(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2013-0091110
(43) 공개일자 2013년08월16일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 9/08* (2006.01)
(21) 출원번호 10-2012-0012389
(22) 출원일자 2012년02월07일
심사청구일자 없음

(71) 출원인
삼성전자주식회사
경기도 수원시 영통구 삼성로 129 (매탄동)
고려대학교 산학협력단
서울 성북구 안암동5가 1
(72) 발명자
강보경
경기도 수원시 영통구 매탄3동 임광아파트 1동 607호
최규영
서울특별시 강서구 화곡동 377-14
(뒷면에 계속)
(74) 대리인
이건주

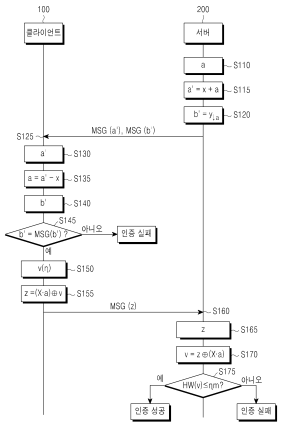
전체 청구항 수 : 총 17 항

(54) 발명의 명칭 **서버 및 클라이언트 간의 인증 방법, 기계로 읽을 수 있는 저장 매체, 클라이언트 및 서버**

(57) 요 약

본 발명의 일 측면에 따른, 서버 및 클라이언트 간의 인증 방법은, 서버 인증 및 응답 값 생성을 위한 제1 블라인딩 값과, 제1 비밀 키를 근거로 생성된 제1 수정된 비밀 키를 포함하는 질의 메시지를 클라이언트로 전송하는 과정과; 상기 클라이언트로부터 상기 제1 블라인딩 값, 제2 비밀 키 및 에러 값을 근거로 생성된 응답 값을 포함하는 응답 메시지를 수신하는 과정과; 상기 응답 값으로부터 상기 에러 값을 산출하는 과정과; 상기 에러 값을 근거로 상기 클라이언트의 인증 성공 여부를 판단하는 과정을 포함한다.

대 표 도 - 도2



(72) 발명자

김효승

서울특별시 성북구 안암동5가 131-5번지 206호

엄지은

서울특별시 서대문구 남가좌2동 현대아파트 102동 102호

이동훈

서울특별시 종로구 내수동 경희궁의 아침 3단지아파트 1404호

이병래

서울특별시 서초구 서초1동 래미안서초유니빌 1115호

특허청구의 범위

청구항 1

서버 및 클라이언트 간의 인증 방법에 있어서,

서버 인증 및 응답 값 생성을 위한 제1 블라인딩 값과, 제1 비밀 키를 근거로 생성된 제1 수정된 비밀 키를 포함하는 질의 메시지를 클라이언트로 전송하는 과정과;

상기 클라이언트로부터 상기 제1 블라인딩 값, 제2 비밀 키 및 에러 값을 근거로 생성된 응답 값을 포함하는 응답 메시지를 수신하는 과정과;

상기 응답 값으로부터 상기 에러 값을 산출하는 과정과;

상기 에러 값을 근거로 상기 클라이언트의 인증 성공 여부를 판단하는 과정을 포함함을 특징으로 하는 서버 및 클라이언트 간의 인증 방법.

청구항 2

제1항에 있어서, 상기 제1 및 제2 비밀 키는 상기 클라이언트 및 서버 간에 공유되어 있음을 특징으로 하는 서버 및 클라이언트 간의 인증 방법.

청구항 3

제1항에 있어서, 상기 클라이언트의 인증 성공 여부를 판단하는 과정은,

상기 에러 값에서 0 또는 1의 개수를 기설정된 임계값과 비교하는 과정과;

상기 비교 결과에 따라 상기 클라이언트의 인증 성공 여부를 판단하는 과정을 포함함을 특징으로 하는 서버 및 클라이언트 간의 인증 방법.

청구항 4

제1항에 있어서, 상기 클라이언트의 인증 성공 여부를 판단하는 과정은,

상기 에러 값의 해밍 웨이트를 기설정된 임계값과 비교하는 과정과;

상기 해밍 웨이트가 상기 임계값 이하인 경우에, 상기 클라이언트의 인증이 성공한 것으로 판단하는 과정을 포함함을 특징으로 하는 서버 및 클라이언트 간의 인증 방법.

청구항 5

제1항에 있어서,

상기 서버 인증을 위해, 상기 제1 블라인딩 값 및 제3 비밀 키를 근거로 생성된 제2 수정된 비밀 키를 상기 클라이언트로 전송하는 과정을 더 포함함을 특징으로 하는 서버 및 클라이언트 간의 인증 방법.

청구항 6

제5항에 있어서,

제2 블라인딩 값을 포함하는 블라인딩 메시지를 상기 클라이언트로부터 수신하는 과정을 더 포함하고,

상기 제2 수정된 비밀 키는 상기 제1 블라인딩 값, 상기 제3 비밀 키 및 상기 제2 블라인딩 값에 근거하여 생성됨을 특징으로 하는 서버 및 클라이언트 간의 인증 방법.

청구항 7

제5항에 있어서, 상기 제1 내지 제3 비밀 키는 상기 클라이언트 및 서버 간에 공유되어 있음을 특징으로 하는 서버 및 클라이언트 간의 인증 방법.

청구항 8

제6항에 있어서,

상기 제1 및 제3 비밀 키, 상기 제1 및 제2 블라인딩 값, 그리고 상기 에러 값은 벡터들이고, 상기 제2 비밀 키는 행렬임을 특징으로 하는 서버 및 클라이언트 간의 인증 방법.

청구항 9

제1항 내지 제8항 중 어느 한 항에 따른 서버 및 클라이언트 간의 인증 방법을 실행하기 위한 프로그램을 기록한 기계로 읽을 수 있는 저장 매체.

청구항 10

제9항의 기계로 읽을 수 있는 저장 매체를 포함하는 서버.

청구항 11

서버 및 클라이언트 간의 인증 방법에 있어서,

서버 인증 및 응답 값 생성을 위한 제1 블라인딩 값과, 제1 비밀 키를 근거로 생성된 제1 수정된 비밀 키를 포함하는 질의 메시지를 상기 서버로부터 수신하는 과정과;

상기 제1 블라인딩 값에 근거하여 상기 서버를 인증하는 과정과;

상기 제1 블라인딩 값, 제2 비밀 키 및 에러 값을 근거로 생성된 응답 값을 포함하는 응답 메시지를 상기 서버로 전송하는 과정을 포함함을 특징으로 하는 서버 및 클라이언트 간의 인증 방법.

청구항 12

제11항에 있어서, 상기 제1 및 제2 비밀 키는 상기 클라이언트 및 서버 간에 공유되어 있음을 특징으로 하는 제한된 리소스를 가진 클라이언트의 인증 방법.

청구항 13

제11항에 있어서,

상기 서버 인증을 위해, 상기 서버로부터 상기 제1 블라인딩 값 및 제3 비밀 키를 근거로 생성된 제2 수정된 비밀 키를 수신하는 과정을 더 포함함을 특징으로 하는 서버 및 클라이언트 간의 인증 방법.

청구항 14

제11항에 있어서, 상기 서버를 인증하는 과정은,

상기 제1 블라인딩 값 및 제3 비밀 키를 근거로 제2 수정된 비밀 키를 생성하는 과정과;

상기 생성된 제2 수정된 비밀 키와 상기 수신된 제2 수정된 비밀 키를 비교하는 과정을 포함함을 특징으로 하는 서버 및 클라이언트 간의 인증 방법.

청구항 15

제14항에 있어서,

상기 제1 및 제3 비밀 키, 상기 제1 및 제2 블라인딩 값, 그리고 상기 에러 값은 벡터들이고, 상기 제2 비밀 키는 행렬임을 특징으로 하는 서버 및 클라이언트 간의 인증 방법.

