모바일 RFID 시스템에 적용할 수 있는 ECC 알고리즘 연구

A Study of ECC Algorithm using Mobile RFID System

김갑열[1]

Kap-Yol Kim[1]

요약

정보 통신 기술은 빠르게 변화하고 있다. 많은 선진국들이 기술 경쟁에 힘쓰고 있다. 또한 개발 중인 한국의 정보 통신 기술은 선진국의 기술과 대등한 수준까지 오르게 되었다. 국내 정보 통신 기술은 모바일 RFID (Radio Frequency Identification) 기술을 개발하고, 선진국에서는 이 기술에 대한 많은 관심을 나타내고 있다. 그러나 모바일 RFID는 보안에 문제가 있으며 암호화 체계는 모바일 RFID 환경에서 중요한 문제이다. 모바일 시스템에서 보안 체계의 구현은 쉬운 문제가 아니며 시스템은 복잡성과 제한된 자원으로 한계성이 있다. 따라서 본 논문에는 모바일 RFID 서비스를 위한 ECC (Elliptic Curve Cryptosystem) 알고리즘을 제안한다.

핵심어: 모바일, RFID, ECC, ODS, 웹 서버

Abstract

The information and communication technology of the world is changing quickly. Many advanced nations endeavor to technical competition. It also demonstrates that domestic information communication technique about under developing is confluent to the rank of advanced nations. The domestic information communication technique develops Mobile RFID (Radio Frequency Identification) techniques, with advanced nations revealing an interest in this technique. However, Mobile RFID presents a security problem and the encryption scheme is an important issue in the Mobile RFID environment. In mobile systems, implementation of security scheme is not an easy proposition and that systems is often delivered for reason of complexity and limited resources. So, in this dissertation, we suggest the ECC (Elliptic Curve Cryptosystem) algorithms for security in Mobile RFID services.

Keyword: Moble, RFID, ECC, ODS, Web Server

1 Department of Computer Science, College of IT, Gachon University
e-mail: kapyol@ctsoft.kr
Received(October 31.2016), Review (December 11.2016), Accepted(December 31.2016)

1. 서론

유비쿼터스 사회는 언제, 어디서나, 어떤 기기로도 서비스를 받을 수 있는 사회를 의미 하며, 유비쿼터스 서비스 기반이 되는 기술 중 사물에 대한 식별을 제공하는 기술은 아주 중요한 요소가 된다.

이와 같이 식별을 제공하는 기술 중 하나가 RFID(Radio Frequency Identification)이다. RFID 응용시스템은 무선 주파수를 이용하여 수 cm에서 수십 m에 떨어져 있는 사물이나 사람에 부착된 태그를 인식하여 태그로부터 정보를 주고받을 수 있도록 하는 기술로 국내에서도 많은 연구가 진행되어 지고 있다. 하지만 기술의 특허를 보유한 해외 업체들에 의해 국제 표준이 주도되어 오고 있기 때문에 국내 RFID 업체들은 수동적인 입장을 취할 수밖에 없었다. 따라서 새로운 형태의 기술 창출이 요구되어 왔고, 세계 최고의 모바일 단말 보급률, 인터넷 인프라 구축 기술 등을 기반으로 RFID 서비스와 접목한 신 개념의 모바일 RFID 기술이 등장하게 되었다. 현재 모바일 RFID 기술의 국제표준활동은 한국의 ETRI를 중심으로 활발하게 전개되고 있으며, 그 전망 또한 상당한 기대와 가치를 평가 받고 있지만 기존의 RFID 응용 시스템이 가지는 보안상의 문제점을 노출 하고 있으며, 특히 개인정보를 다루는 개인화 특수 목적의 응용 서비스의 등장이 불가피한 시점에서 이러한 보안문제는 큰 손실을 야기할 수 있다. 따라서 본 논문에서는 모바일 환경에 효율적으로 알려진 ECC(Elliptic Curve Cryptosystem) 알고리즘을 이용하여 모바일 RFID 응용 시스템에 적용할 수 있는 방안을 연구 한다.

이를 위해 2장에서는 모바일 RFID 개요, ECC 알고리즘 개요 및 정의, 성질 등 관련 기술에 대한 소개를 하며 3장에서는 개인 정보를 활용한 모바일 RFID 서비스 모델을 제시한 후 ECC 알고리즘 적용을 위한 프로토콜 구성 및 절차 구성을 하고 모바일 RFID 응용 서비스에 적용할 수 있는 ECC 알고리즘을 제안한다.

