



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0104195
(43) 공개일자 2020년09월03일

(51) 국제특허분류(Int. Cl.)
G06F 17/11 (2006.01) G06F 7/544 (2017.01)
(52) CPC특허분류
G06F 17/11 (2013.01)
G06F 7/544 (2018.05)
(21) 출원번호 10-2019-0039752
(22) 출원일자 2019년04월04일
심사청구일자 2019년04월04일
(30) 우선권주장
1020190022400 2019년02월26일 대한민국(KR)

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
홍석희
서울특별시 노원구 덕릉로71길 30, 206-2304 (중계동, 양지대림아파트)
김수리
서울특별시 동대문구 왕산로 86, 오피스텔동 1806호(용두동, 동대문 푸르지오시티))
(74) 대리인
윤귀상

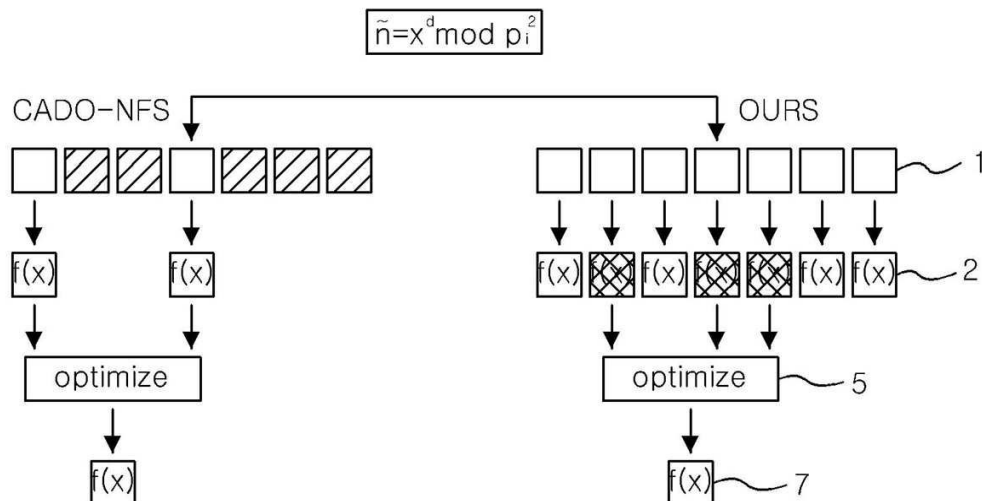
전체 청구항 수 : 총 12 항

(54) 발명의 명칭 다항식 선택 방법, 이를 수행하기 위한 기록매체, 다항식 선택 장치 및 이를 포함하는 GNFS 방식의 인수분해 연산기

(57) 요약

GNFS(General Number Field Sieve) 방식에 따라 인수분해를 하는 인수분해 연산기에 포함되어 인수분해 하는 수(N)에서 1차 다항식(g(x))과 공통근을 갖는 2차 이상의 다항식(f(x))을 선택하는 다항식 선택 장치에서의 다항식 선택 방법에 있어서, 상기 1차 다항식(g(x)) 및 상기 2차 이상의 다항식(f(x))의 계수들을 변수로 하는 방정식의 근을 산출하여 적어도 하나의 상기 2차 이상의 다항식(f(x))을 생성하는 다항식 생성 단계 및 생성한 상기 2차 이상의 다항식(f(x))의 lognorm 값에 따라 생성한 상기 2차 이상의 다항식(f(x)) 중 상기 GNFS 방식의 시빙 단계에 사용할 다항식을 선택하여 lognorm 값을 변형시키는 다항식 최적화 단계를 포함하는 다항식 선택 방법을 개시한다.

대표도 - 도2



이 발명을 지원한 국가연구개발사업

과제고유번호	2014-6-00910
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기술진흥센터
연구사업명	정보보호핵심원천기술개발(R&D)
연구과제명	(안전성 연구 3세부) 암호 소프트웨어 안전성 연구
기 여 율	1/1
과제수행기관명	고려대학교 산학협력단
연구기간	2014.07.01 ~ 2019.06.30

명세서

청구범위

청구항 1

GNFS(General Number Field Sieve) 방식에 따라 인수분해를 하는 인수분해 연산기에 포함되어 인수분해 하는 수 (N)에서 1차 다항식($g(x)$)과 공통근을 갖는 2차 이상의 다항식($f(x)$)을 선택하는 다항식 선택 장치에서의 다항식 선택 방법에 있어서,

상기 1차 다항식($g(x)$) 및 상기 2차 이상의 다항식($f(x)$)의 계수들을 변수로 하는 방정식의 근을 산출하여 적어도 하나의 상기 2차 이상의 다항식($f(x)$)을 생성하는 다항식 생성 단계; 및

생성한 상기 2차 이상의 다항식($f(x)$)의 lognorm 값에 따라 생성한 상기 2차 이상의 다항식($f(x)$) 중 상기 GNFS 방식의 시빙 단계에 사용할 다항식을 선택하여 lognorm 값을 변형시키는 다항식 최적화 단계를 포함하는 다항식 선택 방법.

청구항 2

제1항에 있어서,

상기 다항식 생성 단계는,

중국인의 나머지 정리(CRT: Chinese Remainder Theorem)를 적용하여 상기 1차 다항식($g(x)$) 및 상기 2차 이상의 다항식($f(x)$)의 계수들을 변수로 하는 방정식의 근을 산출하는 단계를 포함하는 다항식 선택 방법.

청구항 3

제1항에 있어서,

상기 다항식 최적화 단계는,

생성한 상기 2차 이상의 다항식($f(x)$) 중 lognorm 값이 작은 미리 설정된 개수의 다항식을 상기 GNFS 방식의 시빙 단계에 사용할 다항식으로 선택하는 단계를 포함하는 다항식 선택 방법.

청구항 4

제3항에 있어서,

상기 다항식 최적화 단계는,

LLL(Lenstra-Lenstra-Lovasz) reduction 알고리즘을 이용하여 상기 GNFS 방식의 시빙 단계에 사용할 다항식의 lognorm 값을 변형시키는 단계를 포함하는 다항식 선택 방법.

청구항 5

제4항에 있어서,

상기 다항식 최적화 단계는,

Minkoski's bound에 기반하여 상기 GNFS 방식의 시빙 단계에 사용할 각 다항식의 계수를 기저로 하여 생성되는 래티스(L)에서 0이 아닌 가장 작은 벡터를 찾아 상기 GNFS 방식의 시빙 단계에 사용할 각 다항식의 lognorm 값을 변형시키는 단계를 포함하는 다항식 선택 방법.

