타원곡선 좌표계를 이용한 RFID 다중객체 간 인증 암호기법

RFID Authenticated Encryption Scheme of Multi-entity by Elliptic Curve's Coordinates

김 성 진* 박 석 천**
Sung-Jin Kim Seok-Cheon Park

요 약

RFID 보안에 있어서 인증암호기법은 태그 정보 보호에 있어서 중요한 요소기술이다. 그러나 인증 암호 기법을 RFID 시스템의 제한적인 컴퓨팅환경에서 구현하는 것은 쉬운 문제가 아니다. 제한적인 컴퓨팅환경은 곧 보안을 구현하기 위한 메모리의 크기제한, 보안기법의 구현상의 복잡성과 전원공급의 제한 등의 문제를 의미한다. 본 논문에서는 EC(Elliptic Curves)의 x-좌표값과 스칼라 연산을 이용한 새로운 인증 암호 기법을 제안하였다. 제안 기법에서 타원곡선의 논리합과 논리곱 연산을 통해 보안 능력을 향상하여 악의적인 공격으로부터 개인정보를 보호할 수 있다.

ABSTRACT

Authenticated Encryption scheme in RFID system is the important issue for ID security. But, implementing authenticated Encryption scheme in RFID systems is not an easy proposition and systems are often delivered for reasons of complexity, limited resources, or implementation, fail to deliver required levels of security. RFID system is so frequently limited by memory, performance (or required number of gates) and by power drain, that lower levels of security are installed than required to protect the information. In this paper, we design a new authenticated encryption scheme based on the EC(Elliptic Curve)'s x-coordinates and scalar operation. Our scheme will be offers enhanced security feature in RFID system with respect to user privacy against illegal attack allowing a ECC point addition and doubling operation.

☞ keyword : RFID, Elliptic Curves, Encryption, Security, ECNR, Authentication

1. 서 론

RFID 시스템은 언제, 어디서, 어떤 장치를 통해서든지 정보를 교류할 수 있는 유비쿼터스 환경에서 다양하게 활용될 수 있다. 이러한 RFID 시스템의 구성 요소 중에서 특히, 태그는 기존 바코드를 대체하여 다양한 영역에서 응용될 수 있으며, 현재, 태그시장에서 저가의 수동형 태그가 90%이상을 차지하고 있다. 이러한 저가의 소규모 RFID 태그를 통해 정보를 전송함에 따라 전송정보 보호에 많은 문제점이 있다. 특히, 불법적인 공격자를 통해 전송되는 정보의 보호를 위한 대응은 미흡한 실정이다.

그러나, RFID 태그의 제한적인 환경(즉, 메모리 제한, 하드웨어 구현의 문제와 전력소모)상에 기존의 암호기법의 적용은 매우 어려운 문제다.

따라서, 본 논문에서는 RFID 태그에서의 메모리 소비는 최소화하고, 전체 RFID시스템상의 보안은 강화할 수 있는 상호인증 기법을 제안하고자 한다. 제안 기법은 수정된 ECC(Elliptic Curve Cryptosystem)과 타원곡선상의 한 x-좌표값을 이용하여 RFID 태그 내 에 적용할 수 있도록 처리량을 최소화할 수 있도록 설계하였다. 제안 기법을 통해 공격자의 불법공격으로부터 정보보호 및 태

* 정 회 원 : 성남산업경제연구센터 선임연구원
sjnetk@hotmail.com(주저자)
** 종신회원 : 경원대학교 소프트웨어학부 정교수
scpark@kyungwon.ac.kr(교신저자)
[2007/08/16 투고 - 2007/08/27 심사 - 2008/02/11 심사완료]

그 내 보안모듈의 경량화로 현실적인 구현을 기대할 수 있다.

