(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2017년03월09일
(11) 등록번호 10-1714466
(24) 등록일자 2017년03월03일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 9/08* (2006.01)
(52) CPC특허분류
H04L 9/3228 (2013.01)
H04L 9/0863 (2013.01)
(21) 출원번호 10-2015-0146263
(22) 출원일자 2015년10월20일
심사청구일자 2015년10월20일
(56) 선행기술조사문헌
KATZ, Jonathan; SHIN, Ji Sun. "Parallel and concurrent security of the HB and HB+ protocols." Springer Berlin Heidelberg, 2006. p. 73-87. (2006)*
Hou, Fangtian, et al. "An analysis of HB-MAP based on OPNET simulation." Wuhan University Journal of Natural Sciences 18.1 (2013): p.49-54. (2013)*
KR101296402 B1
V. Khu-smith and C. J. Mitchell. Electronic transaction security: An analysis of the effectiveness of SSL and TLS, SAM ' 02, p. 425-429. CSREA Press, June 2002. (2002.06.)*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
세종대학교산학협력단
서울특별시 광진구 능동로 209 (군자동, 세종대학교)
(72) 발명자
신지선
서울특별시 송파구 올림픽로 435, 311동 2001호 (신천동,파크리오)
(74) 대리인
두호특허법인

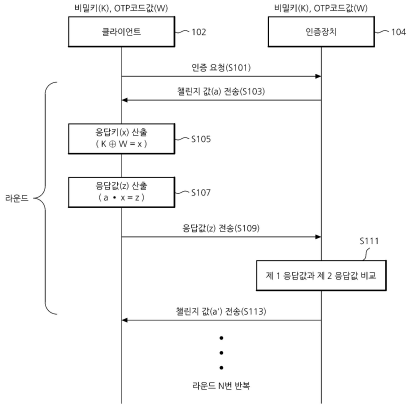
전체 청구항 수 : 총 15 항 심사관 : 양종필

(54) 발명의 명칭 **인증 방법 및 이를 수행하기 위한 장치**

(57) 요 약

인증 방법 및 이를 수행하기 위한 장치가 개시된다. 예시적인 실시예에 따른 인증 방법은, 인증 장치에서, OTP(One Time Password) 코드 값을 생성할 수 있는 클라이언트를 인증하기 위한 방법으로서, 클라이언트와 비밀키 및 OTP 코드 값을 공유하는 단계; 클라이언트로 챌린지 값을 전송하는 단계, 클라이언트로부터 챌린지 값에 대한 제1 응답값을 수신하는 단계, 공유한 비밀키 및 OTP 코드 값을 연산하여 응답키를 산출하고, 챌린지 값과 응답키를 연산하여 제2 응답값을 산출하는 단계; 및 제1 응답값과 제2 응답값을 비교하는 단계를 포함한다.

대 표 도 - 도1



(52) CPC특허분류
H04L 9/3271 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 1711024332
부처명 미래창조과학부
연구관리전문기관 한국연구재단
연구사업명 신진연구자지원
연구과제명 스마트폰의 개인 정보 보호와 프라이버시 강화
기 여 율 1/1
주관기관 세종대학교 산학협력단
연구기간 2013.06.01 ~ 2016.05.31

명 세 서

청구범위

청구항 1

삭제

청구항 2

삭제

청구항 3

삭제

청구항 4

삭제

청구항 5

삭제

청구항 6

삭제

청구항 7

삭제

청구항 8

인증 장치에서, OTP(One Time Password) 코드 값을 생성할 수 있는 클라이언트를 인증하기 위한 방법으로서,

상기 클라이언트와 비밀키 및 OTP 코드 값을 공유하는 단계;

상기 비밀키와 상기 OTP 코드 값을 연산하여 제1 보조키 및 제2 보조키를 생성함으로써 상기 클라이언트가 구비하는 제1 보조키 및 제2 보조키와 동일한 값의 제1 보조키 및 제2 보조키를 획득하는 단계;

상기 클라이언트로 제1 챌린지 값을 전송하는 단계;

상기 클라이언트로부터 제2 챌린지 값을 수신하는 단계;

상기 클라이언트로부터 제1 응답값을 수신하는 단계;

상기 제1 챌린지 값, 상기 제2 챌린지 값, 상기 제1 보조키, 및 상기 제2 보조키를 이용하여 제2 응답값을 산출하는 단계; 및

상기 제1 응답값과 상기 제2 응답값을 비교하는 단계를 포함하고,

상기 비밀키 및 상기 OTP 코드 값은 짝수 비트(2k bit)(k는 1 이상의 자연수)의 길이를 가지며,

상기 제1 보조키 및 상기 제2 보조키를 생성하는 단계는, 상기 비밀키 및 상기 OTP 코드 값을 XOR 연산하고, 연산된 값 중 앞의 k 비트(bit)를 제1 보조키로 하고, 뒤의 k 비트(bit)를 제2 보조키로 하는, 인증 방법.

청구항 9

삭제

청구항 10

청구항 8에 있어서,

상기 제2 응답값을 산출하는 단계는,

상기 제1 챌린지 값과 상기 제1 보조키를 연산하여 제1 응답키를 생성하고, 상기 제2 챌린지 값과 상기 제2 보조키를 연산하여 제2 응답키를 생성하며, 상기 제1 응답키와 상기 제2 응답키를 연산하여 상기 제2 응답값을 산출하는, 인증 방법.

청구항 11

청구항 8에 있어서,

상기 제2 응답값을 산출하는 단계는,

상기 제1 챌린지 값과 상기 제1 보조키를 내적 연산하여 제1 응답키를 생성하고, 상기 제2 챌린지 값과 상기 제2 보조키를 내적 연산하여 제2 응답키를 생성하며, 상기 제1 응답키와 상기 제2 응답키를 XOR 연산하여 상기 제2 응답값을 산출하는, 인증 방법.

청구항 12

청구항 8에 있어서,

상기 제1 응답값과 상기 제2 응답값을 비교하는 단계 이후에,

상기 제1 응답값과 상기 제2 응답값이 일치하는 경우, 상기 클라이언트의 인증을 위한 라운드를 N회(N은 1 이상의 자연수) 반복하는 단계를 더 포함하는, 인증 방법.

청구항 13

청구항 12에 있어서,

상기 인증 장치는,

상기 N회 반복하는 모든 라운드에서 상기 제1 응답값과 상기 제2 응답값이 일치하는 경우, 상기 클라이언트의 인증이 성공한 것으로 판단하는, 인증 방법.

청구항 14

청구항 12에 있어서,

상기 인증 장치는,

상기 N회 반복하는 각 라운드마다 상이한 제1 챌린지 값을 상기 클라이언트로 전송하고, 상기 클라이언트로부터 상기 라운드가 N회 반복하는 동안 동일한 제2 챌린지 값이 수신되는지 여부를 확인하는, 인증 방법.

청구항 15

청구항 8에 있어서,

상기 클라이언트와 노이즈 파라미터(η)($0 < \eta < 1/2$)를 공유하는 단계를 더 포함하고,

상기 제1 응답값을 수신하는 단계는, 상기 클라이언트로부터 $(1 - \eta)$의 확률로 맞는 응답값을 수신하고, η의 확률로 틀린 응답값을 수신하는, 인증 방법.

청구항 16

삭제

청구항 17

삭제

청구항 18

삭제

청구항 19

하나 이상의 프로세서;

메모리; 및

하나 이상의 프로그램을 포함하고, OTP(One Time Password) 코드 값을 생성할 수 있는 클라이언트를 인증하기 위한 장치로서,

상기 하나 이상의 프로그램은 상기 메모리에 저장되고 상기 하나 이상의 프로세서에 의해 실행되도록 구성되며,

상기 프로그램은,

상기 클라이언트와 비밀키 및 OTP 코드 값을 공유하는 단계;

상기 비밀키와 상기 OTP 코드 값을 연산하여 제1 보조키 및 제2 보조키를 생성함으로써 상기 클라이언트가 구비하는 제1 보조키 및 제2 보조키와 동일한 값의 제1 보조키 및 제2 보조키를 획득하는 단계;

상기 클라이언트로 제1 챌린지 값을 전송하는 단계;

상기 클라이언트로부터 제2 챌린지 값을 수신하는 단계;

상기 클라이언트로부터 제1 응답값을 수신하는 단계;

상기 제1 챌린지 값, 상기 제2 챌린지 값, 상기 제1 보조키, 및 상기 제2 보조키를 이용하여 제2 응답값을 산출하는 단계; 및

상기 제1 응답값과 상기 제2 응답값을 비교하는 단계를 실행하기 위한 명령어들을 포함하고,

상기 비밀키 및 상기 OTP 코드 값은 짝수 비트(2k bit)(k는 1 이상의 자연수)의 길이를 가지며,

상기 제1 보조키 및 상기 제2 보조키를 생성하는 단계는, 상기 비밀키 및 상기 OTP 코드 값을 XOR 연산하고, 연산된 값 중 앞의 k 비트(bit)를 제1 보조키로 하고, 뒤의 k 비트(bit)를 제2 보조키로 하는, 장치.

청구항 20

삭제

청구항 21

청구항 19에 있어서,

상기 프로그램은, 상기 제2 응답값을 산출하는 단계에서,

상기 제1 챌린지 값과 상기 제1 보조키를 연산하여 제1 응답키를 생성하는 단계;

상기 제2 챌린지 값과 상기 제2 보조키를 연산하여 제2 응답키를 생성하는 단계; 및

상기 제1 응답키와 상기 제2 응답키를 연산하여 상기 제2 응답값을 산출하는 단계를 실행하기 위한 명령어들을 포함하는 장치.

청구항 22

청구항 19에 있어서,

상기 프로그램은, 상기 제2 응답값을 산출하는 단계에서,

상기 제1 챌린지 값과 상기 제1 보조키를 내적 연산하여 제1 응답키를 생성하는 단계;

상기 제2 챌린지 값과 상기 제2 보조키를 내적 연산하여 제2 응답키를 생성하는 단계; 및

상기 제1 응답키와 상기 제2 응답키를 XOR 연산하여 상기 제2 응답값을 산출하는 단계를 실행하기 위한 명령어들을 포함하는 장치.

