



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2007년09월18일
(11) 등록번호 10-0760044
(24) 등록일자 2007년09월12일

(51) Int. Cl.

H04L 9/28 (2006.01) H04L 9/30 (2006.01)
G06K 17/00 (2006.01) H04L 9/14 (2006.01)

(21) 출원번호 10-2006-0037980

(22) 출원일자 2006년04월27일

심사청구일자 2006년04월27일

(56) 선행기술조사문헌

JP2005071213 A

(뒷면에 계속)

(73) 특허권자

고려대학교 산학협력단

서울 성북구 안암동5가1 고려대학교 내

(72) 발명자

임종인

서울 성북구 안암동5가 고려대학교 생명과학관 B
동 136B호

이동훈

서울 성북구 안암동5가 고려대학교 생명과학관 B
동 142B호

(뒷면에 계속)

(74) 대리인

현종철

전체 청구항 수 : 총 12 항

심사관 : 양종필

(54) 자체 재암호화 프로토콜을 이용하는 태그 리드 시스템 및 그 방법

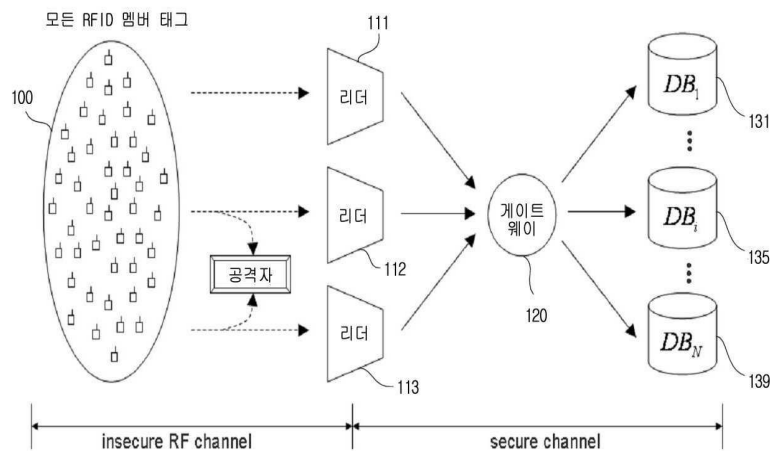
(57) 요약

자체 재암호화 프로토콜을 이용하는 태그 리드 시스템 및 그 방법이 개시된다.

본 발명은 복수의 그룹들 중 어느 하나의 그룹에 포함되고, 수신되는 질의에 대응하여 암호화된 고유 정보를 재암호한 제1암호문을 생성하고, 상기 제1암호문을 상기 그룹을 위한 게이트웨이 대칭키로 암호화한 제2암호문을 생성하는 복수의 멤버 태그, 상기 멤버 태그에 질의를 전송하고, 상기 멤버 태그로부터 상기 제2암호문을 수신하고, 상기 수신된 제2암호문을 출력하는 리더, 상기 제2암호문과 상기 복수의 그룹들에 대응되는 각각의 게이트웨이 대칭키들을 이용하여 그룹 메시지들을 생성하는 게이트웨이 및 상기 복수의 그룹들 중 어느 하나의 그룹에 포함되고, 상기 그룹 메시지들을 상기 멤버 태그가 포함된 그룹의 개인키로 복호화하여 상기 고유 정보를 획득하는 복수의 그룹 데이터베이스를 포함한다.

본 발명에 의하면, 태그가 외부장치를 사용하지 않고 자체적으로 재암호화하여 리더의 모든 질의에 대해서 항상 변경된 형태의 메시지를 전송할 수 있어 정보 노출 문제와 위치 추적 문제를 해결할 수 있고, 태그를 가진 소비자의 프라이버시를 보호할 수 있으며, 제한된 연산 능력을 가진 저가형 태그 또는 저가형 RFID 시스템에 적용될 수 있다.

대표도 - 도1a



(72) 발명자

박정수

서울 서대문구 북가좌2동 335-1

이수미

서울 성북구 안암동5가 고려대학교 생명과학관 B동
140호

최은영

서울 성북구 안암동5가 11-1 502호

(56) 선행기술조사문헌

JP2005151004 A

JP2006065538 A

KR1020060022635 A

W00157807 A1

특허청구의 범위

청구항 1

복수의 그룹들 중 어느 하나의 그룹에 포함되고, 수신되는 질의에 대응하여 암호화된 고유 정보를 재암호한 제1 암호문을 생성하고, 상기 제1암호문을 상기 그룹을 위한 게이트웨이 대칭키로 암호화한 제2암호문을 생성하는 복수의 멤버 태그;

상기 멤버 태그에 질의를 전송하고, 상기 멤버 태그로부터 상기 제2암호문을 수신하고, 상기 수신된 제2암호문을 출력하는 리더;

상기 제2암호문과 상기 복수의 그룹들에 대응되는 각각의 게이트웨이 대칭키들을 이용하여 그룹 메시지들을 생성하는 게이트웨이; 및

상기 복수의 그룹들 중 어느 하나의 그룹에 포함되고, 상기 그룹 메시지들을 상기 멤버 태그가 포함된 그룹의 개인키로 복호화하여 상기 고유 정보를 획득하는 복수의 그룹 데이터베이스를 포함하는 자체 재암호화 프로토콜을 이용하는 태그 리더 시스템.

청구항 2

제 1 항에 있어서,

상기 멤버 태그는

상기 고유 정보를 업데이트 값으로 재암호화하여 제1암호문을 생성하는 것을 특징으로 하는 자체 재암호화 프로토콜을 이용하는 태그 리더 시스템.

청구항 3

제 1 항에 있어서,

상기 멤버 태그는

상기 멤버 태그가 포함된 그룹을 위한 게이트웨이 대칭키를 저장하고, 상기 제1암호문과 상기 그룹을 위한 게이트웨이 대칭키 사이의 배타적 논리합을 연산하여 제2암호문을 생성하는 것을 특징으로 하는 자체 재암호화 프로토콜을 이용하는 태그 리더 시스템.

청구항 4

제 1 항에 있어서,

상기 게이트웨이는

상기 복수의 그룹들에 대응되는 모든 게이트웨이 대칭키를 저장하고, 상기 제2암호문과 상기 복수의 그룹들에 대응되는 각각의 게이트웨이 대칭키들 사이의 배타적 논리합을 연산하여 그룹 메시지들을 생성하는 것을 특징으로 하는 자체 재암호화 프로토콜을 이용하는 태그 리더 시스템.

청구항 5

복수의 그룹들 중 어느 하나의 그룹에 포함되고, 수신되는 질의에 대응하여 암호화된 고유 정보를 재암호한 제1 암호문을 생성하고, 상기 제1암호문을 상기 그룹을 위한 게이트웨이 대칭키로 암호화한 제2암호문을 생성하는 복수의 멤버 태그;

상기 멤버 태그에 질의를 전송하고, 상기 멤버 태그로부터 상기 제2암호문을 수신하고, 상기 수신된 제2암호문을 출력하는 리더;

상기 제2암호문과 상기 복수의 그룹들에 대응되는 각각의 게이트웨이 대칭키들을 이용하여 그룹 메시지들을 생성하고, 상기 그룹 메시지들을 상기 멤버 태그가 포함된 그룹의 개인키로 복호화하여 상기 고유 정보를 획득하는 게이트웨이 데이터베이스를 포함하는 자체 재암호화 프로토콜을 이용하는 태그 리더 시스템.

청구항 6

제 5 항에 있어서,

상기 멤버 태그는

상기 고유 정보를 업데이트 값으로 재암호화하여 제1암호문을 생성하는 것을 특징으로 하는 자체 재암호화 프로토콜을 이용하는 태그 리더 시스템.

