



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2012-0022003
(43) 공개일자 2012년03월09일

(51) 국제특허분류(Int. Cl.)
G06K 17/00 (2006.01) H04B 5/02 (2006.01)
(21) 출원번호 10-2010-0082451
(22) 출원일자 2010년08월25일
심사청구일자 2010년08월25일

(71) 출원인
충남대학교산학협력단
대전광역시 유성구 대학로 99 (궁동, 충남대학교)
(72) 발명자
염홍열
충청남도 아산시 신창면 읍내리 순천향대학교
M114
류재철
대전광역시 유성구 어은로 57, 132동 801호 (어은
동, 한빛아파트)
(뒷면에 계속)
(74) 대리인
특허법인정직파특허

전체 청구항 수 : 총 16 항

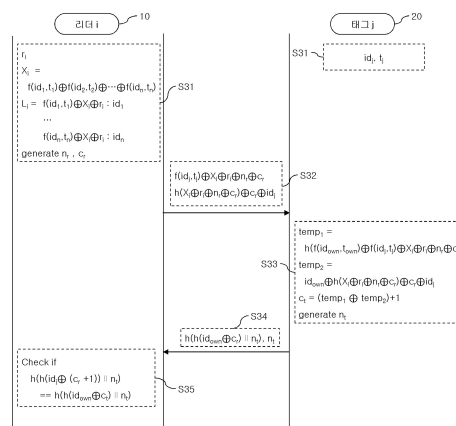
(54) 발명의 명칭 안전하고 효율적인 RFID 태그 검색방법 및 RFID 리더 장치

(57) 요약

리더가 다수의 태그 중에서 특정 태그를 검색하되, XOR 체인 기반 인증 기법을 적용하여 XOR연산 및 해쉬연산만으로 검색할 태그를 인증하는 RFID 태그 검색방법 및 RFID 리더 장치에 있어서, (a) 리더는 모든 태그의 암호키를 모두 XOR연산한 값(이하 총 인증정보)과 총 인증정보에 각 태그의 암호키를 XOR연산한 값(이하 개별 인증정보)을 저장하는 단계; (b) 리더는 검색하고자 하는 태그(이하 검색 태그)의 개별 인증정보를 제1 인증값으로 생성하고, 총 인증정보에 제1 카운터를 XOR연산하여 제2 인증값을 생성하고, 제1 및 제2 인증값을 태그로 전송하는 단계; (c) 태그는 자신의 암호키와 제1 인증값을 XOR연산하여 제1 결과를 생성하고, 제2 인증값으로 제2 결과를 생성하고, 제1 및 제2 결과를 XOR 연산하여 제2 카운터를 생성하는 단계; 및, (d) 리더는 제2 카운터를 수신하여 제1 카운터와 대비하여 검색 태그를 인증하는 단계를 포함하는 구성을 마련한다.

상기와 같은 방법 및 장치에 의하여, XOR 체인 기반 인증 기법을 적용하여 XOR연산 및 해쉬연산만을 이용하여 인증함으로써, 기밀성, 추적 불가능성, 및 메시지 재생공격을 방지하면서도 연산량을 적게 할 수 있다.

대표도 - 도6



(72) 발명자

여돈구

충청남도 아산시 신창면 읍내리 순천향대학교 M114

최현우

충청남도 아산시 신창면 읍내리 순천향대학교 M114

장재훈

충청남도 아산시 신창면 읍내리 순천향대학교 M114

이동희

충청남도 아산시 신창면 읍내리 순천향대학교 M114

이상래

충청남도 아산시 신창면 읍내리 순천향대학교 M114

정영곤

충청남도 아산시 신창면 읍내리 순천향대학교 M114

특허청구의 범위

청구항 1

리더가 다수의 태그 중에서 특정 태그를 검색하는 RFID 태그 검색방법에 있어서,

(a) 상기 리더는 태그의 암호키를 모두 XOR연산한 값(이하 총 인증정보)과 상기 총 인증정보에 각 태그의 암호키를 XOR연산한 값(이하 개별 인증정보)을 저장하는 단계;

(b) 상기 리더는 검색하고자 하는 태그(이하 검색 태그)의 개별 인증정보를 제1 인증값으로 생성하고, 상기 총 인증정보에 제1 카운터를 XOR연산하여 제2 인증값을 생성하고, 상기 제1 및 제2 인증값을 태그로 전송하는 단계;

(c) 상기 태그는 자신의 암호키와 제1 인증값을 XOR연산하여 제1 결과를 생성하고, 상기 제2 인증값으로 제2 결과를 생성하고, 상기 제1 및 제2 결과를 XOR 연산하여 제2 카운터를 생성하는 단계; 및,

(d) 상기 리더는 상기 제2 카운터를 수신하여 상기 제1 카운터와 대비하여 상기 검색 태그를 인증하는 단계를 포함하는 것을 특징으로 하는 RFID 태그 검색방법.

청구항 2

제1항에 있어서,

상기 태그의 암호키는 태그의 식별값 및 비밀값을 해쉬하여 생성되는 것을 특징으로 하는 RFID 태그 검색방법.

청구항 3

제1항에 있어서,

상기 (b)단계에서, 상기 제2 인증값은 상기 총 인증정보를 해쉬한 후 제1 카운터와 XOR연산되고,

상기 (c)단계에서, 상기 제1 결과는 XOR연산후 해쉬되어 생성되는 것을 특징으로 하는 RFID 태그 검색방법.

청구항 4

제1항에 있어서,

상기 (a)단계에서, 상기 개별 인증정보는 상기 리더의 식별정보를 추가하여 XOR연산하여 생성되고,

상기 (b)단계에서, 상기 총 인증정보에 상기 리더의 식별정보를 추가하여 XOR 연산되는 것을 특징으로 하는 RFID 태그 검색방법.

청구항 5

제1항에 있어서,

상기 (b)단계에서, 상기 제2 인증값은 상기 총 인증정보와 제1 카운터에 상기 검색 태그의 식별정보를 추가하여 XOR 연산하여 생성되고,

상기 (c)단계에서, 상기 태그는 상기 제2 인증값에 자신의 식별정보를 XOR 연산하여 상기 제2 결과를 생성하는 것을 특징으로 하는 RFID 태그 검색방법.

청구항 6

제1항에 있어서,

상기 인증값은 인증정보에 리더의 랜덤값 또는 제1 카운터 중 어느 하나 이상을 추가하여 XOR 연산하여 생성되는 것을 특징으로 하는 RFID 태그 검색방법.

청구항 7

제1항에 있어서,

상기 (c)단계에서, 상기 제2 카운터는 상기 제1 및 제2 결과를 XOR 연산한 값을 하나 증가시켜 구해지는 것을 특징으로 하는 RFID 태그 검색방법.

청구항 8

제1항에 있어서,

상기 제2 카운터는 암호화되어 전송되는 것을 특징으로 하는 RFID 태그 검색방법.

청구항 9

제8항에 있어서,

상기 제2 카운터는 태그의 식별정보 또는 랜덤값 중 어느 하나 또는 모두를 이용하여 암호화되는 것을 특징으로 하는 RFID 태그 검색방법.

청구항 10

제1항 내지 제9항 중 어느 한 항의 방법을 수행하는 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

청구항 11

다수의 태그 중에서 특정 태그를 검색하는 RFID 리더 장치에 있어서,

모든 태그의 암호키를 모두 XOR연산한 값(이하 총 인증정보)과 상기 제1 인증값에 각 태그의 암호키를 XOR연산한 값(이하 개별 인증정보)을 저장하는 메모리; 및,

검색하고자 하는 태그(이하 검색 태그)의 개별 인증정보를 제1 인증값으로 생성하고, 상기 총 인증정보에 제1 카운터와 XOR연산하여 제2 인증값을 생성하고, 상기 제1 및 제2 인증값을 태그로 전송하고, 태그로부터 수신한 제2 카운터를 제1 카운터와 대비하여 상기 검색 태그를 인증하는 제어부를 포함하고,

상기 제2 카운터는 상기 태그에 의하여, 태그의 암호키와 제1 인증값을 XOR연산하여 생성된 제1 결과 및, 상기 제2 인증값으로 생성된 제2 결과의 XOR 연산 결과인 것을 특징으로 하는 RFID 리더 장치.

청구항 12

제11항에 있어서,

상기 태그의 암호키는 태그의 식별값 및 비밀값을 해쉬하여 생성되는 것을 특징으로 하는 RFID 리더 장치.

청구항 13

제11항에 있어서,

상기 제2 인증값은 상기 총 인증정보를 해쉬한 후 제1 카운터와 XOR연산되고, 상기 제1 결과는 XOR연산후 해쉬되어 생성되는 것을 특징으로 하는 RFID 리더 장치.

청구항 14

제11항에 있어서,

상기 개별 인증정보는 상기 리더의 식별정보를 추가하여 XOR연산하여 생성되고, 상기 총 인증정보에 상기 리더의 식별정보를 추가하여 XOR 연산되는 것을 특징으로 하는 RFID 리더 장치.

청구항 15

제11항에 있어서,

상기 제2 인증값은 상기 총 인증정보와 제1 카운터에 상기 검색 태그의 식별정보를 추가하여 XOR 연산하여 생성되고, 상기 태그는 상기 제2 인증값에 자신의 식별정보를 XOR 연산하여 상기 제2 결과를 생성하는 것을 특징으로 하는 RFID 리더 장치.

청구항 16

제11항에 있어서,

상기 인증값은 인증정보에 리더의 랜덤값 또는 제1 카운터 중 어느 하나 이상을 추가하여 XOR 연산하여 생성되는 것을 특징으로 하는 RFID 리더 장치.

