쇼어 알고리즘 구현 최적화 동향

이창열 [1], 조성민 [2], 서승현 [3]
[1] 한양대학교 전자공학과 석사과정
[2] 한양대학교 전자공학과 석박통합과정
[3] 한양대학교 ERICA 전자공학부 교수

sshdjjim@hanyang.ac.kr, smcho3315@hanyang.ac.kr, seosh77@hanyang.ac.kr

Trends in Optimization of Shor's Algorithm Implementations

Chang-Yeol Lee[1], Seong-Min Cho[1], Seung-Hyun Seo[2]
[1]Dept. of Electrical Engineering, Hanyang University
[2]School of Electrical Engineering, Hanyang University ERICA

요 약

양자컴퓨터의 발전이 빠르게 진행됨에 따라서 고전컴퓨터에서는 해결하지 못하는 문제에 대하여 양자 알고리즘을 활용하여 해결하고자 하는 연구가 진행되고 있다. 이중 소인수 분해 및 이산로그 문제 해결이 가능한 Shor's Algorithm 및 이에 대한 공개키 암호 해독을 위한 양자 자원량 분석에 대한 연구가 진행되고 있다. 하지만 양자 컴퓨터의 가용 양자 자원량이 제한적이라는 점과, 시간적인 측면에서의 최적화는 암호의 보안강도에 영향을 끼치기 때문에 알고리즘 최적화 연구가 필요하다. 따라서 본 논문에서는 암호를 대상으로 한 Shor's Algorithm 양자 회로의 최적화 동향을 조사하고 향후 연구 방향에 대해서 기술한다.

1. 서론

양자 컴퓨터는 0 과 1 이 확률적으로 동시에 존재하는 중첩의 원리와 연결된 두 입자가 멀리 떨어지더라도 한 입자에 행해지는 작용이 다른 입자에도 영향을 미치는 양자 얽힘 원리를 활용한 컴퓨터이다. 이러한 원리를 통해 기존 고전 컴퓨터로는 다항시간 내에 해결하지 못한 문제를 빠른 속도로 해결할 수 있다. 따라서 이를 활용하여 암호, 물리학, 기계학습, 우주 물리 등의 분야에서 많은 계산량을 요구하는 문제를 해결하기 위해서 여러 양자 알고리즘들이 제시되고 있다. 그중 1994 년에 Peter Shor 가 제안한 Shor's Algorithm 의 경우 고전컴퓨터로는 해결 불가능한 소인수분해와 이산로그 문제에 대하여 해결할 수 있도록 한다[1]. 따라서 기존에 소인수분해 및 이산로그 문제의 어려움에 안전성을 기반하는 암호의 경우 더 이상 안전성을 제공하기 어렵다고 이론적으로 제시되었다. Shor's Algorithm 을 구현하기 위한 양자 자원량에 비하여 현재의 양자컴퓨터는 가용 양자 자원량이 제한적이기 때문에 효율적인 양자회로를 설계 및 구현하는 것이 중요하며, 시간적의 측면에서의 회로 최적화의 경우 암호의 보안강도에 영향을 끼치게 된다. 이에 본 논문에서는 소인수분해 및 이산로그 문제 기반 공개키 암호를 대상으로 하는 Shor's Algorithm 회로의 양자컴퓨터에서의 최적화 동향을 조사하고 향후 연구방향에 대하여 기술한다.

2. 배경지식

2.1 소인수 분해 문제

소인수분해란 1 보다 큰 자연수를 소인수만의 곱으로 나타내거나 합성수를 소수의 곱으로 나타내는 방법이다. RSA 의 경우 큰 수에 대한 소인수 분해가 어렵다는 것에 기반하여 암호의 안정성을 제시하고 있다.

이때 큰 수인 N에 대하여 소인수인 Q, R을 찾고자 한다면 다음과 같은 과정을 따른다.

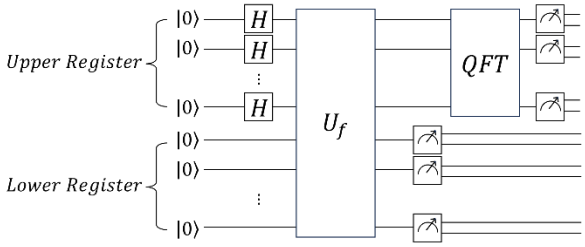
1) N과 서로소이며 $1 < a < N$에 해당하는 임의의 양의 정수 a를 선택한다.
2) $f(x) = a^x \bmod N$의 함수를 계산하고, 함수$f(x)$의 주기 r을 계산한다.
3) 만약 주기 r이 홀수라면 1)으로 돌아가고, 짝수라면 $Q = \gcd(a^{r/2} - 1, N), R = \gcd(a^{r/2} + 1, N)$을 계산한다. 이때 Q 또는 R 의 값이 1 이거나 N 이면 1)으로 돌아가 다시 진행한다.