청구항 7

제 5 항에 있어서,

상기 멤버 태그는

상기 멤버 태그가 포함된 그룹을 위한 게이트웨이 대칭키를 저장하고, 상기 제1암호문과 상기 그룹을 위한 게이트웨이 대칭키 사이의 배타적 논리합을 연산하여 제2암호문을 생성하는 것을 특징으로 하는 자체 재암호화 프로토콜을 이용하는 태그 리더 시스템.

청구항 8

제 5 항에 있어서,

상기 게이트웨이 데이터베이스는

상기 복수의 그룹들에 대응되는 모든 게이트웨이 대칭키를 저장하고, 상기 제2암호문과 상기 복수의 그룹들에 대응되는 각각의 게이트웨이 대칭키들 사이의 배타적 논리합을 연산하여 그룹 메시지들을 생성하는 것을 특징으로 하는 자체 재암호화 프로토콜을 이용하는 태그 리더 시스템.

청구항 9

복수의 그룹들 중 어느 하나의 그룹에 포함된 복수의 멤버 태그에 질의를 전송하는 단계;

상기 멤버 태그가 상기 질의에 대응하여 암호화된 고유 정보를 재암호한 제1암호문을 생성하고, 상기 제1암호문을 상기 그룹을 위한 게이트웨이 대칭키로 암호화한 제2암호문을 생성하는 단계;

상기 생성된 제2암호문을 게이트웨이로 전송하는 단계;

상기 게이트웨이가 상기 제2암호문과 상기 복수의 그룹들에 대응되는 각각의 게이트웨이 대칭키들을 이용하여 그룹 메시지들을 생성하는 단계; 및

상기 복수의 그룹들 중 어느 하나의 그룹에 포함된 복수의 그룹 데이터베이스가 상기 그룹 메시지들을 상기 멤버 태그가 포함된 그룹의 개인키로 복호화하여 상기 고유 정보를 획득하는 단계를 포함하는 자체 재암호화 프로토콜을 이용하는 태그 리더 방법.

청구항 10

제 9 항에 있어서,

상기 제2암호문을 생성하는 단계는

상기 제1암호문과 상기 그룹을 위한 게이트웨이 대칭키 사이의 배타적 논리합을 연산하여 제2암호문을 생성하는 단계이고,

상기 그룹 메시지들을 생성하는 단계는

상기 제2암호문과 상기 복수의 그룹들에 대응되는 각각의 게이트웨이 대칭키들 사이의 배타적 논리합을 연산하여 그룹 메시지들을 생성하는 단계인 것을 특징으로 하는 자체 재암호화 프로토콜을 이용하는 태그 리더 방법.

청구항 11

복수의 그룹들 중 어느 하나의 그룹에 포함된 복수의 멤버 태그에 질의를 전송하는 단계;

상기 멤버 태그가 수신되는 질의에 대응하여 암호화된 고유 정보를 재암호한 제1암호문을 생성하고, 상기 제1암호문을 상기 그룹을 위한 게이트웨이 대칭키로 암호화한 제2암호문을 생성하는 단계;

상기 생성된 제2암호문을 게이트웨이 데이터베이스로 전송하는 단계; 및

상기 게이트웨이 데이터베이스가 상기 제2암호문과 상기 복수의 그룹들에 대응되는 각각의 게이트웨이 대칭키들을 이용하여 그룹 메시지들을 생성하고, 상기 그룹 메시지들을 상기 멤버 태그가 포함된 그룹의 개인키로 복호화하여 상기 고유 정보를 획득하는 단계를 포함하는 자체 재암호화 프로토콜을 이용하는 태그 리드 방법.

청구항 12

제 9 항 내지 제 11 항 중 어느 한 항의 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

명세서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

- <8> 본 발명은 RF 통신에 관한 것으로, 특히, 자체 재암호화 프로토콜을 이용하는 태그 리드 시스템 및 그 방법에 관한 것이다.
- <9> RFID(Radio Frequency Identification) 시스템은 RF통신을 이용하여 원거리에서 개체의 정보를 읽는 자동인식 기술이다. 이 시스템은 물리적인 접촉 없이 사물의 정보를 빠르게 읽을 수 있으므로, 바코드 시스템을 대체하게 될 시스템으로 주목 받고 있다. 최근에 이 시스템은 물류 시스템, 교통관리 시스템, 동물 관리 시스템 등등에서 부분적으로 사용되고 있다.
- <10> RFID 리더(이하 "리더"라 한다.)가 RFID 태그(이하 "태그"라 한다.)에게 질의(query)를 보내면, 태그는 자신의 정보를 리더에게 전송하고, 그 정보는 데이터베이스에게 전송된다. 이러한 방식으로 서비스 공급자는 태그를 갖고 있는 소비자의 정보를 언제 어디서나 쉽게 얻을 수 있고, 그러한 소비자에게 여러 가지 편리한 서비스를 제공하게 된다. 그러나, 태그와 리더는 공개된 채널(insecure channel)에서 통신하기 때문에, 공격자는 전송되는 메시지를 도청할 수 있고, 이 메시지를 이용하여 신용정보, 구매 패턴, 건강정보 같은 소비자의 민감한 정보가 노출될 수 있다. 또한, 공격자는 이 메시지를 분석함으로써, 태그를 가지고 있는 소비자의 위치를 추적할 수 있다.
- <11> RFID 시스템의 가장 큰 특징 중에 하나는 태그가 제한된 자원을 갖는다는 것이다. 그러므로 태그의 연산량을 낮추는 동시에 소비자의 프라이버시를 보호할 필요가 있다. 이를 위한 방법에는 물리적인 방법과 암호화적인 방법이 있고, 암호화적인 방법은 해쉬 함수를 이용하는 방법과 재암호화하는 방법으로 분류된다.
- <12> 초기 발명에서는 'Kill Command' 같은 물리적인 기법을 사용한다. 'Kill Command'는 구입된 상품에서 태그의 정보를 지우고 다시 활성화시키지 않는 방법이다.
- <13> 암호화적인 방법으로는 해쉬 함수(hash function)를 이용한 인증(authentication) 프로토콜 기법이 있다. 'Hash Lock'은 해쉬 함수의 특징인 일방향성(One-way Property)을 이용하여 태그의 ID를 감출 수 있지만, 위치 정보는 노출된다. 'Hash-Chain'은 위치 정보를 숨기면서 전방위 보안(Forward Security)을 제공하지만, 태그의 정보를 확인하기 위해서 데이터베이스는 최대 태그의 개수만큼 해쉬 연산을 실행해야 한다. 또한 이 프로토콜은 재사용 공격(Replay Attack)과 스푸핑 공격(Spoofing Attack)에 취약하다.
- <14> 또 다른 암호화적 방법은 재암호화(Re-encryption) 기법으로써, 공개키 또는 대칭키를 사용하여 태그의 정보를 외부장치를 이용하여 주기적으로 재암호화하는 방법이다. 이 기법은 암호화를 통해서 태그 정보의 노출을 막고, 재암호화를 통하여 태그 사용자의 위치 정보를 숨긴다. 그러나 태그는 다음 재암호화 단계를 실행할 때까지 리더의 질의에 대하여 항상 같은 값을 응답하므로, 위치 정보를 감추기 위해서는 외부장치와 빈번하게 재암호화를 실행해야 한다.
- <15> 따라서, 종래의 태그 리드 시스템은 시스템이 폭넓게 사용될수록 정보 노출과 위치 추적 등으로 인해 소비자의 프라이버시를 보호할 수 없고, 태그의 제한된 연산 능력과 메모리로 인해 많은 자원이 필요한 지수 연산을 태그 내부에서 수행할 수 없어 외부의 공격에 취약한 문제점이 있다.

