(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.
H04L 9/32 (2006.01)
H04L 9/08 (2006.01)

(45) 공고일자 2006년08월10일
(11) 등록번호 10-0611304
(24) 등록일자 2006년08월03일

(21) 출원번호 10-2005-0007568
(22) 출원일자 2005년01월27일

(65) 공개번호 10-2006-0086679
(43) 공개일자 2006년08월01일

(73) 특허권자 삼성전자주식회사
경기도 수원시 영통구 매탄동 416

(72) 발명자 박성준
서울특별시 동작구 사당동 57-18호 14통 7반

(74) 대리인 정홍식

(56) 선행기술조사문헌
JP2002252882 A
KR1020060032102 A
KR1020030073807 A
US20030097584 A1
* 심사관에 의하여 인용된 문헌

심사관 : 이준석

(54) 기 입력된 버튼의 코드값을 이용하여 1회용 비밀키를생성하는 제어기기, 상기 1회용 비밀키를 이용하여 상기제어기기를 인증하는 홈서버, 및, 상기 1회용 비밀키를이용한 제어기기 인증방법

요약

홈네트워크시스템의 1회용 비밀키(one-time password) 생성방법이 개시된다. 본 방법은, 소정의 사용자 아이디(ID) 및 인증키를 포함한 무선 패킷을 홈서버로 전송하여 제어기기를 홈서버에 등록하는 단계, 제어기기 및 홈서버가 각각 소정의 단방향 함수 세트를 생성하여 저장하는 단계, 제어기기 및 홈서버가 양방향 통신을 수행하여, 제어기기 상에서 입력된 버튼에 대응되는 코드값을 인증하는 단계, 제어기기가 소정 단방향함수를 선택하는 단계, 및, 제어기기가 소정의 제1코드값, 제1코드값이 저장된 메모리부 영역을 가리키는 포인터값 및 선택된 단방향함수를 이용하여 단방향 함수 연산을 수행함으로써, 비밀키를 생성하는 단계를 포함한다. 이에 따라, 별도로 토큰을 구비하거나, 잦은 초기화 작업을 수행할 필요 없이도 1회용 비밀키를 생성하여 사용할 수 있게 된다.

대표도

도 2

색인어

홈네트워크, 홈서버, 제어기기, 단방향 함수, 코드값, 포인터값

명세서

도면의 간단한 설명

도 1은 본 발명의 일실시예에 따른 홈네트워크 시스템의 구성을 나타내는 블럭도,

도 2는 본 발명의 일실시예에 따른 제어기기의 구성을 나타내는 블럭도,

도 3은 본 발명의 일실시예에 따른 홈서버의 구성을 나타내는 블럭도,

도 4는 본 발명의 일실시예에 따른 1회용 비밀키 생성방법을 설명하기 위한 흐름도,

도 5는 본 발명의 일실시예에 따른 제어기기 인증방법을 설명하기 위한 흐름도,

도 6은 홈서버에 제어기기를 등록하는 방법을 설명하기 위한 흐름도,

도 7은 1회용 비밀키 생성을 위해 제어기기로부터 홈서버로 전송하는 데이터 구조를 나타내는 모식도,

도 8은 제어기기 및 홈서버 간에 코드값을 인증하기 위한 과정을 설명하기 위한 모식도,

도 9는 포인터값, 코드값, 및, 단방향함수값을 이용하여 1회용 비밀키를 생성하는 연산과정을 설명하기 위한 모식도, 그리고,

도 10 및 도 11은 본 제어기기인증방법을 이용한 통신과정을 설명하기 위한 모식도이다.

* 도면 주요 부분에 대한 부호의 설명 *

100 : 제어기기 110 : 키입력부

120 : 제어부 130 : 제1 메모리부

140 : 제2 메모리부 150 : 비밀키생성부

160 : 코드값 인증부 170 : 인터페이스부

200 : 홈서버 210 : 서버인터페이스부

220 : 홈서버제어부 230 : 제1 서버 메모리부

240 : 제2 서버 메모리부 250 : 연산부

260 : 인증부 270 : 디스플레이부

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 1회용 비밀키를 생성하는 제어기기, 제어기기에 의해 제어되는 홈네트워크시스템, 1회용 비밀키 생성방법 및, 이를 이용한 제어기기 인증방법에 관한 것이다. 보다 상세하게는 제어기기에 구비된 리모콘 기능 수행 과정에서 입력된 버튼의 코드값을 이용하여 1회용 비밀키를 생성하고, 생성된 비밀키를 생성하는 제어기기, 홈네트워크시스템, 1회용 비밀키 생성방법, 및, 이를 이용한 제어기기 인증방법에 관한 것이다.

전자통신기술의 발달에 힘입어, 가정 내에서 사용되는 여러 기기들을 하나의 네트워크로 구성하여, 통합 제어하는 홈네트워크시스템에 대한 연구가 활발하게 진행되고 있다. 홈네트워크시스템은 적어도 하나의 슬레이브 기기, 및, 이를 제어하는 홈서버(home server)로 구성된다. 사용자는 가정내에서 뿐만 아니라, 외부에서도 소정의 제어기기를 이용하여 홈서버에 접속함으로써, 홈네트워크시스템 전체를 제어할 수 있게 된다. 이 경우, 제어기기는 사용자가 항상 휴대하기 용이한 휴대폰, PDA, 노트북 PC 등이 될 수 있다.

이러한 홈네트워크시스템은 사용자의 편의성을 향상시키기 위해서 개발되고 있으나, 동시에 제3자의 접근이 용이하다는 문제점을 안고 있다. 이를 방지하기 위해서, 사용자는 사용자 아이디 및 패스워드를 입력하여 정당 사용자임을 인증하여야 한다. 하지만, 사용자가 입력한 사용자 아이디 및 패스워드는 무선 패킷 형태로 홈서버로 전송되는 바, 제3자가 스니핑(sniffing) 기술을 이용하여 패스워드 등을 가로챌 여지가 있다. 이 경우, 홈네트워크시스템의 보안 시스템은 무용지물이 되기 때문에 이를 방지하기 위한 보안 유지 기술이 도입되고 있다. 그 중 하나로 1회용 비밀키(One-Time Password : OTP)를 이용하는 기술이 사용될 수 있다.

1회용 비밀키 방식이란, 제어기기 및 홈서버 사이에서 전달되는 비밀키를 매번 변경하여 주는 방식을 의미한다. 즉, 사용자가 동일한 패스워드를 입력하더라도, 매번 상이한 비밀키가 전송되므로, 중간에 제3자가 스니핑하더라도 보안을 유지할 수 있게 된다.

종래에 이러한 1회용 비밀키 방식을 구현하는 기술로는 시간 동기(Time Synchronous)방식 및 단방향 해쉬 함수(One-way Hash function) 방식이 사용되었다. 이 중 시간 동기 방식이란, 토큰(Token)으로부터 생성된 난수 및 사용자가 입력한 개인식별번호를 이용하여 비밀키를 매번 변경하여 주는 방식이다. 하지만, 시간 동기 방식에 따르면, 별도의 토큰 장치가 필요하고 서버와의 시간 동기도 이루어져야 한다는 문제점이 있었다.

한편, 단방향 해쉬 함수 방식은, 입력 데이터 스트링을 고정된 길이의 출력인 해쉬코드로 대응시키는 해쉬 함수를 이용하여 비밀키를 생성하는 방식이다. 해쉬 함수란, 첫째, 해쉬코드가 주어지면 그 해쉬코드를 생성하는 데이터 스트링을 찾아내는 것이 계산상 실행 불가능하다는 점, 둘째, 주어진 데이터 스트링에 대하여 같은 해쉬코드를 생성하는 또 다른 데이터 스트링을 찾아내는 것은 계산상 실행 불가능하다는 점과 같은 두 가지 성질을 만족하는 함수를 말한다

하지만, 단방향 해쉬 함수 방식에 따르면, 인증이 이루어 질 때마다 해쉬 함수의 수가 하나씩 줄어들게 되므로, 어느 시점에 다다르면 수시로 초기화를 시켜줘야 한다는 문제점이 있었다. 특히, 홈네트워크시스템은 그 특성상 사용자의 접속이 자주 이루어지므로, 단방향 해쉬 함수 방식을 사용하기에 어려움이 따르게 된다.

결과적으로, 종래의 1회용 비밀키 방식은 홈네트워크 시스템에 적용하기에 부적합하다는 문제점이 있었다.

발명이 이루고자 하는 기술적 과제

본 발명은 상술한 문제점을 해결하기 위한 것으로, 본 발명의 목적은 홈네트워크시스템을 제어하는 제어기기가 리모콘 기능을 구비한 경우, 리모콘 기능 수행과정에서 입력된 버튼의 코드값 및 단방향함수를 이용하여 1회용 비밀키를 생성함으로써, 시간 동기를 맞추거나 토큰장치를 구비할 필요가 없고, 임의로 초기화를 시켜줄 필요가 없이도 1회용 비밀키를 생성하여 사용함으로써 보안을 유지할 수 있는 제어기기 및 그 1회용 비밀키 생성방법을 제공함에 있다.

본 발명의 또다른 목적은, 제어기기 상에서 입력된 버튼의 코드값 및 단방향함수를 이용하여 1회용 비밀키를 생성하여 제어기기를 인증하는 홈서버, 및, 그 제어기기 인증방법을 제공함에 있다.

