(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2024-0158624
(43) 공개일자 2024년11월05일

(51) 국제특허분류(Int. Cl.)
H04L 9/30 (2006.01) *H04L 9/08* (2006.01)
(52) CPC특허분류
H04L 9/30 (2023.01)
H04L 9/0869 (2013.01)
(21) 출원번호 10-2023-0055537
(22) 출원일자 2023년04월27일
심사청구일자 2023년04월27일

(71) 출원인
인하대학교 산학협력단
인천광역시 미추홀구 인하로 100(용현동, 인하대학교)
(72) 발명자
이한호
인천광역시 연수구 컨벤시아대로252번길 30, 1505동 1701호(송도동, 송도 더샵 퍼스트파크 F15BL)
엄용준
경기도 평택시 청북읍 안청로1길 12, 102동 1303호 (부영사랑으로)
(74) 대리인
양성보

전체 청구항 수 : 총 8 항

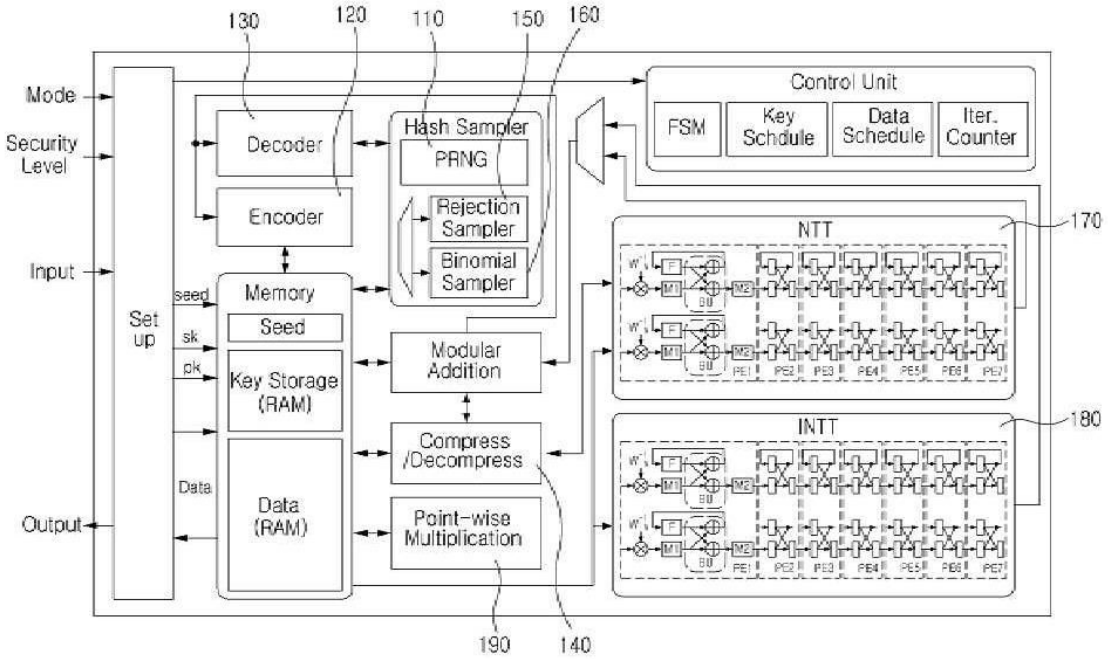
(54) 발명의 명칭 **양자내성암호를 위한 재구성 가능한 모듈-LWE 기반 암복호화 방법 및 시스템**

(57) 요 약

양자내성암호를 위한 재구성 가능한 모듈-LWE 기반 암복호화 방법 및 시스템이 제시된다. 본 발명에서 제안하는 양자내성암호를 위한 재구성 가능한 모듈-LWE 기반 암복호화 방법은 PRNG 모듈을 통해 순열 함수를 이용하여 임의의 입력 또는 키 디코더에서 입력 받은 공용 시드를 이용하여 의사 난수를 생성하고, 기각 샘플러 및 이항 샘

(뒷면에 계속)

대 표 도



플러를 통해 전치 행렬 및 에러를 생성하며, NTT 연산 및 포인트-와이즈 곱셈을 수행하여 공개키 및 비밀키를 출력하는 단계, 인코더 및 디코더를 통해 상기 공개키 및 비밀키와 메시지에 대한 인코딩 및 디코딩을 수행하고, PRNG 모듈, 기각 샘플러 및 이항 샘플러를 통해 변환된 전치 행렬 및 에러를 생성하며, NTT 연산, 포인트-와이즈 곱셈 및 INTT 연산을 수행한 후, 컴프레스를 통해 암호문을 출력하는 단계 및 디컴프레스를 통해 상기 암호문과 비밀키를 수신하여 디컴프레스를 수행한 후, 디컴프레스된 암호문에 대한 NTT 연산을 수행하고, 비밀키와 포인트-와이즈 곱셈을 수행하며, INTT 연산을 수행하고 디컴프레스된 암호문과 뺄셈을 수행한 후 인코더를 통해 메시지를 복원하는 단계를 포함한다.

이 발명을 지원한 국가연구개발사업

과제고유번호	1711193592
과제번호	IITP-2021-0-02052
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	대학ICT연구센터육성지원사업
연구과제명	스마트 모빌리티를 위한 인공지능 시스템반도체 핵심 기술 개발 및 인력 양성
기 여 율	1/3
과제수행기관명	인하대학교 산학협력단
연구기간	2021.07.01 ~ 2028.12.31

이 발명을 지원한 국가연구개발사업

과제고유번호	1711129091
과제번호	2021R1A2C1011232
부처명	과학기술정보통신부
과제관리(전문)기관명	한국연구재단
연구사업명	기초연구사업
연구과제명	고신뢰성 고성능 격자-기반 양자내성암호 하드웨어 아키텍처 연구
기 여 율	1/3
과제수행기관명	인하대학교 산학협력단
연구기간	2021.03.01 ~ 2025.02.28

이 발명을 지원한 국가연구개발사업

과제고유번호	1711134703
과제번호	20210007790012003
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	방송통신산업기술개발사업
연구과제명	HW지원 프라이버시 보장 암호데이터 고속처리 기술 개발
기 여 율	1/3
과제수행기관명	인하대학교 산학협력단
연구기간	2021.04.01 ~ 2024.12.31

명 세 서

청구범위

청구항 1

순열(permutation) 함수를 이용하여 임의의 입력 또는 키 디코더에서 입력 받은 공용 시드(Public Seed)를 이용하여 의사 난수를 생성하는 PRNG 모듈;

수신 받은 메시지를 환(Ring)의 원소에 따른 비트 단위로 마스킹하는 메시지 인코더 및 키 인코더를 포함하는 인코더(Encoder);

입력 받은 암호문을 보안 강도에 따라 압축 및 인코딩하는 컴프레스(Compress) 및 압축된 암호문을 수신하여 환의 원소에 따른 보안 강도에 따라 데이터의 압축을 해제하는 디컴프레스(Decompress);

PRNG 모듈로부터 의사 난수를 입력 받아 공개키 생성 및 암호화를 위한 다항식 행렬과 전치 행렬을 생성하는 기각 샘플러(Rejection Sampler);

PRNG 모듈로부터 의사 난수를 입력 받아 에러를 생성하는 이항 샘플러(Binomial Sampler);

이항 샘플러 및 디컴프레스의 출력을 입력 받아 NTT 연산을 수행하는 NTT 모듈;

연산 이후 덧셈기를 거쳐 RAM에 저장하고, 보안 강도에 따라 일정 횟수를 피드백 과정을 거쳐 행렬 곱셈 연산을 수행하는 포인트-와이즈(Point-wise) 곱셈기;

포인트-와이즈 곱셈기의 출력을 입력 받아 INTT 연산을 수행하는 INTT 모듈; 및

공개키 및 비밀키를 수신하여 역-직렬화를 수행하고 환의 원소로 변환하는 키 디코더 및 연산된 결과로 얻은 메시지의 마스크를 뺄셈을 통해 제거하여 원본 메시지를 최종 출력하는 메시지 디코더를 포함하는 디코더(Decoder)

를 포함하는 암복호화 시스템.

