



(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。 Int. Cl. G06K 17/00 (2006.01)	(45) 공고일자 (11) 등록번호 (24) 등록일자	2007년02월07일 10-0680272 2007년02월01일
---	-------------------------------------	--

(21) 출원번호 (22) 출원일자 심사청구일자	10-2005-0073987 2005년08월11일 2005년08월11일	(65) 공개번호 (43) 공개일자
----------------------------------	---	------------------------

(73) 특허권자 고려대학교 산학협력단
 서울 성북구 안암동5가1 고려대학교 내

(72) 발명자 임종인
 서울 종로구 내수동 파크팰리스 101-901

 이동훈
 경기 고양시 일산구 일산3동 후곡마을8단지아파트 808-804

 이수미
 서울 성북구 안암동5가 149-1

 황영주
 서울 마포구 공덕2동 삼성래미안1차아파트 102-1303

(74) 대리인 현종철

(56) 선행기술조사문헌
KR1019970066914A
* 심사관에 의하여 인용된 문헌

심사관 : 김창주

전체 청구항 수 : 총 10 항

(54) R F I D 인증 시스템 및 그 방법

(57) 요약

RFID 인증 시스템 및 그 방법이 개시된다. RFID 인증 시스템은 ID를 저장하고 있으며, 질의가 오면 상기 ID의 해쉬함수 값 $h(ID)$ 를 생성하여 판독기로 전송하고, 상기 ID와 랜덤값 R 을 연결 연산한 값($ID \parallel R$)의 해쉬함수 값 $h(ID \parallel R)$ 에 대한 왼쪽 반($half_L(h(ID \parallel R))$)을 수신하면 $h(ID \parallel R)$ 에 대한 오른쪽 반($half_R(h(ID \parallel R))$)을 생성하여 판독기로 전송하고, 태그인증이 완료되면 ID를 ID와 R 을 배타논리합 한 값($ID \oplus R$)으로 갱신하는 태그; 상기 태그에 질의하여 $h(ID)$ 를 수신하면 데이터베이스로 전송하고, 데이터베이스로부터 $h(ID \parallel R)$ 를 수신하면 이에 대한 왼쪽 반($half_L(h(ID \parallel R))$) 및 R 을 태그로 전송하는 판독기; 및 상기 태그 정보(DATA), ID, 상기 ID의 해쉬값(HID) 및 랜덤값 생성기(R.N.G)를 구비하며, 상기 $h(ID)$ 를 수신하면 이를 이용하여 태그의 정보를 찾아 확인하고, 상기 R 및 $h(ID \parallel R)$ 를 생성하여 판독기로 전송하고, 태그인증이 완료되면 ID를 $ID \oplus R$ 로 갱신하는 데이터베이스를 포함하는 것을 특징으로 한다.

본 발명에 의하면, 저가의 태그에 유용할 뿐만 아니라, 재전송 공격, 스푸핑 공격을 감지하거나 예방하며, 메시지 유실시에 복구가 가능하다.

대표도

도 5

특허청구의 범위

청구항 1.

태그, 판독기 및 데이터베이스를 구비하는 RFID 인증 시스템에 있어서,

ID를 저장하고 있으며, 질의가 오면 상기 ID의 해쉬함수 값 $h(ID)$ 를 생성하여 판독기로 전송하고, 상기 ID와 랜덤값 R 을 연결 연산한 값($ID \parallel R$)의 해쉬함수 값 $h(ID \parallel R)$ 에 대한 왼쪽 반($half_L(h(ID \parallel R))$)을 수신하면 상기 $h(ID \parallel R)$ 에 대한 오른쪽 반($half_R(h(ID \parallel R))$)을 생성하여 판독기로 전송하고, 태그인증이 완료되면 상기 ID를 상기 ID와 R 을 배타논리합 한 값($ID \oplus R$)으로 갱신하는 태그;

상기 태그에 질의하여 $h(ID)$ 를 수신하면 데이터베이스로 전송하고, 데이터베이스로부터 $h(ID \parallel R)$ 를 수신하면 이에 대한 왼쪽 반($half_L(h(ID \parallel R))$) 및 R 을 태그로 전송하는 판독기; 및

태그 정보(DATA), ID, 상기 ID의 해쉬값(HID) 및 랜덤값 생성기(R.N.G)를 구비하며, 상기 $h(ID)$ 를 수신하면 이를 이용하여 상기 태그의 정보를 찾아 확인하고, 상기 R 및 $h(ID \parallel R)$ 를 생성하여 판독기로 전송하고, 태그인증이 완료되면 ID를 $ID \oplus R$ 로 갱신하는 데이터베이스를 포함하는 것을 특징으로 하는 RFID 인증시스템.

청구항 2.

제1항에 있어서, 상기 왼쪽 반($half_L(h(ID \parallel R))$)은

오른쪽 반($half_R(h(ID \parallel R))$)이고, 상기 오른쪽 반($half_R(h(ID \parallel R))$)은 왼쪽 반($half_L(h(ID \parallel R))$)인 것을 특징으로 하는 RFID 인증시스템.

청구항 3.

제1항에 있어서, 상기 데이터베이스는

상기 태그 정보(DATA), HID 및 ID를 RF통신이나 물리적인 접촉을 통해 안전하게 입력받는 것을 특징으로 하는 RFID 인증시스템.

청구항 4.

태그, 판독기 및 데이터 베이스를 구비하는 RFID인증 시스템에서의 RFID인증방법에 있어서,

판독기가 태그에 인증을 위한 질의하는 단계;

상기 질의에 대해 태그 ID를 해쉬한 값 $h(ID)$ 를 판독기에 전송하는 단계;

상기 $h(ID)$ 를 받으면, 이를 데이터베이스에 전송하는 단계;

상기 판독기로부터 $h(ID)$ 를 받으면, 상기 데이터베이스는 $h(ID)$ 를 통해 태그의 정보를 찾아 확인하고, 랜덤 값 R 과, 상기 ID 와 R 을 연결연산하여 해쉬함수한 값($h(ID \parallel R)$)을 생성하여 판독기로 전송하는 단계;

상기 R 및 $h(ID \parallel R)$ 를 수신하면, $h(ID \parallel R)$ 의 왼쪽 반인 $half_L(h(ID \parallel R))$ 및 R 을 태그에 전송하는 단계;

상기 R 및 $half_L(h(ID \parallel R))$ 를 받으면, 태그는 상기 R 및 $half_L(h(ID \parallel R))$ 가 자신이 만든 $h(ID \parallel R)$ 의 왼쪽과 일치한다면 받은 정보가 타당함을 확인하고, 판독기에게 $h(ID \parallel R)$ 의 오른쪽인 $half_R(h(ID \parallel R))$ 을 보내는 단계; 및

인증이 완료되면 상기 데이터베이스 및 태그는 ID 를 상기 ID 와 상기 랜덤값 R 을 배타논리합 한 값($ID \oplus R$)으로 갱신하는 단계를 포함하는 것을 특징으로 하는 RFID 인증시스템에서의 RFID 인증방법.

청구항 5.

제4항에 있어서, 상기 왼쪽 반($half_L(h(ID \parallel R))$)은

오른쪽 반($half_R(h(ID \parallel R))$)이고, 상기 오른쪽 반($half_R(h(ID \parallel R))$)은 왼쪽 반($half_L(h(ID \parallel R))$)인 것을 특징으로 하는 RFID 인증시스템에서의 RFID 인증방법.

청구항 6.