명세서

기술분야

- [0001] 본 발명은 리더가 다수의 태그 중에서 특정 태그를 검색하는 RFID 태그 검색방법 및 RFID 리더 장치에 관한 것이다.
- [0002] 특히, 본 발명은 XOR 체인 기반 인증 기법을 적용하여 XOR연산 및 해쉬연산만을 이용하여 리더 및 태그가 상호 인증할 수 있는 RFID 태그 검색방법 및 RFID 리더 장치에 관한 것이다.

배경기술

- [0003] RFID(Radio Frequency IDentification) 시스템은 과거 단순히 태그(Tag)가 부착된 물체를 식별하는 기술에 그치지 않고, 실시간으로 물류의 운송을 추적하는 등 다양한 분야에서 사용되고 있다. 특히, 특정한 RFID 태그들의 그룹 내에서 사용자가 찾고자 하는 태그가 있는지 확인 할 수 있게 해주는 RFID 태그 검색 시스템(RFID Tag Search System)이 최근에 RFID 응용분야로써 각광받고 있으며, 이에 대한 연구 또한 활발히 이루어지고 있다.
- [0004] RFID 태그 검색 시스템은 다양한 분야에서 활용될 수 있다. 예를 들어, 도서관에서 책을 찾는하거나 창고에서 특정 재고의 존재 유무를 확인해야 하는 등의 작업에 매우 유용하게 이용될 수 있다. 또한 사회적으로 이슈가 되고 있는 범죄자의 전자발찌에 적용되어 특정 구역을 벗어나는 범죄자를 확인할 수도 있으며, 놀이공원 등 사람이 많은 곳에서 미아를 찾기 위한 방안으로도 적극 활용될 수 있다.
- [0005] RFID 태그 검색 시스템의 구현을 위해서는 안전한 프로토콜의 설계가 요구된다. 이는 이동형 RFID 리더가 중앙서버의 도움 없이 특정 태그를 찾기 위한 연산을 수행하면서 리더 소지자의 프라이버시가 노출될 수 있는 위험이 있기 때문이다. RFID 태그 검색 시스템은 고정식의 리더가 아니라 휴대용의 리더를 사용하므로, 리더 소지자

는 서버로부터 접근 가능한 태그들의 정보를 내려 받아 리더에 저장하고, 휴대용의 리더를 들고 이동하면서 특정 태그를 검색하게 된다. 이때 리더 소지자의 프라이버시가 보장되지 않는다면, 특정 리더 소지자가 찾고자 하는 태그의 정보나 리더 소지자의 위치 등이 공격자에게 노출되어 리더 소지자의 프라이버시가 침해당할 수 있다. 마찬가지로 태그의 위치가 보호되지 않는다면 공격자는 실시간으로 리더가 찾고자 하는 태그의 위치를 추적할 수 있게 된다.

[0006] 또한, 고려되어야 할 다른 한 가지 사항은 RFID 리더 및 태그의 연산량을 최소화해야 한다는 것이다. 이는 RFID 검색 프로토콜의 성능과 직결되는 문제이며, 대량의 RFID 태그들을 상대로 하여도 안정적인 프로토콜의 동작을 보장하기 위함이다.

[0007] RFID 태그 검색 프로토콜은 리더(R_i)가 찾길 원하는 특정 태그(T_j)의 id_j 를 태그들의 그룹(T^*)으로 브로드캐스트 하면, 해당하는 id_j 의 태그가 응답함으로써 수행될 수 있다. 하지만, 이와 같이 단순한 프로토콜은 어떠한 보안성도 제공하지 않는다. 공격자는 단순히 리더와 태그사이의 통신을 도청함으로써 정당한 리더 및 태그로 위장할 수 있게 되는 등 다양한 보안 문제점을 발생시킨다. 그렇기 때문에 RFID 태그 검색 프로토콜을 위해서는 태그가 정당한 리더의 요청인지를 인증할 수 있어야 하고, 리더 또한 정당한 태그의 응답인지를 확인할 수 있어야 한다.

[0008] 따라서 RFID 태그 검색 프로토콜은 RFID 인증 프로토콜을 확장한 개념이라고 볼 수 있다. 그 이유는 태그 그룹에 속해 있는 모든 태그들에 대하여 각각 인증 프로토콜을 반복적으로 수행함으로써, 인증에 성공한 태그를 사용자가 찾고자 하는 태그로 간주할 수 있기 때문이다. 하지만 인증을 통한 태그 검색은 태그의 수가 늘어날수록 리더 및 태그에 미치는 연산량이 급격히 증가하므로 효율적이지 못하다.

[0009] C.C. Tan 등은 RFID 태그 검색 방법(이하 종래기술 1)을 처음으로 제안했다. 리더 소지자가 휴대용 리더를 이용하여 중앙 서버의 도움 없이 특정 태그를 검색할 수 있도록 하기 위해서, 검색 권한을 갖는 태그의 목록(Access List)을 중앙 서버(신뢰기관)로부터 휴대용 리더에 내려 받아 저장하게 했다.

[0010] 태그는 자신의 식별값 id_j 와 신뢰기관과 공유하는 비밀값 t_j 를 가지고, 리더는 자신의 식별값 r_i 와, 태그들에 대한 접근권한 리스트 L_i 를 가진다. 이때 리스트 L_i 는 $L_i = \{ f(r_i, t_j) \}$ (f 는 두 파라미터를 연결하여 해쉬하는 해쉬함수)로서, 각 태그들의 비밀값을 해쉬한 값들의 리스트이다. 신뢰기관에 의해 리더는 태그의 비밀값 t_j 와 리더의 식별자 r_i 를 해쉬한 해쉬값만을 접근리스트로써 저장하기 때문에, 특정 태그에 대한 검색을 수행할 수 있고 리더 측에 태그의 비밀값을 저장할 필요가 없어 보안성을 향상시킬 수 있다.

[0011] 도 1a에서 보는 바와 같이, 상기 종래기술 1은 리더가 난수 n_r 를 이용하여 매번 다른 값으로 태그 검색을 요청하지만, 공격자는 요청 메시지 도청하여 재생공격을 시도함으로써 리더가 찾고자 하는 태그로부터 정상적인 응답을 받을 수 있다.

[0012] 도 1b와 같이, 종래기술 2에서는, 이 문제를 개선하고자, 태그는 이전에 요청된 리더의 랜덤값(n_r)인 old_n 을 저장하게 하였다. 따라서 태그 자신의 id 와 계산 해낸 id_j 가 같더라도 현재 랜덤값 n_r 이 바로 전의 요청메시지에 포함된 랜덤값 old_n 과 같다면 응답을 하지 않는다. 이로 인해 바로 이전의 요청메시지를 이용하는 공격자의 재생공격을 막을 수 있게 된다. 하지만, old_n 이전의 요청메시지로 재생공격을 시도하는 공격자는 막을 수가 없기 때문에 재생공격의 근본적인 해결책이 될 수 없다.

[0013] 앞서 설명한 종래기술 1과 2는 리더가 찾는 태그만이 리더가 정당한지를 검증한 후 응답 메시지를 발생시킨다. 따라서 리더가 특정 태그 그룹에서 찾고자 하는 태그가 존재하는 경우에는 1개의 응답 메시지만이 존재하게 된다. 이것은 공격자가 응답 메시지의 내용을 모르더라도, 응답 메시지의 존재만으로도 리더가 찾고자 하는 태그의 존재 유무를 알 수 있기 때문에, 주기적으로 요청메시지를 태그의 그룹에 전송하여 찾고자 하는 태그의 위치를 추적할 수 있게 된다.

[0014] 도 1c와 도 1d는 id_j 가 같은 태그뿐만 아니라, id_j 가 같지 않더라도 응답 메시지를 발생시킬 수 있도록 하는 종래기술 3과 4의 방법을 도시한 것이다.

[0015] 도 1c와 같이, 종래기술 3에서는, 리더는 찾고자 하는 태그(id_j)의 처음 m 비트만($[id_j]_m$)을 태그의 그룹으로 브

로드캐스트 한다. 리더의 요청메시지를 수신한 태그들은 $[id_j]_m$ 이 자신 id_j 의 처음 m 비트와 같다면 응답메시지를 계산하여 리더로 전송한다. 따라서 리더와 태그 그룹 사이에는 랜덤한 수의 응답이 존재하기 때문에 공격자는 리더가 찾고자 하는 태그의 존재 유무를 알 수가 없게 된다. 하지만 도 1c의 프로토콜 안전성은 특정 태그 그룹에 포함되는 태그의 수에 비례함을 알 수 있다. 즉, 태그 그룹에 포함된 태그의 수가 적을 때에는 처음 m 비트를 가지는 태그가 1개만 존재할 가능성이 있기 때문에 공격자는 태그의 존재유무를 파악할 수 있게 된다.

[0016] 도 1d와 같이, 종래기술 4에서는, λ 는 리더가 찾고 있는 id_j 와 태그의 id 가 일치 하지 않더라도 태그가 응답메시지를 발생할 확률을 의미한다. 따라서 검색 프로토콜이 동작하는 리더와 태그 간에는 랜덤한 수의 응답 메시지가 존재하게 되며, 태그 추적 등과 같은 공격을 막을 수 있게 된다. 하지만, 종래기술 2와 마찬가지로 태그의 수가 적을 경우에는 안전하지 않다.

[0017] 지금까지 분석한 내용을 토대로 C.C. Tan 등이 제안한 4개의 RFID 태그 검색 방법, 즉, 종래기술 1 내지 4는 재생공격 및 태그 추적 공격에 안전하지 않다는 것을 알 수 있다. 게다가 4개의 프로토콜 모두는 리더 소지자의 프라이버시 침해를 발생시킬 수 있는 문제점이 존재한다. 리더가 태그를 검색하기 위해 보내는 요청메시지에는 리더의 고정된 식별자 값인 r_i 가 평균으로 노출되어 있기 때문에, 만일 공격자가 도청을 통하여 이동하는 리더의 식별자를 계속해서 확인할 수 있다면, 리더 소지자의 위치를 추적할 수 있게 된다.

