(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2013년05월06일
(11) 등록번호 10-1258850
(24) 등록일자 2013년04월23일

(51) 국제특허분류(Int. Cl.)
G06K 19/077 (2006.01)
(21) 출원번호 10-2012-0051598
(22) 출원일자 2012년05월15일
심사청구일자 2012년05월15일
(56) 선행기술조사문헌
KR1020100073726 A
JP11276704 A
JP11216251 A
KR1020060132763 A

(73) 특허권자
고려대학교 산학협력단
서울 성북구 안암동5가 1
(72) 발명자
이동훈
서울특별시 종로구 내수동 72 경희궁의아침3단지 아파트 1404호
박정수
서울특별시 서대문구 북가좌2동 335-1
(74) 대리인
특허법인충현

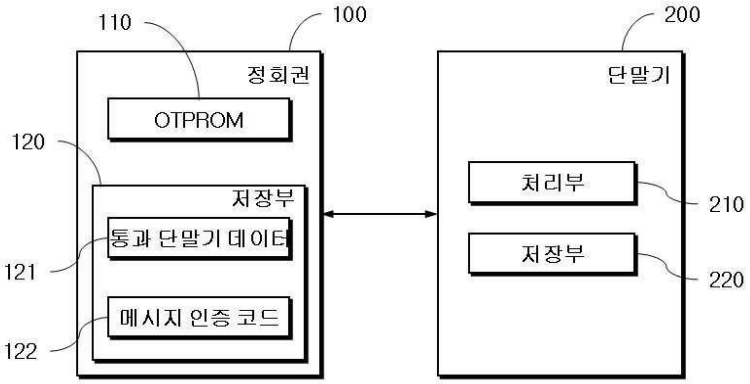
전체 청구항 수 : 총 9 항 심사관 : 임은정

(54) 발명의 명칭 **OTPROM을 이용한 정회권 구현 방법**

(57) 요 약

본 발명은 OTPROM을 이용한 정회권에 관한 것으로서, OTP 값을 저장하는 OTPROM, 및 통과 단말기 데이터, 및 메시지 인증 코드(MAC)를 저장하는 저장부를 포함하고, 상기 메시지 인증 코드는, 상기 OTP 값과 상기 통과 단말기 데이터의 값으로부터 산출된 메시지 인증 코드 함수의 결과 값인 것을 특징으로 하며, OTPROM을 이용하여 정회권을 인증함으로써 정회권의 위조변조를 방지할 수 있다.

대 표 도 - 도1



이 발명을 지원한 국가연구개발사업
과제고유번호 20110020516
부처명 한국연구재단
연구사업명 원천기술개발사업
연구과제명 개인 프라이버시 보장 원격 접근기술(총괄:super mobile 구현을 위한 시스템 SW 원천기술 연구)
주관기관 성균관대학교
연구기간 2011.07.01 ~ 2012.06.30

특허청구의 범위

청구항 1

OTP 값을 저장하는 OTPROM; 및

통과 단말기 데이터, 및 메시지 인증 코드(MAC)를 저장하는 저장부를 포함하고,

상기 메시지 인증 코드는,

상기 OTP 값과 상기 통과 단말기 데이터의 값으로부터 산출된 메시지 인증 코드 함수의 결과 값인 것을 특징으로 하는 정회권.

청구항 2

제 1 항에 있어서,

상기 정회권은,

단말기에 의해 상기 메시지 인증 코드로부터 인증된 경우에만 상기 단말기 통과가 허여되는 것을 특징으로 하는 정회권.

청구항 3

제 1 항에 있어서,

상기 OTPROM의 크기는 미리 설정된 단말기 통과가능 횟수에 따라 업데이트 가능 횟수가 정해지고,

상기 OTP 값은 단말기 통과시 소정의 비트만큼 업데이트되는 것을 특징으로 하는 정회권.

청구항 4

제 1 항에 있어서,

상기 통과 단말기 데이터는 발권데이터, 승차데이터, 및 하차데이터를 포함하고,

상기 통과 단말기 데이터는 단말기로부터 수신하여 저장되는 것을 특징으로 하는 정회권.

청구항 5

정회권으로부터 상기 정회권에 저장된 OTP 값, 통과 단말기 데이터, 및 메시지 인증 코드(MAC)를 수신하여 상기 정회권을 인증하는 처리부;

통과 단말기 데이터를 저장하는 저장부를 포함하고,

상기 메시지 인증 코드는,

상기 정회권에 저장된 OTP 값과 상기 통과 단말기 데이터의 값으로부터 산출된 메시지 인증 코드 함수의 결과 값인 것을 특징으로 하는 단말기.

청구항 6

제 5 항에 있어서,

상기 처리부는,

상기 수신한 OTP 값과 통과 단말기 데이터로부터 메시지 인증 코드 함수의 결과 값을 산출하여 상기 정회권을 인증하고, 상기 인증된 정회권의 상기 단말기 통과를 허여하며, 상기 OTP 값과 상기 단말기의 저장부에 저장된 통과 단말기 데이터를 이용하여 새로운 메시지 인증 코드를 생성하는 것을 특징으로 하는 단말기.