청구항 2

제1항에 있어서,

상기 PRNG 모듈은,

기각 샘플러와 이항 샘플러의 상태에 따라 동작과 동작 횟수를 제어하는

암복호화 시스템.

청구항 3

제1항에 있어서,

상기 NTT 모듈은,

DDF(Dual-path Delay Feedback) NTT 모듈이고,

복수의 스테이지로 구성되어 각 스테이지는 PE(Processing Element)를 포함하며,

상기 NTT의 PE는,

상기 PE의 입력 값과 ROM에 저장된 값을 곱셈 연산한 후, 순서대로 다다 트리 리덕션, BU 연산, 바렛 리덕션 연산을 수행하여 출력하는

암복호화 시스템.

청구항 4

제1항에 있어서,

상기 포인트-와이즈 곱셈기는,

보안 강도에 따라 행렬 크기만큼 가변적인 누산기(Accumulation) 연산을 수행하는

암복호화 시스템.

청구항 5

제1항에 있어서,

상기 컴프레스 및 디컴프레스는,

상기 컴프레스를 통해 암호화 과정 내의 연산 결과를 보안 강도에 따라 쉬프트, 덧셈, 나눗셈의 연산을 수행하고 8비트 단위로 직렬화를 통해 암호문의 크기를 압축하고 인코딩하며,

상기 디컴프레스는,

복호화 과정 내의 연산 결과를 보안 강도에 따라 곱셈, 덧셈, 쉬프트 연산을 수행하고 환의 원소로 바꾸어 프로세서 내에서 연산 가능하도록 데이터를 압축 해제하고 디코딩하는

암복호화 시스템.

청구항 6

PRNG 모듈을 통해 순열(permutation) 함수를 이용하여 임의의 입력 또는 키 디코더에서 입력 받은 공용 시드(Public Seed)를 이용하여 의사 난수를 생성하고, 기각 샘플러 및 이항 샘플러를 통해 전치 행렬 및 에러를 생성하며, NTT 연산 및 포인트-와이즈 곱셈을 수행하여 공개키 및 비밀키를 출력하는 단계;

인코더 및 디코더를 통해 상기 공개키 및 비밀키와 메시지에 대한 인코딩 및 디코딩을 수행하고, PRNG 모듈, 기각 샘플러 및 이항 샘플러를 통해 변환된 전치 행렬 및 에러를 생성하며, NTT 연산, 포인트-와이즈 곱셈 및 INTT 연산을 수행한 후, 컴프레스를 통해 암호문을 출력하는 단계; 및

디컴프레스를 통해 상기 암호문과 비밀키를 수신하여 디컴프레스를 수행한 후, 디컴프레스된 암호문에 대한 NTT 연산을 수행하고, 비밀키와 포인트-와이즈 곱셈을 수행하며, INTT 연산을 수행하고 디컴프레스된 암호문과 뺄셈을 수행한 후 인코더를 통해 메시지를 복원하는 단계

를 포함하는 암복호화 방법.

청구항 7

제6항에 있어서,

상기 암복호화 방법은,

데이터의 행렬의 크기를 조절하기 위한 파라미터(k) 값에 따라 보안 강도 1 단계, 3 단계, 5 단계를 가변적으로 선택하여 사용하는 단계;

유한 상태 기계(Finite State Machine; FSM)을 사용하여 암-복호화 방법의 실행을 변경 또는 재구성하는 단계; 및

변경 또는 재구성된 암-복호화 방법을 사용하여 키 생성(Key Generation), 암호화(Encryption), 복호화(Decryption) 동작을 보안 강도에 따라 가변적으로 데이터를 처리하는 단계

를 포함하는 암복호화 방법.

청구항 8

제7항에 있어서,

상기 암복호화 방법은,

사용되는 데이터의 행렬의 크기를 조절하는 파라미터 값이 높아질수록 상기 보안 강도가 높아지고 데이터 처리량이 증가하므로 상기 보안 강도에 따라 가변적으로 데이터를 처리하는

암복호화 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 양자내성암호를 위한 재구성 가능한 모듈-LWE 기반 암-복호화 방법 및 시스템에 관한 것이다.

배 경 기 술

[0002] RSA(Rivest, Sharmir, and Adleman), ECC(Elliptic Curve Cryptosystem) 등과 같은 소인수분해를 이용한 수학적 난제를 기반으로 하는 기존의 공개키 암호 체계는 양자컴퓨터의 상용화가 도래되며 Shor's Algorithm과 같은 양자 알고리즘에 의하여 다항시간 안에 해독이 가능하게 되기 때문에 새로운 암호 체계가 필요하다.

[0003] 따라서, 양자 컴퓨터로부터 안전한 새로운 공개키 암호 체계인 양자내성암호(Post-Quantum Cryptography)의 필요성이 요구되고 있다. 현재 미국 국립 표준기술 연구소(National Institute of Standards and Technology, NIST)에서 개최한 양자내성암호 알고리즘 공모전에서 최종적으로 격자-기반의 Crystals-KYBER 알고리즘이 선정되어 표준안 작성을 진행 중이다.

[0004] 양자내성암호는 기존 공개키 암호에서 사용한 소인수분해가 아닌 새로운 수학적 난제를 기반으로 설계된 암호로서, 격자-기반, 코드-기반, 다변수-기반, 해시-기반, 아이소제니-기반 등 난제를 기반으로 구분된다. 그 중 격자-기반을 사용하는 양자내성암호는 수백 차원 이상의 격자에서의 수학적 문제를 기반으로 하기 때문에 타 문제 기반보다 효율적인 연산, 안정성에 강점을 지니고 있다.

[0005] 격자-기반 암호 알고리즘 Crystals-KYBER는 3단계의 보안 강도를 가지며 LWE(Learning With Error) 난제를 이용한다. LWE 난제는 암호 키의 크기가 커지고 연산 속도가 느리다는 단점이 있기에 링(Ring)-LWE을 일반화한 모듈(Module)-LWE와 같은 알고리즘을 사용하여 유한 환(Finite Ring)상에서 연산을 수행하거나, 연산 중 가장 많은 시간 자원을 사용하는 다항식 행렬 곱셈에 NTT(Number Theoretic Transform)를 사용하는 등의 최적화를 통하여 구현되고 있다.

[0006] 그러나 상기와 같은 최적화가 이루어지더라도 높은 보안 강도를 가진 양자내성암호는 많은 양의 리소스를 사용하기 때문에 구현이 어렵고, 데이터 암/복호화 시 많은 양의 시간이 소요되기 때문에 상용화되기 어렵다는 단점이 있다.

선행기술문헌

특허문헌

[0007] (특허문헌 0001) 한국등록특허 제10-2462395호(2022.10.28.)

발명의 내용

해결하려는 과제

[0008] 본 발명이 이루고자 하는 기술적 과제는 낮은 복잡도를 가지고 재구성(Reconfigurable) 가능하게 동작하는 모듈-LWE 기반 암복호화 프로세서에 대한 방법을 제공하여 3가지 보안 강도(1, 3, 5 단계)를 제공하는 양자내성암호를 위한 재구성 가능한 모듈-LWE 기반 암호화-복호화 방법 및 시스템을 제공하는데 있다. 또한, 본 발명은 DDF(Dual-path Delay Feedback) NTT 모듈 구성 및 다다 트리 리덕션(Dadda Tree Reduction), 바렛 리덕션(Barrett Reduction) 등 고속 연산 방법을 적용시켜 3가지 보안 강도를 지원하는 키 생성(Key generation), 암호화(Encryption), 복호화(Decryption) 동작을 고속으로 처리하고자 한다.

