타원곡선 알고리즘을 이용한 XML 문서 암호 구현

XML Document Encrypt Implementation using Elliptic Curve Cryptosystem

고 훈*
Hoon Ko

요 약

컴퓨터와 인터넷의 보급과 활용이 일반화 되고 대중화 되면서, 인터넷을 이용한 은행업무 등 비밀을 요하는 다양한 업무를 보게 되었다. 또한 인터넷, 무선통신, 그리고 자료교환에 대한 증가로 인해 많은 사용자와 접속 혹은 사용하는 방법도 빠르게 변화하고 있는 상황이다. 특히 인터넷뱅킹을 이용할 때 인터넷의 구조적인 문제점 때문에 많은 정보들이 유출되고 있고 있다. 기존의 느리고 간단한 암호화 방식으로는 인터넷뱅킹 이용할 때 신용카드 번호 혹은 통장의 계좌번호 및 비밀번호를 노출시킬 수 있다. 이러한 데이터에 대한 보안이 기대에 미치지 못하기 때문에 보다 강력한 암호처리를 필요로 하게 된다. 그러나 전송되는 자료 전체를 암호화 했을 때 소요되는 시간적 공간적 낭비 또한 무시할 수 없는 부분이다. 이에 본 논문에서는 무선기반에서 강력하게 연구되고 있는 타원곡선 알고리즘과 XML의 특징인 DTD의 부분적인 암호를 적용함으로써 보다 빠른 XML의 부분적인 암호를 구현하고자 한다.

Abstract

As the use of the computer and networks generalized, the various tasks which are requested secrets can be processed such as the banking transaction. And because of increasing of data exchange, Internet, and mobile networks, the method which is not connected only but also used with many users has been changed. Especially because of the structural problem of the Internet, a lot of information is leaked out when we use the Internet banking. If we check the Internet banking by using an existing cypher method which is either simple or slow, a credit card number, an account number or password will be leaked out. Because the security of information doesn't meet our expectation, we need more powerful cryptography. But, the wasted space-time which is required shouldn't be ignored when the whole transferred data are encrypted. So, By using both the Elliptic Curve algorithm which is based on mobile networks and the partial encryption of the DTD of XML in this essay, we will implement more faster cypher method of the partial XML.

☞ Keyword : ECC, RSA, XML, Encryption

1. 서 론

인터넷뱅킹은 시간과 공간을 초월하는 서비스로 사용자와 사용하는 범위가 계속 확대 및 증가되어 가고 있지만, 인터넷을 통해 전송되는 데이터에 대한 보호 및 안전성은 사용자들의 기대에 비해 상당히 낙후되어 있다. 또한 전송되는 정보를 중간에 가로채어 정보를 유용하는 범죄도 증가하고 있다. 또한 전송되는 문서를 가로채어서 수정 및 변경 후에 재전송하여 원래 수신자가 문서의 무결성을 제공받지 못한 상태에서 문서를 읽는 문제점도 발생되고 있다. XML은 구조의 특징 상 문서의 특정 부분에 대한 암호를 지원한다.

본 논문에서는 이러한 암호화 방법을 이용하여 메시지의 중요한 부분만을 타원곡선 암호화 방법으로 암호화하고 나머지 부분은 공개함으로써 다양한 어플리케이션으로의 확장을 지원하려 한다[10]. 비밀키 암호화 방식은 빠르지만 키 분배에 어려움이 있어 본 논문에서는 공개키 암호화 알고리즘을 사용하였다. 현재 대표적인 공개키 암호화 알고리즘은 RSA, ElGmal, DSA, ECC 등이 있다. 그러나 RSA, ElGmal, DSA 등의 공개키 암호 시스템은 ECC 방식보다 큰 길이의 키를 사용하기

* 정 회 원 : 충남대학교 차세대 SW인력양성사업단 계약교수
skoh21@cun.ac.kr
[2006/08/31 투고 - 2006/09/03 심사 - 2006/09/13 심사완료]

때문에 처리 속도가 느리며 성능도 떨어지는 단점이 있다. 또한 RSA는 주요 연산이 곱셈인 반면 ECC는 덧셈이기 때문에 계산이 훨씬 빠르다[5].