[0018] 따라서 천지영 등은 r_i 값의 평균 노출을 막고자 AES(Advanced Encryption Standard) 암호 알고리즘을 사용해 리더와 태그 구간을 암호화 하는 RFID 태그 검색 방법(이하 종래기술 5)을 새롭게 제안했다. 즉, 수동형 태그에 적합한 암호 알고리즘을 구현하여 AES-128 암호 알고리즘을 태그 검색 프로토콜에 적용 했다.

[0019] 초기 설정 단계에서 신뢰기관으로부터 검색 가능한 태그의 접근 리스트 L_i 를 내려 받아 저장하고 있다. 각각의 리더 R_i 의 식별자를 r_i 라 하고, 태그 T_j 의 식별자를 ID_j , 비밀값을 t_j 라고 한다. 접근 리스트 L_i 는 $L_i = \{ E_{t_j}(r_i ? ID_j) \}$ 로 구성된다. 이때 $E_{t_j}(r_i ? ID_j)$ 은 각 64비트의 r_i 와 ID_j 를 연결한 $r_i ? ID_j$ 를 128비트 길이의 비밀값 t_j 를 이용하여 AES 암호 알고리즘으로 암호화한 암호문을 나타낸다.

[0020] 도 1e에서 보는 바와 같이, 종래기술 5는, 리더 R_i 가 태그 T_j 를 검색하기 위해, 자신의 식별자 r_i 와 64비트 난수 R 을 평균으로 하고 찾고자하는 T_j 의 식별자인 ID_j 를 비밀값으로 하는 암호문 $E_{ID_j}(r_i ? R)$ 을 태그 그룹으로 브로드캐스트 한다. (2)단계에서, 브로드캐스트 메시지를 수신한 태그들은 자신의 ID_j 를 이용하여 $E_{ID_j}(r_i ? R)$ 를 복호화 한 후, r_i 과 R 을 각각 64비트씩 분리해 낸다. 동시에 r_i 과 ID_j 를 입력으로 하고, t_j 를 비밀값으로 하는 암호문 $K_i = E_{t_j}(r_i ? ID_j)$ 를 생성해 낸다. (3) 단계에서, 각각의 태그들은 난수 r 을 선택하여 응답 메시지 $E_{K_i}(ID_j ? r)(R ? R)$ 를 생성하여 리더에게 전송한다. 일반적인 XOR 연산의 수학기호 방법인 $\oplus$ 가 전자문서에 표시되지 않으므로, 이 연산표기 대신 $?$ 로 사용한다.

[0021] 리더는 태그들로부터 수신한 $E_{K_i}(ID_j ? r)(R ? R)$ 를 자신이 선택했던 난수 $R ? R$ 과 XOR 연산을 수행하고, 생성된 결과값인 암호문 $E_{K_i}(ID_j ? r)$ 에 대해서 접근 리스트의 $E_{t_j}(r_i ? ID_j)$ 를 키로 취하여 암호문을 복호화 한다. 복호화 후 추출된 ID_j 값이 자신이 찾고자 했던 태그의 식별자와 같다면 리더는 특정 태그 그룹에 찾길 원하는 태그가 존재한다는 것을 알 수 있다.

[0022] 이와 같이 종래기술 5는 암호화 알고리즘을 이용해 어떠한 평문도 리더와 태그사이에 노출시키지 않음으로써, 리더 소지자의 프라이버시 침해 문제를 해결하였다. 마찬가지로 리더의 요청메시지에 대해 모든 태그가 응답메시지를 발생시키기 때문에 태그의 추적 문제 또한 해결하였다.

[0023] 하지만 찾고자 하는 태그 그룹에 많은 태그가 존재한다면, 각각의 태그가 발생시키는 모든 응답 메시지에 대해 암호복호화 과정을 거쳐 메시지를 검증해야 하므로, 리더가 가지는 부하는 브로드캐스트 그룹 내의 태그 수에 비례한다고 볼 수 있다.

[0024] 결론적으로, 앞서 본 바와 같은 종래기술의 RFID 태그 검색 방법들은 리더의 프라이버시 문제를 대부분 해결하지 못했고, 해결했다 하더라도 암호화 알고리즘을 사용하였기 때문에 대량의 태그를 상대로 했을 때는 연산량 측면에서 많은 오버헤드를 갖게 했다. 따라서 리더 소지자 및 태그의 다양한 보안 요구사항을 만족시키면서, 리

더 소지지자의 프라이버시 문제를 해결하면서도 효율적으로 동작하는 RFID 태그 검색 기술이 필요하다.

발명의 내용

해결하려는 과제

- [0025] 본 발명의 목적은 상술한 바와 같은 문제점을 해결하기 위한 것으로, XOR 체인 기반 인증 기법을 적용하여 XOR 연산 및 해쉬연산만을 이용하여 인증할 수 있는 RFID 태그 검색방법 및 RFID 리더 장치를 제공하는 것이다.
- [0026] 또한, 본 발명의 목적은 태그의 암호키를 모두 XOR연산한 총 인증정보와 이 정보에 각 태그의 암호키를 XOR연산한 개별 인증정보를 이용하여 카운터를 암호화 하여 태그에 전송하고, 태그가 해독하여 응답한 카운터로 태그를 인증하는 RFID 태그 검색방법 및 RFID 리더 장치를 제공하는 것이다.

과제의 해결 수단

- [0027] 상기 목적을 달성하기 위해 본 발명은 리더가 다수의 태그 중에서 특정 태그를 검색하는 RFID 태그 검색방법에 관한 것으로서, (a) 상기 리더는 태그의 암호키를 모두 XOR연산한 값(이하 총 인증정보)과 상기 총 인증정보에 각 태그의 암호키를 XOR연산한 값(이하 개별 인증정보)을 저장하는 단계; (b) 상기 리더는 검색하고자 하는 태그(이하 검색 태그)의 개별 인증정보를 제1 인증값으로 생성하고, 상기 총 인증정보에 제1 카운터를 XOR연산하여 제2 인증값을 생성하고, 상기 제1 및 제2 인증값을 태그로 전송하는 단계; (c) 상기 태그는 자신의 암호키와 제1 인증값을 XOR연산하여 제1 결과를 생성하고, 상기 제2 인증값으로 제2 결과를 생성하고, 상기 제1 및 제2 결과를 XOR 연산하여 제2 카운터를 생성하는 단계; 및, (d) 상기 리더는 상기 제2 카운터를 수신하여 상기 제1 카운터와 대비하여 상기 검색 태그를 인증하는 단계를 포함하는 것을 특징으로 한다.
- [0028] 또, 본 발명은 RFID 태그 검색방법에 있어서, 상기 태그의 암호키는 태그의 식별값 및 비밀값을 해쉬하여 생성되는 것을 특징으로 한다.
- [0029] 또, 본 발명은 RFID 태그 검색방법에 있어서, 상기 (b)단계에서, 상기 제2 인증값은 상기 총 인증정보를 해쉬한 후 제1 카운터와 XOR연산되고, 상기 (c)단계에서, 상기 제1 결과는 XOR연산후 해쉬되어 생성되는 것을 특징으로 한다.
- [0030] 또, 본 발명은 RFID 태그 검색방법에 있어서, 상기 (a)단계에서, 상기 개별 인증정보는 상기 리더의 식별정보를 추가하여 XOR연산하여 생성되고, 상기 (b)단계에서, 상기 총 인증정보에 상기 리더의 식별정보를 추가하여 XOR 연산되는 것을 특징으로 한다.
- [0031] 또, 본 발명은 RFID 태그 검색방법에 있어서, 상기 (b)단계에서, 상기 제2 인증값은 상기 총 인증정보와 제1 카운터에 상기 검색 태그의 식별정보를 추가하여 XOR 연산하여 생성되고, 상기 (c)단계에서, 상기 태그는 상기 제2 인증값에 자신의 식별정보를 XOR 연산하여 상기 제2 결과를 생성하는 것을 특징으로 한다.
- [0032] 또, 본 발명은 RFID 태그 검색방법에 있어서, 상기 인증값은 인증정보에 리더의 랜덤값 또는 제1 카운터 중 어느 하나 이상을 추가하여 XOR 연산하여 생성되는 것을 특징으로 한다.
- [0033] 또, 본 발명은 RFID 태그 검색방법에 있어서, 상기 (c)단계에서, 상기 제2 카운터는 상기 제1 및 제2 결과를 XOR 연산한 값을 하나 증가시켜 구해지는 것을 특징으로 한다.
- [0034] 또, 본 발명은 RFID 태그 검색방법에 있어서, 상기 제2 카운터는 암호화되어 전송되는 것을 특징으로 한다.
- [0035] 또, 본 발명은 RFID 태그 검색방법에 있어서, 상기 제2 카운터는 태그의 식별정보 또는 랜덤값 중 어느 하나 또는 모두를 이용하여 암호화되는 것을 특징으로 한다.
- [0036] 또한, 본 발명은 상기 방법을 수행하는 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체에 관한 것이다.
- [0037] 또한, 본 발명은 다수의 태그 중에서 특정 태그를 검색하는 RFID 리더 장치에 관한 것으로서, 모든 태그의 암호

키를 모두 XOR연산한 값(이하 총 인증정보)과 상기 제1 인증값에 각 태그의 암호키를 XOR연산한 값(이하 개별 인증정보)을 저장하는 메모리; 및, 검색하고자 하는 태그(이하 검색 태그)의 개별 인증정보를 제1 인증값으로 생성하고, 상기 총 인증정보에 제1 카운터와 XOR연산하여 제2 인증값을 생성하고, 상기 제1 및 제2 인증값을 태그로 전송하고, 태그로부터 수신한 제2 카운터를 제1 카운터와 대비하여 상기 검색 태그를 인증하는 제어부를 포함하고, 상기 제2 카운터는 상기 태그에 의하여, 태그의 암호키와 제1 인증값을 XOR연산하여 생성된 제1 결과 및, 상기 제2 인증값으로 생성된 제2 결과의 XOR 연산 결과인 것을 특징으로 한다.