과제의 해결 수단

[0009] 일 측면에 있어서, 본 발명에서 제안하는 양자내성암호를 위한 재구성 가능한 모듈-LWE 기반 암복호화 시스템은 순열(permutation) 함수를 이용하여 임의의 입력 또는 키 디코더에서 입력 받은 공용 시드(Public Seed)를 이용하여 의사 난수를 생성하는 PRNG 모듈, 수신 받은 메시지를 환(Ring)의 원소에 따른 비트 단위로 마스킹하는 메

시지 인코더 및 키 인코더를 포함하는 인코더(Encoder), 입력 받은 암호문을 보안 강도에 따라 압축 및 인코딩하는 컴프레스(Compress) 및 압축된 암호문을 수신하여 환의 원소에 따른 보안 강도에 따라 데이터의 압축을 해제하는 디컴프레스(Decompress), PRNG 모듈로부터 의사 난수를 입력 받아 공개키 생성 및 암호화를 위한 다항식 행렬과 전치 행렬을 생성하는 기각 샘플러(Rejection Sampler), PRNG 모듈로부터 의사 난수를 입력 받아 에러를 생성하는 이항 샘플러(Binomial Sampler), 이항 샘플러 및 디컴프레스의 출력을 입력 받아 NTT 연산을 수행하는 NTT 모듈, 연산 이후 덧셈기를 거쳐 RAM에 저장하고, 보안 강도에 따라 일정 횟수를 피드백 과정을 거쳐 행렬 곱셈 연산을 수행하는 포인트-와이즈(Point-wise) 곱셈기 및 덧셈기, 포인트-와이즈 곱셈기의 출력을 입력 받아 INTT(Inverse NTT) 연산을 수행하는 INTT 모듈 및 공개키 및 비밀키를 수신하여 역-직렬화를 수행하고 환의 원소로 변환하는 키 디코더 및 연산된 결과로 얻은 메시지의 마스크를 뺄셈을 통해 제거하여 원본 메시지를 최종 출력하는 메시지 디코더를 포함하는 디코더(Decoder)를 포함한다.

[0010] 상기 PRNG 모듈은 기각 샘플러와 이항 샘플러의 상태에 따라 동작과 동작 횟수를 제어한다.

[0011] 상기 NTT 모듈은 DDF(Dual-path Delay Feedback) NTT 모듈이고, 복수의 스테이지로 구성되어 각 스테이지는 PE(Processing Element)를 포함하며, 상기 NTT의 PE는, 상기 PE의 입력 값과 ROM에 저장된 값을 곱셈 연산한 후, 순서대로 다다 트리 리덕션, BU 연산, 바렛 리덕션 연산을 수행하여 출력한다.

[0012] 상기 포인트-와이즈 곱셈기는 보안 강도에 따라 행렬 크기만큼 가변적인 누산기(Accumulation) 연산을 수행한다.

[0013] 상기 컴프레스 및 디컴프레스는 상기 컴프레스를 통해 암호화 과정 내의 연산 결과를 보안 강도에 따라 쉬프트, 덧셈, 나눗셈의 연산을 수행하고 비트 단위로 직렬화를 통해 암호문의 크기를 압축하고 인코딩하며, 상기 디컴프레스는, 복호화 과정 내의 연산 결과를 보안 강도에 따라 곱셈, 덧셈, 쉬프트 연산을 수행하고 환의 원소로 바꾸어 프로세서 내에서 연산 가능하도록 데이터를 압축 해제하고 디코딩한다.

[0014] 또 다른 일 측면에 있어서, 본 발명에서 제안하는 양자내성암호를 위한 재구성 가능한 모듈-LWE 기반 암복호화 방법은 PRNG 모듈을 통해 순열(Permutation) 함수를 이용하여 임의의 입력 또는 키 디코더에서 입력 받은 공용 시드(Public Seed)를 이용하여 의사 난수를 생성하고, 기각 샘플러 및 이항 샘플러를 통해 전치 행렬 및 에러를 생성하며, NTT 연산 및 포인트-와이즈 곱셈을 수행하여 공개키 및 비밀키를 출력하는 단계, 인코더 및 디코더를 통해 상기 공개키 및 비밀키와 메시지에 대한 인코딩 및 디코딩을 수행하고, PRNG 모듈, 기각 샘플러 및 이항 샘플러를 통해 변환된 전치 행렬 및 에러를 생성하며, NTT 연산, 포인트-와이즈 곱셈 및 INTT 연산을 수행한 후, 컴프레스를 통해 암호문을 출력하는 단계 및 디컴프레스를 통해 상기 암호문과 비밀키를 수신하여 디컴프레스를 수행한 후, 디컴프레스된 암호문에 대한 NTT 연산을 수행하고, 비밀키와 포인트-와이즈 곱셈을 수행하며, INTT 연산을 수행하고 디컴프레스된 암호문과 뺄셈을 수행한 후 인코더를 통해 메시지를 복원하는 단계를 포함한다.

발명의 효과

[0015] 본 발명의 실시예들에 따르면 Crystals-KYBER 양자내성암호 아키텍처에 동작에 따른 내부 재구성형 모듈-LWE 프로세서 구조를 사용함으로써, 확장성이 용이하므로 적은 리소스를 사용하여 가변적인 데이터를 처리해주는 동작 방식(예를 들어, 키 생성, 암/복호화)과 3가지의 보안강도(1, 3, 5 단계)와 같은 다양한 기능을 사용할 수 있다. 또한, DDF(Dual-path Delay Feedback) NTT를 사용하고 다다 트리 리덕션과 바렛 리덕션을 사용하여 높은 데이터 처리율을 얻을 수 있어 연산 속도에 이점을 가진다.

도면의 간단한 설명

[0016] 도 1은 본 발명의 일 실시예에 따른 재구성형 모듈-LWE 기반 암복호화 처리 장치의 전체 구성을 설명하기 위한 도면이다.

도 2는 본 발명의 일 실시예에 따른 재구성형 모듈-LWE 기반 암복호화 장치의 키 생성 과정의 데이터 흐름을 설명하기 위한 도면이다.

도 3는 본 발명의 일 실시예에 따른 재구성형 모듈-LWE 기반 암복호화 장치의 암호화 과정의 데이터 흐름을 설명하기 위한 도면이다.

도 4는 본 발명의 일 실시예에 따른 재구성형 모듈-LWE 기반 암복호화 장치의 복호화 과정의 데이터 흐름을 설명하기 위한 도면이다.

도 5은 본 발명의 일 실시예에 따른 DDF(Dual-path Delay Feedback) NTT 모듈의 구조를 나타내는 도면이다.

도 6은 본 발명의 일 실시예에 따른 DDF(Dual-path Delay Feedback) INTT 모듈의 구조를 나타내는 도면이다.

도 7은 본 발명의 일 실시예에 따른 다다 트리 리덕션(Dadda Tree Reduction) 연산을 수행하는 MR1(Modulo Reduction 1)의 구조를 나타내는 도면이다.

도 8은 본 발명의 일 실시예에 따른 바렛 리덕션(Barrett Reduction) 연산을 수행하는 MR2(Modulo Reduction 2)의 구조를 나타내는 도면이다.

도 9는 본 발명의 일 실시예에 따른 재구성형 모듈-LWE 기반 암복호화 시스템의 동작 방법을 설명하기 위한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0017] 이하, 본 발명의 실시 예를 첨부된 도면을 참조하여 상세하게 설명한다.

[0019] 도 1은 본 발명의 일 실시예에 따른 재구성형 모듈-LWE 기반 암복호화 처리 장치의 전체 구성을 설명하기 위한 도면이다.

[0020] 모듈-LWE는 환(Ring) 안에서 n차 다항식을 파라미터 k에 따라 k*k의 다항식 행렬 계산을 수행한다. 본 발명의 실시예에 따른 모듈-LWE의 특성에 따라 파라미터 n=256과 q=3329를 사용하며 보안 강도(Security level) 1, 3, 5단계에 해당되는 파라미터 k=2, 3, 4를 기반으로 설계되었다.

[0021] 모듈-LWE 문제는 링-LWE 문제에 기반한다. 다항식 환(Ring)은 $R_q = Z_q/\langle x^n + 1\rangle$ 안에서 정의되며, 다항식 a(x)와 b(x)는 식1과 같이 나타낼 수 있다:

[0022] $$a(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} \quad \text{(식1-1)}$$

[0023] $$b(x) = b_0 + b_1x + b_2x^2 + \ldots + b_{n-1}x^{n-1} \quad \text{(식1-2)}$$

[0024] 각 다항식 곱셈의 빠른 연산을 위해 NTT 연산을 수행한다. $\tilde{a} = NTT(a)$는 식2와 같이 나타낼 수 있다:

[0025] $$\tilde{a}[i] = \sum_{i=0}^{n-1} a[j]\omega^{ij} mod\ q\ ,\ for\ i = 0.,\ 1,\ \ldots,\ n-1 \quad \text{(식2)}$$

[0026] 다항식 a(x)의 계수는 벡터(Vector) $a = a_0, \ldots, a_{n-1}$이다. N의 값은 다항식의 계수로 1의 n제곱근(Root of Unity)이다. q는 $q \equiv 1 \bmod n$을 만족하는 소수(Prime number)인 q=3329를 사용하며 식 1에서 n 과 w는 $n * n^{-1} \equiv 1\ mod\ q$, $w * w^{-1} \equiv 1 \bmod q$의 조건을 만족하는 숫자로 구성된다.