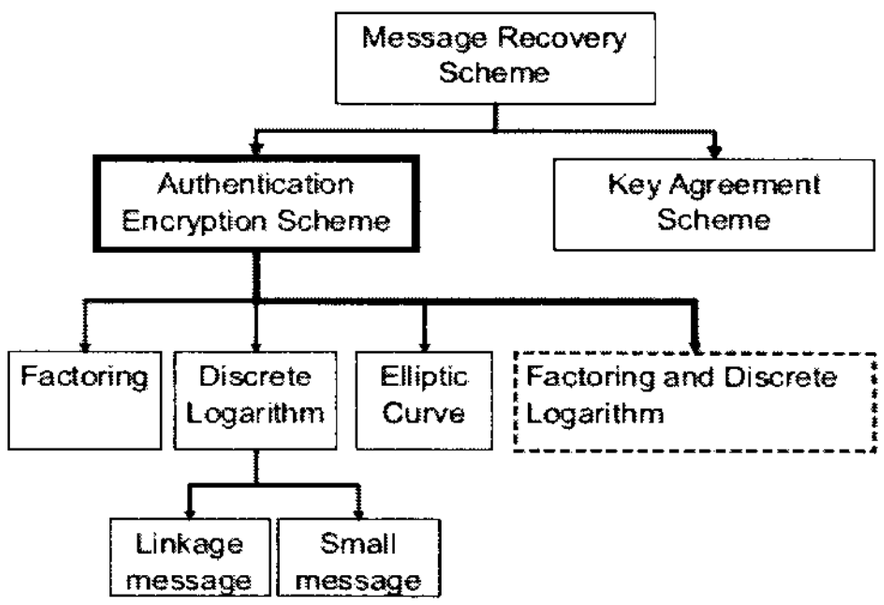
2. 관련연구

본 장에서는 기존의 인증 암호 기법 분류와 연구방향에 대해 제시하였다.

2.1 인증 암호 기법 분류

그림 1은 기존의 인증 암호 기법에 대한 분류를 나타내고 있다[1]. 메시지 복구 기법의 응용은 크게 인증 암호 기법과 키 분산 기법으로 나눠진다.

인증 암호 기법은 다시 네 가지 분류로 나눠진다. 첫째, 인수분해 난해성 문제 둘째, 이산대수문제 셋째, 타원곡선문제 넷째, 인수분해와 이산대수 문제의 복합 문제. 이산대수문제는 다시 일반적인 메시지 길이 문제와 연결 메시지와 작은 메시지 문제로 분류된다.



(그림 1) 인증 암호 기법 분류

2.2 연구 방향

기존의 관련연구로 이산대수, 인수분해, 타원곡선 등의 이산 수학의 어려운 해법에 기반을 둔 인증 암호 기법 연구[2, 3]와 인증 암호 기법에 적합한 설계를 위해 큰 메시지의 연결이나 메시지 흐름을 위한 메시지 연결 기법이 있으며[4, 5], (t, n) 공개키를 이용한 인증 암호 기법이 있다[6, 7].

본 논문에서는 RFID 시스템의 인증 암호 기법의 연구 방향을 다음과 같다.

1) 실제적인 구현에서 서명자는 메시지를 서명할 수 없고, 대리자가 서명한다.
2) RFID 통신 환경에서 짧은 컴퓨팅 시간은 성능에 많은 영향을 준다. 이는 전송시간과 비용을 고려해야 하기 때문인데, 인증 암호 기법에서 컴퓨팅에 소요되는 시간은 더더욱 비용을 증가하기 때문에 효율적인 암호 기법이 요구되는 것이다.
3) 타원곡선 암호 기법은 다른 암호 기법에 비해 효과적인 성능을 발휘한다. 전통적인 공개키 기반의 암호 기법보다 짧은 키 사이즈로 대등한 안전도를 보이고 있다. 예를 들어, ECC 160 비트 키의 암호 기법은 RSA 1024 비트 키가 갖는 암호 방식과 대등한 안전도를 가진다는 것이다. 따라서 공개 키 암호 방식에 적용될 경우 속도를 획기적으로 줄일 수 있어 무선 인터넷을 비롯한 IC 카드 등의 암호 활용에 효과적인 대안이 될 수 있다. 하지만, 현실적으로 태그 내에 암호기능을 내장하기위해서는 보다 경량화된 타원곡선암호기법이 요구된다.

