HIGH PERFORMANCE QUANTUM MODULAR MULTIPLIERS 논문 리뷰

https://www.youtube.com/watch?v=VfDzXf9fDw4

High Performance Quantum Modular Multipliers

- High Performance Quantum Modular Multipliers
  - 기존의 모듈러 곱셈기는 많은 양의 큐비트와 게이트 소모
  - 기존의 비효율적인 양자 회로 설계와 비교하여 양자 회로에서 모듈러 곱셈을 효율적으로 수행할 수 있는 reversible 모듈러 곱셈기 제안
  - 다양한 고전적인 기법을 활용하여 양자컴퓨팅에 적용
    - 정수 나눗셈 (integer division)
    - 몽고메리 리덕션 (Montgomery reduction)
    - 배럿 리덕션 (Barret reduction)
  - 쇼어 알고리즘과 같은 알고리즘에서 사용되는 모듈러 곱셈의 성능 향상

High Performance Quantum Modular Multipliers

- 양자 모듈러 곱셈 과정의 주요 단계
  - 곱셈 후 나눗셈을 통해 리덕션(reduction)을 하고, 그 결과를 출력 레지스터에 남김

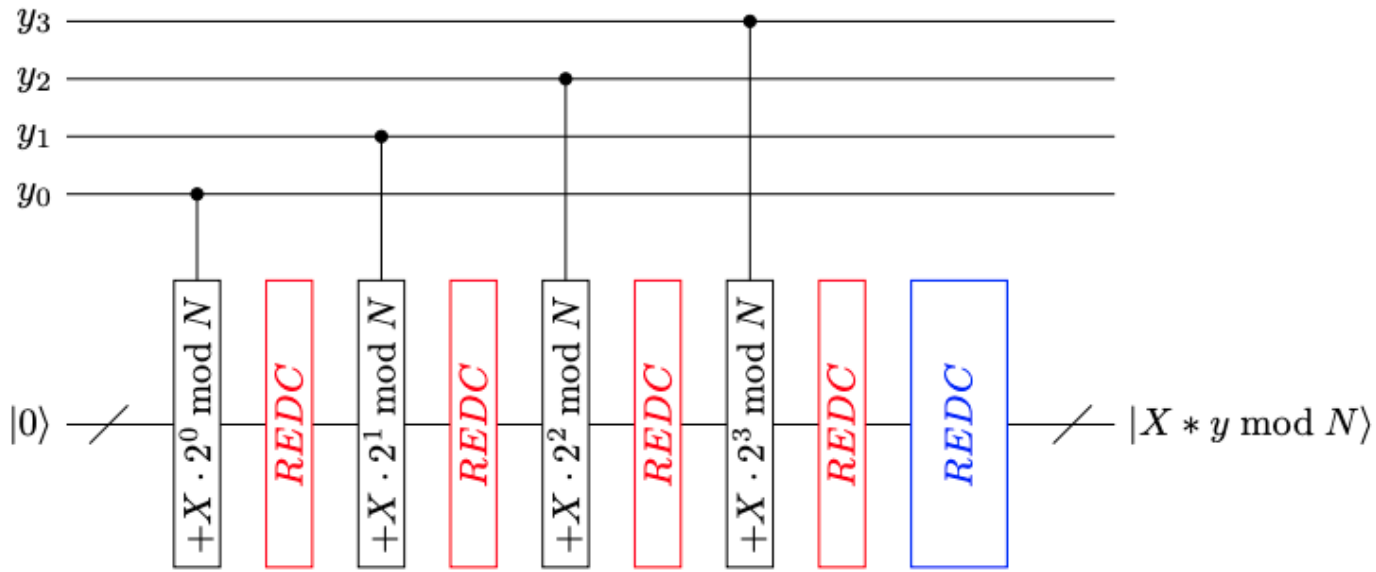
- 이러한 연산은 계산 복잡
  - 곱셈과 나눗셈이 두번씩 필요
  - 결과 계산을 위해 한 번, uncompute 및 안실라 큐비트를 정리하기 위해 한 번
  - 결과 계산 및 uncompute하여 사용한 안실라 큐비트를 clean하게 정리하는 과정에서 발생하는 복잡성

$$
\begin{aligned}
|0\rangle\,|y\rangle\,|0\rangle &\longrightarrow |Xy\rangle\,|y\rangle\,|0\rangle \\
&\longrightarrow |q\rangle\,|Xy-qN\rangle\,|y\rangle\,|0\rangle \\
&\longrightarrow |q\rangle\,|Xy-qN\rangle\,|y\rangle\,|Xy-qN\rangle \\
&\longrightarrow |Xy\rangle\,|y\rangle\,|Xy-qN\rangle \\
&\longrightarrow |0\rangle\,|y\rangle\,|Xy-qN\rangle\,,
\end{aligned}
$$