[0027] 다항식에 대한 INTT 연산은 $b = INTT(\tilde{a})$라고 정의하여 식3과 같이 나타낸다:

[0028] $$b[i] = n^{-1}\sum_{j=0}^{n-1} \tilde{a}[j]\omega^{-ij} mod\ q\ ,\ for\ i = 0.,\ 1,\ \ldots,\ n-1 \quad \text{(식3)}$$

[0029] 모듈-LWE는 링-LWE를 일반화하여 파라미터 k에 따라 다항식 행렬을 생성한다. 다항식 행렬 $\hat{A} = R_q^{k\times k}$로 쓸 수 있으며 동일한 파라미터 n과 q를 갖는 Ring들의 집합이기 때문에 생성한 다항식의 개수를 조절함으로써 보안 강도를 조정할 수 있다.

[0030] 도 1을 참조하면, 본 발명의 일 실시예에 따른 재구성형 모듈-LWE 기반 암복호화 시스템의 구성을 나타내는 도면이다.

[0031] 제안하는 재구성형 모듈-LWE 기반 암복호화 시스템은 내부 구조 모듈을 사용하여 키 생성 과정, 암호화 과정, 복호화 과정을 수행하며, 이는 보안 강도에 따른 데이터 처리 변환이 가능하다.

[0032] 본 발명의 실시예에 따른 재구성형 모듈-LWE 기반 암복호화 시스템은 PRNG 모듈(110), 메시지 인코더 및 키 인

코더를 포함하는 인코더(Encoder)(120), 키 디코더 및 메시지 디코더를 포함하는 디코더(Decoder)(130), 컴프레스(Compress) 및 디컴프레스(Decompress)(140), 기각 샘플러(Rejection Sampler)(150), 이항 샘플러(Binomial Sampler)(160), NTT 모듈(170), INTT 모듈(180), 포인트-와이즈(Point-wise) 곱셈기(190) 및 덧셈기를 포함한다.

[0033] 본 발명의 실시예에 따른 PRNG 모듈(110)은 Keccak 알고리즘의 f-순열(permutation) 함수를 이용하여 구현하였으며 임의의 입력 또는 키 디코더(130)에서 입력 받은 공용 시드(Public Seed)를 이용하여 의사 난수를 생성한다. 본 발명의 실시예에 따른 메시지 인코더(120)는 수신 받은 메시지를 환(Ring)의 원소에 적합하게 1비트 단위로 마스킹(Masking) 해준다.

[0034] 본 발명의 실시예에 따른 컴프레스(140)는 입력 받은 암호문을 보안 강도에 따라 압축 및 인코딩하여 전송하기 용이한 형태로 출력한다.

[0035] 본 발명의 실시예에 따른 디컴프레스(140)는 압축된 암호문을 수신하여 Ring의 원소에 적합하도록 보안 강도에 따라 데이터의 압축을 해제한다.

[0036] 본 발명의 실시예에 따른 기각 샘플러(150)는 PRNG 모듈로부터 의사 난수를 입력 받아 공개키 생성 및 암호화를 위한 다항식 행렬과 전치 행렬 생성에 사용된다.

[0037] 본 발명의 실시예에 따른 이항 샘플러(160)는 PRNG 모듈로부터 의사 난수를 입력 받아 에러 생성에 사용된다.

[0038] 본 발명의 실시예에 따른 NTT 모듈(170)은 이항 샘플러(160) 및 디컴프레스(140)의 출력을 입력 받아 NTT 연산을 수행한다.

[0039] 본 발명의 실시예에 따른 다다 트리 리덕션은 곱셈 연산 이후 값을 환의 원소에 적합하게 리덕션 연산을 수행해준다.

[0040] 본 발명의 실시예에 따른 바렛 리덕션은 덧셈 연산 이후 값을 환의 원소에 적합하게 리덕션 연산을 수행해준다.

[0041] 본 발명의 실시예에 따른 포인트-와이즈 곱셈기(190)는 Bow-tie 연산 이후 덧셈기를 거쳐 RAM에 저장하고, 보안 강도에 따라 일정 횟수를 피드백 과정을 거쳐 행렬 곱셈 연산을 수행한다.

[0042] 본 발명의 실시예에 따른 INTT 모듈(180)은 포인트-와이즈 곱셈기(190)의 출력을 입력 받아 INTT 연산을 수행한다.

[0043] 본 발명의 실시예에 따른 메시지 디코더(130)는 연산된 결과로 얻은 메시지의 마스크를 뺄셈을 통해 제거하여 원본 메시지를 최종 출력한다.

[0044] 본 발명의 실시예에 따른 키 디코더(130)는 공개키 및 비밀키를 수신하여 역-직렬화를 수행하고 환의 원소로 변환한다.

[0046] 도 2는 본 발명의 일 실시예에 따른 재구성형 모듈-LWE 기반 암복호화 장치의 키 생성 과정의 데이터 흐름을 설명하기 위한 도면이다.

[0047] 본 발명의 일 실시예에 따른 재구성형 모듈-LWE 기반 암복호화 장치의 키 생성 과정은 Keccak 알고리즘의 f-순열(permutation) 함수를 이용한 PRNG 모듈에서 의사 난수를 생성하고 이를 이용하여 샘플러에서 다항식 행렬과 에러를 생성하고 NTT 연산을 수행한 뒤 곱셈 연산과 덧셈 연산을 통해 공개키와 비밀키를 생성한다.

[0049] 도 3는 본 발명의 일 실시예에 따른 재구성형 모듈-LWE 기반 암복호화 장치의 암호화 과정의 데이터 흐름을 설명하기 위한 도면이다.

[0050] 재구성형 모듈-LWE 기반 암복호화 장치의 암호화 과정은 사용자가 암호화하고자 하는 메시지와 공개키를 수신하여 상기 메시지를 링의 원소로 만들기 위해 인코딩하여 1비트 단위로 마스킹한다. 이후, 상기 공개키를 디코더를 통해 공개 시드(Public seed)와 공개 키로 분리하여 출력한 값을 키 생성 과정과 동일하게 기각 샘플러와 이항 샘플러를 통해 암호화에 필요한 다항식 행렬과 에러 벡터를 생성한다. 생성된 에러 벡터를 NTT 모듈 및 INTT 모듈을 통해 NTT 도메인에서 포인트-와이즈 곱셈기와 덧셈기를 이용하여 연산을 수행하고, 연산 결과는 컴프레스(Compress)를 이용하여 암호문을 압축 및 인코딩하여 출력한다.

[0052] 도 4는 본 발명의 일 실시예에 따른 재구성형 모듈-LWE 기반 암복호화 장치의 복호화 과정의 데이터 흐름을 설명하기 위한 도면이다.

[0053] 본 발명의 일 실시예에 따른 재구성형 모듈-LWE 기반 암복호화 장치의 복호화 과정은 암호문을 수신하여 디컴프레스(Decompress)를 통해 암호문의 압축 해제 및 디코딩을 수행하고, 상기 키 생성 프로세서로부터 비밀키를 수신하여 디코딩을 수행한다. NTT 모듈 및 INTT 모듈을 통해 NTT 도메인에서 포인트-와이즈 곱셈기와 뺄셈기를 이용하여 연산을 수행하고, 연산 결과는 메시지 디코더(Decoder)를 이용하여 원본 메시지를 출력한다.

[0055] 도 5은 본 발명의 일 실시예에 따른 DDF(Dual-path Delay Feedback) NTT 모듈의 구조를 나타내는 도면이다.