발명의 구성 및 작용

이상과 같은 목적을 달성하기 위한 본 발명의 일실시예에 따르면, 적어도 하나의 슬레이브 기기, 상기 슬레이브 기기를 제어하는 홈서버, 및, 상기 홈서버를 제어하기 위한 리모콘 기능을 수행하는 제어기기를 포함하는 홈네트워크에서의 제어기기 인증방법은, (a) 상기 제어기기를 상기 홈서버에 등록하는 단계, (b) 상기 제어기기 및 상기 홈서버가 상기 제어기기의 사용자 아이디 및 상기 제어기기에 대하여 부여된 인증키를 파라미터로 하는 단방향 함수 세트를 생성하여 저장하는 단계, (c) 상기 제어기기 상에서 상기 리모콘 기능을 수행하기 위해 입력한 버튼의 코드값을 상기 제어기기 및 상기 홈서버가 각각 저장하는 단계, (d) 상기 제어기기가 자체 구비된 메모리부 중 소정의 제1 코드값이 저장된 영역을 가리키는 포인터값, 상기 제1 코드값. 및, 상기 단방향 함수 세트 중 소정 넘버의 단방향 함수를 이용한 연산을 수행함으로써 제1비밀키를 생성하는 단계, (e) 상기 제어기기가 상기 포인터값, 상기 단방향함수의 넘버 및 상기 제1비밀키를 상기 홈서버로 전송하여 인

증을 요청하는 단계, (f) 상기 홈서버가 자체 구비된 제1 서버 메모리부 중 상기 포인터값이 가리키는 영역에 저장된 코드값, 상기 포인터값, 및, 상기 단방향함수 넘버에 대응되는 단방향함수를 이용한 연산을 수행함으로써 제2비밀키를 생성하는 단계, 및, (g) 상기 홈서버가 상기 제1비밀키 및 상기 제2비밀키가 일치한다고 판단되면, 상기 제어기기에 대한 인증을 완료하는 단계를 포함한다.

바람직하게는, 상기 (a)단계는, 상기 제어기기가 상기 홈서버로 등록 요청 패킷을 전송하는 단계, 상기 홈서버가 소정의 인증키를 생성한 후, 디스플레이하는 단계, 상기 제어기기의 사용자가 상기 인증키를 입력하면, 상기 제어기기가 상기 인증키의 각 바이트 값을 상기 홈서버로 전송하는 단계, 상기 제어기기 및 상기 홈서버가 각각 상기 인증키를 변환하여 사용자 아이디를 생성하는 단계, 및, 상기 제어기기 및 상기 홈서버가 상기 생성된 사용자 아이디 및 상기 인증키를 각각 저장하는 단계를 포함할 수 있다.

또한 바람직하게는, 상기 (a)단계는, 상기 제어기기가 상기 홈서버로 등록 요청 패킷을 전송하는 단계, 상기 홈서버가 소정의 인증키를 생성한 후, 상기 제어기기로 전송하는 단계, 상기 제어기기의 사용자가 상기 인증키를 입력하면, 상기 제어기기가 상기 인증키의 각 바이트값을 상기 홈서버로 전송하는 단계, 상기 제어기기 및 상기 홈서버가 각각 상기 인증키를 변환하여 사용자 아이디를 생성하는 단계, 및, 상기 제어기기 및 상기 홈서버가 상기 사용자 아이디 및 상기 인증키를 각각 저장하는 단계를 포함할 수도 있다.

이러한 경우, 상기 (c)단계는, 상기 제어기기가 상기 코드값, 상기 코드값이 저장될 메모리부 영역을 가리키는 포인터값, 및, 상기 인증키를 이용하여 소정 연산을 수행한 후, 상기 연산값을 상기 홈서버로 전송하는 단계, 상기 홈서버가 상기 전송된 연산값 및 상기 인증키를 이용하여 상기 코드값을 확인한 후, 소정의 응답 패킷을 전송하는 단계, 상기 제어기기가 상기 응답패킷을 수신하면, 상기 홈서버가 상기 코드값을 정상 수신하였다고 판단하고, 상기 코드값을 상기 메모리부 영역에 저장하는 단계, 및, 상기 홈서버가 상기 제1 서버 메모리부의 소정 영역에 상기 확인된 코드값을 저장하는 단계를 포함할 수 있다.

또는, 상기 (c)단계는, 상기 제어기기가 상기 인증키의 첫번째 값 및 상기 코드값을 이용하여 소정의 제1연산을 수행한 후, 제1연산결과값을 상기 홈서버로 전송하는 단계, 상기 홈서버가 상기 제1연산결과값에 의해 확인된 코드값 및 상기 인증키의 두번째 값을 이용하여 소정의 제2연산을 수행한 후, 제2연산결과값을 상기 제어기기로 전송하는 단계, 상기 제어기기가 상기 인증키의 두번째 값을 이용하여 상기 제2연산결과값으로부터 상기 코드값을 확인한 후, 인증하는 단계, 상기 제어기기가 상기 인증된 코드값 및 상기 인증키의 세번째 값을 이용하여 소정의 제3연산을 수행한 후, 제3연산결과값을 상기 홈서버로 전송하는 단계, 상기 홈서버가 상기 인증키의 세번째 값을 이용하여 상기 제3연산결과값으로부터 상기 코드값을 확인한 후, 인증하고 저장하는 단계, 상기 홈서버가 상기 인증된 코드값 및 상기 인증키의 네번째 값을 이용하여 소정의 제4연산을 수행한 후, 제4연산결과값을 상기 제어기기로 전송하는 단계, 및, 상기 제어기기가 상기 인증키의 네번째 값을 이용하여 상기 제4연산결과값을 확인한 후, 인증을 완료하고 상기 코드값을 저장하는 단계를 포함할 수도 있다.

보다 바람직하게는, 상기 (c)단계는, 상기 홈서버 및 상기 제어기기가 상기 메모리부의 포인터값 및 상기 제1 서버 메모리부의 포인터값을 동기화시키는 단계, 및, 상기 홈서버가 상기 제어기기로부터 전송된 포인터값이 가리키는 제1 서버 메모리부 영역에 상기 확인된 코드값을 저장하는 단계를 포함할 수도 있다.

한편, 본 발명의 일실시예에 따르면, 적어도 하나의 슬레이브 기기, 및, 상기 슬레이브 기기를 제어하는 홈서버를 포함하는 홈네트워크를 제어하는 제어기기는, 상기 홈서버와의 사이에서 데이터를 송수신하는 인터페이스부, 상기 홈서버를 제어하기 위한 소정의 버튼을 구비하며, 상기 버튼 중 선택된 버튼에 대응되는 코드값을 출력하는 키입력부, 상기 키입력부로부터 출력되는 코드값을 상기 홈서버로 전송하여, 인증하는 코드값 인증부, 상기 코드값 인증부에 의해 인증된 코드값을 소정 영역에 저장하는 제1 메모리부, 소정의 단방향 함수 세트가 저장되는 제2 메모리부, 상기 제1 메모리부 중 소정의 제1 코드값이 저장된 영역을 가리키는 포인터값 및 상기 제1 코드값과, 상기 단방향 함수 세트 중 선택된 소정 단방향함수를 이용하여 1회용 비밀키를 생성하는 비밀키생성부, 및, 상기 포인터값, 상기 단방향함수의 넘버, 및, 상기 1회용 비밀키를 포함한 패킷을 생성한 후, 상기 생성된 패킷을 상기 인터페이스부를 통해 상기 홈서버로 전송하여 인증을 요청하는 제어부를 포함한다.

바람직하게는, 상기 제어부는, 상기 키입력부를 통해 소정의 인증키가 입력되면 상기 인증키를 변환하여 소정의 사용자 아이디를 생성한 후, 상기 인증키 및 상기 사용자 아이디를 상기 제2 메모리부에 저장할 수 있다.

또한 바람직하게는, 상기 제어부는, 상기 키입력부를 통해 입력된 인증키의 각 바이트값을 상기 인터페이스부를 통해서 상기 홈서버로 전송함으로써, 상기 홈서버가 상기 인증키를 상기 사용자 아이디로 변환한 후, 등록하도록 할 수도 있다.

한편, 상기 제어부는, 상기 등록이 이루어지면, 복수개의 단방향함수를 포함한 단방향 함수 세트를 생성하여 상기 제2 메모리부에 저장하는 것이 바람직하다.

또한 바람직하게는, 상기 코드값 인증부는, 상기 코드값 및 상기 인증키를 이용한 소정 연산을 수행하여 상기 연산결과값을 상기 인터페이스부를 통해 상기 홈서버로 전송한 후, 상기 홈서버로부터 전송되는 응답패킷에 기록된 코드값이 상기 코드값과 동일하면, 상기 코드값을 인증할 수 있다.

한편, 본 발명의 일실시예에 따르면, 소정의 제어기기 및 적어도 하나의 슬레이브 기기를 포함한 홈네트워크 상에서 상기 제어기기의 제어에 따라 상기 슬레이브 기기를 제어하는 홈서버는, 상기 제어기기로부터 메모리부 영역을 지정하는 포인터값, 소정의 단방향함수 넘버, 및, 제1 비밀키를 수신하는 서버 인터페이스부, 상기 제어기기 상에서 입력된 버튼에 대응되는 코드값이 저장된 제1 서버 메모리부, 소정의 단방향함수 세트가 저장되는 제2 서버 메모리부, 상기 제1 서버 메모리부 영역 중 상기 포인터값에 의해 지정된 영역에 저장된 코드값, 상기 포인터값, 및, 상기 단방향함수 세트 중 상기 단방향함수 넘버에 대응되는 단방향함수를 이용하여 제2 비밀키를 연산하는 연산부, 및, 상기 제1 비밀키 및 상기 제2 비밀키가 일치하면 상기 제어기기를 인증하는 홈서버 제어부를 포함한다.

