(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2010-0121048
(43) 공개일자 2010년11월17일

(51) Int. Cl.
G06K 17/00 (2006.01) *H04L 9/18* (2006.01)
(21) 출원번호 10-2009-0040002
(22) 출원일자 2009년05월08일
심사청구일자 2009년05월08일

(71) 출원인
인천대학교 산학협력단
인천광역시 연수구 송도동 12-1, 11, 12번지
(72) 발명자
이병수
서울특별시 서초구 방배동 904-9
이귀봉
경기도 부천시 오정구 원종2동 211-1 현대아파트 가-209
(뒷면에 계속)
(74) 대리인
김태원

전체 청구항 수 : 총 4 항

(54) ＲＦＩＤ 태그와 리더기의 보안강화 시스템

(57) 요 약

본 발명은 RFID 태그와 리더기의 보안 강화 시스템에 관한 것으로, 특히 유비쿼터스 기술의 핵심으로 인식되고 있는 RFID의 적용분야가 넓어짐에 따라 보안에 대한 관심이 높아져 다양한 보안 기술이 연구되고 있으나 보안의 취약성으로 인해 위치추적 방지, 정보도용, 정품식별, 위폐식별, 도난방지 등이 보안요소의 장애요소로 분석되는데 이는 태그에 저장된 자료는 바코드가 일반인에게 읽혀질 수 있는 것처럼 구체적인 정보를 알 수 없어 크게 위협이 되지 않는다는 시각이다. 그러나 신분증이나 여권 등의 보안을 요구하는 곳에서는 태그 정보 자체가 보호되어야 한다. 본 발명은 이러한 보안의 취약성을 보완하기 위해 ECC 알고리즘을 적용한 RFID 태그와 리더기의 보안 강화 시스템에 관한 것이다.

대 표 도 - 도2

Time to break in MIPS year	RSA/DSA(bits)	ECC(bits)	Key size ratio
10^4	512	106	*5:1*
10^8	768	132	*6:1*
10^{11}	1024	160	*7:1*
10^{20}	2048	210	*10:1*
10^{78}	21000	600	*35:1*

(72) 발명자

이민순

인천광역시 남구 용현동 유원아파트 1동502호

김준환

인천광역시 남동구 간석4동 우성아파트 6동 802호

특허청구의 범위

청구항 1

신호를 송수신하는 안테나,

신호를 부호화하는 디코더를 포함하는 트랜시버,

단일식별정보를 갖도록 전자적으로 프로그래밍이 된 주파수 태그 형태의 트랜스폰더로 이루어지는 RFID 태그와 리더기 보안강화 시스템에 있어서,

상기 보안 강화 시스템의 패턴분석은 공개키의 기반 구조이며 이산대수 문제에 근거한 암호법인 ECC 알고리즘에 개선된 몽고메리 알고리즘을 적용한 것을 특징으로 하는 RFID 태그와 리더기 보안강화 시스템

청구항 2

제 1항에 있어서,

상기 ECC 알고리즘의 나눗셈 계산 시 가장 많은 자원과 시간이 필요하게 되는데 이를 해결하는 몽고메리 모듈러 곱셈 알고리즘은

입력은 x,y,P 이고, 출력 $S=Mongo(x,y)=xyR^{-1} \bmod P$라고 하면,

S=0

for I from 0 to k-1 do

$m_i = t_0 \wedge x_i * y_0$

$S=(S + xy + m_iP) /2$

end

(여기서 k는 피승수 y의 비트 사이즈이다)

인 것을 특징으로 하는 RFID 태그와 리더기 보안강화 시스템.

청구항 3

제 2항에 있어서,

상기 몽고메리 모듈러 곱셈 알고리즘의 결과 알고리즘은

Pre-Processing

$A^*=Mongo(A,2^{2k})=A^*2^{2k*}2^{-k} \bmod P=A^*2^k \bmod P$

$B^*=Mongo(B,2^{2k})=B^*2^{2k*}2^{-k} \bmod P=B^*2^k \bmod P$

Main-Processing

$S'=Mongo(A^*,B^*)=A^*2^{k*}B^*2^{k*}2^{-k} \bmod P=A^*B^*2^k \bmod P$

Post-Processing

$S=Mongo(S^*,1)=A^*B^*2^{k*}2^{-k}=A^*B \bmod P$

인 것을 특징으로 하는 RFID 태그와 리더기 보안강화 시스템.

