Journal of the Korea Academia-Industrial cooperation Society
Vol. 13, No. 2 pp. 795-800, 2012

http://dx.doi.org/10.5762/KAIS.2012.13.2.795

실수체 기반 타원곡선 암호시스템의 연산항 연구

우찬일[1*], 구은희[1]
[1]서일대학교 정보통신과

A Study on the Operation Components for Elliptic Curve Cryptosystem based on a Real Number Field

Chan-Il Woo[1*] and Eun-Hee Goo[1]
[1]**Dept. of Information and Communication Engineering, Seoil College**

요 약 최근 들어 유, 무선 네트워크를 통한 통신이 비약적으로 발전함에 따라 다양한 서비스가 통신망을 통하여 일상적으로 이루어지고 있다. 이에 따라 데이터 및 개인 정보를 보호할 수 있는 기술이 필수적으로 요구되어 지고 있으며, 이러한 정보보호 문제를 해결할 수 있는 보안 기술에 대한 연구가 활발하게 진행되고 있다. 본 논문에서는 다양한 암호 알고리즘들 중 타원곡선 암호의 키 선택 범위를 확장하기 위하여 실수체 기반 타원곡선 알고리즘의 연산항에 대한 연구를 수행하였다. 실험 결과, 실수체를 사용한 타원곡선 암호는 기존의 정수를 이용한 타원곡선 암호보다 다양한 키를 선택할 수 있어 보다 안전한 암호 시스템을 구현할 수 있음을 알 수 있었다.

Abstract Recently, as communication is evolved by leaps and bounds through wired/wireless networks, variety of services are routinely made through communication networks. Accordingly, technology that is for protecting data and personal information is required essentially, and study of security technology is actively being make progress to solve these information protection problems. In this paper, to expand selection scope of the key of elliptic curve cryptography, arithmetic items of real number based elliptic curve algorithm among various cryptographic algorithms was studied. The result of an experiment, we could know that elliptic curve cryptography using the real number can choose more various keys than existing elliptic curve cryptography using integer and implement securer cryptographic system.

Key Words : Elliptic Curve, Real Number, Information Security, Encryption, ECC

1. 서론

통신망의 발달과 모바일 단말기들의 발전으로 인하여 개인 정보 및 멀티미디어 데이터를 보호할 수 있는 방법에 대한 연구가 활발하게 진행되고 있다. 정보 보호를 위해 암호 시스템에 사용되고 있는 암호 알고리즘들은 고대시대부터 사용되던 치환과 전치를 이용한 단순 알고리즘에서부터 시작하여 현재는 수학적 이론을 바탕으로 한 알고리즘들을 적용하여 보다 안전한 암호 시스템을 만들 수 있게 되었다[1].

일반적으로 암호 시스템에서 사용되는 암호 알고리즘들은 암호문을 생성하거나 해독할 때 키를 사용하며, 이러한 키를 어떠한 방법으로 사용하느냐에 따라 대칭키와 공개키 암호로 나눌 수 있다. 만약, 송신자와 수신자가 동일한 키를 사용하여 암호문을 생성하고 해독할 경우 이를 대칭키 암호라고 한다. 대칭키 암호의 대표적인 것으로는 DES, SEED, AES 등이 있다. 또한, 송신자와 수신자가 각각 서로 다른 키를 사용하여 암호문을 생성하고 해독할 경우 이를 공개키 암호라 하고 RSA, ECC 등이 대표적인 공개키 암호에 해당한다[1-3]. 이와 같은 암호 시스템에 사용되는 키는 다양한 방법으로 생성할 수 있는데 컴퓨터 기술의 비약적인 발전으로 인하여 간단한

본 논문은 2011년도 서일대학 학술연구비에 의해 연구되었음.
*교신저자 : 우찬일(ciwoo@seoil.ac.kr)
접수일 11년 12월 15일 수정일 12년 01월 19일 게재확정일 12년 02월 10일

알고리즘을 사용하여 키를 생성하게 되면 쉽게 해독될 수 있어 보다 복잡한 알고리즘을 사용하여 키를 생성하거나 보다 긴 길이의 키를 사용하여 암호 시스템의 안전도를 향상시키고 있다. 대칭키 암호 알고리즘들은 일반적으로 256비트 이하의 키를 사용하고 있으며, 빠른 연산이 가능하여 소프트웨어 또는 하드웨어로 구현하기가 용이하다. 그러나 RSA 공개키 암호 알고리즘의 경우 1,024비트 이상의 키 사용을 권장하고 있으며, 지수승 연산으로 인하여 대칭키 암호에 비하여 연산 속도가 매우 느린 단점이 있다.