바람직하게는, 상기 홈서버 제어부는, 상기 제어기기로부터 수신된 포인터값 및 상기 제1 서버 메모리부의 포인터값을 동기화할 수 있다.

또한 바람직하게는, 소정 데이터를 디스플레이하는 디스플레이부를 더 포함할 수 있다. 이 경우, 상기 홈서버 제어부는, 상기 제어기기로부터 등록 요청 패킷이 수신되면 상기 제어기기에 대한 인증키를 생성한 후, 상기 디스플레이부를 제어하여 상기 인증키를 디스플레이할 수 있다.

한편, 상기 홈서버 제어부는, 상기 제어기기로부터 상기 인증키가 전송되면 상기 전송된 인증키를 변환하여 사용자 아이디를 생성하고, 상기 사용자 아이디 및 상기 인증키를 파라미터로 하는 상기 단방향함수세트를 생성한 후, 상기 사용자 아이디, 상기 인증키 및 상기 단방향함수세트를 상기 제2 서버 메모리에 저장할 수 있다.

보다 바람직하게는, 본 홈서버는, 상기 인증키를 이용하여 상기 제어기기가 전송한 코드값을 인증하는 인증부;를 더 포함할 수 있다. 이 경우, 상기 홈서버 제어부는, 상기 인증부에 의해 인증된 코드값을 상기 제1 서버 메모리부에 저장할 수 있다.

이하에서, 첨부된 도면을 참조하여 본 발명에 대하여 자세하게 설명한다.

도 1은 본 발명의 일실시예에 따른 홈네트워크 시스템의 구성을 나타내는 블럭도이다. 도 1에 따르면, 홈네트워크 시스템은 제어기기(100), 홈서버(200), 및, 적어도 하나 이상의 슬레이브 기기(310, 320,..., n)를 포함한다.

제1 내지 제n 슬레이브 기기(310, 320,..., n)는 PC, DVD 플레이어, TV, 보일러, 에어컨, 전등, 냉장고, 전열기기 등과 같은 다양한 종류의 기기가 될 수 있다. 홈서버(200)는 외부에 존재하는 임의의 노드와 데이터를 송수신할 수 있는 장치로써, 별도의 서버(server)로 구현되거나, 가전기기 중 하나에 구현될 수 있다. 본 실시예에서 홈서버(200)는 TV로 구현되는 것이 바람직하다.

한편, 제어기기(100)는 외부에서도 홈서버(200)에 접속할 수 있는 통신 기능을 구비한 장치를 의미한다. 특히, 제어기기(100)는 홈네트워크시스템 내부의 각종 가전장치의 동작을 직접 제어하는 리모콘 기능을 구비한다. 제어기기(100)는 리모콘 기능 수행 과정에서 입력된 버튼의 코드값을 내부 메모리부의 각 레지스터에 순차적으로 저장하여 둔다. 또한, 제어기기(100)는 홈서버(200)로 각 코드값을 전송하여 줌으로써, 홈서버(200)와 코드값을 공유하게 된다. 이 경우, 코드값 유출을 방지하기 위해서 임의의 인증키를 이용하여 코드값을 암호화하여 전송하는 것이 바람직하다.

한편, 제어기기(100)가 홈서버(200)에 접속하기 위해서는, 제어기기(100)에 대한 인증이 이루어져야 한다. 이를 위해, 제어기기(100)는 홈서버(200)에 사전에 등록 되어 있어야 한다. 등록이 이루어지면, 제어기기(100) 및 홈서버(200)는 사용자 아이디, 인증키, 커스텀 코드(costom code) 등을 파라미터로 하는 단방향함수세트를 생성한다. 커스텀 코드는 홈서버(200)의 제조회사 등에서 부여한 고유코드를 의미한다. 구체적인 등록과정에 대한 설명은 후술한다.

이에 따라, 제어기기(100)는 기 입력되었던 버튼의 코드값 및, 상술한 단방향함수세트 중 하나의 단방향함수를 이용하여 연산을 수행함으로써 1회용 비밀키(이하, 제1 비밀키)를 생성할 수 있다.

한편, 홈서버(200)도 제어기기(100)로부터 기 전송되었던 코드값 및 단방향함수를 이용하여 1회용 비밀키(이하, 제2비밀키)를 생성할 수 있다. 이에 따라, 제1 및 제2비밀키의 일치여부를 확인하여 일치한다면, 제어기기(100)가 정당한 것이라고 인증하게 된다. 이 경우, 코드값 및 단방향함수 중 하나가 순차적으로 변하게 되므로, 매 인증시마다 제1 및 제2비밀키가 변경되게 된다. 또한, 사용자가 제어기기(100)에 구비된 버튼을 누를 때마다 내부 메모리부의 각 레지스터에 저장된 값이 수시로 변경되므로, 별도로 초기화를 하지 않더라도 매번 상이한 비밀키를 생성하여 사용할 수 있게 된다.

도 2는 본 발명의 일실시예에 따른 제어기기(100)의 구성을 나타내는 블럭도이다. 도 2에 따르면, 본 제어기기(100)는 키입력부(110), 제어부(120), 제1 메모리부(130), 제2 메모리부(140), 비밀키생성부(150), 코드값인증부(160), 및, 인터페이스부(170)를 포함한다.

키입력부(110)는 제어기기(100) 본체에 구비된 각종 버튼이 입력되면, 입력된 버튼에 대응되는 코드값(code value)을 제어부(120)로 출력한다.

제어부(120)는 키입력부(110)를 통해 입력받은 코드값을 제1 메모리부(130) 상의 소정 영역에 저장한다. 이 경우, 제어부(120)는 홈서버(200)와의 사이에서 인증이 완료된 코드값만을 제1 메모리부(130)에 저장하는 것이 바람직하다.

한편, 제어부(120)는 홈서버(200)에 대한 등록이 이루어지면, 사용자 아이디, 인증키, 및, 커스텀 코드 등을 파라미터(parameter)로 하는 복수개의 단방향함수 체인(hash function chain)으로 이루어진 단방향함수세트를 생성한다. 제2 메모리부(140)는 생성된 단방향함수세트가 저장되는 영역이다. 홈서버(200)에 등록하는 과정 및 사용자아이디 생성과정에 대한 설명은 후술한다.

비밀키생성부(150)는 단방향함수세트 상의 단방향함수를 순차적으로 선택하게 된다. 이에 따라, 제1 메모리부(130)에 저장된 코드값, 코드값이 저장된 제1 메모리부(130) 주소를 가리키는 포인터값, 및, 선택된 단방향함수를 이용하여 단방향함수 연산을 수행함으로써 제1 비밀키를 생성한다.

한편, 코드값인증부(160)는 키입력부(110)를 통해 입력받은 코드값을 홈서버(200)와의 사이에서 인증하는 역할을 한다. 즉, 코드값인증부(160)는 사전 등록된 인증키의 각 비트 및 코드값을 이용한 소정 연산을 수행하여, 그 연산 결과값을 홈서버(200)로 전송한다. 홈서버(200)와의 데이터 송수신 작업은 인터페이스부(170)를 통해 이루어진다. 이에 따라, 홈서버(200)가 전송된 연산 결과값으로부터 코드값을 확인하면, 소정의 응답패킷을 전송한다. 코드값인증부(160)는 응답 패킷 내에 포함된 코드값을 확인하여 전송시와 동일한 코드값이라면 인증을 완료하게 된다. 한편, 홈서버(200)도 확인된 코드값 및 인증키의 각 비트값을 이용한 연산을 수행한 후, 연산 결과값을 응답패킷에 기록하여 제어기기(100)로 전송할 수 있다. 또한, 코드값 인증 작업은 인증키의 비트크기에 따라 소정 회수 이상 이루어 질 수 있다. 이에 대한 구체적인 설명은 후술한다.

한편, 제어부(120)는 비밀키생성부(150)에 의해 제1 비밀키가 생성되면, 제1 비밀키 생성과정에서 사용된 단방향함수를 지정하는 단방향함수 넘버, 제1 비밀키 생성과정에서 사용된 포인터값, 및, 제1 비밀키를 포함한 패킷을 생성한다. 이에 따라, 생성된 패킷을 인터페이스부(170)를 통해 홈서버(200)로 전송하여 인증을 요청하게 된다.

도 3은 본 발명의 일실시예에 따른 홈서버(200)의 구성을 나타내는 블럭도이다. 도 3에 따르면, 본 홈서버(200)는 서버인터페이스부(210), 홈서버제어부(220), 제1 서버 메모리부(230), 제2 서버 메모리부(240), 연산부(250), 인증부(260), 및, 디스플레이부(270)를 포함한다.

서버인터페이스부(210)는 제어기기(100)와의 사이에서 데이터를 송수신하는 역할을 수행한다.

인증부(260)는 서버인터페이스부(210)를 통해서 입력되는 코드값을 인증하는 역할을 수행한다. 즉, 제어기기(100)로부터 코드값 및 인증키의 연산 결과값이 수신되면, 인증키를 이용하여 연산결과값으로부터 코드값을 독출한다. 이에 따라, 독출된 코드값 및 인증키를 이용한 연산을 수행하여 응답패킷을 생성한다. 상술한 제어기기(100)의 코드값인증부(160) 및 홈서버(200)의 인증부(260)는 배타적 논리합(eXclusive OR : XOR) 연산을 이용하여 코드값 및 인증키를 연산하는 것이 바람직하다.