[0038] 또, 본 발명은 RFID 리더 장치에 있어서, 상기 태그의 암호키는 태그의 식별값 및 비밀값을 해쉬하여 생성되는 것을 특징으로 한다.

[0039] 또, 본 발명은 RFID 리더 장치에 있어서, 상기 제2 인증값은 상기 총 인증정보를 해쉬한 후 제1 카운터와 XOR연산되고, 상기 제1 결과는 XOR연산후 해쉬되어 생성되는 것을 특징으로 한다.

[0040] 또, 본 발명은 RFID 리더 장치에 있어서, 상기 개별 인증정보는 상기 리더의 식별정보를 추가하여 XOR연산하여 생성되고, 상기 총 인증정보에 상기 리더의 식별정보를 추가하여 XOR 연산되는 것을 특징으로 한다.

[0041] 또, 본 발명은 RFID 리더 장치에 있어서, 상기 제2 인증값은 상기 총 인증정보와 제1 카운터에 상기 검색 태그의 식별정보를 추가하여 XOR 연산하여 생성되고, 상기 태그는 상기 제2 인증값에 자신의 식별정보를 XOR 연산하여 상기 제2 결과를 생성하는 것을 특징으로 한다.

[0042] 또, 본 발명은 RFID 리더 장치에 있어서, 상기 인증값은 인증정보에 리더의 랜덤값 또는 제1 카운터 중 어느 하나 이상을 추가하여 XOR 연산하여 생성되는 것을 특징으로 한다.

발명의 효과

[0043] 상술한 바와 같이, 본 발명에 따른 RFID 태그 검색방법 및 RFID 리더 장치에 의하면, XOR 체인 기반 인증 기법을 적용하여 XOR연산 및 해쉬연산만을 이용하여 인증함으로써, 기밀성, 추적 불가능성, 및 메시지 재생공격을 방지하고 리더의 프라이버시 침해 문제를 해결하면서도 연산량을 적게 할 수 있는 효과가 얻어진다.

도면의 간단한 설명

[0044] 도 1은 종래의 RFID 인증 방법을 설명하는 흐름도이다.

도 2는 본 발명을 실시하기 위한 전체 RFID 시스템 구성의 일례를 도시한 도면이다.

도 3은 본 발명의 일실시예에 따른 리더의 구성에 대한 블록도이다.

도 4는 본 발명의 제1 실시예에 따른 RFID 태그 검색방법을 설명하는 흐름도이다.

도 5는 본 발명의 제2 실시예에 따른 RFID 태그 검색방법을 설명하는 흐름도이다.

도 6은 본 발명의 제3 실시예에 따른 RFID 태그 검색방법을 설명하는 흐름도이다.

도 7 내지 10은 본 발명과 종래 기술의 안정성 및 효율성을 대비한 표이다.

* 도면의 주요 부분에 대한 부호의 설명 *

10 : 리더	11 : 메모리
12 : 제어부	13 : 통신수단
20 : 태그	30 : 서버

발명을 실시하기 위한 구체적인 내용

[0045] 이하, 본 발명의 실시를 위한 구체적인 내용을 도면에 따라서 설명한다.

[0046] 또한, 본 발명을 설명하는데 있어서 동일 부분은 동일 부호를 붙이고, 그 반복 설명은 생략한다.

- [0047] 먼저, 본 발명을 실시하기 위한 전체 RFID 시스템 구성의 일례를 도 2를 참조하여 설명한다.
- [0048] 도 2에서 도시한 바와 같이, 본 발명을 실시하기 위한 RFID 시스템은 리더(10), 다수의 태그(20), 및 서버(30)로 구성된다.
- [0049] 태그(20)는 RFID태그 등 정보를 저장하는 소형 회로 장치로서 리더(10)로부터 무선신호(radio frequency)를 수신하면 수신된 데이터에 응답하여 그 결과를 리더(10)로 송신하는 장치이다. 태그(20)는 회로에 의해 연산을 처리하거나 데이터를 저장하고 읽을 수 있다.
- [0050] 리더(10)는 무선신호를 브로드캐스팅하고 상기 무선신호에 반응하는 태그(20)로부터 신호를 수신한다. 이를 통해, 태그(20)에 저장된 데이터를 수신하거나 태그(20)가 일정한 작업(또는 연산)을 처리하게 하거나, 또 그 처리 결과를 수신한다. 리더(10)가 무선신호를 브로드캐스팅하면 무선신호를 받는 태그(20)들은 상기 리더(10)의 무선신호에 반응한다.
- [0051] 서버(30)는 신뢰기관의 서버로서, 컴퓨팅 기능을 가진 통상의 서버 또는 컴퓨터 단말이다. 서버(30)는 상기 리더(10)와 데이터 통신을 하고, 상기 태그(20) 및 리더(10)에 관한 정보를 저장한다. 그래서 서버(30)는 리더(10)가 필요로 하는 태그 검색과 관련한 정보를 리더(10)에 전송한다.
- [0052] 즉, 리더(10)는 태그를 검색하기 위한 접근리스트 등을 사전에 신뢰기관 서버(30)로부터 수신하여 자신의 메모리에 저장한다. 접근리스트는 리더(10)가 접근 가능한 모든 태그의 암호키로 만든 총 인증정보 및 개별 태그의 암호키로 만든 개별 인증정보를 포함한다. 따라서 리더(10)는 접근 리스트에 포함된 태그(20)에 대해서만 안전한 태그 검색을 할 수 있다.
- [0053] 태그(20)들은 각자 자신을 식별할 수 있는 고유한 식별자(id_j)와 비밀값(t_j)을 저장한다. 태그의 식별자(id_j)는 리더(10)와 공유되고, 태그의 비밀값(t_j)는 공유되지 않고 자신만 저장한다. 태그의 암호키는 태그의 식별자(id_j)와 비밀값(t_j)를 암호화한 값이다.
- [0054] 이때, 리더(10)는 총 인증정보와, 검색하고자 하는 태그(이하 검색태그)의 개별 인증정보로 카운터를 암호화하여 브로드캐스팅한다. 리더(10) 근방에 있는 태그(20)들은 리더(10)가 브로드캐스트한 암호화된 카운터를 모두 수신한다.
- [0055] 각 태그(20)는 암호화된 카운터를 수신하면, 태그(20)는 저장하고 있던 자신의 식별자(id_j)와 비밀값(t_j)를 이용하여 암호키를 만든다. 그리고 태그(20)는 자신의 암호키로 암호화된 카운터를 해독하여 해독한 카운터를 리더(10)에 반환한다.
- [0056] 리더(10)는 해독한 카운터를 수신하여 자신이 이용하였던 카운터와 대비하여, 검색태그를 인증한다. 즉, 리더(10)는 자신의 근방에 있는 모든 태그(20)로부터 카운터를 반환 수신한다. 암호화한 카운터는 오직 검색태그의 암호키로만 해독되므로, 제대로 해독하여 반환한 카운터는 오직 검색태그에 의해 반환되는 카운터이다. 따라서 리더(10)는 반환 수신한 카운터와 원래 자신이 생성한 카운터와 동일한 경우, 상기 카운터를 반환한 태그를 검색태그로 인증함으로써 태그 검색을 완료한다.
- [0057] 다음으로, 본 발명의 일실시예에 따른 RFID 리더의 구성을 도 3을 참조하여 설명한다.
- [0058] 도 3에서 보는 바와 같이, 리더(10)는 메모리(11), 제어부(12), 및 통신수단(13)을 포함하여 구성된다.
- [0059] 메모리(11)는 데이터를 저장하기 위한 리더(10)의 지역 저장영역이다.
- [0060] 메모리(11)에는 사전에 신뢰기관 서버(30)로부터 수신한 접근 리스트 등이 저장된다. 접근리스트는 리더(10)가 접근 가능한 모든 태그의 암호키로 만든 총 인증정보 및 개별 태그의 암호키로 만든 개별 인증정보를 포함한다.
- [0061] 제어부(12)는 검색하고자 하는 태그(이하 검색 태그)의 개별 인증정보와, 총 인증정보를 이용하여 제1 카운터를 암호화한 인증값을 생성한다. 생성된 인증값은 통신수단(13)을 통해 브로드캐스트되고, 각 태그(20)들은 이 인증값에 반응하여 결과값을 반환한다. 이때, 결과값은 상기 인증값을 해독하여 구한 제2 카운터이다. 역시 이 결과값 역시 통신수단(13)을 통해, 제어부(12)가 수신한다. 이때, 제어부(12)는 각 태그(20)로부터 해독한 제2 카운터를 수신하고, 자신의 제1 카운터와 대비하여 동일한 경우 해당 제2 카운터를 송신한 태그(20)를 검색태그로 인증한다.