판독기, 태그 및 데이터베이스를 구비하는 RFID 인증시스템에 있어서,

ID 를 저장하며, 질의 및 랜덤값(S)이 오면 상기 ID 를 해쉬함수한 값 $h(ID)$ 및 상기 R 의 왼쪽 반에 해당하는 $half_L(R)$ 을 생성하여 판독기로 전송하고, 판독기로부터 R 의 오른쪽 반에 해당하는 $half_R(R)$ 을 수신하여 자신이 생성한 것과 일치하는지 체크하고, 인증이 완료되면 ID 를 상기 ID 와 $R \parallel R$ 을 배타논리합 한 값($ID \oplus (R \parallel R)$)으로 갱신하는 태그;

랜덤숫자생성기($R.N.G$)를 구비하며, 태그에 질의할 때 상기 $R.N.G$ 에서 생성된 랜덤숫자(S)를 함께 전송하며, 태그로부터 $h(ID)$ 및 $half_L(R)$ 를 수신하면 S , $h(ID)$ 및 $half_L(R)$ 를 데이터베이스로 전송하고, 데이터베이스로부터 상기 $half_R(R)$ 를 수신하면 이를 태그로 전송하는 판독기; 및

상기 RFID 태그의 정보($DATA$), 상기 ID , ID 의 해쉬값(HID) 및 메모리 연결을 위한 데이터베이스 엔트리(AE)를 구비하며, 판독기로부터 $h(ID)$, S 및 R 의 오른쪽 반 값인 $half_R(R)$ 을 수신하면 $h(ID)$ 를 통해 태그의 정보를 확인하고, ID 와 S 를 이용하여 R 을 생성하며, 상기 R 의 왼쪽부분이 판독기로부터 받은 값과 같다면 태그를 정당하다고 판단하고 자신의 인증을 위해 $half_R(R)$ 을 생성하여 판독기로 전송하며, 상기 R 을 통해 ID 를 $ID = ID \oplus (R \parallel R)$ 로 갱신하며 상기 갱신되는 정보들은 AE 에 의해 연결되는 메모리에 저장하는 데이터베이스를 포함하는 것을 특징으로 하는 RFID 인증시스템.

청구항 7.

제6항에 있어서, 상기 왼쪽 반($half_L(h(ID \parallel R))$)은

오른쪽 반($half_R(h(ID \parallel R))$)이고, 상기 오른쪽 반($half_R(h(ID \parallel R))$)은 왼쪽 반($half_L(h(ID \parallel R))$)인 것을 특징으로 하는 RFID 인증시스템.

청구항 8.

RFID 태그, 판독기 및 데이터 베이스를 구비하는 RFID인증 시스템에서의 RFID인증방법에 있어서,

판독기가 랜덤 값 S 를 생성하여 태그에게 질의하면서 상기 S를 전송하는 단계;

상기 S와 함께 질의를 받으면, 상기 태그는 $h(ID \parallel S)$ 를 R 값으로 생성하고, ID의 해쉬함수 값 $h(ID)$ 및 상기 R의 왼쪽 반 값인 $half_L(R)$ 를 생성하여 상기 판독기로 전송하는 단계;

상기 판독기는 태그로부터 받은 정보와 함께 S를 같이 데이터베이스로 전송하는 단계;

상기 $h(ID)$, S, $half_L(R)$ 을 받으면, 데이터베이스는 $h(ID)$ 를 통해 태그의 정보를 확인하고, ID 와 S 를 이용하여 R을 생성하고, 생성된 R 의 왼쪽부분이 판독기로부터 받은 값과 같다면 태그를 정당하다고 판단하고, 자신의 인증을 위해 R 의 오른쪽 부분인 $half_R(R)$ 을 판독기로 전송하며, 데이터베이스는 R 을 통해 ID 를 $ID = ID \oplus (R \parallel R)$ 로 갱신하며 갱신되는 정보들은 AE에 의해 연결되는 메모리에 저장하는 단계;

$half_R(R)$ 를 받으면, 판독기는 태그에게 $half_R(R)$ 를 전송하는 단계; 및

세션이 안전하게 끝나면, 태그와 데이터베이스는 ID 를 $ID \oplus (R \parallel R)$ 로 갱신하는 단계를 포함하는 것을 특징으로 하는 RFID 인증시스템에서의 RFID 인증방법.

청구항 9.

제8항에 있어서, 상기 왼쪽 반($half_L(h(ID \parallel R))$)은

오른쪽 반($half_R(h(ID \parallel R))$)이고, 상기 오른쪽 반($half_R(h(ID \parallel R))$)은 왼쪽 반($half_L(h(ID \parallel R))$)인 것을 특징으로 하는 RFID 인증시스템에서의 RFID 인증방법.

청구항 10.

제4항, 제5항, 제8항, 제9항 중 어느 한 항에 기재된 발명을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

명세서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 RFID(Radio Frequency Identification)인증에 관한 것으로서, 특히 저가형 RFID 태그를 위한 RFID 태그 인증 시스템 및 그 방법에 관한 것이다.

RFID란 일정주파수 대역을 이용하여 무선으로 원거리에서도 대상물을 분석할 수 있고, 각종 데이터를 주고받을 수 있도록 하는 초소형 칩으로 차세대 정보통신의 핵심기술이다. 이는 2차 세계대전 당시 영국에서 자국 전투기 자동식별용으로 개발되어 최초로 사용되었다. 그 당시 이용된 태그는 고가의 태그로 경제성이 없어 대중에게 널리 보급되지 못했었다. RFID 태그는 다른 접촉식 카드와는 달리 이용자가 카드를 판독기에 삽입하는 시간이 필요치 않으며 기계적인 접촉이 없기 때문에 마찰이나 손상이 없고, 오염이나 환경의 영향이 적다는 장점을 가지고 있다. 이러한 장점과 함께 RFID 태그의 가격이 낮아짐에 따라 기존에 광학 바코드를 이용하였던 많은 분야들에서 RFID 시스템으로 그 체제를 바꾸고 있어 그 활용도가 넓어지고 있다. RFID 시스템은 개인 정보를 가지는 태그와 태그의 정보를 받아 데이터베이스에서 전송하는 판독기, 그리고 모든 태그들의 정보를 가지는 데이터베이스로 구성된다. 유비쿼터스 환경에서 RFID 시스템은 공장 자동화, 물류·유통 관리, 보안, 출입통제, 인물·동물 추적, 요금 징수, 위조지폐방지, 홈 네트워크 등에 유용하게 쓰일 것이다.

RFID 시스템이 실용화됨에 따라 개인 정보 프라이버시 침해에 대한 위험이 커지고 있다. 저가의 RFID 태그는 그 크기가 작고 그 안에 개인 식별이 가능한 유일한 번호를 저장한다. 이런 경우, RFID 태그는 사용자 모르게 사용자의 물건에 내장 될 수 있고, 유비쿼터스 환경에서 사용자가 모르는 사이 판독기와 통신할 수도 있다. 이는 판독기를 가지는 모든 공격자가 태그의 정보를 알 수 있게 하며, 유일한 태그의 식별 번호를 통해 사용자의 위치를 추적할 수 있게 한다.

RFID 시스템에서 개인정보 프라이버시와 위치 프라이버시를 보장하기 위한 방법 중 하나가 RFID 인증 프로토콜이다. 도 1은 RFID 인증 프로토콜 모델을 도시한 것으로서, 판독기와 태그 간의 통신은 무선으로 불안전하며, 판독기와 데이터베이스간의 통신은 유선으로 안전하다. RFID 인증 프로토콜에서 판독기가 ①을 통해 질의를 하면, 개인 정보프라이버시를 보장하기 위해서 태그와 판독기가 서로 인증할 수 있는 타당한 정보 ②, ⑤를 주고받으며 서로를 타당하다 인증한 후, 태그는 자신의 유일한 정보 ⑥를 전송한다. 위치 프라이버시를 만족하기 위해서 태그가 자신의 타당성을 위해 판독기에게 전송하는 정보 ②는 매 인증 세션마다 달라진다.

기존에 제안된 RFID 인증 프로토콜들을 살펴보면, Weis가 제안한 프로토콜은 개인정보 프라이버시를 보장하기 위한 것이다. 그리고 Henrici와 Muller이 제안한 프로토콜은 개인 정보 프라이버시와 위치 프라이버시를 보장하며 재전송 공격을 막지만 스푸핑 공격을 감지하지 못하며, 태그의 메모리량이 크고 세 번의 해쉬 연산을 필요로 한다.

이를 보다 상세히 설명하면 다음과 같다. 먼저, Hash-Lock Scheme(이하 HL) 프로토콜에 대해 설명한다. Weis가 제안한 HL의 태그는 수동적이며 오직 읽기 기능(read-only identification functionality)을 갖는 몇 백 비트의 메모리를 갖는다. 표 1은 HL의 구성요소 및 연산도구를 나타낸 것이다.

[표 1]

	필요한 메모리	연산도구
태그	<u>metaID</u> , ID	$h()$
판독기	-	-
데이터베이스(DB)	<u>metaID</u> , key, ID	-

여기서, ID는 태그의 실질적인 데이터들, key는 랜덤값들, metaID는 key 의 해쉬값($=h(key)$)을, $h()$ 는 일방향 해쉬함수를 나타낸다.