발명이 이루고자 하는 기술적 과제

- <16> 따라서, 본 발명이 이루고자 하는 첫번째 기술적 과제는 정보 노출 문제와 위치 추적 문제를 해결할 수 있고, 태그를 가진 소비자의 프라이버시를 보호할 수 있으며, 태그의 연산량을 낮추어 제한된 연산 능력을 가진 저가형 태그 또는 저가형 RFID 시스템에 적용될 수 있는 자체 재암호화 프로토콜을 이용하는 태그 리드 시스템을 제공하는데 있다.
- <17> 본 발명이 이루고자 하는 두번째 기술적 과제는 상기의 자체 재암호화 프로토콜을 이용하는 태그 리드 시스템에 적용된 자체 재암호화 프로토콜을 이용하는 태그 리드 방법을 제공하는데 있다.

발명의 구성 및 작용

- <18> 상기의 첫번째 기술적 과제를 이루기 위하여, 본 발명은 복수의 그룹들 중 어느 하나의 그룹에 포함되고, 수신되는 질의에 대응하여 암호화된 고유 정보를 재암호한 제1암호문을 생성하고, 상기 제1암호문을 상기 그룹을 위한 게이트웨이 대칭키로 암호화한 제2암호문을 생성하는 복수의 멤버 태그, 상기 멤버 태그에 질의를 전송하고, 상기 멤버 태그로부터 상기 제2암호문을 수신하고, 상기 수신된 제2암호문을 출력하는 리더, 상기 제2암호문과 상기 복수의 그룹들에 대응되는 각각의 게이트웨이 대칭키들을 이용하여 그룹 메시지들을 생성하는 게이트웨이 및 상기 복수의 그룹들 중 어느 하나의 그룹에 포함되고, 상기 그룹 메시지들을 상기 멤버 태그가 포함된 그룹의 개인키로 복호화하여 상기 고유 정보를 획득하는 복수의 그룹 데이터베이스를 포함하는 자체 재암호화 프로토콜을 이용하는 태그 리드 시스템을 제공한다.
- <19> 또한, 상기의 첫번째 기술적 과제를 이루기 위하여, 본 발명은 복수의 그룹들 중 어느 하나의 그룹에 포함되고, 수신되는 질의에 대응하여 암호화된 고유 정보를 재암호한 제1암호문을 생성하고, 상기 제1암호문을 상기 그룹을 위한 게이트웨이 대칭키로 암호화한 제2암호문을 생성하는 복수의 멤버 태그, 상기 멤버 태그에 질의를 전송하고, 상기 멤버 태그로부터 상기 제2암호문을 수신하고, 상기 수신된 제2암호문을 출력하는 리더, 상기 제2암호문과 상기 복수의 그룹들에 대응되는 각각의 게이트웨이 대칭키들을 이용하여 그룹 메시지들을 생성하고, 상기 그룹 메시지들을 상기 멤버 태그가 포함된 그룹의 개인키로 복호화하여 상기 고유 정보를 획득하는 게이트웨이 데이터베이스를 포함하는 자체 재암호화 프로토콜을 이용하는 태그 리드 시스템을 제공한다.
- <20> 상기의 두번째 기술적 과제를 이루기 위하여, 본 발명은 복수의 그룹들 중 어느 하나의 그룹에 포함된 복수의 멤버 태그에 질의를 전송하는 단계, 상기 멤버 태그가 상기 질의에 대응하여 암호화된 고유 정보를 재암호한 제1암호문을 생성하고, 상기 제1암호문을 상기 그룹을 위한 게이트웨이 대칭키로 암호화한 제2암호문을 생성하는 단계, 상기 생성된 제2암호문을 게이트웨이로 전송하는 단계, 상기 게이트웨이가 상기 제2암호문과 상기 복수의 그룹들에 대응되는 각각의 게이트웨이 대칭키들을 이용하여 그룹 메시지들을 생성하는 단계 및 상기 복수의 그룹들 중 어느 하나의 그룹에 포함된 복수의 그룹 데이터베이스가 상기 그룹 메시지들을 상기 멤버 태그가 포함된 그룹의 개인키로 복호화하여 상기 고유 정보를 획득하는 단계를 포함하는 자체 재암호화 프로토콜을 이용하는 태그 리드 방법을 제공한다.
- <21> 또한, 상기의 두번째 기술적 과제를 이루기 위하여, 본 발명은 복수의 그룹들 중 어느 하나의 그룹에 포함된 복수의 멤버 태그에 질의를 전송하는 단계, 상기 멤버 태그가 수신되는 질의에 대응하여 암호화된 고유 정보를 재암호한 제1암호문을 생성하고, 상기 제1암호문을 상기 그룹을 위한 게이트웨이 대칭키로 암호화한 제2암호문을 생성하는 단계, 상기 생성된 제2암호문을 게이트웨이 데이터베이스로 전송하는 단계 및 상기 게이트웨이 데이터베이스가 상기 제2암호문과 상기 복수의 그룹들에 대응되는 각각의 게이트웨이 대칭키들을 이용하여 그룹 메시지들을 생성하고, 상기 그룹 메시지들을 상기 멤버 태그가 포함된 그룹의 개인키로 복호화하여 상기 고유 정보를 획득하는 단계를 포함하는 자체 재암호화 프로토콜을 이용하는 태그 리드 방법을 제공한다.
- <22> 태그 리드 시스템(RFID 시스템)에서 프라이버시 보호를 위해 고려할 사항은 다음과 같다. 태그 리드 시스템(RFID 시스템)에는 메시지 도청(Eavesdropping), 분석(Analysis), 변경(Alteration) 등등 다양한 취약점이 존재한다. 이러한 취약점을 이용하여 공격자(Adversary)는 태그의 민감한 정보를 노출시키려고 하고, 태그의 위치를 추적하여 태그를 가진 소비자의 프라이버시를 침해 하려고 할 것이다.
- <23> 삭제
- <24> 첫째, 정보 노출(Information Leakage)이다. 유비쿼터스 환경에서 대부분의 사람들은 정보를 가진 태그를 여러

개씩 몸에 소지하게 될 것이다. 태그의 정보들 중에는 매우 개인적이고, 다른 사람들에게 노출되기를 원하지 않는 정보가 있을 것이다. 예를 들어, 대부분의 사람들은 자신들이 가진 약의 이름, 고가의 제품, 책의 이름 등이 다른 사람들에게 노출되는 것을 원하지 않을 것이다. 그러한 민감한 정보를 가진 태그가 폭넓게 사용된다면, 태그는 자신도 모르는 사이에 불완전한 채널을 통해서 인증되었는지 알 수 없는 리더에게 그러한 정보를 전송하게 될 것이다. 그러므로 태그의 정보가 공격자에게 쉽게 노출되어, 태그 사용자의 프라이버시는 침해될 것이다.

<25> 둘째, 위치 추적 (Traceability)이다. 리더의 질의에 대하여 태그가 응답을 보낼 때, 공격자는 그 응답이 목표 태그의 응답인지 아닌지를 구별할 수 있다면, 태그의 위치 추적이 가능해 진다. 또한 공격자가 태그 응답의 내용을 이해 할 수 없어도, 목표 태그와 응답 사이에 어떤 관계(link)를 만들 수 있다면, 공격자는 목표 태그의 위치를 추적할 수 있다. 다시 말하면, 공격자는 태그를 가진 목표 소비자의 위치를 추적할 수 있게 된다.

