결정론적인 소수 생성에 관한 연구

박 중 길[†] · 박 봉 주[††] · 백 기 영[†] · 천 왕 성[†††] · 류 재 철[††††]

요 약

비대칭 암호 알고리즘을 설계하는 데 있어서 매우 큰 소수를 구하는 것은 필수적이다. 그러나 지금까지는 결정론적인(deterministic) 큰 소수를 발견하기는 매우 어려웠기 때문에, 일반적으로 확률적으로 소수일 가능성이 높은 의사소수(pseudoprime)를 비대칭 암호 알고리즘에서 사용하였다. 이 논문에서 결정론적인 소수 생성 방법을 제안하며, 제안된 방법에 의해 생성된 소수는 증명이 가능한 100% 정확한 소수이다. 또한 이 방법에 의해 생성된 소수는 신뢰성, 비도, 원시원소(primitive element) 생성 능력 등을 보장한다.

A Deterministic Method of Large Prime Number Generation

Jung-Gil Park[†] · Bong-Joo Park[††] · Ki-Young Baek[†] · Wang-Sung Chun[†††] · Jae-Cheol Ryou[††††]

ABSTRACT

It is essential to get large prime numbers in the design of asymmetric encryption algorithm. However, the pseudoprime numbers with high possibility to be primes have been generally used in the asymmetric encryption algorithms, because it is very difficult to find large deterministic prime numbers. In this paper, we propose a new method of deterministic prime number generation. The prime numbers generated by the proposed method have a 100% precise prime characteristic. They are also guaranteed reliability, security strength, and an ability of primitive element generation.

1. 서 론

광범위한 정보 유기체인 인터넷등 각종 정보 통신망에서 가장 중요한 자산인 정보를 외부의 위협으로부터 보호하는 것은 매우 중요하다. 이 정보 보호의 수단으로 암호화 메커니즘을 사용하며, 이들 암호화 메커니즘은 대칭 암호, 비대칭 암호가 있으며, 대칭암호 체계는 소규모의 네트워크에서 적합한 체계로서 보다 광범위한 형태로 운용되는 네트워크 환경에서 대칭암호 체계를 사용한다면, 키 관리가 매우 어렵게 되기 때문에 키 관리가 용이한 비대칭 체계를 적용할 수 밖에 없다. 이러한 비대칭 시스템은 소수의 특성을 이용하여 구축되며, 특정한 소수에 대하여 그에 따른 비밀키/공개키 등을 생성하게 된다[1, 2]. 그러므로 올바르고 안전성 있는 소수의 생성이 키의 안전성(512 비트 이상의 소수)에 기본이 된다.

오늘날 컴퓨터의 처리 능력 향상으로 인하여 보다 높은 수준의 정보 보호가 요구되며, 그에 따라 키의 크기가 늘어날 수 밖에 없다. 키의 크기가 증가되면 소수의 크기도 증가되어 정확한 소수를 생성하는 것이 중요한 문제로 대두된다. 이전의 소수 생성 방식은 임의의 수를 생성하여 소수인가를 확률적으로 검증하므로 채택된 소수가 확실한 소수인지를 증명할 수 없었다[1, 3-6]. 이러한 소수 생성 방식의 단점을 보완하여 100% 정확한 소수를 생성하는 알고리즘을 제안한다.

† 준 회 원 : 충남대학교 대학원 컴퓨터과학과
†† 정 회 원 : (주)테크노밸리 책임연구원
††† 정 회 원 : 한국통신공사 멀티미디어연구소
†††† 종신회원 : 충남대학교 컴퓨터과학과 교수

논문접수 : 1999년 11월 17일, 심사완료 : 2000년 8월 31일

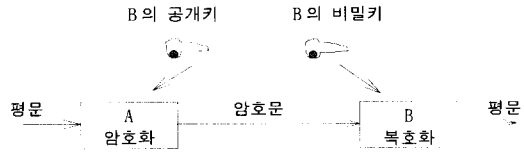
이 방식에 의해 생성된 소수는 비도 측면에서 강하고 확실한 소수 특성을 만족하며, 원시원소의 생성 능력도 제공한다.

2. 소수 기반의 보안 메커니즘

소수에 기반을 둔 보안 메커니즘은 크게 비대칭 암호시스템(공개키 암호시스템), 디지털 서명(digital signature), 그리고 인증(authentication) 등이 있다[1, 2].

