



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2009-0034246
(43) 공개일자 2009년04월07일

(51) Int. Cl.

H04L 9/32 (2006.01) H04B 5/02 (2006.01)

H04W 84/16 (2009.01) G06K 17/00 (2006.01)

(21) 출원번호 10-2007-0099520

(22) 출원일자 2007년10월02일

심사청구일자 2007년10월02일

(71) 출원인

고려대학교 산학협력단

서울 성북구 안암동5가1 고려대학교 내

(72) 발명자

최진영

서울 성북구 안암동5가 고려대학교 컴퓨터학과 정형기법연구실

김현석

서울 성북구 안암동5가 고려대학교 컴퓨터학과 정형기법연구실

오정현

서울 성북구 안암동5가 고려대학교 컴퓨터학과 정형기법연구실

(74) 대리인

현종철

전체 청구항 수 : 총 19 항

(54) RFID 환경에서의 보안 방법, 이를 기록한 기록 매체 및 그 시스템

(57) 요약

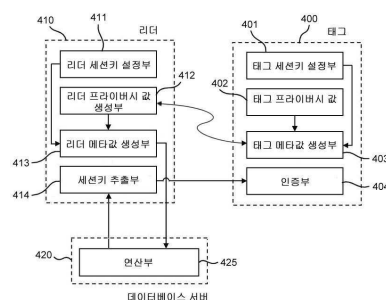
RFID 환경에서의 보안 방법, 이를 기록한 기록 매체 및 그 시스템이 개시된다.

본 발명에 따른 RFID 환경에서의 보안 방법은,

RFID 리더 및 RFID 태그에서 데이터 베이스 서버 간의 세션키를 각각 생성하는 단계; 상기 태그가 상기 리더로부터 쿼리(query)를 수신하면, 상기 태그에서 자신의 식별자를 이용하여 태그 프라이버시 값을 생성하는 단계; 상기 태그에서 상기 태그 프라이버시 값을 포함하는 태그 파라미터를 이용하여 태그 메타값을 생성하는 단계; 상기 생성된 태그 메타값이 상기 리더로 전송되면, 상기 리더의 식별자를 이용하여 생성한 리더 프라이버시 값을 포함하는 리더 파라미터를 이용하여 리더 메타값을 생성하고, 상기 리더 메타값과 상기 태그 메타값을 상기 데이터베이스 서버로 전송하는 단계; 상기 데이터베이스 서버에서 상기 태그 메타값 및 상기 리더 메타값에 따라 배타적 논리합 연산을 수행하고, 상기 수행된 배타적 논리합 연산의 결과값을 상기 리더에 전송하는 단계; 및 상기 배타적 논리합 연산의 결과값으로부터 리더 자신의 세션키를 이용하여 상기 태그의 세션키를 추출하고, 상기 추출된 태그의 세션키를 상기 태그에 전송하면 상기 태그에서 상기 리더의 인증을 수행하는 단계를 포함한다.

본 발명에 의하면, 태그와 리더가 각각의 자신의 식별자를 프라이버시(Privacy)라는 통신참여자의 식별자를 입력값으로 하여 익명의 값을 출력하는 함수를 이용하여 태그와 리더 자신의 프라이버시를 외부에 노출시키지 않을 수 있고, 태그에게 리더의 안전한 인증을 위해 사전에 리더와 태그가 데이터베이스와의 세션키를 각각 설정하여 이를 기반으로 리더 자신의 정보를 보호하고, 태그로부터 인증을 받을 수 있으며, 상기 태그의 정보와 리더의 정보를 배타적 논리합 연산에 의해 암호화함으로써 암호화 과정에 수반되는 연산량이 적으므로 메모리의 가용성을 높일 수 있으며, 태그의 정보를 인증된 리더기에 의해 데이터베이스에 접근할 수 있도록 하고, 태그의 정보에 대한 중간자 공격과 재생 공격을 방지하여 사용자의 안전성과 신뢰성을 제공할 수 있는 효과가 있다.

대표도 - 도4



특허청구의 범위

청구항 1

RFID 리더 및 RFID 태그에서 데이터 베이스 서버 간의 세션키를 각각 생성하는 단계;

상기 태그가 상기 리더로부터 쿼리(query)를 수신하면, 상기 태그에서 자신의 식별자를 이용하여 태그 프라이버시 값을 생성하는 단계;

상기 태그에서 상기 태그 프라이버시 값을 포함하는 태그 파라미터를 이용하여 태그 메타값을 생성하는 단계;

상기 생성된 태그 메타값이 상기 리더로 전송되면, 상기 리더의 식별자를 이용하여 생성한 리더 프라이버시 값을 포함하는 리더 파라미터를 이용하여 리더 메타값을 생성하고, 상기 리더 메타값과 상기 태그 메타값을 상기 데이터베이스 서버로 전송하는 단계;

상기 데이터베이스 서버에서 상기 태그 메타값 및 상기 리더 메타값에 따라 배타적 논리합 연산을 수행하고, 상기 수행된 배타적 논리합 연산의 결과값을 상기 리더에 전송하는 단계; 및

상기 배타적 논리합 연산의 결과값으로부터 리더 자신의 세션키를 이용하여 상기 태그의 세션키를 추출하고, 상기 추출된 태그의 세션키를 상기 태그에 전송하면 상기 태그에서 상기 리더의 인증을 수행하는 단계를 포함하는 RFID 환경에서의 보안 방법.

청구항 2

제 1 항에 있어서,

상기 태그 파라미터는

상기 리더의 식별자, 상기 데이터 베이스 서버의 공개키, 상기 태그의 세션키 및 상기 태그 프라이버시 값을 포함하는 것을 특징으로 하는 RFID 환경에서의 보안 방법.

청구항 3

제 2 항에 있어서,

상기 리더의 식별자는 상기 데이터 베이스 서버의 공개키로 암호화된 것을 특징으로 하는 RFID 환경에서의 보안 방법.

청구항 4

제 2 항에 있어서,

상기 태그 메타값 $Anonymous(T)$ 은 하기의 식 (1)에 의해 연산되는 것을 특징으로 하는 RFID 환경에서의 보안 방법.

$$Anonymous(T) = E_{DB_{public}} \{ R, Privacy(T), SKey T \} \quad (1)$$

(상기 식 1에서 R 은 상기 리더의 식별자, $SKey T$ 는 상기 태그 T 의 세션키, $Privacy(T)$ 는 상기 태그 프라이버시 값, DB_{public} 는 상기 데이터 베이스 서버의 공개키, E 는 해쉬 기반 암호화 연산을 의미한다.)

청구항 5

제 1 항에 있어서,

상기 리더 파라미터는

상기 태그의 식별자, 상기 데이터 베이스 서버의 공개키, 상기 리더의 세션키 및 상기 리더 프라이버시 값을 포

함하는 것을 특징으로 하는 RFID 환경에서의 보안 방법.

청구항 6

제 5 항에 있어서,

상기 태그의 식별자는

상기 데이터 베이스 서버의 공개키로 암호화된 것을 특징으로 하는 RFID 환경에서의 보안 방법.

청구항 7

제 5 항에 있어서,

상기 리더 메타값 $Anonymous(R)$ 은 하기의 식 (2)에 의해 연산되는 것을 특징으로 하는 RFID 환경에서의 보안 방법.

$$Anonymous(R) = E_{DB_{public}} \{ T, Privacy(R), SKey R \} \quad (2)$$

(상기 식 1에서 T 는 상기 태그의 식별자, $SKey R$ 는 상기 리더 R 의 세션키, $Privacy(R)$ 는 상기 리더 프라이버시 값, DB_{public} 는 상기 데이터 베이스 서버의 공개키, E 는 해쉬 기반 암호화 연산을 의미한다.)

청구항 8

제 1 항에 있어서,

상기 리더의 인증을 수행하는 단계는

상기 리더에서 상기 추출된 태그의 세션키를 이용하여 상기 리더의 식별자를 암호화한 리더 암호화값을 태그에 전송하는 단계;

상기 태그에서 상기 암호화값으로부터 상기 태그의 세션키와 리더의 식별자를 연산하는 단계; 및

상기 연산된 태그의 세션키 및 리더의 식별자로부터 상기 리더를 인증하는 단계를 포함하는 것을 특징으로 하는 RFID 환경에서의 보안 방법

청구항 9

제 1 항에 있어서,

상기 리더의 인증을 수행하는 단계는

상기 태그에서 상기 인증된 리더에게 상기 쿼리에 대응되는 태그 정보를 전송하는 단계를 더 포함하는 것을 특징으로 하는 RFID 환경에서의 보안 방법.

