情報保護學會論文誌
第 22 卷 第 6 號, 2012. 12

Closest Vector Problem에 기반한 Interactive Proof*

이 경 희,[1†] 양 대 헌[2‡]
[1]수원대학교 전기공학과, [2]인하대학교 컴퓨터 정보 공학부

Closest Vector Problem Based Interactive Proof*

Kyunghee Lee,[1†] DaeHun Nyang[2‡]
[1]University of Suwon, [2]Inha University

요 약

이 논문에서는 래티스(Lattice)의 CVP (Closest Vector Problem)에 기반한 영지식 증명 기반의 인증프로토콜을 제안한다. CVP를 이용해서 암호시스템을 설계할 때 흔히 사용하는 길이가 짧은 기저벡터를 트랩도어 또는 비밀키로 사용하지 않는 프로토콜로서 의의를 가지며, 프로토콜의 설계가 단순하고 안전성 증명도 쉬워진다. 제안한 프로토콜의 안전성을 completeness, soundness, simulatability로 증명한다.

ABSTRACT

In this paper, we propose a new closest vector problem based interactive proof that is useful for authentication. Contribution of this paper is that the proposed protocol does not use a special form of a lattice, but a general lattice, which makes the protocol design very simple and easy to be proved. We prove its security in terms of completeness, soundness, simulatability.
Keywords: Closest Vector Problem, Interactive Proof, Authentication Protocol

I. 서 론

래티스(Lattice)는 기하학 그리고 군론에서 R^n의 이산 부분군 (discrete subgroup)으로 기저벡터 (basis vector)의 선형 결합에 의해 생성 (span)된다. 공개키 암호시스템의 개념이 제시되었을 때, 래티스를 암호시스템에 이용하려는 노력이 있었고, 그 결과로 Ajtai 등이 Shortest Vector Problem이 worst case에 안전스템을 제안했고[1], Goldreich 등이 Closest Vector Problem에 기반한 공개키 암호시스템과 전자서명 기법을 제안했다[4]. GGH 암호 스킴은 곧 Nguyen 등에 의해 깨졌으며, 서명 기법은 Nyang등에 의해 깨졌다[8,10]. 이후, NTRU 암호기법이 래티스에 기반한 암호시스템으로 설계되었고, 표준화 되었지만, NTRU 전자 서명기법은 안전하지 않은 것으로 알려졌다[12]. NTRU 암호시스템은 타원곡선이나 소인수 기반 암호시스템에 비해 처리속도가 월등히 빠르지만 키 길이가 길다는 점, 그리고 암호문의 길이 대 평문의 길이 비인 expansion factor가 크다는 점이 단점으로 알려져 있다[13]. 이후에 래티스를 암호시스템에 이용하는 연구는 주로 암호 공격 쪽이었고, 설계에는 많은 진전이 이루어지지 않았다.

접수일(2012년 7월 18일), 게재확정일(2012년 11월 12일)
* 이 논문은 인하대학교의 지원에 의하여 연구되었습니다. 이 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행 되었습니다.
† 주저자, khlee@suwon.ac.kr
‡ 교신저자, nyang@inha.ac.kr

하지만, 2009년 Craig Gentry가 fully homomorphic한 암호시스템을 제안하면서 다시 래티스에 관한 관심이 고조되고 있다[3]. Gentry의 기법은 최근까지 풀리지 않던 문제, 즉 덧셈과 곱셈이 모두 가능한 공개키 암호시스템의 존재에 대해 긍정적인 답을 주었고, 이에 따라 많은 후속연구가 뒤따랐다. Interactive Proof를 이용한 인증 기법으로는 Fiat-Shamir기법, Schnorr 기법 그리고 Guillous-Quisquater 기법 등이 알려져 있다[2,5,9]. 각각 소인수 분해 문제, 이산대수문제, RSA 문제에 안전성을 기반하고 있다. 영지식 증명을 이용한 이런 프로토콜은 Fiat-Shamir의 변환 기법을 이용하면 전자서명으로 변환할 수 있으며, 이 외에도 다양한 기능을 가지는 암호프로토콜을 설계할 때 프리미티브로 사용되고 있다. 래티스 문제에 기반한 대화식 영지식 증명들도 발표되었지만, ideal 래티스 등의 특별한 형태의 래티스를 가정하거나 래티스를 shortest벡터와 함께 생성해야 한다[6,7]. 이 논문에서는 임의의 래티스를 이용한 Closest Vector Problem에 기반한 대화식 영지식 증명 프로토콜을 제안한다. 특별한 형태의 래티스를 사용하지 않으므로, 래티스 생성 및 키 설정이 단순하고, 이에 따라 안전성의 분석이 쉬워지고 직관적이다. 영지식 증명 형태의 인증프로토콜은 암호학에서 지식을 증명하는 프리미티브의 하나로, 전자서명, 그룹서명, 익명인증, 사용자 인증 등 지식의 증명이 필요한 복잡한 암호 프로토콜의 설계에 활용할 수 있다. 이 논문에서 제안하는 프로토콜을 이용하면 래티스에 기반한 새로운 형태의 다양한 암호프로토콜 설계에 도움이 될 것이다.

