdot s, \ell)$$

[0062] 여기서, p , t , ℓ 은 단계 S201에서 설정된 시스템 파라미터이며, C_1 , C_2 는 암호문에 포함되는 각 행렬을 나타내고, $Trunc(C_1 \cdot s, \ell)$ 는 $C_1 \cdot s$ 및 ℓ 을 입력으로 하여 $C_1 \cdot s$ 중에서 $\frac{n}{2} - \ell$ 번째 항에서 $\frac{n}{2} - 1$ 번째 항까지의 계수로 재구성된 방정식을 출력하는 트렁케이트 함수를 나타낸다.

[0063] 이어서 제2 장치(230)는 수학식 4에서 획득된 V 에 디코딩 함수 D 를 적용함으로써 아래 수학식 5와 같이 메시지 m 을 획득할 수 있다.

[0064] [수학식 5]

$$m = D(V)$$

[0066] 한편, 도 2에서는 제1 장치(220)가 메시지를 생성하는 단계(S205)가 공개키를 획득하는 단계(S204-1) 이전에 수행되는 것으로 도시되어 있으나, 제1 장치는 이에 제한되지 않고 공개키를 획득한 후 메시지를 생성할 수도 있다.

[0067] 도 3은 일 실시예에 따른 시스템에서 Ring-LWER 기반 양자 내성 공개키 암호화를 위한 방법을 수행하는 전자 장치의 블록도를 나타낸다. 일 실시예에서, 도 2에 도시된 전자 장치(210), 제1 장치(220) 및 제2 장치(230)는 각각 도 3에 도시된 바와 같이 구성될 수 있다. 도 3을 참조하면, 전자 장치(예: 전자 장치(210), 제1 장치(220) 및 제2 장치(230))는 트랜시버(transceiver)(310), 프로세서(320) 및 메모리(330)를 포함할 수 있다. 도 3에 도시된 구성요소들 외에 다른 범용적인 구성요소들이 전자 장치에 더 포함될 수 있음을 본 실시 예와 관련된 기술분야에서 통상의 지식을 가진 자라면 이해할 수 있다.

[0068] 트랜시버(310)는 유/무선 통신을 수행하기 위한 장치이다. 트랜시버(310)가 이용하는 통신 기술에는 GSM(Global System for Mobile communication), CDMA(Code Division Multi Access), LTE(Long Term Evolution), 5G, WLAN(Wireless LAN), Wi-Fi(Wireless-Fidelity), 블루투스(Bluetooth™), RFID(Radio Frequency Identification), 적외선 통신(Infrared Data Association; IrDA), ZigBee, NFC(Near Field Communication)

등이 있을 수 있다.

