(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2008년03월27일
(11) 등록번호 10-0817222
(24) 등록일자 2008년03월20일

(51) Int. Cl.
G06K 17/00 (2006.01) *G06F 19/00* (2006.01)
(21) 출원번호 10-2007-0020043
(22) 출원일자 2007년02월28일
심사청구일자 2007년02월28일
(56) 선행기술조사문헌
KR1020070054885 A

(73) 특허권자
롯데정보통신 주식회사
서울 금천구 가산동 533
고려대학교 산학협력단
서울 성북구 안암동5가1 고려대학교 내
(72) 발명자
조덕길
경기 남양주시 와부읍 도곡리 우성아파트 115-302
남형훈
서울 도봉구 창1동 주공4단지아파트 405-902
(뒷면에 계속)
(74) 대리인
특허법인다울

전체 청구항 수 : 총 13 항 심사관 : 김창주

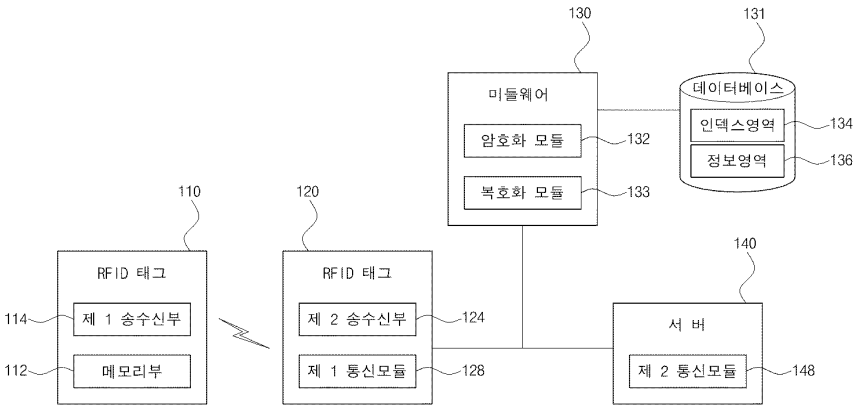
(54) 전자 상품 코드를 암호화/복호화하는 방법 및 이를 이용한ＲＦＩＤ 시스템

(57) 요 약

본 발명은 AES 암호화/복호화 알고리즘을 바탕으로 전자 상품 코드를 암호화/복호화함으로써 RFID 인증시에 전자 상품 코드의 보안을 향상시키는 전자 상품 코드를 암호화/복호화하는 방법 및 이를 이용한 RFID 시스템에 관한 것이다.

본 발명에 의한 전자 상품 코드를 암호화하는 RFID 시스템은, 전자 상품 코드(EPC)를 저장하고, 저장된 전자 상품 코드를 RFID 리더에 전송하며, 암호화된 전자상품코드를 RFID 리더로부터 수신하여 저장하는 RFID 태그와; 상기 RFID 태그에 저장된 전자 상품코드를 읽어 들여 미들웨어에 전달하며, 상기 미들웨어로부터 전달되는 암호화된 전자 상품코드를 상기 RFID 태그에 전송하는 RFID 리더; 상기 RFID 리더로부터 전송된 전자 상품코드에 난수를 패딩(padding)한 후 암호화 알고리즘을 바탕으로 상기 난수가 패딩된 전자 상품 코드(EPC)를 암호화하며, 상기 암호화된 전자 상품 코드를 전단코드와 후단코드로 분할하여 데이터베이스에 저장하고, 상기 암호화된 전자 상품 코드를 상기 RFID 리더를 경유하여 RFID 태그에 전송하는 암호화모듈을 구비하는 미들웨어; 및 상기 미들웨어의 암호화모듈에 의해 암호화된 전자 상품 코드의 전단코드와 후단코드가 각각 저장되는 인덱스 영역과 정보영역을 구비하는 데이터베이스를 포함하여 이루어지는 것을 특징으로 한다.

대표도



(72) 발명자

김기수

서울 구로구 구로동 104-9

이동훈

경기 고양시 일산동구 정발산동 밤가시마을 901동 201호

최은영

서울 성북구 안암동5가 11-1 502호

김주혜

서울 영등포구 신길3동 325-105

김일중

서울 동대문구 제기동 148-29

특허청구의 범위

청구항 1

전자 상품 코드를 암호화하는 RFID 시스템에 있어서,

전자 상품 코드(EPC)를 저장하고, 저장된 전자 상품 코드를 RFID 리더에 전송하며, 암호화된 전자상품코드를 RFID 리더로부터 수신하여 저장하는 RFID 태그와;

상기 RFID 태그에 저장된 전자 상품코드를 읽어 들여 미들웨어에 전달하며, 상기 미들웨어로부터 전달되는 암호화된 전자 상품코드를 상기 RFID 태그에 전송하는 RFID 리더;

상기 RFID 리더로부터 전송된 전자 상품코드에 난수를 패딩(padding)한 후 암호화 알고리즘을 바탕으로 상기 난수가 패딩된 전자 상품 코드(EPC)를 암호화하며, 상기 암호화된 전자 상품 코드를 전단코드와 후단코드로 분할하여 데이터베이스에 저장하고, 상기 암호화된 전자 상품 코드를 상기 RFID 리더를 경유하여 RFID 태그에 전송하는 암호화모듈을 구비하는 미들웨어; 및

상기 미들웨어의 암호화모듈에 의해 암호화된 전자 상품 코드의 전단코드와 후단코드가 각각 저장되는 인덱스 영역과 정보영역을 구비하는 데이터베이스를 포함하여 이루어지는 것을 특징으로 하는 전자 상품 코드를 암호화하는 RFID 시스템.

청구항 2

제1항에 있어서,

상기 미들웨어의 암호화모듈은 96bit의 전자 상품 코드에 32bit의 난수를 패딩한 후 AES-128알고리즘을 이용하여 128bit의 전자 상품 코드로 암호화하며,

상기 암호화된 전자상품코드를 각각 64bit의 전단코드와 후단코드로 분할하여 데이터베이스의 인덱스영역과 정보영역에 각각 저장하는 것을 특징으로 하는 전자 상품 코드를 암호화하는 RFID 시스템.

청구항 3

제2항에 있어서,

상기 미들웨어의 암호화모듈은 암호화된 전자 상품 코드의 후단코드에 대해 32bit의 CRC(Cyclic Redundancy Check)를 생성하여 64bit의 전단코드에 패딩한 후 이를 RFID 리더를 경유하여 RFID 태그에 전송하여 저장되도록 하는 것을 특징으로 하는 전자 상품 코드를 암호화하는 RFID 시스템.

