(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2020년12월04일
(11) 등록번호 10-2187267
(24) 등록일자 2020년11월30일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) *G06N 10/00* (2019.01)
H04L 9/30 (2006.01)
(52) CPC특허분류
H04L 9/0841 (2013.01)
G06N 10/00 (2019.01)
(21) 출원번호 10-2020-0084339
(22) 출원일자 2020년07월08일
심사청구일자 2020년07월08일
(56) 선행기술조사문헌
David Jao 외 1명, Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies, International Workshop on Post-Quantum Cryptography. Springer, (2011.)*
Suhri Kim 외 4명, Efficient Isogeny Computations on Twisted Edwards Curves “, Security and Communication Networks 2018 (2018).*
KR1020100098017 A
KR1020200058252 A
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
국방과학연구소
대전광역시 유성구 북유성대로488번길 160 (수남동)
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
이경식
대전광역시 유성구 북유성대로488번길 160(수남동)
안재홍
대전광역시 유성구 북유성대로488번길 160(수남동)
(뒷면에 계속)
(74) 대리인
리앤목특허법인

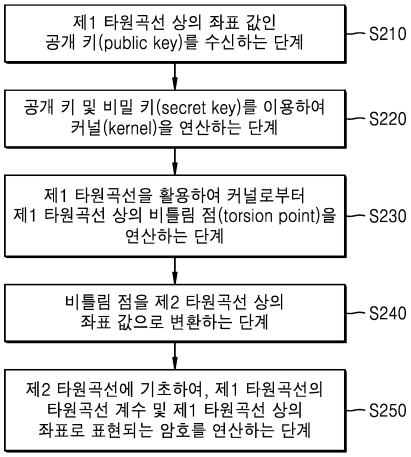
전체 청구항 수 : 총 7 항 심사관 : 양종필

(54) 발명의 명칭 **타원곡선에 기반한 초 특이성 디피-헬만 암호 교환 방법 및 장치**

(57) 요 약

본 개시는 초 특이성 디피-헬만 암호 교환 방법에 관한 것으로, 적어도 하나 이상의 프로세서(processor)에서 수행되는 타원곡선에 기반한 초 특이성 디피-헬만 암호 교환 방법은, 제1 타원곡선 상의 좌표로 표현되는 공개 키(public key)를 수신하고, 공개 키에 이용하여 커널(kernel)을 연산하고, 커널로부터 제1 타원곡선 상의 비틀림 점(torsion point)을 연산하고, 비틀림 점을 제2 타원곡선 상의 좌표로 변환하고, 제2 타원곡선 상의 좌표에 기초하여 제1 타원곡선의 타원곡선 계수 및 제1 타원곡선 상의 좌표로 표현되는 암호를 연산함으로써, 초 특이성 디피-헬만 암호 교환 방법의 연산량을 절감시킬 수 있다.

대 표 도 - 도2



(52) CPC특허분류
H04L 9/3066 (2013.01)
H04L 2209/046 (2013.01)
(72) 발명자
김수리
서울특별시 성북구 안암로 145, 자연계 캠퍼스 미래융합관 301호(안암동5가)
권지훈
서울특별시 송파구 올림픽로35길 125(신천동)
윤기순
서울특별시 금천구 가산디지털1로 186(가산동)
박영호
서울특별시 광진구 군자로 121(군자동)
홍석희
서울특별시 성북구 안암로 145(안암동5가)

공지예외적용 : 있음

명 세 서

청구범위

청구항 1

적어도 하나 이상의 프로세서(processor)에서 수행되는 초 특이성 디피-헬만 암호 교환(Supersingular Isogeny Diffie-Hellman Key Exchange) 방법에 있어서,

몽고메리 타원곡선(Montgomery curve)인 제1 타원곡선 상의 좌표로 표현되는 공개 키(public key)를 수신하는 단계;

상기 공개 키를 이용하여 커널(kernel)을 연산하는 단계;

상기 커널로부터 상기 제1 타원곡선 상의 비틀림 점(torsion point)을 연산하는 단계;

상기 비틀림 점을 에드워드 타원곡선(Edward curve)인 제2 타원곡선 상의 좌표로 변환하는 단계; 및

상기 제2 타원곡선 상의 좌표에 기초하여 상기 제1 타원곡선의 타원곡선 계수 및 상기 제1 타원곡선 상의 좌표로 표현되는 암호를 연산하는 단계;를 포함하는, 초 특이성 디피-헬만 암호 교환 방법.

청구항 2

삭제

청구항 3

제1 항에 있어서,

상기 제1 타원곡선은 3-아이소제니(isogeny) 또는 4-아이소제니(isogeny)에 기반한 타원곡선인, 초 특이성 디피-헬만 암호 교환 방법.

청구항 4

제3 항에 있어서,

상기 제1 타원곡선 상의 비틀림 점을 연산하는 단계는 더블링(doubling) 또는 트리플링(tripling)을 활용하는 것인, 초 특이성 디피-헬만 암호 교환 방법.

청구항 5

제1 항, 제3 항 및 제4 항 중 어느 한 항에 따른 초 특이성 디피-헬만 암호 교환 방법을 컴퓨터에서 실행하기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록 매체.

청구항 6

초 특이성 디피-헬만 암호 교환(Supersingular Isogeny Diffie-Hellman Key Exchange) 장치에 있어서,

몽고메리 타원곡선(Montgomery curve)인 제1 타원곡선 상의 좌표로 표현되는 공개 키(public key)를 수신할 수 있는 통신 모듈;

메모리; 및

프로세서를 포함하고,

상기 프로세서는 상기 공개 키에 기초하여 커널(kernel)을 연산하고, 상기 커널로부터 상기 제1 타원곡선 상의 비틀림 점(torsion point)을 연산하고, 상기 비틀림 점을 에드워드 타원곡선(Edward curve)인 제2 타원곡선 상의 좌표로 변환하고, 상기 제2 타원곡선 상의 좌표에 기초하여 상기 제1 타원곡선의 타원곡선 계수 및 상기 제1 타원곡선 상의 좌표로 표현되는 암호를 연산하는, 초 특이성 디피-헬만 암호 교환 장치.

청구항 7

삭제

청구항 8

제6 항에 있어서,

상기 제1 타원곡선은 3-아이소제니(isogeny) 또는 4-아이소제니(isogeny)에 기반한 타원곡선인, 초 특이성 디피-헬만 암호 교환 장치.

청구항 9

제8 항에 있어서,

상기 프로세서는 더블링(doubling) 또는 트리플링(tripling)을 활용하여 상기 제1 타원곡선 상의 비틀림 점을 연산하는, 초 특이성 디피-헬만 암호 교환 장치.