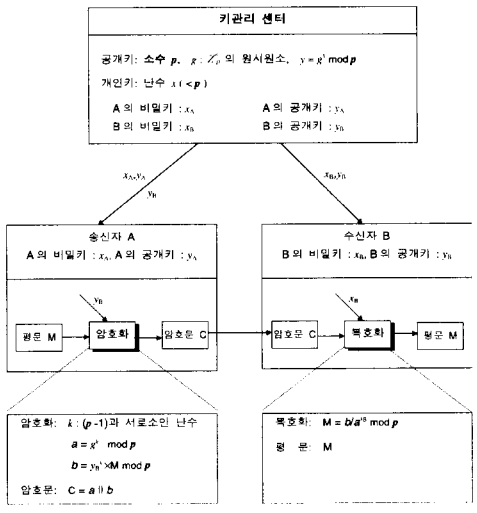
2.1 비대칭 암호시스템

비대칭 암호 시스템은 (그림 1)에서 보듯이 공개키와 비밀키로써 암복호화를 수행한다. 대표적인 비대칭 알고리즘은 RSA, ElGamal, Elliptic Curve Cryptosystem과 같은 것들이 있다[1].



(그림 1) 비대칭 암호 시스템

이와 같은 알고리즘들은 서로 유사하게 구현되었으며, 큰 소수를 기반으로 생성된 키를 사용하여 암/복호화를 수행한다. 대표적인 것으로 ElGamal 알고리즘을 사용한 비대칭 시스템은 (그림 2)에서 보는 바와 같다.

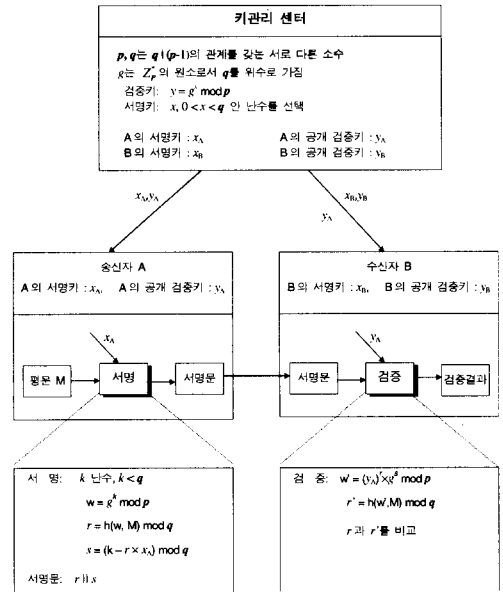


(그림 2) ElGamal 알고리즘

2.2 디지털 서명

디지털 서명은 메시지의 무결성, 송신자 인증, 부인-봉쇄를 지원하는 메커니즘이다. 대표적인 디지털 서명 알고리즘들은 DSA(Digital Signature Algorithm), DSA 유사형, GOST 알고리즘, 그리고 Schnorr 알고리즘이 있다[1].

이와 같은 알고리즘들도 서로 유사한 방법으로, 큰 소수를 기반으로 생성된 키를 사용하여 서명 생성 및 검증을 수행한다. 대표적인 것으로 Schnorr 알고리즘을 사용한 디지털 서명 시스템은 (그림 3)과 같이 구현된다.

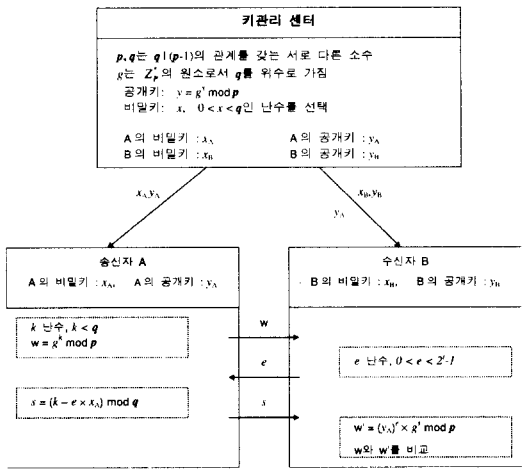


(그림 3) Schnorr 디지털 서명 알고리즘

2.3 인 증

인증은 메시지 송수신자가 서로의 신원을 확인하는 절차로 구성된 메커니즘이며, Fiat-Shamir, Micali-Shamir, Guillou-Quisquater, Schnorr, 그리고 Brickell-McCurley등의 인증 방식이 있다[1].

이와 같은 알고리즘들도 서로 유사한 방법으로, 큰 소수를 기반으로 생성된 키를 사용하여 상호 인증을 수행한다. 대표적인 것으로 Schnorr 알고리즘을 사용한 상호 인증 시스템을 (그림 4)에서 설명한다.