High Performance Quantum Modular Multipliers

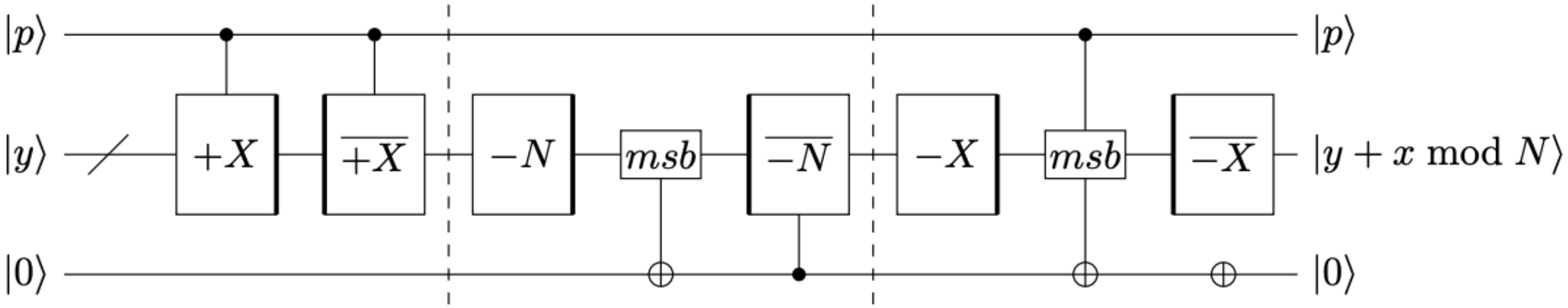
- 양자 모듈러 곱셈
  - 곱셈 후 나눗셈을 하는 곱셈기의 복잡성으로 인해 초기 모듈러 곱셈기는 각 부분 곱의 덧셈 후에 리덕션을 포함하는 방식으로 설계

  - 모듈러 덧셈을 구현하기 위해 여러 개의 정수 덧셈기(integer adder)가 필요
  - 각 단계에서 이러한 덧셈기가 추가되면서, 모듈러 곱셈기의 오버헤드가 이 요인에 따라 선형적으로 증가



High Performance Quantum Modular Multipliers

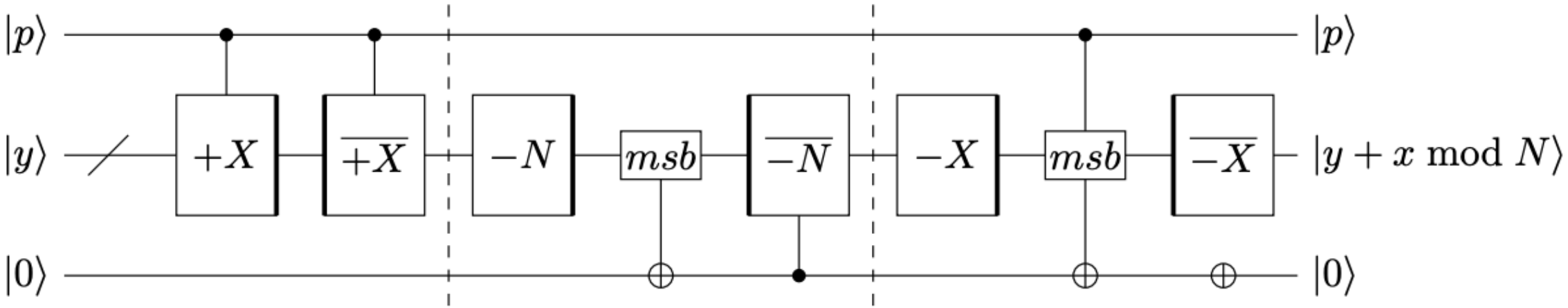
- 모듈러 덧셈 (Modular addition)
  - 3개의 in-place 정수 덧셈기 필요
  - 해당 회로는 Quantum –Classical 덧셈기
  - Quantum – Quantum 이면 X 덧셈을 full quantum integer adder 로 변환