청구항 10

제 1 항 내지 제 9 항 중 어느 하나의 방법을 컴퓨터에서 수행하도록 프로그램으로 기록된 기록매체.

청구항 11

태그 정보를 요청하는 RFID 리더, 태그 정보를 제공하는 RFID 태그 및 데이터 베이스 서버를 포함하는 RFID 환경에서의 보안 시스템에 있어서,

상기 태그는

상기 데이터 베이스 서버 간의 세션키를 설정하는 태그 세션키 설정부;

상기 리더로부터 쿼리를 수신하여 태그 자신의 식별자를 이용하여 태그 프라이버시 값을 생성하는 태그 프라이

버시 값 생성부;

상기 태그 프라이버시 값을 포함하는 태그 파라미터를 이용하여 태그 메타값을 생성하는 태그 메타값 생성부;
및

상기 리더의 인증을 수행하는 인증부를 포함하고,

상기 리더는

상기 데이터 베이스 서버 간의 세션키를 설정하는 리더 세션키 설정부;

상기 리더 자신의 식별자를 이용하여 리더 프라이버시 값을 생성하는 리더 프라이버시 값 생성부;

상기 리더 프라이버시값 생성부에서 생성한 리더 프라이버시 값을 포함하는 리더 파라미터를 이용하여 리더 메타값을 생성하는 리더 메타값 생성부; 및

상기 데이터 베이스 서버로부터 전송되는 배타적 논리합 연산의 결과값으로부터 상기 태그의 세션키를 추출하는 세션키 추출부;

상기 데이터베이스 서버는

상기 리더 송수신부로부터 수신한 상기 태그 메타값 및 상기 리더 메타값에 따라 배타적 논리합 연산을 수행하는 연산부를 포함하는 RFID 환경에서의 보안 시스템.

청구항 12

제 11 항에 있어서,

상기 리더는

상기 태그에게 태그 정보를 요청하는 질의 생성부를 더 포함하는 것을 특징으로 하는 RFID 환경에서의 보안 시스템.

청구항 13

제 11 항에 있어서,

상기 리더는

상기 태그 메타값을 수신하고, 상기 리더 메타값 생성부로부터 생성된 리더 메타값 및 상기 수신한 태그 메타값을 상기 데이터베이스 서버로 전송하는 리더 송수신부를 포함하는 것을 특징으로 하는 RFID 환경에서의 보안 시스템.

청구항 14

제 11 항에 있어서,

상기 태그 파라미터는

상기 리더의 식별자, 상기 데이터 베이스 서버의 공개키, 상기 태그의 세션키 및 상기 태그 프라이버시 값을 포함하는 것을 특징으로 하는 RFID 환경에서의 보안 시스템.

청구항 15

제 14 항에 있어서,

상기 리더의 식별자는 상기 데이터 베이스 서버의 공개키로 암호화된 것을 특징으로 하는 RFID 환경에서의 보안 시스템.

청구항 16

제 14항에 있어서,

상기 태그 메타값 $Anonymous(T)$ 은 하기의 식 (3)에 의해 연산되는 것을 특징으로 하는 RFID 환경에

서의 보안 시스템.

$$Anonymous(T) = E_{DB_{public}} \{ R, Privacy(T), SKey T \} \quad (3)$$

(상기 식 1에서 R 은 상기 리더의 식별자, $SKey T$ 는 상기 태그 T 의 세션키, $Privacy(T)$ 는 상기 태그 프라이버시 값, DB_{public} 는 상기 데이터 베이스 서버의 공개키, E 는 해쉬 기반 암호화 연산을 의미한다.)

청구항 17

제 11 항에 있어서,

상기 리더 파라미터는

상기 태그의 식별자, 상기 데이터 베이스 서버의 공개키, 상기 리더의 세션키 및 상기 리더 프라이버시 값을 포함하는 것을 특징으로 하는 RFID 환경에서의 보안 시스템.

청구항 18

제 17 항에 있어서,

상기 태그의 식별자는

상기 데이터 베이스 서버의 공개키로 암호화된 것을 특징으로 하는 RFID 환경에서의 보안 시스템.

청구항 19

제 17 항에 있어서,

상기 리더 메타값 $Anonymous(R)$ 은 하기의 식 (4)에 의해 연산되는 것을 특징으로 하는 RFID 환경에서의 보안 시스템.

$$Anonymous(R) = E_{DB_{public}} \{ T, Privacy(R), SKey R \} \quad (4)$$

(상기 식 1에서 T 는 상기 태그의 식별자, $SKey R$ 는 상기 리더 R 의 세션키, $Privacy(R)$ 는 상기 리더 프라이버시 값, DB_{public} 는 상기 데이터 베이스 서버의 공개키, E 는 해쉬 기반 암호화 연산을 의미한다.)

명세서

발명의 상세한 설명

기술 분야

<1> 본 발명은 네트워크 통신에 관한 것으로서, 특히 RFID 환경에서 프로세스 알제브라 언어인 CSP를 이용하여 보안 프로토콜 행위를 명세한 CSP 코드를 정형적으로 검증할 수 있는 RFID 환경에서의 보안 방법, 이를 기록한 기록 매체 및 그 시스템에 관한 것이다.

배경 기술

<2> 최근 유비쿼터스 환경에서의 지능 기반 사회의 네트워킹은 장소나 시간에 제약없이 최상의 서비스를 받기 위한 편리성을 제공한다.

<3> 지능 기반 사회는 광대역 통합망(BeN), USN 및 IPv6의 3대 인프라를 기반으로 구축되며, 사물 간의 자율 통신이

이루어지는 유비쿼터스 네트워크 환경에서의 정보화 혜택이 주어지는 사회이다.