청구항 4

암호화된 전자 상품 코드를 복호화하는 RFID 시스템에 있어서,

RFID 리더로부터 소정의 거리 이내에 접근되면, 암호화된 전자 상품 코드(EPC)가 읽혀지는 RFID 태그와;

상기 RFID 태그로부터 읽어 들인 암호화된 전자 상품 코드를 미들웨어에 전송하고, 서버로부터 전자 상품 코드에 관련된 정보를 수신하는 RFID 리더;

상기 RFID 리더로부터 암호화된 전자 상품 코드를 전송받고, 데이터베이스를 검색하여 상기 암호화된 전자 상품 코드에 대응하는 CRC(Cyclic Redundancy Check)를 생성하여 상기 암호화된 전자 상품 코드에 포함된 CRC와 비교하며, 상기 비교결과가 같다면, 상기 암호화된 전자 상품 코드의 전단코드에 대응하는 후단코드를 결합한 후 복호화 알고리즘을 바탕으로 복호화하고, 상기 복호화된 전자 상품 코드로부터 원 전자 상품 코드를 추출하여 서버에 저장하도록 전송하는 복호화모듈을 구비하는 미들웨어;

암호화된 전자 상품 코드의 전단코드와 후단코드가 각각 저장된 인덱스 영역과 정보영역을 구비하며, 미들웨어의 복호화모듈로부터 요청되는 전단코드와 후단코드를 검색하는 데이터베이스; 및

상기 미들웨어의 복호화모듈로부터 전송된 전자 상품 코드를 바탕으로 전자 상품 코드에 관련하여 저장된 정보

를 상기 RFID 리더에 제공하는 서버를 포함하여 이루어지는 것을 특징으로 하는 암호화된 전자 상품 코드를 복호화하는 RFID 시스템.

청구항 5

제4항에 있어서,

상기 암호화된 전자 상품 코드는 64bit의 전단코드에 패딩된 CRC를 포함하여 이루어지며, 상기 미들웨어의 복호화모듈은 상기 전단코드에 일치하는 상기 데이터베이스의 인덱스 영역에 저장된 64bit의 전단코드를 검색하고 이에 대응하는 후단코드에 대한 32bit의 CRC를 생성한 후, 상기 암호화된 전자 상품 코드의 CRC와 비교하는 것을 특징으로 하는 암호화된 전자 상품 코드를 복호화하는 RFID 시스템.

청구항 6

제5항에 있어서,

상기 32bit의 CRC 비교결과가 같다면, 상기 미들웨어의 복호화모듈은 상기 암호화된 전자 상품 코드의 64bit의 전단코드와 상기 데이터베이스의 정보영역에 저장된 64bit의 후단코드를 결합한 후 AES-128 복호화 알고리즘을 바탕으로 복호화하고, 복호화된 전자 상품 코드로부터 96bit의 원 전자 상품 코드를 추출하는 것을 특징으로 하는 암호화된 전자 상품 코드를 복호화하는 RFID 시스템.

청구항 7

RFID 시스템에서 전자 상품 코드를 암호화하는 방법에 있어서,

전자 상품 코드(EPC)에 난수를 패딩(padding)하는 단계와;

상기 난수가 패딩되면, 암호화 알고리즘을 바탕으로 상기 난수가 패딩된 전자 상품 코드를 암호화하는 단계와;

상기 암호화된 전자 상품 코드를 전단코드와 후단코드로 분할하는 단계; 및

상기 후단코드에 대해 CRC(Cyclic Redundancy Check)를 생성하여 상기 전단코드에 결합시킨 후 암호화된 전자 상품코드로 저장하는 단계를 포함하여 이루어지는 것을 특징으로 하는 RFID 시스템에서 전자 상품 코드를 암호화하는 방법.

청구항 8

제7항에 있어서,

상기 전자 상품 코드는 96bit로 이루어지고 난수는 32bit로 이루어지며, AES-128 알고리즘을 바탕으로 상기 난수가 패딩된 전자 상품 코드를 암호화하며, 상기 전단코드와 후단코드는 각각 64bit로 이루어지고, CRC는 32bit로 이루어지는 것을 특징으로 하는 RFID 시스템에서 전자 상품 코드를 암호화하는 방법.

청구항 9

RFID 시스템에서 암호화된 전자 상품 코드를 복호화하는 방법에 있어서,

암호화된 전자 상품 코드를 읽어들인 후 이에 일치하는 암호화된 전자 상품 코드의 전단코드를 데이터베이스에서 검색하는 단계와;

상기 전단코드에 대응하는 후단코드에 대한 CRC를 생성하고 생성된 CRC를 상기 암호화된 전자 상품 코드에 포함된 CRC와 비교하는 단계와;

상기 비교결과 CRC가 동일하다면 상기 암호화된 전자 상품 코드의 전단코드에 데이터베이스에 저장된 후단코드를 결합시키는 단계와;

상기 결합된 전단코드와 후단코드를 암호화 알고리즘을 바탕으로 복호화하고 이로부터 원 전자 상품 코드를 추출하는 단계; 및

상기 추출된 원 전자 상품 코드를 바탕으로 전자 상품 코드와 관련된 정보를 제공하는 단계를 포함하여 이루어지는 것을 특징으로 하는 RFID 시스템에서 암호화된 전자 상품 코드를 복호화하는 방법.

청구항 10

제9항에 있어서,

상기 비교결과 32bit로 이루어진 CRC값이 동일하다면 상기 암호화된 전자 상품 코드에 포함된 64bit의 전단코드에 데이터베이스에 저장된 64bit의 후단코드를 결합시킨 후 AES-128 복호화 알고리즘을 바탕으로 복호화하며, 상기 복호화된 전자 상품 코드로부터 96bit의 원 전자 상품 코드를 추출하는 것을 특징으로 하는 RFID 시스템에서 암호화된 전자 상품 코드를 복호화하는 방법.