- [0069] 프로세서(320)는 전자 장치의 전반적인 동작을 제어하고 데이터 및 신호를 처리할 수 있다. 프로세서(320)는 적어도 하나의 하드웨어 유닛으로 구성될 수 있다. 또한, 프로세서(320)는 메모리(330)에 저장된 프로그램 코드를 실행하여 생성되는 하나 이상의 소프트웨어 모듈에 의해 동작할 수 있다. 프로세서(320)는 메모리(330)에 저장된 프로그램 코드를 실행하여 전자 장치의 전반적인 동작을 제어하고 데이터 및 신호를 처리할 수 있다. 프로세서(320)는 본 개시에서 설명되는 적어도 하나의 방법을 수행하도록 구성될 수 있다.
- [0070] 메모리(330)는 본 개시에서 설명된 적어도 하나의 방법을 수행하기 위한 프로그램을 실행하는 데 필요한 프로그램 코드 및 정보를 저장할 수 있다. 메모리(330)는 휘발성 메모리 또는 비휘발성 메모리일 수 있다.
- [0071] 도 4는 일 실시예에 따른 시스템의 전자 장치에 의한 양자 내성 공개키 암호화를 위한 방법의 흐름도를 나타낸다. 도 4는 도 2에 도시된 전자 장치(210)의 동작 방법을 예시할 수 있다.
- [0072] 도 4를 참조하면, 단계 S401에서, 전자 장치는 적어도 하나의 시스템 파라미터를 설정할 수 있다. 즉, 전자 장치는 공개키 및 비밀키 생성에 이용하기 위한 적어도 하나의 시스템 파라미터를 설정할 수 있다. 시스템 파라미터의 구체적인 내용은 도 2의 단계 S201에서 상세히 설명된다.
- [0073] 단계 S402에서, 전자 장치는 적어도 하나의 시스템 파라미터에 기초하여 사이클로토믹 방정식을 선택할 수 있다. 일 실시예에 따르면, 전자 장치는 적어도 하나의 시스템 파라미터에 포함된 사이클로토믹 방정식의 최고차항의 지수의 값에 기초하여, 제1 사이클로토믹 방정식 및 제2 사이클로토믹 방정식 중 하나를 선택할 수 있다. 제1 사이클로토믹 방정식은 상기 지수의 값이 2의 거듭제곱 형태인 것에 기초하여 선택될 수 있고, 제2 사이클로토믹 방정식은 상기 지수의 값이 2의 거듭제곱과 3의 거듭제곱의 곱 형태인 것에 기초하여 선택될 수 있다. 예를 들어, 도 2에서 설명된 바와 같이 제1 사이클로토믹 방정식은 $x^n + 1$ 일 수 있고, 제2 사이클로토믹 방정식은 $x^n - x^{n/2} + 1$ 일 수 있다. 사이클로토믹 방정식을 선택하는 것에 대한 구체적인 내용은 도 2의 단계 S202에서 상세히 설명된다.
- [0074] 단계 S403에서, 전자 장치는 선택된 사이클로토믹 방정식에 의해 정의되는 링을 이용하여 Ring-LWER 문제에 기반하는 공개키 및 비밀키를 생성할 수 있다. 일 실시예에서, 공개키는 링에서 랜덤으로 선택된 제1 다항식 및 제1 다항식에 Ring-LWER 문제를 적용하여 획득되는 제2 다항식을 포함할 수 있다. 예를 들어, 도 2에서 설명된 바와 같이, 전자 장치는 선택된 사이클로토믹 방정식에 따라 사이클로토믹 링 $R_q = \mathbb{Z}_q[X]/\langle x^n + 1 \rangle$ 또는 사이클로토믹 링 $R_q = \mathbb{Z}_q[X]/\langle x^n - x^{n/2} + 1 \rangle$ 를 획득할 수 있다. 전자 장치는 R_q 에서 다항식 a 를 제1 다항식으로 선택할 수 있으며, 다항식 a 와 분포 D_s 에서 선택된 다항식 s 및 분포 D_e 에서 선택된 다항식 e 에 Ring-LWER 문제를 적용함으로써 다항식 $b = [a \cdot s + e]_p$ 를 제2 다항식으로서 획득할 수 있다. 또한 일 실시예에서, 비밀키 sk 는 분포 D_s 에서 선택된 다항식 s 일 수 있다. 공개키 및 비밀키의 생성에 대한 내용은 도 2의 단계 S203에서 상세히 설명된다.
- [0075] 단계 S404에서, 전자 장치는 암호화를 수행하는 제1 장치를 위해 공개키를 공개하고, 복호화를 수행하는 제2 장치에 비밀키를 전송할 수 있다. 예를 들어, 제1 장치는 도 2의 제1 장치(220)일 수 있고, 제2 장치는 도 2의 제2 장치(230)일 수 있다. 전자 장치는 제1 장치가 공개키를 획득할 수 있도록 공개키를 공개할 수 있고, 제2 장치에게 비밀키를 전송할 수 있다.
- [0076] 일 실시예에서, 제1 장치는 전자 장치로부터 획득된 공개키에 기초하여 메시지를 암호화함으로써 암호문을 생성하고 이를 제2 장치에 전송할 수 있다. 구체적으로, 제1 장치는 제1 다항식에 기초하여 제1 행렬을 획득하고, 제2 다항식 및 메시지에 기초하여 제2 행렬을 획득함으로써, 제1 행렬 및 제2 행렬을 포함하는 암호문을 생성할 수 있다. 또한, 제1 장치는 제1 다항식에 Ring-LWER 문제에 대한 연산을 수행하는 것에 기초하여 제1 행렬을 획득할 수 있다. 또한, 제1 장치는 제2 다항식에 Ring-LWER 문제에 대한 연산 및 트렁케이트 함수를 적용한 결과와 메시지에 인코딩 함수를 적용한 결과를 더하는 것에 기초하여 제2 행렬을 획득할 수 있다. 여기서 트렁케이트 함수는, 입력된 다항식에서 기 결정된 조건을 만족하는 항들의 계수를 추출하는 것에 기초하여 재구성된 다항식을 출력하는 함수일 수 있다. 예를 들어, 도 2를 참조하면, 제1 다항식은 a 에 대응할 수 있고, 제2 다항식

은 $b = [a \cdot s + e]_p$ 에 대응할 수 있으며, 메시지는 m 에 대응하고, 제1 행렬 및 제2 행렬은 각각 C_1 및 C_2 에 대응할 수 있다. 제1 장치에 의한 공개키 획득과 암호화 과정은 도 2의 단계 S204-1 및 S206에서 상세히 설명된다.

