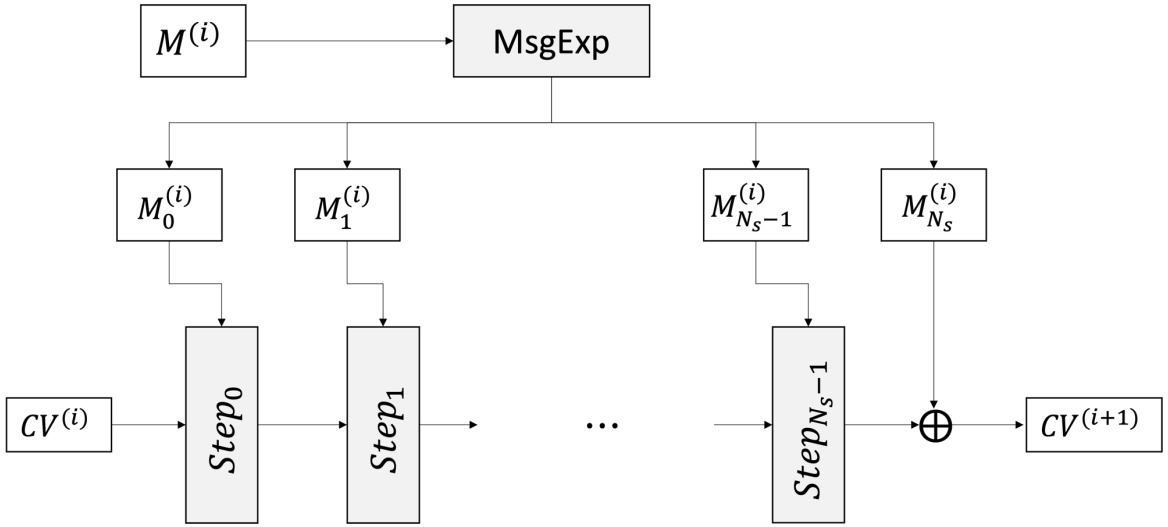
Parallel quantum circuit for LSH

https://youtu.be/WNU5sMFjRsI

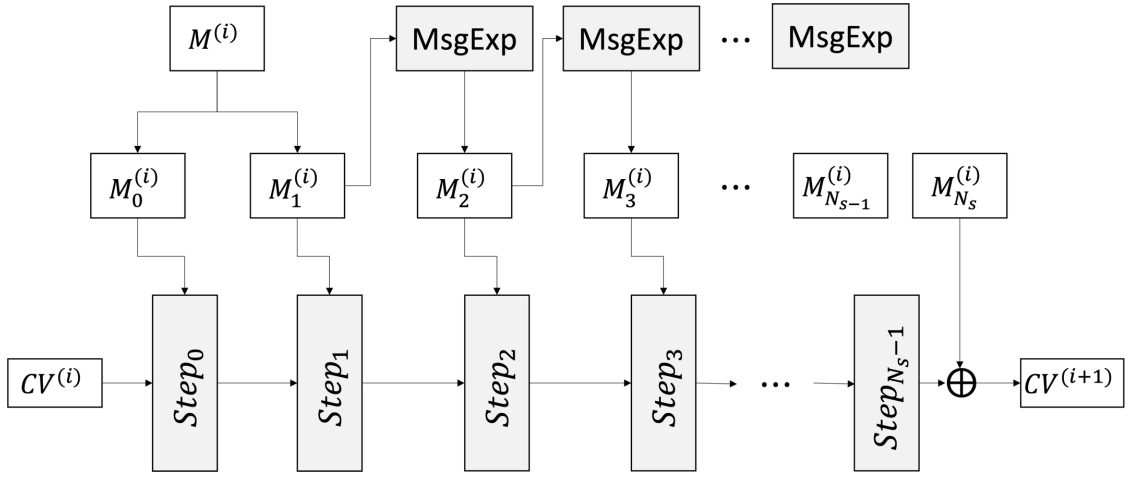
IT융합공학부 송경주

연구 동기

- 2014년 한국에서 설계한 한국 표준 해시함수 LSH에 대한 병렬구조의 양자회로 제안
- 적절한 양자 자원의 trade-off 를 통해 LSH의 양자 회로 Depth를 줄이기 위해 고안함
- 병렬 구조가 가능한 부분을 찾아 메시지 확장 및 Mix 함수에 대해 병렬구조의 양자회로를 구현함
- 이전의 연구보다 양자회로 Depth가 약 96% 감소한 결과를 얻음