High Performance Quantum Modular Multipliers

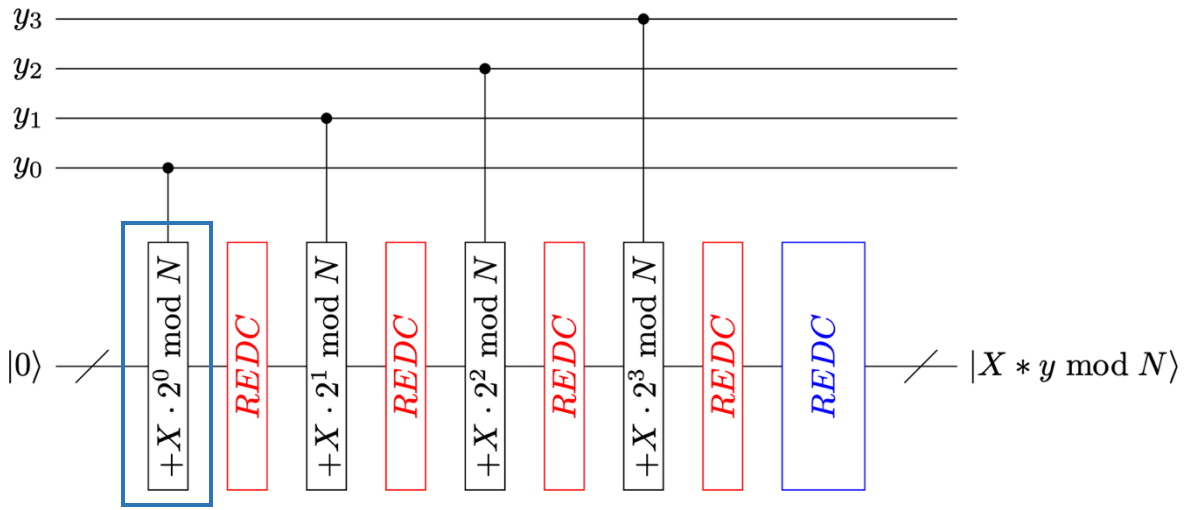
- 모듈러 덧셈 (Modular addition)

1. $(X + y) - N > 0$ 이면 reduction, $(X + y) - N < 0$ 이면 msb →1 , 안실라 큐비트에 저장(제어 큐비트)
2. 안실라 큐비트를 clean 하게 만들기 위해 X 값을 뺌
3. Reuction 수행 → $X + y - N - X = y - N < 0$, reduction을 수행 X → $X + y - X = y > 0$
4. MSB 값 XOR
5. 다시 X 연산 취소, NOT 연산으로 쓰레기 큐비트 되돌림

