Improved quantum circuits for elliptic curve discrete logarithms 논문리뷰

https://youtu.be/7HdXoy_1TdI

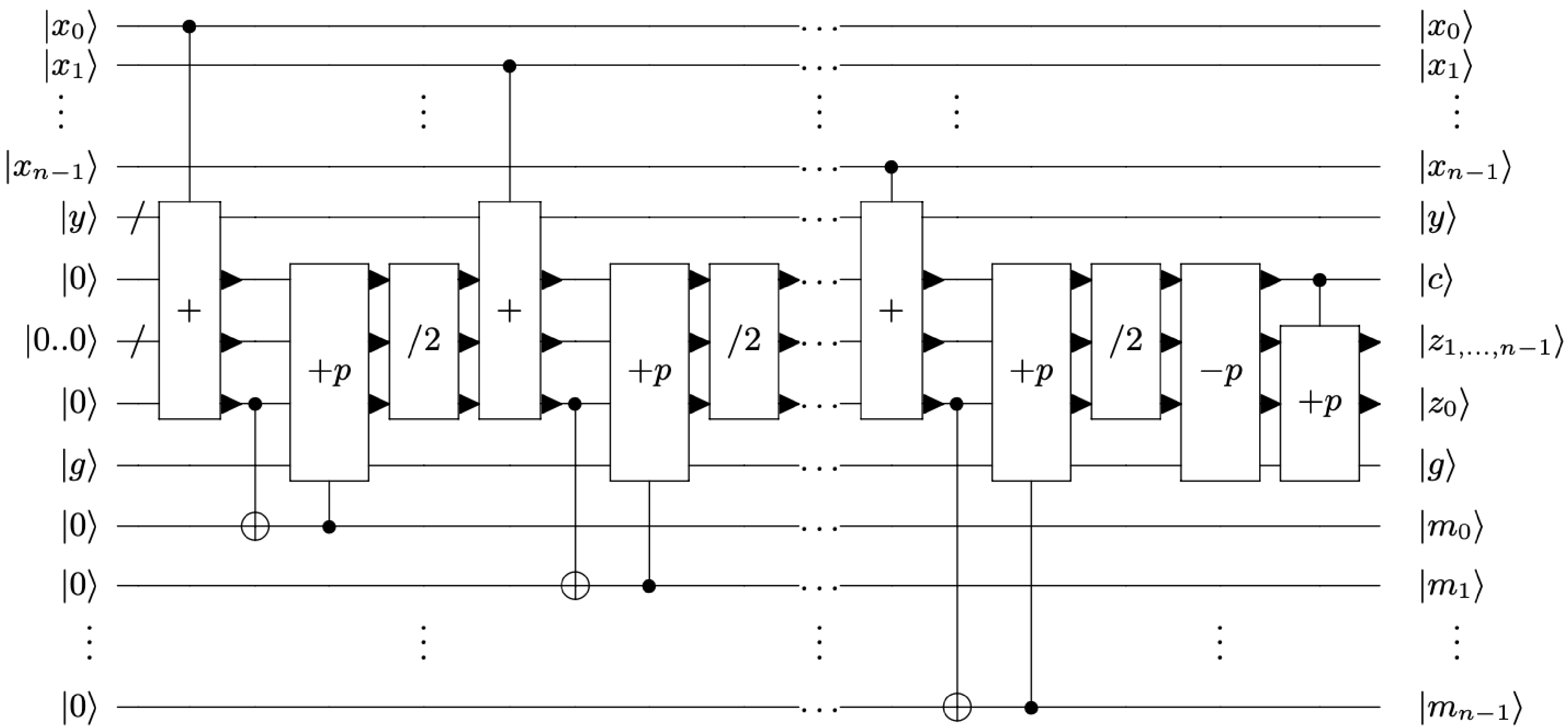
정보컴퓨터공학과 송경주

Improved quantum circuits for elliptic curve discrete logarithms [1]

- [2]의 논문을 개선하여 향상된 width, T-gate, depth 의 NIST Cuvre 양자회로를 제안하였음
- Windowed Montgomery multiplication, improved Kaliski's inversion quantum circuit 등을 적용함