II. 정 의

정수 집합은 Z, 실수 집합은 R, 볼드체 소문자 알파벳은 래티스 열벡터, 소문자 알파벳은 열벡터로 표현한다.

Lattice: 주어진 n개의 선형 독립적인 실수 벡터 집합 $B=\{\mathbf{b}_1,\mathbf{b}_2,\ldots,\mathbf{b}_n\}$에 대해, 기저 B에 의해 생성되는 래티스는 $\mathbf{b}_i$의 모든 선형 조합들의 집합으로 정의된다.

$$L(B)=\sum_i k_i\mathbf{b}_i : k_i\in Z, \mathbf{b}_1,\ldots,\mathbf{b}_n\in R^n, \quad 3$$

여기서 i=1,2,…,n, 그리고 래티스 $L(B)$의 랭크는 n이다.

Closest Vector Problem (CVP): 래티스 L(B)와 래티스 위에 있지 않은 벡터 v가 주어졌을 때, v와 가장 가까운 래티스 벡터를 찾는 문제이다.

CVP_γ: CVP의 근사치 버전으로, 주어진 벡터 v와 가장 가까운 래티스 벡터까지의 거리를 d라고 할 때 γd이하인 래티스 벡터를 찾는 문제이다. 이 문제는 Dinur등에 의해 래티스 차원(dim)의 다항식으로 표현되는 정도의 거리만큼 (정확히는 $2^{(\log\dim)^{1-e}}, e=(\log\log\dim)^{-c}$, $c<1/2$) 가까운 래티스 벡터를 찾는 것도 NP-Hard임이 알려졌다[14].

III. 래티스 기반의 대화식 증명 프로토콜

3.1 프로토콜

■ 시스템 파라미터 설정:

임의의 래티스 L을 생성하고, 이를 시스템의 모든 사용자가 공유하는 시스템 파라미터로 설정한다. 이때 L은 짧은 길이를 갖는 기저 벡터 집합을 구하는 LLL 알고리즘 (Lenstra - Lenstra - Lovász의 래티스 기저 리덕션 알고리즘) 등을 통해 충분히 reduce되어 더 짧은 길이의 기저를 구할 수 없는 래티스이다[11]. 연산자 *는 행렬과 열벡터의 곱으로 열벡터를 출력으로 한다. $|\mathbf{a}|$는 열벡터 $\mathbf{a}$의 Euclidean 길이, $(a1,a2,\ldots,an)^T$는 열벡터로 행벡터 (a1,a2, …, an)의 transpose를 의미한다.

■ 키 생성:

i=1,…,n, 그리고 $k(>3)$에 대해 $|\mathbf{si}|\le(3\gamma d)^k/n$를 만족하는 래티스 L위의 임의의 n개의 래티스 점 $\mathbf{s1}, \mathbf{s2}, \ldots \mathbf{sn}$을 선택하고, 행렬 $S=[\mathbf{s1}, \mathbf{s2}, \ldots, \mathbf{sn}]$가 사용자의 비밀키가 된다. 공개키는 L의 원소가 아니면서 $\mathbf{si}$들과의 거리가 $\gamma d/n$인 임의의 열벡터 $\mathbf{p1}=\mathbf{s1}+\mathbf{a1}$, $\mathbf{p2}=\mathbf{s2}+\mathbf{a2}$, $\mathbf{pn}=\mathbf{sn}+\mathbf{an}$로 이루어진 행렬 $P=[\mathbf{p1}, \mathbf{p2}, \ldots, \mathbf{pn}]$ 이다. 여기서 $\mathbf{ai}$는 길이가 $\gamma d/n$보다 작거나 같은 임의의 열벡터이다. 따라서 $|\mathbf{ai}|\le\gamma d/n$를 만족하는 랜덤한 열벡터 $\mathbf{ai}$들로 이루어진 행렬 $A=[\mathbf{a1}, \mathbf{a2}, \ldots \mathbf{an}]$에 대해서, 공개키 $P=S+A$로 나타낼 수 있다. 이때, LLL 등의 알고리즘에 의해 $\text{CVP}_{2\gamma}$ 문제의 답을 찾을 수 없도록, II절에서 언급한 [14]의 근사치 결과를 이용해서 γ와 n을 설정한다.

