(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2013년03월26일
(11) 등록번호 10-1247914
(24) 등록일자 2013년03월20일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *G06K 9/00* (2006.01)
(21) 출원번호 10-2010-7028121
(22) 출원일자(국제) 2009년05월15일
심사청구일자 2010년12월14일
(85) 번역문제출일자 2010년12월14일
(65) 공개번호 10-2011-0009237
(43) 공개일자 2011년01월27일
(86) 국제출원번호 PCT/US2009/044238
(87) 국제공개번호 WO 2009/140654
국제공개일자 2009년11월19일
(30) 우선권주장
12/121,556 2008년05월15일 미국(US)
(56) 선행기술조사문헌
US20060123241 A1*
WO2006115491 A1*
US20070239994 A1
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
퀄컴 인코포레이티드
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(72) 발명자
나가라자 나겐드라
미국 92121 캘리포니아주 샌디에고 모어하우스 드라이브 5775
(74) 대리인
특허법인코리아나

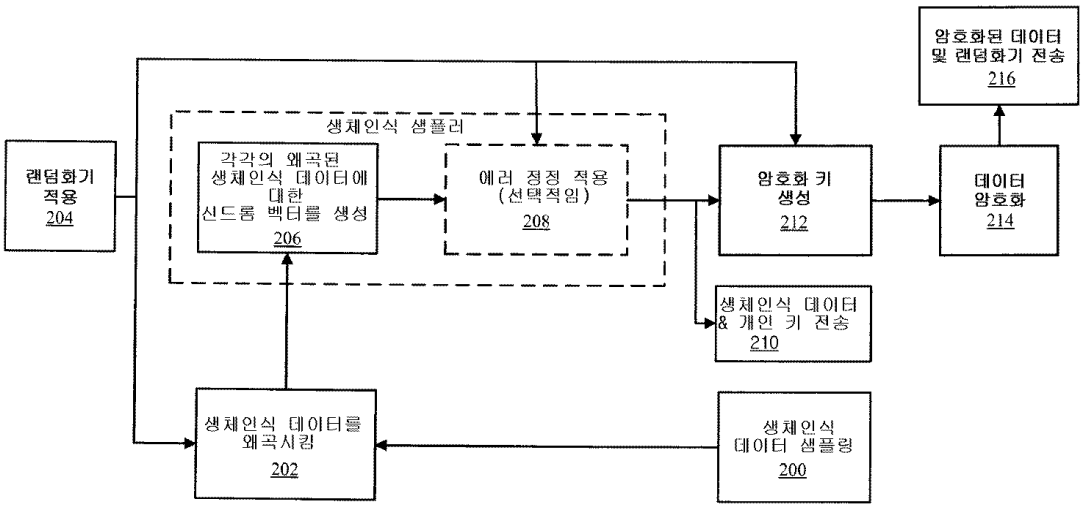
전체 청구항 수 : 총 44 항 심사관 : 양종필

(54) 발명의 명칭 **보안 생체인식 모델을 이용한 아이덴티티 기반 대칭 암호체계**

(57) 요 약

액세스 및 데이터 송신 모두가 효과적으로 매우 안전하게 이루어지는 고도의 보안 생체인식 모델을 이용하여 아이덴티티-기반 암호체계를 제공하는 방법, 장치, 및 컴퓨터 프로그램 제품이 본 명세서에 설명된다. 신드롬 벡터로서 생체인식 데이터를 생성하고 안전하게 저장하는 구현을 통해서, 생체인식 데이터의 고유한 변동성에 대한 허용오차를 제공한다. 또한, 생체인식 데이터가 신드롬 생성 알고리즘 및 생체인식 데이터로의 액세스를 획득할 수도 있는 공격자에 의해 복제되지 않도록 보증하기 위해, 본 양태는 개인 키를 더욱 안전하게 유지하고 암호체계 사용자-아이덴티티를 의존적으로 만들도록 제공한다. 본 명세서에 개시된 이러한 시스템, 장치 및 컴퓨터 프로그램 제품은 대칭 및/또는 비대칭 아이덴티티-기반 암호체계를 구성하는 보안 생체인식을 이용하여 말단 사용자들에게 엔드-투-엔드 인증을 제공한다.

대 표 도



특허청구의 범위

청구항 1

랜덤화된 생체인식 데이터 (randomized biometric data) 를 이용하여 데이터 송신을 암호화하는 방법으로서,

컴퓨팅 디바이스의 사용자에 관련된 생체인식 데이터 샘플을 수신하는 단계;

상기 생체인식 데이터 샘플을 복수의 왜곡된 생체인식 데이터로 왜곡시키는 단계;

상기 복수의 왜곡된 생체인식 데이터 각각을 신드롬 벡터 (syndrome vector) 로서 저장하는 단계;

상기 저장된 왜곡된 생체인식 데이터의 랜덤 샘플을 획득하는 단계;

상기 컴퓨팅 디바이스에 관련된 개인 키 (private key) 와 상기 왜곡된 생체인식 데이터의 상기 랜덤 샘플의 조합을 이용하여 암호화 키를 생성하는 단계; 및

상기 암호화 키를 이용하여 데이터 송신을 암호화하는 단계를 포함하는, 데이터 송신 암호화 방법.

청구항 2

제 1 항에 있어서,

제 2 컴퓨팅 디바이스와의 첫 번째 통신의 확립 시에, 상기 저장된 왜곡된 생체인식 데이터 및 상기 개인 키를 상기 제 2 컴퓨팅 디바이스에 전달하는 단계를 더 포함하는, 데이터 송신 암호화 방법.

청구항 3

제 1 항에 있어서,

상기 생체인식 데이터 샘플을 왜곡시키는 단계는, 상기 생체인식 데이터 샘플을 상기 복수의 왜곡된 생체인식 데이터로 랜덤으로 왜곡시키는 단계를 더 포함하는, 데이터 송신 암호화 방법.

청구항 4

제 3 항에 있어서,

상기 생체인식 데이터 샘플을 상기 복수의 왜곡된 생체인식 데이터로 랜덤으로 왜곡시키는 단계 및 상기 저장된 왜곡된 생체인식 데이터의 랜덤 샘플을 획득하는 단계는, 동기화된 랜덤화 (synchronized randomization) 로서 수행되는, 데이터 송신 암호화 방법.

청구항 5

제 1 항에 있어서,

상기 생체인식 데이터 샘플을 왜곡시키는 단계는, 상기 생체인식 데이터 샘플을 상기 복수의 왜곡된 생체인식 데이터로 동적으로 왜곡시키는 단계를 더 포함하는, 데이터 송신 암호화 방법.

청구항 6

제 1 항에 있어서,

상기 복수의 왜곡된 생체인식 데이터 중 하나 이상의 왜곡된 생체인식 데이터에 에러 정정을 적용하는 단계를 더 포함하는, 데이터 송신 암호화 방법.

청구항 7

제 6 항에 있어서,

상기 에러 정정을 적용하는 단계는, 상기 복수의 왜곡된 생체인식 데이터 중 하나 이상의 왜곡된 생체인식 데이터에 에러 정정을 랜덤으로 적용하는 단계를 더 포함하는, 데이터 송신 암호화 방법.

청구항 8

제 7 항에 있어서,

상기 생체인식 데이터 샘플을 왜곡시키는 단계, 상기 에러 정정을 적용하는 단계 및 상기 암호화 키를 생성하는 단계는, 동기화된 랜덤화로 또한 수행되는, 데이터 송신 암호화 방법.

청구항 9

제 1 항에 있어서,

상기 암호화 키를 생성하는 단계는, 일-방향 함수를 이용하여 상기 암호화 키를 생성하는 단계를 더 포함하는, 데이터 송신 암호화 방법.

청구항 10

랜덤화된 생체인식 데이터를 이용하여 데이터 송신을 암호화하도록 구성된 적어도 하나의 프로세서로서,

컴퓨팅 디바이스의 사용자에 관련된 생체인식 데이터 샘플을 수신하는 제 1 모듈;

상기 생체인식 데이터 샘플을 복수의 왜곡된 생체인식 데이터로 왜곡시키는 제 2 모듈;

상기 복수의 왜곡된 생체인식 데이터 각각을 신드롬 벡터로서 저장하는 제 3 모듈;

상기 저장된 왜곡된 생체인식 데이터의 랜덤 샘플을 획득하는 제 4 모듈;

상기 컴퓨팅 디바이스에 관련된 개인 키와 상기 왜곡된 생체인식 데이터의 상기 랜덤 샘플의 조합을 이용하여 암호화 키를 생성하는 제 5 모듈; 및

상기 암호화 키를 이용하여 데이터 송신을 암호화하는 제 6 모듈을 포함하는, 프로세서.

청구항 11

컴퓨터로 하여금 컴퓨팅 디바이스의 사용자에 관련된 생체인식 데이터 샘플을 수신하게 하기 위한 제 1 세트의 코드;

상기 컴퓨터로 하여금 상기 생체인식 데이터 샘플을 복수의 왜곡된 생체인식 데이터로 왜곡시키도록 하기 위한 제 2 세트의 코드;

상기 컴퓨터로 하여금 상기 복수의 왜곡된 생체인식 데이터 각각을 신드롬 벡터로서 저장하게 하기 위한 제 3 세트의 코드;

상기 컴퓨터로 하여금 상기 저장된 왜곡된 생체인식 데이터의 랜덤 샘플을 획득하게 하기 위한 제 4 세트의 코드;

상기 컴퓨터로 하여금 상기 컴퓨팅 디바이스에 관련된 개인 키와 상기 왜곡된 생체인식 데이터의 상기 랜덤 샘플의 조합을 이용하여 암호화 키를 생성하게 하기 위한 제 5 세트의 코드; 및

상기 컴퓨터로 하여금 상기 암호화 키를 이용하여 데이터 송신을 암호화하게 하기 위한 제 6 세트의 코드를 포함하는, 컴퓨터-판독가능 매체.

청구항 12

컴퓨팅 디바이스의 사용자에 관련된 생체인식 데이터 샘플을 수신하는 수단;

상기 생체인식 데이터 샘플을 복수의 왜곡된 생체인식 데이터로 왜곡시키는 수단;

상기 복수의 왜곡된 생체인식 데이터 각각을 신드롬 벡터로서 저장하는 수단;

상기 저장된 왜곡된 생체인식 데이터의 랜덤 샘플을 획득하는 수단;

상기 컴퓨팅 디바이스에 관련된 개인 키와 상기 왜곡된 생체인식 데이터의 상기 랜덤 샘플의 조합을 이용하여 암호화 키를 생성하는 수단; 및

상기 암호화 키를 이용하여 데이터 송신을 암호화하는 수단을 포함하는, 장치.

청구항 13

프로세서 및 상기 프로세서와 통신하는 메모리를 포함하는 컴퓨팅 플랫폼;

상기 프로세서와 통신하는 하나 이상의 생체인식 센서;

상기 프로세서 및 상기 생체인식 센서와 통신하고, 상기 생체인식 센서에 의해 캡처된 생체인식 데이터를 복수의 왜곡된 생체인식 데이터로 왜곡시키도록 동작가능한 생체인식 데이터 왜곡기;

상기 프로세서, 상기 메모리 및 상기 생체인식 데이터 왜곡기와 통신하고, 상기 복수의 왜곡된 생체인식 데이터 각각에 대한 신드롬 벡터를 생성하고 저장하도록 동작가능한 생체인식 샘플러;

상기 프로세서 및 상기 생체인식 샘플러와 통신하고, 상기 저장된 왜곡된 생체인식 데이터의 랜덤 샘플을 획득하고 상기 랜덤 샘플 및 개인 키에 기초하여 암호화 키를 생성하도록 동작가능한 암호화 키 생성기;

상기 프로세서 및 상기 암호화 키 생성기와 통신하고, 상기 저장된 왜곡된 생체인식 데이터의 샘플을 랜덤으로 획득하기 위한 랜덤화기 (randomizer) 를 적용하도록 동작가능한 랜덤화 모듈; 및

상기 암호화 키를 이용하여 데이터 송신을 암호화하도록 동작가능한 암호화 엔진을 포함하는, 장치.

청구항 14

제 13 항에 있어서,

통신 모듈을 더 포함하고,

상기 통신 모듈은, 제 2 컴퓨팅 디바이스와의 첫 번째 통신의 확립시에 에러 정정되고 왜곡된 생체인식 데이터를 상기 제 2 컴퓨팅 디바이스에 전달하도록 동작가능한, 장치.

청구항 15

제 13 항에 있어서,

상기 랜덤화 모듈은 상기 생체인식 데이터 왜곡기와 또한 통신하고,

상기 랜덤화 모듈은 상기 생체인식 데이터 샘플을 상기 복수의 왜곡된 생체인식 데이터로 랜덤으로 왜곡시키기 위해 상기 생체인식 데이터 왜곡기에 랜덤화기를 적용하도록 또한 동작가능한, 장치.

청구항 16

제 13 항에 있어서,

상기 생체인식 데이터 왜곡기는 상기 생체인식 데이터의 왜곡을 동적으로 변화시키도록 또한 동작가능한, 장치.

청구항 17

제 13 항에 있어서,

상기 복수의 왜곡된 생체인식 데이터 중 하나 이상의 왜곡된 생체인식 데이터에 에러 정정을 적용하도록 동작가능한 에러 정정 모듈을 더 포함하는, 장치.

청구항 18

제 17 항에 있어서,

상기 랜덤화 모듈은 상기 에러 정정 모듈과 또한 통신하고,

상기 랜덤화 모듈은 상기 복수의 왜곡된 생체인식 데이터 중 하나 이상의 왜곡된 생체인식 데이터에 에러 정정을 랜덤으로 적용하게 하기 위해 상기 에러 정정 모듈에 랜덤화기를 제공하도록 또한 동작가능한, 장치.

청구항 19

제 18 항에 있어서,

상기 랜덤화 모듈은 상기 에러 정정 모듈 및 상기 생체인식 데이터 왜곡기와 또한 통신하고,

상기 랜덤화 모듈은, 상기 저장된 왜곡된 생체인식 데이터의 샘플을 랜덤으로 획득하기 위해 상기 암호화 키 생성기에, 상기 복수의 왜곡된 생체인식 데이터 중 하나 이상의 왜곡된 생체인식 데이터에 에러 정정을 랜덤으로 적용시키기 위해 상기 에러 정정 모듈에, 그리고 상기 생체인식 데이터 샘플을 상기 복수의 왜곡된 생체인식 데이터로 랜덤으로 왜곡시키기 위해 상기 생체인식 데이터 왜곡기에, 동기화된 랜덤화기를 제공하도록 또한 동작가능한, 장치.

청구항 20

제 19 항에 있어서,

상기 동기화된 랜덤화기 및 암호화된 데이터를 상기 복수의 왜곡된 생체인식 데이터를 소유한 다른 컴퓨팅 디바이스에 전달하도록 동작가능한 통신 모듈을 더 포함하는, 장치.

청구항 21

제 13 항에 있어서,

상기 암호화 키 생성기는 일-방향 함수를 이용하여 상기 암호화 키를 생성하도록 또한 동작가능한, 장치.

청구항 22

생체인식 데이터에 기초한 대칭 아이덴티티 기반 암호해독 방법으로서,

제 1 디바이스로부터 생체인식 데이터 및 개인 키를 수신하는 단계;

상기 제 1 디바이스와의 관계에 기초하여 상기 생체인식 데이터 및 상기 개인 키를 저장하는 단계;

상기 제 1 디바이스로부터 제 1 암호화된 데이터 및 대응하는 제 1 랜덤화기를 수신하는 단계;

상기 제 1 디바이스로부터 수신된 상기 제 1 랜덤화기에 기초하여 상기 제 1 디바이스에 대응하는 상기 저장된 생체인식 데이터의 제 1 랜덤 샘플을 획득하는 단계;

상기 제 1 디바이스에 대응하는 상기 개인 키와 상기 생체인식 데이터의 상기 제 1 랜덤 샘플의 조합을 이용하여 제 1 암호해독 키를 생성하는 단계; 및

상기 제 1 암호해독 키를 이용하여 상기 제 1 암호화된 데이터를 암호해독하는 단계를 포함하고,

상기 제 1 디바이스로부터 생체인식 데이터 및 개인 키를 수신하는 단계는, 상기 제 1 디바이스로부터 왜곡된 생체인식 데이터를 수신하는 단계를 포함하는, 대칭 아이덴티티 기반 암호해독 방법.

청구항 23

제 22 항에 있어서,

상기 제 1 디바이스로부터 생체인식 데이터 및 개인 키를 수신하는 단계는, 상기 제 1 디바이스와의 첫 번째 통신에 기초하여 상기 생체인식 데이터 및 상기 개인 키를 수신하는 단계를 더 포함하는, 대칭 아이덴티티 기반 암호해독 방법.

청구항 24

삭제

청구항 25

제 22 항에 있어서,

상기 왜곡된 생체인식 데이터를 수신하는 단계는, 랜덤으로 왜곡된 생체인식데이터를 수신하는 단계를 더 포함하는, 대칭 아이덴티티 기반 암호해독 방법.

청구항 26

제 25 항에 있어서,

상기 왜곡의 랜덤성은 상기 제 1 랜덤화기에 기초하는, 대칭 아이덴티티 기반 암호해독 방법.

청구항 27

제 22 항에 있어서,

상기 생체인식 데이터 및 개인 키를 수신하는 단계는, 상기 생체인식 데이터, 상기 개인 키, 및 상기 제 1 디바이스를 식별하는 디바이스 식별자를 수신하는 단계를 더 포함하는, 대칭 아이덴티티 기반 암호해독 방법.

청구항 28

제 27 항에 있어서,

상기 제 1 디바이스와의 관계에 기초하여 상기 생체인식 데이터 및 상기 개인 키를 저장하는 단계는, 상기 디바이스 식별자에 기초하여 상기 생체인식 데이터 및 상기 개인 키를 저장하는 단계를 더 포함하는, 대칭 아이덴티티 기반 암호해독 방법.

청구항 29

제 28 항에 있어서,

상기 제 1 암호화된 데이터 및 대응하는 제 1 랜덤화기를 수신하는 단계는, 상기 제 1 디바이스로부터 상기 제 1 암호화된 데이터, 상기 대응하는 제 1 랜덤화기 및 상기 디바이스 식별자를 수신하는 단계를 더 포함하는, 대칭 아이덴티티 기반 암호해독 방법.

청구항 30

제 29 항에 있어서,

상기 저장된 생체인식 데이터의 제 1 랜덤 샘플을 획득하는 단계는, 상기 디바이스 식별자에 기초하여 저장매체로부터 생체인식 데이터를 검색하는 단계를 더 포함하는, 대칭 아이덴티티 기반 암호해독 방법.

청구항 31

제 22 항에 있어서,

상기 생체인식 데이터 및 상기 개인 키를 저장하는 단계는, 상기 생체인식 데이터 및 상기 개인 키를 상기 제 1 디바이스와 연관시키는 생체인식 어드레스 북에 상기 생체인식 데이터 및 상기 개인 키를 등록하는 단계를 더 포함하는, 대칭 아이덴티티 기반 암호해독 방법.

청구항 32

제 22 항에 있어서,

상기 제 1 암호해독 키를 생성하는 단계는, 일-방향 함수를 이용하여 상기 제 1 암호해독 키를 생성하는 단계를 더 포함하는, 대칭 아이덴티티 기반 암호해독방법.

청구항 33

제 32 항에 있어서,

상기 일-방향 함수를 이용하여 상기 제 1 암호해독 키를 생성하는 단계는, 상기 제 1 암호화된 데이터를 암호화하는데 이용된 일-방향 함수를 이용하여 상기 제 1 암호해독 키를 생성하는 단계를 더 포함하는, 대칭 아이덴티티 기반 암호해독 방법.

청구항 34

제 22 항에 있어서,

상기 제 1 디바이스로부터 제 2 암호화된 데이터 및 대응하는 제 2 랜덤화기를 수신하는 단계로서, 상기 제 2 랜덤화기는 상기 제 1 랜덤화기와는 상이한, 상기 수신하는 단계;

상기 제 1 디바이스로부터 수신된 상기 제 2 랜덤화기에 기초하여 상기 제 1 디바이스에 대응하는 상기 저장된

생체인식 데이터의 제 2 랜덤 샘플을 획득하는 단계;

상기 제 1 디바이스에 대응하는 상기 개인 키와 상기 생체인식 데이터의 제 2 랜덤 샘플의 조합을 이용하여 제 2 암호해독 키를 생성하는 단계; 및

상기 제 2 암호해독 키를 이용하여 상기 제 2 암호화된 데이터를 암호해독하는 단계를 더 포함하는, 대칭 아이덴티티 기반 암호해독 방법.