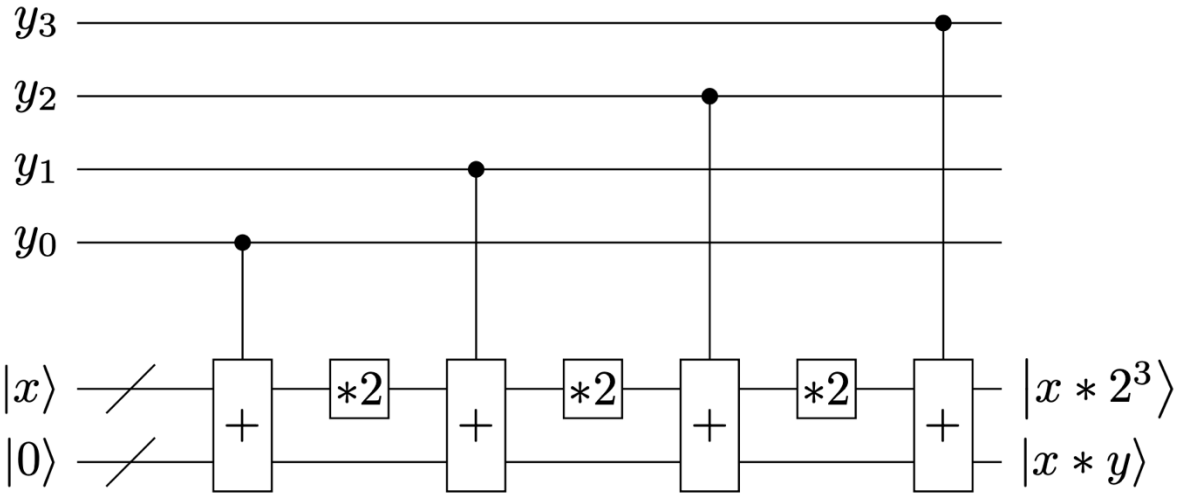


High Performance Quantum Modular Multipliers

- 양자-양자 모듈러 곱셈
  - 양자-클래식 모듈러 곱셈과 마찬가지로 각 부분 곱의 덧셈 후에 리덕션을 포함하는 방식으로 설계
  - 각 축소된 부분 곱은 $y_i(2^i x) mod\ N$ 형태
  - 양자-클래식 곱셈기는 $2^i \cdot X\ mod\ N$을 미리 계산할 수 있지만, 양자-양자 곱셈기에서는 양자 회로를 통해 계산해야함