■ 프로토콜:

1. 증명자(Prover)는 $x=\mathbf{r}+e$를 확인자(Verifier)

에 전송한다. **r**은 $3\gamma d$에 비해 충분히 긴 (예를 들어, $k(>3)$에 대해 $|\mathbf{r}| \le (3\gamma d)^{k^2}$) 임의의 래티스 벡터이고, e는 길이가 γd인 임의의 열벡터이다.

2. 확인자는 랜덤수 벡터 c를 선택하고 열벡터 형태 $c=(c1,c2,\ldots\ cn)^T \in\{-1,1\}^n$로 증명자에게 전송한다.
3. 증명자는 래티스의 한 점 $\mathbf{y} = \mathbf{r} + S^* c$를 확인자에 전송한다.(참고로, **r**은 래티스위의 한 점, 그리고 $S^*c=c1^*\mathbf{s1}+\ldots+cn^*\mathbf{sn}$은 n개의 래티스 점들의 선형 합이므로 래티스의 점이다.)
4. 확인자는 y가 래티스 L의 벡터인지, 그리고 $|P^* c + x, \mathbf{y}| \le 2\gamma d$ 인지 확인하고, 맞는다면 증명을 신뢰한다.

3.2 안전성 증명

대화식 영지식 증명은 completeness, soundness, simulatability에 대한 안전성 증명이 필요하며, 이 절에서는 3.1에서 제안한 프로토콜의 안전성을 이 세 가지 면에서 증명한다.

정리 1 (Completeness) 만약 증명자가 비밀키 S를 알고 있다면, 위의 사용자는 항상 위의 프로토콜을 통과한다.

증명: $P = S + A$이고, $y = r + S^* c$이므로,

$|P^* c + x, y| = |(S + A)^*c + x, \mathbf{r} + S^*c|$

또한, $x = \mathbf{r} + e$ 이므로,

$|(S + A)^*c + x, \mathbf{r} + S^*c| = |S^*c + \mathbf{r} + e + A^*c, S^*c + \mathbf{r}|$

$S^*c + \mathbf{r} + e + A^*c$와 $S^*c + \mathbf{r}$ 사이의 거리는 $e + A^*c$와 0 사이의 거리와 같고, 원점에서 $e + A^*c$까지의 거리는 $e + A^*c$의 길이이므로,

$|S^*c + \mathbf{r} + e + A^*c, S^*c + \mathbf{r}| = |e+A^*c, 0|$

$=|e+A^*c|=|e+c1^*a1+c2^*a2+\ldots+cn^*an|$

$\le |e| + |c1^*a1| + |c2^*a2| + \ldots + |cn^*an| = |e|+|a1|+|a2|+\ldots+|an| \le 2\gamma d$

즉, $|P^* c + x, y| \le 2\gamma d$

따라서, S를 알고 있는 사용자는 항상 위의 프로토콜을 통과한다.■

정리 2 (Soundness) $CVP_{2\gamma}$ 문제를 다항시간 안에 풀지 못한다면, 비밀을 모르는 증명자가 통과할 확률은 무시할 만큼 작다.

증명:

1. $CVP_{2\gamma}$ 가정에 의해 **p1**,…,**pn**들로부터 거리가 γ내에 있는 래티스 벡터 **s1**,…,**sn** 중 하나라도 구할 수 없다. …(*)
2. 3.1절의 프로토콜을 다항식 시간 내에 p의 확률로 통과할 수 있는 S를 모르는 공격자 A의 존재를 가정하자.
3. 이 공격자 A를 이용해서 다음과 같이 (*)에 대한 모순을 보일 수 있다:
   a. 공격자의 성공확률이 p이므로, $1/p$번 실행해서 공격자가 적어도 한 번은 성공적인 출력을 내는 실험을 시행한다.
   b. 시뮬레이터는 이 첫 번째 실행에서 공격자가 성공적으로 $\mathbf{y1} = \mathbf{r} + S^*c$를 출력하는 지점을 기록한다. 그리고 그때까지의 입출력을 모두 기록한다.
   c. 공격자를 재설정(rewind)한다.
   d. 성공적으로 b의 답을 출력하는 지점 바로 직전까지, 즉, 첫 번째 실행에서 b단계에서 기록한 것 과 같은 입력을 공격자에게 준다. 결정적인(deterministic) 공격자는 같은 출력시퀀스를 줄 것이다.
   e. 성공적으로 출력하는 지점에서 첫 번째 실행에서의 입력과는 다른 입력 c'을 준다.
   f. p^2의 확률로 그 지점에서 공격자가 성공할 것이고 이때의 출력은 $\mathbf{y2} = \mathbf{r} + S^*c'$ 가 된다.
   g. 이제 시뮬레이터는