- [0062] 통신수단(13)은 앞서 본 바와 같이, 데이터를 송수신하기 위한 전송수단이다. 특히, RFID 등 무선 데이터 통신 방식의 전송수단이다.
- [0063] 다음으로, 본 발명의 제1 실시예에 따른 RFID 태그 검색방법을 도 4를 참조하여 구체적으로 설명한다.
- [0064] 도 4에서 보는 바와 같이, 먼저, 리더(10)는 태그의 암호키를 모두 XOR연산한 값(이하 총 인증정보)과 상기 총 인증정보에 각 태그(20)의 암호키를 XOR연산한 값(이하 개별 인증정보)을 저장한다(S11). 바람직하게는, 태그의 암호키는 태그의 식별값 및 비밀값을 해쉬하여 생성된다.
- [0065] 각 태그(20)는 태그의 식별값 id_j 와 비밀값 t_j 를 가진다. 이때, 태그의 암호키는 $f(id_j, t_j)$ 라고 표시된다. 단, $f(,)$ 는 두 파라미터를 연결하여 해쉬값을 생성하는 해쉬 함수이다.
- [0066] 신뢰기관 서버(30)는 도 4와 같이, 리더가 검색 가능한 각 태그의 식별값과 태그의 비밀값을 연결하여 각각 해쉬하고, 해쉬하여 생성된 각 값들을 XOR 연산하여 최종 결과값인 리더의 총 인증정보 X_i 를 얻는다. 그리고 나서 X_i 는 태그의 id_j 에 매칭 되는 각 $f(id_j, t_j)$ 와 XOR 연산하여 검색하고자 하는 태그들의 접근 리스트인 L_i 를 생성한다. 접근 리스트 L_i 는 태그 검색 프로토콜이 동작되기 이전에 오프라인 상에서 신뢰기관으로부터 리더로 안전하게 전송된다.
- [0067] 즉, 총 인증정보는 X_i 으로, $f(id_1, t_1) \oplus f(id_2, t_2) \oplus \dots \oplus f(id_n, t_n)$ 이고, 각 태그 id_j 의 개별 인증정보는 $f(id_j, t_j) \oplus X_i$ 이다. 개별 인증정보의 리스트를 접근 리스트 L_i 이다. 일반적인 XOR 연산의 수학적표기 방법인 $\oplus$ 가 전자문서에 표시되지 않으므로, 이 연산표기 대신 ?로 사용한다.
- [0068] 다음으로, 리더(10)는 검색하고자 하는 태그(이하 검색 태그)의 개별 인증정보를 제1 인증값으로 생성하고, 상기 총 인증정보에 제1 카운터를 XOR연산하여 제2 인증값을 생성하고, 상기 제1 및 제2 인증값을 태그(20)로 전송한다(S12). 바람직하게는, 상기 제2 인증값은 상기 총 인증정보를 해쉬한 후 제1 카운터와 XOR 연산한다.
- [0069] 검색 태그가 태그 id_j 이면, 개별 인증정보는 $f(id_j, t_j) \oplus X_i$ 이므로, 이 값이 제1 인증값이 된다. 한편, 태그(10)는 제1 카운터 c_r 를 생성하고, 총 인증정보 X_i 를 해쉬한 값에 제1 카운터 c_r 를 XOR 연산하여 $h(X_i \oplus r_i) \oplus c_r$ 를 구한다. 이때, $h(,)$ 는 해쉬함수이다. 이 값이 제2 인증값이 된다.
- [0070] 다음으로, 제1 및 제2 인증값을 수신한 모든 태그(20)는 자신의 암호키와 제1 인증값을 XOR연산하여 제1 결과를 생성하고, 상기 제2 인증값으로 제2 결과를 생성하고, 상기 제1 및 제2 결과를 XOR 연산하여 제2 카운터를 생성한다(S13).
- [0071] 즉, 제1 결과는 자신의 암호키 $f(id_{own}, t_{own})$ 와 제1 인증값을 XOR 연산하여, $f(id_{own}, t_{own}) \oplus f(id_j, t_j) \oplus X_i$ 이 되고, 제2 결과는 제2 인증값이므로, 곧 $h(X_i \oplus r_i) \oplus c_r$ 이다.
- [0072] 그리고 제1 결과 및 제2 결과를 XOR 연산하여 구한 제2 카운터 c_t 를 암호화 하여 전송한다(S14). 이때 태그의 식별정보 id_{own} 와 제2 카운터 c_t 를 해쉬하여 암호화 한다. 즉, 태그(20)는 $h(id_{own} \oplus c_t)$ 를 전송한다.
- [0073] 다음으로, 리더(10)는 암호화된 제2 카운터를 수신하여 상기 제1 카운터와 대비하여 상기 검색 태그를 인증한다(S15). 즉, 리더(10)는 인증값을 수신한 모든 태그로부터 암호화된 제2 카운터를 수신한다. 이때, 리더(10)는 $h(id_j \oplus c_r + 1)$ 을 연산하여, 수신한 $h(id_{own} \oplus c_r)$ 와 대비하여 동일하면, 검색 태그로 인식된다. 나머지 태그들은 동일하지 않을 것이고, 검색태그가 아닌 것으로 인식될 것이다.
- [0074] 다음으로, 본 발명의 제2 실시예에 따른 RFID 태그 검색방법을 도 5를 참조하여 구체적으로 설명한다. 제2 실시예는 제1 실시예와 동일하며, 다만, 리더의 식별값 r_i 와 태그의 식별값 id_j 를 추가하여 XOR연산을 해줌으로써 암호화 강도를 높였다.
- [0075] 도 5에서 보는 바와 같이, 리더(10)는 태그의 암호키를 모두 XOR연산한 총 인증정보와 상기 총 인증정보에 각 태그(20)의 암호키를 XOR연산한 개별 인증정보를 저장한다. 이때, 상기 개별 인증정보는 상기 리더의 식별정보

를 추가하여 XOR연산하여 생성한다(S21). 앞서 제1 실시예와 마찬가지로, 태그의 암호키는 태그의 식별값 및 비밀값을 해쉬하여 생성된다.

[0076] 각 태그(20)는 태그의 식별값 id_j 와 비밀값 t_j 를 가지므로, 태그의 암호키는 $f(id_j, t_j)$ 이고, 총 인증정보는 X_i 으로, $f(id_1, t_1)?f(id_2, t_2)?...?f(id_n, t_n)$ 이고, 각 태그 id_j 의 개별 인증정보는 $f(id_j, t_j)?X_i?r_i$ 이다. 또한, 접근 리스트는 개별 인증정보의 리스트들이다.

[0077] 다음으로, 리더(10)는 검색 태그의 개별 인증정보를 제1 인증값으로 생성하고, 상기 총 인증정보에 제1 카운터를 XOR연산하여 제2 인증값을 생성하고, 상기 제1 및 제2 인증값을 태그(20)로 전송한다. 이때, 제2 인증값은 총 인증정보에 리더의 식별정보를 추가하여 XOR 연산한다. 제1 실시예와 마찬가지로, 상기 제2 인증값은 상기 총 인증정보를 해쉬한 후 제1 카운터와 XOR 연산한다. 또한, 추가적으로 태그의 식별정보를 추가하여 XOR연산한다(S22).

[0078] 즉, 개별 인증정보 $f(id_j, t_j)?X_i?r_i$ 이 제1 인증값이 되고, $h(X_i?r_i)?c_r?id_j$ 이 제2 인증값이 된다. 리더(10)는 제1 및 제2 인증값을 모든 태그로 브로드캐스팅한다.

[0079] 다음으로, 태그(20)는 자신의 암호키와 제1 인증값을 XOR연산하여 제1 결과를 생성하고, 상기 제2 인증값으로 제2 결과를 생성하고, 상기 제1 및 제2 결과를 XOR 연산하여 제2 카운터를 생성한다. 이때, 제2 인증값에 태그 자신의 식별정보를 추가하여 XOR연산을 하여 제2 결과를 얻는다(S23).

[0080] 즉, 각 태그(20)는 수신한 제1 인증값에 자신의 암호키 $f(id_{own}, t_{own})$ 를 XOR 연산하여, 제1 결과로서, $f(id_{own}, t_{own})?f(id_j, t_j)?X_i?r_i$ 을 얻는다, 또한, 각 태그(20)는 수신한 제2 인증값에 태그 자신의 식별정보 id_{own} 를 XOR연산하여, 제2 결과로서, $id_{own}?h(X_i?r_i)?c_r?id_j$ 을 계산한다.

[0081] 그리고 각 태그(20)는 제1 결과 및 제2 결과를 XOR 연산하여 제2 카운터 c_t 를 구하고, 제2 카운터 c_t 를 암호화하여 전송한다(S14). 제1 실시예와 마찬가지로, 태그의 식별정보 id_{own} 와 제2 카운터 c_t 를 해쉬하여 암호화한다.

[0082] 다음으로, 리더(10)는 상기 제2 카운터를 수신하여 상기 제1 카운터와 대비하여 상기 검색 태그를 인증한다(S15). 즉, 리더(10)는 $h(id_j?c_r+1)$ 을 연산하여, 수신한 $h(id_{own}?c_r)$ 와 대비하여 동일하면, 검색 태그로 인식된다.

[0083] 다음으로, 본 발명의 제3 실시예에 따른 RFID 태그 검색방법을 도 6을 참조하여 구체적으로 설명한다. 본 발명의 제3 실시예는 제2 실시예에 비하여, 추가적으로 랜덤값과 카운터를 이용하여 암호화를 보다 강화한 것이다.

[0084] 즉, 리더(10)는 인증정보에 리더의 랜덤값 또는 제1 카운터 중 어느 하나를 추가하여 XOR 연산하여 인증값을 생성한다. 또한, 태그(20)도 자신의 랜덤값 n_t 를 발생시켜, 리더(10)로 전송하는 제2 카운터에 랜덤값을 포함시켜 암호화한다.

[0085] 도 6에서 보는 바와 같이, 태그(20)는 태그의 식별값을 id_j , 그리고 태그의 비밀값을 t_j 를 가진다. 신뢰기관 서버(30)는 도 6와 같이, 리더가 검색 가능한 각 태그의 식별값과 태그의 비밀값을 연결하여 각각 해쉬하여 각 태그 id_j 의 암호키 $f(id_j, t_j)$ 를 얻는다.

[0086] 또한, 각 태그의 암호키들을 XOR 연산하여 최종 결과값인 리더의 총 인증정보 X_i 를 얻는다. 그리고 나서 X_i 는 태그의 id_j 의 각 암호키 $f(id_j, t_j)$ 와 XOR 연산하여 검색하고자 하는 태그들의 접근 리스트인 L_i 를 생성한다. 즉, 리더(10)는 사전 준비 단계에서 생성한 인증정보 값들(L_i, X_i)과 리더의 식별값 r_i 를 가진다(S31).