따라서, 공개키 암호에서는 보다 작은 크기의 키를 사용하여 1,024비트의 RSA와 동일한 안전도를 제공할 수 있다면 빠른 연산 속도와 보다 작은 메모리 공간 사용으로 인하여 활용도가 매우 우수한 공개키 암호 시스템을 구현할 수 있다. 공개키 암호 알고리즘들 중 타원곡선(elliptic curve)을 이용한 암호는 160비트의 키로 1,024비트의 RSA와 동일한 안전도를 제공할 수 있는 장점이 있으며, 타원곡선 전자서명 알고리즘(elliptic curve digital signature algorithm)이 IEEE와 NIST의 표준으로 채택되었다[3].

지금까지의 타원곡선 암호에 대한 연구는 유한체를 기반으로 한 정수근에 대하여 주로 이루어 졌다. 그러나 정수 기반의 타원곡선 암호에서는 선택할 수 있는 근의 개수가 실수체보다 제한되는 단점이 있어 본 논문에서는 타원곡선 군을 실수체로 확장하여 보다 많은 근을 선택할 수 있도록 타원곡선 방정식의 a와 b 값들의 변화에 따른 정수 근과 실수 근을 비교 분석하였다.

2. 관련 연구

2.1 타원곡선

타원곡선 이론은 약 150년 전부터 정수론과 대수기하학 분야에서 광범위하게 연구되어 왔으며, 1980년대 중반 Kobliz[5]와 Miller[6]에 의해 타원곡선 암호(ECC, elliptic curve cryptography)가 제안되어 현재까지 많은 관심을 모으로 있다. 타원곡선 암호는 타원곡선의 이산대수 문제(elliptic curve discrete logarithm problem)의 어려움을 기반으로 한 것으로 RSA 공개키 암호 알고리즘에 비해 현저히 작은 키를 사용하여도 동일한 안전도를 제공하는 장점이 있다. 즉, 타원곡선 암호는 160비트의 키로 1,024비트의 키를 갖는 RSA 암호 알고리즘과 동일한 안전도를 갖는 것으로 알려져 있다[1,8]. 표 1은 RSA 공개키 암호 알고리즘과 동일한 안전도를 갖는 타원곡선 암호 알고리즘에서 사용되는 키 길이를 비교한 것으로 타원곡선 암호가 상대적으로 작은 길이의 키를 사용하더라도 보다 긴 길이의 키를 사용하는 RSA 암호 알고리즘과 동일한 안전도를 가지는 것을 나타내고 있다[1,4].

[표 1] 동일한 안전도를 갖는 키 길이 비교
[Table 1] Comparison with length of keys that have equal safety

RSA (bits)	ECC (bits)	기타
512	106	5:1
768	132	6:1
1,024	160	7:1
2,048	210	10:1
21,000	600	35:1

2.2 타원곡선 알고리즘

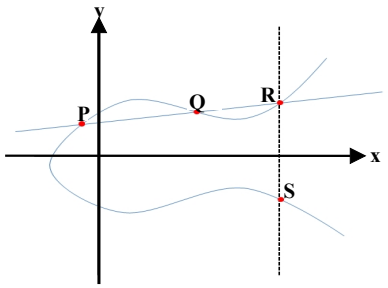
타원곡선은 유한체 상에 정의되어 타원곡선 군이 생성되며, 생성된 타원곡선 군은 식 (1)의 타원곡선 방정식을 만족하는 순서쌍들과 무한원점(point of infinity)을 포함하는 집합을 의미한다[3]. 즉, 타원곡선은 식 (1)과 식 (2)를 만족하는 (x, y) 점들의 집합을 의미하며, 사칙연산이 가능하고 항등원과 역원이 존재한다. 식 (1)에서 방정식 $x^3 + ax + b = 0$이 하나의 실근만 가지게 되면 타원곡선은 군이 되나 $x^3 + ax + b = 0$이 중근을 갖는 경우 타원곡선은 군이 되지 않는다. 따라서, 타원곡선 군은 $x^3 + ax + b = 0$이 중근을 갖지 않을 때 정의된다. 또한 실수체 위에서 $x^3 + ax + b = 0$이 서로 다른 세 실근을 가질 필요 충분 조건은 식 (2)에 해당한다.