2. 관련연구

2.1 모바일 RFID

RFID는 무선주파수를 이용하여 사물에 부착된 태그(Tag)의 IC칩에 저장되어 있는 고유 정보

(Data)를 안테나와 리더를 통해서 비접촉 방식으로 수집하여 대상물체를 판독 및 인식하는 기술로 유비쿼터스 사회의 핵심 기술로 인식되고 있다[1].

RFID 서비스는 동 기술을 이용하여 식료품부터 원격의료 서비스까지 다양한 분야에 활용될 것으로 기대되고 있으며 세계적인 이동통신 인프라를 바탕으로 발전해온 국내 휴대폰 기술은 개인 복합 멀티미디어 정보 단말로서 다양한 컨텐츠 및 기술 수용과 함께 휴대폰에 RFID 리더를 탑재하여 사물과 사물 사이의 직접적 정보소통을 보다 쉽고 효율적으로 할 수 있는 모바일 RFID 기술을 개발하게 되었다[2].

이 기술의 등장으로 RFID 기술 중심에 소외되어 있던 국내 사정이 180° 바뀌게 되어, 현재 모바일 RFID 기술의 국제 표준을 주도 하고 있으며 지난 2007년 4월 20일 ISO의 정보통신기술위원회(JTC1/SC6) 국제표준화 회의에서 우리나라가 제안한 객체식별자(OID) 기술이 미국, 영국, 프랑스, 중국, 일본 등의 적극적인 지지를 받아 국제 표준에 채택되는 쾌거를 이루기도 하였다.

[그림 1] 모바일 RFID 네트워크 구조
[Fig. 1] RFID network structure of mobile

그림 1은 기본적인 ODS(Object Directory Service) 와 Web Server를 갖춘 모바일 RFID 네트워크 구조도를 보여 주며 모바일 RFID 응용 서비스를 위한 기본 구성 요소들이 된다.

모바일 RFID 응용 서비스는 RFID 리더가 탑재된 휴대폰으로 모바일 RFID 서비스 용도로 곳곳에 부착된 태그를 읽고, 이 태그 정보를 이용해 태그 ID와 URL의 매핑 정보를 가지고 있는 ODS로 콘텐츠를 가진 Web Server URL을 요청하게 된다. ODS는 관련 콘텐츠의 Web Server URL을 반환하고, 휴대폰은 반환된 URL을 이용하여 해당 콘텐츠를 제공하는 Web Server에 콘텐츠를 요

청한다. Web Server는 식별 가능한 코드 정보를 이용하여 Database에 매핑되는 콘텐츠를 Xml 또는 Html 형태로 서비스하게 된다[3].

위와 같이 모바일 RFID 응용 서비스의 형태를 보면 개인이 가진 RFID 리더를 이용하기 때문에 개인화 중심적인 서비스 콘텐츠가 많이 등장할 것으로 보이며, 이는 특히 개인정보의 중요성을 볼 때 보안에 중점적인 관심을 기울여야 하는 결과를 가지게 된다. 비록 모바일 RFID 태그의 정보가 코드형태의 데이터이기 때문에 Web Server URL을 알 수 없고, 접근할 수 없을 경우 무의미한 데이터일 수 있지만, 리더가 Web Server와 직접 통신을 하므로 Web Server URL 노출은 불가피하며, 따라서 코드 정보 중 콘텐츠의 정보를 의미하는 Serial 데이터를 보호하는데 중점을 둬야할 것이다.

2.2 ECC 알고리즘

ECC 알고리즘은 1985년 밀러와 코블리치에 의해 제안된 알고리즘으로 유한체(finitc fields) 위에서 정의된 타원곡선 군에서의 이산대수 문제의 어려움을 기초한 암호 시스템이다.

ECC 알고리즘은 일반적으로 160비트 키 길이를 이용하여 RSA의 1024 비트 키 길이를 가지는 암호 시스템과 대등한 안전도를 가진다고 알려져 있으며, 특히 160 비트 이상과 193 비트 이상의 키 길이를 가지는 ECC 알고리즘은 각각 10년에서 20년 이상 안전도를 가진 것으로 평가 되고 있어 그 효율성을 인정받고 있다. 다음 표 1은 RSA와 ECC의 키 사이즈에 비례한 보안 강도를 보여준다[4][5].