발명의 설명

기 술 분 야

[0001] 본 개시는 타원곡선에 기반한 초 특이성 디피-헬만 암호 교환 방법 및 장치에 관한 것으로서, 보다 상세하게는 초 특이성 디피-헬만 암호 교환 방법의 연산량을 감소시킬 수 있는 방법 및 장치에 관한 것이다.

배 경 기 술

[0002] 양자 컴퓨터의 등장이 가시화됨에 따라, 양자 컴퓨터로 풀기 어려운 계산 문제에 기반하여 안전성을 보장하는 암호 알고리즘을 양자 내성 암호 알고리즘(post-quantum cryptographic algorithm)이라고 한다.

[0003] 양자 내성 암호 알고리즘에는 다변수 다항식-기반(multivariate polynomial-based), 부호-기반(code-based), 격자-기반(lattice-based), 해시-기반(hash-based), 그리고 아이소제니-기반(isogeny-based) 암호 알고리즘이 포함될 수 있다.

[0004] 그 중, 초 특이성 디피-헬만 암호 교환 방법은 (SIDH: Supersingular Isogeny Diffie-Hellman key exchange) 2011년에 제안된 아이소제니(isogeny) 기반 암호 알고리즘이다. 초 특이성 디피-헬만 암호 교환 방법은 안전하지 않은 통신 채널을 통해 두 당사자 간에 공통의 비밀 키를 공유할 수 있는 암호 교환 방법으로서, 사후 양자 암호화 알고리즘 중의 하나로 주목 받고 있다.

[0005] 종래에는 Couveignes와 Stolbunov가 처음으로 아이소제니 기반 암호를 제안하였지만, Couveignes와 Stolbunov가 제안한 암호는 Childs 등이 제안한 공격 방법에 취약할 뿐만 아니라, 속도가 매우 느려 많은 관심을 받지 못했다.

[0006] 초 특이성 디피-헬만 암호 교환 방법은 초 특이성 곡선(suoersingular curve)을 사용하여 Childs 공격에 대응할 수 있어 양자 컴퓨터를 소유한 공격자의 암호 분석 공격을 저항할 수 있다는 장점을 가지고 있다. 또한, 초 특이성 디피-헬만 암호 교환 방법은 사후 양자 암호화 알고리즘 중에서 가장 작은 키 크기를 가지고 있는 장점이 있다.

[0007] 현재는 초 특이성 디피-헬만 암호 교환 방법에서, 몽고메리 사다리(Montgomery ladder)를 이용한 몽고메리 곡선(Montgomery curve)기반 초 특이성 디피-헬만 암호 교환 방법에 대한 연구가 활발하다.

선행기술문헌

특허문헌

[0008] (특허문헌 0001) KR 10-1233682

(특허문헌 0002) KR 10-1835065

(특허문헌 0003) KR 10-1776137

발명의 내용

해결하려는 과제

[0009] 실시예들은 연산 효율이 증대된 초 특이성 디피-헬만 암호 교환 방법 및 장치를 제공할 수 있다.

[0010] 실시예들을 통해 해결하고자 하는 과제가 상술한 과제로 제한되는 것은 아니며, 언급되지 아니한 과제들은 본 명세서 및 첨부된 도면으로부터 본 실시예들이 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0011] 적어도 하나 이상의 프로세서(processor)에서 수행되는 일 실시예에 관한 초 특이성 디피-헬만 암호 교환(Supersingular Isogeny Diffie-Hellman Key Exchange) 방법은, 제1 타원곡선 상의 좌표로 표현되는 공개 키(public key)를 수신하는 단계, 공개 키를 이용하여 커널(kernel)을 연산하는 단계, 커널로부터 제1 타원곡선 상의 비틀림 점(torsion point)을 연산하는 단계, 비틀림 점을 제2 타원곡선 상의 좌표로 변환하는 단계 및 제2 타원곡선 상의 좌표에 기초하여 제1 타원곡선의 타원곡선 계수 및 제1 타원곡선 상의 좌표로 표현되는 암호를 연산하는 단계를 포함할 수 있다.

[0012] 또한, 제1 타원곡선은 몽고메리 타원곡선(Montgomery curve)이고, 제2 타원곡선은 에드워드 타원곡선(Edwards curve)일 수 있다.

[0013] 또한, 제1 타원곡선은 3-아이소제니(isogeny) 또는 4-아이소제니(isogeny)에 기반한 타원곡선일 수 있다.

[0014] 또한, 제1 타원곡선 상의 비틀림 점을 연산하는 단계는 더블링(doubling) 또는 트리플링(tripling)을 활용하는 것일 수 있다.

[0015] 다른 실시예에 관한 컴퓨터로 읽을 수 있는 기록 매체는, 상술한 초 특이성 디피-헬만 암호 교환 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 것일 수 있다.

[0016] 또 다른 실시예에 관한 초 특이성 디피-헬만 암호 교환 장치는 제1 타원곡선 상의 좌표로 표현되는 공개 키(public key)를 수신할 수 있는 통신 모듈, 메모리 및 프로세서를 포함하고, 프로세서는 공개 키에 기초하여 커널(kernel)을 연산하고, 커널로부터 제1 타원곡선 상의 비틀림 점(torsion point)을 연산하고, 비틀림 점을 제2 타원곡선 상의 좌표로 변환하고, 제2 타원곡선 상의 좌표에 기초하여 제1 타원곡선의 타원곡선 계수 및 제1 타원곡선 상의 좌표로 표현되는 암호를 연산할 수 있다.

[0017] 또한, 제1 타원곡선은 몽고메리 타원곡선(Montgomery curve)이고, 제2 타원곡선은 에드워드 타원곡선(Edwards curve)일 수 있다.

[0018] 또한, 제1 타원곡선은 3-아이소제니(isogeny) 또는 4-아이소제니(isogeny)에 기반한 타원곡선일 수 있다.

[0019] 또한, 프로세서는 더블링(doubling) 또는 트리플링(tripling)을 활용하여 제1 타원곡선 상의 비틀림 점을 연산할 수 있다.

발명의 효과

[0020] 상술한 바와 같이 실시예들에 관한 초 특이성 디피-헬만 암호 교환 방법 및 장치에 의하면 초 특이성 디피-헬만 암호 교환 방법의 연산량을 절감시킬 수 있어 신속한 암호 교환이 가능할 수 있다.

[0021] 실시예들에 의한 효과가 상술한 효과들로 제한되는 것은 아니며, 언급되지 아니한 효과들은 본 명세서 및 첨부된 도면으로부터 본 실시예들이 속하는 기술분야에서 통상의 지식을 가진 자에게 명확히 이해될 수 있을 것이다.