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

$$4a^3 + 27b^2 \neq 0 \quad (2)$$

그림 1은 타원곡선을 나타낸다. 그림 1에서 타원곡선 위의 두 점 *P*와 *Q*가 서로 다른 경우, 이 두 점의 합을 구하기 위하여 *P*와 *Q*를 잇는 선을 그으면 타원곡선 위의 다른 점 *R*과 교차하는데 여기서, 점 *R*을 -(*P*+*Q*)로 정의하고 점 *R*의 *x*축에 대칭 이동되는 점 *S*는 *P*+*Q*로 정의한다.

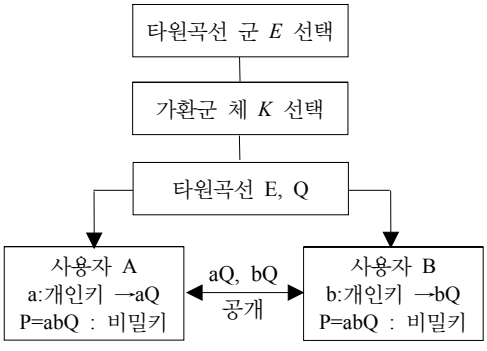
만약, 두 점 *P*와 *Q*가 같게 되면, 같은 점 *P*를 더한 경우와 같아 *P*+*P*=2*P* 연산을 통하여 2*P*를 구한다. 이와 같은 정의로 인하여 타원곡선이 정의된 유한체상의 원소를 구할 수 있다[8].



[그림 1] 타원곡선 그래프
[Fig. 1] Graph of elliptic curve

2.3 타원곡선 암호

타원곡선 $E(Z_p)$는 p(p는 소수)개의 원소를 갖는 유한체 (Z_p)의 점들로 구성되어 있다. 여기서, $E(Z_p)$의 임의의 두 원소 P와 Q가 주어졌을 때 위수 n과 연산하여 $Q=nP$를 만족하는 정수 n을 구하는 것을 이산대수 문제라 한다. 타원곡선 암호는 이러한 이산대수의 문제를 기반으로 만들어졌다. 여기서, n을 구하는 것은 매우 어렵다고 알려져 있으며 타원곡선의 이산대수 문제는 소인수 분해나 일반적인 이산대수 문제보다 훨씬 더 어려운 문제로 증명되고 있다. 타원곡선 암호의 안전성은 최초의 점에서 위수 n의 횟수만큼 덧셈 연산을 이용하여 이동함으로 마지막 점을 암호화 키로 갖기 때문에 원래의 시작점을 역추적하기가 상당히 어렵다는 점을 이용한다. 즉, nP를 얼마나 빠르게 찾아 낼 수 있느냐에 따라 암호의 효율성이 나타나는 것으로 결과의 점 Q의 값을 알고 있을 때 비밀키 n과 최초의 점 P를 밝혀내는 것은 불가능하다는 특성을 그대로 사용한다. Diffie-Hellman 비밀키 교환 알고리즘 및 Massey-Omura 암호 알고리즘 그리고 ElGamal 암호 알고리즘은 타원곡선 위에서 응용 될 수 있으며, 그림 2는 Diffie-Hellman 비밀키 교환 과정을 나타내고 있다 [3,8].



[그림 2] 타원곡선 Diffie-Hellman 키 교환
[Fig. 2] Exchange of elliptic curve Diffie-Hellman keys

3. 실수체 타원곡선 암호

3.1 실수체 문제점

타원곡선 암호에서 실수를 사용할 경우, 계산 속도가 느리고 반올림에 의한 오차로 인하여 정확한 값을 가질 수 없는 단점이 있어 일반적으로 타원곡선 암호에서는 실수를 사용하지 않았다. 그러나 본 논문에서는 컴퓨터 기술의 발전으로 인하여 실수를 사용하더라도 정수와 마찬가지로 계산될 수 있어 많은 시간 차이가 발생하지 않는다는 것을 전제로 실수체를 타원곡선 암호에 사용하며, 실수체를 사용함으로써 발생하는 반올림에 대한 오차는 실수체 타원곡선 군을 생성할 때 근사점 테이블을 사용하여 해결한다.