청구항 7

OTPROM의 OTP 값, 통과 단말기 데이터, 및 메시지 인증 코드(MAC)를 단말기에 전송하는 단계; 및

상기 단말기에 의해 인증된 경우, 상기 단말기로부터 새로운 통과 단말기 데이터 및 메시지 인증 코드를 수신하여 저장하고, 상기 OTP 값을 소정의 비트만큼 업데이트하는 단계를 포함하고,

상기 메시지 인증 코드는,

상기 OTP 값과 상기 통과 단말기 데이터의 값으로부터 산출된 메시지 인증 코드 함수의 결과 값인 것을 특징으로 하는 정회권 인증 방법.

청구항 8

정회권으로부터 상기 정회권에 저장된 OTP 값, 통과 단말기 데이터, 및 메시지 인증 코드(MAC)를 수신하는 단계;

상기 수신한 OTP 값과 통과 단말기 데이터로부터 메시지 인증 코드 함수의 결과 값을 산출하는 단계;

상기 산출한 결과 값을 인증하는 단계;

상기 산출한 결과 값이 인증된 경우, 상기 OTP 값과 단말기에 저장된 통과 단말기 데이터를 이용하여 새로운 메시지 인증 코드를 생성하는 단계; 및

상기 단말기에 저장된 통과 단말기 데이터 및 상기 생성한 새로운 메시지 인증 코드를 상기 정회권에 송신하고, 상기 정회권의 단말기 통과를 허여하는 단계를 포함하는 정회권 인증 방법.

청구항 9

제 7 항 내지 제 8 항 중에 어느 한 항의 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

명 세 서

기 술 분 야

[0001] 본 발명은 OTPROM을 이용한 정회권에 관한 것으로서, 더욱 상세하게는 한번만 프로그램될 수 있는 OTPROM을 이용하여 위변조를 방지하는 정회권, 단말기, 정회권 인증방법, 및 기록매체에 관한 것이다.

배 경 기 술

[0002] 정회권이란, 특정 구역 내에서 일정 횟수만큼 버스, 지하철, 또는 특정 서비스를 이용할 수 있는 승차권을 의미한다. 많은 사람들이 출퇴근 등에 대중교통수단을 이용하고 있으며, 대중교통을 이용하는 승객들은 좀 더 저렴하게 대중교통을 이용하기 위하여 정회권을 선호한다. 대중교통 등의 서비스를 제공하는 서비스 제공자들도 정회권의 승차가능 횟수만큼 고객을 확보할 수 있어 정회권의 제공이 이루어지고 있다. 서비스를 제공하는 서비스 제공자로써, 비용적인 측면이나 복잡성 측면에서 단순한 칩을 이용하여 정회권을 제공하고자 하나, 너무 단순한 경우, 특정 사용자들에 의해 상기 정회권에 사용되는 칩의 데이터 위변조 문제가 발생할 수 있는 문제점이 존재한다.

[0003] 승차권의 위변조를 방지하기 위하여 종래에는 공개특허 "지하철 승차권의 독취방법 및 독취장치(출원번호: 10-1998-0046080)"에서와 같이, 승차권에 마그네틱 스트라이프를 부착하고, 상기 마그네틱 스트라이프를 독취하여 변조승차권인지를 판단하는 방법을 이용하고 있으나, 상기 마그네틱 스트라이프의 변조가 가능한바, 상기 정회권 위변조의 방지에 근본적인 해결책이 되지 못하는 문제점이 있다.

발명의 내용

해결하려는 과제

[0004] 본 발명이 해결하고자 하는 첫 번째 과제는 OTPROM을 이용한 정회권을 제공하는 것이다.

[0005] 본 발명이 해결하고자 하는 두 번째 과제는 OTPROM을 이용한 정회권을 인증하는 단말기를 제공하는 것이다.

[0006] 본 발명이 해결하고자 하는 세 번째 과제는 OTPROM을 이용한 정회권 인증방법을 제공하는 것이다.

[0007] 또한, 상기된 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록 매체를 제공

하는데 있다.

과제의 해결 수단

[0008] 본 발명은 상기 첫 번째 과제를 달성하기 위하여, OTP 값을 저장하는 OTPROM; 및 통과 단말기 데이터, 및 메시지 인증 코드(MAC)를 저장하는 저장부를 포함하고, 상기 메시지 인증 코드는, 상기 OTP 값과 상기 통과 단말기 데이터의 값으로부터 산출된 메시지 인증 코드 함수의 결과 값인 것을 특징으로 하는 정회권을 제공한다.

[0009] 본 발명의 다른 실시예에 의하면, 상기 정회권은, 단말기에 의해 상기 메시지 인증 코드로부터 인증된 경우에만 상기 단말기 통과가 허여되는 것을 특징으로 하는 정회권일 수 있다.