<26> 본 발명에 따른 자체 재암호화 프로토콜(SREP)은 다음과 같이 구성된다.

<27> 본 발명에 따른 프로토콜의 모든 태그는 여러개의 그룹으로 나누어지고, 그 그룹들의 태그 정보는 여러 개의 데이터베이스에서 각각 그룹별로 관리된다. 본 발명에 따른 프로토콜은 어떤 그룹의 멤버 태그에서 생성된 암호문을 해당되는 그룹 데이터베이스로 분류하기 위한 새로운 구성요소를 추가하고 이를 '게이트웨이'라고 한다.

<28> 본 발명에 따른 태그 리더 시스템(RFID 시스템)의 구성요소들은 일반적인 태그 리더 시스템(RFID 시스템)과 달리, RFID 멤버 태그(이하 "멤버 태그"라 한다.), RFID 리더(이하 "리더"라 한다.), 게이트웨이, 그룹 데이터베이스로 구성된다.

<29> 본 발명에 따른 태그 리더 시스템(RFID 시스템)은 게이트웨이를 데이터베이스와 통합한 게이트웨이 데이터베이스를 포함할 수 있다.

<30> 이하에서는 도면을 참조하여 본 발명의 바람직한 실시예를 설명하기로 한다.

<31> 도 1a는 본 발명의 일 실시예에 따른 태그 리더 시스템의 구조도이다.

<32> 멤버 태그(100) 즉, RFID 멤버 태그(RFID Member Tag)는 크기가 작고, 제한된 연산 능력을 가진 마이크로 칩이다. 멤버 태그(100)는 주위에 있는 리더(111-113)의 질의에 대하여 자신의 정보를 전송한다.

<33> 복수의 멤버 태그(100)는 복수의 그룹들 중 어느 하나의 그룹에 포함된다. 복수의 멤버 태그(100)는 수신되는 질의에 대응하여 암호화된 고유 정보를 재암호한 제1암호문을 생성하고, 제1암호문을 그룹을 위한 게이트웨이 대칭키로 암호화한 제2암호문을 생성한다. 이때, 멤버 태그(100)는 고유 정보를 업데이트 값으로 재암호화하여 제1암호문을 생성할 수 있다. 멤버 태그(100)는 각각 멤버 태그가 포함된 그룹을 위한 게이트웨이 대칭키를 저장할 수 있다. 또한, 멤버 태그(100)는 제1암호문과 멤버 태그가 포함된 그룹을 위한 게이트웨이 대칭키 사이의 배타적 논리합을 연산하여 제2암호문을 생성할 수 있다.

<34> 리더(111-113) 즉, RFID 리더 (RFID Reader)는 안테나와 칩을 가진 무선통신 장치이다. 리더는 근처에 있는 멤버 태그(100)에게 RF통신으로 질의를 보내면, 그 질의를 받은 멤버 태그(100)는 리더(111-113)에게 자신의 정보를 보내고, 그 정보를 받은 리더(111-113)는 게이트웨이(120)에게 전송한다. 리더(111-113)는 멤버 태그(100)에 비해 높은 연산 능력을 갖는다.

<35> 리더(111-113)는 멤버 태그(100) 중 하나 이상의 멤버 태그에 질의를 전송한다. 또한, 리더(111-113)는 질의를 받은 멤버 태그로부터 제2암호문을 수신하고, 수신된 제2암호문을 게이트웨이(120)로 전송한다. 리더(111-113)는 도 1a와 같이 시스템에 복수로 존재할 수 있다.

<36> 게이트웨이(Gateway, 120)는 리더(111-113)와 마찬가지로 높은 연산 능력을 갖는다. 게이트웨이는 메시지를 자신의 키 즉, 게이트웨이 대칭키로 각각 연산하여 모든 그룹 데이터베이스(131-139)에게 전송한다.

<37> 게이트웨이(120)는 제2암호문과 복수의 멤버 태그(100)가 포함된 복수의 그룹들에 대응되는 각각의 게이트웨이 대칭키들을 이용하여 그룹 메시지들을 생성한다. 게이트웨이(120)는 복수의 그룹들에 대응되는 모든 게이트웨이 대칭키를 저장할 수 있다. 또한, 게이트웨이(120)는 제2암호문과 복수의 그룹들에 대응되는 각각의 게이트웨이 대칭키들 사이의 배타적 논리합을 연산하여 그룹 메시지들을 생성할 수 있다.

<38> 그룹 데이터베이스 (Group Database, 131-139)는 게이트웨이(120)로부터 메시지를 받으면 자신의 개인키로 복호화를 실행한다. 본 발명에 따른 프로토콜에서 각 그룹 데이터베이스(131-139)는 자신이 관리하는 그룹의 정보와 개인키를 안전하게 관리한다고 가정한다.

<39> 복수의 그룹 데이터베이스(131-139)는 복수의 멤버 태그(100)가 속한 복수의 그룹들 중 어느 하나의 그룹에 포함된다. 또한, 복수의 그룹 데이터베이스(131-139)는 게이트웨이(120)에 의해 생성된 그룹 메시지들을 멤버 태그가 포함된 그룹의 개인키로 복호화하여 멤버 태그의 고유 정보를 획득한다.

<40> 본 발명에 따른 자체 재암호화 프로토콜(SREP)은 초기화 단계와 실행 단계로 나누어진다. 초기화 단계는 제조업체에 의해서 안전하게 실행된다고 가정한다. 멤버 태그의 정보를 얻기 위해 리더가 멤버 태그에게 질의를 보내면 실행 단계가 시작된다.

<41> 초기화(Setup) 단계는 제조업체에 의해 다음과 같이 수행된다.

<42> 첫번째는 그룹화 과정이다. 제조업체는 모든 멤버 태그를 여러 개의 그룹으로 랜덤하게(Randomly) 나눈다. 그룹의 수(N)는 안전성과 효율성을 고려하여 적절하게 정해진다.

<43> 두번째는 키 생성 과정이다. G 는 ElGamal 암호 시스템 기반의 그룹이라고 하고, q 는 그룹 G 의 위수(order)라고 하며, g, s 는 그룹 G 의 생성자(generator)라고 한다. 제조업체는 각 그룹의 키 4개를 다음의 표 1과 같이 생성한다.

【표 1】

<44>

키	표기법	계산식
그룹 개인키 (Group Private Key)	x_i	$x_i \in \overrightarrow{RZ_{q-1}}$
그룹 공개키 (Group Public Key)	y_i	$y_i = g^{x_i}$
업데이트 공개키 (Update Public Key)	u_i	$u_i = s^{x_i}$
게이트웨이 대칭키 (Gateway Symmetric Key)	GS_i	$GS_i \in \overrightarrow{RZ_{q-1}}$

<45> 세번째는 암호화 과정이다. m_{ij} 는 멤버 태그의 정보라고 한다. Tag_{ij} 는 i 번째 그룹의 j 번째 태그를 의미한다.

<46> 제조업체는 각 멤버 태그마다 새로운 임의의 값 k_0, k_1, k_2, k_3 를 뽑아서 암호문 C_{ij} 와 업데이트 값 UD_{ij} 를 수학식 1에 의하여 계산된다.

$$C_{ij} = [(\alpha_0, \beta_0); (\alpha_1, \beta_1)] = [(m_{ij} y_i^{k_0}, g^{k_0}); (y_i^{k_1}, g^{k_1})]$$

$$UD_{ij} = [(\gamma_0, \delta_0); (\gamma_1, \delta_1)] = [(u_i^{k_2}, s^{k_2}); (u_i^{k_3}, s^{k_3})]$$

<47>

<48> C_{ij}, UD_{ij}, GS_i 를 각 멤버 태그에 안전하게 저장한다. 또한 제조업체는 모든 GS_i 를 게이트웨이

에 저장하고, 각 그룹의 개인키 x_i 는 각각 해당되는 그룹 데이터베이스에 안전하게 저장한다.