도면의 간단한 설명

[0022] 도 1은 일 실시예에 관한 초 특이성 디피-헬만 암호 교환 장치에 관한 도면이다.

도 2는 다른 실시예에 관한 초 특이성 디피-헬만 암호 교환 방법에 관한 구체적인 흐름도이다.

도 3은 3-아이소제니에 기반한 타원곡선에서 타원곡선 계수를 복원하는 알고리즘에 관한 도면이다.

도 4는 3-아이소제니에 기반한 타원곡선에서 암호를 연산하는 알고리즘에 관한 도면이다.

도 5는 4-아이소제니에 기반한 타원곡선에서 타원곡선 계수를 복원하는 알고리즘에 관한 도면이다.

도 6은 4-아이소제니에 기반한 타원곡선에서 암호를 연산하는 알고리즘에 관한 도면이다.

도 7은 도 1에 도시된 초 특이성 디피-헬만 암호 교환 장치가 암호를 교환하는 일 양태를 도시한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0023] 본 명세서에서 다양한 곳에 등장하는 "일부 실시예에서" 또는 "일 실시예에서" 등의 어구는 반드시 모두 동일한 실시예를 가리키는 것은 아니다.

[0024] 본 실시예들에서 사용되는 용어는 본 실시예들에서의 기능을 고려하면서 가능한 현재 널리 사용되는 일반적인 용어들을 선택하였으나, 이는 당 분야에 종사하는 기술자의 의도 또는 판례, 새로운 기술의 출현 등에 따라 달라질 수 있다. 또한, 특정한 경우는 출원인이 임의로 선정한 용어도 있으며, 이 경우 해당되는 부분에서 상세히 그 의미를 기재할 것이다. 따라서, 본 실시예들에서 사용되는 용어는 단순한 용어의 명칭이 아닌, 그 용어가 가지는 의미와 본 실시예들 전반에 걸친 내용을 토대로 정의되어야 한다.

[0025] 본 실시예들은 다양한 변경을 가할 수 있고 여러 가지 형태를 가질 수 있는바, 일부 실시예들을 도면에 예시하고 상세하게 설명하고자 한다. 그러나, 이는 본 실시예들을 특정한 개시형태에 대해 한정하려는 것이 아니며, 본 실시예들의 사상 및 기술범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 본 명세서에서 사용한 용어들은 단지 실시예들의 설명을 위해 사용된 것으로, 본 실시예들을 한정하려는 의도가 아니다.

[0026] 본 실시예들에 사용되는 용어들은 다르게 정의되지 않는 한, 본 실시예들이 속하는 기술분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미가 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 실시예들에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않아야 한다.

[0027] 본 개시의 일부 실시예는 기능적인 블록 구성들 및 다양한 처리 단계들로 나타내어질 수 있다. 이러한 기능 블록들의 일부 또는 전부는, 특정 기능들을 실행하는 다양한 개수의 하드웨어 및/또는 소프트웨어 구성들로 구현될 수 있다. 예를 들어, 본 개시의 기능 블록들은 하나 이상의 마이크로프로세서들에 의해 구현되거나, 소정의 기능을 위한 회로 구성들에 의해 구현될 수 있다. 또한, 예를 들어, 본 개시의 기능 블록들은 다양한 프로그래밍 또는 스크립팅 언어로 구현될 수 있다. 기능 블록들은 하나 이상의 프로세서들에서 실행되는 알고리즘으로 구현될 수 있다. 또한, 본 개시는 전자적인 환경 설정, 신호 처리, 및/또는 데이터 처리 등을 위하여 종래 기술을 채용할 수 있다. “매커니즘”, “요소”, “수단” 및 “구성”등과 같은 용어는 넓게 사용될 수 있으며, 기계적이고 물리적인 구성들로서 한정되는 것은 아니다. 또한, 명세서에 기재된 "...부", "...모듈" 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어 또는 소프트웨어로 구현되거나 하드웨어와 소프트웨어의 결합으로 구현될 수 있다.

[0028] 이하 첨부된 도면을 참고하여 본 개시를 상세히 설명하기로 한다.

[0029] 도 1은 일 실시예에 관한 초 특이성 디피-헬만 암호 교환 장치(100)에 관한 도면이다.

[0030] 도 1을 참조하면, 일 실시예에 관한 초 특이성 디피-헬만 암호 교환 장치(100)는 통신 모듈(110), 메모리(120) 및 프로세서(130)를 포함할 수 있다.

[0031] 통신 모듈(110)은 초 특이성 디피-헬만 암호 교환 장치(100)가 외부의 장치와 데이터를 송신 또는 수신할 수 있도록 한다. 외부의 장치는 예를 들어, 암호를 교환하는 다른 초 특이성 디피-헬만 암호 교환 장치(100)일 수 있다. 또한, 송신 또는 수신되는 데이터는 어느 하나의 초 특이성 디피-헬만 암호 교환 장치(100)가 다른 하나의 초 특이성 디피-헬만 암호 교환 장치(100)와 교환하는 암호일 수 있다.

[0032] 예를 들어, 통신 모듈(110)은 RF신호, 레이저 신호, 유선 신호 등으로 각종 정보를 송신 또는 수신할 수 있는 장치를 의미할 수 있으나, 이에 제한되지 않는다.

[0033] 메모리(120)는 초 특이성 디피-헬만 암호 교환 장치(100) 내에서 처리되는 각종 데이터들을 저장하는 하드웨어로서, 예를 들어, 메모리(120)는 초 특이성 디피-헬만 암호 교환 장치(100)에서 처리된 데이터들 및 처리될 데이터들을 저장할 수 있다.

[0034] 메모리(120)는 DRAM(dynamic random access memory), SRAM(static random access memory) 등과 같은 RAM(random access memory), ROM(read-only memory), EEPROM(electrically erasable programmable read-only memory), CD-ROM, 블루레이 또는 다른 광학 디스크 스토리지, HDD(hard disk drive), SSD(solid state drive), 또는 플래시 메모리를 포함할 수 있으나, 이에 제한되지 않는다.

[0035] 프로세서(130)는 초 특이성 디피-헬만 암호 교환 방법을 위한 전반적인 기능을 수행할 수 있다. 예를 들어, 프로세서(130)는 초 특이성 디피-헬만 암호 교환 장치(100)내의 메모리(120)에 저장된 프로그램들을 실행함으로써, 초 특이성 디피-헬만 암호 교환 장치(100)를 전반적으로 제어할 수 있다.