청구항 6

제1항 내지 제5항 중 어느 하나의 항에 따른 다항식 선택 방법을 수행하기 위한, 컴퓨터 프로그램이 기록된 컴퓨터로 판독 가능한 기록 매체.

청구항 7

GNFS(General Number Field Sieve) 방식에 따라 인수분해를 하는 인수분해 연산기에 포함되어 인수분해 하는 수 (N)에서 1차 다항식($g(x)$)과 공통근을 갖는 2차 이상의 다항식($f(x)$)을 선택하는 다항식 선택 장치에 있어서,

상기 1차 다항식($g(x)$) 및 상기 2차 이상의 다항식($f(x)$)의 계수들을 변수로 하는 방정식의 근을 산출하여 적어도 하나의 상기 2차 이상의 다항식($f(x)$)을 생성하는 다항식 생성부; 및

생성한 상기 2차 이상의 다항식($f(x)$)의 lognorm 값에 따라 생성한 상기 2차 이상의 다항식($f(x)$) 중 상기 GNFS 방식의 시빙 단계에 사용할 다항식을 선택하여 lognorm 값을 변형시키는 다항식 최적화부를 포함하는 다항식 선택 장치.

청구항 8

제7항에 있어서,

상기 다항식 생성부는,

중국인의 나머지 정리(CRT: Chinese Remainder Theorem)를 적용하여 상기 1차 다항식($g(x)$) 및 상기 2차 이상의 다항식($f(x)$)의 계수들을 변수로 하는 방정식의 근을 산출하는 다항식 선택 장치.

청구항 9

제7항에 있어서,

상기 다항식 최적화부는,

생성한 상기 2차 이상의 다항식($f(x)$) 중 lognorm 값이 작은 미리 설정된 개수의 다항식을 상기 GNFS 방식의 시빙 단계에 사용할 다항식으로 선택하는 다항식 선택 장치.

청구항 10

제9항에 있어서,

상기 다항식 최적화부는,

LLL(Lenstra-Lenstra-Lovasz) reduction 알고리즘을 이용하여 상기 GNFS 방식의 시빙 단계에 사용할 다항식의 lognorm 값을 변형시키는 다항식 선택 장치.

청구항 11

제10항에 있어서,

상기 다항식 최적화부는,

Minkoski's bound에 기반하여 상기 GNFS 방식의 시빙 단계에 사용할 각 다항식의 계수를 기저로 하여 생성되는 래티스(L)에서 0이 아닌 가장 작은 벡터를 찾아 상기 GNFS 방식의 시빙 단계에 사용할 각 다항식의 lognorm 값을 변형시키는 다항식 선택 장치.

청구항 12

제7항 내지 제11항 중 어느 하나의 항에 따른 다항식 선택 장치를 포함하는 GNFS(General Number Field Sieve) 방식의 인수분해 연산기.

발명의 설명

기술 분야

본 발명은 다항식 선택 방법, 이를 수행하기 위한 기록매체, 다항식 선택 장치 및 이를 포함하는 GNFS(General Number Field Sieve) 방식의 인수분해 연산기에 관한 것으로, 더욱 상세하게는 translation-rotation에 적합한 다항식 선택 방법, 이를 수행하기 위한 기록매체, 다항식 선택 장치 및 이를 포함하는 GNFS 방식의 인수분해 연산기에 관한 것이다.

배경 기술

- [0002] GNFS(General Number Field Sieve) 방식은 인수분해 및 이산대수 문제를 해결하는 가장 효율적인 방법으로 알려져 있으며, 다항식 선택, 시빙, 행렬연산, 제곱근 계산의 4 단계로 구성되어있다.
- [0003] GNFS 방식의 4 단계에서 다항식 선택 단계가 가장 중요하다 할 수 있는데, 인수분해하기 적합한 다항식을 선택해야 시빙 단계가 효율적이며 행렬 연산도 적합하다.
- [0004] 이러한 다항식 선택 방법으로 Kleinjung의 알고리즘이 있다. Kleinjung 알고리즘에 따르면 인수분해 하는 수에 대해 translation을 이용하여 함수값이 작은 다항식을 선택하고, rotation 과정을 이용하여 시빙 단계에 효율적일 확률이 높은 다항식을 생성하는 방식이다.
- [0005] 즉, Kleinjung 알고리즘에 따르면 collision 방식에 따라 인수분해 하는 수 N에 대해 공통근(m)을 갖는 다항식 $g(x)$ 및 $f(x)$ 의 계수들을 변수로 하는 방정식($\tilde{n} \equiv x^d \bmod p_i^2$)의 근(x)을 일부 산출하고, 산출한 일부 근을 이용하여 d차 다항식 $f(x)$ 를 생성하며, 생성한 다항식을 모두 최적화하여 최종 다항식을 선택한다.
- [0006] 이와 같은 경우, 인수분해 하는 수 N에 대해 공통근(m)을 갖는 다항식 $g(x)$ 및 $f(x)$ 의 계수들을 변수로 하는 방정식($\tilde{n} \equiv x^d \bmod p_i^2$)의 다른 근으로부터는 다항식이 생성될 수 없으며, 실제로 RSA 암호 시스템 중 하나인 RSA-768에서 collision 방식에 따라 산출되지 않은 근으로부터 생성된 다항식이 인수분해에 사용됨이 확인된 바 있다.

발명의 내용

해결하려는 과제

- [0007] 본 발명의 일측면은 중국인의 나머지 정리(CRT: Chinese Remainder Theorem)를 이용하여 다항식을 생성하고, 생성한 다항식 중 일부 다항식에 한하여 LLL(Lenstra-Lenstra-Lovasz) reduction 알고리즘을 적용한 최적화 단계를 진행하는 다항식 선택 방법, 이를 수행하기 위한 기록매체, 다항식 선택 장치 및 이를 포함하는 GNFS 방식의 인수분해 연산기를 제공한다.
- [0008] 본 발명의 기술적 과제는 이상에서 언급한 기술적 과제로 제한되지 않으며, 언급되지 않은 또 다른 기술적 과제들은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

