



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2013년12월04일
(11) 등록번호 10-1336864
(24) 등록일자 2013년11월28일

(51) 국제특허분류(Int. Cl.)
G06K 17/00 (2006.01)
(21) 출원번호 10-2012-0062707
(22) 출원일자 2012년06월12일
심사청구일자 2012년06월12일
(56) 선행기술조사문헌
KR1020120022003 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
고려대학교 산학협력단
서울 성북구 안암동5가 1
(72) 발명자
정익래
서울특별시 광진구 중곡1동 254-12 호동아파트 203
노건태
서울특별시 강남구 개포3동 주공아파트 707동 1304호
천지영
서울특별시 성북구 하월곡4동 두산위브 아파트 118동 104호
(74) 대리인
특허법인충현

전체 청구항 수 : 총 8 항

심사관 : 홍기완

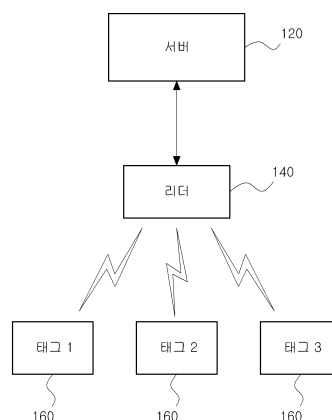
(54) 발명의 명칭 R F I D 태그 검색방법

(57) 요약

본 발명은 RFID 태그 검색 방법에 관한 것으로, 보다 구체적으로는 서버로부터 접근이 허용되는 적어도 하나의 태그에 관한 비밀값이 포함된 접근리스트정보를 수신하는 단계; 임의의 제1 난수를 생성한 후, 상기 제1 난수와, 상기 접근리스트정보로부터 검색하고자 하는 태그의 현재 비밀값을 제1 해시연산하여 제1 해시연산값을 생성하는 단계; 상기 접근리스트정보에 기재된 현재 비밀값에 연속하는 다음 비밀값과, 상기 제1 난수를 제1 해시연산하여 제2 해시값을 생성하는 단계; 및 상기 제1 해시값, 제2 해시값 및 제1 난수를 상기 태그로 전송하는 단계; 상기 태그로부터 제3 해시값을 수신하는 단계; 상기 제3 해시값에 대한 정당성 검사를 수행하고, 검사결과에 기초하여 태그를 검색하는 단계;를 포함한다.

본 발명의 RFID 태그 검색 방법은 서로 다른 해시함수를 이용하는 해시체인기법을 통해 각 태그별 할당된 비밀값에 대한 정당성검사를 수행함에 따라, 리더의 프라이버시를 보호할 수 있는 효과가 있다.

대 표 도 - 도1



이 발명을 지원한 국가연구개발사업

과제고유번호	KI002113
부처명	지식경제부
연구사업명	산업융합원천기술개발사업
연구과제명	Car-헬스케어 보안 기술개발
기 여 율	1/1
주관기관	고려대학교 산학협력단
연구기간	2012.03.01 ~ 2013.02.28

특허청구의 범위

청구항 1

서버로부터 접근이 허용되는 적어도 하나의 태그에 관한 비밀값이 포함된 접근리스트정보를 수신하는 단계;

임의의 제1 난수를 생성한 후, 상기 제1 난수와, 상기 접근리스트정보로부터 검색하고자 하는 태그의 현재 비밀값을 제1 해시연산하여 제1 해시연산값을 생성하는 단계;

상기 접근리스트정보에 기재된 현재 비밀값에 연속하는 다음 비밀값과, 상기 제1 난수를 제1 해시연산하여 제2 해시값을 생성하는 단계;

상기 제1 해시값, 제2 해시값 및 제1 난수를 상기 태그로 전송하는 단계;

상기 태그로부터 제3 해시값을 수신하는 단계; 및

상기 제3 해시값에 대한 정당성검사를 수행하고, 검사결과에 기초하여 태그를 검색하는 단계;

를 포함하는 RFID 태그 검색방법.

청구항 2

제1항에 있어서,

상기 태그로부터 수신한 제3 해시값에 기초하여 상기 태그의 현재 비밀값을 갱신하는 단계;

를 더 포함하는 것을 특징으로 하는 RFID 태그 검색방법.

청구항 3

제2항에 있어서,

상기 태그의 현재 비밀값을 갱신하는 단계는

상기 현재 비밀값과, 제1 난수 및 상기 태그로부터 수신한 제2 난수에 대하여 XOR연산을 수행한 다음 제2 해시연산하고, 이어서 제1 해시연산하여 획득한 값이 상기 제3 해시값과 동일한지 여부를 확인하는 과정; 및

상기 제1 해시연산하여 획득한 값이 상기 제3 해시값과 동일한 경우에는 상기 현재 비밀값에 대하여 제2 해시연산을 연속수행하여 획득한 값을 현재 비밀값으로 갱신하는 과정;

을 포함하는 것을 특징으로 하는 RFID 태그 검색방법.

청구항 4

제2항에 있어서,

상기 태그의 현재 비밀값을 갱신하는 단계는

상기 다음 비밀값과, 제1 난수 및 제2 난수에 대하여 XOR연산을 수행한 다음 제2 해시연산하고, 이어서 제1 해시연산하여 획득한 값이 상기 제3 해시값과 동일한지 여부를 확인하는 과정; 및

상기 제1 해시연산하여 획득한 값이 상기 제3 해시값과 동일한 경우에는 상기 다음 비밀값에 대하여 제2 해시연산을 연속수행하여 획득한 값을 현재 비밀값으로 갱신하는 과정;

을 더 포함하는 것을 특징으로 하는 RFID 태그 검색방법.