3.2 실수체 암호

3.2.1 타원곡선 군 찾기

실수체 위에서의 타원곡석 방정식인 식 (1)의 점 P, Q 및 $P+Q$의 좌표를 각각 (x_1, y_1), (x_2, y_2) 그리고 (x_3, y_3)라 할 경우, 다음 식들이 성립된다.

$$P \neq Q: \quad x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \qquad (3)$$
$$y_3 = -y_1 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3)$$

$$P = Q: x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1 \qquad (4)$$
$$y_3 = -y_1 + \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3)$$

여기서, 추출된 타원곡선 군은 정수 좌표, 소수점 이하 유한소수 자리까지의 좌표, 소수점 이하 무한소수 좌표 등이 추출된다.

3.2.2 근사 테이블 생성

타원곡선 군이 추출된 좌표 값들을 그대로 암호에 사용하게 되면 실수체 사용으로 인한 반올림 오차가 발생하기 때문에 이러한 문제를 해결하기 위하여 소수점 이하 일정한 길이의 자릿수까지 일치되는 좌표 값들을 추출하게 되는데 이를 근사 테이블이라 한다. 이것은 일반적인 타원곡선 암호에서의 근사 테이블이 생성되는 과정 및 타원곡선 군을 생성하는 과정과 동일하다.

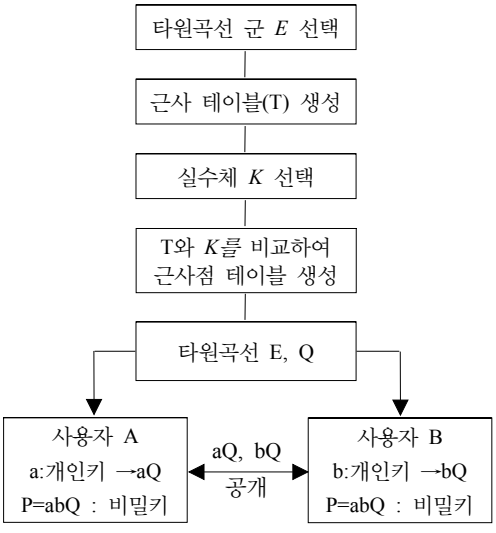
3.2.3 실수체 선택

근사 테이블에서 생성된 좌표 값을 임의로 하나 선택하여 타원곡선 암호의 가장 핵심인 이산대수 문제를 적용한 $Q=nP$를 구하는 연산을 통하여 원하는 좌표 값으로부터 Q를 추출하여 타원곡선 상에 나타낸다.

3.2.4 실수체 군 생성

앞에서 생성된 실수체 $Q=nP$ 값들은 실제로 타원곡선에 완벽하게 일치하지 않는다. 만약 이러한 값을 암호에 사용한다면 정확한 암, 복호화가 이루어지지 않을 것이다. 따라서 근사테이블에 $Q=nP$에서 추출한 값들을 대입하여 오차가 가장 적은 값으로 대응시킨다. 이렇게 대응된 값은 근사 테이블과는 다른 새로운 테이블을 생성하게 되는데 이 테이블은 실수체 군이 생성된 것으로 근사점 테이블이라고 부르며 이 실수체 군이 암호에 사용될 체가 된다.

그림 3은 실수체 군을 이용한 실수체 기반 타원곡선 알고리즘의 Diffie-Hellman 비밀키 교환 과정을 나타낸다. 실수체 기반 타원곡선 암호의 구조는 일반적인 타원곡선 암호와 동일하지만 타원곡선 군과 체(가환군)를 찾는 과정이 한층 더 복잡해 진다. 암, 복호화에 사용되는 키 생성 알고리즘이 복잡해지게 되면 암호 시스템의 안전도는 한층 더 높아진다.



[그림 3] 실수체 타원곡선 Diffie-Hellman 키 교환
[Fig. 3] Exchange of elliptic curve Diffie-Hellman keys

표 2는 유한체 ECC와 실수체 ECC를 비교하여 나타내었다.