청구항 11

전자 상품 코드를 암호화 및 복호화하는 RFID 시스템에 있어서,

RFID 리더로부터 전송된 전자 상품코드에 난수를 패딩(padding)한 후 암호화 알고리즘을 이용하여 상기 난수가 패딩된 전자 상품 코드(EPC)를 암호화하며, 상기 암호화된 전자 상품 코드를 전단코드와 후단코드로 분할하여 데이터베이스에 저장하고, 상기 암호화된 전자 상품 코드의 후단코드에 대해 CRC(Cyclic Redundancy Check)를 생성하여 상기 전단코드에 패딩한 후, RFID 리더를 경유하여 RFID 태그에 전송하는 암호화모듈과;

상기 RFID 리더로부터 암호화된 전자 상품 코드를 전송받아 암호화된 전자 상품 코드의 전단코드에 일치하는 데이터베이스에 저장된 전자 상품 코드의 전단코드와 후단코드를 검색하고, 데이터베이스에서 검색한 후단코드에 대한 CRC(Cyclic Redundancy Check)를 생성하여 상기 암호화된 전자 상품 코드에 포함된 CRC와 비교하며, 상기 비교결과가 같다면, 상기 암호화된 전자 상품 코드의 전단코드에 상기 데이터베이스에서 검색한 후단코드를 결합한 후 복호화 알고리즘을 이용하여 복호화하고, 상기 복호화된 전자 상품 코드로부터 원 전자 상품 코드를 추출하여 서버에 저장하도록 전송하는 복호화모듈을 구비하는 미들웨어를 포함하여 이루어지는 것을 특징으로 하는 전자 상품 코드를 암호화 및 복호화하는 RFID 시스템.

청구항 12

제11항에 있어서,

상기 원 전자 상품 코드는 96bit이며, 상기 전자 상품 코드에 패딩되는 난수는 32bit이고, 암호화 및 복호화 알고리즘에 의해 암호화 및 복호화된 전자 상품 코드는 128bit이며, 암호화된 전자 상품 코드의 전단코드와 후단코드는 각각 64bit이고, 후단코드에 대한 CRC는 32bit인 것을 특징으로 하는 전자 상품 코드를 암호화 및 복호화하는 RFID 시스템.

청구항 13

제12항에 있어서,

상기 암호화모듈 및 복호화모듈은 암호화 및 복호화 알고리즘으로 AES-128 알고리즘을 이용하는 것을 특징으로 하는 전자 상품 코드를 암호화 및 복호화하는 RFID 시스템.

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

<11> 본 발명은 전자 상품 코드를 암호화/복호화하는 방법 및 이를 이용한 RFID 시스템에 관한 것으로, 특히 AES 암호화/복호화 알고리즘을 바탕으로 전자 상품 코드를 암호화/복호화함으로써 RFID 인증시에 전자 상품 코드의 보안을 향상시키는 전자 상품 코드를 암호화/복호화하는 방법 및 이를 이용한 RFID 시스템에 관한 것이다.

<12> 일반적으로, 무선인식 시스템에서, 객체 인식정보를 포함하고 있는 물체를 무선인식 태그(RFID tag)라 하고, 그 태그에 소정의 데이터를 기록하거나 태그에 기록되어 있는 데이터를 판독하는 장치를 인식기(identifier), 무선인식 리더(RFID reader) 또는 단말기(terminal)이라고 한다. RFID 태그는 무선 주파수를 이용한 전자기적 객체 식별 장치로서, 내부에 중앙처리장치가 없고 단순한 제어장치와 메모리 및 송수신 안테나만이 있다는 점에서 스

마트 카드와 구별된다.

<13> 그러나, 스마트 카드가 강력한 보안 기능을 구비하고 있는 반면에 RFID 태그는 표식체 또는 인식체로서의 메모리 역할을 하는 것에 불과하므로 보안 능력이 거의 없다는 문제점이 있었다.

<14> 이러한 문제점을 해결하기 위해 특허공개 제 10-2004-0092669호에는 "보안기능을 구비한 무선인식 단말기 및 태그"가 개시되어 있으며, 이에 대해 간략히 설명하면 다음과 같다.

<15> 상기 공개특허에서는, RFID 태그의 고유번호와 마스터 키를 기초로 생성된 인증 암호(Tc1)를 RFID 태그에 기록해 두고 RFID 리더의 인식영역 내에 RFID 태그가 접근하면 RFID 리더가 상기 RFID 태그의 고유번호와 인증암호(Tc1)를 수신한다. 이어서, RFID 리더는 RFID 리더에 저장된 마스터 키와 수신된 RFID 태그의 고유번호를 이용하여 인증암호(Tc2)를 생성한 뒤 RFID 태그의 인증암호(Tc1)와 비교함으로써 인증여부를 결정한다.

<16> 그러나, 상기와 같은 공개특허에서는, RFID 태그로부터 RFID 리더에 전자 상품 코드(EPC:Electronic Product Code)를 전송할 때 전자 상품 코드가 평문으로 보내지기 때문에 제3자에 의해 노출되기 쉽다는 문제점이 있다. 즉, 제3자가 RFID 태그로부터 RFID 리더에 전송되는 전자 상품 코드를 해킹하거나 인식하여 불법적으로 복제하거나 시스템을 방해할 수 있다는 문제점이 있다.

발명이 이루고자 하는 기술적 과제

<17> 상기와 같은 문제점을 해결하기 위해 본 발명은 AES 암호화/복호화 알고리즘을 바탕으로 전자 상품 코드를 암호화/복호화함으로써 RFID 인증시에 전자 상품 코드의 보안을 향상시키는 전자 상품 코드를 암호화/복호화하는 방법 및 이를 이용한 RFID 시스템을 제공하는 것을 그 목적으로 한다.

발명의 구성 및 작용

<18> 상술한 목적들을 달성하기 위하여, 본 발명의 일 실시예에 따른 전자 상품 코드를 암호화하는 RFID 시스템은, 전자 상품 코드(EPC)를 저장하고, 저장된 전자 상품 코드를 RFID 리더에 전송하며, 암호화된 전자상품코드를 RFID 리더로부터 수신하여 저장하는 RFID 태그와; 상기 RFID 태그에 저장된 전자 상품코드를 읽어 들여 미들웨어에 전달하며, 상기 미들웨어로부터 전달되는 암호화된 전자 상품코드를 상기 RFID 태그에 전송하는 RFID 리더; 상기 RFID 리더로부터 전송된 전자 상품코드에 난수를 패딩(padding)한 후 암호화 알고리즘을 바탕으로 상기 난수가 패딩된 전자 상품 코드(EPC)를 암호화하며, 상기 암호화된 전자 상품 코드를 전단코드와 후단코드로 분할하여 데이터베이스에 저장하고, 상기 암호화된 전자 상품 코드를 상기 RFID 리더를 경유하여 RFID 태그에 전송하는 암호화모듈을 구비하는 미들웨어; 및 상기 미들웨어의 암호화모듈에 의해 암호화된 전자 상품 코드의 전단코드와 후단코드가 각각 저장되는 인덱스 영역과 정보영역을 구비하는 데이터베이스를 포함하여 이루어지는 것을 특징으로 한다.