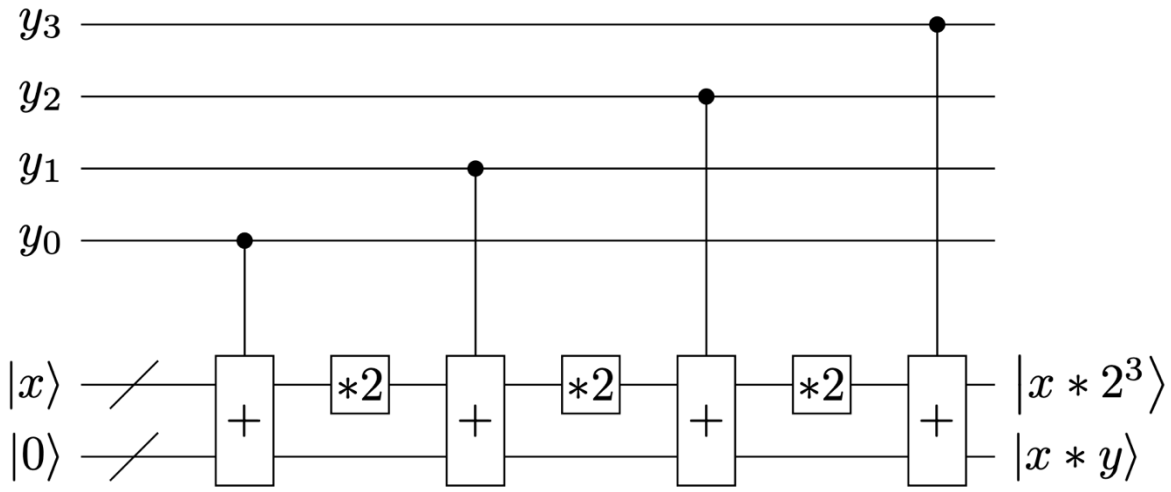


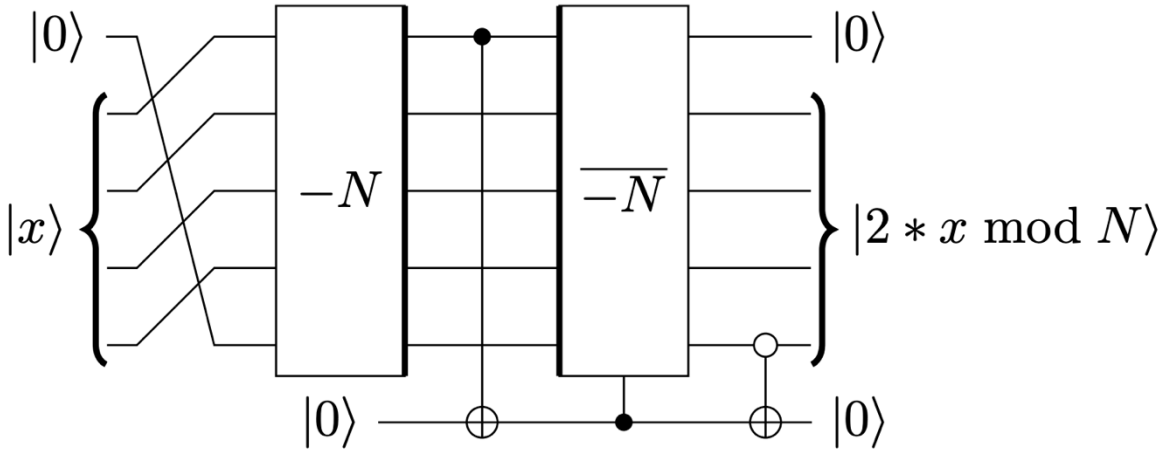
미리 연산 가능



High Performance Quantum Modular Multipliers

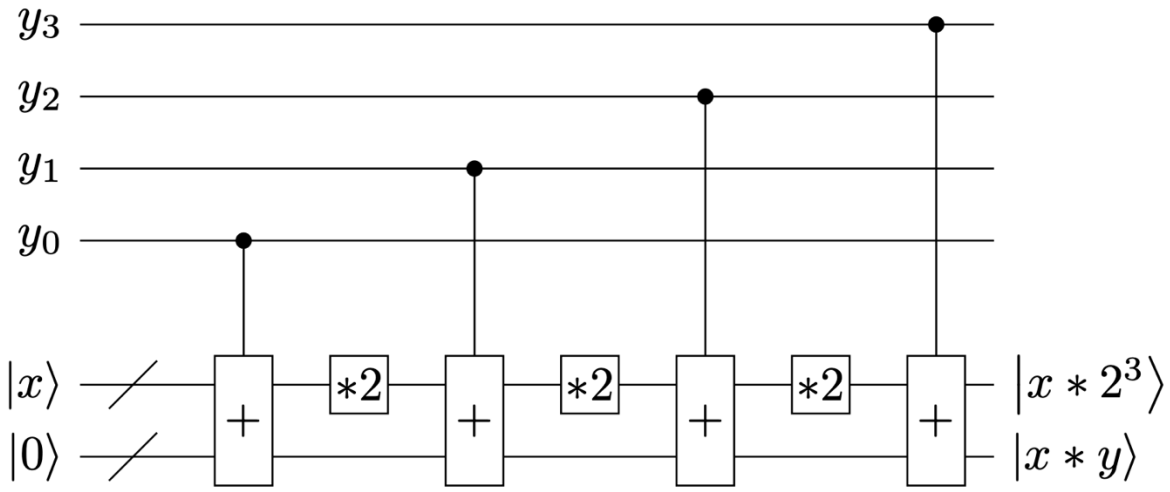
- 양자-양자 모듈러 곱셈
  - 양자-클래식 모듈러 곱셈과 마찬가지로 각 부분 곱의 덧셈 후에 리덕션을 포함하는 방식으로 설계
  - 각 축소된 부분 곱은 $y_i(2^i x) mod\ N$ 형태
  - 양자-클래식 곱셈기는 $2^i \cdot X\ mod\ N$을 미리 계산할 수 있지만, 양자-양자 곱셈기에서는 양자 회로를 통해 계산해야함

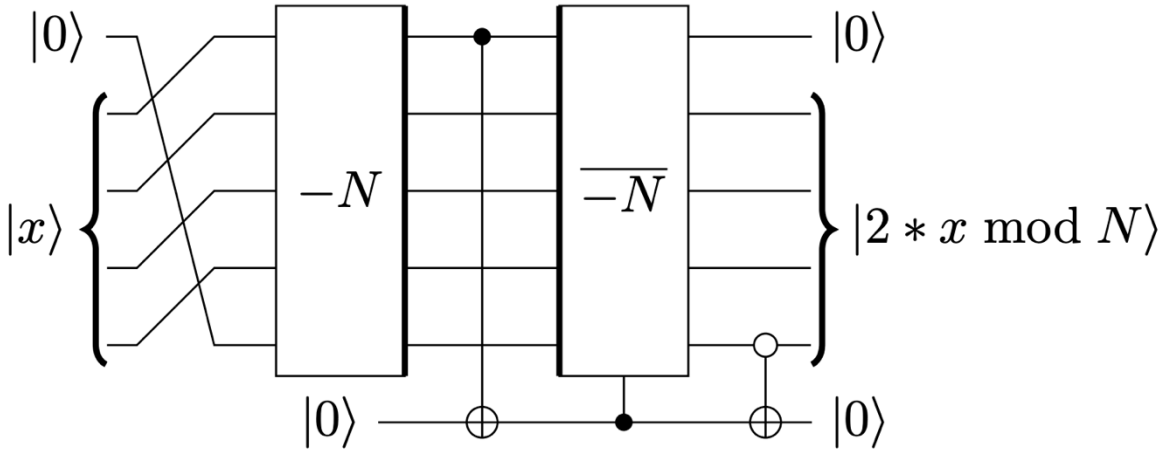




High Performance Quantum Modular Multipliers

- 양자-양자 모듈러 곱셈
  - 비트 시프트 연산으로 $2x$ 연산
  - Reduction 과정
    - N을 빼고 결과가 음수인지 확인
    - 음수라면 뺄셈을 되돌림 즉 $2x$ <N이기 때문에 reduction 필요 x

