Draper 양자 덧셈기에 대한 T 게이트 최적 구현

임세진*, 장경배*, 김현준*, 서화정*†
* 한성대학교 대학원 IT융합공학과

Ⅰ. 서 론

● 양자 회로를 통한 암호 공격에는 많은 양자 자원이 요구되는데, 이를 최소화하는 최적화된 양자 회로가 필요함

● 회로의 깊이가 낮을수록 실행시간이 단축되므로, 낮은 깊이로 양자 회로를 구현하는 것은 중요한 최적화 요소이며, 구현 비용이 높은 T 게이트 수와 깊이를 줄이는 것이 핵심임 → 본 논문은 암호의 덧셈 연산에 사용되는 Draper 양자 덧셈기에 대해 T 게이트 최적 구현을 제안함

Ⅱ. 관련연구

● 양자 덧셈기는 다항 깊이는 가지는 Ripple Carry 덧셈기와 대수 깊이를 가지는 Carry Lookahead 덧셈기로 나눌 수 있음

● Carry Lookahead 덧셈기는 캐리 연산을 병렬로 수행함으로써 대수 깊이를 갖게 되며, 대표적으로 Draper 덧셈기가 있음

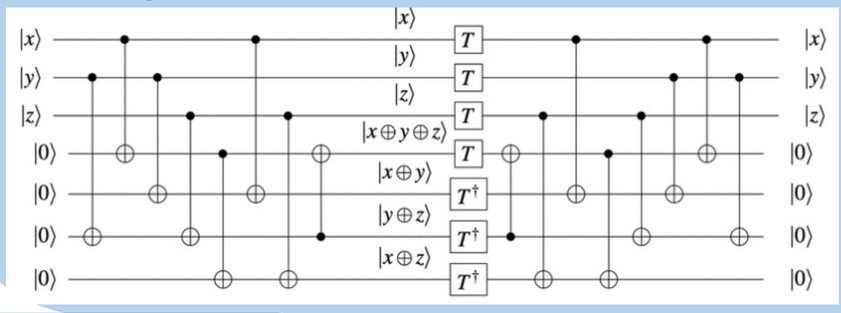
● 표는 Draper 덧셈기의 양자 자원을 나타냄 (덧셈 결과의 저장 위치 : in-place / out-of-place, n : 피연산자의 비트 수)

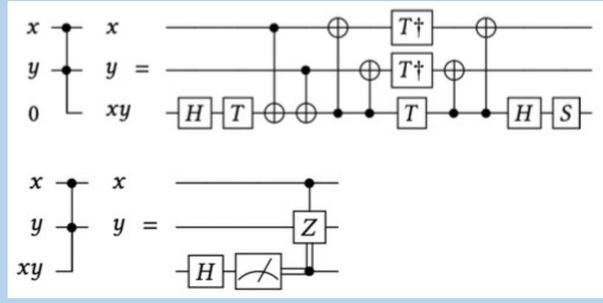
	#Qubit	#Toffoli	Toffoli-depth
in-place	$4n-w(n)-\lfloor \log n \rfloor$	$-7+10n-3w(n)-3w(n-1)$ $-3\lfloor \log n \rfloor -3\lfloor \log (n-1) \rfloor$	$8+\lfloor \log n \rfloor +\lfloor \log (n-1) \rfloor$ $+\left\lfloor \log \frac{n}{3} \right\rfloor +\left\lfloor \log \frac{n-1}{3} \right\rfloor$
out-of-place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

● Toffoli 게이트는 T 게이트가 포함된 회로로 분해 가능하며, T 게이트를 적게 사용하고 T 깊이를 줄일수록 효율적인 회로임

● 회로는 Toffoli 게이트 분해 기법을 나타냄 (왼쪽 : Selinger의 분해, 오른쪽 : Gidney의 logical AND 분해)

● Selinger : 보조 큐비트 4, T 게이트 7, T 깊이 1, logical AND: 보조 큐비트 1 (재활용 X), T 게이트 4, T 깊이 2





✓ logical AND : Compute, Uncompute 쌍으로 구성
✓ Uncompute : T 게이트가 사용 X
- 측정 연산으로 Reverse 연산 대체
✓ 하나의 Toffoli 게이트 쌍 = 하나의 logical AND 쌍
- 14 → 7개의 T 게이트 사용

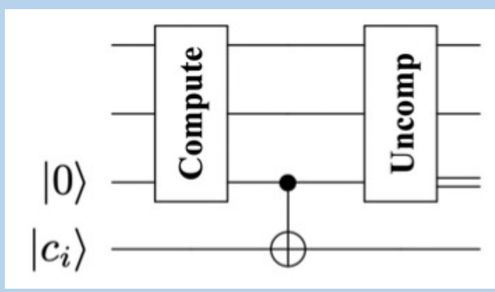
Ⅲ. 구 현 Ⅳ

● logical AND의 Compute 회로는 T 깊이가 2지만, 실제 구현 시 H, T 게이트 연산을 초기에 한번에 병렬처리 할 수 있어 T 깊이를 1로 취급하고 마지막에 1만 더하면 됨

● P라운드와 P^{-1}라운드, in-place의 경우 맨 처음과 마지막의 Toffoli 연산에 logical AND 쌍 적용

● out-of-place의 경우 맨 처음의 Toffoli 게이트 대신 Compute 회로 적용

● 나머지 라운드에서는 보조 큐비트를 할당하여 하나의 Toffoli 게이트를 logical AND 쌍으로 대체



Ⅳ. 성능평가

● logical AND를 적용한 분해가 Selinger보다 적은 큐비트를 사용하면서 T 게이트 수와 T 깊이 측면에서 최적화를 달성함

	#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)	$-5+9n-2w(n)-2w(n-1)$ $-2\lfloor \log n \rfloor -2\lfloor \log (n-1) \rfloor$	$-20+28n-8w(n)-8w(n-1)$ $-8\lfloor \log n \rfloor -8\lfloor \log (n-1) \rfloor$	$4+\lfloor \log n \rfloor +\lfloor \log (n-1) \rfloor$ $+\left\lfloor \log \frac{n}{3} \right\rfloor$
	$6n-2w(n)-2\lfloor \log n \rfloor$	$-4+16n-8w(n)-8\lfloor \log n \rfloor$	$3+\lfloor \log n \rfloor +\left\lfloor \log \frac{n}{3} \right\rfloor$

✓ Draper 덧셈기는 Toffoli 연산을 병렬로 수행
- 사용되는 보조 큐비트 수 x n이 필요
✓ Selinger
- #T : Toffoli 게이트 수 x 7
- T 깊이 : Toffoli 깊이
✓ logical AND
- #T : (Toffoli 게이트 쌍 + 나머지 Toffoli 게이트) x 4
- T 깊이 : Toffoli 깊이 + 1

Ⅴ. 결 론

● 제안하는 T 게이트 최적화 덧셈기 회로는 기본적인 암호의 덧셈 연산에 사용되어 성능을 개선할 수 있으며, SHA2와 같이 주연산이 덧셈인 경우 큰 성능 향상을 기대할 수 있음