- <4> 이에 정보통신부는 IT839 전략을 통하여 8대 서비스의 도입과 이를 위한 3대 인프라 구축, 9대 신성장동력 산업의 선순환을 이루어 세계 최강의 IT 선진국으로서의 위상 강화와 유비쿼터스 사회의 조기 진입으로 국민 소득 2만불 시대를 앞당기고자 하고 있다.
- <5> 그 중에서, RFID 시스템은 태그와 리더기, 백엔드(back-end) 데이터베이스로 구성되는 무선 인식 시스템으로 2000년 이후 급격한 속도로 개발, 보급되고 있으며 향후 바코드 시스템을 대체할 것으로 예상되고 있다.
- <6> RFID 태그는 그 용도와 기능, 크기 등에 따라 매우 다양하지만, 가장 널리 사용될 것으로 예상되는 것은 저가 수동형 태그로 향후 바코드 시스템을 대체할 것으로 기대된다. 바코드의 경우 물품의 종류만을 기록하며 빛을 이용하여 인식하는 장치로 코드 체계만 표준화되어 있으면 매우 간단하게 구현 가능하며, 보안이나 프라이버시 문제는 고려될 필요가 없다. 한편, RFID 태그는 각 물품 고유의 코드를 가지게 되어 물품의 종류, 생산 이력 등이 저장되고 활용된다. 또한 인식 범위가 바코드 시스템보다 넓어 물류관리에 편리하게 활용되고 있다. 하지만 이러한 장점은 보안과 프라이버시 보호의 측면에서는 새로운 역기능을 유발한다. 개인이 보유한 물품의 정보가 리더기를 통하여 유출될 수 있으며, 태그의 정보를 복사하여 위조될 우려가 있다.
- <7> RFID 시스템에서 요구되는 정보보호 기능은 다음 두가지로 나누어 볼 수 있다.
- <8> 첫 번째는, 기밀성 및 인증 기능으로 적법한 리더와 태그에게만 정보를 전달하고, 도청자로부터 통신을 방해받지 않는 방법이다.
- <9> 두 번째는, 프라이버시 보호 기능으로 원하지 않는 태그 정보의 노출로 인한 개인 프라이버시 침해를 막는 방법이다.
- <10> 이와 함께, RFID 시스템에서의 보안 위협은 물리적 공격, 도청, 스푸핑, DoS 공격 등이 있다.
- <11> 물리적 공격은 태그를 다른 방법으로 획득하여 물리적인 방법으로 태그의 내용을 다른 태그에 복사하여 위장하는 공격이다.
- <12> 그리고, 도청은 RF를 이용하여 통신하므로, 정보가 암호화되지 않았을 경우, 통신내용이 인가되지 않은 사람에게 노출되는 것으로, 실제로 리더기로부터 전송되는 신호는 900MHz 급이며, 수동형 RFID 시스템의 경우 100M 이상의 거리에서도 신호 탐지가 가능하다.
- <13> 한편, 스푸핑은 통신상의 내용을 가로채어 변조하는 적극적인 공격 방법이며, DoS 공격은 강한 전파인 방해 전파를 발생시켜 정상적인 통신을 교란함으로써 서비스가 이루어지지 못하게 방해하는 방법이다. 이는 실질적으로 초기에 사용되어진 물리적 보안인 액티브 제밍(Active Jamming)과 유사하다.
- <14> 이와 같이, RFID를 위한 컴퓨팅 환경은 일반적인 인터넷 환경과는 달리 많은 제약사항을 가진다. 이러한 제약사항은 셀룰러 폰(Cellular Phone) 등을 이용한 무선 인터넷보다 더욱 자원 측면적 한계를 갖는다. 즉, 유비쿼터스를 위한 RFID 환경을 구축하기 위해서는 모든 상품이나 사람 등 객체에 설치되는 태그 가격은 5센트 이하로 구현되어야 하며, 대신에 리더 장비나 백 엔드(Back End) 시스템에서 많은 성능과 자원 측면에서 열악한 태그 장비의 자원적 한계를 극복할 수 있도록 설계 운영되어야 한다. 이에 보안 기술 적용에 대한 부분도 이러한 운영, 환경 측면을 충분히 고려하여야 한다.
- <15> 실질적으로, 보안 프로토콜을 구현하기 전에 설계 단계에서 사용자와 개발자에게 안전성과 신뢰성을 제공하기 위한 기술이 요구되고 있다. 예를 들면, 정당하지 않은 자가 RFID 리더를 이용하여 RFID 태그로부터 무단히 정보를 가져가는, 특히 프라이버시와 관계되는 정보를 불법적으로 가져가는 상황이 발생한다.
- <16> 그러나, 종래의 RFID 태그에서는 상당히 제한된 환경에서의 신뢰하고 안심할 만한 보안 방법 또는 보안 프로토콜이 사용자의 안전성과 신뢰성을 제공하기에는 인식 범위가 바코드 시스템보다 넓어 보안과 프라이버시 보호의 측면에서는 문제점이 있으며, 개인이 보유한 정보가 리더기를 통하여 유출될 수 있으며, 태그의 정보를 복사하여 위조될 우려가 있다는 문제점이 있다.

발명의 내용

해결 하고자하는 과제

- <17> 따라서, 본 발명이 해결하고자 하는 첫 번째 과제는 태그의 정보를 인증된 리더기에 의해 데이터베이스에 접근

할 수 있도록 하고, 태그의 정보에 대한 중간자 공격과 재생 공격을 방지하여 사용자의 안전성과 신뢰성을 제공할 수 있도록 프로세스 알제브라 언어인 CSP를 이용하여 보안프로토콜 행위를 명세한 CSP 코드를 정형적으로 검증할 수 있는 RFID 환경에서의 보안 방법을 제공하는 것이다.

<18> 그리고, 본 발명이 해결하고자 하는 두 번째 과제는 상기 RFID 환경에서의 보안 방법을 이용한 RFID 환경에서의 보안 방법을 제공하는 것이다.

<19> 또한, 본 발명이 해결하고자 하는 세 번째 과제는 상기 RFID 환경에서의 보안 방법을 컴퓨터에서 수행할 수 있는 프로그램을 기록한 기록매체를 제공하는 것이다.

과제 해결수단

<20> 상기 첫 번째 과제를 해결하기 위하여 본 발명은,

<21> RFID 리더 및 RFID 태그에서 데이터 베이스 서버 간의 세션키를 각각 생성하는 단계; 상기 태그가 상기 리더로부터 쿼리(query)를 수신하면, 상기 태그에서 자신의 식별자를 이용하여 태그 프라이버시 값을 생성하는 단계; 상기 태그에서 상기 태그 프라이버시 값을 포함하는 태그 파라미터를 이용하여 태그 메타값을 생성하는 단계; 상기 생성된 태그 메타값이 상기 리더로 전송되면, 상기 리더의 식별자를 이용하여 생성한 리더 프라이버시 값을 포함하는 리더 파라미터를 이용하여 리더 메타값을 생성하고, 상기 리더 메타값과 상기 태그 메타값을 상기 데이터베이스 서버로 전송하는 단계; 상기 데이터베이스 서버에서 상기 태그 메타값 및 상기 리더 메타값에 따라 배타적 논리합 연산을 수행하고, 상기 수행된 배타적 논리합 연산의 결과값을 상기 리더에 전송하는 단계; 및 상기 배타적 논리합 연산의 결과값으로부터 리더 자신의 세션키를 이용하여상기 태그의 세션키를 추출하고, 상기 추출된 태그의 세션키를 상기 태그에 전송하면 상기 태그에서 상기 리더의 인증을 수행하는 단계를 포함하는 RFID 환경에서의 보안 방법을 제공한다.

<22> 한편, 상기 태그 파라미터는 상기 리더의 식별자, 상기 데이터 베이스 서버의 공개키, 상기 태그의 세션키 및 상기 태그 프라이버시 값을 포함하는 것을 특징으로 한다.

<23> 그리고, 상기 리더의 식별자는 상기 데이터 베이스 서버의 공개키로 암호화된 것을 특징으로 한다.

<24> 아울러, 상기 태그 메타값 $Anonymous(T)$ 은, R 이 상기 리더의 식별자, $SKey T$ 는 상기 태그 T 의 세션키, $Privacy(T)$ 는 상기 태그 프라이버시 값, DB_{public} 는 상기 데이터 베이스 서버의 공개키, E 는 해쉬 기반 암호화 연산을 의미할 때,

$$Anonymous(T) = E_{DB_{public}} \{ R, Privacy(T), SKey T \}$$
 의 연산식에 의해 연산될 수 있다.

<25> 그리고, 상기 리더 파라미터는 상기 태그의 식별자, 상기 데이터 베이스 서버의 공개키, 상기 리더의 세션키 및 상기 리더 프라이버시 값을 포함하는 것을 특징으로 한다.

<26> 한편, 상기 태그의 식별자는 상기 데이터 베이스 서버의 공개키로 암호화된 것을 특징으로 한다.

<27> 그리고, 상기 리더 메타값 $Anonymous(R)$ 은, T 가 상기 태그의 식별자, $SKey R$ 는 상기 리더 R 의 세션키, $Privacy(R)$ 는 상기 리더 프라이버시 값, DB_{public} 는 상기 데이터 베이스 서버의 공개키, E 는 해쉬 기반 암호화 연산을 의미할 때,

$$Anonymous(R) = E_{DB_{public}} \{ T, Privacy(R), SKey R \}$$
 의 식에 의해 연산될 수 있다.

<28> 아울러, 상기 리더의 인증을 수행하는 단계는, 상기 리더에서 상기 추출된 태그의 세션키를 이용하여 상기 리더의 식별자를 암호화한 리더 암호화값을 태그에 전송하는 단계; 상기 태그에서 상기 암호화값으로부터 상기 태그의 세션키와 리더의 식별자를 연산하는 단계; 및 상기 연산된 태그의 세션키 및 리더의 식별자로부터 상기 리더

를 인증하는 단계를 포함할 수 있다.

<29> 또한, 상기 리더의 인증을 수행하는 단계는, 상기 태그에서 상기 인증된 리더에게 상기 쿼리에 대응되는 태그 정보를 전송하는 단계를 더 포함할 수 있다.