<LSH 동작 구조>



<LSH 양자회로 구조>

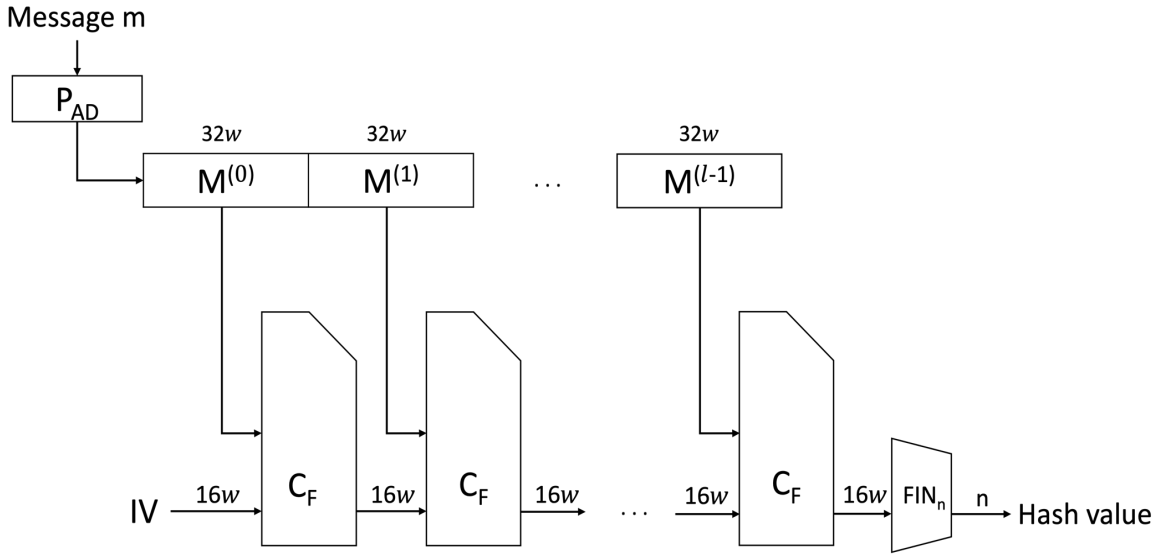
LSH hash function

- LSH 해시함수

: 한국에서 설계하였으며 한국 암호화 모듈 검증 프로그램(KCMVP)에서 승인된 한국 국가 표준(KSM X 3262) 해시함수

- LSH 해시함수 동작 단계

1. 초기화 (Initialization)
   - 입력된 메시지를 word의 배수로 패딩
   - 패딩 된 값을 word 크기의 메시지 블록으로 나눔
   - 초기화 벡터(IV)를 사용하여 연결변수(CV) 초기화
2. 압축 (Compression)
   - 압축함수를 진행하며 연결변수(CV) 업데이트
3. 마무리 (Finalization)
   - 최종 연결변수(CV)에서 해시 값 출력



Parallel LSH quantum circuit (제안 기법)

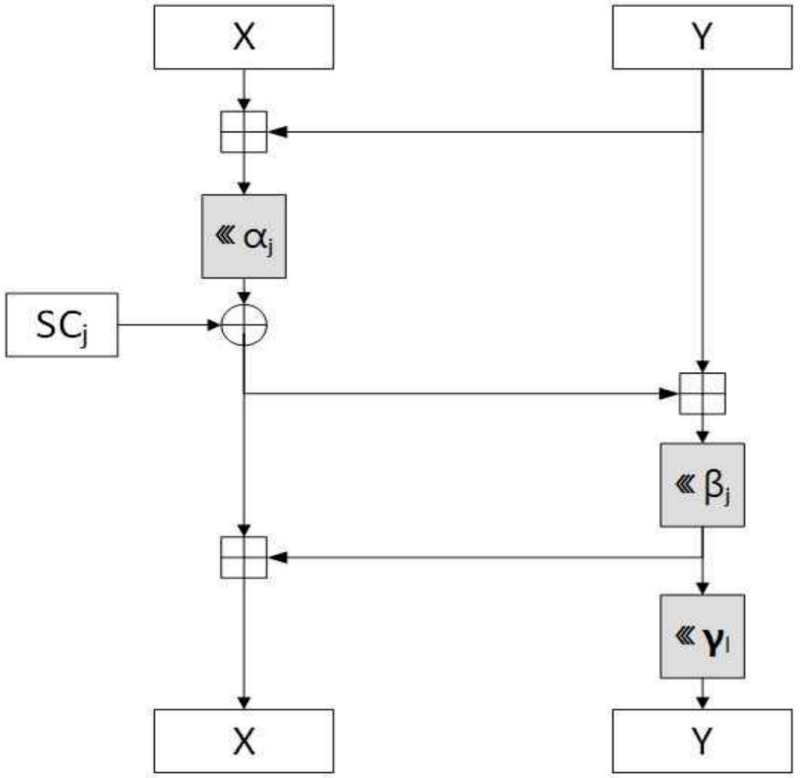
- LSH 해시함수에서 독립적으로 연산가능한 부분 → 병렬구조 설계
- LSH 해시함수 동작 과정 주 메시지 확장(MsgExp), 믹스(Mix) 함수에서 각 메시지는 블록 단위로 독립적으로 연산 → 서로의 결과에 영향을 주지 않는 특징을 가짐