본 논문에서는 타원곡선 암호 기법을 세부적으로 다시 분류하고, RFID 시스템에 적용 가능한 개선된 타원곡선 인증기법을 제안하고, 보안 분석과 성능 분석을 통해 제시한 기법의 성능에 대해 평가하였다.

2.3 타원곡선 암호 기법 분류

모든 디지털 ECC 신호 기법에서는 신호생성을 위해 비밀키(개인키)를 이용하여 메시지를 암호화하여 메시지 암호문을 만들다. 이때, 해시함수와 같은 암호화함수를 사용하게 된다. 암호문은 수신

측에서 공개키를 이용하여 복호화를 수행한다. 수신측에서 공개키를 검증하여 적합하지 않을 경우 수신이 취소된다. 이러한 인증 기법을 다시 분류하면 메시지 복원기법과 메시지 추가 기법으로 분류할 수 있다[8].

2.3.1 메시지 복원 기법

이 방식은 전송하고자 하는 메시지를 암호화하고 이를 복호화하는 기법으로 이 방식에는 EDCSA(Elliptic Curve Digital Signature Algorithm), ECGDSA(Elliptic Curve German Digital Signature Algorithm) 기법이 있다.[8] 이 기법의 처리 방식은 그림 2의 ECDSA 신호 기법과 같다.

Input : domain parameter
private key d
hashfunction h message m
Output : signature(r,s)
1. k = rand(1, n-1)
2. $R = k \cdot p$ $r = R_x \bmod n$
3. $s = k^{-1}(h(m)+d \cdot r) \bmod n$
4. if $r \vee s = 0$ goto 1
5. return(r,s)

(그림 2) ECDSA 신호 기법

2.3.2. 메시지 추가 기법

이 방식은 신호와 함께 여분의 메시지를 같이 전송하여 메시지 복원에 이용하는 방식으로 ECMR((Elliptic Curve Miyaji message recovery signature), ECNR(Elliptic Curve Nyberg-Rueppel message recovery signature) 기법이 있다. 또한 이 방식에서는 전송하고자 하는 메시지가 수신측에서 받아서 복구하기에 큰 메시지일 경우에는 나머지 잔여 메시지에 대해서는 잉여 신호 비트로 처리한다. 이 기법의 처리 방식은 그림 3의 ECNR 신호 기법과 같다.

Input : domain parameter
private key d
message with redundancy M
Output : signature(r,s)
1. k = rand(1, n-1)
2. $R = k \cdot p$ $\Pi = R_x$
3. r = (M + Π)mod n
4. s = (k - dr)mod n
5. return(r,s)

(그림 3) ECNR 신호 기법

ECNR 신호 방식에서 신호의 생성은 ECDSA와 유사하나 2 단계에서 Rx가 복구가능한 메시지로 변경되었고, 단계 4에서 신호 s도 모듈라 역(inversion)연산에 가장 많은 비용이 소요되기 때문에 이를 줄이기 위해 수정되었다. 실제 에너지 소비량을 비교하면 역산을 사용하지 않은 타원곡선 암호기법(ECGDSA, ECNR)에서 40%정도의 에너지 소비 효율이 있었다[8]. 역연산을 배제한 방식들의 공통점은 신호 생성단계에서 각 타원곡선 점에 대해 한 번의 스칼라 곱셈을 수행하고, 신호 검증 단계에서 두 번의 스칼라 곱셈을 수행함으로써 연산 오버헤드를 줄이고 있다. 타원곡선을 이용한 인증기법들의 성능의 차이는 곧 스칼라 계산 및 처리의 효율을 의미한다. 따라서, 효과적인 스칼라 연산의 구현이 필요하며, 태그 내 메시지(m)를 암호화하기 위해 해싱함수를 포함해야하는 문제점을 가지고 있어 이에 대한 개선이 필요하다.