<30> 상기 두 번째 과제를 해결하기 위하여 본 발명은,

<31> 태그 정보를 요청하는 RFID 리더, 태그 정보를 제공하는 RFID 태그 및 데이터 베이스 서버를 포함하는 RFID 환경에서의 보안 시스템에 있어서, 상기 태그는 상기 데이터 베이스 서버 간의 세션키를 설정하는 태그 세션키 설정부; 상기 리더로부터 쿼리를 수신하여 태그 자신의 식별자를 이용하여 태그 프라이버시 값을 생성하는 태그 프라이버시 값 생성부; 상기 태그 프라이버시 값을 포함하는 태그 파라미터를 이용하여 태그 메타값을 생성하는 태그 메타값 생성부; 및 상기 리더의 인증을 수행하는 인증부를 포함하고, 상기 리더는 상기 데이터 베이스 서버 간의 세션키를 설정하는 리더 세션키 설정부; 상기 리더 자신의 식별자를 이용하여 리더 프라이버시 값을 생성하는 리더 프라이버시 값 생성부; 상기 리더 프라이버시 값 생성부에서 생성한 리더 프라이버시 값을 포함하는 리더 파라미터를 이용하여 리더 메타값을 생성하는 리더 메타값 생성부; 및 상기 데이터 베이스 서버로부터 전송되는 배타적 논리합 연산의 결과값으로부터 상기 태그의 세션키를 추출하는 세션키 추출부; 상기 데이터 베이스 서버는 상기 리더 송수신부로부터 수신한 상기 태그 메타값 및 상기 리더 메타값에 따라 배타적 논리합 연산을 수행하는 연산부를 포함할 수 있다.

<32> 또한, 상기 리더는 상기 태그에게 태그 정보를 요청하는 질의 생성부를 더 포함할 수 있다.

<33> 그리고, 상기 리더는 상기 태그 메타값을 수신하고, 상기 리더 메타값 생성부로부터 생성된 리더 메타값 및 상기 수신한 태그 메타값을 상기 데이터 베이스 서버로 전송하는 리더 송수신부를 포함하는 것을 특징으로 한다.

<34> 아울러, 상기 태그 파라미터는 상기 리더의 식별자, 상기 데이터 베이스 서버의 공개키, 상기 태그의 세션키 및 상기 태그 프라이버시 값을 포함하는 것을 특징으로 한다.

<35> 한편, 상기 리더의 식별자는 상기 데이터 베이스 서버의 공개키로 암호화된 것을 특징으로 한다.

<36> 여기서, 상기 태그 메타값 $Anonymous(T)$ 은, R 이 상기 리더의 식별자, $SKey T$ 는 상기 태그 T 의 세션키, $Privacy(T)$ 는 상기 태그 프라이버시 값, DB_{public} 는 상기 데이터 베이스 서버의 공개키, E 는 해쉬 기반 암호화 연산을 의미할 때, $Anonymous(T) = E_{DB_{public}} \{ R, Privacy(T), SKey T \}$ 에 의해 연산되는 것을 특징으로 한다.

<37> 아울러, 상기 리더 파라미터는 상기 태그의 식별자, 상기 데이터 베이스 서버의 공개키, 상기 리더의 세션키 및 상기 리더 프라이버시 값을 포함하는 것을 특징으로 한다.

<38> 그리고, 상기 태그의 식별자는 상기 데이터 베이스 서버의 공개키로 암호화된 것을 특징으로 한다.

<39> 그리고, 상기 리더 메타값 $Anonymous(R)$ 은, T 가 상기 태그의 식별자, $SKey R$ 는 상기 리더 R 의 세션키, $Privacy(R)$ 는 상기 리더 프라이버시 값, DB_{public} 는 상기 데이터 베이스 서버의 공개키, E 는 해쉬 기반 암호화 연산을 의미할 때, $Anonymous(R) = E_{DB_{public}} \{ T, Privacy(R), SKey R \}$ 에 의해 연산되는 것을 특징으로 한다.

효 과

<40> 본 발명에 의하면, 태그와 리더가 각각의 자신의 식별자를 프라이버시(Privacy)라는 통신참여자의 식별자를 입

력값으로 하여 익명의 값을 출력하는 함수를 이용하여 태그와 리더 자신의 프라이버시를 외부에 노출시키지 않을 수 있고, 태그에게 리더의 안전한 인증을 위해 사전에 리더와 태그가 데이터베이스와의 세션키를 각각 설정하고, 데이터베이스는 리더에게 배타적 논리합 연산을 수행한 결과값을 전송하여, 리더가 태그의 세션키 값을 도출하고, 도출한 태그의 세션키 값으로 리더 자신의 식별자를 암호화하는데 이용함으로써, 리더 자신의 정보를 보호하고, 태그로부터 인증을 받을 수 있으며, 상기 태그의 정보와 리더의 정보를 배타적 논리합 연산에 의해 암호화함으로써 암호화 과정에 수반되는 연산량이 적으므로 메모리의 가용성을 높일 수 있으며, 태그의 정보를 인증된 리더기에 의해 데이터베이스에 접근할 수 있도록 하고, 태그의 정보에 대한 중간자 공격과 재생 공격을 방지하여 사용자의 안전성과 신뢰성을 제공할 수 있는 효과가 있다.

발명의 실시를 위한 구체적인 내용

- <41> 도 1은 RFID 환경의 개략도를 도시한 것이다.
- <42> 도 1을 참조하면, RFID 환경은 태그 정보를 요청하는 RFID 리더(100), 자신의 태그 정보를 제공하는 RFID 태그(110) 및 RFID 태그(100)에 대한 정보를 미리 저장하고 있는 데이터베이스 서버(120)를 포함한다.
- <43> 이하, 상기 도 1에 도시된 RFID 리더(100), RFID 태그(110) 및 데이터베이스 서버(120)는 하기에 첨부도면과 함께 같이 상술될 것이다.
- <44> 도 2는 RFID 환경에서의 해시 기반의 보안 프로토콜의 해시-락 기법에 따른 보안 방법이 적용되는 신호 흐름을 도시한 것이다.
- <45> 여기서, 태그는 해시 메커니즘을 처리할 수 있는 H/W 기반의 암호화 모듈로써, 보안적 요구사항을 처리한다.
- <46> 태그에서는 메타 식별자(metaID) 정보만을 보관할 수 있는 저장 공간을 보유하고, 락(Lock)과 언락(Unlock) 처리 기능을 수행한다. 여기서, 언락(Unlock)된 태그 만이 태그-리더 장비와 운용 가능하다.
- <47> 하기의 표 1은 해시-락 기법에서의 각 변수를 정의한 것이다.

표 1

변수	정의
T	RF 태그의 식별자
R	RF 리더의 식별자
DB	백 엔드 데이터베이스의 식별자
XKey	통신참여자 X의 세션키(session key)
metaID	키를 해시값으로 처리한 값
ID	태그의 식별자
Xn	통신 참여자 X에 의해 생성된 난수값
H	해시 함수

- <48>
- <49> 상기 표 1을 기반으로 RFID 환경에서의 해시 기반의 보안 프로토콜에 따른 보안 방법이 적용되는 신호 흐름은 도 2와 같다. 여기서, RFID 리더(100), RFID 태그(110) 및 데이터베이스 서버(120)는 도 1에 도시된 바와 동일하다.
- <50> 우선, 리더(100)는 태그(110)로부터 정보를 얻기 위하여 쿼리(query)를 태그(110)에 전송한다(200 과정).
- <51> 태그(110)는 리더(100)에게 태그를 나타내는 metaID와 태그 난수값을 전송한다(210 과정).
- <52> 즉, 태그(110)는 리더(100)로부터 리더의 쿼리에 포함된 리더의 키값과 태그에서 생성된 난수를 입력으로 배타적 논리합 연산(XOR)을 수행하고, 그 배타적 논리합 연산을 수행한 값을 해시 처리한 결과값인 태그(110)를 나타내는 태그의 metaID와 상기 태그에서 생성된 난수값을 리더(100)에 전송한다.