청구항 5

삭제

청구항 6

리더로부터 태그 검색을 위해 생성된 제1 해시값, 제2 해시값 및 제1 난수를 수신하는 단계;

상기 제1 해시값 및 제2 해시값에 대한 정당성검사를 수행하여 제3 해시값을 생성하는 단계; 및

상기 제3 해시값 및 자신이 생성한 임의의 제2 난수를 상기 리더로 전송하는 단계;

를 포함하되,

상기 제3 해시값을 생성하는 단계는

기저장된 현재 비밀값과 상기 제1 난수를 XOR연산한 후 제1 해시연산하여 생성된 값을 상기 제2 해시값과 AND연산한 값과, 상기 현재 비밀값에 연속하는 다음 비밀값과 상기 제1 난수를 XOR연산한 후 제1 해시연산하여 생성된 값이 상기 제1 해시값과 동일한지 여부를 판단하는 과정; 및

상기 현재 비밀값과 상기 제1 난수 및 자신이 생성한 제2 난수에 대하여 XOR 연산한 후, 제2 해시연산을 수행하고, 이어서 제1 해시연산을 수행하여 제3 해시값을 생성하는 과정;

을 포함하는 것을 특징으로 하는 RFID 태그 검색방법.

청구항 7

리더로부터 태그 검색을 위해 생성된 제1 해시값, 제2 해시값 및 제1 난수를 수신하는 단계;

상기 제1 해시값 및 제2 해시값에 대한 정당성검사를 수행하여 제3 해시값을 생성하는 단계; 및

상기 제3 해시값 및 자신이 생성한 임의의 제2 난수를 상기 리더로 전송하는 단계;

를 포함하되,

상기 제3 해시값을 생성하는 단계는

기저장된 현재 비밀값의 이전 비밀값과 상기 제1 난수를 XOR연산한 후, 제1 해시연산하여 생성된 값을 상기 제2 해시값과 AND연산한 값과, 상기 현재 비밀값을 상기 제1 난수와 XOR연산한 후, 제1 해시연산하여 생성된 값이 상기 제1 해시값과 동일한지 여부를 판단하는 과정; 및

상기 현재 비밀값과 상기 제1 난수 및 자신이 생성한 제2 난수에 대하여 XOR 연산한 후, 제2 해시연산을 수행하고, 이어서 제1 해시연산을 수행하여 제3 해시값을 생성하는 과정;

을 포함하는 것을 특징으로 RFID 태그 검색방법.

청구항 8

제6항 또는 제7항에 있어서,

상기 현재 비밀값을 이전 비밀값으로 갱신하거나, 상기 현재 비밀값에 대하여 제2 해시연산을 연속 수행하여 획득한 값을 현재 비밀값으로 갱신하는 단계;

를 더 포함하는 것을 특징으로 RFID 태그 검색방법.

청구항 9

제1항 내지 제4항 또는 제6항 내지 제7항 중 어느 한 항에 따른 방법을 컴퓨터로 실행하기 위한 프로그램이 기록된 컴퓨터 판독가능 기록매체.

명세서

기술분야

- [0001] 본 발명은 RFID 태그 검색방법에 관한 것으로, 특히 다수의 태그로부터 각종 정보를 수신하며, 사용자가 휴대하는 리더의 프라이버시를 보호할 수 있는 RFID 태그 검색방법에 관한 것이다.

배경기술

- [0002] 최근 들어, IT기술의 발달에 따라 공급사슬관리(SCM: Supply Chain Managemnet), 생산관리 등과 같은 다양한 분야에서 RFID 기술이 널리 사용되고 있다. 이러한 RFID란, Radio Frequency Identification의 약자로서, IC칩과 무선신호를 통해 식품, 동물, 사물 등의 다양한 개체의 정보를 체계적으로 관리할 수 있는 차세대 인식 기술을 말한다. 특히, 물품의 생산에서 판매에 이르는 전과정의 정보를 초소형의 IC칩에 내장시켜 무선주파수를 통해 추적할 수 있도록 함으로써, 지금까지의 유통분야에서 일반적으로 물품관리를 위해 사용되었던 바코드를 대체할 수 있는 차세대 인식기술로 주목받고 있다.
- [0003] 이러한 RFID는 판독 및 해독 기능을 하는 리더(Reader)와 정보를 제공하는 태그(Tag)로 구성되는데, 제품에 부착되는 태그에는 생산, 유통, 보관, 소비의 전 과정에 대한 정보를 담고, 리더가 안테나를 통해 상기 정보를 읽고, 읽은 정보를 인공위성이나 이동통신망을 통해 정보시스템으로 통합하여 사용하고 있다.
- [0004] 특히, 종래의 바코드는 저장용량이 적고, 실시간 정보 파악이 어려울 뿐만 아니라, 매우 근접한 상태 예를 들면, 수 cm 정도의 거리 내에서만 해당 정보를 읽을 수 있다는 단점이 존재한다.
- [0005] 이와 달리, RFID 기술은 완제품 상태로 공장에서 출시되어 슈퍼마켓 진열장에 진열되기까지의 전 과정을 추적할 수 있다. 특히, 리더는 초당 수백 개까지의 태그가 부착된 제품의 데이터를 읽을 수 있고, 대형 할인점에서 RFID기술을 이용하는 경우에는 계산대를 통과하자마자 태그가 부착된 상품의 가격이 집계되어, 소비자가 구매하고자 하는 상품의 계산시간을 크게 감소시킬 수 있는 장점을 갖는다.
- [0006] 하지만 이와 같은 많은 장점을 가지고 있음에도 불구하고, RFID기술은 보안이 취약하다는 단점을 가지고 있다. 예를 들어, RFID 기술을 구성하는 리더는 주로 사용자에 의해 휴대되는데, 태그로부터 수신한 각종 정보가 쉽게 노출되었다.
- [0007] 이를 방지하고자, 다양한 RFID 태그 검색 프로토콜이 연구되고 있다. 하지만 종래의 RFID 태그 검색 프로토콜은 리더의 프라이버시를 보호하지 않는 문제점이 발생할 뿐만 아니라, 리더와 다수의 태그 간에 전방향 안전성에 문제점이 발생했다.
- [0008] 상술한 바와 같이, RFID 태그 검색방법에 대한 선행기술을 살펴보면 다음과 같다.
- [0009] 선행기술 1은 한국공개특허 제2011-0048929호(2011.05.12)로서, 태그 위치 추정 방법에 관한 것이다. 이러한 선행기술 1은 복수의 태그 중 통신범위 내에 위치한 제1 태그를 베이스 태그로 선정하고, 복수의 태그 중 위치를 추정하려는 제2 태그를 검색하며, 제2 태그와 레인징(ranging) 절차를 수행하여 제2 태그와의 제1 거리 정보를 추정하고, 제1 태그로부터 제1 태그와 제2태그간의 추정된 제2 거리 정보를 수신하고, 제1 거리 정보와 제2 거리 정보를 이용하여 제2 태그의 위치 정보를 추정한다.
- [0010] 선행기술 2는 한국등록특허 제1036195호(2011.05.16)로서, 무선 인식 태그간 데이터 중계방법에 관한 것이다. 이러한 선행기술 2는 소정의 무선인식 태그가 소정의 단말로 적어도 하나 이상의 데이터(또는 RFID 정보) 수신을 요청하고, 단말에서 적어도 하나 이상의 무선인식 태그(2,3,4...N) 중 무선인식 태그가 요청하는 데이터(또는 RFID 정보)를 저장하는 특정 무선인식 태그를 검색한 후 추출하여, 단말에서 추출된 특정 무선인식 태그로 무선인식 태그가 요청하는 데이터(또는 RFID 정보) 송신을 요청하고, 특정 무선인식 태그에서 단말로 무선인식 태그가 요청하는 데이터(또는 RFID 정보)를 송신하고, 단말에서 특정 무선인식 태그가 송신한 데이터(또는 RFID 정보)를 무선인식 태그로 제공한다.

