(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년10월22일
(11) 등록번호 10-2035249
(24) 등록일자 2019년10월16일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) *H04L 9/32* (2006.01)
(52) CPC특허분류
H04L 9/0866 (2013.01)
H04L 9/3278 (2013.01)
(21) 출원번호 10-2017-0171006
(22) 출원일자 2017년12월13일
심사청구일자 2017년12월13일
(65) 공개번호 10-2019-0070472
(43) 공개일자 2019년06월21일
(56) 선행기술조사문헌
보안성이 향상된 퍼지추출 기술 기반 사용자 인증 및 키 동의 스킴(최윤성, 원동호, 2016년6월)*
(뒷면에 계속)
전체 청구항 수 : 총 22 항

(73) 특허권자
세종대학교산학협력단
서울특별시 광진구 능동로 209 (군자동, 세종대학교)
(72) 발명자
신지선
서울특별시 광진구 능동로 209
(74) 대리인
두호특허법인

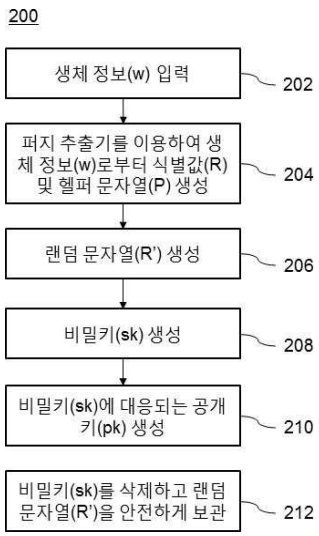
심사관 : 장상배

(54) 발명의 명칭 **생체 정보를 이용한 암호화 키 생성 장치 및 방법**

(57) 요 약

생체 정보를 이용한 암호화 키 생성 장치 및 방법이 제공된다. 일 실시예에 따른 암호화 키 생성 방법은 사용자의 생체 정보(w)를 입력받는 단계; 퍼지 추출기(Fuzzy Extractor)를 이용하여, 상기 생체 정보(w)에 대응되는 식별값(R) 및 헬퍼 문자열(P)을 생성하는 단계; 랜덤 문자열(R')을 생성하고, 상기 식별값(R) 및 상기 랜덤 문자열(R')로부터 비밀키(sk)를 생성하는 단계; 상기 비밀키(sk)에 대응되는 공개키(pk)를 생성하는 단계; 및 상기 랜덤 문자열(R')을 상기 비밀키(sk) 대신 저장하는 단계를 포함한다.

대 표 도 - 도2



(56) 선행기술조사문헌

Security Improvement on Biometric Based Authentication Scheme for Wireless Sensor Networks Using Fuzzy Extraction(Youngsung CHOI 외 2명, 2016년)*

KR1020110121874 A

WO2016105728 A1

WO2017075063 A1

*는 심사관에 의하여 인용된 문헌

이 발명을 지원한 국가연구개발사업

과제고유번호	1711058858
부처명	과학기술정보통신부
연구관리전문기관	정보통신기술진흥센터
연구사업명	정보보호핵심원천기술개발
연구과제명	(함수암호 3세부) 함수서명 설계기법 및 응용기술 연구
기 여 율	1/1
주관기관	고려대학교산학협력단
연구기간	2017.08.01 ~ 2018.05.31

명 세 서

청구범위

청구항 1

하나 이상의 프로세서들, 및

상기 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비한 컴퓨팅 장치에서 수행되는 방법으로서,

사용자의 생체 정보(w)를 입력받는 단계;

퍼지 추출기(Fuzzy Extractor)를 이용하여, 상기 생체 정보(w)에 대응되는 식별값(R) 및 헬퍼 문자열(P)을 생성하는 단계;

랜덤 문자열(R')을 생성하고, 상기 식별값(R) 및 상기 랜덤 문자열(R')로부터 비밀키(sk)를 생성하는 단계;

상기 비밀키(sk)에 대응되는 공개키(pk)를 생성하는 단계; 및

상기 랜덤 문자열(R')을 상기 비밀키(sk) 대신 저장하는 단계를 포함하는, 방법.

청구항 2

청구항 1에 있어서,

상기 식별값(R) 및 헬퍼 문자열(P)을 생성하는 단계는, 입력된 상기 생체 정보(w)를 삭제하는 단계를 더 포함하는, 방법.

청구항 3

청구항 1에 있어서,

상기 랜덤 문자열(R')의 길이는 상기 식별값보다 크거나 같도록 구성되는, 방법.

청구항 4

청구항 1에 있어서,

상기 비밀키는 상기 식별값(R) 및 상기 랜덤 문자열(R')을 XOR(eXclusive OR) 연산함으로써 생성되는, 방법.

청구항 5

청구항 1에 있어서,

상기 저장하는 단계의 수행 이후,

상기 사용자의 생체 정보(w')를 재입력받는 단계;

상기 재입력된 생체 정보(w') 및 상기 헬퍼 문자열(P)을 이용하여 상기 식별값(R)을 복원하는 단계; 및

상기 복원된 식별값(R) 및 기 저장된 랜덤 문자열(R')을 이용하여 상기 비밀키(sk)를 재생성하는 단계를 더 포함하는, 방법.

청구항 6

청구항 1에 있어서,

상기 랜덤 문자열(R')은 상기 컴퓨팅 장치에 구비된 물리적 복제 불가능 함수(Physical Unclonable Function, PUF)에 의하여 생성되는, 방법.

청구항 7

하나 이상의 프로세서들, 및

상기 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비한 컴퓨팅 장치에서 수행되는 방법으로서,

인증 서버로부터 사용자의 아이디에 대응되는 비밀키(sk_{id})를 수신하는 단계;

상기 사용자의 생체 정보(w)를 입력받는 단계;

퍼지 추출기(Fuzzy Extractor)를 이용하여, 상기 생체 정보(w)에 대응되는 식별값(R) 및 헬퍼 문자열(P)을 생성하는 단계;

상기 비밀키(sk_{id}) 및 상기 식별값(R)으로부터 저장값(R')을 계산하는 단계; 및

상기 저장값(R')을 상기 비밀키(sk_{id}) 대신 저장하는 단계를 포함하는, 방법.

청구항 8

청구항 7에 있어서,

상기 식별값(R) 및 헬퍼 문자열(P)을 생성하는 단계는, 입력된 상기 생체 정보(w)를 삭제하는 단계를 더 포함하는, 방법.

청구항 9

청구항 7에 있어서,

상기 저장값(R')은 상기 비밀키(sk_{id}) 및 상기 식별값(R)을 XOR(eXclusive OR) 연산함으로써 생성되는, 방법.

청구항 10

청구항 7에 있어서,

상기 저장하는 단계의 수행 이후,

상기 사용자의 생체 정보(w')를 재입력받는 단계;

상기 재입력된 생체 정보(w') 및 상기 헬퍼 문자열(P)을 이용하여 상기 식별값(R)을 복원하는 단계; 및

상기 복원된 식별값(R) 및 기 저장된 저장값(R')을 이용하여 상기 비밀키(sk_{id})를 재생성하는 단계를 더 포함하는, 방법.

청구항 11

청구항 10에 있어서,

상기 비밀키(sk_{id})는 상기 식별값(R) 및 상기 저장값(R')을 XOR(eXclusive OR) 연산함으로써 생성되는, 방법.