한편, 인증키는 제어기기(100)의 등록 과정에서 홈서버 제어부(220)에 의해 부여되는 값이다. 즉, 홈서버 제어부(220)는 제어기기(100)로부터 등록 요청 패킷이 전송되면, 인증키를 생성한 후 디스플레이부(270)를 통해 디스플레이한다. 제어기

기(100)의 사용자는 디스플레이된 인증키를 확인한 후, 제어기기(100)를 통해 입력한다. 제어기기(100)는 입력된 인증키를 자동변환하여 사용자 아이디를 생성한다. 이에 따라 생성된 사용자 아이디 및 인증키는 제2 서버 메모리부(240)에 저장된다. 실시예에 따라서, 홈서버 제어부(220)는 생성된 인증키를 제어기기(100)로 직접 전송하여 줄 수도 있다.

제1 서버 메모리부(230)는 인증부(260)에 의해 인증이 완료된 코드값만을 저장한다. 이 경우, 홈서버 제어부(220)는 제어기기(100)로부터 전송된 패킷에 기록된 포인터값에 기준하여 제1 서버 메모리부(230)의 포인터값을 동기화(syncronous)시킨다. 동기화 작업을 수행하기 위해서, 홈서버제어부(220)는 제어기기(100)로부터 전송된 포인터값을 확인한다. 이에 따라, 전송된 포인터값이 제1 서버 메모리부(230)의 현재 포인터값보다 크다면, 현재 포인터값을 제어기기(100)로 통지한다. 한편, 전송된 포인터값이 제1 서버 메모리부(230)의 현재 포인터값보다 작다면, 제1 서버 메모리부(230)의 현재 포인터값을 전송된 포인터값으로 조정한 후, 조정된 포인터값을 제어기기(100)로 통지한다. 제어기기(100)는 홈서버제어부(220)로부터 전송된 포인터값을 확인하여 조정된 포인터값을 다시 홈서버(200)로 전송함으로써, 양측이 포인터값을 동기화하였음을 확인할 수 있도록 한다.

한편, 홈서버제어부(220)는 제어기기(100)가 등록되면, 사용자 아이디, 인증키, 및, 커스텀 코드 등을 파라미터로 하는 단방향함수세트를 생성한다. 생성된 단방향함수세트는 제2 서버 메모리부(240)에 저장된다.

연산부(250)는 제어기기(100)로부터 소정의 포인터값, 단방향함수 넘버, 및, 1회용 비밀키(이하, 제1 비밀키)가 전송되면, 전송된 포인터값을 이용하여 제1 서버 메모리부(230)로부터 코드값을 독출한다. 또한, 전송된 단방향함수 넘버에 대응되는 단방향함수를 제2 서버 메모리부(240)에 저장된 단방향함수세트로부터 선택한다. 이에 따라, 연산부(250)는 독출된 코드값, 포인터값, 및 단방향함수를 이용하여 단방향함수연산을 수행함으로써 제2 비밀키를 생성하게 된다.

홈서버제어부(220)는 연산부(250)에서 연산한 제2 비밀키와 제어기기(100)로부터 전송된 제1 비밀키를 비교하여 일치여부를 확인한다. 그 결과, 일치한다면 제어기기(100)에 대한 인증을 완료하게 된다.

도 4는 본 발명의 일실시예에 따른 제어기기(100)의 1회용 비밀키 생성방법을 설명하기 위한 흐름도이다. 도 4에 따르면, 제어기기(100)는 먼저 홈서버(200)로부터 인증키를 부여받아 등록하게 된다(S410). 등록방법에 대해서는 후술한다.

이에 따라, 제어기기(100) 및 홈서버(200) 각각은 등록된 사용자 아이디, 인증키, 및, 커스텀 코드를 입력 파라미터로 하는 단방향함수세트를 생성한 후, 저장한다(S420).

한편, 리모콘 기능을 수행하거나, 기타 다른 목적으로 제어기기(100)상의 소정 버튼을 선택하였다면, 선택된 버튼의 코드값을 홈서버(200)와의 사이에서 상호 인증한 후, 저장한다(S430). 인증 방법에 대해서는 후술한다.

이러한 상태에서, 제어기기(100)의 사용자가 홈네트워크시스템을 원격제어하기 위해서 홈서버(100)에 접속을 시도한다면, 먼저 인증을 요청하여야 한다.

이를 위해서, 제어기기(100)는 코드값, 제1 메모리부(130)상에 코드값이 저장된 영역을 가리키는 포인터값, 및 소정의 단방향함수를 이용한 단방향을 수행함으로써 제1 비밀키를 생성한다(S440). 생성된 제1 비밀키는 홈서버(200)와의 사이에서의 인증 과정에 사용된다.

도 5는 본 발명의 일실시예에 따른 홈네트워크시스템에서의 제어기기(100) 인증방법을 설명하기 위한 흐름도이다. 도 5에 따르면, 제어기기(100)가 등록되면(S510), 제어기기(100) 상에 입력되는 버튼의 코드값을 양방향 통신 방법을 통해 인증하게 된다(S520). 이에 따라, 인증된 코드값은 제어기기(100) 및 홈서버(200)가 각각 저장한다(S530).

다음으로, 제어기기(100)는 코드값, 코드값 저장영역을 지정하는 포인터값, 및, 단방향함수를 이용하여 제1비밀키를 생성한다(S540). 이에 따라, 포인터값, 단방향함수넘버, 및, 제1 비밀키를 홈서버(200)로 전송하여 인증을 요청한다(S550).

홈서버(200)는 전송된 포인터값을 확인하여, 제1 서버 메모리부(230)에 저장된 코드값을 독출한다. 또한, 단방향함수넘버를 확인하여 기 생성한 단방향함수세트 중 하나의 단방향함수를 선택한다. 이에 따라, 코드값, 포인터값, 단방향함수를 이용하여 제2 비밀키를 생성하게 된다(S560).

이에 따라, 홈서버(200)는 생성된 제2비밀키 및 수신한 제1비밀키를 비교하여 일치여부를 확인한 후(S570), 일치하다면 해당 제어기기(100)를 인증하게 된다(S580). 인증이 이루어지면, 제어기기(100)는 소정의 프로토콜을 이용하여 홈서버(200)로 제어신호를 전송함으로써 홈네트워크 시스템을 제어할 수 있게 된다.

도 6은 제어기기(100)를 등록하는 방법을 설명하기 위한 흐름도이다. 도 6에 따르면, 제어기기(100)에서 소정의 등록 요청 패킷을 전송하면(S610), 홈서버(200)는 임의의 인증키를 생성하여 디스플레이부(270)를 통해 디스플레이하게 된다(S620). 이 경우, 제어기기(100)에 디스플레이 소자가 구비되었다면, 홈서버(200)에서 인증키를 제어기기(100)로 전송하여 줄 수도 있다. 하지만, 제3자의 도청 위험이 있는 바, 디스플레이부(270)를 통해 직접 확인할 수 있도록 하는 것이 바람직하다.

제어기기(100)의 사용자는 디스플레이된 인증키를 입력하게 된다(S630). 제어기기(100)는 인증키를 자동변환하여 사용자 아이디를 생성한 후, 저장한다(S640). 이 경우, 인증키에 대해서 비트단위 XOR(bitwise eXclusive OR) 연산을 수행함으로써 사용자 아이디를 생성할 수 있다. 구체적으로는 인증키가 총 4바이트인 경우, 첫번째 바이트 및 두번째 바이트를 XOR연산하고, 세번째 바이트 및 네번째 바이트를 XOR연산한다. 다음으로, 두개의 연산 결과값을 이용하여 XOR연산함으로써 1바이트의 연산결과값을 얻을 수 있게 된다. 이에 따라 연산된 결과값이 바로 사용자 아이디가 된다.

한편, 제어기기(100)의 사용자가 입력하는 인증키가 정상적인 것인지 확인하는 절차가 필요하다. 이를 위해, 제어기기(100)는 입력되는 인증키의 각 바이트값을 홈서버(200)로 전송한다(S650).

홈서버(200)는 자신이 부여한 인증키와 수신된 인증키가 일치하면, 인증키를 변환하여 사용자 아이디를 생성한 후, 저장한다(S660).

다음으로, 제어기기(100) 및 홈서버(200)는 사용자 아이디, 인증키, 및, 커스텀 코드를 파라미터(parameter)로 사용하는 단방향함수세트를 생성한 후, 제2 메모리부(140) 및 제2 서버 메모리부(240)에 각각 저장한다(S670). 생성된 단방향함수세트는 코드값, 포인터값 등과 함께 비밀키 생성과정에 사용된다.

도 7은 제어기기(100)로부터 홈서버(200)로 전송되는 메시지의 구조를 나타내는 모식도이다. 도 7에 따르면, 메시지(400)는 리더 코드(leader code : 410)), 커스텀 코드(custom code : 420a, 420b), 버튼 코드(button code : 430a, 430b), 시퀀스 넘버(sequence number : 440), 포인터값(450), 사용자 아이디(user ID : 460), XOR 영역(470), 및, 스톱 비트(stop bit : 480) 등을 포함한다.

리더 코드(410)는 패킷 헤더에 해당하는 부분으로, 목적지 주소 및 송신자 주소 등이 기록되는 영역이다. 커스텀 코드(420a, 420b)는 홈서버(200)의 제조회사에서 부여한 고유코드 등이 기록되는 영역이다. 버튼 코드(430a, 430b)는 제어기기(100) 상에서 선택된 버튼에 대응되는 코드값이 기록되는 영역이다. 커스텀 코드 및 버튼 코드는 정보 확인을 위하여 각각 두 영역으로 구분되어, 동일 데이터를 중복 기록하는 형태로 구성하는 것이 바람직하다.