[0077] 일 실시예에서, 제2 장치는 전자 장치로부터 수신된 비밀키에 기초하여 암호문을 복호화할 수 있다. 구체적으로, 제2 장치는 제1 행렬과 비밀키에 트렁케이트 함수를 적용한 결과 및 제2 행렬에 기초한 연산을 수행함으로써 메시지를 획득할 수 있다. 예를 들어, 도 2를 참조하면, 제1 행렬 및 제2 행렬은 각각 C_1 및 C_2 에 대응할 수 있고, 비밀키는 $sk = s$ 에 대응하며, 메시지는 m 에 대응할 수 있다. 제2 장치에 의한 복호화 과정의 상세한 내용은 도 2의 단계 S208에서 확인될 수 있다.

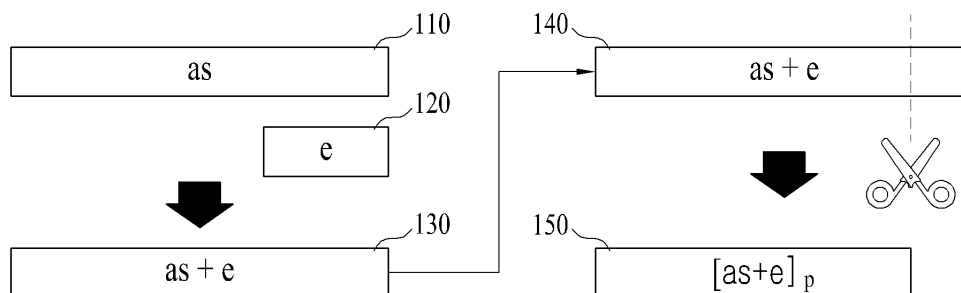
[0078] 전술한 실시예들에 따른 전자 장치 또는 단말은, 프로세서, 프로그램 데이터를 저장하고 실행하는 메모리, 디스크 드라이브와 같은 영구 저장부(permanent storage), 외부 장치와 통신하는 통신 포트, 터치 패널, 키(key), 버튼 등과 같은 사용자 인터페이스 장치 등을 포함할 수 있다. 소프트웨어 모듈 또는 알고리즘으로 구현되는 방법들은 상기 프로세서상에서 실행 가능한 컴퓨터가 읽을 수 있는 코드들 또는 프로그램 명령들로서 컴퓨터가 읽을 수 있는 기록 매체 상에 저장될 수 있다. 여기서 컴퓨터가 읽을 수 있는 기록 매체로 마그네틱 저장 매체(예컨대, ROM(read-only memory), RAM(random-access memory), 플로피 디스크, 하드 디스크 등) 및 광학적 판독 매체(예컨대, 시디롬(CD-ROM), 디브이디(DVD: Digital Versatile Disc)) 등이 있다. 컴퓨터가 읽을 수 있는 기록 매체는 네트워크로 연결된 컴퓨터 시스템들에 분산되어, 분산 방식으로 컴퓨터가 판독 가능한 코드가 저장되고 실행될 수 있다. 매체는 컴퓨터에 의해 판독가능하며, 메모리에 저장되고, 프로세서에서 실행될 수 있다.

[0079] 본 실시 예는 기능적인 블록 구성들 및 다양한 처리 단계들로 나타내어질 수 있다. 이러한 기능 블록들은 특정 기능들을 실행하는 다양한 개수의 하드웨어 또는/및 소프트웨어 구성들로 구현될 수 있다. 예를 들어, 실시 예는 하나 이상의 마이크로프로세서들의 제어 또는 다른 제어 장치들에 의해서 다양한 기능들을 실행할 수 있는, 메모리, 프로세싱, 로직(logic), 룩 업 테이블(look-up table) 등과 같은 직접 회로 구성들을 채용할 수 있다. 구성 요소들이 소프트웨어 프로그래밍 또는 소프트웨어 요소들로 실행될 수 있는 것과 유사하게, 본 실시 예는 데이터 구조, 프로세스들, 루틴들 또는 다른 프로그래밍 구성들의 조합으로 구현되는 다양한 알고리즘을 포함하여, C, C++, 자바(Java), 어셈블리(assembler) 등과 같은 프로그래밍 또는 스크립팅 언어로 구현될 수 있다. 기능적인 측면들은 하나 이상의 프로세서들에서 실행되는 알고리즘으로 구현될 수 있다. 또한, 본 실시 예는 전자적인 환경 설정, 신호 처리, 및/또는 데이터 처리 등을 위하여 종래 기술을 채용할 수 있다. “매커니즘”, “요소”, “수단”, “구성”과 같은 용어는 넓게 사용될 수 있으며, 기계적이고 물리적인 구성들로서 한정되는 것은 아니다. 상기 용어는 프로세서 등과 연계하여 소프트웨어의 일련의 처리들(routines)의 의미를 포함할 수 있다.

