암호해독을 위한 쇼어 알고리즘 최적화 연구 동향 분석

조재한, 신다윗, 김호원
부산대학교
jaehan@islab.re.kr, dawit@islab.re.kr, howonkim@gmail.com

Analyzing research trends in optimizing shore algorithms for cryptocurrency

Cho Jae Han, Shin Da Wit, Kim Ho Won†
Pusan National Univ.

요 약

1982년 리처드 파인만이 양자 컴퓨터를 제안한 이후, 이와 관련된 연구가 꾸준히 진행되고 있다. 양자 컴퓨터의 기술이 점차 발전하게 되면서, 기존의 고전 컴퓨터가 해결하지 못하는 문제를 해결할 수 있게 되었다. 따라서 이를 위해 다양한 양자 알고리즘이 제시되고 있다. 이중 쇼어 알고리즘은 기존 컴퓨터가 해결하지 못하는 소인수 분해 문제를 다항 시간 안에 해결할 수 있음이 알려지면서, 소인수 분해 문제를 기반으로 제작된 공개 키 암호 알고리즘이 해독될 수 있음이 확인되었다. 하지만 현재 사용하고 있는 암호 알고리즘을 해독하기 위해서는 충분한 양의 양자 컴퓨팅 파워가 필요하며, 이를 해결하기 위해 다양한 알고리즘 최적화 연구가 진행되고 있다. 본 논문에서는 알고리즘 최적화를 위한 연구 동향에 관해 설명한다.

Ⅰ. 서 론

0과 1, 0과 1이 중첩된 상태를 이용하여 연산을 진행하는 양자 컴퓨터는 기존 고전 컴퓨터가 해결할 수 없었던 수학적 난제들을 해결할 수 있다. 따라서 양자 컴퓨터에 관한 다양한 연구가 진행되고 있으며, 양자 알고리즘은 대표적인 연구 분야 중 하나이다. 현재 연구를 통해 다양한 양자 알고리즘이 제안되었으며, 대표적인 양자 알고리즘으로는 쇼어 알고리즘(Shor's Algorithm)이 있다. 쇼어 알고리즘을 활용하면 고전 컴퓨터가 해결할 수 없었던 소인수 분해 문제를 다항 시간 안에 해결할 수 있으며, 이는 소인수 분해 문제를 기반으로 작동하는 공개 키 암호 알고리즘이 해독될 수 있음을 의미한다. 하지만, 현재 쇼어 알고리즘으로 효율적인 소인수 분해를 진행하기 위해서는 높은 양자 컴퓨팅 파워가 필요하다. 따라서, 이를 해결하기 위해 해당 알고리즘에 관한 최적화 연구가 다양하게 진행되고 있다. 본 논문에서는 2장에서 대표적인 양자 알고리즘인 쇼어 알고리즘과 그로버 알고리즘에 관해 설명하며, 3장에서는 쇼어 알고리즘의 최적화를 위한 연구에 관해 설명한다. 이후 4장 결론으로 마무리한다.

Ⅱ. 배경지식

양자 컴퓨터에서 작동하는 양자 알고리즘은 알고리즘이 사용하는 주요 기술을 기반으로 크게 두 종류로 나눌 수 있다. 첫 번째는 양자 푸리에 기반 알고리즘이며, 도이치-조사 알고리즘(Deutsch's Algorithm), 사이먼 알고리즘(Simon's Algorithm), 쇼어 알고리즘 등이 양자 푸리에를 기반으로 하는 알고리즘이다. 두 번째는 진폭 증폭 알고리즘이며, 대표적인 알고리즘으로는 그로버 알고리즘이 있다. 본 장에서는 다양한 양자 알고리즘 중 대표적인 양자 알고리즘인 쇼어 알고리즘과 그로버 알고리즘에 관해 설명한다.

2.1 쇼어 알고리즘

1994년 Peter Shor가 제안한 쇼어 알고리즘은 다항 시간 안에 소인수 분해 문제 및 이산 로그 문제를 해결하는 양자 알고리즘이다. 쇼어 알고리즘을 활용한 소인수 분해의 과정은 아래와 같다.