$$\mathbf{y1}-\mathbf{y2} = S^*(c-c')$$

를 계산한다.

   h. 이제 a-g의 과정을 n번 반복하면, n번 각각의 c, c' 그리고 **y1**, **y2**는 알려져 있으므로 S를 쉽게 계산할 수 있다. 이 S를 출력한다.
4. 따라서 3.1절의 프로토콜을 성공적으로 공격하는 공격자를 이용하면 P로부터 S를 계산할 수 있게 되고, 이는 가정 (*)에 모순이다. 따라서 공격자의 이득은 무시할 만큼 작다.■

정리 3 (Simulatability) 정직한 증명자와 정직한 확인자가 수행하는 3.1의 프로토콜은 S에 관한 아무런 knowledge도 유출하지 않는다.

증명: 확인자는 증명자의 도움 없이 (S에 대한 knowledge 없이) 다음과 같이 증명자와 확인자가 만들어 내는 transcript와 구별 불가능한(indistinguishable) transcript를 만들 수 있다.

1. $|e| \le 2\gamma d$인 임의의 열벡터 e를 고른다.
2. 다음을 만족하는 임의의 래티스 점 $\mathbf{r}$을 고른다:

$$|-P^*c + \mathbf{r} + e| \le (3\gamma d)^{k^2} + (3\gamma d)^k + \gamma d$$

이때, 임의의 $\mathbf{r}$을 뽑았을 때 위의 식을 만족할 확률은 $(3\gamma d)^{k^2} + (3\gamma d)^k + 3\gamma d$를 반지름으로 하는 구의 부피에서 $(3\gamma d)^{k^2} + (3\gamma d)^k + \gamma d$를 반지름으로 하는 구의 부피의 비율이므로, $\Pr_1 = ((3\gamma d)^{k^2} + (3\gamma d)^k + \gamma d)^n / ((3\gamma d)^{k^2} + (3\gamma d)^k + 3\gamma d)^n$이다 (n차원 구의 부피는 반지름의 n제곱에 비례한다). $(3\gamma d)^{k^2} + (3\gamma d)^k \gg \gamma d$인 경우 $\Pr \cong 1$이므로, 위 부등식을 만족하는 $\mathbf{r}$은 쉽게 찾을 수 있다.

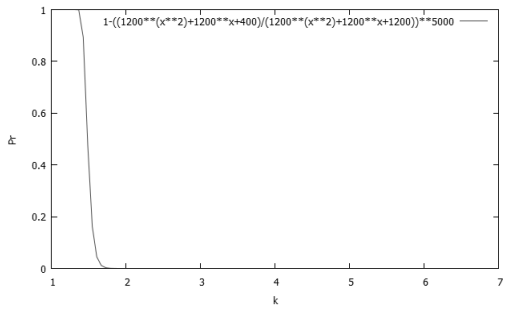
3. 시뮬레이션 된 transcript는 다음과 같다:

$$\langle x = -P^*c + \mathbf{r} + e,\ c,\ \mathbf{y} = \mathbf{r} \rangle,$$

이 transcript는 다음과 같이 검증식을 통과한다.

$$|P^*c + x, \mathbf{y}| = |P^*c - P^*c + \mathbf{r} + e, \mathbf{r}| = |\mathbf{r} - \mathbf{r} + e, 0| \le |e, 0| \le 2\gamma d \quad (1)$$