3)의 경우 유클리드 알고리즘을 활용하면 최대공약수를 효율적으로 찾을 수 있다. 하지만 2)의 과정에서 주기 r에 대해 함수 $f(x)$가 반복되는 x 값 두개를 찾기 위해서는 $O(\sqrt{r})$ 의 시간이 필요하기 때문에 $a^x \bmod N$ 함수의 주기 r을 다항시간 내에 찾아내는

것은 어렵다. RSA-2048 의 경우 r이 617 자릿수로 r은 대략 10^{617}이다. 따라서 약 $\sqrt{r} \approx 10^{309}$ 정도의 시간이 필요하다. 이는 고전 컴퓨터에서는 불가능한 작업이다[2].

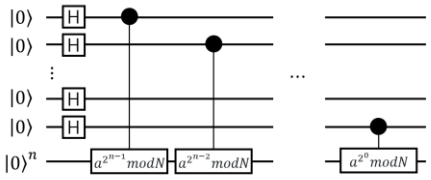
2.2Shor's Algorithm

Peter Shor 가 1994 년에 제안한 양자 알고리즘으로 양자적 성질을 활용하여 소인수분해 문제 및 이산로그 문제를 다항시간 안에 해결 가능한 알고리즘이다. 소인수분해 문제에서 고전 컴퓨터로는 해결하기 어려운 $a^x \bmod N$ 함수의 주기 r을 찾는 문제에 대하여 $QFT(Quantum\ Fouier\ Transformation)$ 을 적용하여 다항시간 내에 해결 가능하도록 한다. Shor's Algorithm 은 그림 1 과 같이 표현할 수 있다[1][2].



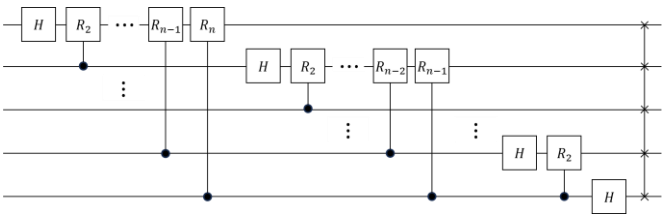
<그림 1>Shor's Algorithm Circuit

우선 함수 $f(x) = a^x \bmod N$을 계산하기 위해서 양자상태 $\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle|a^x mod N\rangle$ 을 만들어야 하므로 Hadamard Gate 와 Operator U 를 통과한다. 이때 Operator U 는 $f(x) = a^x \bmod N$를 계산하기 위한 함수로 그림 2 와 같이 설계해야 한다.



<그림 2>Operator U Circuit

그 후에 Lower Register 를 Measurement 를 하게 되면 $|a^{x_0} mod N\rangle$을 관측하게 된다. 이때 x_0는 0 과 2^{n-1}사이의 수이다. 이로 인하여 Upper Register 는 $\frac{1}{\sqrt{2^{n/r}}}(|l\rangle + |l+r\rangle + |l+2r\rangle + \cdots + |l+(m-1)r\rangle)$ 으로 Collapse 된다. 마지막으로 QFT는 파동함수의 주기성을 찾는 대에 있어서 유용함으로 Upper Register 에



<그림 3>QFT(Quantum Fouier Transformation) Circuit

<그림 3>의 QFT 회로를 사용하여 함수 $f(x) = a^x \bmod N$에 대한 주기 r을 구한다. Shor's Algorithm 의 경우 크기가 N 인 수를 소인수 분해할 때 $O(log^3 N)$의 시간 복잡도를 요구한다.

3. 연구 동향

3.1. Shor's Algorithm 구현 최적화

Shor's Algorithm 의 경우 공간과 시간적인 측면에서 최적화가 진행되고 있다. 공간의 경우 구현에 사용되는 큐비트 수를 줄이는 관점으로 연구가 진행되고 있으며, 시간의 경우 Depth 를 줄이는 관점으로 연구가 진행되고 있다. 특히 Depth 의 경우 Operator U 에서 Modular exponential 연산의 Depth 를 줄이기 위해 많은 연구들이 진행되고 있다.