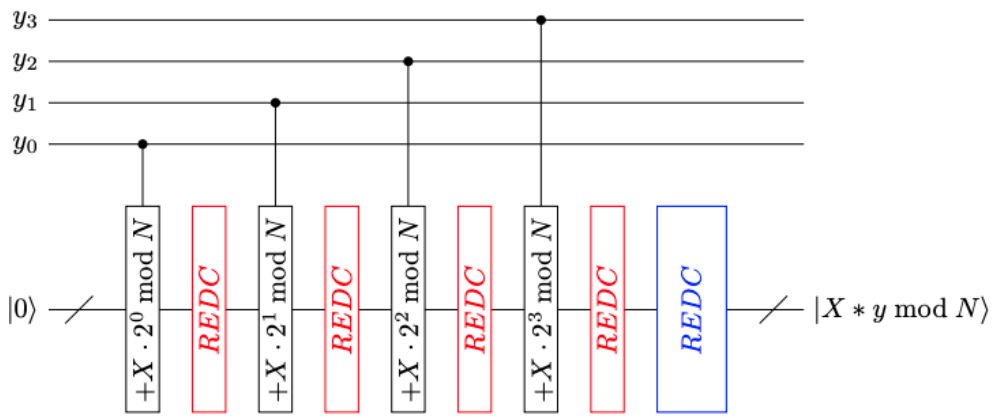


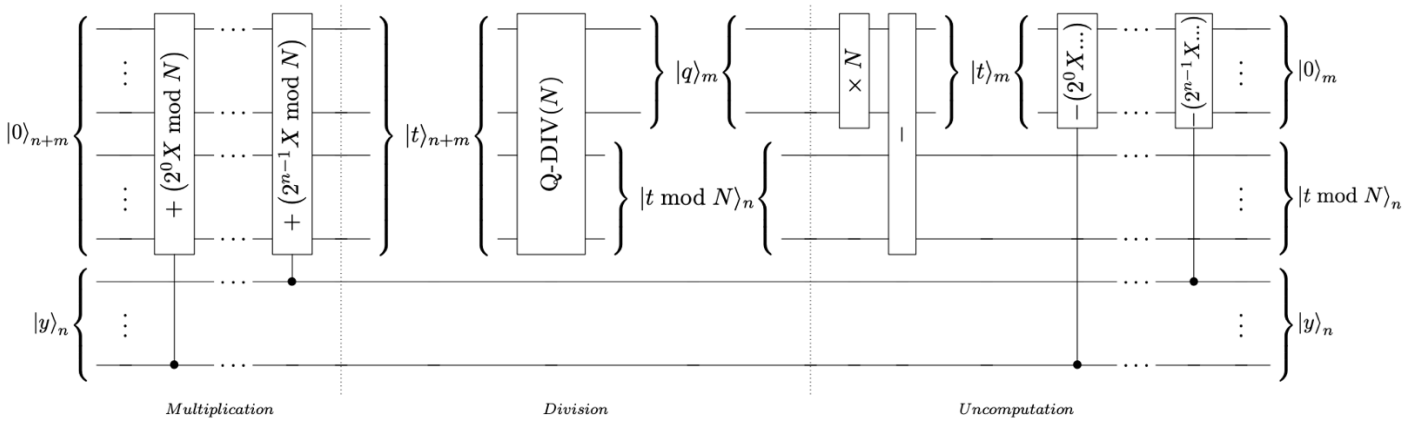


High Performance Quantum Modular Multipliers

- 해당 기초적인 지식을 바탕으로 총 3가지의 기법 구현
  - 정수 나눗셈 (integer division)
  - 몽고메리 리덕션 (Montgomery reduction)
  - 배럿 리덕션 (Barret reduction)

- 각 부분 곱의 덧셈 후 Reduction 이 아닌 정수 곱셈 후 Reduction





Q & A