(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2009년09월15일
(11) 등록번호 10-0917177
(24) 등록일자 2009년09월07일

(51) Int. Cl.
G06K 17/00 (2006.01) *G06K 19/07* (2006.01)
H04L 9/32 (2006.01)
(21) 출원번호 10-2007-0120343
(22) 출원일자 2007년11월23일
심사청구일자 2007년11월23일
(65) 공개번호 10-2009-0053481
(43) 공개일자 2009년05월27일
(56) 선행기술조사문헌
US20050049979 A1*
JP2005107744 A
KR1020040094061 A
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
포항공과대학교 산학협력단
경상북도 포항시 남구 효자동 산31 포항공과대학교내
(72) 발명자
최홍준
경북 포항시 남구 효자동 포항공과대학교 컴퓨터공학과
홍성제
경북 포항시 남구 지곡동 교수아파트 5-404
김종
경북 포항시 남구 지곡동 교수아파트 8-103
(74) 대리인
리앤목특허법인

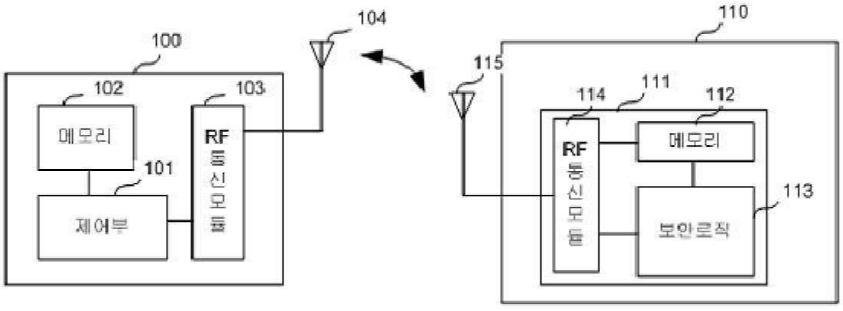
전체 청구항 수 : 총 1 항 심사관 : 김창주

(54) 상품 위조 방지를 위한 오프라인 R F I D 인증 방법

(57) 요 약

본 발명은, RFID 리더가 RFID 태그 내에 안전하게 저장되어 있는 데이터를 읽어 들여, 중앙 서버나 데이터베이스의 접속 없이 리더 내에서의 간단한 연산을 통해 상품의 진위 여부를 판정할 수 있도록 하는 상품 위조 방지를 위한 오프라인 RFID 인증 방법에 관한 것이다. 본 발명의 오프라인 RFID 인증 시스템은 진품 인증을 위해 사용되는 데이터를 안전한 방법으로 저장하고, 리더의 질의에 간단한 연산으로 응답할 수 있는 기능을 가진 RFID 태그와; 상기 태그가 저장하고 있는 데이터의 무결성을 검증하고, 자신이 만든 질의에 대한 태그의 응답의 정당성을 체크하는 기능을 가진 RFID 리더를 포함한다. 본 발명에 의하면, 모든 태그에 대한 정보를 중앙 관리하는 서버가 필요로 하지 않으므로 네트워크 기능이 없는 리더가 간단한 연산만 수행가능하면 쉽게 상품의 진품 여부를 확인할 수 있게 되어, 상품 위조를 방지하고 신뢰성 있는 유통구조를 확립할 수 있다.

대 표 도 - 도1



특허청구의 범위

청구항 1

삭제

청구항 2

삭제

청구항 3

삭제

청구항 4

삭제

청구항 5

삭제

청구항 6

오프라인 RFID 인증 방법에 있어서,

(a) 상품 출하 전 제조자가 상품 인증에 사용되는 정보인 태그의 비밀키와 제조자의 디지털 서명을 만든 후 태그에 저장하고 그 태그를 상품에 부착하는 단계;

(b) 상품 출하 후 리더가 상품에 부착된 태그로부터 정보를 읽어 들여 실제로 그 태그가 정당한 제조자로부터 만들어진 태그인지를 인증하는 단계를 포함하고, 상기 단계 (b)는

(b1) 리더가 태그에게 인증 과정의 시작을 알리는 요청 단계;