청구항 16

제11항 내지 제15항 중 어느 한 항에 따른 서버 및 클라이언트 간의 인증 방법을 실행하기 위한 프로그램을 기록한 기계로 읽을 수 있는 저장 매체.

청구항 17

제16항의 기계로 읽을 수 있는 저장 매체를 포함하는 클라이언트.

명 세 서

기 술 분 야

[0001] 본 발명은 경량 인증 기법에 관한 것으로, 특히 제한된 리소스를 가진 장치에서 최소한의 자원(회로, 파워 등)을 이용하는 인증 방법에 관한 것이다.

배 경 기 술

[0002] 인증이란 대상의 진위를 검증하는 것으로, 인증을 받으려는 대상과 인증을 요구하는 대상이 서로 사전에 공유하고 있는 비밀 키를 알고 있는지를 확인하는 것으로 이루어진다. 일반적인 인증 방법으로서, 인증을 요구하는 대상이 질의 값을 보내면 인증을 받으려는 대상이 비밀 키를 이용하여 정당한 응답 값을 생성하고 돌려보냄으로써 비밀 키를 알고 있음을 증명하는 질의-응답(challenge-response) 방식이 사용된다.

[0003] 이러한 질의-응답을 이용한 인증 방법은 크게 공개 키(또는 비대칭 키) 암호 시스템을 사용하는 방법, 비밀 키(또는 대칭 키) 암호 시스템을 사용하는 방법, 해시 함수를 사용하는 방법, 논리 연산을 사용하는 방법으로 구분한다. 하지만, 제한된 리소스를 가지는 장치는 계산 능력, 저장 능력이 매우 낮기 때문에, 대칭 키/공개 키 암호 시스템과 같이 높은 연산량을 요구하는 인증 방법을 사용할 수 없다.

[0004] 제한된 리소스를 가지는 장치 중에서도 특히 RFID(Radio Frequency Identification)는 기존의 바코드 시스템을 대체하여 유통/물류/재고 관리 등의 다양한 서비스를 제공할 수 있는 비접촉형 인식 매체이다. RFID 시스템에서는 리더와 RFID 장치 사이에 비접촉의 RF 통신을 사용하여 메시지를 주고 받게 되며, 리더는 RFID 장치가 정당한지의 여부를 확인하기 위해 인증 방법을 사용하게 된다. 경우에 따라 리더와 RFID 장치의 상호 인증 방법을 사용하기도 한다.

발명의 내용

해결하려는 과제

[0005] 현재 RFID 시스템에 존재하는 다양한 보안 문제 및 사용자의 프라이버시 침해 문제를 해결하기 위해 다양한 경량 인증 방법들이 제안되고 있다. 논리 연산을 이용한 수학적 난제 기반의 인증 방법은 주로 NP-Hard(Nondeterministic Polynomial - Hard) 문제인 LPN(Learning Parity with Noise) 문제의 어려움에 기반을 두고 있기 때문에 이론적인 안전성 증명이 가능하다.

[0006] 그러나 이러한 종래의 논리 연산을 이용한 수학적 난제 기반의 인증 방법은 중간자 공격에 취약하다는 문제점이 있다.

[0007] 본 발명의 특정 실시 예들의 목적은 종래기술과 관련된 문제점들 및/또는 단점들 중의 적어도 하나를 적어도 부분적으로 해결, 경감 또는 제거하는 것이다.

[0008] 본 발명의 일 목적은 종래에 제시되었던 경량 인증 기법에 비하여 중간자 공격에 안전하고, 저장량/연산량/전송량 등의 최소화를 통한 자원 효율성을 제공하며, 수학적 난제에 기반한 안전성 증명이 가능한 인증 방법을 제공함에 있다.

[0009] 본 발명의 다른 목적은 양방향 인증을 통해 인증 시간을 줄일 수 있는 인증 방법을 제공함에 있다.

과제의 해결 수단

[0010] 본 발명의 일 측면에 따른, 서버 및 클라이언트 간의 인증 방법은, 서버 인증 및 응답 값 생성을 위한 제1 블라인딩 값과, 제1 비밀 키를 근거로 생성된 제1 수정된 비밀 키를 포함하는 질의 메시지를 클라이언트로 전송하는 과정과; 상기 클라이언트로부터 상기 제1 블라인딩 값, 제2 비밀 키 및 에러 값을 근거로 생성된 응답 값을 포함하는 응답 메시지를 수신하는 과정과; 상기 응답 값으로부터 상기 에러 값을 산출하는 과정과; 상기 에러 값을 근거로 상기 클라이언트의 인증 성공 여부를 판단하는 과정을 포함한다.

[0011] 본 발명의 다른 측면에 따른, 서버 및 클라이언트 간의 인증 방법은, 서버 인증 및 응답 값 생성을 위한 제1 블라인딩 값과, 제1 비밀 키를 근거로 생성된 제1 수정된 비밀 키를 포함하는 질의 메시지를 상기 서버로부터 수

신하는 과정과; 상기 제1 블라인딩 값에 근거하여 상기 서버를 인증하는 과정과; 상기 제1 블라인딩 값, 제2 비밀 키 및 에러 값을 근거로 생성된 응답 값을 포함하는 응답 메시지를 상기 서버로 전송하는 과정을 포함한다.

[0012] 본 발명의 또 다른 측면에 따라, 서버 및 클라이언트 간의 인증 방법을 실행하기 위한 프로그램을 기록한 기계로 읽을 수 있는 저장 매체가 제공된다.

[0013] 본 발명의 또 다른 측면에 따라, 상기 기계로 읽을 수 있는 저장 매체를 포함하는 서버 또는 클라이언트가 제공된다.

발명의 효과

[0014] 본 발명에 의하면, 제한된 리소스를 가진 장치의 연산 능력 내에서 인증을 수행할 수 있으며, 저장량과 전송량이 적어 경량 장치에 적용할 수 있고, 인증 과정에서 가장 강한 공격으로 알려진 중간자 공격에 대응하여 서버와 클라이언트 간에 서로 안전하게 양방향 인증할 수 있기 때문에, 저가형 RFID 태그와 같은 제한된 리소스를 가진 장치에 안전하게 적용할 수 있다는 이점이 있다.

도면의 간단한 설명

[0015] 도 1은 본 발명의 바람직한 실시 예에 따른 인증 시스템을 나타내는 도면,

도 2는 본 발명의 바람직한 제1 실시 예에 따른 클라이언트 및 서버 간의 인증 방법을 설명하기 위한 도면,

도 3은 본 발명의 바람직한 제2 실시 예에 따른 클라이언트 및 서버 간의 인증 방법을 설명하기 위한 도면,

도 4는 본 발명의 바람직한 제3 실시 예에 따른 클라이언트 및 서버 간의 인증 방법을 설명하기 위한 도면.

발명을 실시하기 위한 구체적인 내용

[0016] 이하 본 발명의 바람직한 실시 예들을 첨부한 도면을 참조하여 상세히 설명한다. 하기 설명에서는 구체적인 구성 소자 등과 같은 특정 사항들이 나타나고 있는데 이는 본 발명의 보다 전반적인 이해를 돕기 위해서 제공된 것일 뿐 이러한 특정 사항들이 본 발명의 범위 내에서 소정의 변형이나 혹은 변경이 이루어질 수 있음은 이 기술분야에서 통상의 지식을 가진 자에게는 자명하다 할 것이다. 또한, 본 발명을 설명함에 있어서 본 발명과 관련된 공지 기술에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에 그 상세한 설명을 생략하기로 한다.

[0017] 이하, 본 발명의 실시 예들에서 제1, 제2 등과 같은 서수를 사용하고 있으나, 이는 단지 동일한 명칭의 대상들을 서로 구분하기 위한 것이고, 그 순서는 임의로 정할 수 있으며, 후 순위의 대상에 대해 선행하는 설명을 준용할 수 있다.