- <53> 여기서, 리더의 키 값은 리더마다 미리 정의할 수 있고, 리더의 쿼리에 포함된 값을 이용할 수 있다.
- <54> 그 다음, 리더(100)는 태그(110)로부터 전송된 metaID와 태그의 난수값을 백엔드(back-end) 서버인 데이터 베이스 서버(120)에 포워딩한다(220 과정).
- <55> 데이터 베이스 서버(130)는 포워딩 받은 값인 태그의 난수값과 상기 metaID의 값을 비교하여 서로 대응되는 태그로부터의 것임이 확인되면, 상기 포워딩된 태그의 난수값과 metaID를 포함하는 데이터가 어느 태그로부터 전송된 것인지를 확인한다.
- <56> 그리고, 데이터 베이스 서버(230) 자신이 생성한 난수값과 상기 리더에 대응되는 키 값을 이용하여 배타적 논리합 연산을 수행하고, 상기 수행한 배타적 논리합 연산의 결과값과 함께 데이터 베이스 난수값을 리더(100)로 전송하게 된다(230 과정). 이 경우에 배타적 논리합 연산을 한 후에 해시 처리할 수 있다.
- <57> 그 다음, 리더(100)는 데이터 베이스 서버(120)로부터 전송된 배타적 논리합 연산의 결과값과 데이터 베이스 난수값을 태그(110)에게 포워딩한다(240 과정).
- <58> 마지막으로, 태그(110)는 데이터 베이스 서버(120)로부터 리더(100)를 통해 포워딩된 값인 배타적 논리합 연산의 결과값과 데이터 베이스 난수값으로부터 정상적인 데이터 베이스 서버(120)로부터의 데이터인지의 여부를 인증한 후, 리더(100)에게 자신의 태그 정보를 해쉬 처리하여 전송한다(250 과정).
- <59> 도 3은 RFID 환경에서의 해시 기반의 보안 프로토콜의 랜더마이즈 해시-락 기법에 따른 보안 방법이 적용되는 신호 흐름을 도시한 것이다.
- <60> 우선, 리더(100)는 태그(110)로부터 정보를 얻기 위하여 쿼리(query)를 태그(110)에 전송한다(300 과정).
- <61> 태그(110)는 자신의 태그 난수값을 생성하고, 태그 자신의 ID와 리더의 식별자 R을 붙인 $ID \parallel R$ 의 해시 값을 연산하고, 상기 연산된 해시 값과 리더의 식별자를 포함하는 메시지를 리더에게 전송한다(310 과정).
- <62> 이와 같이, 리더는 모든 알려진 태그 k에 대하여 $ID_k \parallel R$ 의 해시 처리 값을 전송받는다.
- <63> 그러면, 리더는 모든 알려진 태그의 ID값들을 데이터 베이스 서버에 요청하고(320 과정), 리더는 모든 알려진 태그의 ID값들을 데이터 베이스 서버로부터 수신한다(330 과정).
- <64> 상기 데이터 베이스 서버로부터 리더는 $ID_k \parallel R$ 의 해시 처리 값을 만족하는 태그의 ID를 찾으면, 태그에게 상기 ID인 ID_k 를 전송한다(340 과정).
- <65> 이를 기반으로, 태그(110)는 데이터 베이스 서버(120)로부터 리더(100)를 통해 포워딩된 값인 ID_k 와 태그의 ID가 일치하면 태그는 잠긴 상태에서 빠져나오게 된다.
- <66> 실질적으로, RFID 보안 설계 단계에서는 사용자와 개발자에게 안전성과 신뢰성을 제공하기 위한 보안 프로토콜 기술이 요구되고 있는데, 그러한 요구를 만족시키기 위하여 진행되는 노력 중 대표적으로 정형 기법이라는 연구가 있으며, 이는 정형 명세와 정형 검증의 두 가지 방법으로 분류된다.
- <67> 정형 명세는 개발하고자 하는 시스템의 동작 및 시스템이 만족해야 하는 특성을 정형적인 표현 방법을 이용하여 모델링하는 방법이고, 정형 검증은 정형적으로 명세된 시스템을 대상으로 그 시스템이 정확한지 혹은 그 시스템의 요구사항으로 주어지는 특성을 만족하는지를 논리적으로 증명하는 방법이다.
- <68> 그 중 정형 검증은 정리증명과 모델체킹 기법으로 분류되며, 전자는 보안 로직을 이용하여 특정한 논리식으로 시스템을 명세하고 정확한 논리 증명단계로써 정확성을 검증하는 방식이고, 후자는 프로토콜의 인증과정을 유한 상태 기계의 형식으로 모델링하고 그 모델이 만족해야 하는 요구사항이나 특성을 모델에서 만족되는지를 검증도구를 이용하여 자동으로 증명하는 방식으로 FDR과 같은 방법을 적용할 수 있다.
- <69> 이하에서는 정형 검증 도구 중에서 FDR이라는 모델체킹 도구를 이용하여 RFID 보안 프로토콜인 해쉬기반 프로토콜의 취약성을 분석하여 보안 프로토콜의 안정성을 향상시키고자 한다.
- <70> CSP는 프로세스 알제브라 언어로서, 병렬성을 가지는 통신 프로토콜의 동작을 효율적으로 명세하기 위한 언어이다. 최초 일반 통신 프로토콜 및 제어 시스템의 명세를 위해 사용됐으나, 점차 보안 프로토콜의 명세를 위한 영역으로 확대되어 가고 있다. CSP에서 제공하는 퓨어 싱크로나이제이션(pure synchronization)과 인터리빙 패러렐리즘(Interleaving parallelism)의 개념을 사용하여 분산 시스템 환경하에서 동작하는 클라이언트 서버와 공

격자 모델을 정형적으로 표현할 수 있는 장점을 가지고 있다. 예를 들어, 분산시스템 환경 하에서 동작하는 보안 시스템은 하기와 같이 간략히 표현될 수 있다.

SYSTEM = CLIENT1 || CLIENT2 || SERVER || INTRUDER

이렇게 CSP 언어를 이용하여 보안프로토콜 행위를 명세하고 FDR 정형검증 도구를 이용하여 보안속성을 검증하는 연구가 진행되었다. 그러나, CSP 언어를 이용한 정형명세과정은 정형적 설계 방법에 익숙하지 않은 보안프로토콜 설계자에게는 매우 복잡한 명세언어라는 단점을 가지고 있다.

이에 따라, 보안프로토콜의 행위를 간략히 명세할 수 있도록 Casper 도구가 개발되었다.

Casper 도구로 보안프로토콜의 행위와 검증속성을 명세하게 되며, 자동 변환 기능을 이용하여 CSP 명세코드를 생성할 수 있다.

결국, 자동 생성된 CSP 명세코드를 FDR 정형검증도구에 입력하여 보안프로토콜을 검증하게 된다.

그리고, FDR 도구는 CSP 명세언어를 입력으로 받아들이는 모델체크 도구로, 이는 CSP 명세 언어로 기술된 보안 프로토콜 모델이 보안성 및 인증속성과 같은 보안속성들을 만족하는지를 검증하게 되며, 만일 만족하지 않을 경우에는 CSP 이벤트로 기술된 반례를 보여주어 보안상 취약점 분석을 도와주게 된다.

여기서, FDR 도구는 가지의 검증 방법을 지원하고 있다.

첫 번째는 안전성(safety) 검증으로 Trace refinement 이고, 두 번째는 교착상태(deadlock) 검증으로 Failures refinement 이며, 세 번째는 라이브락(livelock) 검증으로 Failures-Divergence이다.

한편, Casper를 이용한 해시-엔락킹 프로토콜 명세는 하기의 표 2와 같다.

표 2

```
# Free variable
R, T : Agent
D B : Server
key : Sessionkey
Id : Text
H : HashFunction

InverseKeys = (key, key)

# Protocol description
0.      → T : R
1. T    → R : (H(key)) % metalD
2. R    → DB : metalD % (H(key))
3. DB   → R : key, Id
4. R    → T : key
5. T    → R : Id

#Intruder Information
Intruder = Mallory
IntruderKnowledge={      Tag,      Reader,
DataBase}
```

표 2를 참조하면, 자유변수 영역에서 R은 리더, T는 태그로서, 각각 에이전트(Agent)로 나타내고, DB는 백엔드 서버의 역할을 한다.

키(Key)sms 세션(session) 키, Id는 태그의 정보를 표현하고, InverseKeys는 세션 키에 대한 암호화 및 복호화를 표현하며, H는 해시 함수를 의미한다.

다음으로, 프로토콜 기술 영역은 해시-엔락킹 프로토콜을 명세한 부분으로, 여기서 % 표현은 메시지 1에서 태그

T가 H(key) 값을 metaID로서 수신자인 리더 R에게 복호화의 목적이 아닌 단지 다른 수신자인 데이터 베이스인 DB에게 전달하는 목적을 가지고 있다. 따라서, 메시지 2에서 이 메시지가 데이터베이스에게 전달되어 복호화된 다.

<84> 마지막으로 침입자 영역에 대한 정보가 제시되어 있다. 해시 연락킹 프로토콜에서는 metaID의 값을 중간자 공격 및 재생 공격에 이용함에 따라 태그 정보의 노출 및 추적이 가능하게 되었을 뿐만 아니라, 리더기와 태그의 인증에 실패하는 결과를 초래하였다.