(b2) 태그가 자신이 저장하고 있는 제조자의 디지털 서명과 자신의 고유번호를 리더에게 전송하는 단계;

(b3) 리더가 제조자의 서명의 정당성을 확인하고 그 값의 일부를 이용해서 태그에게 질의를 하는 단계;

(b4) 태그가 리더로부터 받은 질의에 자신의 비밀키를 이용해 연산후 그 결과를 리더에게 응답하는 단계;

(b5) 리더가 태그로부터 받은 정보를 추가 연산 후 결과값을 제조자의 서명으로부터 추출한 태그의 값과 비교하여 진품 인증을 마치는 단계를 포함하는 것을 특징으로 하는 상품 위조 방지를 위한 오프라인 RFID 인증 방법.

청구항 7

삭제

청구항 8

삭제

명 세 서

발명의 상세한 설명

기 술 분 야

<1> 본 발명은 RFID 리더가 RFID 태그 내에 안전하게 저장되어 있는 데이터를 읽어 들여, 중앙 서버나 데이터베이스의 접속 없이 리더 내에서의 간단한 연산을 통해 상품의 진위 여부를 판정할 수 있도록 하는 상품 위조 방지를 위한 오프라인 RFID 인증 방법에 관한 것이다.

배 경 기 술

<2> 위조 상품으로 인한 피해는 전 세계적으로 발생하고 있으며 그로 인한 경제적 손실은 해마다 증가하고 있는 추세이다. 2004년 국제 상공회의소의 통계에 따르면 세계 무역규모의 5~7%가 위조 상품 거래로, 그 경제적 피해규모는 한해 50억 달러(USD) 이상으로 추산된다. 또한 상품의 위조로 발생할 수 있는 문제는 상품에만 국한된 것이 아니라, 올바른 유통구조를 침해함으로써 정당한 일자리나 세금의 감소가 발생할 수 있으며, 저질 상품으로 인한 소비자의 안전, 창작 의욕 상실 등 사회 전반적인 악영향을 가지고 올 수 있다.

<3> 이와 같은 문제점들에 대한 최근 산업체의 인식이 점점 증가하면서, 위조 방지를 위한 기술적인 방법의 하나로 RFID 기술을 이용한 상품 인증기술이 주목을 받고 있다.

<4> 현재 RFID를 이용한 다양한 응용 분야가 시장에서 적용되고 있다. 출입통제, 차량원격시동, 전자지불시스템, 도서관, 재고관리 등등, 일상생활에서 다양하게 기술을 접할 수 있다. 하지만 상품 인증에 관련한 기술은 아직 널리 사용되고 있는 상황은 아니며, 보안적인 문제와 대규모 인프라등의 문제가 해결되어야 한다.

<5> RFID(Radio Frequency Identification)는 자동인식 기술의 하나로 사물에 고유한 일련번호를 가진 태그를 부착하고, 무선 신호를 통해서 태그의 정보를 읽어 사물을 자동으로 인식한다. 게다가 태그는 자체적으로 간단한 암호학적 연산을 수행할 수 있기 때문에 안전한 데이터 통신을 지원하는데, 이는 기존의 바코드 시스템과는 다르게 상품 위조 또는 변조를 막기 위한 수단으로 사용될 수 있다.

<6> 태그에 저장되어 있는 정보를 리더가 읽고 표시하는 단순한 방식은 여전히 태그 자체의 위조 문제를 가지고 있기 때문에 태그로부터 전송되는 데이터는 재사용이나 복제가 불가능하도록 암호학적 방법이 추가되어야 한다.