[0010] 본 발명의 또 다른 실시예에 의하면, 상기 OTPROM의 크기는 미리 설정된 단말기 통과가능 횟수에 따라 업데이트 가능 횟수가 정해지고, 상기 OTP 값은 단말기 통과시 소정의 비트만큼 업데이트되는 것을 특징으로 하는 정회권일 수 있다.

[0011] 본 발명은 상기 두 번째 과제를 달성하기 위하여, 정회권으로부터 상기 정회권에 저장된 OTP 값, 통과 단말기 데이터, 및 메시지 인증 코드(MAC)를 수신하여 상기 정회권을 인증하는 처리부; 통과 단말기 데이터를 저장하는 저장부를 포함하고, 상기 메시지 인증 코드는, 상기 정회권에 저장된 OTP 값과 상기 통과 단말기 데이터의 값으로부터 산출된 메시지 인증 코드 함수의 결과 값인 것을 특징으로 하는 단말기를 제공한다.

[0012] 본 발명의 다른 실시예에 의하면, 상기 처리부는, 상기 수신한 OTP 값과 통과 단말기 데이터로부터 메시지 인증 코드 함수의 결과 값을 산출하여 상기 정회권을 인증하고, 상기 인증된 정회권의 상기 단말기 통과를 허여하며, 상기 OTP 값과 상기 단말기의 저장부에 저장된 통과 단말기 데이터를 이용하여 새로운 메시지 인증 코드를 생성하는 것을 특징으로 하는 단말기일 수 있다.

[0013] 본 발명은 상기 세 번째 과제를 달성하기 위하여, OTPROM의 OTP 값, 통과 단말기 데이터, 및 메시지 인증 코드(MAC)를 단말기에 전송하는 단계; 및 상기 단말기에 의해 인증된 경우, 상기 단말기로부터 새로운 통과 단말기 데이터 및 메시지 인증 코드를 수신하여 저장하고, 상기 OTP 값을 소정의 비트만큼 업데이트하는 단계를 포함하고, 상기 메시지 인증 코드는, 상기 OTP 값과 상기 통과 단말기 데이터의 값으로부터 산출된 메시지 인증 코드 함수의 결과 값인 것을 특징으로 하는 정회권 인증 방법을 제공한다.

[0014] 상기 다른 기술적 과제를 해결하기 위하여, 본 발명은 상기된 정회권 인증방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록 매체를 제공한다.

발명의 효과

[0015] 본 발명에 따르면, OTPROM을 이용하여 정회권을 인증함으로써 정회권의 위조변조를 방지할 수 있다. 또한, 본 발명에 따르면, 일반 메모리와 OTPROM만을 이용하므로 비용면에서 효율적으로 정회권을 구현할 수 있다.

도면의 간단한 설명

[0016] 도 1은 본 발명의 일 실시예에 따른 정회권과 단말기를 도시한 블록도이다.

도 2는 본 발명의 다른 실시예에 따른 정회권을 지하철 승차권을 예로 들어 승하차시 정회권의 메모리 변화를 도시한 도면이다.

도 3은 본 발명의 일 실시예에 따른 정회권에서의 정회권 인증방법의 흐름도이다.

도 4는 본 발명의 다른 실시예에 따른 단말기에서의 정회권 인증방법의 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0017] 본 발명에 관한 구체적인 내용의 설명에 앞서 이해의 편의를 위해 본 발명이 해결하고자 하는 과제의 해결 방안의 개요 혹은 기술적 사상의 핵심을 우선 제시한다.

[0018] 본 발명의 일 실시예에 따른 정회권은 OTP 값을 저장하는 OTPROM, 및 통과 단말기 데이터, 및 메시지 인증 코드(MAC)를 저장하는 저장부를 포함하고, 상기 메시지 인증 코드는, 상기 OTP 값과 상기 통과 단말기 데이터의 값으로부터 산출된 메시지 인증 코드 함수의 결과 값인 것을 특징으로 한다.

[0019] 이하 첨부된 도면을 참조하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 본 발명을 용이하게 실

시할 수 있는 실시 예를 상세히 설명한다. 그러나 이들 실시예는 본 발명을 보다 구체적으로 설명하기 위한 것으로, 본 발명의 범위가 이에 의하여 제한되지 않는다는 것은 당업계의 통상의 지식을 가진 자에게 자명할 것이다.

[0020] 본 발명이 해결하고자 하는 과제의 해결 방안을 명확하게 하기 위한 발명의 구성을 본 발명의 바람직한 실시예에 근거하여 첨부 도면을 참조하여 상세히 설명하되, 도면의 구성요소들에 참조번호를 부여함에 있어서 동일 구성요소에 대해서는 비록 다른 도면상에 있더라도 동일 참조번호를 부여하였으며 당해 도면에 대한 설명시 필요한 경우 다른 도면의 구성요소를 인용할 수 있음을 미리 밝혀둔다. 아울러 본 발명의 바람직한 실시 예에 대한 동작 원리를 상세하게 설명함에 있어 본 발명과 관련된 공지 기능 혹은 구성에 대한 구체적인 설명 그리고 그 이외의 제반 사항이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우, 그 상세한 설명을 생략한다.

