Journal of the Korea Academia-Industrial cooperation Society
Vol. 14, No. 3 pp. 1439-1444, 2013

http://dx.doi.org/10.5762/KAIS.2013.14.3.1439

실수체 기반 타원곡선 암호의 성능 평가에 관한 연구

우찬일[1*], 구은희[1], 이승대[2]
[1]서일대학교 정보통신과, [2]남서울대학교 전자공학과

A Study on the Performance Evaluation of Elliptic Curve Cryptography based on a Real Number Field

Chan-Il Woo[1*], Eun-Hee Goo[1] and Seung-Dae Lee[2]
[1]Dept. of Information and Communication Engineering, Seoil University
[2]Dept. of Electronic Engineering, Namseoul University

요 약 최근 들어, 네트워크의 급속한 발전으로 온라인 뱅킹과 주식 거래 같은 응용프로그램들의 사용이 증가함에 따라 데이터에 대한 보안은 점점 더 중요해 지고 있다. 따라서, 데이터 보호를 위해 인터넷과 같은 개방형 네트워크에서 공개키 또는 대칭키 암호 알고리즘이 널리 사용되고 있다. 일반적으로 공개키 암호시스템은 인수분해와 이산대수의 문제를 기반으로 하고 있어, 대칭키 암호시스템에 비해 처리속도가 상대적으로 느리다. 공개키 암호시스템 중 타원곡선 암호는 RSA에 비해 보다 작은 사이즈의 키를 사용하여도 동일한 보안성을 제공하는 장점이 있어 처리 속도가 빠르다. 본 논문에서는 실수체를 기반으로 하는 타원곡선 암호의 효율적인 키 생성 방법을 제안한다.

Abstract Recently, as the use of the applications like online banking and stock trading is increasing by the rapid development of the network, security of data content is becoming more and more important. Accordingly, public key or symmetric key encryption algorithm is widely used in open networks such as the internet for the protection of data. Generally, public key cryptographic systems is based on two famous number theoretic problems namely factoring or discrete logarithm problem. So, public key cryptographic systems is relatively slow compared to symmetric key cryptography systems. Among public key cryptographic systems, the advantage of ECC compared to RSA is that it offers equal security for a far smaller key. For this reason, ECC is faster than RSA. In this paper, we propose a efficient key generation method for elliptic curve cryptography system based on the real number field.

Key Words : Cryptography, ECC, Key Generation, Security

1. 서론

컴퓨터와 유, 무선 네트워크 기술의 비약적인 발전은 유선 네트워크로만 제공되던 인터넷 뱅킹이나 주식 거래 그리고 게임 등과 같은 서비스가 무선 네트워크를 통해서도 동일하게 서비스되고 있다. 이와 같은 정보통신 기술의 발전은 스마트폰처럼 휴대가 가능한 단말기들을 이용하여 언제, 어디서나 원하는 정보에 쉽게 접근할 수 있는 환경을 제공하고 있다.

그러나 컴퓨터뿐만 아니라 스마트폰 등에 저장되어 있는 중요한 정보뿐만 아니라 유, 무선 네트워크를 통해 전송되는 데이터들은 다양한 형태의 보안 위협에 노출될 수 있다. 따라서 이러한 문제를 해결하기 위한 인증, 암호 기술과 같은 정보보호 기술에 대한 연구가 활발하게 진행되고 있다.

암호 기술은 암호화 및 복호화에 사용되는 키에 따라

본 논문은 2012년도 서일대학교 학술연구비에 의해 연구되었음.
*Corresponding Author : Chan-Il Woo(Seoil Univ.)
Tel: +82-2-490-7556 email: ciwoo@seoil.ac.kr
Received December 17, 2012 Revised January 2, 2013 Accepted March 7, 2013

