정 보 보 호 학 회 지
제 30 권 제3호, 2020. 6

격자문제 관련 최신 양자계산 알고리즘

김 정 산*

요 약

본 논문에서는 특정 격자문제와 관련하여 고전계산 알고리즘에 비해 지수적으로 빠르게 문제를 해결하는 최신 양자계산 알고리즘들을 소개한다. 먼저 물리적, 전산학적 문제들을 대수적으로 정형화하는 숨은 부분군 문제의 개념을 소개하고, 양자계산 알고리즘이 효율적으로 해결하는 숨은 부분군 문제들을 통하여 기존 암호체계에 영향을 줄 수 있는 양자계산 알고리즘의 부류에 대해 알아본다. 아울러 격자문제와 관련이 있는 다항시간 양자계산 알고리즘의 연구에 대한 전반적인 성과를 정리하고, 격자문제에 기반한 post-quantum cryptography가 갖추어야 할 기본 요건에 관하여 논한다.

Ⅰ. 서 론

양자역학적 성질에 기반한 양자계산이론(quantum computation theory)은 정보의 전달과 처리에 있어서 지금까지 고전적으로는 기대하기 힘들었던 비약적인 발전의 실마리들을 제시한다. 이는 물리적 혹은 전산학적으로 중요한 의미를 지닌 여러 대수적(algebraic) 문제들에 대하여, 고전계산 알고리즘보다 지수적으로 빠른(exponentially fast) 수행속도를 보여주는 여러 양자계산 알고리즘들이 이미 존재한다는 것으로 확인할 수 있다[1-3].

양자계산 알고리즘에서의 효율적인 계산속도의 향상은 양자중첩(quantum superposition)상태를 이용하여 많은 데이터들을 병렬처리(quantum parallelism)하는 데 있다. 양자중첩상태를 구현하는 데 그 핵심적인 역할을 하는 양자 푸리에변환(quantum Fourier transform: QFT)은 기존의 이산 푸리에변환(discrete Fourier transformation)을 양자역학적인 성질에 기반하여 지수적으로 빠르게 수행한다[4,5]. 양자 푸리에변환은 임의의 유니터리(unitary) 변환의 고유값(eigenvalue)을 효율적으로 추정 할 수 있는 양자 위상측정(quantum phase estimation)을 가능케 해주며, 이는 고전계산이론으로는 효율적으로 해결하기 어려운 여러 중요한 문제들을 빠르게 해결하는데 그 중추적인 역할을 한다[6,7].

양자계산 알고리즘들을 비롯한 양자계산이론의 발전은, 단순히 양자계산이론이 고전적인 계산이론의 한계를 넘어설 수 있다는 학문적인 의미보다 훨씬 많은 점을 시사한다. 특히 양자계산 알고리즘들이 제공하는 계산 속도의 향상은 기존의 정보통신 및 암호체계(cryptosystem)의 안전성(security)에 큰 영향을 미칠 수 있다는 것이 이미 잘 알려져 있다. 따라서 양자 컴퓨터가 개발되더라도 쉽게 해독되지 않는 암호, 즉 post-quantum cryptography를 구성하기 위해서는 shortest vector problem(SVP)등의 격자문제(lattice problem)와 같이 아직 효율적인 양자 알고리즘이 알려져있지 않은 문제에 그 안전성의 기반을 두어야 할 것이다[8,9].

본 논문에서는 특정 격자문제와 관련하여 고전계산 알고리즘에 비해 지수적으로 빠르게 문제를 해결하는 최신 양자계산 알고리즘들을 소개한다. 먼저 여러 문제들을 대수적으로 정형화(formalization)하는 개념인 숨은 부분군 문제를 소개하고, 양자계산 알고리즘이 효율적으로 해결하는 숨은 부분군 문제들을 통하여 기존 암호체계에 영향을 줄 수 있는 양자계산 알고리즘의 부류에 대해 알아본다[10]. 아울러 격자문제와 관련이 있는 다항시간(polynomial-time) 양자계산 알고리즘의 연구에 대한 전반적인 성과를 정리하고, 격자문제에 기반한 post-quantum cryptography가 갖추어야 할 기본 요건에 관하여 논한다.