[0087] 구체적으로, 리더 R_i 는 특정 태그 T_j 를 찾기 위해, 리더의 전파가 도달하는 임의의 태그들에게 $f(id_j, t_j)?X_i?r_i?n_r?c_r$ 와 $h(X_i?r_i?n_r?c_r)?c_r?id_j$ 를 포함하는 요청 메시지를 브로드캐스트 한다(S32).

[0088] 다음으로, 리더(R_i)로부터 요청 메시지를 수신한 각각의 태그들(T^*)은, 자신이 가지고 있는 식별값(id_{own})과 비밀

값(t_{own})을 이용하여 해쉬값인 $f(id_{own}, t_{own})$ 를 계산해 내고, 계산된 해쉬값과 요청 메시지의 첫 번째값인 $f(id_j, t_j) \oplus X_i \oplus r_i \oplus n_r \oplus c_r$ 를 XOR 연산한 후 최종 해쉬한 값인 $temp_1$ 을 생성해 낸다. 또한 태그 자신의 식별값(id_{own})과 요청 메시지의 두 번째 값인 $h(X_i \oplus r_i \oplus n_r \oplus c_r) \oplus c_r \oplus id_j$ 를 XOR 연산한 값인 $temp_2$ 를 생성해 낸다. 이렇게 생성된 $temp_1$ 과 $temp_2$ 를 XOR 연산한 후 결과값에 1을 더한 값($(temp_1 \oplus temp_2) + 1$)이 태그의 카운터 값(c_t)이 된다(S33).

[0089] 그리고 태그들(T^*)은 자신의 식별값(id_{own})과 카운터값(c_t)을 XOR 연산한 후 해쉬한 값에 난수 n_t 를 연결하여 한 번 더 해쉬한다. 그리고 나서 생성된 해쉬값 $h(h(id_{own} \oplus c_t) \oplus n_t)$ 과 난수 n_t 를 포함하는 응답 메시지를 요청 메시지를 송신한 리더(R_i)에게 전송한다(S34).

[0090] 임의의 태그들(T^*)로부터 응답 메시지들을 수신한 리더(R_i)는, 찾고자 했던 태그의 식별값(id_j)과 1이 증가된 카운터 값(c_r+1), 그리고 전달 받은 응답 메시지의 두 번째 값인 난수 n_t 를 이용해 수식 $h(h(id_{own} \oplus c_t) \oplus n_t)$ 를 계산하고, 계산한 결과값이 응답메시지의 첫 번째 값과 일치하는지 검증한다(S35). 만일 일치한다면, 리더는 요청 메시지를 전송한 임의의 태그 그룹 내에 찾고자 했던 태그(T_j)가 존재함을 알 수 있다.

[0091]

[0092] 다음으로, 본 발명의 일실시예에 따른 발명의 효과를 도 7을 참조하여 보다 구체적으로 설명한다.

[0093] 먼저, 본 발명의 안전성 분석을 설명한다.

[0094] RFID 태그 검색 방법은 기본적으로 무선구간에서 동작하므로, 공격자는 도청(Eavesdropping Attack)을 통해 전송되는 메시지를 쉽게 훔쳐보는 것이 가능하다. 따라서 도청된 메시지는 공격자의 재생 공격(Replay Attack)에 이용될 수 있어 정당한 리더가 요청한 메시지를 위조하거나 또는 정당한 태그가 응답한 메시지를 훔쳐 내는 데 악용될 수 있다. 또한 리더 소지자는 휴대용 리더를 이용해 이동하면서 태그를 검색해야 하는 경우가 생기는데, 이때 적절한 보안이 보장되지 않는다면 리더 소지자의 위치를 공격자에 의해 추적당할 수도 있다. 마찬가지로 태그를 몸에 지니고 있는 사용자 또한 공격자에 의해 위치를 추적당할 수도 있다. 위와 같은 공격을 통해 발생할 수 있는 보안 문제 해결하기 위해, 안전한 RFID 태그 검색 방법은 도 7과 같은 보안 요구사항을 만족해야 한다.

[0095] 먼저, 안전성의 기밀성 측면을 설명한다.

[0096] 본 발명의 RFID 태그 검색방법에서는, 리더에서 태그로 전송되는 요청메시지와 태그에서 리더로 전송되는 응답 메시지에 포함된 값들을 기본적으로 XOR 연산과 해쉬함수($h()$, $f()$)를 사용하여 생성하였기 때문에 기밀성을 만족한다. 따라서 공격자는 이들 메시지로부터 리더/태그의 식별값(r_i, id_j)이나 태그의 비밀값(t_j)과 같은 어떠한 의미 있는 정보도 추출해 낼 수 없게 된다.

[0097] 개체인증 측면을 설명한다.

[0098] 본 발명에서는, 리더가 자신이 찾고자 했던 태그의 식별값(id_j)과 기대하는 카운터값($c_r + 1$)을 이용하여 수신한 응답 메시지의 첫 번째 값을 검증함으로써 정당한 태그임을 인증할 수 있다. 한편 본 발명에서는 재생공격 및 태그 추적공격 등을 막기 위해 태그 검색 요청 메시지를 수신한 모든 태그들이 응답 메시지를 발생시키게 하였기 때문에 태그 측에서 리더를 인증하지는 않는다.

[0099] 다음으로, 추적불가능 측면을 설명한다.

[0100] 종래기술 1 내지 5에서는 리더의 식별자(r_i)가 평문으로 전송되기 때문에 요청 메시지를 전송하는 리더를 확인할 수 있을 뿐만 아니라, 이동하면서 태그를 검색하는 리더 소지자의 위치를 추적할 수도 있었다. 하지만 본 발명은 리더의 식별값을 포함하여 리더를 구별할 수 있는 어떠한 정보도 공격자는 확인할 수 없기 때문에 리더 소지자의 위치 추적을 불가능하게 한다. 마찬가지로 리더의 요청 메시지를 수신한 모든 태그는 응답메시지를 발생시키기 때문에, 응답 메시지에서부터 태그를 구별하거나 위치를 추적할 수 없게 된다. 리더의 추적불가능성은 종래 기술 5에서도 개선된 사항이지만, 본 발명에서는 암호화 연산을 사용 하지 않음으로써 효율성이 대폭 향상된다.

[0101] 다음으로, 물리공격 안전성 측면을 설명한다.

[0102] RFID 태그 검색 방법에서는 사용자가 리더를 소지하여 이동하면서 원하는 태그를 검색하게 되는 경우가 대부분이다. 이때 리더가 분실된다면 공격자는 습득한 리더로부터 저장된 정보를 유출시킬 수 있게 된다. 만일 리더가 검색 권한을 갖는 태그의 비밀값이 평문 형태로 저장되어 있다면, 공격자는 유출한 태그의 비밀값을 이용해 리더의 요청 메시지에 대해 정당한 태그인척 위장할 수 있게 된다. 이와 같은 공격을 방지하기 위해서는 리더 측에 저장되는 태그의 비밀값은 평문 형태가 아니라 비밀값을 검증할 수 있는 검증값 형태로 저장되어야 한다는 것이다. $f(id_j, t_j) \oplus X_i \oplus r_i$ 값은 제안한 프로토콜에서 태그의 비밀값에 대한 검증값으로 사용된다. 한편, 태그의 물리공격 안전성 측면에서는, 저가의 태그는 공격자의 물리적인 공격에 의해 태그의 비밀값을 노출시킬 수 있는 가능성이 존재하기 때문에 물리공격 으로부터 안전하다고 볼 수는 없다.

[0103] 다음으로, 재생공격 안전성을 설명한다.

[0104] 공격자는 도청을 통해 리더 및 태그가 전송한 메시지를 저장해 뒀다가 다시 재전송하는 공격을 수행할 수 있다. 본 발명에서는 이와 같은 재생공격에 대한 안전성을 보장하기 위해 기본적으로 요청 메시지를 수신한 모든 태그들이 응답 메시지를 발생시키게 하였으며, 또한 카운터값(c_r, c_t)을 이용하게 했다. 먼저, 공격자가 리더의 요청 메시지를 저장하였다가 이를 이용한 재생공격의 경우, 요청 메시지를 수신한 모든 태그들이 응답 메시지를 발생시키기 때문에 요청 메시지를 이용한 재생공격에 안전하게 된다. 만일 공격자가 태그의 응답 메시지들을 이용하여 재생공격을 수행하게 되더라도, 리더는 기대하는 카운터값을 이용하여 응답 메시지를 검증하기 때문에 공격자의 재생공격으로부터 안전하다.

[0105] 도 8은 본 발명과, 종래기술 1 내지 5와의 안전성을 비교한 표이다. 본 발명은 도 7의 보안요구 사항을 만족시킴을 알 수 있다.

[0106] 다음으로, 효율성 분석을 설명한다.

[0107] 종래기술 1 내지 5와의 비교 분석을 통해 효율성을 평가 한다. 도 9는 종래기술과 본 발명에서 리더가 생성하는 요청 메시지와 태그가 요청 메시지를 수신하여 응답 메시지를 생성하기까지의 연산량을 비교한 표이다.

[0108] 도 9에서 연산량의 비교 결과, 종래기술 1,2는 리더와 태그 측에서 7번의 해쉬 연산과 3번의 XOR 연산, 그리고 2번의 난수생성 연산을 수행한다. 본 발명에서는 7번의 해쉬 연산과 12번의 XOR 연산, 그리고 3번의 난수생성 연산을 수행한다. 본 발명이 종래기술 1,2에 비해 높은 연산량을 필요로 하는 이유는, 종래기술 1,2가 제공하는 못하는 재생공격과 추적공격을 막기 위해 추가적인 연산이 필요했기 때문이다.