청구항 23

청구항 19에 있어서,

상기 프로그램은, 상기 클라이언트와 노이즈 파라미터(η)($0 < \eta < 1/2$)를 공유하는 단계를 실행하기 위한 명령어들을 더 포함하고,

상기 제1 응답값을 수신하는 단계는, 상기 클라이언트로부터 $(1 - \eta)$의 확률로 맞는 응답값을 수신하고, η의 확률로 틀린 응답값을 수신하는, 장치.

청구항 24

삭제

청구항 25

삭제

청구항 26

삭제

청구항 27

하나 이상의 프로세서;

메모리; 및

하나 이상의 프로그램을 포함하고, OTP(One Time Password) 코드 값을 생성할 수 있는 장치로서,

상기 하나 이상의 프로그램은 상기 메모리에 저장되고 상기 하나 이상의 프로세서에 의해 실행되도록 구성되며,

상기 프로그램은,

인증을 수행하는 기기와 비밀키 및 OTP 코드 값을 공유하는 단계;

상기 비밀키와 상기 OTP 코드 값을 연산하여 제1 보조키 및 제2 보조키를 생성함으로써 상기 인증을 수행하는 기기가 구비하는 제1 보조키 및 제2 보조키와 동일한 값의 제1 보조키 및 제2 보조키를 획득하는 단계;

상기 인증을 수행하는 기기로부터 제1 챌린지 값을 수신하는 단계;

상기 인증을 수행하는 기기로 제2 챌린지 값을 전송하는 단계;

상기 제1 챌린지 값, 상기 제2 챌린지 값, 상기 제1 보조키, 및 상기 제2 보조키를 이용하여 응답값을 산출하는 단계; 및

상기 산출한 응답값을 상기 인증을 수행하는 기기로 전송하는 단계를 실행하기 위한 명령어들을 포함하고,

상기 비밀키 및 상기 OTP 코드 값은 짝수 비트(2k bit)(k는 1 이상의 자연수)의 길이를 가지며,

상기 제1 보조키 및 상기 제2 보조키를 생성하는 단계는, 상기 비밀키 및 상기 OTP 코드 값을 XOR 연산하고, 연산된 값 중 앞의 k 비트(bit)를 제1 보조키로 하고, 뒤의 k 비트(bit)를 제2 보조키로 하는, 장치.

청구항 28

삭제

청구항 29

청구항 27에 있어서,

상기 프로그램은, 상기 응답값을 산출하는 단계에서,

상기 제1 챌린지 값과 상기 제1 보조키를 연산하여 제1 응답키를 생성하는 단계;

상기 제2 챌린지 값과 상기 제2 보조키를 연산하여 제2 응답키를 생성하는 단계; 및

상기 제1 응답키와 상기 제2 응답키를 연산하여 상기 응답값을 산출하는 단계를 실행하기 위한 명령어들을 포함하는 장치.

청구항 30

청구항 27에 있어서,

상기 프로그램은, 상기 응답값을 산출하는 단계에서,

상기 제1 챌린지 값과 상기 제1 보조키를 내적 연산하여 제1 응답키를 생성하는 단계;

상기 제2 챌린지 값과 상기 제2 보조키를 내적 연산하여 제2 응답키를 생성하는 단계; 및

상기 제1 응답키와 상기 제2 응답키를 XOR 연산하여 상기 응답값을 산출하는 단계를 실행하기 위한 명령어들을 포함하는 장치.

청구항 31

청구항 27에 있어서,

상기 프로그램은, 상기 인증을 수행하는 기기와 노이즈 파라미터(η)($0 < \eta < 1/2$)를 공유하는 단계를 실행하기 위한 명령어들을 더 포함하고,

상기 응답값을 전송하는 단계는, $(1 - \eta)$의 확률로 맞는 응답값을 전송하고, η의 확률로 틀린 응답값을 전송하는, 장치.

발명의 설명

기 술 분 야

[0001] 본 발명의 실시예는 인증 기법에 관한 것이다.

배 경 기 술

[0002] OTP(One Time Password)는 금융 거래 등 보안이 중요한 분야의 인증 수단으로 널리 사용되고 있다. OTP는 일반적인 비밀번호(Password) 기반의 인증과는 달리 비밀번호를 한번만 사용한다는 점에서 강력한 보안을 제공하지

만, 사용자가 별도의 OTP 발생기(또는 OTP 카드 등)를 가지고 있어야 한다는 점에서 사용성에 제약이 있다.

[0003] 이를 극복하기 위하여 스마트 폰이 OTP 발생기를 대체하여 코드 값을 생성하는 스마트 OTP(Smart OTP)가 제안되었다. 스마트 OTP는 스마트 폰이 OTP 발생기를 대체하여 스마트 폰에서 OTP 코드를 생성하고, 스마트 폰에 내장된 NFC(Near Field Communication) 등의 근거리 무선 통신 기능을 통해 OTP 코드를 전달하는 방법이다. 스마트 OTP는 1) 사용자가 별도의 OTP 발생기를 가지고 있지 않아도 되고, 2) 사용자가 OTP 코드 값을 입력하는 대신 스마트 폰이 NFC 통신을 통해 OTP 코드 값을 전송하기 때문에, OTP 코드 값이 길어져도 사용성과 효율성을 크게 떨어뜨리지 않는다는 장점이 있다.

[0004] 이와 같이, 스마트 OTP는 기존 OTP 방식의 한계를 극복한 활용 가치가 높은 인증 방식이나, 스마트 폰이 갖는 보안 취약점으로 인한 보안 문제를 가지게 된다. 예를 들어, 스마트 OTP를 이용한 근거리 통신 시 통신 내용을 수집하여 비밀 키를 알라내려는 도청 공격(Eavesdropping)이나 가짜 태그 또는 가짜 리더를 이용한 위장 공격(Impersonation)에 노출될 수 있다. 또한, 스마트 OTP는 OTP 코드 값을 스마트 폰에서 생성 및 보관하기 때문에, 악성 코드로 인한 해킹 등으로 인해 OTP 코드 값이 유출될 수 있게 된다.

[0005] 이에, 스마트 OTP가 갖는 사용성 및 효율성을 그대로 유지하면서, 스마트 OTP의 보안성을 강화할 수 있는 방안이 요구된다.

선행기술문헌

[0006] 한국등록특허공보 제10-1296402호(2013.08.14)

발명의 내용

해결하려는 과제

[0007] 본 발명의 실시예는 보안성을 강화할 수 있는 인증 방법 및 이를 수행하기 위한 장치를 제공하기 위한 것이다.

과제의 해결 수단

[0008] 예시적인 실시예에 따른 인증 방법은, 인증 장치에서, OTP(One Time Password) 코드 값을 생성할 수 있는 클라이언트를 인증하기 위한 방법으로서, 상기 클라이언트와 비밀키 및 OTP 코드 값을 공유하는 단계; 상기 클라이언트로 챌린지 값을 전송하는 단계; 상기 클라이언트로부터 상기 챌린지 값에 대한 제1 응답값을 수신하는 단계; 상기 공유한 비밀키 및 OTP 코드 값을 연산하여 응답키를 산출하고, 상기 챌린지 값과 상기 응답키를 연산하여 제2 응답값을 산출하는 단계; 및 상기 제1 응답값과 상기 제2 응답값을 비교하는 단계를 포함한다.

[0009] 상기 제2 응답값을 산출하는 단계는, 상기 공유한 비밀키 및 OTP 코드 값을 XOR 연산하여 응답키를 산출하고, 상기 챌린지 값과 상기 응답키를 내적(Inner Product) 연산하여 제2 응답값을 산출할 수 있다.

[0010] 상기 비밀키 및 상기 OTP 코드 값은, 동일한 비트(Bit)의 길이를 가질 수 있다.

[0011] 상기 제1 응답값과 상기 제2 응답값을 비교하는 단계 이후에, 상기 제1 응답값과 상기 제2 응답값이 일치하는 경우, 상기 클라이언트의 인증을 위한 라운드를 N회(N은 1 이상의 자연수) 반복하는 단계를 더 포함할 수 있다.

[0012] 상기 인증 장치는, 상기 N회 반복하는 모드 라운드에서 상기 제1 응답값과 상기 제2 응답값이 일치하는 경우, 상기 클라이언트의 인증이 성공한 것으로 판단할 수 있다.

[0013] 상기 인증 장치는, 상기 N회 반복하는 각 라운드마다 상이한 챌린지 값을 상기 클라이언트로 전송하고, 상기 클라이언트는, 상기 라운드가 N회 반복되는 동안 동일한 챌린지 값이 수신되는지 여부를 확인할 수 있다.

[0014] 상기 클라이언트와 노이즈 파라미터(η)($0 < \eta < 1/2$)를 공유하는 단계를 더 포함하고, 상기 제1 응답값을 수신하는 단계는, 상기 클라이언트로부터 $(1 - \eta)$의 확률로 맞는 응답값을 수신하고, η의 확률로 틀린 응답값을 수신할 수 있다.

[0015] 예시적인 다른 실시예에 따른 인증 방법은, 인증 장치에서, OTP(One Time Password) 코드 값을 생성할 수 있는 클라이언트를 인증하기 위한 방법으로서, 상기 클라이언트와 비밀키 및 OTP 코드 값을 공유하는 단계; 상기 비

밀키와 상기 OTP 코드 값을 연산하여 제1 보조키 및 제2 보조키를 생성하는 단계; 상기 클라이언트로 제1 챌린지 값을 전송하는 단계; 상기 클라이언트로부터 제2 챌린지 값을 수신하는 단계; 상기 클라이언트로부터 제1 응답값을 수신하는 단계; 상기 제1 챌린지 값, 상기 제2 챌린지 값, 상기 제1 보조키, 및 상기 제2 보조키를 이용하여 제2 응답값을 산출하는 단계; 및 상기 제1 응답값과 상기 제2 응답값을 비교하는 단계를 포함한다.

[0016] 상기 비밀키 및 상기 OTP 코드 값은 짝수 비트(2k bit)(k는 1 이상의 자연수)의 길이를 가지고, 상기 제1 보조키 및 상기 제2 보조키를 생성하는 단계는, 상기 비밀키 및 상기 OTP 코드 값을 XOR 연산하고, 연산된 값 중 앞의 k 비트(bit)를 제1 보조키로 하고, 뒤의 k 비트(bit)를 제2 보조키로 할 수 있다.