$$M_0^{(i)} \leftarrow (M^{(i)}[0], M^{(i)}[1], \cdots, M^{(i)}[15]),$$

$$M_1^{(i)} \leftarrow (M^{(i)}[16], M^{(i)}[17], \cdots, M^{(i)}[31])$$

$$M_j^{(i)}[I] \leftarrow M_{j-1}^{(i)}[I] \boxplus M_{j-2}^{(i)}[\tau(I)]$$
$$(0 \le I \le 15,\ 2 \le j \le N_s)$$

<MsgExp function>

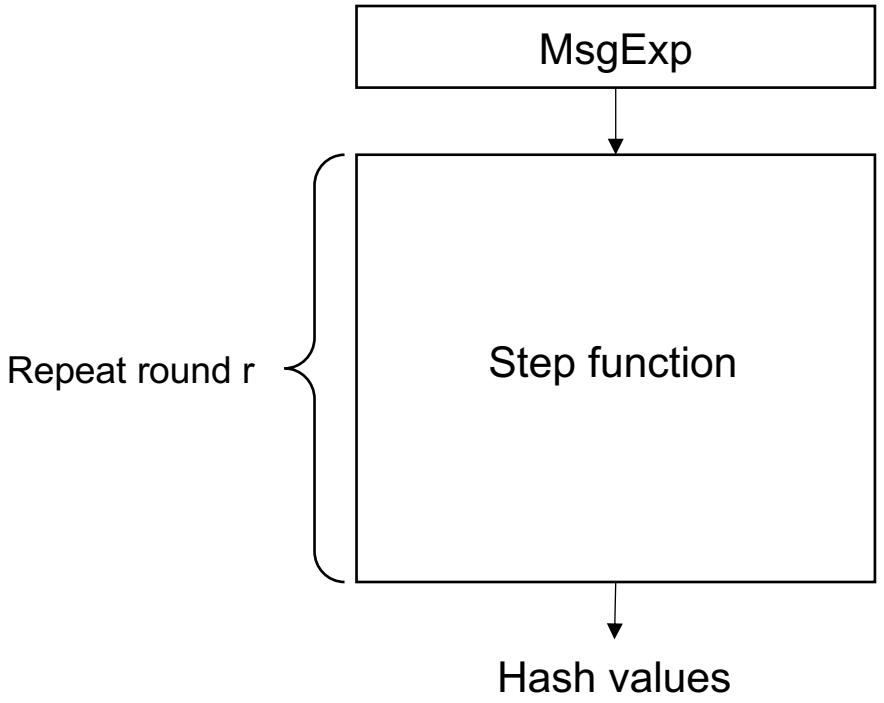


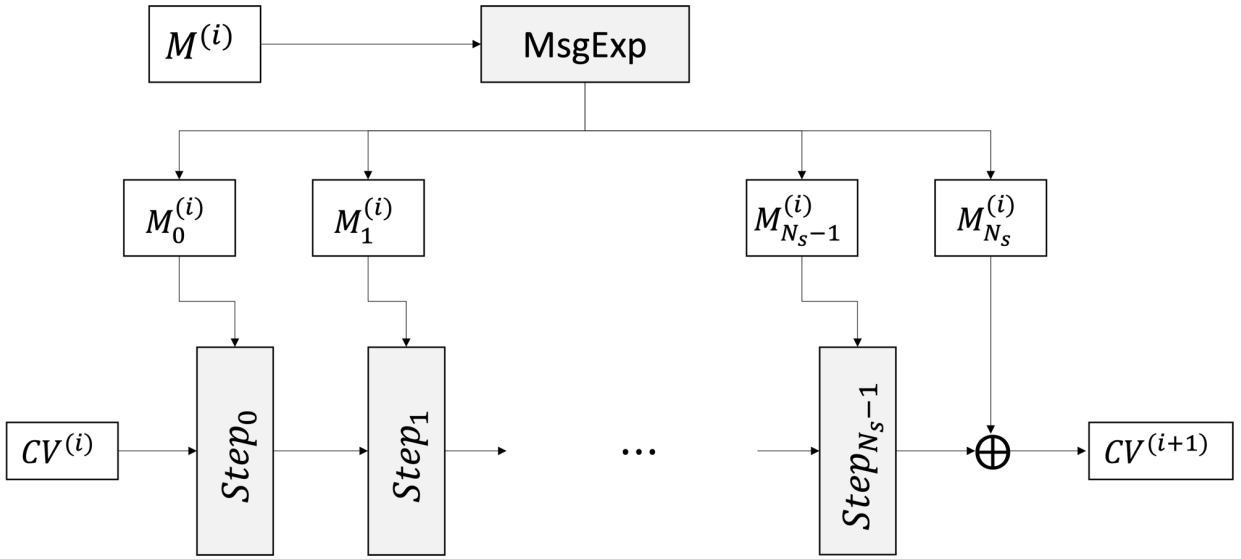
<Mix function>

Parallel LSH quantum circuit (제안 기법)

- 메시지 확장(MsgExp)

- **기본 구조** : 전체 메시지(16개의 메시지 블록)를 확장 한 후 step function을 진행할 때, 확장된 전체 메시지를 저장하기 위한 큐비트 필요