[0021] 도 1은 본 발명의 일 실시예에 따른 정회권과 단말기를 도시한 블록도이다.

[0022] 본 발명의 일 실시예에 따른 정회권(100)은 OTPROM(110) 및 저장부(120)를 포함하고, 저장부(110)는 통과 단말기 데이터(121) 및 메시지 인증 코드(122)를 포함한다.

[0023] 정회권(100)은 사용한 가능 횟수가 미리 정해져 있다. 정회권(100)은 지하철 또는 버스 등의 승차권에 사용될 수 있고, 도서관 출입 또는 놀이동산 출입 등에서도 사용될 수 있다. 즉, 단말기를 반복적으로 통과하거나 이용하는 경우에 사용될 수 있다. 정회권(100)은 사용 가능횟수가 정해져 있으며, 정회권(100)의 사용 가능횟수를 늘리거나 이미 사용한 횟수를 줄이는 방법으로 위변조하는 경우, 정회권을 제공하는 서비스 제공자는 손해를 볼 수 있다. 이에 대해 본 발명의 일 실시예에 따른 정회권은 OTPROM을 이용하여, 정회권(100)의 위변조를 방지한다.

[0024] OTPROM(110)은 OTP 값을 저장한다.

[0025] 보다 구체적으로, OTPROM(110)은 One Time Programmable ROM의 약자로써, OTPROM은 한번 업데이트(0에서 1 또는 1에서 0으로 업데이트)되면 다시 복구되지 않는다. 즉, 일방향성을 갖는다. OTPROM(110)의 크기는 미리 설정된 단말기 통과가능 횟수에 따라 업데이트 가능 횟수가 정해지고, OTP 값은 단말기 통과시 미리 설정된 비트만큼 업데이트된다. OTPROM(110)은 칩 종류의 크기에 따라 다양한 크기를 갖을 수 있으며, 단말기 통과가능 횟수에 따라 OTPROM(110)의 크기가 다르거나, 업데이트 되는 비트의 수를 다르게 할 수 있다. 즉, 상기 단말기 통과가능 횟수와 동일한 비트의 크기를 갖는 OTPROM(110)을 이용하거나, 상기 단말기 통과가능 횟수에 따라 상기 단말기 통과가능 횟수만큼만 OTPROM(110)이 업데이트 되게 업데이트되는 비트 수를 조절할 수도 있다. 또는, 승차와 하차가 함께 이루워지는 경우에는, 승차와 하차시를 나누어 승차시에만 상기 OTP 값을 업데이트할 수도 있다. OTPROM(110)의 OTP 값은 16진수일 수 있으며, 상기 단말기 통과가능 횟수에 따라 크기가 n일 수 있으며, 2진수로 표현할 때, 모두 1이거나 모두 0일 수 있다. 모두 1인 경우, 업데이트시, 1을 갖는 가장 낮은 비트를 0으로 업데이트할 수 있다. 모두 0인 경우, 업데이트시, 0을 갖는 가장 낮은 비트를 1로 업데이트할 수 있다.

[0026] 저장부(120)는 통과 단말기 데이터 및 메시지 인증 코드(MAC)를 저장한다.

[0027] 보다 구체적으로, 저장부(120)는 OTPROM(110)과 달리 저장된 정보를 쓰고 지울 수 있다. 저장부(120)는 정회권이 단말기를 통과할 때의 통과 단말기 데이터와 인증을 위한 메시지 인증 코드를 저장한다. 통과 단말기 데이터(121)와 메시지 인증 코드(122)는 단말기(200) 통과시 단말기(200)로부터 수신한다. 통과 단말기 데이터(121)는 통과한 단말기의 정보 등을 포함하고 있다. 통과 단말기 데이터(121)는 단말기의 위치정보 등을 포함하고 있을 수 있으며, 단말기를 통과한 시간 정보 등을 포함하고 있을 수 있다. 통과 단말기 데이터는 단말기를 통과할 때마다 해당 단말기 데이터로 저장된다. 정회권이 지하철 승차권으로 이용될 경우, 상기 정회권(100)의 통과 단말기 데이터(121)는 발권데이터, 승차데이터, 및 하차데이터를 포함한다. 처음 발권시 발권데이터가 저장되고, 이후, 승차와 하차를 반복하면서, 승차데이터와 하차데이터가 갱신된다.

[0028] 메시지 인증 코드(Massage Authentication Code, MAC, 122)는 상기 OTP 값과 상기 통과 단말기 데이터의 값으로부터 산출된 메시지 인증 코드 함수의 결과 값이다. 정회권(100)의 인증을 위하여, 메시지 인증 코드(MAC) 함수를 이용한다. 상기 메시지 인증 코드 함수는 두 값과 키를 이용하여 산출된다. 즉, OTPROM(110)에 저장된 OTP 값과 마지막으로 저장된 상기 통과 단말기 데이터 값을 이용하여 산출한다. 메시지 인증 코드 함수는 다음 수학식 1과 같을 수 있다.