[0018] 도 1은 본 발명의 바람직한 실시 예에 따른 인증 시스템을 나타내는 도면이다. 상기 인증 시스템은 인증을 받는 인증 대상 장치인 클라이언트(100)와, 인증을 제공하는 장치인 서버(200)와, 각각 기설정된 인증 프로세스를 수행하도록 하는 지시들을 포함하는 프로그램들을 제공하는 프로그램 제공 장치(300)를 포함한다.

[0019] 상기 클라이언트(100)는 기설정된 인증 프로세스에 필요한 비밀 키들 등과 같은 정보를 저장하기 위한 제1 메모리(110)와, 상기 서버(200)와의 유선 또는 무선 통신을 수행하기 위한 제1 통신부(120)와, 상기 제1 메모리(110) 및 제1 통신부(120)를 이용하여 상기 서버(200)에 대해 기설정된 인증 프로세스를 수행하는 제1 제어부(130)를 포함한다.

[0020] 상기 서버(200)는 기설정된 인증 프로세스에 필요한 비밀 키들 등과 같은 정보를 저장하기 위한 제2 메모리(210)와, 상기 클라이언트(100)와의 유선 또는 무선 통신을 수행하기 위한 제2 통신부(220)와, 상기 제2 메모리(210) 및 제2 통신부(220)를 이용하여 상기 클라이언트(100)에 대해 기설정된 인증 프로세스를 수행하는 제2 제어부(230)를 포함한다.

[0021] 상기 프로그램 제공 장치(300)는 상기 클라이언트(100) 및/또는 서버(200)가 기설정된 인증 프로세스를 수행하도록 하는 지시들을 포함하는 프로그램, 인증 프로세스에 필요한 정보 등을 저장하기 위한 제3 메모리(310)와, 상기 클라이언트(100) 및/또는 서버(200)와의 유선 또는 무선 통신을 수행하기 위한 제3 통신부(320)와, 상기 클라이언트(100) 및/또는 서버(200)의 요청 또는 자동으로 해당 프로그램을 상기 클라이언트(100) 및/또는 서버(200)로 전송하는 제3 제어부(330)를 포함한다.

[0022] 상기 서버(200)와 클라이언트(100)는 비밀 키들 등과 같은 인증 프로세스에 필요한 정보를 공유하며, 상기 공유

정보는 제1 비밀 키에 해당하는 k 비트의 이진 벡터 x와, 제2 비밀 키에 해당하는 k 비트의 이진 벡터 y와, 제3 비밀 키에 해당하는 (m×k) 크기의 이진 행렬 X와, $0<\eta<1/2$을 만족하는 확률 값인 에러 발생 파라미터 η를 포함한다. 이때, 벡터 및 행렬은 각각 비트 열(bit stream)로 표시될 수 있다. 상기 서버(200)와 클라이언트(100)는 각각 해당 사용자의 요청 또는 자동으로 해당 프로그램 및/또는 인증 프로세스에 필요한 정보를 상기 프로그램 제공 장치(300)로부터 수신할 수 있다.

[0023] 도 2는 본 발명의 바람직한 제1 실시 예에 따른 클라이언트 및 서버 간의 인증 방법을 설명하기 위한 도면이다.

[0024] S110 단계에서, 상기 서버(200)는 블라인딩 벡터(blinding vector)에 해당하는 k 비트의 이진 벡터 $a(\in\{0,1\}^k)$를 생성한다. 이진 벡터(또는 행렬)는 0 또는 1로 이루어진 벡터(또는 행렬)를 말한다. 상기 블라인딩 벡터 a는 상기 클라이언트(100)에 알려지지 않은 벡터이며, 상기 블라인딩 벡터 a를 구성하는 각 비트는 0 및 1의 비트 값들 중에서 랜덤하게 선택될 수 있다. 예를 들어, k=10으로 설정될 수 있고, 상기 블라인딩 벡터 a를 예시하자면 아래와 같다.

수학식 1

[0025] $$a = (0\,1\,1\,0\,1\,0\,1\,0\,1\,0)$$

[0026] S115 단계에서, 상기 서버(200)는 기설정된 제1 함수에 따라 제1 비밀 키 x와 블라인딩 벡터 a를 근거로 k 비트의 제1 수정된 비밀 키 a'를 생성한다. 본 예에서, 상기 제1 함수는 상기 클라이언트(100)에 알려진 제1 비밀 키 x와, 상기 클라이언트(100)에 알려지지 않은 블라인딩 벡터 a를 입력 값들로 하며, 상기 제1 비밀 키 x 및 상기 블라인딩 벡터 a를 가산하여 얻어진 상기 제1 수정된 비밀 키 a'(= x + a)를 출력 값으로 하는 함수이다. 이때, 상기 클라이언트(100) 및 서버(200)는 상기 제1 함수를 공유한다. 이때, 상기 클라이언트(100)가 제1 함수를 공유한다는 의미는 상기 클라이언트(00)가 제1 함수를 알고 있다는 것이며, 상기 클라이언트(100)는 상기 제1 함수 또는 이에 대응하는 제1 역함수를 제1 메모리(110)에 저장하고 있다. 본 예에서 상기 제1 함수로서 가산 함수(즉, 덧셈 함수)를 사용하고 있으나, 상기 제1 함수로서 감산 함수, XOR(exclusive OR) 등 다양한 논리 연산 함수를 사용할 수 있으며, 이는 다른 함수의 경우에도 마찬가지로 적용된다. 이하, 비밀 키와 수정된 비밀 키라는 용어를 사용하고 있으나, 수정된 비밀 키와의 구분을 위해, 상기 비밀 키는 오리지널 비밀 키(original secret key)로 칭할 수도 있다. 상기 제1 비밀 키 x와 제1 수정된 비밀 키 a'를 예시하자면 아래와 같다.

수학식 2

[0027] $$x = (0\,1\,1\,0\,0\,1\,0\,0\,1\,0)$$

수학식 3

[0028] $$\begin{array}{r} 0\,1\,1\,0\,0\,1\,0\,0\,1\,0 \\ +0\,1\,1\,0\,1\,0\,1\,0\,1\,0 \\ \hline a' = 1\,1\,0\,0\,1\,1\,1\,1\,0\,0 \end{array}$$

[0029] S120 단계에서, 상기 서버(200)는 기설정된 제2 함수에 따라 제2 비밀 키 y와 상기 블라인딩 벡터 a를 근거로 k 비트의 제2 수정된 비밀 키 b'를 생성한다. 본 예에서, 상기 제2 함수는 상기 클라이언트(100)에 알려진 제2 비밀 키 y와, 상기 클라이언트(100)에 알려지지 않은 블라인딩 벡터 a를 입력 값들로 하며, 상기 제2 비밀 키 y에서 블라인딩 벡터 a의 비트 값이 1인 위치의 비트들을 추출하여 얻어진 제2 수정된 비밀 키 b'(= $y_{\downarrow a}$)를 출력 값으로 하는 부분 추출 함수이다. 이때, 상기 클라이언트(100) 및 서버(200)는 상기 제2 함수를 공유한다. 즉, 상기 클라이언트(100)는 상기 제2 함수를 제1 메모리(110)에 저장하고 있다. 상기 제2 비밀 키 y 및 제2 수정된 비밀 키 b'를 예시하자면 아래와 같다.