청구항 35

생체인식 데이터에 기초하여 대칭 아이덴티티 기반 암호해독을 제공하도록 구성된 적어도 하나의 프로세서로서,

제 1 디바이스로부터 생체인식 데이터 및 개인 키를 수신하는 제 1 모듈;

상기 제 1 디바이스와의 관계에 기초하여 상기 생체인식 데이터 및 상기 개인 키를 저장하는 제 2 모듈;

상기 제 1 디바이스로부터의 제 1 암호화된 데이터 및 대응하는 제 1 랜덤화기를 수신하는 제 3 모듈;

상기 제 1 디바이스로부터 수신된 상기 제 1 랜덤화기에 기초하여 상기 제 1 디바이스에 대응하는 상기 저장된 생체인식 데이터의 제 1 랜덤 샘플을 획득하는 제 4 모듈;

상기 제 1 디바이스에 대응하는 상기 개인 키와 상기 생체인식 데이터의 상기 제 1 랜덤 샘플의 조합을 이용하여 제 1 암호해독 키를 생성하는 제 5 모듈; 및

상기 제 1 암호해독 키를 이용하여 상기 제 1 암호화된 데이터를 암호해독하는 제 6 모듈을 포함하고,

상기 제 1 모듈은 상기 제 1 디바이스로부터 왜곡된 생체인식 데이터를 수신하는, 프로세서.

청구항 36

컴퓨터로 하여금 제 1 디바이스로부터 생체인식 데이터 및 개인 키를 수신하게 하는 제 1 세트의 코드;

상기 제 1 디바이스와의 관계에 기초하여 상기 생체인식 데이터 및 상기 개인 키를 저장하기 위한 제 2 세트의 코드;

상기 컴퓨터로 하여금 상기 제 1 디바이스로부터 제 1 암호화된 데이터 및 대응하는 제 1 랜덤화기를 수신하게 하는 제 3 세트의 코드;

상기 컴퓨터로 하여금 상기 제 1 디바이스로부터 수신된 상기 제 1 랜덤화기에 기초하여 상기 제 1 디바이스에 대응하는 상기 저장된 생체인식 데이터의 제 1 랜덤 샘플을 획득하게 하는 제 4 세트의 코드;

상기 컴퓨터로 하여금 상기 제 1 디바이스에 대응하는 상기 개인 키와 상기 생체인식 데이터의 상기 제 1 랜덤 샘플의 조합을 이용하여 제 1 암호해독 키를 생성하게 하는 제 5 세트의 코드; 및

상기 컴퓨터로 하여금 상기 제 1 암호해독 키를 이용하여 상기 제 1 암호화된 데이터를 암호해독하게 하는 제 6 세트의 코드를 포함하고,

상기 제 1 세트의 코드는 상기 컴퓨터로 하여금 상기 제 1 디바이스로부터 왜곡된 생체인식 데이터를 수신하게 하는, 컴퓨터-판독가능 매체.

청구항 37

제 1 디바이스로부터 생체인식 데이터 및 개인 키를 수신하는 수단;

상기 제 1 디바이스와의 관계에 기초하여 상기 생체인식 데이터 및 상기 개인 키를 저장하는 수단;

상기 제 1 디바이스로부터 제 1 암호화된 데이터 및 대응하는 제 1 랜덤화기를 수신하는 수단;

상기 제 1 디바이스로부터 수신된 상기 제 1 랜덤화기에 기초하여 상기 제 1 디바이스에 대응하는 상기 저장된 생체인식 데이터의 제 1 랜덤 샘플을 획득하는 수단;

상기 제 1 디바이스에 대응하는 상기 개인 키와 상기 생체인식 데이터의 상기 제 1 랜덤 샘플의 조합을 이용하여 제 1 암호해독 키를 생성하는 수단; 및

상기 제 1 암호해독 키를 이용하여 상기 제 1 암호화된 데이터를 암호해독하는 수단을 포함하고,

상기 생체인식 데이터를 수신하는 수단은 상기 제 1 디바이스로부터 왜곡된 생체인식 데이터를 수신하는, 장치.

청구항 38

프로세서 및 상기 프로세서와 통신하는 메모리를 포함하는 컴퓨팅 플랫폼;

상기 프로세서와 통신하고, 제 1 디바이스로부터 생체인식 데이터 및 개인 키를 수신하도록 동작가능한 통신 모듈;

상기 메모리에 저장되고, 상기 제 1 디바이스와의 관계에 기초하여 상기 생체인식 데이터 및 상기 개인 키를 저장하도록 동작가능한 생체인식 어드레스 북;

상기 프로세서와 통신하고, 암호화된 데이터 및 대응하는 랜덤화기의 상기 통신 모듈에 의한 수신에 기초하여 암호해독 키를 생성하도록 동작가능한 암호해독 키 생성기로서, 상기 암호해독 키 생성기는 상기 랜덤화기에 기초하여 상기 저장된 생체인식 데이터의 랜덤 샘플을 획득하고 상기 생체인식 데이터의 상기 랜덤 샘플과 상기 개인 키의 조합을 이용하여 상기 암호해독 키를 생성하도록 또한 동작가능한, 상기 암호해독 키 생성기; 및

상기 프로세서와 통신하고, 상기 암호해독 키를 이용하여 상기 암호화된 데이터를 암호해독하도록 동작가능한 암호해독 엔진을 포함하고,

상기 통신 모듈은 상기 제 1 디바이스로부터 왜곡된 생체인식 데이터를 수신하도록 동작가능한, 장치.

청구항 39

제 38 항에 있어서,

상기 통신 모듈은 상기 제 1 디바이스와의 첫 번째 통신에 기초하여 상기 생체인식 데이터 및 상기 개인 키를 수신하도록 또한 동작가능한, 장치.

청구항 40

삭제

청구항 41

제 38 항에 있어서,

상기 통신 모듈은 랜덤으로 왜곡된 생체인식 데이터를 수신하도록 또한 동작가능한, 장치.

청구항 42

제 41 항에 있어서,

상기 통신 모듈은, 왜곡의 랜덤성이 상기 랜덤화기에 기초하는, 랜덤으로 왜곡된 생체인식 데이터를 수신하도록 또한 동작가능한, 장치.

청구항 43

제 38 항에 있어서,

상기 통신 모듈은, 상기 생체인식 데이터, 상기 개인 키, 및 상기 제 1 디바이스를 식별하는 디바이스 식별자를 수신하도록 또한 동작가능한, 장치.

청구항 44

제 43 항에 있어서,

상기 생체인식 어드레스 북은 상기 디바이스 식별자에 기초하여 상기 생체인식 데이터 및 상기 개인 키를 저장하도록 또한 동작가능한, 장치.

청구항 45

제 44 항에 있어서,

상기 암호해독 키 생성기는 상기 디바이스 식별자에 기초하여 상기 생체인식 어드레스 북으로부터 상기 생체인식 데이터를 검색하도록 또한 동작가능한, 장치.

청구항 46

제 38 항에 있어서,

상기 암호해독 키 생성기는 일-방향 함수를 이용하여 상기 암호해독 키를 생성하도록 또한 동작가능한, 장치.

명 세 서

기 술 분 야

[0001] 본 발명은, 암호화 시스템 (cryptographic systems) 에 관한 것으로, 더욱 상세하게는, 보안 데이터 송신 및 송신을 위한 보안 액세스 모두를 제공하는 생체인식 데이터 (biometric data) 를 이용한 아이덴티티 기반 대칭 암호체계 (identity based symmetric cryptosystem) 를 위한 시스템, 장치 및 방법에 관한 것이다.

배 경 기 술

[0002] 일반적으로, 종래의 패스워드 기반 보안 시스템은 2 개의 페이즈를 포함한다. 첫째, 초기 등록 페이즈 (initial enrollment phase) 로서, 그 동안 사용자가 패스워드를 선택하고, 패스워드는 인증 서버 (authentication server) 와 같은 인증 디바이스에 후속하여 저장된다. 둘째, 인증 페이즈는 사용자가 그의 패스워드를 입력함으로써 리소스 또는 데이터에 대한 액세스를 획득하도록 허용하고, 그후 패스워드는 저장된 버전의 패스워드와 대조하여 검증된다. 그러나, 이러한 패스워드-기반 보안 메커니즘은 매우 취약하다. 예를 들어, 패스워드가 암호화되지 않은 평문 (plain text) 으로 저장된 경우, 시스템에 대한 액세스를 획득하는 공격자 (adversary) 는 시스템 내의 모든 패스워드를 획득할 수 있다. 이 예시에서, 공격자에 의한 단번의 성공적인 공격에도 전체 시스템이 위태로울 수 있다. 추가적으로, 패스워드-기반 컴퓨터 보안 시스템은, 패스워드를 해독하기 위한 모든 가능성이 탐색되는 무제한 공격 (brute force attack), 또는 성공할 가능성이 높은 것들 (예를 들어, 사전의 단어들로부터 유래된 목록) 만 탐색되는 사전 공격 (dictionary attack) 에 대해 영향받기 쉽다.

발명의 내용

해결하려는 과제

[0003] 패스워드-기반 보안 시스템에 관련된 추가적인 문제점은, 패스워드들이 사용자-특정되도록 요구되지 않고 패스워드들이 둘 이상의 개인/사용자들 사이에서 공유될 수 있어서 임의의 소정의 시점에서 패스워드를 소유한 사람을 시스템이 인지하게 하는 것은 어렵다는 것이다. 따라서, 이러한 보안 시스템에서의 인증은 소유-기반이고, 따라서, 패스워드의 소유는 사용자 인증을 확립하기에 충분하다. 이는, 패스워드가 필수적인 부인봉쇄 (requisite non-repudiation) 를 제공할 수 없다는 것을 의미한다.

[0004] 이러한 문제점들 중 몇몇을 해결하기 위해서, 종래의 패스워드 시스템들은 암호화 (encryption) 를 구현하도록 진화되었다. 예를 들어, 패스워드는 암호화 또는 해시 함수 (hash function) 를 이용하여 등록 페이즈 동안에 암호화되고, 그리고 인증 페이즈 동안에는, 사용자가 후보 패스워드 (candidate password) 를 입력할 때, 해시 함수가 후보 패스워드에 적용되어, 암호화된 후보 패스워드가 등록 페이즈 동안에 저장된 암호화된 패스워드와 일치하는 경우에 액세스가 승인된다. 이러한 암호화된 패스워드는, 공격자가 암호화 또는 해시 함수에 대한 지식을 소유하거나 또는 갖지 않는다면, 어떠한 이익도 그 공격자에게 제공하지 않는다. 그러나, 암호화 함수가 강력한 것으로 여겨지지 않는다면, 공격자는 암호화 코드를 해킹하거나 또는 그렇지 않으면 해독할 수 있는 경향을 나타낸다. 이들이 해킹을 방지할 수도 있는 소위 "강력한" 암호화 코드는 특정 예시에서 구현되기에는 매우 고가이고, 복잡하고 및/또는 비효율적일 수도 있다.

[0005] 최근, 사용자 인증을 제공하는 수단으로서 생체인식 데이터가 사용되고 있다. 생체인식 보안 시스템에서, 통상적으로 관찰 (observations) 로서 지칭되는 생체인식 파라미터들을 획득하기 위해 사용자의 물리적 생체인식 특징이 측정된다. 생체인식 특징들은, 지문, 홍채 인식 (iris recognition) 과 같은 안구-관련 특징, 다른 얼굴 인식 특징, 음성 인식 특징 등을 포함할 수도 있지만 이에 한정하지 않는다. 그러나, 생체인식 데

이터가 암호화되지 않은 종래의 생체인식 보안 시스템은 종래의 패스워드 기반 시스템과 동일한 취약성을 갖는다. 구체적으로, 데이터베이스가 중앙 데이터베이스 또는 사용자 디바이스에서 암호화되지 않은 생체인식 템플릿을 저장하는 경우, 파라미터들은 공격 및 오용에 대해 영향을 받기 쉽다. 생체인식 파라미터들이 불법적으로 위치되면, 공격자는 허가되지 않은 액세스를 획득하기 위해 그 공격자의 모습 또는 특성에 일치하도록 파라미터들을 변형시킬 수도 있다. 또한, 인위적인 방식으로 입력된 "가짜 (fake)" 생체인식 데이터를 갖는 위협이 존재한다. 또한, 패스워드 보안과는 다르게, 생체인식 데이터는 비밀이 아니고, 그것만으로는, 지문과 같은 몇몇 생체인식 데이터는 데이터가 획득된 경우 쉽게 위조될 수 있다.

[0006] 추가적으로, 생체인식 데이터의 암호화는 도전적인 태스크인 것으로 증명되었다. 이유들 중에서, 생체인식 특징이 측정되는 방법 및 "노이즈" 로 지칭된 일 측정에서 다른 측정으로의 생체인식 특징의 변형은 생체인식 데이터를 구현하는 암호화 시스템에 방해를 제공한다. 예를 들어, 적절한 암호화 함수를 이용하여 등록 생체인식 파라미터들이 암호화되도록, 등록 페이즈 도중에 생체인식 파라미터들이 캡쳐되고 입력될 수도 있다. 그러나, 인증 페이즈 도중에, 동일한 사용자로부터 획득된 생체인식 파라미터들은 등록시에 취득된 파라미터와는 상이할 수도 있다. 예를 들어, 생체인식 데이터가 얼굴의 특징 인식과 관련되어 있는 경우, 캡처링 장비 및 조명은 상이할 수도 있고 특징 그 자체는 시간이 경과함에 따라 변화할 수도 있다. 따라서, 인증 도중에 캡쳐된 생체인식 데이터가 동일한 암호화 함수를 통해서 통과되는 경우, 그 결과는 등록 데이터와 일치하지 않을 수도 있다. 이와 관련하여, 생체인식에 특정된 노이즈 구조에 대한 에러 정정 및 신드롬 코드 디코딩을 수행하기 위한 어떠한 허용가능한 방법도 존재하지 않는다. 대부분의 이전의 보안 생체인식 시스템은 노이즈의 특성을 지나치게 단순화하지만 실제 동작 컨디션을 반영하지는 않는 메모리-리스 (memory-less) 노이즈 모델 또는 다른 모델을 이용한다. 이와 같이, 보안 생체인식시의 이전의 시도들은 생체인식 특징들의 시변 동적 특성 그리고 그 포착 및 측정 프로세스를 적절히 나타내지 않는다.

[0007] 최근에, 에러 정정을 갖는 생체인식 데이터의 둘 이상의 소스와 비밀 키를 생성하기 위해 패스워드 또는 PIN 과 같은 몇몇 비밀 정보의 조합을 이용하는 다양한 모드의 생체인식 결합 (multimodal biometric fusion) 이 도입되어 있다. 그러나, 이러한 유형의 보안 기술은 대량의 데이터의 저장매체를 요구하고, 구현하는데 리소스 집약의 경향이 있어서, 다른 생체인식 기술보다 구현하는데 비용이 많이 든다. 추가적으로, 온도, 혈류, 심장박동 등과 같은 "활동적인 (live)" 인간 특성이 캡쳐되는, 생체인식 데이터의 활동도 검출 테스팅 (liveliness detection testing) 이 구현되어 있다. 그러나, 활동도 검출 테스팅의 구현은, 핸드헬드 무선 디바이스 등과 같은 리소스 제한된 디바이스 (resource constrained devices) 에서 실현 불가할 수도 있고, 이러한 디바이스들 상에서 현재 이용가능한 유형과는 상이한 유형의 센서를 요구할 것이다.

[0008] 따라서, 액세스 및 송신 모두가 매우 안전하게 효과적으로 이루어질 수 있는 고도의 보안 생체인식 모델을 개발할 필요성이 존재한다. 바람직한 모델은 생체인식 데이터의 고유한 변동성에 대처하고 극복하면서 생체인식 데이터의 복제를 방지하는 모델을 제공할 수 있어야만 한다.

과제의 해결 수단

[0009] 이하, 이러한 양태들의 기본적인 이해를 제공하기 위해 하나 이상의 양태들의 간략한 개요를 나타낸다. 이 개요는 모든 고찰된 양태들의 광범위한 개관은 아니며, 모든 양태들의 키 엘리먼트 또는 중대한 엘리먼트들을 식별하거나 또는 임의의 또는 모든 양태들의 범위를 한정하는 것으로 의도되지는 않는다. 이하 설명되는 더욱 상세한 설명에 대한 서론으로서 하나 이상의 양태들의 몇몇 개념들을 간략화된 형태로 나타내는데 유일한 목적이 있다.

[0010] 본 양태는, 모든 액세스 및 데이터 송신이 매우 안전하게 효과적으로 이루어지는 고도의 보안 생체인식 모델을 이용하여 아이덴티티-기반 암호체계를 제공하는 방법, 장치, 및 컴퓨터 프로그램 제품을 정의한다. 본 명세서에 설명된 일 양태에서, 생체인식 데이터의 신드롬 벡터 (syndrome vectors) 가 생성되고 안전하게 저장되어 생체인식 데이터의 고유한 변동성에 대한 허용오차 (tolerance) 를 제공한다. 또한, 생체인식 데이터가 신드롬 생성 알고리즘 및 생체인식 데이터에 대한 액세스를 획득할 수도 있는 공격자에 의해 복제되지 않도록 보증하기 위해, 본 양태는 개인 키를 더욱 안전하게 유지하고 암호체계가 사용자-아이덴티티 의존성으로 되도록 제공한다. 특정 양태에서, 종래의 키 생성 기술로부터 개인 키를 생성하여 개인 키 및 생체인식 데이터의 입력으로부터의 최종 키를 일-방향 함수로 생성함으로써 추가적인 보안이 달성된다. 여기에 기재된 이러한 시스템, 장치 및 컴퓨터 프로그램 제품은 대칭 및/또는 비대칭적 아이덴티티-기반 암호체계를 구성하는 보안 생체인식을 이용하여 말단 사용자들의 엔드-투-엔드 인증을 제공한다.

[0011] 본 양태는, 제 1 말단 사용자 디바이스와 제 2 말단 사용자 디바이스 사이의 2 개의 통신 포인트들 사이에서 모

든 생체인식 데이터의 한-번의 등록 (one-time registration) 을 제공한다. 특정 양태에서, 한-번의 등록은 말단 사용자 디바이스들 사이의 초기 통신 도중에 수행될 수도 있다. 이 등록은, 원시 (raw) 생체인식 데이터를 공격자가 획득하는 것을 방지하기 위해 신드롬 코딩된 및/또는 왜곡된/변형된 데이터, 그 외에 소거가능한 생체인식 데이터를 이용하여 국부적으로 또는 네트워크-기반으로 생체인식 어드레스 북을 유지하도록 제공할 수도 있다.

[0012] 등록이 수행된 후, 생체인식 데이터는 랜덤으로 샘플링될 수도 있고, 데이터를 암호화시키도록 이용되는 최종 키를 획득하기 위해 일-방향 함수를 이용하여 종래의 개인 키와 조합될 수도 있다. 생체인식 데이터는 생체인식 데이터를 왜곡/변형시킬 수도 있고 및/또는 신드롬 코드를 이용하여 추가적인 보안성을 제공하도록 저장될 수도 있다. 암호화된 데이터가 생체인식 데이터를 등록한 디바이스에 의해 수신되면, 생체인식 데이터는 디바이스 식별자에 따라서 검색되고 암호화 디바이스로부터 수신된 랜덤화기에 기초하며, 암호해독 디바이스가 어떤 생체인식이 암호해독을 위해 사용되어야만 하는지를 결정한다. 그후, 생체인식 데이터 및 랜덤화기는 데이터를 암호화하는데 사용되는 최종 개인 키를 형성하도록 조합된다.

[0013] 일 양태에 따르면, 랜덤화된 생체인식 데이터를 이용하여 데이터 송신을 암호화하기 위한 방법이 제공된다. 이 방법은, 컴퓨팅 디바이스의 사용자와 연관된 생체인식 데이터 샘플을 수신하는 단계 및 그 생체인식 데이터 샘플을 복수의 왜곡된 생체인식 데이터로 왜곡시키는 단계를 포함한다. 그후, 왜곡된 복수의 생체인식 데이터는 신드롬 벡터 (syndrome vector) 로서 저장된다. 이 방법은, 저장된 왜곡된 생체인식 데이터의 랜덤 샘플을 획득하는 단계 및 왜곡된 생체인식 데이터의 랜덤 샘플과 디바이스에 관련된 개인 키의 조합을 이용하여 암호화 키를 생성하는 단계를 더 포함한다. 암호화 키는 일-방향 함수를 이용하여 생성될 수도 있다. 추가적으로, 이 방법은 일-방향 함수를 이용하여 데이터 송신을 암호화하는 단계를 포함한다. 이 방법은, 제 2 컴퓨팅 디바이스와의 첫 번째 통신의 확립시에 저장된 왜곡된 생체인식 데이터 및 개인 키를 제 2 컴퓨팅 디바이스에 전달하게 하는 단계를 더 포함할 수도 있다.