- [0009] 상기 과제를 해결하기 위한 본 발명의 다항식 선택 방법은 GNFS(General Number Field Sieve) 방식에 따라 인수분해를 하는 인수분해 연산기에 포함되어 인수분해 하는 수(N)에서 1차 다항식($g(x)$)과 공통근을 갖는 2차 이상의 다항식($f(x)$)을 선택하는 다항식 선택 장치에서의 다항식 선택 방법에 있어서, 상기 1차 다항식($g(x)$) 및 상기 2차 이상의 다항식($f(x)$)의 계수들을 변수로 하는 방정식의 근을 산출하여 적어도 하나의 상기 2차 이상의 다항식($f(x)$)을 생성하는 다항식 생성 단계 및 생성한 상기 2차 이상의 다항식($f(x)$)의 lognorm 값에 따라 생성한 상기 2차 이상의 다항식($f(x)$) 중 상기 GNFS 방식의 시빙 단계에 사용할 다항식을 선택하여 lognorm 값을 변형시키는 다항식 최적화 단계를 포함한다.
- [0010] 한편, 상기 다항식 생성 단계는, 중국인의 나머지 정리(CRT: Chinese Remainder Theorem)를 적용하여 상기 1차 다항식($g(x)$) 및 상기 2차 이상의 다항식($f(x)$)의 계수들을 변수로 하는 방정식의 근을 산출하는 단계를 포함할 수 있다.
- [0011] 또한, 상기 다항식 최적화 단계는, 생성한 상기 2차 이상의 다항식($f(x)$) 중 lognorm 값이 작은 미리 설정된 개수의 다항식을 상기 GNFS 방식의 시빙 단계에 사용할 다항식으로 선택하는 단계를 포함할 수 있다.
- [0012] 또한, 상기 다항식 최적화 단계는, LLL(Lenstra-Lenstra-Lovasz) reduction 알고리즘을 이용하여 상기 GNFS 방식의 시빙 단계에 사용할 다항식의 lognorm 값을 변형시키는 단계를 포함할 수 있다.
- [0013] 또한, 상기 다항식 최적화 단계는, Minkoski's bound에 기반하여 상기 GNFS 방식의 시빙 단계에 사용할 각 다항식의 계수를 기저로 하여 생성되는 래티스(L)에서 0이 아닌 가장 작은 벡터를 찾아 상기 GNFS 방식의 시빙 단계에 사용할 각 다항식의 lognorm 값을 변형시키는 단계를 포함할 수 있다.
- [0014] 또한, 상기 다항식 선택 방법을 수행하기 위한, 컴퓨터 프로그램이 기록된 컴퓨터로 판독 가능한 기록 매체일 수 있다.

- [0015] 한편, 본 발명의 다항식 선택 장치는 GNFS(General Number Field Sieve) 방식에 따라 인수분해를 하는 인수분해 연산기에 포함되어 인수분해 하는 수(N)에서 1차 다항식($g(x)$)과 공통근을 갖는 2차 이상의 다항식($f(x)$)을 선택하는 다항식 선택 장치에 있어서, 상기 1차 다항식($g(x)$) 및 상기 2차 이상의 다항식($f(x)$)의 계수들을 변수로 하는 방정식의 근을 산출하여 적어도 하나의 상기 2차 이상의 다항식($f(x)$)을 생성하는 다항식 생성부 및 생성한 상기 2차 이상의 다항식($f(x)$)의 lognorm 값에 따라 생성한 상기 2차 이상의 다항식($f(x)$) 중 상기 GNFS 방식의 시빙 단계에 사용할 다항식을 선택하여 lognorm 값을 변형시키는 다항식 최적화부를 포함한다.
- [0016] 한편, 상기 다항식 생성부는, 중국인의 나머지 정리(CRT: Chinese Remainder Theorem)를 적용하여 상기 1차 다항식($g(x)$) 및 상기 2차 이상의 다항식($f(x)$)의 계수들을 변수로 하는 방정식의 근을 산출할 수 있다.
- [0017] 또한, 상기 다항식 최적화부는, 생성한 상기 2차 이상의 다항식($f(x)$) 중 lognorm 값이 작은 미리 설정된 개수의 다항식을 상기 GNFS 방식의 시빙 단계에 사용할 다항식으로 선택할 수 있다.
- [0018] 또한, 상기 다항식 최적화부는, LLL(Lenstra-Lenstra-Lovasz) reduction 알고리즘을 이용하여 상기 GNFS 방식의 시빙 단계에 사용할 다항식의 lognorm 값을 변형시킬 수 있다.
- [0019] 또한, 상기 다항식 최적화부는, Minkowski's bound에 기반하여 상기 GNFS 방식의 시빙 단계에 사용할 각 다항식의 계수를 기저로 하여 생성되는 래티스(L)에서 0이 아닌 가장 작은 벡터를 찾아 상기 GNFS 방식의 시빙 단계에 사용할 각 다항식의 lognorm 값을 변형시킬 수 있다.
- [0020] 또한, 상기 다항식 선택 장치를 포함하는 GNFS(General Number Field Sieve) 방식의 인수분해 연산기일 수 있다.

발명의 효과

- [0021] 본 발명에 따르면 기존 Kleinjung의 알고리즘이 구현된 CADO-NFS 2.1.1 보다 더 높은 Murphy E를 가지는 다항식을 선택할 수 있으며, LLL을 이용한 다항식 최적화 기법이 적용된 CADO-NFS 2.3.0에 비해서도 효율적인 다항식을 선택할 수 있다. 아울러 시빙 단계에서 이러한 다항식을 이용하는 경우 GNFS 방식의 전반적인 속도를 단축할 수 있을 것이다.

도면의 간단한 설명

- [0022] 도 1은 본 발명의 일 실시예에 따른 다항식 선택 장치의 블록도이다.
- 도 2는 본 발명의 일 실시예에 따른 다항식 선택 장치에서의 다항식 선택 방법을 개략적으로 보여주는 도면이다.
- 도 3은 다항식의 lognorm과 Murphy E 값의 관계를 보여주는 도면이다.
- 도 4는 본 발명의 일 실시예에 따른 다항식 선택 방법의 흐름도이다.

발명을 실시하기 위한 구체적인 내용

- [0023] 후술하는 본 발명에 대한 상세한 설명은, 본 발명이 실시될 수 있는 특정 실시예를 예시로서 도시하는 첨부 도면을 참조한다. 이들 실시예는 당업자가 본 발명을 실시할 수 있기에 충분하도록 상세히 설명된다. 본 발명의 다양한 실시예는 서로 다르지만 상호 배타적일 필요는 없음이 이해되어야 한다. 예를 들어, 여기에 기재되어 있는 특정 형상, 구조 및 특성은 일 실시예와 관련하여 본 발명의 정신 및 범위를 벗어나지 않으면서 다른 실시예로 구현될 수 있다. 또한, 각각의 개시된 실시예 내의 개별 구성요소의 위치 또는 배치는 본 발명의 정신 및 범위를 벗어나지 않으면서 변경될 수 있음이 이해되어야 한다. 따라서, 후술하는 상세한 설명은 한정적인 의미로서 취하려는 것이 아니며, 본 발명의 범위는, 적절하게 설명된다면, 그 청구항들이 주장하는 것과 균등한 모든 범위와 더불어 첨부된 청구항에 의해서만 한정된다. 도면에서 유사한 참조부호는 여러 측면에 걸쳐서 동일하거나 유사한 기능을 지칭한다.
- [0024] 이하, 도면들을 참조하여 본 발명의 바람직한 실시예들을 보다 상세하게 설명하기로 한다.
- [0026] 도 1은 본 발명의 일 실시예에 따른 다항식 선택 장치의 블록도이다.
- [0027] 도 1을 참조하면, 본 발명의 일 실시예에 따른 다항식 선택 장치(1000)는 다항식 생성부(10) 및 다항식 최적화

부(20)를 포함한다.