<7> 상품의 위조 방지를 위한 RFID 인증 시스템에 관한 이전 특허들은 다음과 같다. KR 10-2004-0056651 (2004. 7. 21) (정재경)에서는 RFID 태그를 이용한 정품 판별장치 및 방법을 제안하고 있으며, RFID 칩에 정품 관련 데이터를 실장하고, 이를 판별장치로 판독하여 중앙처리장치와의 교신에 의해서 정품여부를 확인할 수 있도록 한다. KR 10-2005-0025257 (2005. 3. 26)(에스케이 텔레콤주식회사)에서는 RFID를 이용한 상품 위조 방지 방법 및 그 시스템을 제안하고 있으며, RFID 태그에 입력된 코드 번호 및 상기 RFID 태그가 부착되는 상품의 정보를 감지하여 이동 통신망으로 연결된 상품 관리 서버로 전송한 후 정상 제조 및 정상 유통된 상품인지 결정한다. KR 10-2003-0020603 (2005. 9. 15)(박미경) 에서는 태그 판독기가 보유하고 있는 다수의 비밀 암호키 중 태그에 저장된 비밀 암호키와 대응되는 비밀 암호키를 태그로부터 수신한 신호에 기초하여 특정한다. 태그 판독기는 태그로부터 암호화된 상품 정보를 수신하여 이를 이 비밀 암호키에 의해 복호화하고 그 결과를 표시부에 평문으로 표현한다.

<8> 상기와 같이 초창기 제안된 RFID 진품 인증 시스템은 단순히 태그에 저장된 상품 관련 정보를 리더가 읽고 화면에 표시해 주는 방식으로, 이는 태그의 정보에 대한 재사용 공격, 도청, 태그 자체의 위조 등의 보안 문제를 고려하지 않은 것이다. 악의적인 공격자는 태그가 리더에게 전송하는 정보를 도청해서 그 정보를 다른 태그에게 복사하면 단순히 태그 위조가 발생할 수 있다.

<9> 이후 제시된 RFID 인증 시스템은 암호학적인 방법을 사용해서 태그 위조의 문제점을 해결한다. 이 기술에서 리더는 암호학적인 연산을 수행하기 위해 태그와 대응되는 비밀키를 필요로 하는데, 여기서는 비밀키를 리더가 미리 저장하고 있어야 하거나 중앙 데이터베이스에 미리 저장되어 있어야 한다. 태그를 인증하는 리더는 임의의 사용자가 될 수 있기 때문에 리더에 비밀키를 저장하고 있는 방식은 키 유출에 따른 문제점을 내포하고 있고, 악의적인 공격자에게 비밀키가 노출되지 않으면서 특정 리더에게 특정 비밀키를 분배해야 하는 비밀키 분배 문제가 발생한다. 외부의 공격으로부터 안전한 중앙 데이터베이스에 비밀키를 모두 저장하는 방식은 리더가 중앙 서버에 실시간으로 접속해야 하기 때문에 리더는 네트워크 기능이 반드시 필요하게 되고, 서버에 문제가 발생하면 인증 시스템 전체가 기능을 할 수 없게 된다. 이런 문제를 해결하기 위해서는 서버와 네트워크에 대한 복잡한 관리가 수반되어야 한다.

발명의 내용

해결 하고자하는 과제

<10> 본 발명은 궁극적으로는 상기와 같은 위조 상품으로 인한 문제점을 해결하기 위한 것으로, 복잡한 중앙 데이터베이스나 리더가 비밀키를 사전에 저장할 필요가 없고 태그에 저장된 정보를 기반으로 누구나 간단한 리더로 쉽고 안전하게 상품의 진위 여부를 확인할 수 있는 오프라인 RFID 인증 방법을 제공하는 것을 목적으로 한다.

과제 해결수단

<11> 상기 문제를 해결하기 위해, 상기 목적을 달성하기 위한 본 발명의 오프라인 RFID 인증 시스템은, 상품 인증에 필요한 데이터를 수정 불가능한 메모리에 저장하고, 인증과정에서 리더에게 그 데이터를 전달 및 리더의 질의에 대한 응답을 수행하는 RFID 태그; 및

<12> 상기 RFID 태그에 저장된 정보와 암호학적 연산을 바탕으로 중앙 서버나 데이터베이스의 접근, 사전 공유 비밀키 없이 리더와 태그 사이의 질의, 응답 메커니즘을 통해 상기 상품이 정상 제조 및 정상 유통된 것인지 여부를 결정하는 RFID 리더를 포함한다.