3. 다중객체간 인증 암호 기법 제안

본 장에서는 Ⅱ장에서 연구방향을 중심으로 타원곡선 알고리즘을 이용한 다중객체(다중 리더 및 태그장치)간 인증 암호 기법을 제안하였다.

본 장에서는 제한적인 통신자원을 가진 모바일 기기 내에서 구현하기에 위한 적합성과 보안의 강화를 동시에 충족하도록 그림 4와 같이 설계하였다.

설계의 기본 기법은 연산에 따른 오버헤드를 최소화하기 위해 역산을 줄이는 ECNR기법을 응용하고 전송량을 줄이고 보안을 유지하기 위해 태그 내 연산에는 x-좌표값 만을 사용하였다. 암호화 제안기법의 근간이 되는 ECNR기법의 각 단계별 동작은 RFID 시스템 구성요소별 처리능력을 고려하여 그 역할을 재배치하였다. 제안된 기법을 설명하기 위해

다음 표 1과 같이 약어를 정리한다.

(표 1) 약어정리

Symbol	Quantity
SA	System Authority
E	Elliptic Curve over the field F_2^m defined by a and b
r, q	Prime order of E
PRNG( )	Pseudo-Random Number Generator
a, b	Elements of F_q that define an elliptic curve E over F_q
g	base point or generator of GF(p)
r	The order of filed
Pub	Elliptic Curve public key
p	large prime such that p-1 has a large prime factor with order q in the Galois's field GF(p)
P	An EC point
P_x	The x-coordinates of a point P
$\|P\|$	The size of a point P
m	message

본 논문에서 제안하는 인증 암호 기법의 기본 아이디어는 다음과 같다. 첫째, 전체 연산 비용을 최소화하기 위해 역(inverse)산을 제한하고, 둘째, 태그의 연산량과 공간을 최소화하기 위해 기저점 좌표계중 x-좌표값만을 연산에 활용하였다. 또한, 타원곡선 알고리즘을 활용하여 보안은 강화할 수 있도록 구성하였다. 제안기법은 초기셋업 후 키생성 및 검증, 신호생성 및 신호 복구의 세 가지 단계를 두어 설명하였다.

3.1 키 생성 및 검증 단계

키 생성단계에서 구성 요소인 SA, 태그, 리더 중에서 SA로 인증 암호 기법과 관련된 기능을 집중하고 최종 단말인 태그에서는 최소 기능으로 운영하도록 구성하였다. 또한, 태그의 연산 기능을 최소화한 보안상의 공백은 SA를 통한 정기적 키 업그레이드로 보안을 강화한다. 처리단계는 다음과 같다. 우선 SA에서 키성성 단계는 ECNR 프로토콜을 기반으로 타원곡선의 요소값을 선정한다. 즉, 타원곡선(E), 차수가 되는 소수(r, q) 및 타원곡선 방정식의 계수(a, b)를 선정한다. 태그와 리더 사이에서 비밀키를 각각 생성하고 이를 조합하여 공개키(Pub)를 생성한다. 즉, 리더가 태그에 접속을 원하면 리더는 먼저 랜덤값 s($\in$[1, n-1])를 선택하고, SA로부터 소수값 r, q를 받아 태그로 리더의 개인키 Rpri를 구하여 기저점 G와 함께 전송한다. 태그는 G를 받아 태그의 개인키 Tpri를 구한다.

Tag	Reader	SA
Setup k = rand(1, n-1) ←	s = rand(1, n-1) ←	Generate E, r, q
	Generate g	
Key-gen. $T_{pri} = g^k \pmod q$ Pub $P = g^{k+s} \pmod q$	$R_{pri} = g^s \pmod q$	
Sign. $c = m \cdot P_x$ →	Pub $P = g^{k+s} \pmod q$ Check $P \in E(F_2^m)$ $d = -k - sc \pmod r$	
	→	**Verify.** $m = cg^d R_{pri}^c \pmod q$

