(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2018-0114182
(43) 공개일자 2018년10월17일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) *H04L 9/30* (2006.01)
H04L 9/32 (2006.01) *H04W 12/02* (2009.01)
H04W 84/18 (2009.01)
(52) CPC특허분류
H04L 9/0841 (2013.01)
H04L 9/3066 (2013.01)
(21) 출원번호 10-2018-7027171
(22) 출원일자(국제) 2017년02월14일
심사청구일자 2018년10월05일
(85) 번역문제출일자 2018년09월19일
(86) 국제출원번호 PCT/IB2017/050815
(87) 국제공개번호 WO 2017/145002
국제공개일자 2017년08월31일
(30) 우선권주장
1603117.1 2016년02월23일 영국(GB)
(뒷면에 계속)

(71) 출원인
엔체인 홀딩스 리미티드
안티구아바부다 세인트존스, 처치 스트리트 44, 피츠제럴드 하우스
(72) 발명자
라이트, 크레이그 스티븐
영국, 씨에프10 2에이치에이치 카디프, 처칠 웨이, 처칠 하우스 7층, 어커트-디키스 앤 로드 엘엘피
사바나, 스테판
영국, 씨에프10 2에이치에이치 카디프, 처칠 웨이, 처칠 하우스 7층, 어커트-디키스 앤 로드 엘엘피
(74) 대리인
특허법인다나

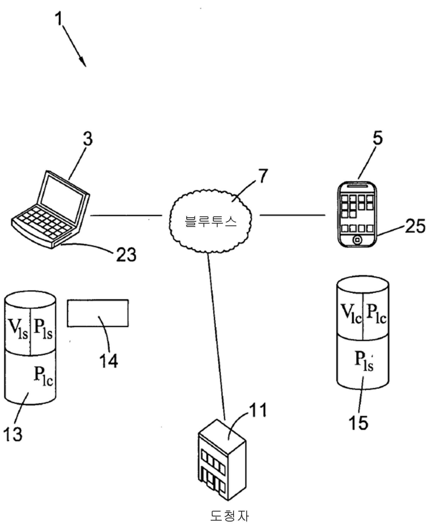
전체 청구항 수 : 총 26 항

(54) 발명의 명칭 **비밀 공유를 위한 타원 곡선 암호를 사용하는 개인용 장치 보안**

(57) 요 약

전자 장치가 키 장치(5)에 연관되는 데이터를 전자 장치(3)에서 암호화하는 방법(400)에 관한 것이다. 각 장치는 비대칭 암호 쌍에 연관되고, 각 쌍은 제1 개인 키와 제1 공개 키를 포함한다. 각각의 제2 개인 키와 공개 키는, 제1 개인 키, 제1 공개 키, 및 결정론적 키에 기초하여 결정될 수 있다. 비밀은 제2 개인 키와 공개 키에 기초하여 결정될 수 있다. 전자 장치(3)에서의 데이터는, 결정된 비밀 또는 결정된 비밀에 기초하는 암호화 키를 사용하여 암호화될 수 있다. 결정론적 키를 나타내는 정보는, 그 정보가 저장될 수 있는 키 장치(5)에 전송될 수 있다.

대 표 도 - 도1



(52) CPC특허분류
H04L 9/3252 (2013.01)
H04W 12/02 (2013.01)
H04W 84/18 (2013.01)
H04L 2209/56 (2013.01)

(30) 우선권주장
1603122.1 2016년02월23일 영국(GB)
1619301.3 2016년11월15일 영국(GB)

명 세 서

청구범위

청구항 1

전자 장치(S)에서 데이터를 암호화하는 컴퓨터 구현 방법으로서,

상기 전자 장치는 키 장치(C)에 연관되고, 상기 전자 장치는 또한 제1 전자 장치 개인 키(V_{1S})와 제1 전자 장치 공개 키(P_{1S})를 갖는 제1 비대칭 암호 쌍(cryptography pair))에 연관되고, 상기 키 장치는 제1 키 장치 개인 키(V_{1C})와 제1 키 장치 공개 키(P_{1C})를 갖는 제2 비대칭 암호 쌍에 연관되며, 상기 방법은,

상기 전자 장치에서 결정론적 키(DK)를 결정하는 단계;

상기 전자 장치에서 상기 키 장치로부터 상기 제1 키 장치 공개 키(P_{1C})를 수신하는 단계;

상기 전자 장치에서, 적어도 상기 제1 전자 장치 개인 키(V_{1S})와 상기 결정론적 키(DK)에 기초하여 제2 전자 장치 개인 키(V_{2S})를 결정하는 단계;

상기 전자 장치에서, 적어도 상기 제1 키 장치 공개 키(P_{1C})와 상기 결정론적 키(DK)에 기초하여 제2 키 장치 공개 키(P_{2C})를 결정하는 단계;

적어도 상기 제2 전자 장치 개인 키(V_{2S})와 상기 제2 키 장치 공개 키(P_{2C})에 기초하여 비밀을 결정하는 단계;

상기 전자 장치에서, 결정된 상기 비밀 또는 상기 결정된 비밀에 기초하는 암호화 키를 사용하여 상기 데이터를 암호화하는 단계; 및

상기 결정론적 키(DK)를 나타내는 정보를 상기 정보가 저장될 수 있는 상기 키 장치에 전송하는 단계를 포함하는, 컴퓨터 구현 방법.

청구항 2

제1항에 있어서, 상기 키 장치에, 상기 결정론적 키(DK)를 나타내는 상기 정보를 저장하는 단계를 더 포함하는, 컴퓨터 구현 방법.

청구항 3

제1항 또는 제2항에 있어서, 상기 결정론적 키(DK)는 메시지(M)에 기초하는, 컴퓨터 구현 방법.

청구항 4

제3항에 있어서, 상기 전자 장치에서 상기 메시지(M)를 생성하는 단계, 및 상기 메시지(M)의 해시 결정에 기초하여 상기 결정론적 키(DK)를 결정하는 단계를 더 포함하는, 컴퓨터 구현 방법.

청구항 5

제1항 내지 제4항 중 어느 한 항에 있어서, 적어도 상기 제1 전자 장치 공개 키(P_{1S})와 상기 결정론적 키(DK)에 기초하여 제2 전자 장치 공개 키(P_{2S})를 결정하는 단계를 포함하는, 컴퓨터 구현 방법.

청구항 6

제1항 내지 제5항 중 어느 한 항에 있어서, 상기 전자 장치로부터 상기 키 장치로, 공통 생성자(G)와 함께 공통 타원 곡선 암호(ECC) 시스템을 사용하는 것을 나타내는 통지를 전송하는 단계를 포함하는, 컴퓨터 구현 방법.

청구항 7

제6항에 있어서, 상기 제1 전자 장치 공개 키(P_{1S})와 상기 제1 키 장치 공개 키(P_{1C})는, 상기 제1 전자 장치 개

인 키(V_{1S})와 상기 제1 키 장치 개인 키(V_{1C}) 각각과 상기 공통 생성자(G)의 타원 곡선 포인트 승산에 기초하는, 컴퓨터 구현 방법.

청구항 8

제6항 또는 제7항에 있어서, 상기 공통 ECC 시스템에서 특정된 허용가능 범위의 랜덤 정수에 기초하여 상기 제1 전자 장치 개인 키(V_{1S})를 생성하는 단계; 및

$P_{1S} = V_{1S} \times G$ 식에 따라 상기 제1 전자 장치 개인 키(V_{1C})와 상기 공통 생성자(G)의 타원 곡선 포인트 승산에 기초하여 상기 제1 전자 장치 공개 키(P_{1S})를 생성하는 단계를 포함하는, 컴퓨터 구현 방법.

청구항 9

제6항 내지 제8항 중 어느 한 항에 있어서, $V_{2S} = V_{1S} + DK$ 식에 따라 상기 제1 전자 장치 개인 키(V_{1S})와 상기 결정론적 키(DK)의 스칼라 가산에 기초하여 상기 제2 전자 장치 개인 키(V_{2S})를 생성하는 단계를 포함하는, 컴퓨터 구현 방법.

청구항 10

제6항 내지 제9항 중 어느 한 항에 있어서, 적어도 상기 결정론적 키(DK)와 상기 제1 전자 장치 공개 키(P_{1S})의 타원 곡선 포인트 가산에 기초하여 상기 제2 전자 장치 공개 키(P_{2S})를 생성하는 단계를 포함하는, 컴퓨터 구현 방법.

청구항 11

제10항에 있어서, 상기 제2 전자 장치 공개 키(P_{2S})는, $P_{2S} = P_{1S} + DK \times G$ 식에 따라 상기 결정론적 키(DK)와 상기 공통 생성자(G)의 타원 곡선 포인트 승산에 대한 상기 제1 전자 장치 공개 키(P_{1S})의 타원 곡선 포인트 가산에 기초하는, 컴퓨터 구현 방법.

청구항 12

제6항 내지 제11항 중 어느 한 항에 있어서, 적어도 상기 결정론적 키(DK)와 상기 제1 키 장치 공개 키(P_{1C})의 타원 곡선 포인트 가산에 기초하여 상기 제2 키 장치 공개 키(P_{2C})를 생성하는 단계를 포함하는, 컴퓨터 구현 방법.

청구항 13

제12항에 있어서, 상기 제2 키 장치 공개 키(P_{2C})는, $P_{2C} = P_{1C} + DK \times G$ 식에 따라 상기 결정론적 키(DK)와 상기 공통 생성자(G)의 타원 곡선 포인트 승산에 대한 상기 제1 키 장치 공개 키(P_{1C})의 타원 곡선 포인트 가산에 기초하는, 컴퓨터 구현 방법.

청구항 14

제1항 내지 제13항 중 어느 한 항에 있어서, 상기 결정된 비밀과 상기 전자 장치의 식별 정보에 기초하여 상기 암호화 키를 결정하는 단계를 포함하는, 컴퓨터 구현 방법.

청구항 15

제1항 내지 제14항 중 어느 한 항에 있어서, 상기 전자 장치에 연관된 데이터 저장소에 상기 제1 키 장치 공개 키(P_{1C})를 저장하는 단계를 포함하는, 컴퓨터 구현 방법.

청구항 16

전술한 바와 같이 데이터를 암호화하는 방법에 따라 암호화되어 있는 데이터를 전자 장치에서 해독하는 컴퓨터 구현 방법으로서,

상기 전자 장치에서, 상기 키 장치로부터 상기 결정론적 키(DK)를 나타내는 정보를 수신하는 단계;

상기 결정론적 키(DK)를 나타내는 수신된 상기 정보에 기초하여 상기 비밀을 결정하는 단계; 및

상기 전자 장치에서, 상기 비밀 또는 상기 비밀에 기초하는 상기 암호화 키를 사용하여 상기 암호화되어 있는 데이터를 해독하는 단계를 포함하는, 컴퓨터 구현 방법.

청구항 17

제16항에 있어서, 상기 전자 장치에서, 인증 메시지(M_A)를 생성하고 상기 인증 메시지(M_A)를 상기 키 장치에 전송하는 단계를 포함하는, 컴퓨터 구현 방법.

청구항 18

제17항에 있어서, 상기 인증 메시지(M_A)의 해시를 결정함으로써 결정론적 인증 키(DK_A)를 결정하는 단계를 포함하는, 컴퓨터 구현 방법.

청구항 19

제16항 내지 제18항 중 어느 한 항에 있어서, 상기 키 장치에서, 제2 키 장치 개인 키(V_{2C})와 제2 키 장치 공개 키(P_{2C})를 갖는 제2 비대칭 암호 쌍을 생성하는 단계를 포함하는, 컴퓨터 구현 방법.

청구항 20

제18항과 제19항에 있어서, 상기 제2 키 장치 개인 키(V_{2C})는 상기 결정론적 인증 키(DK_A)와 상기 제1 키 장치 개인 키(V_{1C})에 기초하고, 상기 제2 키 장치 공개 키(P_{2C})는 상기 결정론적 인증 키(DK_A)와 상기 제1 키 장치 공개 키(P_{1C})에 기초하는, 컴퓨터 구현 방법.

청구항 21

제20항에 있어서, 상기 키 장치에서, 상기 결정론적 인증 키(DK_A)와 상기 제2 키 장치 개인 키(V_{2C})에 기초하여, 서명된 인증 메시지(SM_A)를 생성하는 단계;

상기 전자 장치에서, 상기 키 장치로부터 상기 서명된 인증 메시지(SM_A)를 수신하는 단계;

상기 서명된 인증 메시지(SM_A)를 상기 제2 키 장치 공개 키(P_{2C})로 유효성 확인(validate)하는 단계; 및

상기 서명된 인증 메시지(SM_A)의 유효성 확인 결과에 기초하여 상기 키 장치를 인증하는 단계를 포함하는, 컴퓨터 구현 방법.

청구항 22

제16항 내지 제21항 중 어느 한 항에 있어서, 상기 전자 장치에서, 상기 키 장치로부터의 상기 결정론적 키(DK)를 나타내는 상기 정보를 요청하는 단계;

상기 키 장치에서, 상기 메시지(M)에 기초하여 서명된 메시지(SM)를 생성하는 단계;

상기 서명된 메시지(SM)를 상기 전자 장치에 전송하는 단계;

상기 전자 장치에서, 상기 서명된 메시지(SM)를 유효성 확인하는 단계; 및

상기 전자 장치에서, 상기 데이터를 해독하기 위해 상기 비밀이 결정될 수 있도록 상기 메시지(M)를 검색하는 단계를 포함하는, 컴퓨터 구현 방법.

