암호의 양자 회로 최적화 구현 방법에 대한 연구

양유진[1], 장경배[2], 임세진[1], 오유진[3], 서화정[4]
[1]한성대학교 IT융합공학과 석사과정
[2]한성대학교 IT융합공학과 박사과정
[3]한성대학교 융합보안학과 석사과정
[4]한성대학교 융합보안학과 교수
yujin.yang34@gmail.com, starj1023@gmail.com, dlatpwls834@gmail.com,
oyj0922@gmail.com, hwajeong84@gmail.com

A Study on the Implementation Method of Quantum Circuit Optimization for Cipher

Yu-Jin Yang[1], Kyung-Bae Jang[2], Se-Jin Lim[1], Yu-Jin Oh[3], Hwa-Jeong Seo[4]
[1]Dept. of IT Convergence Engineering, Han-Sung University
[2]Dept. of IT Convergence Engineering, Han-sung University
[3]Dept. of Convergence Security, Han-Sung University
[4]Dept. of Convergence Security, Han-Sung University

요 약

양자 컴퓨터가 발전됨에 따라 이와 관련된 연구들이 꾸준히 발표되고 있다. 그 중 양자 컴퓨터의 응용과 밀접한 연관이 있는 양자 회로 최적화 연구는 양자 컴퓨터 환경에서의 암호 공격 비용 추정 연구에서 핵심으로 여겨진다. 본 논문에서는 양자 회로 최적화를 위한 방법과 암호 구현 분야에서 이를 적용한 논문들에 대해 살펴보고자 한다.

1. 서론

양자 컴퓨터가 발전함에 따라 암호, 화학, 인공지능 등 다양한 분야에서 이를 응용하는 사례들이 보고되고 있다. 양자 컴퓨터 상에서의 연산을 나타내는 양자 회로는 모든 응용에서 빠질 수 없는 요소로, 양자 컴퓨터의 자원적 제약 및 실제 실행과 밀접한 연관이 있기 때문에 이를 최적화하는 연구도 지속적으로 이뤄지고 있는 상황이다. 이와 관련하여 연구적 발전을 위해서는 다양한 최적화 사례들을 아는 것이 중요하다. 암호 관련 분야에 해당하는 암호 공격 비용 측정 연구에서는 양자 회로 최적화 연구를 핵심으로 다루고 있다. 따라서, 본 논문에서는 최적화 방법이 적용된 암호 구현 연구를 바탕으로 양자 회로를 최적화하기 위한 방법들에 대해 살펴본다.

2. 관련 연구

2.1 qubit와 depth

고전컴퓨터 상에서의 bit와 같은 역할을 하는 큐비트(qubit)는 양자 컴퓨터에서 쓰이는 양자 정보로, 하나의 큐비트는 양자 컴퓨터의 중첩 상태를 이용하여 0과 1일 확률을 가진다. depth는 구성된 양자 회로의 깊이를 의미하며 실행 속도와 관련이 있다. 과거에는 큐비트 수에 대한 관심이 더 컸지만, 최근 들어 depth의 중요성도 같이 커지고 있다.

2.2 양자 게이트와 양자 회로

양자 컴퓨터에서는 기존의 논리 게이트를 사용하지 못하기 때문에 그를 대체하기 위하여 다양한 양자 게이트들이 등장하였다. 그 중 CNOT 게이트는 1개의 타겟 큐비트(target qubit)와 이에 영향을 끼치는 제어큐비트(control qubit) 1개를 입력으로 가진다. 고전적인 논리 게이트에서는 XOR 게이트에 대응된다고 볼 수 있다. 고전 논리 게이트에서 AND 게이트의 역할을 수행한다고 볼 수 있는 Toffoli 게이트는 2개의 제어큐비트와 1개의 타겟 큐비트를 가진다. T 게이트는 회전연산을 수행하는 위상 게이트의 일종으로 내결함성(Fault-tolerant) 양자 회로 구현에 사용된다. T-count는 회로에 사용된 T게이트의 수를, T-depth는 T 게이트의 depth를 의미하며 T 게이트가 병렬로 구현되어 있을수록 T-depth는 낮아진다.

양자 컴퓨터 또한 고전 컴퓨터처럼 회로가 존재한다. 이를 양자 회로라 부르며 양자 게이트, 측정 등의

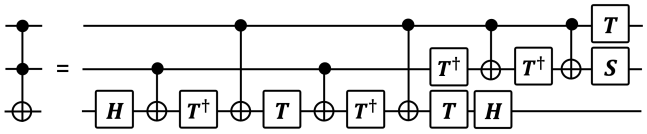
연산 작업들로 구성되는 양자 계산을 위한 모델로 정의된다. 양자 컴퓨터의 경우 고전 컴퓨터보다 자원의 한계가 훨씬 크기 때문에, 양자 컴퓨팅 환경에 직접적으로 동작하는 양자 회로를 최적화하는 연구는 불가피하다.