청구항 4

제 1항에 있어서,

상기 RFID 태그는 내부 배터리로 전원을 공급받는 수동형 태그와, 판독기에서 전원을 공급받는 능동형 태

그로 나누어지는 것을 특징으로 하는 RFID 태그와 리더기 보안강화 시스템

명 세 서

발명의 상세한 설명

기 술 분 야

[0001] 본 발명은 RFID 태그와 리더기의 보안 강화 시스템에 관한 것으로, 특히 유비쿼터스 기술의 핵심으로 인식되고 있는 RFID의 적용분야가 넓어짐에 따라 상기 RFID 보안에 대한 관심이 높아져 다양한 보안 기술이 연구되고 있다. 그러나 열악한 자원 환경으로 보안 기술의 적용이 쉽지 않다. 이러한 보안의 취약성으로 인해 위치추적 방지, 정보도용, 정품식별, 위폐식별, 도난방지 등이 보안요소의 장애요소로 분석되는데 본 발명은 이러한 보안의 취약성을 보완하기 위해 ECC 알고리즘을 적용한 RFID 태그와 리더기의 보안 강화 시스템에 관한 것이다. 즉, 본 발명에서 RFID 에 ECC 알고리즘을 적용하는 방안의 구현은 경량화 RSA로 구현된 연구보다 강도 높은 암호 기법이 리더기와 태그에 적용 가능함을 제시하였다.

배 경 기 술

[0002] 일반적으로 RFID 는 소형 반도체 칩을 사용해 정보를 판독하는 인식 시스템으로서, 현대 사회의 다양한 분야, 즉 유통, 화물운송 등의 분야에서 광범위하게 사용됨에 따라 보안에 대한 관심이 높아져 이에 대한 다양한 보안 기술이 지속적으로 연구되고 있다. 상기 RFID 는 단순한 정보저장의 바코드 인식기술에 비해 원거리에서 다수의 제품을 한꺼번에 인식하여 많은 정보를 저장하는 장점과 함께 정보보호할 수 있는 장점이 있어 추후에도 유통, 화물운송 등에 많이 활용될 것으로 생각 된다.

[0003] 알려진 바와 같이 RFID 기술은 저주파(LF), 고주파(HF), 초고주파(UHF), 및 마이크로파(M/W) 대역의 무선 전파를 사용하여 단말기의 형태에 따라서는 고정형, 휴대형, 모바일형으로 분리되어 각각의 전파 특성에 따라 유통, 운송, 동물 위치관리, 교통카드, 제품관리, 위폐식별 등 여러 분야에 활용되고 있다.

발명의 내용

해결 하고자하는 과제

[0004] 본 발명의 RFID 보안기법에서 해결하고자 하는 첫 번째 과제는 태그와 리더 간의 양방향 데이터 전송에서 도청으로부터 정보가 보호되어야 한다는 것이다. 통상적으로 도청으로부터 정보를 보호하기 위해 일반적으로 알려진 트리워킹 도청 방지 기법을 사용하는데 상기 트리워킹 도청방지기법은 ID의 첫 번째 비트부터 시작하여 비트 단위로 태그를 구분해서 하나 씩 진행하여 하나의 태그를 선별하는 방법으로서, 태그가 보낸 실제 아이디와 리더가 보낸 난수 값이 동시에 전파되어 도청자 입장에서는 일부의 충돌로 인해 정확한 정보를 얻을 수 없는데 이러한 방법은 정보를 암호화해서 보내는 방법이 아니므로 태그와 리더 간의 동기화가 이루어 지지 않을 경우 도청자 ID의 태그를 직접 획득할 수 있다는 문제점이 있다.

[0005] 다음 두 번째로는 도청으로부터 정보를 보호하기 위해서는 보안기법 구현시 태그의 제한적인 자원을 활용하여 최소로 한정된 메모리 공간을 감안해야하는 것이다.

[0006] 세 번째로 강인하고 강력한 암호가 되도록 실시간 상호 작용을 위한 빠르고 신속한 암호 처리 속도가 필요하다는 것이다.

[0007] 네 번째로 정보를 보호하기 위해 태그 신호 간의 상호 간섭배제를 한다는 것이다.

[0008] 다섯 번째로 보다 강력한 암호가 되도록 도청정보를 이용하여 리더가 정당한 태그로 인증할 수 있는 새로운 값을 생성하는 것이 불가능해야 한다는 것이다.

[0009] 그러나 종래의 RFID 보안 기법 가운데에는 이러한 다섯 가지 요구사항을 모두 만족시키는 방법이 많지 않았다.

과제 해결수단

[0010] 상기와 같이 상술 된 다섯 가지의 과제 들을 해결하기 위하여 도청방지 기법을 적용하는데, 상기 도청방지 기법을 적용 위치별로 분류하면, 리더가 보내는 통신 전파를 도청하지 못하게 하는 포워드 채널 보호, 태그가 보내는 통신 전파를 도청하지 못하게 하는 백 워드 채널 보호가 있다.