청구항 23

전자 장치에서 데이터를 암호화하는 컴퓨터 시스템으로서,

제1 전자 장치 개인 키(V_{1S})와 제1 전자 장치 공개 키(P_{1S})를 갖는 제1 비대칭 암호 쌍에 연관된, 상기 전자 장치; 및

제1 키 장치 개인 키(V_{1C})와 제1 키 장치 공개 키(P_{1C})를 갖는 제2 비대칭 암호 쌍에 연관된, 키 장치를 포함하고,

상기 전자 장치는,

결정론적 키(DK)를 결정하고,

상기 키 장치로부터 상기 제1 키 장치 공개 키(P_{1C})를 수신하고,

적어도 상기 제1 전자 장치 개인 키(V_{1S})와 상기 결정론적 키(DK)에 기초하여 제2 전자 장치 개인 키(V_{2S})를 결정하고,

적어도 상기 제1 키 장치 공개 키(P_{1C})와 상기 결정론적 키(DK)에 기초하여 제2 키 장치 공개 키(P_{2C})를 결정하고,

적어도 상기 제2 전자 장치 개인 키(V_{2S})와 상기 제2 키 장치 공개 키(P_{2C})에 기초하여 비밀을 결정하고,

결정된 상기 비밀 또는 상기 결정된 비밀에 기초하는 암호화 키를 사용하여 상기 전자 장치에서 상기 데이터를 암호화하도록 구성된 프로세서를 포함하고,

상기 결정론적 키(DK)를 나타내는 정보는 상기 키 장치에 저장되는, 컴퓨터 시스템.

청구항 24

제23항에 있어서, 상기 컴퓨터 시스템은, 또한, 데이터를 해독하도록 구성되고, 상기 전자 장치의 프로세서는,

상기 키 장치로부터 상기 결정론적 키(DK)를 나타내는 상기 정보를 수신하고,

상기 결정론적 키(DK)를 나타내는 상기 정보에 기초하여 상기 비밀을 결정하고,

상기 결정된 비밀 또는 상기 결정된 비밀에 기초하는 상기 암호화 키를 사용하여 상기 데이터를 해독하도록 구성된, 컴퓨터 구현 방법.

청구항 25

데이터를 암호화하는 전자 장치로서,

상기 전자 장치는 키 장치에 연관되고, 상기 전자 장치는 제1 전자 장치 개인 키(V_{1S})와 제1 전자 장치 공개 키(P_{1S})를 갖는 제1 비대칭 암호 쌍에 연관되고, 상기 키 장치는 제1 키 장치 개인 키(V_{1C})와 제1 키 장치 공개 키(P_{1C})를 갖는 제2 비대칭 암호 쌍에 연관되며, 상기 전자 장치는,

결정론적 키(DK)를 결정하고,

연관된 상기 키 장치로부터 상기 제1 키 장치 공개 키(P_{1C})를 수신하고,

적어도 상기 제1 전자 장치 개인 키(V_{1S})와 상기 결정론적 키(DK)에 기초하여 제2 전자 장치 개인 키(V_{2S})를 결정하고,

적어도 상기 제1 키 장치 공개 키(P_{1C})와 상기 결정론적 키(DK)에 기초하여 제2 키 장치 공개 키(P_{2C})를 결정하고,

적어도 상기 제2 전자 장치 개인 키(V_{2S})와 상기 제2 키 장치 공개 키(P_{2C})에 기초하여 비밀을 결정하고,

결정된 상기 비밀 또는 상기 결정된 비밀에 기초하는 암호화 키를 사용하여 상기 전자 장치에 상기 데이터를 암호화하도록 구성된 처리 장치를 포함하고,

상기 결정론적 키(DK)를 나타내는 정보는, 상기 정보가 저장될 수 있는 상기 키 장치에 전송되는, 컴퓨터 구현 방법.

청구항 26

전자 장치의 처리 장치가 제1항 내지 제22항 중 어느 한 항의 방법을 구현하게 하는 기계 판독가능 명령어를 포함하는, 컴퓨터 프로그램.

발명의 설명

기 술 분 야

[0001] 본 개시 내용은 일반적으로 컴퓨터 관련 보안 및 암호화(encryption) 분야에 관한 것이다. 더욱 구체적으로, 본 개시 내용은, 전자 장치에 저장되는 데이터를 암호화하기 위한 방법, 시스템, 및 장치를 제공한다. 본 개시 내용은, 이동 전화, 태블릿 장치, 또는 랩톱을 포함하지만 이에 한정되지 않는 개인용 연산 장치에 대한 보안을 향상시키는 데 특히 적합하다. 또한, 본 개시 내용은, 암호화된 데이터를 해독하기 위한 방법, 시스템, 및 장치에 관한 것이다.

배 경 기 술

[0002] 암호(Cryptography)는, 전자 장치의 하드 디스크 상의 데이터를 보호하기 위한 기술을 포함하는데, 예를 들어 전자 장치가 분실되거나 도난당한 경우에 그러하다. 전자 장치는, 랩톱 컴퓨터, 데스크톱 컴퓨터, 태블릿 컴퓨터, 이동 통신 장치, 및 다른 임의의 형태의 연산 장치를 포함할 수 있다. 전자 장치는, 자연인, 회사 직원과 같은 사람들의 집단, 은행 시스템과 같은 시스템 등에 연관될 수 있다.

[0003] 일부 경우에, 전자 장치의 하드 디스크 상의 데이터는, 패스워드, 패스프레이즈, 또는 PIN에 의해 보호될 수 있다. 그러나, 4자 내지 8자의 PIN과 같은 짧은 코드는 상이한 문자 조합을 시험함으로써 쉽게 결정될 수 있다. 패스워드와 패스프레이즈는 암호는 PIN보다 안전할 수 있다. 그러나, 보안 수준은, 코드 워드 또는 문장의 긴 세트를 암기하는 사용자에 의존한다.

[0004] 다른 경우에는, 전자 장치의 하드 디스크 상의 데이터를 보호하기 위해 암호 키(cryptographic key)가 사용될 수 있다. 암호 키는, 암호 키를 송신하도록 전자 장치에 물리적으로 접속되어야 하는 USB 드라이브 상에 저장될 수 있다. 그러나, USB 드라이브로부터 전자 장치로 암호 키를 송신하는 동안 생성되는 전자기 신호로 인해, 송신된 키가 여전히 제삼자에 의해 취득될 수 있다.

[0005] 따라서, 이러한 암호 데이터 보호에서의 문제점은 전자 장치로의 비밀 키의 송신에 있다.

[0006] 본 명세서에 포함된 문헌, 행위, 재료, 장치, 물품 등의 임의의 설명은, 이러한 사안들 중 임의의 것 또는 전부가 선행 기술 기반의 일부를 형성하거나 본원의 각 청구항의 우선일 전에 존재하는 것처럼 본 개시 내용과 관련된 분야에서의 일반적인 공통 지식이었음을 인정하는 것으로 받아들여서는 안 된다.

[0007] 본 명세서 전체에 걸쳐, "포함하다"라는 단어 또는 "포함한다" 또는 "포함하는"과 같은 변형은, 명시된 요소, 정수 또는 단계, 혹은 요소, 정수, 또는 단계의 그룹을 포함하지만 다른 임의의 요소, 정수 또는 단계, 혹은 요소, 정수, 또는 단계의 그룹을 배제하지 않음을 의미하는 것으로 이해될 것이다.

[0008] 다음에 따르는 문헌들인, WO2015/175854 A2, CN103440209 B, US2007055880, US2010023771, DE102010002241, US2012011362, US2012100833, US2012331287, WO2013053058, US8522011, US2014082358, US2015213433, 및 EP2975570은, 본 발명의 기술적 배경에 관한 배경 자료를 제공한다.

발명의 내용

[0009] 본 발명은 컴퓨터 구현 방법을 제공할 수 있다. 본 발명은 보안 방법을 제공할 수 있다. 본 발명은 전자 장치(S)에서 데이터를 암호화하는 방법을 제공할 수 있고, 전자 장치는 키 장치(C)에 연관된다. 전자 장치는, 또한, 제1 전자 장치 개인 키(V_{1S})와 제1 전자 장치 공개 키(P_{1S})를 갖는 제1 비대칭 암호 쌍에 연관될 수 있고, 키 장치는, 제1 키 장치 개인 키(V_{1C})와 제1 키 장치 공개 키(P_{1C})를 갖는 제2 비대칭 암호 쌍에 연관될 수 있다.

[0010] 방법은,

[0011] 전자 장치에서 결정론적 키(DK)를 결정하는 단계;

[0012] 전자 장치에서 키 장치로부터 제1 키 장치 공개 키(P_{1C})를 수신하는 단계;

[0013] 전자 장치에서, 적어도 제1 전자 장치 개인 키(V_{1S})와 결정론적 키(DK)에 기초하여 제2 전자 장치 개인 키(V_{2S})를 결정하는 단계;

[0014] 전자 장치에서, 적어도 제1 키 장치 공개 키(P_{1C})와 결정론적 키(DK)에 기초하여 제2 키 장치 공개 키(P_{2C})를 결정하는 단계;

[0015] 적어도 제2 전자 장치 개인 키(V_{2S})와 제2 키 장치 공개 키(P_{2C})에 기초하여 비밀을 결정하는 단계;

[0016] 전자 장치에서, 결정된 비밀 또는 결정된 비밀에 기초하는 암호화 키를 사용하여 데이터를 암호화하는 단계; 및/또는

[0017] 결정론적 키(DK)를 나타내는 정보를, 정보가 저장될 수 있는 키 장치에 전송하는 단계를 포함할 수 있다.

[0018] 방법은, 키 장치에, 결정론적 키(DK)를 나타내는 정보를 저장하는 단계를 더 포함할 수 있다.

[0019] 결정론적 키(DK)는 메시지(M)에 기초할 수 있다. 방법은 전자 장치에서 메시지(M)를 생성하는 단계를 더 포함할 수 있다. 방법은, 메시지(M)의 해시 결정에 기초하여 결정론적 키(DK)를 결정하는 단계를 더 포함할 수 있다. 키 장치에 결정론적 키를 나타내는 정보를 저장하는 단계는, 키 장치에 메시지(M)를 저장하는 단계를 포함할 수 있다.

[0020] 방법은, 적어도 제1 전자 장치 공개 키(P_{1S})와 결정론적 키(DK)에 기초하여 제2 전자 장치 공개 키(P_{2S})를 결정하는 단계를 포함할 수 있다.

[0021] 방법은, 또한, 전자 장치로부터 키 장치로, 공통 생성자(G)와 함께 공통 타원 곡선 암호(ECC) 시스템을 사용하는 것을 나타내는 통지를 전송하는 단계를 포함할 수 있다.

[0022] 제1 전자 장치 공개 키(P_{1S})와 제1 키 장치 공개 키(P_{1C})는, 제1 전자 장치 개인 키(V_{1S})와 제1 키 장치 개인 키(V_{1C}) 각각과 공통 생성자(G)의 타원 곡선 포인트 승산에 기초할 수 있다.

[0023] 방법은, 제1 전자 장치 개인 키(V_{1S})와 제1 전자 장치 공개 키(P_{1S})를 생성하는 단계를 포함할 수 있다. 예를 들어, 제1 전자 장치 개인 키(V_{1S})는 공통 ECC 시스템에서 특정된 허용가능 범위 내의 랜덤 정수에 기초하여 생성될 수 있고, 제1 전자 장치 공개 키(P_{1S})는, $P_{1S} = V_{1S} \times G$ 식에 따라 제1 전자 장치 개인 키(V_{1C})와 공통 생성자(G)의 타원 곡선 포인트 승산에 기초하여 생성될 수 있다.

[0024] 제2 전자 장치 개인 키(V_{2S})는, $V_{2S} = V_{1S} + DK$ 식에 따라 제1 전자 장치 개인 키(V_{1S})와 결정론적 키(DK)의 스칼라 가산에 기초할 수 있다.

[0025] 제2 전자 장치 공개 키(P_{2S})는, 적어도 결정론적 키(DK)와 제1 전자 장치 공개 키(P_{1S})의 타원 곡선 포인트 가산에 기초할 수 있다. 특정한 일례로, 제2 전자 장치 공개 키(P_{2S})는, $P_{2S} = P_{1S} + DK \times G$ 식에 따라 결정론적 키(DK)와 공통 생성자(G)의 타원 곡선 포인트 승산에 대한 제1 전자 장치 공개 키(P_{1S})의 타원 곡선 포인트 가산에 기초할 수 있다.

[0026] 제2 키 장치 공개 키(P_{2C})는, 적어도 결정론적 키(DK)와 제1 키 장치 공개 키(P_{1C})의 타원 곡선 포인트 가산에 기초할 수 있다. 특정한 일례로, 제2 키 장치 공개 키(P_{2C})는, $P_{2C} = P_{1C} + DK \times G$ 식에 따라 결정론적 키(DK)와 공통 생성자(G)의 타원 곡선 포인트 승산에 대한 제1 키 장치 공개 키(P_{1C})의 타원 곡선 포인트 가산에 기초할 수 있다.

[0027] 방법은, 결정된 비밀에 기초하여 암호화 키를 결정하는 단계를 포함할 수 있다. 예를 들어, 암호화 키는, 비밀 및 전자 장치의 식별 정보에 기초할 수 있다. 식별 정보는 전자 장치의 일련번호를 포함할 수 있다.

[0028] 방법은, 서로 통신하도록 전자 장치를 키 장치와 접속하는 단계를 포함할 수 있다. 예를 들어, 전자 장치는, 블루투스 또는 통신 네트워크, 예컨대 인터넷 또는 로컬 통신 네트워크와 같은 무선 프로토콜을 통해 키 장치에 접속될 수 있다. 대안으로, 전자 장치는, 예를 들어 케이블 등의 와이어에 의해 또는 전자 장치의 적절한 포트를 통해 키 장치에 접속될 수 있다.

[0029] 방법은, 전자 장치에 연관된 데이터 저장소에 제1 키 장치 공개 키(P_{1C})를 저장하는 단계를 더 포함할 수 있다.