HL에서 연산도구로 해쉬 함수를 갖는 태그는 태그의 소유자에 의해 자신의 실질적인 데이터 ID를 비롯하여 인증과정에 필요한 일시적인 metaID 값을 저장한다. 이 때, metaID는 랜덤하게 선택된 key의 해쉬 값($metaID = h(key)$)이다. 이러한 과정을 잠금(lock) 과정이라 한다. 잠금 과정 후에, 태그의 소유자는 key와 metaID를 데이터베이스에 저장한다. 이는 보안을 위해서 RF 채널이나 물리적인 접촉으로 안전하게 이루어진다.

도 2는 HL의 인증과정을 도시한 것이다. HL의 인증 과정은 잠금 상태와 열림(unlock)상태로 나누어 이루어진다. 첫 번째로 태그가 잠금 과정을 거쳐 잠겨 있는 상태에서 태그는 모든 판독기의 질의에 metaID를 보냄으로써 응답하고 태그가 열림 상태가 될 때까지 다른 기능은 하지 않는다. 그러나 태그는 판독기가 보내온 정보인 key를 받고 이를 해쉬해 보고 그것이 자신이 가지고 있는 metaID와 같다면 그 정보가 타당하다 판단하고 상태가 열림으로 바뀌면서 ID를 전송한다. 이때, 열림 상태는 공격자가 ID를 도청하는 것을 예방하기 위해서 아주 짧은 순간에 이루어지며, 다시 잠금 상태로 돌아간다. 이러한 잠금 기능으로 태그의 개인 정보 프라이버시는 보장된다.

HL은 태그에 단 한번의 해쉬 연산이 필요하며, 데이터베이스는 안전하다 가정하고 모든 태그의 key들을 관리한다. HL의 안전성은 일방향 해쉬 함수에 기반한다. 해쉬 함수의 특성상 key를 모르는 사람이 metaID로부터 key를 알아내는 것은 어렵기 때문에, 임의의 공격자는 정당한 판독기인척 가장 할 수 없다. 그러나 판독기와 태그 간의 통신은 도청이 가능하므로 특정 태그와 정당한 판독기간의 통신을 도청한 공격자는, 후에 질의를 보내고 도청한 key를 전송함으로써, 태그를 열림 상태로 바꾸고 ID를 얻을 수 있다. 그러므로 HL은 개인 정보 프라이버시 보장이 안 된다. HL은 임의의 태그에 대한 재전송 공격 및 스푸핑 공격을 예방할 수는 없지만, 감지가 가능하다.

그러나 앞에서 언급한 것처럼 특정 태그의 통신을 도청한 후, ID 값을 얻을 수 있어, 개인 프라이버시를 보장하지 못한다. 또한, metaID 가 개인 식별자로 쓰이므로, 태그가 판독기의 질의에 응할 때마다 같은 metaID 를 전송하게 되어 판독기를 비롯하여 도청하는 자들에게 트래킹 (tracking) 이 가능하다. 즉, 판독기를 비롯하여 도청하는 자들은 동일한 metaID 와 key 가 전송되는 것을 도청할 수 있으므로 태그의 위치 프라이버시는 보장되지 못한다.

다음으로, Hash-based ID Variation (이하 HIDV) 프로토콜은 다음과 같다. HIDV는 ID 값을 다양화함으로써 위치 프라이버시를 보장한다. 여기서의 ID 는 HL과 달리 인증을 위한 랜덤 값이며, 태그에 대한 실제 정보는 DATA 로서 데이터베이스에 저장되어있으며, 판독기에 전송할 필요가 있을 시, 데이터베이스가 직접 전달한다. 데이터베이스와 판독기사이의 통신은 안전하다고 가정하므로, 이를 통해 개인 정보 프라이버시가 보장된다. DATA는 태그에도 저장될 수 있으나, 본 발명에서는 인증을 우선 고려하므로 태그는 DATA를 갖지 않는 것으로 가정한다. 표 2는 HIDV의 구성요소 및 연산도구를 표로 나타낸 것이다.

[표 2]

	필요한 메모리	연산도구
태그	ID, TID, LST	$h()$, $\oplus$
판독기	-	-
데이터베이스 (DB)	HID, ID, TID, LT, AE, DATA	$h()$, R.N.G, $\oplus$

여기서, ID는 인증을 위한 랜덤 값으로 인증 성공시 마다 변화하고, HID는 ID의 해쉬 값($=h(ID)$)이고, TID는 현재 진행중인 인증 세션 번호(초기에는 LST와 같은 fosea 값으로 초기화한다.), AE는 메모리 연결을 위한 연결된 데이터 베이스 엔트리(entry)이며, DATA는 사용자 정보, 태그정보와 같은 실질적인 데이터이며, $h()$ 는 일방향 해쉬함수이며, R.N.G는 랜덤 숫자 생성기이며, $\oplus$ 는 XOR 연산(exclusive-or function)이다.

사용자는 태그에 ID 를 임의의 랜덤 값으로 입력하고, TID 와 LST 에는 다른 랜덤 값을 동일하게 입력시킨다. 그리고 안전한 접촉을 통해 데이터베이스에 HID, ID, TID, LST, AE 그리고 DATA 를 입력한다. 이때, HID 는 $h(ID)$ 가 입력된다. HIDV에서 태그의 $h(ID)$ 는 데이터베이스에서 HID 로 해당 태그의 메모리 행을 찾기 위해 쓰이며, TID 와 LST 는 재전송 공격을 막기 위해 사용된다. 그리고 메시지 유실이나 메시지 조작과 같은 공격이 가해지더라도 복구가 가능하도록 AE 가 사용된다. 데이터베이스는 하나의 태그에 대하여 두 개의 메모리 행을 가지며, 이 두 개의 행은 AE 에 의해 서로 연결이 된다.

HIDV의 인증 과정은 다음과 같다. 판독기가 태그에게 질의를 보내면, 태그는 TID 를 1 증가 시킨 후, 도 3 의 ②번과 같은 정보를 전송한다. $h(ID)$ 는 데이터베이스에서 해당 태그의 정보를 찾는데 쓰이며, $h(TID \oplus ID)$ 는 인증 및 재전송 공격을 막기 위해 쓰인다. 이러한 정보를 받은 데이터베이스는 태그를 인증하고 임의의 랜덤 값 R 을 생성하여 태그에게 전송되도록 한다. R 은 ID 를 갱신 (update) 하는데 쓰이며, 이를 통해 다음 인증 세션의 $h(ID)$ 가 바뀌게 되어 위치 프라이버시가 보장되게 된다. 그리고 데이터베이스가 보낸 $h(R \oplus TID \oplus ID)$ 는 태그가 받은 R 이 타당한지 확인하기 위해 쓰인다. HIDV에서 ⑤번째 과정이 제대로 수행되면, 태그는 $h(R \oplus TID \oplus ID)$ 를 생성해 전송받은 값과 비교해 본 후, 값이 같으면 기존의 ID 를 $ID = (ID \oplus R)$ 값으로 갱신하고, LST 값을 TID 값으로 저장한다.

HIDV은 ID 값을 각 인증 세션마다 랜덤한 R 에 의해 갱신하므로, 판독기를 비롯한 도청을 하는 공격자로부터 위치 프라이버시를 보장한다. 그리고 TID 와 LST를 이용하여, 공격자에 의한 재전송 공격을 예방하며, AE를 통하여, 메시지 유실시 복구가 가능하다.

그러나 HIDV은 스푸핑 공격은 막지 못한다. 예를 들어, 공격자는 임의의 태그에 질의를 함으로서 ②의 정보를 받을 수 있으며, 해당 태그가 다음 번 인증 세션을 열지 않는 사이에 얻은 ② 정보를 이용하여 정당한 판독기에 인증을 받을 수 있다. 이와 같은 공격은 판독기나 데이터베이스가 모두 감지할 수 없어 공격자는 정당한 태그로 인증된다. ②를 공격자에게 준 태그 또한 ⑤번 정보를 받지 못해 갱신을 못했다고만 여겨 스푸핑 공격을 감지하지 못한다. 이러한 스푸핑 공격을 통해 공격자들은 정당한 판독기로부터 인증을 받을 수 있다. 다른 문제점으로 태그는 세 가지의 메모리를 가져야하며, 해쉬연산도 세 번을 수행하므로 태그의 가격이 올라간다는 문제점을 들 수 있다.

