양자회로 최적화 기법 및 적용 조사

송경주[1], 이민우[2], 서화정[4]
[1]한성대학교 정보컴퓨터공학과 박사과정
[2]한성대학교 융합보안학과 석사과정
[3]한성대학교 IT융합공학부 교수
thdrudwn98@gmail.com, minunejip@gmail.com, hwajeong84@gmail.com

Research trend on optimization techniques for quantum circuits

Gyeong-Ju Song[1], Min-Woo Lee[2], Hwa-Jeong Seo[3]
[1]Dept. of Information Computer Engineering, Han-Sung University
[2]Dept. of Convergence Security, Han-Sung University
[3]Dept. of IT Convergence Engineering, Han-Sung University

요 약

양자 컴퓨터의 연산 성능이 알려지면서 기존 암호 시스템이 붕괴될 것이라 예상한다. 앞선 많은 연구들은 공격 대상 암호에 대해 양자회로로 구현하고 공격에 필요한 양자자원을 추정하였지만 암호를 공격하기 위해서는 대규모 양자컴퓨터의 동작을 요구한다. 뿐만 아니라 내결함성 양자 컴퓨터에서 유효한 결과를 얻기 위해서는 오류 정정이 필수적이며 오류 정정에도 양자 자원을 소비하며 결과적으로 더 큰 규모의 양자컴퓨터가 필요하고 크기가 커질수록 오류가 증가한다. 이러한 내결함성 대규모 양자회로에서 T 게이트를 구현하는 것이 다른 게이트를 구현하는 것 보다 어렵고 T-depth가 회로의 실행시간에 큰 영향을 미친다. 본 논문에서는 T-depth 최적화 도구 및 T-depth 감소 기법을 적용한 방식을 조사하였다.

1. 서론

양자 컴퓨터는 양자역학 현상을 연산에 이용하여 계산 속도를 높인다. 이러한 양자 컴퓨터의 성능이 알려지며 이론적으로 현재 사용되는 대칭키 암호의 보안 레벨이 절반으로 감소하고 공개키 체계가 붕괴될 것이라 예상된다. 앞선 연구들은 공격 대상 암호에 대해 양자회로로 구현하여 공격에 필요한 양자자원을 추정하는 연구를 진행하였다[1-4]. 하지만 현재의 양자 컴퓨터는 규모가 작아 유효한 암호공격이 어려우며 양자공격에 필요한 양자자원 추정치에 미치는 대규모 양자컴퓨터가 필요할 것이라 예상한다. 내결함성 양자컴퓨터에서 유효한 정보를 얻기 위해서는 오류 정정이 필수적이며 오류 정정에 더 많이 양자자원이 소모되기 때문에 암호공격에 예상되는 양자 자원보다 훨씬 많은 자원이 필요하다. 내결함성 모델에서는 Clifford+T 게이트로 구성된 회로에서 T 게이트를 구현하는 것이 다른 모든 게이트를 구현하는 것보다 훨씬 어렵고 T-depth가 회로의 실행 시간에 직접적으로 결정한다고 알려졌다. 따라서 기존 양자회로 구현에 대해 T-count 및 T-depth를 줄이기 위한 연구들을 진행하고 있으며 병렬구현, 게이트 조합 등의 방법을 시도하였다. 본 논문에서는 양자회로에 대한 최적화 기법 및 적용에 대한 연구 동향을 살펴본다.

2. 배경 지식

양자 컴퓨터는 큐비트의 양자역학 현상을 통해 연산을 진행하고 특정 문제에 대한 계산 속도를 높일 수 있다고 알려져 있다. 양자 알고리즘인 Grover algorithm[5]은 대칭키 암호에 대한 brute-force attack을 가속화하여 보안 강도를 약 절반 정도로 줄이며 Shor algorithm[6]은 일반 컴퓨터에서 난제였던 인수분해를 다항시간 내에 수행할 수 있다고 알려져 있다. 두 양자 알고리즘을 동작하기 위해서는 기존 암호들이 양자회로로 구현되어야 하며 앞선 연구들은 암호에 대해 양자회로로 구현하고 필요한 양자자원을 추정하는 연구들을 진행하였다[1-4]. 내결함성 양자 컴퓨터에서 양자회로를 동작하기 위해서는 회로에 대한 오류 감지 및 정정이 필요하며 이를 위한 오류 수정 알고리즘 연구도 많이 진행되고 있다. 이와 같은 노력 외에도 양자 회로에서 연산 시간에 많은

영향을 미치는 depth를 줄여 회로 자체의 오류를 줄이기 위한 연구들도 진행되었다.