[0030] 또한 또는 대안으로, 본 발명은, 전술한 바와 같이 데이터를 암호화를 방법에 따라 암호화되어 있는 데이터를 전자 장치에서 해독하는 컴퓨터 구현 방법을 제공할 수 있으며, 데이터를 해독하는 방법은,

[0031] 전자 장치에서, 키 장치로부터 결정론적 키(DK)를 나타내는 정보를 수신하는 단계;

[0032] 결정론적 키(DK)를 나타내는 수신된 정보에 기초하여 비밀을 결정하는 단계; 및

[0033] 전자 장치에서, 비밀 또는 비밀에 기초하는 암호화 키를 사용하여 암호화되어 있는 데이터를 해독하는 단계를 포함할 수 있다.

[0034] 방법은, 키 장치를 인증하는 단계를 포함할 수 있다. 이를 위해, 방법은, 전자 장치에서, 인증 메시지(M_A)를 생성하는 단계 및 인증 메시지(M_A)를 키 장치에 전송하는 단계를 포함할 수 있다.

[0035] 방법은, 키 장치에서, 제2 키 장치 개인 키(V_{2C})와 제2 키 장치 공개 키(P_{2C})를 갖는 제2 비대칭 암호 쌍을 생성하는 단계를 포함할 수 있다. 제2 키 장치 개인 키(V_{2C})는, 결정론적 인증 키(DK_A)와 제1 키 장치 개인 키(V_{1C})에 기초할 수 있다. 제2 키 장치 공개 키(P_{2C})는 결정론적 인증 키(DK_A)와 제1 키 장치 공개 키(P_{1C})에 기초할 수 있다.

[0036] 방법은 결정론적 인증 키(DK_A)를 결정하는 단계를 포함할 수 있다. 예를 들어, 결정론적 인증 키(DK_A)는, 인증 메시지(M_A)에 기초하여, 예컨대 인증 메시지(M_A)의 해시를 결정함으로써, 결정될 수 있다.

[0037] 방법은, 키 장치에서, 결정론적 인증 키(DK_A)와 제2 키 장치 개인 키(V_{2C})에 기초하여, 서명된 인증 메시지(SM_A)를 생성하는 단계를 포함할 수 있다.

[0038] 방법은, 전자 장치에서, 키 장치로부터 서명된 인증 메시지(SM_A)를 수신하는 단계; 서명된 인증 메시지(SM_A)를 제2 키 장치 공개 키(P_{2C})로 유효성 확인(validate)하는 단계; 및 서명된 인증 메시지(SM_A)의 유효성 확인 결과에 기초하여 키 장치를 인증하는 단계를 더 포함할 수 있다.

[0039] 데이터를 해독하는 방법은, 전자 장치에서, 키 장치로부터의 결정론적 키(DK)를 나타내는 정보를 요청하는 단계를 포함할 수 있다. 결정론적 키(DK)를 나타내는 정보가 메시지(M)를 포함하는 실시예에서, 키 장치에서의 요청 수신에 응답하여, 키 장치는, 메시지(M)에 기초하여 서명된 메시지(SM)를 생성할 수 있고 서명된 메시지(SM)를 전자 장치에 전송할 수 있다. 서명된 메시지(SM)는, 메시지(M)와 제1 또는 제2 키 장치 개인 키에 기초하여 생성될 수 있다.

[0040] 데이터를 해독하는 방법은, 전자 장치에서, 서명된 메시지(SM)를 유효성 확인하는 단계; 및 전자 장치에서, 데이터를 해독하기 위해 비밀이 결정될 수 있도록 메시지(M)를 검색하는 단계를 더 포함할 수 있다.

[0041] 본 발명은, 또한, 전술한 방법(들)의 임의의 양태 또는 실시예를 구현하기 위한 컴퓨터 구현 시스템을 제공할 수 있다. 본 발명은, 전자 장치에서 데이터를 암호화하기 위한 컴퓨터 시스템을 제공할 수 있고, 컴퓨터 시스템은,

[0042] 제1 전자 장치 개인 키(V_{1S})와 제1 전자 장치 공개 키(P_{1S})를 갖는 제1 비대칭 암호 쌍에 연관된, 전자 장치; 및

[0043] 제1 키 장치 개인 키(V_{1C})와 제1 키 장치 공개 키(P_{1C})를 갖는 제2 비대칭 암호 쌍에 연관된, 키 장치를 포함하고,

[0044] 전자 장치는,

[0045] 결정론적 키(DK)를 결정하고,

[0046] 키 장치로부터 제1 키 장치 공개 키(P_{1C})를 수신하고,

[0047] 적어도 제1 전자 장치 개인 키(V_{1S})와 결정론적 키(DK)에 기초하여 제2 전자 장치 개인 키(V_{2S})를 결정하고,

[0048] 적어도 상기 제1 키 장치 공개 키(P_{1C})와 상기 결정론적 키(DK)에 기초하여 제2 키 장치 공개 키(P_{2C})를 결정하고,

[0049] 적어도 제2 전자 장치 개인 키(V_{2S})와 제2 키 장치 공개 키(P_{2C})에 기초하여 비밀을 결정하고,

[0050] 결정된 비밀 또는 결정된 비밀에 기초하는 암호화 키를 사용하여 전자 장치에서 데이터를 암호화하도록 구성된 프로세서를 포함하고,

[0051] 결정론적 키(DK)를 나타내는 정보는 키 장치에 저장된다.

[0052] 결정론적 키(DK)는 메시지(M)에 기초할 수 있다. 프로세서는 메시지(M)를 생성하도록 구성될 수 있다. 프로세서는, 또한, 메시지(M)의 해시 결정에 기초하여 결정론적 키(DK)를 결정하도록 구성될 수 있다.

[0053] 프로세서는, 적어도 제1 전자 장치 공개 키(P_{1S})와 결정론적 키(DK)에 기초하여 제2 전자 장치 공개 키(P_{2S})를 결정하도록 구성될 수 있다.

[0054] 시스템에서는, 전자 장치와 키 장치 간의 통신을 확립하도록 전자 장치가 인터페이스를 포함할 수 있고 키 장치가 키 장치 인터페이스를 포함할 수 있다. 예를 들어, 전자 장치는, 블루투스 또는 통신 네트워크, 예컨대 인터넷 또는 로컬 통신 네트워크와 같은 무선 프로토콜을 통해 키 장치에 접속될 수 있다. 대안으로, 전자 장치는, 예를 들어, 와이어, 예컨대 케이블에 의해, 또는 전자 장치의 적절한 포트를 통해 키 장치에 접속될 수 있다.

[0055] 전자 장치의 인터페이스는, 공통 생성자(G)와 함께 공통 타원 곡선 암호(ECC) 시스템을 나타내는 통지를 연관된 키 장치의 키 장치 인터페이스에 전송하도록 구성될 수 있다.

[0056] 제1 전자 장치 공개 키(P_{1S})와 제1 키 장치 공개 키(P_{1C})는, 제1 전자 장치 개인 키(V_{1S}) 및 제1 키 장치 개인 키(V_{1C}) 각각과 생성자(G)의 타원 곡선 포인트 승산에 기초할 수 있다.

[0057] 프로세서는, 제1 전자 장치 개인 키(V_{1S})와 제1 전자 장치 공개 키(P_{1S})를 생성하도록 구성될 수 있다. 예를 들어, 제1 전자 장치 개인 키(V_{1S})는, 공통 ECC 시스템에서 특정된 허용가능 범위 내의 랜덤 정수에 기초하여 생성될 수 있고, 제1 전자 장치 공개 키(P_{1S})는, $P_{1S} = V_{1S} \times G$ 식에 따라 제1 전자 장치 개인 키(V_{1C})와 공통 생성자(G)의 타원 곡선 포인트 승산에 기초하여 생성될 수 있다.

[0058] 제2 전자 장치 개인 키(V_{2S})는, $V_{2S} = V_{1S} + DK$ 식에 따라 제1 전자 장치 개인 키(V_{1S})와 결정론적 키(DK)의 스칼라 가산에 기초할 수 있다.

[0059] 제2 전자 장치 공개 키(P_{2S})는, 적어도 결정론적 키(DK)와 제1 전자 장치 공개 키(P_{1S})의 타원 곡선 포인트 가산에 기초할 수 있다. 특정한 일례로, 제2 전자 장치 공개 키(P_{2S})는, $P_{2S} = P_{1S} + DK \times G$ 식에 따라 결정론적 키(DK)와 공통 생성자(G)의 타원 곡선 포인트 승산에 대한 제1 전자 장치 공개 키(P_{1S})의 타원 곡선 포인트 가산에 기초할 수 있다.

[0060] 제2 키 장치 공개 키(P_{2C})는, 적어도 결정론적 키(DK)와 제1 키 장치 공개 키(P_{1C})의 타원 곡선 포인트 가산에 기초할 수 있다. 특정한 일례로, 제2 키 장치 공개 키(P_{2C})는, $P_{2C} = P_{1C} + DK \times G$ 식에 따라 결정론적 키(DK)와 공통 생성자(G)의 타원 곡선 포인트 승산에 대한 제1 키 장치 공개 키(P_{1C})의 타원 곡선 포인트 가산에 기초할 수 있다.

[0061] 프로세서는, 결정된 비밀에 기초하여 암호화 키를 결정하도록 구성될 수 있다. 예를 들어, 암호화 키는, 결정된 비밀 및 전자 장치의 식별 정보에 기초할 수 있다. 식별 정보는 전자 장치의 일련번호를 포함할 수 있다.

[0062] 전자 장치는, 제1 키 장치 공개 키(P_{1C})가 저장될 수 있는 데이터 저장소를 포함할 수 있다.

[0063] 키 장치는, 적어도 결정론적 키를 나타내는 정보를 저장하기 위한 키 장치 데이터 저장소를 포함할 수 있다.

[0064] 전술한 바와 같은 컴퓨터 시스템은, 또한, 데이터를 해독하도록 구성되고, 전자 장치의 프로세서는,

[0065] 키 장치로부터 결정론적 키(DK)를 나타내는 정보를 수신하고;

[0066] 결정론적 키(DK)를 나타내는 정보에 기초하여 비밀을 결정하고;

[0067] 결정된 비밀 또는 결정된 비밀에 기초하는 암호화 키를 사용하여 데이터를 해독하도록 구성된다.

[0068] 프로세서는 키 장치를 인증하도록 구성될 수 있다. 이를 위해, 프로세서는, 인증 메시지(M_A)를 생성하고 인증 메시지(M_A)를 키 장치에 전송할 수 있다.

[0069] 키 장치는, 제2 키 장치 개인 키(V_{2C})와 제2 키 장치 공개 키(P_{2C})를 갖는 제2 비대칭 암호 쌍을 생성하도록 구성될 수 있는 키 장치 프로세서를 포함할 수 있다. 제2 키 장치 개인 키(V_{2C})는, 결정론적 인증 키(DK_A)와 제1 키 장치 개인 키(V_{1C})에 기초할 수 있다. 제2 키 장치 공개 키(P_{2C})는, 결정론적 인증 키(DK_A)와 제1 키 장치 공개 키(P_{1C})에 기초할 수 있다.

[0070] 키 장치 프로세서는, 또한, 결정론적 인증 키(DK_A)를 결정하도록 구성될 수 있다. 예를 들어, 결정론적 인증 키(DK_A)는, 인증 메시지(M_A)에 기초하여, 예컨대 인증 메시지(M_A)의 해시를 결정함으로써, 결정될 수 있다.

[0071] 키 장치 프로세서는, 결정론적 인증 키(DK_A)와 제2 키 장치 개인 키(V_{2C})에 기초하여 서명된 인증 메시지(SM_A)를 생성하도록 구성될 수 있다.

[0072] 전자 장치의 프로세서는, 키 장치로부터 서명된 인증 메시지(SM_A)를 수신하고, 서명된 인증 메시지(SM_A)를 제2 키 장치 공개 키(P_{2C})로 유효성 확인하고, 서명된 인증 메시지(SM_A)의 유효성 확인 결과에 기초하여 키 장치를 인증하도록 구성될 수 있다.

[0073] 전자 장치의 프로세서는, 키 장치로부터의 결정론적 키(DK)를 나타내는 정보를 요청할 수 있다. 결정론적 키(DK)를 나타내는 정보가 메시지(M)를 포함하는 실시예에서, 키 장치에서의 요청 수신에 응답하여, 키 장치 프로세서는, 메시지(M)에 기초하여 서명된 메시지(SM)를 생성할 수 있고 서명된 메시지(SM)를 전자 장치에 전송할 수 있다. 서명된 메시지(SM)는, 메시지(M)와 제1 또는 제2 키 장치 개인 키에 기초하여 생성될 수 있다.

[0074] 전자 장치의 프로세서는, 또한, 서명된 메시지를 유효성 확인하고, 데이터를 해독하기 위해 비밀이 결정될 수 있게끔 메시지(M)를 검색하도록 구성될 수 있다.

[0075] 데이터를 해독하기 위한 전자 장치로서, 이 전자 장치는 키 장치에 연관되고, 전자 장치는 제1 전자 장치 개인 키(V_{1S})와 제1 전자 장치 공개 키(P_{1S})를 갖는 제1 비대칭 암호 쌍에 연관되고, 키 장치는 제1 키 장치 개인 키(V_{1C})와 제1 키 장치 공개 키(P_{1C})를 갖는 제2 비대칭 암호 쌍에 연관되며, 전자 장치는,

[0076] 결정론적 키(DK)를 결정하고,

[0077] 연관된 키 장치로부터 제1 키 장치 공개 키(P_{1C})를 수신하고,

[0078] 적어도 제1 전자 장치 개인 키(V_{1S})와 결정론적 키(DK)에 기초하여 제2 전자 장치 개인 키(V_{2S})를 결정하고,

[0079] 적어도 제1 키 장치 공개 키(P_{1C})와 결정론적 키(DK)에 기초하여 제2 키 장치 공개 키(P_{2C})를 결정하고,

[0080] 적어도 제2 전자 장치 개인 키(V_{2S})와 제2 키 장치 공개 키(P_{2C})에 기초하여 비밀을 결정하고,

[0081] 결정된 비밀 또는 결정된 비밀에 기초하는 암호화 키를 사용하여 전자 장치에 데이터를 암호화하도록 구성된 처리 장치를 포함하고,

[0082] 결정론적 키(DK)를 나타내는 정보는, 정보가 저장될 수 있는 키 장치에 전송된다.