- [0028] 본 발명의 일 실시예에 따른 다항식 선택 장치(1000)는 도 1에 도시된 구성요소보다 많은 구성요소에 의해 구현될 수 있고, 그보다 적은 구성요소에 의해 구현될 수도 있다.
- [0029] 본 발명의 일 실시예에 따른 다항식 선택 장치(1000)는 정보의 입출력이 가능한 장치로, GNFS 방식의 인수분해 방법에서의 다항식 선택 단계를 진행하기 위한 소프트웨어(애플리케이션)가 설치되어 실행될 수 있으며, 도 1에 도시된 다항식 생성부(10) 및 다항식 최적화부(20)는 본 발명의 일 실시예에 따른 다항식 선택 장치(1000)에서 실행되는 소프트웨어에 의해 제어될 수 있다.
- [0030] 본 발명의 일 실시예에 따른 다항식 선택 장치(1000)는 GNFS(General Number Field Sieve) 방식의 인수분해 연산기의 일 구성으로 포함될 수 있다. GNFS는 현재까지 알려진 가장 효율적인 인수분해 방법으로, 다항식 선택, 시빙, 행렬연산 및 제곱근 계산의 4 단계로 이루어진다. 예를 들면, GNFS 방식의 인수분해 연산기는 GNFS를 기반으로 구현된 공개 소프트웨어에 의해 실행되는 CADO-NFS일 수 있으며, 이는 널리 사용되는 공개키 암호 알고리즘 중 하나인 RSA 암호 시스템에 적용될 수 있다. 본 발명의 일 실시예에 따른 다항식 선택 장치(1000)는 이러한 GNFS 방식의 인수분해 연산기의 일 구성으로 포함되어 다항식 선택 단계를 진행할 수 있을 것이다.
- [0031] 본 발명의 일 실시예에 따른 다항식 선택 장치(1000)는 인수분해 하는 수 N (modular N)에서 공통근(m)을 갖는 서로 다른 두 다항식($f(x)$ 및 $g(x)$)을 선택할 수 있다. 이를 수식으로 나타내면 본 발명의 일 실시예에 따른 다항식 선택 장치(1000)는 $f(m) \equiv g(m) \equiv 0 \pmod{N}$ 을 만족하는 $f(x)$ 및 $g(x)$ 를 선택할 수 있다. 일반적으로 인수분해 문제의 다항식 선택에 있어서 $g(x)$ 는 1차 다항식으로 선택하고, $f(x)$ 는 2차 이상의 다항식으로 선택할 수 있다. 즉, $g(x) = m_2x - m_1$ 이라 하면, d 차 다항식 $f(x)$ 는 $N = \sum_{i=1}^d c_i m_1^i m_2^{d-i}$ 를 만족하는 c_i 를 각 차항의 계수로 하여 나타낼 수 있다.
- [0032] 본 발명의 일 실시예에 따른 다항식 선택 장치(1000)는 중국인의 나머지 정리(CRT: Chinese Remainder Theorem)를 이용하여 다항식 $f(x)$ 및 $g(x)$ 의 계수들을 변수로 하는 방정식의 근($\tilde{n} \equiv r^d \pmod{m_2^2}$ 를 만족하는 r)을 산출하고, 산출한 근에 대한 다항식 $f(x)$ 및 $g(x)$ 를 생성할 수 있다.
- [0033] 그리고 본 발명의 일 실시예에 따른 다항식 선택 장치(1000)는 생성한 d 차 다항식 $f(x)$ 중 GNFS 방식의 시빙 단계에 사용할 다항식을 선택할 수 있다. 이때 본 발명의 일 실시예에 따른 다항식 선택 장치(1000)는 d 차 다항식 $f(x)$ 의 $\log\text{norm}(\text{raw}-\log\text{norm})$ 가 작을수록 Murphy E 값이 크다는 사실에 기인하여 시빙 단계에 사용할 다항식을 선택할 수 있다. Murphy E 값은 시빙 단계의 효율성을 나타내는 지표로, 이와 관련한 구체적인 설명은 후술한다.
- [0034] 본 발명의 일 실시예에 따른 다항식 선택 장치(1000)는 선택한 다항식 $f(x)$ 에 한하여 LLL(Lenstra-Lenstra-Lovasz) reduction 알고리즘에 따라 최적화를 진행할 수 있다.
- [0035] 이와 같은 본 발명의 일 실시예에 따른 다항식 선택 장치(1000)에 따라 선택되는 다항식은 높은 Murphy E 값을 기록할 수 있으며, 시빙 단계에서 이러한 다항식을 이용하는 경우 GNFS 방식의 전반적인 속도를 단축할 수 있을 것이다.
- [0036] 이하 도 2 및 도 3을 참조하여, 도 1에 도시된 본 발명의 일 실시예에 따른 다항식 선택 장치(1000)의 각 구성요소에 대해 구체적으로 설명한다.
- [0037] 도 2는 본 발명의 일 실시예에 따른 다항식 선택 장치에서의 다항식 선택 방법을 개략적으로 보여주는 도면이고, 도 3은 다항식의 $\log\text{norm}$ 과 Murphy E 값의 관계를 보여주는 도면이다.
- [0038] 도 2를 참조하면, 다항식 생성부(10)는 인수분해 하는 수 N 에서 1차 다항식 $g(x)$ 와 공통근(m)을 갖는 적어도 하나의 d 차 다항식 $f(x)$ 를 생성할 수 있다. 예를 들면, 다항식 생성부(10)는 인수분해 하는 수 N 에 대해 공통근(m)을 갖는 다항식 $g(x)$ 및 $f(x)$ 의 계수들을 변수로 하는 방정식($\tilde{n} \equiv x^d \pmod{p_i^2}$)의 근(x)(1)을 모두 산출하고, 모든 근(1)을 이용하여 d 차 다항식 $f(x)$ (2)를 생성할 수 있다.
- [0039] 그리고, 다항식 최적화부(20)는 다항식 생성부(10)에서 생성하는 적어도 하나의 d 차 다항식 $f(x)$ (2) 중 GNFS 방식의 시빙 단계에 사용할 다항식을 선택하고, 선택한 다항식에 한하여 시빙 단계의 효율성 향상을 위해 최적화 단계(5)를 진행하여 시빙 단계에 사용할 d 차 다항식 $f(x)$ (7)을 최종 선택할 수 있다.
- [0040] 한편, 종래의 GNFS를 기반으로 구현된 공개 소프트웨어에 의해 실행되는 CADO-NFS에서의 다항식 선택 단계를 살

퍼보면, collision 방식에 따라 인수분해 하는 수 N 에 대해 공통근(m)을 갖는 다항식 $g(x)$ 및 $f(x)$ 의 계수들을 변수로 하는 방정식($\tilde{n} \equiv x^d \bmod p_i^2$)의 근(x)(1)을 일부 산출하고, 산출한 일부 근(1)을 이용하여 d 차 다항식 $f(x)$ (2)를 생성하며, 생성한 다항식을 모두 최적화하여 최종 다항식(7)을 선택한다.