[0036] 프로세서(130)는 하나 또는 복수 개의 프로세서에 의하여 구현될 수 있다. 예를 들어, 프로세서(130)는 다수의 논리 게이트들의 어레이로 구현될 수 있고, 범용적인 마이크로 프로세서와 마이크로 프로세서에서 실행될 수 있는 프로그램이 저장된 메모리의 조합으로 구현될 수도 있다. 예를 들어, 프로세서(230)는 CPU(Central processing unit), GPU(Graphic processing unit), 하드웨어 가속기 등일 수 있다.

[0037] 초 특이성 디피-헬만 암호 교환 방법은 복수 개의 초 특이성 디피-헬만 암호 교환 장치(100)들이 안전하지 않은 환경에서 암호를 교환하는 방법일 수 있다.

[0038] 본 명세서에서, 서로 암호를 교환하는 초 특이성 디피-헬만 암호 교환 장치(100) 중, 어느 하나의 초 특이성 디피-헬만 암호 교환 장치(100)를 앨리스(Alice), 다른 하나의 초 특이성 디피-헬만 암호 교환 장치(100)를 밥(Bob)이라 명명한다. 또한, 후술할 각 수식의 하첨자 A 및 B는 각각 앨리스 또는 밥과 관련된 파라미터를 의미한다.

[0039] 도 2는 다른 실시예에 관한 초 특이성 디피-헬만 암호 교환 방법에 관한 구체적인 흐름도이다. 도 2에 도시된 초 특이성 디피-헬만 암호 교환 방법은 도 1에 도시된 초 특이성 디피-헬만 암호 교환 장치에서 시계열적으로 처리되는 단계들로 구성될 수 있다.

[0040] 단계 210에서, 일 실시예에 관한 초 특이성 디피-헬만 암호 교환 장치(100)인 앨리스 또는 밥은 제1 타원곡선 상의 좌표 값인 공개 키(public key)를 수신할 수 있다.

수학식 1

[0041] $$M_{a,b} : by^2 = x^3 + ax^2 + x, \quad b(a^2 - 4) \neq 0.$$

[0042] 수학식 1은 몽고메리 타원곡선(Montgomery curve)를 의미한다. 일 실시예에 관한 초 특이성 디피-헬만 암호 교환 방법에서, 제1 타원곡선은 위와 같은 몽고메리 타원곡선을 의미할 수 있다.

[0043] 먼저, 앨리스와 밥은 서로소인 두 수 l_A, l_B에 대한 여인수 f를 임의로 잡아 소수 $p = l_A^{e_A} l_B^{e_B} f \pm 1$ 을 선택할 수 있다. 여기서, e_A, e_B는 각각 $\cong l_A^{e_A} \cong l_B^{e_B}$를 만족하는 양의 정수를 의미할 수 있다.

[0044] 앨리스와 밥은 유한체 F_{p^2}에서 위수가 $(l_A^{e_A} l_B^{e_B} f)^2$인 초 특이성 타원곡선 E를 선택한다. 앨리스와 밥은 각각 $l_A^{e_A}$, $l_B^{e_B}$-비틀림 군(torsion group)에 해당하는 기저(base) $\{P_A, Q_A\}$와 $\{P_B, Q_B\}$를 선택한다. 즉, 여기서 앨리스의 기저는 $\{P_A, Q_A\}$ 이고, 밥의 기저는 $\{P_B, Q_B\}$ 이다. 상술한 $\{P_A, Q_A\}$, $\{P_B, Q_B\}$는 본 명세서에서 공개 키(Public key)로 명명될 수 있다.

[0045] 앨리스와 밥은 공개 키를 서로 교환할 수 있다. 보다 구체적으로, 앨리스는 밥으로부터 $\{P_B, Q_B\}$라는 공개 키를 수신하고, 밥은 앨리스로부터 $\{P_A, Q_A\}$를 수신할 수 있다.

[0046] 이하에서는 앨리스가 일 실시예에 관한 초 특이성 디피-헬만 암호 교환 방법을 수행하는 것을 서술하도록 한다. 다만, 앨리스가 수행하는 일 실시예에 관한 초 특이성 디피-헬만 암호 교환 방법을 밥도 실질적으로 동일하게 수행할 수 있음은 통상의 기술자에게 자명할 수 있다.

[0047] 단계 220에서, 초 특이성 디피-헬만 암호 교환 장치(100)인 앨리스 또는 밥은 공개 키를 이용하여 커널(kernel)을 연산할 수 있다.

[0048] 앨리스는 공개 키에 기초하여 커널(kernel)을 연산할 수 있다. 예를 들어, 앨리스는 $m_A, n_A \in Z/l_A^{e_A}Z$ 를 만족하는 임의의 m_A, n_A를 선택할 수 있다. m_A, n_A는 본 명세서에서 개인 키(private key)를 의미할 수 있다. 일 실시예에 관한 초 특이성 디피-헬만 암호 교환 방법에서, 개인 키는 상대방에게 교환되지 않으며, 앨리스와 밥은 후술할 암호를 생성하고, 암호를 교환함으로써 비밀 공유를 확인할 수 있다.

[0049] 앨리스는 공개 키와 개인 키를 이용하여, 커널인 R_A 를 연산할 수 있다. 구체적으로, 앨리스는 $< R_A >=< [m_A]P_A + [n_A]Q_A >$를 연산하여 커널을 연산할 수 있다.

[0050] 단계 S230에서, 초 특이성 디피-헬만 암호 교환 장치(100)인 앨리스 또는 밥은 제1 타원곡선을 활용하여 커널로부터 제1 타원곡선 상의 비틀림 점(torsion point)을 연산할 수 있다.

[0051] 앨리스는 커널로부터 아이소제니(isogeny) 연산을 수행할 수 있다. 위수(order)가 $l_A^{e_A}$인 주어진 순환 군(cyclic subgroup) $< R_A > \in E[l_A^{e_A}]$ 에 대해서, E에서 $E_A = E/< R_A >$로 매핑시킬 수 있는 아이소제니(isogeny)를 $\emptyset_A$라 할 수 있다. 위수가 $l_A^{e_A}$ 인 아이소제니 $\emptyset_A$는 벨류의 공식(V´elu's formula)를 이용하여, 위수가 l_A인 e_A 개의 아이소제니의 합성으로 연산될 수 있다.

[0052] 예를 들어, $E = E_0$, $R = R_0$ 라 하고, $E_{i+1} = E_i/< l_A^{e_A-i-1}R_i >$ $(0 \le i < e)$ 및 $R_{i+1} = \emptyset_i(R_i)$이 되도록 비틀림 점(torsion point) R_i를 정의하고, 커널이 $l_A^{e_A-i-1}R_i$ 인 위수가 l_A인 아이소제니 $\emptyset_i$: $E_i \rightarrow E_{i+}$를 연산하는 것을 i에 따라서 반복적으로 수행할 수 있다. 이에 따라, 위수가 $l_A^{e_A}$ 인 $\emptyset_A$ 아이소제니 연산을 $\emptyset_A = \emptyset_{e_A-1} \circ \cdots \circ \emptyset_0$과 같이 위수가 l_A인 e_A 개의 아이소제니들의 합성으로 나타낼 수 있다.