[0014] 이 방법의 다른 양태에서, 생체인식 데이터 샘플을 왜곡시키는 단계는 생체인식 데이터 샘플을 복수의 왜곡된 생체인식 데이터로 랜덤으로 왜곡시키는 단계를 더 포함할 수도 있고, 일 양태에서, 모든 프로세스가 동일한 랜덤화기를 구현하도록, 랜덤 왜곡은 저장된 왜곡된 생체인식 데이터의 랜덤 샘플링과 동기화될 수도 있다. 추가적으로, 몇몇 양태에서, 생체인식 데이터 샘플을 왜곡하는 단계는, 왜곡 동작이 시간이 경과함에 따라 변화하거나 또는 사전구성 (preconfiguration) 에 기초하여 변화하도록, 생체인식 데이터 샘플을 복수의 왜곡된 생체인식 데이터로 동적으로 왜곡시키는 단계를 더 포함할 수도 있다.

[0015] 이 방법의 추가적인 양태는, 복수의 왜곡된 생체인식 데이터 중 하나 이상의 왜곡된 생체인식 데이터에 에러 정정을 적용하는 단계를 제공할 수도 있다. 에러 정정이 적용된 양태에서, 에러 정정은 랜덤으로 적용될 수도 있고, 랜덤화는 하나 이상의 생체인식 데이터의 왜곡과 동기화되어, 왜곡된 생체인식 데이터의 랜덤 샘플을 획득할 수도 있다. 따라서, 일 양태에서, 생체인식 데이터를 왜곡하는 단계, 에러 정정을 적용하는 단계 및 암호화 키를 생성하는 단계는 동기화된 랜덤화로 모두 수행된다.

[0016] 추가적인 양태는, 랜덤화된 생체인식 데이터를 이용하여 데이터 송신을 암호화하도록 구성된 적어도 하나의 프로세서에 의해 정의된다. 이 프로세서는, 컴퓨팅 디바이스의 사용자에 관련된 생체인식 데이터 샘플을 수신하는 제 1 모듈 및 생체인식 데이터 샘플을 복수의 왜곡된 생체인식 데이터로 왜곡시키는 제 2 모듈을 포함한다. 추가적으로, 프로세서는 복수의 왜곡된 생체인식 데이터 각각을 신드롬 벡터로서 저장하는 제 3 모듈 및 저장된 왜곡된 생체인식 데이터의 랜덤 샘플을 획득하는 제 4 모듈을 포함한다. 또한, 프로세서는 왜곡된 생체인식 데이터의 랜덤 샘플과 디바이스에 관련된 개인 키의 조합을 이용하여 암호화 키를 생성하는 제 5 모듈 및 그 암호화 키를 이용하여 데이터 송신을 암호화하는 제 6 모듈을 포함한다.

[0017] 다른 관련 양태는 컴퓨터-판독가능 매체를 포함하는 컴퓨터 프로그램 제품에 의해 제공된다. 이 컴퓨터-판독가능 매체는, 컴퓨터로 하여금 컴퓨팅 디바이스의 사용자에 관련된 생체인식 데이터 샘플을 수신하게 하는 제 1 세트의 코드 및 컴퓨터로 하여금 생체인식 데이터 샘플을 복수의 왜곡된 생체인식 데이터로 왜곡시키게 하는 제 2 세트의 코드를 포함한다. 추가적으로, 이 매체는 컴퓨터로 하여금 복수의 왜곡된 생체인식 데이터 각각을 신드롬 벡터로서 저장하게 하는 제 3 세트의 코드 및 컴퓨터로 하여금 저장된 왜곡된 생체인식 데이터의 랜덤 샘플을 획득하게 하는 제 4 세트의 코드를 포함한다. 또한 이 매체는, 컴퓨터로 하여금 왜곡된 생체인식 데이터의 랜덤 샘플과 디바이스에 관련된 개인 키의 조합을 이용하여 암호화 키를 생성하게 하는 제 5 세트의 코드 및 컴퓨터로 하여금 그 암호화 키를 이용하여 데이터 송신을 암호화하게 하는 제 6 세트의 코드를 포함한다.

[0018] 다른 관련 양태들을 위한 장치가 제공된다. 이 장치는, 컴퓨팅 디바이스의 사용자에 관련된 생체인식 데이터 샘플을 수신하는 수단 및 생체인식 데이터 샘플을 복수의 왜곡된 생체인식 데이터로 왜곡시키는 수단을 포함한다. 추가적으로, 이 장치는, 복수의 왜곡된 생체인식 데이터 각각을 신드롬 벡터로서 저장하는 수단 및 저장된 왜곡된 생체인식 데이터의 랜덤 샘플을 획득하는 수단을 포함한다. 또한, 이 장치는, 왜곡된 생체인식 데이터의 랜덤 샘플과 디바이스에 관련된 개인 키의 조합을 이용하여 암호화 키를 생성하는 수단 및 그 암호화 키를 이용하여 데이터 송신을 암호화하는 수단을 포함한다.

[0019] 또 다른 관련 양태는 프로세서 및 그 프로세스와 통신하는 메모리를 포함하는 컴퓨팅 플랫폼을 포함하는 장치에 의해 정의된다. 이 장치는, 추가적으로, 프로세서와 통신하는 하나 이상의 생체인식 센서, 및 이 프로세스 및 생체인식 센서와 통신하고, 센서에 의해 캡처된 생체인식 데이터를 복수의 왜곡된 생체인식 데이터로 왜곡시키도록 동작가능한 생체인식 데이터 왜곡기를 포함한다. 이 장치는, 프로세서, 메모리 및 생체인식 데이터 왜곡기와 통신하는 생체인식 샘플러를 더 포함한다. 생체인식 샘플러는 복수의 왜곡된 생체인식 데이터 각각에 대한 신드롬 벡터들을 생성하고 저장하도록 동작가능하다. 이 장치는, 또한, 프로세서 및 생체인식 샘플러와 통신하고, 저장된 왜곡된 생체인식 데이터의 샘플을 랜덤으로 획득하고 생체인식 데이터의 샘플 및 개인 키에 기초하여 암호화 키를 생성하게 하도록 동작가능한 암호화 키 생성기를 포함한다. 암호화 키 생성기는 일-방향 함수를 이용하여 암호화 키를 생성하도록 동작가능할 수도 있다. 추가적으로, 이 장치는 프로세서 및 암호화 키 생성기와 통신하는 랜덤화 모듈을 포함하여, 랜덤화 모듈은 저장된 왜곡된 생체인식 데이터의 랜덤 샘플을 획득하도록 동작가능한다. 또한, 이 장치는 암호화 키를 이용하여 데이터 송신을 암호화하도록 동작가능한 암호화 엔진을 포함한다.

[0020] 이 장치는, 프로세서 및 생체인식 샘플러와 통신하는 통신 모듈을 더 포함할 수도 있고, 이 통신 모듈은 제 2 컴퓨팅 디바이스와의 첫 번째 통신의 확립시에 제 2 컴퓨팅 디바이스에 왜곡된 생체인식 데이터를 전달하도록 동작가능하다. 또한, 통신 모듈은 랜덤화기 및 암호화된 데이터를 제 2 컴퓨팅 디바이스로 전달하도록 동작가능하게 할 수도 있다.

[0021] 다른 양태에서, 랜덤화 모듈은 생체인식 데이터 왜곡기와 통신할 수도 있고 생체인식 데이터를 랜덤으로 왜곡시키도록 동작가능할 수도 있다. 저장된 왜곡된 생체인식 데이터의 샘플을 획득하는데 적용되는 랜덤성 그리고 생체인식 데이터의 왜곡에 적용되는 이러한 랜덤성은 동기화된 랜덤성일 수도 있다. 다른 양태에서, 생체인식 데이터 왜곡기는 사전-구성 등에 기초하여 시간의 경과에 따라 생체인식 데이터의 왜곡을 동적으로 변화시키도록 또한 동작가능할 수도 있다.

[0022] 또한, 이 장치는 복수의 왜곡된 생체인식 데이터 중 하나 이상의 왜곡된 생체인식 데이터에 에러 정정을 적용하도록 동작가능한 에러 정정 모듈을 포함할 수도 있다. 에러 정정 모듈을 포함하는 이러한 양태에서, 랜덤화 모듈은 복수의 왜곡된 생체인식 데이터 중 하나 이상의 왜곡된 생체인식 데이터에 에러 정정을 랜덤으로 적용시키기 위해 에러 정정 모듈과 더 통신할 수도 있다. 따라서, 랜덤화 모듈은, 저장된 왜곡된 생체인식 데이터의 샘플을 랜덤으로 획득하기 위해 암호화 키 생성기에, 복수의 왜곡된 생체인식 데이터 중 하나 이상의 왜곡된 생체인식 데이터에 에러 정정을 랜덤으로 적용하기 위해 에러 정정 모듈에, 그리고 생체인식 데이터 샘플을 복수의 왜곡된 생체인식 데이터로 랜덤으로 왜곡시키기 위해 생체인식 데이터 왜곡기에, 동기화된 램덤화기를 제공하도록 또한 동작가능할 수도 있다.

[0023] 본 발명에 대한 추가적인 양태가 생체인식 데이터에 기초한 대칭 아이덴티티 기반 암호해독을 위한 방법에 의해 제공된다. 이 방법은, 제 1 디바이스로부터 생체인식 데이터 및 개인 키를 수신하는 단계 및 제 1 디바이스와의 관계에 기초하여 생체인식 데이터 및 개인 키를 저장하는 단계를 포함한다. 일 양태에서, 생체인식 데이터는, 전화 번호, IP 어드레스 등과 같은 제 1 디바이스 식별자와 이 생체인식 데이터를 연관시키는 생체인식 어드레스 북 (biometric address book) 에 저장될 것이다. 또한, 이 방법은 제 1 디바이스로부터 제 1 암호화된 데이터 및 대응하는 제 1 랜덤화기를 수신하는 단계 및 제 1 디바이스로부터 수신된 제 1 랜덤화기에 기초하여 제 1 디바이스에 대응하는 저장된 생체인식 데이터의 제 1 랜덤 샘플을 획득하는 단계를 포함한다. 이 방법은, 또한, 생체인식 데이터의 제 1 랜덤 샘플과 제 1 디바이스에 대응하는 개인 키의 조합을 이용하여 제 1 암호해독 키를 생성하는 단계 및 제 1 암호해독 키를 이용하여 제 1 암호화된 데이터를 암호해독하는 단계를 포함한다. 제 1 암호해독 키의 생성은 일-방향 함수를 이용하여 달성될 수도 있다.

[0024] 이 방법의 특정 양태에서, 이 디바이스가 생체인식 어드레스 북을 확인하도록, 생체인식 데이터 및 개인 키는 제 1 디바이스와의 첫 번째 통신에 기초하여 수신될 것이고, 어떠한 엔트리도 디바이스 식별자에 대해 존재하지 않는 경우, 생체인식 데이터 및 개인 키가 요청되고, 그렇지 않으면 제 1 디바이스로부터 검색된다.

[0025] 특정 양태에서, 제 1 디바이스로부터 수신된 생체인식 데이터는 왜곡된 생체인식 데이터로서 몇몇 예시에서는 랜덤으로 왜곡된 생체인식 데이터로서 정의될 수도 있으며, 여기서 왜곡된 생체인식 데이터의 랜덤성은 제 1 랜덤화기에 기초한다.

[0026] 대안적인 양태에서, 이 방법은 제 1 디바이스로부터 제 2 암호화된 데이터 및 대응하는 제 2 랜덤화기를 수신하는 단계 (여기서, 제 2 랜덤화기는 제 1 랜덤화기와는 상이함), 제 1 디바이스로부터 수신된 제 2 랜덤화기에 기초하여 제 1 디바이스에 대응하는 저장된 생체인식 데이터의 제 2 랜덤 샘플을 획득하는 단계, 제 1 디바이스에 대응하는 개인 키와 생체인식 데이터의 제 2 랜덤 샘플의 조합을 이용하여 제 2 암호해독 키를 생성하는 단계 및 제 2 암호해독 키를 이용하여 제 2 암호화된 데이터를 암호해독시키는 단계를 더 포함할 수도 있다.

[0027] 다른 관련 양태는, 생체인식 데이터에 기초한 대칭 아이덴티티 기반 암호해독을 제공하도록 구성된 적어도 하나의 프로세서에 의해 정의된다. 프로세서는, 제 1 디바이스로부터 생체인식 데이터 및 개인 키를 수신하는 제 1 모듈 및 제 1 디바이스와의 관계에 기초하여 생체인식 데이터 및 개인 키를 저장하는 제 2 모듈을 포함한다. 추가적으로, 프로세서는 제 1 디바이스로부터 제 1 암호화된 데이터 및 대응하는 제 1 랜덤화기를 수신하는 제 3 모듈 및 제 1 디바이스로부터 수신된 제 1 랜덤화기에 기초하여 제 1 디바이스에 대응하는 저장된 생체인식 데이터의 제 1 랜덤 샘플을 획득하는 제 4 모듈을 포함한다. 프로세서는, 또한, 제 1 디바이스에 대응하는 개인 키와 생체인식 데이터의 제 1 랜덤 샘플의 조합을 이용하여 제 1 암호해독 키를 생성하는 제 5 모듈 및 그 암호해독 키를 이용하여 제 1 암호화된 데이터를 암호해독하는 제 6 모듈을 포함한다.

[0028] 또 다른 관련 양태들에 대한 컴퓨터 프로그램 제품이 제공된다. 컴퓨터 프로그램 제품은 컴퓨터-판독가능 매체를 포함한다. 이 매체는, 컴퓨터로 하여금 제 1 디바이스로부터의 개인 키 및 생체인식 데이터를 수신하게 하는 제 1 세트의 코드 및 컴퓨터로 하여금 제 1 디바이스와의 관계에 기초하여 개인 키 및 생체인식 데이터를 저장하게 하는 제 2 세트의 코드를 포함한다. 추가적으로, 이 매체는, 컴퓨터로 하여금 제 1 디바이스로부터 제 1 암호화된 데이터 및 대응하는 제 1 랜덤화기를 수신하게 하는 제 3 세트의 코드 및 컴퓨터로 하여금 제 1 디바이스로부터 수신된 제 1 랜덤화기에 기초하여 제 1 디바이스에 대응하는 저장된 생체인식 데이터의 제 1 랜덤 샘플을 획득하게 하는 제 4 세트의 코드를 포함한다. 이 매체는, 추가적으로, 컴퓨터로 하여금 생체인식 데이터의 제 1 랜덤 샘플과 제 1 디바이스에 대응하는 개인 키의 조합을 이용하여 제 1 암호해독 키를 생성하게 하는 제 5 세트의 코드 및 컴퓨터로 하여금 그 암호해독 키를 이용하여 제 1 암호화된 데이터를 암호해독하게 하는 제 6 세트의 코드를 포함한다.

[0029] 다른 관련 양태가 장치에 의해 정의된다. 이 장치는, 제 1 디바이스로부터 생체인식 데이터 및 개인 키를 수신하는 수단 및 제 1 디바이스와의 관계에 기초하여 생체인식 데이터 및 개인 키를 저장하는 수단을 포함한다. 추가적으로, 이 장치는, 제 1 디바이스로부터 제 1 암호화 데이터 및 대응하는 제 1 랜덤화기를 수신하는 수단 및 제 1 디바이스로부터 수신된 제 1 랜덤화기에 기초하여 제 1 디바이스에 해당하는 저장된 생체인식 데이터의 제 1 랜덤 샘플을 획득하는 수단을 포함한다. 또한, 이 장치는, 생체인식 데이터의 제 1 랜덤 샘플과 제 1 디바이스에 대응하는 개인 키의 조합을 이용하여 제 1 암호해독 키를 생성하는 수단 및 그 암호해독 키를 이용하여 제 1 암호화된 데이터를 암호해독하는 수단을 포함한다.

[0030] 이 장치는, 본 발명의 또 다른 관련 양태를 정의한다. 이 장치는, 프로세서 및 이 프로세서와 통신하는 메모리를 포함하는 컴퓨팅 플랫폼을 포함한다. 또한, 이 장치는, 프로세서와 통신하고 제 1 디바이스로부터의 생체인식 데이터 및 개인 키를 수신하도록 동작가능한 통신 모듈, 및 메모리에 저장되고 제 1 디바이스와의 관계에 기초하여 생체인식 데이터 및 개인 키를 저장하도록 동작가능한 생체인식 어드레스 북을 포함한다. 추가적으로, 이 장치는, 프로세서와 통신하고 암호화된 데이터 및 대응하는 랜덤화기의 통신 모듈에 의한 수신에 기초하여 암호해독 키를 생성하도록 동작가능한 암호해독 키 생성기를 포함하고, 여기서, 암호해독 키 생성기는 랜덤화기에 기초하여 저장된 생체인식 데이터의 랜덤 샘플을 획득하고 생체인식 데이터의 랜덤 샘플과 개인 키의 조합을 이용하여 암호해독 키를 생성하도록 또한 동작가능하다. 이 장치는, 또한, 프로세서와 통신하고 암호해독 키를 이용하여 암호화된 데이터를 암호해독시키도록 동작가능한 암호해독 엔진을 포함한다. 암호해독 키 생성기는, 일-방향 함수를 이용하여 암호해독 키를 생성하게 하도록 또한 동작가능할 수도 있다.

[0031] 장치의 특정 양태에서, 통신 모듈은 제 1 디바이스와의 첫 번째 통신에 기초하여 생체인식 데이터 및 개인 키를 수신하도록 또한 동작가능하다. 추가적으로, 선택적인 양태에서, 통신 모듈은 제 1 디바이스로부터의 왜곡된 생체인식 데이터, 몇몇 양태에서는, 랜덤으로 왜곡된 생체인식을 수신하도록 또한 동작가능하다.

[0032] 따라서, 본 양태는, 모든 액세스 및 데이터 송신이 매우 안전하게 효과적으로 이루어지는 고도의 보안 생체인식 모델을 이용하여 아이덴티티-기반 암호체계를 제공하는 방법, 장치, 및 컴퓨터 프로그램 제품을 정의한다.

신드롬 벡터로서 생체인식 데이터를 생성하고 안전하게 저장하는 구현을 통해서, 생체인식 데이터의 고유한 변동성에 대한 허용오차가 제공된다. 또한, 생체인식 데이터가 신드롬 생성 알고리즘 및 생체인식 데이터에 대한 액세스를 획득할 수도 있는 공격자에 의해 복제되지 않도록 보증하기 위해, 본 양태는 개인 키를 더욱 안전하게 유지하고 암호체계가 사용자-식별 의존성으로 되도록 제공한다. 본 명세서에 기재된 이러한 시스템, 장치 및 컴퓨터 프로그램 제품은 대칭 및/또는 비대칭적 아이덴티티-기반 암호체계를 구성하는 보안 생체인식을 이용하여 말단 사용자들의 엔드-투-엔드 인증을 제공한다.

[0033] 전술한 그리고 관련된 목표의 달성을 위해서, 하나 이상의 양태는 청구범위에서 특별히 지적되고 완전하게 이하에 설명된 특징들을 포함한다. 이하의 설명 및 첨부된 도면은 하나 이상의 양태들의 구체적인 예시적 특징들을 상세하게 설명한다. 그러나, 이러한 특징들은, 다양한 양태들의 원리가 채용될 수도 있는 다양한 방법을 설명하고, 이 설명은 모든 이러한 양태들 및 다른 동등물을 포함하도록 의도된다.

도면의 간단한 설명

[0034] 도 1 은, 본 발명의 양태에 따라서, 보안 생체인식 모델을 이용하여 암호화 프로세스를 강조하는 아이덴티티-기반 암호학 (cryptology) 에 대한 시스템의 블록도이다.

도 2 는, 본 발명의 양태에 따라서, 보안 생체인식 모델을 이용하여 암호해독 프로세스를 강조하는 아이덴티티-기반 암호학에 대한 시스템의 블록도이다.

도 3 은, 본 발명의 다른 양태에 따라서, 보안 생체인식 모델을 이용하여 아이덴티티-기반 암호학을 구현하는 컴퓨팅 디바이스의 상세 블록도이다.

도 4 는, 본 발명의 아이덴티티-기반 암호체계에 따라서, 생체인식 데이터 및 암호화된 데이터를 통신하도록 이용된 셀룰러 네트워크의 블록도이다.

도 5 는, 본 발명의 양태에 따라서, 보안 생체인식 모델을 구현하는 아이덴티티-기반 암호체계에서 데이터 암호화를 위한 방법의 흐름도이다.