[0109] 같은 보안성을 제공하는 본 발명과 종래기술 3,4,5와의 비교에 있어서는, 본 발명이 해쉬 연산과 XOR 연산만으로 이루어졌기 때문에, 5번 및 7번의 암호복호 연산을 수행해야 하는 종래기술 3,4,5의 프로토콜보다 뛰어난 성능을 보여준다. 게다가 본 발명과 종래기술 5는 기본적으로 특정 그룹에 속한 모든 태그들의 응답 메시지를 처리해야 하기 때문에, 리더의 브로드캐스트 영역에 존재하는 RFID 태그의 수가 늘어날수록 종래기술 5가 필요로 하는 암호화 연산은 급격히 증가하게 된다.

[0110] 도 10은 암호 연산 회수를 태그의 수로 가정 했을 때, 태그의 수에 따른 연산량을 비교한 그래프이다. 도 10에서와 같이, 종래기술 5에서는 태그의 수가 증가할수록 필요로 하는 계산량이 급격히 증가하는 반면, 본 발명은 종래기술 5보다 낮은 계산량을 필요로 한다.

[0111]

[0112] 이상, 본 발명자에 의해서 이루어진 발명을 실시 예에 따라 구체적으로 설명하였지만, 본 발명은 실시 예에 한정되는 것은 아니고, 그 요지를 이탈하지 않는 범위에서 여러 가지로 변경 가능한 것은 물론이다.

[0113]

산업상 이용가능성

[0114] 본 발명은 리더가 다수의 태그 중에서 특정 태그를 검색하는 RFID 리더 및 태그 장치를 개발하는 데 적용이 가능하다. 특히, 본 발명은 XOR 체인 기반 인증 기법을 적용하여 XOR연산 및 해쉬연산만을 이용하여 리더 및 태그가 상호 인증할 수 있는 RFID 리더 및 태그 장치를 개발하는 데 적용이 가능하다.

도면

도면1a

$$R_i \rightarrow T^* : h(f(r_i, t_j) \| n_r) \oplus id_j, n_r, r_i \quad (1)$$

$$T^* : \text{Derive } h(f(r_i, t_j) \| n_r) \text{ and XOR with } h(f(r_i, t_j) \| n_r) \oplus id_j \quad (2)$$

$$: \text{If } id = id_j \quad (3)$$

$$R_i \leftarrow T_j : h(f(r_i, t_j) \| n_t \| n_r) \oplus id_j, n_t \quad (4)$$

도면1b

$$R_i \rightarrow T^* : h(f(r_i, t_j) \| n_r) \oplus id_j, n_r, r_i \quad (1)$$

$$T^* : \text{Deriving } h(f(r_i, t_j) \| n_r) \text{ and XOR with } h(f(r_i, t_j) \| n_r) \oplus id_j \quad (2)$$

$$: \text{If } id = id_j \text{ and } n_r \neq \text{old}n$$

$$: \text{update old}n = n_r \quad (3)$$

$$R_i \leftarrow T_j : h(f(r_i, t_j) \| n_t) \oplus id_j, n_t \quad (4)$$

도면1c

$$R_i \rightarrow T^* : \text{Broadcast } [id_j]m, r_i, n_n \quad (1)$$

$$T^* : \text{If } idm = [id_j]m \quad (2)$$

$$R_i \leftarrow T_j : h(f(r_i, t_j) \| n_r \| n_t) \oplus id_j, n_t \quad (3)$$

$$R_i : \text{Determines } f(r_i, t_j) \text{ from } L, \text{ obtain } id_j \quad (4)$$

도면1d

$$R_i \rightarrow T^* : \text{Broadcast } h(f(r_i, t_j) \parallel n_r) \oplus id_j, n_r, r_i \quad (1)$$

$$T^* : \text{Derive } h(f(r_i, t_j) \parallel n_r) \text{ and XOR with } h(f(r_i, t_j) \parallel n_r) \oplus id_j \quad (2)$$

: If $id = id_j$:

$$R_i \leftarrow T_j : h(f(r_i, t_j) \parallel n_t) \oplus id_j, n_t \quad (3)$$

: Else:

$$R_i \leftarrow T_j : (rand, n_r) \text{ with prob. } \lambda \quad (4)$$

도면1e

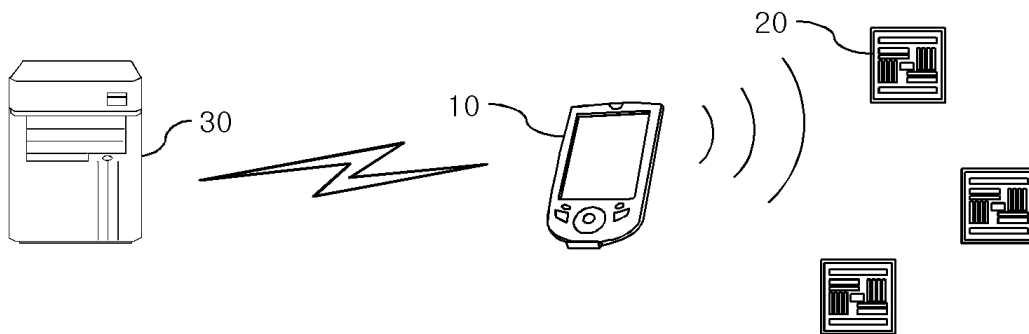
$$R_i \rightarrow T^* : \text{Broadcast } E_{ID_i}(r_j \parallel R) \quad (1)$$

$$T^* : \text{Decrypt } E_{ID_i}(r_j \parallel R) \text{ and} \\ \text{Compute } K_i = E_{t_i}(r_j \parallel ID_i) \quad (2)$$

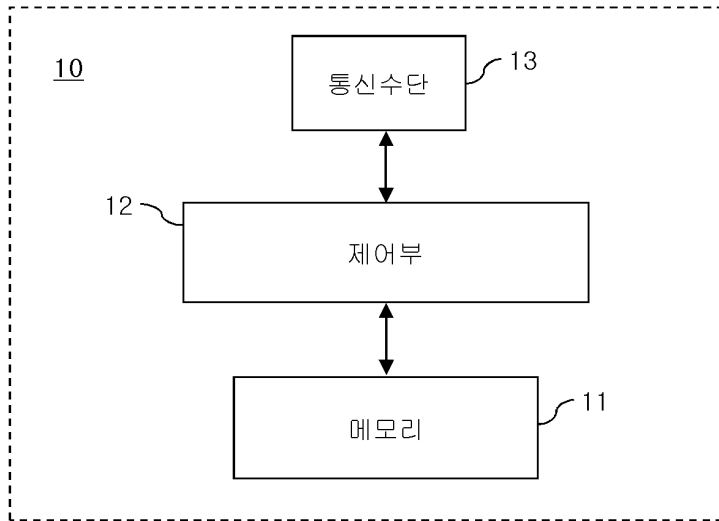
$$R_i \leftarrow T^* : E_{K_i}(ID_i \parallel r) \oplus (R \parallel R) \quad (3)$$