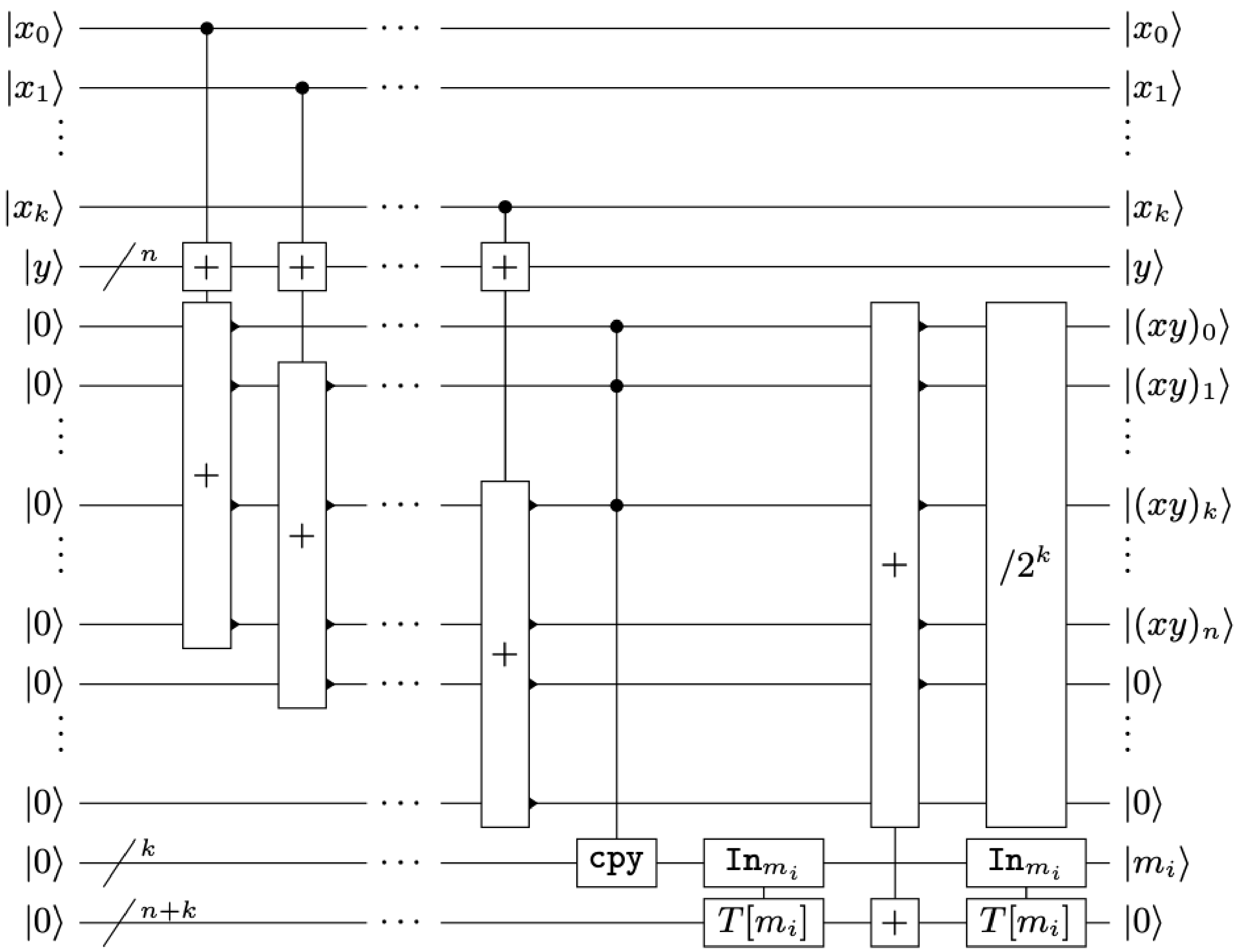
[1] Häner, Thomas, et al. "Improved quantum circuits for elliptic curve discrete logarithms." Post-Quantum Cryptography: 11th International Conference, PQCrypto 2020, Paris, France, April 15–17, 2020, Proceedings 11. Springer International Publishing, 2020.
[2] Martin Roetteler, Michael Naehrig, Krysta M. Svore, and Kristin E. Lauter. Quantum resource estimates for computing elliptic curve discrete logarithms. In ASIACRYPT 2017, volume 10625 of Lecture Notes in Computer Science, pages 241–270. Springer, 2017.