도 6 은 본 발명의 또 다른 양태에 따라서, 보안 생체인식 모델을 구현하는 아이덴티티-기반 암호체계에서 등록 및 인증을 위한 방법의 흐름도이다.

도 7 은 본 발명의 양태에 따라서, 생체인식 특징, 왜곡된 생체인식 특징, 전체 왜곡된 특징 벡터들, 신드롬 특징 벡터들 및 인코딩된 신드롬 벡터들 사이의 의존적 관계를 나타내는 블록도이다.

도 8 은 본 발명의 양태에 따른 지문 특징점 (fingerprint minutiae) 인코딩의 블록도이다.

도 9 는, 본 발명에 따라서, 보안 생체인식 모델을 구현하는 아이덴티티-기반 암호체계에서의 데이터 암호화를 위한 방법의 흐름도이다.

도 10 은 본 발명의 양태에 따라서, 보안 생체인식 모델을 구현하는 아이덴티티-기반 암호체계의 방법 데이터 암호해독의 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0035] 도면을 참조하여 다양한 양태들이 이하 설명된다. 이하의 설명에서, 설명이 목적으로, 하나 이상의 양태의 전반적인 이해를 제공하기 위해 수많은 특정 실시형태가 설명된다. 그러나, 이러한 양태(들)은 이러한 특정 실시형태 없이 실행될 수도 있다는 것이 명백하다.

[0036] 본 출원서에 사용된 바와 같이, 용어 "컴포넌트", "모듈", "시스템" 등은 하드웨어, 펌웨어, 하드웨어와 소프트웨어의 조합, 소프트웨어, 또는 실행중인 소프트웨어와 같은 컴퓨터-관련 엔티티를 포함하지만 이에 한정되지 않도록 의도된다. 예를 들어, 컴포넌트는, 프로세서 상에서 구동되는 프로세스, 프로세서, 오브젝트, 실행가능한 것, 실행중인 스레드, 프로그램 및/또는 컴퓨터일 수도 있지만, 이에 한정하지 않는다. 예시에 의해, 컴퓨팅 디바이스상에서 구동하는 어플리케이션 및 컴퓨터 디바이스 모두는 컴포넌트일 수 있다. 하나 이상의 컴포넌트들은 프로세서 및/또는 실행중인 스레드 내에 상주할 수 있고, 일 컴포넌트는 하나의 컴퓨터상에 국한될 수도 있고 및/또는 2 개 이상의 컴퓨터들 사이에서 분배될 수도 있다. 또한, 이러한 컴포넌트들은 저장된 다양한 데이터 구조를 갖는 다양한 컴퓨터 판독가능 매체로부터 실행될 수 있다. 컴포넌트들은, 로컬 시스템, 분배 시스템, 및/또는 신호에 의한 다른 시스템과의 네트워크 (예를 들어, 인터넷) 내에서의 다른 컴포넌트와 상호작용하는 하나의 컴포넌트로부터의 데이터와 같은 하나 이상의 데이터 패킷을 갖는 신호에 따라

서 로컬 및/또는 원격 프로세스에 의해 통신할 수도 있다.

[0037] 또한, 본 명세서에서 다양한 양태들이 유선 단말기 또는 무선 단말기일 수 있는 단말기와 접속되어 있다. 또한, 단말기는 시스템, 디바이스, 가입자 유닛, 가입자국 (subscriber station), 이동국, 모바일, 이동 디바이스, 원격국, 원결 단말기, 액세스 단말기, 사용자 단말기, 단말기, 통신 디바이스, 사용자 에이전트, 사용자 디바이스, 또는 사용자 장비 (UE) 로 지칭될 수 있다. 무선 단말기는 셀룰러 전화기, 위성 전화기 (satellite phone), 무선 전화기, 세션 초기 프로토콜 (SIP; session Initiation Protocol) 전화기, 무선 가입자 망 (WLL; Wireless Local Loop) 스테이션, 휴대 정보 기기 (PDA), 무선 접속 성능을 갖는 핸드헬드 디바이스, 컴퓨팅 디바이스, 또는 무선 모뎀에 접속된 다른 프로세싱 디바이스일 수도 있다. 또한, 기지국과 관련된 다양한 양태가 여기에 설명된다. 또한, 기지국은 무선 단말기(들)와 통신하기 위해 사용될 수도 있고, 액세스 포인트, 노드 B, 또는 몇몇 다른 용어로 지칭될 수도 있다.

[0038] 또한, 용어 "또는 (or)" 는 배타적인 "or" 이기보다는 포괄적인 "or" 를 의미하는 것으로 의도된다. 즉, 이와 다르게 구체적으로 또는 문맥에서 명백하게 언급되지 않는 한, 문구 "X 가 A 또는 B 를 채용한다 (X employs A or B)" 는 임의의 자연적인 포괄적 대체를 의미하는 것으로 의도된다. 즉, 문구 "X 가 A 또는 B 를 채용한다" 는: X 가 A 를 채용한다; X 가 B 를 채용한다; 또는 X 가 A 및 B 모두를 채용한다를 충족한다. 또한, 본 출원서에 이용된 것과 같은 관사 "a" 및 "an" 및 첨부된 청구범위는, 이와 다르게 구체적으로 또는 문맥에서 명백하게 단수의 형태인 것으로 지적하도록 언급되지 않는 한, "하나 이상 (one or more)" 을 의미하도록 구성되어야만 한다.

[0039] 본 명세서에 설명된 기술은, CDMA, TDMA, FDMA, OFDMA, SC-FDMA 및 다른 시스템과 같은 다양한 무선 통신 시스템에 사용될 수도 있다. 용어 "시스템" 및 "네트워크" 는 상호교환적으로 종종 사용된다. CDMA 시스템은 UTRA (Universal Terrestrial Radio Access), cdma2000 등과 같은 무선 기술을 구현할 수도 있다. UTRA 는 광대역-CDMA (W-CDMA) 및 CDMA 의 다른 변형물을 포함한다. 또한, cdma2000 은 IS-2000, IS-95 및 IS-856 표준을 커버한다. TDMA 시스템은 GSM (Global System for Mobile Communications) 와 같은 무선 기술을 구현할 수도 있다. OFDMA 시스템은 E-UTRA (Evolved UTRA), UMB (Ultra Mobile Broadband), IEEE 802.11 (Wi-Fi), IEEE 802.16 (WiMAX), IEEE 802.20, Flash-OFDM 등과 같은 무선 기술을 구현할 수도 있다. UTRA 및 E-UTRA 는 UMTS (Universal Mobile Telecommunication System) 의 일부이다. 3GPP LTE (3GPP Long Term Evolution) 은, 다운링크상에서 OFDMA 및 업링크상에서 SC-FDMA 를 채용하는 E-UTRA 를 이용하는 UMTS 의 해제이다. UTRA, E-UTRA, UMTS, LTE 및 GSM 은 "3rd Generation Partnership Project" (3GPP) 로 명명된 조직 (organization) 으로부터의 문헌에 기재되어 있다. 추가적으로, cdma2000 및 UMB 는 "3rd Generation Partnership Project 2" (3GPP2) 로 명명된 조직으로부터의 문헌에 기재되어 있다. 또한, 이러한 무선 통신 시스템은 언페어드 무허가 스펙트럼 (unpaired unlicensed spectrums), 802.xx 무선 LAN, BLUETOOTH 및 임의의 다른 단- 또는 장- 범위의 무선 통신 기술을 이용하는 피어-투-피어 (예를 들어, 모바일-투-모바일) *ad hoc* 네트워크 시스템을 추가적으로 포함할 수도 있다.

[0040] 다양한 양태 또는 특징은 수많은 디바이스, 컴포넌트, 모듈 등을 포함할 수도 있는 시스템과 관련하여 설명될 것이다. 다양한 시스템은 추가적인 디바이스, 컴포넌트, 모듈 등을 포함할 수도 있고 및/또는 도면과 관련하여 설명된 모든 디바이스, 컴포넌트, 모듈 등을 포함하지 않을 수도 있는 것으로 이해되고 파악될 것이다. 또한, 이러한 접근방식들의 조합이 이용될 수도 있다.

[0041] 본 명세서의 양태들은, 액세스 및 데이터 송신 모두를 위해 강화된 보안을 초래하는 고도의 보안 생체인식 모델을 이용하여 아이덴티티-기반 암호체계를 위한 방법, 장치 및 컴퓨터 프로그램 제품을 설명한다. 본 양태들은 신드롬 벡터 포맷의 생체인식 데이터를 저장하는 것에 의존하여 생체인식 데이터와 관련된 고유의 변동성의 허용오차를 제공한다. 그러나, 신드롬 벡터만의 이용은 생체인식 데이터를 복제하는 것과 관련된 문제를 검토하지 않아서, 이에 따라, 생체인식 데이터에 의해 제공된 보안을 깨뜨린다. 본 양태들은, 개인 키를 더욱 안전하게 만듦으로써 그리고 암호체계 사용자-아이덴티티를 의존적으로 만듦으로써 이러한 문제를 검토한다. 이를 달성하기 위해, 본 양태에서는, 종래의 키 생성 기술로부터 개인 키가 생성되고, 최종 암호화/암호해독 키는 일-방향 함수를 이용하여 개인 키 및 생체인식 데이터의 입력으로부터 생성된다. 따라서, 본 명세서에 설명된 방법, 장치 및 컴퓨터-프로그램은 대칭 아이덴티티-기반 암호체계를 구성하는 보안 생체인식 데이터를 이용하여 말단 사용자의 엔드-투-엔드 인증을 제공한다.

[0042] 도 1 및 도 2 는 아이덴티티-기반 암호체계 (10) 의 상위-레벨 블록도를 제공한다. 이 암호체계 (10) 는, 컴퓨팅 네트워크 (16) 를 통해서 통신하는 제 1 컴퓨팅 디바이스 (12) 및 제 2 컴퓨팅 디바이스 (14) 를 포함한

다. 도 1 및 도 2 에 도시된 이 체계 (10) 는 무선 통신 디바이스인 데이터 암호화를 위한 제 1 컴퓨팅 디바이스 (12) 및 무선 통신 디바이스인 데이터 암호해독을 위한 제 2 컴퓨팅 디바이스 (14) 를 포함하고, 이 디바이스들은 무선 통신 네트워크인 컴퓨팅 네트워크 (16) 를 통해서 통신하고, 본 명세서에 개시된 암호체계는 컴퓨팅 네트워크를 통해서 데이터를 송신하는 무선 또는 유선의 임의의 컴퓨팅 디바이스에서 활용될 수도 있다.

추가적으로, 도 1 및 도 2 는 제 1 무선 통신 디바이스 (12) 에 의한 암호화 및 제 2 무선 통신 디바이스 (14) 에 의한 암호해독을 나타내고, 대부분의 경우, 각각의 무선 통신 디바이스는 필수적인 하드웨어 및 소프트웨어를 갖는 것으로 구성되어 도 3 에 도시된 것과 같이 개시된 양태들에 대한 암호화 및 암호해독 모두를 수행할 수도 있다.

[0043] 도 1 을 참조하여, 아이덴티티-기반 암호화를 제공하도록 동작가능한 제 1 컴퓨팅 디바이스 (12) 는 프로세서 (20) 및 프로세서 (20) 와 통신하는 메모리 (22) 를 포함하는 컴퓨팅 플랫폼 (18) 을 포함한다. 컴퓨팅 플랫폼 (18) 은 컴퓨팅 디바이스 (12) 의 사용자에 관련된 생체인식 데이터를 감지하고 캡쳐하도록 동작가능한 하나 이상의 생체인식 센서 (24) 를 포함한다. 생체인식 센서는 지문 센서, 음성 센서, 얼굴 특징 센서, 안구/홍채 센서, 및 사용자의 생체인식 특징을 검출하고 캡쳐하는 임의의 다른 센서를 포함할 수도 있지만 이에 한정하지 않는다. 본 명세서에서 설명된 생체인식 센서 (24) 는 독립형 센서이지만, 센서는 프로세서 (20) 의 프로세싱 서브시스템으로서 채용될 수도 있고, 또는 메모리 (22) 내에 위치된 소프트웨어 모듈로서 채용될 수도 있다.

[0044] 컴퓨팅 플랫폼 (18) 의 메모리 (22) 는, 생체인식 센서 (24) 로부터 생체인식 데이터를 수신하고 그 생체인식 데이터를 소거가능한 생체인식 데이터로서 당업계에서 지칭되는 복수의 왜곡된 생체인식 데이터로 왜곡시키도록 동작가능한 생체인식 데이터 왜곡기 (26) 를 포함한다. 생체인식 데이터 왜곡기 (26) 는, 생체인식 데이터를 왜곡하고, 조작하고, 필터링하고 또는 그밖에 변경시키는 임의의 디바이스일 수도 있다. 또한, 생체인식 데이터 왜곡기 (26) 는 전체 수신된 생체인식 데이터 또는 임의의 그 일부에 왜곡을 적용할 수도 있다 또한, 생체인식 데이터 왜곡기 (26) 는 2 개 이상의 유형의 생체인식 센서 (24) 로부터 유출되는 생체인식 데이터를 왜곡하도록 구성되어, 그 결과로 왜곡된 생체인식 데이터가 2 개 이상의 생체인식 센서 (26) 로부터 수신된 생체인식 데이터들의 조합이 된다. 생체인식 데이터 왜곡기 (26) 는 메모리 (22) 내에 위치되어, 이에 따라, 소프트웨어에 채용되는 것으로서 도시되고, 생체인식 데이터 왜곡기 (26) 는 하드웨어에서 구현될 수도 있고, 이에 따라 메모리 (22) 외부에 위치될 수도 있다는 것을 유념해야만 한다. 생체인식 데이터를 왜곡시킴으로써, 추가된 레벨의 안전성이 제공되어 공격자로부터 복제되는 것으로부터 그 데이터를 보호하는 것이 제공된다.

[0045] 추가적으로, 컴퓨팅 플랫폼 (18) 의 메모리 (22) 는 복수의 왜곡된 생체인식 데이터 각각에 대한 신드롬 벡터 (30) 를 생성하고 저장하도록 동작가능한 생체인식 샘플러 (28) 를 포함한다. 나중에 이하 설명될 신드롬 벡터는 생체인식 데이터의 고유의 변동성에 대한 허용오차를 제공한다. 본 양태에서, 왜곡된 생체인식 데이터는 신드롬 벡터 (30) 의 형태로 저장되어, 이에 따라, 생체인식 데이터의 변동성을 정정할 뿐만 아니라 안전한 왜곡된 (즉, 소거가능한) 생체인식 데이터의 이용을 통해서 강화된 안전성을 제공한다.

[0046] 추가적으로, 컴퓨팅 플랫폼 (18) 의 메모리 (22) 는, 암호화 프로세스에서 하나 이상의 함수에, 랜덤 수 또는 임의의 다른 형태의 랜덤성과 같은 랜덤화기 (34) 를 제공하도록 동작가능한 랜덤화 모듈 (32) 을 포함한다.

일 양태에서, 랜덤화 모듈 (32) 은 암호화 키를 생성하기 위해 사용된 왜곡된 생체인식 데이터의 랜덤 선택에 랜덤화기 (34) 를 제공하도록 동작가능하다. 따라서, 랜덤화 모듈 (32) 은 왜곡된 생체인식 데이터의 랜덤 샘플 (38) 및 개인 키 (40) 에 기초하여 암호화 키 (42) 를 생성하도록 동작가능한 암호화 키 생성기 (36) 와 통신할 수도 있다. 암호화 키 (42) 를 생성하도록 이용된 생체인식 데이터의 랜덤 샘플 (38) 이 신드롬 벡터의 랜덤 샘플이 될 수도 있도록, 왜곡된 생체인식 데이터의 랜덤 샘플 (38) 은 신드롬 벡터 (30) 의 형태로 저장된 왜곡된 생체인식 데이터에 랜덤화기 (34) 를 적용함으로써 획득될 수도 있다. 개인 키 (40) 는 개인 키를 생성하기 위한 임의의 종래의 기술에 의해 생성된다. 암호화 키는, 로그 기반 함수 (log based function) 와 같은 일-방향 함수, 예를 들어, Elgamal, Elliptic Curve Menezes-Qu-Vanstone (ECMQV), Elliptic Curve Diffie-Hellman (ECDH) 등을 이용하여 생성될 수도 있다.

[0047] 추가적으로, 컴퓨팅 플랫폼 (18) 의 메모리 (22) 는, 프로세서 (20) 와 통신하고 데이터 (46) 를 암호화시키기 위해 암호화 키 (42) 를 적용하도록 동작가능한 암호화 엔진 (44) 을 포함한다.

[0048] 제 1 컴퓨팅 디바이스 (12) 는, 프로세서 (20) 와 통신하는 통신 모듈 (48) 을 추가적으로 포함한다. 통신 모듈은 생체인식 데이터 및 개인 키를 제 2 컴퓨팅 디바이스 (14) 와 같은 다른 컴퓨팅 디바이스에 통신하도록

동작가능하다. 대부분의 예시에서, 통신 모듈은 다른 컴퓨팅 디바이스와의 첫 번째/초기 통신에 기초하여 생체인식 데이터 및 개인 키 (40) 를 다른 컴퓨팅 디바이스에 통신하도록 구성될 수도 있다. 또한, 통신 모듈은 다른 컴퓨팅 디바이스에 의한 후속 암호해독을 위해 그 다른 컴퓨팅 디바이스에 암호화된 데이터 (46) 및 랜덤화기 (34) 를 통신하도록 동작가능하다.

[0049] 도 2 를 참조하여, 아이덴티티-기반 암호해독을 제공하도록 동작가능한 제 2 컴퓨팅 디바이스 (14) 는 프로세서 (52) 및 그 프로세서 (52) 와 통신하는 메모리 (54) 를 포함하는 컴퓨팅 플랫폼 (50) 을 포함한다. 컴퓨팅 플랫폼 (50) 의 메모리 (54) 는 제 1 컴퓨팅 디바이스 (12) 와 같은 다른 컴퓨팅 디바이스로부터 수신된 생체인식 데이터 (58) 및 개인 키 (40) 를 저장하도록 동작가능한 생체인식 어드레스 북 (56) 을 포함한다. 생체인식 데이터 (58) 및 개인 키 (40) 는, 그 생체인식 데이터와 그 개인 키가 디바이스 식별자 (60) 에 따라 생체인식 어드레스 북 (56) 에서 수신되는, 디바이스에 관련된다. 디바이스 식별자 (60) 는 전화 번호, IP 어드레스 등일 수도 있다. 몇몇 양태에서, 어드레스 북 (56) 에 저장된 생체인식 데이터 (58) 는 왜곡된 생체인식 데이터일 수도 있고, 이 왜곡된 생체인식 데이터는 신드롬 벡터 (30) 의 형태일 수도 있다. 생체인식 어드레스 북 (56) 에서의 엔트리는 다른 컴퓨팅 디바이스와의 초기, 첫 번째 통신에 기초하여 생성될 수도 있다.

다른 컴퓨팅 디바이스는 제 2 컴퓨팅 디바이스 (14) 와의 초기 통신에 기초하여 생체인식 데이터 (58) 및 개인 키 (40) 를 자동으로 전송할 수도 있고, 또는, 제 2 컴퓨팅 디바이스는 다른 컴퓨팅 디바이스에 대한 생체인식 어드레스 북 (56) 내에 엔트리가 현재 존재하지 않는다는 것을 검증한 후에 생체인식 데이터 및 개인 키를 요청할 수도 있다. 대부분의 양태에서, 생체인식 어드레스 북 (56) 은 제 2 컴퓨팅 디바이스 (14) 의 메모리 (54) 에 상주할 수도 있고, 또한, 본 명세서에 개시된 혁신적인 개념으로 이 어드레스 북 (56) 이 네트워크 저장 사이트 (도 2 에는 도시되지 않음) 에 상주하고 제 2 컴퓨팅 디바이스 (14) 에 원격으로 액세스가능하다.

[0050] 추가적으로, 제 2 컴퓨팅 디바이스 (14) 는 제 1 컴퓨팅 디바이스 (12) 로부터의 암호화된 데이터 (46) 및 랜덤화기 (34) 를 수신하도록 동작가능한 프로세서 (52) 와 통신하는 통신 모듈 (62) 을 포함한다. 암호화된 데이터 (46) 및 랜덤화기 (34) 의 수신에 기초하여, 암호해독 키 생성기 (64) 는 암호화된 데이터 (46) 에 대한 적절한 암호해독 키 (66) 를 생성하도록 실시된다.