<13> 상기 목적을 달성하기 위한 본 발명의 오프라인 RFID 인증 방법은,

<14> (a) 상품 출하 전 제조자가 비밀키와 디지털 서명을 만든 후 태그에 저장하고 그 태그를 상품에 부착하는 단계; 및

<15> (b) 상품 출하 후 리더가 상품에 부착된 태그로부터 정보를 읽어 들여 실제로 그 태그가 정당한 제조자로부터 만들어진 태그인지를 인증하는 단계를 포함한다.

<16> 바람직하기로는 상기 인증 단계 (b)는 다시 세부 5단계로

<17> (b1) 리더가 태그에게 인증 과정의 시작을 알리는 요청 단계;

<18> (b2) 태그가 자신이 저장하고 있는 제조자의 디지털 서명과 자신의 고유번호를 리더에게 전송하는 단계;

<19> (b3) 리더가 제조자의 서명의 정당성을 확인하고 그로부터 얻은 데이터를 이용해서 태그에게 질의를 하는 단계;

<20> (b4) 태그가 리더로부터 받은 질의에 자신의 비밀키를 이용해 연산 후 그 결과를 리더에게 응답하는 단계; 및

<21> (b5) 리더가 태그로부터 받은 정보를 추가 연산 후 결과 값을 제조자의 서명으로부터 추출한 태그 값과 비교하여 진품 인증을 마치는 단계로 구성된다.

효 과

<22> 본 발명에서 사용되는 오프라인 RFID 인증 시스템 및 그 방법은 태그의 인증과정에서 리더의 네트워크 기능이나 사전 공유 비밀키, 중앙 데이터베이스로의 접근을 필요로 하지 않는다. 따라서 복잡한 네트워크 인프라 및 키분배가 필요하지 않으며 간단한 암호학적인 연산이 가능한 리더만 있으면 누구나 쉽게 상품의 진위 여부를 확인할 수 있다. 또한 비밀키의 유출이나 도청으로 인한 태그의 복제를 막음으로써, 생산자와 소비자 모두에게 상품 위조 방지를 위한 신뢰성 있는 기술적 장치를 제공하여 건전한 유통구조 확립을 가능하게 한다.

발명의 실시를 위한 구체적인 내용

<23> 이하, 첨부된 도면을 참조하여 본 발명의 구체적인 실시예에 의한 오프라인 RFID 인증 시스템 및 그 방법을 보다 상세히 설명하기로 한다.

<24> 도 1은 본 발명에 의한 오프라인 RFID 인증 시스템의 구성도이다. 도 1에서 보듯이 인증을 위해서 상품(110)에 부착되는 RFID 태그(111)와 상기 태그(111)의 정보를 읽어서 인증을 수행하는 RFID 리더(100)로 구성된다.

<25> 도 1을 참고하면, RFID 리더(100)는 전반적인 제어를 위한 제어부(101), 인증과정에서 수행되는 연산에서 데이터를 일시 저장하기 위한 메모리(102), 태그(110)와 RF 통신을 하기 위한 RF통신 모듈(103), 및 안테나(104)를 포함한다. RFID 태그(111)는 인증을 위해 사용되는 데이터를 저장하기 위한 수정 불가능(Read-only) 메모리(112), 인증과정에서 필요한 암호학적 연산을 수행하기 위한 보안로직(113), 리더(100)와 RF통신을 수행하기 위한 RF통신 모듈(114), 및 안테나(115)를 포함한다.

<26> RFID 리더(100)내 제어부(101)는 RF통신, 인증을 위한 암호학적 연산 등을 전반적으로 수행한다. 태그(111)로부터 받은 제조자의 서명을 검증하고 그로부터 데이터를 복구하는 기능, 태그(111)의 응답을 복구된 데이터와 비교하는 작업을 수행한다. RFID 리더(100)내 메모리(102)는 읽고 쓰기 가능한 메모리로 서명검증에 필요한 제조자의 공개키를 저장하고, 이후 복원된 데이터를 일시 보관하는 역할을 수행한다. 리더와 태그의 RF통신 모듈(103)(114)은 각각 송수신 안테나(104)(115)를 통하여 서로 간 전송되는 RF신호의 송수신 기능을 담당한다.

