



(19) 대한민국특허청(KR)

(12) 등록특허공보(B1)

(45) 공고일자 2023년02월09일

(11) 등록번호 10-2498123

(24) 등록일자 2023년02월06일

(51) 국제특허분류(Int. Cl.)  
 G06F 7/72 (2006.01) G06F 15/78 (2006.01)  
 G06F 15/80 (2006.01) H04L 9/00 (2022.01)

(52) CPC특허분류  
 G06F 7/722 (2013.01)  
 G06F 15/7896 (2013.01)

(21) 출원번호 10-2022-0087617

(22) 출원일자 2022년07월15일

심사청구일자 2022년07월15일

(56) 선행기술조사문헌

KR1020220078155 A\*

KR101952547 B1\*

KR1020220049212 A\*

KR1020210146513 A\*

\*는 심사관에 의하여 인용된 문헌

(73) 특허권자

인하대학교 산학협력단

인천광역시 미추홀구 인하로 100(용현동, 인하대학교)

(72) 발명자

이한호

인천광역시 연수구 컨벤시아대로252번길 30, 1505동 1701호(송도동, 송도 더샵 퍼스트파크 F15BL)

조민재

인천광역시 미추홀구 한나루로403번길 125, 1동 201호(학익동, 남경빌라)

(74) 대리인

양성보

전체 청구항 수 : 총 7 항

심사관 : 지정훈

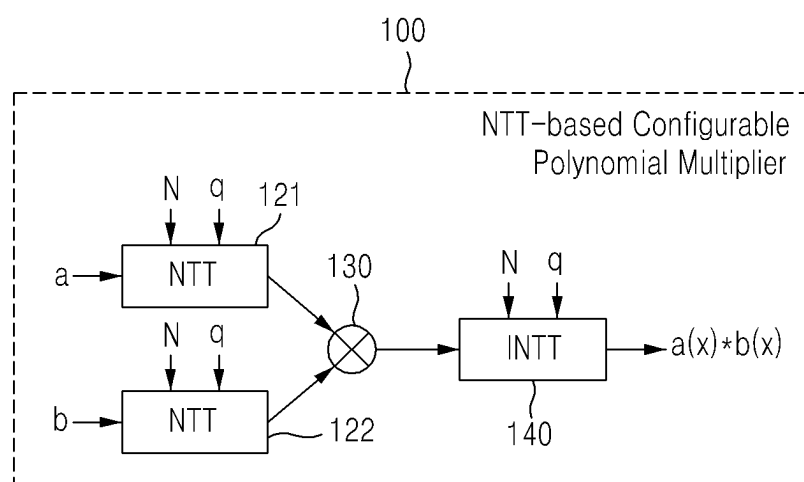
(54) 발명의 명칭 동형암호를 위한 가변적으로 동작하는 NTT 기반 다항식 곱셈기 장치 및 방법

## (57) 요약

동형암호를 위한 가변적으로 동작하는 NTT 기반 다항식 곱셈기 장치 및 그 동작 방법이 제시된다.

일 측면에 있어서, 본 발명에서 제안하는 동형암호를 위한 가변적으로 동작하는 NTT 기반 다항식 곱셈기는 복수의 길이(N)와 모듈러스(q)를 갖는 가변적인 파라미터의 다항식을 수신하여 NTT 형태의 다항식으로 변환하는 복수의 NTT(Number Theoretic Transform) 아키텍처, 상기 복수의 NTT 아키텍처를 통해 NTT 형태로 변환된 복수의 다항식에 대하여 포인트-와이즈(Point-wise) 곱셈 연산을 수행하는 모듈러 곱셈기(Modular Multiplier) 및 복수의 길이(N)와 모듈러스(q)를 갖는 가변적인 파라미터의 NTT 형태의 다항식을 수신하여 원래의 형태의 다항식으로 변환하는 INTT(Inverse NTT) 아키텍처를 포함한다.

대표도 - 도1



(52) CPC특허분류

G06F 15/8046 (2013.01)

H04L 9/008 (2013.01)

이 발명을 지원한 국가연구개발사업

|             |                                           |
|-------------|-------------------------------------------|
| 과제고유번호      | 1711139247                                |
| 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      | 1711134703                     |
| 과제번호        | 20210007790012003              |
| 부처명         | 과학기술정보통신부                      |
| 과제관리(전문)기관명 | 정보통신기획평가원                      |
| 연구사업명       | 방송통신산업기술개발사업                   |
| 연구과제명       | HW지원 프라이머시 보장 암호데이터 고속처리 기술 개발 |
| 기 여 율       | 1/3                            |
| 과제수행기관명     | 인하대학교 산학협력단                    |
| 연구기간        | 2021.04.01 ~ 2024.12.31        |

이 발명을 지원한 국가연구개발사업

|             |                                                |
|-------------|------------------------------------------------|
| 과제고유번호      | 1415172944                                     |
| 과제번호        | 20010589                                       |
| 부처명         | 산업통상자원부                                        |
| 과제관리(전문)기관명 | 한국산업기술평가관리원                                    |
| 연구사업명       | 시스템반도체 핵심 IP 개발 사업                             |
| 연구과제명       | 스마트인증과 데이터 유출의 무결성 보장을 위한 차세대 동형암호(HE)기반 IP 개발 |
| 기 여 율       | 1/3                                            |
| 과제수행기관명     | 인하대학교 산학협력단                                    |
| 연구기간        | 2020.04.01 ~ 2022.12.31                        |

## 명세서

### 청구범위

#### 청구항 1

복수의 길이(N)와 모듈러스(q)를 갖는 가변적인 파라미터의 다항식을 수신하여 NTT 형태의 다항식으로 변환하는 복수의 NTT(Number Theoretic Transform) 아키텍처;

상기 복수의 NTT 아키텍처를 통해 NTT 형태로 변환된 복수의 다항식에 대하여 포인트-와이즈(Point-wise) 곱셈 연산을 수행하는 모듈러 곱셈기(Modular Multiplier); 및

복수의 길이(N)과 모듈러스(q)를 갖는 가변적인 파라미터의 NTT 형태의 다항식을 수신하여 원래의 형태의 다항식으로 변환하는 INTT(Inverse NTT) 아키텍처

를 포함하고,

상기 NTT 아키텍처는,

PE1(Processing Element 1) 및 PE2(Processing Element 2)를 포함하고,

RNS(Residue Number System) 수체계에서 정의된 파라미터인 상기 복수의 길이(N)에 대한 가변성을 지원하는 다항식 곱셈 연산을 수행하기 위해 NTT 연산을 수행하는 파이프라인이 가능한 2-병렬 시스톱-어레이 NTT 아키텍처이고,

MUX를 이용한 단계 조절을 통해 동형암호 암호문의 길이인 상기 복수의 길이(N)에 대한 가변성을 지원하며,

상기 PE1은,

복수의 동형암호의 암호문의 길이인 상기 복수의 길이(N)에 상응하는 모듈러스(q)를 지원하고, CT(Cooley-Tukey) 알고리즘을 통해 비트역순 계산과정을 생략하는 메모리 구조를 가진 FIFO를 이용한 피드백 구조를 이용하여, 한 개의 데이터 경로를 이용하여 NTT 연산을 수행하고,

상기 PE2는,

복수의 동형암호의 암호문의 길이인 상기 복수의 길이(N)에 상응하는 모듈러스(q)를 지원하고, CT(Cooley-Tukey) 알고리즘을 통해 비트역순 계산과정을 생략하는 메모리 구조를 가진 두 개의 데이터 경로를 이용하여 NTT 연산을 수행하는

NTT 기반 다항식 곱셈기.

#### 청구항 2

제1항에 있어서,

상기 모듈러 곱셈기는,

RNS 수체계에서 정의된 파라미터인 모듈러스(q)에 대한 가변성을 지원하는 모듈러 곱셈 연산을 수행하는 바렛 알고리즘 기반 모듈러 곱셈기인

NTT 기반 다항식 곱셈기.

#### 청구항 3

제1항에 있어서,

상기 INTT 아키텍처는,

PE1(Processing Element 1) 및 PE2(Processing Element 2)를 포함하고,

RNS(Residue Number System) 수체계에서 정의된 파라미터인 상기 복수의 길이(N)에 대한 가변성을 지원하는 다항식 곱셈 연산을 수행하기 위해 INTT 연산을 수행하는 파이프라인이 가능한 2-병렬 시스톱-어레이 INTT 아키텍처

텍처이고,

DEMUX를 이용한 단계 조절을 통해 동형암호 암호문의 길이인 상기 복수의 길이(N)에 대한 가변성을 지원하는 NTT 기반 다항식 곱셈기.

