(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2024-0072516
(43) 공개일자 2024년05월24일

(51) 국제특허분류(Int. Cl.)
G06F 17/14 (2006.01) *G06F 7/523* (2006.01)
G06F 7/72 (2006.01)
(52) CPC특허분류
G06F 17/142 (2013.01)
G06F 7/523 (2013.01)
(21) 출원번호 10-2022-0154185
(22) 출원일자 2022년11월17일
심사청구일자 2022년11월17일

(71) 출원인
조선대학교산학협력단
광주광역시 동구 조선대길 126(서석동, 산학협력단)
(72) 발명자
김영식
광주광역시 서구 풍암2로 66 금호타운 201동 1005호
서은영
경기도 성남시 중원구 도촌남로 70-16(도촌동, 동분당 KCC스위첸파티오 1단지) 115동 102호
(74) 대리인
김효성

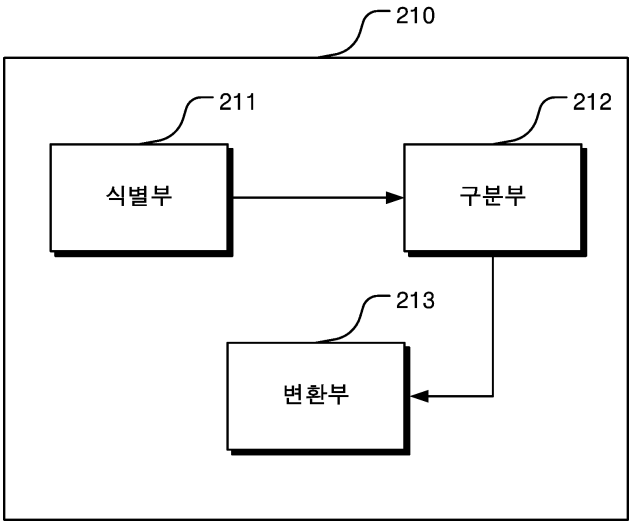
전체 청구항 수 : 총 8 항

(54) 발명의 명칭 **몽고메리 곱셈과 일반 곱셈의 혼용을 통해 다항식의 계수에 대한 NTT를 수행하는 전자 장치 및 그 동작 방법**

(57) 요 약

본 발명은 다항식의 계수에 대한 NTT(Number Theoretic Transform)를 수행하는데 있어서, 다음 단계에서 몽고메리(Montgomery) 곱셈이 수행되도록 지정된 중간 단계의 곱셈에 대해서는, 몽고메리 곱셈이 아닌 일반 곱셈을 수행하도록 연산 스케줄링을 구성함으로써, 연산의 복잡성을 줄일 수 있는 기술에 대한 것이다.

대 표 도 - 도2



(52) CPC특허분류
G06F 7/728 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 1711170177
과제번호 2021R1A2C2011082
부처명 과학기술정보통신부
과제관리(전문)기관명 한국연구재단
연구사업명 개인기초연구(과기정통부)
연구과제명 양자 내성 동형암호기반 스마트카 침입 탐지 시스템 연구
기 여 율 1/1
과제수행기관명 조선대학교
연구기간 2022.03.01 ~ 2023.02.28

명 세 서

청구범위

청구항 1

몽고메리 곱셈과 일반 곱셈의 혼용을 통해 다항식의 계수에 대한 NTT(Number Theoretic Transform)를 수행하는 전자 장치에 있어서,

최고 차수가 2^k-1(k는 2이상의 자연수임)이면서, 정수의 계수를 갖는 다항식 g(x)를 구성하는 2^k개의 계수들의 고속 푸리에 변환을 위한 적어도 하나의 기수(Radix) - 상기 적어도 하나의 기수는, 2의 거듭제곱에 해당되는 2 이상의 자연수로 지정됨 - 에 기반한 NTT의 수행 명령이 인가되면, 상기 NTT의 수행을 위해 사용되는 상기 적어도 하나의 기수에 따른 단계별 NTT 값의 연산 과정을 식별하는 식별부;

상기 적어도 하나의 기수에 따른 단계별 NTT 값의 연산 과정이, 총 t(t는 2이상의 자연수임)단계로 구성되는 것으로 식별된 경우, 상기 t단계의 연산 과정들 각각에 대해, 몽고메리(Montgomery) 곱셈을 수행할 연산 과정과 일반 곱셈을 수행할 연산 과정으로 구분하는 구분부; 및

상기 t단계의 연산 과정들을, 첫 번째 단계를 시작으로 하여 t번째 단계까지 순차적으로 수행함으로써, 상기 2^k개의 계수들에 대응되는 2^k개의 NTT 값들을 생성하되, 각 단계별로, 몽고메리 곱셈을 수행해야 할 연산 과정으로 지정된 연산 과정에 대해서는 곱셈 연산을 몽고메리 곱셈으로 수행하고, 일반 곱셈을 수행해야 할 연산 과정으로 지정된 연산 과정에 대해서는 곱셈 연산을 일반 곱셈으로 수행하는 변환부

를 포함하는 전자 장치.

청구항 2

제1항에 있어서,

상기 구분부는

상기 t단계의 연산 과정들 중, 어느 한 단계의 연산 과정이 몽고메리 곱셈을 수행할 연산 과정으로 지정되는 경우, 다음 단계의 연산 과정을 일반 곱셈을 수행할 연산 과정으로 지정하고, 어느 한 단계의 연산 과정이 일반 곱셈을 수행할 연산 과정으로 지정되는 경우, 다음 단계의 연산 과정을 몽고메리 곱셈을 수행할 연산 과정으로 지정하는 방식으로, 상기 t단계의 연산 과정들 각각에 대해, 몽고메리 곱셈을 수행할 연산 과정과 일반 곱셈을 수행할 연산 과정을 번갈아 가면서 지정함으로써, 상기 t단계의 연산 과정들 각각을, 몽고메리 곱셈을 수행할 연산 과정과 일반 곱셈을 수행할 연산 과정으로 구분하는 것을 특징으로 하는 전자 장치.

청구항 3

제2항에 있어서,

상기 구분부는

상기 t단계의 연산 과정들 중, 마지막 t번째 단계의 연산 과정에 대해서는 무조건 몽고메리 곱셈을 수행할 연산 과정으로 지정하는 것을 특징으로 하는 전자 장치.