발명이 이루고자 하는 기술적 과제

본 발명이 이루고자 하는 첫 번째 기술적 과제는 기존 인증시스템 및 인증방법들보다 더 많은 보안 고려사항들을 만족하며 저가의 태그에 유용한, RFID 인증 시스템을 제공하는 것이다.

본 발명이 이루고자 하는 두 번째 기술적 과제는 상기 RFID 인증 시스템에서의 RFID 인증방법을 제공하는 것이다.

본 발명이 이루고자 하는 세 번째 기술적 과제는 상기 RFID 인증방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공하는 것이다.

발명의 구성

상기 기술적 과제를 이루기 위한 본 발명에 의한 RFID 인증 시스템은, 태그, 판독기 및 데이터베이스를 구비하는 RFID 인증 시스템에 있어서, ID를 저장하고 있으며, 질의가 오면 상기 ID의 해쉬함수 값 $h(ID)$ 를 생성하여 판독기로 전송하고, 상기 ID와 랜덤값 R 을 연결 연산한 값 $(ID \parallel R)$ 의 해쉬함수 값 $h(ID \parallel R)$ 에 대한 왼쪽 반($half_L(h(ID \parallel R))$)을 수신하면 상기 $h(ID \parallel R)$ 에 대한 오른쪽 반($half_R(h(ID \parallel R))$)을 생성하여 판독기로 전송하고, 태그인증이 완료되면 상기 ID를 상기 ID와 R 을 배타논리합 한 값 $(ID \oplus R)$ 으로 갱신하는 태그; 상기 태그에 질의하여 $h(ID)$ 를 수신하면 데이터베이스로 전송하고, 데이터베이스로부터 $h(ID \parallel R)$ 를 수신하면 이에 대한 왼쪽 반($half_L(h(ID \parallel R))$) 및 R 을 태그로 전송하는 판독기; 및 상기 태그 정보(DATA), ID, 상기 ID의 해쉬값(HID) 및 랜덤값 생성기(R.N.G)를 구비하며, 상기 $h(ID)$ 를 수신하면 이를 이용하여 태그의 정보를 찾아 확인하고, 상기 R 및 $h(ID \parallel R)$ 를 생성하여 판독기로 전송하고, 태그인증이 완료되면 ID를 $ID \oplus R$ 로 갱신하는 데이터베이스를 포함하는 것을 특징으로 한다.

상기 기술적 과제를 이루기 위한 본 발명에 의한 RFID 인증 시스템에서의 RFID 인증 방법은, 태그, 판독기 및 데이터 베이스를 구비하는 RFID인증 시스템에서의 RFID인증방법에 있어서, 판독기가 태그에 인증을 위한 질의하는 단계; 상기 질의에 대해 태그 ID를 해쉬한 값 $h(ID)$ 를 판독기에 전송하는 단계; 상기 $h(ID)$ 를 받으면, 이를 데이터베이스에 전송하는 단계; 상기 판독기로부터 $h(ID)$ 를 받으면, 상기 데이터베이스는 $h(ID)$ 를 통해 태그의 정보를 찾아 확인하고, 랜덤 값 R 과, 상기 ID와 R 을 연결연산하여 해쉬함수한 값 $h(ID \parallel R)$ 을 생성하여 판독기로 전송하는 단계; 상기 R 및 $h(ID \parallel R)$ 를 수신하면, $h(ID \parallel R)$ 의 왼쪽 반인 $half_L(h(ID \parallel R))$ 및 R 을 태그에 전송하는 단계; 상기 R 및 $half_L(h(ID \parallel R))$ 를 받으면, 태그는 상기 R 및 $half_L(h(ID \parallel R))$ 가 자신이 만든 $h(ID \parallel R)$ 의 왼쪽과 일치한다면 받은 정보가 타당함을 확인하고, 판독기에게 $h(ID \parallel R)$ 의 오른쪽인 $half_Rh(ID \parallel R)$ 을 보내는 단계; 및 인증이 완료되면 상기 데이터베이스 및 태그는 ID를 상기 ID와 상기 랜덤값 R 을 배타논리합 한 값 $(ID \oplus R)$ 으로 갱신하는 단계를 포함하는 것을 특징으로 한다.

상기 기술적 과제를 이루기 위한 본 발명에 의한 RFID 인증 시스템은, 판독기, 태그 및 데이터베이스를 구비하는 RFID 인증시스템에 있어서, ID를 저장하며, 질의 및 랜덤값(S)이 오면 상기 ID를 해쉬함수한 값 $h(ID)$ 및 상기 R 의 왼쪽 반에 해당하는 $half_L(R)$ 을 생성하여 판독기로 전송하고, 판독기로부터 R 의 오른쪽 반에 해당하는 $half_R(R)$ 을 수신하여 자신이 생성한 것과 일치하는지 체크하고, 인증이 완료되면 ID를 상기 ID와 $R \parallel R$ 을 배타논리합 한 값 $(ID \oplus (R \parallel R))$ 으로 갱신하는 태그; 랜덤숫자생성기(R.N.G)를 구비하며, 태그에 질의할 때 상기 R.N.G에서 생성된 랜덤숫자(S)를 함께 전송하며, 태그로부터 $h(ID)$ 및 $half_L(R)$ 을 수신하면 S, $h(ID)$ 및 $half_L(R)$ 을 데이터베이스로 전송하고, 데이터베이스로부터 상기 $half_R(R)$ 을 수신하면 이를 태그로 전송하는 판독기; 및 상기 RFID 태그의 정보(DATA), 상기 ID, ID의 해쉬값(HID) 및 메모리 연결을 위한 데이터베이스 엔트리(AE)를 구비하며, 판독기로부터 $h(ID)$, S 및 R 의 오른쪽 반 값인 $half_L(R)$ 을 수신하면 $h(ID)$ 를 통해 태그의 정보를 확인하고, ID와 S를 이용하여 R 을 생성하며, 상기 R 의 왼쪽부분이 판독기로부터 받은 값과 같다면 태그를 정당하다고 판단하고 자신의 인증을 위해 $half_R(R)$ 을 생성하여 판독기로 전송하며, 상기 R 을 통해 ID를 $ID = ID \oplus (R \parallel R)$ 로 갱신하며 상기 갱신되는 정보들은 AE에 의해 연결되는 메모리에 저장하는 데이터베이스를 포함하는 것을 특징으로 한다.

상기 기술적 과제를 이루기 위한 본 발명에 의한 RFID 인증 시스템에서의 RFID 인증 방법은, RFID태그, 판독기 및 데이터 베이스를 구비하는 RFID인증 시스템에서의 RFID인증방법에 있어서, 판독기가 랜덤 값 S 를 생성하여 태그에게 질의하면 상기 S를 전송하는 단계; 상기 S와 함께 질의를 받으면, 상기 태그는 $h(ID \parallel S)$ 를 R 값으로 생성하고, ID의 해쉬함수 값 $h(ID)$ 및 상기 R 의 왼쪽 반 값인 $half_L(R)$ 을 생성하여 상기 판독기로 전송하는 단계; 상기 판독기는 태그로부터 받은 정보와 함께 S를 같이 데이터베이스로 전송하는 단계; 상기 $h(ID)$, S, $half_L(R)$ 을 받으면, 데이터베이스는 $h(ID)$ 를 통해 태그의 정보를 확인하고, ID와 S를 이용하여 R 을 생성하고, 생성된 R의 왼쪽부분이 판독기로부터 받은 값과 같다면 태그를 정당하다고 판단하고, 자신의 인증을 위해 R의 오른쪽 부분인 $half_R(R)$ 을 판독기로 전송하며, 데이터베이스는 R을 통해

ID 를 $ID = ID \oplus (R \parallel R)$ 로 갱신하며 갱신되는 정보들은 AE에 의해 연결되는 메모리에 저장하는 단계; half_R(R)를 받으면, 판독기는 태그에게 half_R(R)를 전송하는 단계; 및 세션이 안전하게 끝나면, 태그와 데이터베이스는 ID 를 $ID \oplus (R \parallel R)$ 로 갱신하는 단계를 포함하는 것을 특징으로 한다.

본 발명은 상기 세 번째 기술적 과제를 달성하기 위하여, 상기 RFID 인증방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공한다.