수학식 4

[0030] $$y = (1\,1\,0\,1\,0\,0\,0\,1\,0\,1)$$

수학식 5

[0031] $$b' = y_{\downarrow a} = \begin{array}{r} 1\,1\,0\,1\,0\,0\,0\,1\,0\,1 \\ \underline{0\,1\,1\,0\,1\,0\,1\,0\,1\,0} \\ 1\,0 \quad 0 \quad 0 \quad 0 \end{array}$$

[0032] S125 단계에서, 상기 서버(200)는 상기 제1 수정된 비밀 키 a'를 포함하는 제1 질의 메시지 MSG(a')와 제2 수정된 비밀 키 b'를 포함하는 제2 질의 메시지 MSG(b')를 생성하여 상기 클라이언트(100)로 전송한다. 본 예에서, 2개의 메시지들을 전송하는 것으로 예시하고 있으나, 상기 제1 및 제2 수정된 비밀 키는 하나의 메시지에 포함되어 전송될 수도 있다.

[0033] S130 단계에서, 제1 및 제2 질의 메시지를 수신한 클라이언트(100)는 제1 질의 메시지 MSG(a')로부터 제1 수정된 비밀 키 a'를 추출한다.

[0034] S135 단계에서, 상기 클라이언트(100)는 상기 제1 함수에 대응되는 제1 역함수에 따라 상기 제1 수정된 비밀 키 a'와 제1 비밀 키 x를 근거로 상기 블라인딩 벡터 a를 산출한다. 본 예에서, 상기 제1 역함수는 상기 제1 비밀 키 x 및 상기 제1 수정된 비밀 키 a'를 입력 값들로 하며, 상기 제1 수정된 비밀 키 a'로부터 상기 제1 비밀 키 x를 감산하여 얻어진 상기 블라인딩 벡터 a(=a'-x)를 출력 값으로 하는 감산 함수(즉, 뺄셈 함수)이다. 상기 제1 역함수를 이용하여 상기 블라인딩 벡터 a를 도출하는 식을 예시하자면 아래와 같다.

수학식 6

[0035] $$a = \begin{array}{r} 1\,1\,0\,0\,1\,1\,1\,1\,0\,0 \\ \underline{-\,0\,1\,1\,0\,0\,1\,0\,0\,1\,0} \\ 0\,1\,1\,0\,1\,0\,1\,0\,1\,0 \end{array}$$

[0036] S140 단계에서, 상기 클라이언트(100)는 상기 제2 함수에 따라 상기 블라인딩 벡터 a와 제2 비밀 키 y를 근거로 제2 수정된 비밀 키 b'를 산출(또는 생성)한다.

[0037] S145 단계에서, 상기 클라이언트(100)는 산출된 제2 수정된 비밀 키 b'와 제2 질의 메시지 MSG(b')로부터 추출된 제2 수정된 비밀 키 b'를 비교한다. 산출된 제2 수정된 비밀 키 b'와 추출된 제2 수정된 비밀 키 b'가 동일하면, 상기 서버(200)의 인증이 성공한 것으로 처리하고, 이후의 S150 단계를 수행한다.

[0038] 산출된 제2 수정된 비밀 키 b'와 추출된 제2 수정된 비밀 키 b'가 동일하지 않으면, 상기 서버(200)의 인증이 실패한 것으로 처리하고, 이후의 S150 단계를 수행하지 않는다. 이후의 과정으로서, 상기 클라이언트(100)는 인증 결과를 상기 서버(200)에 전송할 수 있다. 또한, 상기 서버(200)는 모니터와 같은 표시부, 스피커, 프린터 등의 출력부를 구비할 수 있고, 인증 결과를 상기 출력부를 통해 화면, 소리, 인쇄물 등으로 표시할 수 있다. 또는, 상기 클라이언트(100)는 제1 통신부(120)를 통해 인증 결과를 다른 서버, 휴대 단말 등의 통신 단말로 전송할 수도 있다.

[0039] S150 단계에서, 상기 클라이언트(100)는 에러 벡터에 해당하는 m 비트의 이진 벡터 v를 생성한다. $v = \{v_1, v_2, \ldots, v_m\}$이라고 정의할 때, 에러 벡터 v는 $v_i = 1$일 확률이 η인 이진 벡터이다. 에러 벡터 v는 $0<\eta<1/2$를 만족하는 확률 값인 에러 발생 파라미터 η에 따라 그 구성 비트가 결정되는 벡터이다. 전술한 에러 벡터의 비트 수 m과 블라인딩 벡터의 비트 수 k는 각각 자연수이다. 이진 벡터 v는 에러 발생 파라미터 η를 입력 값으로 하

는 랜덤 함수의 출력 값일 수 있으며, v(η)로도 표시할 수 있다. 예를 들어, m=5, η=1/5로 설정될 수 있고, 상기 이진 벡터 v를 예시하자면 아래와 같다.

수학식 7

[0040] $$v = (0\,0\,0\,1\,0)$$

[0041] S155 단계에서, 상기 클라이언트(100)는 기설정된 제3 함수에 따라 제3 비밀 키 X와, 블라인딩 벡터 a와, 에러 벡터 v를 근거로 m 비트의 이진 벡터, 즉 응답 벡터 z를 생성한다. 본 예에서, 상기 제3 함수는 제3 비밀 키 X와, 블라인딩 벡터 a와, 에러 벡터 v를 입력 값들로 하며, 제3 비밀 키 X 및 블라인딩 벡터 a를 내적 연산한 값과, 에러 벡터 v를 배타적 논리합(XOR) 연산하여 얻어진 응답 벡터 z(=$(X \cdot a) \oplus v$)를 출력 값으로 하는 함수이다. 상기 응답 벡터 z를 예시하자면 아래와 같다.

수학식 8

[0042]
$$z = Xa \oplus v$$
$$= \begin{pmatrix} 0&1&1&0&1&1&0&1&0&0 \\ 1&0&1&1&0&1&1&0&1&0 \\ 1&1&0&1&1&0&1&1&0&1 \\ 1&1&1&0&1&1&0&1&1&0 \\ 1&1&1&1&0&1&1&0&1&1 \end{pmatrix} \begin{pmatrix} 0\\1\\1\\0\\1\\0\\1\\0\\1\\0 \end{pmatrix} \oplus \begin{pmatrix} 0\\0\\0\\1\\0 \end{pmatrix}$$
$$= \begin{pmatrix} 1\\1\\1\\0\\0 \end{pmatrix} \oplus \begin{pmatrix} 0\\0\\0\\1\\0 \end{pmatrix} = \begin{pmatrix} 1\\1\\1\\1\\0 \end{pmatrix}$$

[0043] S160 단계에서, 상기 클라이언트(100)는 상기 응답 벡터 z를 포함하는 응답 메시지 MSG(z)를 생성하여 상기 서버(200)로 전송한다.

[0044] S165 단계에서, 상기 서버(200)는 상기 응답 메시지 MSG(z)를 수신하고, 상기 응답 메시지 MSG(z)로부터 상기 응답 벡터 z를 추출한다.

[0045] S170 단계에서, 상기 서버(200)는 상기 제3 함수에 대응되는 제3 역함수에 따라 제3 비밀 키 X와, 블라인딩 벡터 a와, 응답 벡터 z를 근거로 상기 에러 벡터 v를 산출한다. 본 예에서, 상기 제3 역함수는 제3 비밀 키 X와, 블라인딩 벡터 a와, 에러 벡터 v를 입력 값들로 하며, 응답 벡터 z와, 제3 비밀 키 X 및 블라인딩 벡터 a를 내적 연산한 값을 배타적 논리합 연산하여 얻어진 에러 벡터 v(=$z \oplus (X \cdot a)$)를 출력 값으로 하는 함수이다. 상기 제3 역함수를 이용하여 상기 에러 벡터 v를 도출하는 식을 예시하자면 아래와 같다.