청구항 4

몽고메리 곱셈과 일반 곱셈의 혼용을 통해 다항식의 계수에 대한 NTT(Number Theoretic Transform)를 수행하는 전자 장치의 동작 방법에 있어서,

최고 차수가 2^k-1(k는 2이상의 자연수임)이면서, 정수의 계수를 갖는 다항식 g(x)를 구성하는 2^k개의 계수들의 고속 푸리에 변환을 위한 적어도 하나의 기수(Radix) - 상기 적어도 하나의 기수는, 2의 거듭제곱에 해당되는 2 이상의 자연수로 지정됨 - 에 기반한 NTT의 수행 명령이 인가되면, 상기 NTT의 수행을 위해 사용되는 상기 적어도 하나의 기수에 따른 단계별 NTT 값의 연산 과정을 식별하는 단계;

상기 적어도 하나의 기수에 따른 단계별 NTT 값의 연산 과정이, 총 t(t는 2이상의 자연수임)단계로 구성되는 것으로 식별된 경우, 상기 t단계의 연산 과정들 각각에 대해, 몽고메리(Montgomery) 곱셈을 수행할 연산 과정과 일반 곱셈을 수행할 연산 과정으로 구분하는 단계; 및

상기 t단계의 연산 과정들을, 첫 번째 단계를 시작으로 하여 t번째 단계까지 순차적으로 수행함으로써, 상기 2^k개의 계수들에 대응되는 2^k개의 NTT 값들을 생성하되, 각 단계별로, 몽고메리 곱셈을 수행해야 할 연산 과정으로 지정된 연산 과정에 대해서는 곱셈 연산을 몽고메리 곱셈으로 수행하고, 일반 곱셈을 수행해야 할 연산 과정으로 지정된 연산 과정에 대해서는 곱셈 연산을 일반 곱셈으로 수행하는 단계

를 포함하는 전자 장치의 동작 방법.

청구항 5

제4항에 있어서,

상기 구분하는 단계는

상기 t단계의 연산 과정들 중, 어느 한 단계의 연산 과정이 몽고메리 곱셈을 수행할 연산 과정으로 지정되는 경우, 다음 단계의 연산 과정을 일반 곱셈을 수행할 연산 과정으로 지정하고, 어느 한 단계의 연산 과정이 일반 곱셈을 수행할 연산 과정으로 지정되는 경우, 다음 단계의 연산 과정을 몽고메리 곱셈을 수행할 연산 과정으로 지정하는 방식으로, 상기 t단계의 연산 과정들 각각에 대해, 몽고메리 곱셈을 수행할 연산 과정과 일반 곱셈을 수행할 연산 과정을 번갈아 가면서 지정함으로써, 상기 t단계의 연산 과정들 각각을, 몽고메리 곱셈을 수행할 연산 과정과 일반 곱셈을 수행할 연산 과정으로 구분하는 것을 특징으로 하는 전자 장치의 동작 방법.

청구항 6

제5항에 있어서,

상기 구분하는 단계는

상기 t단계의 연산 과정들 중, 마지막 t번째 단계의 연산 과정에 대해서는 무조건 몽고메리 곱셈을 수행할 연산 과정으로 지정하는 것을 특징으로 하는 전자 장치의 동작 방법.

청구항 7

제4항 내지 제6항 중 어느 한 항의 방법을 컴퓨터와의 결합을 통해 실행시키기 위한 컴퓨터 프로그램을 기록한 컴퓨터 판독 가능 기록 매체.

청구항 8

제4항 내지 제6항 중 어느 한 항의 방법을 컴퓨터와의 결합을 통해 실행시키기 위한 저장매체에 저장된 컴퓨터 프로그램.

발명의 설명

기 술 분 야

[0001] 본 발명은 몽고메리 곱셈과 일반 곱셈의 혼용을 통해 다항식의 계수에 대한 NTT(Number Theoretic Transform)를 수행하는 전자 장치 및 그 동작 방법에 대한 것이다.

배 경 기 술

[0002] 최근, 컴퓨터 시스템의 성능이 고도화됨에 따라, 보다 강화된 암호화 시스템에 대한 도입이 필요한 실정이다.

[0003] 이와 관련해서, 다항식을 이용하여 데이터의 암복호화를 수행함으로써, 해커의 공격에 보다 고차원적으로 대응할 수 있는 암호화 시스템들이 등장하고 있다.

[0004] 이러한 다항식을 이용한 암복호화 시스템에서는 다항식들 간의 곱셈 연산을 수행하는 경우가 많다. 다만, 다항식들 간의 곱셈 연산은 다항식의 차수가 높을수록 복잡한 연산 과정이 수반된다는 점에서, 다항식들 간의 곱셈 연산을 보다 손쉽게 하기 위해서, 이산 푸리에 변환을 이용하는 방법이 많이 활용되고 있다.

[0005] 예컨대, $f(x) = f_0 + f_1x + ... + f_{N-1}x^{N-1}$ 라는 다항식과 $g(x) = g_0 + g_1x + ... + g_{N-1}x^{N-1}$ 라는 다항식이 있을 때, 두 다항식 간의 곱을 계산하게 되면, $(f \times g)(x) = a_0 + a_1x + ... + a_{2N-2}x^{2N-2}$ 라는 결과가 산출되게 되고, 이때, 그 계수를 구하는 식은 $a_k = \sum_{n=0}^{k} f_n g_{k-n} (\text{for } k = 0, 1, ..., 2N-2)$ 로 나타낼 수 있다.

[0006] 이러한 계수를 구하는 방식은 [f_0 f_1 ... f_{N-1}]이라는 계수 벡터와 [g_0 g_1 ... g_{N-1}]라는 계수 벡터 간의 이산 콘볼루션을 구하는 방식과 동일하기 때문에, 두 다항식의 계수 벡터에 대해, 이산 푸리에 변환을 수행함으로써, 주파수 도메인의 변환 값들을 생성한 후, 두 다항식에 대한 변환 값들을 서로 곱하고, 그 곱셈 결과를 다시 이산 푸리에 역변환하게 되면, 두 다항식의 곱셈에 대한 계수를 산출할 수 있게 된다.

[0007] 따라서, 이러한 이산 푸리에 변환을 활용한 계수 산출을 수행하게 되면, 이산 콘볼루션 연산 대신에 곱셈 연산을 활용할 수 있으므로, 높은 차수의 다항식들 간의 연산 과정에 대한 복잡성을 줄일 수 있는 장점이 있다.

[0008] 이러한 이산 푸리에 변환을 좀 더 빠르고 쉽게 수행하기 위한 방식으로 고속 푸리에 변환이 제안되었고, 다항식들 간의 연산에서는 정수 계수가 사용된다는 점에서, NTT(Number Theoretic Transform)라고 하는 고속 푸리에 변환 방식이 사용되고 있다.