수학식 1

[0029] $$MAC = h(\text{통과 단말기 데이터} \parallel \text{OTP 값}, Key)$$

[0030] 상기 통과 단말기 데이터 값과 OTP 값을 이용한 MAC 값은 상기 OTP 값의 위변조방지 특성을 이용하는바, 역시 MAC 값의 위변조를 방지할 수 있다.

[0031] 상기 메시지 인증 코드(122)는 단말기(200)에서 산출될 수 있으며, 통과 단말기 데이터(121)는 단말기(200)에 저장된 데이터일 수 있다. 정회권(100)은 단말기(200)로부터 상기 통과 단말기 데이터(121) 및 메시지 인증 코드(122)를 수신하여 저장할 수 있다.

[0032] 정회권(100)은 단말기(200)에 의해 메시지 인증 코드(122)로부터 인증된 경우에만 상기 단말기(200) 통과가 허여될 수 있다. 정회권(100)은 단말기(200)를 통과시 저장하고 있는 OTP 값, 통과 단말기 데이터(121), 및 메시지 인증 코드(122)를 단말기(200)로 전송하여 단말기(200)로부터 메시지 인증 코드(122)로부터 위변조가 있는지를 판단받아 인증절차를 수행하고, 상기 인증된 정회권(100)만 단말기(200)를 통과할 수 있다.

[0033] 단말기(200)는 처리부(210)와 저장부(220)로 구성된다.

[0034] 처리부(210)는 정회권(100)으로부터 정회권(100)에 저장된 OTP 값, 통과 단말기 데이터, 메시지 인증 코드(MAC)을 수신하여 정회권(100)을 인증한다.

[0035] 보다 구체적으로, 처리부(210)는 정회권(100)의 위변조여부를 판단하여 정회권(100)에 대해 단말기(200) 통과를 허여할 것인지를 판단한다. 상기 정회권(100)을 인증하기 위하여, 메시지 인증 코드를 이용한다. 상기 메시지 인증 코드가 맞는지를 판단하기 위하여, 정회권(100)으로부터 OTP 값, 통과 단말기 데이터, 메시지 인증 코드를 수신한다. 상기 수신한 OTP 값과 통과 단말기 데이터로부터 메시지 인증 코드 함수의 결과 값을 산출하여 인증한다. OTP 값은 일방향으로만 업데이트 될 수 있는바, 상기 OTP 값을 다시 되돌릴 수 없다. 따라서, 상기 OTP 값과 정회권(100)이 통과한 이전 통과 단말기 데이터를 이용하여 메시지 인증 코드를 산출하고, 상기 정회권(100)을 인증한다.

[0036] 상기 처리부(210)에서 산출한 메시지 인증 코드와 정회권(100)으로부터 수신한 메시지 인증 코드가 인증된 경우, 상기 정회권의 상기 단말기 통과를 허여하고, 상기 OTP 값과 상기 단말기의 저장부에 저장된 통과 단말기 데이터를 이용하여 새로운 메시지 인증 코드를 생성할 수 있다. 단말기(200)는 정회권(100)을 인증하고, 정회권(100)의 단말기(200) 통과를 허여한다. 또한, 단말기(200)에 저장된 통과 단말기 데이터와 상기 통과 단말기 데이터를 이용하여 새로운 메시지 인증 코드를 생성한다. 상기 새로운 메시지 인증 코드는 상기 수신한 OTP 값을 업데이트한 값과 상기 단말기(200)에 저장된 통과 단말기 데이터로부터 산출된 메시지 인증 코드 함수의 결과 값이다. 상기 정회권(100)의 인증과 새로운 메시지 인증 코드 산출이 완료되면, 상기 단말기(200)에 저장된 통과 단말기 데이터와 상기 산출된 새로운 메시지 인증 코드를 정회권(100)에 전송한다.

[0037] 저장부(220)는 통과 단말기 데이터를 저장한다.

[0038] 보다 구체적으로, 저장부(220)는 단말기(200)의 위치정보, 통과시간 등을 정회권(100)에 전송하고 새로운 메시지 인증 코드를 생성하기 위하여 통과 단말기 데이터를 저장하고 있다. 상기 통과 단말기 데이터는 위치정보, 통과시간, 단말기의 고유정보 등을 포함하고 있을 수 있으며, 상기 OTP 값과 동일한 형태의 16진수의 값일 수 있다.

[0039] 도 2는 본 발명의 다른 실시예에 따른 정회권을 지하철 승차권을 예로 들어 승하차시 정회권의 저장부 변화를 도시한 도면이다.

[0040] 정회권(100)은 일정 횟수동안 단말기를 통과하는 다양한 경우에 사용될 수 있다. 이 중 지하철 승차권을 예로 들어 자세히 살펴보도록 한다.