1) 소인수 분해를 진행할 N에 대해서, 1보다 크고 N보다 작은 정수 a를 임의로 선택 진행

1-1) $\gcd(N, a) \neq 1$이면, $\gcd(N, a)$이 N의 소인수

1-2) $\gcd(N, a) = 1$이면, 함수 $f(x) = a^x \pmod N$의 주기 r을 찾음

2) 주기 r이 홀수면 처음부터 다시 반복하며, 주기 r이 짝수면 아래와 같은 $\gcd_1$, $\gcd_2$를 구함

2-1) $\gcd_1 = \gcd(N, a^{r/2} + 1)$

2-2) $\gcd_2 = \gcd(N, a^{r/2} - 1)$

3) $\gcd_1$과 $\gcd_2$의 결과가 1, N이면 처음부터 다시 반복하며, 1과 N이 아니면 N의 소인수는 $\gcd_1$과 $\gcd_2$

쇼어 알고리즘은 위와 같은 소인수 분해 과정에서 주기 r을 빠르게 찾기 위해 사용된다. $a^x \pmod N$의 주기 r은 양자 중첩을 만들어주는 Hadamard Gate와 $f(x) = a^x \pmod N$를 계산하기 위한 Operator U 로 구성되어있다. 앞선 연산 과정 이후 QFT(Quantum Fouier Transformation)을 통해 연산 목표인 주기 r을 찾아내며, 이후 N에 대한 소인수를 찾는다. 다음과 같은 과정을 통해 기존 고전 컴퓨터가 해결하지 못하였던 소인수 분해 문제를 다항 시간 안에 해결할 수 있다.[1]

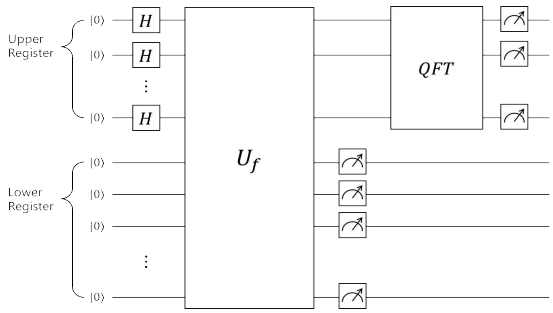

그림 1. Shor's Algorithm Circuit

2.2 그로버 알고리즘

그로버 알고리즘은 탐색 문제에 대한 기하학적 특성과 양자적 특성을 이용하여 탐색 문제를 다항 시간 안에 해결하기 위한 양자 알고리즘이다. 그로버 알고리즘은 양자 중첩, 오라클, 증폭 3단계로 구성되어있다. 그로버 알고리즘의 동작 순서는 아래와 같다.

1) 중첩 상태를 통해 모든 확률을 동일하게 초기화함
2) 오라클 함수를 통해 정답인 부분의 위상을 반전시킴
3) 오답인 부분들의 평균확률이 줄어들고 그만큼 반전시킨 부분의 확률이 증가함
4) 정답 부분의 위상을 반전시키며, 최종 확률을 확인함
5) 해당 알고리즘을 반복 실행하여 정답인 부분의 확률을 증가시킴

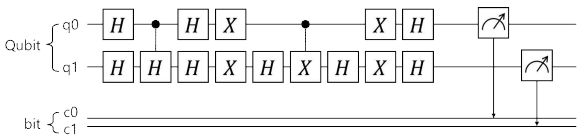

그림 2. 2 큐비트의 그로버 알고리즘 회로

이와 같은 과정을 통해 그로버 알고리즘은 고전 컴퓨터에 비해 빠른 속도로 탐색 문제를 해결할 수 있다.

Ⅲ. 본론

쇼어 알고리즘은 다양한 방면에서 최적화를 위한 연구가 진행되고 있다. 연구 분야는 알고리즘에 필요한 Qubit의 수의 최적화 및 회로의 Depth에 대한 최적화 크게 2가지 연구가 활발히 진행되고 있다. 본 장에서는 해당 최적화 연구에 관해 설명한다.

