《연구논문》 Korean Journal of Optics and Photonics, Vol. 29, No. 2, April 2018, pp. 53-57
DOI: https://doi.org/10.3807/KJOP.2018.29.2.053
ISSN : 1225-6285(Print)
ISSN : 2287-321X(Online)

# Research Trends in Quantum Computational Algorithms for Cryptanalysis

Eunok Bae[1], Jeong San Kim[2], and Soojoon Lee[1†]

[1]*Department of Mathematics and Research Institute for Basic Sciences, Kyung Hee University, 26, Kyungheedae-ro, Dongdaemun-gu, Seoul 02447, Korea*

[2]*Department of Applied Mathematics and Institute of Natural Sciences, Kyung Hee University, 1732, Deogyeong-daero, Giheung-gu, Yongin-si, Gyeonggi 17104, Korea*

(Received February 14, 2018; Revised March 12, 2018; Accepted March 12, 2018)

In this paper, we mainly introduce some quantum computational algorithms that have exponential speedups over the best known classical algorithms, and summarize recent research achievements in quantum algorithms that can affect existing cryptosystems. Finally, we suggest a research direction that can improve these results more progressively.

Keywords: Quantum computational algorithms, Cryptanalysis
OCIS codes: (270.5585) Quantum information and processing; (000.3870) Mathematics

# 암호해독을 위한 양자 계산 알고리즘의 최근 연구동향

**배은옥[1] · 김정산[2] · 이수준[1†]**

[1]경희대학교 수학과, 기초과학 연구소
㉾ 02447 서울시 동대문구 경희대로 26

[2]경희대학교 응용수학과, 자연과학종합연구원
㉾ 17104 경기 용인시 기흥구 덕영대로 1732

(2018년 2월 14일 받음, 2018년 3월 12일 수정본 받음, 2018년 3월 12일 게재 확정)

본 논문에서는 고전 계산 알고리즘에 비해 지수적인 계산 속도의 향상을 주는 양자 계산 알고리즘들을 중점적으로 소개하고, 기존 암호체계에 영향을 줄 수 있는 양자 계산 알고리즘 연구에 대한 최근 연구 성과들을 정리하며 최종적으로 이 결과들을 보다 발전적으로 향상시킬 수 있는 연구 방향을 제시한다.

Keywords: 양자 계산 알고리즘, 암호해독
OCIS codes: (270.5585) Quantum information and processing; (000.3870) Mathematics

## I. 서 론

인터넷의 급속한 확산과 통신기술의 발전으로 보다 고급화된 정보의 전달과 정보 보호방법의 방향이 꾸준히 제시되고 있고, 그에 따른 현 기술의 한계에 대한 염려 또한 심각하게 거론되어 왔다. 인텔(Intel)의 창시자인 무어(G. Moore)의 법칙에 따르면, 마이크로칩의 저장 용량과 계산 처리 속도는 18개월마다 두 배씩 증가하여 왔으며, 향후 그 계산 처리 속도의 향상이 더욱 가속화 될 것으로 판단되고 있다. 이러한 미세 논리회로 석판술(lithography)의 진보는 향후 수 년 이내에 단지 몇 개의 원자로만 이루어진 아주 미세한 논리 게이트를 다루게 될 것이라 예측하고 있다. 이러한 미시적 세계에서는 고전적인 물리법칙(classical physics)만으로 설명할 수 없는 양자적 현상들, 즉 입자들 간의 얽힘(entanglement), 변형(decoherence) 및 간섭(interference)등의 현상들이 실험적으로 관측이 되며, 기존의 논리 게이트의 성질을 결정하는 고전적인 물리법칙은 더 이상 사용할 수 없게 된다. 이에 따라, 가까운 미래에 양자역학의 법칙에 의하여 작동하는 논리 게이트를 구성해야 하며 아울러 반도체 기술의 발전으로 인한 소형화 추세의 극한에서 필연적으로 나타나는 양자 현상

†E-mail: level@khu.ac.kr, ORCID: 0000-0003-2925-1017
Color versions of one or more of the figures in this paper are available online.

은 이제는 피해야 할 자연 현상이 아니라 극복해야 할, 좀 더 정확하게는, 이해하고 이용해야 할 지극히 자연스러운 현상이라 할 수 있다[1].