시퀀스 넘버(440)는 현재 전송되는 메시지가 몇번째 메시지인지를 기록하는 영역이다. 포인터값(450)은 해당 코드값이 기록된 메모리부 영역의 주소를 기록하는 영역이다. 사용자 ID(460)는 기 등록된 사용자 아이디가 기록되는 영역이다. 등록이 이루어지기 전까지는, 사용자 ID(460) 영역에는 널값(null value)이 기록된다. XOR 영역(470)은 시퀀스 넘버(440), 포인터값(450), 및, 사용자 아이디(460)를 XOR연산한 값이 기록되는 영역이다. XOR 영역에 기록된 값을 확인함으로써, 시퀀스 넘버(440), 포인터값(450), 및, 사용자 아이디(460) 등이 에러값인지 여부를 판단할 수 있다. 스톱 비트(m)는 메시지의 종료를 알리는 영역이다.

도 8은 도 7과 같은 구조의 메시지(400)를 전송하여 코드값을 인증하는 과정을 설명하는 모식도이다. 도 8은 인증키가 4바이트로 구성되고, 코드값이 1바이트인 경우를 예로 들어 도시하고 있다.

도 8에 따르면, 제어기기(100)는 소정 버튼이 입력되면, 해당 버튼의 코드값 및 인증키(Authentication Key : AK)의 첫번째 값(AK#1)을 XOR연산한다. 도 8에서 XOR연산은 ⊕으로 표기한다. 그리고 나서, 연산결과값을 버튼코드(430a, 430b) 영역에 기록하여 제1 메시지(400a)를 생성한다. 이에 따라, 제1메시지(400a)를 홈서버(200)로 전송한다. 홈서버(200)는 전송된 제1메시지(400a)의 사용자 아이디를 확인하여, 대응되는 인증키를 제2 서버 메모리부(240)로부터 독출한다. 이에 따라, 인증키의 첫번째 값(AK#1)을 이용하여 버튼코드(430a, 430b)에 기록된 코드값을 확인한다. 한편, 홈서버(200)는 제1메시지(400a)에 기록된 포인터값을 이용하여 제1 서버 메모리부(230)의 포인터값도 동기화시킨다.

다음으로, 홈서버(200)는 확인된 코드값 및 인증키의 두번째 값(AK#2)을 이용하여 XOR 연산을 수행한다. 그리고 나서, 연산결과값을 버튼코드 영역에 기록하여 제2 메시지(400b)를 생성한다. 이에 따라, 제2 메시지(400b)를 제어기기(100)로 전송한다. 이 경우, 제1 서버 메모리부(230)의 포인터값을 조정하였다면, 조정된 포인터값도 제2 메시지(400b)에 기록하여 제어기기(100)로 통지한다.

제어기기(100)는 인증키의 두번째 값(AK#2)을 이용하여 제2 메시지(400b)에 기록된 코드값을 확인한다. 이에 따라, 제1 메시지(400a)를 통해 전송하였던 코드값과 동일하다면, 코드값이 정상적으로 전송되었다고 인증할 수 있다. 한편, 제어기기(100) 및 홈서버(200) 간에는 무선 통신이 이루어지고 있는 바, 보다 정확한 코드값 인증을 위해서 인증키의 나머지 값들을 이용하여 인증작업을 소정 회수 더 실행할 수도 있다.

즉, 제어기기(100)는 코드값 및 인증키의 세번째 값(AK#3)을 이용하여 제3 메시지(400c)를 작성한 후, 홈서버(200)로 전송한다. 홈서버(200)는 이를 확인한 후, 인증키의 네번째 값(AK#4)을 이용하여 제4 메시지(400d)를 작성하여 제어기기(100)로 전송하게 된다. 이상과 같이, 인증키의 마지막 값이 이용될 때까지 코드값이 동일하다면, 코드값에 대한 인증을 완료할 수 있다.

제어기기(100)는 제1 메모리부(130)의 각 레지스터에 순차적으로 코드값을 기록한다. 도 8에 따르면, "1"버튼이 입력되어 인증이 완료된 후, 제1 메모리부(130)의 네번째 레지스터, 즉, 포인터값 4가 지정하는 영역에 코드값 "1"이 저장된다. 한편, 두자릿 수 버튼이 입력된 경우에는, 제1 메모리부(130) 상에서 두개의 코드값이 저장되게 된다. 홈서버(200)도 제1 서버 메모리부(230)의 각 레지스터에 순차적으로 코드값을 기록한다. 이 경우, 동기화 작업이 이루어져 있으므로, 제1 서버 메모리부(230) 중 포인터값 4가 지정하는 영역에 코드값 "1"이 저장된다.

도 9는 제어기기(100) 및 홈서버(200)에서 1회용 비밀키를 생성하기 위한 연산 과정을 설명하는 모식도이다. 도 9에 따르면, 코드값이 저장된 메모리부(130, 230) 및 단방향함수세트(500)를 이용하여 비밀키를 생성한다. 이러한 상태에서, 메모리부(130, 230)로부터 코드값 C, 및 포인터값 P를 독출한다. 다음으로, 단방향함수세트(500)로부터 소정 넘버(N)의 단방향함수를 독출한다. 이에 따라, 독출된 단방향함수를 이용하여 연산을 수행함으로써 1회용 비밀키를 생성하게 된다. 이 경우, 도 9와 같이 단방향함수세트는 사용자 아이디, 인증키, 커스텀 코드 등을 파라미터로 이용하여 생성될 수 있다.

도 9에서는 해쉬(Hash) 함수를 단방향 함수로 사용하고 있음을 알 수 있다. 또한, 도 9에서는 메모리부(130, 230)에 총 16개의 포인터값이 마련되어 있고, 해쉬함수세트는 총 16개의 해쉬함수로 구성된다. 이에 따라 메모리부(130, 230)의 각 포인터값과 해쉬함수세트의 각 해쉬함수를 순차적으로 선택하면서 비밀키를 생성한다. 따라서, 16*16=256 회 동안 매번 상이한 비밀키를 생성할 수 있게 된다. 즉, 최초에는 포인터값 1, 코드값 6, 및, 해쉬함수 H[16]을 이용하여 비밀키를 생성하였다면, 다음에는 해쉬함수 H[15], H[14],... 순으로 변경된다. 이에 따라, 해쉬함수 H[1]까지 사용된다면, 포인터값, 코드값을 각각 2, 3으로 변경한 후, 다시 H[16], H[15], H[14], ... 순으로 해쉬함수 연산을 수행한다.

이러한 상태에서 제어기기(100) 상에서 소정 버튼이 입력된다면, 다시 코드값이 변경되게 된다. 이와 같이, 수시로 코드값이 변경되므로, 총 256 회 비밀키를 생성하더라도 별도의 초기화 작업을 수행할 필요가 없게 된다.

도 10은 본 발명에 따른 제어기기 인증방법을 이용한 통신방법을 설명하기 위한 모식도이다. 도 10에 따르면, 제어기기(100)는 홈서버(200)로 접속(Connection)을 요청한다(단계a). 이에 따라, 홈서버(200)는 제어기기(100)로 인증에 필요한 아이디(ID) 및 패스워드(PW)를 요청한다(단계b). 제어기기(100)는 기 등록된 사용자아이디(U_ID), 포인터값(P), 및, 단방향 함수 넘버(H[N])를 누적시킨 소정의 아이디를 생성한다. 또한, 상술한 방식으로 1회용 비밀키(MK)를 생성한다. 이에 따라, 생성된 아이디 및 1회용 비밀키를 홈서버(200)로 전송한다(단계c).

홈서버(200)는 아이디가 수신되면, 포인터값, 단방향 함수 넘버를 확인한 후, 상술한 방식으로 1회용 비밀키(MK')를 생성한다. 이에 따라, MK 및 MK'를 비교한다. 비교 결과 일치하면, 인증을 완료하고 제어기기(100)로 통지한다(단계d).

제어기기(100) 및 홈서버(200)는 인증이 완료되면 소정 프로토콜을 이용한 통신을 개시한다(단계e). 구체적으로는 IPsec 프로토콜을 이용하여, 보안이 강화된 어플리케이션 데이터를 송수신할 수 있게 된다.

도 11은 제어기기(100)가 아닌 별도의 PC(400)를 이용하여 홈서버(200)에 접속하는 방법을 설명하기 위한 모식도이다. 도 11에 따르면, 소정의 웹 브라우저 프로그램이 설치된 PC(400)를 이용하여 접속을 요청할 수 있다(단계a).

이에 따라, 홈서버(200)는 아이디 및 패스워드를 요청한다(단계b). 한편, 사용자는 제어기기(100)를 통해서 아이디 및 패스워드를 확인한 후, 확인된 값을 PC(400)를 통해 입력한다. 입력된 아이디 및 패스워드는 홈서버(200)로 전송된다(단계c). 구체적으로는, 제어기기(100)는 사용자의 요청에 의해 사용자 아이디(U_ID), 포인터값(P), 단방향 함수 넘버(H[N])를 누적한 아이디를 생성한다. 또한, 현재의 포인터값(P), 이에 의해 지정된 코드값(C), 단방향 함수를 이용하여 비밀키를 생성한다. 이에 따라, 생성된 아이디 및 비밀키를 자체 디스플레이 소자를 이용하여 디스플레이하게 된다.

홈서버(200)는 아이디 및 패스워드를 입력받으면, 1회용 비밀키(MK')를 생성한 후, MK와 일치하는지 확인한다. 확인 결과, 일치한다면 인증을 완료하고 PC(400)로 통지한다(단계d). 도 11에서는 PC(400) 및 홈서버(200)가 SSL/TLS 프로토콜을 이용하여 통신을 개시하는 것을 볼 수 있다. 즉, 현재의 웹브라우저에서 지원하는 SSL/TLS 프로토콜을 사용하면서, 인증방법을 상술한 본 발명의 실시예와 같이 구현할 수 있게 된다.