2022 년 A.V.Antipov 등은 양자 컴퓨팅 시뮬레이션을 지원하는 오픈소스 라이브러리인 PennyLane 을 활용하여 효율적인 Adder, Modular Adder, Modular Multiplication, Modular exponential 을 순차적을 구현하고 이를 사용하여 Shor's Algorithm 을 구현하여 양자 자원량을 분석하였다[3].

3.2. RSA 대상 Shor's Algorithm 양자 자원량 분석

2016 년 THOMAS HANER 등은 n비트 정수를 인수분해하기 위한 Shor's Algorithm 을 $2n + 2$ 큐비트를 사용하여 구현하였다. Adder 를 설계함에 있어서 재사용하기 어려운 Dirty Qubit 수를 줄이고, Adder, Toffoli-gate 와 Clifford-gate 만 사용하여 Modular Multiplication 를 구현하였다. 이를 바탕으로 하여 Shor's Algorithm 을 구현하면 Depth 의 경우 $O(n^3)$, 전체 게이트 수의 경우 $O(n^3 \log n)$으로 구현 가능하다[4].

2021 년 Craig Gidney 등은 기존에 연구된 기술을 결합하여 양자 컴퓨터에서 정수 인수분해를 계산하는 비용을 크게 감소시켰다[5][6][7][8]. 또한 일반적으로는 무시되는 요소인 노이즈, 반복적인 시도의 필요 및 계산의 시간-공간 배치를 한다. 이를 활용하여 n 비트의 RSA 의 정수를 인수 분해할 경우에 $3n + 0.002n \log n$의 물리적 큐비트와 $0.3n^3 + 0.0005n^3 \log n$ 의 Toffoli-gate 를 요구한다[9]. 기존 연구와 비교한 양자 자원량은 <표 1>과 같다.

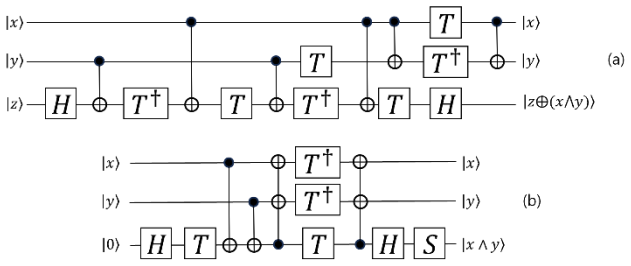
<표 1> 기존 연구와 Craig Gidney 의 Shor's Algorithm 비교

	Abstract Qubits	Measurement Depth	Toffoli+T/2 Count
Gidney et al. 2021[9]	$3n + 0.002n \log n$	$500n^2 + n^2 \log n$	$0.3n^3 + 0.00005n^3 \log n$
Haner et al. 2016[4]	$2n + 2$	$52n^3 + O(n^2)$	$64n^3 \log n + O(n^3)$
Fowler et al. 2012[10]	$3n + O(1)$	$40n^3 + O(n^2)$	$40n^3 + O(n^2)$

3.3. ECC 대상 Shor's Algorithm 양자 자원량 분석

2023 년 HARASHTA TATIMMA LARASATI 등은 ECDLP 암호를 해결하는 Shor's Algorithm 에 필수적으로 사용되는 유한체 역수의 깊이를 줄이는 회로를 제시하였다. 바이너리 유한체를 대상으로 하는 Fermat's Little Theorem (FLT) 회로의 Depth 를 줄였다. 기존 FTL 회로에서 역 제곱 연산을 제거하여 CNOT 게이트

수를 줄이고 표준 Toffoli-gate 가 아닌 Gidney 가 제시한 <그림 4>의 (b)회로인 상대 위상 Toffoli-gate 를 사용하여 T-gate 의 Depth 를 줄여 효율적인 회로를 구현하였다[11].