3. 양자 회로 최적화 연구

회로 최적화를 위해서는 기본적으로 큐비트 수, 게이트 수, depth와 같은 양자 자원의 수를 줄여야 한다. 현재, 양자 회로를 최적화하기 위한 다양한 연구가 진행되고 있다. 본 장에서는 그 중 Toffoli 게이트와 양자 회로의 구조, 선형 레이어를 최적화하는 방법에 대해 간략하게 소개하고 그에 따른 연구 사례들을 살펴본다.

3.1 Toffoli 게이트

제어 큐비트가 많을수록 양자 회로 구현에 필요로 하는 자원수를 의미하는 양자 비용이 증가하기 때문에, Toffoli 게이트는 양자 게이트 중 양자 비용이 비싸다 여겨진다. 이러한 Toffoli 게이트의 물리적 구현은 보통 여러 개의 게이트의 조합으로 이뤄진다. 가장 기본적인 Toffoli 게이트는 (그림 1)처럼 6개의 CNOT 게이트와 T, Tdagger, H게이트로 분해되며, T-count는 7, T-depth는 6이다[1]. Toffoli 게이트는 양자 자원 특히 양자 회로의 depth와 깊은 관련이 있고, 암호 구현 시 자주 사용되는 덧셈기, 곱셈기 등에 필수적으로 사용되기 때문에 이를 최적화하는 것이 상당히 중요하다.



(그림 1) 기본적인 Toffoli 게이트 분해

Amy et al.[2]은 Toffoli 게이트를 Clifford + T 세트로 분해하며 T-count는 유지한 채 T-depth를 3으로 줄인 Toffoli 게이트를 제시하였다. 이는 [1]의 Toffoli 게이트 분해보다 40%의 속도향상이 이뤄진 것으로 암호 구현을 비롯한 다양한 회로 구현에서 사용되고 있다.

[3]은 T-depth 최적화에 더 집중하기 위해 추가적인 보조 큐비트를 4개 더 할당하여 T 게이트를 병렬로 구성함으로써 T-depth가 1인 Toffoli 게이트를 구현하였다. 해당 논문에서는 많은 보조 큐비트를 할당하더라도 T-depth를 1로 줄일 수 없는 회로 구현도 존재함을 보였다.

더 나아가 내결함성 양자 컴퓨팅 환경에서의 실행까지 고려한 Toffoli 게이트 최적화 연구도 이뤄지고 있다. [4]에서는 2가지 내결함성 Toffoli 게이트를 제안하였다. T-count를 7에서 4로 줄인 첫 번째 게이트는 정확한 Toffoli 게이트를 구현하기 위하여 추가적으로 보조 큐비트와 S 게이트, teleportation을 이용하였다. 그 다음 제시한 게이트는 오류감지 Toffoli 게이트로, 감지되지 않은 오류가 있을 확률이 높을수록 T 게이트의 비용이 줄어든다는 점에 주목하여 T 게이트의 개수가 아니라 사용되는 T 게이트의 비용을 줄임으로써 자원 문제를 해결한 것이다.

[5]는 [4]의 첫 번째 내결함성 Toffoli 게이트에 사용되었던 구성을 적용시킨 임시 논리 AND 게이트를 제안하였다. 이를 통해 기존의 Toffoli 게이트의 구현보다 T 게이트 수를 절반가량 줄였고, 임시 논리 AND 게이트를 적용한 가산기를 제시하여 예상 비용의 감소를 보였다.

3.2 선형 연산

선형 계층의 연산을 최적화하는 방법을 도입하여 회로를 최적화하는 연구도 있다. 이는 양자 회로 뿐 아니라 일반적인 컴퓨터의 회로 최적화와도 연관이 깊다. 암호의 치환 연산에 사용되는 S-box와 같은 하위 회로 구현에 적용될 수 있으며 선현 연산 최적화를 거치고 나면 오직 XOR 게이트로만 이뤄진 선형 구성을 가지게 된다. 선형 연산 최적화 기법 또한 Toffoli 게이트와 연관되어 있지만 Toffoli 게이트 자체를 최적화하는 것이 아니라 상대적으로 비용이 낮은 CNOT 게이트로 대체함으로써 사용되는 Toffoli 게이트 수를 줄이는 데 집중한 것이다.

선형 연산 최적화 기법을 응용하는 것으로 PLU 분해 기법이 대표적이다. PLU 혹은 LUP라고도 불리는 이 분해 방법은 행렬을 치환행렬과 두 가지 삼각행렬의 곱으로 나타내는 것이다. 이를 통해 계산량을 줄일 수 있다는 장점이 있다. 해당 방법은 다양한 암호 양자 회로 구현 연구에서 사용이 되었다[6,7].

[8]에서는 가장 효율적인 구현을 검색하여 값을 출력해주는 휴리스틱 알고리즘을 제안하였다. 이를 통해 최적의 행렬 분해를 구성할 수 있다. 해당 논문은 양자와 관련된 논문이 아니지만 PLU 분해와 마찬가지로 XOR로 나오는 결과를 양자 코드로 변환하여 구현이 가능하다.