<27> RFID 태그(111)내 메모리(112)는 인증을 위해 사용되는 데이터를 저장하는 수정 불가능한 메모리이다. 보안로직(113)은 특정 암호학적 연산을 수행하도록 미리 만들어진 것으로 본 발명에서는 해시 함수를 수행할 수 있도록 구성된다.

<28> 도 2와 도 3은 본 발명의 일 실시예에 따른 오프라인 RFID 인증 방법을 설명하기 위한 흐름도로, 도 2는 상품 출하 전 제조자가 인증을 위해 필요한 정보를 태그에 저장하고 물품에 태그를 부착하는 등록 과정을 보여주는 일실시예 흐름도이고, 도 3은 리더가 실제로 상품의 진위 여부를 확인하고자 할 때 리더가 태그를 인증하는 과정을 보여주는 일실시예 흐름도이다.

<29> 도 1 및 도 2에 의하면, 제조자는 태그마다 다른 랜덤한 비밀키를 생성하고(200), 생성된 랜덤 비밀키와 태그의 고유번호를 이용해서 자신의 디지털서명을 생성한다(210). 생성된 두 데이터를 태그(111)의 메모리(112)에 안전하게 저장하고(220) 저장 완료된 태그는 상품에 부착된다(230). 상품(110)과 태그(111)는 물리적으로 결합되어 상품에서 태그를 분리할 경우 태그가 파괴되어 인증과정을 수행할 수 없도록 하는 것이 바람직하다.

<30> 도 1 및 도 3에 의하면, 리더(100)는 자신의 신호 범위 안에 있는 태그(111)에게 인증 요청 신호를 보낸다(300). 리더(100)로부터 인증 요청 신호를 받은 태그(111)는 제조자가 태그에 저장해 놓은 제조자의 서명과 태그의 고유번호(ID)를 리더(100)에게 전송한다(310). 리더(100)는 받은 제조자의 서명을 제조자의 공개키를 이용해서 검증하고, 인증을 위한 데이터를 복구한다(320). 이때 서명 검증이 실패하게 되면 리더는 상품을 위조품으로 판단하고(370), 그렇지 않으면 인증과정을 계속 진행한다. 이후 리더(100)는 복구된 데이터와 리더가 생성한 랜덤 넘버를 이용해서 질의를 생성한 후 태그(111)로 전송한다(330). 질의를 받은 태그(111)는 태그 내부에 저장된 비밀키를 이용해서 응답을 계산하고 리더(100)에게 그 응답을 전송한다(340). 리더(100)는 서명으로부터 복구된 데이터와 응답을 추가 암호학적 연산을 이용해서 비교하게 되는데(350), 이 비교 결과, 같으면 리더는 상품을 정품으로 판단하고(360), 그렇지 않으면 위조품으로 판단한다(370).

<31> 도 4와 도 5는 상술한 도 2와 도 3에서 수행되는 과정에서 데이터의 흐름 및 암호학적 연산을 구체적으로 표현해 주는 도면이다. 여기서 사용하는 주요 암호학적 연산은 태그와 관련된 정보를 실제 정당한 제조자의 의해 제공되었다는 것을 증명하기 위해서 제조자의 디지털 서명이 사용된다. 또한 키 정보를 외부에 알려지지 않게 하기 위해서 특별한 성질을 가지는 해쉬함수(H)를 사용한다. 이하 사용되는 해쉬함수는 다음과 같이 교환법칙이 성립하므로 적용순서에 관계없이 결과값이 동일한 성질을 가진다.

수학식 1

<32> $H(k2, M)) = H(k2, H(k1, M))$

<33> 도 4는 도 2에서 보여준 등록 과정을 구체적인 암호학적 연산을 포함해서 데이터의 흐름도를 자세하게 보여준다.