[표 1] RSA, ECC 키 사이즈 비교

[Table 1] Key Size Comparison of RSA, ECC

RSA	ECC
512 bit	106 bit
768 bit	132 bit
1024 bit	160 bit
1048 bit	211 bit
21000 bit	600 bit

위와 같이 ECC 알고리즘은 작은 키를 이용하여 높은 보안강도를 기대할 수 있는 특징으로 제한적 메모리 공간과 전력을 가지는 모바일 환경의 단말기(예: 휴대폰, PDA)등에 구현하기 용이하다. 또한 현재까지 가장 사용량이 많은 RSA 암호 시스템이 곱셈 연산을 주로 사용하는 반면 ECC 시스템은 덧셈 연산을 주로 사용하기 때문에 계산에 대한 속도 역시 타 시스템 보다 빠르며 H/W와 S/W 구현이 용이하게 된다[6-7].

2.3 ECC 알고리즘 정의 및 성질

p개의 원소를 갖는 유한체 GF(p) 상의 ECC 알고리즘은 체의 표수(characteristic) p 가 3 초과인 경우 암호 알고리즘으로서 실효성을 가지며 이때 타원곡선을 적당히 이동하면 다음과 같은 방정식에 만족하게 된다.

$$E : y^2 = x^3 + ax + b \tag{1}$$
$$a, b \in GF(p)$$

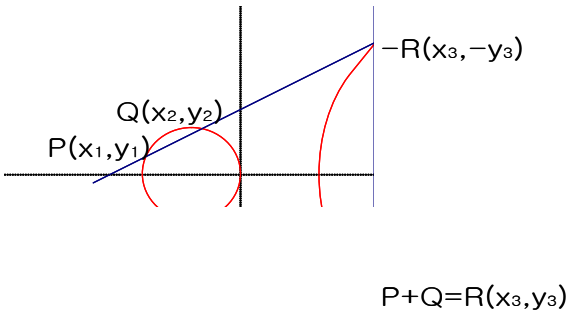
식 (1)을 암호 알고리즘으로서 만족하기 위해서는 p 값은 최소 3 초과인 소수가 입력이 되어야 하고 또한 중근이 존재 하지 않아야 한다. 타원곡선에 점들은 x 축을 대칭으로 y 점이 두 개가 존재 하는데 이때 서로 대칭한 두 점은 서로 역원이며, x 축으로 대칭한 y 점이 없을 경우 역원을 구할 수 없음으로 중근으로 정의하여 암호 알고리즘에서는 사용할 수 없다. 따라서 다음 식 (2),(3)과 같이 각각 정리할 수 있다.

$$E : x^3 + ax + b - y^2 \equiv 0 \pmod{p} \tag{2}$$
$$p > 3 \, AND \, prime$$
$$a, b \in GF(p)$$

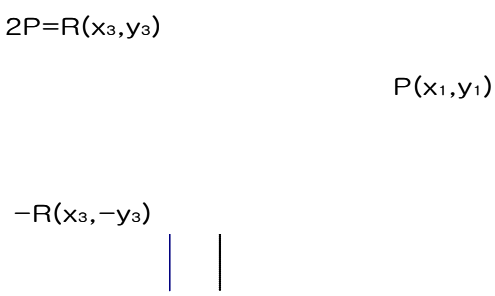
중근 존재 식은 다음 식 (3)과 같다.

$$4a^3 + 27b^2 \equiv 0 \pmod{p} \tag{3}$$

위와 같은 식 (2),(3)을 만족하는 타원곡선 E는 GF(p)상의 모든 점 (x, y)와 무한원점 O로 구성이 되며, 암호 알고리즘에서는 이 점들의 덧셈 연산과 뺄셈 연산을 통해 공개키와 메시지를 공유한다. 이때 곡선상의 점 P, Q에 대한 연산은 그림 2와 3과 같이 나타낼 수 있다.



[그림 2] ECC 알고리즘에서 P+Q 연산
[Fig. 2] P + Q operation in ECC algorithm



[그림 3] ECC 알고리즘에서 P+P 연산
[Fig. 3] P + P operation in ECC algorithm

곡선상의 점 P=(x1, y1), Q=(x2, y2)의 덧셈연산은 두 점 P, Q를 지나는 직선과 타원곡선과 만나는 제3의 교점(x, -y)을 x축에 관해 대칭한 점 R(x, y)을 P+Q=R(x3, y3) 로 정의한다. 또한 곡선상의 한 점 P에 대한 덧셈 연산 P+P 는 그림 2.3 과 같이 점 P에 대한 접선을 그려 yP가 0 이 아니면 –R 과 만나 그 대칭인 R(x3, y3)을 얻을 수 있으며, 그림 2와 3의 정의를 유한체 GF(p)상의 수식으로 정리 하면 다음 식 (4),(5)와 같다.