[0011] 상기 포워드 채널 보호 방법은 리더의 신호가 멀리 전달되는 특성에 의한 도청의 가능성을 막기 위해 침묵 트리워킹, 난수 발생 트리워킹 등의 방식이 제안되었으며, 도청자의 위치에 따라 원거리 도청과 근거리 도청으로 나누어진다. 그런데 원거리에서 도청을 시도할 경우 리더가 태그에 보내는 질의는 도청 가능하지만 질의에 대한 태그의 응답은 신호가 약하기 때문에 도청하기 힘든 것으로 알려져 있다. 블라인드 트리워킹 알고리즘은 이러한 사실을 활용하여 포워드 보안을 개선한 방법이다. 이 방법을 사용하면 태그에 대한 ID 정보를 리더가 유출시키지 않으므로 포워드 채널에 대한 도청 방지 기능을 쉽게 제공할 수 있다.

[0012] 이에 비해 백 워드 채널 보호 방법은 근거리에 있는 도청자인 경우 태그가 최종적으로 보내는 실제 ID를 얻을 수 있기 때문에, 백 워드 채널에 대한 보안이 이루어 지지 않는데, 채널 보안을 위해 태그가 실제 ID를 전송할 때 리더가 동시에 임의의 난수 값을 전파시켜 도청자가 교란된 정보를 얻게 하는 방법이다. 이 방법은 정보를 암호화해서 보내는 방법이 아니므로 태그와 리더 간의 동기화가 이루어지지 않으면 도청자가 태그의 ID를 직접 획득할 수 있다는 단점이 있다.

[0013] 상술과 같이 다양한 RFID 보안기법을 통해 도청 문제를 해결하고자 하였지만 아직 까지는 여러모로 미비하다. 또한, 실용화 단계에서는 연산 능력과 메모리 공간 문제를 만족시키지 못했다. 이에 따라서 상기 과제를 해결하기 위하여 본 발명은 새로운 RFID 보안을 위하여 패턴 분석에 강력한 공개키 기반 구조인 ECC (Elliptic Curve Cryptography) 알고리즘 적용하였다. 일반적으로 차세대 공개키 암호 방법으로 주목받고 있는 ECC 알고리즘은 타원 곡선군의 이산대수 문제의 어려움에 근거한 암호법으로 Neal Koblitz 와 Victor Miller 에 의해 독립적으로 제안 되어진 알고리즘으로 공개키와 비밀키를 생성하는데 적용한다.

[0014] 상기 ECC 알고리즘의 장점은 실질적인 응용분야 특히 처리능력, 에너지 가용능력, 저장능력 등에 있어서 제한된 환경을 요구하는 경우에 매우 유리한 알고리즘으로서, 상기 ECC 알고리즘은 생성된 파라미터 즉 타원곡선 군에 포함되는 점들의 덧셈 연산을 통해 공개키와 메시지를 공유하고 비밀키를 동기화하는데 사용된다. 상기 ECC 알고리즘에서 뺄셈은 암호화된 메시지를 복원하는데 사용한다. 예를 들어 만약 메시지 KG와 임의의 메시지M 을 덧셈 연산하여 암호화된 메시지 KG+M 을 상대에 보냈다면, 암호를 도청하기 위한 공격자는 KG+M 을 도청하더라도 해석할 수 없고, 반면에 메시지를 수신한 수신자는 KG의 역원 -KG을 구하여 상대에게 보낸 메시지에 역원을 더하여 즉, (KG+M)-KG를 연산하여 M을 복원할 수 있다. 이때 KG의 역원 -KG를 구하는 수식은 타원곡선에 한 점이 X축으로 대칭이라는 원리를 이용하면 간단히 풀 수 있는 것이다. 한편, ECC 알고리즘에서는 복잡한 연산 없이 단지 덧셈 연산을 이용하여 공개키 생성과 비밀키 생성, 메시지 암호화, 복호화가 가능한 패턴분석에 강력하고 간편한 암호시스템을 구축할 수가 있다.

[0015] 상기 ECC 알고리즘의 뺄셈의 반복인 나눗셈 계산은 많은 자원과 시간이 필요하며 이를 해결하도록 몽고메리 알고리즘을 적용할 수 있는데 상기 ECC 알고리즘에 몽고메리 모듈러 곱셈 알고리즘을 적용한 식은 다음과 같다.

[0016] 입력이 x,y,P 이고 출력 $S=Mongo(x, y)=xyR^{-1} \bmod P$ 라고 하면 다음과 같이 정의 된다.