수학식 9

$$v = z \oplus Xa = \begin{pmatrix}1\\1\\1\\1\\0\end{pmatrix} \oplus \begin{pmatrix}1\\1\\1\\0\\0\end{pmatrix} = \begin{pmatrix}0\\0\\0\\1\\0\end{pmatrix}$$

[0046]

[0047] S175 단계에서, 상기 서버(200)는 에러 벡터 v의 해밍 웨이트(Hamming weight)를 산출하고, 산출된 해밍 웨이트를 임계값 mq(=m · q)와 비교한다. 이때, q는 1보다 작은 소수로 설정될 수 있으며, 예를 들어 q=1/5로 설정될 수 있다. 상기 해밍 웨이트가 상기 임계값 mq 이하이면, 상기 클라이언트(100)의 인증이 성공한 것으로 처리하고, 상기 해밍 웨이트가 상기 임계값 mq를 초과하면, 상기 클라이언트의 인증이 실패한 것으로 처리한다. 이때, 해밍 웨이트는 에러 벡터 v를 구성하는 비트들 중에서 1의 값을 갖는 비트들의 수를 말한다. 본 예와 다르게, 에러 벡터 v를 구성하는 비트들 중에서 0의 값을 갖는 비트들의 수를 임계값 (에러 벡터 v의 전체 비트 수 - mq)와 비교할 수도 있다. 상기 에러 벡터 v의 해밍 웨이트를 예시하자면 아래와 같다.

수학식 10

$$\mathrm{HW}(v) = HW(0\ 0\ 0\ 1\ 0) = 1 \le \frac{1}{5} \cdot 5$$

[0048]

[0049] 이후의 과정으로서, 상기 서버(200)는 인증 결과를 상기 클라이언트(100)에 전송할 수 있다. 또한, 상기 클라이언트(100)는 모니터와 같은 표시부, 스피커, 프린터 등의 출력부를 구비할 수 있고, 인증 결과를 상기 출력부를 통해 화면, 소리, 인쇄물 등으로 표시할 수 있다. 또는, 상기 서버(200)는 제2 통신부(220)를 통해 인증 결과를 다른 서버, 휴대 단말 등의 통신 단말로 전송할 수도 있다.

[0050] 또한, 상기 클라이언트(100) 및 서버(200)가 비밀 키 및 파라미터를 공유하기 위해서, 상기 클라이언트(100) 및 서버(200)가 각각 프로그램 제공 장치(300)로부터 비밀 키 및 파라미터를 수신하여 저장하는 단계가 S110 단계 이전에 추가될 수도 있다. 또는, 상기 클라이언트(100)가 상기 서버(200)로부터 비밀 키 및 파라미터를 수신할 수도 있고, 그 역의 과정이 수행될 수도 있다.

[0051] 본 발명은, 서버(200)가 블라인딩 벡터를 이용하여 비밀 키를 숨겨서 전송할 뿐 아니라 클라이언트(100) 측에서도 서버(200)를 인증할 수 있도록 한다. 이는 전체 인증 방법의 단계들을 줄이고 안전성을 높이는 장점이 있다.

[0052] 본 실시 예에서는, 클라이언트(100)가 질의 메시지에 포함된 하나의 블라인딩 값에 근거하여 서버(200)를 인증하고, 서버(200)가 응답 메시지에 포함된 응답 값에 근거하여 클라이언트(100)를 인증하는 방법을 예시한다.

[0053] 이하의 제2 실시 예에서는 2 개의 블라인딩 벡터들을 이용한 인증 방법을 예시하고, 제1 실시 예와 중복되는 설명은 생략하기로 한다.

[0054] 도 3은 본 발명의 바람직한 제2 실시 예에 따른 클라이언트 및 서버 간의 인증 방법을 설명하기 위한 도면이다.

[0055] S210 단계에서, 상기 클라이언트(100)는 제2 블라인딩 벡터에 해당하는 k 비트의 이진 벡터 $b(\in\{0,1\}^k)$를 생성한다. 상기 제2 블라인딩 벡터 b는 상기 서버(200)에 알려지지 않은 벡터이며, 상기 제2 블라인딩 벡터 b를 구성하는 각 비트는 0 및 1의 비트 값들 중에서 랜덤하게 선택될 수 있다. 예를 들어, k=10으로 설정될 수 있고, 상기 제2 블라인딩 벡터 b를 예시하자면 아래와 같다.

수학식 11

[0056] $$b = (0\,1\,0\,1\,1\,0\,0\,0\,1\,1)$$

[0057] S215 단계에서, 상기 클라이언트(100)는 상기 제2 블라인딩 벡터 b를 포함하는 블라인딩 메시지 MSG(b)를 생성하여 상기 서버(200)로 전송한다.

[0058] S220 단계에서, 상기 서버(200)는 상기 블라인딩 메시지 MSG(b)를 수신하고, 상기 블라인딩 메시지 MSG(b)로부터 상기 제2 블라인딩 벡터 b를 추출한다.

[0059] S225 단계에서, 상기 서버(200)는 제1 블라인딩 벡터에 해당하는 k 비트의 이진 벡터 a($\in\{0,1\}^k$)를 생성한다. 상기 제1 블라인딩 벡터 a는 상기 클라이언트(200)에 알려지지 않은 벡터이며, 상기 제1 블라인딩 벡터 a를 구성하는 각 비트는 0 및 1의 비트 값들 중에서 랜덤하게 선택될 수 있다. 예를 들어, k=10으로 설정될 수 있고, 상기 제1 블라인딩 벡터 a를 예시하자면 아래와 같다.

수학식 12

[0060] $$a = (0\,1\,1\,0\,1\,0\,1\,0\,1\,0)$$

[0061] S230 단계에서, 상기 서버(200)는 기설정된 제1 함수에 따라 제1 비밀 키 x와 제1 블라인딩 벡터 a를 근거로 k 비트의 제1 수정된 비밀 키 a'를 생성한다. 본 예에서, 상기 제1 함수는 상기 클라이언트(100)에 알려진 제1 비밀 키 x와, 상기 클라이언트(100)에 알려지지 않은 제1 블라인딩 벡터 a를 입력 값들로 하며, 상기 제1 비밀 키 x 및 상기 제1 블라인딩 벡터 a를 가산하여 얻어진 상기 제1 수정된 비밀 키 a'(= x + a)를 출력 값으로 하는 함수이다. 이때, 상기 클라이언트(100) 및 서버(200)는 상기 제1 함수를 공유한다. 상기 제1 비밀 키 x와 제1 수정된 비밀 키 a'를 예시하자면 아래와 같다.

수학식 13

[0062] $$x = (0\,1\,1\,0\,0\,1\,0\,0\,1\,0)$$

수학식 14

[0063] $$\begin{array}{r} 0\,1\,1\,0\,0\,1\,0\,0\,1\,0 \\ +0\,1\,1\,0\,1\,0\,1\,0\,1\,0 \\ \hline a' = 1\,1\,0\,0\,1\,1\,1\,1\,0\,0 \end{array}$$

[0064] S235 단계에서, 상기 서버(200)는 기설정된 제2 함수에 따라 제2 비밀 키 y와 상기 제1 및 제2 블라인딩 벡터 a 및 b를 근거로 k 비트의 제2 수정된 비밀 키 b'를 생성한다. 본 예에서, 상기 제2 함수는 상기 클라이언트(100)에 알려진 제2 비밀 키 y 및 제2 블라인딩 벡터 b와, 상기 클라이언트(100)에 알려지지 않은 블라인딩 벡터 a를 입력 값들로 하며, 제1 및 제2 블라인딩 벡터 a 및 b를 배타적 논리합(XOR) 연산하여 얻어진 선택 벡터(=$a \oplus b$)를 산출하고, 상기 제2 비밀 키 y에서 선택 벡터의 비트 값이 1인 위치의 비트들을 추출하여 얻어진 제2 수정된 비밀 키 b'를 출력 값으로 하는 부분 추출 함수이다. 이때, 상기 클라이언트(100) 및 서버(200)는 상기 제2 함수를 공유한다. 즉, 상기 클라이언트(100)는 상기 제2 함수를 제1 메모리(110)에 저장하고 있다. 상기 선택 벡터 및 제2 수정된 비밀 키 b'를 예시하자면 아래와 같다.