* 경희대학교 응용수학과, 자연과학종합연구원 (교수, freddie1@khu.ac.kr)

Ⅱ. 숨은 부분군 문제(Hidden Subgroup Problem)

지수적인 속도향상을 가져오는 양자계산 알고리즘이 다루는 대부분의 문제들은 대수적 군(group)에서의 숨겨진 부분군(subgroup)을 찾는 대수적인 문제로 정형화 할 수 있으며, 이를 숨은 부분군 문제(hidden subgroup problem: HSP)라 한다. 조금 더 구체적으로 이야기하면 대수적인 군 G에서 정의된 오라클(oracle) 함수 f가 주어져 있을 때, 군 G의 임의의 원소인 a와 b에 대해 $f(a)=f(b)$일 때만 $Ha=Hb$를 만족하는 경우 "함수 f가 군 G의 부분군 H를 숨긴다"고 한다. 숨은 부분군 문제는 부분군 H 를 결정하는 문제이다. 예를 들어, 소인수분해 문제는 순환군(cyclic group) $G=Z_N$ 에서의 숨은 부분군 문제로 정형화 할 수 있으며, 이산로그 문제는 순환군의 직접곱(direct product), $G=Z_{p-1}\times Z_{p-1}$에서의 숨은 부분군 문제로 이해할 수 있다[5].

위수가 $|G|$인 군 G 에서 정의된 숨은 부분군 문제에 대하여, $O(\log|G|)$의 시간으로 숨은 부분군 문제를 해결하는 알고리즘이 있다면 그것을 효율적으로 빠른 알고리즘이라고 할 수 있다. 따라서 소인수분해 문제나 이산로그문제의 어려움에 기반한 RSA 공개키 암호 체계나 Diffie-Hellman 암호가 지금까지 그 안전한 암호체계로 이용될 수 있었던 이유는 순환군이나 순환군의 직접곱에서의 숨은 부분군 문제를 효율적으로 빠르게 해결할 수 있는 고전 알고리즘이 소개된 바가 없기 때문이다. 반면, 양자 계산을 이용한 경우, 임의의 가환군(abelian group)에서 정의된 숨은 부분군 문제를 효율적으로 해결할 수 있는 양자계산 알고리즘이 존재한다[6, 11,12]. 소인수분해 문제(integer factorization)와 이산로그(discrete logarithm) 문제를 비롯하여 펠 방정식(Pell's equation)의 정수해(integer solution)를 찾는 문제, 수체(number field)에서의 주 이데알(principal ideal)문제 및 류군(class group)문제 등 수학적으로 혹은 전산학적으로 중요한 많은 문제들이 특정한 가환군에서의 숨은 부분군 문제를 푸는 것으로 정형화 수 있다.

군 G가 비가환군(non-abelian group)인 경우의 숨은 부분군 문제를 효율적으로 해결할 수 있는 양자계산 알고리즘에 대하여도 많은 연구가 진행되어 왔다[13-15]. 비가환군에서의 숨은 부분군 문제가 흥미로운 이유 중 하나는 수학적으로 의미있는 여러 대수적 문제들이 비가환 숨은 부분군 문제로 정형화 될 수 있기 때문이다. 예를 들어 그래프 동형(graph isomorphism) 문제는 대칭군(symmetry group) S_N에서의 숨은 부분군 문제로 [16], 최소벡터문제(SVP) 등의 격자문제가 정이면체군(dihedral group), D_N에서의 숨은 부분군 문제로 정형화 될 수 있다[17].

임의의 비가환군 G에서의 숨은 부분군 문제를 해결하기 위해 고전적으로는 $O(|G|)$의 질의가 필요하나 양자계산을 이용하면 $O(\log|G|)$의 질의만으로 숨은 부분군 H를 찾을 수 있다는 것이 알려져 있다[18]. 뿐만 아니라 특정한 경우의 비가환군에서의 숨은 부분군 문제는 양자 컴퓨터를 이용하여 효과적으로 해결 할 수 있다. 그러나 일반적인 경우의 비가환군 G에서, f에 대한 $O(\log|G|)$번의 질의를 통하여 얻은 양자상태를 이용하여 H의 generator를 찾는데 지수적인 시간이 걸릴 수 있기 때문에 일반적인 비가환 숨은 부분군 문제를 효율적으로 해결하는 양자 알고리즘은 아직 알려진 바가 없다 하겠다. 몇몇 주요 암호체계들의 기반이 되는 대수적문제와 이에 대응되는 숨은 부분군 문제의 양자계산복잡도(quantum computational complexity)를 표 1에서 확인할 수 있다[10].

