Journal of the Korea Academia-Industrial cooperation Society
Vol. 15, No. 9 pp. 5790-5795, 2014

http://dx.doi.org/10.5762/KAIS.2014.15.9.5790
ISSN 1975-4701 / eISSN 2288-4688

타원곡선 암호의 실수체 확장 연산항에 관한 연구

우찬일[1*], 구은희[2]
[1]서일대학교 정보통신과, [2](주)도넛시스템LSI

Study of the Real Number Field Extension Operand of Elliptic Curve Cryptography

Chan-Il Woo[1*], Eun-Hee Goo[2]
[1]Dept. of Information and Communication Engineering, Seoil University
[2]Donut System LSI Co., Ltd.

요 약 타원곡선 암호는 공개키 암호 알고리즘들 중에서 안전도가 매우 우수하여 정보보호 시스템을 구성하는데 있어 매우 중요한 부분으로 자리 잡고 있다. 그러나 타원곡선 암호는 실수체를 사용할 경우 계산이 느리고 반올림에 의한 오차로 인하여 정확한 값을 가질 수 없는 단점이 있어 최근까지 유한체를 기반으로 타원곡선 암호에 대한 연구가 이루어졌다. 만약, 타원곡선 암호를 실수체로 확장할 수 있다면 유한체 만으로 이루어진 타원곡선 암호시스템보다 다양한 키를 선택할 수 있는 장점이 있다. 따라서 본 논문에서는 실수체를 이용한 타원곡선 암호시스템에서 연산항 확장 방법을 사용하여 사용자가 선택할 수 있는 키 값을 보다 다양하게 하여 안전도가 높은 암호시스템을 구축할 수 있는 방법을 제안한다.

Abstract Elliptic curve cryptography (ECC) is an extremely important part of information protection systems because it has outstanding safety among public key encryption algorithms. On the other hand, as ECC cannot obtain accurate values using a real number field because of the slow calculation and errors from rounding off, studies of ECC have focused on a finite field. If ECC can be extended to the real number field, more diverse keys can be selected compared to ECC only based on a finite field. Accordingly, in this paper, a method for constructing a cryptographic system with a high degree of safety is proposed through the diversification of keys selected by the user based on the operant extension method instead of extracting keys only using integer values.

Key Words : Elliptic Curve Cryptography, Real Number Field, Encryption

1. 서론

정보통신 기술의 발전으로 인하여 다양한 형태의 개인 휴대 기기의 사용이 증가하고 있으며, 스마트폰과 같은 모바일 단말기들을 이용한 인터넷 뱅킹 또한 점점 더 증가하고 있다. 이와 같이 정보통신 기술의 발전은 언제 어디서나 필요한 정보를 얻을 수 있는 환경을 제공해 줄 수 있으나 개인 정보가 노출될 수 있는 문제점이 발생하고 있다. 따라서 이와 같은 정보보호 문제를 해결하기 위하여 새로운 암호 알고리즘에 대한 연구와 함께 보다 안전한 암호시스템을 구성하기 위한 연구가 활발하게 진행되고 있다.

일반적으로 암호시스템을 구성하기 위해 사용되는 암호 알고리즘은 대칭키와 비 대칭키 암호 알고리즘으로 구분할 수 있다[1]. 대칭키 암호 알고리즘은 속도가 빠른 장점이 있으나 키 보관과 분배 등의 문제가 있어 이러한 문제점들을 해결하기 위하여 공개키 암호 알고리즘이 개발 되었다. 공개키 암호 알고리즘은 소인수 분해의 어려움을 기반으로 한 방법과 이산대수 문제를 기반으로 한 방법으로 나눌 수 있다. 소인수 분해의 어려움을 기반으로 한 방법에는 RSA와 Rabin 알고리즘이 있으며, 이산대수 문제를 기반으로 한 방법으로는 ElGamal과 DSA

본 논문은 2014년도 서일대학교 학술연구비에 의해 연구되었음.
*Corresponding Author : Chan-Il Woo(Seoil Univ.)
Tel: +82-2-490-7556 email: ciwoo@seoil.ac.kr
Received Jun 23, 2014 Revised September 10, 2014 Accepted September 11, 2014

그리고 타원곡선암호가 있다[2-4].