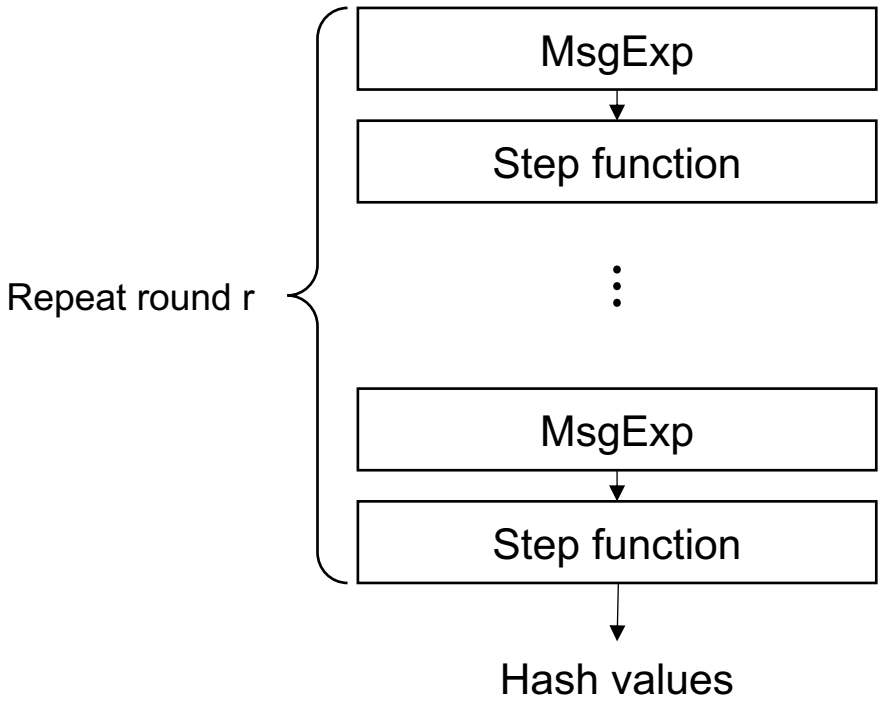


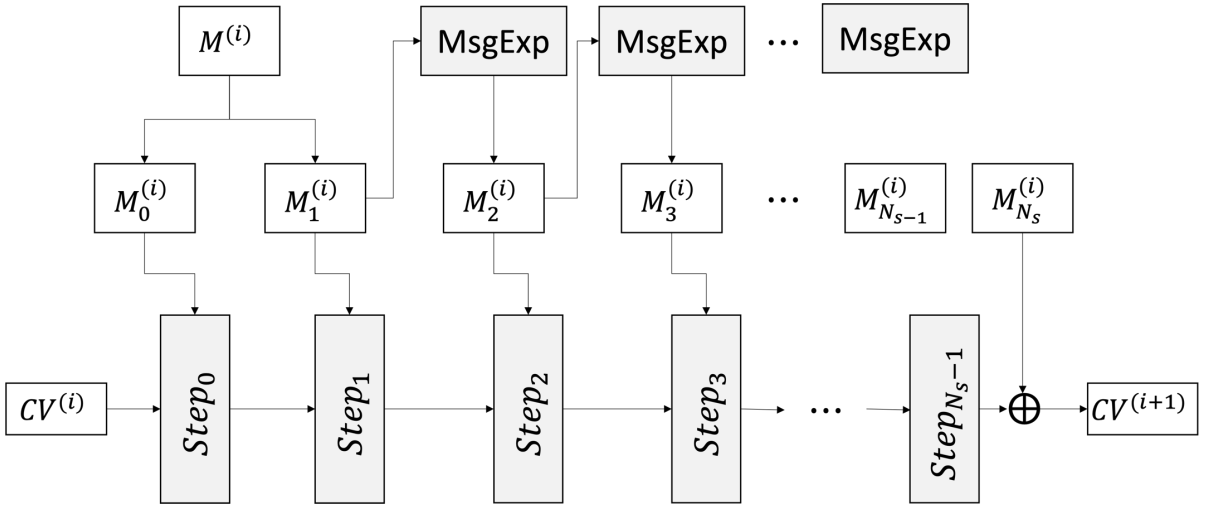


Parallel LSH quantum circuit (제안 기법)

- 메시지 확장(MsgExp)

- **양자회로 구조**: MsgExp와 Step