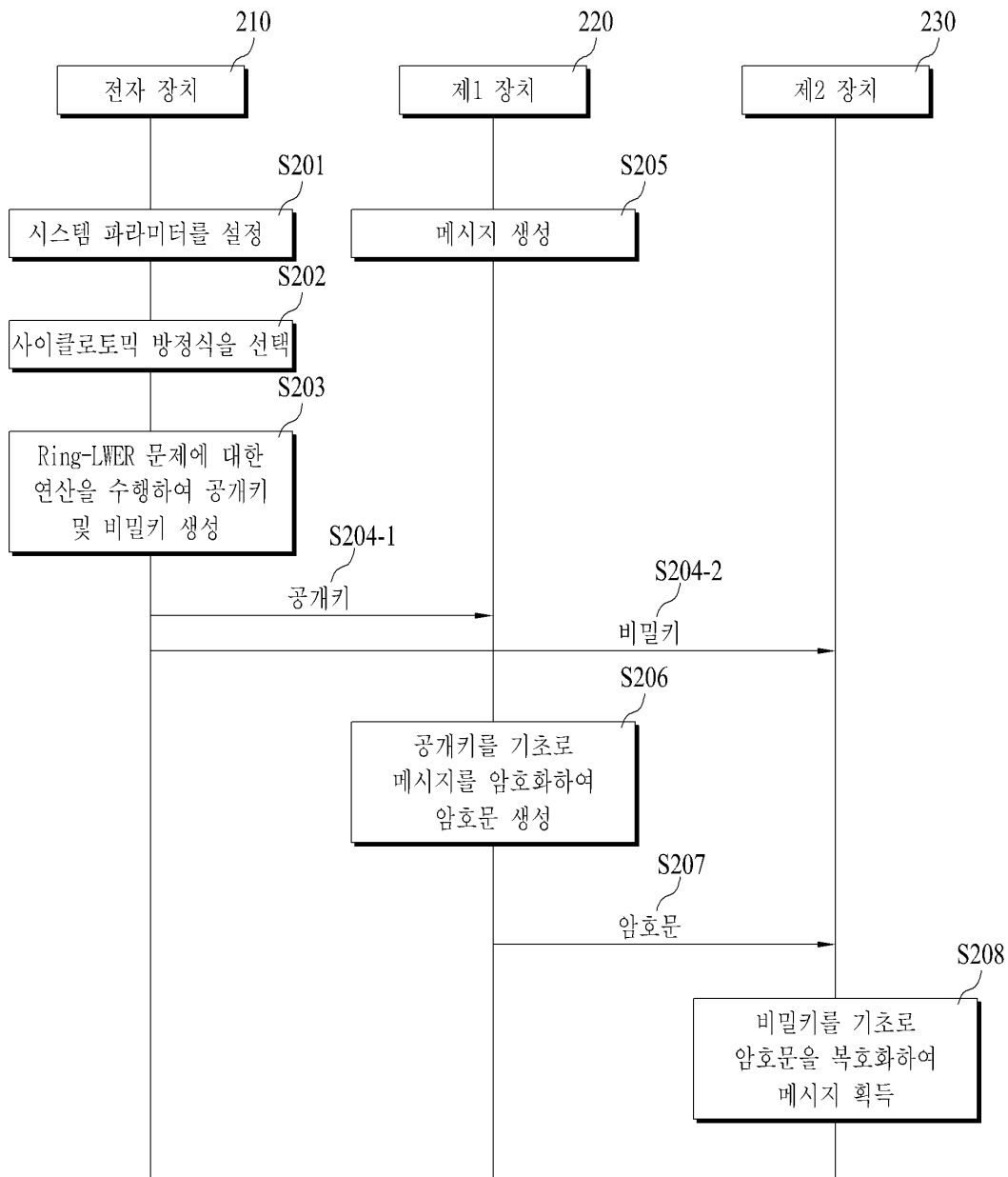
[0080] 전술한 실시예들은 일 예시일 뿐 후술하는 청구항들의 범위 내에서 다른 실시예들이 구현될 수 있다.

도면

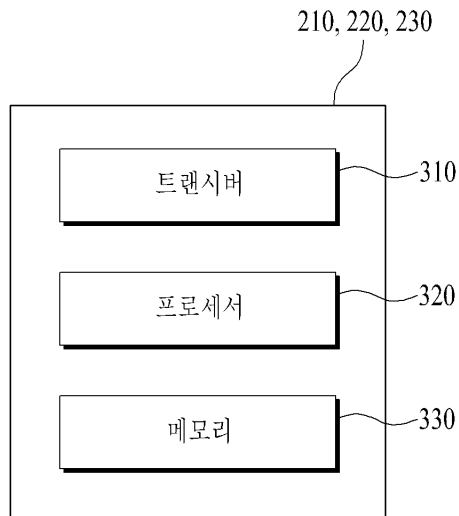
도면1



도면2



도면3



도면4