<49> 도 1b는 도 1a에 사용되는 비밀값들을 도시한 것이다.

<50> 본 발명에 따른 프로토콜의 구성요소는 멤버 태그, 게이트 웨이, 그룹 데이터베이스에 C_{ij} , UD_{ij} , GS_i , x_i 와 같은 비밀값을 저장한다. 또한, 본 발명에 따른 프로토콜은 멤버 태그, 게이트웨이와 그룹 데이터베이스를 통합한 게이트 웨이 데이터베이스에 C_{ij} , UD_{ij} , GS_i , x_i 와 같은 비밀값을 저장할 수 있다.

<51> 도 1c는 도 1a의 게이트웨이(120)에서 각각의 그룹 데이터베이스(131-139)에 그룹 메시지들을 전송하는 과정을 도시한 것이다.

<52> 게이트웨이(120)는 도 1c와 같이 암호문 P_{ij} 와 모든 GS_i 를 각각 배타적 논리합(XOR) 연산하여 각 그룹 데이터베이스(131-139)에게 전송한다.

<53> 도 1d는 도 1a의 그룹 데이터베이스(131-139)에 의한 복호화 과정을 도시한 것이다.

<54> 도 1d에서, m1이 1인 경우는 고유 정보(m0)가 포함된 그룹과 그룹 데이터베이스(131-139)가 포함된 그룹이 동일한 경우이다. 즉, 제2암호문이 정확한 개인키로 복호화된 경우이다. 이때, 복호화에 성공한 그룹 데이터베이스는 고유 정보(m0)를 획득한다.

<55> 도 2는 본 발명의 다른 실시예에 따른 태그 리드 시스템의 구조도이다.

<56> 복수의 멤버 태그(200)는 복수의 그룹들 중 어느 하나의 그룹에 포함되고, 리더(211-213)로부터 수신되는 질의에 대응하여 암호화된 고유 정보를 재암호한 제1암호문을 생성한다. 또한, 복수의 멤버 태그(200)는 제1암호문을 질의를 수신한 멤버 태그의 그룹을 위한 게이트웨이 대칭키로 암호화한 제2암호문을 생성한다. 멤버 태그(200)는 고유 정보를 업데이트 값으로 재암호화하여 제1암호문을 생성할 수 있다. 또한, 멤버 태그(200)는 멤버 태그가 포함된 그룹을 위한 게이트웨이 대칭키를 저장할 수 있다. 멤버 태그(200)는 제1암호문과 멤버 태그(200)가 포함된 그룹을 위한 게이트웨이 대칭키 사이의 배타적 논리합을 연산하여 제2암호문을 생성할 수 있다.

<57> 리더(211-213)는 멤버 태그(200)에 질의를 전송하고, 질의를 받은 멤버 태그로부터 제2암호문을 수신한다. 또한, 리더(211-213)는 수신된 제2암호문을 게이트 웨이 데이터베이스(240)에 전송한다.

<58> 게이트웨이 데이터베이스(240)는 제2암호문과 복수의 그룹들에 대응되는 각각의 게이트웨이 대칭키들을 이용하여 그룹 메시지들을 생성하고, 그룹 메시지들을 멤버 태그가 포함된 그룹의 개인키로 복호화하여 고유 정보를 획득한다. 게이트웨이 데이터베이스(240)는 게이트웨이(120) 및 그룹 데이터베이스(131-139)가 통합된 형태일 수 있다. 또한, 게이트웨이 데이터베이스(240)는 복수의 그룹들에 대응되는 모든 게이트웨이 대칭키를 저장하고, 제2암호문과 복수의 그룹들에 대응되는 각각의 게이트웨이 대칭키들 사이의 배타적 논리합을 연산하여 그룹 메시지들을 생성할 수 있다.

<59> 도 3은 본 발명의 또다른 실시예에 따른 태그 리드 방법의 흐름도이다.

<60> 먼저, 복수의 그룹들 중 어느 하나의 그룹에 포함된 복수의 멤버 태그에 질의를 전송한다(300 과정).

<61> 다음, 질의를 수신한 멤버 태그가 질의에 대응하여 암호화된 고유 정보를 재암호한 제1암호문을 생성하고, 제1암호문을 질의를 수신한 멤버 태그의 그룹을 위한 게이트웨이 대칭키로 암호화한 제2암호문을 생성한다(310 과정). 이 과정(310 과정)은 제1암호문과 질의를 수신한 멤버 태그의 그룹을 위한 게이트웨이 대칭키 사이의 배타적 논리합을 연산하여 제2암호문을 생성하는 과정일 수 있다. 이 과정(310 과정)은 멤버 태그가 수학식 2의 업

테이트값 UD_{ij} 를 이용하여 기존의 암호문 C_{ij} 를 암호문 C'_{ij} 로 재암호화하는 과정일 수 있다.

$$C_{ij} = [(\alpha_0, \beta_0); (\alpha_1, \beta_1)]$$

$$UD_{ij} = [(\gamma_0, \delta_0); (\gamma_1, \delta_1)]$$

<62>

암호문 C'_{ij} 은 수학식 3과 같이 표현된다.

$$C'_{ij} = [(\alpha'_0, \beta'_0); (\alpha'_1, \beta'_1)]$$

$$= [(\alpha_0 \alpha_1 \gamma_0, \beta_0 \beta_1 \delta_0); (\alpha_1 \gamma_0 \gamma_1, \beta_1 \delta_0 \delta_1)]$$

<64>

또한, 멤버 태그는 새롭게 재암호화된 암호문 C'_{ij} 를 GS_i 와 식 (3)과 같이 배타적 논리합(XOR) 연산하여

암호문 P_{ij} 를 생성할 수 있다. 암호문 P_{ij} 은 수학식 4와 같이 표현된다.

$$P_{ij} = C'_{ij} \text{ XOR } GS_i$$

<66>

제2암호문이 생성되면, 생성된 제2암호문을 게이트웨이로 전송한다(320 과정). 이 과정(320 과정)은 암호문

P_{ij} 를 리더를 통해서 게이트웨이에게 전송하는 과정일 수 있다.

<68>

다음, 게이트웨이가 제2암호문과 복수의 그룹들에 대응되는 각각의 게이트웨이 대칭키들을 이용하여 그룹 메시지들을 생성한다(330 과정). 이 과정(330 과정)은 제2암호문과 복수의 그룹들에 대응되는 각각의 게이트웨이 대칭키들 사이의 배타적 논리합을 연산하여 그룹 메시지들을 생성하는 과정일 수 있다. 이 과정(330 과정)은 게이

트웨이가 암호문 P_{ij} 와 모든 GS_i 를 각각 배타적 논리합(XOR) 연산하여 각 그룹 데이터베이스에게 전송하는 과정일 수 있다.

<69>

마지막으로, 복수의 그룹들 중 어느 하나의 그룹에 포함된 복수의 그룹 데이터베이스가 그룹 메시지들을 질의를 수신한 멤버 태그가 포함된 그룹의 개인키로 복호화하여 질의를 수신한 멤버 태그의 고유 정보를 획득한다(340 과정).