양자역학을 이용한 계산 방법은 고전의 계산 이론과는 차별화된 양자역학만이 가지는 특성을 활용한 계산 방법으로, 고전적인 계산 이론과 비교하여 지수적인 계산 속도의 향상을 줄 수 있음이 이미 널리 알려져 있다. 또한 이러한 양자 계산 알고리즘이 기존의 정보통신(information communication) 및 암호체계(cryptosystem) 등에 미칠 수 있는 영향은 지대할 것이다.

본 논문에서는 고전 계산 알고리즘에 비해 지수적인 계산 속도의 향상을 보여주는 최신 양자 알고리즘들을 중심으로 소개하고자 한다. 먼저, 기존 암호체계에 영향을 줄 수 있는 양자 알고리즘의 부류에 대해 알아보고, 암호분석 관련 양자 계산 알고리즘의 연구에 대한 개괄적 성과를 정리한다. 이와 더불어 향후 양자 계산 알고리즘에 대한 연구 방향을 제시하며 본 논문을 마무리하고자 한다.

## II. 암호분석 관련 양자 알고리즘

양자 알고리즘의 출발이라 할 수 있는 쇼어(P. Shor)[2] 및 그로버(L, K. Grover)[3]의 알고리즘 이후 많은 형태의 양자 알고리즘들이 소개되었으며, 여러 방면에 있어서 고전적인 계산 알고리즘으로는 달성하기 어려운 효율적인 해법을 제시하고 있다. 이러한 양자 알고리즘의 수행능력은 그 계산속도의 지수적인 속도향상을 가능케 해 주는 양자 푸리에 변환(quantum Fourier transformation)의 효율적인 구현과, 그 구현이 실질적으로 가능한 양자 중첩 현상에 대한 분석을 통해 이루어졌다. 이러한 양자 계산 알고리즘이 보여주는 지수적인 계산속도의 향상은 기존의 정보통신 및 암호체계의 안전성(security)과 밀접한 관련이 있다.

### 2.1. 숨은 부분군 문제(Hidden subgroup problem)

지수적인 속도향상을 가져오는 양자 계산 알고리즘이 다루는 대부분의 문제들은 대수학적 군(group)에서의 숨은 부분군(hidden subgroup)을 찾는 대수학적인 문제로 정형화 할 수 있으며 이를 숨은 부분군 문제라 한다. 숨은 부분군 문제의 수학적 정의는 다음과 같다:

군 $G$와 $G$에서 정의된 오라클 함수 $f$가 주어져 있을 때, 군 $G$의 임의의 원소인 $a$와 $b$에 대해 $f(a)=f(b)$일 때만 $Ha=Hb$를 만족하는 경우 "함수 $f$가 군 $G$의 부분군 $H$를 숨긴다"고 한다. 숨은 부분군 문제는 부분군 $H$를 결정하는 문제이다.

위수(order)가 $|G|$인 군 $G$에서 정의된 숨은 부분군 문제에 대하여, $\log|G|$의 다항시간(polynomial time)으로 그 문제를 해결하는 알고리즘이 있다면 그것을 효율적인 알고리즘이라고 할 수 있다. 따라서 소인수분해 문제의 어려움에 기반한 RSA 공개키 암호 체계나 이산로그 문제의 어려움에 기반한 디피-헬만(Diffie-Hellman) 암호가 지금까지 그 안전성을 보장 받을 수 있었던 이유는 순환군(cyclic group)이나 순환군의 직접곱(direct product)에서의 숨은 부분군 문제를 효율적으로 해결할 수 있는 고전적 알고리즘이 발견된 바 없음을 의미한다. 반면, 양자 계산을 이용한 경우, 임의의 가환군(abelian group)에서 정의된 숨은 부분군 문제를 효율적으로 해결할 수 있는 양자 알고리즘이 존재한다는 것이 잘 알려져 있다[1,4,5].

비가환군(non-abelian group)에 대한 숨은 부분군 문제를 효율적으로 해결할 수 있는 양자 알고리즘에 대하여도 많은 연구가 진행되어 왔다[6-16]. 비가환군에서의 숨은 부분군 문제가 흥미로운 이유 중 하나는 수학적으로 의미 있는 여러 대수학적 문제들이 비가환군에서의 숨은 부분군 문제로 귀결될 수 있기 때문이다. 예를 들어, 그래프 동형(graph isomorphism) 문제는 대칭군(symmetry group)에서의 숨은 부분군 문제로 정형화 될 수 있고, 특정한 격자 문제(lattice problem)가 정이면체군(dihedral group)에서의 숨은 부분군 문제로 귀결될 수 있다는 것이 알려져 있다[17].