Montgomery modular multiplication

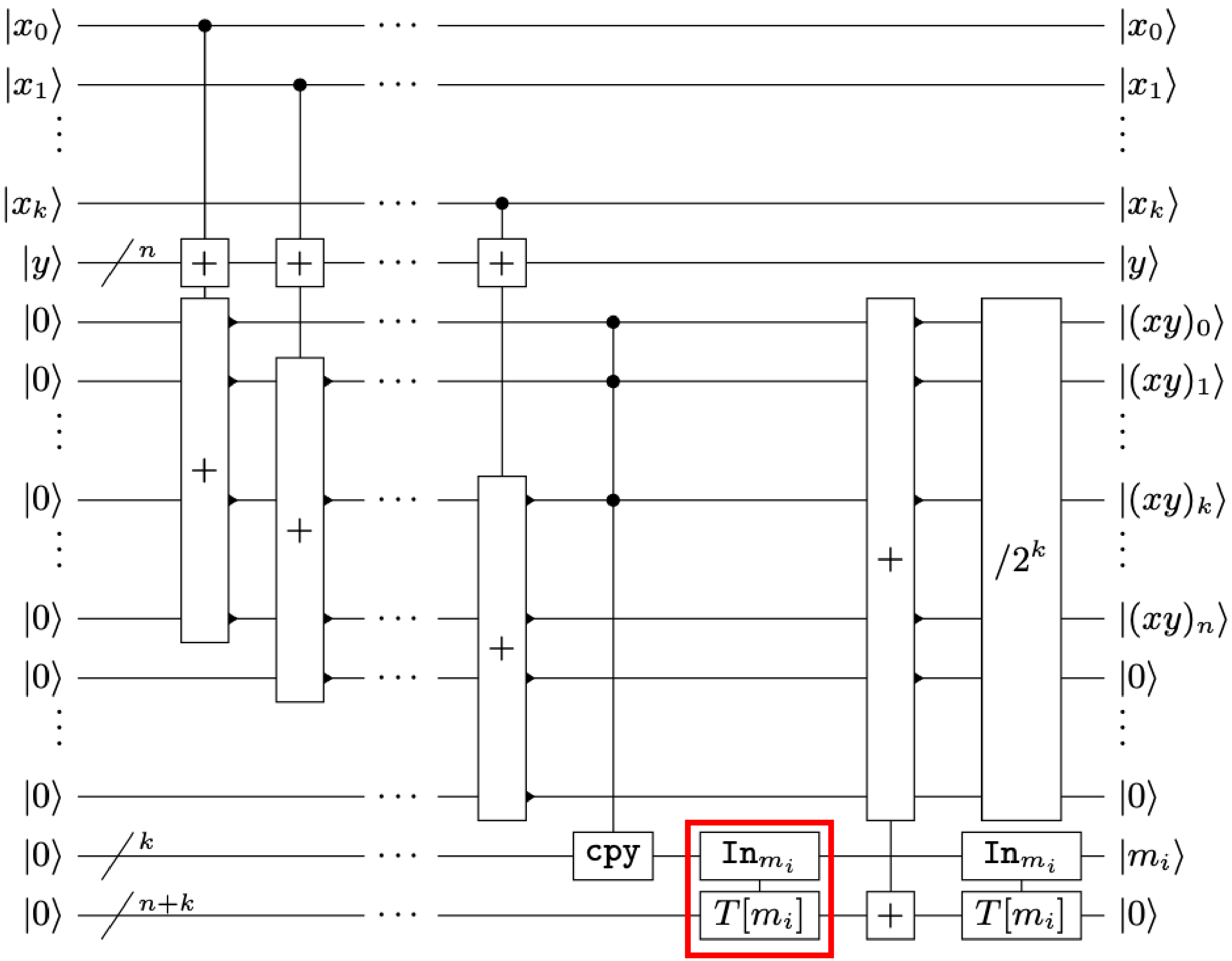


[2] Martin Roetteler, Michael Naehrig, Krysta M. Svore, and Kristin E. Lauter. Quantum resource estimates for computing elliptic curve discrete logarithms. In ASIACRYPT 2017, volume 10625 of Lecture Notes in Computer Science, pages 241–270. Springer, 2017.