<34> 도 4에 의하면, 제조자는 랜덤 넘버 생성기(PRNG)로 비밀키(k)를 생성한다(400). 태그는 태그 제조과정에서 부여받은 고유한 제조번호(ID)를 가지고 있는데, 제조자는 이 값을 태그의 비밀키 k를 이용해서 해쉬한다(H(k,ID)). 그리고 상기 과정에서 계산된 결과(H(k,ID))에 ID를 덧붙여(concatenation) 자신의 개인키(sk)로 디지털 서명(sig)을 생성(410)한다. 생성된 제조자의 디지털 서명(sig)과 태그의 비밀키(k)는 태그의 메모리에 안전하게 저장된다(420).

<35> 도 5는 도 3에서 보여준 인증 과정을 구체적인 암호학적 연산을 포함해서 데이터의 흐름도를 자세하게 보여준다.

<36> 도 5에 의하면, 리더는 먼저 태그에게 인증 과정의 시작을 요청하는 요청(request) 메시지를 보낸다(500). 요청 메시지를 받은 태그는 제조자가 저장해 둔 제조자의 디지털 서명(sig)과 자신의 고유번호(ID)를 리더에게 전송한다(510). 리더는 제조자의 공개키(pk)와 태그의 ID를 이용해서 서명이 적절한지를 검증하고(520), 적절할 경우 서명으로부터 ID의 해쉬값(H(k,ID))을 복구하고 메모리에 그 값을 일시 저장한 다음, 이후 과정을 수행하고, 서명이 적절하지 않을 경우 인증과정을 마치고 상품을 위조품으로 판단한다. 리더는 랜덤넘버 생성기로 임시값(nonce)(n)을 만들고(530) 이것을 이용해서 태그 ID를 해쉬 (H(n,ID))한다(540). 이 결과 값을 질의(c)로 이용해서 태그에게 전송하면(550), 태그는 자신의 비밀키(k)를 이용해서 다시 해쉬 (H(k,c))한다(560). 이 결과를 응답(r)으로 리더에게 전송한다(570). 응답(r)을 받은 리더는 이전에 서명으로부터 저장해놓은 해쉬값(H(k,ID))을 자신이 만든 임시값을 이용해서 다시 해쉬(H(n, H(k,ID))하고 그 결과값(r')을 태그의 응답(r)과 같은지 비교한다. 따라서 최종 비교되는 값은 해쉬 함수의 성질에 따라 다음과 같이 비교될 수 있다.

수학식 2

<37> $H(n, H(k,ID)) = H(k, H(n,ID))$

<38> 비교 결과값이 같으면 리더는 상품이 정당한 제조자로부터 유통된 진품으로 판단하고, 그렇지 않은 경우에는 상품을 위조품으로 결정한다.

<39> 상술한 바와 같이, 본 발명의 오프라인 RFID 인증 시스템 및 그 방법은 인증과정에서 리더는 비밀키를 미리 가지고 있지 않고 리더와 태그 간의 통신만으로 인증을 수행한다. 인증에 필요한 정보를 제조자가 미리 암호학적 방법을 이용해서 태그에 저장하고, 이후 인증과정에서 리더는 태그에 저장된 정보를 기반으로 질의/응답 메커니즘을 수행하는데, 태그로부터 오는 정당한 응답을 이용해서 리더는 그 태그가 제조자로부터 부착된 정당한 태그인지를 확인할 수 있게 된다.

<40> 좀 더 세부적으로 설명하면, 제조자는 RFID 태그를 상품에 부착하기 전에 태그와 관련된 데이터를 이용해서 자신의 디지털 서명값을 생성한 후 태그에 저장한다. 이후 인증과정에서는 리더는 이 서명값으로부터 태그와 관련된 정보를 추출하고, 추출된 정보를 기반으로 리더에게 질의를 보내게 된다. 특정 질의에 대해서 태그는 자신의 비밀키를 이용해서 추가 연산 후 응답을 하게 되는데 이 응답을 리더는 추가적인 암호학적 연산을 수행한 후 서명으로 추출된 정보와 비교함으로써 정당한 태그인지 진위 여부를 판단하게 된다.

<41> 특히, 본 발명은 복잡한 네트워크 인프라나 서버관리등의 문제가 없기 때문에 쉽게 구현이 가능하며, 인증에 필요한 세부 알고리즘들도 구체적으로 알려져 있는 것들을 사용하면 되기 때문에 리더와 태그의 제조기술이 있을 경우 바로 실생활에 적용 가능하다.