발명의 효과

이상 설명한 바와 같이, 본 발명에 따르면, 토큰 장치를 구비하지 않더라도 1회용 비밀키를 생성하여 인증에 사용할 수 있게 된다. 특히, 제어기기 상에서 수시로 선택되는 버튼의 코드값 및 단방향함수를 비밀키 생성과정에서 사용하는 바, 코드값은 제어기기 사용에 따라 수시로 변경되기 때문에, 별도의 초기화 작업을 수행하지 않더라도 1회용 비밀키를 생성할 수 있게 된다. 이에 따라, 홈네트워크시스템의 보안을 강화할 수 있게 된다.

또한, 이상에서는 본 발명의 바람직한 실시예에 대하여 도시하고 설명하였지만, 본 발명은 상술한 특정의 실시예에 한정되지 아니하며, 청구범위에서 청구하는 본 발명의 요지를 벗어남이 없이 당해 발명이 속하는 기술분야에서 통상의 지식을 가진자에 의해 다양한 변형실시가 가능한 것은 물론이고, 이러한 변형실시들은 본 발명의 기술적 사상이나 전망으로부터 개별적으로 이해되어져서는 안될 것이다.

(57) 청구의 범위

청구항 1.

적어도 하나의 슬레이브 기기, 상기 슬레이브 기기를 제어하는 홈서버, 및, 상기 홈서버를 제어하기 위한 리모콘 기능을 수행하는 제어기기를 포함하는 홈네트워크에서의 제어기기 인증방법에 있어서,

(a) 상기 제어기기를 상기 홈서버에 등록하는 단계;

(b) 상기 제어기기 및 상기 홈서버가 상기 제어기기의 사용자 아이디 및 상기 제어기기에 대하여 부여된 인증키를 파라미터로 하는 단방향 함수 세트를 생성하여 저장하는 단계;

(c) 상기 제어기기 상에서 상기 리모콘 기능을 수행하기 위해 입력한 버튼의 코드값을 상기 제어기기 및 상기 홈서버가 각각 저장하는 단계;

(d) 상기 제어기기가 자체 구비된 메모리부 중 소정의 제1 코드값이 저장된 영역을 가리키는 포인터값, 상기 제1 코드값. 및, 상기 단방향 함수 세트 중 소정 넘버의 단방향 함수를 이용한 연산을 수행함으로써 제1비밀키를 생성하는 단계;

(e) 상기 제어기기가 상기 포인터값, 상기 단방향함수의 넘버 및 상기 제1비밀키를 상기 홈서버로 전송하여 인증을 요청하는 단계;

(f) 상기 홈서버가 자체 구비된 제1 서버 메모리부 중 상기 포인터값이 가리키는 영역에 저장된 코드값, 상기 포인터값, 및, 상기 단방향함수 넘버에 대응되는 단방향함수를 이용한 연산을 수행함으로써 제2비밀키를 생성하는 단계; 및,

(g) 상기 홈서버가 상기 제1비밀키 및 상기 제2비밀키가 일치한다고 판단되면, 상기 제어기기에 대한 인증을 완료하는 단계;를 포함하는 것을 특징으로 하는 제어기기 인증방법.

청구항 2.

제1항에 있어서,

상기 (a)단계는,

상기 제어기기가 상기 홈서버로 등록 요청 패킷을 전송하는 단계;

상기 홈서버가 소정의 인증키를 생성한 후, 디스플레이하는 단계;

상기 제어기기의 사용자가 상기 인증키를 입력하면, 상기 제어기기가 상기 인증키의 각 바이트 값을 상기 홈서버로 전송하는 단계;

상기 제어기기 및 상기 홈서버가 각각 상기 인증키를 변환하여 사용자 아이디를 생성하는 단계; 및,

상기 제어기기 및 상기 홈서버가 상기 생성된 사용자 아이디 및 상기 인증키를 각각 저장하는 단계;를 포함하는 것을 특징으로 하는 제어기기 인증방법.

청구항 3.

제1항에 있어서,

상기 (a)단계는,

상기 제어기기가 상기 홈서버로 등록 요청 패킷을 전송하는 단계;

상기 홈서버가 소정의 인증키를 생성한 후, 상기 제어기기로 전송하는 단계;

상기 제어기기의 사용자가 상기 인증키를 입력하면, 상기 제어기기가 상기 인증키의 각 바이트값을 상기 홈서버로 전송하는 단계;

상기 제어기기 및 상기 홈서버가 각각 상기 인증키를 변환하여 사용자 아이디를 생성하는 단계; 및,

상기 제어기기 및 상기 홈서버가 상기 사용자 아이디 및 상기 인증키를 각각 저장하는 단계;를 포함하는 것을 특징으로 하는 제어기기 인증방법.

청구항 4.

제2항 또는 제3항에 있어서,

상기 (c)단계는,

상기 제어기기가 상기 코드값, 상기 코드값이 저장될 메모리부 영역을 가리키는 포인터값, 및, 상기 인증키를 이용하여 소정 연산을 수행한 후, 상기 연산값을 상기 홈서버로 전송하는 단계;

상기 홈서버가 상기 전송된 연산값 및 상기 인증키를 이용하여 상기 코드값을 확인한 후, 소정의 응답 패킷을 전송하는 단계;

상기 제어기기가 상기 응답패킷을 수신하면, 상기 홈서버가 상기 코드값을 정상 수신하였다고 판단하고, 상기 코드값을 상기 메모리부 영역에 저장하는 단계; 및,

상기 홈서버가 상기 제1 서버 메모리부의 소정 영역에 상기 확인된 코드값을 저장하는 단계;를 포함하는 것을 특징으로 하는 제어기기 인증방법.

청구항 5.

제2항 또는 제3항에 있어서,

상기 (c)단계는,

상기 제어기기가 상기 인증키의 첫번째 값 및 상기 코드값을 이용하여 소정의 제1연산을 수행한 후, 제1연산결과값을 상기 홈서버로 전송하는 단계;

상기 홈서버가 상기 제1연산결과값에 의해 확인된 코드값 및 상기 인증키의 두번째 값을 이용하여 소정의 제2연산을 수행한 후, 제2연산결과값을 상기 제어기기로 전송하는 단계;

상기 제어기기가 상기 인증키의 두번째 값을 이용하여 상기 제2연산결과값으로부터 상기 코드값을 확인한 후, 인증하는 단계;

상기 제어기기가 상기 인증된 코드값 및 상기 인증키의 세번째 값을 이용하여 소정의 제3연산을 수행한 후, 제3연산결과값을 상기 홈서버로 전송하는 단계;

상기 홈서버가 상기 인증키의 세번째 값을 이용하여 상기 제3연산결과값으로부터 상기 코드값을 확인한 후, 인증하고 저장하는 단계;

상기 홈서버가 상기 인증된 코드값 및 상기 인증키의 네번째 값을 이용하여 소정의 제4연산을 수행한 후, 제4연산결과값을 상기 제어기기로 전송하는 단계; 및,

상기 제어기기가 상기 인증키의 네번째 값을 이용하여 상기 제4연산결과값을 확인한 후, 인증을 완료하고 상기 코드값을 저장하는 단계;를 포함하는 것을 특징으로 하는 제어기기 인증방법.

청구항 6.

제4항에 있어서,

상기 (c)단계는,

상기 홈서버 및 상기 제어기기가 상기 메모리부의 포인터값 및 상기 제1 서버 메모리부의 포인터값을 동기화시키는 단계; 및,

상기 홈서버가 상기 제어기기로부터 전송된 포인터값이 가리키는 제1 서버 메모리부 영역에 상기 확인된 코드값을 저장하는 단계;를 포함하는 것을 특징으로 하는 제어기기 인증방법.

청구항 7.

적어도 하나의 슬레이브 기기, 및, 상기 슬레이브 기기를 제어하는 홈서버를 포함하는 홈네트워크를 제어하는 제어기기에 있어서,

상기 홈서버와의 사이에서 데이터를 송수신하는 인터페이스부;

상기 홈서버를 제어하기 위한 소정의 버튼을 구비하며, 상기 버튼 중 선택된 버튼에 대응되는 코드값을 출력하는 키입력부;

상기 키입력부로부터 출력되는 코드값을 상기 홈서버로 전송하여, 인증하는 코드값 인증부;

상기 코드값 인증부에 의해 인증된 코드값을 소정 영역에 저장하는 제1 메모리부;

소정의 단방향 함수 세트가 저장되는 제2 메모리부;

상기 제1 메모리부 중 소정의 제1 코드값이 저장된 영역을 가리키는 포인터값 및 상기 제1 코드값과, 상기 단방향 함수 세트 중 선택된 소정 단방향함수를 이용하여 1회용 비밀키를 생성하는 비밀키생성부; 및,

상기 포인터값, 상기 단방향함수의 넘버, 및, 상기 1회용 비밀키를 포함한 패킷을 생성한 후, 상기 생성된 패킷을 상기 인터페이스부를 통해 상기 홈서버로 전송하여 인증을 요청하는 제어부;를 포함하는 것을 특징으로 하는 제어기기.

청구항 8.

제7항에 있어서,

상기 제어부는,

상기 키입력부를 통해 소정의 인증키가 입력되면 상기 인증키를 변환하여 소정의 사용자 아이디를 생성한 후, 상기 인증키 및 상기 사용자 아이디를 상기 제2 메모리부에 저장하는 것을 특징으로 하는 제어기기.

청구항 9.

제8항에 있어서,

상기 제어부는,

상기 키입력부를 통해 입력된 인증키의 각 바이트값을 상기 인터페이스부를 통해서 상기 홈서버로 전송함으로써, 상기 홈서버가 상기 인증키를 상기 사용자 아이디로 변환한 후, 등록할 수 있도록 하는 것을 특징으로 하는 제어기기.

