(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2011-0042420
(43) 공개일자 2011년04월27일

(51) Int. Cl.
H04W 12/08 (2009.01) *H04W 12/06* (2009.01)
(21) 출원번호 10-2009-0099085
(22) 출원일자 2009년10월19일
심사청구일자 2009년10월19일

(71) 출원인
세종대학교산학협력단
서울 광진구 군자동 98 세종대학교
(72) 발명자
권태경
서울특별시 광진구 군자동 세종대학교
정연호
서울특별시 광진구 군자동 세종대학교
신수연
서울 영등포구 대림3동현대1차아파트 101-103 103동 306호
(74) 대리인
특허법인 엠에이피에스

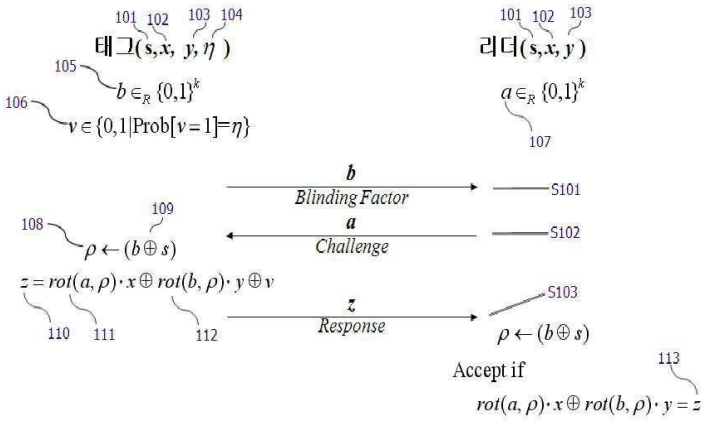
전체 청구항 수 : 총 1 항

(54) 잡음이 포함된 패리티 검증 기반의 안전한 경량 인증 프로토콜

(57) 요 약

본 발명은 RFID 통신에 적용가능한 경량 인증방법에 관한 것으로, 구체적으로 리더와 태그사이에 구현 가능한 새로운 LPN 문제 기반의 안전한 경량 인증 프로토콜에 관한 것이다.

대 표 도 - 도1



이 발명을 지원한 국가연구개발사업
과제고유번호 10557
부처명 서울특별시
연구관리전문기관
연구사업명 서울시 산학연 협력사업, 기술기반 구축사업
연구과제명 차세대 PMP 콘텐츠산업 클러스터 사업
기여율
주관기관 세종대학교 산학협력단
연구기간 2005년 12월 1일 ~ 2010년 11월 30일

특허청구의 범위

청구항 1

LPN 문제 기반의 안전한 경량 인증 프로토콜에 있어서,

challenge(107)에 대한 로테이션연산과 blinding factor(105)를 포함하는 프로토콜

명 세 서

발명의 상세한 설명

기 술 분 야

[0001] 본 발명은 RFID 통신에 적용가능한 경량 인증방법에 관한 것으로, 사생활 침해와 보안 문제를 해결하기 위해서 비밀키를 사용하지 않는 LPN 문제 기반의 안전한 경량 인증 프로토콜에 관한 것이다.

배 경 기 술

[0002] RFID 시스템의 확산을 위해서는 이를 위한 기반 시설 구축 및 관련 기술들의 개발 뿐만 아니라 해당 시스템 구축시 발생 가능한 사생활 침해와 보안 문제를 해결해야 할 필요가 있다.

[0003] 리더의 질의에 대해 무조건 응답하는 RFID 태그는 쉽게 도청 당할 수 있으며 이러한 도청은 객체에 대한 불법적인 추적 및 사생활 침해로 이루어 질 수 있다. 뿐만 아니라 도청으로 얻어낸 정보를 통해 나쁜 의도를 갖는 태그가 정당한 태그로 위장할 가능성도 있다. RFID 태그가 급속하게 생활속으로 침투함에 따라 사생활 침해는 심각한 사회적인 이슈가 될 것으로 예상된다. 따라서 유비쿼터스 컴퓨팅환경 구축을 위해 가장 먼저 해결해야 할 과제가 프라이버시 침해와 같은 보안 문제를 해결하는 것이다.

[0004] RFID 태그의 연산 능력이 사람과 마찬가지로 제한되어 있음을 밝혀내고, 이를 RFID 시스템에 적용시킨 것이 HB 프로토콜이다. 이러한 HB 프로토콜은 다양하게 제안되어졌다.

[0005] 그러나, HB 프로토콜은 첫번째 단계에서 결정된 리더의 난수에 의해 결과값이 결정되기 때문에 재생공격에 취약하고, HB+ 프로토콜은 두번째 단계에서 공격자가 변조된 값을 보냈을 경우 비밀값을 알수 있어 중간자 공격에 취약하다는 문제점이 있다.

발명의 내용

해결 하고자하는 과제

[0006] 본 발명은 blinding factor(105)와 challenge(107)을 로테이션 시켜줌으로써 중간자 공격에 의해 공격자가 원하는 위치의 비트 값이 알려지는 것을 방지하는 프로토콜을 제공하고자 한다.

과제 해결수단

[0007] 본 발명의 제 1측면은 blinding factor(105)을 전송하는 단계를 포함하는 모델을 제공한다.