[0083] 컴퓨터 프로그램은, 전자 장치의 처리 장치가 전술한 방법들 중 임의의 방법을 구현하게 하는 기계 판독가능 명

령어를 포함한다.

[0084] 본 발명의 하나 이상의 실시예 또는 양태는, 제1 노드(C)에서, 제1 노드(C)와 제2 노드(S)와 공통되는 공통 비밀(CS)을 결정하는 컴퓨터 구현 방법을 포함하거나 사용할 수 있다. 제1 노드(C)는 제1 노드 마스터 개인 키(V_{1C})와 제1 노드 마스터 공개 키(P_{1C})를 갖는 제1 비대칭 암호 쌍에 연관될 수 있고, 제2 노드(S)는 제2 노드 마스터 개인 키(V_{1S})와 제2 노드 마스터 공개 키(P_{1S})를 갖는 제2 비대칭 암호 쌍에 연관될 수 있다. 이 방법은,

[0085] 적어도 제1 노드 마스터 개인 키(V_{1C})와 결정론적 키(DK)에 기초하여 제1 노드 제2 개인 키(V_{2C})를 결정하는 단계;

[0086] 적어도 제2 노드 마스터 공개 키(P_{1S})와 결정론적 키(DK)에 기초하여 제2 노드 제2 공개 키(P_{2S})를 결정하는 단계; 및

[0087] 제1 노드 제2 개인 키(V_{2C})와 제2 노드 제2 공개 키(P_{2S})에 기초하여 공통 비밀(CS)을 결정하는 단계를 포함할 수 있고,

[0088] 제2 노드(S)는, 제1 노드 제2 공개 키(P_{2C})와 제2 노드 제2 개인 키(V_{2S})에 기초하는 동일한 공통 비밀(S)을 갖고,

[0089] 제1 노드 제2 공개 키(P_{2C})는, 적어도 제1 노드 마스터 공개 키(P_{1C})와 결정론적 키(DK)에 기초하고,

[0090] 제2 노드 제2 개인 키(V_{2S})는, 적어도 제2 노드 마스터 개인 키(V_{1S})와 결정론적 키(DK)에 기초한다.

[0091] 결정론적 키(DK)는 메시지(M)에 기초한다.

[0092] 따라서, 본 발명은, 전자 장치 및/또는 전자 장치 상에 저장되는 데이터의 향상된 보안을 위한 기술과 장치를 제공할 수 있다. 또한, 본 발명은, 본 발명의 향상된 보안 메커니즘 때문에 개선된 전자 장치를 제공할 수 있다.

도면의 간단한 설명

[0093] 본 개시 내용의 예들을 면을 참조하여 설명한다.

도 1은 데이터를 암호화하는 예시적인 시스템의 개략도이다.

도 2는 도 1의 전자 장치와 키 장치를 등록하기 위한 컴퓨터 구현 방법의 흐름도이다.

도 3은 비밀을 사용하여 도 1의 전자 장치에서 데이터를 암호화하기 위한 컴퓨터 구현 방법의 흐름도이다.

도 4는 도 1의 키 장치를 인증하는 컴퓨터 구현 방법의 흐름도이다.

도 5는 키 장치의 인증 후에 전자 장치에서 암호화된 데이터를 해독하는 컴퓨터 구현 방법의 흐름도이다.

도 6은 예시적인 처리 장치의 개략도를 도시한다.

발명을 실시하기 위한 구체적인 내용

[0094] 개요

[0095] 이제, 전자 장치에서 데이터를 해독하는 방법, 장치, 및 시스템을 설명한다.

[0096] 도 1은 키 장치(5)와 통신하는 전자 장치(3)를 포함하는 컴퓨터 시스템(1)을 도시한다. 전자 장치(3)는 연관된 제1 처리 장치(23)를 갖고, 키 장치(5)는 연관된 제2 처리 장치(25)를 갖는다. 전자 장치(3)는, 랩톱 컴퓨터, 데스크 컴퓨터, 태블릿 컴퓨터, 이동 통신 장치, 컴퓨터 서버, 또는 데이터를 처리할 수 있는 다른 임의의 연산 장치와 같은 개인용 전자 장치일 수 있다. 도 1에 도시된 바와 같은 이러한 특정 예에서, 전자 장치(3)는 랩톱 컴퓨터로 대표된다.

[0097] 키 장치(5)는, 이동 통신 장치, USB 드라이브 등과 같은 휴대용 메모리 장치 등과 같은 다른 개인용 전자 장치일 수 있다. 도 1에 도시된 바와 같은 이러한 특정 예에서, 키 장치(5)는 이동 통신 장치로 대표된다.

[0098] 전자 장치(3)는, 블루투스 또는 통신 네트워크, 예컨대 인터넷 또는 로컬 통신 네트워크와 같은 무선 프로토콜

을 통해 키 장치(5)와 통신할 수 있다. 대안으로, 전자 장치(3)는, 예를 들어, 전자 장치의 USB 포트를 통해 또는 케이블 접속을 통해 키 장치(5)에 물리적으로 접속될 수 있다. 도 1에 도시된 바와 같은 이러한 특정 예에서, 전자 장치(3)는 블루투스(7)를 통해 키 장치 (5)와 통신한다.

[0099] 전자 장치(3)는, 전자 장치 마스터 개인 키(V_{1S})와 전자 장치 마스터 공개 키(P_{1S})를 갖는 제1 비대칭 암호 쌍에 연관된다. 키 장치(5)는, 키 장치 마스터 개인 키(V_{1C})와 키 장치 마스터 공개 키(P_{1C})를 갖는 제2 비대칭 암호 쌍에 연관된다. 제1 및 제2 비대칭 암호 쌍은 등록 동안 생성될 수 있다. 전자 장치(3)와 키 장치(5)에 의해 수행되는 등록 방법(200, 300)을 도 2를 참조하여 이하에서 더욱 상세히 설명한다. 각 장치의 공개 키는, 예를 들어, 블루투스(7)를 통해 공개적으로 장치들(3, 5) 간에 공유될 수 있다.

[0100] 본 발명의 실시예들은, 제1 노드(C)에서, 제1 노드(C) 및 제2 노드(S)와 공통되는 공통 비밀(CS)을 결정하고, 제1 노드(C)가 제1 노드 마스터 개인 키(V_{1C})와 제1 노드 마스터 공개 키(P_{1C})를 갖는 제1 비대칭 암호씩 쌍에 연관되고, 제2 노드(S)가 제2 노드 마스터 개인 키(V_{1S})와 제2 노드 마스터 공개 키(P_{1S})를 갖는 제2 비대칭 암호 쌍에 연관되는 것으로서 대략적으로 제공되는 기술(또는 이러한 기술의 변형(들))을 포함할 수 있고, 그 방법 또는 기술은,

[0101] 적어도 제1 노드 마스터 개인 키(V_{1C})와 결정론적 키(DK)에 기초하여 제1 노드 제2 개인 키(V_{2C})를 결정하는 단계;

[0102] 적어도 제2 노드 마스터 공개 키(P_{1S})와 결정론적 키(DK)에 기초하여 제2 노드 제2 공개 키(P_{2S})를 결정하는 단계; 및

[0103] 제1 노드 제2 개인 키(V_{2C})와 제2 노드 제2 공개 키(P_{2S})에 기초하여 공통 비밀(CS)을 결정하는 단계를 포함하고,

[0104] 제2 노드(S)는, 제1 노드 제2 공개 키(P_{2C})와 제2 노드 제2 개인 키(V_{2S})에 기초하는 동일한 공통 비밀(CS)을 갖고,

[0105] 제1 노드 제2 공개 키(P_{2C})는, 적어도 제1 노드 마스터 공개 키(P_{1C})와 결정론적 키(DK)에 기초하고,

[0106] 제2 노드 제2 개인 키(V_{2S})는, 적어도 제2 노드 마스터 개인 키(V_{1S})와 결정론적 키(DK)에 기초한다.

[0107] 결정론적 키(DK)는 메시지(M)에 기초할 수 있다.

[0108] 본 발명의 예시적인 일 실시예에 따르면, 전자 장치(3)에서 데이터를 암호화하기 위해, 비밀은 전술한 바와 유사한 기술에 기초하여 결정된다. 비밀은, 전자 장치(3)의 개인 암호 키와 키 장치(5)의 공개 암호 키에 의해 결정된다. 비밀을 결정함으로써, 결정된 비밀에 기초하는 암호화 키(E)를 사용하여 데이터가 암호화될 수 있다. 하나 이상의 예에서, 비밀은 암호화 키(E)로서 사용될 수 있다. 이 기술의 장점들 중 하나는, 장치들(3, 5) 중 어떠한 장치에도 비밀 또는 암호화 키(E)를 송신하거나 저장할 필요가 없다는 것이다. 이것은 종래 기술의 구성에 비해 훨씬 더 안전한 해결책을 제공한다.

[0109] 전자 장치(3)에서 비밀을 사용하여 데이터를 암호화하기 위해, 방법(400)은 장치들(3, 5) 간에 어떠한 개인 키도 통신하지 않고 수행되며, 이를 도 3을 참조하여 더 상세히 설명한다.

[0110] 일반적으로, 전자 장치(3)에 의해 수행되는 데이터를 암호화하는 방법은, 키 장치(5)와 통신하도록 전자 장치(3)를 키 장치(5)와 초기에 접속하는 단계를 포함한다. 통신은 유선 접속 또는 블루투스(7)와 같은 무선 접속을 통해 확립될 수 있다.

[0111] 방법은, 전자 장치(3)에 의해 생성되는 메시지(M)에 기초할 수 있는 결정론적 키(DK)를 결정하는 단계를 더 포함한다. 예를 들어, 전자 장치(3)의 처리 장치(23)는, 메시지(M)를 생성할 수 있고 이어서 표준 알고리즘을 사용하여 결정론적 키(DK)를 형성하는 메시지의 해시를 생성할 수 있다.

[0112] 방법은, 적어도 전자 장치 마스터 개인 키(V_{1S})와 결정론적 키(DK)에 기초하여 제2 전자 장치 개인 키(V_{2S})를 결정하는 단계, 및 키 장치 마스터 공개 키(P_{1C})와 결정론적 키(DK)에 기초하여 제2 키 장치 공개 키(P_{2C})를 결정하는 단계를 더 포함한다. 이어서, 비밀은, 제2 전자 장치 개인 키(V_{2S})와 제2 키 장치 공개 키(P_{2C})에 기초하여

결정된다. 선택적으로, 방법은, 적어도 전자 장치 마스터 공개 키(P_{1S})와 결정론적 키(DK)에 기초하여 제2 전자 장치 공개 키(P_{2S})를 결정하는 단계를 포함할 수 있다.

[0113] 추가 방법 단계에서, 데이터는, 결정된 비밀에 기초하는 암호화 키(E)를 사용하여 암호화될 수 있다. 전술한 바와 같이, 결정된 비밀 자체는 암호화 키(E)로서 사용될 수 있고, 또는 암호화 키(E)가 비밀에 기초하여 결정될 수 있다. 전자 장치에 데이터를 암호화한 후에, 비밀은 삭제될 수 있고, 결정론적 키(DK) 또는 메시지(M)만이 안전하게 저장될 수 있는 키 장치(5)에 전송될 수 있다. 이어서, 키 장치(5)에 저장된 결정론적 키(DK) 또는 메시지(M)는 암호화된 데이터를 해독하는 데 사용될 수 있다.

[0114] 암호화될/해독될 데이터는 하나 이상의 개별 파일, 파일을 포함하는 하나 이상의 폴더, 또는 전자 장치의 전체 하드 드라이브를 포함할 수 있음을 이해할 것이다. 일부 예에서, 방법은, 암호화/해독될 파일 및/또는 폴더를 선택하도록 사용자에게 촉구하는 단계를 포함할 수 있다. 이 경우, 키 장치(5)는 각 파일 및 폴더에 대한 결정론적 키를 나타내는 정보를 저장하고 이에 따라 이들을 링크할 수 있다.

[0115] 등록 방법(200, 300)

[0116] 등록 방법(200, 300)의 일례를 도 2를 참조하여 설명하며, 여기서, 방법(200)은 전자 장치(3)에 의해 수행되고, 방법(300)은 키 장치(5)에 의해 수행된다. 이 방법은 각 장치(3, 5)에 대한 제1 및 제2 비대칭 암호 쌍을 확립하는 단계를 포함한다.

[0117] 비대칭 암호쌕 쌍은 공개 키 암호화에 사용되는 것과 같은 연관된 개인 키와 공개 키를 포함한다. 이 예에서, 비대칭 암호 쌍은 타원 곡선 암호(ECC) 및 타원 곡선 연산의 속성을 사용하여 생성된다.

[0118] ECC를 위한 표준은, 효율적 암호 그룹(www.sceg.org)에 의해 기술된 것과 같은 공지된 표준을 포함할 수 있다. 타원 곡선 암호는, 또한, 미국특허 US 5,600,725, US 5,761,305, US 5,889,865, US 5,896,455, US 5,933,504, US 6,122,736, US 6,141,420, US 6,618,483, US 6,704,870, US 6,785,813, US 6,078,667, US 6,792,530에 개시되어 있다.