#### 청구항 4

복수의 길이(N)와 모듈러스(q)를 갖는 가변적인 파라미터의 다항식을 수신하여 NTT 형태의 다항식으로 변환하는 복수의 NTT(Number Theoretic Transform) 아키텍처;

상기 복수의 NTT 아키텍처를 통해 NTT 형태로 변환된 복수의 다항식에 대하여 포인트-와이즈(Point-wise) 곱셈 연산을 수행하는 모듈러 곱셈기(Modular Multiplier); 및

복수의 길이(N)과 모듈러스(q)를 갖는 가변적인 파라미터의 NTT 형태의 다항식을 수신하여 원래의 형태의 다항식으로 변환하는 INTT(Inverse NTT) 아키텍처

를 포함하고,

상기 INTT 아키텍처는,

PE1(Processing Element 1) 및 PE2(Processing Element 2)를 포함하고,

RNS(Residue Number System) 수체계에서 정의된 파라미터인 상기 복수의 길이(N)에 대한 가변성을 지원하는 다항식 곱셈 연산을 수행하기 위해 INTT 연산을 수행하는 파이프라인이 가능한 2-병렬 시스톱-어레이 INTT 아키텍처이고,

DEMUX를 이용한 단계 조절을 통해 동형암호 암호문의 길이인 상기 복수의 길이(N)에 대한 가변성을 지원하며,

상기 PE1은,

복수의 동형암호의 암호문의 길이인 상기 복수의 길이(N)에 상응하는 모듈러스(q)를 지원하고, GS(Gentleman-Sande) 알고리즘을 통해 비트역순 계산과정을 생략하는 메모리 구조를 가진 FIFO를 이용한 피드백 구조를 이용하여, 한 개의 데이터 경로를 이용하여 INTT 연산을 수행하고,

상기 PE2는,

복수의 동형암호의 암호문의 길이인 상기 복수의 길이(N)에 상응하는 모듈러스(q)를 지원하고, GS(Gentleman-Sande) 알고리즘을 통해 비트역순 계산과정을 생략하는 메모리 구조를 가진 두 개의 데이터 경로를 이용하여 INTT 연산을 수행하는

NTT 기반 다항식 곱셈기.

#### 청구항 5

제4항에 있어서,

비트역순 계산과정을 생략하기 위해 상기 NTT 아키텍처 및 상기 INTT 아키텍처의 메모리 구조는 각 단계별로 상이한 크기를 갖는 메모리 뱅크(Memory Bank)로 구성되며, 비트역순의 순서로 미리 배열된 회전인자(Twiddle Factor)의 순서를 갖는

NTT 기반 다항식 곱셈기.

#### 청구항 6

복수의 NTT(Number Theoretic Transform) 아키텍처가 복수의 길이(N)와 모듈러스(q)를 갖는 가변적인 파라미터의 다항식을 수신하여 NTT 형태의 다항식으로 변환하는 단계;

모듈러 곱셈기(Modular Multiplier)가 상기 복수의 NTT 아키텍처를 통해 NTT 형태로 변환된 복수의 다항식에 대하여 포인트-와이즈(Point-wise) 곱셈 연산을 수행하는 단계; 및

INTT(Inverse NTT) 아키텍처가 복수의 길이(N)과 모듈러스(q)를 갖는 가변적인 파라미터의 NTT 형태의 다항식을 수신하여 원래의 형태의 다항식으로 변환하는 단계

를 포함하고,

상기 복수의 NTT 아키텍처가 복수의 길이(N)와 모듈러스(q)를 갖는 가변적인 파라미터의 다항식을 수신하여 NTT 형태의 다항식으로 변환하는 단계는,

상기 복수의 NTT 아키텍처의 PE1를 통해 복수의 동형암호의 암호문의 길이인 상기 복수의 길이(N)에 상응하는 모듈러스(q)를 지원하고, CT(Cooley-Tukey) 알고리즘을 통해 비트역순 계산과정을 생략하는 메모리 구조를 가진 FIFO를 이용한 피드백 구조를 이용하며, 한 개의 데이터 경로를 이용하여 NTT 연산을 수행하고,

상기 복수의 NTT 아키텍처의 PE2를 통해 복수의 동형암호의 암호문의 길이인 상기 복수의 길이(N)에 상응하는 모듈러스(q)를 지원하고, CT(Cooley-Tukey) 알고리즘을 통해 비트역순 계산과정을 생략하는 메모리 구조를 가진 두 개의 데이터 경로를 이용하여 NTT 연산을 수행하는

NTT 기반 다항식 곱셈기의 동작 방법.

## 청구항 7

복수의 NTT(Number Theoretic Transform) 아키텍처가 복수의 길이(N)와 모듈러스(q)를 갖는 가변적인 파라미터의 다항식을 수신하여 NTT 형태의 다항식으로 변환하는 단계;

모듈러 곱셈기(Modular Multiplier)가 상기 복수의 NTT 아키텍처를 통해 NTT 형태로 변환된 복수의 다항식에 대하여 포인트-와이즈(Point-wise) 곱셈 연산을 수행하는 단계; 및

INTT(Inverse NTT) 아키텍처가 복수의 길이(N)과 모듈러스(q)를 갖는 가변적인 파라미터의 NTT 형태의 다항식을 수신하여 원래의 형태의 다항식으로 변환하는 단계

를 포함하고,

상기 INTT 아키텍처가 복수의 길이(N)과 모듈러스(q)를 갖는 가변적인 파라미터의 NTT 형태의 다항식을 수신하여 원래의 형태의 다항식으로 변환하는 단계는,

상기 INTT 아키텍처의 PE1를 통해 복수의 동형암호의 암호문의 길이인 상기 복수의 길이(N)에 상응하는 모듈러스(q)를 지원하고, GS(Gentleman-Sande) 알고리즘을 통해 비트역순 계산과정을 생략하는 메모리 구조를 가진 FIFO를 이용한 피드백 구조를 이용하며, 한 개의 데이터 경로를 이용하여 INTT 연산을 수행하고,

상기 INTT 아키텍처의 PE2를 통해 복수의 동형암호의 암호문의 길이인 상기 복수의 길이(N)에 상응하는 모듈러스(q)를 지원하고, GS(Gentleman-Sande) 알고리즘을 통해 비트역순 계산과정을 생략하는 메모리 구조를 가진 두 개의 데이터 경로를 이용하여 INTT 연산을 수행하는

NTT 기반 다항식 곱셈기의 동작 방법.

## 청구항 8

삭제

## 청구항 9

삭제

## 청구항 10

삭제

## 발명의 설명

## 기술 분야

[0001] 본 발명은 동형암호를 위한 가변적으로 동작하는 NTT 기반 다항식 곱셈기 장치 및 방법에 관한 것이다.

## 배경 기술

[0002] 동형암호는 암호문을 이용하여 연산을 가능하게 해주는 기술로, 평문을 이용한 연산의 결과와 암호문을 이용하

여 연산하고 복호화 한 결과가 같은 값을 가진다. 이런 특징을 이용하면, 암호화된 데이터를 복호화 없이, 암호화된 상태로 개인정보를 풀어보지 않고도 통계분석 및 기계학습(Machine Learning)이 가능하다. 암호화된 상태에서 통계처리나 검색, 기계학습이 가능하기 때문에 해커가 데이터를 해킹하더라도 암호화된 데이터만 탈취할 뿐 원본데이터를 해석할 수 없다. 이 때문에 의료나 금융 분야에서 개인 빅데이터 정보를 활용할 때 정보가 유출되어도 개인 식별이 불가하다는 점에서 도움이 불가한 "완전 암호화"로 불린다.

[0003] 현재 동형암호 기술은 미래 암호 기술의 핵심으로 다양한 응용 가능성 때문에 학계 및 산업계의 관심이 높으나, 수학적 난이도가 높고 기존 암호 체계에 비해 암호복호화 및 연산 속도가 느려, 실용화를 위해서는 고성능 동형암호 하드웨어 아키텍처 구현이 필요하다.

[0004] 동형암호를 위한 방법으로는 격자-기반(Lattice-based) 방법이 있으며, 격자-기반 방법들 중에 하나인 Ring-LWE 암호는 효율적인 하드웨어 아키텍처 구현이 가능하면서 낮은 하드웨어 복잡도를 가지는 반면에 암호화된 데이터 연산시에 연산 횟수가 증가함에 따라 오류가 증가하는 문제가 있어서, 연산 횟수에 제한이 있다. B/FV, CKKS 등 많은 동형암호 알고리즘은 이러한 문제를 해결하고자 RNS(Residue Number System) 수 체계 아래에서 동작한다.

[0005] 따라서 RNS 수 체계 아래에서 연산 횟수에 제한이 없으면서 하드웨어 복잡도가 작은 완전동형 암호 아키텍처 및 암호시스템 연구가 필수적이다. Ring-LWE는 링(Ring) 안에서 계산되며 다항식 곱셈이 주로 쓰이는데 가장 많은 시간자원을 사용하므로 다항식 연산속도를 향상시켜주는 고성능 NTT(Number Theoretic Transform)를 필요로 한다.

## 선행기술문헌

### 특허문헌

[0006] (특허문헌 0001) 한국 공개특허 제10-2019-0138815호 (2019.12.16)

## 발명의 내용

### 해결하려는 과제

[0007] 본 발명이 이루고자 하는 기술적 과제는 동형암호를 위한 암호화 프로세서에 사용되는 고성능 2-병렬 시스토크-어레이(Systolic-array) NTT 코어의 하드웨어 구조 및 방법을 제공하는데 있다. 또한, 동형암호 원리에 맞추어 파라미터  $N$ 과  $q$ 에 대하여 가변성을 제공하여 하나의 하드웨어를 이용하여 복수의 표준을 지원하고자 한다.

[0008] 모듈러 연산기는 덧셈기, 뺄셈기 및 곱셈기로 이루어져 있으며 다양한 파라미터  $q$ 에 대응하도록 하고자 한다. 덧셈기 및 뺄셈기는 입력과 출력되는 수의 크기를 조절해 바렛 모듈로 연산(Barrett Modular Reduction) 없이 비교기(Comparator)만으로 하드웨어 복잡도를 낮추고, 곱셈기는 바렛 모듈러 곱셈기(Barrett Modular Multiplier)를 이용하여 FPGA 기반의 암호시스템을 구현시에 FPGA내에 있는 DSP모듈을 이용하여 구조를 단순화하고, 분할-정복 알고리즘을 이용하여 하드웨어 복잡도를 낮추고자 한다. 또한, MUX, DEMUX를 이용한 분기를 이용하여 다양한 파라미터  $N$ 에 대해 대응하고자 하며, NTT 다항식 곱셈기의 하드웨어 복잡성을 줄이며, 클럭 속도를 높이기 위해 2-병렬 시스토크-어레이 구조, 파이프라인 구조, 및 비트-역순(Bit-Reverse) 연산을 제거하는 방법을 제공하고자 한다.