$x_1 \neq x_2$일때 (4)

$$k = \frac{y_2 - y_1}{x_2 - x_1} (\mathrm{mod}\, p)$$

$$x_3 = k^2 - x_1 - x_2 (\mathrm{mod}\, p)$$

$$y_3 = k(x_1 - x_3) - y_1$$

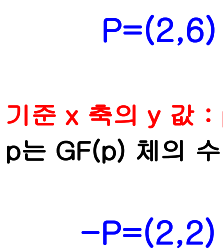
$x_1 = x_2\ AND\ y_1 = y_2 \neq 0$ 일때 (5)

$$k = \frac{3{x_1}^2 + 2y_1}{2y_1} (\mathrm{mod}\, p)$$

$$x_3 = k^2 - x_1 - x_2 (\mathrm{mod}\, p)$$

$$y_3 = k(x_1 - x_3) - y_1$$

식 (4),(5)에 의해 3P를 구하면 P+P=2P, 2P=Q, P+Q=R(x3, y3)로 정의 할 수 있고, 다시 2P를 구하기 위해선 R+(-P)=2P로 연산한다. 한 점에 대한 역원은 ECC 알고리즘에서 메시지 복구를 위한 뺄셈 연산을 위해 사용되고, 유한체 GF(p)상에 한 점 P에 대한 역원은 그림 4와 같다.



[그림 4] 점 P에 대한 역원
[Fig. 4] Inverse to point P

그림 4에서 P(2, 6)에 대한 역원은 y=p/2=4값을 갖는 x 축에 대칭하는 점 –P(2, 2)가 된다. 반대로 –P의 역원은 P로도 정의할 수 있다. 이를 수식으로 정리 하면 다음 식 (6),(7)과 같다.

$$x > 0 \ AND \ y > \frac{p}{2} \text{ 일때} \tag{6}$$

$$x_2 = x$$

$$y_2 = \frac{p}{2} - (y - \frac{p}{2})$$

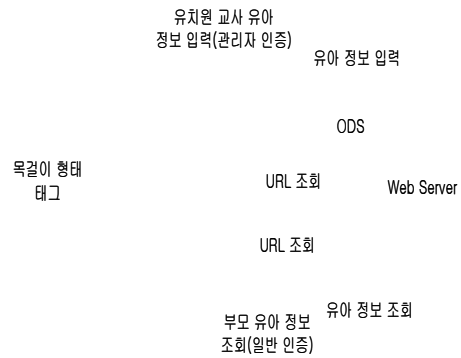
$$x > 0 \ AND \ y < \frac{p}{2} \text{ 일때} \tag{7}$$

$$x_2 = x$$

$$y_2 = \frac{p}{2} + (\frac{p}{2} - y)$$

3. 모바일 RFID에서 ECC 알고리즘 연구

3.1 모바일 RFID 서비스 모델



[그림 5] 유아 관리 서비스 개념도
[Fig. 5] Concept of early child care service

모바일 RFID 시스템에서 사용할 수 있는 서비스 형태는 무궁무진하다. 특히 개인 특성화되는 서비스가 가능할 것으로 예상되기 때문에 보안에 대한 민감한 상황이 존재할 가능성이 크며, 따

라서 본 논문에서는 개인 정보 유출시 심각한 문제를 초래할 수 있는 서비스 모델을 구성한다.