[0119] 방법(200, 300)에서, 이것은, 전자 장치(3) 및 키 장치(5)에 의한 공통 ECC 시스템에 대한 확정(210, 310) 및 공통 생성자(G)의 사용을 포함한다. 일례로, 공통 ECC 시스템은 비트코인에 의해 사용되는 ECC 시스템인 secp256K1에 기초할 수 있다. 공통 생성자(G)는, 선택될 수 있고, 랜덤하게 생성될 수 있고, 또는 할당될 수 있다.

[0120] 전자 장치(3)가 랩톱 컴퓨터이고 키 장치(5)가 이동 통신 장치인 도 1에 도시된 특정 예에서, 각 장치(3, 5) 간의 통신은, 이동 통신 장치(5)에 설치된 전용 애플리케이션과 통신하는 애플리케이션 프로그래밍 인터페이스(API)에 의해 실현된다. 이를 위해, 이동 통신 장치에 설치된 전용 애플리케이션과 호환되는 랩톱 컴퓨터에 소프트웨어를 다운로드하여 설치할 수 있다.

[0121] 특정 예에서, 키 장치(5)에는, 키 장치용 소프트웨어 애플리케이션뿐만 아니라 전자 장치용 소프트웨어도 제공될 수 있다. 이러한 방식으로, 키 장치가 전자 장치에 접속되는 경우, 소프트웨어는 키 장치로부터 설치를 실행함으로써 전자 장치에 설치될 수 있다.

[0122] 이제 전자 장치(3)에 의해 수행되는 방법(200)을 참조하면, 방법(200)은 공통 ECC 시스템 및 공통 생성자(G)에 대한 확정(210)을 포함한다. 이는, 공통 생성자 및 공통 ECC 시스템을 나타내는 정보를 전자 장치(3)로부터 키 장치(5)로 전송하는 것, 또는 원격 서버 컴퓨터와 같은 제3 장치로부터 정보를 수신하는 것을 포함할 수 있다. 예를 들어, 전자 장치(3)는, 공통 생성자(G)를 갖는 공통 ECC 시스템을 사용하는 것을 나타내는 통지를 블루투스(7)를 통해 키 장치(5)에 전송할 수 있다. 이어서, 키 장치(5)는, 공통 ECC 시스템 및 공통 생성자(G)를 사용하는 것에 대한 확인을 나타내는 통지를 전송함으로써 확정할 수 있다(310).

[0123] 방법(200)은, 또한, 전자 장치 마스터 개인 키(V_{1S})와 전자 장치 마스터 공개 키(P_{1S})를 포함하는 제1 비대칭 암호 쌍을 전자 장치(3)에서 생성하는 단계(220)를 포함한다. 이러한 특정 예에서, 전자 장치 마스터 개인 키(V_{1S})는, 공통 ECC 시스템에서 특정된 허용가능한 범위의 랜덤 정수에 적어도 부분적으로 기초하여 결정된다. 이어서, 전자 장치 마스터 공개 키(P_{1S})는, 이하의 식에 따라 전자 장치 마스터 개인 키(P_{1S})와 공통 생성자(G)의 타원 곡선 포인트 승산에 기초하여 결정된다.

[0124] $P_{1S} = V_{1S} \times G$ (식 1)

[0125] 따라서, 제1 비대칭 암호 쌍은,

[0126] V_{1S} : 전자 장치에 의해 비밀로 유지되는 전자 장치 마스터 개인 키; 및

[0127] P_{1S} : 공개적으로 알려져 있는 전자 장치 마스터 공개 키를 포함한다.

[0128] 전자 장치(3)는 전자 장치(3)에 연관된 제1 데이터 저장소(13)에 제1 비대칭 암호 쌍을 저장할 수 있다. 보안을 위해, 전자 장치 마스터 개인 키(V_{1S})는, 그 키가 비밀로 유지되는 것을 보장하도록 제1 데이터 저장 장치(13)의 안전한 부분에 저장될 수 있다.

[0129] 이 예에서, 방법(200)은 전자 장치 공개 마스터 키(P_{1S})를 키 장치(3)에 전송하는 단계(230)를 포함한다. 그러나, 전자 장치(3)에 데이터를 암호화하기 위해, 이 단계는 필요하지 않을 수도 있다.

[0130] 이제, 키 장치(5)에 의해 수행되는 방법(300)을 참조해 볼 때, 이러한 특정 예에서, 키 장치(5)는, 전자 장치 마스터 공개 키(P_{1S})를 수신하고, 수신된 전자 장치 마스터 공개 키(P_{1S})를 키 장치(5)의 저장 요소 내에 저장한다(320).

[0131] 방법(200)과 유사하게, 키 장치(5)에서의 방법(300)은, 키 장치 마스터 개인 키(V_{1C})와 키 장치 마스터 공개 키(P_{1C})를 포함하는 제2 비대칭 암호 쌍을 생성하는 단계(340)를 포함한다. 키 장치 마스터 개인 키(V_{1C})도, 공통 ECC 시스템에서 특정된 허용가능 범위 내의 랜덤 정수이다. 이어서, 키 장치 마스터 공개 키(P_{1C})는 이하의 식에 의해 결정된다.

[0132] $P_{1C} = V_{1C} \times G$ (식 2)

[0133] 따라서, 제2 비대칭 암호 쌍은,

[0134] V_{1C} : 키 장치에 의해 비밀로 유지되는 키 장치 마스터 개인 키; 및

[0135] P_{1C} : 공개적으로 알려져 있는 키 장치 마스터 공개 키를 포함한다.

[0136] 키 장치(5)는, 제2 비대칭 암호 쌍을 키 장치의 제2 데이터 저장소(15)에 저장할 수 있다. 방법(300)은, 키 장치 마스터 공개 키(P_{1C})를 저장 장치(13)에 저장될 수 있는 전자 장치(3)에 전송하는 단계(330)를 더 포함한다.

[0137] 일부 대안에서, 각 공개 마스터 키는, 신뢰받는 제삼자와 같은 제3 장치에 연관된 제3 데이터 저장소에서 수신되고 저장될 수 있다. 이것은, 인증 기관과 같은 공개 디렉터리로서 기능하는 제삼자를 포함할 수 있다. 따라서, 일부 예에서, 키 장치 마스터 공개 키(P_{1C})는, 비밀을 결정할 필요가 있을 때에만 전자 장치(3)에 의해 요청 및 수신될 수 있다.

[0138] 등록 단계는 초기 설정으로서 한 번 발생할 필요가 있을 수 있다. 이후, 마스터 키는, 특히 결정론적 키(DK)에 의존하는 비밀을 결정하도록 안전한 방식으로 재사용될 수 있다.

[0139] <u>전자 장치(3)에서의 데이터 암호화</u>

[0140] 이제, 전자 장치(3)의 개인 키와 키 장치(5)의 공개 키에 기초하는 비밀을 결정함으로써 전자 장치(3)에서 데이터를 암호화하는 예시적인 방법(400)을 도 3을 참조하여 설명한다. 비밀은 한 사이클에만 사용될 수 있으며, 각 사이클은 데이터의 암호화와 해독의 완전한 라운드(round)이다.

[0141] 새로운 개인 및 공개 키는 암호화와 해독의 각 사이클마다 전자 장치와 키 장치 모두에 대해 결정될 수 있다는 것을 이해할 것이다. 새로운 개인 및 공개 키는, 예를 들어, 본원에 전체적으로 참고로 원용된 상술한 바와 같은 공동 출원에 더욱 상세히 기술된 바와 같이 메시지(M)를 리해싱(rehash)함으로써 결정될 수 있다. 이러한 방식으로, 각 서브 키가 생성될 수 있고, 이러한 각 서브 키는 마스터 키에 링크된다.

[0142] <u>메시지(M) 생성(410)</u>

[0143] 이 예에서, 방법(400)은 전자 장치(3)에서 메시지(M)를 생성하는 단계(410)를 포함한다. 메시지(M)는, 랜덤, 의사 랜덤, 또는 사용자 정의형일 수 있다. 일례로, 메시지(M)는 유닉스 타임과 논스(nonce)(및 임의의 값)에 기초한다. 예를 들어, 메시지(M)는 다음과 같이 제공될 수 있다.

[0144] 메시지(M) = 유닉스 타임 + 논스 (식 3)

[0145] 일부 예에서, 메시지(M)는 임의적이다. 그러나, 메시지(M)는, 일부 응용분야에서 유용할 수 있는 선택적 값(예컨대, 유닉스 타임 등)을 가질 수 있음을 이해해야 한다.

[0146] 방법(400)은, 메시지(M)를 블루투스(7)를 통해 메시지(M)가 저장될 키 장치(5)에 전송하는 단계(420)를 포함한다. 중요한 것은, 메시지(M)가 개인 키에 관한 정보를 포함하지 않으므로, 메시지(M)가 비보안 네트워크를 통해 키 장치(5)에 전송될 수 있다는 것이다.

[0147] 메시지(M)가 키 장치(5)에 어느 때라도 통신될 수 있음을 이해할 것이다. 예를 들어, 데이터 암호화가 완료된 후에 메시지(M)가 키 장치(5)에 전송될 수 있다.

[0148] 결정론적 키의 결정(430)

[0149] 방법(400)은, 메시지(M)에 기초하여 결정론적 키(DK)를 결정하는 단계(430)를 더 포함한다. 이 예에서, 방법은 메시지의 암호 해시를 결정하는 단계를 포함할 수 있다. 암호 해시 알고리즘의 일례는, 256비트 결정론적 키(DK)를 생성하기 위한 SHA-256을 포함한다. 즉, 아래와 같다.

[0150] DK = SHA-256(M) (식 4)

[0151] 메시지의 선택은, 암호화 키(E)를 생성할 목적으로 임의적일 수 있으며, 각 암호화/해독 사이클마다 새롭게 선택될 것이다. 이 예에서, 메시지(M)는 메시지 길이를 짧게 유지하도록 해싱에 의해 160비트로 감소된다.

[0152] 다른 해시 알고리즘들이 사용될 수 있다는 것을 이해해야 한다. 이것은 SHA(보안 해시 알고리즘) 군의 다른 해시 알고리즘을 포함할 수 있다. 일부 특정 예에서는, SHA3-224, SHA3-256, SHA3-384, SHA3-512, SHAKE128, SHAKE256을 포함하는 SHA-3 서브세트의 인스턴스를 포함한다. 다른 해시 알고리즘은, RACE 인테그리티 프리미티브 이밸류에이션 메시지 다이제스트(RIPEMD) 군의 알고리즘을 포함할 수 있다. 특정 예는 RIPEMD-160을 포함할 수 있다. 다른 해시 함수는, Zémor-Tillich 해시 함수 및 냅색(knapsack) 기반 해시 함수에 기초할 수 있다.

[0153] 제2 개인 및 공개 키의 결정(440, 450, 460)

[0154] 이어서, 방법(400)은, 결정론적 키(DK), 즉, 메시지(M)의 해시에 기초하여 다음에 따르는 제2 키들을 결정하는 단계(440, 450, 460)를 포함한다.

[0155] 제2 전자 장치 개인 키(V_{2S})는, 전자 장치 마스터 개인 키(V_{1S})와 메시지(M)의 해시에 기초하여 결정된다(440). 이는 다음 식에 따라 전자 장치 마스터 개인 키(V_{1S})와 메시지 해시(M)의 스칼라 가산에 기초할 수 있다.

[0156] $V_{2S} = V_{1S} + \text{SHA-256}(M)$ (식 5)

[0157] 제2 전자 장치 공개 키(P_{2S})는, 전자 장치 마스터 공개 키(P_{1S})와 메시지(M)의 해시에 기초하여 결정된다(450). 이것은 다음에 따르는 식에 기초하여 결정될 수 있다.

[0158] $P_{2S} = P_{1S} + \text{SHA-256}(M) \times G$ (식 6)

[0159] 제2 키 장치 공개 키(P_{2C})는, 키 장치 마스터 공개 키(P_{1C})와 메시지(M)의 해시에 기초하여 결정된다(460). 이것은 다음에 따르는 식에 기초하여 결정될 수 있다.

[0160] $P_{2C} = P_{1C} + \text{SHA-256}(M) \times G$ (식 7)

[0161] 타원 곡선 암호가 적용되는 이러한 특정 예에서, 'G'는 생성자를 나타내고, 연산자 '+'는 타원 곡선의 포인트 가산을 나타내며, 연산자 'x'는 타원 곡선 포인트 승산을 나타낸다는 점에 주목해야 한다.

[0162] 또한, 데이터 암호화를 위해, 제2 전자 장치 공개 키(P_{2S})를 결정할 필요가 없을 수 있다는 점에 주목해야 한다. 추가로 후술하는 바와 같이, 비밀을 결정하기 위해, 제2 전자 장치 공개 키(P_{2S})가 필요하지 않을 수 있다.

[0163] 비밀 결정(470)

[0164] 이어서, 전자 장치(3)는, 결정된 제2 전자 장치 개인 키(V_{2S})와 결정된 제2 키 장치 공개 키(P_{2C})에 기초하여 비밀을 결정할 수 있다(470). 비밀은 이하의 식에 따라 전자 장치(3)에 의해 결정될 수 있다.

[0165] CS = $V_{2C} \times P_{2S}$ (식 8)

[0166] <u>비밀 및 암호화 키</u>

[0167] 비밀은, 대칭 암호화 키로서 또는 대칭 암호화 키를 결정하기 위한 기초로서 사용될 수 있다.

[0168] 이러한 특정 예에서, 방법(400)은, 결정된 비밀에 기초하여 암호화 키(E)를 결정하는 추가 단계(480)를 포함한다. 암호화 키(E)는, 또한, 암호화 키(E)가 전자 장치(3)에 특정됨을 보장하도록 전자 장치의 일련번호에 기초한다. 암호화 키(E)는 이하의 식에 따라 결정된다.

[0169] E = SHA256(SHA256(솔트(salt) + 비밀) + 일련번호) (식 9)

[0170] 여기서, 솔트 = 메시지(M)이다.