〔표 1〕 암호체계의 기반문제와 숨은 부분군 문제

기반문제	군	암호체계	양자복잡도
소인수분해	$\mathbb{Z}$	RSA	다항
이산로그	$\mathbb{Z}_p\times\mathbb{Z}_p$	DH, DSA…	다항
타원곡선 이산로그	타원곡선군	ECDH, ECDSA…	다항
주이데알 (principal ideal)	$\mathbb{R}^n$	Buchmann -Williams	다항
단위군 (unit group)	$\mathbb{R}^n$	Smart-Vercauteren	다항
최단격자벡터	정이면체군	NTRU, Ajita-Dwork	초다항
그래프동형	대칭군		지수

Ⅲ. 격자문제 관련 양자계산 알고리즘

대표적인 격자문제인 SVP와 closest vector problem(CVP)은 정이면제군에서의 숨은 부분군 문제로 정형화 될 수 있다[17], 정이면체군 D_N에서의 숨은 부분군 문제는 양자계산알고리즘에 의해 subexponential의 시간인 $O(2^{c\sqrt{\log N}})$에 해결될 수 있음이 Kuperberg에 의해 밝혀졌고[17], 이후, 이러한 양자알고리즘이 다항공간(polynomial space)에서 구현될 수 있음이 보였다[19].

3.1. 반 직접곱군에서의 양자계산 알고리즘

정이면제군 D_N은 순환군 Z_N과 Z_2의 반직접곱(semi-direct product)군 $Z_N \rtimes_\psi Z_2$과 대수적으로 동형(isomorphic)임이 알려져 있고, 따라서 정이면체군 D_N에서의 숨은 부분군 문제는 반 직접곱군에서의 숨은 부분군 문제에 특별한 경우임을 알 수 있다. 이러한 이유로 다양한 반직접곱 군에서의 다항시간 양자계산 알고리즘들이 연구되었다. Moore 등은 임의의 소수(prime number) p와 자연수 N에 대하여 $p=\phi(N)/poly(\log N)$ 인 경우 $Z_N \rtimes_\psi Z_p$에서의 숨은 부분군 문제를 다항시간에 해결하는 양자 알고리즘을 제시하였으며[15], Friedl 등은 임의의 자연수 n과 소수 p의 고정된 거듭제곱(fixed power) p^k에 대하여 $Z_{p^k}^n \rtimes_\psi Z_2$에서의 숨은 부분군 문제를 다항시간에 해결하는 양자 알고리즘을 제시하였다[14]. Radhakrishnan 등은 Heisenberg group이라고도 알려진 $Z_p^2 \rtimes_\psi Z_p$에서의 숨은 부분군 문제가 양자 알고리즘에 의해 다항시간에 해결될수 있음을 증명하였으며[20], 이 결과는 Bacon 등에 의해, 임의의 자연수 n에 대하여 $Z_p^n \rtimes_\psi Z_p$로 발전되었다[21]. Inui 등은 홀수 소수 p와 자연수 k에 대하여 $Z_{p^k} \rtimes_\psi Z_p$에서의 숨은 부분군 문제를 해결하는 다항시간 양자 알고리즘을 제시하였으며[22], Chi 등은 임의의 소수 p와 자연수 N에 대하여, N의 소인수들에서 1을 뺀 값이 p로 나누어지지 않을 경우, $Z_N \rtimes_\psi Z_p$에서의 숨은 부분군 문제를 다항시간에 해결하는 양자 알고리즘을 제시하였다[23].

3.2. 수체에서의 대수적 문제와 양자계산 알고리즘

주어진 비제곱(square-free)양의 정수 d에 대하여 $x^2-dy^2=1$형태의 방정식을 를 펠 방정식(Pell's equation)이며, 이를 만족하는 모든 정수해 순서쌍 (x,y)를 찾는 것을 펠 방정식 문제이다. 펠 방정식은 수론에서 가장 오래된 문제 중 하나이며, 펠 방정식 문제를 해결하는 최적의 고전 알고리즘은 $O(d^{1/4}\mathrm{poly}\log d)$의 계산복잡도를 가진다. 2002년, Hallgren은 펠 방정식 문제를 해결하는 다항시간 양자계산 알고리즘을 제시하였는데[24], 사실 이 알고리즘은 펠 방정식 문제를 특별한 경우로 가지는 더 어려운 문제인 이차 수체(quadratic number field)에서의 단위군(unit group) 문제를 다항시간에 해결한다. 수체의 단위 군을 찾는 알고리즘의 실행 시간은 수체의 판별식(discriminant)과 차수(degree)를 가지고 측정된다. 수체의 차수는 유리수 체 $\mathbb{Q}$상의 벡터 공간으로서 그것의 차원이고, 판별식은 정수환의 기본 영역(fundamental domain)의 부피에 의해 결정된다. 이차 수체에서의 단위군을 찾는 Hallgren의 다항시간 양자 알고리즘은 이후, 알고리즘은 고정된 차수의 수체에서 단위군 문제 및 주 이데알 문제(princopal ideal problem: PIP) 그리고 류군(class group) 문제를 해결하는 다항 시간 양자 알고리즘으로 개선되었다[25,26].