청구항 12

하나 이상의 프로세서들;

메모리; 및

하나 이상의 프로그램들을 포함하고,

상기 하나 이상의 프로그램들은 상기 메모리에 저장되고, 상기 하나 이상의 프로세서들에 의해 실행되도록 구성되며,

상기 하나 이상의 프로그램들은,

사용자의 생체 정보(w)를 입력받기 위한 명령;

퍼지 추출기(Fuzzy Extractor)를 이용하여, 상기 생체 정보(w)에 대응되는 식별값(R) 및 헬퍼 문자열(P)을 생성하기 위한 명령;

랜덤 문자열(R')을 생성하고, 상기 식별값(R) 및 상기 랜덤 문자열(R')로부터 비밀키(sk)를 생성하기 위한 명령;

상기 비밀키(sk)에 대응되는 공개키(pk)를 생성하기 위한 명령; 및

상기 랜덤 문자열(R')을 상기 비밀키(sk) 대신 저장하기 위한 명령을 포함하는, 컴퓨팅 장치.

청구항 13

청구항 12에 있어서,

상기 식별값(R) 및 헬퍼 문자열(P)을 생성하기 위한 명령은, 입력된 상기 생체 정보(w)를 삭제하기 위한 명령을 더 포함하는, 컴퓨팅 장치.

청구항 14

청구항 12에 있어서,

상기 랜덤 문자열(R')의 길이는 상기 식별값보다 크거나 같도록 구성되는, 컴퓨팅 장치.

청구항 15

청구항 12에 있어서,

상기 비밀키는 상기 식별값(R) 및 상기 랜덤 문자열(R')을 XOR(eXclusive OR) 연산함으로써 생성되는, 컴퓨팅 장치.

청구항 16

청구항 12에 있어서,

상기 저장하기 위한 명령의 수행 이후,

상기 사용자의 생체 정보(w')를 재입력 받기 위한 명령;

상기 재입력된 생체 정보(w') 및 상기 헬퍼 문자열(P)을 이용하여 상기 식별값(R)을 복원하기 위한 명령; 및

상기 복원된 식별값(R) 및 기 저장된 랜덤 문자열(R')을 이용하여 상기 비밀키(sk)를 재생성하기 위한 명령을 더 포함하는, 컴퓨팅 장치.

청구항 17

청구항 12에 있어서,

상기 랜덤 문자열(R')은 상기 컴퓨팅 장치에 구비된 물리적 복제 불가능 함수(Physical Unclonable Function, PUF)에 의하여 생성되는, 컴퓨팅 장치.

청구항 18

하나 이상의 프로세서들;

메모리; 및

하나 이상의 프로그램들을 포함하고,

상기 하나 이상의 프로그램들은 상기 메모리에 저장되고, 상기 하나 이상의 프로세서들에 의해 실행되도록 구성되며,

상기 하나 이상의 프로그램들은,

인증 서버로부터 사용자의 아이디에 대응되는 비밀키(sk_{id})를 수신하기 위한 명령;

상기 사용자의 생체 정보(w)를 입력받기 위한 명령;

퍼지 추출기(Fuzzy Extractor)를 이용하여, 상기 생체 정보(w)에 대응되는 식별값(R) 및 헬퍼 문자열(P)을 생성하기 위한 명령;

상기 비밀키(sk_{id}) 및 상기 식별값(R)으로부터 저장값(R')을 계산하기 위한 명령; 및

상기 저장값(R')을 상기 비밀키(sk_{id}) 대신 저장하기 위한 명령을 포함하는, 컴퓨팅 장치.

청구항 19

청구항 18에 있어서,

상기 식별값(R) 및 헬퍼 문자열(P)을 생성하기 위한 명령은, 입력된 상기 생체 정보(w)를 삭제하기 위한 명령을 더 포함하는, 컴퓨팅 장치.

청구항 20

청구항 18에 있어서,

상기 저장값(R')은 상기 비밀키(sk_{id}) 및 상기 식별값(R)을 XOR(eXclusive OR) 연산함으로써 생성되는, 컴퓨팅 장치.

청구항 21

청구항 18에 있어서,

상기 저장하기 위한 명령의 수행 이후,

상기 사용자의 생체 정보(w')를 재입력 받기 위한 명령;

상기 재입력된 생체 정보(w') 및 상기 헬퍼 문자열(P)을 이용하여 상기 식별값(R)을 복원하기 위한 명령; 및

상기 복원된 식별값(R) 및 기 저장된 저장값(R')을 이용하여 상기 비밀키(sk_{id})를 재생성하기 위한 명령을 더 포함하는, 컴퓨팅 장치.

청구항 22

청구항 21에 있어서,

상기 비밀키(sk_{id})는 상기 식별값(R) 및 상기 저장값(R')을 XOR(eXclusive OR) 연산함으로써 생성되는, 컴퓨팅 장치.

발명의 설명

기 술 분 야

[0001] 본 발명의 실시예들은 생체정보를 이용한 암호화 기술과 관련된다.

배 경 기 술

[0003] 최근 들어 지문, 홍채, 얼굴, 정맥 등 하나 이상의 신체적, 행동적 형질에 기반한 인증 방식, 이른바 생체 인식(Biometrics)이 다양한 분야에서 활발히 사용되고 있다. 이와 같은 생체 인식의 하나로 지문, 홍채 등의 생체 정보를 암호화 키로 사용하고자 하는 시도 또한 증가하고 있다.

[0004] 그러나 생체 정보의 경우 한 번 노출되면 복구가 불가능하다는 문제가 있다. 생체 정보는 비밀번호 등과 같이 사용자가 임의로 변경할 수 없기 때문이다. 이에 따라 생체 정보를 암호화 키로 사용하는 암호화 알고리즘에 있어 키의 안정성을 강화하기 위한 기술적인 수단이 필요하게 되었다.

선행기술문헌

특허문헌

[0006] (특허문헌 0001) 대한민국 등록특허공보 제10-1745706호 (2017.06.02.)

발명의 내용

해결하려는 과제

[0007] 본 발명의 실시예들은 생체 정보를 비밀키로 하는 공개키 기반 암호화 시스템에서 비밀키의 안정성을 높이기 위한 기술적 수단을 제공하기 위한 것이다.

과제의 해결 수단

[0009] 예시적인 실시예에 따르면, 하나 이상의 프로세서들, 및 상기 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비한 컴퓨팅 장치에서 수행되는 방법으로서, 사용자의 생체 정보(w)를 입력받는 단계; 퍼지 추출기(Fuzzy Extractor)를 이용하여, 상기 생체 정보(w)에 대응되는 식별값(R) 및 헬퍼 문자열(P)을 생성하는 단계; 랜덤 문자열(R')을 생성하고, 상기 식별값(R) 및 상기 랜덤 문자열(R')로부터 비밀키(sk)를 생성하는 단계; 상기 비밀키(sk)에 대응되는 공개키(pk)를 생성하는 단계; 및 상기 랜덤 문자열(R')을 상기 비밀키(sk) 대신 저장하는 단계를 포함하는, 방법이 제공된다.

[0010] 상기 식별값(R) 및 헬퍼 문자열(P)을 생성하는 단계는, 입력된 상기 생체(w) 정보를 삭제하는 단계를 더 포함할 수 있다.

[0011] 상기 랜덤 문자열(R')의 길이는 상기 식별값보다 크거나 같도록 구성될 수 있다.