임의의 비가환군에서의 숨은 부분군 문제를 해결하기 위해서 고전적으로는 $O(|G|)$의 질의가 필요하나 양자 계산을 이용하면 $O(\log|G|)$의 질의만으로 $H$를 찾을 수 있다는 것이 알려져 있다[11]. 뿐만 아니라 특정한 형태의 비가환군에서는 양자 계산을 이용하여 숨은 부분군 문제를 효율적으로 해결할 수도 있다. 그러나 일반적인 비가환군에서 $f$에 대한 $O(\log|G|)$번의 질의로 얻은 양자 상태를 이용하여 $H$의 생성자(generator)를 찾는데 지수적인 시간이 걸릴 수 있기 때문에, 일반적인 비가환군에서의 숨은 부분군을 찾는 효율적인 양자 알고리즘은 아직 알려진 바가 없다.

**Table 1.** Problems that can be expressed as hidden subgroup problems and cryptosystems based on them

| Problem | Group | Quantum Complexity | Cryptosystem |
|---|---|---|---|
| Factorization | $\mathbb{Z}$ | Polynomial | RSA |
| Discrete log | $\mathbb{Z}_{p-1}\times\mathbb{Z}_{p-1}$ | Polynomial | DH, DSA,… |
| Elliptic curve discrete log | Elliptic curve | Polynomial | ECDH, ECDSA,… |
| Principal ideal | $\mathbb{R}^n$ | Polynomial | Buchmann-Williams |
| Unit group | $\mathbb{R}^n$ | Polynomial | Smart-Vercauteren |
| Shortest lattice vector | Dihedral group | Subexponenial | NTRU, Ajtai-Dwork |
| Graph isomorphism | Symmetric group | Exponential | |

다음에 나오는 표 1에서 기반 문제를 숨은 부분군 문제로 표현할 수 있는 기존 암호 체계들과 그 문제를 해결하는 양자 알고리즘의 복잡도(complexity)를 확인할 수 있다.

### 2.2. 숨겨진 이동 문제(Hidden shift problem)

숨겨진 변환(Hidden translation) 문제라고도 알려진 숨겨진 이동 문제는 숨은 부분군 문제의 자연스러운 변형으로, 숨은 부분군 문제에 대한 새로운 알고리즘을 이끌어 냈고 그 자체로 흥미로운 응용을 가진다. 숨은 이동 문제의 정의는 다음과 같다.

어떤 원소 $s \in G$에 대해, $f_0(g) = f_1(sg)$를 만족하는 두 개의 단사 함수 $f_0$, $f_1$이 주어져 있을 때, 숨겨진 이동 $s$를 찾는 문제가 숨겨진 이동 문제이다.

가환군 $Z_N$에 대한 숨겨진 이동 문제는 반 직접곱(semi-direct product) 군 $Z_N \rtimes_\phi Z_2$에 대한 숨은 부분군 문제와 동치라는 것이 알려져 있다. 다시 말하면, $Z_N$에서의 숨겨진 이동 문제는 정이면체군에서의 숨은 부분군 문제와 동치라는 것을 쉽게 보일 수 있다. 일반적인 가환 숨겨진 이동 문제에 대한 다항시간 양자 계산 알고리즘은 알려진 바 없지만, 쿠퍼버그(G. Kuperberg)의 체(sieve) 알고리즘이, 정이면체군 $G = Z_N \rtimes_\phi Z_2$에 대해, $2^{O(\sqrt{\log|G|})}$시간 안에 숨은 부분군 문제를 양자 계산으로 해결할 수 있으므로, 가환군 $Z_N$에 대한 숨겨진 이동 문제도 또한 양자 계산으로 그 시간 안에 해결될 수 있다는 것이 알려져 있다[10].

반면, 비가환군에 대해서는 일반적으로 숨은 부분군 문제와의 관계가 주어져 있지 않다. 하지만, $S_n \times S_n \leq S_{2n}$을 만족하는 대칭 군과 같이 $G \times G$가 같은 형태의 더 큰 군 $G'$에 포함되게 되는 군에 대해서는 숨겨진 이동 문제와 숨은 부분군 문제가 근본적으로 동치라는 것이 알려져 있다[18].