(그림 4) 제안 기법

3.2 신호 생성 단계

키생성 및 검증 단계를 거친후 태그는 공개키(Pub)를 구하여 메시지 m과 모듈라 곱연산($c = m \cdot P_x$)을 수행함으로써 메시지를 암호화 한다. 이때 사용되는 암호화된 신호 생성 연산은 그림 4와 같이 태그의 연산비용을 줄이기 위해 right-shift연산과 point-double 연산을 이용하여 설계하였다. 연산에 사용되는 요소중 Px(P의 x좌표값)과 m를 스칼라 곱연산을 수행하여 암호화 한다. 이때, P를 n개의 비트로 구성할 경우 전반부 n/2개는 x 좌표로 후반부 n/2개는 y좌표로 인식한다. 따라서, 그림 5에서 Px의 갯수가 n/2개보다 클 동안 쉬프트 연산을 수행하게 된다. 이 과정을 통해 메시지(m)을 전체 n/2개만큼 스칼라 합 연산으로 암호화한다. 쉬프트 연산을 통해 소실되는 P의 후반부 n/2의 자리수 값, 즉, P의 y좌표값은 리더에서 얻을 수 있다.

```
Input : integer m, point |P|x ∈E(F2^m)
Output : m · Px
Q ← ∞  /* identify element  */
while |P| < n/2 do
  Q ← Q + P
  P ← ⌊P/2⌋  /* right shift by one */
  m ← 2m
     /* using a point doubling method */
end
return Q
```

(그림 5) 태그의 신호 생성

스카라 곱연산($m \cdot Px$)을 수행한 후, 계산된 신호(c)를 리더로 전송한다. 리더는 정보(c)를 이용하여 태그의 x좌표와 리더의 y좌표를 조합하여 공개키 P를 계산하여 타원곡선(E(F2m))위의 좌표값인지를 검증한다. 검증이 완료되면 리더는 다시 태그의 랜덤값(k)와 태그 비밀키(c) 그리고 리더의 랜덤값 (s)와 SA의 소수값(r)를 이용하여 $d = -k\text{-}sc \pmod r$를 구하고, 태그에서 생성되는 x-좌표값 c와 리더에서 생성되는 y-좌표값 d의 조합으로 구성된 좌표값(c,d)를 SA에 전송한다.

3.3 메시지 복구 및 검증 단계

SA는 (c, d) 받아 $m = cg^dR_{pri}^c \pmod q$를 연산을 통해 메시지를 복구한다. 이때, $cg^dR_{pri}^c = mg^{kg^{-k}g^{-sc}g^{sc}} = mg^{k\ k\ sc+sc} = m$과정을 거쳐 메시지 m을 검증한다. SA에서 메시지 복구 방식은 기존 복호화 방식에서 사용하던 역(inverse) 연산을 통한 계산 비용을 줄이고, 복호화의 시간을 단축하였다.

4. 성능평가

Ⅳ장에서는 제안한 프로토콜의 보안 및 성능 측면에서 성능평가를 하였다.

4.1 보안 분석

데이터 기밀유지(Data confidentiality) 및 인증(Authentication) 측면에서 보안성에 대해 분석하였다.

4.1.1 데이터 기밀성

제안 프로토콜은 실제메시지가 전송구간에서 불법적인 도청 및 감청에 의해 노출되지 않도록 설계하였다. 비안전구간(insecure ranges)인 태그-리더 간에 전송에서는 공개키 기반의 암호 방식을 적용하여 메시지 전송시 발생되는 불법 공격으로 보안을 유지하였다.

만약, 태그와 리더간에는 $|P|_x$을 통해 일차 키 생성의 유해성 여부를 검사하고 리더와 SA간에 신호생성 유효성을 확인한 후, 메시지를 리더로 알리게 되므로 데이터 기밀성이 보장된다. 또한, 제안 기법은 ECNA 암호 기법에 기반을 두고 태

그와 리더의 개인키 k, s와 기저점 g를 이용하여 만든 공개키을 통해 메시지를 암호화하였기 때문에 공격자에 공격으로부터 데이터의 기밀성을 보장할 수 있다. 또한, 공격자에게 비안전구간상에 데이터 c가 노출되더라고 c 값을 통해 메시지(m)을 복원하기 위해서는 기저점(g), 리더의 개인키(k), 리더의 개인키(s), SA의 소수(q)값을 필요하기 하며, 무엇보다도 P_y 좌표값을 얻을 수 없기 때문에 원본 메시지(m)의 복원이 불가능하다.