[0012] 상기 비밀키는 상기 식별값(R) 및 상기 랜덤 문자열(R')을 XOR(eXclusive OR) 연산함으로써 생성될 수 있다.

[0013] 상기 방법은, 상기 저장하는 단계의 수행 이후, 상기 사용자의 생체 정보(w')를 재입력받는 단계; 상기 재입력된 생체 정보(w') 및 상기 헬퍼 문자열(P)을 이용하여 상기 식별값(R)을 복원하는 단계; 및 상기 복원된 식별값(R) 및 기 저장된 랜덤 문자열(R')을 이용하여 상기 비밀키(sk)를 재생성하는 단계를 더 포함할 수 있다.

[0014] 상기 랜덤 문자열(R')은 상기 컴퓨팅 장치에 구비된 물리적 복제 불가능 함수(Physical Unclonable Function, PUF)에 의하여 생성될 수 있다.

[0015] 다른 예시적인 실시예에 따르면, 하나 이상의 프로세서들, 및 상기 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비한 컴퓨팅 장치에서 수행되는 방법으로서, 인증 서버로부터 사용자의 아이디에 대응되는 비밀키(sk_{id})를 수신하는 단계; 상기 사용자의 생체 정보(w)를 입력받는 단계; 퍼지 추출기(Fuzzy Extractor)를 이용하여, 상기 생체 정보(w)에 대응되는 식별값(R) 및 헬퍼 문자열(P)을 생성하는 단계; 상기 비밀키(sk_{id}) 및 상기 식별값(R)으로부터 저장값(R')을 계산하는 단계; 및 상기 저장값(R')을 상기 비밀키(sk_{id}) 대신 저장하는 단계를 포함하는, 방법이 제공된다.

[0016] 상기 식별값(R) 및 헬퍼 문자열(P)을 생성하는 단계는, 입력된 상기 생체(w) 정보를 삭제하는 단계를 더 포함할 수 있다.

[0017] 상기 저장값(R')은 상기 비밀키(sk_{id}) 및 상기 식별값(R)을 XOR(eXclusive OR) 연산함으로써 생성될 수 있다.

[0018] 상기 방법은, 상기 저장하는 단계의 수행 이후, 상기 사용자의 생체 정보(w')를 재입력받는 단계; 상기 재입력된 생체 정보(w') 및 상기 헬퍼 문자열(P)을 이용하여 상기 식별값(R)을 복원하는 단계; 및 상기 복원된 식별값(R) 및 기 저장된 저장값(R')을 이용하여 상기 비밀키(sk_{id})를 재생성하는 단계를 더 포함할 수 있다.

[0019] 상기 비밀키(sk_{id})는 상기 식별값(R) 및 상기 저장값(R')을 XOR(eXclusive OR) 연산함으로써 생성될 수 있다.

[0020] 다른 예시적인 실시예에 따르면, 하나 이상의 프로세서들; 메모리; 및 하나 이상의 프로그램들을 포함하고, 상기 하나 이상의 프로그램들은 상기 메모리에 저장되고, 상기 하나 이상의 프로세서들에 의해 실행되도록 구성되며, 상기 하나 이상의 프로그램들은, 사용자의 생체 정보(w)를 입력받기 위한 명령; 퍼지 추출기(Fuzzy Extractor)를 이용하여, 상기 생체 정보(w)에 대응되는 식별값(R) 및 헬퍼 문자열(P)을 생성하기 위한 명령; 랜덤 문자열(R')을 생성하고, 상기 식별값(R) 및 상기 랜덤 문자열(R')로부터 비밀키(sk)를 생성하기 위한 명령; 상기 비밀키(sk)에 대응되는 공개키(pk)를 생성하기 위한 명령; 및 상기 랜덤 문자열(R')을 상기 비밀키(sk) 대신 저장하기 위한 명령을 포함하는, 컴퓨팅 장치가 제공된다.

[0021] 상기 식별값(R) 및 헬퍼 문자열(P)을 생성하기 위한 명령은, 입력된 상기 생체(w) 정보를 삭제하기 위한 명령을 더 포함할 수 있다.

[0022] 상기 랜덤 문자열(R')의 길이는 상기 식별값보다 크거나 같도록 구성될 수 있다.

[0023] 상기 비밀키는 상기 식별값(R) 및 상기 랜덤 문자열(R')을 XOR(eXclusive OR) 연산함으로써 생성될 수 있다.

[0024] 상기 프로그램들은, 상기 저장하기 위한 명령의 수행 이후, 상기 사용자의 생체 정보(w')를 재입력 받기 위한 명령; 상기 재입력된 생체 정보(w') 및 상기 헬퍼 문자열(P)을 이용하여 상기 식별값(R)을 복원하기 위한 명령; 및 상기 복원된 식별값(R) 및 기 저장된 랜덤 문자열(R')을 이용하여 상기 비밀키(sk)를 재생성하기 위한 명령을 더 포함할 수 있다.

[0025] 상기 랜덤 문자열(R')은 상기 컴퓨팅 장치에 구비된 물리적 복제 불가능 함수(Physical Unclonable Function, PUF)에 의하여 생성될 수 있다.

[0026] 다른 예시적인 실시예에 따르면, 하나 이상의 프로세서들; 메모리; 및 하나 이상의 프로그램들을 포함하고, 상기 하나 이상의 프로그램들은 상기 메모리에 저장되고, 상기 하나 이상의 프로세서들에 의해 실행되도록 구성되며, 상기 하나 이상의 프로그램들은, 인증 서버로부터 사용자의 아이디에 대응되는 비밀키(sk_{id})를 수신하기 위한 명령; 상기 사용자의 생체 정보(w)를 입력받기 위한 명령; 퍼지 추출기(Fuzzy Extractor)를 이용하여, 상기 생체 정보(w)에 대응되는 식별값(R) 및 헬퍼 문자열(P)을 생성하기 위한 명령; 상기 비밀키(sk_{id}) 및 상기 식별값(R)으로부터 저장값(R')을 계산하기 위한 명령; 및 상기 저장값(R')을 상기 비밀키(sk_{id}) 대신 저장하기 위한 명령을 포함하는, 컴퓨팅 장치가 제공된다.

[0027] 상기 식별값(R) 및 헬퍼 문자열(P)을 생성하기 위한 명령은, 입력된 상기 생체(w) 정보를 삭제하기 위한 명령을 더 포함할 수 있다.

[0028] 상기 저장값(R')은 상기 비밀키(sk_{id}) 및 상기 식별값(R)을 XOR(eXclusive OR) 연산함으로써 생성될 수 있다.

[0029] 상기 컴퓨팅 장치는, 상기 저장하기 위한 명령의 수행 이후, 상기 사용자의 생체 정보(w')를 재입력 받기 위한 명령; 상기 재입력된 생체 정보(w') 및 상기 헬퍼 문자열(P)을 이용하여 상기 식별값(R)을 복원하기 위한 명령; 및 상기 복원된 식별값(R) 및 기 저장된 저장값(R')을 이용하여 상기 비밀키(sk_{id})를 재생성하기 위한 명령을 더 포함할 수 있다.

[0030] 상기 비밀키(sk_{id})는 상기 식별값(R) 및 상기 저장값(R')을 XOR(eXclusive OR) 연산함으로써 생성될 수 있다.