[0051] 암호해독 키 생성기 (64) 는 메모리 (54) 에 저장되고 프로세서 (52) 와 통신한다. 암호해독 키 생성기 (64) 는, 랜덤화기 (34) 에 기초하여 생체인식 어드레스 북 (56) 에 저장된 생체인식 데이터 (58) 의 랜덤 샘플 (38) 을 획득하고 개인 키 (40) 와 생체인식 데이터 랜덤 샘플 (38) 의 조합을 이용하여 암호해독 키 (66) 를 생성하도록 동작가능하다. 명시된 바와 같이, 제 1 컴퓨팅 디바이스 (12) 의 암호화 키 생성기 (도 1 의 36) 에서 생체인식 데이터의 동일한 랜덤 샘플을 선택하도록 이용되는 것과 같이, 동일한 랜덤화기 (34) 가 암호화 키 생성기에서 생체인식 데이터의 랜덤 샘플을 선택하도록 이용된다.

[0052] 추가적으로, 제 2 컴퓨팅 디바이스는 메모리 (54) 에 저장되고 프로세서 (52) 와 통신하는 암호해독 엔진 (68) 을 포함한다. 암호해독 엔진 (68) 은 암호해독 키 (66) 를 이용하여 암호화된 데이터 (46) 를 암호해독하도록 동작가능하여 암호해독된 데이터 (70) 를 결과로 획득한다.

[0053] 도 3 을 참조하여, 일 양태에 따라서, 컴퓨팅 디바이스, 구체적으로, 도 1 및 도 2 에 도시된 아이덴티티-기반 암호체계의 두 가지 양상을 채용하도록 구성된 무선 통신 디바이스 (100) 의 상세한 블록도 표현이다. 무선 통신 디바이스 (100) 는, 셀룰러 전화기, PDA, 양방향 텍스트 페이저, 휴대용 컴퓨터 및 무선 통신 포털을 갖고 네트워크 또는 인터넷에 유선 접속을 가질 수도 있는 별개의 컴퓨터 플랫폼과 같은 컴퓨터화된 통신 디바이스의 임의의 유형을 포함할 수도 있다. 무선 통신 디바이스는, 원격 슬레이브일 수 있고, 또는, 원격 센서, 진단 툴, 데이터 릴레이 등과 같은 무선 네트워크를 통해서 데이터를 간단하게 통신하지만 그 말단-사용자를 갖지 않는 다른 디바이스일 수 있다. 따라서, 본 장치 및 방법은 무선 통신 포털을 포함하고, 무선 모뎀, PCMCIA 카드, 액세스 단말기, 데스크탑 컴퓨터 또는 그 임의의 조합 또는 서브-조합을 포함하지만 이에 한정하지 않는 무선 통신 디바이스 또는 무선 컴퓨터 모듈의 임의의 형태에서 수행될 수 있다.

[0054] 무선 통신 디바이스 (100) 는, 무선 네트워크를 통해서 데이터를 송신하고 루틴 및 어플리케이션을 수신하고 실행할 수 있는 컴퓨터 플랫폼 (102) 을 포함한다. 컴퓨터 플랫폼 (102) 은 RAM 및 ROM, EPROM, EEPROM, 플래시 카드, 또는 컴퓨터 플랫폼들에 공통인 임의의 메모리와 같은 휘발성 및 비휘발성 메모리를 포함할 수도 있는 메모리 (104) 를 포함한다. 또한, 메모리 (104) 는 하나 이상의 플래시 메모리 셀을 포함할 수도 있고, 또는, 자기 매체, 광학 매체, 테이프, 또는 소프트 또는 하드 디스크와 같은 임의의 제 2 또는 제 3 의 저장 디바이스일 수도 있다.

[0055] 또한, 컴퓨터 플랫폼 (102) 은 주문형 반도체 (ASIC; application-specific integrated circuit), 또는 다른

칩셋, 프로세서, 로직 회로, 또는 다른 데이터 프로세싱 디바이스일 수도 있는 프로세서 (106) 를 포함한다.

프로세서 (106), 또는 ASIC 와 같은 다른 프로세서는, 생체인식 데이터 왜곡기 (26), 생체인식 샘플러 (28), 랜덤화 모듈 (32), 암호화 키 생성기 (36), 암호화 엔진 (44), 암호해독 키 생성기 (64) 또는 무선 디바이스 (100) 의 메모리 (104) 에 저장된 암호해독 엔진 (68) 과 같은 임의의 상주 프로그램으로 인터페이싱하는 어플리케이션 프로그래밍 인터페이스 ("API") 계층 (108) 을 실행할 수도 있다. API (108) 는 통상적으로 각각의 무선 디바이스 상에서 실행하는 실행시간 환경이다. 하나의 이러한 실행시간 환경은, 캘리포니아, 샌 디에고 소재의 Qualcomm, Inc. 가 개발한 Wireless® (BREW®) 소프트웨어 용 Binary Runtime Environment 이다. 예를 들어, 무선 컴퓨팅 디바이스상에서의 어플리케이션의 실행을 제어하도록 동작하는 다른 실행시간 환경이 활용될 수도 있다.

[0056] 프로세서 (106) 는, 무선 네트워크상에서 통신 디바이스 (100) 의 기능 및 통신 디바이스의 동작을 가능하게 하는 하드웨어, 펌웨어, 소프트웨어, 및 그 조합에 채용된 다양한 프로세싱 서브시스템 (110) 을 포함한다. 예를 들어, 프로세싱 서브시스템 (110) 은 다른 네트워킹된 디바이스와의 통신을 초기화하고 유지하도록 허용하고 데이터를 교환하는 것을 허용한다. 셀룰러 전화기와 같은 통신 디바이스가 정의된 양태에서, 통신 프로세서 (106) 는, 사운드, 비휘발성 메모리, 파일 시스템, 송신, 수신, 탐색기, 계층 1, 계층 2, 계층 3, 주요 콘트롤, 원격 프로시저, 핸드셋, 전력 관리, 디지털 신호 프로세서, 메시징, 호출 관리기, Bluetooth® 시스템, Bluetooth® LPOS, 포지션 엔진, 사용자 인터페이스, 슬립, 데이터 서비스, 보안, 인증, USIM/SIM, 음성 서비스, 그래픽, USB, 멀티미디어 (예를 들어, MPEG, GPRS 등) (명백함을 위해, 도 3 에 개별적으로 모두 도시됨) 과 같은 프로세싱 서브시스템 (110) 의 하나 또는 그 조합을 포함할 수도 있다. 개시된 양태에 대해, 프로세서 (106) 의 프로세싱 서브시스템 (110) 은 임의의 생체인식 센서 (24) 및 메모리 (104) 내에 저장된 임의의 모듈, 예를 들어, 생체인식 데이터 왜곡기 (24) 또는 메모리 (104) 에 저장된 임의의 모듈 (예를 들어, 생체인식 데이터 왜곡기 (26), 생체인식 샘플러 (28), 랜덤화 모듈 (32), 암호화 키 생성기 (36), 암호화 엔진 (44), 암호해독 키 생성기 (64) 또는 암호해독 엔진 (68)) 을 포함할 수도 있다.

[0057] 추가적으로, 컴퓨터 플랫폼 (102) 은, 무선 통신 디바이스 (100) 의 다양한 컴포넌트들 사이에서 뿐만 아니라 무선 디바이스 (100) 와 무선 네트워크 (16) 사이에서의 통신을 가능하게 하는, 하드웨어, 펌웨어, 소프트웨어 및 그 조합에 채용된 통신 모듈 (112) 을 포함한다. 개시된 양태에서, 통신 모듈 (112) 은 무선 통신 디바이스 (100) 와 다른 유선 또는 무선 디바이스 사이의 모든 해당 통신을 가능하게 한다. 따라서, 통신 모듈 (112) 은 무선 네트워크 통신 접속을 확립하기 위한 필수적인 하드웨어, 펌웨어, 소프트웨어 및/또는 그 조합을 포함할 수도 있다. 몇몇 양태에서, 통신 모듈은, 다른 컴퓨팅 디바이스의 생체인식 어드레스 북에 포함되는 다른 컴퓨팅 디바이스에 생체인식 데이터 (58) 및 개인 키 (40) 를 전송하고, 상주 생체인식 어드레스 북 (56) 에 포함되는 다른 컴퓨팅 디바이스로부터 생체인식 데이터 (58) 및 개인 키 (40) 를 수신하고, 그리고 암호화된 데이터 (46) 및 관련 랜덤화기 (34) 를 전송하거나 수신하도록 동작가능하다.

[0058] 컴퓨팅 플랫폼 (102) 은 무선 통신 디바이스 (100) 의 사용자에 관련된 생체인식 데이터를 감지하고 캡쳐하도록 동작가능한 하나 이상의 생체인식 센서 (24) 를 포함한다. 생체인식 센서는, 지문 센서, 음성 센서, 얼굴 특징 센서, 안구/홍채 센서, 및 사용자의 생체인식 특징을 검출하고 캡쳐하는 임의의 다른 센서를 포함할 수도 있지만 이에 한정하지 않는다. 본 명세서에 설명된 생체인식 센서 (24) 는 독립형 센서이지만, 이 센서는 또한 프로세서 (106) 의 프로세싱 서브시스템 (110) 으로서 채용될 수도 있고 메모리 (104) 내에 위치된 소프트웨어 모듈로서 채용될 수도 있다.

[0059] 컴퓨팅 플랫폼 (102) 의 메모리 (104) 는, 생체인식 센서 (24) 로부터 생체인식 데이터를 수신하고, 그 생체인식 데이터를 당업계에서 소거가능한 생체인식 데이터로서 지칭되는 복수의 왜곡된 생체인식 데이터로 왜곡하도록 동작가능한 생체인식 데이터 왜곡기 (26) 를 포함한다. 생체인식 데이터 왜곡기 (26) 는 생체인식 데이터를 왜곡하고, 조작하고, 필터링하고 또는 그밖에 변경시키는 임의의 알고리즘일 수도 있다. 또한, 생체인식 데이터 왜곡기 (26) 는 전체 수신 생체인식 데이터 또는 임의의 부분에 왜곡을 적용할 수도 있다. 또한, 그 결과 왜곡된 생체인식 데이터가 2 개 이상의 생체인식 센서 (26) 들로부터 수신된 생체인식 데이터들의 조합이 되도록, 생체인식 데이터 왜곡기 (26) 는 생체인식 센서 (24) 의 2 개 이상의 유형으로부터 유입되는 생체인식 데이터를 왜곡하도록 구성될 수도 있다. 생체인식 데이터 왜곡기 (26) 는 메모리 (104) 내에 위치될 수도 있는 것으로, 따라서 소프트웨어 내에 채용되는 것으로 도시되었지만, 생체인식 데이터 왜곡기 (26) 는 하드웨어에서 구현될 수도 있고, 따라서, 메모리 (104) 외부에 위치될 수도 있다는 것에 유의해야만 한다.

[0060] 추가적으로, 컴퓨팅 플랫폼 (102) 의 메모리 (104) 는 복수의 왜곡된 생체인식 데이터 각각에 대해 신드롬 벡터

(30) 를 생성하고 저장하도록 동작가능한 생체인식 샘플러 (28) 를 포함한다. 본 양태에서, 왜곡된 생체인식 데이터는 신드롬 벡터 (30) 의 형태로 저장되고, 이에 따라, 생체인식 데이터의 변동성을 정정할 뿐만 아니라 안전하게 왜곡된 (즉, 소거가능한) 생체인식 데이터의 이용을 통해서 강화된 안전성을 제공한다. 추가적으로, 생체인식 샘플러 (28) 는 왜곡된 생체인식 데이터에 에러 정정을 적용하도록 동작가능한 선택적인 에러 정정 코드 모듈 (114) 을 포함할 수도 있다. 생체인식 샘플러 (28) 가 에러 정정 코드 프로세싱을 구현하는 양태에서, 에러 정정 코드 적용은 랜덤일 수도 있다. 따라서, 에러 정정 코드 모듈 (114) 은 랜덤 수 또는 랜덤성의 임의의 다른 형태와 같은 랜덤화기 (34) 를 에러 정정 코드 모듈 (114) 에 제공하도록 동작가능한 랜덤화 모듈 (32) 과 통신할 수도 있다.

[0061] 일 양태에서, 랜덤화 모듈 (32) 은 암호화 키를 생성하도록 이용된 왜곡된 생체인식 데이터의 랜덤 선택에 랜덤화기 (34) 를 제공하도록 동작가능하다. 따라서, 랜덤화 모듈 (32) 은 왜곡된 생체인식 데이터의 랜덤 샘플 (38) 및 개인 키 (40) 에 기초하여 암호화 키 (42) 를 생성하도록 동작가능한 암호화 키 생성기 (36) 와 통신할 수도 있다. 왜곡된 생체인식 데이터의 랜덤 샘플 (38) 은 신드롬 벡터 (30) 의 형태로 저장된 왜곡된 생체인식 데이터에 랜덤화기 (34) 를 적용함으로써 획득될 수도 있으므로, 암호화 키 (42) 를 생성하도록 이용된 생체인식 데이터의 랜덤 샘플 (38) 이 신드롬 벡터의 랜덤 샘플이 될 수도 있다. 개인 키 (40) 는 개인 키를 생성하게 하기 위한 임의의 종래의 기술에 의해 생성될 수도 있다. 암호화 키는, 로그 기반 함수와 같은 일-방향 함수, 예를 들어, Elgamal, Elliptic Curve Menezes-Qu-Vanstone (ECMQV), Elliptic Curve Diffie-Hellman (ECDH) 등을 이용하여 생성될 수도 있다. 추가적으로, 컴퓨팅 플랫폼 (102) 의 메모리 (104) 는, 프로세서 (20) 와 통신하고 데이터 (46) 를 암호화하기 위해 암호화 키 (42) 를 적용하도록 동작가능한 암호화 엔진 (44) 을 포함한다.

[0062] 암호화 관점에서, 컴퓨팅 플랫폼 (102) 의 메모리 (104) 는, 생체인식 데이터 및 키가 수신되는 디바이스와의 관계에 기초하여 생체인식 데이터 (58) 및 개인 키 (40) 를 저장하도록 동작가능한 생체인식 어드레스 북 (56) 을 포함할 수도 있다. 이 관계는, 전화 번호, IP 주소 등일 수도 있는 디바이스 식별자 (60) 에 기초할 수도 있다. 몇몇 양태에서, 어드레스 북 (56) 에 저장된 생체인식 데이터 (58) 는 왜곡된 생체인식 데이터일 수도 있고, 또한, 이 왜곡된 생체인식 데이터는 신드롬 벡터 (30) 의 형태일 수도 있다. 생체인식 어드레스 북 (56) 에서의 엔트리는 다른 컴퓨팅 디바이스와의 초기, 첫 번째 통신에 기초하여 생성될 수도 있다.

[0063] 추가적으로, 메모리 (104) 는, 랜덤화기 (34) 에 기초하여 생체인식 어드레스 북 (56) 에 저장된 생체인식 데이터 (58) 의 랜덤 샘플 (38) 을 획득하고 개인 키 (40) 와 생체인식 데이터 랜덤 샘플 (38) 의 조합을 이용하여 암호해독 키 (66) 을 생성하도록 동작가능한 암호해독 키 생성기 (64) 를 포함한다. 또한, 메모리 (104) 는 암호화 데이터 (70) 를 결과로 획득하기 위해 암호해독 키 (66) 를 이용하여 암호화 데이터 (46) 를 암호화하도록 동작가능한 암호해독 엔진 (68) 을 포함한다.

[0064] 추가적으로, 무선 통신 디바이스 (100) 는 통신 디바이스에 입력을 생성시키기 위한 압력 메커니즘 (116), 및 통신 디바이스의 사용자에 의한 소비에 대한 정보를 생성하기 위한 출력 메커니즘 (118) 을 갖는다. 예를 들어, 입력 메커니즘 (116) 은 키 또는 키보드, 마우스, 터치-스크린 디스플레이, 마이크로폰 등과 같은 메커니즘을 포함할 수도 있다. 또한, 예를 들어, 출력 메커니즘 (118) 은 디스플레이, 음성 스피커, 햅틱 피드백 메커니즘 등을 포함할 수도 있다.

[0065] 도 4 는, 생체인식 데이터, 암호화 키 및 암호화된 데이터를 통신하기 위해 본 양태와 관련하여 사용될 수도 있는 셀룰러 네트워크 (120) 의 블록도를 나타낸다. 무선 네트워크 (16) 는 셀룰러 네트워크 (120) 내에 포함될 수도 있고, 무선 디바이스들 사이 및/또는 무선 디바이스와 유선 컴퓨팅 디바이스 사이에서 생체인식 데이터, 암호화 키 및 암호화된 데이터를 통신하도록 구현할 수도 있다. 도 4 를 참조하여, 일 양태에서, 제 1 컴퓨팅 디바이스 및 제 2 컴퓨팅 디바이스 (12 및 14) 는 셀룰러 전화기와 같은 무선 통신 디바이스를 포함한다. 본 양태에서, 무선 통신 디바이스는 셀룰러 네트워크 (120) 를 통해서 통신하도록 구성된다. 셀룰러 네트워크 (120) 는, 생체인식 데이터 및/또는 암호화된 데이터를 포함하는 데이터 패킷과 같은 통신 데이터 패킷을 통신하도록 하는 능력을 무선 통신 디바이스 (12 및 14) 에 제공한다. 셀룰러 전화기 네트워크 (120) 는 캐리어 네트워크 (124) 를 통해서 유선 네트워크 (122) 에 접속된 무선 네트워크 (16) 를 포함할 수도 있다. 도 4 는, 무선 통신 네트워크의 컴포넌트들 및 본 체계의 일 양태의 엘리먼트들의 상관관계를 더욱 완전하게 나타내는 상징적인 도면이다. 셀룰러 전화기 네트워크 (120) 는 단지 설명적이고, 무선 통신 디바이스 (12 및 14) 와 같은 원격의 모듈이 무선 네트워크 캐리어 및/또는 서버를 포함하지만 이에 한정하지 않는 무선 네트워크 (16) 의 컴포넌트들 사이에서 및/또는 서로간에 무선으로 통신하는 임의의 시스템을 포함할 수

있다.

[0066] 네트워크 (120) 에서, 본 양태에 따라서, 생체인식 어드레스 북을 포함하는 생체인식 암호화/암호해독을 포함하도록 구성될 수도 있는 컴퓨팅 디바이스 (126) 는 유선 네트워크 (122) (예를 들어, 로컬 영역 네트워크, LAN) 을 통해서 통신할 수 있다. 컴퓨팅 디바이스 (126) 는 무선 디바이스 (12 및 14) 에 그리고 무선 디바이스 (12 및 14) 로부터의 생체인식 데이터 및/또는 암호화된 데이터를 포함하는 데이터 패킷과 같은 통신 데이터 패킷을 수신 및/또는 생성하고 그리고 통신할 수도 있다. 컴퓨팅 디바이스 (126) 는 셀룰러 텔레커뮤니케이션 서비스를 제공하기 위해 필요한 임의의 다른 네트워크 컴포넌트를 갖는 셀룰러 전화기 네트워크 (120) 상에 존재할 수도 있다. 컴퓨팅 디바이스 (126) 는 인터넷, 보안 LAN, WAN, 또는 다른 네트워크와 같은 데이터 링크일 수도 있는 데이터 링크 (128 및 130) 를 통해서 캐리어 네트워크 (124) 와 통신한다. 캐리어 네트워크 (124) 는 모바일 스위칭 센터 ("MSC") (132) 로 전송된 메시지 (일반적으로는 데이터 패킷) 를 제어한다. 또한, 캐리어 네트워크 (124) 는 인터넷 및/또는 POTS ("plain old telephone service") 과 같은 네트워크 (130) 에 의해 MSC (132) 와 통신한다. 통상적으로, 네트워크 (130) 에서, 네트워크 또는 인터넷 부분은 데이터를 전송하고, POTS 부분은 음성 정보를 전송한다. MSC (132) 는, 데이터 네트워크와 같은 다른 네트워크 (136) 에 의한 다수의 기지국 ("BTS") (134), 및/또는 데이터 전송에 대한 인터넷 부분 및 음성 정보를 위한 POT 부분에 접속될 수도 있다. BTS (134) 는 짧은 메세징 서비스 ("SMS"), 또는 다른 통신 방법에 의해 메시지를 무선 통신 디바이스 (12 및 14) 에 무선으로 궁극적으로 브로드캐스팅한다.