function을 반복하여 Step function 에서 사용한 메시지 블록 큐비트를 다음 MsgExp에서 재사용함 (MsgExp와 Step function 반복)





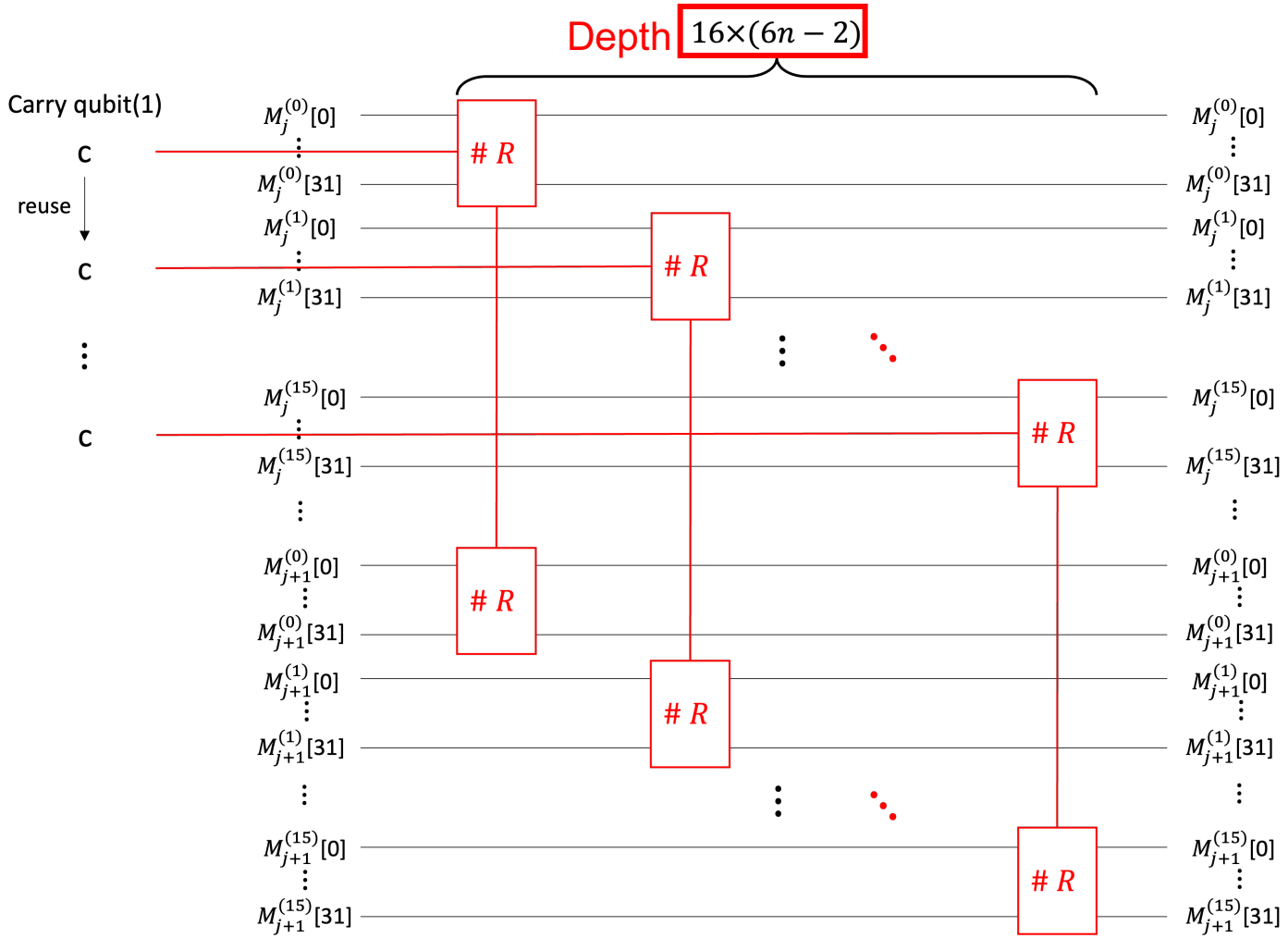
Parallel LSH quantum circuit (제안 기법)