[0031]

발명의 효과

[0032] 본 발명의 실시예들에 따르면, 생체 정보를 비밀키로 하는 공개키 기반 암호화 시스템에서 생체 정보가 노출되더라도 비밀키의 안정성을 지킬 수 있게 되는 바, 암호화 시스템의 보안성을 높일 수 있다.

도면의 간단한 설명

[0034] 도 1은 예시적인 실시예들에서 사용되기에 적합한 컴퓨팅 장치를 포함하는 컴퓨팅 환경을 예시하여 설명하기 위한 블록도

도 2는 본 발명의 제1 실시예에 따른 암호화 키 생성 방법을 설명하기 위한 흐름도

도 3은 본 본 발명의 제1 실시예에 따른 암호화 키 복구 방법을 설명하기 위한 흐름도

도 4는 본 발명의 제2 실시예에 따른 암호화 키 생성 시스템을 설명하기 위한 블록도

도 5는 본 발명의 제2 실시예에 따른 암호화 키 생성 방법을 설명하기 위한 흐름도

도 6은 본 본 발명의 제2 실시예에 따른 암호화 키 복구 방법을 설명하기 위한 흐름도

발명을 실시하기 위한 구체적인 내용

[0035] 이하, 도면을 참조하여 본 발명의 구체적인 실시형태를 설명하기로 한다. 이하의 상세한 설명은 본 명세서에서 기술된 방법, 장치 및/또는 시스템에 대한 포괄적인 이해를 돕기 위해 제공된다. 그러나 이는 예시에 불과하며 본 발명은 이에 제한되지 않는다.

[0036] 본 발명의 실시예들을 설명함에 있어서, 본 발명과 관련된 공지기술에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략하기로 한다. 그리고, 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다. 상세한 설명에서 사용되는 용어는 단지 본 발명의 실시예들을 기술하기 위한 것이며, 결코 제한적이어서는 안 된다. 명확하게 달리 사용되지 않는 한, 단수 형태의 표현은 복수 형태의 의미를 포함한다. 본 설명에서, "포함" 또는 "구비"와 같은 표현은 어떤 특성들, 숫자들, 단계들, 동작들, 요소들, 이들의 일부 또는 조합을 가리키기 위한 것이며, 기술된 것 이외에 하나 또는 그 이상의 다른 특성, 숫자, 단계, 동작, 요소, 이들의 일부 또는 조합의 존재 또는 가능성을 배제하도록 해석되어서는 안 된다.

[0038] 도 1은 예시적인 실시예들에서 사용되기에 적합한 컴퓨팅 장치를 포함하는 컴퓨팅 환경(10)을 예시하여 설명하기 위한 블록도이다. 도시된 실시예에서, 각 컴포넌트들은 이하에 기술된 것 이외에 상이한 기능 및 능력을 가질 수 있고, 이하에 기술되지 것 이외에도 추가적인 컴포넌트를 포함할 수 있다.

[0039] 도시된 컴퓨팅 환경(10)은 컴퓨팅 장치(12)를 포함한다. 일 실시예에서, 컴퓨팅 장치(12)는 본 발명의 실시예들에 따른 생체 정보를 이용한 암호화 키 생성 장치일 수 있다. 일 실시예에서, 컴퓨팅 장치(12)는 데스크탑, 노트북 컴퓨터, 태블릿, 스마트폰, 웨어러블 디바이스 등의 개인 컴퓨팅 디바이스를 포함할 수 있다.

[0040] 컴퓨팅 장치(12)는 적어도 하나의 프로세서(14), 컴퓨터 판독 가능 저장 매체(16) 및 통신 버스(18)를 포함한다. 프로세서(14)는 컴퓨팅 장치(12)로 하여금 앞서 언급된 예시적인 실시예에 따라 동작하도록 할 수 있

다. 예컨대, 프로세서(14)는 컴퓨터 판독 가능 저장 매체(16)에 저장된 하나 이상의 프로그램들을 실행할 수 있다. 상기 하나 이상의 프로그램들은 하나 이상의 컴퓨터 실행 가능 명령어를 포함할 수 있으며, 상기 컴퓨터 실행 가능 명령어는 프로세서(14)에 의해 실행되는 경우 컴퓨팅 장치(12)로 하여금 예시적인 실시예에 따른 동작들을 수행하도록 구성될 수 있다.

[0041] 컴퓨터 판독 가능 저장 매체(16)는 컴퓨터 실행 가능 명령어 내지 프로그램 코드, 프로그램 데이터 및/또는 다른 적합한 형태의 정보를 저장하도록 구성된다. 컴퓨터 판독 가능 저장 매체(16)에 저장된 프로그램(20)은 프로세서(14)에 의해 실행 가능한 명령어의 집합을 포함한다. 일 실시예에서, 컴퓨터 판독 가능 저장 매체(16)는 메모리(랜덤 액세스 메모리와 같은 휘발성 메모리, 비휘발성 메모리, 또는 이들의 적절한 조합), 하나 이상의 자기 디스크 저장 디바이스들, 광학 디스크 저장 디바이스들, 플래시 메모리 디바이스들, 그 밖에 컴퓨팅 장치(12)에 의해 액세스되고 원하는 정보를 저장할 수 있는 다른 형태의 저장 매체, 또는 이들의 적합한 조합일 수 있다.

[0042] 통신 버스(18)는 프로세서(14), 컴퓨터 판독 가능 저장 매체(16)를 포함하여 컴퓨팅 장치(12)의 다른 다양한 컴포넌트들을 상호 연결한다.

[0043] 컴퓨팅 장치(12)는 또한 하나 이상의 입출력 장치(24)를 위한 인터페이스를 제공하는 하나 이상의 입출력 인터페이스(22) 및 하나 이상의 네트워크 통신 인터페이스(26)를 포함할 수 있다. 입출력 인터페이스(22) 및 네트워크 통신 인터페이스(26)는 통신 버스(18)에 연결된다. 입출력 장치(24)는 입출력 인터페이스(22)를 통해 컴퓨팅 장치(12)의 다른 컴포넌트들에 연결될 수 있다. 예시적인 입출력 장치(24)는 포인팅 장치(마우스 또는 트랙패드 등), 키보드, 터치 입력 장치(터치패드 또는 터치스크린 등), 음성 또는 소리 입력 장치, 다양한 종류의 센서 장치 및/또는 촬영 장치와 같은 입력 장치, 및/또는 디스플레이 장치, 프린터, 스피커 및/또는 네트워크 카드와 같은 출력 장치를 포함할 수 있다. 예시적인 입출력 장치(24)는 컴퓨팅 장치(12)를 구성하는 일 컴포넌트로서 컴퓨팅 장치(12)의 내부에 포함될 수도 있고, 컴퓨팅 장치(12)와는 구별되는 별개의 장치로 컴퓨팅 장치(102)와 연결될 수도 있다.

[0045] 도 2는 본 발명의 제1 실시예에 따른 암호화 키 생성 방법(200)을 설명하기 위한 흐름도이다. 도 2에 도시된 방법은 예를 들어, 전술한 컴퓨팅 장치(12)에 의해 수행될 수 있다. 도시된 흐름도에서는 상기 방법을 복수 개의 단계로 나누어 기재하였으나, 적어도 일부의 단계들은 순서를 바꾸어 수행되거나, 다른 단계와 결합되어 함께 수행되거나, 생략되거나, 세부 단계들로 나뉘어 수행되거나, 또는 도시되지 않은 하나 이상의 단계가 부가되어 수행될 수 있다.