### 과제의 해결 수단

[0009] 일 측면에 있어서, 본 발명에서 제안하는 동형암호를 위한 가변적으로 동작하는 NTT 기반 다항식 곱셈기는 가변적인 파라미터 길이( $N$ )와 모듈러스( $q$ )를 갖는 다항식을 수신하여 NTT 형태의 다항식으로 변환하는 가변적으로 동작이 가능한 복수의 NTT(Number Theoretic Transform) 아키텍처, 상기 가변적인 복수의 NTT 아키텍처를 통해 NTT 형태로 변환된 복수의 다항식에 대하여 포인트-와이즈(Point-wise) 곱셈 연산을 수행하는 모듈러 곱셈기(Modular Multiplier) 및 복수의 길이( $N$ )과 모듈러스( $q$ )를 갖는 가변적인 파라미터의 NTT 형태의 다항식을 수신하여 원래의 형태의 다항식으로 변환하는 INTT(Inverse NTT) 아키텍처를 포함한다.

[0010] 본 발명의 실시예에 따른 NTT 아키텍처는 PE1(Processing Element 1) 및 PE2(Processing Element 2)를 포함하고, RNS(Residue Number System) 수체계에서 정의된 파라미터인 상기 복수의 길이( $N$ )에 대한 가변성을 지원하는 다항식 곱셈 연산을 수행하기 위해 NTT 연산을 수행하는 파이프라인이 가능한 2-병렬 시스토크-어레이 NTT 아키텍처를 포함한다.

텍처이고, MUX를 이용한 단계 조절을 통해 동형암호 암호문의 길이인 상기 복수의 길이(N)에 대한 가변성을 지원한다.

[0011] 본 발명의 실시예에 따른 모듈러 곱셈기는 RNS 수 체계에서 정의된 파라미터인 모듈러스(q)에 대한 가변성을 지원하는 모듈러 곱셈 연산을 수행하는 바렛 알고리즘 기반 모듈러 곱셈기이다.

[0012] 본 발명의 실시예에 따른 INTT 아키텍처는 PE1(Processing Element 1) 및 PE2(Processing Element 2)를 포함하고, RNS(Residue Number System) 수 체계에서 정의된 파라미터인 상기 복수의 길이(N)에 대한 가변성을 지원하는 다항식 곱셈 연산을 수행하기 위해 INTT 연산을 수행하는 파이프라인이 가능한 2-병렬 시스톱-어레이 INTT 아키텍처이고, DEMUX를 이용한 단계 조절을 통해 동형암호 암호문의 길이인 상기 복수의 길이(N)에 대한 가변성을 지원한다.

[0013] 본 발명의 실시예에 따른 NTT 아키텍처의 PE1은 복수의 동형암호의 암호문의 길이인 상기 복수의 길이(N)에 상응하는 모듈러스(q)를 지원하고, CT(Cooley-Tukey) 알고리즘을 통해 비트역순 계산과정을 생략하는 메모리 구조를 가진 FIFO를 이용한 피드백 구조를 이용하며, 한 개의 데이터 경로를 이용하여 NTT 연산을 수행한다.

[0014] 본 발명의 실시예에 따른 NTT 아키텍처의 PE2는 복수의 동형암호의 암호문의 길이인 상기 복수의 길이(N)에 상응하는 모듈러스(q)를 지원하고, CT(Cooley-Tukey) 알고리즘을 통해 비트역순 계산과정을 생략하는 메모리 구조를 가진 두 개의 데이터 경로를 이용하여 NTT 연산을 수행한다.

[0015] 본 발명의 실시예에 따른 INTT 아키텍처의 PE1은 복수의 동형암호의 암호문의 길이인 상기 복수의 길이(N)에 상응하는 모듈러스(q)를 지원하고, GS(Gentleman-Sande) 알고리즘을 통해 비트역순 계산과정을 생략하는 메모리 구조를 가진 FIFO를 이용한 피드백 구조를 이용하며, 한 개의 데이터 경로를 이용하여 INTT 연산을 수행한다.

[0016] 본 발명의 실시예에 따른 INTT 아키텍처의 PE2는 복수의 동형암호의 암호문의 길이인 상기 복수의 길이(N)에 상응하는 모듈러스(q)를 지원하고, GS(Gentleman-Sande) 알고리즘을 통해 비트역순 계산과정을 생략하는 메모리 구조를 가진 두 개의 데이터 경로를 이용하여 INTT 연산을 수행한다.

[0017] 본 발명의 실시예에 따르면, 비트역순 계산과정을 생략하기 위해 상기 NTT 아키텍처 및 상기 INTT 아키텍처의 메모리 구조는 각 단계별로 상이한 크기를 갖는 메모리 뱅크(Memory Bank)로 구성되며, 비트역순의 순서로 미리 배열된 회전인자(Twiddle Factor)의 순서를 갖는다.

[0018] 또 다른 일 측면에 있어서, 본 발명에서 제안하는 동형암호를 위한 가변적으로 동작하는 NTT 기반 다항식 곱셈기의 동작 방법은 복수의 NTT(Number Theoretic Transform) 아키텍처가 복수의 길이(N)와 모듈러스(q)를 갖는 가변적인 파라미터의 다항식을 수신하여 NTT 형태의 다항식으로 변환하는 단계, 모듈러 곱셈기(Modular Multiplier)가 상기 복수의 NTT 아키텍처를 통해 NTT 형태로 변환된 복수의 다항식에 대하여 포인트-와이즈(Point-wise) 곱셈 연산을 수행하는 단계 및 INTT(Inverse NTT) 아키텍처가 복수의 길이(N)와 모듈러스(q)를 갖는 가변적인 파라미터의 NTT 형태의 다항식을 수신하여 원래의 형태의 다항식으로 변환하는 단계를 포함한다.

### 발명의 효과

[0019] 본 발명의 실시예들에 따르면 다양한 파라미터 N, q에 대해 동작하는 다항식 곱셈기를 통하여 Ring-LWE 기반 RNS 수 체계에서 동작하는 동형암호 프로세서에서 하드웨어 재사용성을 높이고 중복된 구조를 생략하여 하드웨어 복잡도를 낮추며 하드웨어를 이용하여 가속할 수 있다.

[0020] 가변적으로 동작하는 2-병렬 시스톱-어레이(Systolic-array) NTT 아키텍처는 RNS 수 체계에서 동작하는 동형암호의 고성능 저복잡도의 암호화 아키텍처의 구조 및 방법을 제공하고, 동형암호에서 지정된 복수의 표준을 지원한다. 또한 효율적인 구조의 모듈러 연산기로서 모듈러 덧셈기 및 뺄셈기, 바렛 모듈러 곱셈기(Barrett Modular Multiplier)를 이용하여 FPGA 기반의 암호시스템에서 DSP를 이용하여 곱셈기의 복잡도를 단순화할 수 있다. NTT 다항식 곱셈기의 하드웨어 복잡도를 줄이며, 2-병렬 시스톱-어레이 구조, 파이프라인 구조, 및 비트-역순(Bit-Reverse) 연산을 제거하는 방법을 제공하여 클럭 속도를 높일 수 있다.

### 도면의 간단한 설명

[0021] 도 1은 본 발명의 일 실시예에 따른 NTT 기반의 다항식 곱셈기 장치의 구성을 설명하기 위한 도면이다.

도 2는 본 발명의 일 실시예에 따른 2-병렬 시스톱-어레이 NTT 아키텍처의 구조를 나타내는 도면이다.

도 3은 본 발명의 일 실시예에 따른 NTT 아키텍처를 구성하는 PE1(Processing Element 1) 구조를 나타내는 도면

이다.

도 4은 본 발명의 일 실시예에 따른 NTT 아키텍처를 구성하는 PE2(Processing Element 2) 구조를 나타내는 도면이다.

도 5은 본 발명의 일 실시예에 따른 NTT 아키텍처를 구성하는 메모리 구조를 나타내는 도면이다.

도 6은 본 발명의 일 실시예에 따른 NTT 아키텍처 및 INTT 아키텍처를 구성하는 모듈러 덧셈기를 나타내는 도면이다.

도 7은 본 발명의 일 실시예에 따른 NTT 아키텍처 및 INTT 아키텍처를 구성하는 모듈러 뺄셈기를 나타내는 도면이다.

도 8은 본 발명의 일 실시예에 따른 NTT 아키텍처 및 INTT 아키텍처를 구성하는 모듈러 곱셈기(Modular Multiplier)의 구조를 나타내는 도면이다.

도 9는 본 발명의 일 실시예에 따른 2-병렬 시스톱-어레이 INTT 아키텍처의 구조를 나타내는 도면이다.

도 10은 본 발명의 일 실시예에 따른 INTT 아키텍처를 구성하는 PE1(Processing Element 1) 구조를 나타내는 도면이다.

도 11은 본 발명의 일 실시예에 따른 INTT 아키텍처를 구성하는 PE2(Processing Element 2) 구조를 나타내는 도면이다.