[0041] 정회권(100)은 OTPROM(110), 발권데이터(131), 승차데이터(132), 하차데이터(133), 및 메시지 인증 코드(MAC, 122)를 저장할 수 있다. 상기 OTPROM(110)과 나머지 저장부 부분은 다른 형태의 메모리를 이용할 수 있다. 즉, OTPROM은 일방향성을 갖는 메모리이고, 나머지 메모리는 쓰고 지울 수 있는 메모리를 이용할 수 있다. 지하철에서의 정회권(100)은 발권, 승차, 하차의 절차에 사용되고, 정회권(100)에 미리 설정된 승차가능횟수에 따라 승

차와 하차를 n번 반복한다. 처음 발권시에는 통과한 단말기가 없는바, 정회권(100)은 OTP 값과 발권데이터만 저장하고 있다. 이후 승차를 위해 단말기를 통과하면, 기존 발권데이터 이외에 승차데이터를 저장하게 된다. 상기 승차데이터는 발권데이터를 대체하여 저장될 수도 있다. 또한, 승차데이터를 작성시 OTP 값을 업데이트하고, 상기 OTP 값과 승차 데이터로부터 메시지 인증 코드 함수를 이용하여, 메시지 인증 코드를 생성하고 저장한다. 이후 하차시, 단말기를 통과하면, 하차 데이터를 저장하고, OTP 값과 하차 데이터로부터 메시지 인증 코드 함수를 이용하여, 메시지 인증 코드를 생성하고 저장한다. 하차 단말기 통과시 OTP 값은 업데이트하지 않을 수 있고, 업데이트할 수도 있다. 하차시 OTP 값 업데이트 여부는 단말기 제공자에 의해 미리 설정되어 있을 수 있다. 정회권(100)을 이용하여 승하차시, 단말기는 상기 정회권에 저장된 OTP 값, 승차데이터 또는 하차데이터 중 마지막으로 저장된 데이터 값, 및 메시지 인증 코드를 이용하여 정회권(100)을 인증하고 통과시킨다.

[0042] 도 3은 본 발명의 일 실시예에 따른 정회권에서의 정회권 인증방법의 흐름도이다.

[0043] 310단계는 OTPROM의 OTP 값, 통과 단말기 데이터, 및 메시지 인증 코드(MAC)를 단말기에 전송하는 단계이다.

[0044] 보다 구체적으로, 단말기의 정회권 인증을 위해 정회권에 저장된 OTPROM의 OTP 값, 통과 단말기 데이터, 및 메시지 인증 코드(MAC)를 단말기에 전송한다. 상기 메시지 인증 코드는, 상기 OTP 값과 상기 통과 단말기 데이터의 값으로부터 산출된 메시지 인증 코드 함수의 결과 값이다. 본 단계에 대한 상세한 설명은 도 1의 정회권(100)에 대한 설명에 대응하는바, 도 1의 정회권(100)에 대한 설명으로 대신한다.

[0045] 320단계는 상기 단말기에 의해 인증된 경우, 상기 단말기로부터 새로운 통과 단말기 데이터 및 메시지 인증 코드를 수신하여 저장하고, 상기 OTP 값을 소정의 비트만큼 업데이트하는 단계이다.

[0046] 보다 구체적으로, 310단계에서 단말기로 전송한 OTPROM의 OTP 값, 통과 단말기 데이터, 및 메시지 인증 코드(MAC)를 이용하여 상기 단말기로부터 인증을 받은 정회권은 상기 단말기로부터 새로운 통과 단말기 데이터 및 메시지 인증 코드를 수신한다. 상기 수신한 새로운 통과 단말기 데이터 및 메시지 인증 코드를 저장하고, OTPROM의 OTP 값을 미리 설정된 비트만큼 업데이트한다. 본 단계에 대한 상세한 설명은 도 1의 정회권(100)에 대한 설명에 대응하는바, 도 1의 정회권(100)에 대한 설명으로 대신한다.

[0047] 도 4는 본 발명의 다른 실시예에 따른 단말기에서의 정회권 인증방법의 흐름도이다.

[0048] 410단계는 정회권으로부터 정회권에 저장된 OTP 값, 통과 단말기 데이터, 및 메시지 인증 코드(MAC)를 수신하는 단계이다.

[0049] 보다 구체적으로, 단말기는 정회권 인증을 위하여, 정회권으로부터 정회권에 저장된 OTP 값, 통과 단말기 데이터, 및 메시지 인증 코드(MAC)를 수신한다. 본 단계에 대한 상세한 설명은 도 1의 단말기(200)에 대한 설명에 대응하는바, 도 1의 단말기(200)에 대한 설명으로 대신한다.

[0050] 420단계는 상기 수신한 OTP 값과 통과 단말기 데이터로부터 메시지 인증 코드 함수의 결과 값을 산출하는 단계이다.