[0046] 본 실시예를 구체적으로 설명하기 전, 컴퓨팅 장치(12)는 공개키 기반 전자서명(Digital Signature)을 위한 서명 스킴을 구비하고 있는 것으로 가정한다. 상기 서명 스킴은 키 생성(DKeyGen), 서명(DSign) 및 검증(DVerify) 알고리즘을 구성될 수 있다. 각각의 알고리즘에 대한 상세한 설명을 기재하면 다음과 같다.

[0047] $DKeyGen(1^k)$: 보안 파라미터 k($k \in N$)를 입력으로 받아서 공개키와 비밀키 쌍(pk, sk)를 출력한다.

[0048] DSign(m, sk): 메시지(m)와 비밀키(sk)를 입력으로 받아 서명(σ)을 출력한다.

[0049] DVerify(σ, m, pk): 서명(σ)과 메시지(m)와 공개키(pk)를 입력으로 받아 맞는 서명이면 1을 출력하고 아니면 0을 출력한다.

[0050] 또한, 컴퓨팅 장치(12)는 퍼지 추출기(Fuzzy Extractor)를 포함하는 것으로 가정한다. 퍼지 추출기는 생체 정보를 입력받고, 입력된 생체 정보의 노이즈(noise)를 제거하여 유니크한 값을 생성한다. 생체 정보는 그 특성상 입력 시 그 값이 조금씩 달라질 수 있으나, 이와 같은 퍼지 추출기를 이용할 경우 입력되는 생체 정보로부터 일정한 값을 얻어낼 수 있다. 퍼지 추출기는 다음과 같은 알고리즘을 포함한다.

[0051] Gen(w): 퍼지 데이터(w)를 받아 l 비트 길이의 문자열(R) 및 헬퍼 문자열(P)을 출력한다. 이때 상기 퍼지 데이터(w)는 생체 정보일 수 있다.

[0052] Rep(w', P): 퍼지 데이터(w')와 헬퍼 문자열(P)을 입력으로 받아 R을 출력한다. 기존의 퍼지 데이터(w)를 Gen 알고리즘에 적용하여 생성된 R, P에 대해서 w와 w' 간의 거리가 임계값(t) 이하인 경우(dist(w, w') <= t), Rep(w', P) = R의 관계를 가지게 된다.

[0053] 단계 202에서, 컴퓨팅 장치(12)는 사용자로부터 생체 정보(w)를 입력받는다. 본 발명의 실시예들에서, 생체 정보는 지문, 홍체, 얼굴, 정맥 등, 상기 사용자의 하나 이상의 신체적, 행동적 특징을 포함할 수 있다. 일 실시

예에서, 사용자는 자신이 신뢰하는 오프라인 장치(자신이 사용하는 개인용 컴퓨팅 디바이스)를 이용하여 상기 생체 정보를 입력할 수 있다.

[0054] 단계 204에서, 컴퓨팅 장치(12)는 전술한 퍼지 추출기(Fuzzy Extractor)를 이용하여, 입력된 상기 생체 정보(w)에 대응되는 식별값(R) 및 헬퍼 문자열(P)을 생성한다. 이때 헬퍼 문자열(P)은 공개 가능한 정보이므로, 컴퓨팅 장치(12) 내에 별도의 보안 수단 없이 저장 가능하다. 또한, 상기 생체 정보(w)는 유출되는 것을 방지하기 위하여 상기 식별값(R) 및 헬퍼 문자열(P) 생성 이후 삭제될 수 있다.

[0055] 단계 206에서, 컴퓨팅 장치(12)는 랜덤 문자열(R')을 생성한다. 이때 상기 랜덤 문자열(R')의 길이는 204 단계에서 생성되는 상기 식별값(R)의 길이보다 크거나 같도록 구성될 수 있다.

[0056] 단계 208에서, 컴퓨팅 장치(12)는 상기 식별값(R) 및 상기 랜덤 문자열(R')로부터 비밀키(sk)를 생성한다. 일 실시예에서, 상기 비밀키(sk)는 상기 식별값(R) 및 상기 랜덤 문자열(R')을 XOR(eXclusive OR) 연산함으로써 생성될 수 있다.

[0057] 단계 210에서, 컴퓨팅 장치(12)는 상기 비밀키(sk)에 대응되는 공개키(pk)를 생성한다. 상기 비밀키(sk) 및 공개키(pk)는 전술한 DKeyGen 알고리즘을 이용하여 생성될 수 있다.

[0058] 단계 212에서, 컴퓨팅 장치(12)는 비밀키(sk) 및 식별값(R)을 지우고, 랜덤 문자열(R')을 상기 비밀키(sk) 대신 안전하게 저장한다. 예를 들어, 컴퓨팅 장치(12)는 내부의 보안 스토리지(secure storage) 영역 등의 저장 공간에 상기 랜덤 문자열(R')을 저장할 수 있다.

[0060] 도 3은 본 본 발명의 제1 실시예에 따른 암호화 키 복구 방법(300)을 설명하기 위한 흐름도이다. 도 3에 도시된 방법은 예를 들어, 전술한 컴퓨팅 장치(12)에 의해 수행될 수 있다. 도시된 흐름도에서는 상기 방법을 복수 개의 단계로 나누어 기재하였으나, 적어도 일부의 단계들은 순서를 바꾸어 수행되거나, 다른 단계와 결합되어 함께 수행되거나, 생략되거나, 세부 단계들로 나뉘어 수행되거나, 또는 도시되지 않은 하나 이상의 단계가 부가되어 수행될 수 있다.

[0061] 본 실시예에서, 사용자가 자신의 비밀키를 다시 복구하여 서명을 생성하거나, 또는 공개키로 암호화된 메시지를 복호화하고자 하는 경우에는 다음과 같은 과정을 통해 비밀키를 복구하게 된다.

[0062] 단계 302에서, 컴퓨팅 장치(12)는 사용자로부터 생체 정보(w')를 재입력받는다. 전술한 바와 같이, 생체 정보의 특성 상 재입력된 생체 정보(w')는 앞선 단계 202에서 입력된 생체 정보(w)와는 일부 차이가 존재할 수 있다.

[0063] 단계 304에서, 컴퓨팅 장치(12)는 전술한 퍼지 추출기(Fuzzy Extractor)를 이용하여, 재입력된 상기 생체 정보(w')로부터 식별값(R)을 복원한다. 구체적으로, 컴퓨팅 장치(12)는 상기 재입력된 생체 정보(w') 및 상기 헬퍼 문자열(P)을 이용하여 상기 식별값(R)을 복원할 수 있다(Rep(w', P) = R).

[0064] 단계 306에서, 컴퓨팅 장치(12)는 상기 복원된 식별값(R) 및 기 저장된 랜덤 문자열(R')을 이용하여 상기 비밀키(sk)를 재생성한다. 전술한 바와 같이, 상기 비밀키(sk)는 상기 식별값(R) 및 상기 랜덤 문자열(R')을 XOR(eXclusive OR) 연산함으로써 재생성될 수 있다.