또한, 조합 회로 최적화라는 방법을 이용하여 최적

화한 사례도 있다. [9]에서 제안하는 조합 회로 최적화는 크게 두 단계로 구성된다. 첫 번째 단계에서는 회로의 비선형 구성 요소 즉, 논리곱 연산을 수행하는 AND 게이트를 식별하고 이를 줄이는 단계이다. AND 게이트를 감소시키는 것은 매우 어려운 과정으로 Ad-hooc 휴리스틱을 이용하여 낮은 곱셈 복잡도를 가진 회로를 구성하였다. 두 번째 단계는 회로의 최대 선형 구성 요소를 찾은 후 선형 구성 요소에서 계산된 목표 함수를 계산하기 위해 필요로 하는 XOR 게이트 수를 최소화 한다. XOR 게이트 최소화를 위하여 [9]에서는 새로운 휴리스틱을 제안하였다.

3.3 아키텍처

똑같은 연산을 수행하더라도 회로의 구조를 어떻게 구성하느냐에 따라 비용이 달라진다. 대표적으로 지그재그(zig-zag)와 파이프라인(pipe-line) 아키텍처가 있다.

지그재그 구조는 기본적으로 큐비트에 최적화 되어 있다. 큐비트를 절약하기 위하여 역연산으로 이전 라운드에서 사용된 큐비트를 초기화한 후, 다음 라운드에서 재사용하는 구조로 이뤄졌다. 이때 역연산으로 인해 depth가 증가한다는 한계를 갖는다. Grassl et al.는 최초로 AES 양자 회로를 구현한 논문[6]에서 아키텍처로 지그재그 방식을 채택하였다. 이는 지그재그 구조를 적용한 대표적인 연구로 여겨지며, 향후 해당 논문을 개선하는 다양한 연구들이 발표되었다.

파이프라인 구조는 역연산을 통해 큐비트를 재활용하는 대신, 추가적인 보조큐비트를 할당함으로써 depth의 수를 줄이는 데 집중한 방법이다. 큐비트 뿐 아니라 depth에 대한 중요성이 커짐에 따라 최신 연구들에는 지그재그 보다는 파이프라인 구조가 적용되었다. Jang et. al[10]은 AES의 양자 회로에 파이프라인 아키텍처를 적용함으로써 전체 depth를 감소시켰다.

4 결론

본 논문에서는 양자 회로의 최적화를 위한 방법들과 이를 양자 컴퓨터 환경에서의 암호 양자 회로 구현 연구에 적용한 사례들을 살펴보았다. 제시된 방법들을 적절하게 잘 구성한다면 최적화에 큰 도움이 될 수 있을 것이다. 이밖에도 여전히 양자 회로와 관련된 연구가 활발하게 이뤄지고 있기 때문에 다양한 방법들이 꾸준히 발표될 것으로 기대된다.

5. Acknowledgements

This work was partly supported by Institute for Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (<Q|Crypton>, No.2019-0-00033, Study on Quantum Security Evaluation of Cryptography based on Computational Quantum Complexity, 75%) and this work was partly supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No.2022-0-00627, Development of Lightweight BIoT technology for Highly Constrained Devices, 25%).

참고문헌

[1] Michael A. Nielsen, Chuang Isaac "Quantum computation and quantum information" 2002.

[2] Amy, Matthew, et al. "A meet-in-the-middle algorithm for fast synthesis of depth-optimal quantum circuits." IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 32.6 (2013): 818-830.

[3] Selinger, Peter. "Quantum circuits of T-depth one." Physical Review A 87.4 (2013): 042302.

[4] Jones, Cody. "Low-overhead constructions for the fault-tolerant Toffoli gate." Physical Review A 87.2 (2013): 022328.

[5] Gidney, Craig. "Halving the cost of quantum addition." Quantum 2 (2018): 74.

[6] Grassl, Markus, et al. "Applying Grover's algorithm to AES: quantum resource estimates." Post-Quantum Cryptography: 7th International Workshop, PQCrypto 2016, Fukuoka, Japan, February 24-26, 2016, Proceedings 7. Springer International Publishing, 2016.

[7] Jaques, Samuel, et al. "Implementing Grover oracles for quantum key search on AES and LowMC." Advances in Cryptology–EUROCRYPT 2020: 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10–14, 2020,

Proceedings, Part II 30. Springer International Publishing, 2020.
[8] Xiang, Zejun, et al. "Optimizing implementations of linear layers." IACR Transactions on Symmetric Cryptology (2020): 120-145.
[9] Boyar, Joan, and René Peralta. "A new combinational logic minimization technique with applications to cryptology." Experimental Algorithms: 9th International Symposium, SEA 2010, Ischia Island, Naples, Italy, May 20-22, 2010. Proceedings 9. Springer Berlin Heidelberg, 2010.
[10] Jang, Kyungbae, et al. "Quantum analysis of aes." Cryptology ePrint Archive (2022).