여기에서는 중간 문서 변형을 막는 서명 방법의 기본이 되는 암호학 기법 중에서 빠르고 안전한 타원곡선 기법을 이용해서 웹상의 문서 중 비밀을 요하는 부분을 암호화 하는 기법에 대해서 기술되어 있으며[1][10]. 이 기술을 이용해서 메시지 기밀성, 메시지 무결성 등을 제공하고자 한다. 본 논문의 구성은 다음과 같다. 2장에서는 제안한 방법인 타원곡선을 이용한 XML 문서의 암호를 설계하고 3장에서는 설계를 기초로 하여 구현한 결과를 보여준다. 마지막으로 4장은 결론과 차후 연구 방향 등을 기술한다.

2. 관련연구

2.1 타원곡선 암호화

1985년 밀러와 코블리츠가 제안한 타원 곡선 기반 암호로서, 이산 대수에서 사용하는 유한체의 곱셈군을 타원 곡선군으로 대치한 암호 방식. 특히, 다른 암호 방식에 비해 더 짧은 키 사이즈로 대등한 안전도를 가진다.

예를 들어, RSA 1024 비트 키와 ECC 160 비트 키를 갖는 암호 방식은 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.

2.2 키 교환 방법

DH알고리즘이라고 불리는 키 교환 알고리즘은 비밀키와 공개키를 생성하여 암호화와 복호화를 행하는 방식에 관한 알고리즘이 아니라 메시지를 주고받으려는 두 명의 사람이 비밀리에 비밀키를 전달하기 위한 방법이다[9].

n, g : 크기가 큰 정수들로서 메시지의 송수신에 참여하는 모든 사람들에게 공개되어 있다.

① 송신자는 비교적 크기가 큰 난수 x를 발생시키고 이 값을 보관한다.

② 수신자는 역시 비교적 크기가 큰 난수y를 발생시키고 이 값을 보관한다.

③ 송신자는 다음의 계산을 하여 그 결과를 수신자에게 보낸다.

$$X = g^x \bmod n$$

④ 수신자는 다음의 계산을 하여 그 결과를 송신자에게 보낸다.

$$Y = g^y \bmod n$$

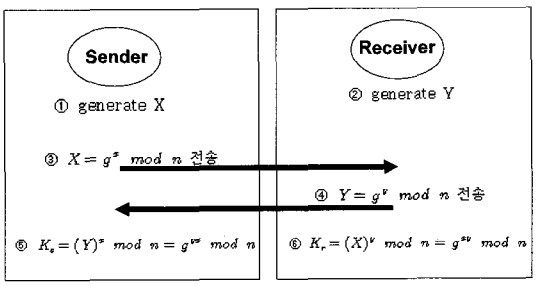
⑤ 송신자는 Y를 받아서 다음의 계산을 한 후 비밀키 Ks를 얻는다.

$$Ks = (Y)^x \bmod n = g^{yx} \bmod n$$

⑥ 수신자는 X를 받아서 다음의 계산을 한 후 비밀키 Kr를 얻는다.

$$Kr = (X)^y \bmod n = g^{xy} \bmod n$$

즉 ⑤와 ⑥에서 계산된 결과인 Ks와 Kr이 같은 값을 갖는다는 것을 알 수 있다. 따라서 송신자와 수신자는 이 값을 비밀키로 하여 메시지를 암호화 / 복호화 할 수 있게 된다.



〈그림 1〉 DH를 이용한 키 교환 방법

2.3 타원곡선 안전성

공개키 암호시스템의 이론적 안전도를 조사하기 위해서는 먼저 시스템을 공격하는 데에 있어서 그 시스템의 기반이 되는 수학적 문제를 푸는 것이 요구되는지를 분석하는 것이다. 실제 소인수 문제에 기반을 둔 공개키 암호시스템(RSA), 이산

대수문제에 기반을 둔 공개키 암호시스템(DSA) 및 타원곡선 이산대수문제에 기반을 둔 타원곡선 암호시스템 모두 수년간 정밀한 분석이 있어왔고, 그러한 시스템 공격방법은 그 기반이 되는 수학적 문제를 해결하는 것이라고 알려져 있다.

〈표 1〉 키 사이즈 비교

ECC	RSA
106 bits	512 bits
132 bits	768 bits
160 bits	1024 bits
211 bits	2048 bits
600 bits	21000 bits

(표 1)은 RSA와 ECC의 키 사이즈에 비례한 보안 강도를 보여준 표이다. ECC는 키 사이즈가 짧기 때문에 RSA 보다 빠른 처리를 하지만 보안 강도는 비슷하다. 또한 타원 곡선 구조상 비트당 높은 암호학적 강도를 가지고 있다.