[0056] 본 발명의 일 실시예에 따른 DDF(Dual-path Delay Feedback) NTT 모듈은 2-병렬 구조로 연산을 수행하며, NTT 모듈은 총 7개의 스테이지(Stage)로 구성되어 있으며, 각 스테이지는 PE(Processing Element)로 구성되어 있다. PE는 곱셈기, 다다 트리 리덕션, 바렛 리덕션과 BU(Butterfly Unit)으로 이루어져 있으며, PE의 입력 값과 ROM에 저장된 ω^i 값과 곱셈 연산 후에 순서대로 다다 트리 리덕션, BU 연산, 바렛 리덕션 연산을 수행하여 출력하는 구조이다. 출력 값은 최종적으로 바렛 리덕션으로 인해 0~q사이의 값을 출력한다.

[0058] 도 6은 본 발명의 일 실시예에 따른 DDF(Dual-path Delay Feedback) INTT 모듈의 구조를 나타내는 도면이다.

[0059] 본 발명의 일 실시예에 따른 DDF(Dual-path Delay Feedback) INTT 모듈은 2-병렬 구조로 연산을 수행하며, INTT 모듈은 총 7개의 스테이지로 구성되어 있고, 각 스테이지는 PE(Processing Element)로 구성되어 있다. PE는 곱셈기, 다다 트리 리덕션, 바렛 리덕션과 BU(Butterfly Unit)으로 이루어져 있다. INTT의 PE는 NTT의 PE와는 반대되는 구조로 입력 값을 BU와 바렛 리덕션 연산한 값을 ROM에 저장된 값과 곱셈연산 후에 다다 트리 리덕션 연산을 수행하여 출력하는 구조이다.

[0061] 도 7은 본 발명의 일 실시예에 따른 다다 트리 리덕션(Dadda Tree Reduction) 연산을 수행하는 MR1(Modulo Reduction 1)의 구조를 나타내는 도면이다.

[0062] 본 발명의 일 실시예에 따른 다다 트리 리덕션 연산을 수행하는 MR1은 곱셈으로 인해 커진 값을 줄여주기 위해 사용한다. 입력에 대해 a modulo q 값인 0 ~ q-1 사이의 값을 출력한다.

[0064] 도 8은 본 발명의 일 실시예에 따른 바렛 리덕션(Barrett Reduction) 연산을 수행하는 MR2(Modulo Reduction 2)의 구조를 나타내는 도면이다.

[0065] 본 발명의 일 실시예에 따른 바렛 리덕션 연산을 수행하는 MR2는 덧셈 연산으로 커진 결과를 링(Ring) 내의 값으로 줄여 주기 위해 바렛 리덕션을 수행한다. 입력에 대해 a modulo q 값인 0 ~ q 사이의 값을 출력한다.

[0067] 도 9는 본 발명의 일 실시예에 따른 재구성형 모듈-LWE 기반 암복호화 시스템의 동작 방법을 설명하기 위한 흐름도이다.

[0068] 제안하는 재구성형 모듈-LWE 기반 암복호화 시스템의 동작 방법은 수신한 다항식 파라미터 k와 동작을 판단하는 단계(910), PRNG 모듈을 통해 순열(permutation) 함수를 이용하여 임의의 입력 또는 키 디코더에서 입력 받은 공용 시드(Public Seed)를 이용하여 의사 난수를 생성하고, 기각 샘플러 및 이항 샘플러를 통해 전치 행렬 및 에러를 생성하며, NTT 연산 및 포인트-와이즈 곱셈을 수행하여 공개키 및 비밀키를 출력하는 단계(920), 인코더 및 디코더를 통해 상기 공개키 및 비밀키와 메시지에 대한 인코딩 및 디코딩을 수행하고, PRNG 모듈, 기각 샘플러 및 이항 샘플러를 통해 전치 행렬 및 에러를 생성하며, NTT 연산, 포인트-와이즈 곱셈 및 INTT 연산을 수행한 후, 컴프레스를 통해 암호문을 출력하는 단계(930) 및 디컴프레스를 통해 상기 암호문과 비밀키를 수신하여 디컴프레스를 수항한 후, 디컴프레스된 암호문에 대한 NTT 연산을 수행하고, 비밀키와 포인트-와이즈 곱셈을 수행하며, INTT 연산을 수행하고 디컴프레스된 암호문과 뺄셈을 수행한 후 인코더를 통해 메시지를 복원하는 단계

(940)를 포함한다.

[0069] 단계(910)에서, 수신한 다항식 파라미터 k와 동작을 판단한다.

[0070] 단계(920)에서, PRNG 모듈을 통해 입력 시드(Seed)를 수신하고(921), PRNG 모듈과 기각 샘플러 및 이항 샘플러를 통해 전치 행렬 및 에러를 생성한다(922). 이후, 에러 벡터에 대한 NTT 연산 수행 및 전치 행렬과 포인트-와이즈 곱셈을 수행한다(923). 마지막으로, 에러 벡터를 더하고 인코더를 통해 공개키 및 비밀키를 출력한다(924).

[0071] 단계(930)에서, 인코더 및 디코더를 통해 상기 공개키 및 비밀키와 메시지에 대한 인코딩 및 디코딩을 수행하고(931), PRNG 모듈, 기각 샘플러 및 이항 샘플러를 통해 변환된 전치 행렬 및 에러를 생성한다(932). 이후, 에러 벡터에 대한 NTT 연산 수행 및 변환된 전치 행렬과 포인트-와이즈 곱셈 및 INTT 연산을 수행한다(933). 미지막으로, 에러 벡터를 더하고 컴프레스를 통해 암호문을 출력한다(934).

[0072] 단계(940)에서, 디컴프레스를 통해 상기 암호문과 비밀키를 수신하여 디컴프레스를 수행한 후, 디코더를 통해 디코딩을 수행한다(941). 디컴프레스된 암호문에 대한 NTT 연산을 수행하고, 비밀키와 포인트-와이즈 곱셈을 수행한다(942). 이후, INTT 연산을 수행하고 디컴프레스된 암호문과 뺄셈을 수행한 후(943), 인코더를 통해 메시지를 복원한다(944).

[0074] 이상에서 설명된 장치는 하드웨어 구성요소, 소프트웨어 구성요소, 및/또는 하드웨어 구성요소 및 소프트웨어 구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성요소는, 예를 들어, 프로세서, 콘트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPGA(field programmable gate array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 콘트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.

[0075] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상 장치(virtual equipment), 컴퓨터 저장 매체 또는 장치에 구체화(embody)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.

[0076] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다.

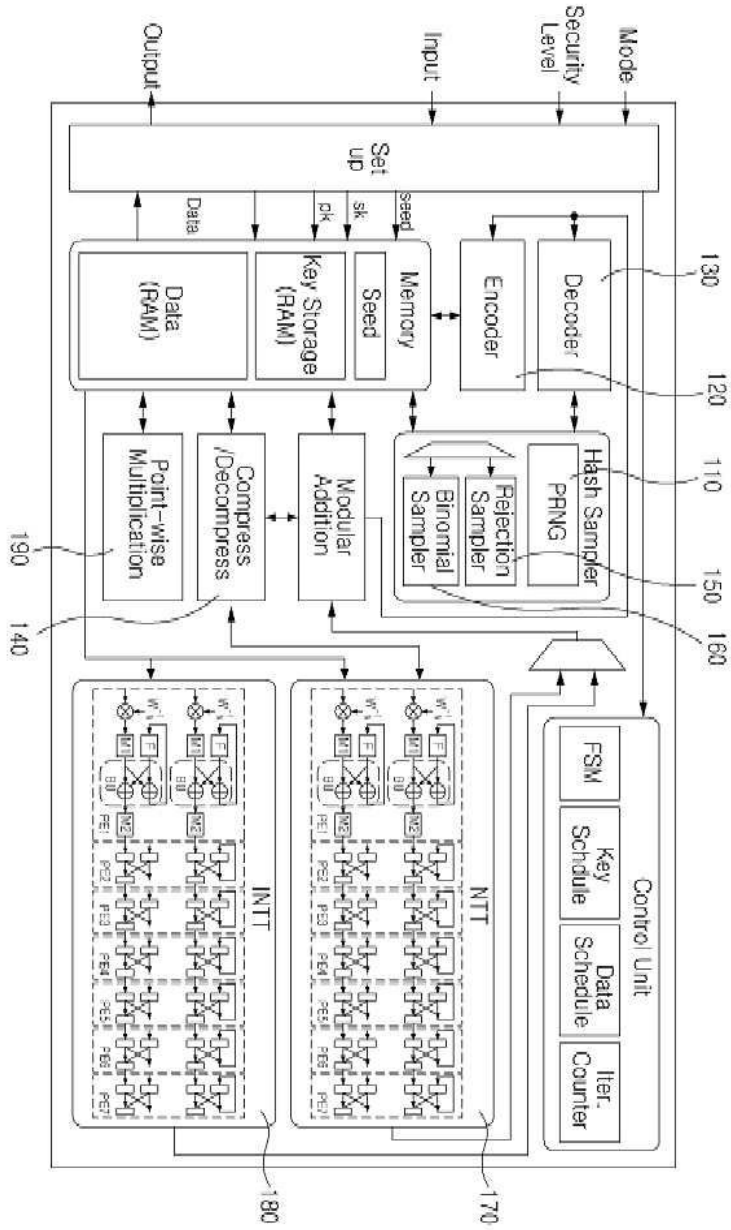
[0077] 이상과 같이 실시예들이 비록 한정된 실시예와 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형

태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.