[0017] 상기 제2 응답값을 산출하는 단계는, 상기 제1 챌린지 값과 상기 제1 보조키를 연산하여 제1 응답키를 생성하고, 상기 제2 챌린지 값과 상기 제2 보조키를 연산하여 제2 응답키를 생성하며, 상기 제1 응답키와 상기 제2 응답키를 연산하여 상기 제2 응답값을 산출할 수 있다.

[0018] 상기 제2 응답값을 산출하는 단계는, 상기 제1 챌린지 값과 상기 제1 보조키를 내적 연산하여 제1 응답키를 생성하고, 상기 제2 챌린지 값과 상기 제2 보조키를 내적 연산하여 제2 응답키를 생성하며, 상기 제1 응답키와 상기 제2 응답키를 XOR 연산하여 상기 제2 응답값을 산출할 수 있다.

[0019] 상기 제1 응답값과 상기 제2 응답값을 비교하는 단계 이후에, 상기 제1 응답값과 상기 제2 응답값이 일치하는 경우, 상기 클라이언트의 인증을 위한 라운드를 N회(N은 1 이상의 자연수) 반복하는 단계를 더 포함할 수 있다.

[0020] 상기 인증 장치는, 상기 N회 반복하는 모든 라운드에서 상기 제1 응답값과 상기 제2 응답값이 일치하는 경우, 상기 클라이언트의 인증이 성공한 것으로 판단할 수 있다.

[0021] 상기 인증 장치는, 상기 N회 반복하는 각 라운드마다 상이한 제1 챌린지 값을 상기 클라이언트로 전송하고, 상기 클라이언트로부터 상기 라운드가 N회 반복하는 동안 동일한 제2 챌린지 값이 수신되는지 여부를 확인할 수 있다.

[0022] 상기 클라이언트와 노이즈 파라미터(η)($0 < \eta < 1/2$)를 공유하는 단계를 더 포함하고, 상기 제1 응답값을 수신하는 단계는, 상기 클라이언트로부터 $(1 - \eta)$의 확률로 맞는 응답값을 수신하고, η의 확률로 틀린 응답값을 수신할 수 있다.

[0023] 예시적인 일 실시예에 따른 장치는, 하나 이상의 프로세서; 메모리; 및 하나 이상의 프로그램을 포함하고, OTP(One Time Password) 코드 값을 생성할 수 있는 클라이언트를 인증하기 위한 장치로서, 상기 하나 이상의 프로그램은 상기 메모리에 저장되고 상기 하나 이상의 프로세서에 의해 실행되도록 구성되며, 상기 프로그램은, 상기 클라이언트와 비밀키 및 OTP 코드 값을 공유하는 단계; 상기 클라이언트로 챌린지 값을 전송하는 단계; 상기 클라이언트로부터 상기 챌린지 값에 대한 제1 응답값을 수신하는 단계; 상기 공유한 비밀키 및 OTP 코드 값을 연산하여 응답키를 산출하고, 상기 챌린지 값과 상기 응답키를 연산하여 제2 응답값을 산출하는 단계; 및 상기 제1 응답값과 상기 제2 응답값을 비교하는 단계를 실행하기 위한 명령어들을 포함한다.

[0024] 상기 프로그램은, 상기 제2 응답값을 산출하는 단계에서, 상기 공유한 비밀키 및 OTP 코드 값을 XOR 연산하여 응답키를 산출하는 단계; 및 상기 챌린지 값과 상기 응답키를 내적 연산하여 제2 응답값을 산출하는 단계를 실행하기 위한 명령어들을 포함할 수 있다.

[0025] 상기 프로그램은, 상기 클라이언트와 노이즈 파라미터(η)($0 < \eta < 1/2$)를 공유하는 단계를 실행하기 위한 명령어들을 더 포함하고, 상기 제1 응답값을 수신하는 단계는, 상기 클라이언트로부터 $(1 - \eta)$의 확률로 맞는 응답값을 수신하고, η의 확률로 틀린 응답값을 수신할 수 있다.

[0026] 예시적인 다른 실시예에 따른 장치는, 하나 이상의 프로세서; 메모리; 및 하나 이상의 프로그램을 포함하고, OTP(One Time Password) 코드 값을 생성할 수 있는 클라이언트를 인증하기 위한 장치로서, 상기 하나 이상의 프로그램은 상기 메모리에 저장되고 상기 하나 이상의 프로세서에 의해 실행되도록 구성되며, 상기 프로그램은, 상기 클라이언트와 비밀키 및 OTP 코드 값을 공유하는 단계; 상기 비밀키와 상기 OTP 코드 값을 연산하여 제1 보조키 및 제2 보조키를 생성하는 단계; 상기 클라이언트로 제1 챌린지 값을 전송하는 단계; 상기 클라이언트로부터 제2 챌린지 값을 수신하는 단계; 상기 클라이언트로부터 제1 응답값을 수신하는 단계; 상기 제1 챌린지 값, 상기 제2 챌린지 값, 상기 제1 보조키, 및 상기 제2 보조키를 이용하여 제2 응답값을 산출하는 단계; 및 상기 제1 응답값과 상기 제2 응답값을 비교하는 단계를 실행하기 위한 명령어들을 포함한다.

[0027] 상기 비밀키 및 상기 OTP 코드 값은 짝수 비트(2k bit)(k는 1 이상의 자연수)의 길이를 가지고, 상기 제1 보조키 및 상기 제2 보조키를 생성하는 단계는, 상기 비밀키 및 상기 OTP 코드 값을 XOR 연산하고, 연산된 값 중 앞

의 k 비트(bit)를 제1 보조키로 하고, 뒤의 k 비트(bit)를 제2 보조키로 할 수 있다.

[0028] 상기 프로그램은, 상기 제2 응답값을 산출하는 단계에서, 상기 제1 챌린지 값과 상기 제1 보조키를 연산하여 제1 응답키를 생성하는 단계; 상기 제2 챌린지 값과 상기 제2 보조키를 연산하여 제2 응답키를 생성하는 단계; 및 상기 제1 응답키와 상기 제2 응답키를 연산하여 상기 제2 응답값을 산출하는 단계를 실행하기 위한 명령어들을 포함한다.

[0029] 상기 프로그램은, 상기 제2 응답값을 산출하는 단계에서, 상기 제1 챌린지 값과 상기 제1 보조키를 내적 연산하여 제1 응답키를 생성하는 단계; 상기 제2 챌린지 값과 상기 제2 보조키를 내적 연산하여 제2 응답키를 생성하는 단계; 및 상기 제1 응답키와 상기 제2 응답키를 XOR 연산하여 상기 제2 응답값을 산출하는 단계를 실행하기 위한 명령어들을 포함할 수 있다.

[0030] 상기 프로그램은, 상기 클라이언트와 노이즈 파라미터(η)($0 < \eta < 1/2$)를 공유하는 단계를 실행하기 위한 명령어들을 더 포함하고, 상기 제1 응답값을 수신하는 단계는, 상기 클라이언트로부터 $(1 - \eta)$의 확률로 맞는 응답값을 수신하고, η의 확률로 틀린 응답값을 수신할 수 있다.

[0031] 예시적인 또 다른 실시예에 따른 장치는, 하나 이상의 프로세서; 메모리; 및 하나 이상의 프로그램을 포함하고, OTP(One Time Password) 코드 값을 생성할 수 있는 장치로서, 상기 하나 이상의 프로그램은 상기 메모리에 저장되고 상기 하나 이상의 프로세서에 의해 실행되도록 구성되며, 상기 프로그램은, 인증을 수행하는 기기와 비밀키 및 OTP 코드 값을 공유하는 단계; 상기 인증을 수행하는 기기로부터 챌린지 값을 수신하는 단계; 상기 공유한 비밀키 및 OTP 코드 값을 연산하여 응답키를 산출하고, 상기 챌린지 값과 상기 응답키를 연산하여 상기 챌린지 값에 대한 응답값을 산출하는 단계; 및 상기 응답값을 상기 인증을 수행하는 기기로 전송하는 단계를 실행하기 위한 명령어들을 포함한다.

[0032] 상기 프로그램은, 상기 응답값을 산출하는 단계에서, 상기 공유한 비밀키 및 OTP 코드 값을 XOR 연산하여 응답키를 산출하는 단계; 및 상기 챌린지 값과 상기 응답키를 내적 연산하여 응답값을 산출하는 단계를 실행하기 위한 명령어들을 포함할 수 있다.

[0033] 상기 프로그램은, 상기 인증을 수행하는 기기와 노이즈 파라미터(η)($0 < \eta < 1/2$)를 공유하는 단계를 실행하기 위한 명령어들을 더 포함하고, 상기 응답값을 전송하는 단계는, $(1 - \eta)$의 확률로 맞는 응답값을 전송하고, η의 확률로 틀린 응답값을 전송할 수 있다.

[0034] 예시적인 또 다른 실시예에 따른 장치는, 하나 이상의 프로세서; 메모리; 및 하나 이상의 프로그램을 포함하고, OTP(One Time Password) 코드 값을 생성할 수 있는 장치로서, 상기 하나 이상의 프로그램은 상기 메모리에 저장되고 상기 하나 이상의 프로세서에 의해 실행되도록 구성되며, 상기 프로그램은, 인증을 수행하는 기기와 비밀키 및 OTP 코드 값을 공유하는 단계; 상기 비밀키와 상기 OTP 코드 값을 연산하여 제1 보조키 및 제2 보조키를 생성하는 단계; 상기 인증을 수행하는 기기로부터 제1 챌린지 값을 수신하는 단계; 상기 인증을 수행하는 기기로 제2 챌린지 값을 전송하는 단계; 상기 제1 챌린지 값, 상기 제2 챌린지 값, 상기 제1 보조키, 및 상기 제2 보조키를 이용하여 응답값을 산출하는 단계; 및 상기 산출한 응답값을 상기 인증을 수행하는 기기로 전송하는 단계를 실행하기 위한 명령어들을 포함한다.

[0035] 상기 비밀키 및 상기 OTP 코드 값은 짝수 비트(2k bit)(k는 1 이상의 자연수)의 길이를 가지고, 상기 제1 보조키 및 상기 제2 보조키를 생성하는 단계는, 상기 비밀키 및 상기 OTP 코드 값을 XOR 연산하고, 연산된 값 중 앞의 k 비트(bit)를 제1 보조키로 하고, 뒤의 k 비트(bit)를 제2 보조키로 할 수 있다.