비밀키(또는 대칭키) 암호와 공개키 암호로 구분되어 진다. 비밀키 암호는 암, 복호화 속도는 빠르지만 암, 복호화에 사용되는 키가 동일하기 때문에 키를 관리하는데 많은 어려운 문제들이 발생할 수 있다. 그러나 공개키 암호는 암, 복호화에 사용되는 키가 서로 달라 키 관리와 관련된 문제들은 발생하지 않지만 비밀키 암호보다 계산이 복잡하여 암, 복호화 속도가 느린 단점이 있다. 대표적인 공개키 암호시스템인 RSA의 경우 암, 복호화에 사용되는 키 사이즈를 줄이게 되면 암, 복호화를 위한 처리 속도는 빨라지는 장점이 있지만 제 3자에 의해 쉽게 해독될 수 있는 문제점이 발생한다. 따라서 공개키 암호시스템에서 작은 사이즈의 키를 사용하더라도 큰 사이즈의 키를 사용했을 경우와 동일한 안전도를 제공할 수 있다면 메모리를 적게 사용할 수 있고 낮은 소비전력으로 보다 빠르게 암, 복호화를 수행할 수 있는 장점이 있다[1].

1980년대 중반 Neal Koblitz[2]와 Victor Miller[3]에 의해 제안된 타원곡선 암호시스템(ECC : elliptic curve cryptography)은 타원곡선의 이산대수 문제(elliptic curve discrete logarithm problem)의 어려움을 기반으로 하고 있으며, 타원곡선의 이산대수 문제는 현재까지 효과적으로 공격할 수 있는 방법이 제시되고 있지 않아 다른 공개키 암호시스템에 비해 훨씬 작은 길이의 키를 사용하더라도 동일한 안전도를 보장 받을 수 있고 빠르게 처리할 수 있는 장점을 갖으며, 타원곡선 암호시스템은 군(group)을 제공할 수 있는 여러 가지의 타원곡선을 활용할 수 있어 안전하고 다양한 암호시스템을 설계하는 것이 용이하여 현재까지 많은 연구가 이루어지고 있다[6].

타원곡선 암호시스템이 가지는 이러한 장점으로 인하여 NIST[4]와 IEEE[5]에서는 전자서명 알고리즘으로 타원곡선 전자서명 알고리즘(ECDSA : elliptic curve digital signature)을 표준으로 채택하였다. 타원곡선 암호시스템은 지금까지 유한체를 기반으로 한 정수근에 대하여 주된 연구가 이루어 졌다. 그러나 타원곡선 암호시스템을 실수체로 확장하여 생성된 키를 암, 복호화에 사용할 수 있다면 정수근만을 사용하는 경우보다 훨씬 다양한 공개키를 선택할 수 있어 보다 효과적인 암호시스템을 구성할 수 있을 것이다.

본 논문에서는 실수체를 기반으로 하는 타원곡선 암호시스템에서 생성된 공개키가 암, 복호화에 효과적으로 사용될 수 있다는 연구결과[7]를 바탕으로 실수체 타원곡선 암호시스템에서 보다 효과적인 키를 생성하기 위한 연구의 일환으로, 실수체 좌표를 소수점 이하 유효 자릿수로 대응하는 방법에 따른 키의 변화에 대한 연구를 수행하였다.

2. 공개키 암호시스템

2.1 공개키 암호

공개키 암호시스템은 비밀키 암호시스템에 비하여 상대적으로 처리 속도가 느린 단점을 가지고 있다. 그러나 암호시스템을 이용하는 사용자가 늘어나고 암호 서비스에 대한 다양한 요구가 제기되면서 비밀키 암호에서 발생되는 키 관리와 인증 문제를 해결하기 위한 암호 알고리즘의 필요성이 대두 되었으며, 이러한 문제를 해결하기 위해 공개키 암호가 제안되었다. 공개키 암호는 소인수분해의 어려움을 기반으로 하는 RSA와 Rabin 암호 그리고 이산대수 문제를 기반으로 하는 ElGamal, 타원곡선 암호 등으로 구분할 수 있다.