<85> 이를 Casper 스크립트를 이용하여 명세하기 위해 해시-연락킹 프로토콜의 두 개체간 사용된 정보에 대한 비밀성과 개체간 상호 Id에 대한 인증을 만족하여야 하며, 이는 하기의 표 3과 같이 표현할 수 있다.

표 3

Secret (R, Key, [T])
Secret (R, Id, [T])
Agreement (T, R, [Id, key])

<86>

<87> 표 3에서 Secret (R, Key, [T]) 의 표현은 "리더 R은 키 정보를 오직 태그 T와만 알고 있다" 라고 풀이할 수 있고, 두 번째 표현은 "리더 R은 Id 정보를 오직 태그 T와만 알고 있다" 라고 풀이할 수 있다.

<88> 그리고, 세 번째 표현은 " 태그 T는 Id 및 key 정보를 통하여 리더 R로부터 자신의 개체를 인증받는다" 라고 풀이할 수 있다.

<89> 이를 모델 체커를 통하여 비밀성과 개체인증 속성의 만족여부를 확인한 결과 첫 번째 표현에서 리더 R이 전달하는 키에 대하여 태그 T와의 비밀성 속성을 만족하지 않았고, 이에 따라 결국 두 개체간의 데이터가 누설되었다.

<90> 또한 Id의 정보도 비밀성 속성을 만족하지 않았으며, 마지막 속성인 개체인증에서도 Id 및 key의 정보를 이용하여 두 개체간의 인증에 실패하였다.

<91> 위 비밀성 요구사항의 반례에 대하여 FDR의 인터프리트(interpret) 기능을 통하여 분석한 결과는 하기의 표 4와 같다.

표 4

0.	→ Tag : Reader
1. Tag	→ I_Reader : H(key)
2. I_Tag	→ DataBase : H(key)
1. I_Tag	→ Reader : H(key)
3. DataBase	→ I_Tag : key, Id
2. Reader	→ I_DataBase : H(key)
Reader believes Id is a secret shared with Tag	
The intruder knows Id	

<92>

<93> 표 4는 FDR을 이용한 반례의 분석 결과로, 태그 T가 리더 R에게 정상적인 데이터를 전송했다고 간주하였으나, 침입자인 I_Reader에 의해 H(key) 정보가 노출되었음을 알 수 있다.

<94> 결과적으로, 태그 T의 metaID 정보는 중간자 공격에 이용되었으며, 또 다른 공격 시나리오로서 리더인 R의 입장에서 태그 T로부터 정상적인 데이터를 전송받았다고 간주하였으나, 태그 침입자인 I_Tag나 데이터 베이스 침입자인 I_Database와 같은 악의적인 개입이 가능하였다.

<95> 이러한 해시-연락킹 프로토콜의 문제점으로 분석되었던 부분은 태그 내에 저장된 정보를 해시 기반 기법으로 태

강할 수 있게 함으로써 발생되었고, 이는 태그의 정보를 인증된 리더기에 의해 데이터베이스에 접근함으로써 태그 정보를 가져갈 수 있도록 함으로써 중간자 공격과 재생 공격을 방지할 수 있다.

<96> 이하, 본 발명의 바람직한 실시예를 첨부도면에 의거하여 상세히 설명하기로 한다.

<97> 한편, 다음에 예시하는 본 발명의 실시예는 여러 가지 다른 형태로 변형할 수 있으며, 본 발명의 범위가 다음에 상술하는 실시예에 한정되는 것은 아니다. 본 발명의 실시예는 당 업계에서 평균적인 지식을 가진 자에게 본 발명을 더욱 완전하게 설명하기 위하여 제공된다.

<98> 도 4는 본 발명에 따른 RFID 환경에서의 보안 시스템의 블록도를 도시한 것이다.

<99> 도 4를 참조하면, 본 발명에 따른 RFID 환경에서의 보안 시스템은 RFID 태그(이하, '태그'라 한다.)(400), RFID 리더(이하, '리더'라 한다.)(410) 및 데이터 베이스 서버(420)로 구성된다.

<100> 한편, 태그(400)는 태그 세션키 설정부(401), 태그 프라이버시 값 생성부(402), 태그 메타값 생성부(403) 및 인증부로 구성될 수 있다.

<101> 그리고, 리더(410)는 리더 세션키 설정부(411), 리더 프라이버시 값 생성부(412), 리더 메타값 생성부(413) 및 세션키 추출부(414)로 구성될 수 있다.

<102> 아울러, 리더(410)는 상기 태그(400)에게 태그 정보를 요청하는 질의 생성부(미도시)를 더 포함할 수 있다.

<103> 또한, 데이터 베이스 서버(420)는 연산부(425)를 포함한다.

<104> 우선, 태그 세션키 설정부(401)는 데이터 베이스 서버(420)와 태그(400)간의 세션키를 설정한다.

<105> 상기 세션키를 설정함으로써, 추후 설정된 세션키를 이용하여 데이터를 전송할 리더(410)의 인증을 수행하게 된다.

<106> 그리고, 태그 프라이버시 값 생성부(402)는 프라이버시(Privacy)라는 함수를 이용하여 익명의 값을 출력하게 되는데, 이는 태그 자신의 식별자를 입력값으로 하는 익명의 값을 출력하게 된다.

<107> 태그 메타값 생성부(403)는 태그 프라이버시 값 생성부(402)에서 생성된 태그 프라이버시 값을 포함하는 태그 파라미터를 이용하여 태그 메타값을 생성한다.

<108> 여기서, 태그 파라미터는 리더(410)의 식별자(R), 상기 데이터 베이스 서버의 공개키(DB_{Public}), 상기 태그(400)에서 데이터 베이스 서버(420)와 설정한 태그의 세션키($SKey T$) 및 태그 프라이버시 값 생성부(402)에서 생성된 태그 프라이버시 값($Privacy(T)$)을 포함하며, 이를 기반으로 태그(400)는 태그 자신의 고유한 암호화된 태그 메타값을 하기의 수학적 식 1에 의거하여 생성하게 된다.

<109> 한편, 상기 리더(410)의 식별자(R)은 자신의 정보를 암호화 하기 위하여 상기 데이터 베이스 서버의 공개키(DB_{Public})로 암호화된 식별자일 수 있으며, 이는 리더(410)가 태그(400)에게 질의 요청, 즉 쿼리 요청시의 쿼리 정보에 포함되어 태그(400)에 전송될 수 있다.

수학적 식 1

$$Anonymous(T) = E_{DB_{public}} \{ R, Privacy(T), SKey T \}$$

<110> 상기 수학적 식 1과 같이 상기 태그 메타값은 R 은 상기 리더의 식별자, $SKey T$ 는 상기 태그 T 의 세션키, $Privacy(T)$ 는 상기 태그 프라이버시 값, DB_{public} 는 상기 데이터 베이스 서버의 공개키, E 는 해쉬 기반 암호화 연산을 의미할 때, 상기 수학적 식 1의 태그 파라미터에 의해 연산될 수 있다.

<112> 그리고, 인증부(404)는 하기에 상술할 리더(410)의 세션키 추출부(414)에서 추출된 태그 세션키를 이용하여 리

더의 식별자를 암호화한 암호화 값을 수신하여, 리더(410)의 인증을 수행하고, 이를 기반으로 하여 인증된 리더(410)에게 태그 자신의 태그 정보를 전송한다.

- <113> 한편, 리더 세션키 설정부(411)는 데이터 베이스 서버(420)와 리더(410)간의 세션키를 설정한다.
- <114> 상기 세션키를 설정함으로써, 추후 설정된 세션키를 이용하여 하기에 상술할 상기 데이터 베이스 서버에서 전송된 배타적 논리합 연산의 결과값으로부터 태그(400)의 세션키를 추출할 수 있는 기반을 마련하게 된다.
- <115> 그리고, 리더 프라이버시 값 생성부(412)는 프라이버시(Privacy)라는 함수를 이용하여 익명의 값을 출력하게 되는데, 이는 리더 자신의 식별자를 입력값으로 하는 익명의 값을 출력하게 된다.
- <116> 즉, 프라이버시(Privacy)라는 함수는 통신 참여자의 식별자를 기반으로 익명의 값을 출력하는 암호화 함수이다.
- <117> 리더 메타값 생성부(413)는 리더 프라이버시 값 생성부(412)에서 생성된 리더 프라이버시 값을 포함하는 리더 파라미터를 이용하여 리더 메타값을 생성한다.
- <118> 여기서, 리더 파라미터는 태그(400)의 식별자(T), 상기 데이터 베이스 서버의 공개키(DB_{Public}), 상기 리더(410)에서 데이터 베이스 서버(420)와 설정한 리더의 세션키($SKey R$) 및 리더 프라이버시 값 생성부(412)에서 생성된 리더 프라이버시 값($Privacy(R)$)을 포함하며, 이를 기반으로 리더(410)는 리더 자신의 고유한 암호화된 리더 메타값을 하기의 수학식 2에 의거하여 생성하게 된다.
- <119> 한편, 상기 태그(400)의 식별자(T)은 자신의 정보를 암호화하기 위하여 상기 데이터 베이스 서버의 공개키(DB_{Public})로 암호화된 식별자일 수 있으며, 이는 태그(400)가 리더(410)에게 태그 메타값을 전송할 경우, 상기 태그 메타값 전송과 동시에 리더(410)에 전송될 수 있다.