도 12는 본 발명의 일 실시예에 따른 NTT 아키텍처의 데이터 흐름을 설명하기 위한 도면이다.

도 13는 본 발명의 일 실시예에 따른 INTT 아키텍처의 데이터 흐름을 설명하기 위한 도면이다.

도 14은 본 발명의 일 실시예에 따른 NTT 기반의 다항식 곱셈기 장치의 동작 방법을 설명하기 위한 흐름도이다.

### 발명을 실시하기 위한 구체적인 내용

- [0022] 본 발명은 RNS(Residue Number System) 수체계에서 동작하는 Ring-LWE(Learning with Error) 기반의 동형암호(Homomorphic Encryption, HE)을 위한 가변적인 파라미터에서 동작하는 NTT(Number Theoretic Transform) 기반 다항식 곱셈기의 장치 및 방법에 관한 것으로, 보다 상세하게는 다양한 암호문의 길이 파라미터  $N$ 과 RNS 수체계의 다양한 모듈러스 파라미터  $q$ 에 대하여 지원이 가능하다. 파이프라인 구조를 이용한 높은 데이터 처리율 대비 낮은 하드웨어 면적을 갖는 시스톱-어레이 방식을 적용하여 NTT기반 다항식 곱셈기의 데이터 메모리 접근을 줄여 하드웨어 복잡도를 단순화하는 방법에 대한 것이다.
- [0023] 본 발명의 실시예에 따른 NTT 기반 다항식 곱셈기는 RNS 수체계에서 동작하는 격자-기반의 Ring-LWE 기법의 동형암호에서 가변적인 파라미터를 지원하기 위해 사용한다. RNS 수체계의 Ring-LWE 기법의 동형암호는 용도에 따른 다양한 암호문의 길이  $N$ 이 요구되며, RNS 수체계에서 동작함으로 다양한 소수(Prime Number)의 모듈러스 파라미터  $q$ 를 요구한다. 또한 다양한 암호문의 길이  $N$ 과 모듈러스  $q$ 에 의하여 높은 보안성을 갖는다.
- [0024] 본 발명의 실시예에 따른 동형암호는 RNS 수체계에서 격자-기반의 Ring-LWE 기법을 사용한다. Ring-LWE는 링(Ring) 안에서 계산되며 다항식 곱셈이 주로 쓰이는데 가장 많은 시간자원을 사용함으로 다항식 연산속도를 향상시켜 주는 고성능 NTT를 필요로 한다.
- [0025] 제안하는 NTT 및 INTT 아키텍처는 높은 데이터 처리율을 얻기 위해 파이프라인이 가능한 구조인 2-병렬 구조를 사용한다. 높은 데이터 처리율 및 낮은 복잡도를 갖기 위해 각 단계별로 회전인자(Twiddle Factor)를 저장하는 메모리 뱅크(Memory Bank)를 이용하며, 회전인자(Twiddle Factor)와 다항식의 계수를 곱하는 모듈러 곱셈기(Modular Multiplier), CT(Cooley-Tukey) 알고리즘, GS(Gentleman-Sande) 알고리즘을 이용한 버터플라이 연산을 위한 모듈러 덧셈기(Modular Adder), 모듈러 뺄셈기(Modular Subtractor)를 포함한다. 이하, 본 발명의 실시예를 첨부된 도면을 참조하여 상세하게 설명한다. 이하, 본 발명의 실시예를 첨부된 도면을 참조하여 상세하게 설명한다.
- [0027] 도 1은 본 발명의 일 실시예에 따른 NTT 기반의 다항식 곱셈기 장치의 구성을 설명하기 위한 도면이다.
- [0028] 본 발명의 실시예에 따른 NTT 기반의 다항식 곱셈기 장치(100)는 복수의 NTT(Number Theoretic Transform) 아키텍처(121, 122), 모듈러 곱셈기(Modular Multiplier)(130) 및 INTT(Inverse NTT) 아키텍처(140)를 포함한다.

- [0029] 본 발명의 실시예에 따른 복수의 NTT 아키텍처(121, 122)는 복수의 길이(N)와 모듈러스(q)를 갖는 가변적인 파라미터의 다항식을 수신하여 NTT 형태의 다항식으로 변환한다.
- [0030] 본 발명의 실시예에 따른 복수의 NTT 아키텍처(121, 122) 각각은 PE1(Processing Element 1)과 PE2(Processing Element 2), PE 내에서 회전인자(Twiddle Factor)와 다항식의 계수를 곱해주는 모듈러 곱셈기(Modular Multiplier), CT 알고리즘의 버터플라이(Butterfly) 연산을 수행하는 모듈러 덧셈기(Modular Adder)와 모듈러 뺄셈기(Modular Subtractor)를 포함하며, 회전인자(Twiddle Factor)를 저장하기 위한 메모리(Memory) 구조를 포함한다.
- [0031] 본 발명의 실시예에 따른 복수의 NTT 아키텍처(121, 122)는 반복적으로 이용되는 다항식 곱셈을 수행하기 위해 NTT 연산을 수행하는 파이프라인이 가능한 2-병렬 시스톱-어레이 NTT 아키텍처이고, 상기 2-병렬 시스톱-어레이 NTT 아키텍처는 CT(Cooley-Tukey) 알고리즘을 사용하여 비트 역순과정을 생략할 수 있다.
- [0032] 본 발명의 실시예에 따른 복수의 NTT 아키텍처(121, 122)는 MUX를 이용한 단계 조절을 통하여 복수의 길이(N)에 대한 가변성을 제공하며, 파라미터 N에 대하여 PE(Processing Element)의 반복 횟수를 조절함으로써 효율적으로 동작한다.
- [0033] 본 발명의 실시예에 따른 복수의 NTT 아키텍처(121, 122) 각각의 PE1은 모듈러 곱셈기를 이용하여 회전인자(Twiddle Factor)와 다항식 계수를 곱하고, 모듈러 덧셈기, 모듈러 뺄셈기를 이용하여 CT 알고리즘을 수행하며, FIFO(First-In-First-Output)를 이용한 피드백(Feed-back) 구조로 효율적으로 다항식을 NTT 변환한다. FIFO의 깊이는 각 단계에 효율적인 2의 승수로 설정된다.
- [0034] 본 발명의 실시예에 따른 복수의 NTT 아키텍처(121, 122) 각각의 PE2는 모듈러 곱셈기를 이용하여 회전인자(Twiddle factor)와 다항식 계수를 곱하고, 모듈러 덧셈기, 모듈러 뺄셈기를 이용하여 CT 알고리즘을 수행하며, 파이프라인이 가능한 2-병렬 구조로 FIFO에 의한 피드백 없이 동작한다.
- [0035] 본 발명의 실시예에 따른 복수의 NTT 아키텍처(121, 122) 각각의 메모리 구조는 각 단계에서 필요한 회전인자(Twiddle Factor)에 개수에 맞춘 독립적인 메모리 뱅크(Bank)로 이루어지며, CT 알고리즘, GS 알고리즘에서 비트 역순 과정을 생략하기 위한 순서로 저장된다.
- [0036] 본 발명의 실시예에 따른 모듈러 곱셈기(130)는 상기 복수의 NTT 아키텍처를 통해 NTT 형태로 변환된 복수의 다항식에 대하여 포인트-와이즈(Point-wise) 곱셈 연산을 수행한다.
- [0037] 본 발명의 실시예에 따른 모듈러 곱셈기(130)는 바렛 알고리즘을 이용한 정수 곱셈기, 가변적인 모듈러스(q) 및 T에 대한 보조 곱셈기를 포함하며 분할-정복 알고리즘을 통한 효율적인 모듈러 곱셈 연산을 지원한다.
- [0038] 본 발명의 실시예에 따른 모듈러 덧셈기 및 모듈러 뺄셈기는 유한체 내의 수를 이용하여 비교기를 이용한 바렛 모듈러 연산 과정을 생략한 효율적인 구조를 지원한다.
- [0039] 본 발명의 실시예에 따른 INTT 아키텍처(140)는 복수의 길이(N)과 모듈러스(q)를 갖는 가변적인 파라미터의 NTT 형태의 다항식을 수신하여 원래의 형태의 다항식으로 변환한다.
- [0040] 본 발명의 실시예에 따른 INTT 아키텍처(140)는 PE1(Processing Element 1)과 PE2(Processing Element 2), GS 알고리즘의 버터플라이 연산을 수행하는 모듈러 덧셈기(Modular Adder)와 모듈러 뺄셈기(Modular Subtractor)를 포함하며, 회전인자와 다항식의 계수를 곱해주는 모듈러 곱셈기(Modular Multiplier), 회전인자를 저장하기 위한 메모리 구조를 포함한다.
- [0041] 본 발명의 실시예에 따른 INTT 아키텍처(140)는 DEMUX를 이용한 단계 조절을 통하여 다양한 복수의 파라미터 N에 대한 가변성을 제공하며, 파라미터 N에 대하여 PE(Processing Element)의 반복 횟수를 조절함으로써 효율적으로 동작한다.
- [0042] 본 발명의 실시예에 따른 INTT(140)의 PE1은 모듈러 덧셈기, 모듈러 뺄셈기를 이용하여 GS 알고리즘을 수행하고, 모듈러 곱셈기를 이용하여 회전인자와 다항식 계수를 곱하며, FIFO를 이용한 피드백 구조로 효율적으로 다항식을 INTT 변환한다. FIFO의 깊이는 각 단계에 효율적인 2의 승수로 설정된다.
- [0043] 본 발명의 실시예에 따른 INTT(140)의 PE2는 모듈러 덧셈기, 모듈러 뺄셈기를 이용하여 GS 알고리즘을 수행하고, 모듈러 곱셈기를 이용하여 회전인자와 다항식 계수를 곱하며, 파이프라인이 가능한 2-병렬 구조로 FIFO에 의한 피드백 없이 동작한다.