[0009] NTT 중에서, Radix(기수)-2 기반의 NTT는 N개의 계수들에 대한 변환을 수행한다고 하였을 때, N개의 계수들을, 짝수번째 위치의 N/2개의 계수들과 홀수번째 위치의 N/2개의 계수들로 분해하여, 각 N/2개의 계수들에 대한 변환을 수행한 결과를 산출하고, 그 산출된 결과를 조합하여 N개의 계수들에 대응되는 변환 값을 연산하는 방식이다.

[0010] 이로 인해, N개의 계수들에 대한 NTT를 수행한다고 하였을 때, N개의 계수들을, 짝수번째 위치의 N/2개의 계수들과 홀수번째 위치의 N/2개의 계수들로 분해하고, 이를 다시 짝수번째 위치의 N/4개의 계수들과 홀수번째 위치의 N/4개의 계수들로 분해하여, 최종 2개의 계수 단위로 분해된 결과로부터 재귀적으로 변환 값들을 조합함으로써, 최종 N개의 계수들에 대한 변환 값을 산출할 수 있게 된다.

[0011] 예컨대, 도 1에 도시된 그림과 같이, (g_0, .., g_{15})까지의 16개의 계수들에 대한 Radix-2 기반의 NTT를 수행한다고 하면, (g_0, .., g_{15})로부터, 짝수번째 위치의 계수들과 홀수번째 위치의 계수들의 그룹으로 분해해 감으로써, 최종적으로 '1단계'로 표시된 부분과 같은 2개의 계수들의 그룹으로 분해할 수 있다.

[0012] 그 이후, '1단계'에서는 2개의 계수들의 그룹 각각에 대해, NTT를 수행함으로써, 2개의 계수들의 그룹 각각에 대응되는 2-포인트 NTT 값을 연산할 수 있고, '2단계'에서는 화살표로 표시한 바와 같이, '1단계'에서 산출된 2-포인트 NTT 값을 조합하여 4-포인트 NTT 값을 연산할 수 있으며, '3단계'에서는 '2단계'에서 산출된 4-포인트 NTT 값을 조합하여 8-포인트 NTT 값을 연산할 수 있고, 마지막 '4단계'에서는 '3단계'에서 산출된 8-포인트 NTT 값을 조합하여 16-포인트 NTT 값, 즉, (g_0, .., g_{15})에 대응되는 16개의 NTT 값을 산출할 수 있게 된다.

[0013] 이러한 NTT는, 전술한 Radix-2 기반의 NTT뿐 아니라, 계수들을 몇 개의 그룹으로 분해하고, 이를 조합하느냐 따라 Radix-2, Radix-4, Radix-8 등과 같은 형태로 구분해서 수행될 수 있다. 예컨대, Radix-4 기반의 NTT는, 계수들을 4개의 그룹으로 분해하고, 그룹별 NTT 값을 조합하여 NTT를 수행하는 방식이라고 볼 수 있다. 이러한 Radix-2, Radix-4, Radix-8 등의 NTT는 서로 혼용해서 사용할 수도 있다. 예컨대, Radix-2, Radix-4, Radix-2의 순서로 각 NTT 값을 연산하는 단계를 구성해서, NTT를 수행하는 방법도 활용될 수 있다.

[0014] 이러한, NTT는, 일반적인 고속 푸리에 변환과 달리, 결과 값에 대해 모듈로(modulo) 연산이 수반되어야 하고, 이러한 모듈로 연산의 수행을 위해서, NTT에서 발생하는 모든 곱셈 연산을 몽고메리(Montgomery) 곱셈으로 수행하게 되어 있다.

[0015] 몽고메리 곱셈이란, $a \bmod q$ 와 $b \bmod q$ 를 곱셈하여, $ab \bmod q$ 를 얻고자 할 때, $a \bmod q$ 와 $b \bmod q$ 를 몽고메리 상의 값인 $aR \bmod q$ 과 $bR \bmod q$ 으로 바꾸게 되면, $abR \bmod q$ 의 값을, 입력 값에 상관없이 일정한 시간에 실수 연산을 하지 않고 얻을 수 있게 해주는 곱셈 방식을 의미한다. 여기서,

R은 2^k 형태의 값을 사용하여 적절한 때에 곱셈 연산을 bitwise shift 연산으로 대신하는 것이 가능하도록 하며, $\gcd(q,R)=1$과 $R \geq q$의 조건을 만족시켜야한다. 서로 소인 두 자연수 q와 R에 대해서 extended Euclidean 알고리즘을 적용하면 $R \cdot R' + q \cdot q' = 1$을 만족하는 정수 R'와 q'이 존재한다. 여기서 R'과 q'는 R과 q의 modulo q와 modulo R에 대한 곱셈의 역원이 됨을 알 수 있다. 즉, $R \cdot R' = 1 \bmod q$ 이므로 $R' = R^{-1} \bmod q$ 이고, $q \cdot q' = 1 \bmod R$ 이므로 $q' = q^{-1} \bmod R$ 이다. 따라서, $z = a \cdot b \cdot R^2$ 이라고 할 때, $z \cdot R^{-1} \bmod q$의 값을 하기의 수학식 1의 연산에 따라 구할 수 있다.

수학식 1

[0017]
$$
\begin{aligned}
z \cdot R^{-1} \bmod q &= z \cdot R \cdot R^{-1} \cdot R^{-1} \bmod q \\
&= z \cdot (1 - q \cdot q^{-1}) \cdot R^{-1} \bmod q \\
&= (z - z \cdot q^{-1} \cdot q) \cdot R^{-1} \bmod q \\
&= (z - (((z \bmod R) \cdot q^{-1}) \bmod R) \cdot q) \cdot R^{-1} \bmod q
\end{aligned}
$$

[0019] 위와 같이 계산된 값은 항상 $-q$와 q 사이에 있는 값이라는 것을 보일 수 있기 때문에, 이런 방식으로 두 수의 곱셈에 대해 modulo q 된 값을 구할 수 있게 된다.