이하, 첨부된 도면들을 참조하여 본 발명에 따른 RFID 태그 인증 시스템 및 그 방법을 상세히 설명한다. 본 발명에 의한 RFID 인증 시스템에서 RFID 태그는 메모리와 해쉬 함수를 가진다. RFID 태그는 그 기능에 따라, 수동형 태그와 능동형 태그로 나눌 수 있는데, 본 발명에서 쓰이는 태그는 읽기/쓰기가 가능한 태그로 능동형 태그이다. 암호학적 해쉬 함수는 $y=h(x)$ 로 정의하며, y를 통해 x에 어떠한 부분정보도 얻지 못한다. 현실적으로 하드웨어에 적합한 암호학적 일방향 해쉬함수는 충분하므로, 이를 통해 RFID 인증 프로토콜의 안전성을 주장한다. 현재의 저가형 태그는 보통 200~2,000개의 게이트를 가진다. SHA-1과 같은 표준 암호학적 해쉬함수의 수행을 위해서는 대략 20,000개의 게이트가 필요하나 이는 가까운 미래에 저가의 태그에서 이용가능하게 될 것으로 예상된다.

한편, RFID 인증 시스템 및 그 방법에서의 보안 고려사항은 다음과 같다. RFID 인증 프로토콜의 예를 들어보자. 현재의 물류 창고에는 물류 창고에 드나드는 차량들이나 사람들의 타당성을 확인하기 위해 경비원이 필요하지만 RFID 인증 시스템을 이용하면 자동화를 실현할 수 있다. 물류창고 입구에 판독기를 설치하고 인증된 태그를 장착한 차량과 사람만이 출입이 가능하도록 한다. RFID 인증 시스템에서 판독기와 태그간의 통신은 무선으로 불안전하며, 판독기와 데이터베이스간의 통신은 유선으로 안전하다 가정한다. 따라서 다음과 같은 보안 요구 사항을 만족해야한다.

(1) 도청(Eavesdropping) : 판독기와 태그 간의 통신은 무선통신으로 도청 가능하다. (2) 트래픽 분석(Traffic Analysis) : 도청 가능한 공격자는 도청된 내용을 가지고 임의의 정보를 분석해 낼 수 있다. (3) 재전송 공격(Replay Attack) : 공격자는 도청된 내용을 정당한 판독기에게 재전송할 수 있다. (4) 스푸핑 공격(Spoofing Attack) : 공격자는 임의의 태그에게 판독기인 척하여 정당한 태그의 정보를 얻어내고, 정당한 판독기에게 태그로부터 얻은 정보를 보여줌으로써 정당한 태그인 척 가장할 수 있다. (5) 서비스 거부(Denial of Service) : 공격자는 자신이 RFID 시스템으로부터 유용한 정보를 얻지 못하더라도 태그와 판독기간의 RF통신에 잡음을 넣거나 통신 내용을 왜곡시킬 수 있다. (6) 메세지 유실 : 공격자에 의한 서비스 거부나 통신상의 문제로 데이터가 훼손, 유실될 수 있다. (7) 물리적인 공격 : 공격자는 태그를 훔치는 등 태그에 대한 물리적인 공격이 가능하다.

한편, 본 발명에서는 상기 RFID 태그 인증 시스템에 대해 크게 두 개의 실시예를 제공한다. 제1실시예는 Improved Hash-based ID Variation-1 (이하 IHIDV-1라 한다.)이며, 제2실시예는 Improved Hash-based ID Variation-2 (이하 IHIDV-2라 한다.)이다.

상기 IHIDV-1은 메모리량과 해쉬 연산량을 줄여 저가의 태그에 유용하다. 상기 IHIDV-1은 재전송 공격이나 스푸핑 공격을 예방하지 못하지만 감지가 가능하므로, 이와 같은 공격이 적은 환경에서 저가의 태그 인증 프로토콜로 활용 가능하다.

태그는 인증을 위한 랜덤 값 ID 만을 가지며, 데이터베이스는 태그 정보인 DATA 와 ID 의 해쉬값인 HID, ID를 갖는다. 이와 같은 입력은 사전엔 RF통신이나 물리적인 접촉을 통해 안전하게 이루어진다. 표 3은 IHIDV-1 의 구성요소 및 연산도구를 나타낸 것이다.

[표 3]

	필요한 메모리	연산도구
태그	$h()$	$h()$, $\oplus$
판독기	-	-
데이터베이스(DB)	HID, $h()$, DATA	$h()$, R.N.G, $\oplus$

여기서, ID는 인증을 위한 랜덤 값으로 인증성공시 마다 변화하며, HID는 ID의 해쉬값($=h(ID)$), DATA는 사용자 정보, 태그 정보와 같은 실질적인 데이터이며, $h()$ 는 일방향 해쉬 함수, R,N,G는 랜덤 숫자 생성기, $\oplus$ 는 XOR 연산(exclusive-or function), $\parallel$ 는 연결연산(concatenate function)이며, $half_L()$ 는 입력되는 값의 왼쪽 반을 출력하는 함수이며, $half_R()$ 는 입력되는 값의 오른쪽 반을 출력하는 함수이다.

도 4는 본 발명에 의한 RFID 태그 인증 시스템의 제1실시예에 대한 구성을 블록도로 도시한 것으로서, 태그(400), 판독기(420) 및 데이터베이스(440)를 포함하여 이루어진다.

상기 태그(400)는 인증을 위한 랜덤값 ID를 저장하고 있다. 상기 태그(400)는 상기 판독기(420)로부터 질의가 들어오면 상기 ID를 해쉬함수한 값 $h(ID)$ 를 생성하여 판독기로 전송한다. 그리고 상기 태그(400)는 상기 ID와 랜덤값 R을 연결 연산한 값($ID \parallel R$)을 해쉬함수한 값 $h(ID \parallel R)$ 에 대한 왼쪽 반을 취한 값 $half_L(h(ID \parallel R))$ 을 생성하여 상기 판독기(420)로 전송하며, 태그에 대한 인증이 완료되면 상기 ID를 상기 ID와 R을 배타논리합 한 값($ID \oplus R$)으로 갱신한다.

상기 판독기(420)는 상기 태그(400)에 태그 인증을 위한 질의를 하며, 질의 결과 상기 태그(400)로부터 상기 ID의 해쉬함수 값 $h(ID)$ 를 수신하면 상기 $h(ID)$ 를 데이터베이스(440)로 전송하고, 데이터베이스(440)로부터 상기 ID와 랜덤값 R을 연결연산(concatenate function)한 값 $ID \parallel R$ 에 대해 해쉬함수를 취한 값 $h(ID \parallel R)$ 를 수신하면 이에 대한 왼쪽 반($half_L(h(ID \parallel R))$) 및 상기 R을 태그(400)로 전송한다.

상기 데이터베이스(440)는 상기 태그 정보(DATA), 상기 ID, 상기 ID의 해쉬값(HID) 및 랜덤값 생성기(R.N.G)를 저장하고 있다. 상기 데이터베이스(440)는 판독기(420)로부터 상기 $h(ID)$ 를 수신하면 이를 이용하여 태그의 정보를 찾아 확인하고, 상기 R.N.G를 이용하여 생성한 랜덤값 R과, ID와 상기 R을 연결연산하여 해쉬함수를 취한 값 $h(ID \parallel R)$ 를 생성하여 판독기(420)로 전송한다. 또한 태그인증이 완료되면 ID를 $ID \oplus R$ 로 갱신한다. 또한 상기 데이터베이스(440)는 태그정보(DATA), HID 및 ID를 RF통신이나 물리적인 접촉을 통해 안전하게 입력받는다.

여기서 상기 태그(400), 판독기(420), 데이터베이스(440)에서 상기 왼쪽 반($half_L(h(ID \parallel R))$)은 오른쪽 반($half_R(h(ID \parallel R))$)으로 대체할 수 있으며, 이 때 상기 오른쪽 반($half_R(h(ID \parallel R))$)은 왼쪽 반($half_L(h(ID \parallel R))$)으로 된다.

다음으로 상기 제1실시예인 IHIDV-1에 대한 RFID 인증방법을 설명하기로 한다. 도 5는 본 발명의 제1실시예인 IHIDV-1에 대한 RFID 인증방법을 설명하기 위한 흐름도를 도시한 것이다.