<70>

이 과정(340 과정)은 전송된 메시지에 대응되는 그룹 데이터베이스가 도 1d의 알고리즘을 실행하여 멤버 태그의

정보 m_{ij} 를 얻는 과정일 수 있다.

<71>

도 4는 본 발명의 또다른 실시예에 따른 태그 리더 방법의 흐름도이다.

<72>

먼저, 복수의 그룹들 중 어느 하나의 그룹에 포함된 복수의 멤버 태그에 질의를 전송한다(400 과정).

<73>

다음, 질의를 수신한 멤버 태그가 질의에 대응하여 암호화된 고유 정보를 재암호한 제1암호문을 생성하고, 제1암호문을 질의를 수신한 멤버 태그의 그룹을 위한 게이트웨이 대칭키로 암호화한 제2암호문을 생성한다(410 과정).

<74>

제2암호문이 생성되면, 생성된 제2암호문을 게이트웨이 데이터베이스로 전송한다(450 과정).

<75>

마지막으로, 게이트웨이 데이터베이스가 제2암호문과 복수의 그룹들에 대응되는 각각의 게이트웨이 대칭키들을 이용하여 그룹 메시지들을 생성하고, 그룹 메시지들을 질의를 수신한 멤버 태그가 포함된 그룹의 개인키로 복호

화하여 고유 정보를 획득한다(460 과정).

<76> 본 발명에 따른 안전성 (Security)을 분석하면 다음과 같다.

<77> 멤버 태그와 리더의 통신에서 수동적 공격자는 모든 암호문 P 를 도청할 수 있고, 능동적 공격자는 이 암호문 P 를 분석, 변경하여 정당한 리더로 인증되도록 할 것이다. 본 발명에 따른 태그 리더 시스템에서 공격자는 암호문 P 와 그 암호문을 이용하여 계산된 형태만을 알 수 있다. 공격자는 암호문 P 를 이용하여 멤버 태그의 비밀 정보인 C' , UD , GS 를 알아내려고 할 것이다. 공격자가 활용할 수 있는 정보는 표 3과 같다.

<78> 만일 공격자가 어떤 멤버 태그의 비밀값들 C' , UD , GS 중에서 단지 한 가지 값만 알더라도, 그 멤버 태그의 암호문 P 를 분석하여 다른 비밀값들도 차례로 알아낼 수 있다. 그러나, 공격자는 어떠한 비밀값도 개별적으로 알 수 없고, 다만 새롭게 재암호화된 암호문들($C'; C''; C''' \dots$)과 GS 가 XOR로 계산된 형태만 알 수 있다. 그러므로 공격자는 멤버 태그의 비밀값들 중에서 어떠한 값도 개별적으로 얻을 수 없다.

<79> 먼저, 정보노출을 분석하면 다음과 같다. 만일 공격자가 암호문 C' 를 안다고 할지라도, 제안된 프로토콜은 공개키 기반 구조이기 때문에, 멤버 태그의 정보(m)를 알 수 없다. 즉 개인키를 가지고 있는 그룹 데이터베이스만이 태그의 정보(m)를 얻을 수 있다.

<80> 다음, 위치추적을 분석하면 다음과 같다. 암호문 P 에서 그룹 대칭키 GS 는 고정되어 있지만, 암호문 C' 는 매 세션마다 재암호화되어 항상 변하므로 암호문 P 는 항상 변한다. 공격자가 매 세션마다 변하는 모든 암호문 P 를 얻더라도, 공격자는 2개의 다른 암호문 P 가 같은 태그에서 왔는지를 결정할 수 없다. 그러므로 제안된 프로토콜에서 공격자는 목표로 하는 태그의 위치를 추적할 수 없다.

<81> 따라서, 본 발명은 정보노출과 위치추적 문제에 안전하므로 멤버 태그를 사용하는 소비자의 프라이버시를 보호할 수 있다.

<82> 본 발명의 멤버 태그는 외부장치 없이 자체적으로 재암호화를 실행하기 때문에, 멤버 태그는 리더의 모든 질의에 대하여 항상 변경된 형태의 메시지를 전송하게 되고, 공격자는 멤버 태그를 추적하는 것이 완전히 불가능해진다. 본 발명에 따른 프로토콜은 외부장치 없이 자체적으로 재암호화를 실행하므로, 인증되지 않은 외부장치가 멤버 태그에 잘못된 값을 갱신하여 발생하는 잠재적인 모든 문제들을 근본적으로 해결할 수 있다. 본 발명에 따른 태그는 외부장치 없이 자체적으로 재암호화를 실행하기 때문에, 매 세션마다 변경된 형태의 메시지를 리더에게 전송한다. 그러므로 본 발명의 프로토콜은 종래의 프로토콜보다 훨씬 더 강한 프라이버시를 제공한다.

<83> 또한 본 발명에 따른 프로토콜은 시도-응답 기법(Challenge-Response technique)을 적용하는 경우, 재사용 공격(Replay Attack)과 스푸핑 공격(Spoofing Attack)에 대하여 안전하다는 것을 알 수 있다.

<84> 다음, 본 발명에 따른 효율성(Efficiency)을 분석하면 다음과 같다.

<85> 태그 리더 시스템은 멤버 태그의 연산량을 줄이는 것이 가장 중요하므로, 이를 중심으로 제안된 프로토콜을 평가해본다.

<86> 리더가 멤버 태그에 질의를 보내면 멤버 태그는 자체 재암호화와 그룹 대칭 암호화를 실행하고, 리더에게 암호

문 P 를 전송한다. 멤버 태그는 자체 재암호화 단계에서 8번의 곱셈 연산을 실행하고, 그룹 대칭 암호화 단계에서 1번의 XOR연산을 실행한다.

<87> 본 발명에 따른 프로토콜은 곱셈 연산을 사용하기 때문에, 종래의 프로토콜보다 훨씬 효율적이다. 이때, XOR연산은 곱셈 연산에 비해 상대적으로 연산량이 작기 때문에 무시한다. 이를 정리하면 표 2와 같다.

【표 2】

프로토콜	연산량
종래의 프로토콜	지수 연산
본 발명에 따른 프로토콜(SREP)	곱셈 연산

<89> 상술한 바와 같이, 본 발명은 태그의 제한된 연산 능력을 사용하여 태그 사용자의 프라이버시를 보호하는 프로토콜을 제안한다. 본 발명에 따른 프로토콜의 태그는 외부장치를 사용하지 않고 자체적으로 재암호화하므로, 리더의 모든 질의에 대해서 항상 변경된 형태의 메시지를 전송한다. 제안된 프로토콜은 정보 노출 문제와 위치 추적 문제를 해결함으로써, 태그를 가진 소비자의 프라이버시를 보호할 수 있다. 또한, 본 발명에 따른 태그는 단지 곱셈과 XOR연산만을 사용하여 암호화를 실행하기 때문에, 제한된 연산 능력을 가진 저가형 태그 또는 저가형 RFID 시스템에 적용하는 것이 가능하다.

<90> 바람직하게는, 본 발명의 멤버 태그(또는 RFID 태그)는 능동형 태그(Active Tag) 또는 수동형 태그(Passive Tag)를 포함할 수 있다.

<91> 수동형 태그의 특징은 제한된 연산 능력, 소형, 경량, 저비용 등이 있다. 따라서, 본 발명은 수동형 태그를 이용하여 저가형 시스템을 구성할 수 있다.

<92> 또한, 본 발명은 능동형 태그를 이용하여 종래의 능동형 태그를 이용한 시스템보다 처리 속도를 향상시킬 수 있다.