[0020] 몽고메리 곱셈에서 사용하는 R의 값을 선택함에 있어, $R > q^2$ 이라는 조건을 만족시키는 R을 선택할 경우, 한 번의 곱셈에서는 몽고메리 곱셈을 하지 않더라도, 두 번째 곱셈에서 몽고메리 곱셈을 실시함에 따라 그 결과로 한 번에 modulo q가 된 값을 얻을 수 있게 된다. 이것을 일반적으로 $R > q^t$의 조건으로 확장시키면, 총 t번의 곱셈을 할 때, $t-1$번의 곱셈에 대해서는 몽고메리 곱셈을 하지 않고, 마지막 한 번의 곱셈에만 몽고메리 곱셈을 적용하는 방식으로 확장시킬 수 있다.

[0021] 즉, 몽고메리 곱셈의 특성상 모든 중간 단계의 곱셈 연산에서 일일이 몽고메리 곱셈을 수행하지 않더라도, 다음 단계의 곱셈 연산에서만 몽고메리 곱셈이 수행된다면, 최종 결과 값에 대한 변동이 없기 때문에, 여러 단계의 곱셈 연산이 있을 때, 중간 단계의 곱셈 연산에서 몽고메리 곱셈을 생략하는 방법을 고려할 수 있다.

[0022] 이와 관련해서, NTT는 앞서 설명한 바와 같이, NTT를 수행하기 위한 기수(Radix)에 따라, NTT 값을 생성하기 위한 소정의 단계들로 구분되고, 하위 단계로부터 재귀적으로 상위 단계로 이어지는 연산이 수행된다는 점에서, 이러한 단계별 연산 과정에서 중간 단계의 곱셈에 대해서는 몽고메리 곱셈을 생략하더라도 최종 NTT 결과 값에 대해서는 영향을 미치지 않게 된다. 하지만, 기존의 NTT는 중간 단계의 곱셈을 포함한 모든 곱셈 연산 과정에서 몽고메리 곱셈이 수행되도록 구성되어 있다는 점에서, 연산을 위한 불필요한 비용(cost)이 발생하는 단점이 있었다.

[0023] 따라서, 다항식의 계수에 대한 NTT를 수행하는데 있어서, 중간 단계의 곱셈에 대해서는, 몽고메리 곱셈이 아닌 일반 곱셈을 수행하도록 연산 스케줄링을 구성함으로써, 연산의 복잡성을 줄일 수 있는 기술에 대한 도입을 고려할 수 있다.

발명의 내용

해결하려는 과제

[0024] 본 발명은 다항식의 계수에 대한 NTT(Number Theoretic Transform)를 수행하는데 있어서, 다음 단계에서 몽고메리(Montgomery) 곱셈이 수행되도록 지정된 중간 단계의 곱셈에 대해서는, 몽고메리 곱셈이 아닌 일반 곱셈을 수행하도록 연산 스케줄링을 구성함으로써, 연산의 복잡성을 줄일 수 있는 기술을 제시하고자 한다.

과제의 해결 수단

[0025] 본 발명의 일실시예에 따른 몽고메리 곱셈과 일반 곱셈의 혼용을 통해 다항식의 계수에 대한 NTT(Number Theoretic Transform)를 수행하는 전자 장치는 최고 차수가 2^k-1(k는 2이상의 자연수임)이면서, 정수의 계수를 갖는 다항식 g(x)를 구성하는 2^k개의 계수들의 고속 푸리에 변환을 위한 적어도 하나의 기수(Radix) - 상기 적어도 하나의 기수는, 2의 거듭제곱에 해당되는 2이상의 자연수로 지정됨 - 에 기반한 NTT의 수행 명령이 인가되면, 상기 NTT의 수행을 위해 사용되는 상기 적어도 하나의 기수에 따른 단계별 NTT 값의 연산 과정을 식별하는 식별부, 상기 적어도 하나의 기수에 따른 단계별 NTT 값의 연산 과정이, 총 t(t는 2이상의 자연수임)단계로 구성되는 것으로 식별된 경우, 상기 t단계의 연산 과정들 각각에 대해, 몽고메리(Montgomery) 곱셈을 수행할 연산 과정과 일반 곱셈을 수행할 연산 과정으로 구분하는 구분부 및 상기 t단계의 연산 과정들을, 첫 번째 단계를 시작으로 하여 t번째 단계까지 순차적으로 수행함으로써, 상기 2^k개의 계수들에 대응되는 2^k개의 NTT 값들을 생성하되, 각 단계별로, 몽고메리 곱셈을 수행해야 할 연산 과정으로 지정된 연산 과정에 대해서는 곱셈 연산을 몽고메리 곱셈으로 수행하고, 일반 곱셈을 수행해야 할 연산 과정으로 지정된 연산 과정에 대해서는 곱셈 연산을 일반 곱셈으로 수행하는 변환부를 포함한다.

[0026] 또한, 본 발명의 일실시예에 따른 몽고메리 곱셈과 일반 곱셈의 혼용을 통해 다항식의 계수에 대한 NTT를 수행하는 전자 장치의 동작 방법은 최고 차수가 2^k-1(k는 2이상의 자연수임)이면서, 정수의 계수를 갖는 다항식 g(x)를 구성하는 2^k개의 계수들의 고속 푸리에 변환을 위한 적어도 하나의 기수(Radix) - 상기 적어도 하나의 기수는, 2의 거듭제곱에 해당되는 2이상의 자연수로 지정됨 - 에 기반한 NTT의 수행 명령이 인가되면, 상기 NTT의 수행을 위해 사용되는 상기 적어도 하나의 기수에 따른 단계별 NTT 값의 연산 과정을 식별하는 단계, 상기 적어도 하나의 기수에 따른 단계별 NTT 값의 연산 과정이, 총 t(t는 2이상의 자연수임)단계로 구성되는 것으로 식별된 경우, 상기 t단계의 연산 과정들 각각에 대해, 몽고메리 곱셈을 수행할 연산 과정과 일반 곱셈을 수행할 연산 과정으로 구분하는 단계 및 상기 t단계의 연산 과정들을, 첫 번째 단계를 시작으로 하여 t번째 단계까지 순차적으로 수행함으로써, 상기 2^k개의 계수들에 대응되는 2^k개의 NTT 값들을 생성하되, 각 단계별로, 몽고메리 곱셈을 수행해야 할 연산 과정으로 지정된 연산 과정에 대해서는 곱셈 연산을 몽고메리 곱셈으로 수행하고, 일반 곱셈을 수행해야 할 연산 과정으로 지정된 연산 과정에 대해서는 곱셈 연산을 일반 곱셈으로 수행하는 단계를 포함한다.