수학식 2

$$Anonymous(R) = E_{DB_{public}} \{ T, Privacy(R), SKey R \}$$

- <120>
- <121> 상기 수학식 1과 같이 상기 리더 메타값 $Anonymous(R)$ 은 T 가 상기 태그의 식별자, $SKey R$ 는 상기 리더 R 의 세션키, $Privacy(R)$ 는 상기 리더 프라이버시 값, DB_{public} 는 상기 데이터 베이스 서버의 공개키, E 는 해쉬 기반 암호화 연산을 의미할 때, 상기 수학식 2의 리더 파라미터에 의해 연산될 수 있다.
- <122> 그리고, 세션키 추출부(414)는 상기 데이터 베이스 서버의 연산부(425)에서 상기 태그의 태그 메타값에 포함된 태그 프라이버시 값과 리더의 리더 메타값에 포함된 리더 프라이버시 값을 입력으로 하여 배타적 논리합 연산(XOR)을 수행한 배타적 논리합 연산의 결과값을 기반으로 태그의 세션키를 추출한다.
- <123> 이는, 리더(410)는 상기 데이터 베이스 서버의 공개키를 저장하고 있기 때문에 상기 데이터 베이스 서버의 연산부(425)에서 전송된 배타적 논리합 연산의 결과값을 입력값으로 하여 상기 태그의 세션키를 추출할 수 있다.
- <124> 그러면, 상기 리더의 세션키 추출부(414)에서 추출한 태그의 세션키 값으로 리더의 식별자 R 을 암호화하여 태그에게 전송한다.
- <125> 여기서, 상기 리더(410)는 상기 태그 메타값을 수신하고, 상기 리더 메타값 생성부(413)에서 생성된 리더 메타값 및 상기 수신한 태그 메타값을 상기 데이터베이스 서버(420)로 전송하는 리더 송수신부(미도시)를 포함할 수 있다.
- <126> 상기와 같은 과정을 거침으로써, 태그의 인증부(404)에서 상기 리더(410)의 세션키 추출부(414)에서 추출한 태그의 세션키 값으로 리더의 식별자 R 을 암호화한 값을 수신하고, 상기 태그는 자신의 태그의 세션키 값을 기반

으로 리더의 식별자 R 을 검출하여 리더를 인증한다.

- <127> 그러면, 태그는 인증된 리더(410)에게 태그 자신의 태그 정보를 전송할 수 있음으로써 보안이 확립된 RFID 환경에서 데이터 전송을 수행할 수 있어서, 공격자로부터 안전한 데이터 전송이 가능하다.
- <128> 도 5는 본 발명에 따른 RFID 환경에서의 보안 방법의 흐름도를 도시한 것이다.
- <129> 도 5를 참조하면, 우선, RFID 리더(이하, '리더'라 함) 및 RFID 태그(이하, '태그'라 함)에서 데이터 베이스 서버 간의 세션키를 각각 생성한다(510 과정).
- <130> 상기 태그와 리더는 데이터 베이스 서버 간의 세션키를 각각 생성함으로써, 태그는 태그 세션키를 이용하여 데이터를 전송할 리더의 인증을 수행할 수 있고, 리더는 데이터 베이스 서버에서 전송된 배타적 논리합 연산의 결과값으로부터 태그의 세션키를 추출할 수 있는 기반을 마련하게 된다.
- <131> 그 다음, 상기 태그가 상기 리더로부터 쿼리(query)를 수신하면, 상기 태그에서 자신의 식별자를 이용하여 태그 프라이버시 값을 생성한다(520 과정).
- <132> 이는, 프라이버시(Privacy)라는 함수를 이용하여 익명을 값을 생성하는 것으로, 상기 프라이버시 함수를 기반으로 태그 자신의 식별자를 입력값으로 하는 익명의 값을 출력하게 된다.
- <133> 그 다음, 상기 태그에서 상기 태그 프라이버시 값을 포함하는 태그 파라미터를 이용하여 태그 메타값을 생성한다(530 과정).
- <134> 여기서, 태그 파라미터는 리더의 식별자(R), 상기 데이터 베이스 서버의 공개키(DB_{Public}), 상기 태그에서 데이터 베이스 서버와 설정한 태그의 세션키($SKey T$) 및 상기 생성된 태그 프라이버시 값($Privacy(T)$)을 포함하며, 이를 기반으로 태그는 태그 자신의 고유한 암호화된 태그 메타값을 상기의 수학식 1에 의거하여 생성하게 된다.
- <135> 한편, 상기 리더의 식별자(R)은 자신의 정보를 암호화 하기 위하여 상기 데이터 베이스 서버의 공개키(DB_{Public})로 암호화된 식별자일 수 있으며, 이는 리더가 태그에게 질의 요청, 즉 쿼리 요청시의 쿼리 정보에 포함되어 태그에 전송될 수 있다.
- <136> 그 다음, 상기 생성된 태그 메타값이 상기 리더로 전송되면, 상기 리더의 식별자를 이용하여 생성한 리더 프라이버시 값을 포함하는 리더 파라미터를 이용하여 리더 메타값을 생성하고, 상기 리더 메타값과 상기 태그 메타값을 상기 데이터베이스 서버로 전송한다(540 과정).
- <137> 여기서, 리더 파라미터는 태그의 식별자(T), 상기 데이터 베이스 서버의 공개키(DB_{Public}), 상기 리더에서 데이터 베이스 서버와 설정한 리더의 세션키($SKey R$) 및 리더 프라이버시 값 생성부에서 생성된 리더 프라이버시 값($Privacy(R)$)을 포함하며, 이를 기반으로 리더는 리더 자신의 고유한 암호화된 리더 메타값을 상기의 수학식 2에 의거하여 생성하게 된다.
- <138> 한편, 상기 태그의 식별자(T)는 자신의 정보를 암호화하기 위하여 상기 데이터 베이스 서버의 공개키(DB_{Public})로 암호화된 식별자일 수 있으며, 이는 태그가 리더에게 태그 메타값을 전송할 경우, 상기 태그 메타값 전송과 동시에 리더에 전송될 수 있다.
- <139> 그 다음, 상기 데이터베이스 서버에서 상기 태그 메타값 및 상기 리더 메타값에 따라 배타적 논리합 연산을 수행하고, 상기 수행된 배타적 논리합 연산의 결과값을 상기 리더에 전송한다(550 과정).
- <140> 이는 상기 데이터 베이스 서버에서 상기 태그의 태그 메타값에 포함된 태그 프라이버시 값과 리더의 리더 메타

값에 포함된 리더 프라이버시 값을 입력으로 하여 배타적 논리합 연산(XOR)을 수행한 배타적 논리합 연산의 결과값을 리더에게 전송한다.