도 5를 참조하면, 먼저 판독기(420)가 태그(400)에게 질의한다.(참조번호 ①) 판독기(420)로부터 질의를 받은 태그(400)는 자신의 가진 ID를 해쉬한 값 $h(ID)$ 를 판독기(420)에 전송한다.(참조번호 ②) 그러면 판독기(420)는 상기 ②에서 받은 정보를 데이터베이스(440)에 전송한다.(참조번호 ③) 데이터베이스(440)는 $h(ID)$ 를 통해 태그(400)의 정보를 찾아 확인하고, ID를 갱신하기 위한 랜덤 값 R을 생성한다. 그리고 R과 함께 판독기(420)나 공격자가 R를 조작하는 것을 방지하기 위해 $h(ID \parallel R)$ 을 생성해 같이 보낸다.(참조번호 ④) 판독기(420)는 태그(400)에게 R과 $h(ID \parallel R)$ 의 왼쪽 반인 $half_L(h(ID \parallel R))$ 을 전송한다.(참조번호 ⑤)

상기 R과 $half_L(h(ID \parallel R))$ 를 받은 태그(400)는 ⑤에서 받은 정보가 자신이 만들 수 있는 $h(ID \parallel R)$ 의 왼쪽과 일치한다면, 자신이 받은 정보가 타당함을 확인하고, 자신도 판독기(420)에게 $h(ID \parallel R)$ 의 오른쪽인 $half_R(h(ID \parallel R))$ 을 보냄으로써 R을 제대로 받았음을 알린다.(참조번호 ⑥)

위와 같은 세션이 정상적으로 완료되면 태그(400)는 인증되고, 데이터베이스와 태그의 ID는 $ID = ID \oplus R$ 로 갱신한다.

상기 제1실시예인 IHIDV-1의 안전성 및 장·단점은 다음과 같다. 상기 IHIDV-1은 데이터베이스(440)에 태그(400)의 개인 정보 DATA가 저장되고 이는 안전하다 가정하므로 개인 정보 프라이버시를 만족하며, 데이터베이스가 생성한 랜덤 값 R에 의해서 ID가 갱신됨으로써 위치 프라이버시를 보장한다.

공격자는 도청에 의해 얻은 ②를 재전송할 수 있지만, 이미 전 단계에서 데이터베이스가 저장하는 HID 값이 바뀌었으므로 공격은 성공되지 못한다. IHIDV-1은 스푸핑 공격을 예방하지는 못하지만, 감지가 가능하다. 공격자는 임의의 태그에게 질의를 하여 $h(ID)$ 를 얻을 수 있으며, 정당한 판독기에게 인증을 요구한다. 정당한 태그가 다음 인증 세션을 요청하지 않았다면, 판독기는 공격자를 정당하다고 판단하고 ⑤를 전송한다. 그러나 공격자가 ⑥을 보내지 않으므로 판독기는 스푸핑 공격을 감지하게 된다. 판독기와 태그가 ⑤, ⑥을 서로 주고 받는 것은 메시지 유실에 대한 감지 기능도 수행한다.

다음으로, 본 발명에 의한 RFID 인증시스템의 제2실시예인 IHIDV-2를 설명하기로 한다. 상기 IHIDV-2의 태그는 IHIDV-1과 같이 ID를 위한 메모리와 해쉬 함수만을 가진다. 그리고 태그에게 요구되어지는 해쉬 연산량은 두 번이다. IHIDV-2의 장점은 재전송 공격이나 스푸핑 공격을 예방하며, 메시지 유실 시에도 복구가 가능한 것으로, 이러한 목적을 달성하기 위해서 판독기가 R.N.G를 가진다고 가정한다. 그리고 본 프로토콜에서 쓰이는 해쉬 함수는 R.N.G를 L비트라고 했을 때, $h\{0,1\}^* \rightarrow \{0,1\}^{\frac{1}{2}L}$ 라 가정한다. 표 4는 IHIDV-2의 구성요소 및 연산도구를 나타낸 것이다.

[표 4]

	필요한 메모리	연산도구
태그	ID	$h()$, $\oplus$
판독기	-	R.N.G
데이터베이스(DB)	HID, $h()$, DATA, AE	$h()$, $\oplus$

표 4에서, ID는 인증을 위한 랜덤 값으로 인증 성공시 마다 변화하며, HID는 ID의 해쉬값($=h(ID)$), DATA는 사용자 정보, 태그정보와 같은 실질적인 데이터이며, AE는 메모리 연결을 위한 연결된 데이터베이스 엔트리(entry)이며, $h()$ 는 일방향 해쉬 함수, S는 판독기가 R.N.G를 이용하여 매 세션마다 생성하는 랜덤 값으로 R 생성시 사용하며, R은 데이터 베이스와 태그가 ID와 S를 이용하여 $h(ID \parallel S)$ 로 생성하며, ID를 갱신하는데 사용하며, R.N.G는 랜덤 숫자 생성기, $\oplus$ 는 XOR 연산(exclusive-or function), $\parallel$ 는 연결연산(concatenate function)이며, $half_L()$ 는 입력되는 값의 왼쪽 반을 출력하는 함수이며, $half_R()$ 는 입력되는 값의 오른쪽 반을 출력하는 함수이다.

도 6은 본 발명에 의한 RFID 태그 인증 시스템의 제2실시예에 대한 구성을 블록도로 도시한 것으로서, 태그(600), 판독기(620) 및 데이터베이스(640)를 포함하여 이루어진다.

상기 태그(600)는 ID를 저장하며, 판독기(620)으로부터 질의 및 랜덤값(S)이 오면 상기 ID를 해쉬함수한 값 $h(ID)$ 및 상기 R의 왼쪽 반에 해당하는 $half_L(R)$ 을 생성하여 판독기(620)로 전송한다 또한 판독기(620)로부터 상기 R의 오른쪽 반에 해당하는 $half_R(R)$ 를 수신하여 자신이 생성한 것과 일치하는지 체크하고, 인증이 완료되면 ID를 상기 ID와 $R \parallel R$ 을 배타 논리합 한 값($ID \oplus (R \parallel R)$)으로 갱신한다.

상기 판독기(520)는 랜덤숫자생성기(R.N.G)를 구비하며, 태그(600)에 질의할 때 상기 R.N.G에서 생성된 랜덤숫자(S)를 함께 전송하고, 태그(600)로부터 $h(ID)$ 및 $half_L(R)$ 를 수신하면 상기 S, $h(ID)$ 및 $half_L(R)$ 를 데이터베이스(640)로 전송한다. 또한 데이터베이스(640)로부터 상기 $half_R(R)$ 를 수신하면 이를 태그(600)에게 전송한다.

상기 데이터베이스(540)는 상기 태그(600)의 일반적인 정보(DATA), 상기 ID, ID의 해쉬값(HID) 및 메모리 연결을 위한 데이터베이스 엔트리(AE)를 구비하며, 판독기(620)로부터 $h(ID)$, S 및 상기 R의 오른쪽 반 값인 $half_L(R)$ 을 수신하면 $h(ID)$ 를 통해 태그의 정보를 확인하고, ID와 S를 이용하여 R을 생성하며, 상기 R의 왼쪽부분이 판독기로부터 받은 값과 같다면 태그를 정당하다고 판단하고 자신의 인증을 위해 $half_R(R)$ 를 생성하여 판독기로 전송한다. 또한 상기 R을 통해 ID를 $ID = ID \oplus (R \parallel R)$ 로 갱신하며 상기 갱신되는 정보들은 AE에 의해 연결되는 메모리에 저장한다.

여기서 상기 태그(600), 판독기(620), 데이터베이스(640)에서 상기 왼쪽 반($half_L(h(ID \parallel R))$)은 오른쪽 반($half_L(h(ID \parallel R))$)으로 대체할 수 있으며, 이 때 상기 오른쪽 반($half_L(h(ID \parallel R))$)은 왼쪽 반($half_L(h(ID \parallel R))$)으로 된다.

다음으로 상기 제2실시예인 IHIDV-2에 대한 RFID 인증방법을 설명하기로 한다. 도 7은 본 발명의 제2실시예인 IHIDV-2에 대한 RFID 인증방법을 설명하기 위한 흐름도를 도시한 것이다.