[0036] 상기 프로그램은, 상기 응답값을 산출하는 단계에서, 상기 제1 챌린지 값과 상기 제1 보조키를 연산하여 제1 응답키를 생성하는 단계; 상기 제2 챌린지 값과 상기 제2 보조키를 연산하여 제2 응답키를 생성하는 단계; 및 상기 제1 응답키와 상기 제2 응답키를 연산하여 상기 응답값을 산출하는 단계를 실행하기 위한 명령어들을 포함할 수 있다.

[0037] 상기 프로그램은, 상기 응답값을 산출하는 단계에서, 상기 제1 챌린지 값과 상기 제1 보조키를 내적 연산하여 제1 응답키를 생성하는 단계; 상기 제2 챌린지 값과 상기 제2 보조키를 내적 연산하여 제2 응답키를 생성하는 단계; 및 상기 제1 응답키와 상기 제2 응답키를 XOR 연산하여 상기 응답값을 산출하는 단계를 실행하기 위한 명령어들을 포함할 수 있다.

[0038] 상기 프로그램은, 상기 인증을 수행하는 기기와 노이즈 파라미터(η)($0 < \eta < 1/2$)를 공유하는 단계를 실행하기 위한 명령어들을 더 포함하고, 상기 응답값을 전송하는 단계는, $(1 - \eta)$의 확률로 맞는 응답값을 전송

하고, η의 확률로 틀린 응답값을 전송할 수 있다.

발명의 효과

[0039] 본 발명의 실시예에 의하면, 스마트 OTP의 인증 방법을 개선함으로써, 스마트 OTP가 갖는 장점을 그대로 활용하면서 스마트 OTP가 갖는 보안 취약성을 보완할 수 있게 된다. 구체적으로, 인증을 위한 근거리 무선 통신 시 도청 공격과 같은 수동적 공격이나 능동적 공격에 대해 보안성을 강화할 수 있게 된다.

도면의 간단한 설명

[0040] 도 1은 예시적인 실시예에 따른 인증 방법을 나타낸 도면

도 2는 예시적인 다른 실시예에 따른 인증 방법을 나타낸 도면

도 3은 예시적인 일 실시예에 따른 인증 장치의 구성을 나타낸 블럭도

도 4는 예시적인 다른 실시예에 따른 인증 장치의 구성을 나타낸 블럭도

도 5는 예시적인 실시예들에서 사용되기에 적합한 예시적인 컴퓨팅 장치를 포함하는 컴퓨팅 환경을 나타낸 도면

발명을 실시하기 위한 구체적인 내용

[0041] 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.

[0042] 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.

[0043] 이하의 설명에 있어서, 신호 또는 정보의 "전송", "통신", "송신", "수신" 기타 이와 유사한 의미의 용어는 일 구성요소에서 다른 구성요소로 신호 또는 정보가 직접 전달되는 것뿐만이 아니라 다른 구성요소를 거쳐 전달되는 것도 포함한다. 특히 신호 또는 정보를 일 구성요소로 "전송" 또는 "송신"한다는 것은 그 신호 또는 정보의 최종 목적지를 지시하는 것이고 직접적인 목적지를 의미하는 것이 아니다. 이는 신호 또는 정보의 "수신"에 있어서도 동일하다. 또한 본 명세서에 있어서, 2 이상의 데이터 또는 정보가 "관련"된다는 것은 하나의 데이터(또는 정보)를 획득하면, 그에 기초하여 다른 데이터(또는 정보)의 적어도 일부를 획득할 수 있음을 의미한다.

[0044] 또한, 본 명세서에서 기재한 "제1", "제2" 등은 서로 다른 구성 요소임을 구분하기 위해서 지칭하는 것일 뿐, 그 순서에 구애받지 않으며 발명의 상세한 설명과 청구범위에서 그 명칭이 일치하지 않을 수 있다.

[0045] 도 1은 예시적인 실시예에 따른 인증 방법을 나타낸 도면이다. 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. 또한 실시예에 따라 상기 방법에 도시되지 않은 하나 이상의 단계들이 상기 방법과 함께 수행될 수도 있다.

[0046] 도 1을 참조하면, 클라이언트(102) 및 인증 장치(104)는 무선 네트워크를 통해 통신 가능하게 연결된다. 무선 네트워크는 예를 들어, NFC(Near Field Communication), 블루투스(Bluetooth), 와이파이(WiFi), 지그비

(Zigbee), WLAN(Wireless Local Area Network), UWB(Ultra Wide Band), BCC(Body Coupled Communication) 등 비교적 가까운 거리에서 디바이스간의 통신을 가능하도록 하는 무선 네트워크일 수 있다.

[0047] 클라이언트(102)는 인증 대상이 되는 단말기이다. 클라이언트(102)는 사용자가 휴대할 수 있는 단말기(예를 들어, 스마트 폰, 휴대폰, 태블릿, 스마트 워치와 같은 웨어러블 기기, 노트북 등)로서, OTP 코드 값을 생성하는 기능을 구비할 수 있다. 인증 장치(104)는 클라이언트(102)를 인증하기 위한 장치이다. 클라이언트(102)는 일종의 태그(Tag)이고, 인증 장치(104)는 일종의 리더(Reader)일 수 있다.

[0048] 클라이언트(102)와 인증 장치(104)는 동일한 비밀키(K)를 공유한다. 그리고, 클라이언트(102)와 인증 장치(104)는 소정 시점에서 동일한 OTP 코드값(W)을 공유한다. 예시적인 실시예에서, 클라이언트(102)와 인증 장치(104)는 시간 동기화 방식을 통해 소정 시점에서 동일한 OTP 코드값(W)을 공유할 수 있다. 그러나, 이에 한정되는 것은 아니며 그 이외의 다양한 방식을 통해 OTP 코드값(W)을 공유할 수 있다. 여기서, 비밀키(K) 및 OTP 코드값(W)는 동일한 길이(예를 들어, k-bit)를 가질 수 있다.

[0049] 먼저, 클라이언트(102)가 인증 장치(104)로 인증 요청을 전송한다(S 101).

[0050] 다음으로, 인증 장치(104)가 클라이언트(102)로 챌린지 값(a)을 전송한다(S 103). 인증 장치(104)는 챌린지 값(a)을 랜덤하게 생성하여 클라이언트(102)로 전송할 수 있다. 챌린지 값(a)은 예를 들어, n-bit의 길이를 가질 수 있다.

[0051] 다음으로, 클라이언트(102)가 비밀키(K)와 OTP 코드값(W)을 연산하여 응답키(x)를 산출한다(S 105). 예시적인 실시예에서, 클라이언트(102)는 비밀키(K)와 OTP 코드값(W)을 XOR(Exclusive OR) 연산하여 응답키(x)를 산출할 수 있다.

[0052] 다음으로, 클라이언트(102)가 인증 장치(104)로부터 수신한 챌린지 값(a)과 상기 산출한 응답키(x)를 연산하여 응답값(z)을 산출한다(S 107). 예시적인 실시예에서, 클라이언트(102)는 챌린지 값(a)과 응답키(x)를 내적(Inner Product) 연산하여 응답값(z)을 산출할 수 있다. 이 경우, 응답값(z)는 1bit의 값(즉, 0 또는 1)을 가지게 된다.

[0053] 다음으로, 클라이언트(102)가 응답값(z)을 인증 장치(104)로 전송한다(S 109).

[0054] 다음으로, 인증 장치(104)가 클라이언트(102)로부터 수신한 응답값(이하, 제1 응답값이라 지칭될 수 있음)과 인증 장치(104)에서 자체적으로 산출한 응답값(이하, 제2 응답값이라 지칭될 수 있음)을 서로 비교하여, 제1 응답값과 제2 응답값이 일치하는지 여부를 확인한다(S 111). 여기서, 인증 장치(104)는 클라이언트(102)와 마찬가지로, 비밀키(K)와 OTP 코드값(W)을 XOR 연산하여 응답키를 산출한 후, 챌린지 값(a)과 응답키를 내적(Inner Product) 연산하여 제2 응답값을 산출할 수 있다.

[0055] 단계 S 111의 확인 결과, 제1 응답값과 제2 응답값이 일치하는 경우, 인증 장치(104)는 이전 라운드의 챌린지 값(a)과는 다른 챌린지 값(a')을 클라이언트(102)로 전송한다(S 113). 여기서, 인증 장치(104)가 클라이언트(102)로 챌린지 값을 전송하고, 클라이언트(102)가 챌린지 값에 대응하는 응답값을 인증 장치(104)로 전송하기까지의 과정이 하나의 라운드를 이룰 수 있다.

[0056] 인증 장치(104)는 단계 S 111에서 제1 응답값과 제2 응답값이 일치하는 경우, 바로 클라이언트(102)의 인증 성공을 결정하는 것이 아니라, 상기 라운드를 기 설정된 횟수 만큼 반복한다. 즉, 클라이언트(102)가 전송하는 응답값(z)은 0 또는 1의 1bit의 값으로, 공격자가 비밀키(K), OTP 코드값(W), 응답키(x) 등을 알지 못하더라도 응답값(z)을 맞출 확률은 1/2인 바, 인증의 보안성을 높이기 위해 상기 라운드를 기 설정된 횟수(N) 만큼 반복하게 된다.

[0057] 여기서, N번의 라운드를 반복하여 각 라운드마다 제1 응답값과 제2 응답값이 모두 일치하는 경우, 인증 장치(104)는 클라이언트(102)의 인증이 성공한 것으로 판단한다. 반면, N번의 라운드를 반복하는 과정에서 제1 응답값과 제2 응답값이 일치하지 않는 경우, 인증 장치(104)는 클라이언트(102)의 인증이 실패한 것으로 판단한다. 이와 같이, N번의 라운드를 반복함으로써, 공격자의 인증 성공 확률을 $(1/2)^N$로 낮출 수 있게 된다.

[0058] 인증 장치(104)는 N번의 라운드를 반복하는 동안 각 라운드마다 상이한 챌린지 값을 클라이언트(102)로 전송할 수 있다. 클라이언트(102)는 N번의 라운드를 반복하는 동안 동일한 챌린지 값을 수신하는 경우, 공격자가 있는 것으로 판단할 수 있다. 이때, 클라이언트(102)는 바로 인증 수행을 중단할 수 있다. 또한, 클라이언트(102)는 공격 사실을 사용자에게 경고할 수 있다.

