

SHA-3 양자 회로 개선

<https://youtu.be/fBiqCzIV7aY>

장경배

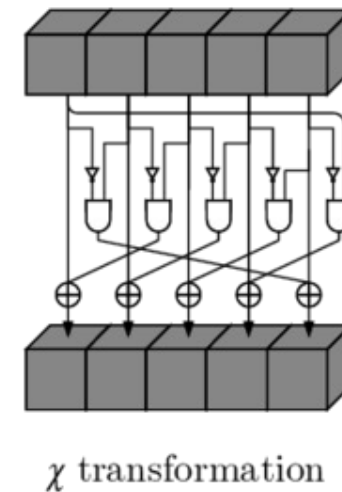
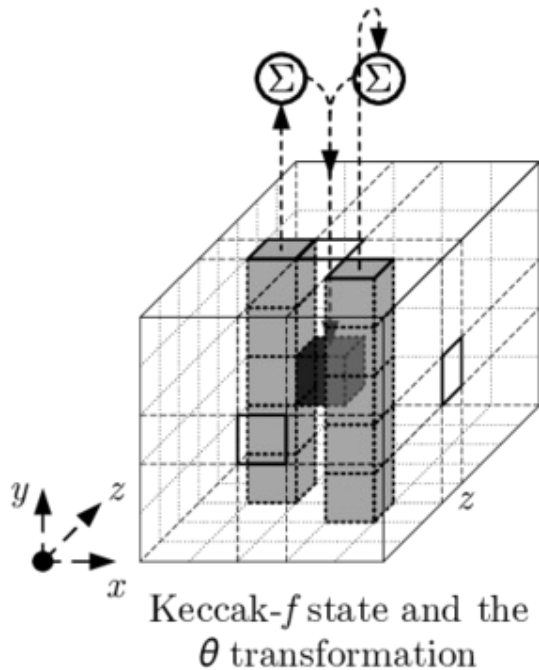
Quantum Circuit Implementation of SHA-3

- SHA-3 양자 회로 연구들

Cipher	Paper	Year
SHA-3	M. Amy et al. “Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3”, SAC 2016 .	2016
	T. Häner and M. Soeken, “Lowering the T-depth of Quantum Circuits By Reducing the Multiplicative Depth Of Logic Networks”, ACM Transactions on Quantum Computing , 2022.	2022
	G. Meuli, M. Soeken, and G. D. Micheli, “Xor-and-inverter graphs for quantum compilation”, npj Quantum Information , 8(1), 1–11, 2022.	2022
	G. Song, K. Jang, and H. Seo, “Improved Low-Depth SHA3 Quantum Circuit for Fault-Tolerant Quantum Computers”, Applied Sciences , 2023.	2023

SHA-3


- 1,600-bit State $S[x][y][z]$ 를 입력 대상으로 24 라운드 함수 수행
 - 라운드 함수는 다음과 같이 구성 됨, θ (theta) $\rightarrow \rho$ (rho) $\rightarrow \pi$ (pi) $\rightarrow \chi$ (chi) $\rightarrow \iota$ (iota)
 - State $S[x][y][z]$ 는 3차원 배열로 표현될 수 있으며, 각 x, y, z 크기는 5, 5, 64
($1600 = 5 \times 5 \times 64$)



$$S[x][y][z] = S[x][y][z] \oplus \left(\bigoplus_{i=0}^4 S[x-1][i][z] \oplus S[x+1][i][z-1] \right)$$

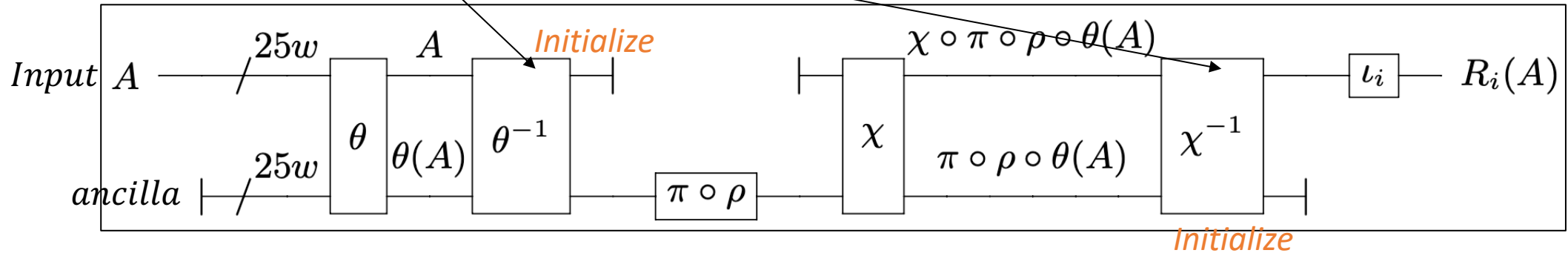
$$S[x][y][z] = S[x][y][z] \oplus (\sim S[x+1][y][z] \cdot S[x+2][y][z])$$