2.4 속도

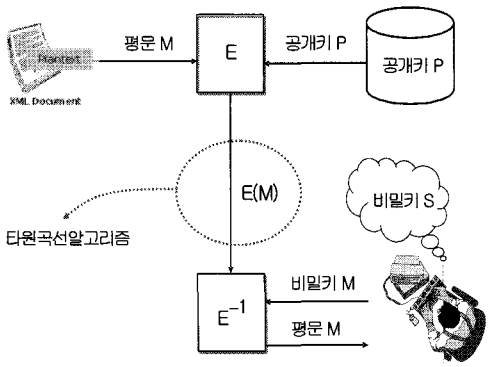
(표 1) 비슷한 수준의 비도에 따른 RSA와 ECC의 키사이즈를 보여준 표이다. RSA와 비교하여 상당히 더 작은 키 크기가 ECC에 사용되어질 수 있다. 따라서 RSA보다 더 짧은 키 길이를 가지는 ECC를 사용하는 것은 계산적으로 빠르다는 장점이 있다.

또한 RSA는 주요연산이 곱셈인 반면에 ECC는 덧셈으로 처리를 하기 때문에 상대적으로 빠르며, 사용되는 키의 길이도 RSA 보다 짧다.

3. 타원곡선 이용 XML 문서암호 설계

3.1 타원곡선 암호화 방법

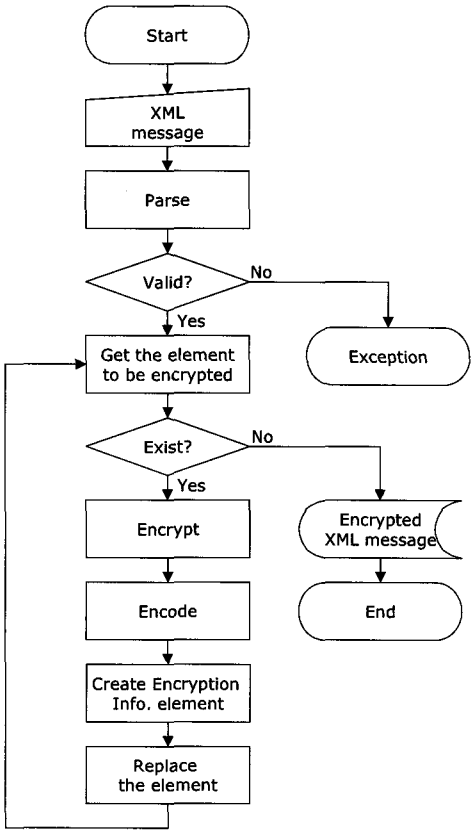
XML 문서의 구조적 특징을 이용해 보안이 필요한 부분만을 골라서 암호화는 방식을 사용한다 [12][13]. 그러나 XML 문서의 특성상 문서의 구조 유효성을 판단해야 하기 때문에 유효성 검사를 하기 때문에 일반 문서를 암호화 하는 방법보다는 시간이 많이 소요된다.



〈그림 2〉 타원곡선 알고리즘을 이용한 암호화

그러나 구조적인 문서, 부분적 암호화 가능성 등 일반 문서보다 유리한 장점이 있고, 전자문서 표준 및 전자상거래 상에서 XML을 이용하는 환경이 계속 증가하고, 계속적인 속도 개선으로 XML의 암호화 시간도 많이 개선되고 있고, 계속적으로 개선될 것이다.