[0059] 한편, N번의 라운드를 반복 수행하는 경우, 클라이언트(102)와 인증 장치(104) 간에 N개의 챌린지 값 및 응답값을 생성하게 된다. 그러면, 클라이언트(102)와 인증 장치(104) 간의 통신을 듣고 그 내용을 수집한 도청 공격자(Eavesdropper)가 가우시안 알고리즘(Gaussian Elimination)을 이용하여 비밀키(K)를 알아낼 수도 있다.

[0060] 이에, 본 발명의 실시예에서는, 이러한 도청 공격으로부터 보안을 강화하기 위해, 클라이언트(102)와 인증 장치(104)가 동일한 노이즈 파라미터(Noise Parameter)(η)를 추가로 공유할 수 있다. 여기서, $0 < \eta < 1/2$ 일 수 있다. 이 경우, 클라이언트(102)는 각 라운드에서 $(1 - \eta)$의 확률로 맞는 응답값을 전송하고, η의 확률로 틀린 응답값을 전송하게 된다. 그리고, 인증 장치(104)는 N번의 라운드를 실행한 후에 클라이언트(102)로부터 전송되는 응답값 중 맞는 답의 개수가 $N(1 - \eta)$ 이상이면 인증이 성공한 것으로 판단할 수 있다.

[0061] 이와 같이, 클라이언트(102)가 각 라운드에서 $(1 - \eta)$의 확률로 맞는 응답값을 전송하고 η의 확률로 틀린 응답값을 전송하게 되면, 도청 공격자가 N번의 라운드에서 도청 결과로 N개의 챌린지 값 및 응답값을 얻게 되더라도, 이 중에서 $N\eta$개는 틀린 값으로 이루어져 있으므로, 이렇게 잘못된 값이 섞여 있는 자료에서 비밀키 등을 알아내는 것은 매우 어렵게 된다.

[0062] 하지만, 가짜 리더를 이용하여 통신에 직접 참여하는 능동적 공격자(Active Adversary)의 경우, 챌린지 값을 같은 값으로 반복하여 클라이언트(102)의 응답값을 수집하고, 그 중에서 더 빈도수가 높은 값을 맞는 응답값으로 취할 수 있게 된다. 이렇게 여러 챌린지 값에 대해 맞는 응답값을 얻게 되면, 비밀키도 유출될 수 있게 된다.

[0063] 이에, 본 발명의 다른 실시예에서는 능동적 공격자로부터도 보안을 유지할 수 있는 방안을 제안하기로 한다.

[0064] 도 2는 예시적인 다른 실시예에 따른 인증 방법을 나타낸 도면이다. 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. 또한 실시예에 따라 상기 방법에 도시되지 않은 하나 이상의 단계들이 상기 방법과 함께 수행될 수도 있다.

[0065] 도 2를 참조하면, 클라이언트(202)와 인증 장치(204)는 동일한 비밀키(K)를 공유한다. 그리고, 클라이언트(202)와 인증 장치(204)는 소정 시점에서 동일한 OTP 코드값(W)을 공유한다. 예시적인 실시예에서, 클라이언트(202)와 인증 장치(204)는 시간 동기화 방식을 통해 소정 시점에서 동일한 OTP 코드값(W)을 공유할 수 있다.그러나, 이에 한정되는 것은 아니며 그 이외의 다양한 방식을 통해 OTP 코드값(W)을 공유할 수 있다. 여기서, 비밀키(K) 및 OTP 코드값(W)는 동일한 길이를 가질 수 있다. 예를 들어, 비밀키(K) 및 OTP 코드값(W)는 짝수 비트(즉, 2k-bit)의 길이를 가질 수 있다.

[0066] 먼저, 클라이언트(202)와 인증 장치(204)는 각각 비밀키(K)와 OTP 코드값(W)을 연산하고, 연산된 값을 이용하여 제1 보조키(x)와 제2 보조키(y)를 생성한다(S 201). 예시적인 실시예에서, 클라이언트(202)와 인증 장치(204)는 각각 비밀키(K)와 OTP 코드값(W)을 XOR 연산하고, 연산된 값 중 앞의 k-bit를 제1 보조키(x)로 하고, 뒤의 k-bit를 제2 보조키(y)로 할 수 있다. 이 경우, 클라이언트(202)와 인증 장치(204)는 동일한 제1 보조키(x)와 제2 보조키(y)를 공유하게 된다.

[0067] 다음으로, 클라이언트(202)가 인증 장치(204)로 인증 요청 및 제2 챌린지 값(b)을 전송한다(S 203). 그러나, 이에 한정되는 것은 아니며 클라이언트(202)는 인증 요청과 제2 챌린지 값(b)을 별도로 전송할 수도 있다. 예를 들어, 클라이언트(202)는 인증 요청 전송 후 그에 이어서 제2 챌린지 값(b)을 전송할 수도 있다.

[0068] 다음으로, 인증 장치(204)가 클라이언트(202)로 제1 챌린지 값(a)을 전송한다(S 205). 이하, 제1 챌린지 값(a) 및 제2 챌린지 값(b)의 기재에서 “제1” 및 “제2”는 반드시 순서를 의미하는 것은 아니며, 인증 장치(204)와 클라이언트(202) 중 전송하는 주체에 따라 구분하기 위하여 사용될 수 있다. 즉, 인증 장치(204)가 전송하는 것은 제1 챌린지 값(a), 클라이언트(202)가 전송하는 것은 제2 챌린지 값(b)으로 구분될 수 있다. 여기서는, 클라이언트(202)가 제2 챌린지 값(b)을 인증 장치(204)로 전송한 후, 인증 장치(204)가 제1 챌린지 값(a)을 클라이언트(202)로 전송하는 것으로 설명하였으나, 이에 한정되는 것은 아니며 그 전송 순서는 변경될 수 있다. 인증 장치(204) 및 클라이언트(202)는 제1 챌린지 값(a) 및 제2 챌린지 값(b)을 각각 랜덤하게 생성할 수 있다.

[0069] 다음으로, 클라이언트(202)는 제1 챌린지 값(a), 제2 챌린지 값(b), 제1 보조키(x), 및 제2 보조키(y)를 이용하여 제1 챌린지 값(a)에 대응하는 응답값(z)을 산출한다(S 207).

[0070] 구체적으로, 클라이언트(202)는 제1 챌린지 값(a)과 제1 보조키(x)를 연산하여 제1 응답키(X)를 생성하고, 제2

챌린지 값(b)과 제2 보조키(y)를 연산하여 제2 응답키(Y)를 생성하며, 제1 응답키(X)와 제2 응답키(Y)를 연산하여 응답값(z)을 산출할 수 있다. 예시적인 실시예에서, 클라이언트(202)는 제1 챌린지 값(a)과 제1 보조키(x)를 내적(Inner Product) 연산하여 제1 응답키(X)를 생성하고, 제2 챌린지 값(b)과 제2 보조키(y)를 내적(Inner Product) 연산하여 제2 응답키(Y)를 생성하며, 제1 응답키(X)와 제2 응답키(Y)를 XOR 연산하여 응답값(z)을 산출할 수 있다. 이 경우, 응답값(z)는 1bit의 값(즉, 0 또는 1)을 가지게 된다.

[0071] 다음으로, 클라이언트(202)는 응답값(z)을 인증 장치(204)로 전송한다(S 209).

[0072] 다음으로, 인증 장치(204)는 클라이언트(202)로부터 수신한 응답값(이하, 제1 응답값이라 지칭될 수 있음)과 인증 장치(204)에서 자체적으로 산출한 응답값(이하, 제2 응답값이라 지칭될 수 있음)을 서로 비교하여, 제1 응답값과 제2 응답값이 일치하는지 여부를 확인한다(S 211). 여기서, 인증 장치(204)는 클라이언트(202)와 마찬가지로, 제1 챌린지 값(a)과 제1 보조키(x)를 내적(Inner Product) 연산하여 제1 응답키(X)를 생성하고, 제2 챌린지 값(b)과 제2 보조키(y)를 내적(Inner Product) 연산하여 제2 응답키(Y)를 생성하며, 제1 응답키(X)와 제2 응답키(Y)를 XOR 연산하여 제2 응답값을 산출할 수 있다.

[0073] 단계 S 211의 확인 결과, 제1 응답값과 제2 응답값이 일치하는 경우, 클라이언트(202)는 이전 라운드의 제2 챌린지 값(b)과는 다른 제2 챌린지 값(b')을 인증 장치(204)로 전송하고(S 213), 인증 장치(204)는 이전 라운드의 제1 챌린지 값(a)과는 다른 제1 챌린지 값(a')을 클라이언트(202)로 전송한다(S 215).

[0074] 인증 장치(204)는 단계 S 211에서 제1 응답값과 제2 응답값이 일치하는 경우, 바로 클라이언트(202)의 인증 성공을 결정하는 것이 아니라, 상기 라운드를 기 설정된 횟수 만큼 반복하게 된다. 여기서, N번의 라운드를 반복하여 각 라운드마다 제1 응답값과 제2 응답값이 모두 일치하는 경우, 인증 장치(204)는 클라이언트(202)의 인증이 성공한 것으로 판단한다. 반면, N번의 라운드를 반복하는 과정에서 제1 응답값과 제2 응답값이 일치하지 않는 경우, 인증 장치(204)는 클라이언트(202)의 인증이 실패한 것으로 판단한다.

[0075] 인증 장치(204)는 N번의 라운드를 반복하는 동안 각 라운드마다 상이한 제1 챌린지 값을 클라이언트(202)로 전송할 수 있다. 클라이언트(202)는 N번의 라운드를 반복하는 동안 동일한 제1 챌린지 값을 수신하는 경우, 공격자가 있는 것으로 판단할 수 있다. 또한, 클라이언트(202)는 N번의 라운드를 반복하는 동안 각 라운드마다 상이한 제2 챌린지 값을 인증 장치(204)로 전송할 수 있다. 인증 장치(204)는 N번의 라운드를 반복하는 동안 동일한 제2 챌린지 값을 수신하는 경우, 공격자가 있는 것으로 판단하여 인증이 실패한 것으로 결정할 수 있다.