Quantum Circuit Implementation of SHA-3

Cipher	Paper	Year
 SHA-3	M. Amy et al. “Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3”, SAC 2016 .	2016
	T. Häner and M. Soeken, “Lowering the T-depth of Quantum Circuits By Reducing the Multiplicative Depth Of Logic Networks”, ACM Transactions on Quantum Computing , 2022.	2022
	G. Meuli, M. Soeken, and G. D. Micheli, “Xor-and-inverter graphs for quantum compilation”, npj Quantum Information , 8(1), 1–11, 2022.	2022
	G. Song, K. Jang, and H. Seo, “Improved Low-Depth SHA3 Quantum Circuit for Fault-Tolerant Quantum Computers”, Applied Sciences, 2023.	2023

Quantum Circuit Implementation of SHA-3 (2016)

- **M. Amy et al. (2016):** SHA-3 양자 회로 구현 또한 최초
 - SHA-3의 경우, SHA-2와 비교하여 상대적으로 구현 연산이 간단
 - 큐비트를 줄일 수 있는, **in-place 구조**의 SHA-3 양자 회로 제시
 - **Reverse 연산** (θ^{-1} , χ^{-1})을 통해, 사용된 *Input* (*A*), *ancilla* 큐비트들 초기화 후 **재사용**



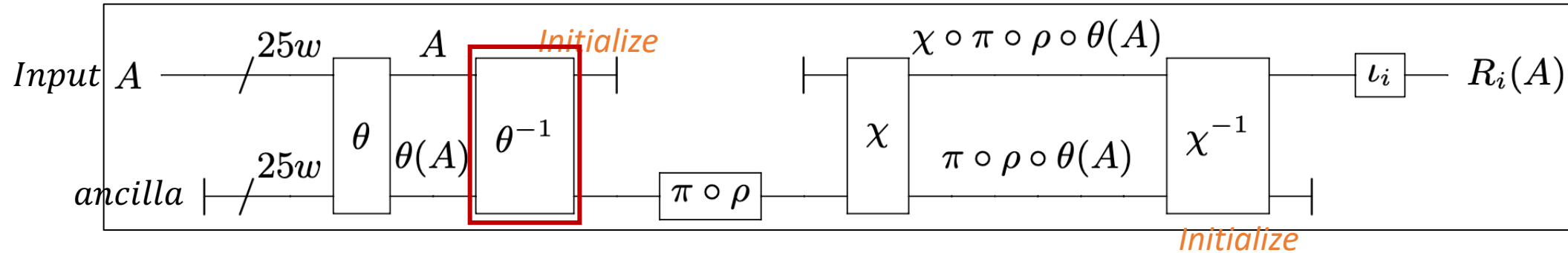
M. Amy et al. (2016)

- In-place 구조로, **3200 (= 1600 + 1600)의 큐비트**만이 사용되었지만, **Reverse 연산**으로 인한 **회로 Depth 증가**, **많은 양자 게이트**가 사용되었음

Quantum Circuit Implementation of SHA-3 (2016)

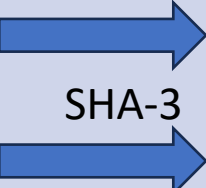
- 또한, 비효율적인 θ^{-1} 가 구현 되었음 (Output으로부터 Input을 생성하여 Input을 초기화하여 재사용)
 - θ : 17,600 CNOT gates, θ^{-1} : **136,000** CNOT gates
- θ 의 경우 선형 연산에 해당, 오히려 PLU 분해를 사용한 in-place 구현이 더 효율적 $\rightarrow \theta^{-1}$ 필요 x

$$\text{Linear layer } \theta : A'[x][y][z] \leftarrow A[x][y][z] \oplus \left(\bigoplus_{y' \in \mathbb{Z}_4} A[x-1][y'][z] \oplus A[x+1][y'][z-1] \right)$$