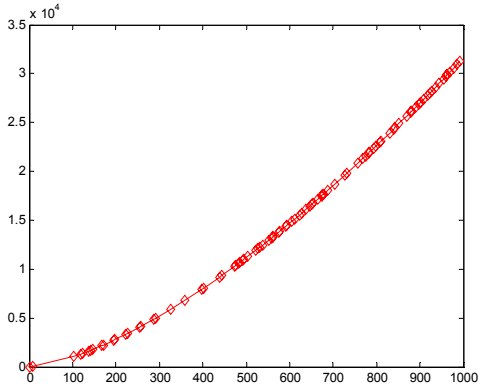
[표 2] 유한체와 실수체의 비교
[Table 2] Comparison between finite field and real number field

구분	유한체 ECC	실수체 ECC
타원곡선 군 생성	$y^2 = x^3 + ax + b$	$y^2 = x^3 + ax + b$ 사용할 값을 선택하여 근사 테이블 생성
K(체) 선택 및 Q 계산	생성된 E에서 ECC에 사용될 K 선택 nP를 이용하여 공개키 생성	생성된 실수 좌표를 이용하여 nP 선택 선택된 nP를 근사 테이블에 대응시켜 근사점 테이블생성
암/복호화	타원곡선을 이용하여 키 생성 후 메시지 암/복호화	

4. 실험 및 결과

본 논문에서는 실수체 타원곡선 군 생성에 필요한 식 (1)의 타원곡선 방정식에서 a와 b의 변화에 따른 정수근과 실수 근을 비교 분석하였다.

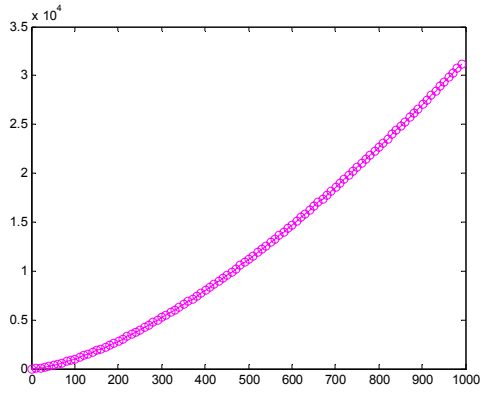
그림 4는 타원곡선 방정식에서 a와 b의 값을 각각 3과 4로 설정하였을 경우에 대하여 정수로 이루어진 x, y 좌표를 나타낸다.



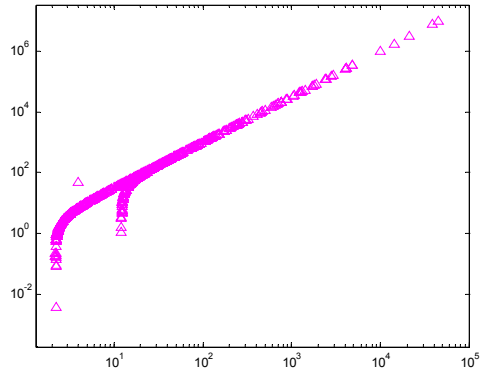
[그림 4] 타원곡선의 정수근 좌표
[Fig. 4] Finite field coordinate of elliptic curve

그림 5는 정수 및 소수점이하 12자리까지의 실수 값으로 나타나는 좌표들을 나타낸다.

그림 6은 $Q = nP$ 를 나타낸 그림이다. 암호화에 사용되는 실수체 군을 생성하기 위해 근사 테이블에 실수체 $Q = nP$ 를 대입하여 가장 오차가 작은 값으로 이동하여 새로운 실수체 군을 생성한다.

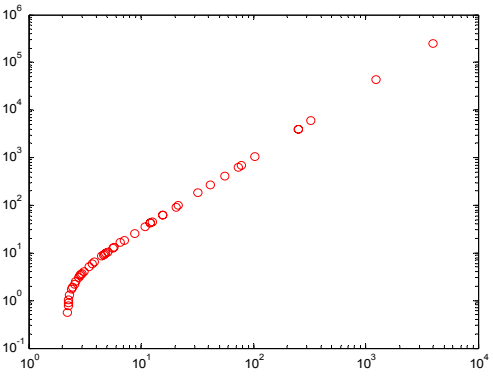


[그림 5] 타원곡선의 정수 및 실수근 좌표
[Fig. 5] Finite and real number coordinate of elliptic curve



[그림 6] 실수체 $Q = nP$ 생성
[Fig. 6] Real number field $Q = nP$ formation

그림 7은 근사 점들로 이동한 새로운 실수체 군을 나타낸다.