[0008] 또한, 본 발명의 제2측면은 challenge(105)를 로테이션 시키는 단계를 포함하여 중간자 공격을 방지하는 모델을 제공한다.

효 과

[0009] 본 발명에 따른 LPN 문제 기반의 안전한 경량 인증 프로토콜에 의하면,

[0010] 리더와 태그 사이의 통신에서 중간자 공격을 방지할 수 있는 경량 인증을 하는 것이 가능하다.

발명의 실시를 위한 구체적인 내용

[0011] 아래에서는 첨부한 도면을 참조하여 본 발명이 속하는 기술 분야에서 통산의 지식을 가진 자가 용이하게 실시할 수 있도록 본 발명의 실시 예를 상세히 설명한다. 그러나 본 발명은 여러가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시 예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설

명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

[0012] 본 발명의 일 실시 예에 따른 LPN 문제 기반의 안전한 경량 인증 프로토콜은 아래와 같은 과정을 포함한다.

[0013] 이하에서는 blinding factor(105), challenge(107) 의 로테이션을 포함하는 경량 인증 실시 예에 대해서 설명한다.

[0014] 도1은 본 발명의 일 실시예에 따른 LPN 문제 기반의 안전한 경량 인증 프로토콜을 도시한 도면이다.

[0015] 리더와 태그는 k비트 비밀값(101,102,103)과 성공확률변수(104)를 갖는다.

[0016] 본 발명의 일 실시예에서 첫번째 단계(S101)는 다음과 같은 과정을 포함한다.

[0017] (a) 태그는 임의의 k비트 blinding factor(105)를 생성한다.

[0018] (b) 태그는 리더에게 생성한 blinding factor(105)를 전송한다.

[0019] 이하에서 두번째 단계(S102)는 다음과 같은 과정을 포함한다.

[0020] (a) 리더는 challenge(107) 를 태그에게 전송한다.

[0021] (b) 태그는 blinding factor(105) 와 비밀값(101)의 XOR 연산(108) 수행을 통해 rotation factor(109)를 생성한다.

[0022] (c) 결과값(110)을 XOR 연산(108) 과 두번의 로테이션연산(111,112)수행을 통해 생성한다.

[0023] 이하에서 마지막 단계(S103)는 다음과 같은 단계를 포함한다.

[0024] (a) 태그는 응답으로 결과값(110)를 전송한다.

[0025] (b) 리더는 태그로부터 전송받은 결과값(110)과 자신이 연산한 결과값(113)을 비교한다.

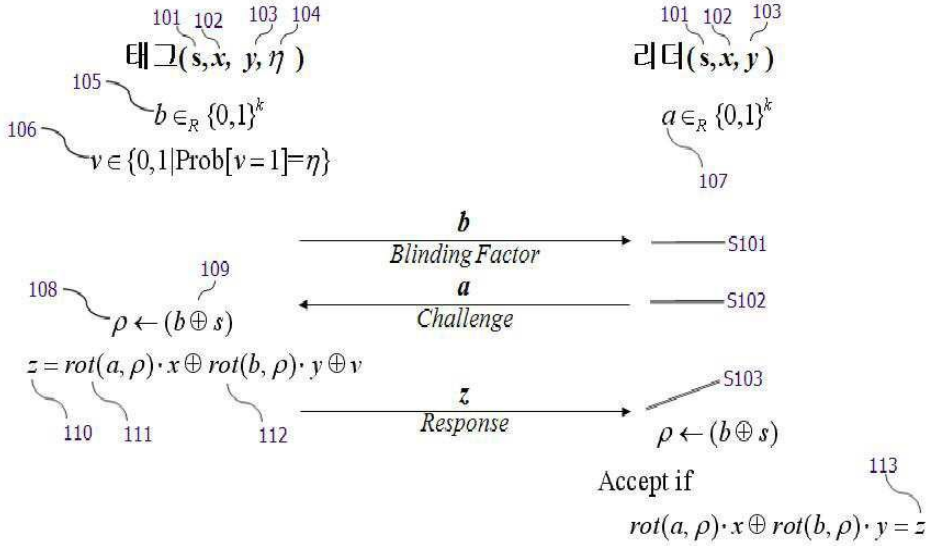
[0026] 이상에서 설명한 본 발명의 일 실시 예에 따르면 blinding factor(105)와 로테이션연산(111,112)을 사용하므로 중간자 공격을 방지하는 경량 인증이 가능하다.

도면의 간단한 설명

[0027] 도 1은 LPN 문제 기반의 안전한 경량 인증 프로토콜을 도시한 도면.

도면

도면1


101 102 103 104
태그(s,x, y,η)
105
b ∈R {0,1}^k
106
v ∈ {0,1|Prob[v=1]=η}
101 102 103
리더(s,x, y)
a ∈R {0,1}^k
107
b
Blinding Factor
S101
a
Challenge
S102
108
109
ρ ← (b⊕s)
z = rot(a, ρ)·x ⊕ rot(b, ρ)·y ⊕ v
110 111 112
z
Response
S103
ρ ← (b⊕s)
Accept if
113
rot(a, ρ)·x ⊕ rot(b, ρ)·y = z