도 7을 참조하면, 먼저 판독기(620)는 태그(600)에게 질의를 보낼 때, 랜덤 값 S를 생성해서 같이 보낸다.(참조번호 ①) 판독기(620)로부터 랜덤값 S와 함께 질의를 받으면, 태그(600)는 두 가지 데이터를 생성한다. 첫 번째는 $h(ID)$ 값으로 해

당 태그의 정보는 찾는 데 이용된다. 두 번째는 R 값으로 이는 $h(ID \parallel S)$ 로 생성된다. R 은 나중에 세션이 다 끝난 후, ID 를 갱신하기 위해 쓰이며, 현재는 데이터베이스와 태그가 서로 같은 R 을 생성했는지 확인함과 동시에 인증을 위해 R 의 왼쪽 부분인 $half_L(R)$ 만을 전송한다.(참조번호 ②)

그 다음에 판독기(620)는 태그(600)로부터 받은 정보와 함께 S 를 같이 데이터베이스(640)로 전송한다.(참조번호 ③)

데이터베이스(640)는 $h(ID)$ 를 통해 태그(600)의 정보를 확인하고, ID 와 S 를 이용하여 R을 생성한다. 생성된 R 의 왼쪽 부분이 판독기(620)로부터 받은 값과 같다면 태그를 정당하다고 판단하고 자신의 인증을 위해 R 의 오른쪽 부분인 $half_R(R)$ 을 전송한다. 이와 함께, 데이터베이스(640)는 R 을 통해 ID 를 $ID = ID \oplus (R \parallel R)$ 로 갱신하며 갱신되는 정보들은 AE에 의해 연결되는 메모리에 저장된다.(참조번호 ④) 판독기(620)는 ④의 내용을 태그(600)에게 전송한다.(참조번호 ⑤)

세션이 안전하게 끝나는 경우, 태그와 데이터베이스는 $ID = ID \oplus (R \parallel R)$ 로 갱신한다. 이와 같이 하는 이유는 기존에 제시된 인증방법들과 달리 본 발명에서 생성되는 R은 해쉬함수에 의해 생성된 값으로 1/2 L비트이기 때문이다.

상기 제2실시예인 IHIDV-2의 안전성 및 장·단점은 다음과 같다. 상기 IHIDV-2은 데이터베이스(640)가 태그(600)의 실질적인 개인 정보를 보관하므로 개인 정보 프라이버시를 보장하며, 올바른 인증 세션마다 태그에 저장된 ID 값이 매번 바뀌므로 위치 프라이버시를 만족한다.

정당한 판독기가 태그의 ID 값을 알아내려고 하는 공격을 생각해 보면, 판독기가 ID를 알아내기 위하여 S를 자신에게 유리한 값으로 보내어도, 해쉬 함수의 성질에 의하여 판독기는 R 과 S 를 사용하여 ID 값을 유추할 수 없다. 공격자가 도청을 통해 $h(ID)$ 를 재전송하는 경우, 정당한 판독기는 매번 랜덤한 S 를 전송하게 되므로 공격자는 $half_L(R)$ 을 생성할 수 없어 데이터베이스로부터 인증을 받을 수 없으며, 이와 같은 이유로 스푸핑 공격도 불가능하다. 이는 HIDV의 단점을 극복한다. 즉, IHIDV-2는 판독기에 R,N,G 를 둬으로써 HIDV에 요구되는 1/3 의 메모리에 두 번의 해쉬 연산을 가지고 재전송 공격과 스푸핑 공격을 예방한다.

그리고, HIDV에서처럼 데이터베이스에 하나의 태그 당 두 개의 메모리 행이 존재하고, AE 에 의해 두 행이 연결되어 있어 메시지 유실 시에도 복구가 가능하다.

상기 IHIDV-2에 대한 예를 설명하면 다음과 같다. IHIDV-2가 진행되는 과정을 실제적인 예를 통해 알아본다. ID= 14의 값을 가지는 임의의 태그를 가정해 보자. 초기화 단계에 데이터베이스에는 그 태그에 대한 정보 DATA 와 함께 HID=h(14), ID=14 가 저장된다. 이때, AE 에는 아무것도 저장되지 않는다. 표 5는 초기화된 데이터 베이스의 메모리를 나타낸 것이다.

[표 5]

HID	ID	AE	DATA
h(14)	14	-	사용자 정보, 태그정보 등

정당한 판독기가 S=5 를 생성해서 태그에게 질의를 하면 태그는 $R=h(ID \parallel S) = h(14 \parallel 15)$ 를 생성한다. 이때 생성된 R 을 3이라 하자. 태그는 판독기에게 $h(14)$ 와 $half_L(3)$ 을 전송한다. 판독기는 태그로부터 받은 정보와 함께 R 을 데이터베이스에 전송한다. 데이터베이스는 $h(14)$ 를 이용하여 ID 를 확인하고 R 을 생성하여 정당한 태그인지 인증한다. 인증한 후, 데이터베이스는 표 6 과 같이 갱신된다. 표 6은 첫 번째 인증세션 후, 데이터베이스의 메모리를 나타낸 것이다.

[표 6]

HID	ID	AE	DATA
h(14)	14	$h(14 \oplus (3 \parallel 3))$	사용자정보, 태그정보 등
$h(14 \oplus (3 \parallel 3))$	$14 \oplus (3 \parallel 3)$	h(14)	사용자정보, 태그정보 등

데이터베이스는 하나의 태그에 대해 두 개의 메모리 행을 가진다. 이는 상술한 HIDV와 같은 방법으로 AE에 의해 서로 연결되어 있다. 데이터베이스의 갱신 후, 데이터베이스가 half_R(3)을 전송하고 태그가 그 정보를 정상적으로 받는다면 태그에 저장되어 있는 ID는 $ID = h(14 \oplus (3 \parallel 3))$ 로 바뀌게 된다.

메시지 유실 시를 고려해 보자. 위의 경우, 태그가 마지막의 half_R(3)을 받지 못했다면, 데이터베이스는 갱신되었지만, 태그의 ID 정보는 갱신되지 못한다. 그러므로 태그는 다음 번 인증 세션에 $HID=h(14)$ 를 보내게 된다. 그러나, 데이터베이스는 h(14)를 찾을 수 있으므로 이를 이용하여 인증하고, AE에 의해 연결된 메모리 행을 새로 생성된 R로 갱신한다. 이러한 과정을 통해 메시지 유실시 복구가 가능하다.

본 발명은 컴퓨터로 읽을 수 있는 기록 매체에 컴퓨터(정보 처리 기능을 갖는 장치를 모두 포함한다)가 읽을 수 있는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록 매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다. 컴퓨터가 읽을 수 있는 기록 장치의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피 디스크, 광데이터 저장장치 등이 있다.

본 발명은 도면에 도시된 실시예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

이하, 본 발명과 기존의 RFID인증시스템 및 그 방법에 따른 효과를 비교하면 다음과 같다.

IHIDV-2의 경우 태그는 상술한 IHIDV 프로토콜에서 요구하는 메모리의 $\frac{1}{3}$ 을 요구하며 한번의 인증 세션을 위해 두 번의 해쉬 연산을 수행한다. 그리고 개인 정보 프라이버시 및 위치 프라이버시 보장은 물론, 재전송 공격과 스푸핑 공격이 모두 불가능하며, 메시지 유실 시에도 복구가 가능하다.

기존 RFID인증 프로토콜들과 본 발명을 비교 분석해 본다. 메모리량 비교를 위해서 ID를 비롯한 모든 구성 요소들을 모두 L비트로 가정하고, 해쉬함수는 $h(\{0,1\}^* \rightarrow \{0,1\}^{\frac{1}{2}L})$ 라 하여, 해쉬값이 저장되는 메모리는 $\frac{1}{2}L$ 비트로 계산한다.

기존의 프로토콜들은 태그에게 2L 혹은 3L비트의 메모리가 필요하지만, 본 발명들은 단지 L비트만의 메모리를 요구한다. 데이터베이스도 상술한 HIDV보다 적은 양의 메모리가 요구되어진다. 해쉬 연산의 경우 HIDV의 태그는 태그 인증과 재전송 공격을 예방하기 위해 총 세 번의 연산을 수행하지만, 본 발명들은 두 번의 연산으로 인증 프로토콜의 보안 고려사항을 만족한다. 표 7은 메모리 및 연산량 비교를 나타낸 것이다.