발명의 효과

[0027] 본 발명은 다항식의 계수에 대한 NTT(Number Theoretic Transform)를 수행하는데 있어서, 다음 단계에서 몽고메리(Montgomery) 곱셈이 수행되도록 지정된 중간 단계의 곱셈에 대해서는, 몽고메리 곱셈이 아닌 일반 곱셈을 수행하도록 연산 스케줄링을 구성함으로써, 연산의 복잡성을 줄일 수 있는 기술을 제시할 수 있다.

도면의 간단한 설명

[0028] 도 1은 Radix 2 기반의 NTT(Number Theoretic Transform)를 설명하기 위한 도면이다.

도 2는 본 발명의 일실시예에 따른 몽고메리 곱셈과 일반 곱셈의 혼용을 통해 다항식의 계수에 대한 NTT를 수행하는 전자 장치의 구조를 도시한 도면이다.

도 3은 본 발명의 일실시예에 따른 몽고메리 곱셈과 일반 곱셈의 혼용을 통해 다항식의 계수에 대한 NTT를 수행하는 전자 장치의 동작 방법을 도시한 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0029] 이하에서는 본 발명에 따른 실시예들을 첨부된 도면을 참조하여 상세하게 설명하기로 한다. 이러한 설명은 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 각 도면을 설명하면서 유사한 참조부호를 유사한 구

성요소에 대해 사용하였으며, 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 본 명세서 상에서 사용되는 모든 용어들은 본 발명이 속하는 기술분야에서 통상의 지식을 가진 사람에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다.

[0030] 본 문서에서, 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있다는 것을 의미한다. 또한, 본 발명의 다양한 실시예들에 있어서, 각 구성요소들, 기능 블록들 또는 수단들은 하나 또는 그 이상의 하부 구성요소로 구성될 수 있고, 각 구성요소들이 수행하는 전기, 전자, 기계적 기능들은 전자회로, 집적회로, ASIC(Application Specific Integrated Circuit) 등 공지된 다양한 소자들 또는 기계적 요소들로 구현될 수 있으며, 각각 별개로 구현되거나 2 이상이 하나로 통합되어 구현될 수도 있다.

[0031] 한편, 첨부된 블록도의 블록들이나 흐름도의 단계들은 범용 컴퓨터, 특수용 컴퓨터, 휴대용 노트북 컴퓨터, 네트워크 컴퓨터 등 데이터 프로세싱이 가능한 장비의 프로세서나 메모리에 탑재되어 지정된 기능들을 수행하는 컴퓨터 프로그램 명령들(instructions)을 의미하는 것으로 해석될 수 있다. 이들 컴퓨터 프로그램 명령들은 컴퓨터 장치에 구비된 메모리 또는 컴퓨터에서 판독 가능한 메모리에 저장될 수 있기 때문에, 블록도의 블록들 또는 흐름도의 단계들에서 설명된 기능들은 이를 수행하는 명령 수단을 내포하는 제조물로 생산될 수도 있다. 아울러, 각 블록 또는 각 단계는 특정된 논리적 기능(들)을 실행하기 위한 하나 이상의 실행 가능한 명령들을 포함하는 모듈, 세그먼트 또는 코드의 일부를 나타낼 수 있다. 또, 몇 가지 대체 가능한 실시예들에서는 블록들 또는 단계들에서 언급된 기능들이 정해진 순서와 달리 실행되는 것도 가능함을 주목해야 한다. 예컨대, 잇달아 도시되어 있는 두 개의 블록들 또는 단계들은 실질적으로 동시에 수행되거나, 역순으로 수행될 수 있으며, 경우에 따라 일부 블록들 또는 단계들이 생략된 채로 수행될 수도 있다.

[0032] 도 2는 본 발명의 일실시예에 따른 몽고메리 곱셈과 일반 곱셈의 혼용을 통해 다항식의 계수에 대한 NTT를 수행하는 전자 장치의 구조를 도시한 도면이다.

[0033] 도 2를 참조하면, 본 발명에 따른 전자 장치(210)는 식별부(211), 구분부(212) 및 변환부(213)를 포함한다.

[0034] 식별부(211)는 최고 차수가 2^k-1(k는 2이상의 자연수임)이면서, 정수의 계수를 갖는 다항식 g(x)를 구성하는 2^k개의 계수들의 고속 푸리에 변환을 위한 적어도 하나의 기수(Radix)(상기 적어도 하나의 기수는, 2의 거듭제곱에 해당되는 2이상의 자연수로 지정됨)에 기반한 NTT의 수행 명령이 인가되면, 상기 NTT의 수행을 위해 사용되는 상기 적어도 하나의 기수에 따른 단계별 NTT 값의 연산 과정을 식별한다.

[0035] 예컨대, k를 4라고 하고, 이때의 다항식 g(x)를 $g(x) = g_0 + g_1x + \ldots + g_{15}x^{15}$ 라고 가정하자. 이때, 전자 장치(110) 상에, (g_0, .., g_{15})라는 계수들의 고속 푸리에 변환을 위한 Radix-2 기반의 NTT 수행 명령이 인가되었다고 하는 경우, 식별부(211)는 상기 NTT의 수행을 위해 사용되는 기수인 'Radix-2'에 따른 단계별 NTT 값의 연산 과정을 식별할 수 있다.

[0036] 이때, Radix-2 기반의 NTT는 도 1에 도시된 그림과 같이, 1단계부터 4단계까지로 구분되는 2-포인트 NTT 값의 연산 과정(1단계), 4-포인트 NTT 값의 연산 과정(2단계), 8-포인트 NTT 값의 연산 과정(3단계), 16-포인트 NTT 값의 연산 과정(4단계)으로 구분되기 때문에, 식별부(211)는 4단계로 구분되는 NTT 값의 연산 과정을 식별할 수 있다.

[0037] 이러한 방식으로, 식별부(211)는 적어도 하나의 기수에 기반한 NTT의 수행 명령이 인가되면, 상기 NTT의 수행을 위해 사용되는 상기 적어도 하나의 기수에 따른 단계별 NTT 값의 연산 과정을 식별할 수 있다. 전술한 예에서는 Radix-2 기반의 NTT 수행 명령이 인가되었을 경우의 식별부(211)의 동작을 예를 든 것으로서, 만약, 전자 장치(110) 상에 Radix-4, Radix-8 등에 따른 NTT 수행 명령이 인가되었다고 하는 경우, 식별부(211)는 해당 기수에 따른 단계별 NTT 값의 연산 과정을 식별할 수 있다. 또한, 상기 다항식 g(x)에 대해서, 전자 장치(110) 상에, 1단계에서는 Radix-2로, 2단계에서는 Radix-4로, 3단계에서는 Radix-2로 NTT를 수행하도록 하는 것과 같이, 둘 이상의 기수에 따라 NTT 값을 연산하도록 하는 명령이 인가되었다고 하는 경우, 식별부(211)는 'Radix-2+Radix-4+Radix-2'라고 하는 기수에 따라서 구분될 수 있는, 2-포인트 NTT 값의 연산 과정(1단계, Radix-2), 8-포인트 NTT 값의 연산 과정(2단계, Radix-4), 16-포인트 NTT 값의 연산 과정(3단계, Radix-2)을 식별할 수 있다.