발명의 내용

해결하려는 과제

- [0011] 상기와 같은 종래 기술의 문제점을 해결하기 위해, 본 발명은 리더의 프라이버시를 보호할 수 있는 RFID 태그 검색 방법을 제공하고자 한다.

과제의 해결 수단

- [0012] 위와 같은 과제를 해결하기 위한 본 발명의 일 실시 예에 따른 건물 RFID 태그 검색 방법은 서버로부터 접근이 허용되는 적어도 하나의 태그에 관한 초기 비밀값이 포함된 접근리스트정보를 수신하는 단계; 임의의 제1 난수를 생성한 후, 상기 제1 난수와, 상기 접근리스트정보로부터 검색하고자 하는 태그의 현재 비밀값을 제1 해시연산하여 제1 해시연산값을 생성하는 단계; 상기 접근리스트정보에 기재된 현재 비밀값에 연속하는 다음 비밀값과, 상기 제1 난수를 제1 해시연산하여 제2 해시값을 생성하는 단계; 및 상기 제1 해시값, 제2 해시값 및 제1 난수를 상기 태그로 전송하는 단계; 상기 태그로부터 제3 해시값을 수신하는 단계; 상기 제3 해시값에 대한 정당성 검사를 수행하고, 검사결과에 기초하여 태그를 검색하는 단계;를 포함한다.
- [0013] 보다 바람직하게는 상기 태그로부터 수신한 제3 해시값에 기초하여 상기 태그의 현재 비밀값을 갱신하는 단계;를 더 포함할 수 있다.
- [0014] 보다 바람직하게는 상기 현재 비밀값과, 제1 난수 및 상기 태그로부터 수신한 제2 난수에 대하여 XOR연산을 수행한 다음 제2 해시연산하고, 이어서 제1 해시연산하여 획득한 값이 상기 제3 해시값과 동일한지 여부를 확인하는 과정; 및 상기 제1 해시연산하여 획득한 값이 상기 제3 해시값과 동일한 경우에는 상기 현재 비밀값에 대하여 제2 해시연산을 연속수행하여 획득한 값을 현재 비밀값으로 갱신하는 과정;을 포함하는 태그의 현재 비밀값을 갱신하는 단계를 포함할 수 있다.
- [0015] 보다 바람직하게는 상기 다음 비밀값과, 제1 난수 및 제2 난수에 대하여 XOR연산을 수행한 다음 제2 해시연산하고, 이어서 제1 해시연산하여 획득한 값이 상기 제3 해시값과 동일한지 여부를 확인하는 과정; 및 상기 제1 해시연산하여 획득한 값이 상기 제3 해시값과 동일한 경우에는 상기 다음 비밀값에 대하여 제2 해시연산을 연속수행하여 획득한 값을 현재 비밀값으로 갱신하는 과정;을 더 포함하는 태그의 현재 비밀값을 갱신하는 단계를 포함할 수 있다.
- [0016] 위와 같은 과제를 해결하기 위한 본 발명의 일 실시 예에 따른 건물 RFID 태그 검색 방법은 리더로부터 태그 검색을 위해 생성된 제1 해시값, 제2 해시값 및 제1 난수를 수신하는 단계; 상기 제1 해시값 및 제2 해시값에 대한 정당성검사를 수행하여 제3 해시값을 생성하는 단계; 및 상기 제3 해시값 및 자신이 생성한 제2 난수를 상기 리더로 전송하는 단계;를 포함한다.
- [0017] 보다 바람직하게는 기저장된 현재 비밀값과 상기 제1 난수를 XOR연산한 후 제1 해시연산하여 생성된 값을 상기 제2 해시값과 AND연산한 값과, 상기 현재 비밀값에 연속하는 다음 비밀값과 상기 제1 난수를 XOR연산한 후 제1 해시연산하여 생성된 값이 상기 제1 해시값과 동일한지 여부를 판단하는 과정; 상기 현재 비밀값과 상기 제1 난수 및 자신이 생성한 제2 난수에 대하여 XOR 연산한 후, 제2 해시연산을 수행하고, 이어서 제1 해시연산을 수행하여 제3 해시값을 생성하는 과정;을 포함하는 제3 해시값을 생성하는 단계를 포함할 수 있다.
- [0018] 보다 바람직하게는 상기 현재 비밀값의 이전 비밀값과 상기 제1 난수를 XOR연산한 후, 제1 해시연산하여 생성된 값을 상기 제2 해시값과 AND연산한 값과, 상기 현재 비밀값을 상기 제1 난수와 XOR연산한 후, 제1 해시연산하여 생성된 값이 상기 제1 해시값과 동일한지 여부를 판단하는 과정; 상기 현재 비밀값과 상기 제1 난수 및 자신이 생성한 제2 난수에 대하여 XOR 연산한 후, 제2 해시연산을 수행하고, 이어서 제1 해시연산을 수행하여 제3 해시값을 생성하는 과정;을 포함하는 제3 해시값을 생성하는 단계를 포함할 수 있다.
- [0019] 보다 바람직하게는 상기 현재 비밀값을 이전 비밀값으로 갱신하거나, 상기 현재 비밀값에 대하여 제2 해시연산을 연속수행하여 획득한 값을 현재 비밀값으로 갱신하는 단계;를 더 포함할 수 있다.