$$R_i : E_{K_i}(ID_i \parallel r)$$

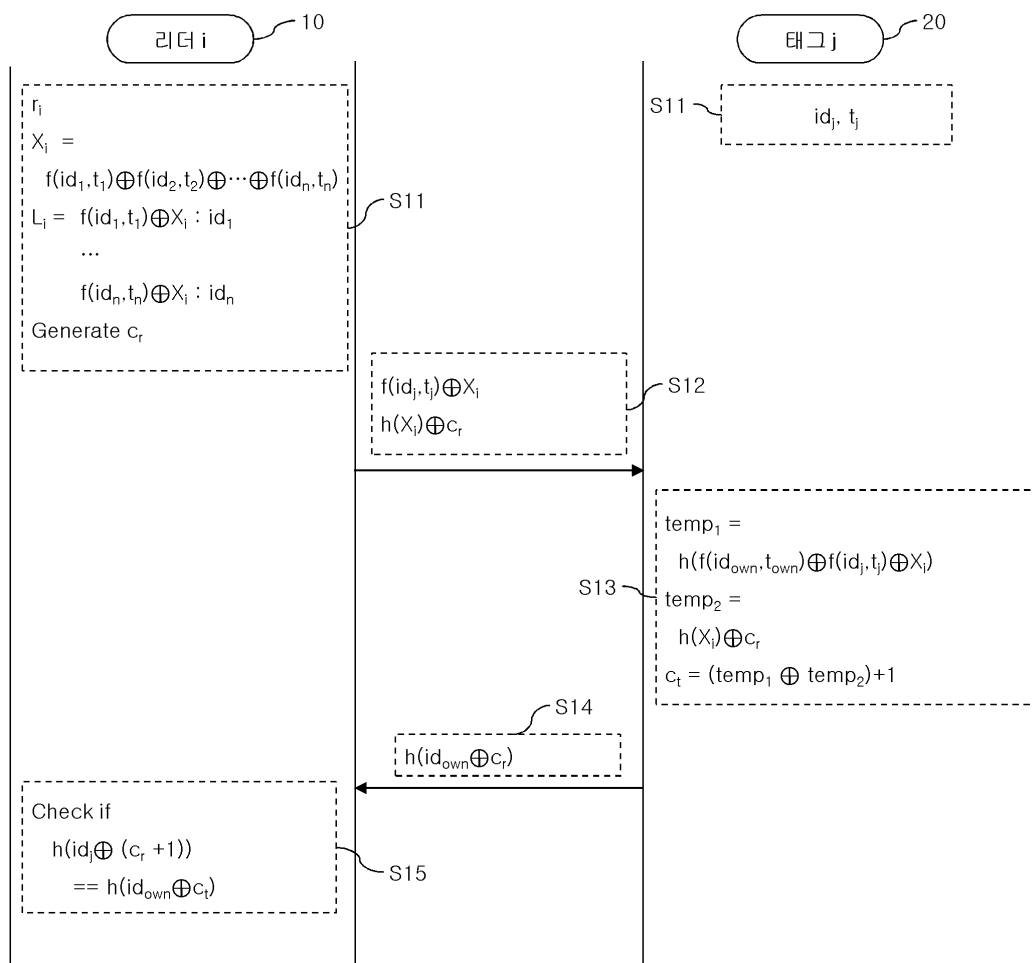
도면2



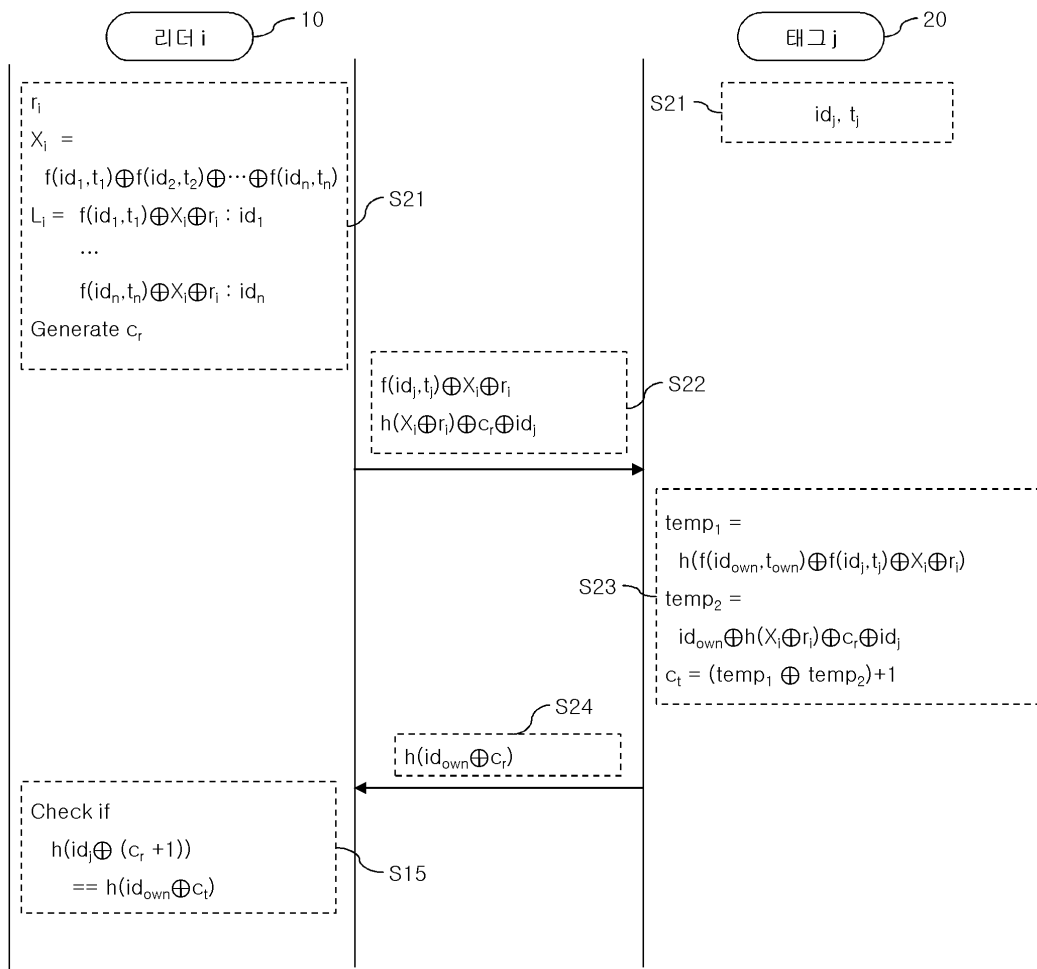
도면3



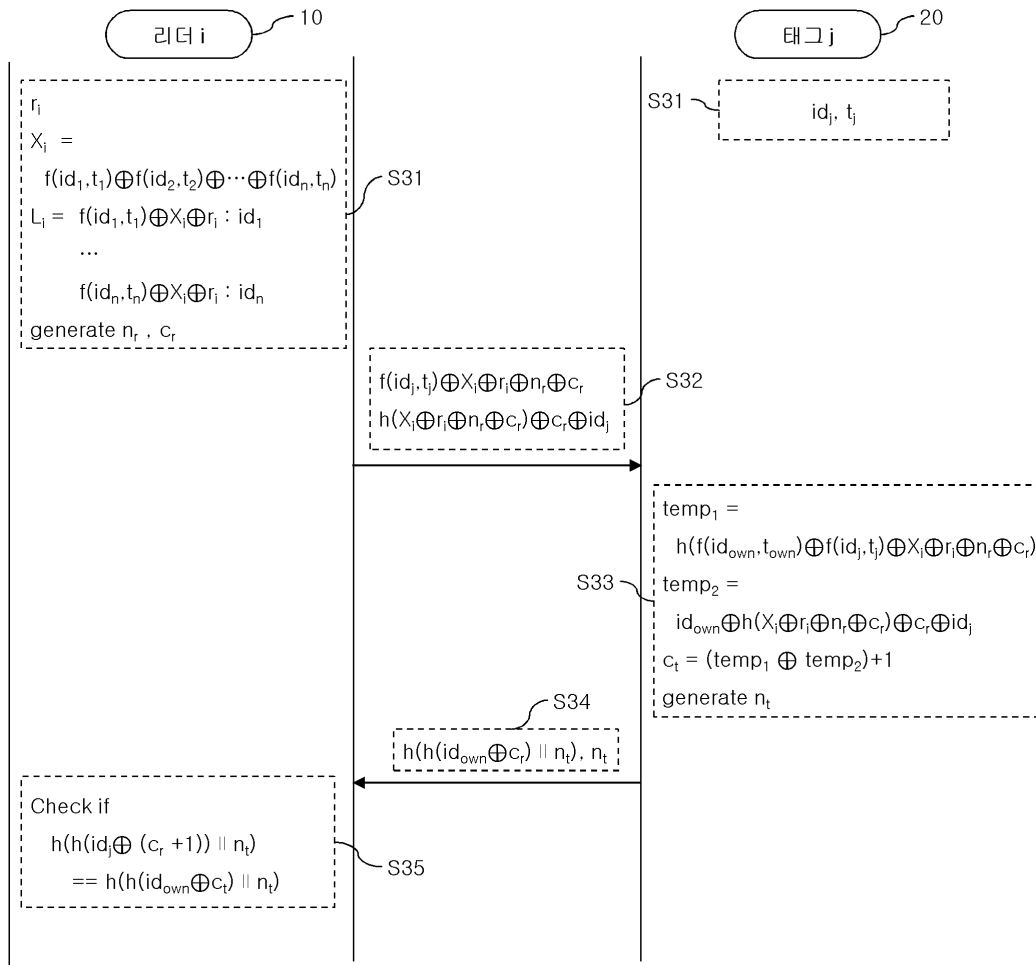
도면4



도면5



도면6



도면7

보안 요구사항	내용
메시지 기밀성	· 공격자가 도청 공격을 통해 리더와 태그 사이에 전송되는 태그 검색 메시지를 습득했다 하더라도, 그 메시지에서 어떠한 의미 있는 정보도 알아낼 수 없도록 기밀성이 보장되어야 한다.
개체 인증	· 태그는 리더로부터 수신 한 요청 메시지가 정당한 리더에 의해 생성되었음을 확신할 수 있어야 한다. · 리더는 태그로부터 수신 한 응답 메시지가 정당한 태그에 의해 생성되었음을 확신할 수 있어야 한다.
추적불가능성	· 같은 리더가 생성한 요청 메시지들의 관계를 구별할 수 없게 하여 리더의 위치 추적 공격을 방지해야 한다. · 태그에 의해 발생하는 응답메시지를 랜덤하게 하여 특정 태그의 존재유무를 통한 태그의 위치를 추적 공격을 할 수 없게 해야 한다.
물리공격 안전성	· 공격자는 리더에 저장된 정보를 유출할 수 있고 만일 유출된 정보에 태그의 비밀값이 포함되어 있다면 정당한 태그로써 위장할 수 있게 된다. 따라서 리더에는 태그에 대한 비밀정보가 평문형태로 저장되지 않아야 한다.
재생공격 안전성	· 도청을 통해 리더 및 태그가 전송한 메시지를 저장하고 있다가 다시 재전송시키는 공격자의 재생공격에 대한 안전성이 보장되어야 한다.

도면8

안전성 항목	종래기술 1,2	종래기술 3,4	종래기술 5	본 발명
메시지 기밀성	○	○	○	○
개체 인증	○	○	○	○
추적불가능성	X	△	○	○
물리공격 안전성	△	△	△	△
재생공격 안전성	X	○	○	○

○: 만족함, X: 만족하지 않음, △: 부분적으로 만족함

도면9

방법	리더	태그
종래기술 1,2	$3\pi(h)+2\pi(\oplus)+1\pi(r)$	$4\pi(h)+1\pi(\oplus)+1\pi(r)$
종래기술 3,4	$3\pi(E)+2\pi(\oplus)+0\pi(r)$	$4\pi(E)+4\pi(\oplus)+1\pi(r)$
종래기술 5	$2\pi(E)+1\pi(\oplus)+1\pi(r)$	$3\pi(E)+1\pi(\oplus)+1\pi(r)$
본 발명	$3\pi(h)+8\pi(\oplus)+2\pi(r)$	$4\pi(h)+4\pi(\oplus)+1\pi(r)$

$\pi(h)$: 해쉬 연산, $\pi(\oplus)$: 배타적 논리합 연산,
 $\pi(E)$: 암호화 연산, $\pi(r)$: 난수생성 연산

도면10