2014년 Hallgren 등은 임의의 차수를 갖는 수체에 대해 적용이 가능하고, 판별식과 차수 두 가지 파라미터 모두에 대하여 다항시간에 단위 군 문제를 해결하는 양자 알고리즘을 발견하였다[27]. 이를 바탕으로 2016년 Song 등은 임의의 차수를 갖는 수체에서 류 군문제와 PIP를 해결하는 효율적인 양자 알고리즘을 발견하였다[28]. 이러한 양자 알고리즘에서는 $\mathbb{R}^n$에서의 연속 숨은 부분군 문제라는 새로운 정의를 도입하고, 임의의 차수를 가지는 수체에서의 단위 군을 찾는 문제를 $\mathbb{R}^n$에서의 연속 숨은 부분군 문제로 정형화 하였다. 이러한 연속 숨은 부분군 문제는, 일반적인 숨은 부분군 문제를 해결하는 양자 알고리즘의 구조로 생각될 수는 있지만 분석하기가 매우 어렵기 때문에, 기존 양자 푸리에 변환을 직접 이용하는 방법 대신 변형된 양자 위상 추정(quantum phase estimation)을 이용하는 등 새로운 접근법을 통해 근 10년간 해결되지 않았던 문제점을 극복하였다.

펠 방정식 문제를 비롯한 수체에서의 단위군 문제, 주이데알 문제, 그리고 류군 문제는 수체의 부분환인 '대수적 정수환(ring of algebraic integers)'(혹은 단순히 '정수환)에서의 이데알들에 의해 주어지는(induce) 이데알 격자(ideal lattice)에서의 SVP 및 CVP 문제를 푸는 것으로 이해할 수 있다. 따라서 Hallgren 과 Song 등의 양자 알고리즘은 이데알 격자라는 특별한 구조의 격자에서는 SVP 나 CVP문제를 다항시간에 해결하는 양자계산 알고리즘이라 할 수 있다. 아울러 이러한 격자문제에 기반 한 Buchmann과 Williams의 키 교환 프로토콜은 Hallgren 과 Song등의 양자 알고리즘에 의해 안전하지 않음을 의미하기도 한다[29,30].

Ⅳ. 결 론

본 논문에서는 특정 격자문제와 관련하여 고전 계산 알고리즘에 비해 지수적으로 빠르게 문제를 해결하는 최신 양자계산 알고리즘들을 살펴보았다. 먼저 물리적 혹은 전산학적 문제들을 대수적으로 정형화한 개념인 숨은 부분군 문제를 소개하고, 양자계산 알고리즘들이 효율적으로 해결하는 숨은 부분군 문제들을 통하여 기존 암호체계에 영향을 줄 수 있는 양자 알고리즘의 부류를 살펴보았다. 또한 격자문제와 관련이 있는 다항시간 양자계산 알고리즘들의 연구에 대한 전반적인 성과를 정리하였다.

아직까지 일반적인 격자문제에 기반한 암호기술에 대한 직접적인 영향을 미치는 다항시간 양자 계산 알고리즘은 제시되지 않았다. 물론 일반적인 경우의 SVP나 CVP는 NP-hard 부류의 문제들이기 때문에, 아무런 제한이 없는 일반적인 격자문제에 기반한 암호체계의 구성은 그 효율성이 다분히 낮을 것이라 할 수 있다. 즉, 암호체계를 이용하는 인증된 사용자들 사이에서의 연산조차도 효율적으로 수행된다는 보장을 하기가 어렵다. 이러한 이유로 암호 시스템을 보다 효율적이면서도 안전하게 구성하기 위해 수체에서의 이데알 격자 등, 어느 정도의 대수적인 구조를 가지는 격자들을 이용하였으며, 아울러 이러한 구조의 격자에서 SVP나 CVP등의 문제들 역시 높은 차수의 수체에서는 여전히 어려울 것이라는 가정을 상용하여 왔다. 예를 들어, PIP에 기반한 암호체계는 충분히 높은 차수의 수체에서 특정한 생성자(generator)를 계산하는 것이 어렵다는 가정하였다[31]. 주어진 수체의 기저를 형성하는 Ring-LWE (Learning with errors) 문제는 높은 차수의 이데알 격자 상의 SVP가 어렵다는 것을 가정하에 효율적으로 안전할 수 있다. [32,33]