발명의 효과

- [0020] 본 발명의 RFID 태그 검색 방법은 서로 다른 해시함수를 이용하는 해시체인기법을 통해 각 태그별 할당된 비밀값에 대한 정당성검사를 수행함에 따라, 리더의 프라이버시를 보호할 수 있는 효과가 있다.
- [0021] 또한, 본 발명의 RFID 태그 검색 방법은 중앙 데이터베이스 서버를 통하지 않고 리더와 태그간에 해시값의 송수신을 통해 태그 검색을 수행함에 따라, 태그 검색에 따른 소요시간이 감소하는 효과가 있다.
- [0022] 더불어, 본 발명의 RFID 태그 검색 방법은 서로 다른 해시함수를 이용하는 해시체인기법을 사용하여 리더와 다수의 태그 간 전방향 안전성을 향상시킬 수 있는 효과가 있다.

도면의 간단한 설명

- [0023] 도 1은 본 발명의 일 실시 예에 따른 RFID 태그 검색방법을 이용한 태그 검색 시스템의 블록도이다.
- 도 2는 리더에서 수행되는 RFID 태그 검색방법의 순서도이다.
- 도 3은 태그에서 수행되는 RFID 태그 검색방법의 순서도이다.
- 도 4는 본 발명의 일 실시 예에 따른 RFID 태그 검색방법을 나타내는 도면이다.
- 도 5는 해시체인기법을 이용한 해시값을 연산과정을 나타낸 블록도이다.

발명을 실시하기 위한 구체적인 내용

- [0024] 이하, 본 발명을 바람직한 실시 예와 첨부한 도면을 참고로 하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며, 여기에서 설명하는 실시 예에 한정되는 것은 아니다.
- [0025] 이하, 도 1을 참조하여 본 발명의 일 실시 예에 따른 RFID 태그 검색방법을 이용한 태그 검색 시스템의 블록도에 대하여 보다 구체적으로 살펴보도록 한다.
- [0026] 도 1은 본 발명의 일 실시 예에 따른 RFID 태그 검색방법을 이용한 태그 검색 시스템의 블록도이다.
- [0027] 도 1에 도시된 바와 같이, 본 발명의 RFID 태그 검색방법을 이용하는 태그 검색 시스템(100)은 서버(120), 리더(140) 및 다수의 태그(160)를 포함한다.
- [0028] 서버(CDS, Central Database Server, 120)는 접속이 허용되는 적어도 하나의 태그에 관한 비밀값을 포함하는 접근리스트정보를 각각의 리더(140)로 전송한다. 이때, 상기 접근리스트정보는 하기의 표 1에 기재된 바와 같이, 각각의 태그별 초기 비밀값이 할당되어 저장되어 있다.

표 1

[0029]

ID	Seed
T ₁	$S_{1,j}^0$
T ₂	$S_{2,j}^0$
T ₃	...
T ₄	$S_{n,j}^0$

- [0030] 뿐만 아니라, 상기 서버(120)는 상기 초기 비밀값을 각각 해당하는 태그(160)로 전송하여 각 태그 내 저장되도록 한다. 즉, 상기 서버(120)는 초기 설정과정에서 사용될 뿐, 본 발명의 본격적인 태그 검색 과정에서는 실제

작업이 수행되지는 않는다.

[0031] 리더(140)는 상기 서버(120)로부터 접근이 허용되는 적어도 하나의 태그에 관한 초기 비밀값이 포함된 접근리스트정보를 수신하고, 임의의 제1 난수를 생성하여, 상기 제1 난수와, 상기 접근리스트정보로부터 태그의 현재 비밀값을 제1 해시연산하여 제1 해시연산값을 생성하며, 상기 접근리스트정보에 기재되며, 현재 비밀값에 연속하는 다음 비밀값과, 상기 제1 난수를 제1 해시연산하여 제2 해시값을 생성하고, 생성한 상기 제1 해시값, 제2 해시값 및 제1 난수를 태그(160)로 전송하며, 상기 태그(160)로부터 제3 해시값을 수신하고, 상기 제3 해시값에 대한 정당성검사를 수행하고, 그 검사결과에 따라 태그를 검색하며, 이후 상기 태그(160)의 현재 비밀값을 갱신한다.