두 함수 $f_0$, $f_1$이 단사 함수인 경우, 숨겨진 이동 문제는 숨은 부분군 문제와 관련이 있지만, 일대일 조건이 없는 숨겨진 이동 문제도 생각해 볼 수 있다. 예를 들면, 반담(W. van Dam)외 2명은 일대일이 아닌 함수에 대한 숨겨진 이동 문제로 변형될 수 있는 르장드르 기호(Legendre's symbol) 문제를 풀기 위한 효율적인 양자 알고리즘을 소개하였는데[19] 이들의 결과는, 특정한 형태의 의사 난수(pseudorandom) 함수의 값을 양자 계산을 사용하여 효율적으로 예측할 수 있기 때문에, 이러한 의사 난수 함수를 이용하는 암호 체계에 양자 계산이 위협을 줄 수 있음을 보여준다[20]. 또한, 숨겨진 이동 문제에 대한 연구는 양자 기각 추출법(quantum rejection sampling)과 같은 새로운 알고리즘 기술에도 영감을 줄 수 있고[21], 더 나아가, 양자 공격에 대해 안전한 고전 암호 시스템을 설계하는 데에 응용할 수 있을 것으로 기대한다[22].

### 2.3. 기존 암호체계에 영향을 줄 수 있는 최신 양자 알고리즘

양자 알고리즘이 고전 알고리즘에 비해 지수적인 속도의 향상을 갖게 하는 문제들은 대부분 대수학적, 특히 정수론을 기반으로 하는 문제들이다. 쇼어는 인수분해 및 이산 로그를 위한 양자 알고리즘을 발견하였고[2], 할그렌(S. Hallgren)은 정수론에 등장하는 펠(Pell)의 방정식의 해를 찾는 양자 알고리즘을 발견하였다[23]. 이러한 알고리즘들은 이후 수체(number field)의 단위 군(unit group)을 찾는 문제 및 그와 관련된 문제들로 더 일반화되었다.

수체의 단위 군을 찾는 문제에 대한 양자 알고리즘의 실행시간은 수체의 판별식(discriminant)과 차수(degree)를 가지고 측정된다. 수체의 차수는 $\mathbb{Q}$상의 벡터 공간으로서 그것의 차원이고, 판별식은 정수환의 기본 영역(fundamental domain)의 부피와 관련되어 있다.

참고문헌[24,25]에서 소개된 양자 알고리즘들은 고정된 상수 차수의 수체에서만 효율적으로 수행되기 때문에, 그 결과 이후, 임의의 차수를 가지는 수체에서의 단위 군을 계산하는 양자 알고리즘을 찾는 노력이 계속 되었다. 그 결과, 근 10년만인 2014년에 할그렌 외 3인의 저자들이 임의의 차수를 갖는 수체에 대해 적용이 가능하고, 판별식과 차수 두 가지 파라미터 모두에서 효율적으로 단위 군을 계산할 수 있는 양자 알고리즘을 발견하였다[26]. 또한, 이 결과를 이용하여 2016년에 송(F. Song)과 비아세(J. Biasse)는 임의의 차수를 갖는 수체에서의 류 군(class group)을 계산하고 주 이데알(principal ideal) 문제를 해결하는 효율적인 양자 알고리즘을 발견하였다[26].

참고문헌[26,27]에 소개된 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. 더 나아가 임의의 차수를 가지는 수체에서의 류 군을 찾는 문제와 주 이데알 문제도 $\mathbb{R}^n$에서의 연속 숨은 부분군 문제로 귀결시킴으로써 그 문제들을 해결하는 효율적인 양자 계산 알고리즘을 개발하였고[27], 이는 수체와 관련된 가정을 기반으로 하는 여러 종류의 암호체계를 위협하기에 충분하다는 것이 증명되었다.

이와 더불어, 참고문헌[28]에서는 기존의 숨겨진 이동 문제에 연속성을 결합한 $\mathbb{R}^n$에서의 연속 숨겨진 이동 문제를 새롭게 정의하고, 이 문제를 해결하는 효율적인 양자 계산 알고리즘을 발견하였다.

## III. 결 론

본 논문을 통해 양자 계산 이론에 필요한 기본 개념과 암호관련 양자 계산 알고리즘의 최근 연구 동향 및 공개키 암호체계에 영향을 줄 수 있는 다양한 양자 알고리즘에 대하여 정리해 보았다.