<19> 본 발명의 다른 실시예에 따른 암호화된 전자 상품 코드를 복호화하는 RFID 시스템은, RFID 리더로부터 소정의 거리 이내에 접근되면, 암호화된 전자 상품 코드(EPC)가 읽혀지는 RFID 태그와; 상기 RFID 태그로부터 읽어 들인 암호화된 전자 상품 코드를 미들웨어에 전송하고, 서버로부터 전자 상품 코드에 관련된 정보를 수신하는 RFID 리더와; 상기 RFID 리더로부터 암호화된 전자 상품 코드를 전송받고, 데이터베이스를 검색하여 상기 암호화된 전자 상품 코드에 대응하는 CRC(Cyclic Redundancy Check)를 생성하여 상기 암호화된 전자 상품 코드에 포함된 CRC와 비교하며, 상기 비교결과가 같다면, 상기 암호화된 전자 상품 코드의 전단코드에 대응하는 후단코드를 결합한 후 복호화 알고리즘을 바탕으로 복호화하고, 상기 복호화된 전자 상품 코드로부터 원 전자 상품 코드를 추출하여 서버에 저장하도록 전송하는 복호화모듈을 구비하는 미들웨어; 암호화된 전자 상품 코드의 전단코드와 후단코드가 각각 저장된 인덱스 영역과 정보영역을 구비하며, 미들웨어의 복호화모듈로부터 요청되는 전단코드와 후단코드를 검색하는 데이터베이스; 및 상기 미들웨어의 복호화모듈로부터 전송된 전자 상품 코드를 바탕으로 전자 상품 코드에 관련하여 저장된 정보를 상기 RFID 리더에 제공하는 서버를 포함하여 이루어지는 것을 특징으로 한다.

<20> 또한, 본 발명의 다른 실시예에 따른 전자 상품 코드를 암호화 및 복호화하는 RFID 시스템은, RFID 리더로부터 전송된 전자 상품코드에 난수를 패딩(padding)한 후 암호화 알고리즘을 이용하여 상기 난수가 패딩된 전자 상품 코드(EPC)를 암호화하며, 상기 암호화된 전자 상품 코드를 전단코드와 후단코드로 분할하여 데이터베이스에 저장하고, 상기 암호화된 전자 상품 코드의 후단코드에 대해 CRC(Cyclic Redundancy Check)를 생성하여 상기 전단코드에 패딩한 후, RFID 리더를 경유하여 RFID 태그에 전송하는 암호화모듈과; 상기 RFID 리더로부터 암호화된 전자 상품 코드를 전송받아 암호화된 전자 상품 코드의 전단코드에 일치하는 데이터베이스에 저장된 전자 상품

코드의 전단코드와 후단코드를 검색하고, 데이터베이스에서 검색한 후단코드에 대한 CRC(Cyclic Redundancy Check)를 생성하여 상기 암호화된 전자 상품 코드에 포함된 CRC와 비교하며, 상기 비교결과가 같다면, 상기 암호화된 전자 상품 코드의 전단코드에 상기 데이터베이스에서 검색한 후단코드를 결합한 후 복호화 알고리즘을 이용하여 복호화하고, 상기 복호화된 전자 상품 코드로부터 원 전자 상품 코드를 추출하여 서버에 저장하도록 전송하는 복호화모듈을 구비하는 미들웨어를 포함하여 이루어지는 것을 특징으로 한다.

<21> 또한, 본 발명의 다른 실시예에 따른 RFID 시스템에서 전자 상품 코드를 암호화하는 방법은, 전자 상품 코드(EPC)에 난수를 패딩(padding)하는 단계와; 상기 난수가 패딩되면, 암호화 알고리즘을 바탕으로 상기 난수가 패딩된 전자 상품 코드를 암호화하는 단계와; 상기 암호화된 전자 상품 코드를 전단코드와 후단코드로 분할하는 단계; 및 상기 후단코드에 대해 CRC(Cyclic Redundancy Check)를 생성하여 상기 전단코드에 결합시킨 후 암호화된 전자 상품코드로 저장하는 단계를 포함하여 이루어지는 것을 특징으로 한다.

<22> 또한, 본 발명의 다른 실시예에 따른 RFID 시스템에서 암호화된 전자 상품 코드를 복호화하는 방법은, 암호화된 전자 상품 코드를 읽어들인 후 이에 일치하는 암호화된 전자 상품 코드의 전단코드를 데이터베이스에서 검색하는 단계와; 상기 전단코드에 대응하는 후단코드에 대한 CRC를 생성하고 생성된 CRC를 상기 암호화된 전자 상품 코드에 포함된 CRC와 비교하는 단계와; 상기 비교결과 CRC가 동일하다면 상기 암호화된 전자 상품 코드의 전단코드에 데이터베이스에 저장된 후단코드를 결합시키는 단계와; 상기 결합된 전단코드와 후단코드를 암호화 알고리즘을 바탕으로 복호화하고 이로부터 원 전자 상품 코드를 추출하는 단계; 및 상기 추출된 원 전자 상품 코드를 바탕으로 전자 상품 코드와 관련된 정보를 제공하는 단계를 포함하여 이루어지는 것을 특징으로 한다.

<23> 이하, 첨부된 도면을 참조하여 본 발명의 바람직한 실시예를 상세히 설명하기로 한다.

<24> 도 1은 본 발명의 일 실시예에 따른 전자 상품 코드를 암호화하는 RFID 시스템의 구성을 간략히 나타내는 블록도이다.

<25> 도 1에 도시된 전자 상품 코드를 암호화하는 RFID 시스템은 RFID 태그(110), RFID 리더(120), 미들웨어(130), 미들웨어 데이터베이스(131) 및 서버(140)를 포함한다.

<26> 먼저, 본 발명에서는 상기 RFID 태그(110), RFID 리더(120), 미들웨어(130) 및 서버(140)에 사용되는 메모리부 및 송수신부에 대한 상세한 설명은 생략한다.

<27> RFID 태그(110)는 제1메모리부(112)에 96bit의 전자 상품 코드(EPC)를 저장하며, 상기 저장된 전자 상품 코드를 제1송수신부(114)를 통해 RFID 리더(120)에 전송하고, 96bit의 암호화된 전자상품코드를 RFID 리더(120)로부터 수신하여 제1메모리부(112)에 저장한다.

<28> RFID 태그(110)는 RFID 리더(120)로부터에 소정의 거리 이내에 접근되면, 제1메모리부(112)에 저장된 96bit의 암호화된 전자 상품 코드(EPC)가 제1송수신부(114)를 통해 RFID 리더(120)에 전송되어 RFID 리더(120)에 의해 읽혀지게 된다.