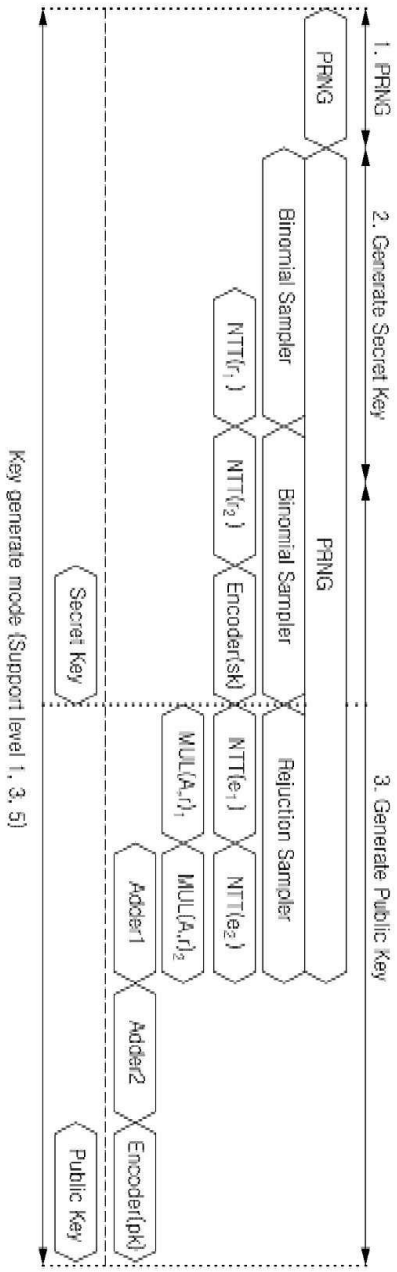
[0078] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

도면

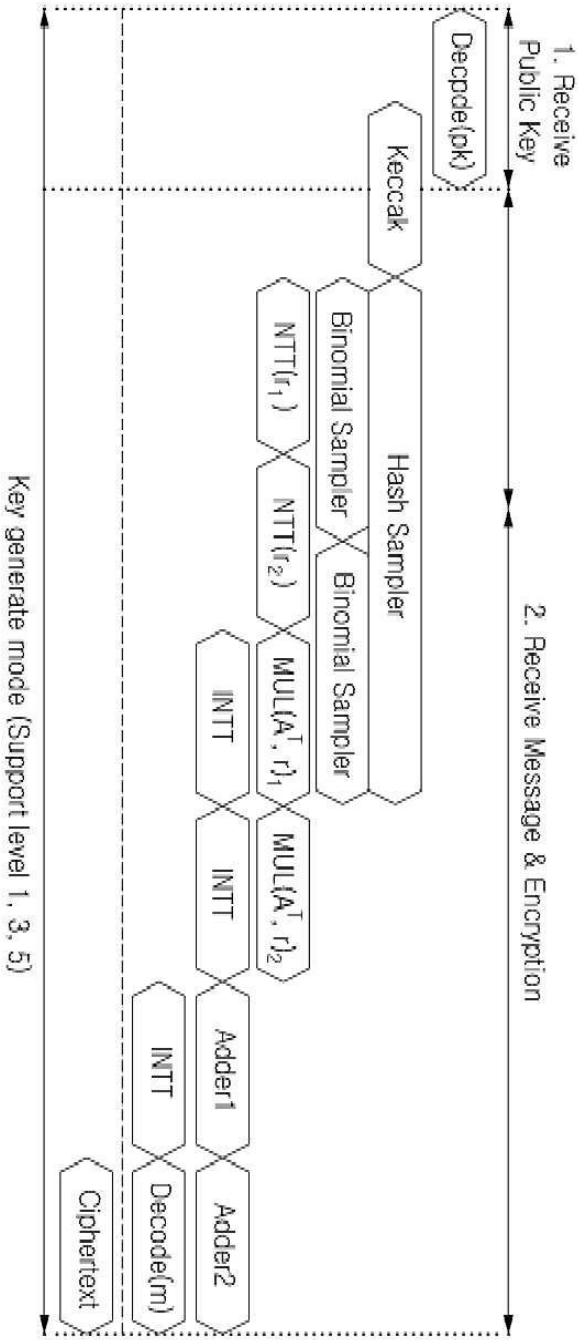
도면1



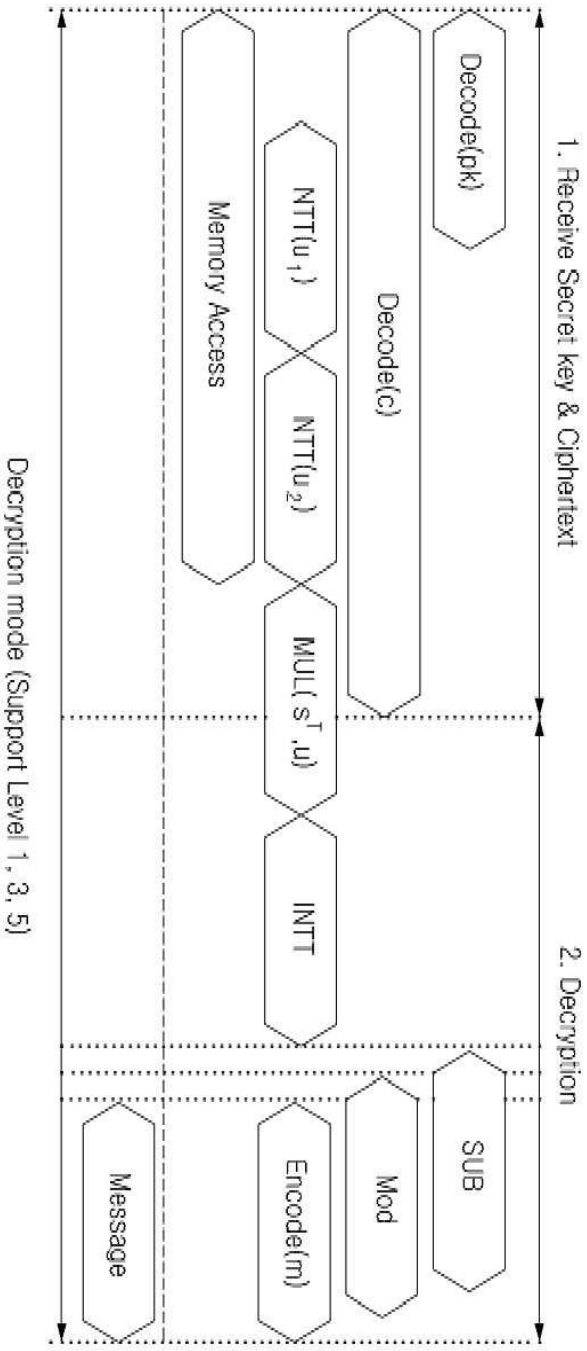
도면2


1. PRNG
2. Generate Secret Key
3. Generate Public Key
PRNG
Binomial Sampler
NTT(r_1)
NTT(r_2)
Encoder(sk)
MUL(A,r)$_1$
Adder1
Secret Key
PRNG
Binomial Sampler
Rejuction Sampler
NTT(e_1)
NTT(e_2)
MUL(A,r)$_2$
Adder2
Encoder(pk)
Public Key
Key generate mode (Support level 1, 3, 5)