3-1 쇼어 알고리즘의 큐비트 수 최적화 연구

2024년 Clemence Chevignard 등은 쇼어 알고리즘의 효율성을 극대화하기 위해 필수적인 논리적 큐비트 수를 최적화하는 연구를 진행하였다. 이들의 연구에서는 실제 연산을 처리하는 레지스터의 크기를 $O(\log n)$로 줄임으로써 소인수 분해의 공간 복잡도를 혁신적으로 개선하였다. 제안된 방법은 필요한 연산 공간을 최소화하면서도 모듈식 지수 연산 결과를 효과적으로 계산할 수 있는 방안을 제시하였다. 이는 쇼어 알고리즘의 전반적인 효율성을 크게 향상하는 결과를 가져왔다. [2]

3-2 쇼어 알고리즘의 Depth 최적화 연구

2023년 Dewang Sun 등은 approximate QTF를 활용하여 쇼어 알고리즘의 Depth를 줄이는 최적화 연구를 진행하였다. 해당 연구는 쇼어 알고리즘의 QFT와 approximate QFT 구현 간의 정확성과 런타임의 비교를 진행하였다. 이후, 다양한 입력 크기에 대한 속도 향상 및 상대적 차이에 대한 데이터를 기반으로 효율적인 접근 방식을 제안하는 연구를 진행하였다.[3]

또한, 2023년 Harashta Tatimma Larasati 등은 페르마의 소정리(FLT)를 기반으로 Inversion 회로의 Depth를 줄이는 연구를 진행하였다. 해당 연구는 워터폴 방식을 사용하여 Itoh-Tsujii의 변형 FLT를 양자 회로로 변환하여 역 제곱 연산을 제거하여 CNOT 게이트 수를 줄이고 T Depth를 줄이는 연구이다. 또한, Gidney의 상대 위상 Toffoli 게이트를 통합하여 회로의 T Depth와 회로 전체 Depth를 더욱 줄여 계산 시간의 효율성을 향상했다.[4]

Ⅳ. 결론

양자 컴퓨터가 제안된 이후, 쇼어 알고리즘이 고전 컴퓨터가 해결하지 못하던 소인수 분해 문제 및 이산 로그 문제를 해결할 수 있음이 알려지면서, 알고리즘의 최적화를 위한 다양한 연구가 진행되고 있다. 최적화 연구는 크게 큐비트 수의 최적화와 회로의 Depth 최적화 각각에 초점을 맞추어 진행되고 있지만, 두 개의 최적화를 동시에 적용하는 연구는 앞선 연구들에 비해 많이 진행되고 있지 않다. 따라서, 향후 연구로는 큐비트의 최적화 및 회로의 Depth 최적화를 함께 진행하는 연구를 진행할 예정이다.

ACKNOWLEDGMENT

이 논문은 2024년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2019-0-00033, 미래컴퓨팅 환경에 대비한 계산 복잡도 기반 암호 안전성 검증 기술개발, 100%)

참 고 문 헌

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

[2] Chevignard, C., Fouque, P.-A., & Schrottenloher, A. (2024). Reducing the Number of Qubits in Quantum Factoring. Retrieved from https://eprint.iacr.org/2024/222

[3] D. Sun, N. Zhang and F. Franchetti, "Optimization and Performance Analysis of Shor's Algorithm in Qiskit," 2023 IEEE High Performance Extreme Computing Conference (HPEC), Boston, MA, USA, 2023, pp. 1-7, doi: 10.1109/HPEC58863.2023.10363522.

[4] H. T. Larasati, D. S. C. Putranto, R. W. Wardhani, J. Park and H. Kim, "Depth Optimization of FLT-Based Quantum Inversion Circuit," in IEEE Access, vol. 11, pp. 54910-54927, 2023, doi: 10.1109/ACCESS.2023.3280632.0.