[0038] 이와 관련해서, 사용자는 상기 다항식 g(x)의 차수를 고려해서, NTT를 수행하기 위한 각 단계별 기수를 적절하게 선택하여, 본 발명의 전자 장치(110) 상에 입력할 수 있다. 앞서 설명한 바와 같이, 사용자는 Radix-2,

Radix-4, Radix-8 등과 같이 단일의 기수에 기반한 NTT 수행 명령을 전자 장치(110)에 인가할 수도 있고, 각 단계별로 Radix-2, Radix-4, Radix-8 등을 적절히 조합하여 NTT가 수행되도록 하는 명령을 전자 장치(110) 상에 인가할 수 있다. 본 발명에서는 Radix-2 만으로 구성된 NTT 수행 명령을 전자 장치(110) 상에 인가하는 것보다, Radix-4 이상의 크기를 갖는 기수를 어느 하나 이상의 단계에 포함시킨 형태의 NTT 수행 명령을 전자 장치(110) 상에 인가하는 것이 바람직하다.

[0039] 이렇게, 식별부(211)에 의해, 상기 적어도 하나의 기수에 따른 단계별 NTT 값의 연산 과정이 식별된 결과, 상기 적어도 하나의 기수에 따른 단계별 NTT 값의 연산 과정이, 총 t(t는 2이상의 자연수임)단계로 구성되는 것으로 식별된 경우, 구분부(212)는 상기 t단계의 연산 과정들 각각에 대해, 몽고메리(Montgomery) 곱셈을 수행할 연산 과정과 일반 곱셈을 수행할 연산 과정으로 구분한다.

[0040] 이때, 본 발명의 일실시예에 따르면, 구분부(212)는 상기 t단계의 연산 과정들 중, 어느 한 단계의 연산 과정이 몽고메리 곱셈을 수행할 연산 과정으로 지정되는 경우, 다음 단계의 연산 과정을 일반 곱셈을 수행할 연산 과정으로 지정하고, 어느 한 단계의 연산 과정이 일반 곱셈을 수행할 연산 과정으로 지정되는 경우, 다음 단계의 연산 과정을 몽고메리 곱셈을 수행할 연산 과정으로 지정하는 방식으로, 상기 t단계의 연산 과정들 각각에 대해, 몽고메리 곱셈을 수행할 연산 과정과 일반 곱셈을 수행할 연산 과정을 번갈아 가면서 지정함으로써, 상기 t단계의 연산 과정들 각각을, 몽고메리 곱셈을 수행할 연산 과정과 일반 곱셈을 수행할 연산 과정으로 구분할 수 있다.

[0041] 또한, 본 발명의 일실시예에 따르면, 구분부(212)는 상기 t단계의 연산 과정들 중, 마지막 t번째 단계의 연산 과정에 대해서는 무조건 몽고메리 곱셈을 수행할 연산 과정으로 지정할 수 있다.

[0042] 관련해서, 도 1의 예와 같이, NTT 값의 연산 과정이 1단계, 2단계, 3단계, 4단계 연산 과정으로 구성되어 있다고 하는 경우, 구분부(212)는 1단계 연산 과정을 일반 곱셈을 수행할 연산 과정으로 지정하고, 2단계 연산 과정을 몽고메리 곱셈을 수행할 연산 과정으로 지정하며, 3단계 연산 과정을 일반 곱셈을 수행할 연산 과정으로 지정할 수 있다. 그리고, 4단계 연산 과정은 마지막 연산 과정이므로, 구분부(212)는 4단계 연산 과정을 몽고메리 곱셈을 수행할 연산 과정으로 지정할 수 있다.

[0043] 아울러, 구분부(212)는 위의 예시와 반대로, 1단계 연산 과정을 몽고메리 곱셈을 수행할 연산 과정으로 지정하고, 2단계 연산 과정을 일반 곱셈을 수행할 연산 과정으로 지정하며, 3단계 연산 과정을 몽고메리 곱셈을 수행할 연산 과정으로 지정할 수 있다. 그리고, 4단계 연산 과정은 마지막 연산 과정이므로, 구분부(212)는 4단계 연산 과정을 몽고메리 곱셈을 수행할 연산 과정으로 지정할 수 있다.

[0044] 이렇게, 구분부(212)는 상기 t단계의 연산 과정들 각각에 대해, 몽고메리 곱셈을 수행할 연산 과정과 일반 곱셈을 수행할 연산 과정을 번갈아 가면서 지정하되, 마지막 t번째 단계의 연산 과정에 대해서는 무조건 몽고메리 곱셈을 수행할 연산 과정으로 지정함으로써, 상기 t단계의 연산 과정들 각각을, 몽고메리 곱셈을 수행할 연산 과정과 일반 곱셈을 수행할 연산 과정으로 구분할 수 있다.

[0045] 이렇게, 구분부(212)에 의해, 상기 t단계의 연산 과정들 각각에 대한 몽고메리 곱셈 또는 일반 곱셈을 수행할 연산 과정으로의 구분이 완료되면, 변환부(213)는 상기 t단계의 연산 과정들을, 첫 번째 단계를 시작으로 하여 t번째 단계까지 순차적으로 수행함으로써, 상기 2^k개의 계수들에 대응되는 2^k개의 NTT 값들을 생성하되, 각 단계별로, 몽고메리 곱셈을 수행해야 할 연산 과정으로 지정된 연산 과정에 대해서는 곱셈 연산을 몽고메리 곱셈으로 수행하고, 일반 곱셈을 수행해야 할 연산 과정으로 지정된 연산 과정에 대해서는 곱셈 연산을 일반 곱셈으로 수행한다.