Windowed Montgomery multiplication



Windowed Montgomery multiplication



- QROM

- 큐비트의 상태에 따라 해당 index에 있는 Table 값을 큐비트로 가져옴.
- Table 에는 classic 값이 담겨있음.
- $T[m_i] = t_{m_i}p,\ \ t_{m_i} = p^{-1}m_i \bmod 2^k$

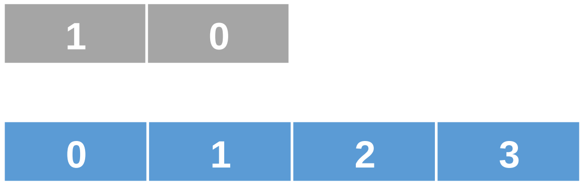
Windowed Montgomery multiplication

- QROM [3]

- 큐비트의 인덱스 값에 따라 해당 인덱스의 classic table 결과를 가져옴

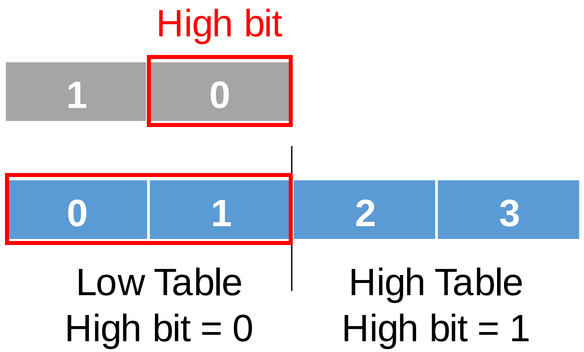
Address qubit = 1 0

Table = [0, 1, 2, 3]



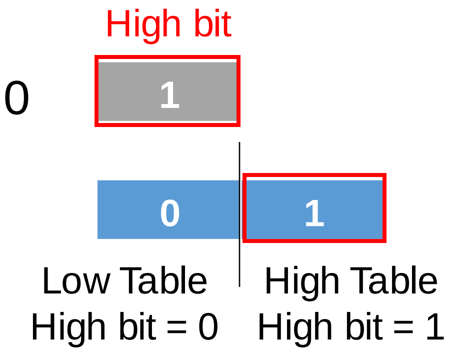
1) Address qubit = 1 0

Table = [0, 1, 2, 3]



2) Address qubit = 1 0

Table = [0, 1, 2, 3]



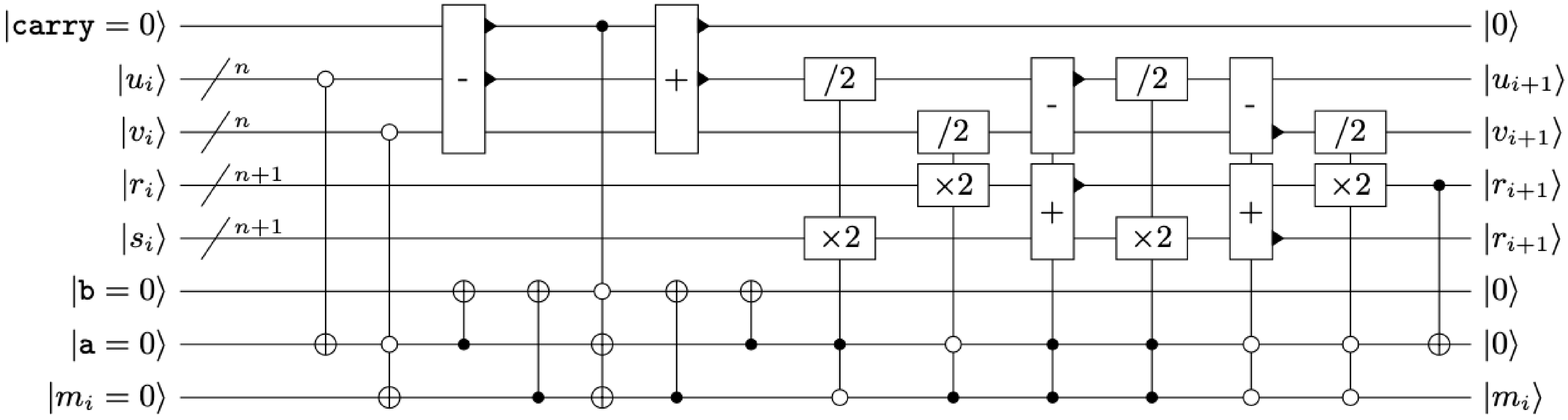
Kaliski’s algorithm

- Binary Extended Euclidean Algorithm기반으로 설계된 Modular 역원 알고리즘
- 최대 2n번 반복
  → 양자회로에서는 기본적으로 2n번 동작되도록 하고 반복동안 맞는 조건에 대해서만 연산 수행 (큐비트의 중간상태를 확인할 수 없어 특정 조건에 따라 반복문을 멈추기 불가)