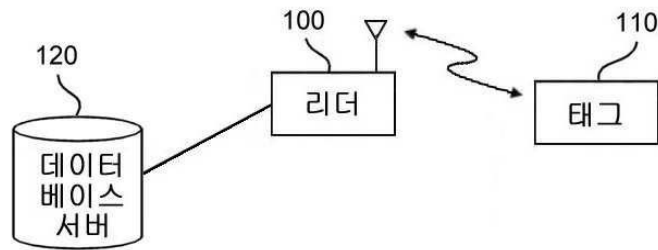
- <141> 마지막으로, 상기 배타적 논리합 연산의 결과값으로부터 리더 자신의 세션키를 이용하여 상기 태그의 세션키를 추출하고, 상기 추출된 태그의 세션키를 상기 태그에 전송하면 상기 태그에서 상기 리더의 인증을 수행한다(560 과정).
- <142> 여기서, 태그는 리더의 인증을 수행하기 위하여 상기 리더에서 상기 추출된 태그의 세션키를 이용하여 상기 리더의 식별자를 암호화한 리더 암호화값을 태그에 전송하고, 상기 태그에서 상기 암호화값으로부터 상기 태그의 세션키와 리더의 식별자를 추출해내고, 상기 추출된 태그의 세션키 및 리더의 식별자로부터 상기 리더를 인증한다.
- <143> 그러면, 상기 태그에서 상기 리더를 인증하였으므로, 상기 인증된 리더에게 상기 쿼리에 대응되는 태그 정보를 전송하게 된다.
- <144> 즉, 태그는 추출된 태그의 세션키값으로 리더의 식별자를 암호화한 값을 리더로부터 수신하고, 상기 태그는 자신의 세션키 값을 기반으로 리더의 식별자를 검출하여 리더를 인증한다.
- <145> 이와 같이, 태그는 인증된 리더에게 태그 자신의 태그 정보를 전송할 수 있음으로써 보안이 확립된 RFID 환경에서 데이터 전송을 수행할 수 있어서 공격자로부터 안전한 데이터 전송을 수행할 수 있다.
- <146> 상술한 바와 같이, 본 발명은 태그와 리더가 각각의 자신의 식별자를 프라이버시(Privacy)라는 통신참여자의 식별자를 입력값으로 하여 익명의 값을 출력하는 함수를 이용하여 태그와 리더 자신의 프라이버시를 외부에 노출시키지 않을 수 있다.
- <147> 또한 본 발명은, 태그에게 리더의 안전한 인증을 위해 사전에 리더와 태그가 데이터베이스와의 세션키를 각각 설정하고, 데이터베이스는 리더에게 배타적 논리합 연산을 수행한 결과값을 전송하여, 리더가 태그의 세션키 값을 도출하고, 도출한 태그의 세션키 값으로 리더 자신의 식별자를 암호화하는데 이용함으로써, 리더 자신의 정보를 보호하고, 태그로부터 인증을 받을 수 있도록 한다.
- <148> 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.
- <149> 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다. 컴퓨터가 읽을 수 있는 기록 장치의 예로는 ROM, RAM, CD-ROM, DVD±ROM, DVD-RAM, 자기 테이프, 플로피 디스크, 하드 디스크(hard disk), 광데이터 저장장치 등이 있다. 또한, 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 장치에 분산되어 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.
- <150> 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.

도면의 간단한 설명

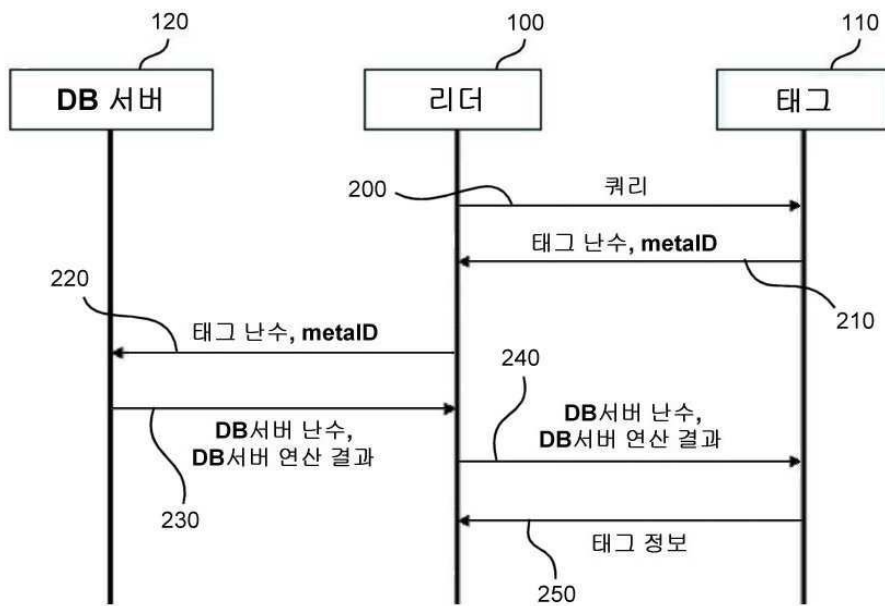
- <151> 도 1은 RFID 환경의 개략도를 도시한 것이다.
- <152> 도 2는 RFID 환경에서의 해시 기반의 보안 프로토콜의 해시-락 기법에 따른 보안 방법이 적용되는 신호 흐름을 도시한 것이다.
- <153> 도 3은 RFID 환경에서의 해시 기반의 보안 프로토콜의 랜더마이즈 해시-락 기법에 따른 보안 방법이 적용되는 신호 흐름을 도시한 것이다.
- <154> 도 4는 본 발명에 따른 RFID 환경에서의 보안 시스템의 블록도를 도시한 것이다.
- <155> 도 5는 본 발명에 따른 RFID 환경에서의 보안 방법의 흐름도를 도시한 것이다.

도면

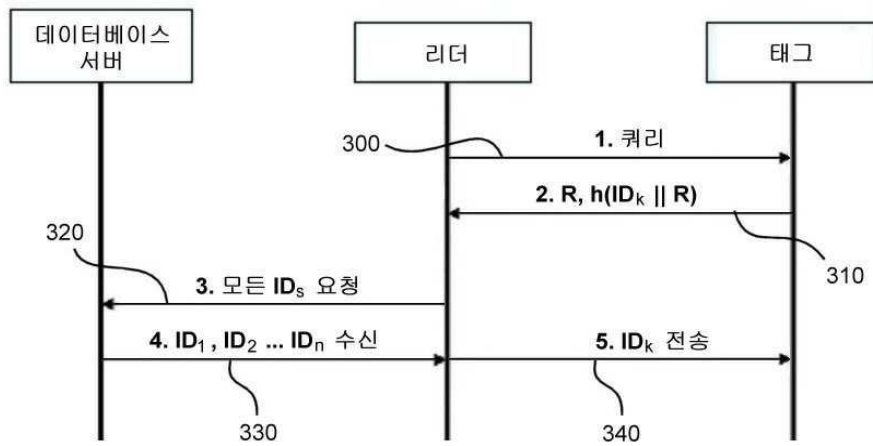
도면1



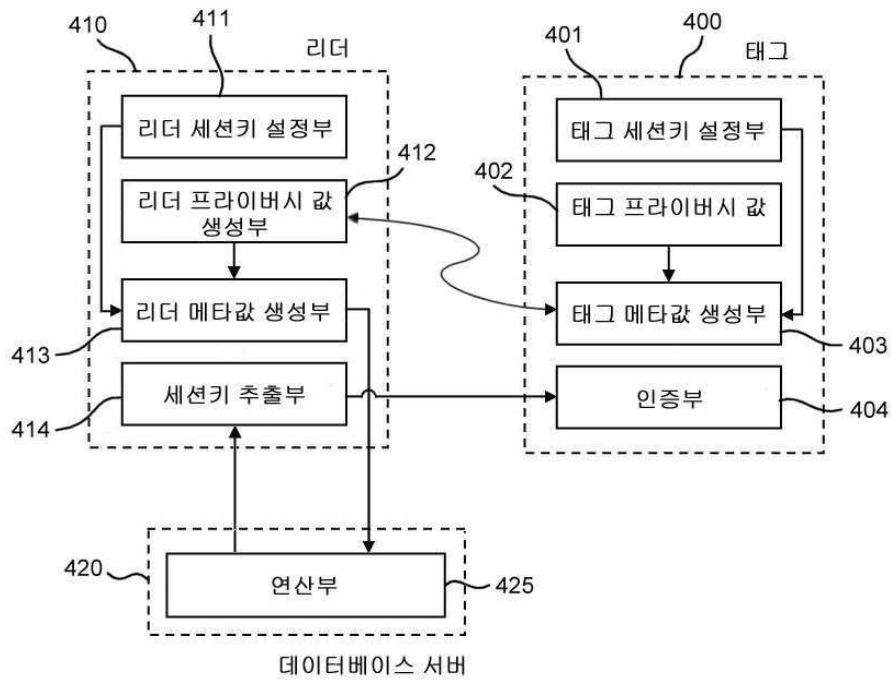
도면2



도면3



도면4



도면5