[Table 1] The public key cryptography and symmetric key cryptography comparison

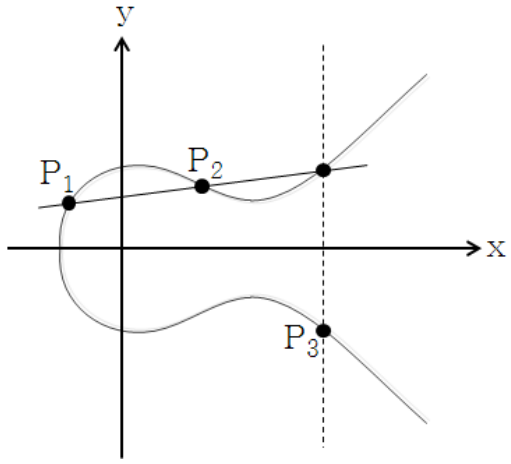
	Public key cryptography	Symmetric key cryptography
Key relationships	Encryption key ≠ Decryption key	Encryption key = Decryption key
Encryption key	public	private
Decryption key	private	private
Algorithm	public	public
Number of keys	2n	n(n-1)/2
Per capita number of key	1	n-1
Processing speed	slow	fast
Authentication	Anyone	Owner of the key

2.2 타원곡선 암호

타원곡선 이론은 약 150년 전부터 정수론과 대수기하학 분야에서 광범위하게 연구되어 왔으며, Andrew Wiles가 Fermat의 마지막 정리를 증명하면서 타원곡선 이론을 사용하였다. 타원곡선은 공개키 암호에서 요구되는 복잡한 연산을 수행하기 위한 방법을 제공하는 것으로, 타원곡선을 이용한 암호를 타원곡선 암호라고 한다. 타원곡선 (E)은 식 (1) 함수의 그래프 형태로 무한대의 특수한 점도 함께 포함된다.

$$y^2 = x^3 + ax + b \tag{1}$$

Fig. 1은 전형적인 타원곡선 그래프를 나타내고 있다.



[Fig. 1] Elliptic curve

Fig. 1에서 타원곡선 상의 두 점 P_1과 P_2를 지나는 직선을 그리게 되면 그 선은 타원곡선 상의 서로 다른 점과 만나게 된다. 타원곡선 상의 이 점은 x 축에 반사되어 P_1과 P_2의 합인 P_3을 얻을 수 있다[8].

타원곡선을 이용한 암호는 다른 공개키 암호와 비교하여 같은 수준의 보안성을 제공을 위해 필요한 비트 수가 적은 장점이 있다. 타원곡선 암호의 이러한 장점은 스마트폰과 같은 모바일 단말기와 같이 자원이 제한되는 환경에 보다 더 유리하게 적용할 수 있으며, 서로 다른 두 개의 암호 알고리즘이 주어진 키 사이즈에 대하여 동일한 안전도를 가진다는 것은 암호 알고리즘이 깨어지거나 암, 복호화에 사용된 키가 노출되는데 걸리는 시간이 같다는 것을 의미한다[8]. 따라서 주어진 키 사이즈에 대한 암호 알고리즘의 안전도는 일반적으로 키의 전수조사를 통하여 시도될 수 있는 시간을 의미한다. Table 2는 서로 다른 암호알고리즘에서 동일한 안전성을 갖기 위한 키 사이즈를 비교하여 나타내었다[6].

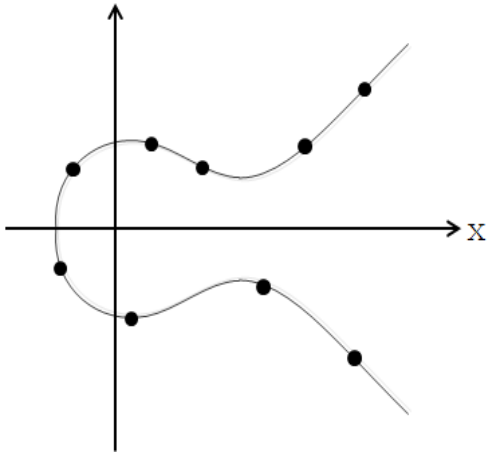
[Table 2] The comparison of safety of the cryptosystem