[0041] 이와 같은 경우, 인수분해 하는 수 N 에 대해 공통근(m)을 갖는 다항식 $g(x)$ 및 $f(x)$ 의 계수들을 변수로 하는 방정식($\tilde{n} \equiv x^d \bmod p_i^2$)의 다른 근으로부터는 다항식이 생성될 수 없으며, 실제로 RSA 암호 시스템 중 하나인 RSA-768에서 collision 방식에 따라 산출되지 않은 근으로부터 생성된 다항식이 인수분해에 사용됨이 확인된 바 있다.

[0042] 반면, 본 발명의 일 실시예에 따른 다항식 선택 장치(1000)는 인수분해 하는 수 N 에 대해 공통근(m)을 갖는 다항식 $g(x)$ 및 $f(x)$ 의 계수들을 변수로 하는 방정식($\tilde{n} \equiv x^d \bmod p_i^2$)의 모든 근에 대하여 다항식을 생성하되, 그 중 일부 다항식을 최적화하여 최종 다항식을 선택하므로, RSA-768의 인수분해에 사용되는 다항식을 선택할 수 있음은 물론 그 효율을 높일 수 있다.

[0043] 구체적으로는, 다항식 생성부(10)는 인수분해 하는 수를 N 이라 하면, modular N 에서 공통근(m)을 갖는 1차 다항식 $g(x)$ 및 2차 이상의 d 차 다항식 $f(x)$ 를 생성할 수 있다. 이를 수식으로 나타내면, 다항식 생성부(10)는 $f(m) \equiv g(m) \equiv 0 \bmod N$ 을 만족하는 $f(x)$ 및 $g(x)$ 를 생성할 수 있다.

[0044] 여기서, $g(x) = m_2x - m_1$ 이라 하면, d 차 다항식 $f(x)$ 는 $N = \sum_{i=1}^d c_i m_1^i m_2^{d-i}$ 를 만족하는 c_i 를 각 차항의 계수로 하여 나타낼 수 있으며, 인수분해 하는 수 $N = \sum_{i=1}^d c_i m_1^i m_2^{d-i}$ 를 전개하면 아래 수학적 식 1과 같이 나타낼 수 있다.

수학적 식 1

$$N = c_d \left(m_1^d + \frac{c_{d-1}}{c_d} m_1^{d-1} m_2 \right) + \sum_{i=0}^{d-2} c_i m_1^i m_2^{d-i}$$

[0046] 수학적 식 1에서 c_i 는 다항식 $f(x)$ 의 각 차항의 계수, d 는 다항식 $f(x)$ 의 최고 차수, m_1 및 m_2 는 각각 $g(x) = m_2x - m_1$ 를 만족하는 값을 의미한다.

[0047] 여기서, $c_d \left(m_1 + \frac{c_{d-1}}{dc_d} m_2 \right)^d = c_d m_1^d + c_{d-1} m_1^{d-1} m_2 + m_2^2 R_0$ 라 하고, $R_0 = c_d \sum_{i=2}^d \binom{d}{i} m_1^{d-i} \left(\frac{c_{d-1}}{dc_d} m_2 \right)^i$ 라 하면, 수학적 식 1은 아래 수학적 식 2와 같이 나타낼 수 있다.

수학적 식 2

$$d^d c_d^{d-1} N = (c_d d m_1 + c_{d-1} m_2)^2 - d^d c_d^{d-1} m_2^2 R_0 + d^d c_d^{d-1} \sum_{i=0}^{d-2} c_i m_1^i m_2^{d-i}$$

[0049] GNFS 방식에 따르면 $\tilde{n} = d^d c_d^{d-1} N$ 이 주어지며, $\tilde{m} = d c_d m_1 + c_{d-1} m_2$ 이라 하면, 수학적 식 2는 임의의 $\tilde{R}$ 에 대해 아래 수학적 식 3과 같이 나타낼 수 있다.

수학적 식 3

$$\tilde{n} \equiv \tilde{m}^d + m_2^2 \tilde{R} \bmod m_2^2$$

[0051] 다항식 생성부(10)는 GNFS 방식에서 주어지는 $\tilde{n} = d^d c_d^{d-1} N$ 에 대해 중국인의 나머지 정리(CRT)를 이용하여 수학적 식 3을 만족하는 $\tilde{m}$ 및 m_2 를 산출할 수 있다.