(그림 4) Schnorr 인증 알고리즘

3. 새로운 소수 생성 알고리즘 설계 및 구현

3.1 소수 생성

일반적으로 사용되고 있는 소수 생성 방법은 요구되는 크기의 범위에서 임의의 홀수를 선택하여 소수인가를 검사하는 것이다. 만일 아니라면 다른 임의의 홀수를 선택하여 소수 판정 법을 다시 반복 수행한다. 기존의 소수 생성 방법은 소수 판정 법에 대한 기법을 중심으로 개선되어 왔으나 대부분 확률적인 검사법이었다. 그러므로 소수로 채택된 것도 100% 신뢰할 수 없는 의사소수라고 할 수 있다.

기존의 소수 생성 절차를 보면 다음과 같다.

단계 1. 난수 발생기 등을 사용하여 홀수 n을 선택한다.

단계 2. 소수 판정 법을 수행한다(k 회 반복). 만일 검사에 실패하면 1 단계를 다시 수행한다.

단계 3. 만일 n이 충분한 신뢰성이 있다면 소수로 선택하고, 아니면 1 단계를 다시 수행한다.

위에서 사용되는 기존의 소수 판정 법을 분류해 보면 다음과 같다 [3-8].

〈표 1〉 소수판정 분류

소수판정 분류	방 법
인수 분해를 이용하지 않는 방법	• Solovay-Strassen : 확률적인 의사소수 판정법 (1978년)
N-1 인수분해를 이용하는 방법 (이러한 형태의 소수 N은 희박함)	• (N-1)이 인수 분해가 가능한 경우만 소수로 판정이 가능한 방법 • Rabin-Miller의 방법 : 확률적인 강한 의사소수 판정법 (1976) • Fermat 정리의 역
N+1 인수분해를 이용하는 방법 (이러한 형태의 소수 N은 희박함)	• (N+1)이 인수 분해가 가능한 경우만 소수로 판정이 가능한 방법 • 연분 수를 이용하는 판정 방법(1975년) • Lucas 판정 방법(1969년)
Jacobi Sum Test	• 10 진수 10000자리 이상일 때 효과적임 (1981년)

3.2 이론적인 배경

비대칭 암호시스템의 강도(안전성 정도)는 매우 큰 수의 소인수 분해와 이산대수의 어려움에 기초를 둔다. 주어진 자연수 a, x, p에 대하여,

$$y = a^x \bmod p \tag{1}$$

를 구하는 방법은 많이 알려져 있으며, 쉽게 계산이 가능하다. 그러나 일반적으로 y, a, p를 알고 x를 구하기는 어려우며, 특히 p가 매우 큰 소수일 경우 x를 구하기란 이산대수(discrete logarithm) 문제로 현실적으로 불가능하다[1, 2]. 이러한 이론에 근거한 ElGamal 암호시스템과 Diffie-Hellman의 키분배 알고리즘 등의 암호시스템을 구축하기 위해서는 매우 큰 소수가 필수적이다.

정리 1 임의의 양의 정수 n 에 대하여 다음 두 식은 동치이다[9].

(1) n은 소수.

(2) $g^{n-1} \equiv 1 \bmod n$을 만족하는 $g \in Z_n^*$가 존재하고, $p|(n-1)$을 만족하는 모든 p에 대하여 $g^{(n-1)/p} \neq 1 \bmod n$이다.

정리 1은 임의의 정수 n에 대하여 n이 소수인지 아닌지를 명확하게 판단할 수 있는 방법에 대하여 설명하고 있다. 단, 그 선행조건으로 n-1을 소인수 분해할 수 있어야 한다. 즉, n-1을 소수의 곱으로 표현할 수 있어야 한다. 이 조건을 만족하는 n에 대해서만 소수인가를 판별할 수 있으므로 매우 큰 수(512 비트 이

상)에 대하여 정리 1을 소수 판정 법으로 사용하기에는 극히 제한적인 범위에 한하여 가능한 것으로 알려져 왔다. 그러나 정리 1을 이용하면 매우 큰 소수를 발생시킬 수 있는 알고리즘을 만들 수 있음을 이 논문에서는 제시한다.

ElGamal 암호시스템과 Diffie-Hellman의 키분배 Z_n^*의 원시원소 g를 구하여 사용하고 있다. 정리 2는 이와 같은 g를 구하는 방법을 보여준다.방식에서는 소수 n에 대하여

정리 2 임의의 소수 n과 $g \in Z_n^*$에 대하여 다음 두 식은 동치이다[9].