(a) Kaliski’s algorithm

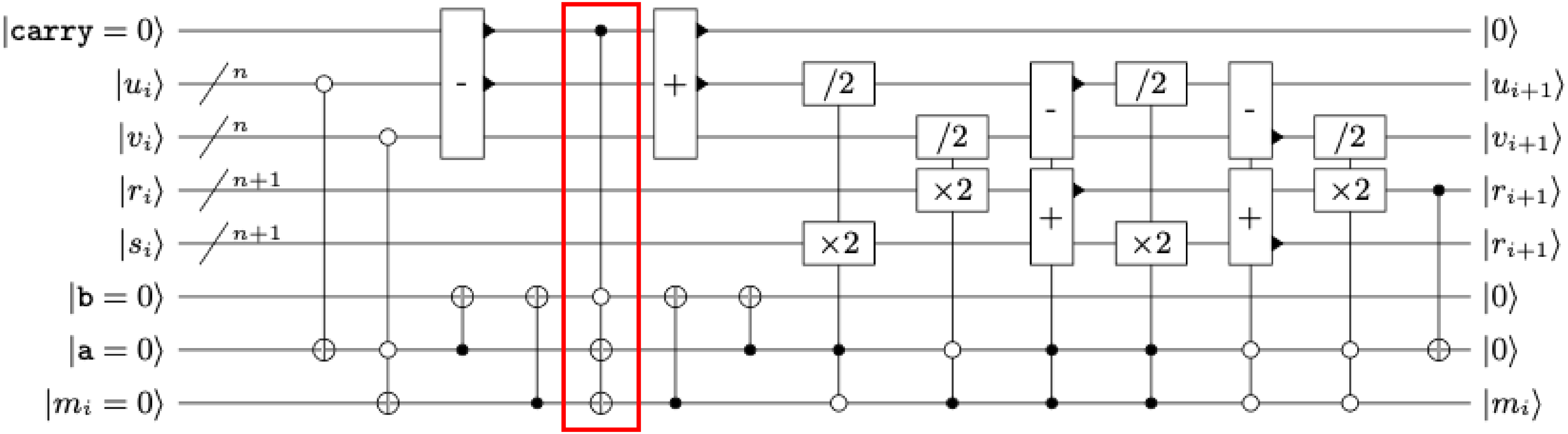
if u odd and v even **then**
  $v \leftarrow v/2$
  $r \leftarrow 2r$
else if u even and v odd **then**
  $u \leftarrow u/2$
  $s \leftarrow 2s$
else if u odd and v odd and $u > v$ **then**
  $u \leftarrow (u-v)/2$
  $r \leftarrow r + s$
  $s \leftarrow 2s$
else if u odd and v odd and $v \geq u$ **then**
  $v \leftarrow (v-u)/2$
  $s \leftarrow r + s$
  $r \leftarrow 2r$
end if

RNSL’s inversion quantum circuit [2]



(a) Round operation from [2] .

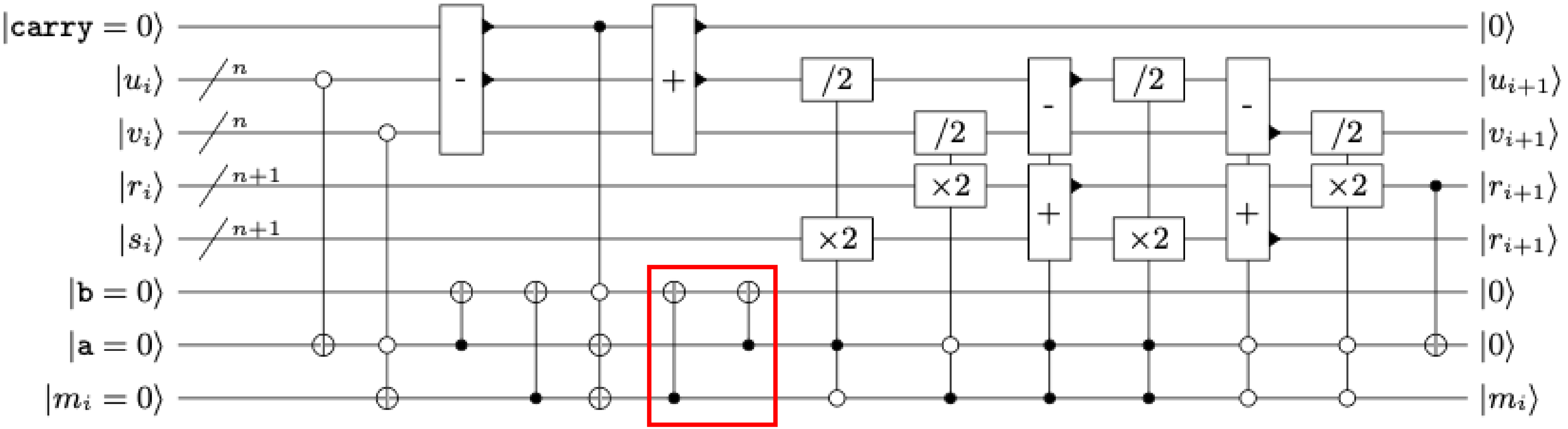
[2] Martin Roetteler, Michael Naehrig, Krysta M. Svore, and Kristin E. Lauter. Quantum resource estimates for computing elliptic curve discrete logarithms. In ASIACRYPT 2017, volume 10625 of Lecture Notes in Computer Science, pages 241–270. Springer, 2017.