[0067] 도 5 는, 본 양태에 따른, 보안 생체인식 모델을 이용하여 아이덴티티-기반 암호화를 위한 방법의 흐름도이다. 이벤트 (200) 에서, 원시 생체인식 데이터가, 샘플링되고, 캡처되고, 측정되고 또는 이와 다르게 몇몇 양태에 따라서 무선 컴퓨팅 디바이스일 수도 있는 컴퓨팅 디바이스의 사용자로부터 획득된다. 사전에 언급된 바와 같이, 생체인식 데이터는 특징적으로 샘플링될 수 있는 사용자에 연관된 임의의 생체인식 특징 또는 특성을 포함할 수도 있다. 생체인식 데이터의 예는, 지문 데이터, 음성 데이터, 안구 또는 홍채 특성 등과 같은 얼굴 특징 데이터를 포함하지만 이에 한정하지는 않는다.

[0068] 이벤트 (202) 에서, 원시 생체인식 데이터는 왜곡되고, 조작되고, 그렇지 않으면 변경되어, 소거가능한 생체인식 데이터로 지칭되는 복수의 왜곡된 생체인식 데이터를 결과로 획득한다. 몇몇 양태에서, 생체인식 데이터의 왜곡은 생체인식 데이터의 랜덤 왜곡일 수도 있다. 따라서, 이벤트 (204) 에서, 랜덤 수 등과 같은 선택적인 랜덤화기는 왜곡 프로세스를 랜덤화하기 위해 적용될 수도 있다. 추가적으로, 몇몇 양태에서, 생체인식 데이터의 왜곡은 왜곡 알고리즘의 사전-구성에 기초하여 시간 경과에 따라서 동적으로 변화할 수도 있다.

[0069] 이벤터 (206) 에서, 복수의 왜곡된 생체인식 데이터는 복수의 대응하는 신드롬 벡터들을 결과로 획득하기 위해 인코딩된 신드롬이다. 임의의 공지된 또는 미래에 공지되는 신드롬 코드는 신드롬 코드의 생성을 제공하기 위해 구현될 수도 있다. 예를 들어, Slepian Wolf (SW) 코드 또는 Wyner-Ziv (WZ) 코드는 신드롬 코드로서 이용될 수도 있다. 추가적으로, 등록 도중에 신드롬 인코더로 하여금 생체인식 데이터의 고유의 변동성을 추정하게 하고 정확한 양의 신드롬 비트를 인코딩하여 성공적인 신드롬 디코딩을 수행하게 하는 임베디드 신드롬 코드가 구현될 수도 있다. 생체인식 신드롬 벡터의 더욱 상세한 논의를 위해, 발명의 명칭이 "Biometric Based User Authentication and Data Encryption" 으로 2007년 7월 26일자로 발행된 미국 특허 공개 번호 제 2007/0174633호를 참조한다. 본 명세서에서, 이 출원은 여기에 완전하게 설명된 것처럼 참조로서 통합된다. 나중에 논의될 도 7 및 도 8 은, 신드롬 벡터들이 생체인식 데이터로부터 어떻게 형성되는지에 대한 더욱 상세한 논의를 제공한다.

[0070] 선택적인 이벤트 (208) 에서, 생체인식 데이터를 더욱 보안하기 위해 신드롬 벡터의 적어도 일부에 에러 정정이 적용된다. 에러 정정이 신드롬 벡터에 적용되는 이러한 양태에서, 에러 정정의 적용은 랜덤일 수도 있다. 따라서, 이벤트 (204) 에서, 랜덤 수 등과 같은 선택적인 랜덤화기는 에러 정정 프로세스에 적용될 수도 있다. 랜덤화기가 생체인식 데이터 (이벤트 202) 및 에러 정정 프로세스 (이벤트 204) 모두에 적용되는 이러한 양태에서, 랜덤화는 동일한 랜덤화기, 예를 들어, 동일한 랜덤 수를 구현하도록 동기화될 수도 있다.

[0071] 이벤트 (210) 에서, 개인 키에 따른 신드롬 벡터 포맷의 왜곡된 생체인식 데이터는 다른 컴퓨터 디바이스에 통신된다. 몇몇 양태에서, 왜곡된 생체인식 데이터와 개인 키의 통신은 초기에 다른 컴퓨팅 디바이스와의 접촉이 발생하는 경우에 발생한다. 예를 들어, 첫 번째 전화 호출, 데이터 호출 등에 기초한다. 데이터를 암호화하고 암호해독하도록 구현되는 개인 키는 임의의 종래의 공지된 또는 미래의 생성 기술에 의해 생성될 수도 있다.

[0072] 이벤트 (212) 에서, 암호화된 데이터를 송신하는 필요성에 기초하여, 암호화 키는 왜곡된 생체인식 데이터의 랜

덤 샘플과 개인 키의 조합에 기초하여 생성된다. 이벤트 (204) 에서, 랜덤 수 등과 같은 랜덤화기는 암호화 키를 생성하는데 사용되도록 왜곡된 생체인식 데이터 샘플의 선택에 적용될 수도 있다. 랜덤화기가 생체인식 데이터의 하나 이상의 왜곡 (이벤트 202) 및 에러 정정 프로세서 (이벤트 204) 에 적용되는 이러한 양태에서, 동일한 랜덤화기 예를 들어, 동일한 랜덤 수를 구현하도록 랜덤화기가 동기화될 수도 있다. 몇몇 양태에서, 일-방향 함수가 구현되어 암호화 키를 생성할 수도 있다. 일 방향-함수의 예시는 Elgamel, Elliptic Curve Menezes-Qu-Vanstone (ECMQV), Elliptic Curve Diffie-Hellman (ECDH) 등을 포함하지만 이에 한정하지는 않는다.

[0073] 이벤트 (214) 에서, 송신될 데이터는 생성된 암호화 키를 이용하여 암호화되고, 이벤트 (216) 에서, 암호화된 데이터 및 랜덤화기는 고안된 컴퓨팅 디바이스로 통신된다.

[0074] 도 6 은, 본 양태에 따라서, 등록 및 인증을 위한 신드롬 및 해싱 기반 생체인식 보안 시스템을 위한 방법의 흐름도이다. 이 방법은, 압축된 신드롬 벡터를 생성하기 위해 신드롬 코드에 의해 왜곡된 생체인식 파라미터를 압축하는 방법이다. 종래의 압축과 다르게, 오리지널 왜곡된 생체인식 데이터는 신드롬 코드에 의해 생성된 신드롬 벡터로부터 단독으로 복원되거나 또는 근사될 수는 없다. 오리지널 왜곡된 생체인식의 신드롬 벡터 및 해시가 생체인식 데이터베이스에 저장된다.

[0075] 등록 페이즈 (300) 의 이벤트 (302) 에서, 생체인식 데이터가 사용자로부터 캡쳐되고, 감지되고, 측정되거나 또는 획득된다. 이하, 이벤트 (304) 에서 생체인식 데이터는 소거가능한/왜곡된 생체인식 데이터를 형성하기 위해 왜곡되고, 조작되고 또는 그렇지 않으면 변경된다. 이벤트 (306) 에서, 신드롬 인코더는 등록 신드롬 벡터를 제조하기 위해 왜곡된 생체인식 데이터에 적용된다. 신드롬 코드의 임의의 유형이 이용되어 신드롬 벡터를 생성할 수도 있다. 예를 들어, SW 코드 또는 WZ 코드는 신드롬 코드로서 사용될 수도 있다. 신드롬 코드는, 소위 "반복-누적 코드 (repeat-accumulate codes)", 즉, "제품-누적 코드" 및 "확대된 해밍-누적 코드 (extended Hamming-accumulate codes)" 로부터 유래될 수 있다. 본 발명의 일 양태에서, 신드롬 인코더는 이진 값의 입력에 반대하는 것으로서 정수-값 입력에서 동작할 수 있다. 추가적으로, 신드롬 인코더는 생체인식 데이터베이스의 저장 요건을 최소화하기 위해 매우 높은 압축률을 가질 수도 있다. 추가적으로, 신드롬 인코더는 레이트-적응될 수 있고, 증분 방식으로 동작하도록 구성될 수 있다.

[0076] 선택적으로, 이벤트 (308) 에서, 메시지 인증 또는 해시 함수가 왜곡된 생체인식 파라미터에 적용되어 등록 해시를 생성한다. 해시 함수는 임의의 알려진 또는 미래의 알려진 암호그래픽 해시 함수일 수 있다. 이벤트 (310) 에서, 등록 신드롬 벡터 및 등록 해시 페어가 생체인식 데이터베이스에 저장된다.

[0077] 인증 페이즈 (320) 의 이벤트 (322) 에서, 생체인식 데이터는 다시 캡쳐되고, 감지되고, 또는 그렇지 않으면 사용자로부터 획득된다. 이하, 이벤트 (324) 에서, 생체인식 데이터는 왜곡되고, 조작되며, 또는 그렇지 않으면 등록 페이즈 (이벤트 304) 에서 발생된 동일한 왜곡, 조작 또는 변경에 따라서 변경되어, 인증 왜곡된 생체인식 데이터 (E') 를 결과로 획득한다. 이벤트 (326) 에서, 생체인식 데이터베이스는 매칭 등록 신드롬 벡터 및 등록 해시를 위치시키도록 탐색된다. 서치는 데이터베이스의 모든 엔트리를 체크할 수 있고, 또는 탐구적으로 오더링된 탐색이 이용되어 매치를 찾는 프로세스를 촉진할 수 있다. 이벤트 (328) 에서, 신드롬 디코딩이 등록 신드롬 벡터에 적용된다. 현재 알려져 있거나 미래에 알려지는 임의의 신드롬 디코더가 구현될 수도 있다. 몇몇 양태에서, 신뢰도 확산 (belief propagation) 또는 터보 코드 (turbo code) 를 이용하는 신드롬 디코더가 구현될 수도 있고, 이러한 디코더는 복잡성이 낮은 개선된 에러 복원력을 제안한다. 이벤트 (330) 에서, 디코딩된 등록 왜곡된 생체인식 데이터 (E) 와 인증 왜곡된 생체인식 데이터 (E') 사이의 직접 비교가 이루어질 수 있다. 등록 왜곡된 생체인식 데이터가 동일한지 또는 그렇지 않은지를 결정하는 종래의 비교 알고리즘을 사용하는 직접 비교가 이벤트 (332) 에서의 인증 왜곡된 생체인식 데이터와 유사한 임계값을 충족하는 경우, 액세스가 승인된다. 등록 왜곡된 생체인식 데이터가 동일하지 않은지 동일한지를 결정하는 직접 비교가 인증 왜곡된 생체인식 데이터와 유사한 임계값을 충족하지 않는 경우, 액세스 (334) 에서, 액세스는 거절된다.

[0078] 선택적으로, 이벤트 (336) 에서, 직접 비교가 구현되지 않거나 및/또는 실행가능한 경우, 해시 함수가 인증 왜곡된 생체인식 데이터에 적용되어 인증 해시를 생성한다. 그후, 이벤트 (338) 에서, 생체인식 데이터베이스에 저장된 등록 해시가 인증 해시와 비교되고, 그 값이 일치하거나 실질적으로 일치하는 것으로 판정되는 경우, 이벤트 (332) 에서, 액세스가 승인된다. 비교가, 해시 값이 이벤트 (334) 에서 일치하지 않는 것으로 판정되는 경우에는, 액세스가 거절된다. 인증 프로세스에서 해시 함수의 선택적인 이용은 생체인식 데이터의 하나의 측정/캡쳐로부터 생체인식 데이터의 후속 측정/캡쳐로 변동성의 추가적인 허용오차를 제공한다.

[0079] 도 7 은, 본 발명의 양태에 따라서, 생체인식 데이터, 왜곡된 생체인식 데이터, 완전하게 왜곡된 특징 벡터, 신드롬 피처 벡터와 인코딩된 신드롬 벡터 사이의 의존적인 관계를 나타내는 블록도이다. 임의의 신드롬 코드의 키 파라미터는 신드롬 벡터의 비트들의 수이다. 수많은 비트들을 갖는 신드롬 벡터는 생체인식 데이터에 대한 더욱 많은 정보를 운반하고 생체인식에서의 노이즈 및 변형을 허용하는 것을 더욱 쉽게 한다. 반대로, 작은 수의 비트를 갖는 신드롬 벡터는, 이들이 신드롬 벡터에 대한 소유권을 획득하는 경우, 공격자에 적은 정보를 제공한다.

[0080] 예를 들어, 신드롬 벡터의 길이가 기저 생체인식 데이터의 길이와 동일한 경우, 오리지널 생체인식 데이터가 신드롬 벡터로부터 정확하게 회복되기 때문에, 임의의 양의 노이즈/변형이 허용될 수 있다. 그러나, 동일한 길이의 신드롬 벡터를 획득하는 공격자는 생체인식 데이터를 용이하게 회복하여, 시스템의 보안을 타협할 수 있다. 다른 예시에서, 신드롬 벡터가 적은 수의 비트를 포함하는 경우, 공격자는 신드롬 벡터로부터 생체인식 데이터를 용이하게 회복시킬 수 없기 때문에, 우수한 보안이 제공된다. 그러나, 작은 비트 길이의 신드롬 벡터 예시에서, 등록 생체인식 데이터 및 인증 데이터 사이의 허용가능한 변형은 제한되어 있다.

[0081] 도 7 에 도시된 바와 같이, 블록 (350) 의 원시 생체인식 데이터는 홍채 스캔으로서 도시된다. 앞서 언급된 바와 같이, 생체인식 데이터는 컴퓨팅 디바이스의 사용자에 관련된 임의의 생체인식 데이터일 수도 있다. 블록 (352) 에서, 원시 생체인식 데이터는, 도 7 에 도시된 바와 같이, 그 각각이 전체 피처의 세그먼트를 포함하는 복수의 왜곡된 생체인식 데이터를 형성하도록 왜곡되고, 이 왜곡으로부터 왜곡된 전체 피처가 획득될 수도 있다.

[0082] 블록 (354) 에서, 왜곡된 전체 피처 벡터가 왜곡된 생체인식 데이터로부터 추출되고, 블록 (356) 에서, 왜곡된 전체 피처 벡터는 신드롬 피처 벡터로 축소된다. 신드롬 피처 벡터는, 보안 시스템 개발자가 신드롬 인코딩 및 신드롬 디코딩에 적절한지를 결정하는 전체 피처 벡터의 일부를 캡쳐한다. 블록 (358) 에서, 신드롬 코드는 신드롬 피처 벡터로부터의 신드롬 벡터를 인코딩하도록 이용된다.

[0083] 블록 (360) 에서, 인코딩된 신드롬 벡터는 에러 정정을 선택적으로 수행하여 그 데이터를 더 압축할 수도 있다. 신드롬 벡터가 에러 정정되면, 이들 신드롬 벡터는 암호해독을 위해 신드롬 인코딩된 생체인식 데이터에 의존하는 다른 컴퓨팅 디바이스에 저장되고 및/또는 송신된다.

[0084] 도 8 은 지문 생체인식 데이터 (370) 및 추출된 피처 벡터 (372) 의 예시를 나타낸다. 추출된 피처 벡터 (372) 는 신드롬 피처 벡터의 예시 (도 7 의 블록 (356)) 이다. 지문 생체인식 데이터 (370) 의 피처는 관찰 윈도우 (374) 에 의해 둘러싸인 영역과 같은 측정 필드에서만 측정된다. 특징점 (minutiae; 376) 은 특징점 (376) 의 공간 위치 좌표 (a, b) 및 각도 (c) 를 나타내는 삼중항 (triplet), 예를 들어, (a, b, c) 로 매핑된다. 하나의 특징점은 얼라인먼트의 목적으로, 중심 특징점 (380) 과 같은 "코어 (core") 특징점으로서 고안될 수 있다.

[0085] 지문 생체인식 데이터 (370) 가 측정되는 평면이 픽셀들의 어레이를 갖는 디지털 센서에 의해 양자화되기 때문에, 피처 벡터 (372) 는 매트릭스로서 저장된다. 각각의 센서 픽셀은 매트릭스에서의 특정 엔트리 (378) 에 해당한다. 특징점 엔트리 (378) 의 존재는 "1" 엔트리로 나타나고, 감지된 특징점의 부족은 매트릭스에서 "0" 엔트리로 나타낸다. 더욱 일반적인 표현으로, 특징점의 존재를 나타내는 "1" 엔트리는 특징점의 각도 (c) 를 나타내는 엔트리로 대체될 수도 있다.

[0086] 도 9 는, 본 양태에 따라서, 보안 생체인식 모델을 이용하는 아이덴티티-기반 암호체계에서 데이터 암호화를 위한 방법의 흐름도이다. 이벤트 (400) 에서, 원시 생체인식 데이터가 수신되고, 샘플링되고, 캡쳐되고, 측정되고, 또는 그렇지 않은 경우 컴퓨팅 디바이스의 사용자로부터 획득된다. 앞서 언급된 바와 같이, 생체인식 데이터는 특징적으로 샘플링될 수 있는 사용자에 관련된 임의의 생체인식 특징 또는 특성을 포함할 수도 있다. 생체인식 데이터의 예는, 지문 데이터, 음성 데이터, 안구 또는 홍채 특성 등과 같은 얼굴 특징 데이터를 포함하지만 이에 한정하지 않는다.

[0087] 이벤트 (410) 에서, 원시 생체인식 데이터가 왜곡되고, 조작되거나 그렇지 않으면 변경되어 소거가능한 생체인식 데이터를 지칭하는 복수의 왜곡된 생체인식 데이터를 결과로 획득한다. 왜곡 프로세스는 소프트웨어, 하드웨어, 펌웨어 또는 그 임의의 조합으로 구현될 수도 있다. 몇몇 양태에서, 생체인식 데이터의 왜곡은 생체인식 데이터의 랜덤 왜곡일 수도 있다. 랜덤 수 등과 같은 랜덤화기는 왜곡 프로세스를 랜덤화하도록 적용될 수도 있다. 추가적으로, 몇몇 양태에서, 생체인식 데이터의 왜곡은 왜곡 알고리즘의 사전-구성에 기초하여 시간 경과에 따라서 동적으로 변화할 수도 있다.

[0088] 이벤트 (420) 에서, 복수이 왜곡된 생체인식 데이터는 생체인식 데이터베이스에서 신드롬 벡터로서 저장된다. 사전에 언급된 바와 같이, 임의의 알려진 또는 미래의 알려질 신드롬 코드가 구현되어 신드롬 코드의 생성을 제공할 수도 있다. 선택적인 이벤트 (430) 에서, 에러 정정이 신드롬 벡터의 적어도 일부에 적용되어 생체인식 데이터를 더욱 안전하게 할 수도 있다. 에러 정정이 신드롬 벡터에 적용되는 이러한 양태에서, 에러 정정의 적용은 랜덤이다. 따라서, 랜덤 수 등과 같은 랜덤화기는 에러 정정 프로세스에 적용될 수도 있다. 랜덤화기가 생체인식 데이터 (이벤트 410) 및 에러 정정 프로세스 (이벤트 430) 의 왜곡 모두에 적용되는 이러한 양태에서, 동일한 랜덤화기, 예를 들어 동일한 랜덤 수를 구현하도록 랜덤화는 동기화될 수도 있다.

[0089] 이벤트 (440) 에서, 왜곡된 생체인식의 랜덤 샘플이 생체인식 데이터베이스로부터 획득된다. 따라서, 랜덤 수 등과 같은 랜덤화기는 왜곡된 생체인식 데이터의 샘플의 선택에 적용된다. 랜덤화기가 생체인식 데이터 (이벤트 410) 및 에러 정정 프로세스 (이벤트 430) 의 왜곡 중 하나 이상에 적용되는 이러한 양태에서, 동일한 랜덤화기, 예를 들어, 동일한 랜덤 수를 구현하도록 랜덤화기는 동기화될 수도 있다.

[0090] 이벤트 (450) 에서, 암호화 키는 왜곡된 생체인식 데이터의 랜덤 샘플과 개인 키의 조화에 기초하여 생성된다. 몇몇 양태에서, 일-방향 함수가 구현되어 암호화 키를 생성할 수도 있다. 일-방향 함수의 예는, Elgamel, Elliptic Curve Menezes-Qu-Vanstone (ECMQV), Elliptic Curve Diffie-Hellman (ECDH) 등을 포함하지만 이에 한정하지는 않는다. 이벤트 (460) 에서, 데이터는 생성된 암호화 키를 이용하여 암호화된다.