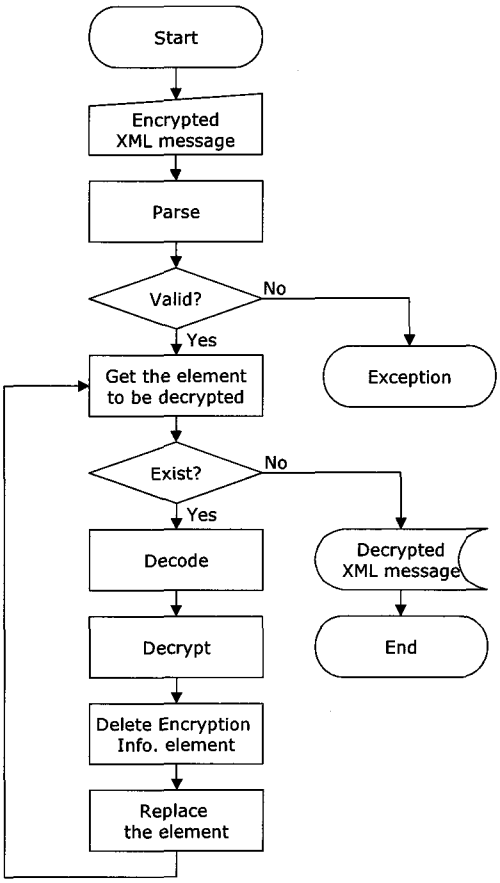
XML 문서의 구조적 특징을 이용해 보안이 필요한 부분만을 골라 암호화하는 방식을 사용한다. (그림 1)은 XML 메시지 암호화 모듈의 프로세스 순서를 나타낸다. 송신자가 XML 메시지를 작성한다. 메시지 암호화 모듈은 우선 해당 메시지가 유효한(well-formed) XML 문서 구조를 가졌는지에 대해 검사를 한다. 그런 다음 메시지 내 요소들 중 암호화될 요소들을 검출하고, 해당 요소들을 비밀키 암호 알고리즘을 사용하여 암호화한다. 이 때 사용되는 비밀키는 해당 그룹에 대한 세션키가 된다. 이렇게 암호화된 요소는 다시 XML 메시지 내의 해당 요소와 대체되기 위해 인코딩된다. 암호화된 내용을 복호 할 때 필요한 정보들은 암호화된 내용과 같이 추가된다. 이 과정을 통해 보호를 요하는 요소만 암호화 된 XML 메시지가 작성된다.



〈그림 3〉 XML 메시지 암호화 순서도

XML 메시지의 복호 과정은 암호화 과정과 유사하다. (그림 2)은 XML 메시지 복호 모듈의 프로세스 순서를 나타낸다. 메시지 복호 모듈은 우선 해당 메시지가 유효한(well-formed) XML 문서 구조를 가졌는지에 대해 검사를 한다. 그런 다음 메시지 내 요소들 중 복호 되어야 하는 요소들을 검출하고, 해당 요소들을 디코딩 한다. 디코딩 된 요소를 복호하기 위해 세션 키를 사용한다. 복호가 끝나면 암호화된 요소와 이와 관련된 정보들은 복호 된 요소로 대체된다.

본 실험에서는 타원곡선 E를 단순화하기 위해 $K = F_p = Z_p$(p: 소수, p개의 원소를 같는 유한체)로 정의하고, $E(Z_p)$는 $\{(x,y) \in (Z_p, Z_p) \mid y^2 = x^3 + ax + b\,(a,b \in Z_p)\} \cup \{0\}$ 으로 구성된다.



(그림 4) XML 메시지 복호 순서도

본 실험에서 Z_p클래스는 0~P-1까지의 수로 표현했다. 문자열을 받으면 그것을 Z_p형을 바꾸어 준다.

```
public Zp(String a)
{
                    :
for(int i = 0; i<a.length(); i++) {
        first=first.add(second.multiply(new
BigInteger(String.valueOf((long)a.charAt(i) ))));
second = second.shiftLeft(16);
}
num = first;
}
```

Z_p를 받으면 그것을 문자열 형태로 바꾸어 준다.

```
if (!temp.equals(new BigInteger("0")) ) do {.
        result +=
            (char)temp.mod(multi).longValue();
        temp = temp.shiftRight(16);
} while(temp.compareTo(new BigInteger("0")) == 1 );
            return result;
}
public BigInteger val()
{
            return num;
}
}
```

Z_p를 타원곡선을 생성하는 상수의 정의 부분과 타원곡선 ECC_A, ECC_B의 정의한다.

```
public static final EllipticPt ALPHA =
new EllipticPt
(new Zp(new BigInteger("12.....02")),
 new Zp(new BigInteger("34.....57")));
                    :
 private final Zp ECC_A =
       new Zp( new BigInteger("78.....89"));
private final Zp ECC_B =
      new Zp( new BigInteger("98.....57"));
```

위에서 정의된 모듈을 이용해서 XML 문서에 대해서 암호화를 수행하게 된다.