[0044] 더욱 상세하게는, 본 발명의 실시예에 따른 NTT 기반 다항식 곱셈기 장치(100)은 두 개의 다항식을 수신하여 합성곱(Convolution) 형태의 다항식을 생성한다.

[0045] 본 발명의 실시예에 따른 복수의 NTT 아키텍처(121, 122)는 다항식을 수신하여 NTT 형태의 다항식으로 변환한다.

[0046] 본 발명의 실시예에 따른 모듈러 곱셈기(130)는 NTT 형태로 변환된 두 다항식의 포인트-와이즈(Point-wise) 곱셈을 수행한다.

[0047] 본 발명의 실시예에 따른 INTT 아키텍처(140)는 다항식 곱셈의 결과를 INTT 연산을 통하여 NTT 형태의 다항식에서 원본 형태의 다항식 형태로 변환한다.

[0048] 본 발명의 실시예에 따른 NTT 아키텍처(121, 122)는 파이프라인 구조의 2-병렬 시스톱-어레이 NTT 아키텍처로 CT(Cooley-Tukey) 알고리즘을 사용하여 비트 역순과정을 생략할 수 있다.

[0049] 본 발명의 실시예에 따른 모듈러 곱셈기(130)는 포인트-와이즈 다항식 곱셈연산을 이용하여 합성곱(Convolution)보다 낮은 복잡도를 갖는 고속의 다항식 곱셈을 수행한다.

[0050] 본 발명의 실시예에 따른 INTT 아키텍처(140)는 파이프라인 구조의 2-병렬 시스톱-어레이 INTT 아키텍처로 GS(Gentlemen-Sande) 알고리즘을 사용하여 비트 역순과정을 생략할 수 있다.

[0051] 도 1을 참조하면, 본 발명의 실시예에 따른 NTT 아키텍처(121, 122)는 빠른 다항식 곱셈을 이용하기 위해 NTT 연산을 수행한다. NTT 연산은 식 (1)과 같이 나타낼 수 있다:

$$A_i = \sum_{j=0}^{n-1} a_j w_n^{ij} \bmod q, \text{ for } i = 0, 1, \dots, n-1 \quad \text{식(1)}$$

[0053] 또한, 본 발명의 실시예에 따른 Ring-LWE의 모든 연산은  $R_q = \mathbb{Z}_q[x]/f(x)$ 의 조건을 만족시키면서 동작하므로 다항식  $a(x)$ 와  $b(x)$ 는 식(2-1) 및 식(2-2)와 같이 나타낼 수 있다:

$$a(x) = a_0 + a_1x + a_2x^2 + \dots + a_{n-1}x^{n-1} \quad \text{식(2-1)}$$

$$b(x) = b_0 + b_1x + b_2x^2 + \dots + b_{n-1}x^{n-1} \quad \text{식(2-2)}$$

[0056] 벡터(Vector)  $\mathbf{a} = a_0, \dots, a_{n-1}$ 는 다항식  $a(x)$ 의 계수이며, 숫자  $n$ 은 2의 자승이다.  $q$ 는  $q \equiv 1 \pmod{2N}$ 을 만족하는 소수(prime number)이다. 수학식 1에서  $n$ 과  $w$ 는  $n * n^{-1} \equiv 1 \bmod q, w * w^{-1} \equiv 1 \bmod q, n * n^{-1} \equiv 1 \bmod q, w * w^{-1} \equiv 1 \bmod q$ 의 조건을 만족하는 숫자로 구성된다. 모듈러 곱셈기(130)는  $AB=A*B \pmod q$ 와 같은 연산을 수행하며 다항식 간의 Point-wise 곱셈을 진행하며 정해진  $q$ 값에 대해 모듈러 연산을 진행한다.

[0057] 본 발명의 실시예의 INTT 아키텍처(140)는 다항식 곱셈 이후 NTT 형태의 다항식에서 원래 형태의 다항식으로 변환하기 위하여 INTT 연산을 수행한다. INTT 연산은 식(3)과 같이 나타낼 수 있다:

$$a_i = n^{-1} \sum_{j=0}^{n-1} A_j w_n^{-ij} \bmod q, \text{ for } i = 0, 1, \dots, n-1 \quad \text{식(3)}$$

[0059] 다항식의 곱셈 연산은 수학식 1,2,3을 이용하여 아래의 식(4)로 표현할 수 있다:

$$a(x) * b(x) = INTT(NTT(a) \cdot NTT(b)) \quad \text{식(4)}$$

[0061] 식(4)의 좌변의 다항식 곱셈은 합성곱(Convolution) 연산으로  $O(N^2)$ 의 시간복잡도를 가지나, 우변의 NTT 기반의 다항식 곱셈은 포인트-와이즈 곱셈 연산으로  $O(N \log N)$ 의 시간 복잡도를 가져 고성능 저복잡도의 구조를 갖는다.

[0063] 도 2는 본 발명의 일 실시예에 따른 2-병렬 시스톱-어레이 NTT 아키텍처의 구조를 나타내는 도면이다.

[0064] 제안하는 NTT 기반 다항식 곱셈기 장치는 NTT 아키텍처를 이용하여 고성능 저복잡도의 다항식 곱셈 연산을 수행하는 장치로 PE1(Processing Element 1), PE2 (Processing Element 2), MUX를 포함한다. PE1과 PE2는 입력 받

은 다항식을 CT(Cooley-Tukey) 알고리즘으로 버터플라이 연산을 수행하며 MUX는 분기를 통해 최대 16개의 단계를 결정하는 방식으로 다항식의 길이 파라미터 N에 대하여  $N=2^{12}, 2^{13}, 2^{14}, 2^{15}, 2^{16}$ 의 N을 가변적으로 지원한다. 도 2의 NTT 아키텍처는 CT 알고리즘을 이용하여 상기 식(1)로 나타낸다.

[0066] 도 3은 본 발명의 일 실시예에 따른 NTT 아키텍처를 구성하는 PE1(Processing Element 1) 구조를 나타내는 도면이다.

[0067] 제안하는 NTT 기반 다항식 곱셈기 장치는 NTT 아키텍처의 CT 알고리즘을 수행하는 장치로 모듈러 곱셈기, 모듈러 덧셈기, 모듈러 뺄셈기, 메모리, FIFO를 포함한다.

[0068] 본 발명의 실시예에 따른 NTT의 PE1은 하나의 데이터 경로를 FIFO를 이용한 피드백 구조를 이용하여, 메모리에서 회전인자(Twiddle Factor)를 수신하여 입력 받은 다항식의 계수와 모듈러 곱셈기를 통하여 곱하고, 모듈러 덧셈기 및 모듈러 뺄셈기를 이용하여 CT 알고리즘을 수행한다. 각 단계의 PE1의 FIFO의 깊이는 단계 1에서 32768개, 단계 2에서 16384개, 단계 3에서 8192개로 1/2씩 줄어든다.

[0070] 도 4은 본 발명의 일 실시예에 따른 NTT 아키텍처를 구성하는 PE2(Processing Element 2) 구조를 나타내는 도면이다.

[0071] 제안하는 NTT 기반 다항식 곱셈기 장치는 NTT 아키텍처의 CT 알고리즘을 수행하는 장치로 모듈러 곱셈기, 모듈러 덧셈기, 모듈러 뺄셈기, 메모리를 포함한다.

[0072] 본 발명의 실시예에 따른 NTT의 PE2은 2개의 데이터 경로를 이용하여 2개의 다항식의 계수를 입력 받아, 메모리에서 회전인자(Twiddle Factor)를 수신하여 입력 받은 다항식의 계수와 모듈러 곱셈기를 통하여 곱하고, 모듈러 덧셈기 및 모듈러 뺄셈기를 이용하여 CT 알고리즘을 수행한다.

[0074] 도 5은 본 발명의 일 실시예에 따른 NTT 아키텍처를 구성하는 메모리 구조를 나타내는 도면이다.

[0075] 제안하는 NTT 아키텍처의 각 단계별로 필요한 회전인자(Twiddle Factor)의 개수에 맞춘 독립적인 메모리 뱅크(Memory Bank)로 이루어지며, CT 알고리즘, GS 알고리즘에서 비트역순 과정을 생략하기 위한 순서로 저장된다. 각 단계에서 필요한 회전인자(Twiddle Factor)의 개수는  $2^{Stage\#-1}$  개이며 계산과정에서 비트역순 계산과정을 생략하기 위하여 회전인자를 비트 역순으로 저장한다.

[0077] 도 6은 본 발명의 일 실시예에 따른 NTT 아키텍처 및 INTT 아키텍처를 구성하는 모듈러 덧셈기를 나타내는 도면이다.

[0078] 본 발명의 실시예에 따른 모듈러 덧셈기는 모듈러 연산의 일종으로 입력 in1, in2의 덧셈 연산의 결과를 q보다 작은 링(Ring)으로 축소시켜주는 역할을 한다. 유한체 내의 존재하는 in1, in2에 대하여 비교 연산을 통해 모듈러 덧셈 연산을 수행한다.

[0080] 도 7은 본 발명의 일 실시예에 따른 NTT 아키텍처 및 INTT 아키텍처를 구성하는 모듈러 뺄셈기를 나타내는 도면이다.