도면의 간단한 설명

<42> 도 1은 본 발명이 적용되는 RFID 시스템의 구성도이다.

<43> 도 2는 상품 출하 전에 제조자가 인증을 위해 필요한 정보를 태그에 저장하고 물품에 태그를 부착하는 등록 과정을 보여주는 일실시예 흐름도이다.

<44> 도 3은 리더가 실제로 상품의 진위 여부를 확인하고자 한때 리더가 태그를 인증하는 과정을 보여주는 일실시예 흐름도이다.

<45> 도 4는 도 2에서 보여준 등록 과정을 구체적인 암호학적 연산을 포함해서 데이터의 흐름을 자세하게 보여주는 인증 방법의 흐름도이다.

<46> 도 5는 도 3에서 보여준 인증 과정을 구체적인 암호학적 연산을 포함해서 데이터의 흐름을 자세하게 보여주는 인증 방법의 흐름도이다.

<47> <도면의 주요부분에 대한 부호의 설명>

<48> 100 : RFID 리더

<49> 110 : 상품

<50> 111 : RFID 태그

<51> k : 태그의 비밀키

<52> sk, pk : 제조자의 개인키, 공개키

<53> PRNG : 랜덤 넘버 생성기

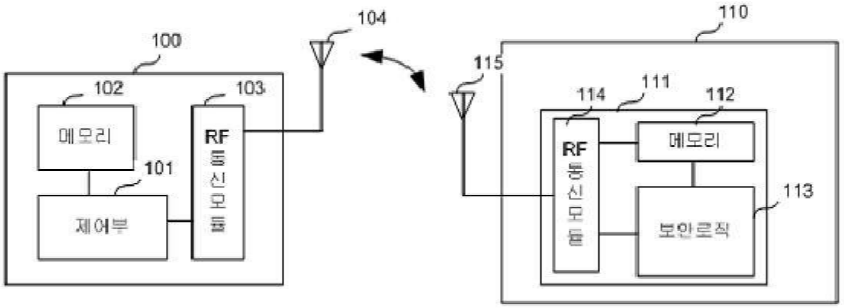
<54> ID : 태그의 고유번호

<55> E(), D() : 암호화, 복호화 함수

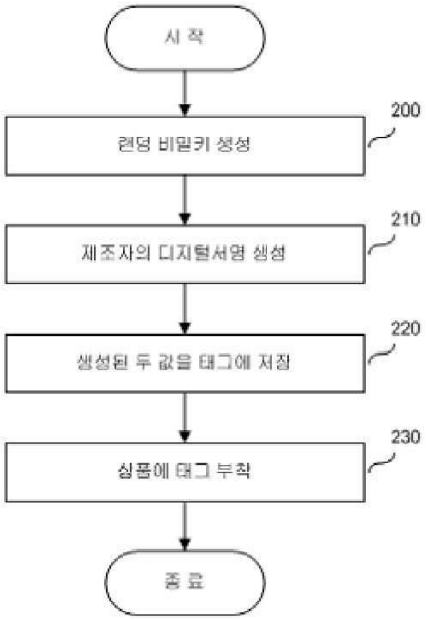
<56> H() : 교환법칙이 성립하는 해쉬함수

도면

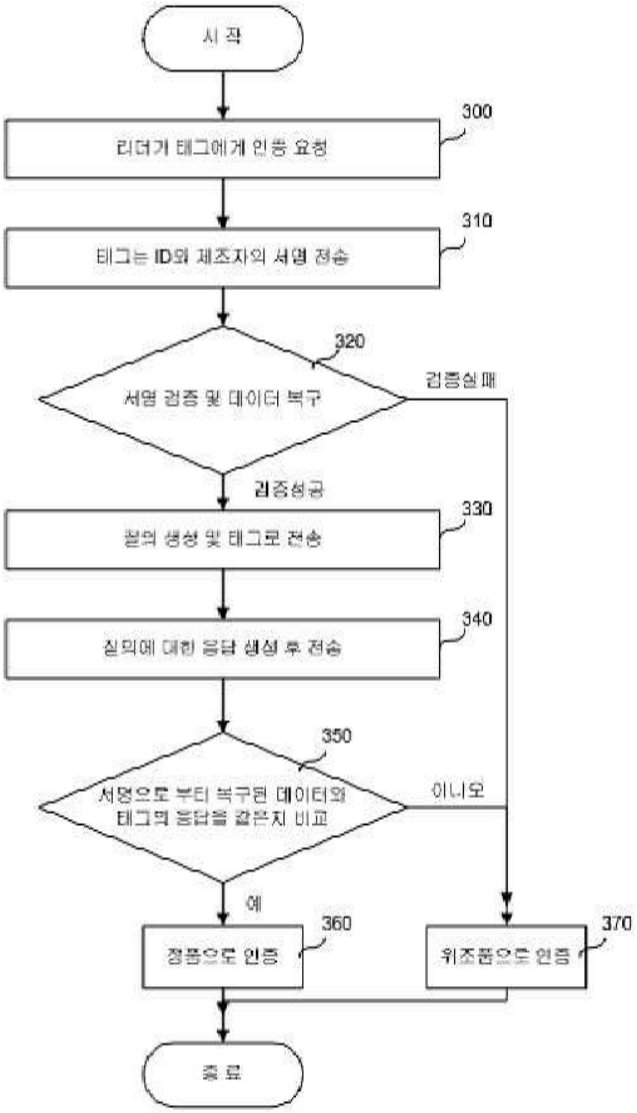