<29> RFID 리더(120)는 제2송수신부(124)를 통해 RFID 태그(110)로부터 96bit의 전자 상품코드를 수신받으며, 제1통신모듈(128)을 통해 수신된 전자 상품 코드를 미들웨어의 암호화모듈(132)에 전달하고 미들웨어의 암호화모듈(132)로부터 96bit의 암호화된 전자 상품코드를 전송받으며, 제2송수신부(124)를 통해 상기 암호화된 전자 상품 코드를 RFID 태그(110)에 전송한다.

<30> RFID 리더(120)는 제2송수신부(124)를 통해 RFID 태그(110)에 저장된 96bit의 암호화된 전자 상품 코드를 수신하며, 제1통신모듈(128)을 통해 상기 암호화된 전자 상품 코드를 미들웨어의 복호화모듈(133)에 전송하고 서버(140)로부터 전자 상품 코드에 관련된 정보를 수신한다.

<31> 미들웨어(130)는 RFID 리더(120)로부터 전송된 96bit의 전자 상품코드에 32bit의 난수를 패딩(padding)한 후 AES-128 암호화 알고리즘을 바탕으로 상기 난수가 패딩된 전자 상품 코드(EPC)를 암호화하여 128bit의 암호화된 전자 상품 코드를 생성하는 암호화모듈(132)을 구비한다.

<32> 또한 미들웨어의 암호화모듈(132)는 암호화된 전자 상품 코드를 64bit의 전단코드와 64bit의 후단코드로 분할하여 각각 데이터베이스(131)의 인덱스영역(index)(134)과 정보영역(info)(136)에 저장한다.

<33> 미들웨어의 암호화모듈(132)은 상기 암호화된 전자 상품 코드의 후단코드에 대해 32bit의 CRC(Cyclic Redundancy Check)를 생성한 후 64bit의 전단코드에 패딩함으로써 96bit의 암호화된 코드를 생성하고, 이를 RFID 리더(120)를 경유하여 RFID 태그(110)에 전송한다.

<34> 또한, 미들웨어의 복호화모듈(133)은 RFID 리더(120)로부터 96bit의 암호화된 전자 상품 코드(64bit의 전단코드+32bit의 CRC)를 전송받으며, 상기 암호화된 전자 상품 코드의 전단코드에 일치하는 데이터베이스(131)의 인덱스 영역(134)에 저장된 64bit의 전단코드를 검색하고 이에 대응하는 후단코드에 대한 32bit의 CRC를 생성한 후 상기 암호화된 전자 상품 코드의 CRC와 비교한다.

<35> 미들웨어(130)의 복호화모듈(133)은, 상기 32bit의 CRC의 비교결과가 같다면 상기 96bit의 암호화된 전자 상품 코드의 64bit의 전단코드와 정보영역에 저장된 64bit의 후단코드를 결합한 후 AES-128 복호화 알고리즘을 바탕으로 복호화함으로써 128bit의 복호화된 전자 상품 코드를 생성한다.

<36> 이어서 미들웨어(131)의 복호화모듈(133)은 128bit의 복호화된 전자 상품 코드로부터 96bit의 원 전자 상품 코드를 추출하여 서버(140)에 전송하여 저장되도록 한다.

<37> 서버(140)는 제2통신모듈(148)을 통해 미들웨어의 복호화모듈(133)로부터 전송된 원 전자 상품 코드를 바탕으로 전자 상품 코드에 관련하여 저장된 정보를 검색하고 이에 따른 검색결과(전자 상품 코드에 관련된 정보)를 RFID 리더(120)에 제공한다.

<38> 이때, 상기 제1, 제2 통신모듈 및 미들웨어의 통신모듈(미도시)은 유선망을 통해 연결되며, 다른 실시예에서는 무선망을 통해 연결되거나 송수신부에서 겸용으로 사용될 수도 있다.

<39> 이하, 도 2 및 도 3을 참조하여 본 발명의 일 실시예에 따른 RFID 시스템에서 전자 상품 코드를 암호화하는 방법을 설명하는데, 도 2는 발명의 일 실시예에 따른 RFID 시스템에서 전자 상품 코드를 암호화하는 방법을 나타내는 흐름도이고, 도 3은 도 2에 도시된 전자 상품 코드의 암호화에 따른 실 예를 나타내는 도면이다.

<40> 먼저, 미들웨어의 암호화모듈(132)에서 96bit의 전자 상품 코드(EPC)(도 3의 "fe5c048da90f9443c516c3c4")에 32bit의 난수를 패딩(padding)(도 3의 "649f0e8b")하여 결합한다(S210).

<41> 상기 S210단계에서 32bit의 난수가 전자 상품 코드에 128bit로 패딩되면, AES-128 암호화 알고리즘을 바탕으로 상기 난수가 패딩된 전자 상품 코드를 암호화한다(S220)(도 3의 "9b6b3e5711a113a457a08687").

<42> 상기 S220단계에서 암호화된 전자 상품 코드를 64bit의 전단코드(EEC_L)(도 3의 "9b6b3e5711a113a4")와 64bit의 후단코드(EEC_R)(도 3의 "3a5223a01ace4b76")로 분할하여 각각 데이터베이스의 인덱스영역 및 정보영역에 저장한다(S230).

<43> 상기 S230단계에서 전단코드(EEC_L)와 후단코드(EEC_R)로 분할되면, 상기 후단코드에 대해 32bit의 CRC(Cyclic Redundancy Check)(도 3의 "57a08687")를 생성한다(S240).

<44> 상기 S240단계에서 상기 CRC가 생성되면, 생성된 CRC를 전단코드(EEC_L)와 결합시킨 후 96bit의 암호화된 전자 상품코드(64bit의 전단코드+32bit의 CRC)(도 3의 "9b6b3e5711a113a457a08687")로 저장한다(S250).

<45> 이하, 도 4 및 도 5를 참조하여 본 발명의 일 실시예에 따른 RFID 시스템에서 암호화된 전자 상품 코드를 복호화하는 방법을 설명하는데, 도 4는 발명의 일 실시예에 따른 RFID 시스템에서 암호화된 전자 상품 코드를 복호화하는 방법을 나타내는 흐름도이고, 도 5는 도 4에 도시된 암호화된 전자 상품 코드의 복호화에 따른 실 예를 나타내는 도면이다.

<46> 먼저, RFID 태그가 일정 거리 이내에 접근하면, RFID 태그로부터 96bit의 암호화된 전자 상품 코드(도 5의 "9b6b3e5711a113a457a08687")를 RFID 리더에서 수신하여 미들웨어의 복호화모듈에 전송한다(S410).