[0076] 또한, 본 실시예에서도, 클라이언트(202)와 인증 장치(204)가 동일한 노이즈 파라미터(Noise Parameter)(η)를 추가로 공유한 후, 클라이언트(202)가 각 라운드에서 $(1-\eta)$의 확률로 맞는 응답값을 전송하고, η의 확률로 틀린 응답값을 전송할 수 있다. 그리고, 인증 장치(204)는 N번의 라운드를 실행한 후에 클라이언트(202)로부터 전송되는 응답값 중 맞는 답의 개수가 $N(1-\eta)$ 이상이면 인증이 성공한 것으로 판단할 수 있다.

[0077] 본 발명의 실시예에 의하면, 인증 장치(204)뿐만 아니라 클라이언트(202)도 챌린지 값을 인증 장치(204)로 전송하고 이를 이용하여 응답값을 산출함으로써, 가짜 리더를 이용한 능동적 공격자(Active Adversary)로부터도 보안을 유지할 수 있게 된다. 즉, 클라이언트(202)는 인증 장치(204)가 전송한 제1 챌린지 값(a) 뿐만 아니라 자신이 랜덤하게 생성한 제2 챌린지 값(b)을 이용하여 응답값을 산출하므로, 능동적 공격자가 의도적으로 반복하거나 특정한 값으로 선택한 제1 챌린지 값이 주는 영향이 클라이언트(202)가 선택한 제2 챌린지 값에 의해 중화되어 결국 클라이언트(202)의 응답값을 획득하기가 매우 어렵게 된다.

[0078] 도 3은 예시적인 일 실시예에 따른 인증 장치의 구성을 나타낸 블럭도이다.

[0079] 도 3을 참조하면, 인증 장치(104)는 통신부(111), OTP 생성부(113), 챌린지값 생성부(115), 응답값 산출부(117), 인증 결과 처리부(119), 및 저장부(121)를 포함할 수 있다.

[0080] 통신부(111)는 무선 네트워크를 통해 클라이언트(102)와 통신 가능하게 연결되며, 클라이언트(102)와 무선 통신을 수행한다. 예를 들어, 통신부(111)는 클라이언트(102)로부터 인증 요청을 수신할 수 있다. 통신부(111)는 챌린지 값을 클라이언트(102)로 전송할 수 있다. 통신부(111)는 클라이언트(102)로부터 챌린지 값에 대응하는 응답값을 수신할 수 있다.

[0081] OTP 생성부(113)는 클라이언트(102)와 동기화된 OTP 코드 값을 생성한다. 예를 들어, OTP 생성부(113)는 소정 시점의 시간 정보를 이용하여 클라이언트(102)와 동기화된 OTP 코드 값을 생성할 수 있다.

[0082] 챌린지 값 생성부(115)는 챌린지 값을 생성하고, 생성한 챌린지 값을 통신부(111)를 통해 클라이언트(102)로 전송할 수 있다. 챌린지 값 생성부(115)는 각 라운드마다 서로 다른 챌린지 값을 생성할 수 있다.

[0083] 응답값 산출부(117)는 저장부(121)에 저장된 비밀키 및 OTP 생성부(113)가 생성한 OTP 코드 값을 연산하여 응답키를 산출하고, 상기 챌린지 값과 상기 응답키를 연산하여 응답값을 산출할 수 있다. 예시적인 실시예에서, 응답값 산출부(117)는 저장부(121)에 저장된 비밀키 및 OTP 생성부(113)가 생성한 OTP 코드 값을 XOR 연산하여 응답키를 산출하고, 상기 챌린지 값과 상기 응답키를 내적 연산하여 응답값을 산출할 수 있다.

[0084] 인증 결과 처리부(119)는 클라이언트(102)로부터 수신한 응답값(즉, 제1 응답값)과 응답값 산출부(117)가 산출한 응답값(즉, 제2 응답값)을 비교하여 제1 응답값과 제2 응답값이 일치하는지 여부를 확인할 수 있다. 인증 결과 처리부(119)는 제1 응답값과 제2 응답값의 일치 여부에 따라 인증 수행을 위한 라운드를 기 설정된 횟수만큼 반복하도록 할 수 있다.

[0085] 인증 결과 처리부(119)는 기 설정된 횟수만큼 라운드를 반복하여 각 라운드마다 제1 응답값과 제2 응답값이 모두 일치하는 경우, 클라이언트(102)의 인증이 성공한 것으로 판단할 수 있다. 또한, 인증 결과 처리부(119)는 기 설정된 횟수만큼 라운드를 반복하는 과정에서 제1 응답값과 제2 응답값이 일치하지 않는 경우, 클라이언트(102)의 인증이 실패한 것으로 판단할 수 있다.

[0086] 저장부(121)는 비밀키를 저장한다. 비밀키는 클라이언트(102)와 공유된다. 저장부(121)는 OTP 생성부(113)가 생성하는 OTP 코드 값을 저장할 수 있다. 저장부(121)는 챌린지 값 생성부(115)가 생성하는 챌린지 값을 저장할 수 있다. 저장부(121)는 응답값 산출부(117)가 산출하는 응답키 및 응답값을 저장할 수 있다.

[0087] 한편, 클라이언트(102)의 경우, 챌린지값 생성부(115) 및 인증 결과 처리부(119)를 제외하고 인증 장치(104)와 유사한 구성을 가질 수 있다.

[0088] 도 4는 예시적인 다른 실시예에 따른 인증 장치의 구성을 나타낸 블럭도이다.

[0089] 도 4를 참조하면, 인증 장치(204)는 통신부(211), OTP 생성부(213), 보조키 생성부(215), 챌린지값 생성부(217), 응답값 산출부(219), 인증 결과 처리부(221), 및 저장부(223)를 포함할 수 있다.

[0090] 통신부(211)는 무선 네트워크를 통해 클라이언트(202)와 통신 가능하게 연결되며, 클라이언트(202)와 무선 통신을 수행한다. 예를 들어, 통신부(211)는 클라이언트(202)로부터 인증 요청을 수신할 수 있다. 통신부(211)는 제1 챌린지 값을 클라이언트(202)로 전송할 수 있다. 통신부(211)는 클라이언트(202)로부터 제2 챌린지 값을 수신할 수 있다. 통신부(211)는 클라이언트(202)로부터 응답값을 수신할 수 있다.

[0091] OTP 생성부(213)는 클라이언트(202)와 동기화된 OTP 코드 값을 생성한다. 예를 들어, OTP 생성부(213)는 소정 시점의 시간 정보를 이용하여 클라이언트(202)와 동기화된 OTP 코드 값을 생성할 수 있다.

[0092] 보조키 생성부(215)는 저장부(223)에 저장된 비밀키와 상기 생성된 OTP 코드 값을 이용하여 보조키를 생성할 수 있다. 예를 들어, 보조키 생성부(215)는 비밀키와 OTP 코드값을 XOR 연산하고, 연산된 값 중 앞의 k-bit를 제1 보조키로 하고, 뒤의 k-bit를 제2 보조키로 할 수 있다. 이때, 비밀키와 OTP 코드값은 2k-bit의 길이를 가질 수 있다.

[0093] 챌린지 값 생성부(217)는 제1 챌린지 값을 생성하고, 생성한 챌린지 값을 통신부(211)를 통해 클라이언트(202)로 전송할 수 있다. 챌린지 값 생성부(217)는 각 라운드마다 서로 다른 제1 챌린지 값을 생성할 수 있다.

[0094] 응답값 산출부(219)는 제1 챌린지 값, 제2 챌린지 값, 제1 보조키, 및 제2 보조키를 이용하여 응답값을 산출할 수 있다. 구체적으로, 응답값 산출부(219)는 제1 챌린지 값과 제1 보조키를 연산하여 제1 응답키를 생성하고, 제2 챌린지 값과 제2 보조키를 연산하여 제2 응답키를 생성하며, 제1 응답키와 제2 응답키를 연산하여 응답값을 산출할 수 있다. 예시적인 실시예에서, 응답값 산출부(219)는 제1 챌린지 값과 제1 보조키를 내적(Inner Product) 연산하여 제1 응답키를 생성하고, 제2 챌린지 값과 제2 보조키를 내적(Inner Product) 연산하여 제2 응답키를 생성하며, 제1 응답키와 제2 응답키를 XOR 연산하여 응답값을 산출할 수 있다.

[0095] 인증 결과 처리부(221)는 클라이언트(202)로부터 수신한 응답값(즉, 제1 응답값)과 응답값 산출부(219)가 산출한 응답값(즉, 제2 응답값)을 비교하여 제1 응답값과 제2 응답값이 일치하는지 여부를 확인할 수 있다. 인증 결과 처리부(221)는 제1 응답값과 제2 응답값의 일치 여부에 따라 인증 수행을 위한 라운드를 기 설정된 횟수만큼

반복하도록 할 수 있다.

[0096] 인증 결과 처리부(221)는 기 설정된 횟수만큼 라운드를 반복하여 각 라운드마다 제1 응답값과 제2 응답값이 모두 일치하는 경우, 클라이언트(202)의 인증이 성공한 것으로 판단할 수 있다. 또한, 인증 결과 처리부(221)는 기 설정된 횟수만큼 라운드를 반복하는 과정에서 제1 응답값과 제2 응답값이 일치하지 않는 경우, 클라이언트(202)의 인증이 실패한 것으로 판단할 수 있다.

[0097] 저장부(223)는 비밀키를 저장한다. 비밀키는 클라이언트(202)와 공유된다. 저장부(223)는 OTP 생성부(213)가 생성하는 OTP 코드 값을 저장할 수 있다. 저장부(223)는 보조키 생성부(215)가 생성하는 제1 보조키 및 제2 보조키를 저장할 수 있다. 저장부(223)는 챌린지 값 생성부(217)가 생성하는 챌린지 값을 저장할 수 있다. 저장부(223)는 응답값 산출부(219)가 산출하는 응답키 및 응답값을 저장할 수 있다.

[0098] 한편, 클라이언트(202)의 경우, 인증 결과 처리부(221)를 제외하고 인증 장치(204)와 유사한 구성을 가질 수 있다.

[0099] 또한, 상기에 기재된 실시예들에서는 인증 장치(104)가 클라이언트(102)를 직접 인증하는 것으로 설명하였으나, 이에 한정되는 것은 아니며 인증 장치(104)가 별도의 인증 서버(미도시)와 클라이언트(102) 사이에서 메시지의 중개 역할을 하고, 인증 서버(미도시)가 클라이언트(102)의 인증을 수행할 수도 있다.