- [0052] 중국인의 나머지 정리(CRT)에 대해 간략히 설명하면, 한 정수 x 에 대해 다른 정수들로 나눈 나머지를 알면 x 는 유일해를 갖는다는 정리로, 예를 들면, $x \equiv a_1 \bmod p_1, x \equiv a_2 \bmod p_2, \dots, x \equiv a_n \bmod p_n$ 의 근($a_1, a_2, \dots, a_n$)을 알면 x 는 $\bmod p_1 p_2 \dots p_n$ 에 대해 유일하게 결정된다는 정리이다.
- [0053] 수학식 3은 $\tilde{n} \equiv r^d \bmod m_2^2$ 와 같이 간략히 나타낼 수 있는데, 다항식 생성부(10)는 GNFS 방식에서 주어지는 $\tilde{n} = d^d c_d^{d-1} N$ 에 대해 $\tilde{n} \equiv r^d \bmod m_2^2$ 를 만족하는 근(r)을 산출하고, 수학식 1 내지 3에 따라 $\tilde{m}$, m_1 및 m_2 를 선택할 수 있으며, $\tilde{m}$, m_1 및 m_2 로부터 다항식의 각 차항의 계수를 결정할 수 있다.
- [0054] 다항식 생성부(10)에서의 중국인의 나머지 정리(CRT) 적용 방법에 대해 간략히 설명하면, 다항식 생성부(10)는 $m_2 = p_1 p_2 \dots p_n$ 과 같이 소수의 곱으로 이루어진다는 점에 기인하여, 각 p_i 에 대해 $r^d \equiv \tilde{n} \bmod p_i$ 값을 계산할 수 있다. 다항식 생성부(10)는 Hensel lemma를 이용하여 각 p_i 에 대해 계산한 r^d 를 $r^d \equiv \tilde{n} \bmod p_i^2$ 값으로 리프트(lift)할 수 있다. 다항식 생성부(10)는 중국인의 나머지 정리(CRT)를 이용하여 $r^d \equiv \tilde{n} \bmod p_1^2 \dots p_n^2 \equiv \tilde{n} \bmod m_2^2$ 값을 산출할 수 있다. 즉, 다항식 생성부(10)는 $\tilde{n} \equiv r^d \bmod m_2^2$ 를 만족하는 근(r)을 산출할 수 있다.
- [0055] 예를 들면, m_2 를 이루는 소수의 개수가 1개 이고, $f(x)$ 의 차수가 d 인 경우, 다항식 생성부(10)는 총 d^l 개의 근(r)을 산출할 수 있다. RSA 암호 시스템 중 하나인 RSA-768에 적용되는 GNFS 방식에 따르면, $l=9$, $d=6$ 으로 주어지는데, 이와 같은 경우, 다항식 생성부(10)는 $f(x)$ 의 어느 차항의 계수에 대하여 6^9 개의 근(r)을 산출하여 d 차 다항식 $f(x)$ 를 생성할 수 있을 것이다.
- [0056] 다항식 최적화부(20)는 다항식 생성부(10)에서 생성하는 적어도 하나의 d 차 다항식 $f(x)$ 중 GNFS 방식의 시빙 단계에 사용할 n 개의 다항식을 선택하여 시빙 단계의 효율성 향상을 위해 최적화할 수 있다.
- [0057] 다항식 최적화부(20)는 d 차 다항식 $f(x)$ 의 $\log\text{norm}(\text{raw}-\log\text{norm})$ 이 작을수록 Murphy E 값이 크다는 사실에 기인하여 시빙 단계에 사용할 다항식을 선택할 수 있다.
- [0058] 다항식의 $\log\text{norm}$ 값은 함수값의 크기를 나타낼 수 있으며, $\log\text{norm}$ 값이 작을수록 함수값이 작다고 볼 수 있다.
- [0059] Murphy E 값은 시빙 단계의 효율성을 나타내는 지표로, Murphy E 값이 클수록 작은 소수로 나누어 떨어질 확률이 높다는 것을 의미하고, 본 실시예에서 이는 좋은 다항식을 의미한다. 공통근을 갖는 다항식 쌍 $f(x)$ 및 $g(x)$ 에 대하여 Murphy E는 아래 수학식 4와 같이 계산할 수 있다.

수학식 4

$$\frac{6}{\pi^2} \int \rho\left(\frac{\log|F(x,y)| + \alpha(F)}{\log B_1}\right) \rho\left(\frac{\log|G(x,y)| + \alpha(G)}{\log B_2}\right) dx dy$$

- [0060]
- [0061] 도 3을 참조하면, d 차 다항식 $f(x)$ 의 $\log\text{norm}$ 값과 따른 Murphy E 값 간의 상관관계, 즉, d 차 다항식 $f(x)$ 의 $\log\text{norm}$ 값이 작을수록 높은 Murphy E 값을 가짐을 확인할 수 있다. 여기서 d 차 다항식 $f(x)$ 의 Murphy E 값은 시빙 단계를 위한 최적화 단계를 진행한 이후에 산출되는 값이다. 도 3에서 가로축은 d 차 다항식 $f(x)$ 의 $\log\text{norm}$ 값을 의미하고, 세로축은 Murphy E 값을 의미한다.
- [0062] 따라서 다항식 최적화부(20)는 다항식 생성부(10)에서 생성하는 적어도 하나의 d 차 다항식 $f(x)$ 중 $\log\text{norm}$ 값이 작은 미리 설정된 n 개의 다항식을 최적화 단계를 진행할 다항식으로 선택할 수 있다.
- [0063] 한편, 다항식 생성부(10)에서 생성하는 다항식은 단순히 공통근을 가지는 다항식으로, 시빙 단계의 효율성 향상을 위해 최적화 단계가 요구된다. 따라서, 다항식 최적화부(20)는 n 개의 다항식에 한하여 LLL(Lenstra-Lenstra-Lovasz) reduction 알고리즘에 따라 최적화를 진행할 수 있다.
- [0064] 이러한 다항식 최적화 단계는 GNFS 방식의 다항식 선택 단계에서 일반적으로 행해지는 것으로,

$f(x) \equiv g(x) \bmod N$ 을 만족하는 다항식에 있어서, $f(x)' = f(x) + h(x)g(x)$ 와 같이 그 크기(lognorm 값)가 작은 다항식으로 변형시키는 단계로 볼 수 있다.

[0065] 예를 들면, $f(x) \equiv g(x) \bmod N$ 을 만족하는 다항식 $f(x)$ 및 $g(x)$ 에 있어서, $f(x)$ 를 $f(x)' = f(x) + h(x)g(x)$ 로 변형하더라도 $g(x)$ 와 공통근을 갖는다. 일반적으로 널리 사용되는 최적화 단계 알고리즘인 Root optimization에 따르면 $h(x)$ 는 3차 이하의 다항식으로 선택된다. $f(x) \leftarrow f(x) + h(ax^2 + bx + c)g(x)$ (a, b, c 는 $[-3, 3]$ 범위)라 하면, 주어진 집합에 대해 $f(x)$ 가 나누어지는지를 확인하여 $f(x)$ 가 나누어 떨어질 확률을 측정하는 지표인 alpha 값을 각각 계산하고, alpha 값이 가장 높은 a, b, c 를 선택하여 $f(x)'$ 를 출력할 수 있을 것이다.

[0066] LLL reduction 알고리즘은 이러한 다항식 최적화 단계에 적용되는 알고리즘으로, 다항식의 기저로 생성되는 래티스(L)에서 0이 아닌 가장 작은 벡터를 찾는 방식으로 다항식 최적화를 진행할 수 있다. 즉, LLL reduction 알고리즘은 주어진 기저를 거의 수직인 기저로 변환시키는 것이라 할 수 있다.