[0053] 한편, 위수 l_A가 3인 아이소제니를 3-아이소제니라 하며, 트리플링(tripling)은 위수 l_A가 3인 아이소제니에 대해 상술한 바와 같은 연산을 진행하는 것을 의미한다.

[0054] 또한, l_A가 4인 아이소제니를 4-아이소제니라 하며, 더블링(doubling)은 l_A가 4인 아이소제니에 대해 상술한 바와 같은 연산을 진행하는 것을 의미한다.

수학식 2

[0055] $$E_d : x^2 + y^2 = 1 + dx^2y^2, \ d \neq 0, 1.$$

[0056] 수학식 2는 에드워드 타원곡선(Edward curve)을 의미한다. 일 실시예에 관한 초 특이성 디피-헬만 암호 교환 방법에서, 제2 타원곡선은 에드워드 타원곡선을 의미할 수 있다.

[0057] 에드워드 타원곡선에서 항등원은 (0,1) 이고, (0,-1)은 위수가 2인 점, (1,0) 및 (-1,0)은 위수가 4인 타원곡선 위의 점이다. 에드워드 타원곡선 위에 위수가 4인 점이 항상 존재하는 것은 에드워드 타원곡선의 다양한 활용을 저해할 수 있기 때문에, 에드워드 타원 곡선은 다음과 같이 변형될 수 있다.

수학식 3

[0058] $$E_{a,d} : ax^2 + y^2 = 1 + dx^2y^2,$$

[0059] 상술한 수학식 3에서 a와 d는 0이 아니다. 수학식 3은 수학식 2의 에드워드 타원곡선을 일부 변형한 에드워드 타원곡선의 일 양태를 나타낸 식이다. 수학식 3의 에드워드 타원곡선은 수학식 1의 몽고메리 타원곡선으로 변환될 수 있고, 수학식 1의 몽고메리 타원곡선이 수학식 3의 에드워드 타원곡선의 형태로 변환될 수 있다.

수학식 4

[0060]
$$(x,y) \rightarrow (u,v) = \left(\frac{1+y}{1-y}, \frac{1+y}{(1-y)x} \right)$$

수학식 5

[0061]
$$(u,v) \rightarrow (x,y) = \left(\frac{u}{v\sqrt{a}}, \frac{u-1}{u+1} \right)$$

[0062] 수학식 4 및 5에서 (x,y)는 에드워드 타원곡선 상의 좌표를, (u,v)는 에드워드 타원곡선 상의 좌표를 의미한다. 또한, 수학식 4는 에드워드 타원곡선을 몽고메리 타원곡선의 형태로 변환하는 식이고, 수학식 5는 몽고메리 타원곡선을 에드워드 타원곡선의 형태로 변환하는 식이다.

[0063] 수학식 4에서 몽고메리 타원곡선의 좌표인 u좌표는 에드워드 타원곡선의 y좌표만을 이용해 표현이 가능함을 확인할 수 있다. 또한, 수학식 5에서 에드워드 타원곡선의 y좌표는 수학식 4의 몽고메리 타원곡선의 좌표인 u좌표만일 이용해 표현이 가능함을 확인할 수 있다. 이러한 특징은 투영 좌표계(projective coordinate)를 이용하면 더 두드러질 수 있다. 몽고메리 타원곡선 위의 점 (x,y)을 투영 좌표계 상의 $(X_M : Z_M)$으로 표현하고, 에드워드 타원곡선 위의 점(x,y)를 $(Y_E : Z_E)$로 표현하면, 두 타원곡선 간의 변환은 다음과 같을 수 있다.

수학식 6

[0064]
$$(X_M : Z_M) \rightarrow (Y_E : Z_E) = (X_M - Z_M : X_M + Z_M),$$
$$(Y_E : Z_E) \rightarrow (X_M : Z_M) = (Y_E + Z_E : Z_E - Y_E).$$

[0065] 수학식 6에서, 투영 좌표계를 이용하면 몽고메리 타원곡선과 에드워드 타원곡선의 변환은 덧셈 두 번으로 변환이 가능함을 확인할 수 있다.

[0066] 이러한 특징을 활용하여, 일 실시예에 관한 초 특이성 디피-헬만 암호 교환 방법은 암호 연산 과정에서 몽고메리 타원곡선과 에드워드 타원곡선을 적절히 혼합하여 활용하는 효율적인 연산 방법을 제공할 수 있다.

[0067] 단계 240에서, 초 특이성 디피-헬만 암호 교환 장치(100)인 앨리스 또는 밥은 비틀림 점을 제2 타원곡선 상의 좌표 값으로 변환할 수 있다.

[0068] 또한, 단계 250에서, 초 특이성 디피-헬만 암호 교환 장치(100)인 앨리스 또는 밥은 제2 타원곡선에 기초하여 제1 타원곡선의 타원곡선 계수 및 제1 타원곡선 상의 좌표로 표현되는 암호를 연산할 수 있다.

[0069] 도 3은 3-아이소제니에 기반한 타원곡선에서 타원곡선 계수를 복원하는 알고리즘에 관한 도면이다.

[0070] 도 3을 참조하면, $P = (Y_3 : Z_3)$은 에드워드 타원곡선인 E_d 상의 3-비틀림 점을 의미한다. $P = (Y_3 : Z_3)$는 몽고메리 타원곡선인 제1 타원곡선 상의 점이 에드워드 타원 곡선인 제2 타원곡선 상의 좌표로 변환된 것이다.

[0071] 앨리스는 제2 타원곡선인 에드워드 타원곡선 상의 좌표로 변환된 비틀림 점을 이용하여, 도 3의 알고리즘에 따른 연산을 수행하여 제1 타원곡선인 몽고메리 타원곡선의 타원곡선 계수를 연산할 수 있다. 즉, 앨리스는 제2 타원곡선에 관한 수식을 이용한 도 3의 알고리즘을 통하여 제1 타원곡선의 타원곡선 계수를 연산할 수 있다.

[0072] 도 4는 3-아이소제니에 기반한 타원곡선에서 암호를 연산하는 알고리즘에 관한 도면이다.