[0081] 본 발명의 실시예에 따른 모듈러 뺄셈기는 모듈러 연산의 일종으로 입력 in1, in2의 뺄셈 연산의 결과를 q보다 작은 링(Ring)으로 축소시켜주는 역할을 한다. 유한체 내의 존재하는 in1, in2에 대하여 비교 연산을 통해 모듈러 뺄셈 연산을 수행한다.

[0083] 도 8은 본 발명의 일 실시예에 따른 NTT 아키텍처 및 INTT 아키텍처를 구성하는 모듈러 곱셈기(Modular Multiplier)의 구조를 나타내는 도면이다.

[0084] 본 발명의 실시예에 따른 모듈러 곱셈기는 바렛 모듈러 알고리즘(Barrett Modular Algorithm)을 이용한다. 가변적인 파라미터 q를 값을 사용하였으며, 입력 A, B는 정수 곱셈기를 이용하여 A\*B의 결과를 갖게 된다. 그 결과는 복잡도를 낮추기 위한 분할-정복 알고리즘을 통해 T와 q의 보조 곱셈기에 입력되고, 연산한 결과와 덧셈 혹은 뺄셈을 진행한다. 또한 Q보다 큰 값에 한하여 Q 값을 뺄셈한 결과를 도출한다.

[0086] 도 9는 본 발명의 일 실시예에 따른 2-병렬 시스템-어레이 INTT 아키텍처의 구조를 나타내는 도면이다.

[0087] 제안하는 NTT 기반 다항식 곱셈기 장치는 INTT 아키텍처를 이용하여 고성능 저복잡도의 다항식 곱셈 연산을 수행하는 장치로 PE1 (Processing Element 1), PE2 (Processing Element 2), DEMUX를 포함한다. PE1과 PE2는 입력 받은 다항식을 GS(Gentleman-Sande) 알고리즘으로 Butterfly 연산을 수행하며 DEMUX는 분기를 통해 최대 16

개의 단계를 결정하는 방식으로 다항식의 길이 파라미터 N에 대하여  $N=2^{12}, 2^{13}, 2^{14}, 2^{15}, 2^{16}$ 의 N을 가변적으로 지원한다. 도 9의 INTT 아키텍처는 GS(Gentleman-Sande) 알고리즘을 이용하며 식(3)로 나타낸다:

$$a_i = n^{-1} \sum_{j=0}^{n-1} A_j w_n^{-ij} \bmod q, \text{ for } i = 0, 1, \dots, n-1$$

식(3)

도 10은 본 발명의 일 실시예에 따른 INTT 아키텍처를 구성하는 PE1(Processing Element 1) 구조를 나타내는 도면이다.

제안하는 NTT 기반 다항식 곱셈기 장치의 INTT 아키텍처의 GS 알고리즘을 수행하는 장치로 모듈러 곱셈기, 모듈러 덧셈기, 모듈러 뺄셈기, 메모리, FIFO를 포함한다.

본 발명의 실시예에 따른 INTT의 PE1은 하나의 데이터 경로를 FIFO를 이용한 피드백 구조를 이용하여, 모듈러 덧셈기 및 모듈러 뺄셈기를 이용하여 GS 알고리즘을 수행하고, 메모리에서 회전인자(Twiddle Factor)를 수신하여 입력 받은 다항식의 계수와 모듈러 곱셈기를 통하여 곱한다. 각 단계의 PE1의 FIFO의 깊이는 단계 1에서 1개, 단계 2에서 2개, 단계 3에서 4개로 2배씩 늘어난다.

도 11은 본 발명의 일 실시예에 따른 INTT 아키텍처를 구성하는 PE2(Processing Element 2) 구조를 나타내는 도면이다.

제안하는 NTT 기반 다항식 곱셈기 장치의 INTT 아키텍처의 GS 알고리즘을 수행하는 장치로 모듈러 곱셈기, 모듈러 덧셈기, 모듈러 뺄셈기, 메모리를 포함한다.

본 발명의 실시예에 따른 INTT의 PE2는 2개의 데이터 경로를 이용하여 2개의 다항식의 계수를 입력 받아, 메모리에서 회전인자(Twiddle Factor)를 수신하여 입력 받은 다항식의 계수와 모듈러 곱셈기를 통하여 곱하고, 모듈러 덧셈기 및 모듈러 뺄셈기를 이용하여 GS 알고리즘을 수행한다.

도 12는 본 발명의 일 실시예에 따른 INTT 아키텍처의 데이터 흐름을 설명하기 위한 도면이다.

도 12를 참조하면, 제안하는 NTT 장치는 각 단계는 전 단계의 PE의 출력을 입력 받는 파이프라인 구조로 동작한다. 1단계 PE1에서 출력된 결과는 2단계 PE1에 16429 사이클(cycle) 지연 후에 파이프라인 구조로 입력되고, 2단계에서 출력은 3단계에  $24666-16429 = 8237$  사이클 지연 후에 입력된다. 각 단계별로 파이프라인 구조로 데이터가 처리되며 각 단계별로 FIFO 깊이에 비례하여 2배씩의 지연을 갖는다. MUX를 통한 파라미터 N 가변 조절 시 앞선 단계를 건너뛰고 단계2 또는 3 또는 단계 4, 단계 5 등에서 시작하는 데이터의 흐름을 갖는다.

도 13는 본 발명의 일 실시예에 따른 INTT 아키텍처의 데이터 흐름을 설명하기 위한 도면이다.

도 13를 참조하면, 제안하는 INTT 장치는 각 단계는 전 단계의 PE의 출력을 입력 받는 파이프라인 구조로 동작한다. 1단계 PE1에서 출력된 결과는 2단계 PE1에 45 사이클 지연 후에 파이프라인 구조로 입력되고, 2단계에서 출력은 3단계에  $92-45 = 47$  사이클 지연 후에 입력된다. 각 단계별로 파이프라인 구조로 데이터가 처리되며 각 단계별로 FIFO 깊이에 비례하여 2배씩의 지연을 갖는다. DEMUX를 통한 파라미터 N가변 조절 시 뒤쪽 단계를 건너뛰고 단계 12, 단계 13, 단계 14, 단계 15등에서 출력되는 데이터의 흐름을 갖는다.

도 14은 본 발명의 일 실시예에 따른 NTT 기반의 다항식 곱셈기 장치의 동작 방법을 설명하기 위한 흐름도이다.

제안하는 NTT기반 다항식 곱셈기 장치의 다항식 곱셈 수행 방법은 입력 받은 두 개의 다항식을 NTT아키텍처를 통해 NTT 형태로 변환하는 단계(1410), 모듈러 곱셈기(Modular Multiplier)를 이용하여 포인트-와이즈(Point-wise) 다항식 곱셈을 수행하는 단계(1420) 및 INTT 아키텍처를 통해 원래의 형태의 다항식으로 변환하는 단계(1430)를 포함한다.

단계(1410)에서, 복수의 NTT(Number Theoretic Transform) 아키텍처가 복수의 길이(N)와 모듈러스(q)를 갖는 가변적인 파라미터의 다항식을 수신하여 NTT 형태의 다항식으로 변환한다.

본 발명의 실시예에 따르면, 수신한 다항식 $a(x)$ 의 파라미터, 복수의 길이(N)와 모듈러스(q)를 판단한다(1411). 이후, 복수의 길이(N)에 대하여 NTT 아키텍처의 MUX를 설정하고(1412), 모듈러스(q)에 대하여 PE1 및 PE2를 이용한 CT 알고리즘을 수행한다(1413).

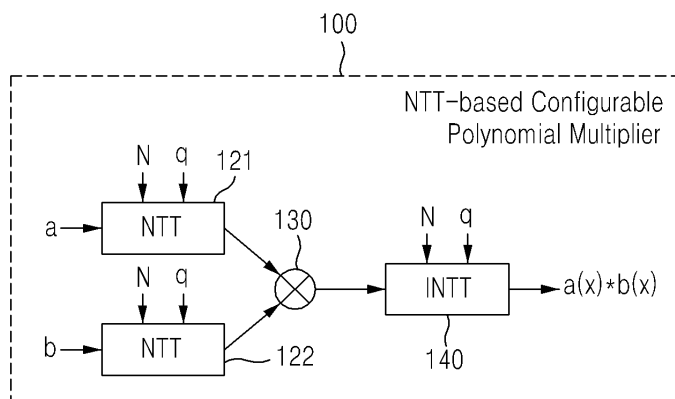
본 발명의 실시예에 따르면, 수신한 다항식 $b(x)$ 의 파라미터, 복수의 길이(N)와 모듈러스(q)를 판단한다(1414).

이후, 복수의 길이(N)에 대하여 NTT 아키텍처의 MUX를 설정하고(1415), 모듈러스(q)에 대하여 PE1 및 PE2를 이용한 CT 알고리즘을 수행한다(1416).