공개키 암호 알고리즘은 대칭키 암호 알고리즘에 비하여 처리 속도는 떨어지는 단점이 있으나 암호화에 사용되는 공개키로 복호화에 사용되는 개인키를 유추하는 것이 매우 어려운 장점이 있다. 이러한 장점으로 인하여 공개키 암호 알고리즘은 다양한 분야에서 응용되고 있다. 공개키 암호 알고리즘들 중 RSA의 경우 키의 길이가 2048비트 이상이 되어야 안전한 것으로 평가되고 있다. 그러나 타원곡선 암호에서는 160비트 정도의 키 길이로 1024 비트의 RSA와 유사한 수준의 안전성을 보장할 수 있으며, 224비트의 타원곡선 암호는 2048비트의 RSA와 비슷한 수준의 안전성을 보장할 수 있다. 이러한 특성은 타원곡선 암호의 키 길이가 증가할수록 그 비율은 더욱 증가하여 300비트의 타원곡선 암호는 3,000비트의 RSA 보다 더 안전하게 된다.

공개키 암호시스템을 사용하는 곳에서는 다양한 공개키 암호 알고리즘을 사용할 수 있으나 이러한 공개키 암호 알고리즘들 중 타원곡선 암호는 가장 유용하게 사용되어 지고 있다. 타원곡선 암호시스템에 대한 연구는 지금까지 유한체를 기반으로 제안 되었다[5-7]. 그러나 타원곡선 암호를 실수체로 확장하여 암호시스템을 구성할 수 있는 방법이 제안되어 기존의 유한체 타원곡선 보다 더 안전한 암호시스템을 구성할 수 있게 되었다[8].

본 논문에서는 실수체를 기반으로 한 타원곡선 암호시스템에서 연산항 확장 방법을 사용하여 사용자가 선택할 수 있는 키 값을 보다 다양하게 하여 안전도가 높은 암호시스템을 구축할 수 있는 방법을 위해 기존에 사용되었던 유한체에 정의된 타원곡선 군 뿐만 아니라 실수체 위에 정의된 타원곡선 군을 사용한 연산항 확장 방법을 비교 분석한다.

2. 관련 연구

일반적으로 공개키 암호 시스템은 수학적 연산과 키 사이즈의 증가로 인하여 처리 속도가 느린 문제가 발생하는데, 이러한 문제는 타원곡선 위에 정의되는 값을 이용하여 이산 대수 문제를 정의하면 새로운 종류의 일방향 함수를 정의할 수 있어 키를 구하기 위한 계산 량과 키 사이즈를 어느 정도 해결할 수 있다.

2.1 타원곡선 정의

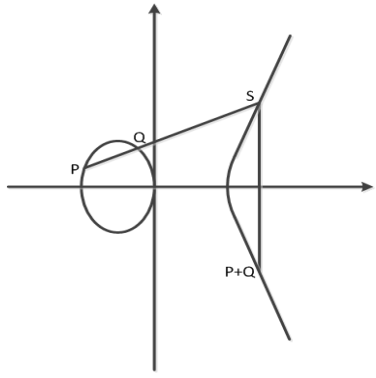
유한체 $GF(p)$상에 정의되는 타원곡선 군은 식 (1)에서 (x, y)의 좌표를 가진 점들로 구성된다.

$$y^2 = x^3 + ax + b \quad (1)$$

여기서, 계수 a와 b는 $a, b \in GF(p)$ 이고 $x^3 + ax + b$가 중근을 갖지 않으면 타원곡선 위에서 군을 정의할 수 있다.

2.2 타원곡선 이산대수 문제

타원곡선 이산대수 문제는 타원곡선 상의 임의의 한 점 P에 정수 k를 곱한 값이 $Q = kP$일 때, 사용자 또는 공격자가 점 P와 Q를 알고 있다 하더라도, P에 곱해지는 k를 계산하는 것이 어렵다는 점을 이용하는 것을 의미한다. 타원곡선 위의 임의의 점 P에 대해서 $P + O = O + P = P$ (O: 무한원점) 가 정의된다.



[Fig. 1] Elliptic curve

이와 같이 정의되는 값은 일정한 배수 $P = P + 2$, $15P = P + 5$ 와 같이 계산될 수 있다.

2.3 타원곡선 암호시스템

타원곡선 암호 시스템을 구성하기 위하여 타원곡선 군에 의하여 이산 대수 문제를 정의하고 이를 만족하는 $Q = kP$를 만족하는 k를 찾는다. 찾아진 k의 값이 타원곡선 상에 만족하는 k 값이면 이는 키 값이 되므로 타원곡선 암호 시스템에 적용할 수 있다.