(a) Round operation from [27].

u-v 음수일 경우

u	v	a	m	b	u-v 음수 (1)	
					a	m
~~0~~	~~0~~	~~1~~	~~0~~	~~1~~	~~1~~	~~0~~
0	**1**	**1**	**0**	**1**	**1**	**0**
~~1~~	~~0~~	~~0~~	~~1~~	~~1~~	~~0~~	~~1~~
~~1~~	~~1~~	~~0~~	~~0~~	~~0~~	~~1~~	~~1~~

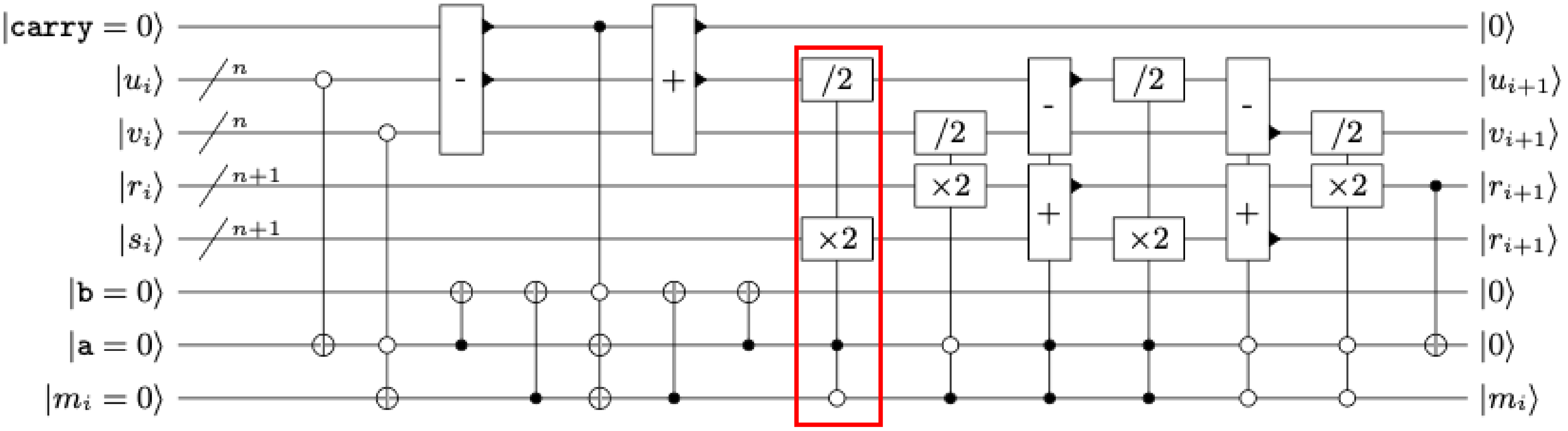


(a) Round operation from [27].

u-v 음수일 경우

u	v	a	m	b	u-v 음수 (1)		b
					a	m	
~~0~~	~~0~~	~~1~~	~~0~~	~~1~~	~~1~~	~~0~~	~~0~~
0	1	1	0	1	1	0	0
~~1~~	~~0~~	~~0~~	~~1~~	~~1~~	~~0~~	~~1~~	~~0~~
~~1~~	~~1~~	~~0~~	~~0~~	~~0~~	~~1~~	~~1~~	~~0~~

b 리셋



(a) Round operation from [27].