Symmetric key cryptography	RSA	ECC
	1,024	160
Triple DES	2,048	224
AES-128	3,072	256
AES-192	7,680	384
AES-256	15,360	512

3. 타원곡선 암호 키 생성

3.1 실수체 타원곡선 군 생성

타원곡선 위의 좌표(x, y)는 정수 좌표, 소수점이하 유한 자릿수 좌표, 소수점이하 무한 자릿수 좌표로 구성된다. 소수점이하 유한 자릿수로 나타나는 좌표는 소수점 이하 자릿수에 따라 원소의 개수가 결정되나 소수점 이하 무한 자릿수로 나타나는 좌표는 타원곡선 상에 정확하게 나타내지 못하는 문제점이 있다. 따라서 본 논문에서는 실수체로 구성되는 타원곡선 좌표들에서 소수점 이하의 적절한 유효자리를 갖는 좌표들만 추출하여 실수체 타원곡선 군을 생성한다. 이와 같이 생성된 실수체 군들의 좌표를 타원곡선 위에 나타내면 Fig. 2와 같이 구성될 수 있다.



[Fig. 2] Real number field group

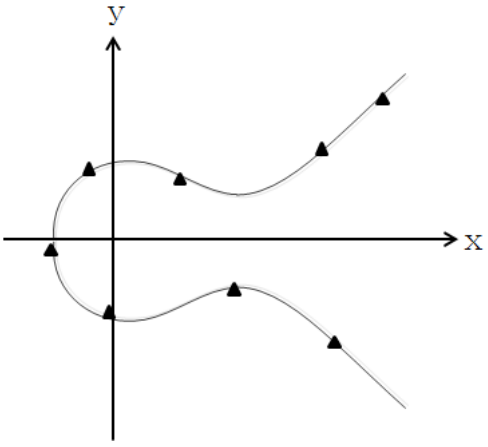
3.2 근사 점 생성

타원곡선 위의 한 점 P의 위수를 n이라고 하면 집합 $H = \{P, 2P, \cdots, nP = O\}$에서 H의 임의의 원소 Q에 대하여 적당한 자연수 k가 존재하여 $Q = kP$가 되고 여기서, k와 P를 알면 Q를 구하는 것은 어렵지 않지만 n이 충분히 클 경우 점 P와 점 Q가 주어질 때 k를 구하는 것은 쉽지 않으며, 이것을 타원곡선 이산대수 문제라고 한다.

본 논문에서는 소수점 이하 적절한 유효자리의 실수체 근을 사용하기 때문에 집합 H의 임의의 원소 Q가 타원곡선에 일치하지 않는 경우가 발생한다. 따라서 이러한 문제를 해결하기 위하여 Fig. 2와 같이 선택된 실수체 군에 대응시키는 과정이 필요하며, 이와 같이 실수체 군에 대응된 점들을 근사 점으로 정의한다[7]. 근사 점을 생성하기 위해 실수체 타원곡선 군에 대응시키기 위한 방법들

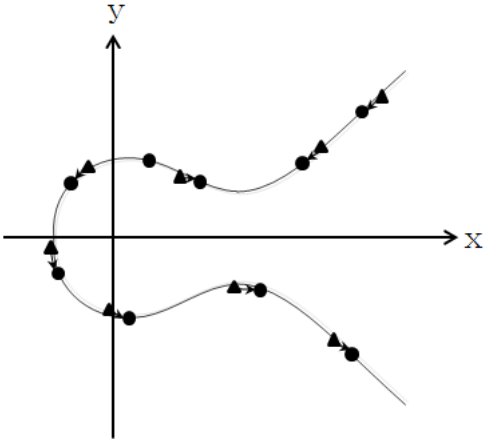
은 다양하게 고려될 수 있으나, 본 논문에서는 x 좌표를 기준으로 대응시키는 방법과 y 좌표를 기준으로 대응시키는 방법 그리고 x, y 좌표 중 가장 근접한 좌표를 기준으로 대응 시키는 방법들에 대하여 실험하였다.