[0032] 태그(160)는 리더(140)로부터 태그 검색을 위해 생성된 제1 해시값, 제2 해시값 및 제1 난수를 수신하고, 상기 제1 해시값 및 제2 해시값에 대한 정당성검사를 수행하고, 이에 따른 제3 해시값을 생성하며, 상기 제3 해시값 및 자신이 생성한 임의의 제2 난수를 상기 리더(140)로 전송하며, 상기 현재 비밀값을 갱신한다.

[0033] 이하, 도 2를 참조하여 리더의 RFID 태그 검색 방법에 대하여 자세히 살펴보도록 한다.

[0034] 도 2는 리더에서 수행되는 RFID 태그 검색방법의 순서도이다.

[0035] 도 2에 도시된 바와 같이, 본 발명의 리더에서 수행되는 RFID 태그 검색 방법은 리더(140)가 서버(120)로부터 접근이 허용되는 적어도 하나의 태그에 대하여 각각 할당된 비밀값이 포함된 접근리스트정보를 수신한다(S210).

[0036] 이후, 상기 리더(140)는 임의의 제1 난수 r_R 를 생성한 후, 상기 제1 난수 r_R 와, 상기 접근리스트정보로부터 태

그(160)의 현재 비밀값 $S_{j,i}^c$ 을 제1 해시연산(G)하여 제1 해시연산값 a_t 을 생성한다(S220).

[0037] 이어서, 상기 리더(140)는 상기 접근리스트정보에 기재되며 현재 비밀값 $S_{j,i}^c$ 에 연속하는 다음 비밀값 $S_{j,i}^N$ 과, 상기 제1 난수 r_R 를 제1 해시연산(G)하여 제2 해시값 a_{t+1} 을 생성한다(S230).

[0038] 이에 따라, 상기 리더(140)는 앞서, 과정 S220 및 S230을 통해 생성한 상기 제1 해시값 a_t , 제2 해시값 a_{t+1} 및 제1 난수 r_R 를 태그(160)로 전송한다(S240).

[0039] 이후, 리더(140)는 상기 태그(160)로부터 생성된 제3 해시값 b_t 을 수신하고, 수신한 상기 제3 해시값 b_t 에 대한 정당성검사를 수행하고, 그 검사결과에 기초하여 최종적으로 태그(160)를 검색한다(S250). 즉, 상기 리더(140)

는 상기 현재 비밀값 $S_{j,i}^c$ 과, 제1 난수 r_R 및 상기 태그로부터 수신한 제2 난수 r_t 에 대하여 XOR연산을 수행한 다음, 제2 해시연산(H)하고, 이어서 제1 해시연산(G)하여 획득한 값이 상기 제3 해시값 b_t 과 동일한지 여부를 확인하여 정당성 검사를 수행한다. 이후, 상기 제1 해시연산(G)하여 획득한 값이 상기 제3 해시값 b_t 과 동일한

경우에는 현재 비밀값에 대하여 제2 해시연산(H)을 연속수행한 후, 획득한 값을 현재 비밀값 $S_{j,i}^c$ 으로 갱신한다.

[0040] 또는 상기 리더(140)가 상기 현재 비밀값과 연속하도록 접근리스트정보 상에서 배열되는 다음 비밀값 $S_{j,i}^N$ 과, 제1 난수 r_R 및 제2 난수 r_t 에 대하여 XOR연산을 수행한 다음, 제2 해시연산(H)하고, 이어서 제1 해시연산(G)하여 획득한 값이 상기 제3 해시값 b_t 과 동일한지 여부를 확인하여 정당성검사를 수행한다. 이후, 제1 해시연산

(G)하여 획득한 값이 상기 제3 해시값 b_t 과 동일한 경우에는 상기 다음 비밀값 $S_{j,i}^N$ 에 대하여 제2 해시연산

(H)을 연속 수행한 후, 획득한 값을 현재 비밀값 $S_{j,i}^c$ 으로 갱신한다.