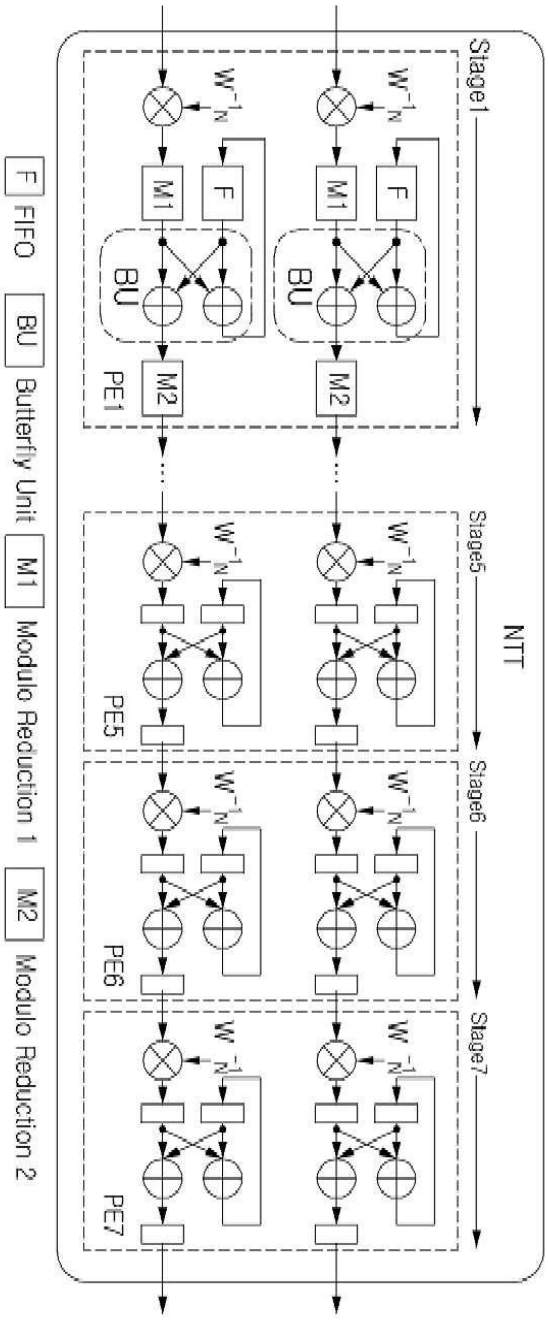
도면3


1. Receive Public Key
2. Receive Message & Encryption
Key generate mode (Support level 1, 3, 5)
Decpde(pk)
Keccak
Hash Sampler
Binomial Sampler
Binomial Sampler
NTT(r1)
NTT(r2)
MUL(AT, r)1
MUL(AT, r)2
INTT
INTT
INTT
Adder1
Adder2
Decode(m)
Ciphertext

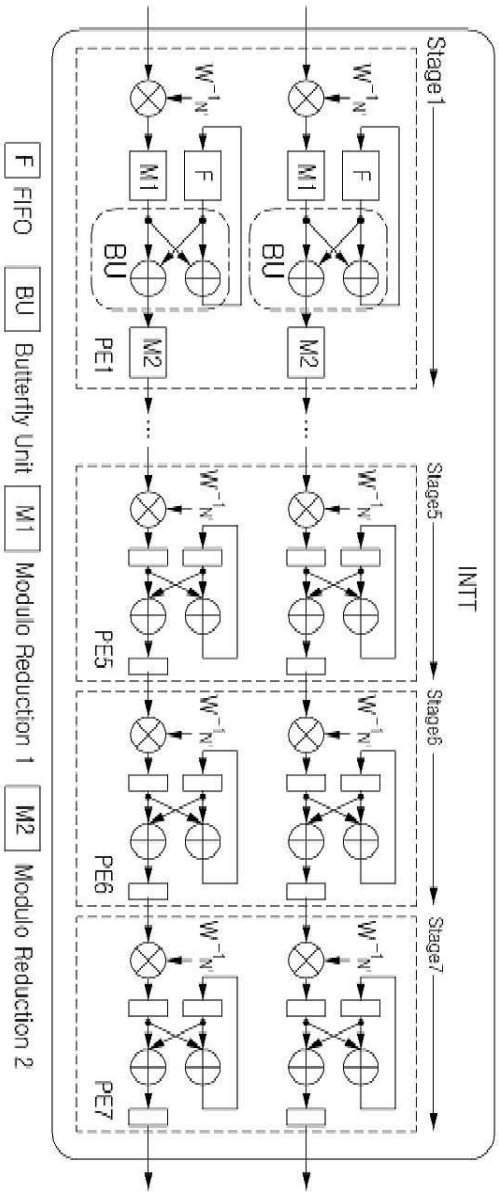
도면4


1. Receive Secret key & Ciphertext
2. Decryption
Decode(pk)
Decode(c)
NTT(u 1)
NTT(u 2)
MUL(s T ,u)
INTT
Memory Access
SUB
Mod
Encode(m)
Message
Decryption mode (Support Level 1, 3, 5)

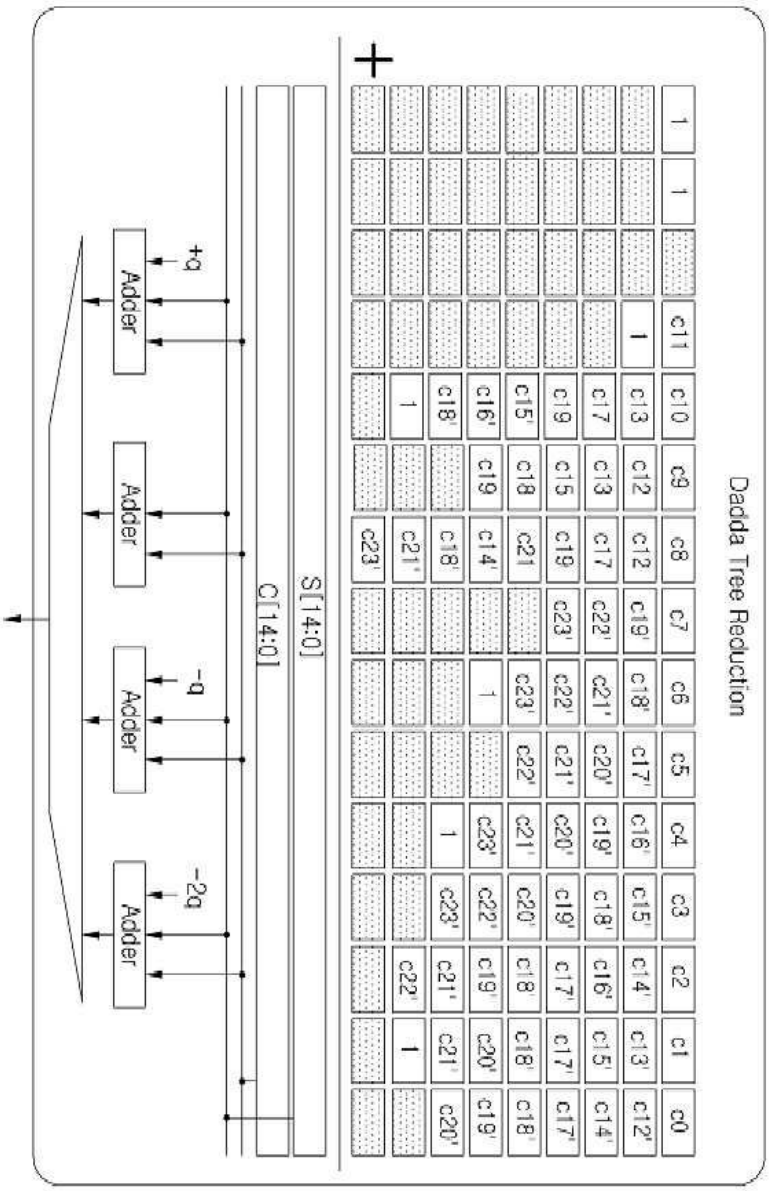
도면5


NTT
Stage1
Stage5
Stage6
Stage7
PE1
PE5
PE6
PE7
BU
F
M1
M2
F FIFO
BU Butterfly Unit
M1 Modulo Reduction 1
M2 Modulo Reduction 2