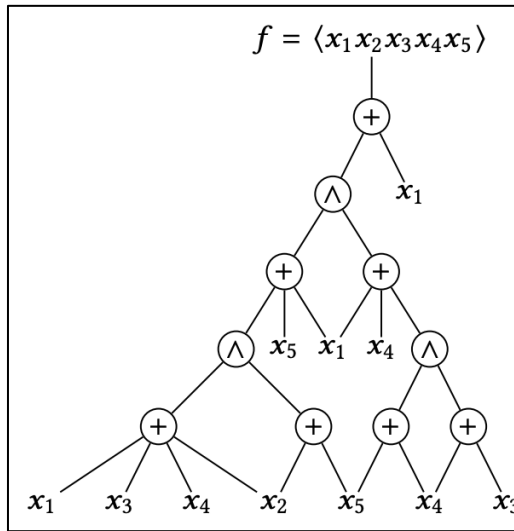
M. Amy et al. (2016)

Quantum Circuit Implementation of SHA-3

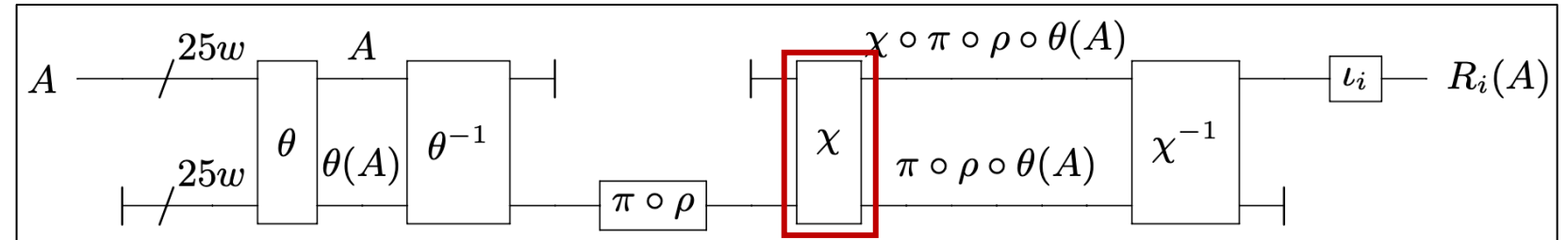
Cipher	Paper	Year
 SHA-3	M. Amy et al. “Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3”, SAC 2016 .	2016
	T. Häner and M. Soeken, “Lowering the T-depth of Quantum Circuits By Reducing the Multiplicative Depth Of Logic Networks”, ACM Transactions on Quantum Computing , 2022.	2022
	G. Meuli, M. Soeken, and G. D. Micheli, “Xor-and-inverter graphs for quantum compilation”, npj Quantum Information , 8(1), 1–11, 2022.	2022
	G. Song, K. Jang, and H. Seo, “Improved Low-Depth SHA3 Quantum Circuit for Fault-Tolerant Quantum Computers”, Applied Sciences, 2023.	2023

Quantum Circuit Implementation of SHA-3 (2022)

- T. Haner et al. (2022), G. Meuli et al (2022): 두 논문 모두, XOR-AND-Graph (XAG)의 양자 구현에서 **T 게이트와 T-depth를 최적화** 시키는 알고리즘을 제시 (SHA-3 양자 구현이 메인인 아님)
→ SHA3의 χ 연산 최적화에 적용



< XOR-AND-Graph >



$$\chi : A'[x][y][z] \leftarrow A[x][y][z] \oplus A[x+2][y][z] \oplus A[x+1][y][z])A[x+2][y][z]$$