- [0041] 이하, 도 3을 참조하여, 태그에서 수행되는 RFID 태그 검색방법에 대하여 자세히 살펴보도록 한다.
- [0042] 도 3은 태그에서 수행되는 RFID 태그 검색방법의 순서도이다.
- [0043] 도 3에 도시된 바와 같이, 본 발명의 태그에서 수행되는 RFID 태그 검색방법은 태그(160)가 리더(140)로부터 태그 검색을 위해 생성된 제1 해시값 a_t , 제2 해시값 a_{t+1} 및 제1 난수 r_R 를 수신한다(S310).
- [0044] 이에 따라, 상기 태그는 상기 제1 해시값 a_t 및 제2 해시값 a_{t+1} 에 대한 정당성검사를 수행하여 제3 해시값 b_t 을 생성한다(S320). 이러한 제1 해시값 a_t 및 제2 해시값 a_{t+1} 에 대한 정당성 검사를 보다 자세히 살펴보면 다음과 같다.
- [0045] 먼저, 상기 태그(160)가 기저장된 현재 비밀값 $S_{j,k}^c$ 과 상기 제1 난수 r_R 를 XOR연산한 후 제1 해시연산(G)하여 생성된 값을 상기 제2 해시값 a_{t+1} 과 AND연산한 값과, 상기 현재 비밀값 $S_{j,k}^c$ 에 연속하는 다음 비밀값 $S_{j,k}^N$ 과 상기 제1 난수 r_R 를 XOR연산한 후 제1 해시연산(G)하여 생성된 값이 상기 제1 해시값 a_t 과 동일한지 여부를 판단한다. 이때, 상기 태그(160)가 만약 동일하다고 판단한 경우, 상기 현재 비밀값 $S_{j,k}^c$ 과 상기 제1 난수 r_R 및 자신이 생성한 제2 난수 r_t 에 대하여 XOR 연산한 후 제2 해시연산(H)을 수행하고, 이어서 제1 해시연산(G)을 수행하여 제3 해시값 b_t 을 생성한다.
- [0046] 또는, 상기 태그(160)가 상기 현재 비밀값의 이전 비밀값 $S_{j,k}^0$ 과 상기 제1 난수 r_R 를 XOR연산한 후 제1 해시연산(G)하여 생성된 값을 상기 제2 해시값 a_{t+1} 과 AND연산한 값과, 상기 현재 비밀값 $S_{j,k}^c$ 을 상기 제1 난수 r_R 와 XOR연산한 후, 제1 해시연산(G)하여 생성된 값이 상기 제1 해시값 a_t 과 동일한지 여부를 판단한다. 이때, 상기 태그(160)가 만약 동일하다고 판단한 경우, 상기 현재 비밀값 $S_{j,k}^c$ 과 상기 제1 난수 r_R 및 자신이 생성한 제2 난수 r_t 에 대하여 XOR 연산한 후, 제2 해시연산(H)을 수행하고, 이어서 제1 해시연산(G)을 수행하여 제3 해시값 b_t 을 생성한다.
- [0047] 상기 태그(160)는 상술한 바와 같이 생성된 상기 제3 해시값 b_t 및 자신이 생성한 임의의 제2 난수 r_t 를 리더(140)로 전송한다(S330).
- [0048] 이어서, 상기 태그(160)는 상기 현재 비밀값에 대하여 갱신을 수행할 수 있는데, 예를 들어, 상기 현재 비밀값 $S_{j,i}^c$ 을 이전 비밀값 $S_{j,i}^0$ 으로 갱신할 수 있다. 또는 상기 현재 비밀값 $S_{j,i}^c$ 에 대하여 제2 해시연산(H)을 연속 수행하여 획득한 값을 현재 비밀값 $S_{j,i}^c$ 으로 갱신할 수 있다.
- [0049] 이하, 도 4를 통해 리더와 태그가 수행하는 연산과정 및 전송 내용에 대하여 자세히 살펴본다.
- [0050] 도 4는 본 발명의 일 실시 예에 따른 RFID 태그 검색방법을 나타내는 도면이다.
- [0051] 도 4에 도시된 바와 같이, 본 발명의 RFID 태그 검색방법은 리더(140)가 서버(120)로부터 접근이 허용되는 적어도 하나의 태그에 대하여 각각 할당된 비밀값이 포함된 접근리스트정보를 수신한다.
- [0052] 이후, 상기 리더(140)는 임의의 제1 난수 r_R 를 생성한 후, 상기 제1 난수 r_R 와, 상기 접근리스트정보로부터 태

그(160)의 현재 비밀값 $S_{j,i}^c$ 을 제1 해시연산(G)하여 제1 해시연산값 a_t 을 생성한다.

[0053] 이어서, 상기 리더(140)는 상기 접근리스트정보에 기재되며 현재 비밀값 $S_{j,i}^c$ 에 연속하는 다음 비밀값 $S_{j,i}^N$ 과, 상기 제1 난수 r_R 를 제1 해시연산(G)하여 제2 해시값 a_{t+1} 을 생성한다.

[0054] 이에 따라, 상기 리더(140)는 앞서, 과정 S220 및 S230을 통해 생성한 상기 제1 해시값 a_t , 제2 해시값 a_{t+1} 및 제1 난수 r_R 를 태그(160)로 전송한다.

[0055] 태그(160)가 리더(140)로부터 태그 검색을 위해 생성된 제1 해시값 a_t , 제2 해시값 a_{t+1} 및 제1 난수 r_R 를 수신한다.

[0056] 이에 따라, 상기 태그는 상기 제1 해시값 a_t 및 제2 해시값 a_{t+1} 에 대한 정당성검사를 수행하여 제3 해시값 b_t 을 생성한다. 이러한 제1 해시값 a_t 및 제2 해시값 a_{t+1} 에 대한 정당성 검사를 보다 자세히 살펴보면 다음과 같다.

[0057] 먼저, 상기 태그(160)가 기저장된 현재 비밀값 $S_{j,k}^c$ 과 상기 제1 난수 r_R 를 XOR연산한 후 제1 해시연산(G)하여 생성된 값을 상기 제2 해시값 a_{t+1} 과 AND연산한 값과, 상기 현재 비밀값 $S_{j,k}^c$ 에 연속하는 다음 비밀값 $S_{j,k}^N$ 과 상기 제1 난수 r_R 를 XOR연산한 후 제1 해시연산(G)하여 생성된 값이 상기 제1 해시값 a_t 과 동일한지 여부를 판단한다. 이때, 상기 태그(160)가 만약 동일하다고 판단한 경우, 상기 현재 비밀값 $S_{j,k}^c$ 과 상기 제1 난수 r_R 및 자신이 생성한 제2 난수 r_t 에 대하여 XOR 연산한 후 제2 해시연산(H)을 수행하고, 이어서 제1 해시연산(G)을 수행하여 제3 해시값 b_t 을 생성한다.

[0058] 또는, 상기 태그(160)가 상기 현재 비밀값의 이전 비밀값 $S_{j,k}^0$ 과 상기 제1 난수 r_R 를 XOR연산한 후 제1 해시연산(G)하여 생성된 값을 상기 제2 해시값 a_{t+1} 과 AND연산한 값과, 상기 현재 비밀값 $S_{j,k}^c$ 을 상기 제1 난수 r_R 와 XOR연산한 후, 제1 해시연산(G)하여 생성된 값이 상기 제1 해시값 a_t 과 동일한지 여부를 판단한다. 이때, 상기 태그(160)가 만약 동일하다고 판단한 경우, 상기 현재 비밀값 $S_{j,k}^c$ 과 상기 제1 난수 r_R 및 자신이 생성한 제2 난수 r_t 에 대하여 XOR 연산한 후, 제2 해시연산(H)을 수행하고, 이어서 제1 해시연산(G)을 수행하여 제3 해시값 b_t 을 생성한다.