3.1 양자 게이트

양자 회로에서 Clifford+T 세트는 내결함성 게이트 세트를 형성하며 H, CNOT, T 게이트는 Clifford+T 집합에서의 최초 생성 집합이다. 대표적인 Clifford+T 양자 게이트 NOT(X), Hadamard(H), T, Controlled-NOT(CNOT), T, $P := T^2$, $Z := T^4$, $T^\dagger := T^7$, $P^\dagger := T^6$ 등은 양자회로에서 사용된다. 양자컴퓨터는 Clifford+T 게이트 세트로 구성된 양자회로로 동작하는데, 연속적인 T 게이트는 phase 게이트로 대체될 수 있어 양자회로 비용을 줄일 수 있다. 아래 수식은 양자 게이트 동작을 보여준다.

$$H: \mid x_1\rangle \rightarrow \frac{\mid 0\rangle + (-1)^{x_1} \mid 1\rangle}{\sqrt{2}}$$
$$CNOT: \mid x_1 x_2\rangle \rightarrow \mid x_1(x_1 \oplus x_2)\rangle$$
$$X: \mid x_1\rangle \rightarrow \mid x_1 \oplus 1\rangle$$
$$T: \mid x_1\rangle \rightarrow e^{\frac{\pi i}{4} x_1} \mid x_1\rangle$$
$$Z: \mid x_1\rangle \rightarrow (-1) e^{\frac{\pi i}{4} x_1} \mid x_1\rangle$$
$$P: \mid x_1\rangle \rightarrow e^{\frac{\pi i}{2} x_i} \mid x_1\rangle$$

Toffoli 게이트는 Clifford+T 양자 게이트로 분해할 수 있는데, 분해 방식은 다양하며 <그림 1>은 [7]에서 T-depth: 3, T-count: 7 로 분해한 Toffoli 게이트를 보여준다.

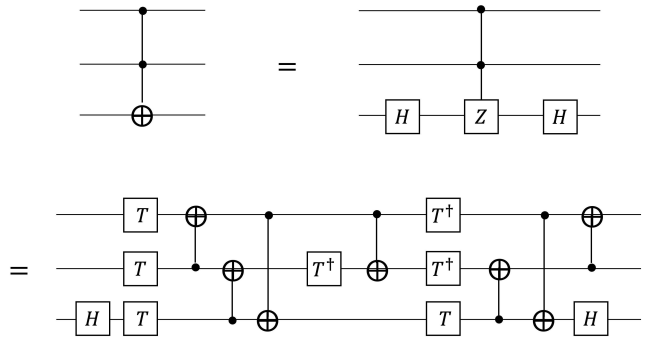

그림 1 Toffoli gate[7] (T-depth: 3, T-count: 7)

3. 연구동향

3.1 T-depth 최적화 도구[8]

해당 논문에서는 내결함성 양자컴퓨터를 위한 양자회로의 T-depth를 최적화 방식을 제안하였다. 일반적으로 양자회로에서 T 게이트가 내결함성 양자컴퓨터에서 가장 많은 비용을 필요로 한다. Clifford+T 게이트로 구성된 양자회로를 추가적인 ancilla을 통해 재합성하여 T 게이트를 최적으로 병렬화하여 T-depth를 줄이는 메트로이드 분할을 수행한다. 해당 자동화 tool은 ancilla 및 큐비트 수 및 특정 회로에 제한되지 않게 보편적으로 T-depth를 최적화한다. 제한하는 기법은 추가적인 ancilla 큐비트 없이 T-depth 약 61.1%, T-count 약 39.9% 감소한 결과를 보이며, ancilla 큐비트를 사용하면 T-depth를 약 80.7%, 최대 99.7% 까지 감소함을 보였다.

3.2 T-depth 감소 기법 적용[9]

해당 논문에서는 두 개의 Toffoli gate 사이에 위치한 Controlled-phase gate의 상호 교환을 통해 T-depth 및 T-count를 줄이는 기술 적용을 제안하였으며 SHA3에 대해 양자회로에 적합한 4가지의 양자회로 덧셈기를 선정하고 해당 방법으로 T-depth를 약 33% 감소시켰다. 두 개의 Toffoli gate 사이에 있는 양자회로에 대해 Controlled-phase gate의 교환을 통해 T-depth가 6에서 4 or 5 로 감소하였다. 해당 논문에서는 제안하는 방식은 [10]의 10가지 경우에 대해 모두 적용할 수 있지만, 해당 논문에서는 <그림 2>와 같이 세 가지 경우: 두 Control line과 target line이 모두 공유되는 경우, Control line들만 공유되는 경우, target line 만이 공유되는 경우에 대해 자세히 설명하였다.