즉, 키값을 생성하고 타원곡선 상의 값임을 증명할 수

있으면 이 값들을 이용하여 암호 시스템을 만들 수 있다. 그리고 이러한 값들은 ElGamal System을 이용하여 공통키 값을 교환 한 후 암호 시스템에 적용한다. 본 논문에서는 타원곡선 정의 방법과 암호 시스템에서 사용되는 값들을 기반으로 하여 실수체를 적용한 타원곡선 암호시스템을 평가한다.

3. 제안 방법

3.1 실수체 타원곡선 정의

실수체 타원곡선 암호시스템은 식 (1)의 타원곡선 방정식을 이용하여 타원곡선 군을 정의한다. 타원곡선 군에 정의되는 값들은 다양한 값들을 포함하는데, 기본적으로 이 값들은 타원곡선 상에 나타나는 (x, y) 좌표 값이 되므로 정수 쌍과 정수와 실수 값을 가지는 좌표 그리고 실수만의 좌표 값을 나타낸다.

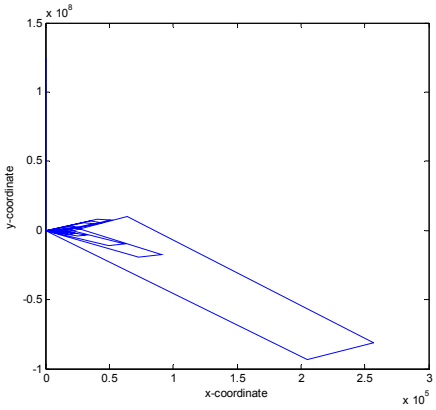
3.2 실수체 근사 타원곡선 군 생성

타원곡선 방정식에 사용되는 각 계수 값을 사용자가 선택하여 타원곡선 군(Q)을 생성한다. 원시원소 p로부터 실수체 타원곡선 군을 추출하기 위한 식은 다음과 같다.

$$s = \frac{(3x_P^2 - p)}{(2y_P)} \tag{2}$$

$$x_R = s^2 - 2x_P \tag{3}$$

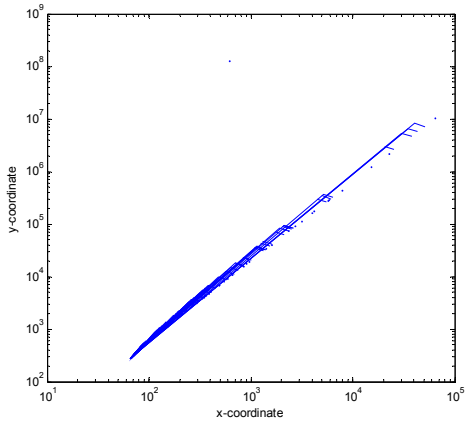
$$y_R = y_P + s(x_R - x_P) \tag{4}$$



[Fig. 2] Elliptic curve group by substituting coefficient value(a=2, b=3)

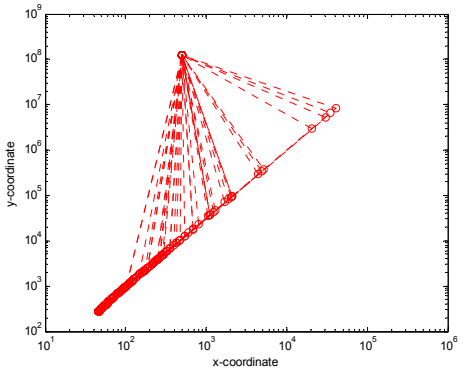
따라서 타원곡선 군 Q에 정의되는 값은 식 (1)을 이용하여 원시원소 p를 추출한 뒤 식 (2)에서 식 (4)까지를 이용하여 정의한다. Fig. 2는 식 (1)에서 계수 a와 b에 각각 2와 3을 대입하여 생성된 타원곡선 군을 나타내고 있다.

Fig. 3은 그림 2에서 구해진 좌표들을 키로 사용하기 위한 근사 타원곡선 군을 나타낸다. 여기서 사용되는 P(x, y) 점을 이산 대수 문제를 적용하여 정의하면 다양한 $1P$, $2P$ 등의 값을 찾을 수 있다.