[0066] 한편, 일 실시예에서 상기 랜덤 문자열(R')은 컴퓨팅 장치(12)에 구비된 물리적 복제 불가능 함수(Physical Unclonable Function, PUF)에 의하여 생성될 수 있다. PUF는 마치 인간의 지문 등과 같이 하드웨어 디바이스에 포함된 각 소자의 고유한 특성을 보안에 적용한 것으로서, PUF 회로에 입력신호인 챌린지(challenge) 비트(bit)를 입력하면 PUF 셀(cell) 각각은 고유한 리스판스(response) 비트(bit)를 출력하도록 구성된다. PUF 회로에서는 같은 셀(cell) 회로를 반복하여 동일한 공정으로 제조하여도 각 셀들이 가진 미세한 차이에 의해 다른 리스판스(response)를 출력하게 되며, 이러한 성질이 PUF 회로에서 물리적인 복제 불가의 특성을 갖게 한다.

[0067] 컴퓨팅 장치(12)는 예컨대, 디바이스에서 측정한 온도 등의 환경 정보를 PUF 회로의 입력값(챌린지)으로 저장하고, 상기 챌린지에 따른 리스판스를 206 단계의 랜덤 문자열(R')로 이용할 수 있다. 이 경우, 컴퓨팅 장치(12)는 별도로 랜덤 문자열(R')을 안전하게 저장할 필요 없이 필요할 때마다 PUF 회로를 이용하여 랜덤 문자열(R')을 생성할 수 있다. 예를 들어, 상기 306 단계에서 컴퓨팅 장치(12)는 저장된 랜덤 문자열(R')이 아닌 PUF 회로를 이용하여 새로 생성된 랜덤 문자열(R')로 비밀키를 복구할 수 있다. 다만, 이 경우 동일한 챌린지에 대한 리스판스에서도 생체 정보와 유사하게 노이즈가 발생할 수 있으므로, 컴퓨팅 장치(12)는 퍼지 추출기 등을 이용하여 PUF 의 출력값의 노이즈를 제거할 수 있다.

[0069] 도 4는 본 발명의 제2 실시예에 따른 암호화 키 생성 시스템(400)을 설명하기 위한 블록도이다. 도시된 바와 같

이, 본 실시예에서 암호화 키 생성 시스템(400)은 전술한 컴퓨팅 장치(12) 이외에 인증 서버(402)를 더 포함할 수 있다. 컴퓨팅 장치(12)는 네트워크(404)를 통해 인증 서버(402)와 통신할 수 있다. 개시되는 실시예들에서, 네트워크(404)는 근거리 통신망(local area network; LAN), 원거리 통신망(wide area network; WAN) 또는 이들의 조합으로 구성될 수 있다.

[0070] 일 실시예에서, 인증 서버(402)는 컴퓨팅 장치(12)의 사용자가 신뢰할 수 있는 서버(trusted authority server)로서, 아이디 기반 서명(Identity-Based Signature Scheme) 서비스를 제공하는 서버일 수 있다. 아이디 기반 서명은 다음의 알고리즘을 포함할 수 있다.

[0071] Setup(1^k): 보안 파라미터 k(k∈N)를 입력으로 받아서 마스터 공개키와 마스터 비밀키 쌍(mpk, msk)를 출력한다.

[0072] KeyGen(id, msk): 사용자의 아이디(id)와 마스터 비밀키(msk)를 입력으로 받아서 id에 대한 비밀키 sk_{id}를 출력한다.

[0073] Sign(m, sk_{id}): 메시지(m) 및 아이디(id)에 대응하는 비밀키(sk_{id})를 입력으로 받아 서명(σ)을 출력한다.

[0074] Verify(σ, m, mpk): 서명(σ)과 메시지(m)와 마스터 공개키(mpk)를 입력으로 받아 맞는 서명이면 1을 출력하고 아니면 0을 출력한다.

[0076] 도 5는 본 발명의 제2 실시예에 따른 암호화 키 생성 방법(500)을 설명하기 위한 흐름도이다. 도 5에 도시된 방법은 예를 들어, 전술한 컴퓨팅 장치(12) 및 인증 서버(402)에 의해 수행될 수 있다. 도시된 흐름도에서는 상기 방법을 복수 개의 단계로 나누어 기재하였으나, 적어도 일부의 단계들은 순서를 바꾸어 수행되거나, 다른 단계와 결합되어 함께 수행되거나, 생략되거나, 세부 단계들로 나뉘어 수행되거나, 또는 도시되지 않은 하나 이상의 단계가 부가되어 수행될 수 있다.

[0077] 본 실시예를 구체적으로 설명하기 전, 컴퓨팅 장치(12) 및 인증 서버(402)는 아이디 기반 서명(IBS)을 위한 서명 스킴을 구비하고 있는 것으로 가정한다. 또한, 컴퓨팅 장치(12)는 제1 실시예에서 설명한 퍼지 추출기(Fuzzy Extractor)를 포함하는 것으로 가정한다.

[0078] 단계 502에서, 인증 서버(402)는 인증 서버(402)는 전술한 Setup 알고리즘을 이용하여 마스터 공개키와 마스터 비밀키 쌍(mpk, msk)을 계산하고, 이 중 마스터 공개키(mpk)를 공개한다.

[0079] 단계 504에서, 사용자는 컴퓨팅 장치(12)를 통해 자신의 아이디(id)를 인증 서버(402)로 송신한다.

[0080] 단계 506에서, 인증 서버(402)는 전술한 KeyGen 알고리즘을 이용하여 비밀키(sk_{id})를 계산한다.

[0081] 단계 508에서, 인증 서버(402)는 계산된 비밀키(sk_{id})를 안전하게 컴퓨팅 장치(12)로 송신한다.

[0082] 단계 510에서, 컴퓨팅 장치(12)는 사용자로부터 생체 정보(w)를 입력받는다. 본 발명의 실시예들에서, 생체 정보는 지문, 홍채, 얼굴, 정맥 등, 상기 사용자의 하나 이상의 신체적, 행동적 특징을 포함할 수 있다. 일 실시예에서, 사용자는 자신이 신뢰하는 오프라인 장치(자신이 사용하는 개인용 컴퓨팅 디바이스)를 이용하여 상기 생체 정보를 입력할 수 있다.

[0083] 단계 512에서, 컴퓨팅 장치(12)는 전술한 퍼지 추출기(Fuzzy Extractor)를 이용하여, 입력된 상기 생체 정보(w)에 대응되는 식별값(R) 및 헬퍼 문자열(P)을 생성한다. 이때 헬퍼 문자열(P)은 공개 가능한 정보이므로, 컴퓨팅 장치(12) 내에 별도의 보안 수단 없이 저장 가능하다. 또한, 상기 생체 정보(w)는 유출되는 것을 방지하기 위하여 상기 식별값(R) 및 헬퍼 문자열(P) 생성 이후 삭제될 수 있다.

[0084] 단계 514에서, 컴퓨팅 장치(12)는 비밀키(sk_{id}) 및 식별값(R)으로부터 저장값(R')을 계산한다. 일 실시예에서, 상기 저장값(R')은 상기 식별값(R) 및 상기 비밀키(sk_{id})를 XOR(eXclusive OR) 연산함으로써 생성될 수 있다.

[0085] 단계 516에서, 식별값(R) 및 비밀키(sk_{id})를 모두 삭제하고, 상기 저장값(R')을 상기 비밀키(sk_{id}) 대신 안전하게 저장한다. 예를 들어, 컴퓨팅 장치(12)는 내부의 보안 스토리지(secure storage) 영역 등의 저장 공간에 상기 랜덤 문자열(R')을 저장할 수 있다.

