Draper 양자 덧셈기에 대한 T 게이트 최적 구현

임세진*, 장경배*, 김현준*, 서화정**

*한성대학교 (대학원생)

**한성대학교 (교수)

T gate Optimal Implementation of Draper Quantum Adder

Se-jin Lim*, Kyung-bae Jang*, Hyun-jun Kim*, Hwa-jeong Seo**

*Hansung University (Graduate student)

**Hansung University (Professor)

요 약

양자컴퓨터에서 동작하는 Grover 알고리즘과 Shor 알고리즘에 의해 현재 사용되고 있는 암호의 보안 강도 감소 및 무력화 시기가 다가오고 있다. 따라서 양자컴퓨터에 대한 암호의 보안 강도를 정확히 측정하기 위해 양자 공격 회로를 구현하여 요구되는 양자 자원을 추정하는 등의 연구가 수행되고 있다. 양자컴퓨터를 통한 해킹에는 많은 양자 자원이 필요하며, 안정적인 구동 환경이 갖춰져야 하므로 실현되기 위해서는 아직까지 상당한 시간이 소요될 것으로 보인다. 이에 연구자들은 필요한 양자 자원을 최소화할 수 있는 최적화된 양자 회로를 제시하고 있다. 회로의 깊이가 낮을수록 실행시간이 단축되므로, 낮은 깊이로 양자회로를 구현하는 것은 중요한 최적화 요소이며, 구현 비용이 높은 T 게이트의 수와 깊이를 줄이는 것이 핵심이다. 따라서 본 논문에서는 암호의 덧셈 연산에 사용할 수 있는 Draper 양자 덧셈기에 대해 T 게이트 최적 구현을 제안한다.

I. 서론

암호의 무작위 대입 공격의 가속화에 활용될 수 있는 Grover 알고리즘을 사용하면 기존 암호의 보안 강도가 제곱근만큼 감소하게 된다. 또한 Shor 알고리즘은 공개키 암호가 기반하고 있는 난제를 다항시간 내에 풀 수 있다. 따라서 두 양자 알고리즘에 의해 현재 사용되고 있는 암호의 보안 강도가 감소되고 무력화될 수 있다는 점에서 암호학계에서는 양자컴퓨터 시대를 대비하기 위한 연구를 수행하고 있다. 이러한 연구 중 하나로, 양자컴퓨터에 대한 암호의 보안 강도를 정확히 측정하기 위해 양자 공격 회로를 구현하여 요구되는 양자 자원을 추정하는 연구가 있다. 양자컴퓨터를 통한 해킹에는 많은 양자 자원이 필요하며, 안정적인 구동 환경이 갖춰져야 하므로 실현되기 위해서는 아직까지 상당한 시간이 소요될 것으로 보인다. 이에 연구자들은 필요한 양자 자원을 최소화할 수 있는 최적화된 양자 회로를 제시하고 있다. 회로의 깊이가 낮을수록 실행시간이 단축되므로, 낮은 깊이로 양자 회로를 구현하는 것은 중요한 최적화 요소이며, 구현 비용이 높은 T 게이트의 수와 깊이를 줄이는 것이 핵심이다[1]. 따라서 본 논문에서는 암호의 덧셈 연산에 사용할 수 있는 Draper 양자 덧셈기[2]에 대해 T 게이트 최적 구현을 제안한다.

II. 관련 연구

2.1 Draper 덧셈기[2]

덧셈 연산을 양자회로로 구현한 양자 덧셈기는 다항 깊이를 가지는 Ripple Carry Adder (RCA)와 대수 깊이를 가지는 Carry Lookahead Adder (CLA)로 나눌 수 있다. CLA는 캐리 연산을 병렬로 수행할 수 있기 때문에 대수 깊이를 갖게 된다. Draper 덧셈기는 대표적인 CLA이며, 덧셈 결과를 저장하는 위치에 따라 피연산자 중 하나에 저장하는 in-place 구현과 새로운 큐비트에 저장하는 out-of-place 구현이 있다. 아래 표 1은 Draper

	#Qubit	#Toffoli	Toffoli-depth
in-place	$4n-w(n)-\lfloor \log n \rfloor$	$-7+10n-3w(n)-3w(n-1)$ $-3\lfloor \log n \rfloor -3\lfloor \log (n-1) \rfloor$	$8+\lfloor \log n \rfloor +\lfloor \log (n-1) \rfloor$ $+\left\lfloor \log \frac{n}{3} \right\rfloor +\left\lfloor \log \frac{n-1}{3} \right\rfloor$
out-of-place	$1+4n-w(n)-\lfloor \log n \rfloor$	$-1+5n-3w(n)-3\lfloor \log n \rfloor$	$4+\lfloor \log n \rfloor +\left\lfloor \log \frac{n}{3} \right\rfloor$