[Fig. 3] The whole of approximate elliptic curve group by substituting coefficient value(a=2, b=3)

Fig. 3을 살펴보면 좌표 값들이 집중적으로 모여 있는 부분과 그렇지 않은 부분으로 구분된다. 타원곡선 암호 시스템에서는 일반적으로 집중적으로 모여 있는 좌표 값들을 주로 사용하고, 그 외에 나타난 값들은 무한대 값에 수렴하거나 좌표도 몇 개 되지 않아 가장 가까운 좌표 값으로 대체하여 사용한다. 이와 같이 타원곡선 방정식에 의하여 구해진 타원곡선 군은 이산 대수 문제를 적용시킨 $x = kP$를 사용할 때 임의의 원소 값들이 타원곡선 상에 정확하게 일치하지 않는 경우가 발생한다. 이를 해결하기 위하여 방정식에 의하여 구해진 타원곡선 상의 값과 암호 시스템에 사용되어질 $x = kP$ 값을 비교하여 정확하게 타원곡선 위에 일치하는 값을 선택한다. 이렇게 선택되어진 타원곡선 군이 정수 및 실수 값을 원소로 가지는 근사 값이 되는 것으로 앞에서 구한 타원곡선 군의 근사 타원곡선 군을 구하면 Fig. 4와 같이 표현할 수 있다.

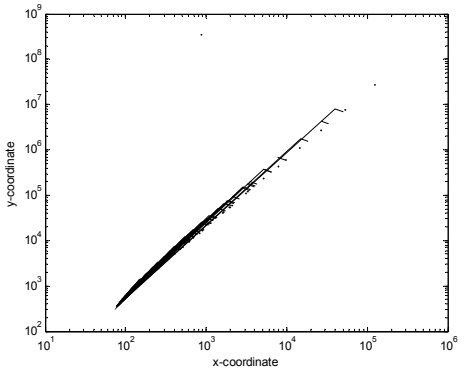


[Fig. 4] Log approximate elliptic curve group by substituting coefficient value(a=2, b=3)

Fig. 4에서 구해진 근사 타원곡선 군을 살펴보면 실제 Fig. 3과 같이 타원곡선 방정식에서 구한 타원곡선 군과 거의 유사한 점을 사용하는 것을 볼 수 있다. 그러나 근사 타원곡선 군이 구해진 그래프를 살펴보면 하나의 점이 유독 다르게 표현되어 있는 것을 볼 수 있는데, 이 좌표는 실수 값이 가지는 오차와 유한체 타원곡선에서 사용할 수 없는 무한대 점이 특정한 한 점으로 맵핑되어 사용되어 지는 것을 나타낸다.

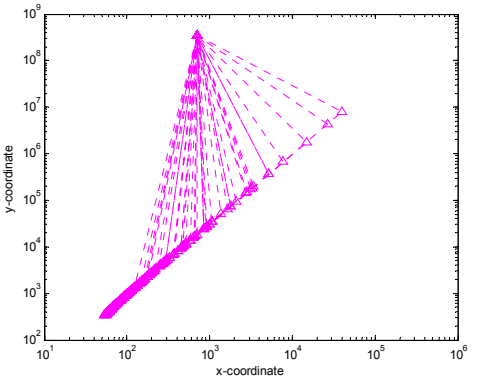
3.3 제안된 타원곡선 군 생성

타원곡선 군을 생성하기 위하여 타원곡선 방정식을 이용할 때 방정식 계수로 들어가는 a, b의 값은 일반적으로 정수 값을 기준으로 대입된다. 본 논문에서는 이 계수 값에 정수뿐만 아니라 실수 값을 함께 대입하여 그 특성을 평가한다.



[Fig. 5] The whole of approximate elliptic curve group by substituting coefficient value (a=0.127, b=72.5)

Fig. 5는 실수 계수 값 a=0.127, b=72.5를 사용하여 타원곡선 군을 구한 결과를 보여준다. Fig. 6은 실수 값을 이용하여 근사 타원곡선 군을 구한 결과를 나타낸다. 그림에서 정수 계수를 사용한 것과 유사한 근사 타원곡선 군이 구해지는 것을 알 수 있는데, 이것은 정수 좌표와 유한 자리수의 실수 좌표 그리고 무한대 점을 일정한 좌표 값으로 맵핑하는 좌표 등을 이용하여 암호 시스템을 구현할 수 있음을 나타낸다.