[0100] 도 5는 예시적인 실시예들에서 사용되기에 적합한 예시적인 컴퓨팅 장치를 포함하는 컴퓨팅 환경을 도시한다.

[0101] 도 5에 도시된 예시적인 컴퓨팅 환경(500)은 컴퓨팅 장치(510)를 포함한다. 통상적으로, 각 구성은 상이한 기능 및 능력을 가질 수 있고, 이하에 기술되지 않았더라도 그 구성에 적합한 컴포넌트를 추가적으로 포함할 수 있다. 컴퓨팅 장치(510)는 가령 휴대폰, 스마트폰, 휴대용 미디어 플레이어, 휴대용 게임 장치, PDA(Personal Digital Assistant), 태블릿, 랩톱 컴퓨터, 웨어러블 기기와 같이 사용자와 연관된 컴퓨팅 장치(예를 들어, 클라이언트(102))일 수 있다. 또한, 컴퓨팅 장치(510)는 인증을 수행하는 컴퓨팅 장치(예를 들어, 인증 장치(104))일 수 있다.

[0102] 컴퓨팅 장치(510)는 적어도 하나의 프로세서(512), 컴퓨터 판독 가능 저장 매체(514) 및 버스(560)를 포함한다. 프로세서(512)는 버스(560)와 연결되고, 버스(560)는 컴퓨터 판독 가능 저장 매체(514)를 포함하여 컴퓨팅 장치(510)의 다른 다양한 컴포넌트들을 프로세서(512)에 연결한다.

[0103] 프로세서(512)는 컴퓨팅 장치(510)로 하여금 앞서 언급된 예시적인 실시예에 따라 동작하도록 할 수 있다. 예컨대, 프로세서(512)는 컴퓨터 판독 가능 저장 매체(514)에 저장된 컴퓨터 실행 가능 명령어를 실행할 수 있고, 컴퓨터 판독 가능 저장 매체(514)에 저장된 컴퓨터 실행 가능 명령어는 프로세서(512)에 의해 실행되는 경우 컴퓨팅 장치(510)로 하여금 소정의 예시적인 실시예에 따른 동작들을 수행하도록 구성될 수 있다.

[0104] 컴퓨터 판독 가능 저장 매체(514)는 컴퓨터 실행 가능 명령어 내지 프로그램 코드(예컨대, 애플리케이션(530)에 포함되는 명령어), 프로그램 데이터(예컨대, 애플리케이션(530)에 의해 사용되는 데이터) 및/또는 다른 적합한 형태의 정보를 저장하도록 구성된다. 컴퓨터 판독 가능 저장 매체(514)에 저장된 애플리케이션(530)은 프로세서(512)에 의해 실행 가능한 명령어의 소정의 집합을 포함한다.

[0105] 도 5에 도시된 메모리(516) 및 저장 장치(518)는 컴퓨터 판독 가능 저장 매체(514)의 예이다. 메모리(516)에는 프로세서(512)에 의해 실행될 수 있는 컴퓨터 실행 가능 명령어가 로딩될 수 있다. 또한, 메모리(516)에는 프로그램 데이터가 저장될 수 있다. 예컨대, 이러한 메모리(516)는 랜덤 액세스 메모리와 같은 휘발성 메모리, 비휘발성 메모리, 또는 이들의 적합한 조합일 수 있다. 다른 예로서, 저장 장치(518)는 정보의 저장을 위한 하나 이상의 착탈 가능하거나 착탈 불가능한 컴포넌트를 포함할 수 있다. 예컨대, 저장 장치(518)는 하드 디스크, 플래시 메모리, 자기 디스크, 광 디스크, 컴퓨팅 장치(510)에 의해 액세스되고 원하는 정보를 저장할 수 있는 다른 형태의 저장 매체, 또는 이들의 적합한 조합일 수 있다.

[0106] 컴퓨팅 장치(510)는 또한 하나 이상의 입출력 장치(570)를 위한 인터페이스를 제공하는 하나 이상의 입출력 인터페이스(520)를 포함할 수 있다. 입출력 인터페이스(520)는 버스(560)에 연결된다. 입출력 장치(570)는 입출력 인터페이스(520)를 통해 컴퓨팅 장치(510)(의 다른 컴포넌트들)에 연결될 수 있다. 입출력 장치(570)는 포인팅 장치, 키보드, 터치 입력 장치, 음성 입력 장치, 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.

[0107] 한편, 소정의 실시예는 본 명세서에서 기술한 과정을 컴퓨터상에서 수행하기 위한 프로그램을 포함하는 컴퓨터 판독 가능 저장 매체를 포함할 수 있다. 이러한 컴퓨터 판독 가능 저장 매체는 프로그램 명령, 로컬 데이터 파일, 로컬 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 그 컴퓨터 판독 가능 저장 매체는 본 발명을 위하여 특별히 설계되고 구성된 것들일 수 있다. 컴퓨터 판독 가능 저장 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM, DVD와 같은 광 기록 매체, 플롭티컬 디스크와 같은 자기-광 매체, 및 롬, 램, 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함할 수 있다.