수학식 15

$$\begin{array}{r} 0\,1\,1\,0\,1\,0\,1\,0\,1\,0 \\ \oplus\,0\,1\,0\,1\,1\,0\,0\,0\,1\,1 \\ \hline a \oplus b = 0\,0\,1\,1\,0\,0\,1\,0\,0\,1 \end{array}$$

[0065]

수학식 16

$$b' = y_{\downarrow a \oplus b} = 0101$$

[0066]

[0067] S240 단계에서, 상기 서버(200)는 상기 제1 수정된 비밀 키 a'를 포함하는 제1 질의 메시지 MSG(a')와 제2 수정된 비밀 키 b'를 포함하는 제2 질의 메시지 MSG(b')를 생성하여 상기 클라이언트(100)로 전송한다. 본 예에서, 2개의 메시지들을 전송하는 것으로 예시하고 있으나, 상기 제1 및 제2 수정된 비밀 키는 하나의 메시지에 포함되어 전송될 수도 있다.

[0068] S245 단계에서, 제1 및 제2 질의 메시지를 수신한 클라이언트(100)는 제1 질의 메시지 MSG(a')로부터 제1 수정된 비밀 키 a'를 추출한다.

[0069] S250 단계에서, 상기 클라이언트(100)는 상기 제1 함수에 대응되는 제1 역함수에 따라 상기 제1 수정된 비밀 키 a'와 제1 비밀 키 x를 근거로 상기 블라인딩 벡터 a를 산출한다. 본 예에서, 상기 제1 역함수는 상기 제1 비밀 키 x 및 상기 제1 수정된 비밀 키 a'를 입력 값들로 하며, 상기 제1 수정된 비밀 키 a'로부터 상기 제1 비밀 키 x를 감산하여 얻어진 상기 블라인딩 벡터 a(=a'-x)를 출력 값으로 하는 감산 함수(즉, 뺄셈 함수)이다. 상기 제1 역함수를 이용하여 상기 블라인딩 벡터 a를 도출하는 식을 예시하자면 아래와 같다.

수학식 17

$$\begin{array}{r} 1\,1\,0\,0\,1\,1\,1\,1\,0\,0 \\ -\,0\,1\,1\,0\,0\,1\,0\,0\,1\,0 \\ \hline a = 0\,1\,1\,0\,1\,0\,1\,0\,1\,0 \end{array}$$

[0070]

[0071] S255 단계에서, 상기 클라이언트(100)는 상기 제2 함수에 따라 상기 제1 및 제2 블라인딩 벡터 a 및 b와 제2 비밀 키 y를 근거로 제2 수정된 비밀 키 b'를 산출한다.

[0072] S260 단계에서, 상기 클라이언트(100)는 산출된 제2 수정된 비밀 키 b'와 제2 질의 메시지 MSG(b')로부터 추출된 제2 수정된 비밀 키 b'를 비교한다. 산출된 제2 수정된 비밀 키 b'와 추출된 제2 수정된 비밀 키 b'가 동일하면, 상기 서버(200)의 인증이 성공한 것으로 처리하고, 이후의 S265 단계를 수행한다.

[0073] 산출된 제2 수정된 비밀 키 b'와 추출된 제2 수정된 비밀 키 b'가 동일하지 않으면, 상기 서버(200)의 인증이 실패한 것으로 처리하고, 이후의 S265 단계를 수행하지 않는다. 이후의 과정으로서, 상기 클라이언트(100)는 인증 결과를 상기 서버(200)에 전송할 수 있다.

[0074] 이후의 S265, S270, S275, S280, S285 및 S290 단계들은 제1 실시 예의 S150, S155, S160, S165, S170 및 S175 단계들과 동일하므로, 중복되는 설명은 생략하기로 한다.

[0075] 전술한 실시 예들에서는, 서버(200)가 제1 수정된 비밀 키 외에 서버 인증을 위한 제2 수정된 비밀 키를 전송한다.

[0076] 이하의 제3 실시 예에서는 제1 수정된 비밀 키만을 이용한 인증 방법을 예시하고, 제1 실시 예와 중복되는 설명은 생략하기로 한다.

[0077] 도 4는 본 발명의 바람직한 제3 실시 예에 따른 클라이언트 및 서버 간의 인증 방법을 설명하기 위한 도면이다.

[0078] S310 단계에서, 상기 서버(200)는 블라인딩 벡터에 해당하는 k 비트의 이진 벡터 $a(\in\{0,1\}^k)$를 생성한다. 상기 블라인딩 벡터 a는 상기 클라이언트(100)에 알려지지 않은 벡터이며, 상기 블라인딩 벡터 a를 구성하는 각 비트는 0 및 1의 비트 값들 중에서 랜덤하게 선택될 수 있다.

[0079] S315 단계에서, 상기 서버(200)는 기설정된 제1 함수에 따라 제1 비밀 키 x와 블라인딩 벡터 a를 근거로 k 비트의 수정된 비밀 키 a'를 생성한다. 본 예에서, 상기 제1 함수는 상기 클라이언트(100)에 알려진 제1 비밀 키 x와, 상기 서버(200)에 알려지지 않은 블라인딩 벡터 a를 입력 값들로 하며, 상기 제1 비밀 키 x 및 상기 블라인딩 벡터 a를 가산하여 얻어진 상기 수정된 비밀 키 a'(= x + a)를 출력 값으로 하는 함수이다. 이때, 상기 클라이언트(100) 및 서버(200)는 상기 제1 함수를 공유한다.

[0080] S320 단계에서, 상기 서버(200)는 상기 수정된 비밀 키 a'를 포함하는 질의 메시지 MSG(a')를 생성하여 상기 클라이언트(200)로 전송한다.

[0081] S325 단계에서, 질의 메시지를 수신한 클라이언트(100)는 질의 메시지 MSG(a')로부터 수정된 비밀 키 a'를 추출한다.

[0082] S330 단계에서, 상기 클라이언트(100)는 상기 제1 함수에 대응되는 제1 역함수에 따라 상기 수정된 비밀 키 a'와 제1 비밀 키 x를 근거로 상기 블라인딩 벡터 a를 산출한다. 본 예에서, 상기 제1 역함수는 상기 제1 비밀 키 x 및 상기 수정된 비밀 키 a'를 입력 값들로 하며, 상기 수정된 비밀 키 a'로부터 상기 제1 비밀 키 x를 감산하여 얻어진 상기 블라인딩 벡터 a(=a'-x)를 출력 값으로 하는 감산 함수(즉, 뺄셈 함수)이다.

[0083] S335 단계에서, 상기 클라이언트(100)는 블라인딩 벡터 a에 근거하여 상기 서버를 인증하고, 그 성공 여부를 결정한다.

[0084] 예를 들어, 상기 클라이언트(100)는 이전에 수신한 블라인딩 벡터들의 리스트를 제1 메모리(110)에 저장하고 있고, 상기 클라이언트(100)는 상기 서버(200)로부터 수신한 블라인딩 벡터 a가 상기 리스트에 존재하지 않는 경우에 상기 서버(200)의 인증이 성공한 것으로 결정할 수 있다.

[0085] 또한, 예를 들어, 상기 서버(200) 및 클라이언트(100)는 블라인딩 벡터의 생성 규칙에 대한 정보를 공유할 수 있고, 상기 클라이언트(100)는 상기 서버(200)로부터 수신한 블라인딩 벡터 a가 상기 생성 규칙을 만족하는 경우에 상기 서버(200)의 인증이 성공한 것으로 결정할 수 있다. 예를 들어, 상기 생성 규칙은 블라인딩 벡터의 1~2 번째 비트 값과 마지막 두 비트 값들이 동일하여야 한다는 조건을 포함할 수 있다.