(1) g는 Z_n^*의 원시원소이다.

(2) $g^{n-1} \equiv 1 \bmod n$이고, $p|(n-1)$을 만족하는 모든 p에 대하여 $g^{(n-1)/p} \neq 1 \bmod n$ 이다.

3.3 알고리즘 설계 및 구현

먼저 홀수인 소수 P를 선택한다. 이때 P는 작은 소수이어도 가능하다. 그리고 또 하나의 홀수인 소수 H를 선택하여 N을 다음과 같이 둔다.

$$N = 2 \times P \times H + 1 \quad (2)$$

그러므로 N-1의 소인수는 2, P, H이다. 이와 같은 N에 대하여 정리 1을 이용하여 소수인가를 판별한다. N이 소수가 아닌 경우에 다른 홀수 소수 H'를 선택하여

$$N = 2 \times P \times H' + 1 \quad (3)$$

으로 하고, 반복하여 정리 1을 적용하여 소수인가를 판별한다.

이와 같은 방법으로 처음 소수 P 보다 큰 또 다른 소수 N을 구할 수 있다. 소수 도약 알고리즘을 단계별로 구성하면 다음과 같다.

알고리즘 1. 소수 도약

단계 1. 소수 P를 선택
단계 2. 작은 소수 H를 선택
단계 3. $N = 2 \times P \times H + 1$
단계 4. if ($2^{N-1} \neq 1 \bmod N$) then goto 단계 2
단계 5. if ($2^{(N-1)/P} = 1 \bmod N$) then goto 단계 2
단계 6. if ($2^{(N-1)/2} = 1 \bmod N$) then goto 단계 2
단계 7. if ($2^{(N-1)/H} = 1 \bmod N$) then goto 단계 2
단계 8. N은 소수이다.

단계 8에서 생성된 소수 N을 P로 놓고 알고리즘 1을 반복 수행하는 방법으로서 원하는 크기의 소수를 구할 수 있다. 이와 같은 방법으로 원하는 크기의 소수를 생성하는 알고리즘은 다음과 같다.

알고리즘 2. 소수 생성

단계 1. 소수 P를 선택
단계 2. 소수 도약(알고리즘 1)을 수행하여 확장된 소수 N을 생성
단계 3. 소수 N이 원하는 크기(n 비트)가 아닐 경우, N을 P로 놓고 하여 단계 2 수행

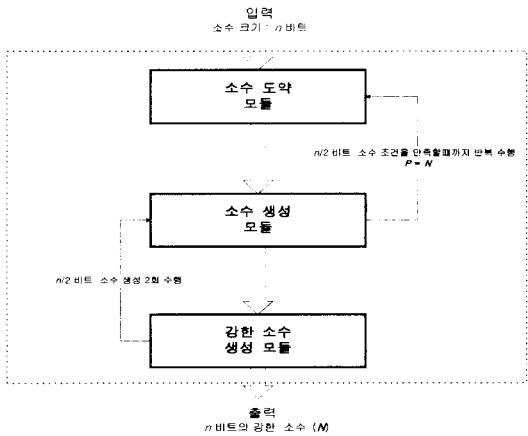
이 알고리즘에 의해 생성된 소수는 강한 소수라고는 할 수 없는데, 이는 최종 생성된 소수는 매우 큰 소수 P와 작은 소수 H에 대하여 $2 \times P \times H + 1$ 형태로 이루어져 있기 때문이다[1].

그러나 다음과 같은 알고리즘에 의해 원하는 크기(n 비트)의 강한 소수를 구할 있다.

알고리즘 3. 강한 소수 생성

단계 1. 소수 생성(알고리즘 2.)을 이용하여 $n/2$ 비트 소수 P를 생성
단계 2. 소수 생성(알고리즘 2.)을 이용하여 $n/2$ 비트 소수 H를 생성
단계 3. $N = 2 \times P \times H + 1$에 대하여 정리 1을 이용하여 N이 소수인가 판단 N이 소수가 아니면 단계 2 수행

제안한 소수 생성 알고리즘의 전체적인 블럭 구성도는 (그림 5)와 같다.