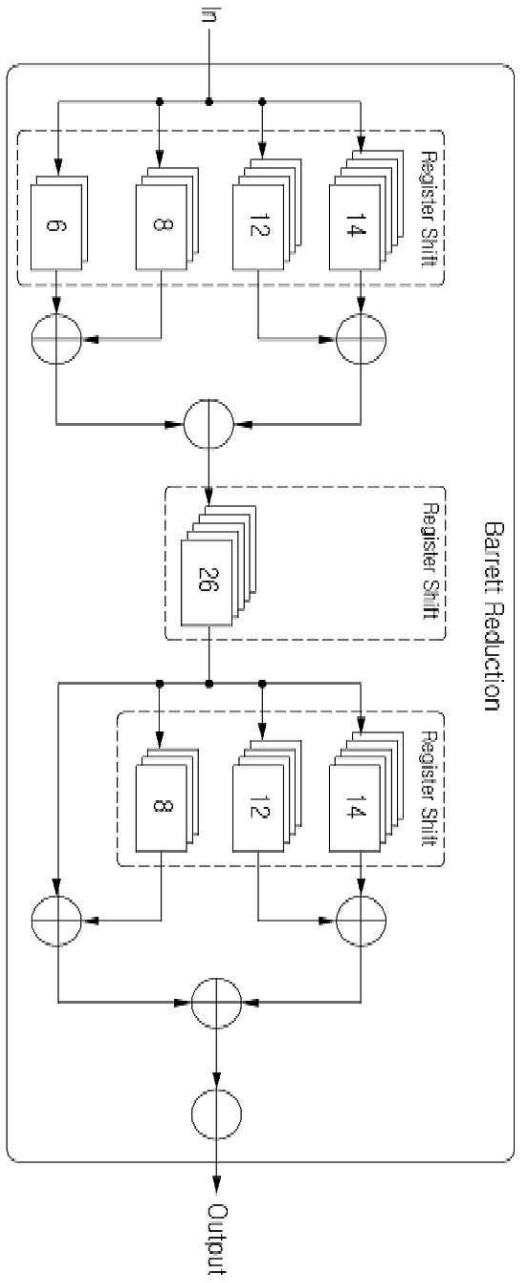
도면6


Stage1
Stage5
Stage6
Stage7
INTT
PE1
PE5
PE6
PE7
BU
M1
M2
F
FIFO
Butterfly Unit
Modulo Reduction 1
Modulo Reduction 2

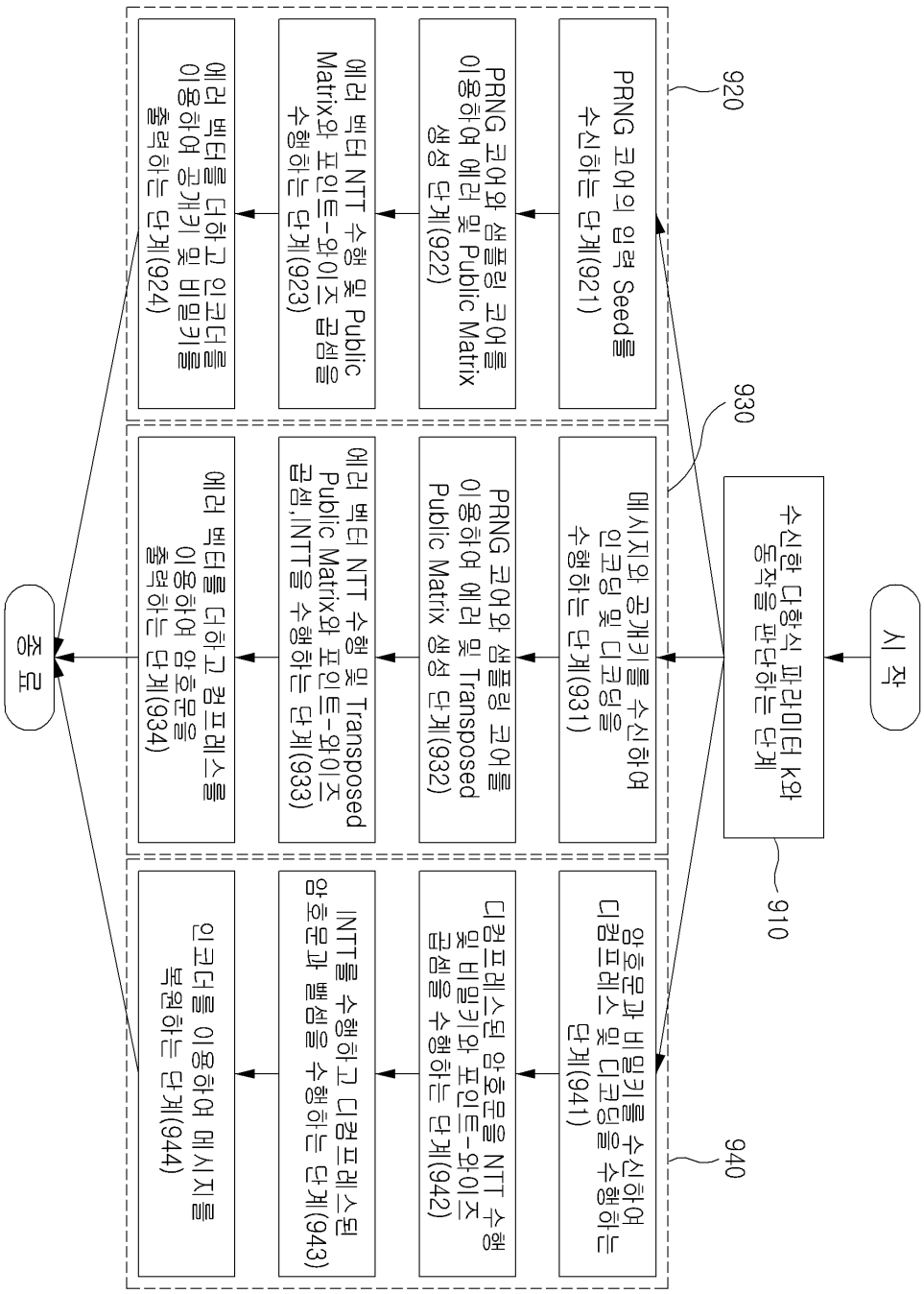
도면7


Dadda Tree Reduction
+
S[14:0]
C[14:0]
+q
-q
-2q
Adder
Adder
Adder
Adder

도면8


In
Register Shift
6
8
12
14
Register Shift
26
Barrett Reduction
Register Shift
8
12
14
Output

도면9


시 작
수신한 다항식 파라미터 k와 동작을 판단하는 단계
910
920
PRNG 코어의 입력 Seed를 수신하는 단계(921)
PRNG 코어와 샘플링 코어를 이용하여 에러 및 Public Matrix 생성 단계(922)
에러 벡터 NTT 수행 및 Public Matrix와 포인트-와이즈 곱셈을 수행하는 단계(923)
에러 벡터를 더하고 인코더를 이용하여 공개키 및 비밀키를 출력하는 단계(924)
930
메시지와 공개키를 수신하여 인코딩 및 디코딩을 수행하는 단계(931)
PRNG 코어와 샘플링 코어를 이용하여 에러 및 Transposed Public Matrix 생성 단계(932)
에러 벡터 NTT 수행 및 Transposed Public Matrix와 포인트-와이즈 곱셈,INTT을 수행하는 단계(933)
에러 벡터를 더하고 컴프레스를 이용하여 암호문을 출력하는 단계(934)
940
암호문과 비밀키를 수신하여 디컴프레스 및 디코딩을 수행하는 단계(941)
디컴프레스된 암호문을 NTT 수행 및 비밀키와 포인트-와이즈 곱셈을 수행하는 단계(942)
INTT를 수행하고 디컴프레스된 암호문과 뺄셈을 수행하는 단계(943)
인코더를 이용하여 메시지를 복원하는 단계(944)
종 료