[0091] 도 10 은, 본 양태에 따라서, 보안 생체인식 모델을 이용하여 아이덴티티-기반 암호체계에서의 데이터 암호해독을 위한 방법의 흐름도이다. 이벤트 (500) 에서, 컴퓨팅 디바이스는 다른 컴퓨팅 디바이스로부터의 생체인식 데이터 및 개인 키를 수신한다. 몇몇 양태에서, 컴퓨팅 디바이스들은 모두 무선 컴퓨팅 디바이스일 수도 있고, 다른 양태에서는, 컴퓨팅 디바이스들 중 하나 이상의 디바이스는 PC 등과 같은 유선 컴퓨팅 디바이스일 수도 있다. 생체인식 데이터 및 관련 개인 키의 수신은 생체인식 데이터를 전송하는 디바이스와의 초기 통신에 기초할 수도 있다. 예를 들어, 이 경우에는, 생체인식 데이터 및 개인 키를 자동적으로 통신하는, 전화 번호, IP 주소 등으로의 첫 번째 호출에 기초하여 수신 디바이스와의 첫 번째 통신인 것으로 전송 디바이스가 인식하도록, 시스템이 구성될 수도 있다. 이와 다르게, 다른 디바이스로부터의 통신의 수신시에, 수신/암호해독 디바이스는 생체인식 어드레스 북에서 다른 디바이스에 대한 생체인식 데이터 엔트리의 존재/부재를 검증하도록, 시스템이 구성될 수도 있다. 다른 디바이스에 대한 엔트리가 생체인식 어드레스 북에서 검증되지 않는 경우, 수신 디바이스는 다른 디바이스가 생체인식 데이터 및 개인 키를 통신하도록 요청한다. 몇몇 양태에서, 생체인식 데이터는 신드롬 벡터의 형태로 왜곡된 생체인식 데이터일 수도 있고, 또한, 왜곡된 생체인식 데이터는 랜덤으로 왜곡된 생체인식 데이터일 수도 있다. 또한, 생체인식 데이터 및 개인 키는 일정 시간 내의 별개의 시점에서 통신된 별개의 통신으로 수신될 수 있다는 것에 유의해야만 한다.

[0092] 이벤트 (510) 에서, 생체인식 데이터 및 개인 키는 생체인식 어드레스 북에 등록된다. 생체인식 데이터 및 개인 키를 그 어드레스 북에 등록하는 것은 생체인식 데이터와 개인 키를 전달하였는 디바이스와의 관계를 요구한다. 이 관계는, 전화 번호, IP 번호 등과 같은 디바이스 식별자를 통해서 이루어질 수도 있다.

[0093] 이벤트 (520) 에서, 랜덤 수 등과 같은 암호화 데이터 및 랜덤화기가 수신된다. 암호화된 데이터 및 랜덤화기의 수신은 생체인식 데이터 및 개인 키의 수신과 동시에 발생할 수도 있고, 또는 암호화된 데이터 및 랜덤화기의 수신은 일정 시간의 후반 포인트에 있을 수도 있다. 이벤트 (530) 에서, 암호화된 데이터를 통신했던 디바이스에 관련된 생체인식 데이터의 랜덤 샘플이 획득된다. 이와 관련하여, 디바이스 식별자는 생체인식 어드레스 북으로부터 생체인식 데이터를 검색하는 것을 허용하고, 랜덤화기는 검색된 생체인식 데이터의 랜덤 샘플을 획득하도록 제공한다.

[0094] 이벤트 (540) 에서, 암호화 키는 생체인식 데이터의 랜덤 샘플 및 개인 키에 기초하여 생성된다. 수많은 양태에서, 암호해독 키가 데이터를 암호화하는데 구현하는 동일한 일-방향 함수를 이용하여 생성된다. 따라서, 일-방향 함수는 Elgamel, Elliptic Curve Menezes-Qu-Vanstone (ECMQV), Elliptic Curve Diffie-Hellman (ECDH) 등을 포함하지만 이에 한정하지는 않는다. 이벤트 (550) 에서, 데이터는 생성된 암호해독 키를 이용하여 암호해독된다.

[0095] 본 명세서에 개시된 실시형태와 관련하여 설명된 다양한 설명적인 로직, 로지컬 블록, 모듈, 및 회로는, 범용 프로세서, DSP (디지털 신호 프로세서), ASIC, 필드 프로그래머블 게이트 어레이 (FPGA), 또는 다른 프로그래머블 로직 디바이스, 이산 게이트 또는 트랜지스터 로직, 이산 하드웨어 컴포넌트, 또는 본 명세서에 설명된 기능들을 수행하도록 설계된 임의의 조합으로 구현 또는 수행될 수도 있다. 범용 프로세서는 마이크로프로세서일 수도 있지만, 대안적으로는, 프로세서는 임의의 종래의 프로세서, 컨트롤러, 마이크로컨트롤러, 또는 상태

머신일 수도 있다. 프로세서는, 또한, 컴퓨팅 디바이스의 조합, 예를 들어, DSP 와 마이크로프로세서의 조합, 복수의 마이크로프로세서, DSP 코어와 관련된 하나 이상의 마이크로프로세서, 또는 임의의 다른 이러한 구성일 수도 있다. 추가적으로, 적어도 하나의 프로세서는 하나 이상의 전술한 단계 및/또는 동작들을 수행하도록 동작가능한 하나 이상의 모듈을 포함할 수도 있다.

[0096] 또한, 본 명세서에 개시된 양태와 관련하여 설명된 방법 또는 알고리즘의 단계 및/또는 동작들이 하드웨어에서 직접, 프로세서에 의해 실행된 소프트웨어 모델에서, 또는 이 둘의 조합으로 채용될 수도 있다. 소프트웨어 모듈은 RAM 메모리, 플래시 메모리, ROM 메모리, EPROM 메모리, EEPROM 메모리, 레지스터, 하드 디스크, 탈착식 디스크, CD-ROM, 또는 당업계에 알려진 저장 매체의 임의의 다른 형태에 상주할 수도 있다. 예시적인 저장 매체는 프로세서에 커플링될 수도 있고, 이 프로세서는 저장 매체로부터 정보를 판독하고 저장 매체에 정보를 기록할 수 있다. 대안적으로, 저장 매체는 프로세서와 일체형일 수도 있다. 또한, 몇몇 양태에서, 프로세서 및 저장 매체는 ASIC 에 상주할 수도 있다. 추가적으로, ASIC 는 사용자 단말기에 상주할 수도 있다. 대안적으로, 프로세서 및 저장 매체는 사용자 단말기에서 이산 컴포넌트들로서 상주할 수도 있다. 추가적으로, 몇몇 양태에서, 방법 또는 알고리즘의 단계 및/또는 동작들은, 컴퓨터 프로그램 제품으로 통합될 수도 있는 머신 판독가능 매체 및/또는 컴퓨터 판독가능 매체상에서 하나의 또는 임의의 조합 또는 코드의 세트 및/또는 명령으로서 상주할 수도 있다.

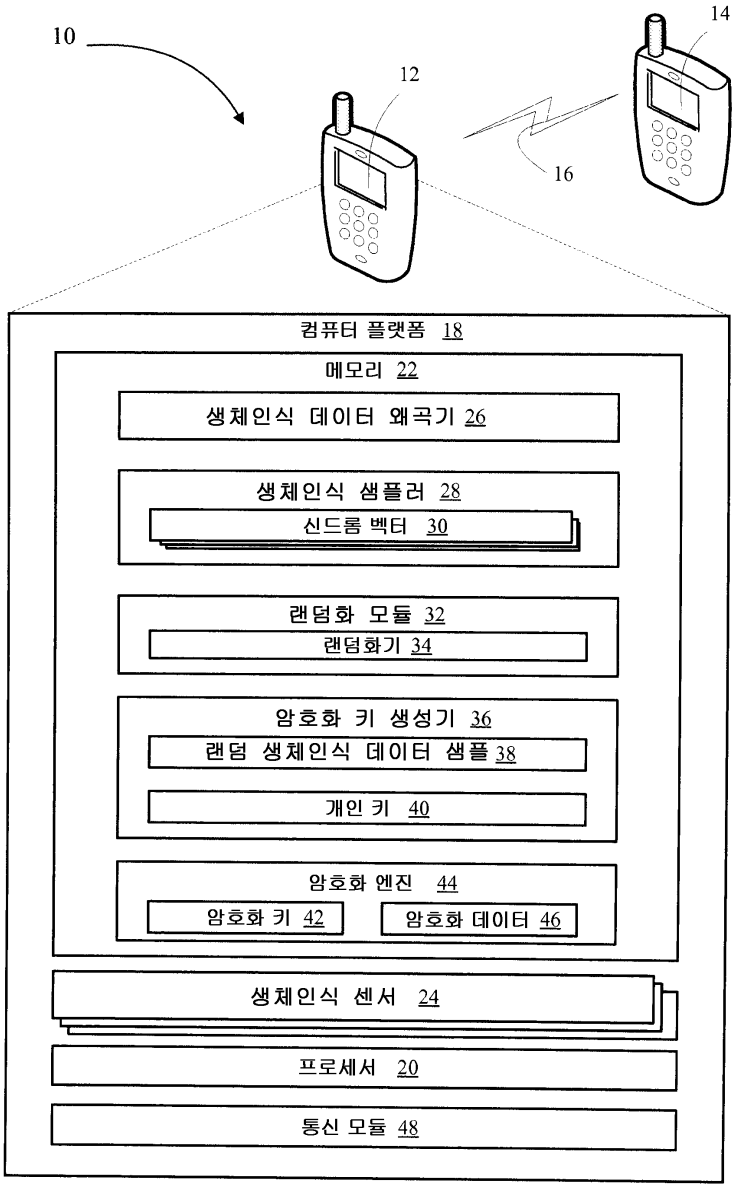
[0097] 하나 이상의 양태에서, 설명된 기능들은 하드웨어, 소프트웨어, 펌웨어, 또는 임의의 조합으로 구현될 수도 있다. 소프트웨어에서 구현되는 경우, 이 기능들은 컴퓨터-판독가능 매체상의 하나 이상의 명령 또는 코드로서 저장 또는 송신될 수도 있다. 컴퓨터-판독가능 매체는 하나의 장소에서 다른 장소로 컴퓨터 프로그램의 전송을 용이하게 하는 임의의 매체를 포함하는 컴퓨터 저장 매체 및 통신 매체 모두를 포함한다. 저장 매체는 컴퓨터에 의해 액세스될 수 있는 임의의 이용가능한 매체일 수도 있다. 한정이 아닌 예시의 방법으로, 이러한 컴퓨터-판독가능 매체는 RAM, ROM, EEPROM, CD-ROM 또는 다른 광학 디스크 저장매체, 자기 디스크 저장매체, 또는 다른 자기 저장 디바이스, 또는 명령 또는 데이터 구조의 형태로 원하는 프로그램 코드를 운반하고 또는 저장하도록 이용될 수 있고 컴퓨터에 의해 액세스될 수 있는 임의의 다른 저장 매체를 포함할 수 있다. 또한, 임의의 접속은 컴퓨터-판독가능 매체로 지칭될 수도 있다. 예를 들어, 소프트웨어가 웹사이트, 서버, 또는 동축 케이블, 광섬유 케이블, 트위스티드 페어, 디지털 가입자 회선 (DSL; digital subscriber line), 또는 무선 기술 (예를 들어, 적외선, 무선, 및 마이크로웨이브) 을 이용하는 다른 원격 소스로부터 송신되는 경우, 동축 케이블, 광섬유 케이블, 트위스티드 페어, DSL, 또는 적외선, 무선, 및 마이크로웨이브와 같은 무선 기술은 매체의 정의에 포함된다. 본 명세서에서 이용된 것과 같은 디스크 (disk) 및 디스크 (disc) 는 컴팩트 디스크 (CD), 레이저 디스크, 광학 디스크, DVD (digital versatile disc), 플로피 디스크 및 블루레이 디스크를 포함하고, 여기서, 디스크 (disk) 는 일반적으로 데이터를 자기적으로 복원하고, 디스크 (disc) 는 일반적으로 데이터를 레이저를 통해서 광학적으로 복원한다. 전술한 조합은 컴퓨터-판독가능 매체의 범위내에 포함되어야만 한다.

[0098] 이는, 본 명세서의 양태들은, 액세스 및 데이터 송신 모두가 안전하게 효과적으로 이루어지는 고도의 보안 생체인식 모델을 이용하여 아이덴티티-기반 암호체계를 제공하는 방법, 장치, 및 컴퓨터 프로그램 제품을 설명한다. 신드롬 벡터로서 생체인식 데이터를 생성하고 안전하게 저장하는 구현을 통해서, 생체인식 데이터의 고유의 변동성에 대한 허용오차가 제공된다. 또한, 생체인식 데이터가 신드롬 생성 알고리즘 및 생체인식 데이터에 대한 액세스를 획득할 수도 있는 공격자에 의해 복제되지 않는다는 것을 보증하기 위해, 본 양태는 더욱 안전한 개인 키를 유지하고 암호체계 사용자-기반 의존성을 이루는 것을 제공한다. 이러한 시스템, 장치 및 컴퓨터 프로그램에서와 같이, 개시된 설명은 대칭 및/또는 비대칭 아이덴티티-기반 암호체계를 구성하는 안전한 생물측정학을 이용하여 말단의 유저들의 엔드-투-엔드 인증을 제공한다.

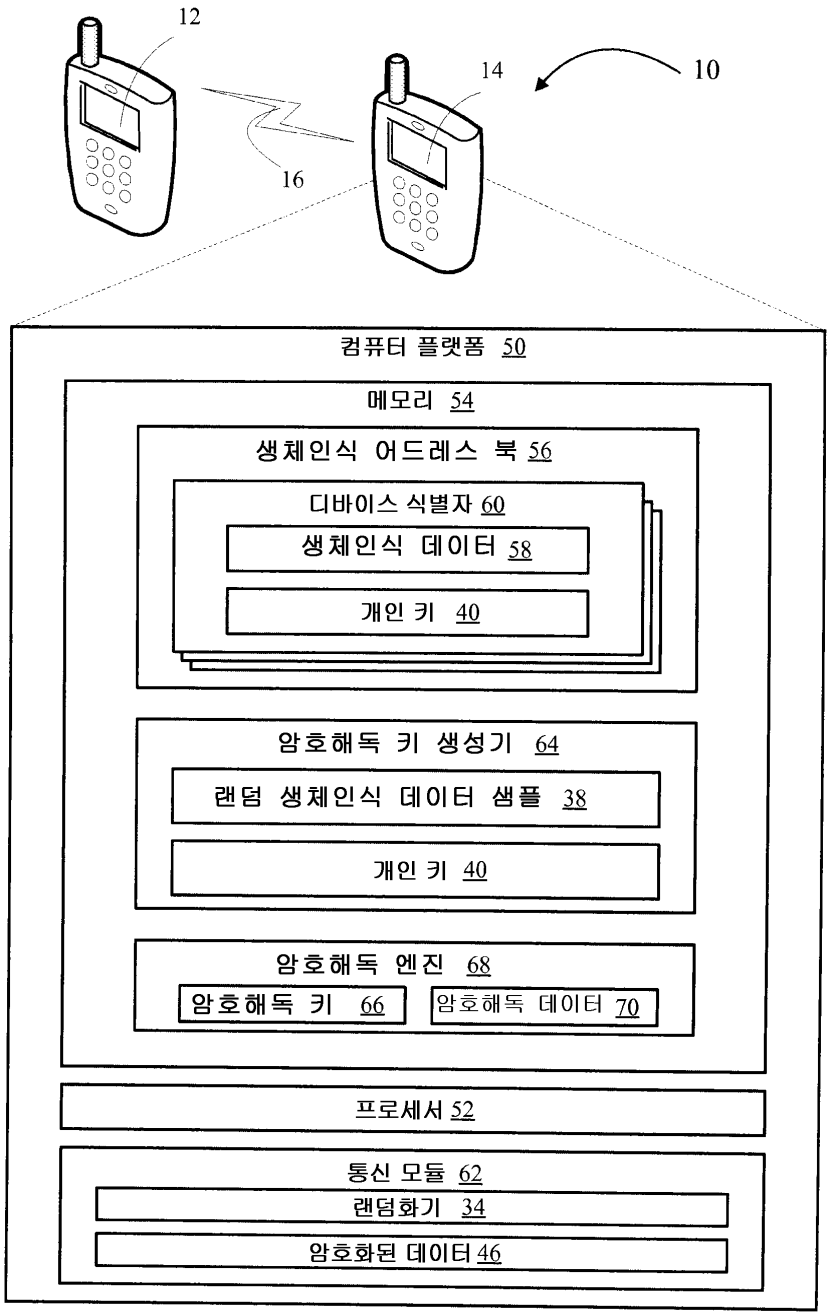
[0099] 전술한 개시물이 예시적인 양태 및/또는 실시형태를 논의하지만, 다양한 변경 및 변형이 첨부된 청구범위에 의해 정의되는 것과 같은 설명된 양태 및/또는 실시형태의 범위로부터 벗어나지 않고 이루어질 수 있다는 것에 유의해야만 한다. 또한, 설명된 양태 및/또는 실시형태의 엘리먼트가 단수로 설명되거나 청구될 수도 있지만, 단수로의 한정이 명백하게 나타나지 않는 한 복수가 고려된다. 추가적으로, 모든 또는 일부의 임의의 양태 및/또는 실시형태가, 이와 다르게 언급되지 않는 한, 임의의 다른 양태 및/또는 실시형태의 모든 또는 일부에 의해 사용될 수도 있다.

도면

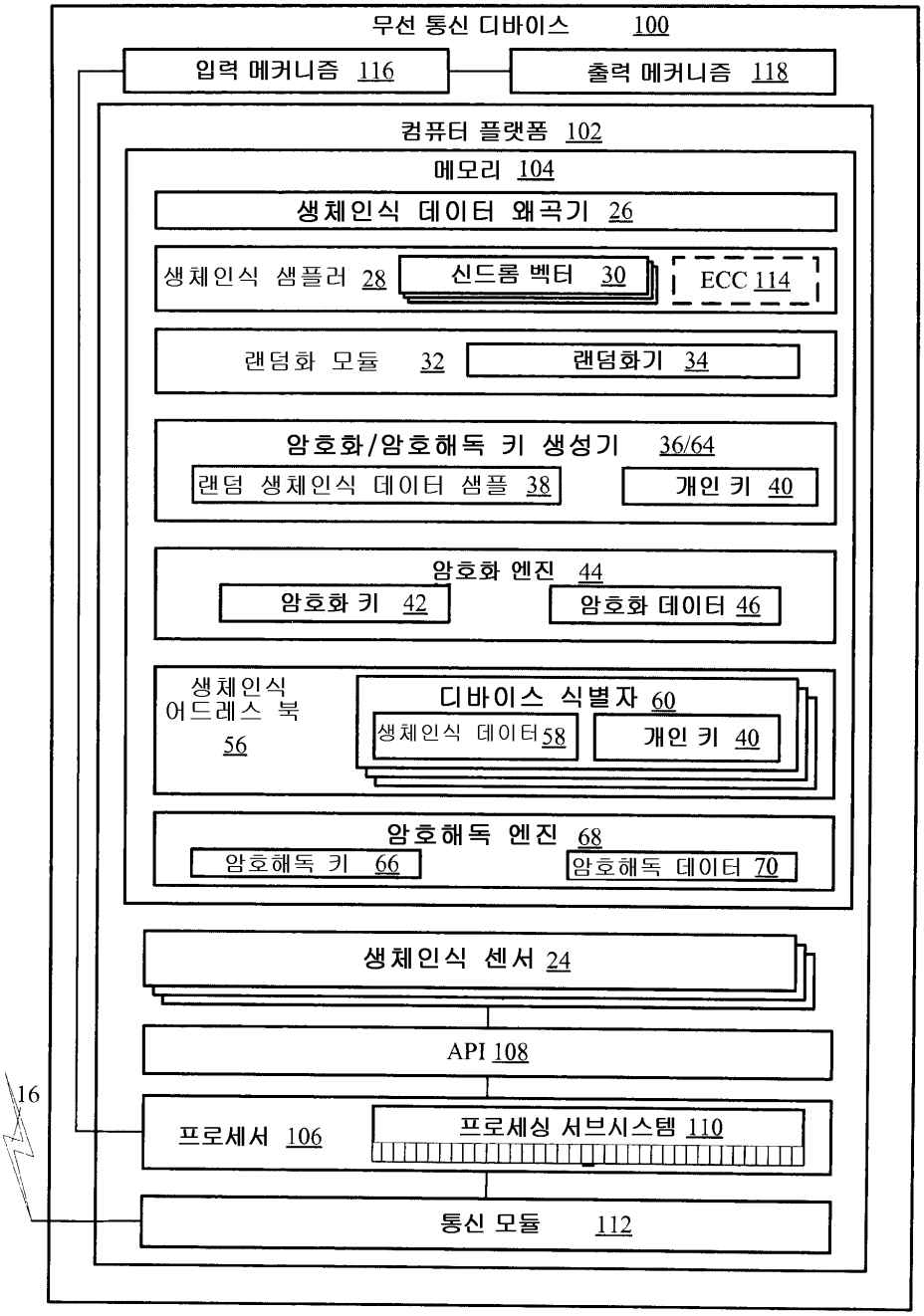
도면1


10
12
14
16
컴퓨터 플랫폼 18
메모리 22
생체인식 데이터 왜곡기 26
생체인식 샘플러 28
신드롬 벡터 30
랜덤화 모듈 32
랜덤화기 34
암호화 키 생성기 36
랜덤 생체인식 데이터 샘플 38
개인 키 40
암호화 엔진 44
암호화 키 42
암호화 데이터 46
생체인식 센서 24
프로세서 20
통신 모듈 48