< SHA-3의 χ 연산 >

- SHA-3에 대한 구현이 구체적으로 명시되어 있지 않지만, **χ 연산을 Toffoli depth 1로 최적화**

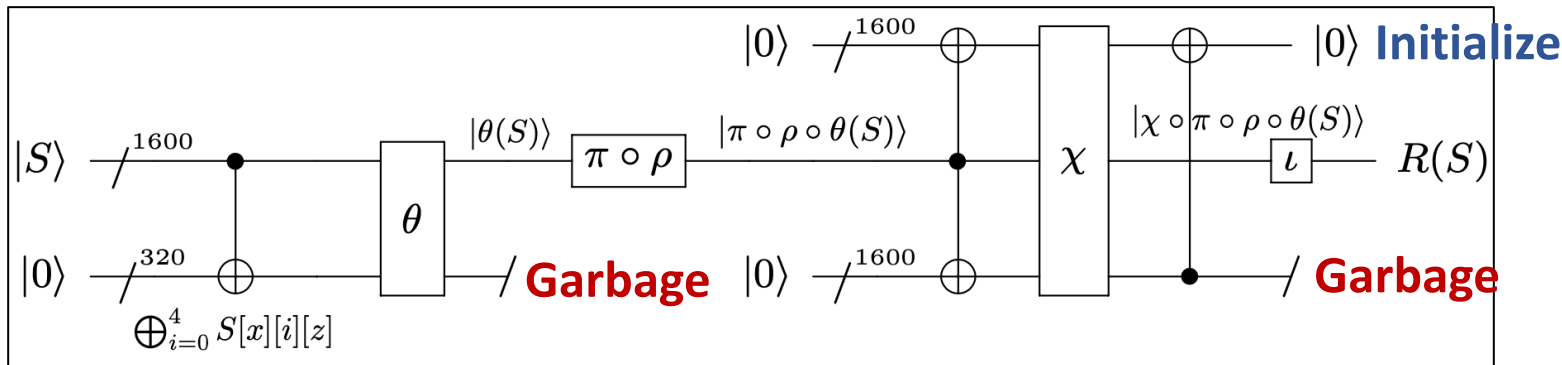
Quantum Circuit Implementation of SHA-3

- **M. Amy (2016): In-place 구조**
 - 적은 큐비트, 높은 Depth 및 게이트
- **T. Haner et al. (2022), G. Meuli et al. (2022): Out-of-place 구조**
 - 높은 큐비트, 낮은 Depth 및 게이트
 - **최근, SHA-3 구현 결과와 거의 유사**, 큐비트 개수는 Theta (Linear 연산)의 최적화로 인한 차이
→ 논문화를 위해서는, 개선이 필요

Hash function	Source	Architecture	#Qubit	Toffoli depth	Full depth
SHA3-256	Amy et al. (2016)	in-place	3,200	264	10,128
	Häner et al. (2022)	Out-of-place	46,400	24	-
	Meuli et al. (2022)		44,798	24	-
	Jang et al. (2024)		49,280	24	578

Quantum Circuit Implementation of SHA-3

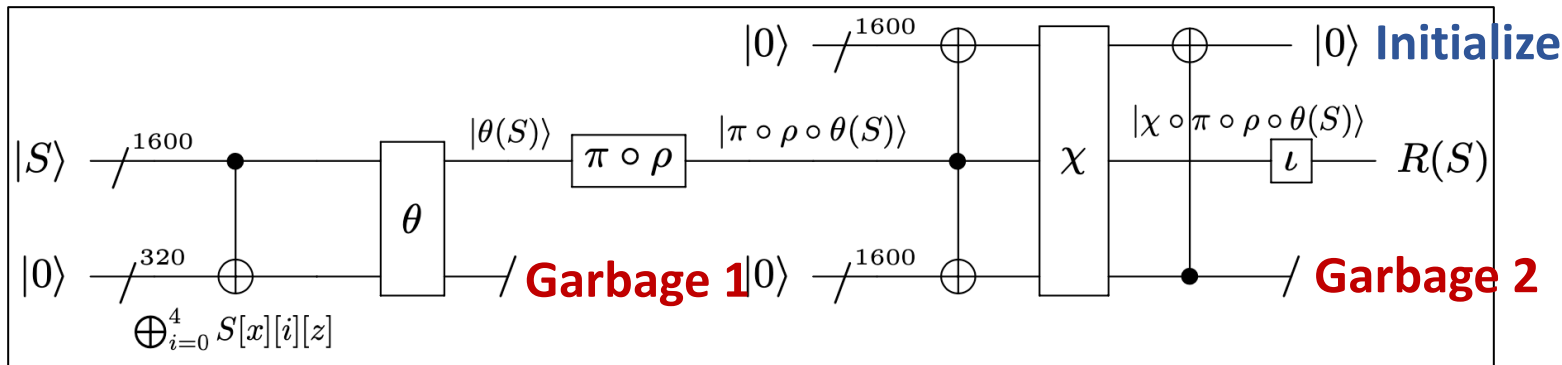
- 기존에 구현했던 SHA-3 양자 회로에서 **큐비트 수 감소**
 - AES 최적화 기법과 유사하기도 하면서 다르기도 함
- 기존 구현에서는 매 라운드 θ 에서 **320 큐비트**, χ 에서 **1600 큐비트**가 **버려졌음** → Garbage
 - χ 에서 **다른 1600 큐비트 만 초기화** 후, 다음 라운드에서 재사용