그림 5는 본 논문에서 제시하는 유아 관리 서비스 모델에 대한 개념도로 유치원에 다니는 자녀에게 목걸이 형태의 태그를 부착 당일 자녀의 교육 및 급식 등 유치원에서 있었던 사항들을 부모가 조회하는 서비스이다. 먼저 유치원 교사는 태그를 부착한 유아의 정보를 모바일 단말로 인식하여 ODS 서버로부터 해당 콘텐츠를 제공하는 Web Server URL을 받는다. 이후 관리자 로그인을 통해 해당 유아의 정보를 입력할 수 있는 콘텐츠를 제공받아 당일 받았던 교육 내용과 급식, 발육 상태 또한 특이 사항 등을 기록한다. 유치원에서 돌아온 유아는 부모가 가진 모바일 단말을 통해 다시 Web Server URL을 받고 해당 콘텐츠 서버에 접속하여 당일 자녀에 대한 사항 등을 조회하여 자녀의 교육 및 발육 상태 등을 체크할 수 있다. 본 서비스 모델에서는 유아의 기본적인 개인 정보를 통한 서비스를 제공함으로 정보 유출시 범죄에 악용될 우려가 있고, 또한 유치원의 운영 시스템 등이 노출될 수 있다. 따라서 콘텐츠를 제공하는 Web Server와 콘텐츠를 제공받는 모바일 단말 사이 강력한 보안 모듈이 필요하게 된다. 이에 본 논문에서는 ECC 알고리즘을 이용 RFID 태그에 시리얼 정보를 보호하고 자체적인 인증 모듈과 융합하여 ECC 알고리즘으로 바뀐 형태의 데이터 전송으로 암호화 뿐만 아니라 2중 인증 효과를 가질 수 있도록 한다[8-9].

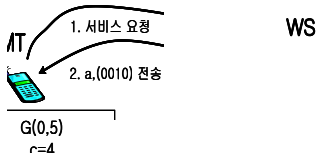
3.2 ECC 알고리즘 적용

ECC 알고리즘은 160비트 이상의 키를 이용할 경우 RSA 암호 알고리즘 1024 키 이상의 보안 강도를 기대 할 수 있다. 하지만 본 논문에서 제안하는 암호 알고리즘은 유한체 GF(p)상에 체의 표수 p를 32 비트 이상의 소수를 사용하고 모바일 단말과 Web Server는 미리 서로 공유한 형태로 가정한다. 또한 상수 항 b 값 역시 서로 알고 있다고 가정하고 프로그램 설치 시 서로 동기된다. 다음 그림 6은 본 논문에서 제안하는 ECC 알고리즘에서 키 정의를 나타낸다.

WS: Web Server
MT: 모바일 단말(예, 휴대폰)
타원곡선 상의 한 점: G
WS/MT 공개 키: kG, c1, c2 비밀 키: c, k
태그 메시지: M

[그림 6] 유아 관리 서비스 개념도
[Fig. 6] Concept of early child care service

다음 그림 7은 본 논문에서 제안하는 ECC 알고리즘 단계별 처리 과정을 나타낸다.



.[그림 7] 제안 ECC 알고리즘 단계별 처리과정

[Fig. 7] Concept of early child care service

그림 7에서는 설명의 편의를 위해 GF(p)상에 체의 표수는 11, x의 계수 a는 2, 상수 항 b는 3으로 설정했다.

식 (2)에 의해 위의 값들을 적용하면 타원 곡선의 점들을 얻을 수 있다. MT가 WS에게 서비스를 요청하면 WS는 응답으로 a 값을 보낸 다. 이후 MT와 WS는 유한체 GF(p)상 점들을 계산 해 내는데, 실제 32 비트 점들을 다 계산 하는 데는 무리가 있음으로 체의 표수 p에 랜덤 변수 값인 a를 나눈 값의 배수로 점을 찾아 처음 (2) 식을 만족하는 값을 G 값으로 선정한다. MT 또한 같은 방법으로 a 값 수신 후 G 값을 선정한다. 이후 WS의 공개키 생성 과정은 그림 8과 같다.

```
WS 공개키 생성{
    랜덤 값 k 생성;
    선정된 G 값 P와 P' 복사;
    for(k번 반복){
        if(P == P'){
                P+P = 2P;
                Q = 2P;
            }
        else if(P != Q){
                P+Q = R;
                Q = R;
            }
        }
    kG=Q;       kG MT에 전송;
}
```

[그림 8] WS의 공개키 생성 알고리즘 코드

[Fig. 8] WS public key generation algorithm code

그림 3.4에서 WS는 랜덤 값 k 만큼 수식 (4), (5)를 반복 연산 하여 kG를 구할 수 있는 것을 알 수 있다. MT 역시 같은 방법으로 랜덤 값 c를 생성 후 c1을 계산 해 내고 WS로부터 전송 받은 kG 값에 랜덤 값 c를 연산 ckG를 구할 수 있다. 이후 과정은 그림 3.5와 같다.

```
MT 암호문 c2 생성{
    M = Serial 데이터 파싱 후 좌표 변환;
    P = M;        P' = ckG;
        if(P == P'){
                P+P = 2P;
                Q = 2P;
            }
        else if(P != P'){
                P+P' = R;
                Q = R;
            }
    c2=Q;         c1, c2 WS에 전송;
}

WS 메시지 복호화{
    수신한 c1 값 P와 P' 복사
    for(k번 반복){
        if(P == P'){
                P+P = 2P;
                Q = 2P;
            }
        else if(P != Q){
                P+Q = R;
                Q = R;
            }
        }

    kc1=Q;        kc1의 역원을 구함;
    P = c2;       P' = -kc1;
        if(P == P'){
                P+P = 2P;
                Q = 2P;
            }
        else if(P != P'){
                P+P' = R;
                Q = R;
            }
    M=Q;
}
```