[0171] 이러한 특정 예에서는, 랜덤 솔트의 개념이 암호화 키(E)를 결정하는 데 사용된다. 결정된 비밀에 기초하여 암호화 키(E)를 계산하기 위한 임의의 적절한 기술이 (존재한다면) 사용될 수 있다는 것을 이해할 것이다.

[0172] 방법(400)은, 결정된 암호화 키(E)를 사용하여 전자 장치(3)에서 데이터를 암호화하는 단계(490)를 더 포함한다. 암호화 키(E)를 사용하여 데이터를 암호화하기 위한 임의의 적절한 방법이 사용될 수 있다는 것을 이해할 것이다.

[0173] 중요한 것은, 암호화 키 또는 비밀이 키 장치(5)의 데이터 저장소에 저장되어 있는 메시지(M)에 기초하여 재계산될 수 있으므로, 전자 장치(3)가 암호화 키(E) 또는 비밀을 저장할 필요가 없다는 것이다.

[0174] <u>암호화된 데이터 해독</u>

[0175] 이제, 전자 장치(3)에서의 데이터 암호화에 이어서, 전자 장치(3)에서 암호화된 데이터를 해독하는 방법을 도 4와 도 5를 참조하여 설명한다. 데이터를 해독하기 위해, 전자 장치(3)는 데이터가 암호화될 때 미리 결정된 비밀을 재계산한다.

[0176] 초기에, 전자 장치(3)는 서로 통신하도록 키 장치(5)에 접속된다. 각 장치(3, 5)를 접속하는 단계는, 장치들 상에서 실행되고 있는 각 소프트웨어가 호환 가능하고 동기화되는지 여부를 결정하는 단계를 포함할 수 있다.

[0177] <u>키 장치(5) 인증(500)</u>

[0178] 암호화된 데이터가 전자 장치(3)에서 해독되기 전에, 이러한 특정 예에서, 키 장치(5)는 초기에 전자 장치(3)에 의해 인증된다.

[0179] 키 장치(5)를 인증하는 방법(500)을 도 4를 참조하여 설명한다. 키 장치(5)를 인증하는 방법(500)은 전자 장치(3)에서의 데이터의 해독 사이클의 일부일 수 있다.

[0180] 방법(500)은, 키 장치(5)가 키 장치(5)임을 인증하는 데 사용될 인증 메시지(M_A)를 전자 장치(3)에서 생성하는 단계(510)를 포함한다. 생성된 메시지(M_A)는 키 장치(5)의 인증만을 위해 사용될 수 있다는 것을 이해할 것이다. 그러나, 일부 예에서, 인증 메시지(M_A)는, 다음 암호화-해독 사이클을 위한 암호화 프로세스에서 사용되는, 도 3을 참조하여 기술된 바와 같이 메시지(M)를 형성할 수 있다.

[0181] 방법(500)은, 전자 장치(3)로부터 블루투스(7)를 통해 키 장치(5)에서 인증 메시지(M_A)를 수신하는 단계(520)를 포함한다.

[0182] 이어서, 키 장치(5)는 메시지(M_A)에 기초하여 결정론적 인증 키(DK_A)를 결정한다(530). 예를 들어, 결정론적 인증 키(DK_A)는, 방법(400)의 단계(430)와 유사한 인증 메시지의 해시일 수 있으며, 이하의 식에 따라 결정될 수 있다.

[0183] DK_A = SHA-256(M_A) (식 10)

[0184] 이어서, 키 장치(5)는 결정적 인증 키(DK_A)에 기초하여 새로운 비대칭 암호 쌍을 결정한다. 이 예에서 특정하게, 방법(500)은 이하의 식에 따라 제2 키 장치 개인 키(V_{2C})를 결정하는 단계(540)를 포함한다.

[0185] $V_{2C} = V_{1C}$ + SHA-256(M_A) (식 11)

[0186] 방법(500)은, 또한, 이하의 식에 따라 제2 키 장치 공개 키(P_{2C})를 결정하는 단계(550)를 포함한다.

[0187] $P_{2C} = P_{1C} + \text{SHA-256}(M_A) \times G$ (식 12)

[0188] 방법(300)은, 인증 메시지(M_A)와 결정된 제2 키 장치 개인 키(V_{2C})에 기초하여 서명된 메시지(SM_A)를 생성하는 단계(560)를 더 포함한다. 서명된 메시지를 생성하는 단계는, 디지털 서명 알고리즘을 적용하여 인증 메시지(M_A)에 디지털 서명하는 단계를 포함한다. 일례로, 이는 타원 곡선 디지털 서명 알고리즘(ECD)에서 제2 키 장치 개인 키(V_{2C})를 메시지에 적용하여 서명된 메시지(SM_A)를 취득하는 것을 포함한다. 인증 메시지(M_A)는 이하의 식에 따라 서명될 수 있다.

[0189] $SM_A = Sig - V_{2C} <M_A>$ (식 13)

[0190] ECDSA의 예는, secp256k1, secp256r1, secp384r1, se3cp521r1을 갖는 ECC 시스템에 기초하는 것을 포함한다.

[0191] 서명된 인증 메시지(SM_A)는 키 장치(5)의 인증을 위해 전자 장치(3)에 후속 전송된다(570).

[0192] 방법(500)은, 키 장치(5)로부터 서명된 인증 메시지(SM_A)를 수신하는 단계(580)를 포함한다. 이어서, 전자 장치(3)는, 단계(550)에서 결정된 제2 키 장치 공개 키(P_{2C})로 서명된 인증 메시지(SM_A) 상의 서명을 유효성 확인한다(590).

[0193] 디지털 서명의 검증은, 타원 곡선 디지털 서명 알고리즘(ECD)에 따라 행해질 수 있다. 중요한 것은, V_{2C}와 P_{2C}가 암호 쌍을 형성하므로, 제2 키 장치 개인 키(V_{2C})로 서명된, 서명된 인증 메시지(SM_A)가 대응하는 제2 키 장치 공개 키(P_{2C})로 올바르게 검증되어야 한다는 것이다. 이들 키는, 키 장치의 등록시 생성된 키 장치 마스터 개인 키(V_{1C})와 키 장치 마스터 공개 키(P_{1C})의 결정론적인 것이므로, 서명된 인증 메시지(SM_A)의 검증은, 서명된 메시지(SM_A)를 전송하는 혐의가 있는 키 장치(5)가 등록시와 동일한 키 장치(5)임을 인증하는 기초로서 사용될 수 있다.

[0194] <u>암호화된 데이터를 해독하도록 암호화 키(E) 재계산</u>

[0195] 키 장치(5)의 성공적인 인증에 이어서, 전자 장치(3)는 비밀을 재계산하여 암호화 키(E)를 재계산함으로써 암호화된 데이터를 해독한다. 이제, 암호화된 데이터를 해독하는 예시적인 방법(600)을 도 5를 참조하여 설명한다.

[0196] 방법(600)은, 방법(400)의 단계(420)에서 설명된 바와 같이 암호화 사이클에서 미리 사용되어 키 장치(5)에 저장된 메시지(M)를 요청하는 단계(610)를 포함한다.

[0197] 이어서, 방법(600)은 메시지(M)를 수신하는 단계(630)를 포함한다. 이러한 특정 예에서, 메시지(M)는, 메시지(M)가 전자 장치(3)에 전송되기 전에 제2 키 장치 개인 키(V_{2C})를 사용하여 키 장치(5)에 의해 서명된다(620). 메시지(M)는 이하의 식에 따라 서명될 수 있다.

[0198] $SM = Sig - V_{2C} <M>$ (식 14)

[0199] 방법(600)은 서명된 메시지(SM)를 검증하는 단계(650)를 더 포함한다. 이것은, 제2 키 장치 공개 키(P_{2C})를 독립적으로 결정한 후 타원 곡선 디지털 서명 알고리즘(ECDSA)을 SM과 P_{2C}에 행해질 수 있다. 제2 키 장치 공개 키는 이하의 식에 따라 결정될 수 있다.

[0200] $P_{2C} = P_{1C} + \text{SHA-256}(M) \times G$ (식 15)

[0201] 이어서, 방법(600)은, 서명된 메시지(M)로부터 메시지(M)를 검색(660)하는 단계를 포함하여, 이에 따라 도 3을 참조하여 설명한 바와 같은 단계(430 내지 470) 후에 전자 장치(3)가 비밀을 재계산(670)할 수 있다.

[0202] 추가 단계(680)에서, 암호화 키(E)는, 방법(400)의 단계(480)를 참조하여 기술된 바와 같이 비밀과 전자 장치의 일련 번호에 기초하여 재결정된다. 일단 암호화 키(E)가 결정되면, 데이터가 해독될 수 있다(690).

[0203] 암호화된 데이터를 해독하기 위해, 일부 실시예에서는 도 4를 참조하여 기술된 인증 방법이 필요하지 않을 수 있다는 것을 이해할 것이다.

[0204] 처리 장치

[0205] 전술한 바와 같이, 전자 장치(3)와 키 장치(5)는, 랩톱 컴퓨터, 태블릿 컴퓨터, 이동 통신 장치, 컴퓨터 서버 등과 같은 개인용 전자 장치일 수 있다. 전자 장치는, 처리 장치(23, 25), 데이터 저장소(13, 15), 및 사용자 인터페이스(14)를 포함할 수 있다.

[0206] 도 6은 처리 장치(23, 25)의 일례를 도시한다. 처리 장치(23, 25)는 전자 장치(3) 또는 키 장치(5)에서 사용될 수 있다. 처리 장치(23, 25)는, 버스(1530)를 통해 서로 통신하는 프로세서(1510), 메모리(1520), 및 인터페이스 장치(1540)를 포함한다. 메모리(1520)는 전술한 방법(200, 300, 400, 500 및 600)을 구현하기 위한 명령어와 데이터를 저장하고, 프로세서(1510)는 메모리(1520)로부터의 명령어를 수행하여 방법(200, 300, 400, 500 및 600)을 구현한다. 인터페이스 장치(1540)는, 블루투스(7)와 같은 통신 네트워크, 및 일부 예에서 사용자 인터페이스(14)와 데이터 저장소(13, 15)와 같은 주변 장치와의 통신을 용이하게 하는 통신 모듈을 포함할 수 있다. 처리 장치(1501)가 독립적 네트워크 요소일지라도, 치리 장치(1501)가 다른 네트워크 요소의 일부일 수도 있다는 점에 주목해야 한다. 또한, 처리 장치(1501)에 의해 수행되는 일부 기능들은 다수의 네트워크 요소 간에 분산될 수 있다. 예를 들어, 전자 장치(3)는, 전자 장치(3)에 관련된 보안 근거리 통신망에서 방법(200, 400) 및 방법(500, 600)의 일부를 수행하기 위한 다수의 처리 장치(23)를 가질 수 있다.

[0207] 본 개시 내용에서 사용자, 발행자, 판매자, 제공자, 또는 기타 엔티티가 (서명, 발행, 결정, 계산, 전송, 수신, 생성 등을 포함한) 특정 액션을 수행한다고 설명하는 경우, 이러한 표현은 명확한 제시를 위해 사용된 것이다. 이들 액션은 이들 엔티티에 의해 동작되는 연산 장치에 의해 수행된다는 것을 이해해야 한다.

[0208] 서명은 암호 함수를 실행하는 것을 포함할 수 있다. 이 함수는, 일반 텍스트에 대한 입력 및 개인 키와 같은 키에 대한 입력을 갖는다. 프로세서는, 서명으로서 사용될 수 있는 숫자 또는 스트링을 계산하는 함수를 실행할 수 있다. 이어서, 서명은 서명된 텍스트를 제공하도록 일반 텍스트와 함께 제공된다. 메시지 텍스트 또는 키가 단일 비트만큼 변경되면 서명이 완전히 변경된다. 서명 계산에는 연산 능력이 거의 필요하지 않지만, 주어진 서명이 있는 메시지를 재생성하는 것은 사실상 불가능하다. 이렇게 함으로써, 일반 텍스트는, 개인 키가 사용가능할 경우에만 변경될 수 있으며 유효 서명을 수반할 수 있다. 또한, 다른 엔티티는 공개적으로 이용가능한 공개 키를 사용하여 서명을 쉽게 검증할 수 있다.

[0209] 대부분의 경우에, 암호화와 해독은, 프로세서가, 암호화된 메시지 또는 일반 텍스트 메시지를 각각 나타내는 출력 스트링을 계산하기 위한 암호 함수를 실행하는 것을 포함한다.

[0210] 키, 토큰, 메타데이터, 트랜잭션, 오퍼, 계약, 서명, 스크립트, 메타데이터, 초대장 등은, "스트링"" 또는 "int" 또는 다른 유형 또는 텍스트 파일의 프로그램 코드의 변수와 같이 데이터 메모리 상에 저장된 숫자, 텍스트, 또는 스트링으로서 표현된 이진 데이터를 가리킨다.

[0211] 피어투피어 원장의 일례는 비트코인 블록체인이다. 비트코인 통화로 자금을 전달하거나 수수료를 지불하는 것은, 비트코인 블록체인 상에 트랜잭션을 생성하며, 이때 자금 또는 수수료가 트랜잭션으로부터의 출력이다. 비트코인 트랜잭션의 일례는, 입력 트랜잭션 해시, 트랜잭션 양, 하나 이상의 목적지, 지불인 또는 수취인의 공개 키, 입력 트랜잭션을 입력 메시지로서 사용함으로써 생성된 서명 및 서명을 계산하기 위한 지불인의 개인 키를 포함한다. 트랜잭션은, 공개 키를 사용하여 입력 트랜잭션 해시가 비트코인 블록체인의 복사본에 존재하고 서명이 올바른지를 확인함으로써 검증될 수 있다. 동일한 입력 트랜잭션 해시가 다른 곳에서 미리 사용되지 않았음을 보장하도록, 트랜잭션은 연산 노드들의 네트워크("마이너")에 방송된다. 마이너는, 입력 트랜잭션 해시가 아직 접속되어 있지 않고 서명이 유효한 경우에만 블록체인 상의 트랜잭션을 수락하고 기록한다. 입력 트랜잭션 해시가 이미 다른 트랜잭션에 링크되어 있으면, 마이너가 트랜잭션을 거부한다.