[0046] 관련해서, 도 1의 예와 같이, NTT 값의 연산 과정이 1단계, 2단계, 3단계, 4단계 연산 과정으로 구성되어 있다고 하고, 구분부(212)에 의해, 1단계 연산 과정은 일반 곱셈을 수행할 연산 과정으로 지정되었고, 2단계 연산 과정은 몽고메리 곱셈을 수행할 연산 과정으로 지정되었으며, 3단계 연산 과정은 일반 곱셈을 수행할 연산 과정으로 지정되었고, 4단계 연산 과정은 몽고메리 곱셈을 수행할 연산 과정으로 지정되었다고 하는 경우, 변환부(213)는 1단계, 2단계, 3단계, 4단계 연산 과정을 순차적으로 수행함으로써, 16개의 계수들에 대응되는 16개의 NTT 값들을 생성하되, 1단계 연산 과정에서는 곱셈 연산을 일반 곱셈으로 수행하고, 2단계 연산 과정에서는 곱셈 연산을 몽고메리 곱셈으로 수행하며, 3단계 연산 과정에서는 곱셈 연산을 일반 곱셈으로 수행하고, 4단계 연산 과정에서는 곱셈 연산을 몽고메리 곱셈으로 수행할 수 있다.

[0047] 도 3은 본 발명의 일실시예에 따른 몽고메리 곱셈과 일반 곱셈의 혼용을 통해 다항식의 계수에 대한 NTT를 수행

하는 전자 장치의 동작 방법을 도시한 순서도이다.

[0048] 단계(S310)에서는 최고 차수가 2^k-1(k는 2이상의 자연수임)이면서, 정수의 계수를 갖는 다항식 g(x)를 구성하는 2^k개의 계수들의 고속 푸리에 변환을 위한 적어도 하나의 기수(상기 적어도 하나의 기수는, 2의 거듭제곱에 해당되는 2이상의 자연수로 지정됨)에 기반한 NTT의 수행 명령이 인가되면, 상기 NTT의 수행을 위해 사용되는 상기 적어도 하나의 기수에 따른 단계별 NTT 값의 연산 과정을 식별한다.

[0049] 단계(S320)에서는 상기 적어도 하나의 기수에 따른 단계별 NTT 값의 연산 과정이, 총 t(t는 2이상의 자연수임) 단계로 구성되는 것으로 식별된 경우, 상기 t단계의 연산 과정들 각각에 대해, 몽고메리 곱셈을 수행할 연산 과정과 일반 곱셈을 수행할 연산 과정으로 구분한다.

[0050] 단계(S330)에서는 상기 t단계의 연산 과정들을, 첫 번째 단계를 시작으로 하여 t번째 단계까지 순차적으로 수행함으로써, 상기 2^k개의 계수들에 대응되는 2^k개의 NTT 값들을 생성하되, 각 단계별로, 몽고메리 곱셈을 수행해야 할 연산 과정으로 지정된 연산 과정에 대해서는 곱셈 연산을 몽고메리 곱셈으로 수행하고, 일반 곱셈을 수행해야 할 연산 과정으로 지정된 연산 과정에 대해서는 곱셈 연산을 일반 곱셈으로 수행한다.

[0051] 이때, 본 발명의 일실시예에 따르면, 단계(S320)에서는 상기 t단계의 연산 과정들 중, 어느 한 단계의 연산 과정이 몽고메리 곱셈을 수행할 연산 과정으로 지정되는 경우, 다음 단계의 연산 과정을 일반 곱셈을 수행할 연산 과정으로 지정하고, 어느 한 단계의 연산 과정이 일반 곱셈을 수행할 연산 과정으로 지정되는 경우, 다음 단계의 연산 과정을 몽고메리 곱셈을 수행할 연산 과정으로 지정하는 방식으로, 상기 t단계의 연산 과정들 각각에 대해, 몽고메리 곱셈을 수행할 연산 과정과 일반 곱셈을 수행할 연산 과정을 번갈아 가면서 지정함으로써, 상기 t단계의 연산 과정들 각각을, 몽고메리 곱셈을 수행할 연산 과정과 일반 곱셈을 수행할 연산 과정으로 구분할 수 있다.

[0052] 또한, 본 발명의 일실시예에 따르면, 단계(S320)에서는 상기 t단계의 연산 과정들 중, 마지막 t번째 단계의 연산 과정에 대해서는 무조건 몽고메리 곱셈을 수행할 연산 과정으로 지정할 수 있다.

[0053] 이상, 도 3을 참조하여 본 발명의 일실시예에 따른 전자 장치의 동작 방법에 대해 설명하였다. 여기서, 본 발명의 일실시예에 따른 전자 장치의 동작 방법은 도 2를 이용하여 설명한 전자 장치(210)의 동작에 대한 구성과 대응될 수 있으므로, 이에 대한 보다 상세한 설명은 생략하기로 한다.

[0054] 본 발명의 일실시예에 따른 전자 장치의 동작 방법은 컴퓨터와의 결합을 통해 실행시키기 위한 저장매체에 저장된 컴퓨터 프로그램으로 구현될 수 있다.

[0055] 또한, 본 발명의 일실시예에 따른 전자 장치의 동작 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 본 발명을 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.

[0056] 이상과 같이 본 발명에서는 구체적인 구성 요소 등과 같은 특정 사항들과 한정된 실시예 및 도면에 의해 설명되었으나 이는 본 발명의 보다 전반적인 이해를 돕기 위해서 제공된 것일 뿐, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상적인 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다.

[0057] 따라서, 본 발명의 사상은 설명된 실시예에 국한되어 정해져서는 아니되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등하거나 등가적 변형이 있는 모든 것들은 본 발명 사상의 범주에 속한다고 할 것이다.