u-v 음수일 경우

u	v	a	m	b	u-v 음수 (1)		b	u	s
					a	m			
~~0~~	~~0~~	~~1~~	~~0~~	~~1~~	~~1~~	~~0~~	~~0~~		
0	1	1	0	1	1	0	0	u/2	2s
~~1~~	~~0~~	~~0~~	~~1~~	~~1~~	~~0~~	~~1~~	~~0~~		
~~1~~	~~1~~	~~0~~	~~0~~	~~0~~	~~1~~	~~1~~	~~0~~		

분기 3

Kaliski's inversion algorithm

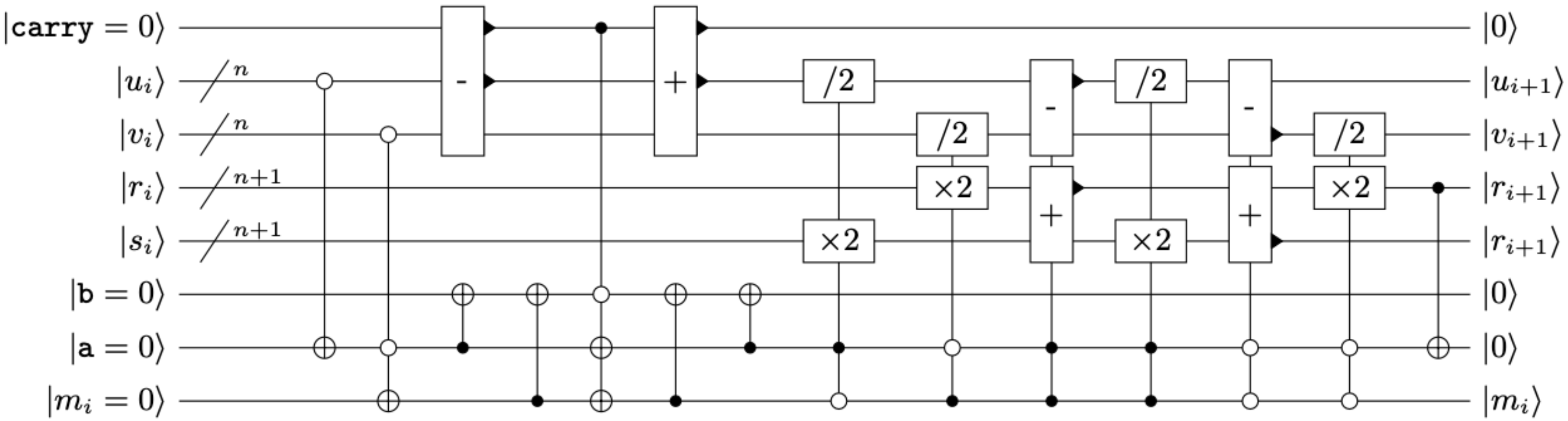
(a) Kaliski's algorithm

if u odd and v even **then**
  $v \leftarrow v/2$
  $r \leftarrow 2r$
else if u even and v odd **then**
  $u \leftarrow u/2$
  $s \leftarrow 2s$
else if u odd and v odd and $u > v$ **then**
  $u \leftarrow (u - v)/2$
  $r \leftarrow r + s$
  $s \leftarrow 2s$
else if u odd and v odd and $v \geq u$ **then**
  $v \leftarrow (v - u)/2$
  $s \leftarrow r + s$
  $r \leftarrow 2r$
end if