[표 7]

		HIDV [3]	HIDV [5]	IHIDV-1	IHIDV-2
메모리 량	태그	2L	3L	1L	1L
	판독기	-	-	-	-
	데이터베이스	2L	10L	2L	8L
연산도구	태그	해쉬 함수	해쉬 함수	해쉬 함수	해쉬 함수
	판독기	-	-	-	R, N, G
	데이터베이스	해쉬 함수	해쉬 함수 R, N, G	해쉬 함수 R, N, G	해쉬 함수
해쉬 함수 연산 량	태그	1	3	2	2
	판독기	-	-	-	-
	데이터베이스	-	3	2	2

HIDV와 본 발명들은 개인 정보 프라이버시와 위치 프라이버시를 만족한다. IHIDV-1은 재전송 공격과 스푸핑 공격, 메시지 유실을 감지한다. HIDV는 재전송 공격을 막고 메시지 유실시 복구가 가능하지만, 스푸핑 공격을 감지하지 못한다. 이와는 달리 IHIDV-2는 상술한 IHIDV의 $\frac{1}{3}$ 에 메모리와 두 번의 해쉬 연산으로 재전송 공격, 스푸핑 공격을 예방하며, 메시지 유실시에도 복구가 가능하다. 표 8은 공격에 대한 안정성 비교를 나타낸 것이다.

[표 8]

	HL [3]	HIDV [5]	IHIDV-1	IHIDV-2
개인 정보 프라이버시	보장 안 됨	보장	보장	보장
위치 프라이버시	보장 안 됨	보장	보장	보장
도청에 의한 재 전송 공격	감지	예방	감지	예방
스푸핑 공격	공격됨	공격됨	감지	예방
메시지 유실	감지	복구	감지	복구

본 발명에 의한 IHIDV-1은 메모리량과 해쉬 연산량을 줄여 저가의 태그에 유용하다. 상기 IHIDV-1은 상술한 종래의 HIDV에 비해 태그에게 요구되는 메모리량이 1/2로 적으며 해쉬 연산은 두 번 수행한다. 그러므로 태그의 비용을 감소시킬 수 있다. 이러한 특징을 적용하여 IHIDV-1은 저가의 태그를 사용해야하고 스푸핑 공격이나 메시지 유실의 가능성이 적은 시스템에서 활용할 수 있다. 이는 몇 년 안의 저가의 태그에 이용 가능하므로, 여러 가지의 유비쿼터스 환경에 유용할 것이다. 본 발명들은 저가의 태그에 유용할 뿐만 아니라, 재전송 공격, 스푸핑 공격을 감지하거나 예방하며, 메시지 유실 시에 복구가 가능하다는 것을 장점으로 들 수 있다.

발명의 효과

상기에서 살펴본 바와 같이, 본 발명에 따른 RFID 인증시스템 및 그 방법에 의하면, 저가의 태그에 유용할 뿐만 아니라, 재전송 공격, 스푸핑 공격을 감지하거나 예방하며, 메시지 유실시에 복구가 가능하다는 장점이 있다.

도면의 간단한 설명

도 1은 RFID 인증 프로토콜 모델을 도시한 것이다.

도 2는 HL의 인증과정을 도시한 것이다.

도 3는 HIDV의 인증과정을 도시한 것이다.

도 4는 본 발명에 의한 RFID 태그 인증 시스템의 제1실시예에 대한 구성을 블록도로 도시한 것이다.

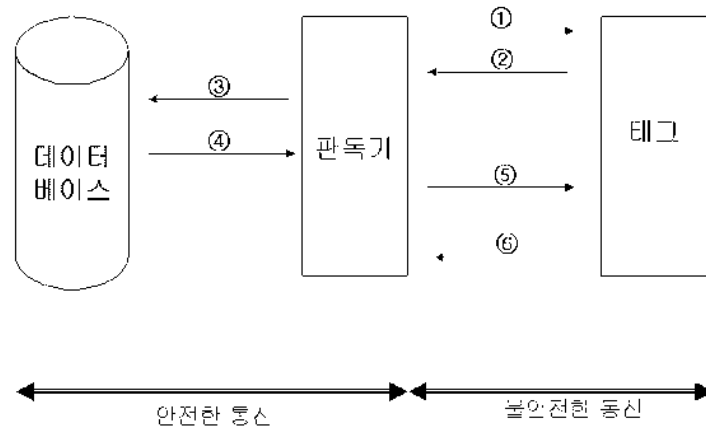
도 5는 본 발명의 제1실시예에 대한 RFID 인증방법의 흐름도이다.

도 6은 본 발명에 의한 RFID 태그 인증 시스템의 제2실시예에 대한 구성을 블록도로 도시한 것이다.

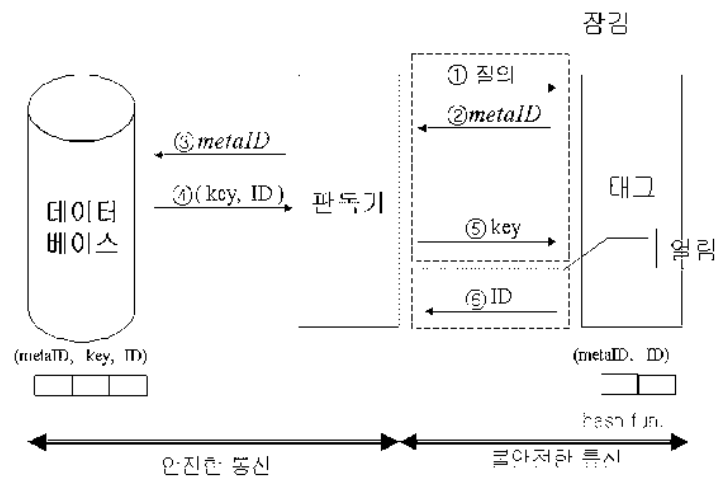
도 7은 본 발명의 제2실시예에 대한 인증방법의 흐름도이다.

도면

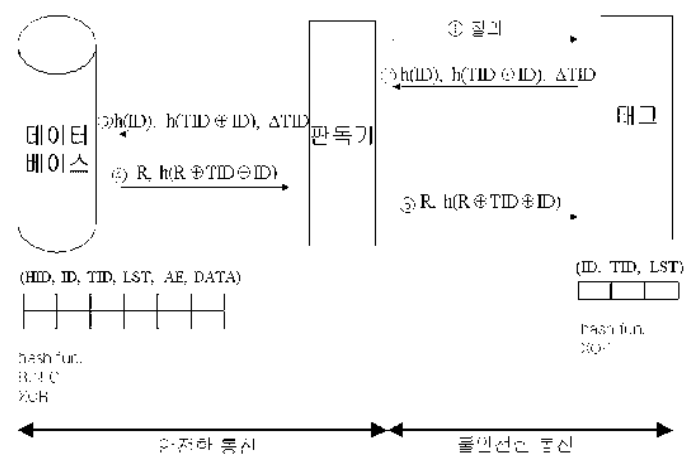
도면1



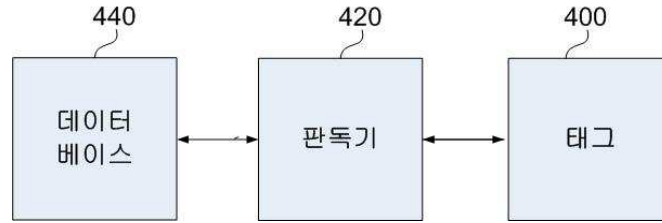
도면2



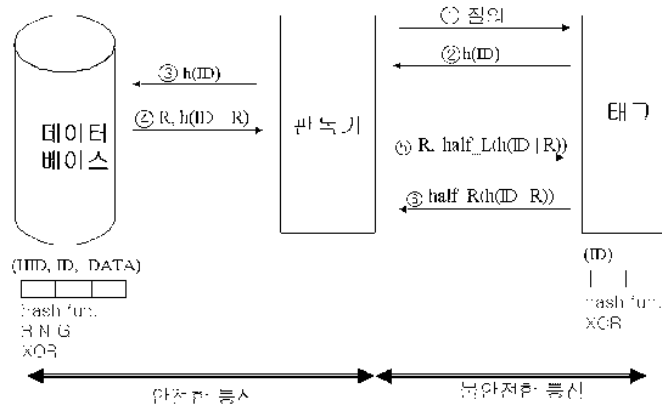
도면3



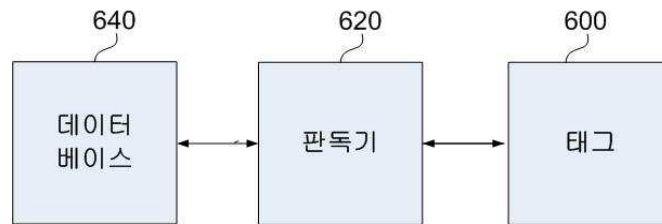
도면4



도면5



도면6



도면7