[0067] 예를 들면, LLL reduction 알고리즘에 따르면, $f(x)=3x^2+2x+1$ 인 경우, 이를 (3,2,1)인 벡터로 나타낼 수 있으며, 다음과 같이 Column이 한 벡터를 의미하는 래티스(L)를 구성하여 다항식을 그 크기가 작은 다항식으로 변형시킬 수 있다.

$$L = \begin{bmatrix} \ell & t & u & v & w \\ s^6c_6 & 0 & 0 & 0 & 0 \\ s^5c_5 & 0 & 0 & 0 & 0 \\ s^4c_4 & s^4m_2 & 0 & 0 & 0 \\ s^3c_3 & -s^3m_1 & s^3m_2 & 0 & 0 \\ s^2c_2 & 0 & -s^2m_1 & s^2m_2 & 0 \\ sc_1 & 0 & 0 & -sm_1 & sm_2 \\ c_0 & 0 & 0 & 0 & m_1 \end{bmatrix}$$

[0068] $\ell f(x) + tg(x)x^3 + ug(x)x^2 + vg(x)x + wg(x) \in L \rightarrow \ell f(x) + (tx^3 + ux^2 + vx + w)g(x)$

[0069] 다항식 최적화부(20)는 선택한 n 개의 다항식 최적화에 있어서 LLL reduction 알고리즘을 채택할 수 있는데, 도 3과 같은 다항식의 lognorm과 Murphy E 값 간의 선형 관계를 유지할 수 있도록 Minkowski's bound를 이용할 수 있다.

[0070] LLL reduction 알고리즘은 상술한 바와 같이 가장 작은 벡터를 찾는 것으로, 이를 위해 $\{b_1, \dots, b_n\}$ 을 기저로 생성되는 래티스(L)는 $L = \{\sum_{i=1}^n a_i b_i | a_i \in \mathbb{Z}\}$ 로 정의될 수 있는데, 이러한 래티스(L)의 0이 아닌 가장 작은 벡터의 크기를 $\lambda_1(L)$ 이라 하면, Minkowski's bound에 의해 $\lambda_1 \leq \sqrt{n} \det(L)^{1/n}$ 를 만족한다.

[0071] 다항식 최적화부(20)는 이러한 Minkoski's bound를 이용하여, 다항식의 계수를 기저로 하여 생성되는 래티스(L)에서 0이 아닌 가장 작은 벡터를 찾는 방식으로 다항식 최적화를 진행할 수 있다.

[0072] 이처럼 다항식 최적화부(20)는 다항식 생성부(10)에서 생성하는 적어도 하나의 d 차 다항식 $f(x)$ 의 lognorm 값에 따라 n 개의 다항식을 선택하고, 선택한 n 개의 다항식에 Minkoski's bound에 기반한 LLL reduction 알고리즘을 적용하여 선택한 n 개의 다항식을 lognorm이 작은 다항식으로 변형시킬 수 있다.

[0073] 이와 같은 본 발명의 일 실시예에 따른 다항식 선택 장치(1000)는 인수분해 하는 수 N 에 대해 공통근(m)을 갖는 다항식 $g(x)$ 및 $f(x)$ 의 계수들을 변수로 하는 방정식($\tilde{n} \equiv x^d \bmod p_i^2$)의 모든 근에 대하여 다항식을 생성하되, 그 중 일부 다항식을 최적화하여 최종 다항식을 선택하므로, RSA-768의 인수분해에 사용되는 다항식을 선택할 수 있음은 물론 그 효율을 높일 수 있다.

[0075] 이하 도 4를 참조하여 본 발명의 일 실시예에 따른 다항식 선택 방법에 대하여 설명한다.

- [0076] 도 4는 본 발명의 일 실시예에 따른 다항식 선택 방법의 흐름도이다.
- [0077] 본 발명의 일 실시예에 따른 다항식 선택 방법은 도 1에 도시된 본 발명의 일 실시예에 따른 다항식 선택 장치(1000)와 실질적으로 동일한 구성에서 진행될 수 있다. 따라서 도 1의 다항식 선택 장치(1000)와 동일한 구성요소는 동일한 도면부호를 부여하고 반복되는 설명은 생략한다.
- [0078] 도 4를 참조하면, 다항식 생성부(10)는 인수분해 하는 수(N)에서 1차 다항식($g(x)$)과 공통근을 갖는 2차 이상의 다항식($f(x)$)을 생성할 수 있다(S100).
- [0079] 다항식 생성부(10)는 중국인의 나머지 정리(CRT)를 적용하여 1차 다항식($g(x)$) 및 2차 이상의 다항식($f(x)$)의 계수들을 변수로 하는 방정식($\tilde{n} \equiv r^d \bmod m_2^2$)의 근을 산출하고, 산출한 근을 이용하여 2차 이상의 다항식($f(x)$)을 생성할 수 있다.
- [0080] 예를 들면, 다항식 생성부(10)는 $m_2 = p_1 p_2 \cdots p_n$ 과 같이 소수의 곱으로 이루어진다는 점에 기인하여, 각 p_i 에 대해 $r^d \equiv \tilde{n} \bmod p_i$ 값을 계산할 수 있다. 다항식 생성부(10)는 Hensel lemma를 이용하여 각 p_i 에 대해 계산한 r^d 를 $r^d \equiv \tilde{n} \bmod p_i^2$ 값으로 리프트(lift)할 수 있다. 다항식 생성부(10)는 중국인의 나머지 정리(CRT)를 이용하여 $r^d \equiv \tilde{n} \bmod p_1^2 \cdots p_n^2 \equiv \tilde{n} \bmod m_2^2$ 값을 산출할 수 있다. 즉, 다항식 생성부(10)는 $\tilde{n} \equiv r^d \bmod m_2^2$ 를 만족하는 근(r)을 산출할 수 있다. 다항식 생성부(10)는 산출한 모든 근(r)에 대한 다항식을 생성할 수 있다.
- [0081] 다항식 최적화부(20)는 생성한 2차 이상의 다항식($f(x)$) 중 GNFS 방식의 시빙 단계에 사용할 다항식을 선택할 수 있다(S200).
- [0082] 다항식 최적화부(20)는 d차 다항식 $f(x)$ 의 $\log\text{norm}(\text{raw}-\log\text{norm})$ 이 작을수록 Murphy E 값이 크다는 사실에 기인하여 시빙 단계에 사용할 다항식을 선택할 수 있다.
- [0083] 다항식 최적화부(20)는 다항식 생성부(10)에서 생성하는 적어도 하나의 d차 다항식 $f(x)$ 중 $\log\text{norm}$ 값이 작은 미리 설정된 n 개의 다항식을 최적화 단계를 진행할 다항식으로 선택할 수 있다.
- [0084] 다항식 최적화부(20)는 선택한 다항식에 한하여 $\log\text{norm}$ 값을 변형시켜 GNFS 방식의 시빙 단계에 사용할 다항식을 최종 선택할 수 있다(S300).
- [0085] 다항식 최적화부(20)는 LLL(Lenstra-Lenstra-Lovasz) reduction 알고리즘을 이용하여 선택한 다항식의 $\log\text{norm}$ 을 작게 변형시킬 수 있는데, Minkoski's bound에 기반하여 선택한 다항식의 계수를 기저로 하여 생성되는 래티스(L)에서 0이 아닌 가장 작은 벡터를 찾는 방식으로 선택한 다항식의 $\log\text{norm}$ 값을 작게 변형시키는 최적화 단계를 진행할 수 있다.
- [0087] 이와 같은, 본 발명의 다항식 선택 방법은 어플리케이션으로 구현되거나 다양한 컴퓨터 구성요소를 통하여 수행될 수 있는 프로그램 명령어의 형태로 구현되어 컴퓨터 판독 가능한 기록 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능한 기록 매체는 프로그램 명령어, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다.
- [0088] 상기 컴퓨터 판독 가능한 기록 매체에 기록되는 프로그램 명령어는 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 분야의 당업자에게 공지되어 사용 가능한 것일 수도 있다.
- [0089] 컴퓨터 판독 가능한 기록 매체의 예에는, 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM, DVD 와 같은 광기록 매체, 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 ROM, RAM, 플래시 메모리 등과 같은 프로그램 명령어를 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다.
- [0090] 프로그램 명령어의 예에는, 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용하여 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드도 포함된다. 상기 하드웨어 장치는 본 발명에 따른 처리를 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.
- [0091] 이상에서는 실시예들을 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 특허 청구범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있