4.1.2 데이터 인증

제안 기법은 무선 단말태그에서 개인키(k)와리더의 개인키(s) 및 기저점(g)를 곱하여 공개키를 생성하고, 생성된 공개키의 x-좌표값을 리더에 전송하고, 리더는 이를 받아 전송된 공개키가 GF(p)에 속하는지를 1차 검사하여 데이터의 유효성을 확인하여 데이터를 인증하게 된다. 또한, 태그부터의 x-좌표값(c)과 리더로부터 y-좌표값(d)를 값을 SA로 전송하면 SA는 전송된 값이 $cg^dw^c = m'g^{kg^{-k}}{}^{sc}g^{sc} = m'g^{k-k-sc+sc} = m'$ 값이 같은지를 검사하여 2차 인증과정을 거쳐 최종 (c, d) 좌표값이 매칭되는 메시지를 찾게 된다. 따라서, 두 번의 인증과정을 거치게 된다.

4.2. 성능 분석

이 절에서는 성능평가를 위해, 컴퓨팅 시간분석을 통해 제안기법의 성능을 분석하였다.

특히, 시스템의 성능 평가 대상은 태그내의 연산으로 하고, 성능 평가 대상은 암호화에 소요되는 계산 비용을 사용하였다.

계산 비용 산출을 위해 아래의 표 2와 같은 약어로 정의하고 제한적인 컴퓨팅 자원을 가지고 있는 태그에서의 계산 비용을 중심으로 산출하였다. 본 논문에서 제시하는 태그의 연산식은 키생성에 필요한 공개키(T_{pub}) 생성비용과 암호화에 필요한 신호(c)생성 비용으로 나눌 수 있다.

(표 2) 성능평가 인자 약어표

약어	소요시간
T_{mul}	스칼라 곱연산 시간
T_h	해시연산 시간
T_{exp}	모듈러 P에 따른 누승연산 시간
T_{inv}	모듈러 P에 따른 역연산 시간
T_{ec_mul}	타원곡선상의 곱연산 시간
T_{ec_add}	타원곡선상의 합연산 시간
|p|	소수 p의 비트 크기
|h|	해시함수의 처리 비트 크기

공개키 생성 비용은 태그의 개인키(g^k)과 리더의 개인키(g^s)의 스칼라 곱연산 소요되는 시간으로 k, s 값은 각각 n-1보다 작기 때문에 전체 소요시간은 $g^{(k+s)}$로서 k+s 의 연산량은 $2^{(n-1)}T_{ec_mul}$를 넘지 않는다. 신호생성 시간은 공개키 사이즈의 1/2 크기 동안 반복적으로 스칼라 합과 곱 연산을 수행하는 시간으로 $n/2 \times (T_{ec_add} + T_{ec_mul})$과 같다. 따라서 제안기법에서 태그에서 연산시간은 다음 식(1)과 같다.

$$\Pr oposed_{Tag}\cos t \le \frac{n}{2}T_{ec-add} + 2^{n-2}nT_{ec-\mu l} \text{ --- (1)}$$

표 3에서는 제안기법의 태그 연산 비용과 신호생성시간을 기존 타원곡선 적용기법인 TH_ECC 프로토콜[9]과 비교하였을 때 산술적으로 제안 기법은 TH_ECC기법에 약 50% 의 연산 비용으로 통해 메시지를 암호화할 수 있다.