[0017] S=0

[0018] for I from 0 to k-1 do

[0019] $m_i = t_0 \wedge x_i * y_0$

[0020] $S=(S + xy + m_iP) /2$

[0021] end

[0022] (여기서 k는 피승수 y의 비트 사이즈이다)

[0023] 상기 몽고메리 알고리즘은 Y의 모든 비트에 대하여 몽고메리 알고리즘을 적용하면 결과 값 xy에 2^{-K} 의 작은 값이 출력되는 경우가 발생하는데 연산 후 올바른 값을 얻으려면 초기 좌표값에 2^{2K} 로 전처리를 하고 다음에 후처리 과정에서 1을 곱하여 $S=S*R \bmod P=S*2^{k} \bmod P$ 의 과정과 동일한 결과를 얻을 수 있고 쉬프트 연산에 비효율적인 연산을 제거할 수 있는 알고리즘이다.

[0024] 본 발명의 리더기 보안 강화 시스템의 상기 몽고메리 알고리즘의 구현 내용은 다음과 같다.

[0025] Pre-Processing

[0026] $A^{*}=Mongo(A,2^{2k})=A^{*}2^{2k*}2^{-k}modP=A^{*}2^{k}modP$

[0027] $B^{*}=Mongo(B,2^{2k})=B^{*}2^{2k*}2^{-k}modP=B^{*}2^{k}modP$

[0028] Main-Processing

[0029] $S'=Mongo(A^{*},B^{*})=A^{*}2^{k*}B^{*}2^{k*}2^{-k}modP$

[0030] $= A^{*}B^{*}2^{k} modP$

[0031] Post-Processing

[0032] $S=Mongo(S^{*},1)=A^{*}B^{*}2^{k*}2^{-k}=A^{*}BmodP$

[0033] 본 발명에 따른 RFID 태그와 리더기의 보안 강화 시스템은 기본적으로 안테나, 디코더를 포함하는 트랜시버, 단일식별정보를 갖도록 전자적으로 프로그래밍 된 주파수 태그 형태의 트랜스폰더로 구성된다. 여기서 상기 안테나가 트랜시버, 디코더와 결합하면 판독기로 불린다.

[0034] 상기 시스템의 패턴분석은 공개키의 기반 구조이며 이산대수 문제에 근거한 암호법인 ECC 알고리즘에 개선된 몽고메리 알고리즘을 적용한 것을 특징으로 한다. 또한, 본 발명 리더기 보안 강화 시스템은 상기 RFID 태그는 내부 배터리로 전원을 공급받는 능동형 태그와, 판독기에서 전원을 공급받는 수동형 태그로 나누어지는 것을 특징으로 한다.

효 과

[0035] 본 발명은 안전한 식별정보를 제공함으로써 RFID의 적용분야를 더욱 확대할 수 있다. 예를 들면 Passive 태그의 경우에 쇠고기 원산지를 추적하는 RFID 태그를 부착할 경우 쇠고기 진위 여부를 신뢰성 수준에서 조사할 수 있으며, 각종 농산물에 부착하여 유통 경로를 추적하여 수입산과 국내산의 판정도 정확히 할 수 있다. 종래의 RFID 역시 원산지 추적할 수 있지만 태그의 위변조로부터는 자유롭지 못하다. 이에 따라서 Active 태그의 적용분야는 추적을 원하지 않는 여권 또는 신분증 등에 적용함으로써 개인 프라이버시를 보호할 수 있는 효과가 있어 가까운 미래에 널리 활용될 수 있을 것으로 기대된다.

발명의 실시를 위한 구체적인 내용

[0036] 이하 도면을 참조로 본 발명에 대해 상세히 설명한다.

[0037] 도 1은 본 발명의 위치에 따른 도청 방지 기법을 나타내는 도면이다.

[0038] 도시된 바와 같이 적용위치 별로 분류하면 포워드 채널과 백 워드 채널이 있다. 포워드 채널보안은 리더가 보내는 통신 전파를 도청하지 못하게 하고 백 워드 채널보안은 태그가 보내는 통신전파를 도청하지 못하게 한다.

[0039] 본 발명에서는 리더와 태그를 중심으로 종래의 정보보호 기법인 트리워킹을 살펴보고 도청 측면에서 기존의 RFID 보안 기법과 ECC 알고리즘을 적용한 후 적용방안을 제시한다.