[0212] 두 개의 항목이 연관되어 있는 경우, 이는 이들 항목 간에 논리적 접속이 있음을 나타낸다. 예를 들어, 데이터베이스에서, 두 개의 항목에 대한 식별자는, 두 개의 항목을 서로 연관짓도록 동일한 레코드에 저장될 수 있다. 트랜잭션에서, 두 개의 항목에 대한 식별자는, 두 개의 항목을 서로 연관짓도록 트랜잭션 스트링에 포함될 수 있다.

[0213] 다른 엔티티를 인가하는 단계는, 개인 키를 사용하여 트랜잭션의 서명 스트링을 계산하는 단계, 및 엔티티가 서명을 사용하여 트랜잭션을 검증할 수 있도록 서명 스트링을 엔티티에 제공하는 단계를 포함할 수 있다.

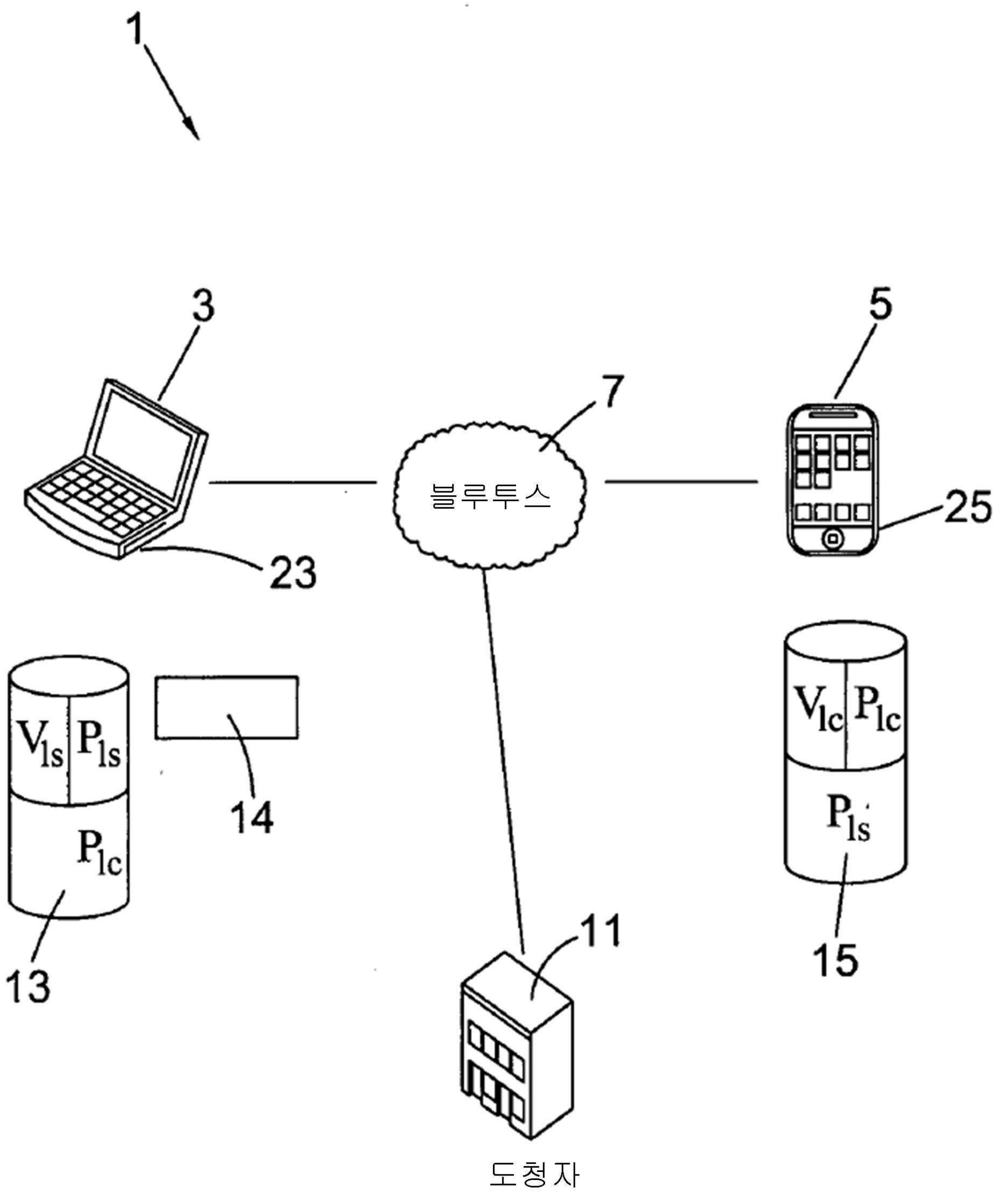
[0214] 다른 엔티티와의 계정을 갖는 사용자는, 이메일 어드레스, 이름, 및 잠재적 공개 키와 같은 사용자에 관한 정보를 저장하는 엔티티를 포함할 수 있다. 예를 들어, 엔티티는, 또한, 사용자의 개인 키들 중 하나 이상을 저장할

수 있다. 일부 예에서, 엔티티는, SQL, OrientDB, MongoDB, 또는 다른 데이터베이스와 같은 데이터베이스를 관리할 수 있다.

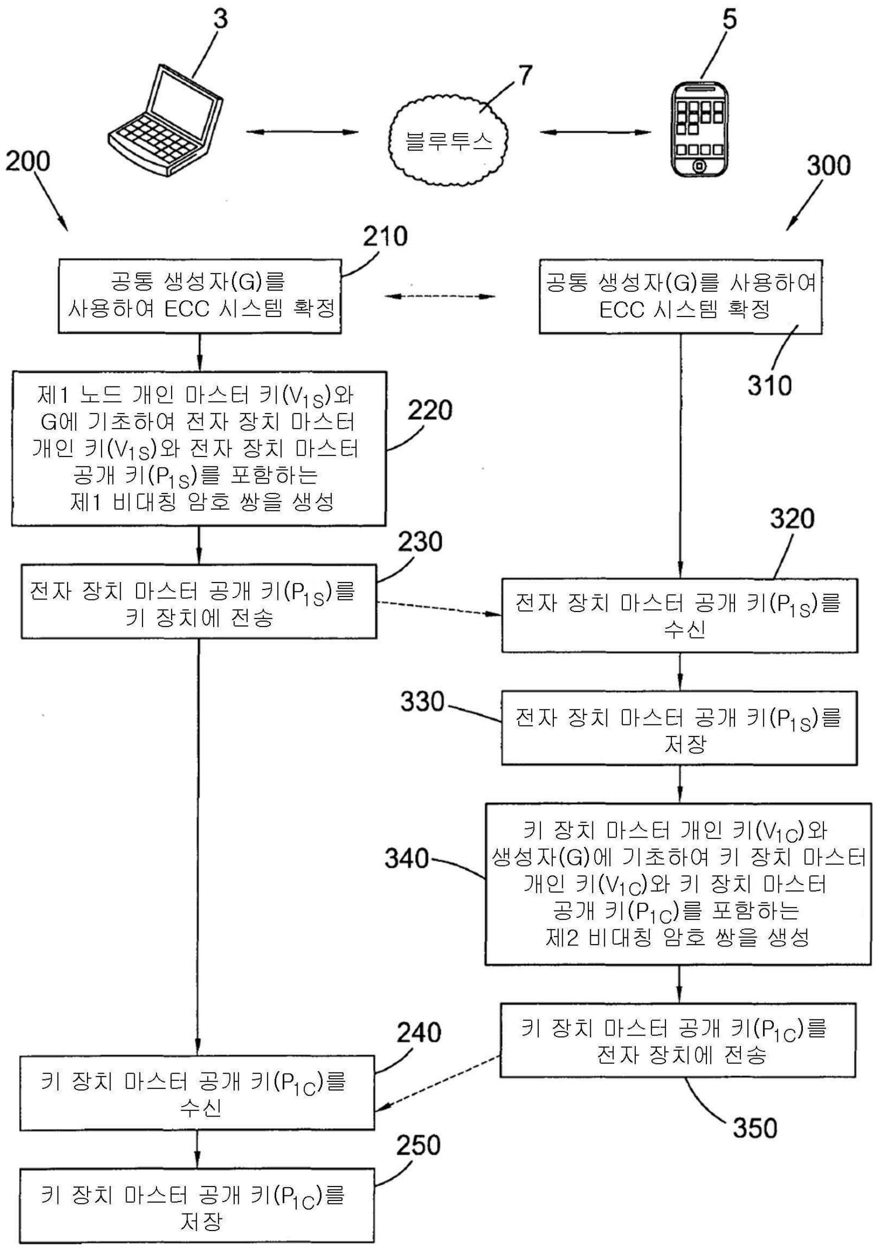
[0215] 통상의 기술자라면, 본 개시 내용의 넓은 일반적 범위를 벗어나지 않고, 상술한 실시예에 대해 다양한 변형 및/또는 수정이 이루어질 수 있음을 이해할 것이다. 따라서, 본 실시예들은 모든 면에서 예시적이고 제한적이지 않은 것으로 간주되어야 한다.