[Fig. 6] Log approximate elliptic curve group by substituting coefficient value(a=0.127, b=72.5)

3.4 실수체 타원곡선 암호시스템

제안된 시스템에서 사용될 근사점 타원곡선 군이 생성되면 구해진 실수체 근사 타원곡선 군을 이용하여 기존에 타원곡선 암호 시스템에서 사용되어지고 있는 비밀키 교환 과정인 Diffie-Hellman 키 교환 방법을 사용하여 암호 시스템을 구현할 수 있다. 비록 키 교환 과정은 비밀키 방식을 사용하는 것이지만 타원곡선의 유한체 이산로그 문제를 해결할 수 있기 까지는 사용자가 선택한 k 값을 알아내기가 어렵기 때문에 타원곡선 암호 시스템에서 많이 사용되어지는 방법이다. 또한 실수체를 사용하게 되면 실제 공격자가 유추해 낼 수 있는 단순한 정수 유한체 뿐만이 아닌 실수 값이 추가되어 사용되어지므로 많은 수의 전수 조사가 대입이 필요한 결과를 가져온다. 이러한 장점을 가진 실수체 기반의 타원곡선을 이용하고 사용자가 선택하는 계수 값 또한 실수 값을 사용한다면 전수 조사의 시간이 무한히 길어지는 것을 의미한다. 따라서 암호 시스템이 보다 안전해 지는 것을 기대할 수 있다.

4. 실험 및 결과

본 논문에서는 타원곡선 방정식을 이용하여 x, y 좌표 값을 추출할 때, 일반적으로 정수 값만을 사용하여 타원곡선 군을 생성하는 것이 아니라 계수 값 자체도 실수 값을 가질 수 있으므로 이를 이용하여 타원곡선 군을 생성한다. Table 1은 타원곡선 방정식의 계수 a와 b에 1부터 1,000까지의 값들을 대입한 후 근의 개수를 비교한 것을 나타낸다. 정수 계수 는 2, 5, 7씩 증가시키며 타원곡선 근의 개수를 구하였으며, 실수 계수는 0.2, 0.3, 0.5씩 증가시켜 각 구간에서 타원곡선 군을 생성하였다. 실험 결과 정수 계수를 가지는 타원곡선 군과 실수 계수를 가지는 타원곡선 군에서 각각의 근의 개수는 큰 차이가 없으나, 소수점 이하 자리수를 다양하게 할 경우 정수근만을 사용하는 경우에 비하여 보다 안전한 암호시스템을 구성할 수 있는 장점이 있다.

[Table 1] Comparison between finite number and real number

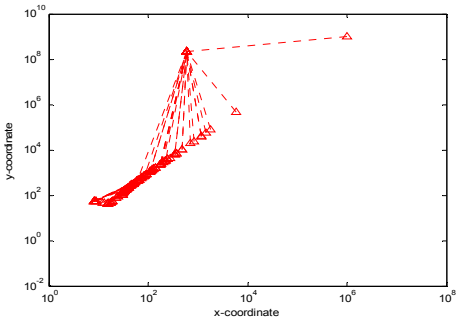
Coefficient		Finite number	Real number
a	b		
1~50	1~50	about 420	about 430
51~100	51~100	about 450	about 455
101~500	101~500	about 440	about 450
501~1000	501~1000	about 500	about 490

Table 2는 정수와 실수 계수의 근을 구할 때 소요되는 시간을 나타낸다. 이 결과 또한 정수 계수를 사용할 때와 실수 계수를 사용할 때 소요되는 시간과 비슷함을 알 수 있다.

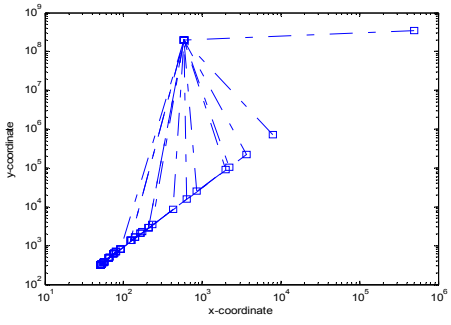
[Table 2] Time Comparison between finite number and real number

Coefficient		Finite number	Real number
a	b		
1~50	1~50	593ms	600ms
51~100	51~100	566ms	585ms
101~500	101~500	505ms	625ms
501~1000	501~1000	510ms	701ms

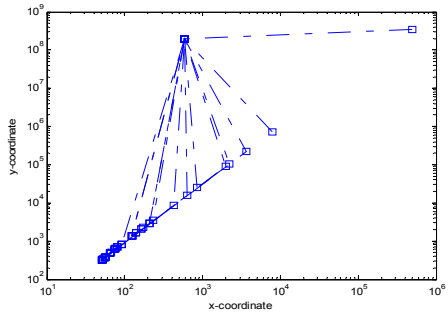
Fig. 7은 실수 계수를 이용하여 근사 타원곡선 군을 추출한 결과를 나타낸다. 실험 결과 정수를 사용한 Fig. 4와 유사한 결과가 나타남을 알 수 있다.