그러나, Hallgren 과 Song등의 다항시간 양자 알고리즘은 이데알 격자라는 특별한 구조의 격자에서는 SVP 나 CVP가 양자계산이론에서는 더 이상 어려운 문제가 아님을 시사한다. 비록 post-quantum cryptography의 좋은 후보로 여겨지는 격자기반 암호체계라 할지라도, 특수한 격자문제에 기반 한 암호이론은, 다시 말해 그 구조가 조금 더 명확한 격자에서의 암호이론은 양자계산적인 공격으로부터 안전하지 못할 수 있음을 의미한다. 그렇기 때문에 양자 컴퓨터에 의한 공격에 안전할 수 있는 암호 시스템을 고려하기 위해서는 최신 양자계산 알고리즘들의 이해와, 아울러 이러한 양자알고리즘들에 의한 암호분석(cryptoanalysis)역시 필수적으로 병행되어져야 할 것이다.

참 고 문 헌

[1] A. Berthiaume, G. Brassard, "The quantum challenge to structural complexity theory", *Proceedings of the 7th Annual IEEE Conference on Complexity Theory* (Piscataway, NJ), IEEE Computer Society Press, pp. 132-137, 1992.

[2] A. Berthiaume, G. Brassard, "Oracle Quantum Computing", *Journal of Modern Optics*, Vol. 41, pp. 2521-2535, 1994.

[3] C. H. Bennett, E. Bernstein, G. Brassard, U. Vazirani, "Strengths and Weaknesses of Quantum Computing", *SIAM Journal on Computing*, Vol. 26, pp. 1510-1523, 1997.

[4] E. Bernstein, U. Vazirani, "Quantum complexity theory", *Proceeding of the 25th ACM Symposium on Theory of Computation*, San Diego, CA, 1993, pp.11-20; SIAM Journal on Computing, Vol. 26, pp. 1411-1473, 1997.

[5] M. Nielson and I. Chuang, *Quantum computation and quantum information*, Cambridge University Express, 2000.

[6] P. W. Shor, "Algorithms for quantum computa-

tion: discrete logarithms and factoring," *in Proceedings of the 35th Annual IEEE Symposium on the Foundations of Computer Science*, (IEEE Computer Society Press, Piscataway, NJ, USA, 1994); SIAM J. Comput, 26, 1484-1509, 1997.

[7] L. K. Grover, "A fast quantum mechanical algorithm for database search", i*n Proceedings of the 28th Annual ACM Symposium on Theory of Computing* (ACM, NY, USA, 1996); *Phys. Rev. Lett,* 79, 325-328, 1997.

[8] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography", *STOC* 2005, ACM pp. 84-93, 2005.

[9] V. Lyubashevsky, C. Peikert, O. Regev, "On ideal lattices and learning with errors over rings", In *Advances in cryptology- EUROCRYPT 2010*, volume 6110 of LNCS, pp. 1-23, Springer, 2010.

[10] E. Bae, J. S. Kim, S. Lee, "Research trends in quantum computational algorithms for cryptoanalysis", *Korean Journal of Optics and Photonics*, 29(2) pp. 53-57, 2018.

[11] D. Boneh, R. Lipton, "Quantum cryptanalysis of hidden linear functions", in *Proceedings of Crypto'95,* LNCS, 963, pp. 427-437, 1995.

[12] A. Y. Kitaev, "Quantum measurements and the abelian stabilizer problem," arXiv:quant-ph/9511026v1, 1995.

[13] S. Hallgren, "The Hidden Subgroup Problem and Quantum Computing using Group Representations", *SIAM Journal on Computing*, Vol. 32, No. 4, pp. 916–934, 2003.

[14] K. Friedl, G. Ivanyos, F. Magniez, M. Santha, P. Sen, "Hidden Translation and Orbit Coset in Quantum Computing", *Proceedings of the 35th Annual ACM Symposium on Theory of Computing,* pp. 1–9, 2003.

[15] C. Moore, D. N. Rockmore, A. Russell, L. J. Schulman, "The Power of Basis Selection in Fourier Sampling: Hidden Subgroup Problems in Affine Groups", *Proceedings of the 15th Annual ACM-SIAM Symposium on Discrete Algorithms*, pp. 1106–1115, 2004

[16] M. Ettinger, P. Høyer, "A Quantum Observable for the Graph Isomorphism Problem", quant-ph/9901029, 1999.