[0086] 또한, 예를 들어, 상기 서버(200) 및 클라이언트(100)는 보안 코드 테이블을 공유할 수 있고, 상기 클라이언트(100)는 상기 서버(200)로부터 수신한 블라인딩 벡터 a가 상기 보안 코드 테이블에 매칭되는 경우에 상기 서버(200)의 인증이 성공한 것으로 결정할 수 있다. 예를 들어, 상기 보안 코드 테이블은 블라인딩 벡터의 1~3번째 비트 값들로 이루어진 제1 보안 코드와 제1 보안 코드와 대응되며 블라인딩 벡터의 마지막 3개의 비트 값들로 이루어진 제2 보안 코드를 포함할 수 있다.

[0087] 상기 서버(200)의 인증이 실패하면, 상기 클라이언트(100)는 이후의 S340 단계를 수행하지 않고, 상기 서버(200)의 인증이 성공하면, 상기 클라이언트(100)는 이후의 S340 단계를 수행한다.

[0088] 이후의 S340, S345, S350, S355, S360 및 S365 단계들은 제1 실시 예의 S150, S155, S160, S165, S170 및 S175 단계들과 동일하므로, 중복되는 설명은 생략하기로 한다.

[0089] 전술한 실시 예들에서, 서버는 리더 장치이고, 클라이언트는 RFID 장치일 수 있다.

[0090] 또한, 전술한 실시 예들에서, 이해의 편이를 벡터, 행렬, 키 등으로 구분하고 있으나, 이들은 모두 값이라는 용어로 대체될 수 있다. 특히, 제1, 제2 등과 같은 서수는 그 대상이 언급되는 순서에 따라 임의대로 지정될 수 있음에 주의하여야 한다.

[0091] 본 발명의 실시 예들은 하드웨어, 소프트웨어 또는 하드웨어 및 소프트웨어의 조합의 형태로 실현 가능하다는 것을 알 수 있을 것이다. 이러한 임의의 소프트웨어는 예를 들어, 삭제 가능 또는 재기록 가능 여부와 상관없이, ROM 등의 저장 장치와 같은 휘발성 또는 비휘발성 저장 장치, 또는 예를 들어, RAM, 메모리 칩, 장치 또는 집적 회로와 같은 메모리, 또는 예를 들어 CD, DVD, 자기 디스크 또는 자기 테이프 등과 같은 광학 또는 자기적으로 기록 가능함과 동시에 기계로 읽을 수 있는 저장 매체에 저장될 수 있다. 메모리는 본 발명의 실시

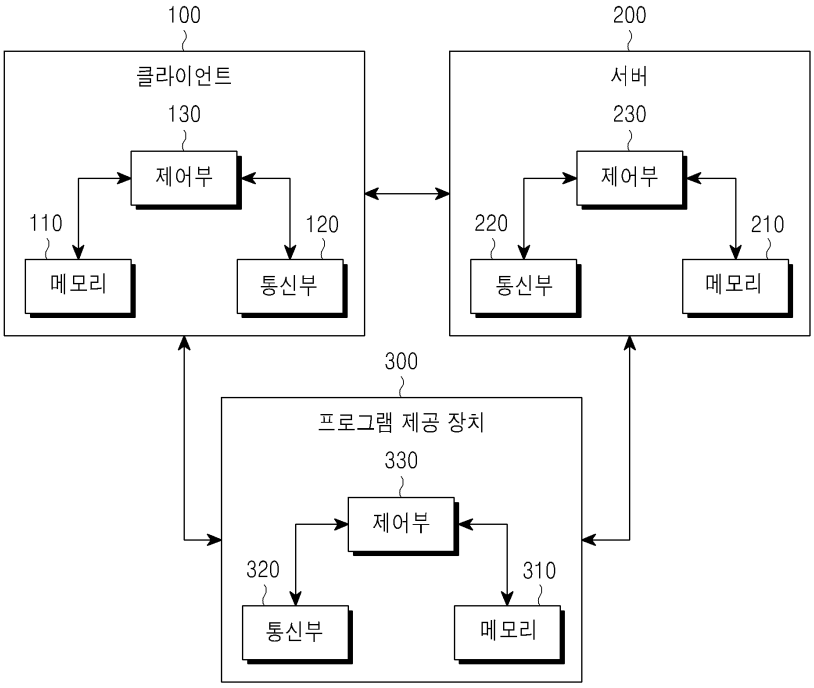
예들을 구현하는 지시들을 포함하는 프로그램 또는 프로그램들을 저장하기에 적합한 기계(예를 들어, 컴퓨터)로 읽을 수 있는 저장 매체의 한 예임을 알 수 있을 것이다. 따라서, 본 발명은 본 명세서의 임의의 청구항에 기재된 방법을 구현하기 위한 코드를 포함하는 프로그램 및 이러한 프로그램을 저장하는 기계로 읽을 수 있는 저장 매체를 포함한다. 또한, 이러한 프로그램은 유선 또는 무선 연결을 통해 전달되는 통신 신호와 같은 임의의 매체를 통해 전자적으로 이송될 수 있고, 본 발명은 이와 균등한 것을 적절하게 포함한다.

부호의 설명

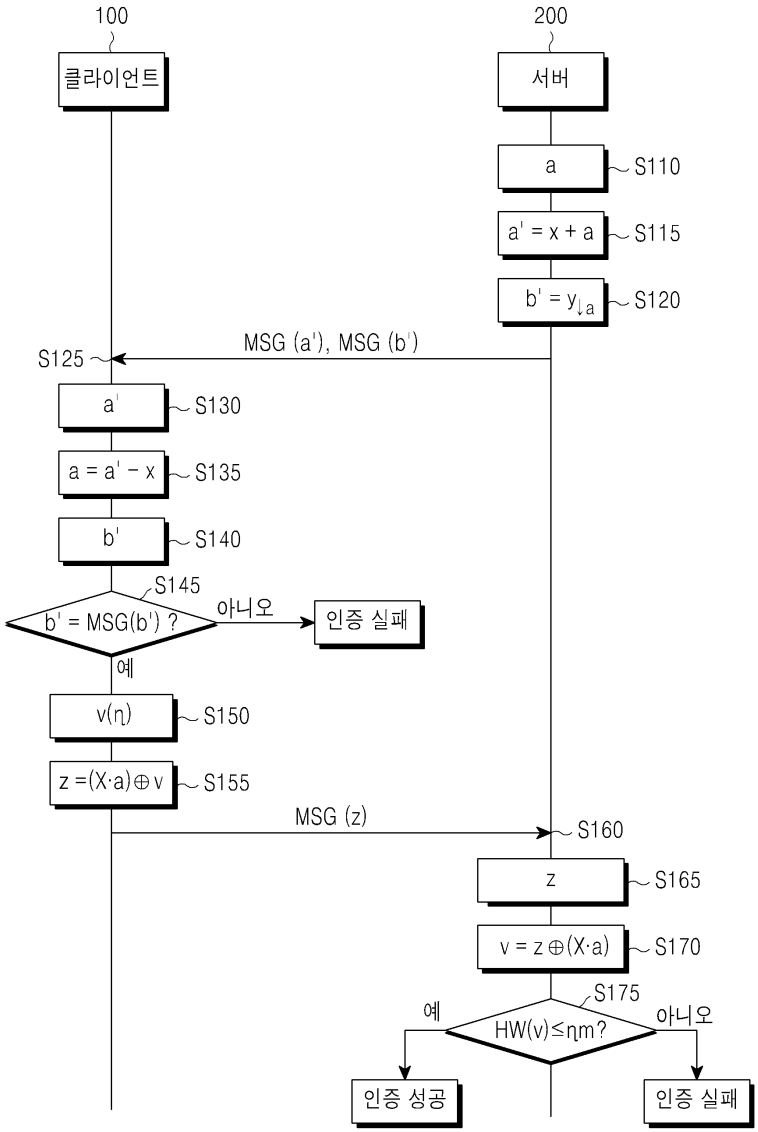
[0092] 100: 클라이언트, 110: 제1 메모리, 120: 제1 통신부, 130: 제1 제어부, 200: 서버, 210: 제2 메모리, 220: 제2 통신부, 230: 제2 제어부, 300: 프로그램 제공 장치, 310: 제3 메모리, 320: 제3 통신부, 330: 제3 제어부