[0108] 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

[0109] 102, 202 : 클라이언트

104, 204 : 인증 장치

111, 211 : 통신부

113, 213 : OTP 생성부

115, 217 : 챌린지값 생성부

117, 219 : 응답값 산출부

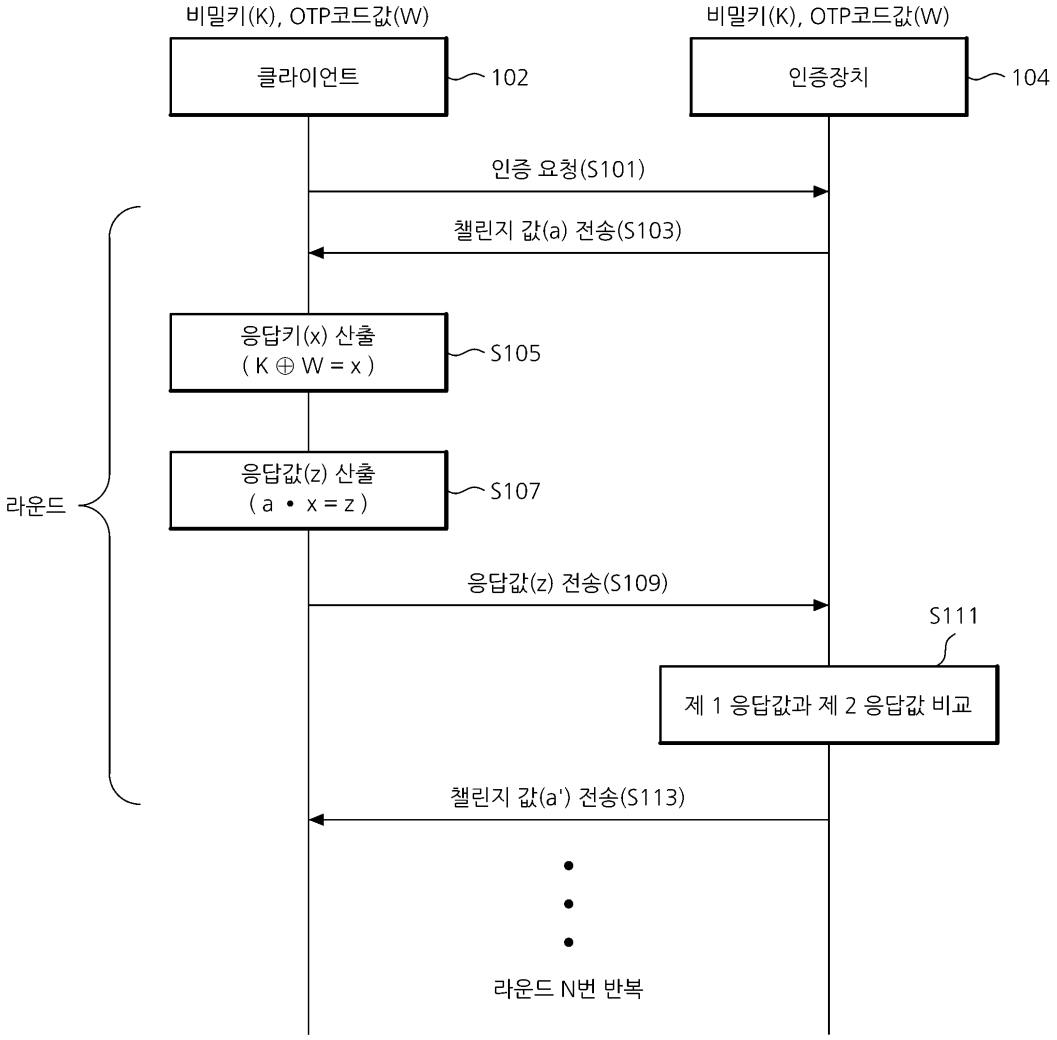
119, 221 : 인증 결과 처리부

121, 223 : 저장부

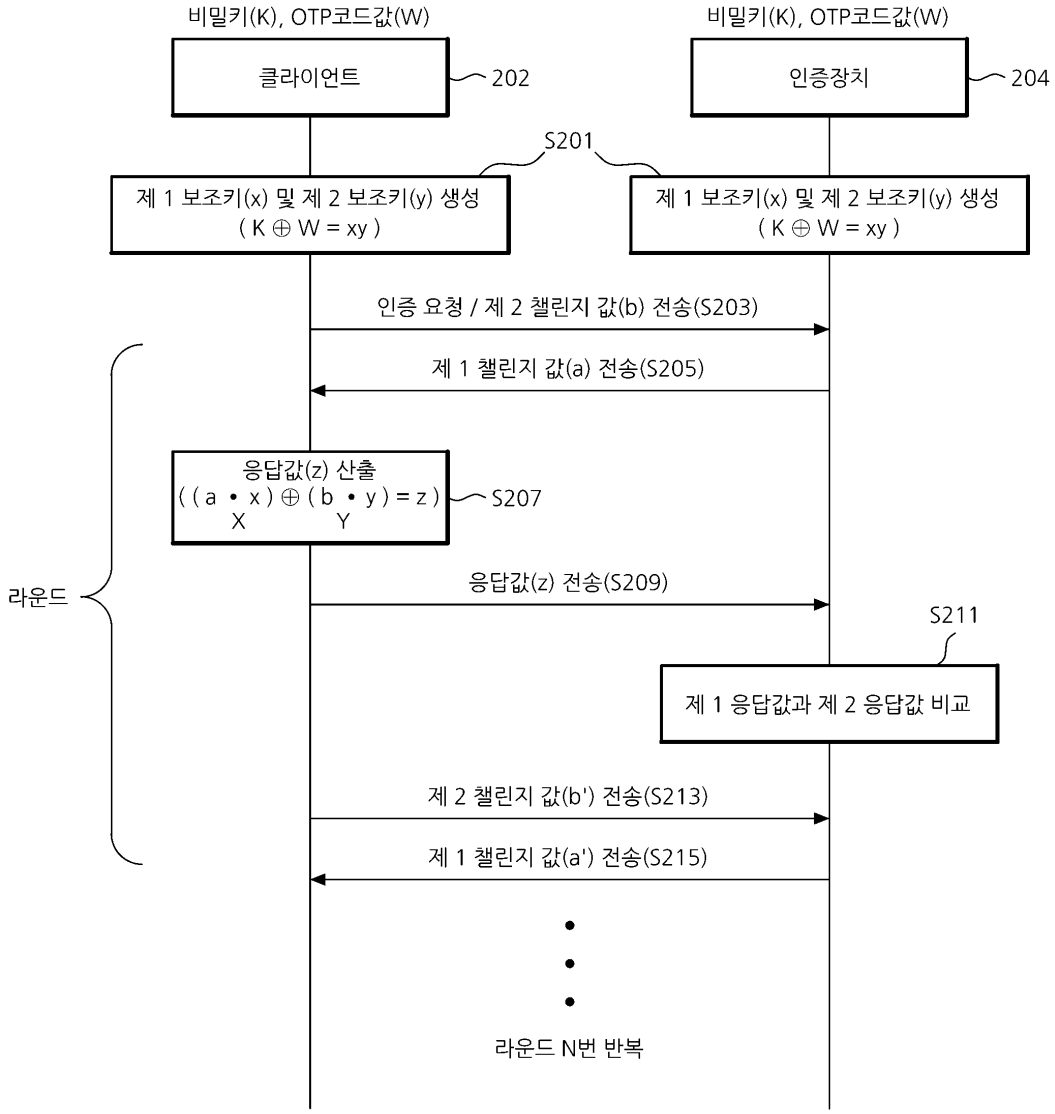
215 : 보조키 생성부

도면

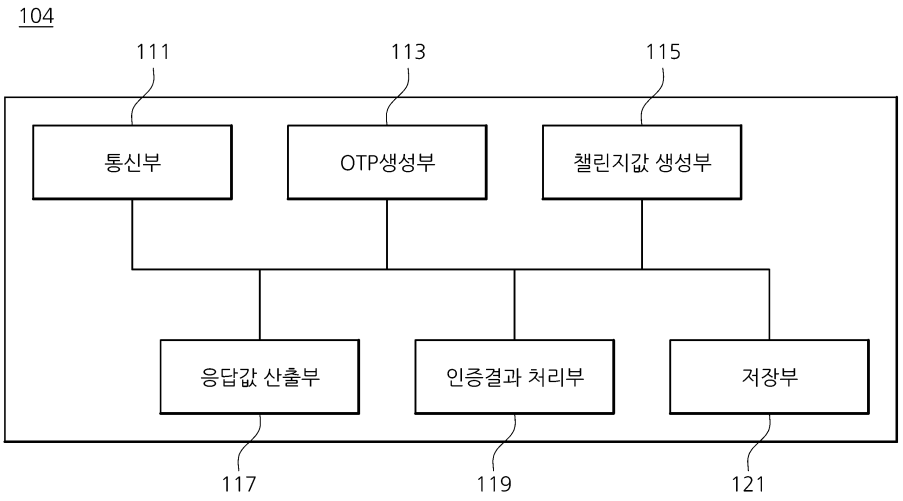
도면1


비밀키(K), OTP코드값(W)
클라이언트
102
비밀키(K), OTP코드값(W)
인증장치
104
인증 요청(S101)
챌린지 값(a) 전송(S103)
응답키(x) 산출
(K ⊕ W = x)
S105
응답값(z) 산출
(a • x = z)
S107
라운드
응답값(z) 전송(S109)
S111
제 1 응답값과 제 2 응답값 비교
챌린지 값(a') 전송(S113)
라운드 N번 반복

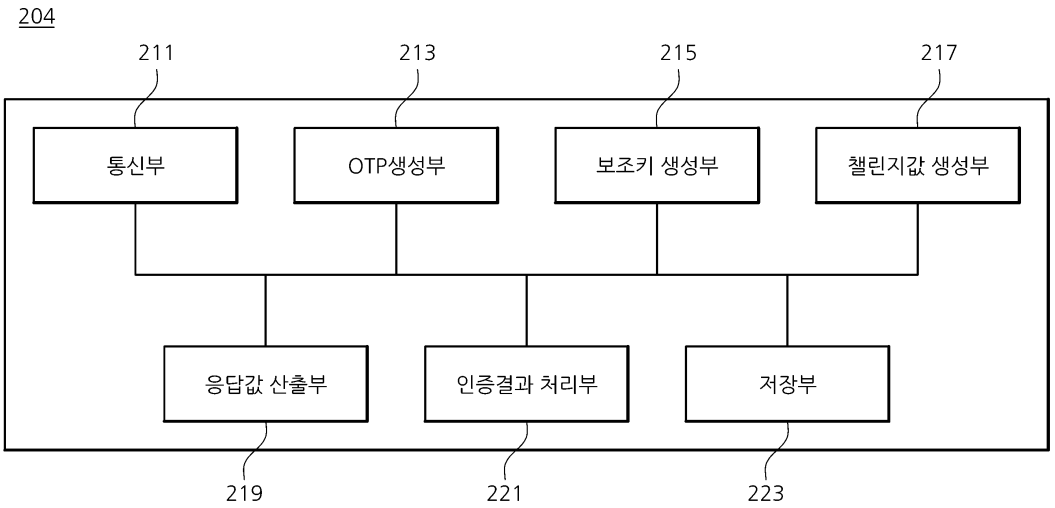
도면2


비밀키(K), OTP코드값(W)
클라이언트
202
비밀키(K), OTP코드값(W)
인증장치
204
S201
제 1 보조키(x) 및 제 2 보조키(y) 생성
(K ⊕ W = xy)
제 1 보조키(x) 및 제 2 보조키(y) 생성
(K ⊕ W = xy)
인증 요청 / 제 2 챌린지 값(b) 전송(S203)
제 1 챌린지 값(a) 전송(S205)
응답값(z) 산출
((a • x) ⊕ (b • y) = z)
X Y
S207
라운드
응답값(z) 전송(S209)
S211
제 1 응답값과 제 2 응답값 비교
제 2 챌린지 값(b') 전송(S213)
제 1 챌린지 값(a') 전송(S215)
라운드 N번 반복

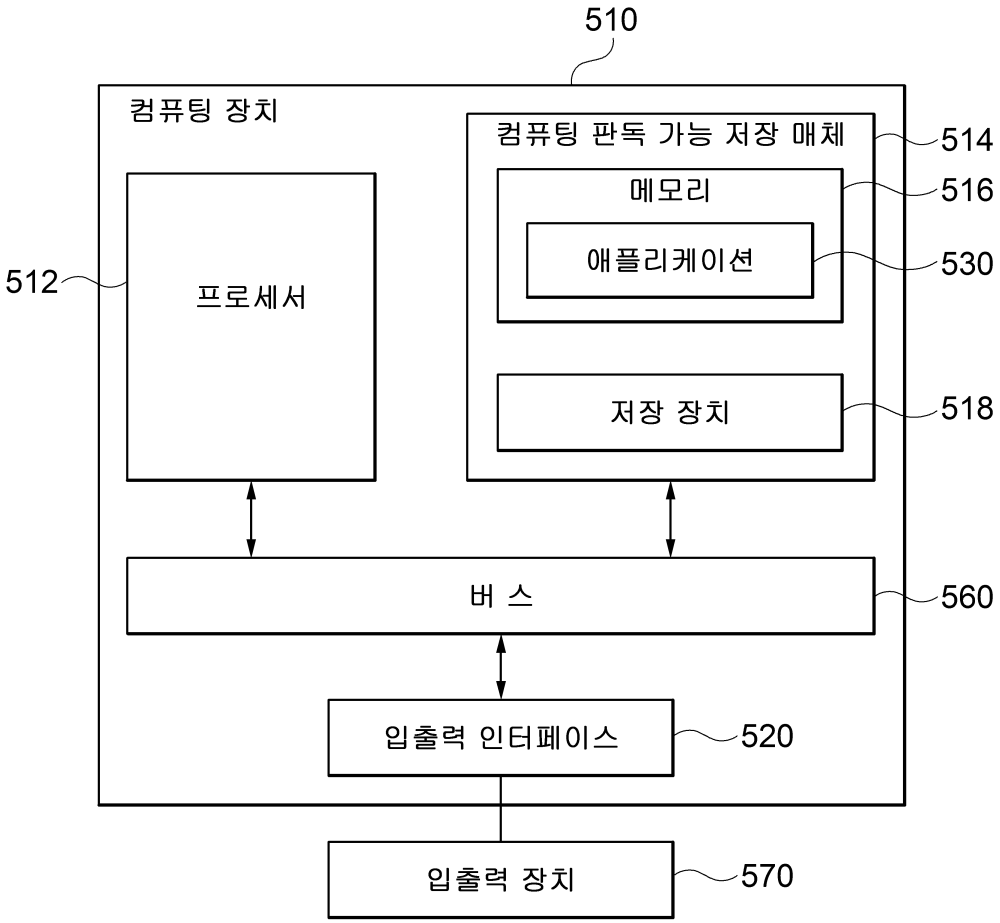
도면3


104
111
113
115
통신부
OTP생성부
챌린지값 생성부
응답값 산출부
인증결과 처리부
저장부
117
119
121

도면4


204
211
213
215
217
통신부
OTP생성부
보조키 생성부
챌린지값 생성부
응답값 산출부
인증결과 처리부
저장부
219
221
223

도면5


500
510
컴퓨팅 장치
컴퓨팅 판독 가능 저장 매체
514
메모리
516
애플리케이션
530
512
프로세서
저장 장치
518
버 스
560
입출력 인터페이스
520
입출력 장치
570