수행되는 소스코드 중 for구문에서 i로 정의되어 있는 부분에서 i가 최후에 처리될 때가 아니면 그냥 수행하게 되고 else 구문에서 i가 최종으로 처리될 때, 끝자리를 끊어주게 된다.

result[i/2] = encrypt(plain_pt, publickey, k); 부분은 문자열을 잘라서 암화화 하여 처리되는 결과는 result[] 배열에 저장되고, result[] 각각은 두개의 원소를 같은 배열로 정의되어 있다.[2][3]

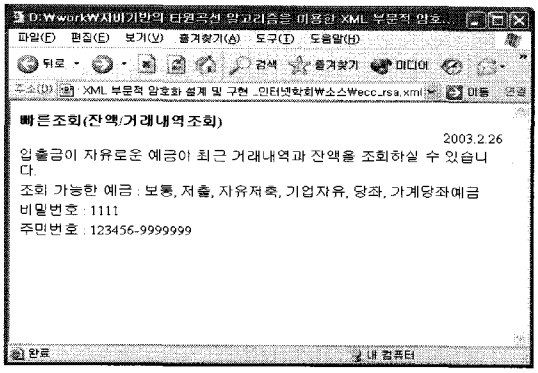
```
public static EllipticPt[][] encrypt( String plain, EllipticPt publickey )
{
        :
for (int i = 0; i < result.length*2; i+=2) {
        :
Zp k = new Zp( new BigInteger(kBIT, new Random()) );
String x, y;
        :
if (i< 2*result.length -2) {
x = plain.substring(i*TRIM,(i+1)*TRIM);
y = plain.substring((i+1)*TRIM, (i+2)*TRIM);
}
else {
if ((i+1)*TRIM >= plain.length()) {
x = plain.substring(i*TRIM, plain.length());
y="";
}
else {
x = plain.substring(i*TRIM, (i+1)*TRIM);
y = plain.substring((i+1)*TRIM, plain.length());
}
}
plain_pt = new EllipticPt (new Zp(x), new Zp(y) );
result[i/2] = encrypt( plain_pt, publickey, k);
}
```

3. 구현 결과

위에서 제시한 방법으로 실험한 결과이다. 먼저 실험 환경은 아래와 같다.

OS : Windows 2000 Advanced Server
JAVA : JDK 1.3
JCE : JCE 1.2
수행하기 위한 XML 문서는 K은행의 인터넷

뱅킹을 할 때 계좌조회 때 사용되는 모듈을 임의로 XML화해서 계좌번호(account)와 비밀번호(secret) 부분을 암호화 해 보았다.



〈그림 5〉 XML 평문 문서

(그림 6)(그림 7)(그림 8)은 타원곡선 알고리즘을 이용하여 암호화한 XML 문서이다.

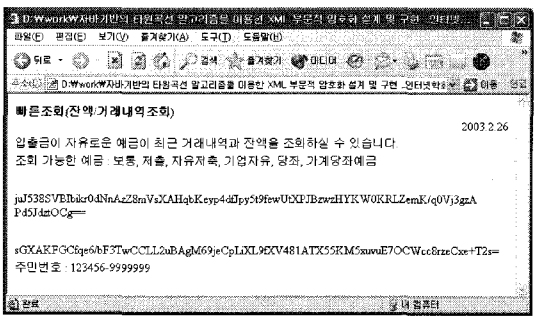
```
<DecryptionInfo>
<PropertyList></PropertyList>
<Key><Value>jIpuj+CR42s=</Value>
</Key>
</DecryptionInfo>

<CipherText>juJ538SVBIbikr0dNnAzZ8mVsX
            AHqbKeyp4dfJpy5t9fewUtXPJB
            zwzHYKW0KRLZemK/q0Vj3gzA
            }Pd5JdztOCg==
</CipherText>
</EncryptedData>

<DecryptionInfo>
<PropertyList></PropertyList>
<Key><Value>elsItrZM/iA=</Value>
</Key>
</DecryptionInfo>

<CipherText>sGXAKFGCfqe6/bF3TwCCLL2uBAg
            M69jeCpLiXL9fXV481ATX55KM5x
            uvuE7OCWcc8rzeCxe+T2s=
</CipherText>
</EncryptedData>

<number> <heading>주민번호 : </heading>123456-9999999</number>
```

〈그림 6〉 타원곡선 알고리즘으로 구현한 결과 1

4. 결 론

최근의 인터넷 환경에서 많이 사용되고 있는 e-mail 혹은 은행 및 카드 업무를 위한 인터넷상의 정보 입력은 많은 보안상의 취약점이 노출되어 있으며 또한 느리다. 이러한 단점들을 극복하기