부호의 설명

[0058] 210: 전자 장치

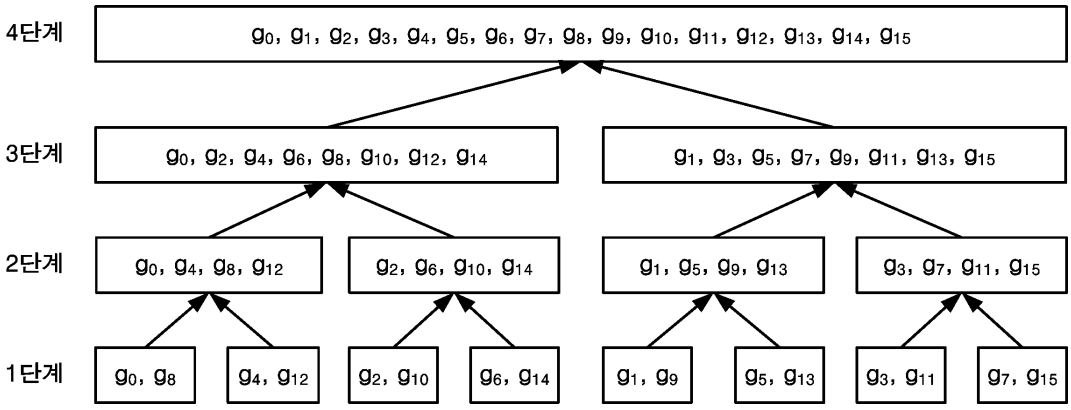
211: 식별부

212: 구분부

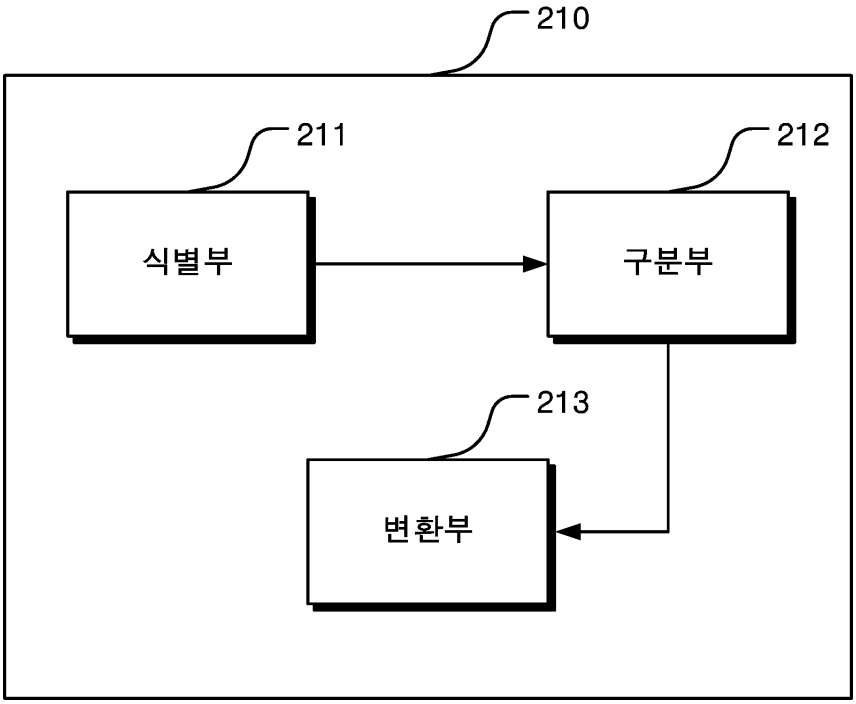
213: 변환부

도면

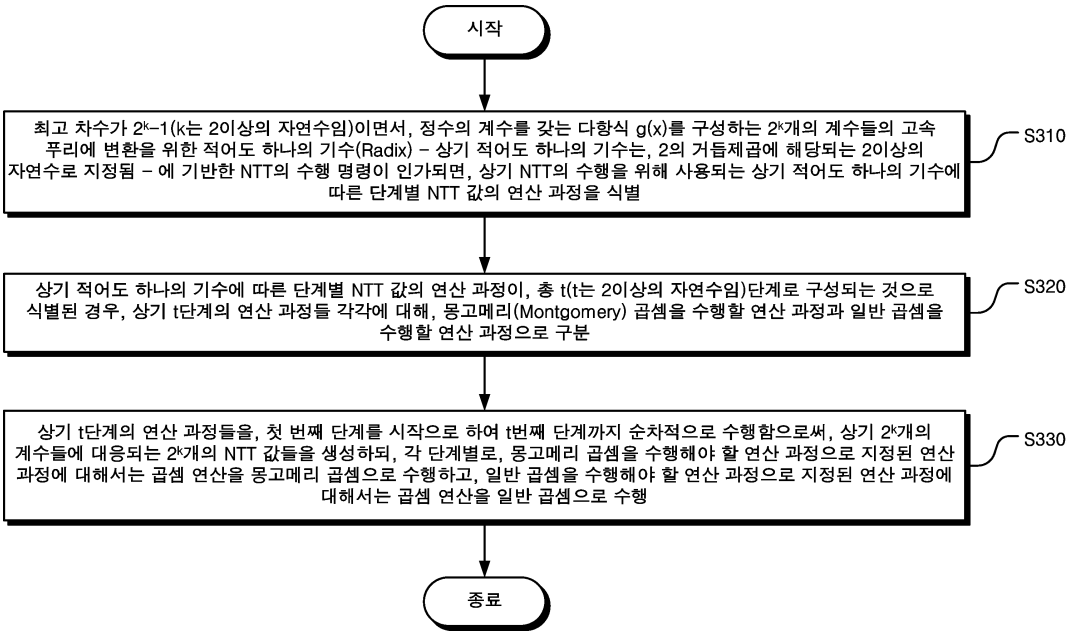
도면1



도면2



도면3


시작
최고 차수가 2^k−1(k는 2이상의 자연수임)이면서, 정수의 계수를 갖는 다항식 g(x)를 구성하는 2^k개의 계수들의 고속 푸리에 변환을 위한 적어도 하나의 기수(Radix) - 상기 적어도 하나의 기수는, 2의 거듭제곱에 해당되는 2이상의 자연수로 지정됨 - 에 기반한 NTT의 수행 명령이 인가되면, 상기 NTT의 수행을 위해 사용되는 상기 적어도 하나의 기수에 따른 단계별 NTT 값의 연산 과정을 식별
S310
상기 적어도 하나의 기수에 따른 단계별 NTT 값의 연산 과정이, 총 t(t는 2이상의 자연수임)단계로 구성되는 것으로 식별된 경우, 상기 t단계의 연산 과정들 각각에 대해, 몽고메리(Montgomery) 곱셈을 수행할 연산 과정과 일반 곱셈을 수행할 연산 과정으로 구분
S320
상기 t단계의 연산 과정들을, 첫 번째 단계를 시작으로 하여 t번째 단계까지 순차적으로 수행함으로써, 상기 2^k개의 계수들에 대응되는 2^k개의 NTT 값들을 생성하되, 각 단계별로, 몽고메리 곱셈을 수행해야 할 연산 과정으로 지정된 연산 과정에 대해서는 곱셈 연산을 몽고메리 곱셈으로 수행하고, 일반 곱셈을 수행해야 할 연산 과정으로 지정된 연산 과정에 대해서는 곱셈 연산을 일반 곱셈으로 수행
S330
종료