[0059] 상기 태그(160)는 상술한 바와 같이 생성된 상기 제3 해시값 b_t 및 자신이 생성한 임의의 제2 난수 r_t 를 리더(140)로 전송한다.

[0060] 이어서, 상기 태그(160)는 상기 현재 비밀값에 대하여 갱신을 수행할 수 있는데, 예를 들어, 상기 현재 비밀값 $S_{j,i}^c$ 을 이전 비밀값 $S_{j,i}^0$ 으로 갱신할 수 있다. 또는 상기 현재 비밀값 $S_{j,i}^c$ 에 대하여 제2 해시연산(H)을 연속 수행하여 획득한 값을 현재 비밀값 $S_{j,i}^c$ 으로 갱신할 수 있다.

[0061] 이후, 리더(140)가 상기 태그(160)로부터 생성된 제3 해시값 b_t 을 수신하고, 수신한 상기 제3 해시값 b_t 에 대한 정당성검사를 수행하고, 그 검사결과에 기초하여 최종적으로 태그(160)를 검색한다. 즉, 상기 리더(140)는 상기

현재 비밀값 $S_{j,i}^c$ 과, 제1 난수 r_R 및 상기 태그로부터 수신한 제2 난수 r_t 에 대하여 XOR연산을 수행한 다음, 제2 해시연산(H)하고, 이어서 제1 해시연산(G)하여 획득한 값이 상기 제3 해시값 b_t 과 동일한지 여부를 확인하여 정당성 검사를 수행한다. 이후, 상기 제1 해시연산(G)하여 획득한 값이 상기 제3 해시값 b_t 과 동일한 경우에는

는 현재 비밀값에 대하여 제2 해시연산(H)을 연속수행한 후, 획득한 값을 현재 비밀값 $S_{j,i}^c$ 으로 갱신한다.

[0062] 또는 상기 리더(140)가 상기 현재 비밀값과 연속하도록 접근리스트정보 상에서 배열되는 다음 비밀값 $S_{j,i}^N$ 과, 제1 난수 r_R 및 제2 난수 r_t 에 대하여 XOR연산을 수행한 다음, 제2 해시연산(H)하고, 이어서 제1 해시연산(G)하여 획득한 값이 상기 제3 해시값 b_t 과 동일한지 여부를 확인하여 정당성검사를 수행한다. 이후, 제1 해시연산

(G)하여 획득한 값이 상기 제3 해시값 b_t 과 동일한 경우에는 상기 다음 비밀값 $S_{j,i}^N$ 에 대하여 제2 해시연산

(H)을 연속 수행한 후, 획득한 값을 현재 비밀값 $S_{j,i}^c$ 으로 갱신한다.

[0063] 특히, 본 발명에서는 서로 다른 해시함수를 포함하는 해시 체인 기법을 이용하여 각 단계별 해시값을 연산할 수 있다.

[0064] 도 5는 해시 체인 기법을 이용한 해시값을 연산과정을 나타낸 블록도이다.

[0065] 도 5에 도시된 바와 같이, 현재 비밀값 $S_{j,i}^t$ 에 대하여 제2 해시연산(H)을 수행하면 $H(S_{j,i}^t)$ 을 획득할 수 있고,

제1 해시연산(G)을 수행하는 경우에는 제1 해시값 a_t 을 획득할 수 있다. 이어서, 앞서 생성된 $H(S_{j,i}^t)$ 을

다시 제2 해시연산(H)을 수행하면 상기 현재 비밀값에 연속하는 다음 비밀값을 $S_{j,i}^{t+1}$ 획득할 수 있고, 제1 해

시연산(G)을 수행하면 제3 해시값 b_t 을 획득할 수 있다. 또한, 상기 다음 비밀값 $S_{j,i}^{t+1}$ 을 다시 제2 해시연산

(H)하면, $H(S_{j,i}^{t+1})$ 을 획득할 수 있으며, 제1 해시연산(G)하는 경우에는 제2 해시값 a_{t+1} 을 획득할 수 있다.

이후, 상기 $H(S_{j,i}^{t+1})$ 을 제1 해시연산(G)하면 제4 해시값 b_{t+1} 을 획득할 수 있다.

[0066] 본 발명의 RFID 태그 검색 방법은 서로 다른 해시함수를 이용하는 해시체인기법을 통해 각 태그별 할당된 비밀값에 대한 정당성검사를 수행함에 따라, 리더의 프라이버시를 보호할 수 있는 효과가 있다.

[0067] 또한, 본 발명의 RFID 태그 검색 방법은 중앙 데이터베이스 서버를 통하지 않고 리더와 태그간에 해시값의 송수신을 통해 태그 검색을 수행함에 따라, 태그 검색에 따른 소요시간이 감소하는 효과가 있다.

[0068] 더불어, 본 발명의 RFID 태그 검색 방법은 서로 다른 해시함수를 이용하는 해시체인기법을 사용하여 리더와 다수의 태그 간 전방향 안전성을 향상시킬 수 있는 효과가 있다.

[0069] 상기에서는 본 발명의 바람직한 실시 예에 대하여 설명하였지만, 본 발명은 이에 한정되는 것이 아니고 본 발명의 기술 사상 범위 내에서 여러 가지로 변형하여 실시하는 것이 가능하고 이 또한 첨부된 특허청구범위에 속하는 것은 당연하다.