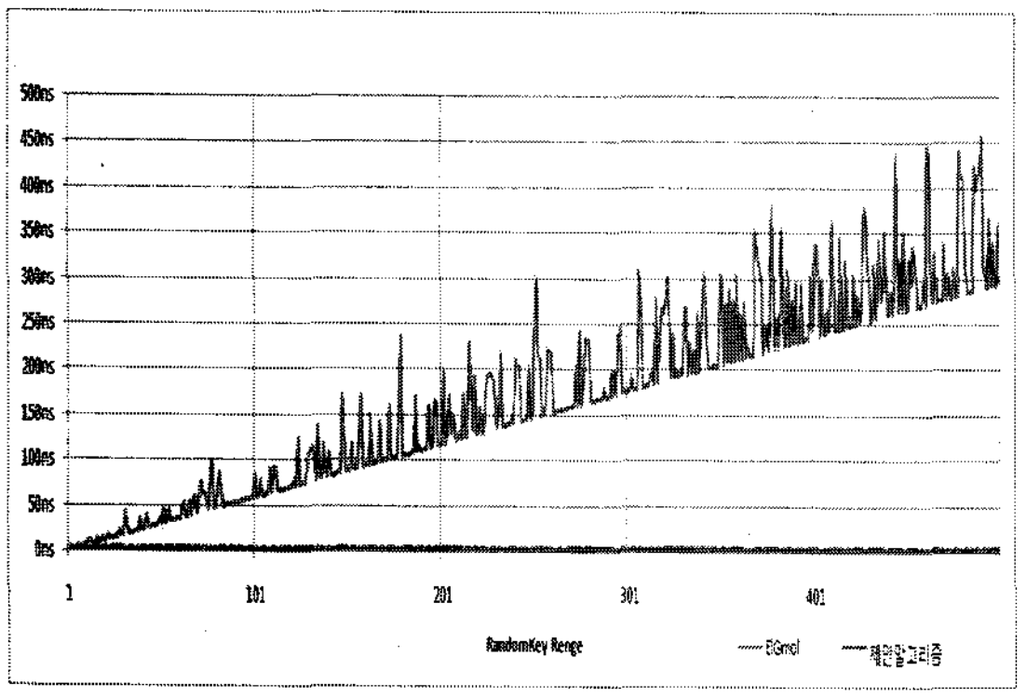
(표 3) 제안기법 연산 비용 및 시간비교

프로토콜	연산비용	신호생성시간
TH_ECC	$(n+1)\|p\|+\|h\|$	$2T_{ec\_mul}+T_{ec\_add}+T_{mul}+(n+1)T_h$
MEECC	$\frac{(n+1)}{2}\|p\|$	$\frac{n}{2}T_{ec-add}+2^{n-2}nT_{ec-mul}$

제안기법의 성능 개선을 평가를 위해 논 논문에서는 기존의 타원곡선기법인 ElGamal 기법[10]

과 제안기법의 공개키생성 속도를 그림 6과 같이 비교하였다.

시험 결과를 통해 x축을 랜덤키의 크기로 하고, y축을 소요시간으로 할 경우 ElGamal 방식은 랜덤키 값이 증가할수록 스칼라곱에 비례하여 계산 시간이 현저히 상승하였고, 제안방식에서는 랜덤키 값에 상관없이 일회의 더하기 연산을 수행하므로 약 3ns의 속도가 일정함을 확인하였다.



(그림 6) 공개키 생성 추이

따라서, 태그 구현시에 소비전력을 줄이고 연산 속도에 향상 효과를 기대할 수 있다.

5. 결 론

본 논문에서 제안한 기법은 타원곡선 기반의 암호 기법으로 RFID 시스템에 구현할 수 있도록 보안을 위한 연산량을 경량화 하였으며, 태그 보안 구현을 위해 보안 함수와 암호 메시지 전송 사이즈를 50%로 경량화 하였고, 보안 강도를 강화하기 위해 타원 곡선 기반으로 인증 암호 기법으로 짧은 연산시간과 효과적인 연산비용을 통해 태그에 보안 강화와 구현시의 효율성을 대응할 수 있기를 기대한다. 향후 태그의 보안모듈을 현재기술 범위에서 상용화가 가능한 3,000게이트이하의 보안 모듈을 설계하고자 한다.