[0051] 보다 구체적으로, 정회권의 인증을 위해 메시지 인증 코드를 이용한다. 410단계에서 수신한 메시지 인증 코드에 위변조가 없는지를 판단하기 위하여 상기 수신한 OTP 값과 통과 단말기 데이터로부터 메시지 인증 코드 함수의 결과 값을 산출한다. 본 단계에 대한 상세한 설명은 도 1의 단말기(200)에 대한 설명에 대응하는바, 도 1의 단말기(200)에 대한 설명으로 대신한다.

[0052] 430단계는 상기 산출한 결과 값을 인증하는 단계이다.

[0053] 보다 구체적으로, 420단계의 메시지 인증 코드 함수의 결과 값을 인증한다. 본 단계에 대한 상세한 설명은 도 1의 단말기(200)에 대한 설명에 대응하는바, 도 1의 단말기(200)에 대한 설명으로 대신한다.

[0054] 440단계는 상기 산출한 결과 값이 인증된 경우, 상기 OTP 값과 단말기에 저장된 통과 단말기 데이터를 이용하여 새로운 메시지 인증 코드를 생성하는 단계이다.

[0055] 보다 구체적으로, 430단계의 비교결과, 상기 산출한 결과 값이 인증된 경우 상기 410단계에서 수신한 메시지 인증 코드에 위변조가 없다는 것을 의미하는바, 정회권에 위변조가 없다는 것을 인증할 수 있다. 하지만, 상기 산출한 결과 값이 인증되지 않는 경우, 상이 정회권에 위변조가 있거나, 오류가 발생했다는 것을 의미하는바, 정회권을 인증할 수 없다. 인증이 완료된 정회권에 대해서만 정회권의 메시지 인증 코드를 업데이트하기 위하여 상기 OTP 값과 단말기에 저장된 통과 단말기 데이터를 이용하여 새로운 메시지 인증 코드를 생성한다. 본 단계에 대한 상세한 설명은 도 1의 단말기(200)에 대한 설명에 대응하는바, 도 1의 단말기(200)에 대한 설명으로 대

신한다.

[0056] 450단계는 상기 단말기에 저장된 통과 단말기 데이터 및 상기 생성한 새로운 메시지 인증 코드를 상기 정회권에 송신하고, 상기 정회권의 단말기 통과를 허여하는 단계이다.

[0057] 보다 구체적으로, 단말기에 저장된 통과 단말기 데이터와 440단계에 생성한 새로운 메시지 인증 코드를 정회권에 업데이트하기 위하여 정회권에 송신하고, 인증된 정회권의 단말기 통과를 허여한다. 에 저장된 통과 단말기 데이터를 이용하여 새로운 메시지 인증 코드를 생성한다. 본 단계에 대한 상세한 설명은 도 1의 단말기(200)에 대한 설명에 대응하는바, 도 1의 단말기(200)에 대한 설명으로 대신한다.

[0058] 본 발명의 실시예들은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 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 포함한다. 상기된 하드웨어 장치는 본 발명의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0059] 이상과 같이 본 발명에서는 구체적인 구성 요소 등과 같은 특정 사항들과 한정된 실시예 및 도면에 의해 설명되었으나 이는 본 발명의 보다 전반적인 이해를 돕기 위해서 제공된 것일 뿐, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상적인 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다.

[0060] 따라서, 본 발명의 사상은 설명된 실시예에 국한되어 정해져서는 아니되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등하거나 등가적 변형이 있는 모든 것들은 본 발명 사상의 범주에 속한다고 할 것이다.