[0073] 도 4를 참조하면, $P = (Y_3 : Z_3)$는 에드워드 타원곡선인 E_d 상의 3-비틀림 점을 의미한다. 또한, $Q_m = (X_m : Z_m)$는 제1 타원곡선인 몽고메리 타원곡선 상의 추가적인 좌표를 의미한다.

[0074] 앨리스는 추가적인 좌표 $Q_m = (X_m : Z_m)$을 제2 타원곡선인 에드워드 타원곡선 상의 좌표 값인 y,z로 변환할 수 있다. 또한, 앨리스는 $P = (Y_3 : Z_3)$ 와 y,z를 활용하여 제1 타원곡선 상의 좌표 값으로 표현되는 암호인 X',Z'를 생성할 수 있다. 즉, 앨리스는 제2 타원곡선에 관한 수식을 이용한 도 4의 알고리즘을 통하여, 제1 타원곡선 상의 좌표로 표현되는 암호를 연산할 수 있다.

[0075] 도 5는 4-아이소제니에 기반한 타원곡선에서 타원곡선 계수를 복원하는 알고리즘에 관한 도면이다.

[0076] 도 5를 참조하면, $P_e = (Y_4 : Z_4)$는 에드워드 타원곡선인 E_d 상의 4-비틀림 점을 의미한다. $P_e = (Y_4 : Z_4)$는 몽고메리 타원곡선인 제1 타원곡선 상의 점이 에드워드 타원 곡선인 제2 타원곡선 상의 좌표로 변환된 것이다.

[0077] 앨리스는 제2 타원곡선인 에드워드 타원곡선 상의 좌표로 변환된 비틀림 점을 이용하여, 도 5의 알고리즘에 따른 연산을 수행함으로써 제1 타원곡선인 몽고메리 타원곡선의 타원곡선 계수를 연산할 수 있다. 즉, 앨리스는 제2 타원곡선에 관한 수식을 이용한 도 5의 알고리즘을 통하여 제1 타원곡선의 타원곡선 계수를 연산할 수 있다.

[0078] 도 6은 4-아이소제니에 기반한 타원곡선에서 암호를 연산하는 알고리즘에 관한 도면이다.

[0079] 도 6을 참조하면, $P_e = (Y_4 : Z_4)$는 에드워드 타원곡선인 E_d 상의 4-비틀림 점을 의미한다. 또한, $Q = (X_m : Z_m)$는 몽고메리 타원곡선 상의 추가적인 좌표를 의미한다.

[0080] 앨리스는 추가적인 좌표 $Q = (X_m : Z_m)$을 제2 타원곡선인 에드워드 타원곡선 상의 좌표 값인 y,z로 변환할 수 있다. $P_e = (Y_4 : Z_4)$ 와 y,z값을 이용하여 제1 타원곡선 상의 좌표 값으로 표현되는 암호(X',Z')가 생성될 수 있다. 즉, 앨리스는 제2 타원곡선에 관한 수식을 이용한 도 6의 알고리즘을 통하여, 제1 타원곡선 상의 좌표로 표현되는 암호를 연산할 수 있다.

[0081] 앨리스와 밥이 도 3 내지 도 6의 알고리즘을 활용하는 일 예로서, 앨리스가 3-아이소제니 기반 제1 타원곡선을 활용하고, 밥이 4-아이소제니 기반 제1 타원곡선을 활용하는 경우, 앨리스는 도 3 및 도 4에 따른 알고리즘을, 밥은 도 5 및 도 6에 따른 알고리즘을 활용할 수 있다.

[0082] 앨리스와 밥이 도 3 내지 도 6의 알고리즘을 활용하는 다른 예로서, 앨리스가 4-아이소제니 기반 제1 타원곡선을 활용하고, 밥이 3-아이소제니 기반 제1 타원곡선을 활용하는 경우, 앨리스는 도 5 및 도 6에 따른 알고리즘을, 밥은 도 3 및 도 4에 따른 알고리즘을 활용할 수 있다.

[0083] 정리하면, 앨리스는 상술한 도 3 내지 도 6의 알고리즘을 활용하여, 제1 타원곡선으로 표현되는 비틀림 점 및 추가적인 좌표를 제2 타원곡선 상의 좌표로 변환할 수 있다. 또한, 앨리스는 상술한 도 3 내지 도 6의 알고리즘을 활용하여, 제2 타원곡선에 관한 수식을 이용하여 제1 타원곡선의 타원곡선 계수 또는 제1 타원곡선 상의 좌표로 표현되는 암호를 연산할 수 있는 알고리즘을 제시할 수 있다.

표 1

[0084]

	비교예	실시예에 관한 방법
트리플링	7M+5S+3a+7s	7M+5S+2a+7s
3-아이소제니 계수 복원	2M+3S+12a+3s	2M+3S+7a+2s
4-아이소제니 계수 복원	4S+4a+1s	4S+2a

[0085] 표 1은 일 실시예에 관한 초 특이성 디피-헬만 암호 교환 방법과 몽고메리 타원곡선만을 활용하는 비교예에 따른 암호 교환 방법의 연산량을 비교한 것이다. 표 1에서 M, S는 각각 유한체 곱셈과 유한체 제곱 연산을 의미하

며, a와 s는 각각 유한체 덧셈과 유한체 뺄셈 연산을 의미한다.

[0086] 표 1을 참조하면, 일 실시예에 관한 초 특이성 디피-헬만 암호 교환 방법의 연산량이 비교예에 따른 암호 교환 방법의 연산량보다 작음을 확인할 수 있다. 즉, 일 실시예에 관한 초 특이성 디피-헬만 암호 교환 방법은 연산 과정 중에 제1 타원곡선인 몽고메리 타원곡선과 제2 타원곡선인 에드워드 타원곡선을 활용하여, 연산량을 감소시킴으로써 연산 효율이 증대된 초 특이성 디피-헬만 암호 교환 방법을 제공할 수 있다.

[0087] 도 7은 도 1에 도시된 초 특이성 디피-헬만 암호 교환 장치(100)가 암호를 교환하는 일 양태를 도시한 도면이다.

[0088] 도 7을 참조하면, 앨리스(710)와 밥(720)은 단계 S210 내지 단계 S250의 과정을 통하여 암호(730,740)를 생성한 뒤, 생성한 암호(730,740)를 교환할 수 있다.

[0089] 앨리스(710)와 밥(720)은 교환된 암호(730,740)에 기초하여 다시 단계 S220과 동일한 과정을 수행할 수 있다. 예를 들어, 앨리스(710)가 밥(720)이 생성한 암호(740)를 수신하는 경우, 암호(740)는 $(E_B, \emptyset_B(P_A), \emptyset_B(P_A))$ 와 같이 표현될 수 있다.