[0087] 도 6은 본 본 발명의 제2 실시예에 따른 암호화 키 복구 방법(600)을 설명하기 위한 흐름도이다. 도 6에 도시된 방법은 예를 들어, 전술한 컴퓨팅 장치(12)에 의해 수행될 수 있다. 도시된 흐름도에서는 상기 방법을 복수 개

의 단계로 나누어 기재하였으나, 적어도 일부의 단계들은 순서를 바꾸어 수행되거나, 다른 단계와 결합되어 함께 수행되거나, 생략되거나, 세부 단계들로 나뉘어 수행되거나, 또는 도시되지 않은 하나 이상의 단계가 부가되어 수행될 수 있다.

[0088] 단계 602에서, 컴퓨팅 장치(12)는 사용자로부터 생체 정보(w')를 재입력받는다. 전술한 바와 같이, 생체 정보의 특성 상 재입력된 생체 정보(w')는 앞선 단계 510에서 입력된 생체 정보(w)와는 일부 차이가 존재할 수 있다.

[0089] 단계 604에서, 컴퓨팅 장치(12)는 전술한 퍼지 추출기(Fuzzy Extractor)를 이용하여, 재입력된 상기 생체 정보(w')로부터 식별값(R)을 복원한다. 구체적으로, 컴퓨팅 장치(12)는 상기 재입력된 생체 정보(w') 및 상기 헬퍼 문자열(P)을 이용하여 상기 식별값(R)을 복원할 수 있다(Rep(w', P) = R).

[0090] 단계 606에서, 컴퓨팅 장치(12)는 상기 복원된 식별값(R) 및 기 저장된 저장값(R')을 이용하여 상기 비밀키(sk_{id})를 재생성한다. 전술한 바와 같이, 상기 비밀키(sk_{id})는 상기 식별값(R) 및 상기 저장값(R')을 XOR(eXclusive OR) 연산함으로써 재생성될 수 있다.

[0092] 한편, 본 발명의 실시예는 본 명세서에서 기술한 방법들을 컴퓨터상에서 수행하기 위한 프로그램, 및 상기 프로그램을 포함하는 컴퓨터 판독 가능 기록매체를 포함할 수 있다. 상기 컴퓨터 판독 가능 기록매체는 프로그램 명령, 로컬 데이터 파일, 로컬 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체는 본 발명을 위하여 특별히 설계되고 구성된 것들이거나, 또는 컴퓨터 소프트웨어 분야에서 통상적으로 사용 가능한 것일 수 있다. 컴퓨터 판독 가능 기록매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM, DVD와 같은 광 기록 매체, 및 롬, 램, 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 상기 프로그램의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함할 수 있다.

[0093] 이상에서 본 발명의 대표적인 실시예들을 상세하게 설명하였으나, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자는 상술한 실시예에 대하여 본 발명의 범주에서 벗어나지 않는 한도 내에서 다양한 변형이 가능함을 이해할 것이다. 그러므로 본 발명의 권리범위는 설명된 실시예에 국한되어 정해져서는 안 되며, 후술하는 특허청구범위뿐만 아니라 이 특허청구범위와 균등한 것들에 의해 정해져야 한다.

부호의 설명

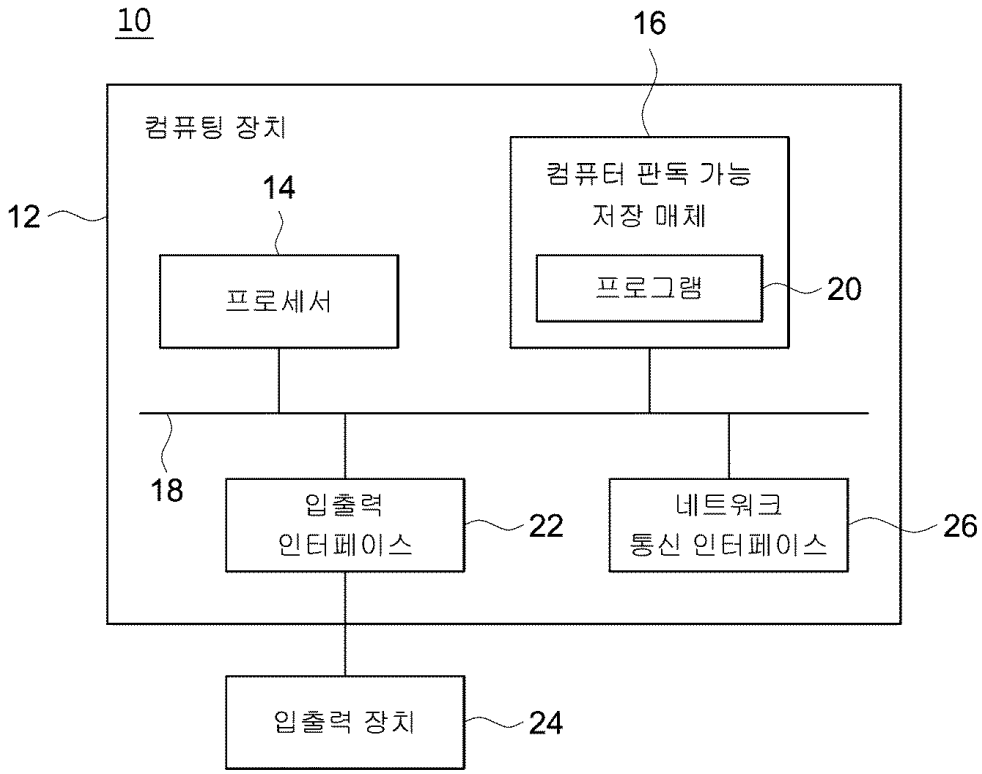
[0095] 12: 컴퓨팅 장치

402: 인증 서버

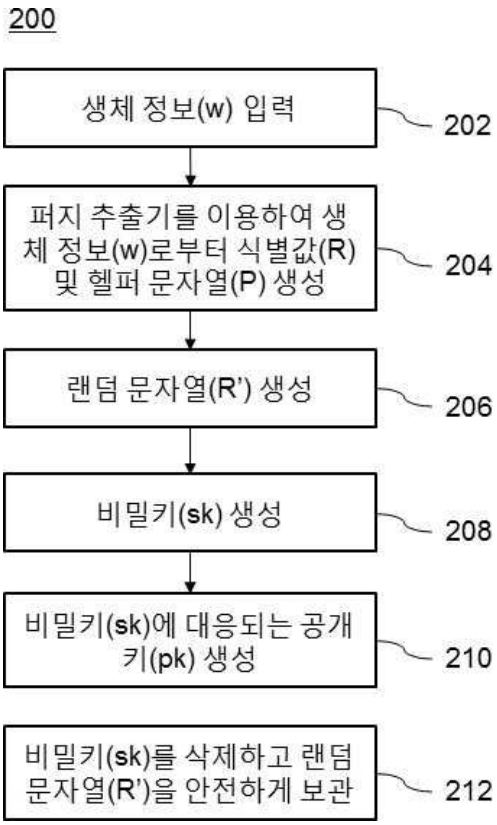
404: 네트워크

도면

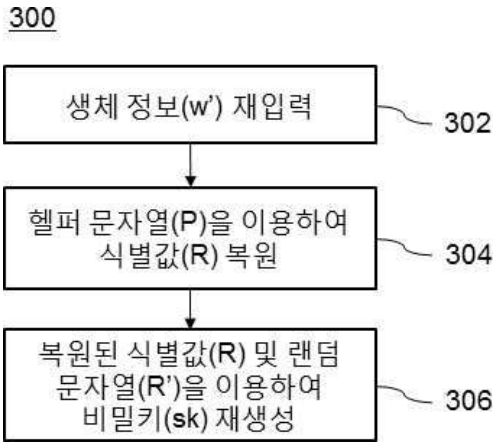
도면1


10
16
컴퓨팅 장치
14
12
컴퓨터 판독 가능
저장 매체
프로세서
프로그램
20
18
입출력
인터페이스
22
네트워크
통신 인터페이스
26
입출력 장치
24