도면1


100
102
메모리
101
제어부
103
RF
통신
모듈
104
110
115
114
111
112
RF
통신
모듈
메모리
113
보안로직

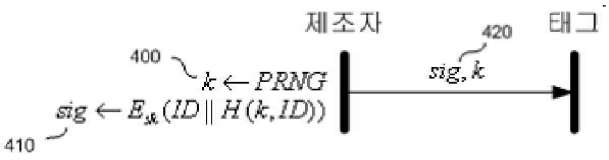
도면2


시작
랜덤 비밀키 생성
200
제조자의 디지털서명 생성
210
생성된 두 값을 태그에 저장
220
상품에 태그 부착
230
종료

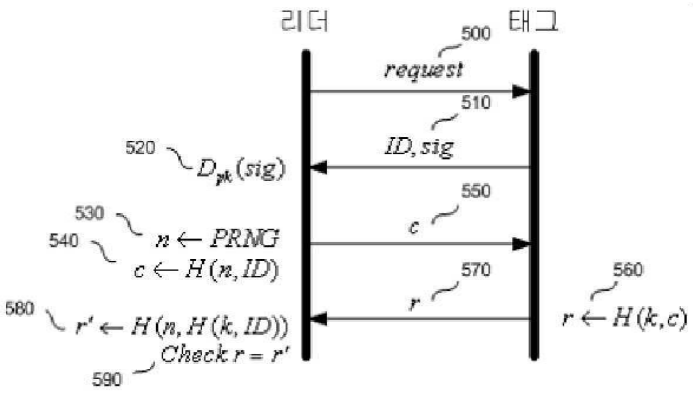
도면3


시 작
300
리더가 태그에게 인증 요청
310
태그는 ID와 제조자의 서명 전송
320
서명 검증 및 데이터 복구
검증실패
검증성공
330
질의 생성 및 태그로 전송
340
질의에 대한 응답 생성 후 전송
350
서명으로 부터 복구된 데이터와
태그의 응답을 같은지 비교
아니오
예
360
정품으로 인증
370
위조품으로 인증
종 료

도면4


제조자
태그
400
$k \leftarrow PRNG$
$sig \leftarrow E_{sk}(ID \| H(k, ID))$
410
420
sig, k

도면5


리더
태그
500
request
510
ID, sig
520
$D_{pk}(sig)$
530
$n \leftarrow PRNG$
540
$c \leftarrow H(n, ID)$
550
c
560
$r \leftarrow H(k, c)$
570
r
580
$r' \leftarrow H(n, H(k, ID))$
590
Check r = r'