위의 시뮬레이션 된 transcript의 첫 번째 원소 x는 원래의 transcript와 마찬가지로 R^n의 임의의 열벡터이고, 이 벡터의 길이는 시뮬레이션 단계 2의 부등식 조건에 의해 원래 transcript길이 분포와 같다. 또한, 이 벡터는 임의의 래티스 점에 에러 성분이 합해진 값이다. 이때, 시뮬레이션된 transcript의 $x = -P^*c + \mathbf{r} + e = (-S^*c + \mathbf{r}) + (e - c1^*a1 - c2^*a2 - \ldots - cn^*an)$ 이고, 여기서 공개키의 에러 벡터 성분과 e의 길이를 더한 값은 honest한 증명자와 확인자간의 transcript에서의 x에서의 길이보다 $2\gamma d$만큼 길 수 있다. 이 사건이 생길 확률은 $(3\gamma d)^{k^2} + (3\gamma d)^k + 3\gamma d$를 반지름으로 하는 구의 부피에서 $(3\gamma d)^{k^2} + (3\gamma d)^k + \gamma d$를 반지름으로 하는 구의 부피를 뺀 비율 즉, $\Pr = 1 - ((3\gamma d)^{k^2} + (3\gamma d)^k + \gamma d)^n / ((3\gamma d)^{k^2} + (3\gamma d)^k + 3\gamma d)^n$이다. 충분히 큰 k에 대해서 $((3\gamma d)^{k^2} + (3\gamma d)^k + \gamma d)^n / ((3\gamma d)^{k^2} + (3\gamma d)^k + 3\gamma d)^n \cong 1$이므로, Pr은 무시할 만큼 작아 통계적으로 구별 불가능하다. 〔그림 1〕은 n=10,000, γ=4, d=100일 때, 확률 Pr을 나타낸다. 그림에서 보이는 것처럼, k가 3보다 크면 Pr은 0에 가깝다.



〔그림 1〕 k값 변화에 따른 시뮬레이션 실패확률

두 번째 원소는 임의의 열벡터 $c \in \{-1,1\}^n$, 세 번째 원소는 임의의 래티스 점으로, honest한 증명자와 확인자가 S를 이용해 생성하는 transcript와 길이 분포가 같다. 이는 앞의 시뮬레이션 에러 확률 분포와 비슷하게 $\mathbf{r}$이 S^*c에 비해 충분히 길다는 사실을 이용해 보일 수 있고, 적당한 k에 대해 0에 근접한다. (2)

(1)과 (2)에 의해, 위의 transcript는 honest한 증명자와 확인자가 S를 이용해 생성하는 transcript와 구별 불가능 하다[1]. ■

여기서 이용한 안전성 가정은 CVP_γ인데 일반적으로 공개키 암호시스템을 구현하기 위한 기법들과는 다르게 별도의 트랩도어(Trapdoor)가 필요하지 않다. 즉, 짧은 길이를 가지는 기저벡터 집합을 트랩도어의 형태로 이용하지 않으므로 GGH 기법 등에 적용했던 공격이 불가능하다. 즉, 확인자가 증명자가 보낸 $x = \mathbf{r} + e$에서 $\mathbf{r}$을 얻어야 $\mathbf{y}$에서 S를 알아낼 수 있다. 하지만 x에서 $\mathbf{r}$을 얻기 위해서는 CVP_γ문제를 풀어야하는데 이미 가정에서 $CVP_{2\gamma}$문제가 어렵다고 했으므로 이는 계산상 불가능하다. 또한 증명자의 입장에서 S를 모르고서 이 프로토콜을 통과하기 위해서는 P^*c+x와 적어도 $2\gamma d$만큼 가까운 래티스 벡터를 찾아내야 하고 이는 계산상 불가능하다.

IV. 결 론

Fiat-Shamir 변환을 이용하면 손쉽게 interactive proof로 부터 전자서명을 얻어낼 수 있는데, 앞서 제안한 interactive proof의 경우는 조금 다르다. 이는 서버가 x를 복원하지 못하는 구조 때문에 random oracle의 입력으로 x를 사용하지 못하기 때문이다. 즉, $\mathbf{y} - P^*c$의 결과가 $\mathbf{r}$이라는 래티스 벡터와 가까운 벡터라는 점에서 x와 비슷하지만, x와는 같지 않기 때문이다. 따라서, $\mathbf{y} - P^*c$와 r을 같게 해서

1) 참고로, 원래의 transcript를 검증할 때 계산하는 $|P*c + x, y|$는 c가 매번 다르므로 고정적으로 $|a1|+|a2|+,,,+|an|$를 포함하지 않고, $|e|+|a1|+|a2|+\ldots+|an|$는 c의 원소가 모두 1일 때 이 벡터가 가질 수 있는 최댓값일 뿐이다. 따라서 여러 개의 transcript를 검증할 경우 결과 값들의 길이 차이는 0보다 크고 $2\gamma d$보다는 작거나 같게 되어, 시뮬레이션 된 transcript의 길이 차들의 범위와 같다.