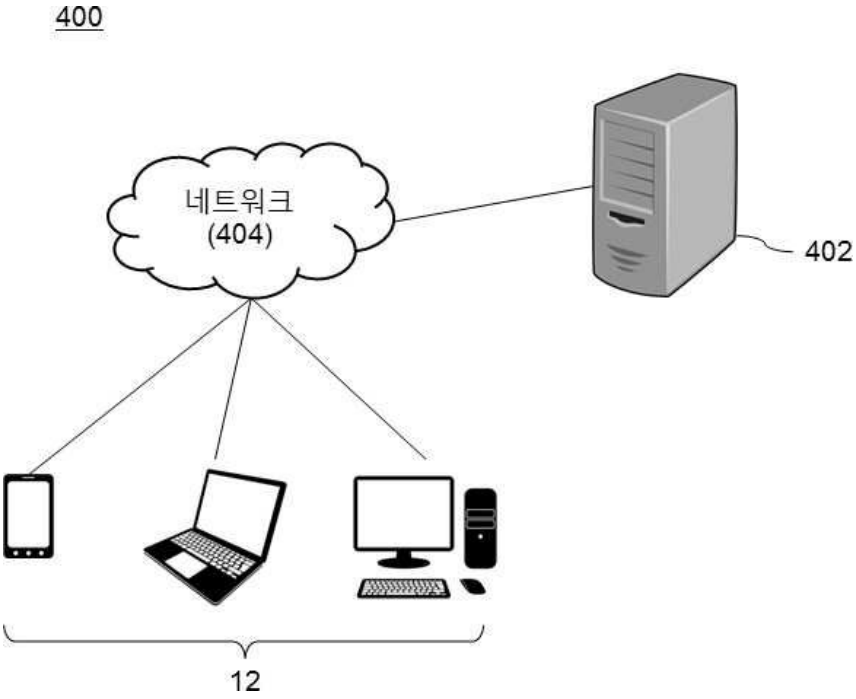
도면2


200
생체 정보(w) 입력
202
퍼지 추출기를 이용하여 생체 정보(w)로부터 식별값(R) 및 헬퍼 문자열(P) 생성
204
랜덤 문자열(R') 생성
206
비밀키(sk) 생성
208
비밀키(sk)에 대응되는 공개키(pk) 생성
210
비밀키(sk)를 삭제하고 랜덤 문자열(R')을 안전하게 보관
212

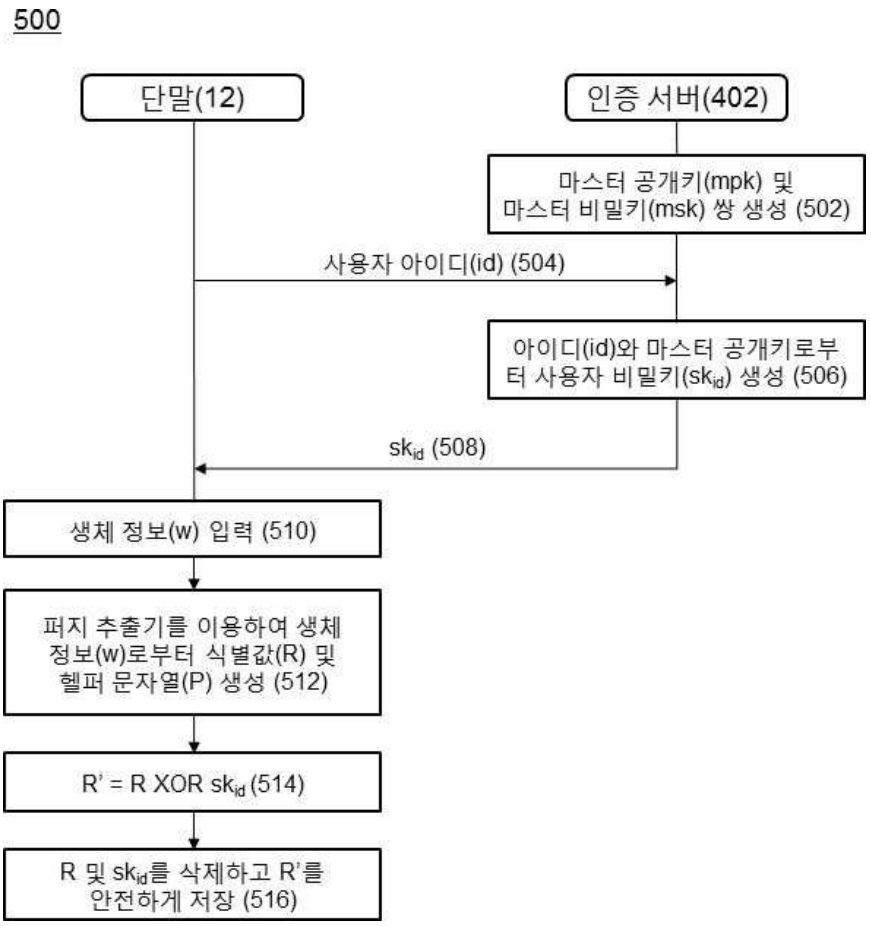
도면3


300
생체 정보(w') 재입력
302
헬퍼 문자열(P)을 이용하여
식별값(R) 복원
304
복원된 식별값(R) 및 랜덤
문자열(R')을 이용하여
비밀키(sk) 재생성
306

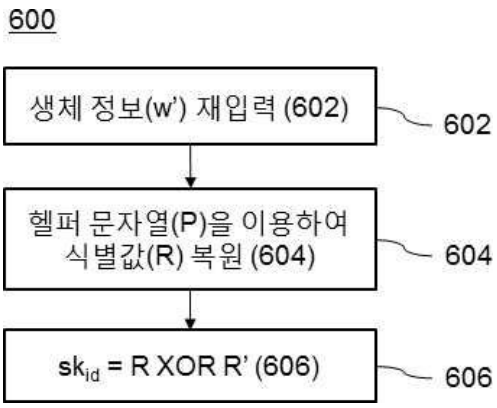
도면4


400
네트워크
(404)
402
12

도면5


500
단말(12)
인증 서버(402)
마스터 공개키(mpk) 및 마스터 비밀키(msk) 쌍 생성 (502)
사용자 아이디(id) (504)
아이디(id)와 마스터 공개키로부터 사용자 비밀키(sk_{id}) 생성 (506)
sk_{id} (508)
생체 정보(w) 입력 (510)
퍼지 추출기를 이용하여 생체 정보(w)로부터 식별값(R) 및 헬퍼 문자열(P) 생성 (512)
R' = R XOR sk_{id} (514)
R 및 sk_{id}를 삭제하고 R'를 안전하게 저장 (516)

도면6


600
생체 정보(w') 재입력 (602)
602
헬퍼 문자열(P)을 이용하여 식별값(R) 복원 (604)
604
sk_{id} = R XOR R' (606)
606