청구항 10.

제9항에 있어서,

상기 제어부는,

상기 등록이 이루어지면, 복수개의 단방향함수를 포함한 단방향 함수 세트를 생성하여 상기 제2 메모리부에 저장하는 것을 특징으로 하는 제어기기.

청구항 11.

제10항에 있어서,

상기 코드값 인증부는, 상기 코드값 및 상기 인증키를 이용한 소정 연산을 수행하여 상기 연산결과값을 상기 인터페이스부를 통해 상기 홈서버로 전송한 후, 상기 홈서버로부터 전송되는 응답패킷에 기록된 코드값이 상기 코드값과 동일하면, 상기 코드값을 인증하는 것을 특징으로 하는 제어기기.

청구항 12.

소정의 제어기기 및 적어도 하나의 슬레이브 기기를 포함한 홈네트워크 상에서 상기 제어기기의 제어에 따라 상기 슬레이브 기기를 제어하는 홈서버에 있어서,

상기 제어기기로부터 메모리부 영역을 지정하는 포인터값, 소정의 단방향함수 넘버, 및, 제1 비밀키를 수신하는 서버 인터페이스부;

상기 제어기기 상에서 입력된 버튼에 대응되는 코드값이 저장된 제1 서버 메모리부;

소정의 단방향함수 세트가 저장되는 제2 서버 메모리부;

상기 제1 서버 메모리부 영역 중 상기 포인터값에 의해 지정된 영역에 저장된 코드값, 상기 포인터값, 및, 상기 단방향함수 세트 중 상기 단방향함수 넘버에 대응되는 단방향함수를 이용하여 제2 비밀키를 연산하는 연산부; 및,

상기 제1 비밀키 및 상기 제2 비밀키가 일치하면 상기 제어기기를 인증하는 홈서버 제어부;를 포함하는 것을 특징으로 하는 홈서버.

청구항 13.

제12항에 있어서,

상기 홈서버 제어부는

상기 제어기기로부터 수신된 포인터값 및 상기 제1 서버 메모리부의 포인터값을 동기화시키는 것을 특징으로 하는 홈서버.

청구항 14.

제13항에 있어서,

소정 데이터를 디스플레이하는 디스플레이부;를 더 포함하며,

상기 홈서버 제어부는, 상기 제어기기로부터 등록 요청 패킷이 수신되면 상기 제어기기에 대한 인증키를 생성한 후, 상기 디스플레이부를 제어하여 상기 인증키를 디스플레이하는 것을 특징으로 하는 홈서버.

청구항 15.

제14항에 있어서,

상기 홈서버 제어부는,

상기 제어기기로부터 상기 인증키가 전송되면 상기 전송된 인증키를 변환하여 사용자 아이디를 생성하고, 상기 사용자 아이디 및 상기 인증키를 파라미터로 하는 상기 단방향함수세트를 생성한 후, 상기 사용자 아이디, 상기 인증키 및 상기 단방향함수세트를 상기 제2 서버 메모리에 저장하는 것을 특징으로 하는 홈서버.

청구항 16.

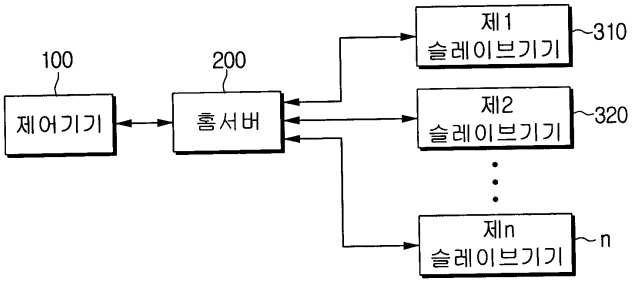
제15항에 있어서,

상기 인증키를 이용하여 상기 제어기기가 전송한 코드값을 인증하는 인증부;를 더 포함하며,

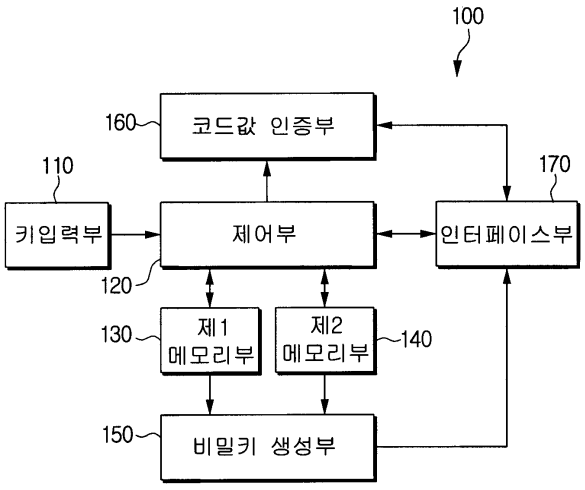
상기 홈서버 제어부는, 상기 인증부에 의해 인증된 코드값을 상기 제1 서버 메모리부에 저장하는 것을 특징으로 하는 홈서버.

도면

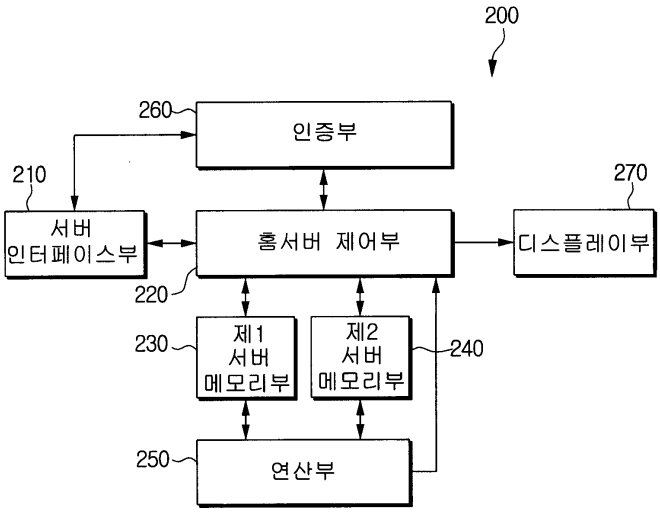
도면1



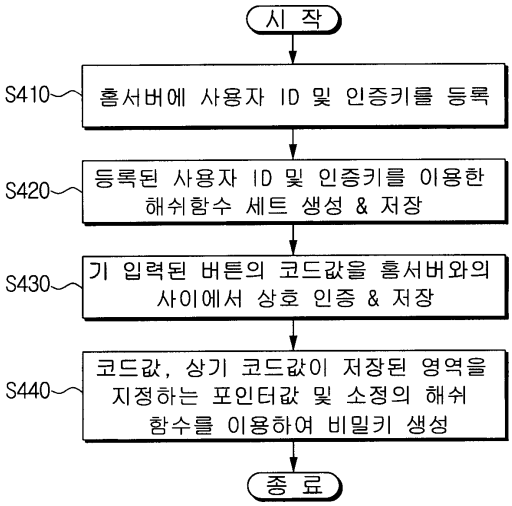
도면2



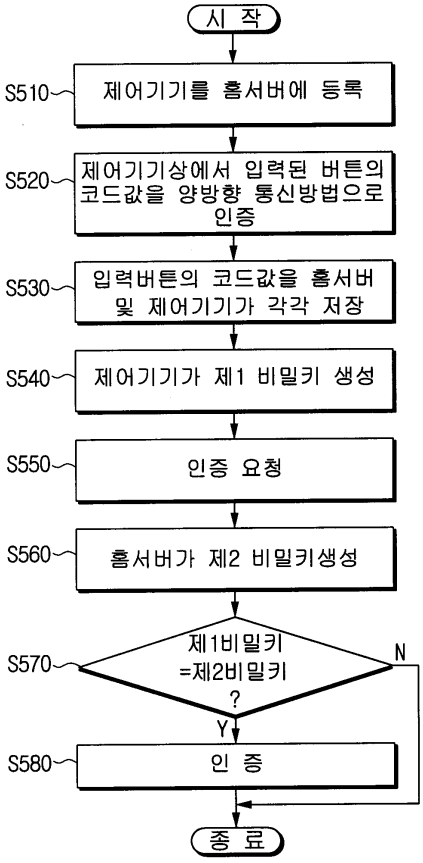
도면3


200
260
인증부
210
270
서버
인터페이스부
홈서버 제어부
디스플레이부
220
230
제1
서버
메모리부
제2
서버
메모리부
240
250
연산부

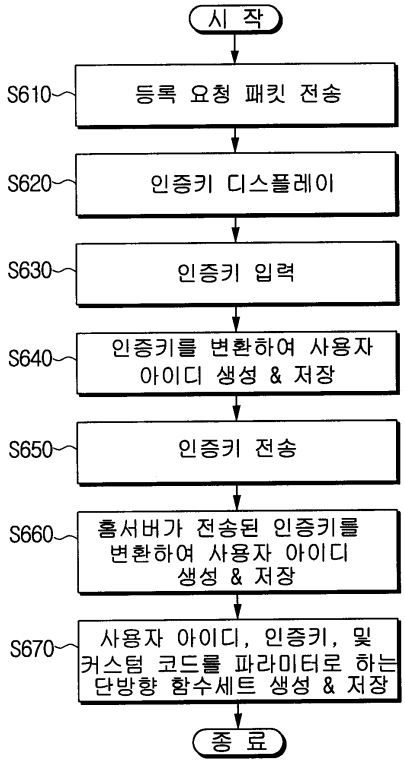
도면4


시 작
S410
홈서버에 사용자 ID 및 인증키를 등록
S420
등록된 사용자 ID 및 인증키를 이용한
해쉬함수 세트 생성 & 저장
S430
기 입력된 버튼의 코드값을 홈서버와의
사이에서 상호 인증 & 저장
S440
코드값, 상기 코드값이 저장된 영역을
지정하는 포인터값 및 소정의 해쉬
함수를 이용하여 비밀키 생성
종 료