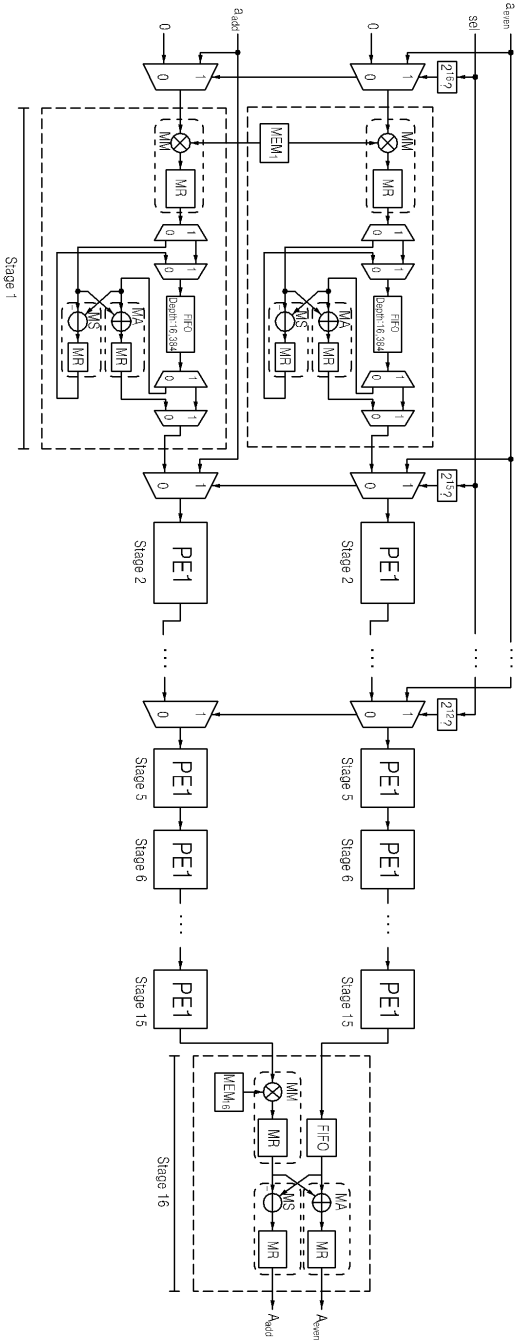
- [0109] 본 발명의 실시예에 따른 NTT 아키텍처를 활용하여 입력 받은 2개의 다항식을 NTT 형태로 변환하여 포인트-와이즈(Point-wise) 다항식 곱셈에 적합한 형태로 변환한다.
- [0110] 단계(1420)에서 NTT 형태로 변환된 2개의 다항식의 포인트-와이즈 다항식 곱셈을 수행한다. 단계(1410)을 통하여 NTT 형태로 변환되지 않은 다항식의 곱셈은 합성곱(Convolution)으로 진행되어  $O(N^2)$ 의 높은 시간복잡도를 가지나 단계(1410)을 통하여 NTT 형태로 변환된 다항식의 곱셈은 포인트-와이즈 곱셈으로 수행되어  $O(N \log N)$ 의 시간복잡도를 갖는다.
- [0111] 단계(1430)에서, INTT(Inverse NTT) 아키텍처가 복수의 길이(N)과 모듈러스(q)를 갖는 가변적인 파라미터의 NTT 형태의 다항식을 수신하여 원래의 형태의 다항식으로 변환한다.
- [0112] 두 다항식 곱의 파라미터, 복수의 길이(N)와 모듈러스(q)를 판단하고(1431), 복수의 길이(N)에 대하여 INTT 아키텍처의 DEMUX를 설정한다(1432). 이후, 모듈러스(q)에 대하여 PE1 및 PE2를 이용한 GS 알고리즘을 수행한다(1433).
- [0113] 본 발명의 실시예에 따른 NTT 기반의 다항식의 곱셈 장치에서 파라미터 N은  $N=2^{12}, 2^{13}, 2^{14}, 2^{15}, 2^{16}$ 으로 다양한 동형암호의 암호문의 길이를 지원하며, RNS 수체계 아래에서 지원하는 다양한 파라미터 q에 대하여  $q \equiv 1 \pmod{2N}$ 를 만족하는 모든 q에 대하여 동작이 가능하다. 동형암호는 RNS 수체계에서 Ring-LWE 기법으로 만들어진 암호체제로 복수의 파라미터 N과 q에 대하여 중복으로 표준이 설정되어 있는 암호체제로 도 14의 일련의 과정으로 다양한 파라미터 N, q를 지원하며 하드웨어를 통한 가속이 가능하다.
- [0115] 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 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.
- [0116] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

## 도면

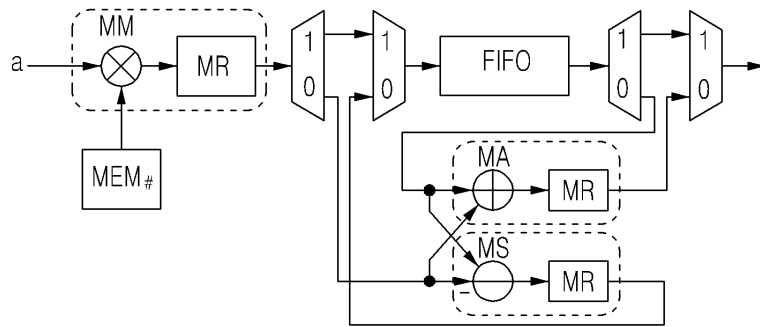
### 도면1



도면2

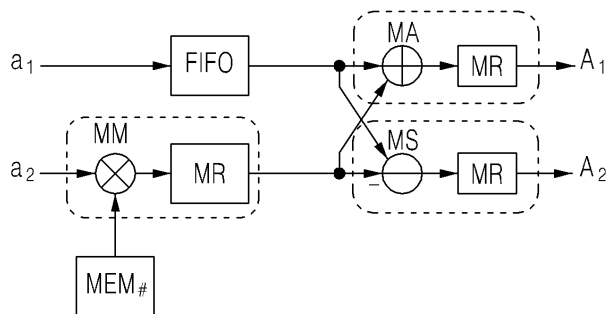


도면3



MM : Modular Multiplier  
 MA : Modular Adder  
 MS : Modular Subtractor

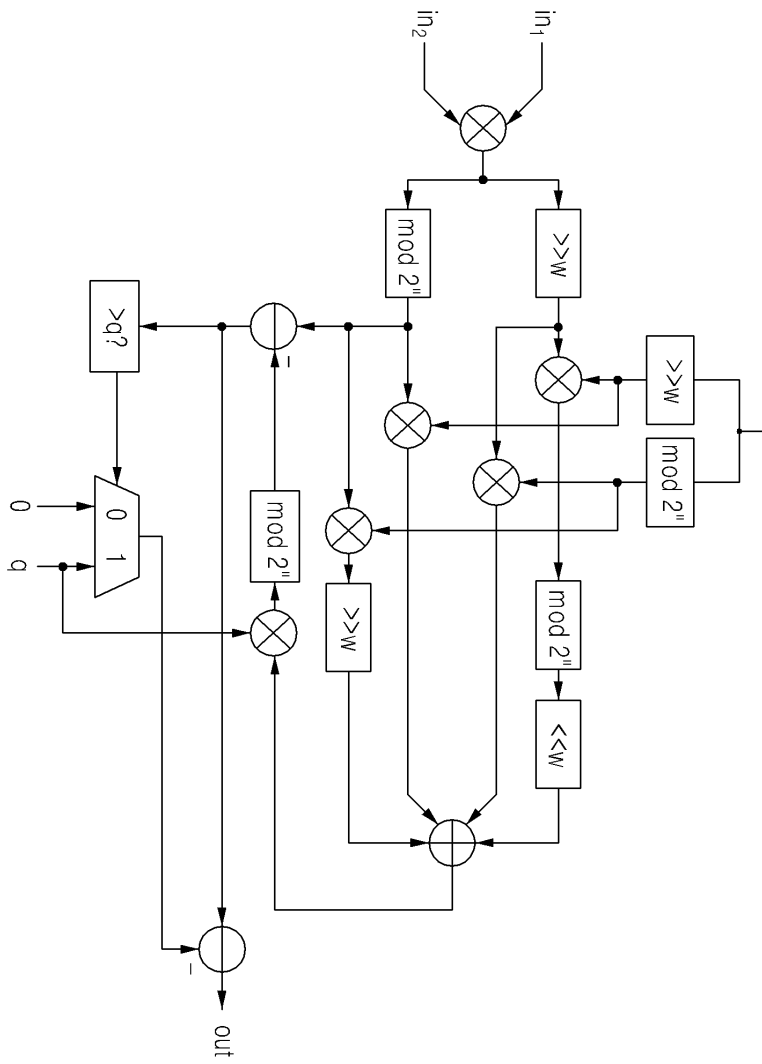
도면4



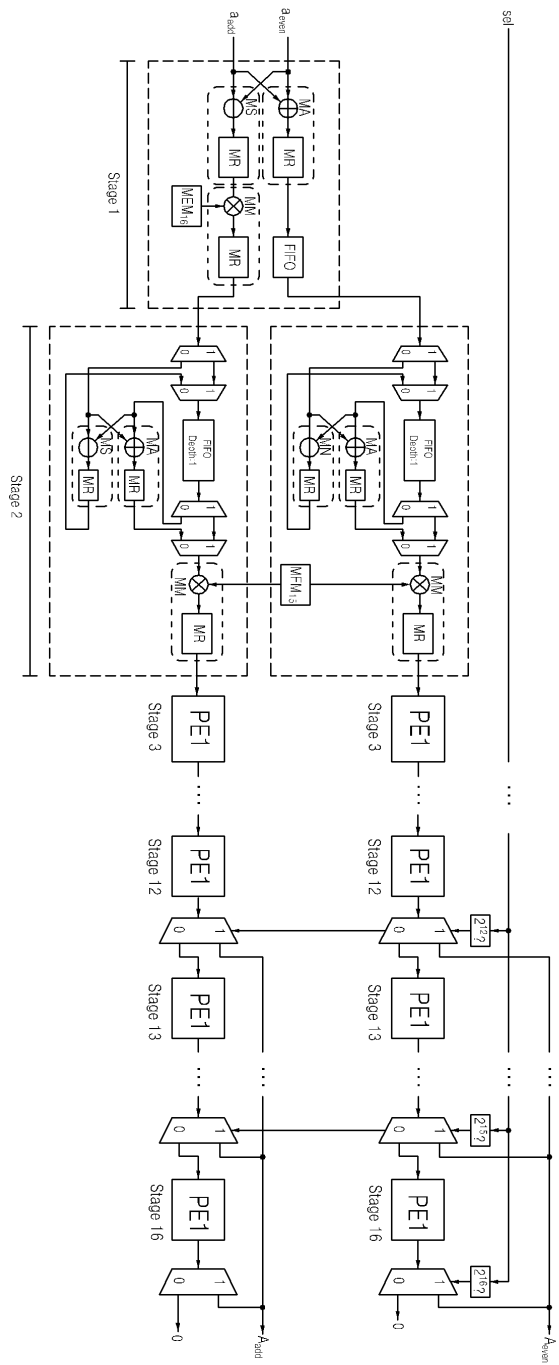
MM : Modular Multiplier  
 MA : Modular Adder  
 MS : Modular Subtractor