[0090] 앨리스(710)는 다시 암호(740)에 기초하여, $< R'_A >=< [m_A]\emptyset_B(P_A) + [n_A]\emptyset_B(P_A) >$ 를 연산하고, 상술한 바와 같이 벨류의 공식(V´elu's formula)를 이용하여 타원곡선 $E_{BA} = E_B/< R'_A >$ 를 연산할 수 있다. 밥(720)도 앨리스(710)와 동일한 과정을 통하여, $E_{AB} = E_A/< R'_B >$ 를 연산할 수 있다.

[0091] 앨리스(710)와 밥(720)은 각각 E_{BA}, E_{AB}의 타원곡선 계수를 연산할 수 있다. 앨리스(710)와 밥(720)은 각각 타원곡선 계수에 기초하여 J-불변값(J-invarinant)을 계산할 수 있다.

[0092] 앨리스(710)와 밥(720)은 계산된 J-불변값을 비교하여, 비밀을 공유할 수 있다. 예를 들어, 앨리스(710)와 밥(720)은 J-불변값이 일치하는 지 여부를 판단함에 따라 서로가 동일한 비밀을 공유하였는지를 확인할 수 있다.

[0093] 상술한 바와 같이 초 특이성 디피-헬만 암호 교환 방법은 개인 키를 공유하지 않고도 공개 키에 기초하여 암호 교환자들이 동일한 암호를 안전하게 공유할 수 있는 방법을 제공할 수 있다.

[0094] 본 실시예들은 컴퓨터에 의해 실행되는 프로그램 모듈과 같은 컴퓨터에 의해 실행 가능한 명령어를 포함하는 기록 매체의 형태로도 구현될 수 있다. 컴퓨터 판독 가능 매체는 컴퓨터에 의해 액세스될 수 있는 임의의 가용 매체일 수 있고, 휘발성 및 비휘발성 매체, 분리형 및 비분리형 매체를 모두 포함한다. 또한, 컴퓨터 판독가능 매체는 컴퓨터 저장 매체 및 통신 매체를 모두 포함할 수 있다. 컴퓨터 저장 매체는 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터와 같은 정보의 저장을 위한 임의의 방법 또는 기술로 구현된 휘발성 및 비휘발성, 분리형 및 비분리형 매체를 모두 포함한다. 통신 매체는 전형적으로 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈과 같은 변조된 데이터 신호의 기타 데이터, 또는 기타 전송 메커니즘을 포함하며, 임의의 정보 전달 매체를 포함한다.

[0095] 또한, 본 명세서에서, "부"는 프로세서 또는 회로와 같은 하드웨어 구성(hardware component), 및/또는 프로세서와 같은 하드웨어 구성에 의해 실행되는 소프트웨어 구성(software component)일 수 있다.

[0096] 전술한 본 명세서의 설명은 예시를 위한 것이며, 본 명세서의 내용이 속하는 기술분야의 통상의 지식을 가진 자는 본 발명의 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 쉽게 변형이 가능하다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다. 예를 들어, 단일형으로 설명되어 있는 각 구성 요소는 분산되어 실시될 수도 있으며, 마찬가지로 분산된 것으로 설명되어 있는 구성 요소들도 결합된 형태로 실시될 수 있다.

[0097] 본 실시예의 범위는 상기 상세한 설명보다는 후술하는 특허청구범위에 의하여 나타내어지며, 특허청구범위의 의미 및 범위 그리고 그 균등 개념으로부터 도출되는 모든 변경 또는 변형된 형태가 포함되는 것으로 해석되어야 한다.

부호의 설명

[0098] 100: 초 특이성 디피-헬만 암호 교환 장치

110: 통신 모듈

120: 메모리

130: 프로세서

710: 앨리스(Alice)

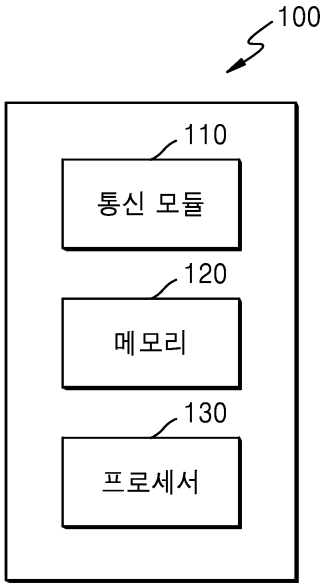
720: 밥(Bob)

730: 암호

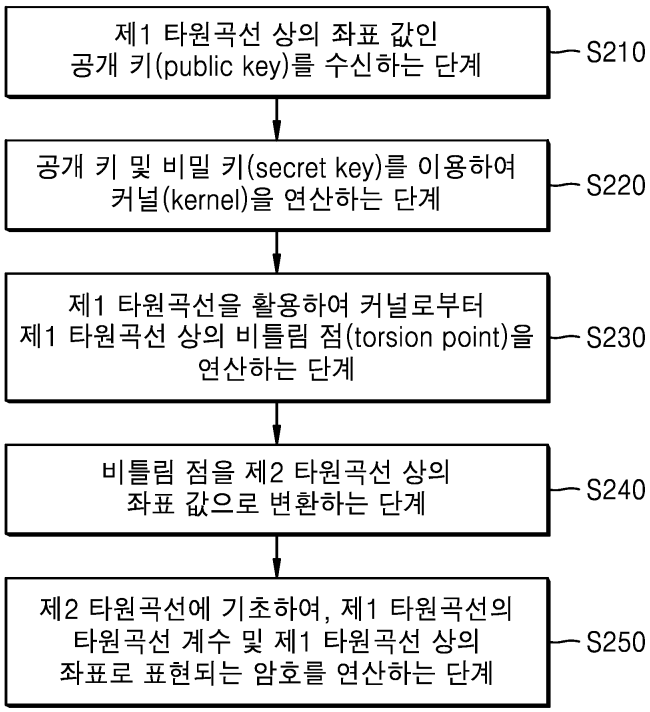
740: 암호

도면

도면1



도면2



도면3

Algorithm 1 Computing 3-isogeny on Edwards curves

Require: 3-torsion point $P = (Y_3 : Z_3)$ on an Edwards curve E_d

Ensure: The 3-isogenous Montgomery curve with projective curve coefficients C_M/D_M where $C_M = A' + 2C'$ and $D_M = A' - 2C'$.