도면

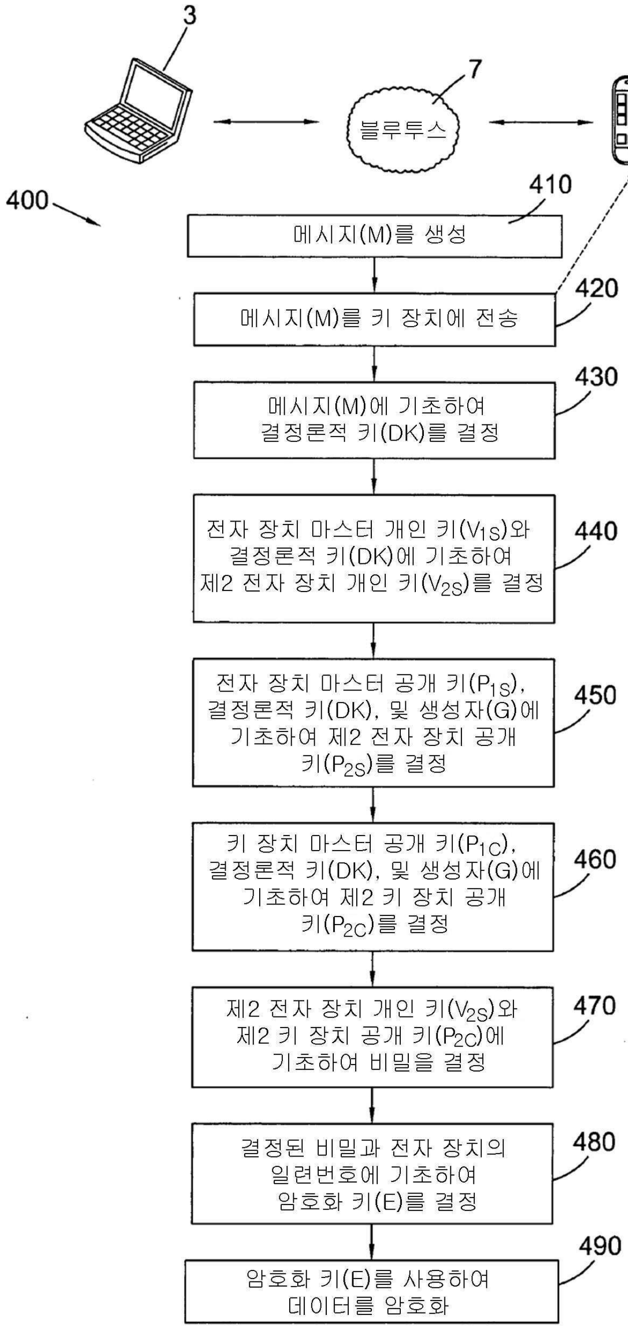
도면1



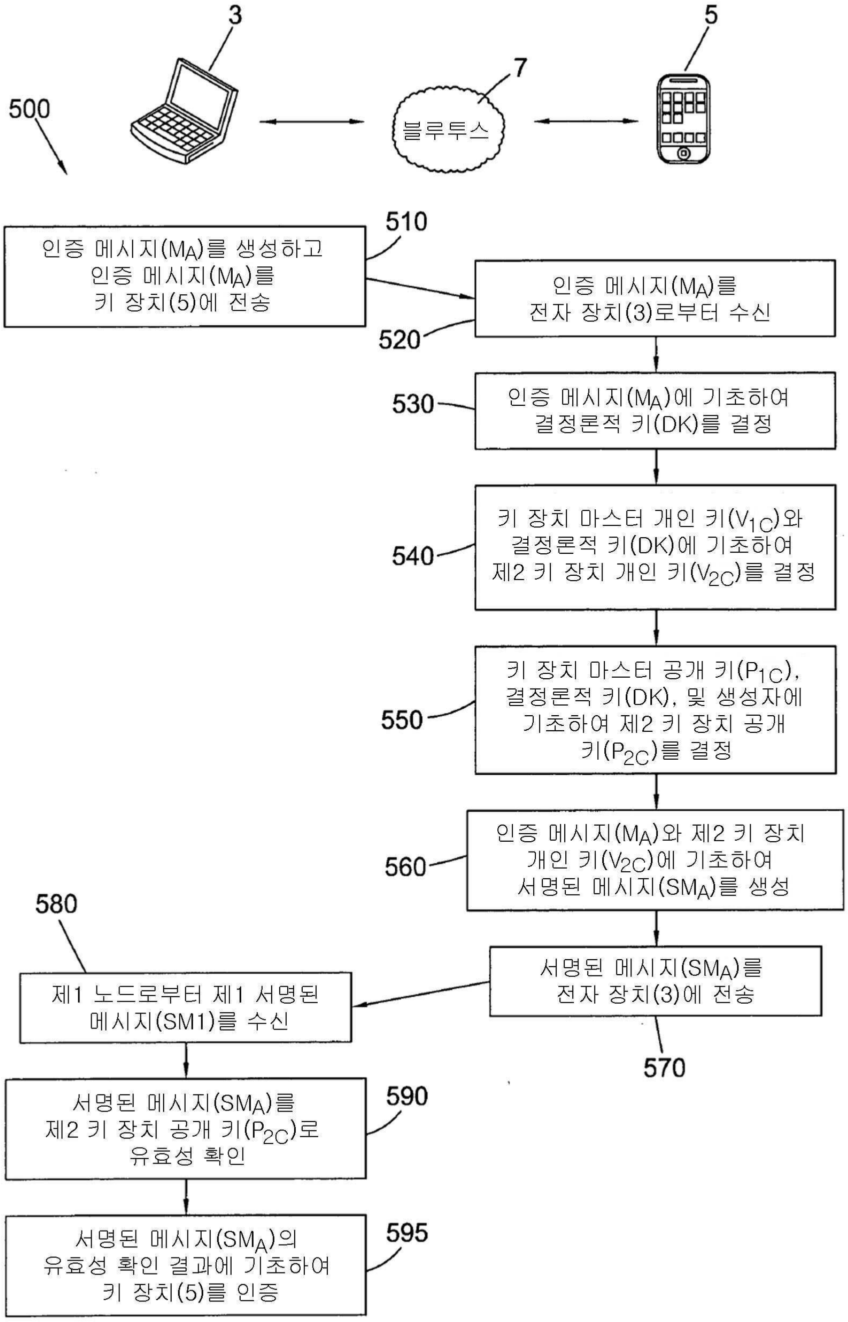
도면2


3
7
5
블루투스
200
300
210
공통 생성자(G)를 사용하여 ECC 시스템 확정
공통 생성자(G)를 사용하여 ECC 시스템 확정
310
제1 노드 개인 마스터 키(V_{1S})와 G에 기초하여 전자 장치 마스터 개인 키(V_{1S})와 전자 장치 마스터 공개 키(P_{1S})를 포함하는 제1 비대칭 암호 쌍을 생성
220
230
320
전자 장치 마스터 공개 키(P_{1S})를 키 장치에 전송
전자 장치 마스터 공개 키(P_{1S})를 수신
330
전자 장치 마스터 공개 키(P_{1S})를 저장
340
키 장치 마스터 개인 키(V_{1C})와 생성자(G)에 기초하여 키 장치 마스터 개인 키(V_{1C})와 키 장치 마스터 공개 키(P_{1C})를 포함하는 제2 비대칭 암호 쌍을 생성
240
키 장치 마스터 공개 키(P_{1C})를 전자 장치에 전송
키 장치 마스터 공개 키(P_{1C})를 수신
350
250
키 장치 마스터 공개 키(P_{1C})를 저장

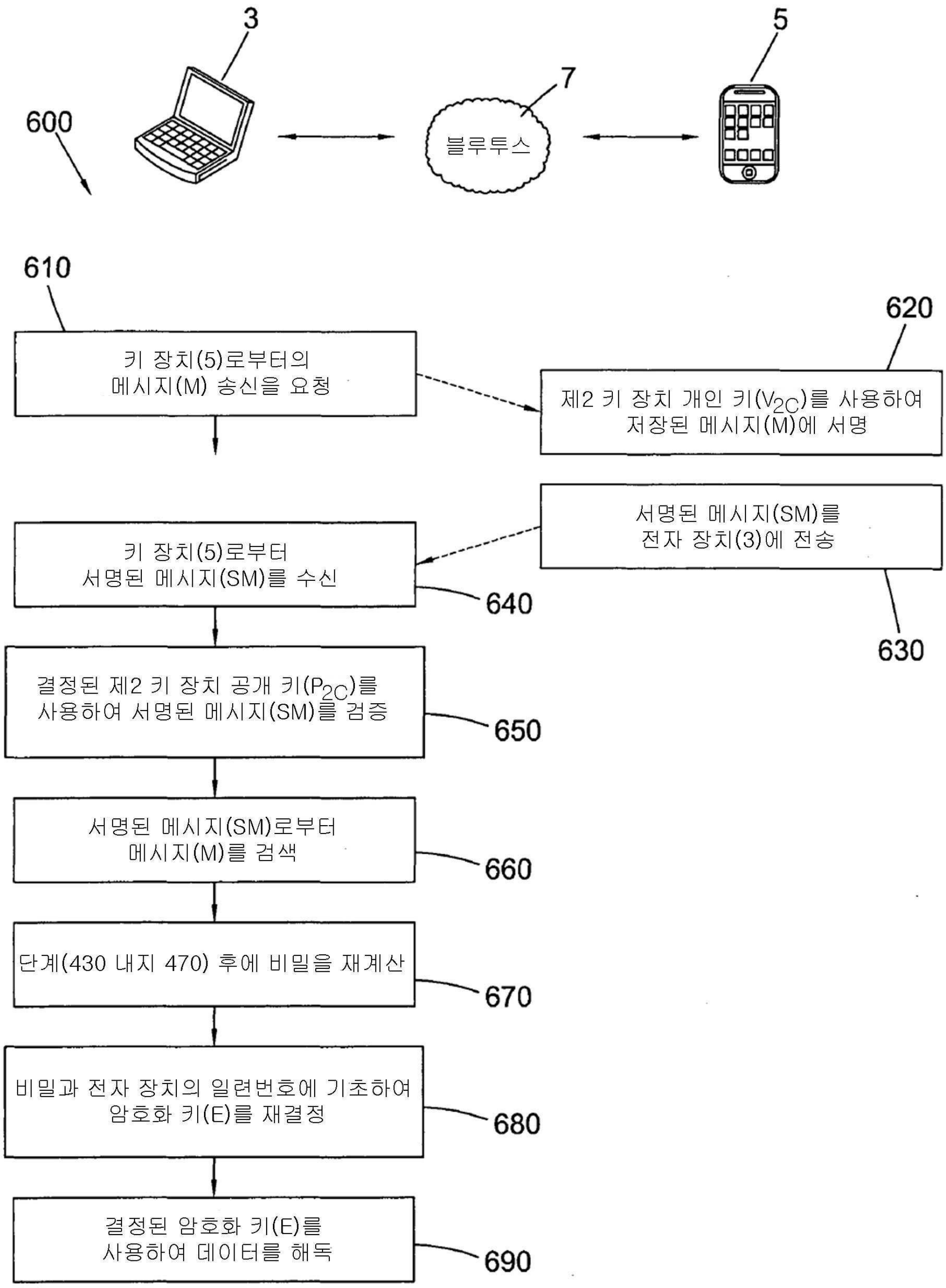
도면3


3
5
7
블루투스
400
410
메시지(M)를 생성
420
메시지(M)를 키 장치에 전송
430
메시지(M)에 기초하여 결정론적 키(DK)를 결정
440
전자 장치 마스터 개인 키(V_{1S})와 결정론적 키(DK)에 기초하여 제2 전자 장치 개인 키(V_{2S})를 결정
450
전자 장치 마스터 공개 키(P_{1S}), 결정론적 키(DK), 및 생성자(G)에 기초하여 제2 전자 장치 공개 키(P_{2S})를 결정
460
키 장치 마스터 공개 키(P_{1C}), 결정론적 키(DK), 및 생성자(G)에 기초하여 제2 키 장치 공개 키(P_{2C})를 결정
470
제2 전자 장치 개인 키(V_{2S})와 제2 키 장치 공개 키(P_{2C})에 기초하여 비밀을 결정
480
결정된 비밀과 전자 장치의 일련번호에 기초하여 암호화 키(E)를 결정
490
암호화 키(E)를 사용하여 데이터를 암호화

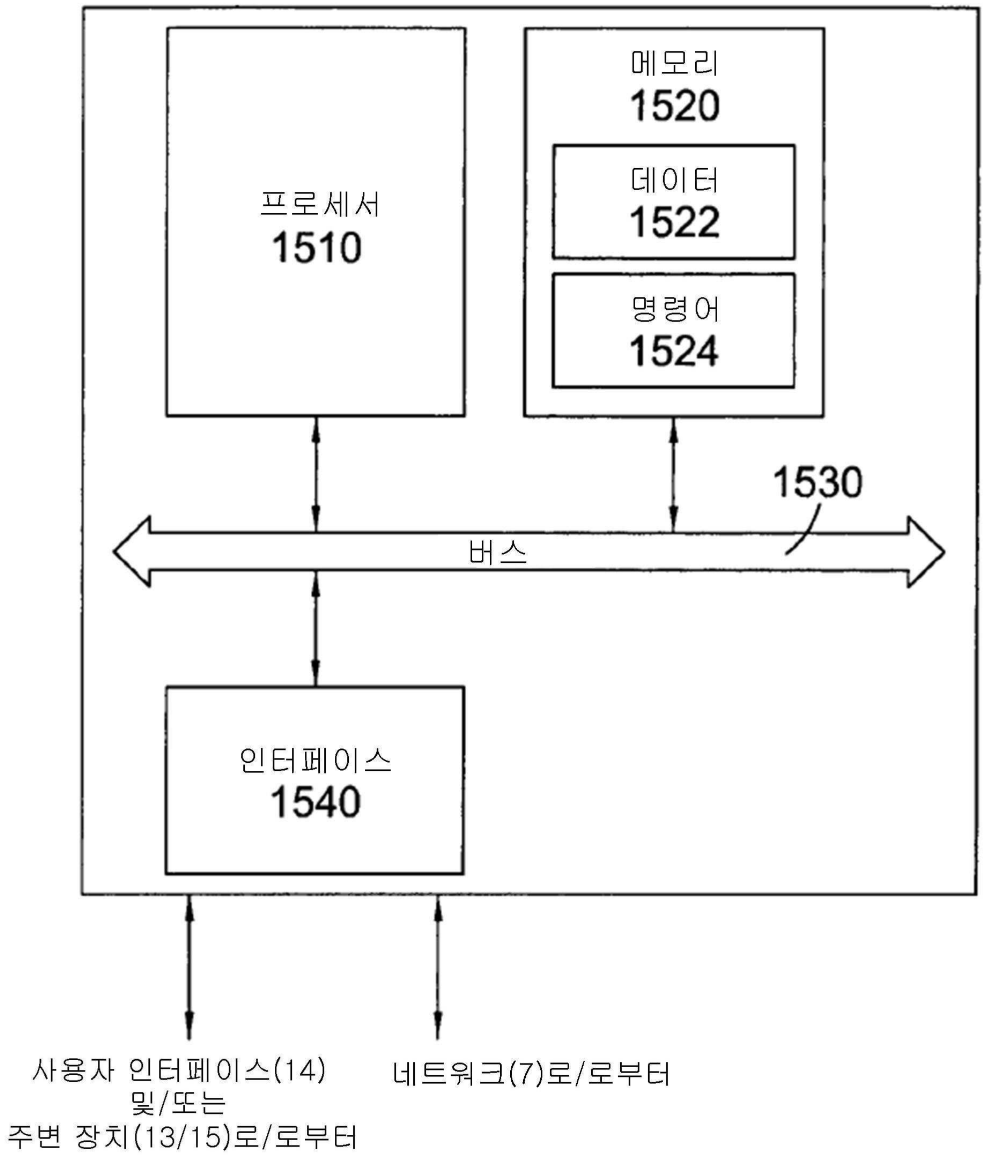
도면4


3
5
7
500
블루투스
510
인증 메시지(M_A)를 생성하고 인증 메시지(M_A)를 키 장치(5)에 전송
520
인증 메시지(M_A)를 전자 장치(3)로부터 수신
530
인증 메시지(M_A)에 기초하여 결정론적 키(DK)를 결정
540
키 장치 마스터 개인 키(V_{1C})와 결정론적 키(DK)에 기초하여 제2 키 장치 개인 키(V_{2C})를 결정
550
키 장치 마스터 공개 키(P_{1C}), 결정론적 키(DK), 및 생성자에 기초하여 제2 키 장치 공개 키(P_{2C})를 결정
560
인증 메시지(M_A)와 제2 키 장치 개인 키(V_{2C})에 기초하여 서명된 메시지(SM_A)를 생성
570
서명된 메시지(SM_A)를 전자 장치(3)에 전송
580
제1 노드로부터 제1 서명된 메시지(SM1)를 수신
590
서명된 메시지(SM_A)를 제2 키 장치 공개 키(P_{2C})로 유효성 확인
595
서명된 메시지(SM_A)의 유효성 확인 결과에 기초하여 키 장치(5)를 인증

도면5


3
5
7
600
블루투스
610
키 장치(5)로부터의 메시지(M) 송신을 요청
620
제2 키 장치 개인 키(V_{2C})를 사용하여 저장된 메시지(M)에 서명
서명된 메시지(SM)를 전자 장치(3)에 전송
630
키 장치(5)로부터 서명된 메시지(SM)를 수신
640
결정된 제2 키 장치 공개 키(P_{2C})를 사용하여 서명된 메시지(SM)를 검증
650
서명된 메시지(SM)로부터 메시지(M)를 검색
660
단계(430 내지 470) 후에 비밀을 재계산
670
비밀과 전자 장치의 일련번호에 기초하여 암호화 키(E)를 재결정
680
결정된 암호화 키(E)를 사용하여 데이터를 해독
690

도면6


메모리
1520
데이터
1522
명령어
1524
프로세서
1510
1530
버스
인터페이스
1540
사용자 인터페이스(14)
및/또는
주변 장치(13/15)로/로부터
네트워크(7)로/로부터