참 고 문 헌

[1] Min-Shiang Hwang and Chi-Yu Liu, "Authenticated Encryption Schemes: Current Status and Key Issues," International Journal of Network Security, Vol.1, No.2, PP.61 - 73, Sep. 2005.

[2] C. Ma and K. Cheng, "Publicly verifiable authenticated encryption," IEEE Electronics Letters, vol. 39, no. 3, pp. 281 - 282, 2003.

[3] T. S. Wu and C. L. Hsu, "Convertible authenticated encryption scheme,"The journal of Systems and Software, vol. 39, no. 3, pp. 281 - 282, 2002.

[4] B. H. Chen, "Improvement of authenticated encryption schemes with message linkages for message flows,"Computers and Electrical Engineering, vol. 30, no. 7, pp. 465 - 469, 2004.

[5] C. L. Hsu, T. S. Wu, and T. C. Wu, "Improvements of generalization of threshold signature and authenticated encryption for group communications," Information Processing Lettes, vol. 81, no. 1, pp. 41 - 45,2002.

[6] C. L. Hsu and T. C. Wu, "Authenticated encryption scheme with (t, n) shared verification," IEE Proceedings 20, 1998. Computers and Digital Techniques, vol. 145,no. 2, pp. 117 - 120, 1998.

[7] J. Z. Lu and H. Y. Chen, "Improvement of authenticated encryption scheme with (t, n) shared verifica-tion," in Computer Software and Applications Con-ference, 2000. COMPSAC 2000. The 24th Annual International, pp. 445 - 448, Oct. 2000.

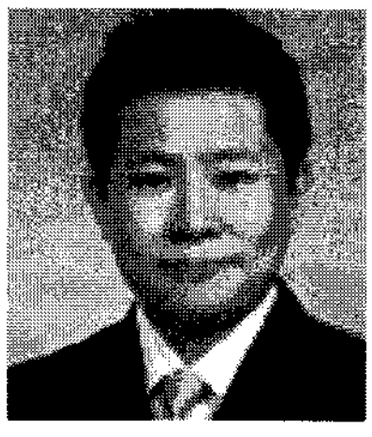
[8] J. Z. Lu and H. Y. Chen, "Improvement of authenticated encryption scheme with (t, n) shared verifica-tion," in Computer Software and

Applications C. Ruland and T. Lohmann, "Digital Signatures Based on Elliptic Curves in RFIDs," IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.1, January 2007.

[9] Sungjin Kim, Seokcheon Park, "RFID Security Protocol by Lightweight ECC Algorithm." ALPIT, Volume 6, August 2007

[10] Y. Tsiounis and M. Yung, "On the security of ElGamal based encryption," In PKC'8, pp. 117-34, 1998.

◐ 저 자 소 개 ◑



김 성 진(Sung-Jin Kim)

1996년 : 서경대학교 컴퓨터과학과(공학사)
1998년 : 경원대학교 대학원 전자계산학과(공학석사)
2008년 : 경원대학교 대학원 전자계산학과(공학박사)
1999년 ~ 2007년 : 서울현대전문학교 컴퓨터정보학과 교수
2007년 ~ 현 재 : 성남산업경제연구센터 선임연구원
관심분야 : 유비쿼터스 컴퓨팅, RFID, 정보보호
E-mail : sjnetk@hotmail.com

박 석 천(Seok-Cheon Park)

1977년 : 고려대학교전자공학과 학사
1982년 : 고려대학교 대학원 컴퓨터공학 석사
1989년 : 고려대학교 대학원 컴퓨터공학 박사
1979년 ~ 1985년 : 금성통신연구소
1991년 ~ 1992년 : University of California, Irvine Post Doc.
1988년 ~ 현 재 : 경원대학교 소프트웨어학부 정교수
관심분야 : 모바일 통신, 유비쿼터스 컴퓨팅, 정보보안, USN
E-mail : scpark@kyungwon.ac.kr