Fig. 3은 생성된 임의의 실수체 $Q = kP$의 점들을 나타내고 있다.



[Fig. 3] Coordinates of real number field(Q=kP)

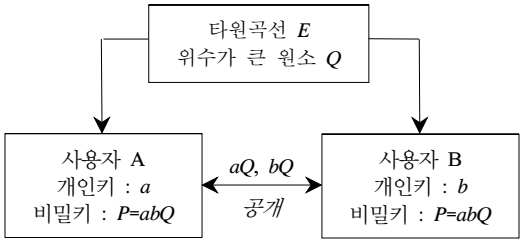
Fig. 4는 Fig. 3에 나타난 임의의 원소 Q를 x 좌표를 기준으로 소수점 이하의 적절한 유효자리를 갖는 Fig. 2의 점들로 대응시키는 방법을 나타내고 있다.



[Fig. 4] Generation of approximate coordinates

3.3 타원곡선 Diffie-Hellman 키 교환

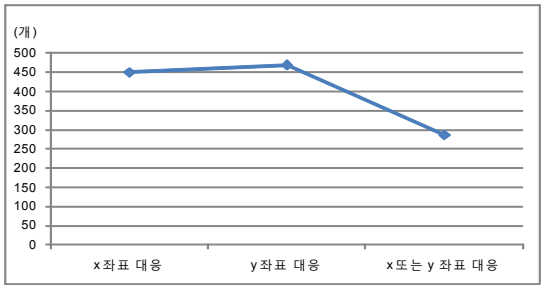
공개키 암호 체계의 효시가 된 Diffie-Hellman 키 교환 방법은 공개키가 공개되더라도 유한체의 이산로그 문제를 해결하기 전까지는 안전하기 때문에 소수 p가 충분히 크다면 Diffie-Hellman 키 교환 방법에 사용된 개인키는 노출될 가능성이 거의 없어지게 된다.



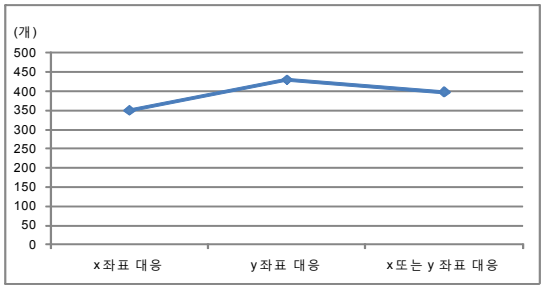
[Fig. 5] Elliptic curve Diffie-Hellman key exchange

4. 실험 및 결과

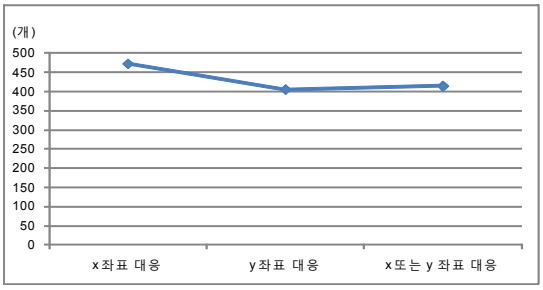
본 논문에서는 $y^2 = x^3 - ax - b$ 의 타원곡선 방정식에서 임의의 a, b 값을 사용하여 1,000개의 좌표를 생성한 후 소수점 이하 첫 번째 자리부터 열 번째 자릿수까지의 변화에 따라 근사 점 생성을 위한 실수체 군 대응 방법을 x 좌표 기준과 y 좌표 기준 그리고 x 또는 y 좌표 중 가장 가까운 좌표를 기준으로 하여 소수점 이하 열 자릿수까지의 좌표들에 대하여 실험하였으며, 계수 a와 b 값의 변화에 따른 소수점 이하의 자릿수의 평균적인 실험 결과는 Fig. 6에 나타내었다.