- Sequential LSH quantum circuit

$$M_0^{(i)} \leftarrow M^{(i)}[0], \cdots, M^{(i)}[15]$$
$$M_1^{(i)} \leftarrow M^{(i)}[16], \cdots, M^{(i)}[31]$$
$$M_j^{(i)}[l] \leftarrow M_{j-1}^{(i)}[l] \boxplus M_{j-2}^{(i)}[\tau(l)]$$

Sequential quantum circuit

- 메시지 블록 쌍 M_j, M_{j-1} 이 순차적으로 연산 됨
- 덧셈에 사용된 1개의 carry qubit은 리셋 되어 다음 블록 쌍 덧셈에서 재사용됨
- 결과적으로 메시지 블록 쌍 M_j, M_{j-1} 에 대해 32(64)-bit 씩 16개의 덧셈이 순서대로 진행됨



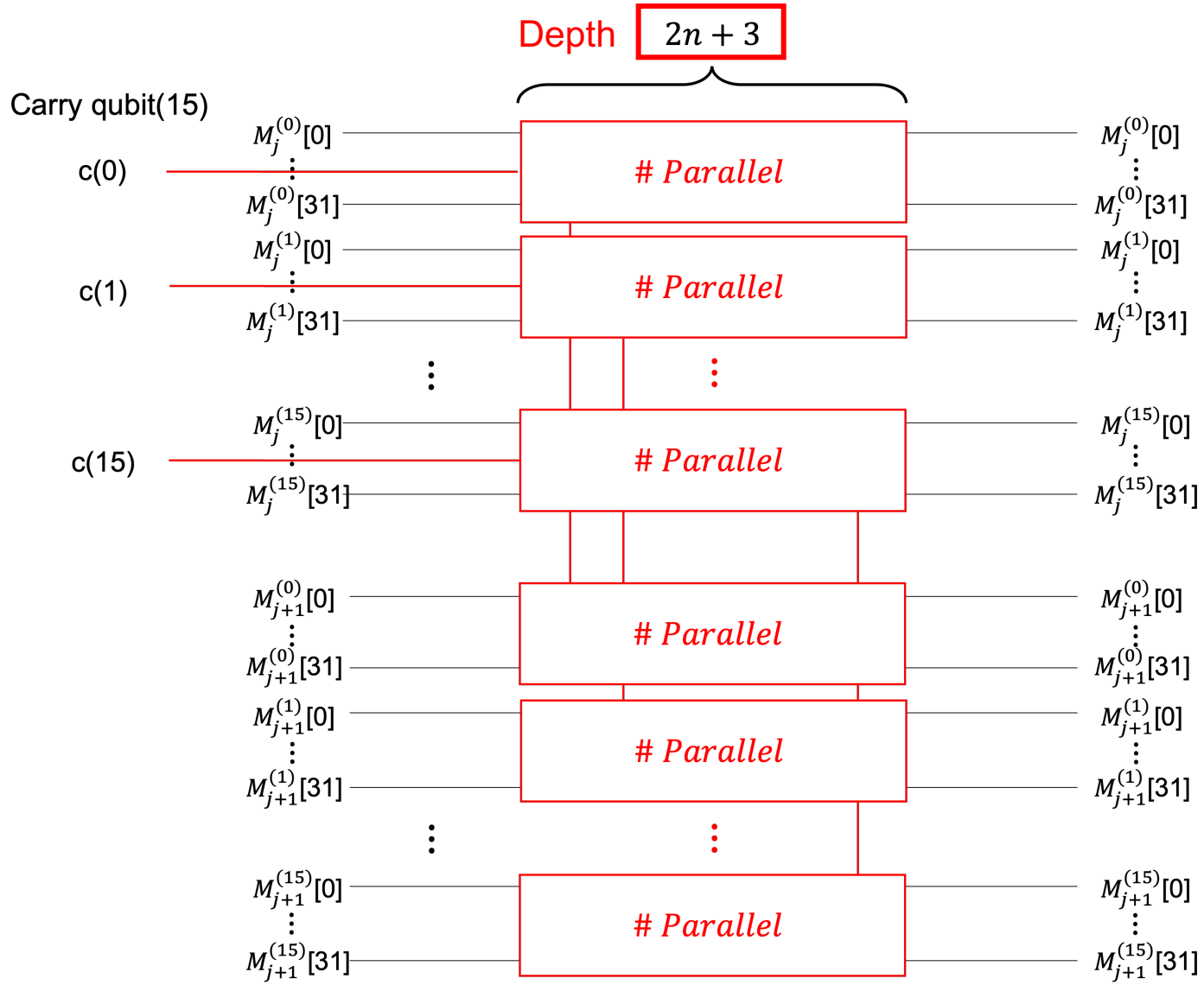
Parallel LSH quantum circuit (제안 기법)