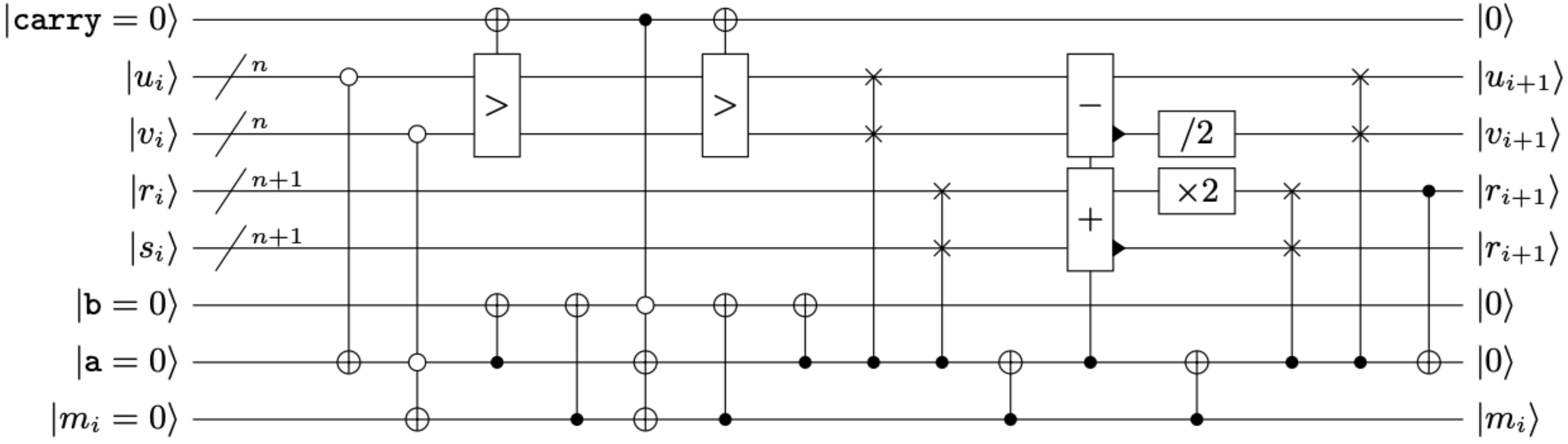
(b) Equivalent formulation

$b_{swap} \leftarrow$ `false`
if u even and v odd, or u and v both odd and $u > v$ **then**
  swap u and v
  swap r and s
  $b_{swap} \leftarrow$ `true`
end if
if u odd and v odd **then**
  $v \leftarrow v - u$
  $s \leftarrow r + s$
end if
$v \leftarrow v/2$
$r \leftarrow 2r$
if b_{swap} **then**
  swap u and v
  swap r and s
end if

Quantum inversion algorithm

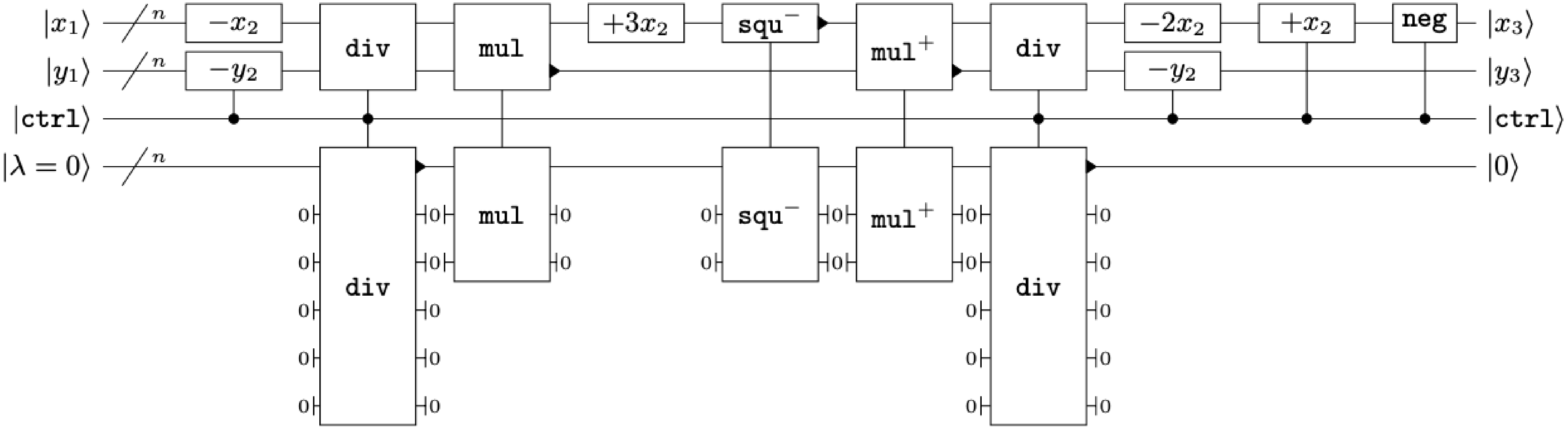


RNSL's inversion quantum circuit



Thomas's inversion quantum circuit

Thomas's Curve quantum circuit



Q & A