잘 알려진 고전 계산 알고리즘에 비해 지수적인 계산 속도의 향상을 가져오는 양자 계산 알고리즘들이 다루는 대부분의 문제들은 대수학적인 구조 중 하나인 군에서의 숨은 부분군을 찾는 문제로 정형화 될 수 있기 때문에, 가환군이나 비가환군에서의 숨은 부분군 문제나 그것의 변형에 관한 연구가 현재까지도 활발히 진행되고 있다.

지난 몇 년 동안, 준 동형 암호화(homomorphic encryption)의 발견과 암호 시스템을 보다 효율적이고 안전하게 만드는 노력들을 기반으로 수체와 관련된 가정이 상용되어 왔다. 이러한 암호 시스템들은 높은 차수의 수체를 기반으로 설정된다. 특히, 참고문헌[29]에서는 특정한 생성자를 모르는 경우의 주 이데알 문제가 어렵다는 것을 가정하였고, 참고문헌[30,31]에서는, 주어진 수체의 기저를 형성하는 Ring-LWE (Learning with errors) 문제가 높은 차수의 수체의 이데알 격자 상의 최단 벡터를 찾는 것이 어렵다는 것을 가정하였다.

그러나, 참고문헌[26]의 양자 알고리즘은 참고문헌[29]에서의 수체의 상수 차수 가정을 가능하지 않게 만든다. 또한, 최단 벡터 계산에 관한 상대적으로 높은 차수의 수체 가정은 양자 컴퓨터에 대한 보안 측면에서 여전히 열려있지만 높은 차수에서도 수체의 단위 군을 효율적으로 계산 가능하다는 것이 알려져 있으므로, 이를 토대로 새로운 준 동형 암호 시스템이 실제로 양자 컴퓨터의 공격에 안전한지 여부는 계속적으로 연구되어야 할 것이다.

마지막으로, 참고문헌[28]의 저자들은 여기에서 소개된 양자 알고리즘을 활용하여 특정한 비가환군에서의 숨은 부분군 문제를 $\mathbb{R}^n$에서의 연속 숨겨진 이동 문제로 귀결시키는 방법을 연구 중에 있으며, 향후 이러한 문제를 해결하는 양자 알고리즘이 기존 암호 시스템에 미치는 영향에 대한 연구도 기대가 된다.

## 감사의 글

이 논문은 2016년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업(2016R1A2B4014928)의 지원으로 수행되었습니다.