Fiat-Shamir 변환을 적용할 수 있는 방법을 찾는 것을 향후 연구 과제로 남겨둔다.

참고문헌

〔1〕 M. Ajtai and C. Dwork, "A public-key cryptosystem with worst-case/average-case equivalence," In Proc. 29th Annual ACM Symp. on Theory of Computing (STOC), pp. 284 - 293, May 1997.

〔2〕 A. Fiat and A. Shamir, "How to prove to yourself: practical solutions to identification and signature problems," Advances in Cryptology - Crypto 1986, pp. 186-194, Aug. 1987.

〔3〕 C. Gentry, "Fully homomorphic encryption using ideal lattices," In STOC 2009, pp. 169-178, May 2009.

〔4〕 O. Goldreich, S. Goldwasser, and S. Halevi, "Public-key cryptosystems from lattice reduction problems," Advances in cryptology-Crypto 1997, pp. 112 - 131. Aug. 1997.

〔5〕 L. Guillou and J. J. Quisquater, "A paradoxical identity-based signature scheme resulting from zero-knowledge," Advances in Cryptology-Crypto 1988, pp. 216-231, Aug. 1988.

〔6〕 V. Lyubashevsky, "Lattice-based identification schemes secure under active attacks," PKC 2008, pp. 162 - 179, March 2008.

〔7〕 D. Micciancio and S. Vadhan, "Statistical zero-knowledge proofs with efficient provers: lattice problems and more," Advances in cryptology - Crypto 2002, pp. 282 - 298, Aug. 2003.

〔8〕 P. Q. Nguyen, "Cryptanalysis of the Goldreich-Goldwasser-Halevi Cryptosystem from Crypto '97," Advances in Cryptology Crypto 1999, pp. 288-304, Aug. 1999.

〔9〕 C. P. Schnorr, "Efficient Identification and Signatures for Smart cards," Advances in Cryptology-Crypto 1989, pp. 239-251. Aug. 1989.

〔10〕 양대헌, "Chosen Message Attack Against Goldreich-Goldwasser-Halevis Lattice Based Signature Scheme," 한국정보보호학회 논문지, 14(1), pp. 47-57, 2004년 2월.

〔11〕 A. K. Lenstra, H. W. Lenstra, and L. Lovász, "Factoring polynomials with rational coefficients," Mathematische Annalen Vol. 261, No. 4, pp. 515 - 534, April 1982.

〔12〕 C. Gentry and M. Szydlo, "Cryptanalysis of the Revised NTRU signature scheme," Advances in Cryptology-Eurocrypt'02, pp. 299-320, April 2002.

〔13〕 A. Scholten and F. Vercauteren, "An Introduction to Elliptic and Hyperelliptic Curve Cryptography and the NTRU Cryptosystem," http://www.math.unibonn.de/~saxena/courses/WS2010-ref4.pdf

〔14〕 I. Dinur et al., "Approximating CVP to Within Almost-Polynomial Factors is NP-Hard," Combinatorica, vol. 23, no. 2, pp. 205 - 243, April 2003.

〈著者紹介〉

이 경 희 (KyungHee Lee) 정회원
1993년 2월 : 연세대학교 컴퓨터과학과 학사
1998년 8월 : 연세대학교 컴퓨터 과학과 석사
2004년 2월 : 연세대학교 컴퓨터 과학과 박사
1993년 1월~1996년 5월 : LG소프트(주) 연구원
2000년 12월~2005년 2월 : 한국전자통신연구원 선임연구원
2005년 3월~현재 : 수원대학교 전기공학과 조교수
〈관심분야〉 바이오인식, 정보보호, 컴퓨터비전, 인공지능, 패턴인식

양 대 헌 (DaeHun Nyang) 정회원
1994년 2월 : 한국과학기술원 과학기술 대학 전기 및 전자 공학과 졸업
1996년 2월 : 연세대학교 컴퓨터 과학과 석사
2000년 8월 : 연세대학교 컴퓨터 과학과 박사
2000년 9월~2003년 2월 : 한국전자통신연구원 정보보호연구본부 선임연구원
2003년 2월~현재 : 인하대학교 컴퓨터정보공학과 부교수
〈관심분야〉 암호이론, 암호프로토콜, 인증프로토콜, 무선 인터넷 보안