[그림 9] MT c2 생성 및 WS 복화 의사 코드
[Fig. 9] MT c2 generation and WS replication psuedo code

그림 3.5에서 MT의 c2 생성 과정은 태그로부터 전송 받은 시리얼 값 10110011(2)를 4비트 단

위로 파싱하여 좌표상의 점 M(11, 3)으로 변환한다. 변환된 M 값은 ckG와 덧셈 연산을 통해 c2를 계산 해 내고 MT는 생성된 c1 값과 c2 값을 WS에게 전송한다.

이후 암호문 c1과 c2를 전송 받은 WS는 자신의 비밀 키 k와 c1을 덧셈 연산을 하여 kc1을 계산 해 내고 이때 kc1은 MT가 연산한 ckG 값과 동일한 값을 가진다. 즉 서로의 비밀 키를 공유하지 않고도 비밀 키로 연산된 값을 동기화 할 수 있는 것이다. 다시 WS는 c2에 kc1 값을 뺄셈 연산을 하면 메시지 M에 대한 좌표 점을 얻을 수 있는데 이때의 연산은 kc1 값의 역원을 구해 덧셈 연산을 하면 된다.

최종으로 M의 좌표 점 (11, 3)을 좌항, 우항으로 구분 2진 값으로 변환하면, 원래의 시리얼 형태의 데이터로 데이터베이스에 매핑되는 서비스 콘텐츠를 제공할 수 있다.

4. 결론

본 논문에서 제안하는 ECC 알고리즘은 모바일 컴퓨팅 환경에 적합한 구성을 위해 32 비트의 키를 가질 수 있도록 유한체 상의 체의 표수 p 를 32 비트로 제안하였다. 비록 보안 강도가 기존 암호시스템보다 낮게 되지만, 한 번의 키 교환으로 일정기간 같은 패턴의 키를 교환하는 일반적인 암호 시스템과 달리 x 계수 a 값을 통신 때 마다 갱신함으로서 보안 강도의 상승효과를 가질 수 있다. 또한 G 값 선정에서도 WS가 랜덤으로 선택한 후 교환하는 방식이 아닌 a 값에 의해 유동적으로 동기화함으로서 G 값 패턴을 알아내기 힘들어 WS가 가지고 있는 콘텐츠에 대한 정보 역시 획득하기 어렵게 된다.

일반적으로 Web Server에서 모바일 단말에 제공하는 서비스 형태가 Web 페이지 형태의 Xml 또는 Html이고 특히 본 논문에서 제시하는 서비스 모델에서는 관리자 인증과 일반 인증을 구분하고 있어 자체 인증 시스템 구현이 필요 하다. 이에 본 논문에서 제안하는 ECC 알고리즘 적용 시 암호화 된 데이터 전송으로 자체 인증시스템과 함께 2중 인증 효과를 가질 것으로 기대한다.

References

[1] W. Kim, J. J. Na, RFID Search System Construction and Operation Guide V1.2, NIDA.KO, Dec, (2006).

[2] H. J. Kim, The korean Institute of Communications and Information Science. (2007), Vol.24, No.6, pp.103-108.

[3] H. J. Kim, Standard Trend - Mobile RFID, TTA Journal No.99, Dec, (2006).

[4] SEC1, Elliptic Curve Cryptography. (2000), Vol.1, pp.62.

[4] Seroussi. G, In Information Theory and Networking Workshop IEEE. (1999), p.41.

[5] POSTECH, Telecommunications Technology Association. (2001).

[6] C. Geuer-Pollmann. XML pool encryption, In Proceedings of the 2002 ACM workshop on XML security, (2002), November, USA.

[7] A. Weimerskirch.. C. Paar, S. C. Shantz, In Australasian Conference on Information Security and Privacy. (2001), pp502-513.

[8] M. Saeki, Elliptic curve cryptosystems, School of Computer Science McGill University, Montreal, (1997).