## References

1. J. Kim, Y. Lim, E. Bae, and D. Kim, “A research on the technique of cryptosystem security analysis using quantum computational algorithms” (in Korean), *National Security Research Institute Report* (Grant No. 2017-013, 2017).
2. P. W. Shor, “Algorithms for quantum computation: discrete logarithms and factoring,” in *Proc. 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).
3. L. K. Grover, “A fast quantum mechanical algorithm for database search” in *Proc. 28th Annual ACM Symposium on Theory of Computing* (ACM, NY, USA, 1996), Phys. Rev. Lett. **79**, 325-328 (1997).
4. D. Boneh and R. Lipton, “Quantum cryptanalysis of hidden linear functions,” in *Proc. Crypto’95*, *LNCS* **963**, 427-437 (1995).
5. A. Y. Kitaev, “Quantum measurements and the abelian stabilizer problem,” arXiv:quant-ph/9511026v1 (1995).
6. M. Ettinger and P. Høyer, “A quantum observable for the graph isomorphism problem,” arXiv:quant-ph/9901029v1 (1999).
7. S. Hallgren, “The hidden subgroup problem and quantum computing using group representations,” SIAM J. Comput. **32**, 916-934 (2003).
8. M. Grigni, L. Schulman, M. Vazirani, and U. Vazirani, “Quantum mechanical algorithms for the non-abelian hidden subgroup problem,” in *Proc. 33rd Annual ACM Symposium on Theory of Computing* (2001), Combinatorica **24**, 137-154 (2004).
9. K. Friedl, G. Ivanyos, F. Magniez, M. Santha, and P. Sen, “Hidden translation and translating coset in quantum computing,” in *Proc. 35th Annual ACM Symposium on Theory of Computing* (2003), SIAM J. Comput. **43**, 1-24 (2014).
10. G. Kuperberg, “A subexponential-time quantum algorithm for the dihedral hidden subgroup problem,” SIAM J. Comput. **35**, 170-188 (2005).
11. M. Ettinger, P. Høyer, and E. Knill, “The quantum query complexity of the hidden subgroup problem is polynomial,” Inf. Process. Lett. **91**, 43-48 (2004).
12. D. Gavinsky, “Quantum solution to the hidden subgroup problem for poly-near-hamiltonian groups,” Quantum Inf. Comput. **4**, 229-235 (2004).
13. Y. Inui and F. Le Gall, “Efficient quantum algorithm for the hidden subgroup problem over a class of semi-direct product groups,” Quantum Inf. Comput. **7**, 559-570 (2007).
14. C. Moore, D. N. Rockmore, A. Russell, and L. J. Schulman, “The power of strong Fourier sampling: Quantum algorithms for affine groups and hidden shifts,” in *Proc. 15th Annual ACM-SIAM Symposium on Discrete Algorithms* (SIAM, Philadelphia, USA, 2004), SIAM J. Comput. **37**, 938-958 (2007).
15. O. Regev, “A subexponential-time algorithm for the dihedral hidden subgroup problem with polynomial space,” arXiv: quant-ph/0406151v1 (2004).
16. D. Bacon, A. Childs, and W. van Dam, “From optimal measurement to efficient quantum algorithms for the hidden subgroup problem over semidirect product groups,” in *Proc. 46th Annual IEEE Symposium on the Foundations of Computer Science*, 469-478 (2005).
17. O. Regev, “Quantum computation and lattice problems,” in *Proc. 43rd Annual IEEE Symposium on the Foundations of Computer Science*, 520-529 (2002).
18. S. Hallgren, C. Moore, M. Rötteler, A. Russell, and P. Sen, “Limitations of quantum coset states for graph isomorphism,” in *Proc. 38th Annual ACM Symposium on Theory of Computing*, 604-617 (2006).

19. W. van Dam, S. Hallgren, and L. Ip, “Quantum algorithms for some hidden shift problems,” SIAM J. Comput. **36**, 763-778 (2006).
20. I. B. Damgård, “On the randomness of Legendre and Jacobi sequences,” in *Proc. Advances in Cryptology-CRYPTO 1988*, **403**, 163-172 (1990).
21. M. Ozols, M. Roetteler, and J. Roland, “Quantum rejection sampling,” in *Proc. 3rd Innovations in Theoretical Computer Science Conference*, 290-308 (2012).
22. O. Regev, “Quantum computation and lattice problems,” SIAM J. Comput. **33**, 738-760 (2004).
23. S. Hallgren, “Polynomial-time quantum algorithm for Pell’s equation and the principal ideal problem,” in *Proc. 34th Annual ACM Symposium on Theory of Computing* (2002), J. ACM **54**, 1-19 (2007).
24. S. Hallgren, “Fast quantum algorithms for computing the unit group and class group of a number field,” in *Proc. 37th Annual ACM Symposium on Theory of Computing*, 468-474 (2005).
25. A. Schmidt and U. Vollmer, “Polynomial-time quantum algorithm for the computation of the unit group of a number field,” in *Proc. 37th Annual ACM Symposium on Theory of Computing*, 475-480 (2005).
26. K. Eisenträger, S. Hallgren, A. Kitaev, and F. Song, “A quanum algorithm for computing the unit group of an arbitrary degree number field,” in *Proc. 46th Annual ACM Symposium on Theory of Computing*, 293-302 (2014).
27. J. F. Biasse and F. Song, “Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields,” in *Proc. 27th Annual ACM-SIAM Symposium on Discrete Algorithms*, (2016).
28. E. Bae and S. Lee, “Quantum algorithm for continuous hidden shift problems” in preparation.
29. C. Gentry and S. Halevi, “Implementing gentry’s fully-homomorphic encryption scheme,” in *Proc. Eurocrypt 2011*, 132-150 (2011).
30. V. Lyubashevsky, C. Peikert, and O. Regev, “On ideal lattices and learning with errors over rings,” in *Proc. Advances in cryptology-CRYPTO 2010*, **6110**, 1-23 (2010).
31. Z. Brakerski and V. Vaikuntanathan, “Fully homomorphic encryption from ring-LWE and security for key dependent messages,” *in Proc. Advances in cryptology-Eurocrypt 2011*, **6841**, 505-524 (2011).