<93> 바람직하게는, 본 발명의 자체 재암호화 프로토콜을 이용하는 태그 리드 방법을 컴퓨터에서 실행시키기 위한 프로그램을 컴퓨터로 읽을 수 있는 기록매체에 기록하여 제공할 수 있다.

<94> 본 발명은 소프트웨어를 통해 실행될 수 있다. 소프트웨어로 실행될 때, 본 발명의 구성 수단들은 필요한 작업을 실행하는 코드 세그먼트들이다. 프로그램 또는 코드 세그먼트들은 프로세서 판독 가능 매체에 저장되거나 전송 매체 또는 통신망에서 반송파와 결합된 컴퓨터 데이터 신호에 의하여 전송될 수 있다.

<95> 본 발명은 도면에 도시된 일 실시예를 참고로 하여 설명하였으나 이는 예시적인 것에 불과하며 당해 분야에서 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 실시예의 변형이 가능하다는 점을 이해할 것이다. 그러나, 이와 같은 변형은 본 발명의 기술적 보호범위내에 있다고 보아야 한다. 따라서, 본 발명의 진정한 기술적 보호범위는 첨부된 특허청구범위의 기술적 사상에 의해서 정해져야 할 것이다.

발명의 효과

<96> 상술한 바와 같이, 본 발명에 의하면, 태그의 제한된 연산 능력 내에서 태그 사용자의 프라이버시를 보호하는 자체 재암호화 프로토콜을 이용함으로써, 태그가 외부장치를 사용하지 않고 자체적으로 재암호화하여 리더의 모든 질의에 대해서 항상 변경된 형태의 메시지를 전송할 수 있어 정보 노출 문제와 위치 추적 문제를 해결할 수 있고, 태그를 가진 소비자의 프라이버시를 보호할 수 있으며, 태그가 단지 곱셈과 논리적 배타합(XOR) 연산만을 수행하여 암호화를 실행하기 때문에, 태그의 연산량을 낮추어 제한된 연산 능력을 가진 저가형 태그 또는 저가형 RFID 시스템에 적용될 수 있는 효과가 있다.

도면의 간단한 설명

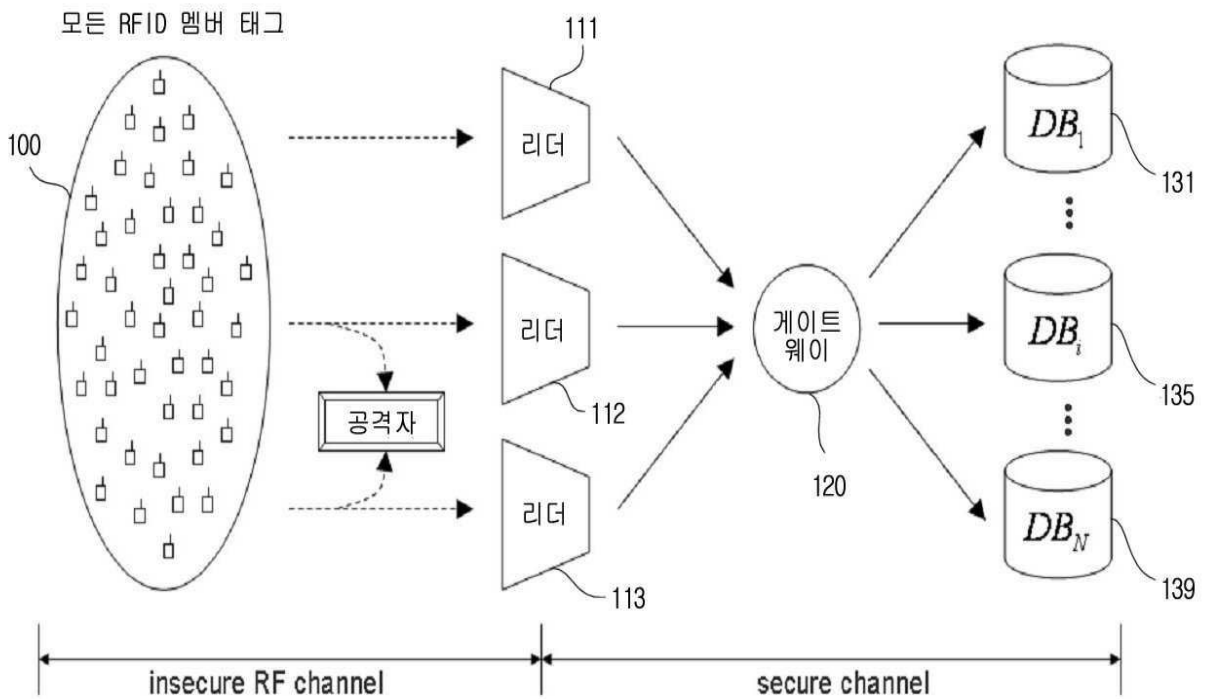
<1> 도 1a는 본 발명의 일 실시예에 따른 태그 리드 시스템의 구조도이다.

<2> 도 1b는 도 1a에 사용되는 비밀값들을 도시한 것이다.

- <3> 도 1c는 도 1a의 게이트웨이에서 각각의 그룹 데이터베이스에 그룹 메시지들을 전송하는 과정을 도시한 것이다.
- <4> 도 1d는 도 1a의 그룹 데이터베이스에 의한 복호화 과정을 도시한 것이다.
- <5> 도 2는 본 발명의 다른 실시예에 따른 태그 리드 시스템의 구조도이다.
- <6> 도 3은 본 발명의 또다른 실시예에 따른 태그 리드 방법의 흐름도이다.
- <7> 도 4는 본 발명의 또다른 실시예에 따른 태그 리드 방법의 흐름도이다.