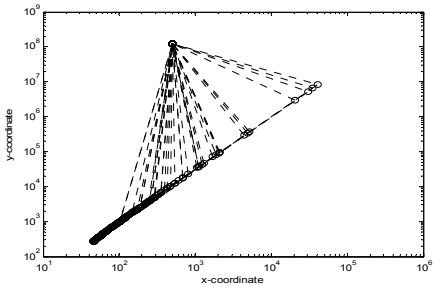
(a) a=3.9, b=56.2



(b) a=3.9, b=56.2



(c) a=67.2, b=0.875



(d) a=0.6, b=1.25

[Fig. 7] Log approximate elliptic curve group by substituting coefficient value

5. 결론

본 논문에서는 타원곡선 암호시스템에서 실수체를 기반으로 안전도가 높은 암호시스템을 구축하기 위하여 연산항 확장 방법을 사용하여 키를 보다 다양하게 선택하기 위한 방법을 제안 하였다. 제안 방법에서는 기존에 사용되었던 유한체에 정의된 타원곡선 군뿐만 아니라 실수체 위에 정의된 타원곡선 군을 사용하여 연산항을 확장하기 위한 방법을 정수체를 사용한 방법과 비교 분석하였다. 실험 결과 타원곡선 방정식의 계수에 실수 값과 정수 값을 각각 대입하여 생성되는 근의 개수는 비슷한 것을 알 수 있었으며, 이러한 이유는 계수 값에 어떠한 값을 사용하더라도 초기 값만의 변화를 가져오므로 키가 구해지는 범위에는 큰 변화가 없음을 알 수 있다. 그러나 정수 계수를 실수 계수로 확장하여 사용할 경우 타원곡선 군이 매핑 되는 근사 값의 범위에 따라 보다 안전한 암호 시스템을 구성할 수 있는 장점이 있다. 향후 연구과제로는 소수점 이하 자리 수에 따른 타원곡선 암호시스템의 특성에 대한 보다 다양한 평가 방법에 대한 연구가 필요할 것으로 생각된다.

References

[1] W.Diffie, M.E.Hellman, “New directions in cryptography,” IEEE Trans. on Information Theory, Vol. 22, No. 6, pp.644-654, 1976.
DOI: http://dx.doi.org/10.1109/TIT.1976.1055638

[2] T.ElGamal, “A public key cryptosystem and a signature scheme based on the discrete logarithm,” IEEE Trans. on Information Theory, Vol. 31, No. 4, pp. 469-472, 1985.
DOI: http://dx.doi.org/10.1109/TIT.1985.1057074

[3] M.O.Rabin, “Digitalized Signatures and public Key Functions as Interactable as Factorization,” Technical Report, MIT/LCS/TR212, MIT Lab., Computer Science, Cambridge, Mass 1979.

[4] R.L.Rivest, A. Shamir, L.Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” Communitations of the ACM, Vol. 21, No. 2, pp. 120-126, 1978.
DOI: http://dx.doi.org/10.1145/359340.359342

[5] M.Wiener and R.Zuccherato, “Fast Attacks on Elliptic Curve Crypto-system,” in Selected Areas in Crypto-graphy-SAC’98, 1998.

[6] A.Menezes, “Elliptic Curve Crypto systems,” CryptoBytes, Vol. 1, No. 2, pp. 1-4, 1995.

[7] V.S.Miller, “Use of Elliptic Curves in Cryptography,” in Advances in Cryptology-Proc. of CRYPTO’85, pp. 417-426, 1986.

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

우 찬 일(Chan-Il Woo) **[정회원]**

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

<관심분야>
정보보호, 암호 프로토콜, 디지털워터마킹

구 은 희(Eun-Hee Goo) **[정회원]**

- 2002년 2월 : 단국대학교 대학원 전자컴퓨터 공학과 (공학석사)
- 2009년 2월 : 단국대학교 대학원 전자컴퓨터공학과 (공학박사)
- 2011년 ~ 2013년 2월 : 서일대학교 정보통신과 강의전담 교수
- 2013년 3월 ~ 현재 : ㈜도넛시스템 LSI 책임 연구원

<관심분야>
정보보호, 암호 알고리즘, 네트워크, 모바일 프로그램