도면

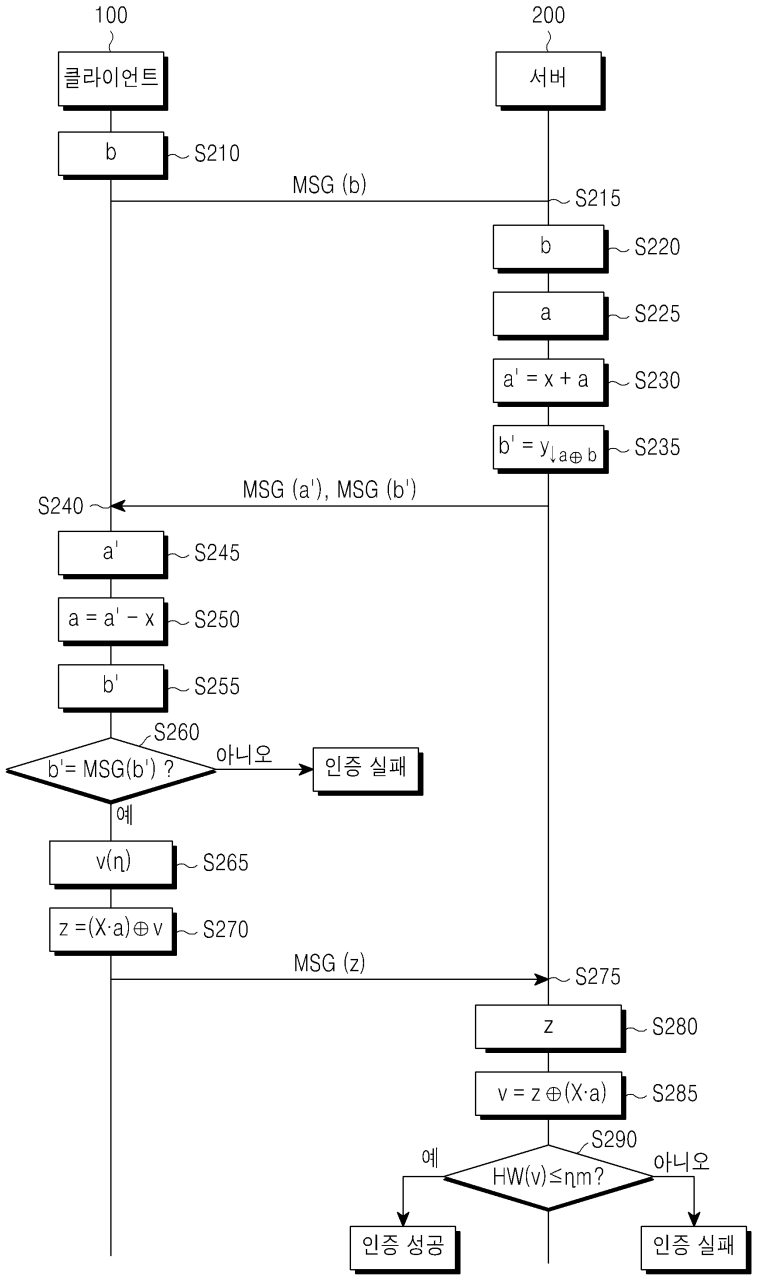
도면1



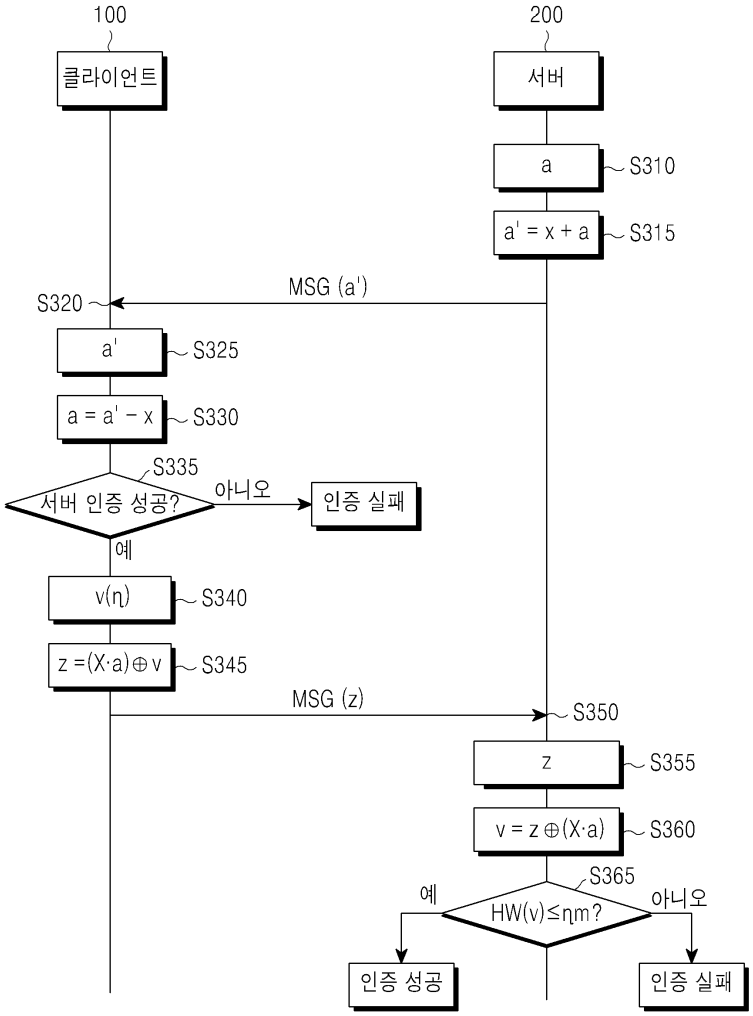
도면2


100
200
클라이언트
서버
a
S110
a' = x + a
S115
b' = y↓a
S120
MSG (a'), MSG (b')
S125
a'
S130
a = a' − x
S135
b'
S140
S145
b' = MSG(b') ?
아니오
인증 실패
예
v(η)
S150
z =(X·a)⊕v
S155
MSG (z)
S160
z
S165
v = z⊕(X·a)
S170
S175
예
HW(v)≤ηm?
아니오
인증 성공
인증 실패

도면3


100
200
클라이언트
서버
b
S210
MSG (b)
S215
b
S220
a
S225
a' = x + a
S230
b' = y↓a⊕b
S235
MSG (a'), MSG (b')
S240
a'
S245
a = a' − x
S250
b'
S255
S260
b'= MSG(b') ?
아니오
인증 실패
예
v(η)
S265
z =(X·a)⊕v
S270
MSG (z)
S275
z
S280
v = z ⊕(X·a)
S285
S290
예
HW(v)≤ηm?
아니오
인증 성공
인증 실패

도면4


100
200
클라이언트
서버
a
S310
a' = x + a
S315
MSG (a')
S320
a'
S325
a = a' − x
S330
S335
서버 인증 성공?
아니오
인증 실패
예
v(η)
S340
z =(X·a)⊕v
S345
MSG (z)
S350
z
S355
v = z ⊕(X·a)
S360
S365
예
HW(v)≤ηm?
아니오
인증 성공
인증 실패