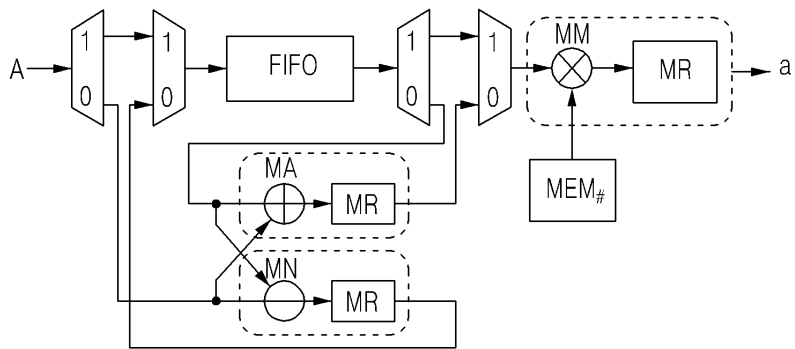
도면8



도면9

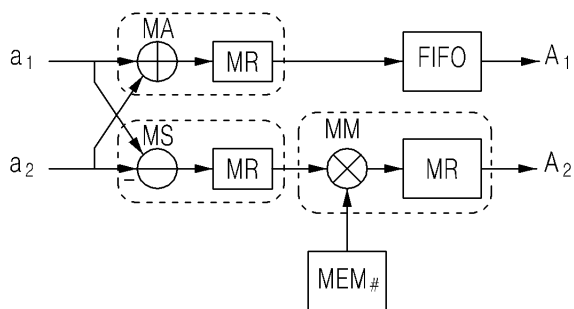


도면10



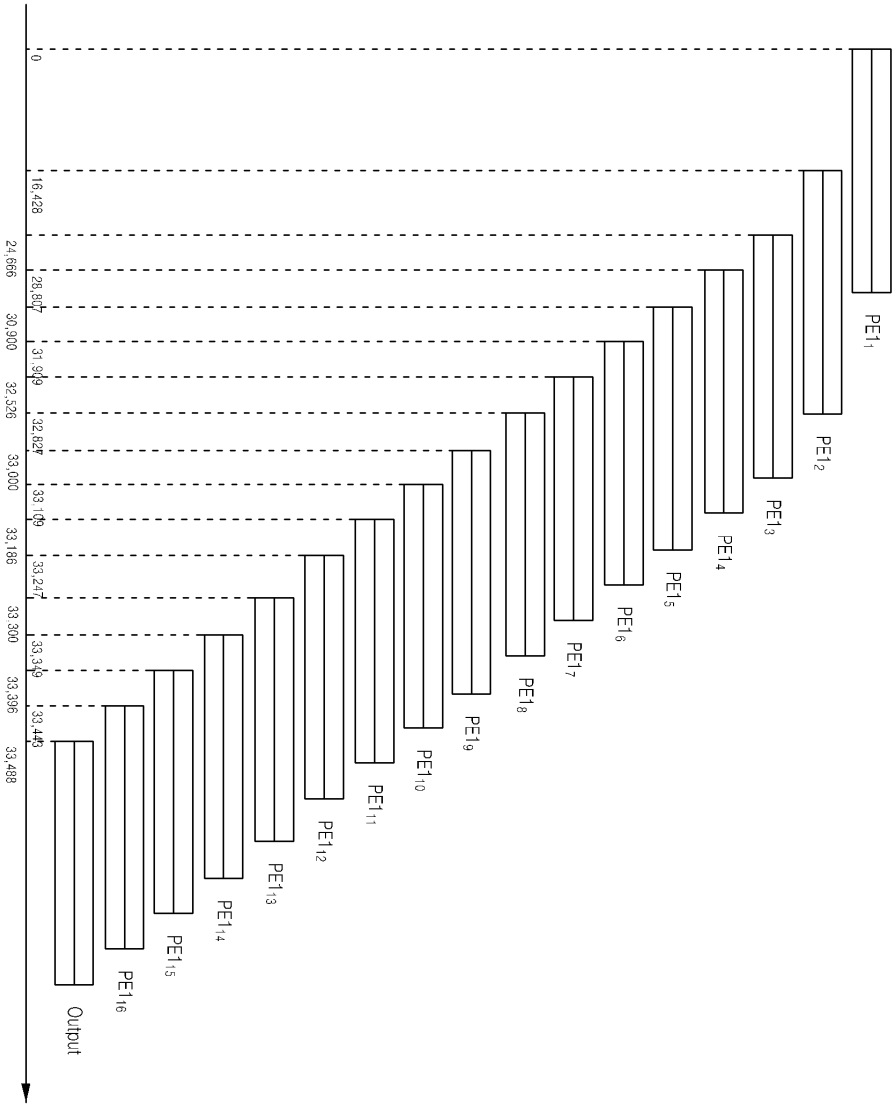
- [ MM ] : Modular Multiplier
- [ MA ] : Modular Adder
- [ MS ] : Modular Subtractor

도면11

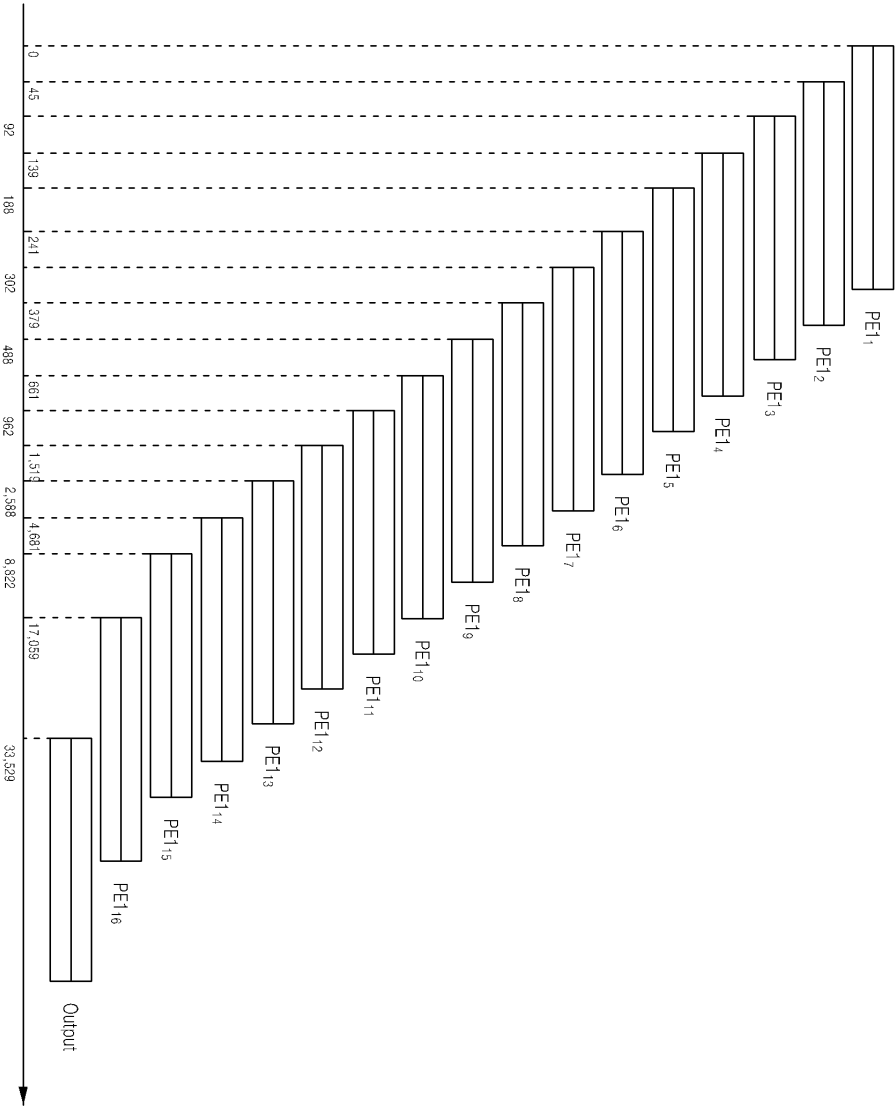


- [ MM ] : Modular Multiplier
- [ MA ] : Modular Adder
- [ MS ] : Modular Subtractor

도면12



도면13



도면14