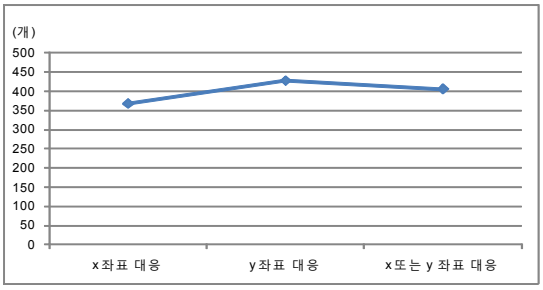
(a) a = 1, b = 6



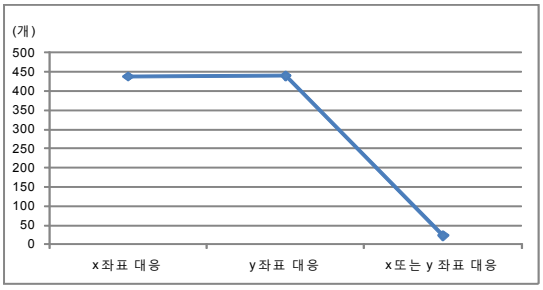
(b) a = 2, b = 5



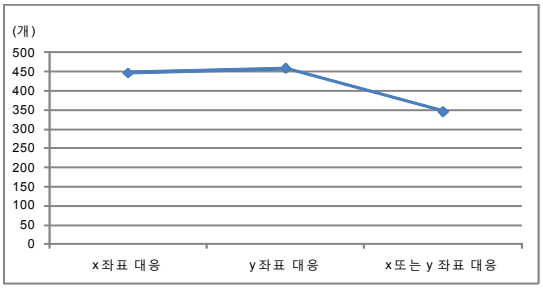
(c) a = 3, b = 4



(d) a = 8, b = 50



(e) a = 50, b = 21



(f) a = 190, b = 180

[Fig. 6] Experimental results

실험 결과를 살펴보면, 소수점 이하의 자릿수 변화에 따라 x 좌표와 가까운 좌표로 대응하는 방법과 y 좌표와 가까운 좌표로 대응하는 방법 그리고 x 또는 y 좌표 둘 중 가장 가까운 좌표로 대응하는 방법을 각각 적용하였을 경우, 근소한 실수체 군들의 차이가 나타내고 있으나 x 또는 y 좌표 중 가장 가까운 하나의 좌표로 대응 시키는 방법을 x, y 좌표 중 하나의 좌표로 강제적으로 대응시키는 방법과 비교할 경우 계수 a, b에 따라 대응 되는 실수체 군들이 급격하게 감소되는 현상이 발생됨을 알 수 있다. 이러한 이유는 Fig. 3의 실수체($Q=kP$) 원소들이 Fig. 2의 유효자리를 갖는 실수체 군들 중 하나의 실수체 좌표에 집중적으로 대응되기 때문이다.

5. 결론

타원곡선 암호를 실수체로 확장하여 암, 복호화를 위한 키를 생성할 경우 정수근만을 사용하는 경우보다 키를 선택할 수 있는 폭이 더욱 넓어지게 되어 더욱 효과적인 암호시스템을 구성할 수 있을 것이다. 본 논문에서는 타원곡선 암호를 실수체로 확장하여 사용하여도 암, 복호화가 가능하다는 연구 결과를 바탕으로 효율적인 키 생성을 위한 실수체 군 대응 방법에 대한 연구를 수행하였다. 실수체를 타원곡선 암호에 적용할 경우, 소수점 이하 유효 자릿수의 범위에 따라 선택할 수 있는 키의 범위가 달라질 수 있으며, 타원곡선 좌표에서 소수점 이하 자릿수가 길 경우 소수점 이하 자릿수를 적절한 유효 자릿수로 제한해야 한다. 그리고 타원곡선 위의 집합으로 계산된 실수체 좌표는 타원곡선 상에 정확하게 매칭 되지 않을 수 있기 때문에 이러한 좌표들은 타원곡선상의 유효 자릿수를 갖는 좌표들로 대응시키는 과정이 필요하다.