<47> 상기 S410단계에서 RFID 리더로부터 96bit의 암호화된 전자 상품 코드(64bit의 전단코드+32bit의 CRC)(도 5의 "9b6b3e5711a113a457a08687")를 전송받으면, 미들웨어의 복호화모듈은 암호화된 전자 상품 코드의 전단(도 5의 "9b6b3e5711a113a4")에 일치하는 미들웨어 데이터베이스의 인덱스 영역에 저장된 64bit의 전단코드(도 5의 "9b6b3e5711a113a4")를 검색한다(S420).

<48> 상기 S420단계에서 일치하는 전단코드가 검색되면, 상기 검색된 전단코드에 대응하는 데이터베이스의 정보영역에 저장된 64bit의 후단코드(도 5의 "3a5223a01ace4b76")에 대한 32bit의 CRC(도 5의 "57a08687")를 생성한다(S430).

<49> 상기 S430단계에서 32bit의 CRC가 생성되면 상기 생성된 CRC를 상기 암호된 전자 상품 코드에 포함된 CRC와 비교한다(S440).

<50> 상기 S440단계에서 CRC값들의 비교결과 CRC값이 동일하다면 암호화된 전자 상품 코드의 전단코드(도 5의 "9b6b3e5711a113a4")에 정보영역에 저장된 후단코드(도 5의 "3a5223a01ace4b76")를 결합시킨다(S450).

<51> 상기 S450단계에서 결합된 64bit의 전단코드와 64bit의 후단코드를 AES-128복호화 알고리즘을 바탕으로 복호화(도 5의 "fe5c048da90f9443c516c3c4649f0e8b")함으로써 128bit의 복호화된 전자 상품 코드를 생성한다(S460).

<52> 상기 S460단계에서 복호화된 전자 상품 코드가 생성되면, 128bit의 복호화된 전자 상품 코드로부터 96bit의 원 전자 상품 코드(도 5의 fe5c048da90f9443c516c3c4)를 추출한다(S470).

<53> 상기 S470단계에서 원 전자 상품 코드가 추출되면 미들웨어의 복호화모듈은 이를 서버에 전송하고, 전송된 원 전자 상품 코드를 바탕으로 서버에 저장된 전자 상품 코드와 관련된 정보를 RFID 리더에 제공한다(S480).

<54> 본 발명이 속하는 기술분야의 당업자는 본 발명이 그 기술적 사상이나 필수적 특징을 변경하지 않고서 다른 구체적인 형태로 실시될 수 있다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적인 것이 아닌 것으로서 이해해야만 한다.

발명의 효과

<55> 상술한 바와 같이, 본 발명에 의한 전자 상품 코드를 암호화/복호화하는 방법 및 이를 이용한 RFID 시스템은, AES 암호화/복호화 알고리즘을 바탕으로 전자 상품 코드를 암호화/복호화함으로써 RFID 인증시에 전자 상품 코드의 보안을 향상시킨다는 효과가 있다.

<56> 또한, 본 발명은 전자 상품 코드가 RFID 태그로부터 RFID 리더에 전송될 때 제3자에게 노출되는 것을 차단함으로써 사용자의 정보보호를 강화할 수 있다는 효과가 있다.

도면의 간단한 설명

<1> 도 1은 본 발명의 일 실시예에 따른 전자 상품 코드를 암호화하는 RFID 시스템의 구성을 간략히 나타내는 블록도이다.

<2> 도 2는 발명의 일 실시예에 따른 RFID 시스템에서 전자 상품 코드를 암호화하는 방법을 나타내는 흐름도이다.

<3> 도 3은 도 2에 도시된 전자 상품 코드의 암호화에 따른 실 예를 나타내는 도면이다.

<4> 도 4는 발명의 일 실시예에 따른 RFID 시스템에서 암호화된 전자 상품 코드를 복호화하는 방법을 나타내는 흐름도이다.

<5> 도 5는 도 4에 도시된 전자 상품 코드의 복호화에 따른 실 예를 나타내는 도면이다.