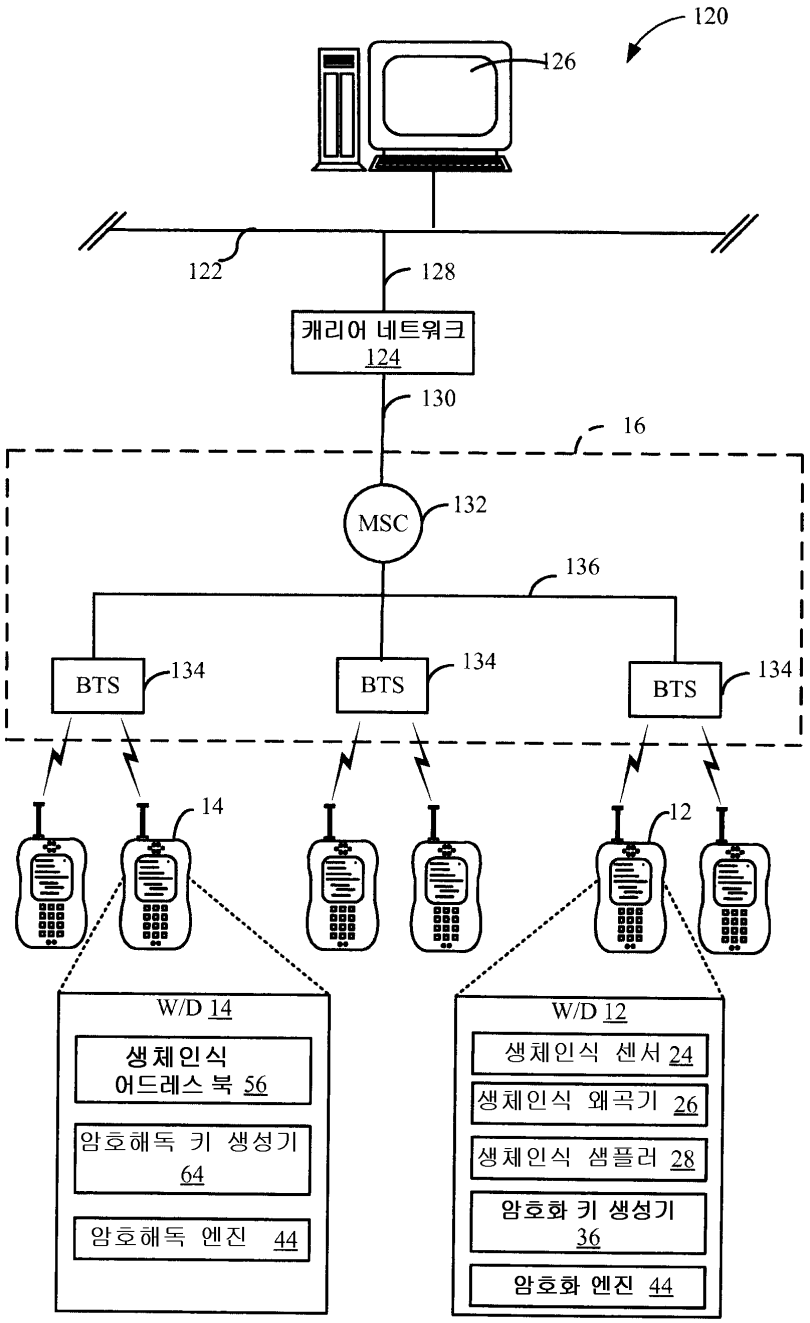
도면2


12
14
10
16
컴퓨터 플랫폼 50
메모리 54
생체인식 어드레스 북 56
디바이스 식별자 60
생체인식 데이터 58
개인 키 40
암호해독 키 생성기 64
랜덤 생체인식 데이터 샘플 38
개인 키 40
암호해독 엔진 68
암호해독 키 66
암호해독 데이터 70
프로세서 52
통신 모듈 62
랜덤화기 34
암호화된 데이터 46

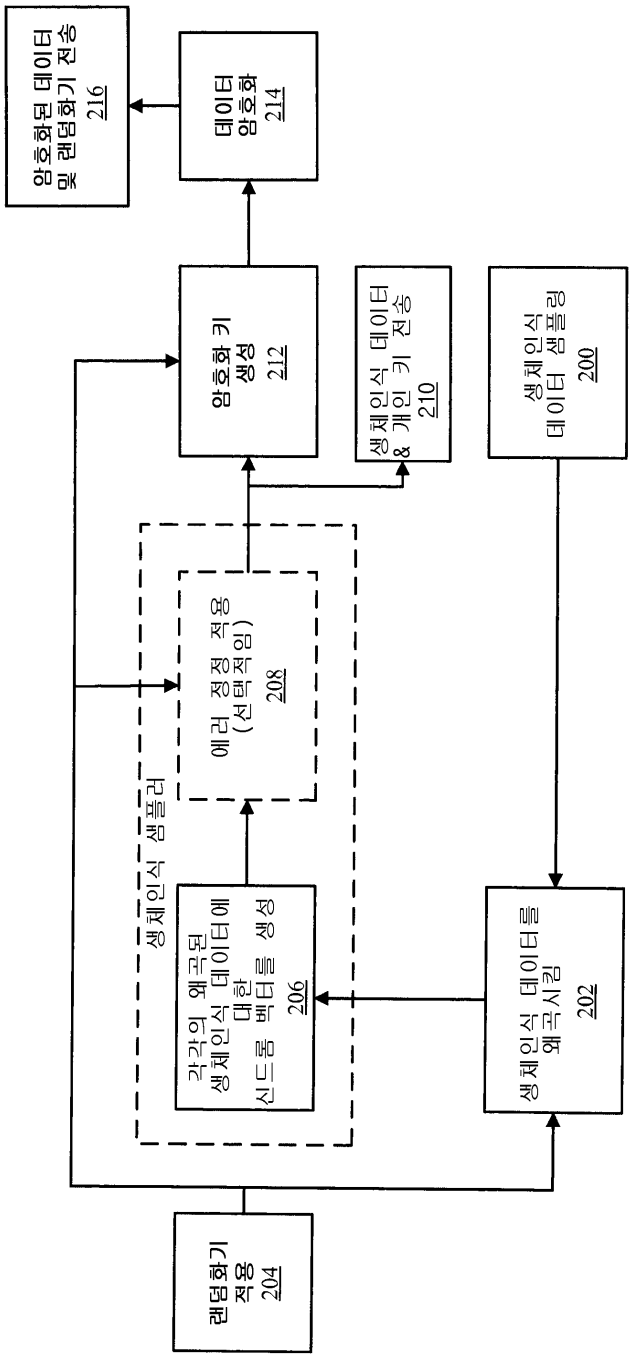
도면3


무선 통신 디바이스 100
입력 메커니즘 116
출력 메커니즘 118
컴퓨터 플랫폼 102
메모리 104
생체인식 데이터 왜곡기 26
생체인식 샘플러 28
신드롬 벡터 30
ECC 114
랜덤화 모듈 32
랜덤화기 34
암호화/암호해독 키 생성기 36/64
랜덤 생체인식 데이터 샘플 38
개인 키 40
암호화 엔진 44
암호화 키 42
암호화 데이터 46
생체인식 어드레스 북 56
디바이스 식별자 60
생체인식 데이터 58
개인 키 40
암호해독 엔진 68
암호해독 키 66
암호해독 데이터 70
생체인식 센서 24
API 108
16
프로세서 106
프로세싱 서브시스템 110
통신 모듈 112

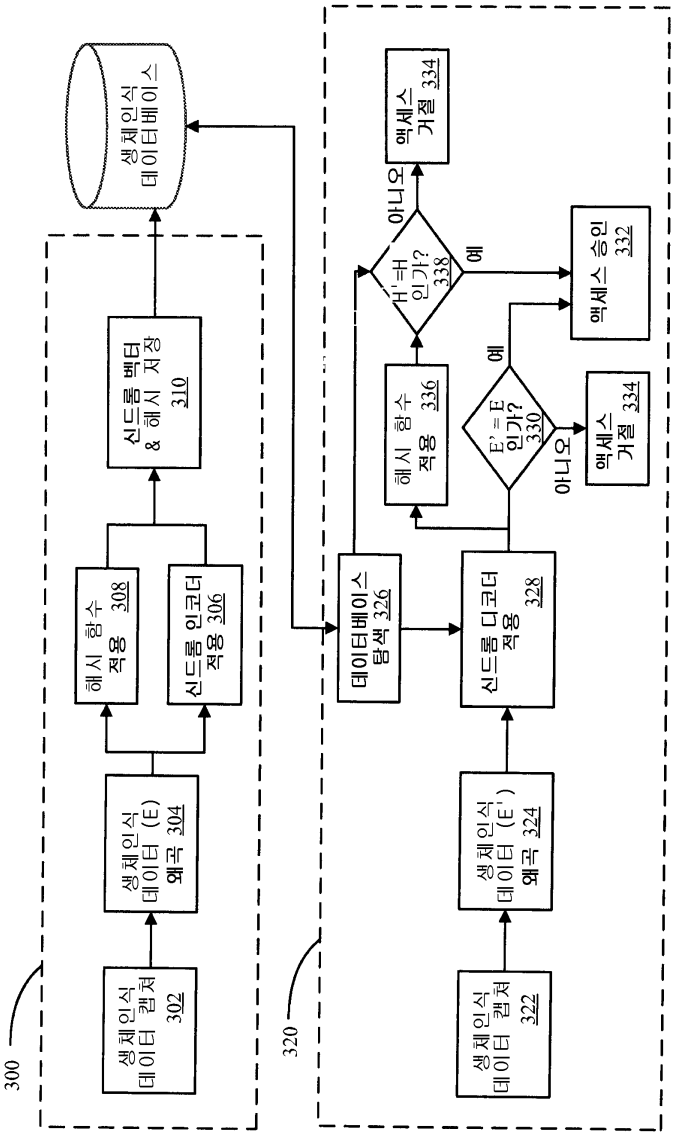
도면4


120
126
122
128
캐리어 네트워크
124
130
16
MSC
132
136
BTS
134
BTS
134
BTS
134
14
12
W/D 14
생체인식
어드레스 북 56
암호해독 키 생성기
64
암호해독 엔진 44
W/D 12
생체인식 센서 24
생체인식 왜곡기 26
생체인식 샘플러 28
암호화 키 생성기
36
암호화 엔진 44

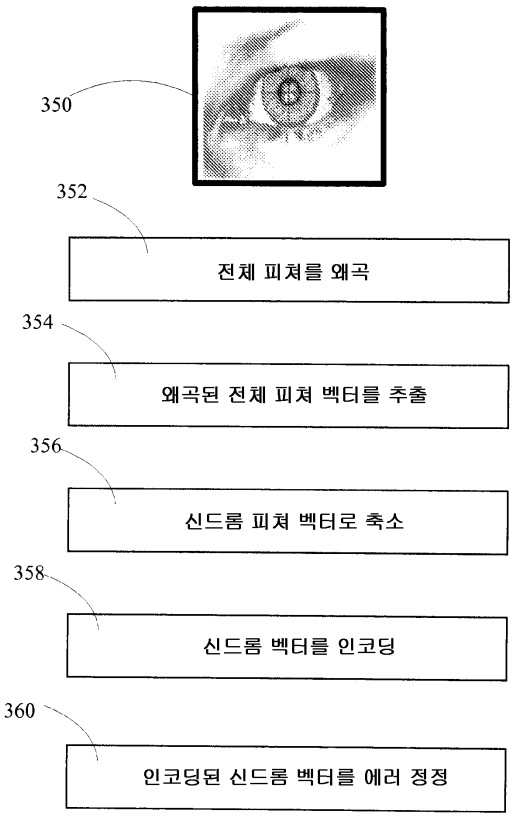
도면5


암호화된 데이터 및 랜덤화기 전송 216
데이터 암호화 214
암호화 키 생성 212
생체인식 데이터 & 개인 키 전송 210
생체인식 데이터 샘플링 200
에러 정정 적용 (선택적임) 208
생체인식 샘플러
각각의 왜곡된 생체인식 데이터에 대한 신드롬 벡터를 생성 206
생체인식 데이터를 왜곡시킴 202
랜덤화기 적용 204

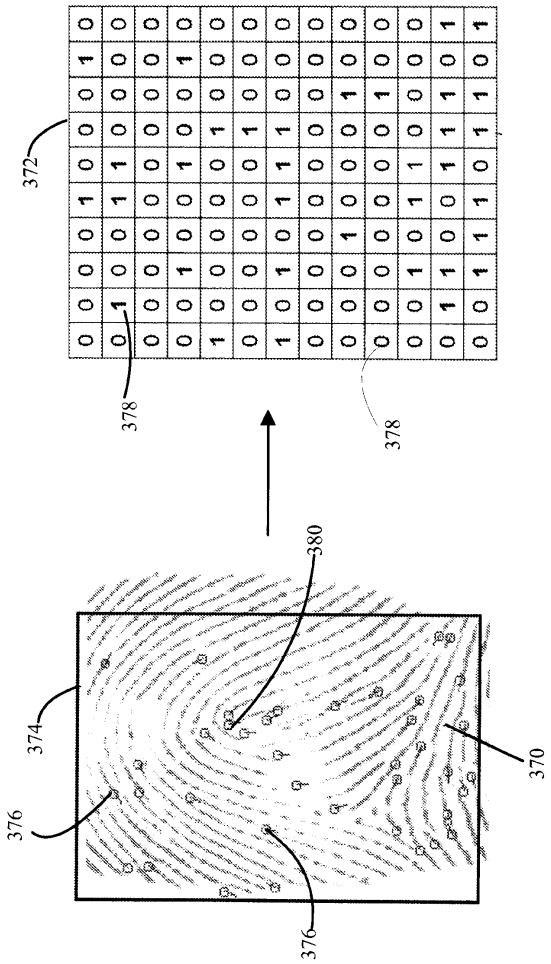
도면6


생체인식 데이터베이스
300
생체인식 데이터 캡처 302
생체인식 데이터 (E) 왜곡 304
해시 함수 적용 308
신드롬 인코더 적용 306
신드롬 벡터 & 해시 저장 310
320
생체인식 데이터 캡처 322
생체인식 데이터 (E') 왜곡 324
신드롬 디코더 적용 328
데이터베이스 탐색 326
해시 함수 적용 336
H'=H 인가? 338
아니오
예
액세스 거절 334
E'=E 인가? 330
예
아니오
액세스 승인 332
액세스 거절 334

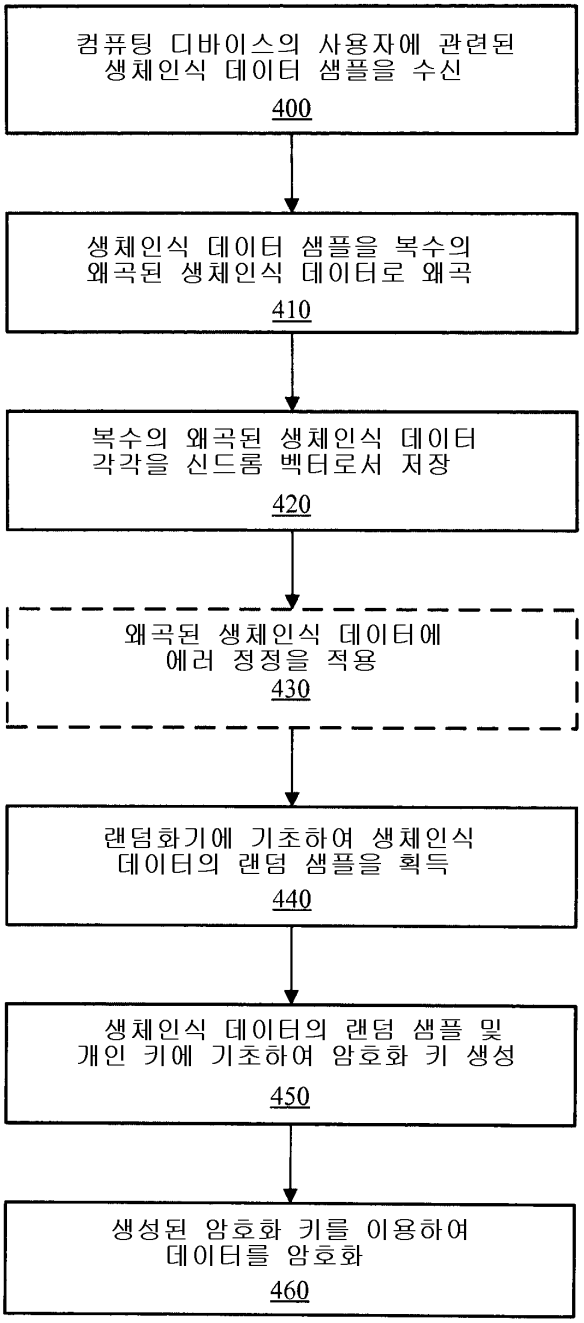
도면7


350
352
전체 피쳐를 왜곡
354
왜곡된 전체 피쳐 벡터를 추출
356
신드롬 피쳐 벡터로 축소
358
신드롬 벡터를 인코딩
360
인코딩된 신드롬 벡터를 에러 정정

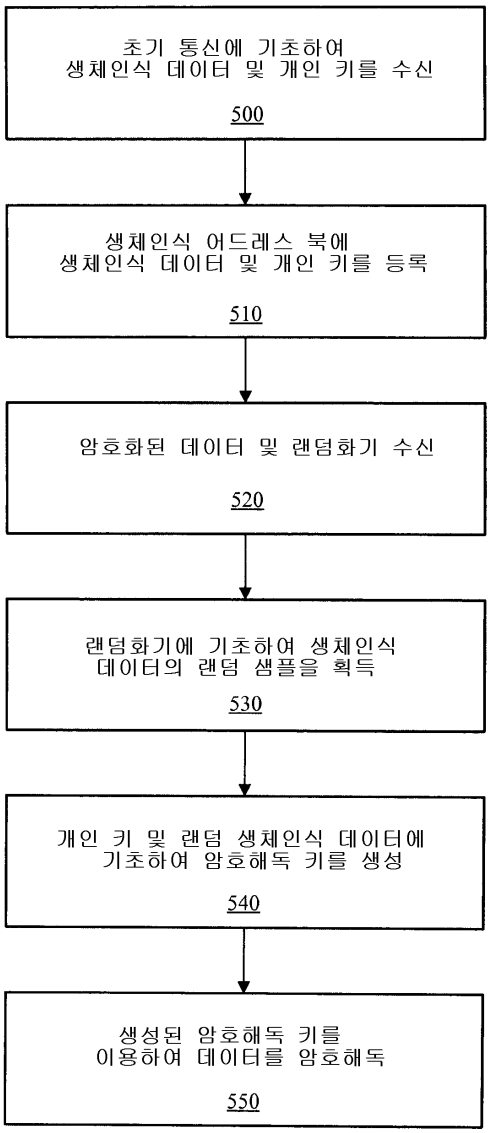
도면8



도면9


컴퓨팅 디바이스의 사용자에 관련된 생체인식 데이터 샘플을 수신
400
생체인식 데이터 샘플을 복수의 왜곡된 생체인식 데이터로 왜곡
410
복수의 왜곡된 생체인식 데이터 각각을 신드롬 벡터로서 저장
420
왜곡된 생체인식 데이터에 에러 정정을 적용
430
랜덤화기에 기초하여 생체인식 데이터의 랜덤 샘플을 획득
440
생체인식 데이터의 랜덤 샘플 및 개인 키에 기초하여 암호화 키 생성
450
생성된 암호화 키를 이용하여 데이터를 암호화
460

도면10


초기 통신에 기초하여
생체인식 데이터 및 개인 키를 수신
500
생체인식 어드레스 북에
생체인식 데이터 및 개인 키를 등록
510
암호화된 데이터 및 랜덤화기 수신
520
랜덤화기에 기초하여 생체인식
데이터의 랜덤 샘플을 획득
530
개인 키 및 랜덤 생체인식 데이터에
기초하여 암호해독 키를 생성
540
생성된 암호해독 키를
이용하여 데이터를 암호해독
550