1: $t_0 \leftarrow Y_3 + Z_3$ // $t_0 = Y_3 + Z_3$
2: $t_0 \leftarrow t_0^2$ // $t_0 = (Y_3 + Z_3)^2$
3: $t_1 \leftarrow Y_3^2$ // $t_1 = Y_3^2$
4: $t_2 \leftarrow Z_3^2$ // $t_2 = Z_3^2$
5: $t_3 \leftarrow t_0 - t_1$ // $t_3 = Z_3^2 + 2Y_3Z_3$
6: $t_4 \leftarrow t_0 - t_2$ // $t_4 = Y_3^2 + 2Y_3Z_3$
7: $C_M \leftarrow t_0 + t_3$ // $C_M = Y_3^2 + 4Y_3Z_3 + 2Z_3^2$
8: $t_2 \leftarrow t_2 + t_2$ // $t_2 = 2Z_3^2$
9: $C_M \leftarrow C_M + t_2$ // $C_M = (Y_3 + 2Z_3)^2$
10: $D_M \leftarrow t_0 + t_4$ // $D_M = Z_3^2 + 4Y_3Z_3 + 2Y_3^2$
11: $t_1 \leftarrow t_1 + t_1$ // $t_1 = 2Y_3^2$
12: $D_M \leftarrow D_M + t_1$ // $D_M = (Z_3 + 2Y_3)^2$
13: $C_M \leftarrow C_M \cdot t4$ // $C_M = (Y_3 + 2Z_3)^3 Y_3$
14: $D_M \leftarrow D_M \cdot t3$ // $D_M = (Z_3 + 2Y_3)^3 Z_3$
15: return C_M, D_M

도면4

Algorithm 2 Evaluating 3-isogeny on Montgomery curves

Require: 3-torsion point $P = (Y_3 : Z_3)$ on E_d and a curve point $Q_m = (X_m : Z_m)$ on $M_{a,b}$ corresponding to a point $Q_e = (Y : Z)$ on an Edwards curve E_d.

Ensure: Image point $Q' = (X' : Z')$ on the image curve $M_{a,b}$ birationally equivalent to $\phi(E_d)$

1: $y \leftarrow X - Z$ // y : convert to point on an Edwards curve
2: $z \leftarrow X + Z$ // z : convert to point on an Edwards curve
3: $t_0 \leftarrow z \cdot Y_3$ // $t_0 = z \cdot Y_3$
4: $t_1 \leftarrow y \cdot Z_3$ // $t_1 = y \cdot Z_3$
5: $t_2 \leftarrow t_0 + t_1$ // $t_2 = (z \cdot Y_3 + y \cdot Z_3)$
6: $t_2 \leftarrow t_2^2$ // $t_2 = (z \cdot Y_3 + y \cdot Z_3)^2$
7: $X' \leftarrow t_2 \cdot X$ // $X' = (1/2) \cdot (y + z) \cdot (z \cdot Y_3 + y \cdot Z_3)^2$
8: $t_0 \leftarrow t_0 - t_1$ // $t_0 = (z \cdot Y_3 - y \cdot Z_3)$
9: $t_0 \leftarrow t_0^2$ // $t_0 = (z \cdot Y_3 - y \cdot Z_3)^2$
10: $Z' \leftarrow t_0 \cdot Z$ // $Z' = (1/2) \cdot (z - y) \cdot (ZY_3 - YZ_3)^2$
11: return X', Z'

도면5

Algorithm 3 Computing 4-isogeny on Edwards curves

Require: 4-torsion point $P_m = (X_m : Z_m)$ on a Montgomery curve $M_{a,b}$ corresponding to a 4-torsion point $P_e = (Y_4 : Z_4)$ on an Edwards curve E_d

Ensure: The 4-isogenous Montgomery curve with projective curve coefficients C_M/D_M where $C_M = A' + 2C'$ and $D_M = 4C'$ with coefficient c_0 that are used to evaluate the 4-isogeny

1: $C_M \leftarrow X_m^2$ // $C_M = (1/4) \cdot (Y_4 + Z_4)^2$
2: $t_0 \leftarrow Z_m^2$ // $t_0 = (1/4) \cdot (Y_4 - Z_4)^2$
3: $c_0 \leftarrow C_M + C_M$ // $c_0 = (1/2) \cdot (Y_4 + Z_4)^2$
4: $c_0 \leftarrow c_0 + c_0$ // $t_0 = (Y_4 - Z_4)^2$
5: $C_M \leftarrow C_M^2$ // $C_M = (1/16) \cdot (Y_4 + Z_4)^4$
6: $D_M \leftarrow t_0^2$ // $D_M = (1/16) \cdot (Y_4 - Z_4)^4$
7: return C_M, D_M, c_0

도면6

Algorithm 4 Evaluating 4-isogeny on Montgomery curves

Require: 4-torsion point $P = (Y_4 : Z_4)$, a curve point $Q = (X_m : Z_m)$ on $M_{a,b}$ corresponding to a point $Q_e = (Y : Z)$ on an Edwards curve E_d, and c_0 computed from Algorithm 3.

Ensure: Image point $Q' = (X' : Z')$ on the image curve $\phi(M_{a,b})$ birationally equivalent to $\phi(E_d)$

1: $z \leftarrow X + Y$ // z : convert to point on an Edwards curve
2: $y \leftarrow X - Y$ // y : convert to point on an Edwards curve
3: $t_0 \leftarrow y \cdot z$ // $t_0 = YZ$
4: $t_1 \leftarrow c_0 \cdot t_0$ // $t_2 = YZ(Y_4 + Z_4)^2$
5: $t_0 \leftarrow Y \cdot Z_4$ // $t_0 = YZ_4$
6: $t_2 \leftarrow Z \cdot Y_4$ // $t_1 = ZY_4$
7: $t_3 \leftarrow t_0 + t_2$ // $t_3 = YZ_4 + ZY_4$
8: $t_4 \leftarrow t_0 - t_2$ // $t_4 = YZ_4 - ZY_4$
9: $t_3 \leftarrow t_3^2$ // $t_3 = (YZ_4 + ZY_4)^2$
10: $t_4 \leftarrow t_4^2$ // $t_4 = (YZ_4 - ZY_4)^2$
11: $X' \leftarrow t_1 + t_4$ // $X' = YZ(Y_4 + Z_4)^2 + (YZ_4 - ZY_4)^2$
12: $Z' \leftarrow t_3 - t_1$ // $Z' = (YZ_4 + ZY_4)^2 - YZ(Y_4 + Z_4)^2$
13: $X' \leftarrow X' \cdot t_3$ // $X' = (YZ(Y_4 + Z_4)^2 + (YZ_4 - ZY_4)^2)(YZ_4 + ZY_4)^2$
14: $Z' \leftarrow Z' \cdot t_4$ // $Z' = ((YZ_4 + ZY_4)^2 - YZ(Y_4 + Z_4)^2)(YZ_4 - ZY_4)^2$
15: return X', Z'

도면7