도면

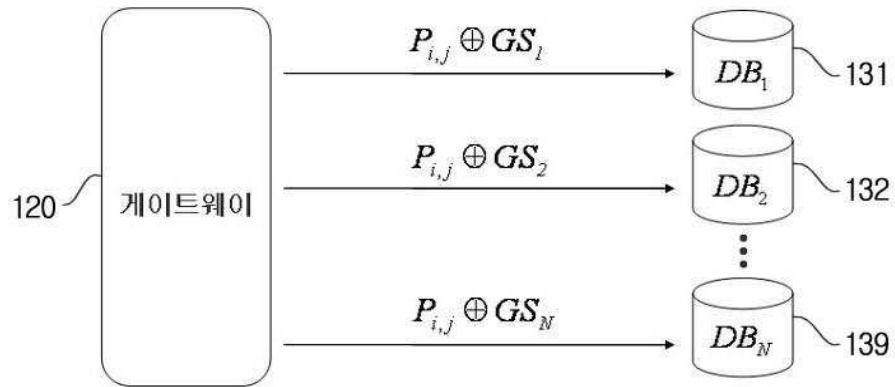
도면1a



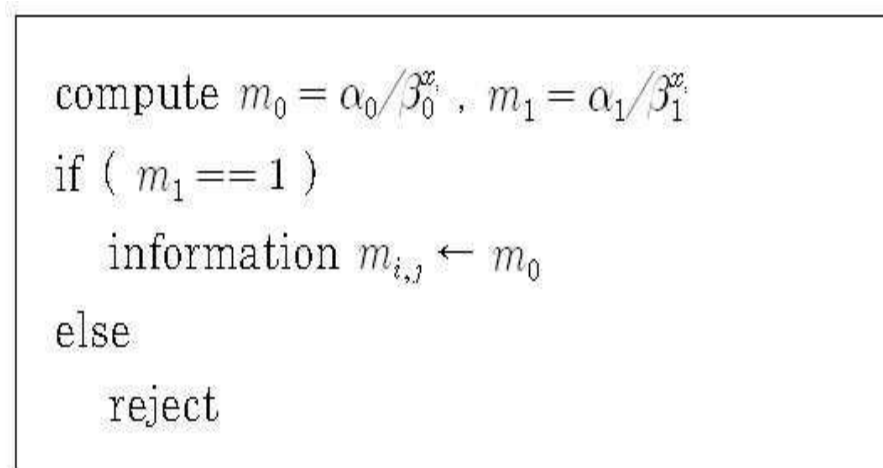
도면1b

구성요소	j -번째 멤버 태그	i -번째 그룹	암호문	업데이트 값	게이트웨이 대칭키	그룹 개인키
모든 RFID 멤버 태그	tag3	group ₁	$C_{1,3}$	$UD_{1,3}$	GS_1	-
	tag11		$C_{1,11}$	$UD_{1,11}$		
	⋮		⋮	⋮		
	tag4		$C_{1,4}$	$UD_{1,4}$		
	tag23	group ₂	$C_{2,23}$	$UD_{2,23}$	GS_2	-
	tag7		$C_{2,7}$	$UD_{2,7}$		
	⋮		⋮	⋮		
	tag52		$C_{2,52}$	$UD_{2,52}$		
	⋮	⋮	⋮	⋮	⋮	-
	tag97	group _N	$C_{N,97}$	$UD_{N,97}$	GS_N	-
	tag _n		$C_{N,n}$	$UD_{N,n}$		
	⋮		⋮	⋮		
	tag36		$C_{N,36}$	$UD_{N,36}$		
리더	-	-	-	-	-	-
게이트웨이	-	-	-	-	GS_1 ⋮ GS_N	-
그룹 데이터베이스	-	group ₁	-	-	-	x_1
	-	group ₂	-	-	-	x_2
	-	⋮	-	-	-	⋮
	-	group _N	-	-	-	x_N

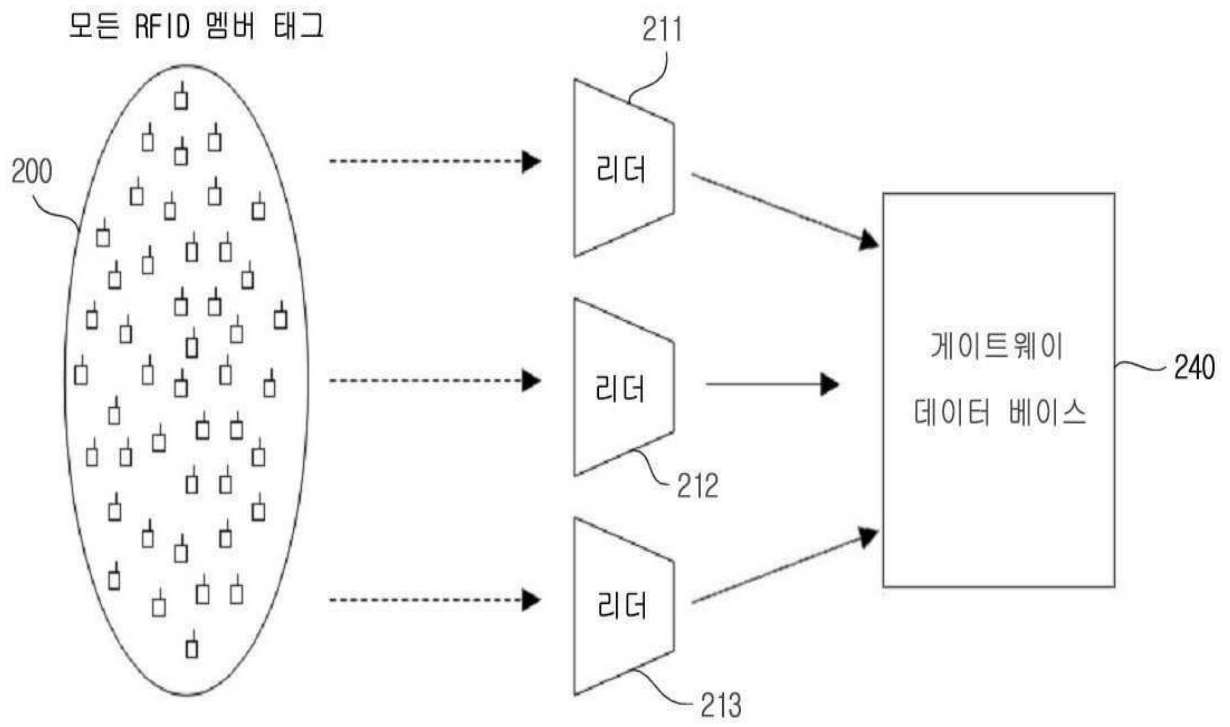
도면1c



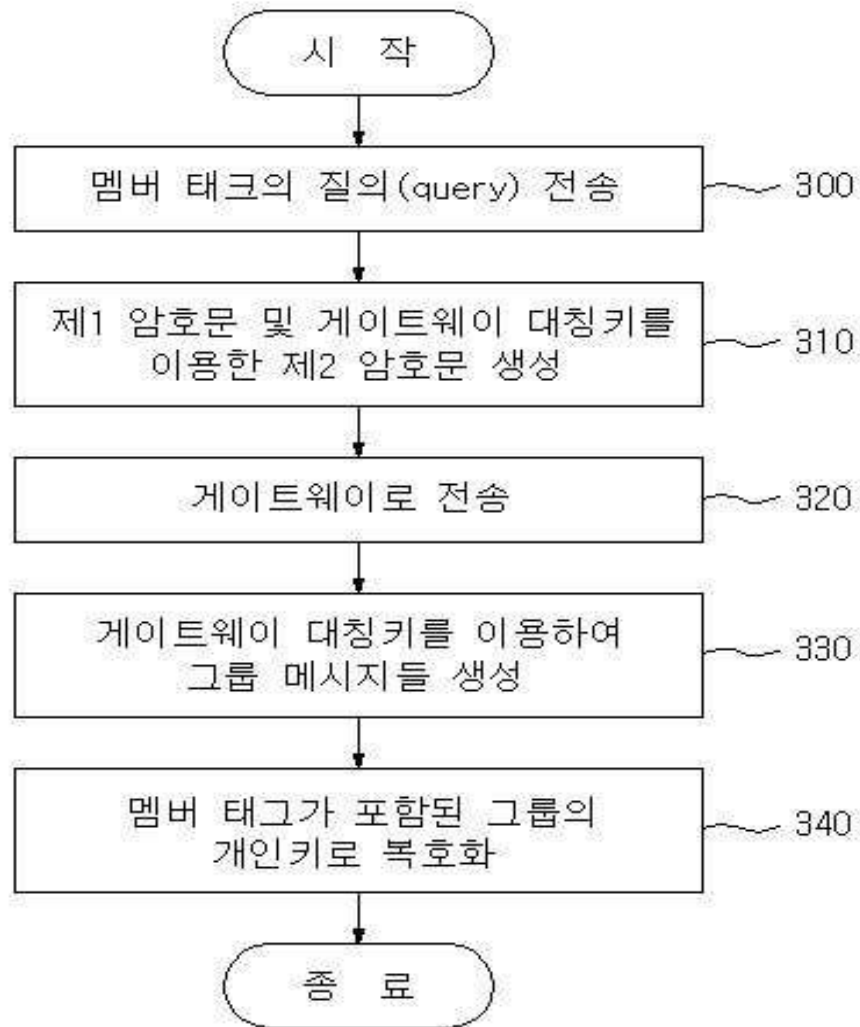
도면1d



도면2



도면3



도면4