[17] G. Kuperberg, "A subexponential-time quantum algorithm for the dihedral hidden subgroup problem", *SIAM Journal on Computing*, 35(1) pp. 170-188, 2005.

[18] M. Ettinger, P. Høyer, E. Knill, "The quantum query complexity of the hidden subgroup problem is polynomial", *Inform. Process. Lett*., 91 pp. 43-48, 2004.

[19] O. Regev, Quantum Computation and Lattice Problems, SIAM Journal on Computing, 33(3), pp.738–760, 2004.

[20] J. Radhakrishnan, M. R¨otteler and P. Sen, "On the Power of Random Bases in Fourier Sampling: Hidden Subgroup Problem in the Heisenberg Group", *Proceedings of the 32nd International Colloquium on Automata, Languages and Programming,* pp. 1399–1412, 2005.

[21] D. Bacon, A. Childs, W. van Dam, "From Optimal Measurement to Efficient Quantum Algorithms for the Hidden Subgroup Problem over Semidirect Product Groups", *Proceedings of the 46th Annual Symposium on Foundations of Computer Science*, pp. 469–478, 2005.

[22] Y Inui, F Le Gall, "Efficient quantum algorithms for the hidden subgroup problem over a class of semi-direct product groups", *Quantum Information and Computation* 7(5&6), pp. 559-570, 2007.

[23] D. P. Chi, J. S. Kim, S. Lee, "Notes on the hidden subgroup problem on some semi-direct product groups", *Phys. Lett. A,* 359, 114, 2006.

[24] S. Hallgren, "Polynomial-time quantum algorithm for Pell's equation and the principal ideal problem," *in Proceedings of the 34th Annual ACM Symposium on Theory of Computing,* 2002; *J. ACM* 54, pp. 1-19, 2007.

[25] S. Hallgren, "Fast quantum algorithms for computing the unit group and class group of a number field," *in Proceedings of the 37th Annual ACM*

Symposium on Theory of Computing, 468-474, 2005.

[26] A. Schmidt, U. Vollmer, "Polynomial-time quantum algorithm for the computation of the unit group of a number field," i*n Proceedings of the 37th Annual ACM Symposium on Theory of Computing*, pp. 475-480, 2005.

[27] K. Eisenträger, S. Hallgren, A. Kitaev, F. Song, "A quanum algorithm for computing the unit group of an arbitrary degree number field," in *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, pp. 293-302, 2014.

[28] J. F. Biasse, F. Song, "Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields," in Proceedings of the 27th Annual ACM-SIAM Symposium on Discrete Algorithms, 2016.

[29] J. Buchmann, H. C. Williams, "A key exchange system based on imaginary quadratic fields", *J. Cryptology* 1, 107–118, 1988.

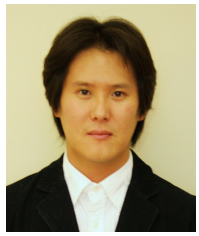
[30] J. A. Buchmann, H. C. Williams, "A key exchange system based on real quadratic fields Extended abstract", *in Advances in Cryptology — CRYPTO' 89 Proceedings. CRYPTO*, 1989; *Lecture Notes in Computer Science,* 435. Springer, New York, NY, 1989.

[31] C. Gentry, S. Halevi, "Implementing gentry's fully-homomorphic encryption scheme," in *Eurocrypt 2011*, pp. 132-150, 2011.

[32] V. Lyubashevsky, C. Peikert, O. Regev, "On ideal lattices and learning with errors over rings," in *Advances in cryptology-CRYPTO 2010*, 6110, pp. 1-23, 2010.

[33] Z. Brakerski, V. Vaikuntanathan, "Fully homomorphic encryption from ring-LWE and security for key dependent messages," in *Advances in cryptology-Eurocrypt 2011*, 6841, pp. 505-524, 2011.

〈저자소개〉



김 정 산 (Jeong San Kim)

1999년 2월 : 경희대학교 문리대 수학과 졸업

2002년 2월 : 서울대학교 수리과학부 석사

2006년 2월 : 서울대학교 수리과학부 박사

2011년8월~2015년 2월 : 수원대학교 수학과 조교수

2015년3월~현재 : 경희대학교 응용수학과 부교수

<관심분야> 양자계산 및 양자정보이론