(그림 5) 강한 소수 생성 알고리즘의 구성도

3.4 검증 및 평가

생성된 소수에 대하여 평가할 수 있는 기준은 소수의 신뢰성, 비도, 원시원소 g 값 생성 능력, 수행 시간으로 분류할 수 있다. 보안에 관련된 암호시스템, 키 분배, 디지털 서명, 상호 인증 알고리즘에 적용되는 소수는 그 자체의 특성 뿐만이 아니고 알고리즘의 특성을 만족해야 한다. 특히, g 값은 알고리즘 전체의 성능에 영향을 미치는 값으로서 모든 소수에 대해 용이하게 생성되는 것이 아니므로 생성된 소수에 대하여 g 값을 생성하지 못한다면 의미를 잃게 된다. 다음은 각 기준에 대하여 설명하고 있다.

- 소수의 신뢰성
  - ○ 생성된 소수가 100% 소수 인가를 의미한다.

- 비 도
  - ○ 보안 시스템의 공격 위험을 분석했을 때, 강한 소수인 경우는 위험이 낮은 것으로 평가되는 반면에 약한 소수인 경우는 위험도가 높다.
  - ○ 소수를 N이라 했을 때, $(N-1) = A \cdot B$로 구성된다고 가정하면 A, B의 크기가 비슷한 경우 N을 강한 소수라 할 수 있으며, 차이가 큰 경우 약한 소수라 한다. 강한 소수는 인수 분해에 의한 분석이 어렵다는 것을 의미한다.

- 원시원소 g 값 생성 능력
  - ○ 비대칭 방식을 적용하는 키분배, 암호화, 디지털 서명 알고리즘은 원시원소 g 값을 생성하여 사용하고 있다. 기존의 알고리즘을 이용하여 생성된 소수에서 g를 생성하는 문제는 매우 중요하다.
  - ○ g는 $(p-1)$이 소인수분해 가능한 p에 대하여 정리 2를 적용하여 구할 수 있다. 그러나 임의적으로 발생시킨 난수인 p에 대하여 $p-1$을 인수분해하는 문제는 NP-complete이므로 g를 생성할 수 있는 확률은 매우 희박하다.

이와 같은 기준에 의해 기존의 소수 생성 알고리즘과 제안한 소수 생성 알고리즘을 비교 분석한 내용을 <표 2>, <표 3>에서 비교 분석하였다.

〈표 2〉 기존의 소수 생성 알고리즘 평가

소수 판정법	신뢰도	비 도	원시원소 g 값 생성 능력
Solovay-Strassen	의사소수	확률적인 안전성	확률적으로 생성
Rabin-Miller	의사소수	확률적인 안전성	확률적으로 생성
Fermat 정리의 역	의사소수	확률적인 안전성	확률적으로 생성
Lucas 판정 방법	의사소수	확률적인 안전성	확률적으로 생성
Jacobi Sum Test	의사소수	확률적인 안전성	확률적으로 생성

〈표 3〉 제안한 소수 생성 알고리즘의 성능 평가

판정법 / 비교 기준	기존 소수 판정법	제안한 소수 생성 알고리즘
소수의 신뢰성	● 확률 1에 근사한 소수를 생성하는 방법으로, 소수의 신뢰성은 반복 회수의 증가에 의존한다 ($1-2^{k}$ 확률의 신뢰도). ● 의사소수	● 소수
소수의 비도	● 생성된 소수는 임의의 난수이므로 비도는 확률적으로 측정 가능.	● 강한 소수를 생성함. ● 외부의 공격(소인수분해, 이산대수 문제)이 어려우므로 전산망 보안 체계에 적합함.
원시원소 g 값 생성능력	● g 값은 소수 N에 대해 $N-1$이 소인수분해 가능해야 생성할 수 있음. ● 확률적으로 생성된 소수에 대하여 g 값을 생성.	● $N-1 = 2 \times P \times H$의 식에 의하여 생성되므로 100% g 값을 생성할 수 있음.
수행시간 및 효율성	● 소수생성 시간이 랜덤함. ● 강한 소수를 생성하기 위해서 소수 N에 대해 $N-1$이 작은 소수를 갖는 것을 배제하는 과정이 별도 필요함(이 과정에서 소인수분해의 어려움 때문에, $N-1$이 일정 크기(약 70 비트) 이상의 작은 소수를 갖지 않는다는 보장은 거의 불가능함).	● 소수생성 시간이 다소 랜덤함(전체적인 수행시간은 확률적인 방법과 유사). ● 별도의 강한 소수 생성과정이 필요 없음.