표 1. Draper 덧셈기의 양자 자원

덧셈기 회로에 사용되는 양자 자원을 나타내며 $w(n)$은 아래 수식 (1)과 같다. 여기서 n은 덧셈을 수행하는 피연산자의 비트 수를 의미한다. 본 논문에서는 T 게이트의 개수 및 깊이에 대한 최적화에 초점을 맞추었으며, Draper 덧셈기에 해당 기법을 적용했을 때 가장 낮은 T 깊이를 가질 수 있으므로 적용 대상 덧셈기로 채택하였다.

$$w(n)=n-\sum_{k=1}^{\infty}\left\lfloor \frac{n}{2^k} \right\rfloor \quad (1)$$

2.2 Toffoli 게이트 분해

양자 회로 구현에 사용되는 양자 게이트 중 Toffoli 게이트는 T 게이트가 포함된 회로를 사용하여 분해할 수 있다. T 게이트는 구현 비용이 높기 때문에 T 게이트를 적게 사용할수록, T 깊이를 줄일수록 효율적인 회로 구현이 가능하다.

2.2.1 Selinger[3]

Selinger는 논문에서 여러 가지 Toffoli 분해 기법을 제안했다. 그림 1은 그 중 T 깊이가 가장 낮은 기법이며, 보조 큐비트 4개를 사용함으로써 T 깊이를 1로 줄이고 전체 깊이 또한 7로 낮게 형성하였다. Toffoli 연산이 끝나면 보조 큐비트는 다시 0으로 초기화되어 다음 연산에 재활용 할 수 있다.

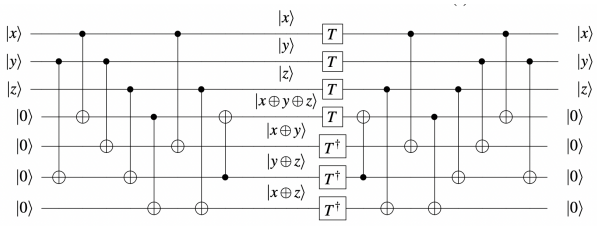

그림 1. Selinger가 제안한 Toffoli 분해 기법

2.2.2 Gidney[4]

Gidney는 논문에서 Toffoli 게이트 연산 및 연산 해제 쌍을 Compute, Uncompute로 대체할 수 있는 logical AND 게이트를 제안하였다. 그림 2는 logical AND 게이트 쌍을 나타내며, 위에가 Compute, 아래가 Uncompute 회로이다. Compute 회로를 보면 4개의 T 게이트를 사용하여 구현된 것을 알 수 있다. 앞의 Selinger의 분해와 같이 logical AND 게이트 이전에는 Toffoli 게이트 분해를 위해서는 7개의 T 게이트가 요구되었지만, 이를 4개로 줄였다. 또한 가장 큰 이점은 Uncompute 회로에서 T 게이트가 사용되지 않는다는 것이다. 일반적으로 회로 연산을 해제하려면 Compute 연산을 역순으로 수행하지만, 측정 연산을 사용함으로써 이 과정을 획기적으로 줄였다. 대신 측정이 수행된 큐비트는 폐기된다. 따라서 하나의 Toffoli 게이트 쌍을 logical AND 쌍으로 대체하게 되면 14개가 아닌 8개의 T 게이트만을 사용하여 구현할 수 있다.

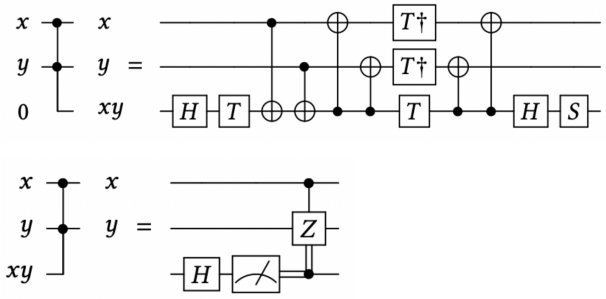

그림 2. Gidney의 logical AND 게이트

III. T 게이트 최적 구현 제안

본 장에서는 Draper 덧셈기의 in-place, out-of-place의 Toffoli 분해에 대해 logical AND 게이트를 적용한 T 게이트 최적 구현 방법에 대해 설명한다. logical AND의 Compute 회로만 보면 T 깊이가 2로, Selinger의 회로보다 1만큼 크지만, 실제로 덧셈기 회로에 적용하면 logical AND의 타겟 큐비트인 세 번째 큐비트에