〈그림 7〉 타원곡선 알고리즘으로 구현한 결과 1



〈그림 8〉 타원곡선 알고리즘으로 구현한 결과 2

위해서 많은 연구들이 진행되고 있다. 본 실험에서는 그동안 진행되어 온 타원곡선 알고리즘을 전자문서 표준안으로 채택된 XML에 응용함으로써 앞으로 XML을 이용한 전자서명 및 전자 상거래, 기타 여러 가지 금융 업무에 응용했을 때, 기존의 방법보다도 효과적일 것이라고 말하고자 한다. 본 실험을 기초로 앞으로 많은 타원곡선을 이용한 응용 부분이 많이 개발되기를 바란다.

향후 본 실험을 기초로 무선 상에서 공개키 기

반의 전자서명 및 보안 메일을 전송할 때, 기존의 방법에 비해 전송속도 및 상호간에 신뢰하면서도 빠른 서비스를 제공하는 방법을 연구해야 할 것이다. 또한 현재의 키 교환방법의 위험성을 해결하는 방법에 대해서도 연구가 필요하다.

참 고 문 헌

[1] K. Itoh, T. Izu, M. Takenaka, "A Practical Countermeasure against Add-ress-bit Differential Power Analysis," CHESS2003, LNCS2779, pp.382-396, 2003.

[2] Jonathan Knudesen, "Java Cryptography", O'REILLY, 1998

[3] K. Okeya, T. Takagi, "The Width-w NAF Method Provides Small Memory and Fast Effliptic Scalar Multiplications Secure against Side Channel Attacks," *CT-RSA* 2003, pp.328-32, 2003.

[4] Richard E. Smith "Internet Cryptography" Addison Wesley, 5th-Edition, 2002.

[5] C. G. Pollman, "XML Pool Encryption," *XMLSEC02*, USA, pp.1-9, 22, Nov. 2002.

[6] E. Damiani, C. Vimercati, S. Paraboshi and P. Samarati, "Securing XML Documents," *EDBT2000*, pp.27-31, June, 2000.

[7] H. Cheng and X. Li, "Partial encryption of compressed images and video," *IEEE Transaction on Signal Processing*, vol.48, no.8, pp.2439-2451, 2000.

[8] J. H. Cheon and S. T. Chee, "Elliptic Curves and Resilient Functions," *ICISC 2000*, LNCS 2015, pp. 64-72, Springer-Verlag, 2001.

[9] Louis Goubin, "A Refined Power-Analysis Attack on Elliptic Curve Cryptosystems," *PKC 2003*, LNCS 2567, pp.199-211, 2003.

[10] 안만기, 하재철, 이훈재, 문상재, "타원곡석 암호시스템에서 랜덤 m-ary 방법을 사용한 전력분석 공격의 대응방법," 정보보호학회 논문지, 13권 3호, pp.35-43, 2003.

[11] 한동국, 장남수, 장상운, 임종인, "랜덤한 덧셈-뺄셈 체인에 대한 부채컬 공격," 정보보호학회 논문지, 14권 5호, pp.121-133, 2004.

[12] 최동희, 박석, "접근제어 정책구현을 위한 역할 기반 XML 암호화," *정보보호학회 논문지*, 15(1), pp3-15, 2005.

[13] 박영희 외 5인, "Diffe-Hallman 키 교환을 이용한 확장성을 가진 계층적 그룹키 설정 프로토콜," *정보보호학회 논문지*, 13(5), pp.3-15, 2003.

[14] 이원구, 이재광, "자바기반의 타원곡선 알고리즘을 이용한 보안 메일 시스템의 설계 및 구현," *한국정보호 진흥원*, 2001.

◐ 저 자 소 개 ◑

고 훈 (Hoon Ko)

1998년 호원대학교 컴퓨터학과 졸업(학사)
2000년 숭실대학교 대학원 컴퓨터학과 졸업(석사)
2004년 숭실대학교 대학원 컴퓨터학과 졸업(박사)
2002년 ~ 2006년 대진대학교 컴퓨터공학과 초빙교수
2006년 ~ 현재 충남대학교 차세대 SW인력양성사업단 계약교수
관심분야 : 네트워크보안, 인증, 홈네트워크 보안, MSEC, OTP, Urban Computing etc.
E-mail : skoh21@cun.ac.kr