음을 이해할 수 있을 것이다.

부호의 설명

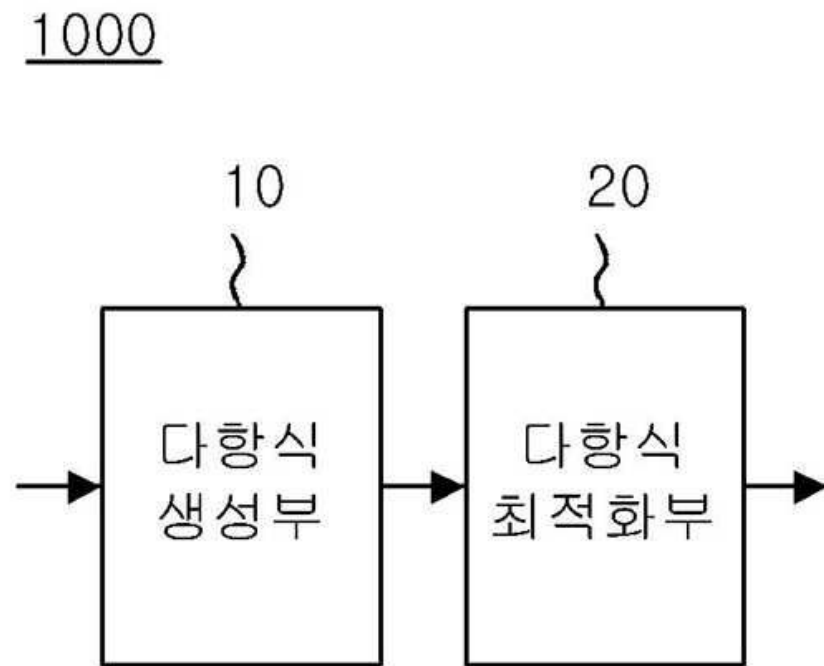
1000: 다항식 선택 장치

10: 다항식 생성부

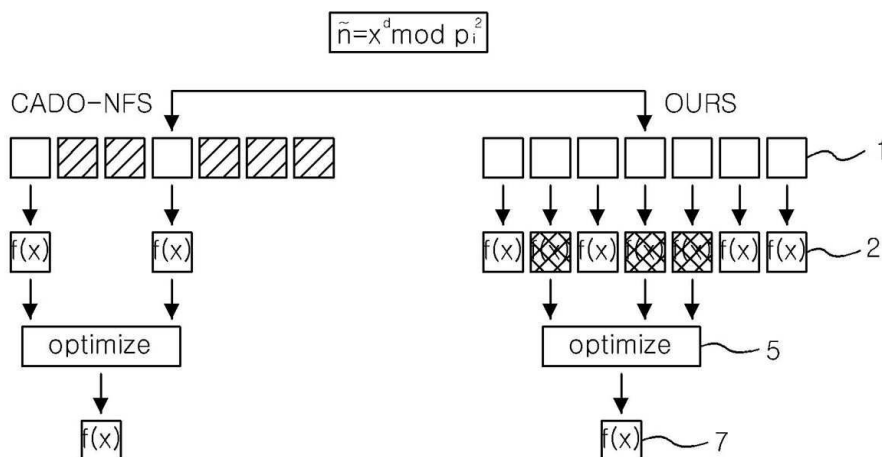
20: 다항식 최적화부

도면

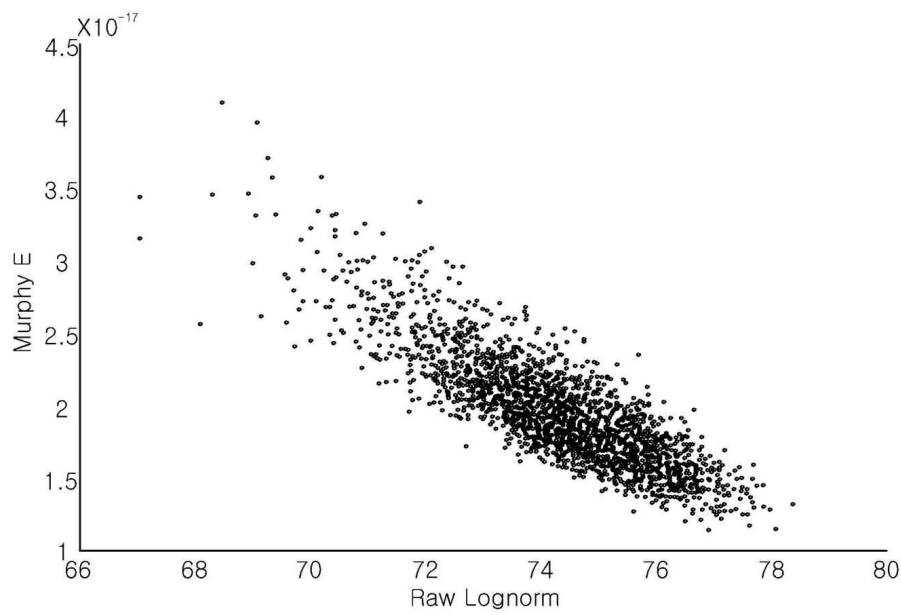
도면1



도면2



도면3



도면4