- Parallel LSH quantum circuit

$$M_0^{(i)} \leftarrow M^{(i)}[0], \cdots, M^{(i)}[15]$$
$$M_1^{(i)} \leftarrow M^{(i)}[16], \cdots, M^{(i)}[31]$$
$$M_j^{(i)}[l] \leftarrow M_{j-1}^{(i)}[l] \boxplus M_{j-2}^{(i)}[\tau(l)]$$

Parallel quantum circuit

- 메시지 블록 쌍 M_j, M_{j-1} 이 병렬로 연산됨
- 덧셈에 사용된 15개의 carry qubit은 리셋 되어 다음 라운드에서 재사용
- 결과적으로 메시지 블록 쌍 M_j, M_{j-1} 에 대해 32(64)-bit 씩 16개의 덧셈이 동시에 진행됨



Parallel LSH quantum circuit (제안 기법)

- Mix function (in step function)

- 입력된 16word 배열 $T = T[0], \cdots T[15]$ 에 대해 $T[i],\ T[i+8]\ (0 \le i \le 7)$ 쌍으로 Mix function 진행

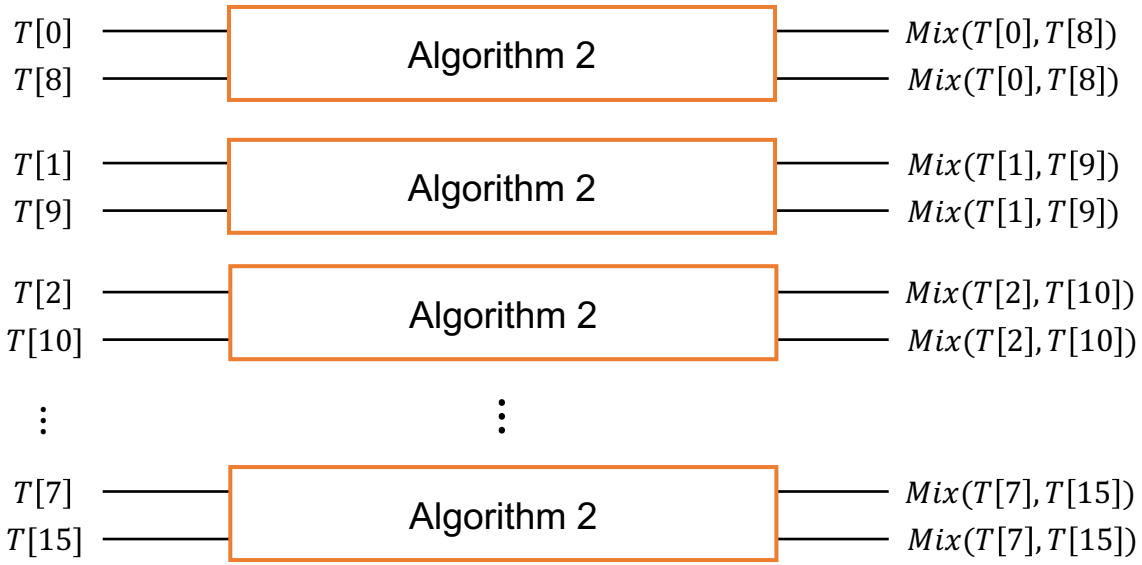
$$T[i], T[i+8] \rightarrow\ Mix_{j,i}(T[i], T[i+8]) \quad (0 \le i \le 7)$$