	#Qubit	#T	T-depth
Selinger (in/out)	$8n-w(n)-\lfloor \log n \rfloor$	$-49+70n-21w(n)-21w(n-1)$ $-21\lfloor \log n \rfloor -21\lfloor \log(n-1) \rfloor$	$8+\lfloor \log n \rfloor +\lfloor \log(n-1) \rfloor$ $+\left\lfloor \log\frac{n}{3} \right\rfloor +\left\lfloor \log\frac{n-1}{3} \right\rfloor$
	$1+8n-w(n)-\lfloor \log n \rfloor$	$-7+35n-21w(n)-21\lfloor \log n \rfloor$	$4+\lfloor \log n \rfloor +\left\lfloor \log\frac{n}{3} \right\rfloor$
logical AND (in/out)	$-5+9n-2w(n)-2w(n-1)$ $-2\lfloor \log n \rfloor -2\lfloor \log(n-1) \rfloor$	$-20+28n-8w(n)-8w(n-1)$ $-8\lfloor \log n \rfloor -8\lfloor \log(n-1) \rfloor$	$4+\lfloor \log n \rfloor +\lfloor \log(n-1) \rfloor$ $+\left\lfloor \log\frac{n}{3} \right\rfloor$
	$6n-2w(n)-2\lfloor \log n \rfloor$	$-4+16n-8w(n)-8\lfloor \log n \rfloor$	$3+\lfloor \log n \rfloor +\left\lfloor \log\frac{n}{3} \right\rfloor$

표 2. Draper 덧셈기에 대한 Selinger와 logical AND 분해 자원 비교

처음으로 수행되는 H 게이트, T 게이트 연산을 초기에 한번에 병렬로 처리할 수 있어 T 깊이를 1로 계산하고 마지막에 1만 더하면 된다. 또한 Draper 덧셈기에서 Propogate 연산을 수행하는 P라운드와 P라운드 연산을 해제하는 P^{-1}라운드, 그리고 in-place의 맨 처음과 마지막의 Toffoli 게이트에 logical AND 쌍을 적용할 수 있다. out-of-place의 경우, 맨 처음의 Toffoli 게이트 대신 Compute 연산을 적용할 수 있다. G와 C 라운드는 이전 단계에서 Toffoli 게이트가 적용된 타겟 큐비트에 동일하게 Toffoli 게이트를 적용하게 되는데, Compute 연산은 타겟 큐비트가 0으로 초기화된 상태의 큐비트여야 한다는 조건이 있다. 따라서 G와 C라운드에서는 새로운 보조 큐비트를 할당하여 그림 3과 같이 하나의 Toffoli 게이트를 logical AND 게이트 쌍으로 분해하여 Compute 연산을 수행한 결과를 CNOT 게이트를 통해 타겟 큐비트에 전달하고 Uncompute한다.

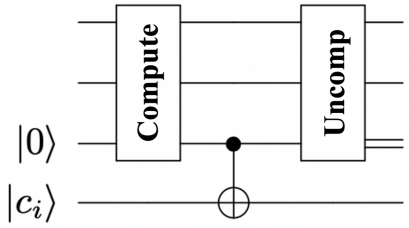

그림 3. G, C라운드에 적용한 기법

IV. 성능 평가

Selinger의 분해와 logical AND를 사용한 분해에 대한 자원 비교 결과는 표 2와 같다. Toffoli 게이트 당 보조 큐비트 4개가 필요한 Selinger는 병렬로 연산을 수행하는 Draper 덧셈기에서 $4n$개의 보조 큐비트가 필요하게 된다. T 게이트의 수는 Toffoli 게이트 수에 7만큼 곱한 값을, T 깊이는 Toffoli 깊이와 동일한 값을 갖게 된다. logical AND 게이트를 적용한 경우, 두 버전 모두에서 T 게이트 수가 줄었는데 특히 in-place에서 좀 더 큰 폭으로 줄었으며, T 깊이도 $4+\left\lfloor \log\frac{n-1}{3} \right\rfloor$ 만큼 줄었다. Selinger에 비해 큐비트를 n 이하로 사용하여 T 게이트 최적화를 달성한 것을 알 수 있다. out-of-place의 경우, P라운드 쌍에 logical AND 게이트 쌍을 적용하여 T 깊이를 줄였으며 보조 큐비트를 사용함으로써 기존 Draper 덧셈기보다 회로를 병렬화하여 최적화할 수 있다. 결론적으로 Selinger보다 1 적은 T 깊이를 갖게 되며, 큐비트를 $2n$개 이상 적게 사용하면서 T 게이트 수도 절반 이상 줄였기 때문에 out-of-place도 T 게이트 최적화를 달성하였다.

V. 결론

본 논문에서는 대수 깊이를 가지는 CLA인 Draper 덧셈기의 연산 구조 및 Gidney의 logical AND 게이트의 적용 조건을 고려하여 T 게이트 수와 깊이 측면에서 최적화한 양자 회로를 제안하였다. 이러한 덧셈기 회로는 기본적인 암호의 덧셈 연산에 사용되어 성능을 개선할 수 있으며, SHA2와 같이 주연산이 덧셈인 해시 알고리즘 구현에 적용될 경우 큰 성능 향상을 기대할 수 있다.

VI.Acknowledgement

This work was 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, 100%).

[참고문헌]

[1] K. Jang, A. Baksi, H. Kim, G. Song, H. Seo, A. Chattopadhyay, "Quantum analysis of aes," Cryptology ePrint Archive. 2022.

[2] Draper, Thomas G., et al. "A logarithmic-depth quantum carry lookahead adder," arXiv preprint quant-ph/0406142, 2004.

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

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