부호의 설명

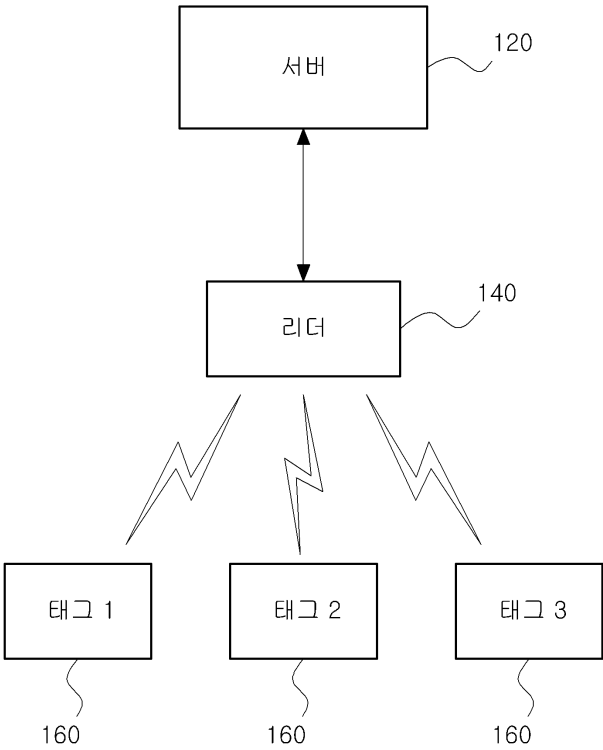
- [0070]
- 120: 서버

140: 리더

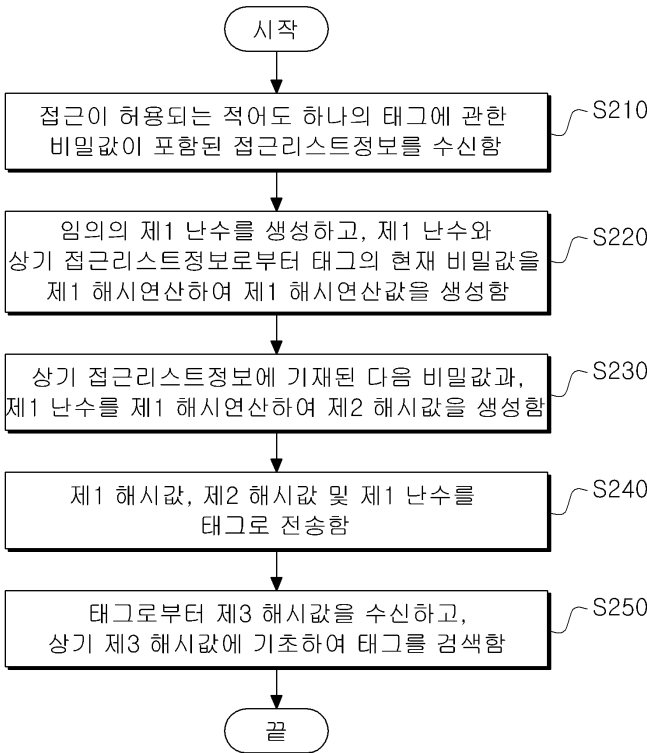
160: 태그

도면

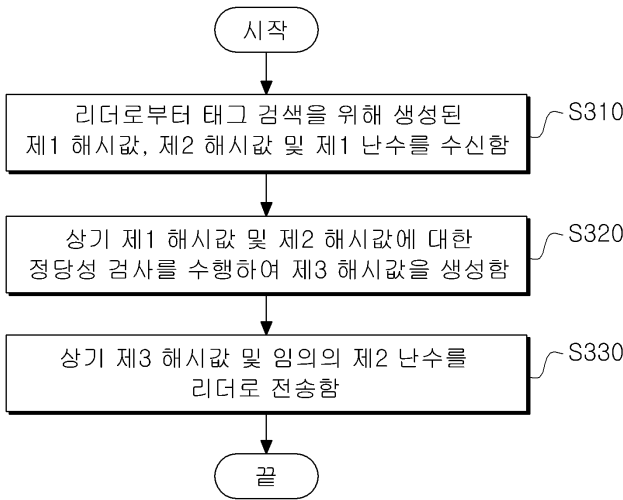
도면1



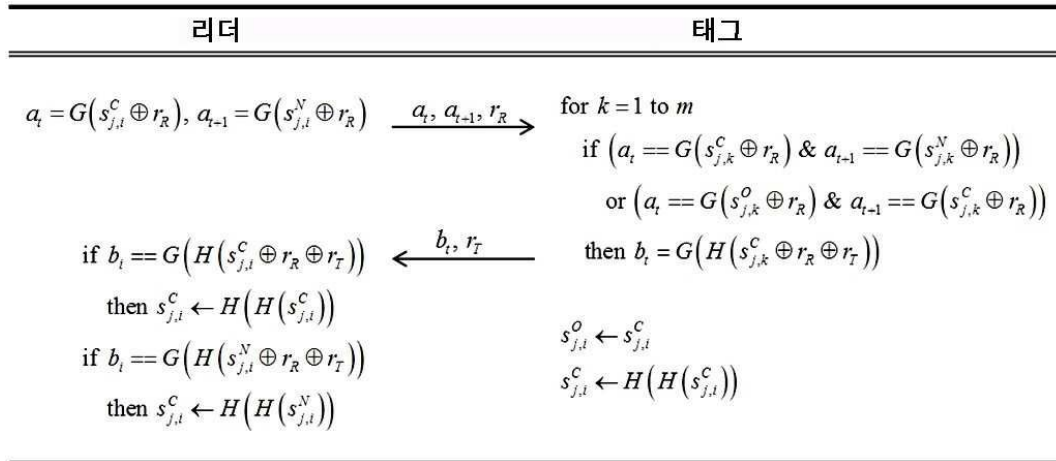
도면2



도면3



도면4



도면5