<6> <도면의 주요 부분에 대한 부호의 설명>

<7> 110 : RFID 태그

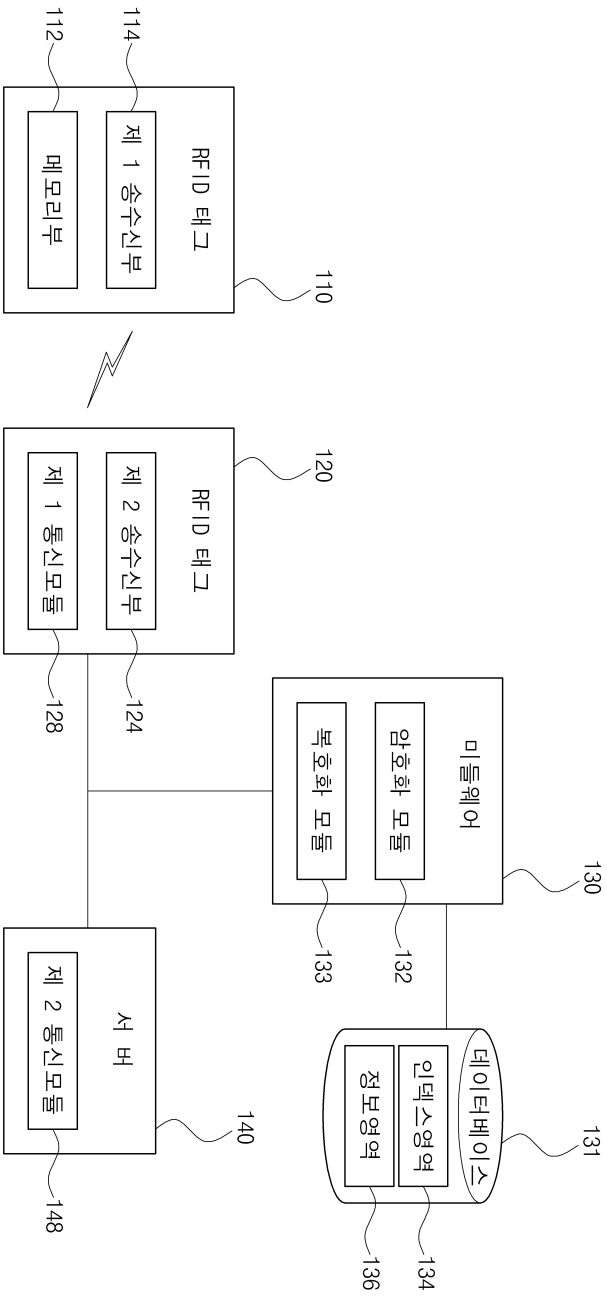
<8> 120 : RFID 리더

<9> 130: 미들웨어

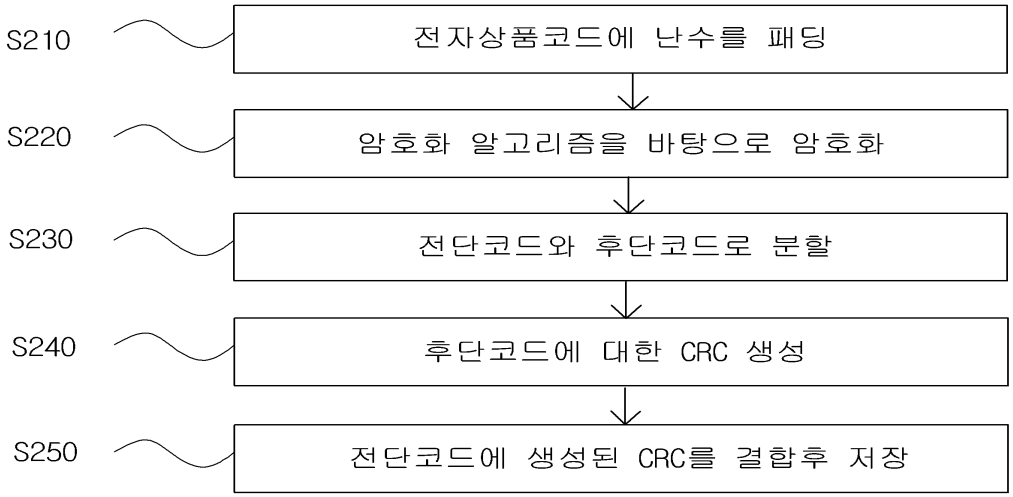
<10> 140 : 서버

도면

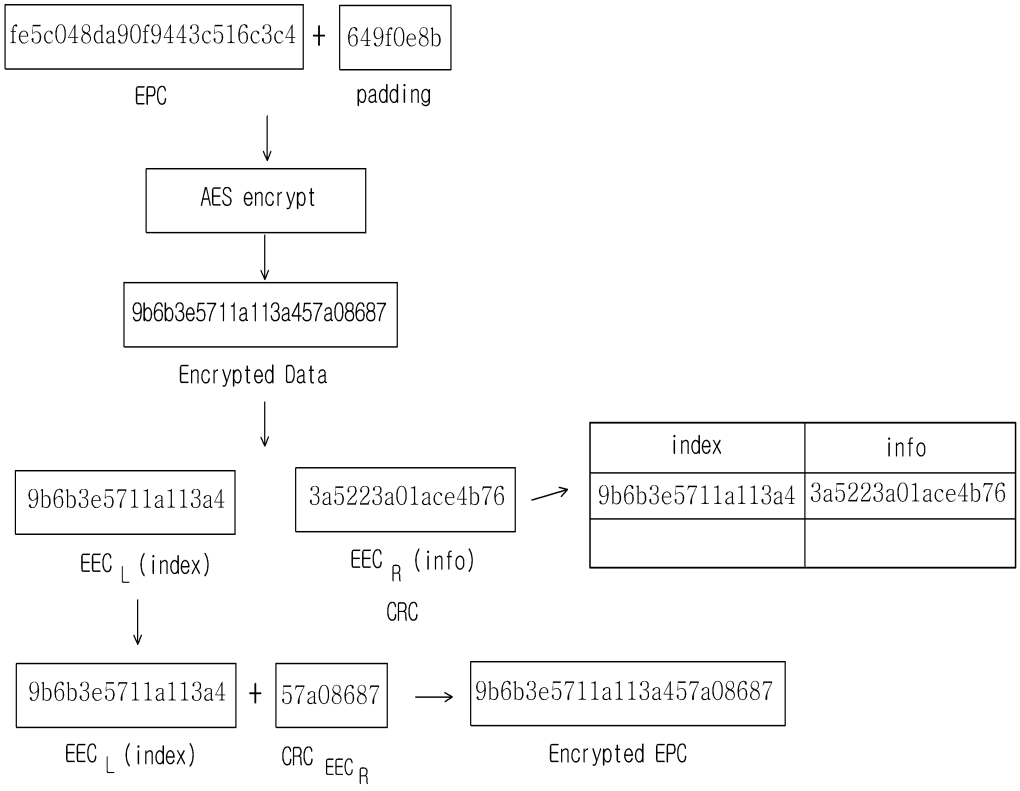
도면1


RFID 태그
메모리부
제 1 송수신부
112
114
110
RFID 태그
제 1 통신모듈
제 2 송수신부
120
128
124
미들웨어
복호화 모듈
암호화 모듈
130
133
132
데이터베이스
정보영역
인덱스영역
131
136
134
서 버
제 2 통신모듈
140
148