본 논문에서는 실수체를 갖는 타원곡선 암호에서 소수점 이하 유효 자릿수로 제한된 좌표들을 타원곡선 상의 좌표들로 대응시키는 과정에서 x좌표에 가까운 좌표로 대응 하는 방법과 y좌표에 가까운 좌표로 대응 하는 방법 그리고 x, y 좌표 중 가까운 좌표로 대응 하는 방법에 대한 연구를 수행하였다. 다양한 계수들에 대한 실험 결과, 대부분의 경우 실수체 군들은 근소한 차이를 나타내고 있었으나 x, y 좌표 중 가장 가까운 하나의 좌표로 강제로 대응 시키는 방법의 경우 계수에 따라 대응 되는 실수체 군들이 급격하게 감소되는 현상이 발생됨을 알 수 있었다. 이러한 이유는 실수체 원소들이 유효자리를 갖는 실수체 군들 중 하나의 실수체에 집중적으로 대응되기 때문인 것으로 예상된다. 향후 연구과제로는 다양한 측면에서 실수체 군을 생성하는 방법과 실수체 군에 대응시키기 위한 다양한 좌표 매칭 방법에 대한 연구가 필요할 것이다.

References

[1] David J. Malan, Matt Welsh, Michael D. Smith, "A Public-key Infrastructure for Key Distribution in TinyOS Based on Elliptic Curve Cryptography", First IEEE International Conference on Sensor and Ad-hoc Communications and Network, Oct. 2004.

[2] N. Koblitz, "Elliptic Curve Cryptosystems," Mathemetics of Computation, Vol. 48, pp.203-209, 1987.

[3] V. S. Miller, "Use of Elliptic Curves in Cryptography," in Advances in Cryptology-Proc. of CRYPTO'85, pp. 417-426, 1986.

[4] NIST, http://csrc.nist.gov/encryption

[5] IEEE, http://www.ieee.org

[6] Youngho Park, Public Key Encryption, Vol. 16, No. 3, Physics&High Technology, March, 2007.

[7] Eunhee Goo, Joonmo Kim, "Elliptic Curve Cryptography over the Real Number Plane," The 24th ITC-CSCC 2009, pp. 1177-1179, 2009.

[8] Mark Stamp, *Information Security:Principles and Practice*, Wiley, 2005.

우 찬 일(Chan-Il Woo) **[정회원]**

- 1995년 2월 : 단국대학교 대학원 전자공학과 (공학석사)
- 2003년 2월 : 단국대학교 대학원 전자공학과 (공학박사)
- 1995년 11월 ~ 1997년 2월 : LG이노텍(주) 연구원
- 2004년 3월 ~ 현재 : 서일대학교 정보통신과 교수

<관심분야>
정보보호, 디지털워터마킹, 데이터베이스 보안

구 은 희(Eun-Hee Goo) **[정회원]**

- 2002년 2월 : 단국대학교 대학원 전자컴퓨터공학과 (공학석사)
- 2009년 2월 : 단국대학교 대학원 전자컴퓨터공학과 (공학박사)
- 2011년 3월 ~ 2013년 2월 : 서일대학정보통신과 강의전담 교수

<관심분야>
정보보호, 암호 알고리즘, 네트워크, 모바일 프로그램

이 승 대(Seung-Dae Lee) **[정회원]**

- 1992년 2월 : 단국대학교 대학원 전자공학과 (공학석사)
- 1999년 8월 : 단국대학교 대학원 전자공학과 (공학박사)
- 1995년 4월 ~ 현재 : 남서울대학교 전자공학과 교수

<관심분야>
정보통신, 유무선통신, 정보보호