[0040] 통상 태그는 패시브(Passive) 태그와 액티브(Active) 태그로 분류할 수 있는데 패시브 태그는 고정된 공개키를 가지고 정품을 구별하거나 유통경로를 추적관리에 적용할 수 있으며 특성상 제조단계에서 키를 확정하나 위치 추적에는 취약하며 액티브 태그는 랜덤화된 트리 워킹으로 공개키를 보호하며 난수에 의한 가상의 공개 키로 위치 추적에서 벗어나며 공개키는 가상태그 정보가 된다. 실제 태그정보는 비밀키로 암호화된다.

[0041] 상기 트리 워킹 방식들의 공통점은 비트 단위로 태그를 구분한다는 것이다. 상기 트리워킹에는 포워드 채널 보호 방법과 백 워드 채널보안이 있는데 1)포워드 채널 보호 방법은 침묵 트리워킹(Silent Tree Walking), 도청자 리더의 트리 워킹을 방해하는 방해자 태그, 블라인드 트리워킹(Blinded Tree Walking)알고리즘, 태그가 자신의 실제 ID가 아닌 난수 값을 이용하여 생성한 가상 ID로 응답하는 랜덤화 트리워킹이 있다. 2)백 워드 채널 보안에는 태그가 실제 정보를 전송할 때 리더가 교란된 정보를 제공하고 충돌이 발생한 비트 재생 불가로 백 워드 보안을 유지하며 태그와 리더 간의 동기화가 이루어지지 않을 경우 도청자가 태그의 ID를 직접획득 가능하다.

[0042] 도 2는 공개키 암호방식인 RSA/DSA의 방식과 본 발명에 적용하는 ECC 알고리즘 방식의 차를 나타내는 도면으로서 동일 안전도에서 타원곡선에 대한 도메인 변수 크기를 비교하는 도면이다. 나타난 바와 같이 10^{11} 을 예로 들

면 RSA/DSA 가 1024비트인 경우에 ECC는 160비트로서 키 사이즈 비(Key size ratio)에서 대략 7:1이 되는 것을 알 수 있다. 즉 ECC 알고리즘이 7배 정도 우수하다 할 수 있다. 상기 ECC 알고리즘은 타원곡선 군의 이산대수 문제의 어려움에 근거한 암호법으로서 실제 적용에서는 몽고메리 모듈러 연산 알고리즘을 적용하여 암호화를 한다.

[0043] 본 발명에서 실제 암호화 처리를 위한 개선된 몽고메리 모듈러 연산 알고리즘은 다음과 같다.

[0044] Pre-Processing

[0045] $A^{*}=Mongo(A,2^{2k})=A^{*}2^{2k*}2^{-k}modP=A^{*}2^{k}modP$

[0046] $B^{*}=Mongo(B,2^{2k})=B^{*}2^{2k*}2^{-k}modP=B^{*}2^{k}modP$

[0047] Main-Processing

[0048] $S'=Mongo(A^{*},B^{*})=A^{*}2^{k*}B^{*}2^{k*}2^{-k}modP$

[0049] $= A^{*}B^{*}2^{k} \ modP$

[0050] Post-Processing

[0051] $S=Mongo(S^{*},1)=A^{*}B^{*}2^{k*}2^{-k}=A^{*}BmodP$

산업이용 가능성

[0052] 본 발명은 RFID 정보보호 분야에 사용될 수 있다.

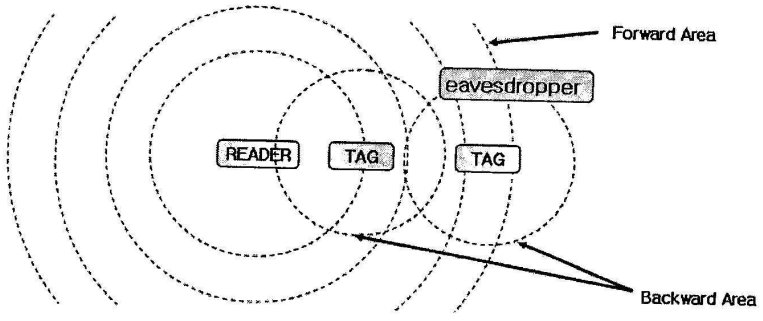
도면의 간단한 설명

[0053] 도 1은 본 발명의 위치에 따른 도청 방지 기법을 나타내는 도면이다.

[0054] 도 2는 공개키 암호방식인 RSA/DSA의 방식과 본 발명에 적용하는 ECC 알고리즘 방식의 차를 나타내는 도면이다.

도면

도면1



도면2

Time to break in MIPS year	RSA/DSA(bits)	ECC(bits)	Key size ratio
10^4	512	106	*5:1*
10^8	768	132	*6:1*
10^{11}	1024	160	*7:1*
10^{20}	2048	210	*10:1*
10^{78}	21000	600	*35:1*