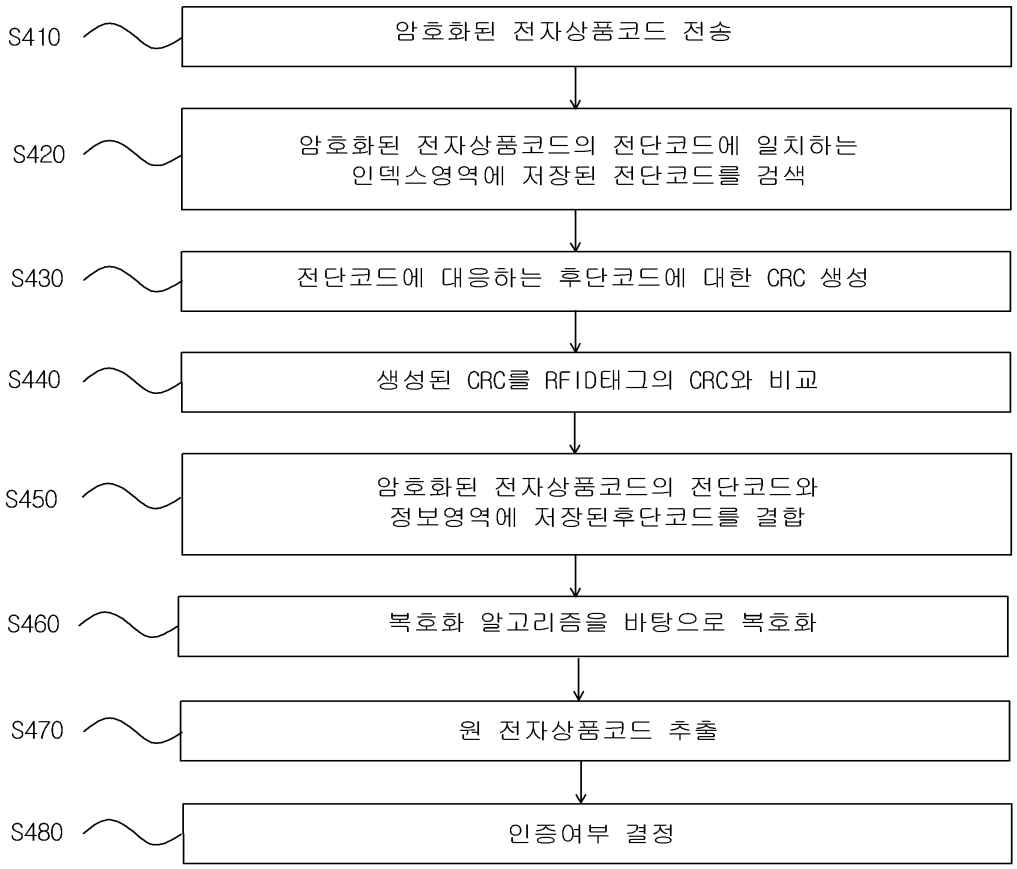
도면2


S210
전자상품코드에 난수를 패딩
S220
암호화 알고리즘을 바탕으로 암호화
S230
전단코드와 후단코드로 분할
S240
후단코드에 대한 CRC 생성
S250
전단코드에 생성된 CRC를 결합후 저장

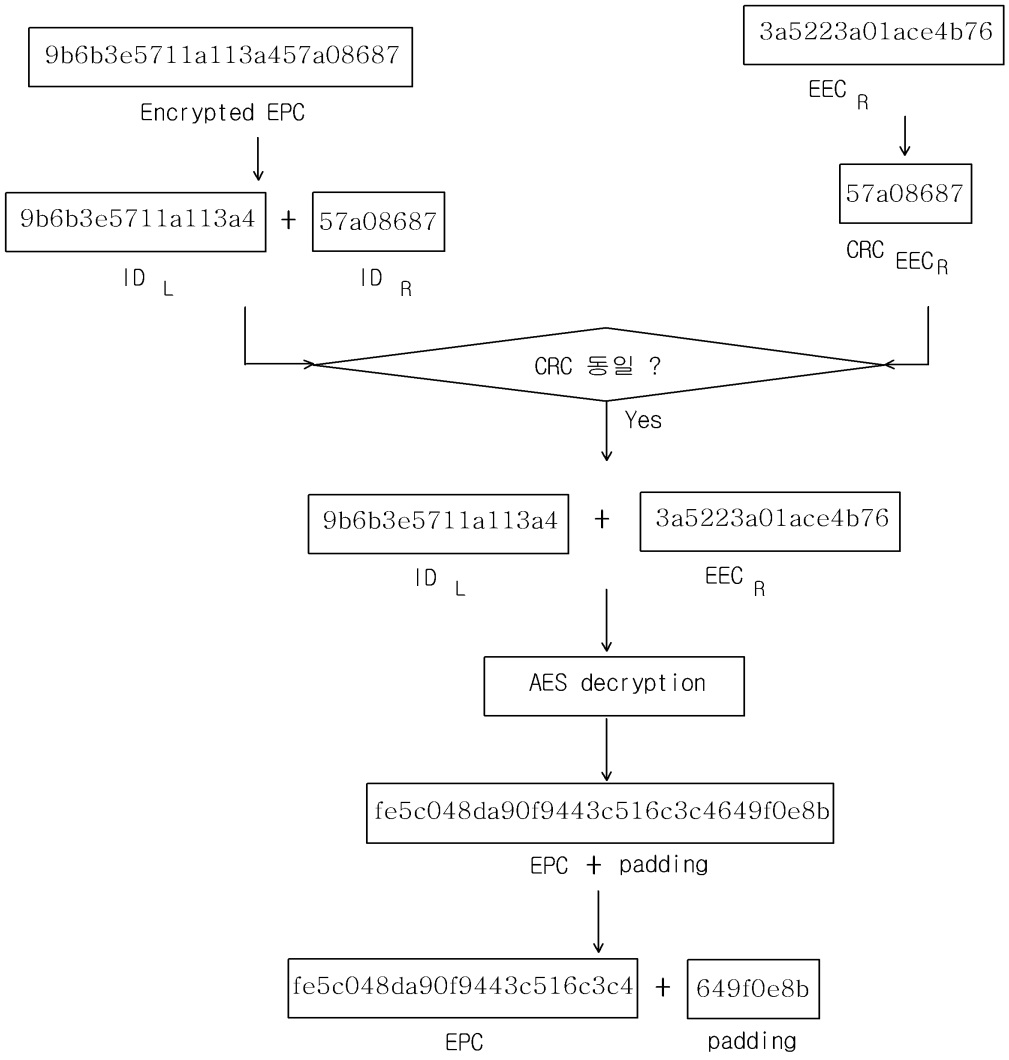
도면3


fe5c048da90f9443c516c3c4
+
649f0e8b
EPC
padding
AES encrypt
9b6b3e5711a113a457a08687
Encrypted Data
9b6b3e5711a113a4
3a5223a01ace4b76
index
info
9b6b3e5711a113a4
3a5223a01ace4b76
EEC L (index)
EEC R (info)
CRC
9b6b3e5711a113a4
+
57a08687
9b6b3e5711a113a457a08687
EEC L (index)
CRC EEC R
Encrypted EPC

도면4


S410
암호화된 전자상품코드 전송
S420
암호화된 전자상품코드의 전단코드에 일치하는
인덱스영역에 저장된 전단코드를 검색
S430
전단코드에 대응하는 후단코드에 대한 CRC 생성
S440
생성된 CRC를 RFID태그의 CRC와 비교
S450
암호화된 전자상품코드의 전단코드와
정보영역에 저장된후단코드를 결합
S460
복호화 알고리즘을 바탕으로 복호화
S470
원 전자상품코드 추출
S480
인증여부 결정

도면5


9b6b3e5711a113a457a08687
Encrypted EPC
9b6b3e5711a113a4
+
57a08687
ID L
ID R
3a5223a01ace4b76
EEC R
57a08687
CRC EEC R
CRC 동일 ?
Yes
9b6b3e5711a113a4
+
3a5223a01ace4b76
ID L
EEC R
AES decryption
fe5c048da90f9443c516c3c4649f0e8b
EPC + padding
fe5c048da90f9443c516c3c4
+
649f0e8b
EPC
padding