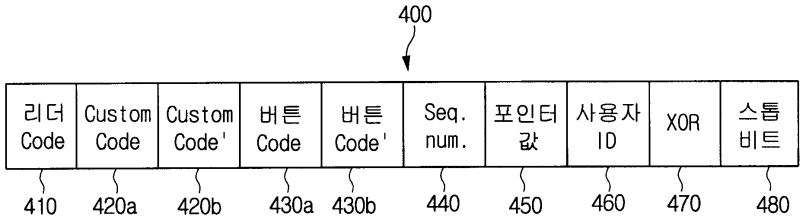
도면5


시 작
S510
제어기기를 홈서버에 등록
S520
제어기기상에서 입력된 버튼의 코드값을 양방향 통신방법으로 인증
S530
입력버튼의 코드값을 홈서버 및 제어기기가 각각 저장
S540
제어기기가 제1 비밀키 생성
S550
인증 요청
S560
홈서버가 제2 비밀키생성
S570
제1비밀키 =제2비밀키 ?
N
Y
S580
인 증
종 료

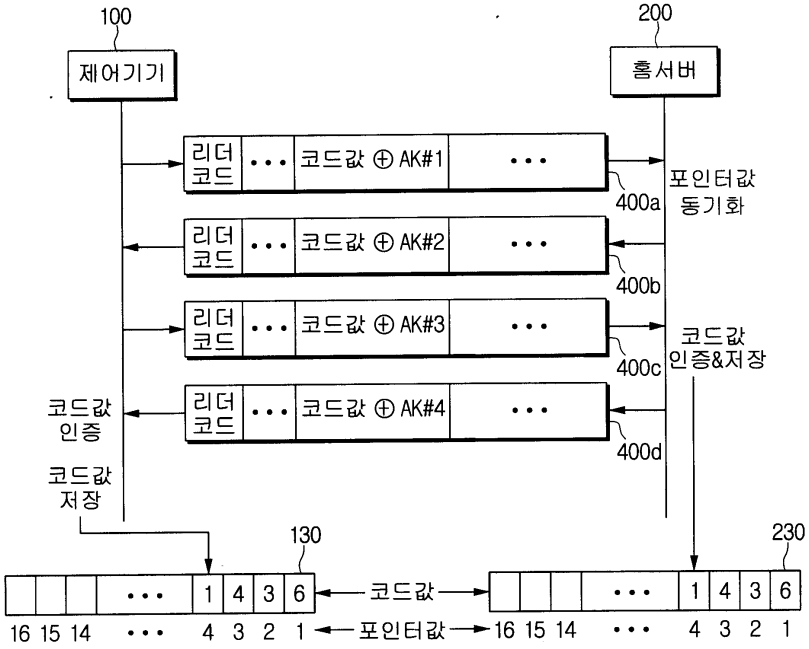
도면6


시 작
S610
등록 요청 패킷 전송
S620
인증키 디스플레이
S630
인증키 입력
S640
인증키를 변환하여 사용자 아이디 생성 & 저장
S650
인증키 전송
S660
홈서버가 전송된 인증키를 변환하여 사용자 아이디 생성 & 저장
S670
사용자 아이디, 인증키, 및 커스텀 코드를 파라미터로 하는 단방향 함수세트 생성 & 저장
종 료

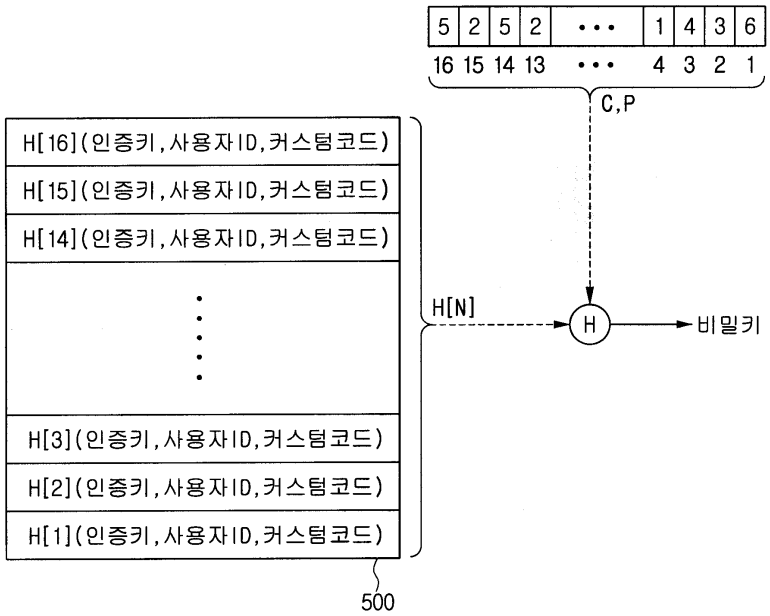
도면7


400
리더 Code
Custom Code
Custom Code'
버튼 Code
버튼 Code'
Seq. num.
포인터 값
사용자 ID
XOR
스톱 비트
410
420a
420b
430a
430b
440
450
460
470
480

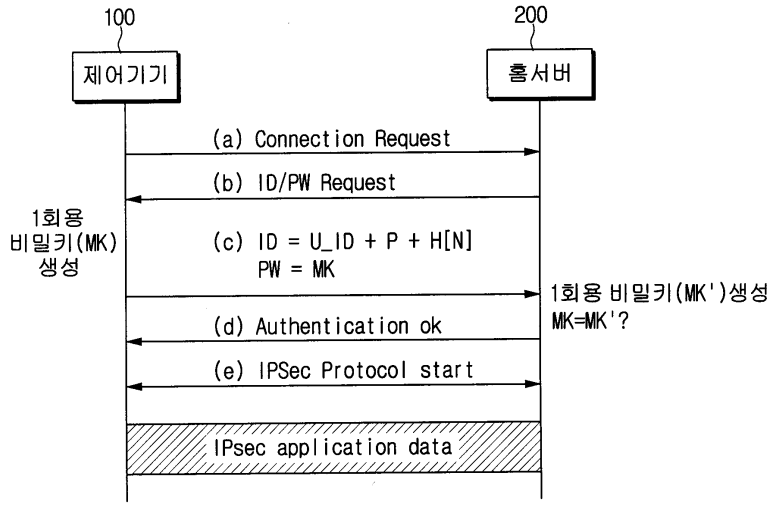
도면8


100
제어기기
200
홈서버
리더 코드
코드값 ⊕ AK#1
코드값 ⊕ AK#2
코드값 ⊕ AK#3
코드값 ⊕ AK#4
400a
400b
400c
400d
포인터값 동기화
코드값 인증&저장
코드값 인증
코드값 저장
130
230
코드값
포인터값
16 15 14 ••• 4 3 2 1

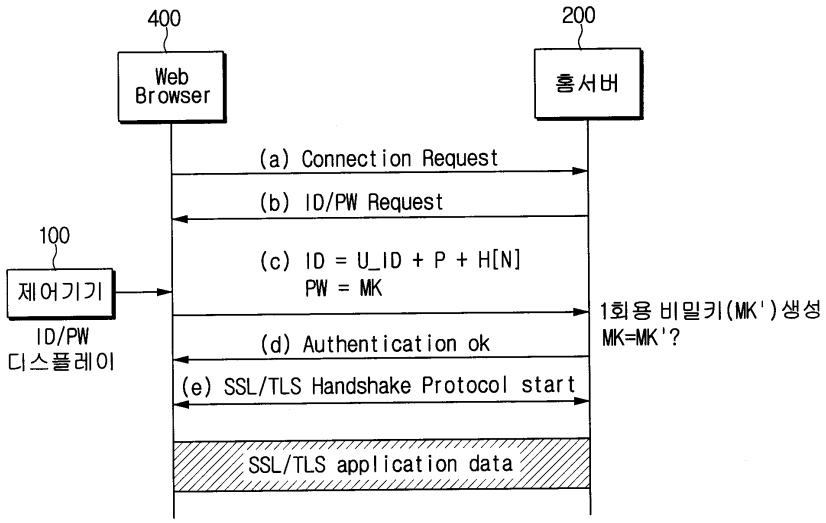
도면9


5 2 5 2 ••• 1 4 3 6
16 15 14 13 ••• 4 3 2 1
C,P
H[16](인증키,사용자ID,커스텀코드)
H[15](인증키,사용자ID,커스텀코드)
H[14](인증키,사용자ID,커스텀코드)
H[3](인증키,사용자ID,커스텀코드)
H[2](인증키,사용자ID,커스텀코드)
H[1](인증키,사용자ID,커스텀코드)
H[N]
H
비밀키
500

도면10


100
제어기기
200
홈서버
(a) Connection Request
(b) ID/PW Request
1회용
비밀키(MK)
생성
(c) ID = U_ID + P + H[N]
PW = MK
1회용 비밀키(MK')생성
MK=MK'?
(d) Authentication ok
(e) IPSec Protocol start
IPsec application data

도면11


400
Web
Browser
200
홈서버
(a) Connection Request
(b) ID/PW Request
100
제어기기
ID/PW
디스플레이
(c) ID = U_ID + P + H[N]
PW = MK
1회용 비밀키(MK')생성
MK=MK'?
(d) Authentication ok
(e) SSL/TLS Handshake Protocol start
SSL/TLS application data