4. 결 론

인터넷등 각종 정보 통신망에서 보안 서비스를 제공하기 위해서는 비대칭 암호 알고리즘을 주로 이용하며, 이러한 비대칭 암호 알고리즘은 큰 소수를 사용한다. 그러므로 비대칭 암호 알고리즘을 설계하는데 있어서, 매우 큰 소수를 구하는 것은 필수적이다. 그러나 지금까지는 큰 소수를 발견한다는 것이 어려웠기 때문에, 소인수 분해하기 어려운 정도를 이용하여 확률적으로 소수일 가능성이 높은 의사소수를 사용하였다. 이 논문에서는 기존의 소수 생성 방법의 문제점인 확률적인 검증 방식과 달리 증명이 가능한 소수를 직접 생성하는 방식을 독자적으로 제안하여, 알고리즘의 기본 개념을 설계 및 구현하였다. 즉 소수 생성에 관련된 방법론을 기존의 불확실한 방법에서 확실한 방법으로의 전환을 가능하게 하였다. 또한 제안된 방법에 의해 생성된 소수는 신뢰성, 비도, 원시원소 생성 능력 등을 보장하여, 추후 이를 이용하여 많은 비대칭 알고리즘들이 구축되리라 사료된다.

참 고 문 헌

[1] Bruce Schneier, *Applied Cryptography, Second Edition*, John Wiley & Sons, 1996.

[2] William Stallings, *Network and Internetwork Security*, Prentice-Hall, 1995.

[3] R. Alfred, A. Granville and C. Pomerance, "There are infinitely many Carmichael Numbers," *Ann. Of Math*, 1994.

[4] H. Cohen and A. K. Lenstra, "Implementation of a new Primality Test," *Math. Comp.*48, 1987.

[5] R. Solvay and V. Strassen, "A Fast Monte-Carlo Test for Test for Primality," *SIAM Journal on Computing*, Vol.6, Mar. 1977.

[6] G. L. Miller, "Riemanns Hypothesis and Test for Primality," *Journal of Computer System Science*, Vol.13, No.3, pp.300-317, Dec. 1976.

[7] H. Riesel, "Prime Numbers and Computational Algebraic Number Theory," GTM 138, Springer-Verlag, New-York, 1995.

[8] Riesel, *Prime Numbers and Computer Methods for Factorization*, Birkhäuser, Boston, 1985.

[9] R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications*, Cambridge university press, 1986.

박 중 길

e-mail : jgpark@home.cnu.ac.kr

1986년 동국대학교 전자계산학과 졸업

1988년 서강대학교 전자계산학과 (석사)

1988년 2000년 국방과학연구소 선임연구원

2000년~현재 국가보안기술연구소 선임연구원

1998년~현재 충남대학교 컴퓨터과학과 박사과정중

관심분야 : 컴퓨터통신보안, 접근통제, 암호이론

박 봉 주

e-mail : bjpark@joohong.co.kr

1986년 서강대학교수학과 졸업 (이학사)

1988년 서강대학교 대학원 수학과 졸업(이학석사)

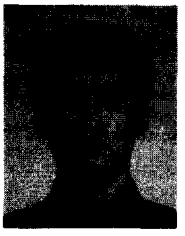
2000년 서강대학교 대학원 수학과 졸업(이학박사)

1988년~2000년 국방과학연구소 선임연구원

2000년~2000년 국가보안기술연구소 선임연구원

2000년~현재 (주)테크노밸리 책임연구원

관심분야 : 정보보호, 컴퓨터통신, S/W 및 H/W 고속 프로토콜



백 기 영

e-mail : cloud@home.cnu.ac.kr

1996년 충남대학교 컴퓨터과학과 졸업 (학사)

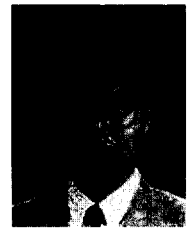
1998년 충남대학교 대학원 컴퓨터과학과 (석사)

1998년~현재 충남대학교 대학원 컴퓨터과학과 박사과정

관심분야 : 보안 프로토콜, PKI, 디렉토리 서버

천 왕 성

e-mail : wschun@kt.co.kr
1997년 한국과학기술원 전산학과 석사과정 졸업
1997년~현재 한국통신공사 멀티미디어연구소 근무
관심분야 : 정보 보안, 객체 지향 모델링



류 재 철

e-mail : jcryou@home.cnu.ac.kr
1985년 한양대학교 산업공학과 (학사)
1988년 Iowa State University 전산학과(석사)
1990년 Northwestern University 전산학과(박사)
1991년~현재 충남대학교 컴퓨터과학과 부교수
관심분야 : 컴퓨터 및 통신망 보안, 전자상거래, 분산