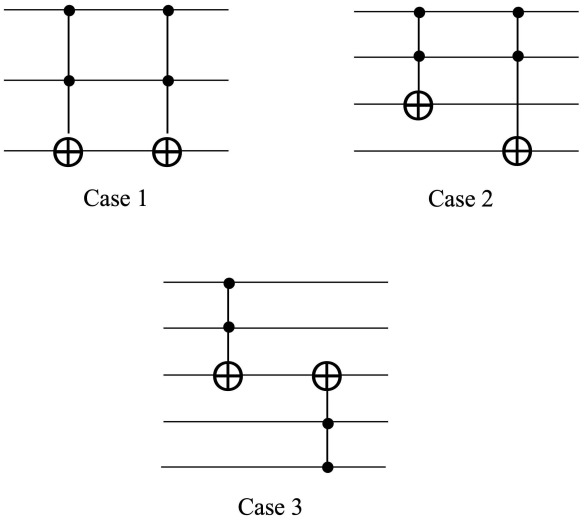

그림 2 T-depth 감소를 적용한 세 가지 경우

두 개의 Toffoli 게이트가 두 개의 control line과 한 개의 target line을 공유하는 경우에 대해 두 개의 Toffoli 게이트 중 왼쪽 Toffoli 게이트의 오른쪽에 Control-phase(CP)와 $CP^{\dagger}$를 생성한다. 두 게이트는 서로 역연산을 진행하므로 최종 결과에 영향을 주지 않는다. 만약, subcircuit과 CP 게이트 사이에서 교환법칙이 성립하는 경우라면 CP 게이트를 오른쪽 Toffoli 게이트의 왼쪽으로 이동할 수 있다. (subcircuit: 두 개의 Toffoli 게이트 사이에 위치한 양자회로). 해당 경우가 성립된다면 T-depth를 6에서 4로 T-count를 14에서 8로 줄일 수 있다.

두 번째 경우는 두 개의 control line을 공유하며 target line을 공유하지 않을 때, 첫 번째 경우와 같은 방법으로 T-depth를 줄일 수 있다. 이때, Toffoli 게이트가 off-control part를 가져도 해당 방법을 사용할 수 있다.

세 번째 경우인 하나의 target line만 공유했을 때, T-count는 바뀌지 않지만 서로 다른 line에서 T 게이트가 구성되므로 T-depth를 공유할 수 있어 전체적인 T-depth가 3n에서 2n+1로 감소하며 추가 1 큐비트를 사용하면 n+1로 감소한다.

4. 결론

본 논문에서는 양자회로 최적화 기법에 대해 살펴보았다. T-depth 최적화 도구는 Clifford+T 게이트의 양자회로에 대해 추가 ancilla 큐비트를 사용하여 재합성하는 방법으로 메트로이드 분할을 수행하여 최적의 T 게이트 병렬화로 T-depth를 줄인다. T-depth 감소 기법을 적용하는 방식은 크게 3가지 경우: 두 Control line과 target line이 모두 공유되는 경우, Control line들만 공유되는 경우, target line 만이 공유되는 경우에 사용되는 예시를 조사하였지만 해당 방법은 [10]의 모든 10가지 경우에 대해 적용할 수 있다. 본 논문에서는 양자회로 최적화 기법 조사를 통해 양자회로가 여러 방식으로 양자자원을 감소시킬 수 있다는 것을 확인하였다.

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] Grassl, M., Langenberg, B., Roetteler, M., & Steinwandt, R. “Applying Grover’s algorithm to AES: quantum resource estimates.” In Post-Quantum Cryptography: 7th International Workshop, PQCrypto 2016, Fukuoka, Japan, Proceedings 7 (pp. 29-43). Springer International Publishing, 2016, February 24-26.

[2] Amy, M., Di Matteo, O., Gheorghiu, V., Mosca, M., Parent, A., & Schanck, J. “Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3.” In Selected Areas in Cryptography - SAC 2016: 23rd International Conference, St. John's, NL, Canada, August 10-12, 2016, Revised Selected Papers (pp. 317-337). Cham: Springer International Publishing, 2017, October.

[3] Song, G., Jang, K., Kim, H., Eum, S., Sim, M., Kim, H., ... & Seo, H. “SPEEDY Quantum Circuit for Grover’s Algorithm.” Applied Sciences, 6870. 2022, 12.14.

[4] Jang, K., Song, G., Kwon, H., Uhm, S., Kim, H., Lee, W. K., & Seo, H. “Grover on PIPO.” Electronics, 1194. 2021, 10.10.

[5] Grover, Lov K. "A fast quantum mechanical algorithm for database search." Proceedings of the twenty-eighth annual ACM symposium on Theory of computing. 1996.

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

[7] 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.
[8] Amy, Matthew, Dmitri Maslov, and Michele Mosca. "Polynomial-time T-depth optimization of Clifford+ T circuits via matroid partitioning." IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 33.10 (2014): 1476-1489, 2014.
[9] Lee, J., Lee, S., Lee, Y. S., & Choi, D. T depth reduction method for efficient SHA 256 quantum circuit construction. IET Information Security, 17(1), 46-65. (2023).
[10] Rahman, Md Zamilur, and Jacqueline E. Rice. "Templates for positive and negative control Toffoli networks." Reversible Computation: 6th International Conference, RC 2014, Kyoto, Japan, July 10-11, 2014. Proceedings 6. Springer International Publishing, 2014.