<그림 4> (a)Standard decomposition of Toffoli-gate used in Qskit (b)Gindy's relative-phase (GRT) Toffoli-gate decomposition

2023 년 DEDY SEPTONO CATUR PUTRANTO 등은 회로 깊이를 줄이는 관점에서 바이너리 타원 곡선에 대한 양자 암호 해독을 제시하며, 주로 큐비트를 줄이는 것에 중점을 둔 이전 연구와 달리 Depth 를 줄인 회로를 제시하였다. 이를 위해 기존의 Karatsuba 곱셈기 및 역수 기반 FTL 회로를 개선하였다. 전체 회로에서 CNOT 과 Toffoli-gate 횟수와 Depth 를 줄이는 대신에 큐비트가 늘어나는 trade-off 가 존재한다[12]. 기존 연구와 양자 자원량을 비교한 결과는 다음 <표 2>과 같다.

<표 2> 최적화 회로 양자 자원량

	Quantum cryptanalysis of binary elliptic curves
Depth	$7n + 6n\log_2(3)$
Toffoli-gate count	$4n^3 + 3n\log 3 + 1 + 25n^2\log n + 2n^2 + O(n^{log3+1})$
Qubit count	$4n + 7n\log n + 7$

4. 결론

Shor's Algorithm 을 구현할 수 있는 양자 컴퓨터의 개발이 가속화되면서 소인수분해 및 이산로그 문제 기반 공개키 암호의 해독이 현실로 다가오고 있다. 이에 최근 해당 공개키 암호를 해독하기 위한 Shor's Algorithm 의 양자 자원량을 정밀하게 추정하고자 하는 연구들이 활발하게 진행되고 있다. 특히 논리적 큐비트 수에 대한 분석만 이루어졌던 초기의 연구들과 달리 기존에는 고려하지 않던 노이즈, 물리적 큐비트, 계산에 필요한 반복적인 시도 등을 고려한 최적화 구현 및 이에 대한 양자 자원량 분석 연구들이 활발하게 진행되고 있다. 본 논문에서는 대표적인 소인수분해 및 이산로그 문제 기반 공개키 암호인 RSA 및 ECC 암호를 대상으로 하는 Shor's Algorithm 의 최적화 연구 동향 및 이에 대한 양자 자원량 분석 결과를 조사하였다.

향후 양자 연산기 및 알고리즘을 큐비트와 Depth 측면에서 최적화하고 이를 Shor's Algorithm 에 적용한 후 양자 자원량을 분석하고자 한다.

[Acknowledgement]

본 연구는 2023 년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No. 00256221. 국가연구망 암호통신 강화를 위한 양자컴퓨팅 활용 양자보안비도 분석)

참고문헌

[1] Shor, Peter W. "Algorithms for quantum computation: discrete logarithms and factoring." Proceedings 35th annual symposium on foundations of computer science. Ieee, 1994.

[2] LaPierre, Ray, and Ray LaPierre. "Shor algorithm." Introduction to Quantum Computing (2021): 177-192.

[3] Antipov, A. V., E. O. Kiktenko, and A. K. Fedorov. "Efficient realization of quantum primitives for Shor's algorithm using PennyLane library." Plos one 17.7 (2022): e0271462.

[4] Häner, Thomas, Martin Roetteler, and Krysta M. Svore. "Factoring using 2n+ 2 qubits with Toffoli based modular multiplication." arXiv preprint arXiv:1611.07995 (2016).

[5] Zalka, Christof. "Shor's algorithm with fewer (pure) qubits." arXiv preprint quant-ph/0601097 (2006).

[6] Horsman, Clare, et al. "Surface code quantum computing by lattice surgery." New Journal of Physics 14.12 (2012): 123011.

[7] Ekerå, Martin, and Johan Håstad. "Quantum algorithms for computing short discrete logarithms and factoring RSA integers." Post-Quantum Cryptography: 8th International Workshop, PQCrypto 2017, Utrecht, The Netherlands, June 26-28, 2017, Proceedings 8. Springer International Publishing, 2017.

[8] M. Eker ˚ a. Quantum algorithms for computing general discrete logarithms and orders with tradeoffs. Journal of Mathematical Cryptology, 15(1):359–407, 2021.

[9] Gidney, Craig, and Martin Ekerå. "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits." Quantum 5 (2021): 433.

[10] A. G. Fowler, M. Mariantoni, J. M. Martinis, and A. N. Cleland. Surface codes: Towards practical large-scale quantum computation. Physical Review A, 86(3):032324, 2012.

[11] Larasati, Harashta Tatimma, et al. "Depth Optimization of FLT-Based Quantum Inversion Circuit." IEEE Access (2023).

[12] Putranto, Dedy Septono Catur, et al. "Depth-optimization of Quantum Cryptanalysis on Binary Elliptic Curves." IEEE Access (2023).