[그림 7] 실수체 군 생성
[Fig. 7] Real number field group formation

본 논문에서는 타원곡선 군 생성을 위해 a와 b의 범위를 1부터 1,000까지 변화 시켰으며 변수 x는 0.1에서 100까지 변화시킨 후 그에 따른 근의 개수를 비교 분석하였다.

[표 3] 유한체와 실수체의 근의 개수 비교
[Table 3] Comparison with the value numbers of value finite field and real number field

a	b	근의 개수	
		정수근	소수점 이하 12자리
…	…	…	…
1	192	1	104
5	200	1	107
14	562	1	113
20	756	2	105
55	26	2	110
123	403	2	98
352	699	2	223
687	942	2	88
755	7	1	96
970	661	3	97
…	…	…	…

타원곡선 방정식의 a와 b의 값 변화에 따른 근을 추출한 결과 표 3에서와 같이 실수 근의 개수가 정수근의 개수보다 a와 b 값의 모든 범위에 걸쳐 월등히 많이 생성됨을 알 수 있었으며, 어떤 특정 a와 b의 값 보다는 전반적으로 모든 a와 b에서 많게는 100개 이상 근의 개수가 차이 남을 알 수 있었다.

이와 같은 결과를 분석해 보면 특정 a, b 값에서 보다 많은 근을 생성하는 것이 아니라 어떠한 a, b 값을 갖더라도 실수체에서는 정수근에 비하여 상대적으로 많은 근을 얻을 수 있음을 알 수 있었다.

5. 결론

본 논문에서는 기존의 타원곡선 암호를 기반으로 실수체를 사용한 타원곡선 암호의 키 생성을 위한 연산항에 대한 연구를 수행하였다. 실험 결과 실수체를 암호 시스템의 키로 사용할 경우 기존의 정수근을 사용한 타원곡선 암호보다 월등히 많은 근을 생성할 수 있어 보다 다양한 키 선택을 할 수 있음을 알 수 있었다. 또한 실수체를 생성하는데 있어서 특정 데이터가 아닌 랜덤하게 선택된 값을 사용하더라도 정수근과 비교하여 월들이 많은 수의 근을 생성할 수 있음을 알 수 있었다.

본 연구의 초기 목적은 실수체를 가장 많이 생성하기 위한 a와 b 값을 찾아내는 것이었지만 실험을 통하여 특

정 a, b 값이 아닌 어떠한 값을 대입하더라도 일정 수준 이상의 결과를 도출할 수 있음을 알 수 있었다. 결과적으로 실수체를 타원곡선 암호에 적용하게 되면 키 선택에 있어서 보다 다양한 키를 선택할 수 있어 암호 시스템의 안전도가 매우 향상될 수 있을 것으로 생각된다. 향후 연구과제로는 연산 속도를 향상 시킬 수 있는 방법과 실수체 군 생성에 대한 보다 다양한 연구가 필요할 것으로 생각된다.

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] B.Schneier, "Applied Cryptography," John Wiley & Sons, 1996.

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

[4] Lee Jee Myong, Lee Chan Ho, Kwon Woo Suk, “Design of Programmable and Configurable Elliptic Curve Cryptosystem Coprocessor”, Journal of The IEEK, Vol 42-SD, No. 6, pp. 67-74, June, 2005.

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

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

[7] I.F. Blake, G. Seroussi, and N.P. Smart, Elliptic Curves in Cryptography, Cambridge University Press, 1999.

[8] Suntae Hwang, Seung Hyek Lee, "An Efficient Digital Contents Cryptosystem using Elliptic Curve Cryptography Algorithm", Journal of Information Technology Applications and Management, Vol. 11, part 4, pp. 25-33, 2004. 12.

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 ~ 현재 : 서일대학교 정보통신과 강의전담 교수

<관심분야>
정보보호, 암호 알고리즘, 네트워크, 모바일 프로그램