부호의 설명

[0061] 100: 정회권

110: OTPROM

120: 저장부

121: 통과 단말기 데이터

122: 메시지 인증 코드

131: 발권 데이터

132: 승차 데이터

133: 하차 데이터

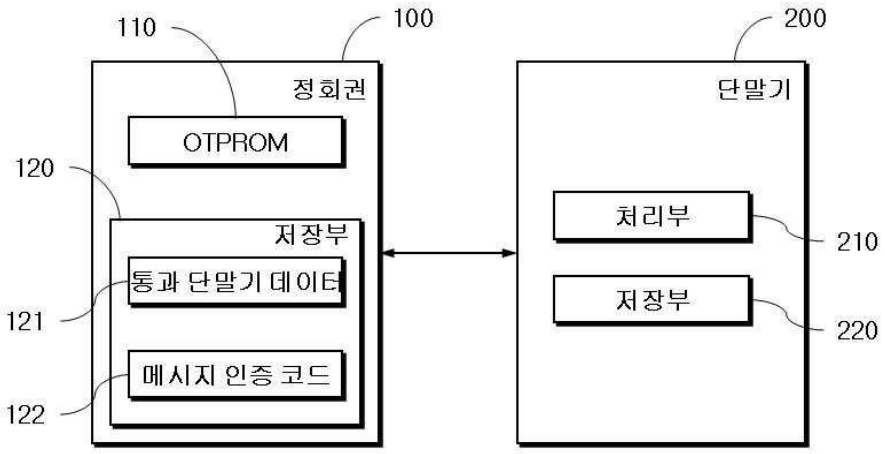
200: 단말기

210: 처리부

220: 저장부

도면

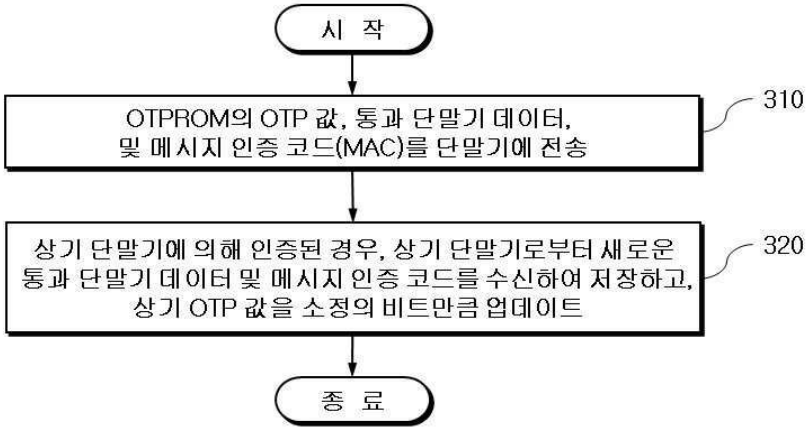
도면1


110
100
200
정회권
OTPROM
120
저장부
통과 단말기 데이터
121
메시지 인증 코드
122
단말기
처리부
210
저장부
220

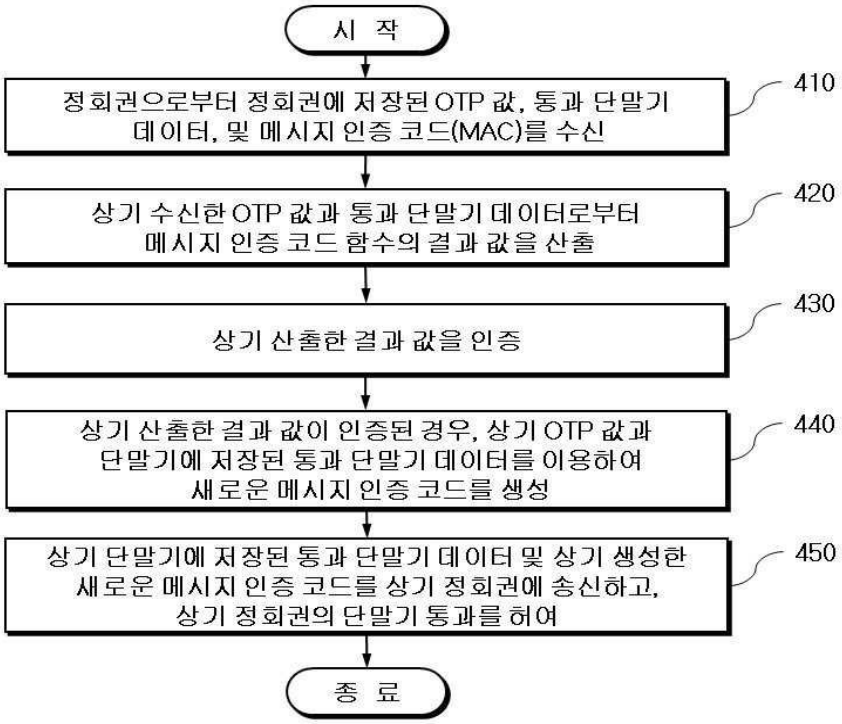
도면2


110
100
OTPROM
131
발권 데이터
132
승차 데이터
133
하차 데이터
122
MAC
정회권 메모리 구조
OTPROM
발권 데이터
OTPROM(update)
발권 데이터
승차 데이터
MAC
OTPROM
발권 데이터
승차 데이터
하차 데이터
MAC
발권
승차
하차
n회 반복

도면3


시 작
OTPROM의 OTP 값, 통과 단말기 데이터,
및 메시지 인증 코드(MAC)를 단말기에 전송
310
상기 단말기에 의해 인증된 경우, 상기 단말기로부터 새로운
통과 단말기 데이터 및 메시지 인증 코드를 수신하여 저장하고,
상기 OTP 값을 소정의 비트만큼 업데이트
320
종 료

도면4


시 작
정회권으로부터 정회권에 저장된 OTP 값, 통과 단말기
데이터, 및 메시지 인증 코드(MAC)를 수신
410
상기 수신한 OTP 값과 통과 단말기 데이터로부터
메시지 인증 코드 함수의 결과 값을 산출
420
상기 산출한 결과 값을 인증
430
상기 산출한 결과 값이 인증된 경우, 상기 OTP 값과
단말기에 저장된 통과 단말기 데이터를 이용하여
새로운 메시지 인증 코드를 생성
440
상기 단말기에 저장된 통과 단말기 데이터 및 상기 생성한
새로운 메시지 인증 코드를 상기 정회권에 송신하고,
상기 정회권의 단말기 통과를 허여
450
종 료