- Parallel mix function에서 8개의 $T[i], T[i+8]$ 쌍이 모두 병렬로 한번에 연산 됨

Algorithm 2 : Parallel quantum circuit for Mix function

Input: $T[i],\ T[i+8]\ (0 \le i \le 7)$

$T[i+8] \leftarrow$ Parallel_adder($T[i],\ T[i+8]$)
a_rotation($T[i]$)
Applying X gate to $T[i]$ according to $SC[i]$
b_rotation($T[i+8]$)
$T[i] \leftarrow$ Parallel_adder($T[i+8],\ T[i]$)
c_rotation($T[i+8]$)



Evaluation (평가)

- 개발 환경 : IBM 에서 제공하는 양자 프로그래밍 툴 ProjectQ
- 양자 자원 추정: ProjectQ 에서 제공하는 ResourceSimulation 사용

- 양자 자원 trade-off 결과
  - 이전 연구 <Table 1>과 제안하는 병렬 양자회로 <Table 2>의 양자자원을 비교
  - 제안 회로의 CNOT, X gates 수가 증가하였지만 더 비싼 자원인 Toffoli gates 수 감소

	Quantum gates				Depth
	Qubit	Toffoli	CNOT	X	
LSH 256-224	1,537	63,488	145,152	1,536	210,051
LSH 256-256	1,537	63,488	145,152	3,492	210,049
LSH 512-224	3,073	139,104	312,832	7,663	421,851
LSH 512-256	3,073	139,104	312,832	7,696	421,851
LSH 512-384	3,073	139,104	312,832	7,668	421,850
LSH 512-512	3,073	139,104	312,832	7,680	421,852

<Table 1. Sequential LSH quantum circuit>

	Quantum gates				Depth
	Qubit	Toffoli	CNOT	X	
LSH 256-224	1,552	62,464	170,752	59,392	6,879
LSH 256-256	1,552	62,464	170,752	59,392	6,879
LSH 512-224	3,088	138,000	375,760	134,688	14,517
LSH 512-256	3,088	138,000	375,760	134,688	14,517
LSH 512-384	3,088	138,000	375,760	134,688	14,517
LSH 512-512	3,088	138,000	375,760	134,688	14,517

<Table 2. Parallel LSH quantum circuit>

Evaluation (평가)

- 개발 환경 : IBM 에서 제공하는 양자 프로그래밍 툴 ProjectQ
- 양자 자원 추정: ProjectQ 에서 제공하는 ResourceSimulation 사용

- 양자 자원 trade-off 결과
  - 적절한 quantum gates의 trade-off 결과 Depth가 크게 줄어듦
  - 제안하는 Parallel LSH는 이전 연구의 Sequential LSH보다 Depth가 약 96% 감소함

	Quantum gates				Depth
	Qubit	Toffoli	CNOT	X	
LSH 256-224	1,537	63,488	145,152	1,536	210,051
LSH 256-256	1,537	63,488	145,152	3,492	210,049
LSH 512-224	3,073	139,104	312,832	7,663	421,851
LSH 512-256	3,073	139,104	312,832	7,696	421,851
LSH 512-384	3,073	139,104	312,832	7,668	421,850
LSH 512-512	3,073	139,104	312,832	7,680	421,852

<Table 1. Sequential LSH quantum circuit>

	Quantum gates				Depth
	Qubit	Toffoli	CNOT	X	
LSH 256-224	1,552	62,464	170,752	59,392	6,879
LSH 256-256	1,552	62,464	170,752	59,392	6,879
LSH 512-224	3,088	138,000	375,760	134,688	14,517
LSH 512-256	3,088	138,000	375,760	134,688	14,517
LSH 512-384	3,088	138,000	375,760	134,688	14,517
LSH 512-512	3,088	138,000	375,760	134,688	14,517

<Table 2. Parallel LSH quantum circuit>

Q & A