<기존 SHA-3 양자 회로 구조>

Quantum Circuit Implementation of SHA-3

- 개선 버전에서는 기존 **Garbage 큐비트**들을 초기화 후, 재사용
 - 모두 초기화 시키진 못하지만 **그래도 이득**, 또한 **Depth 증가 없음**
- Reverse로 큐비트를 초기화하기 시작하는 라운드의 **Garbage2 (1600 qubits)**는 초기화 할 수 없음



<기존 SHA-3 양자 회로 구조>

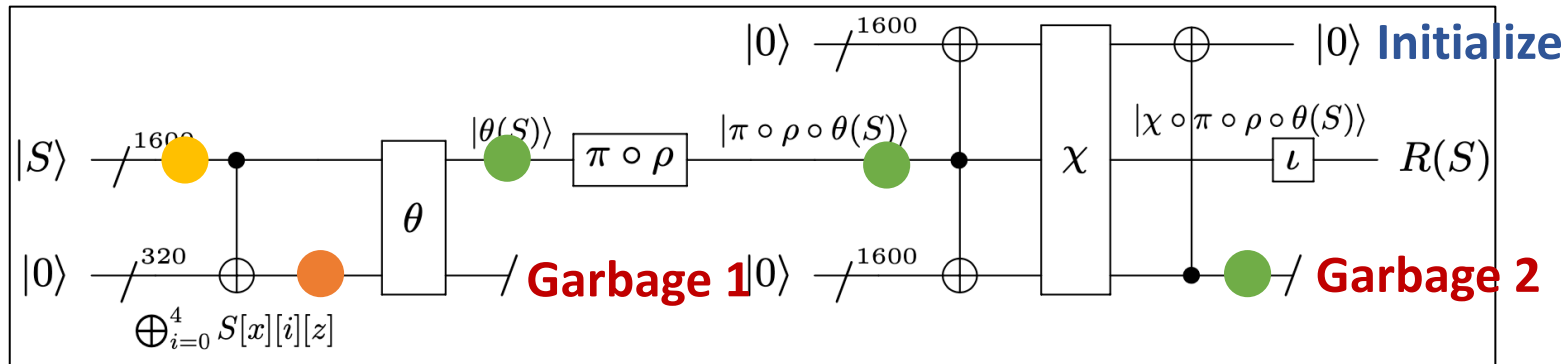
Quantum Circuit Implementation of SHA-3

Case 1). 매 라운드 Reverse를 수행하는 경우

- Garbage 1만을 초기화할 수 있음 (320 qubits) → **C**에 해당

Note:

- Garbage 1 + Garbage2 + Initialize = **A** (3520 = 320 + 1600 + 1600)
- Garbage 1 + Garbage2 = **B** (1920 = 320 + 1600)
- Garbage2 = **C** (320)



Quantum Circuit Implementation of SHA-3

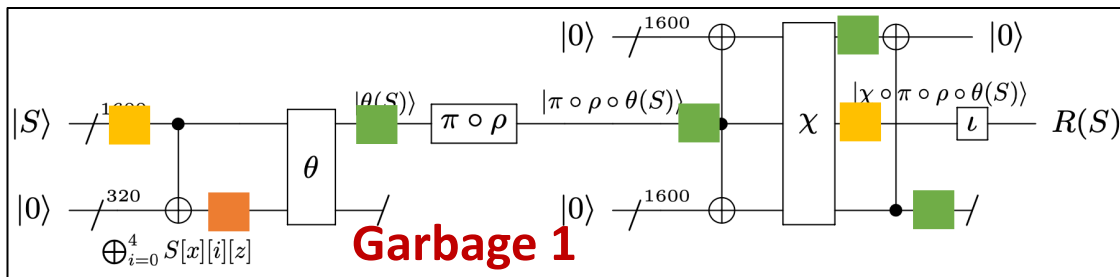
Case 2). 2 라운드 간격으로 Reverse를 수행하는 경우

- 첫 Reverse에서는 Garbage 1, 두번째 Reverse에서는 Garbage 1 + Garbage 2 + Initialize를 초기화할 수 있음 (320 qubits) → **C**와 **A**에 해당

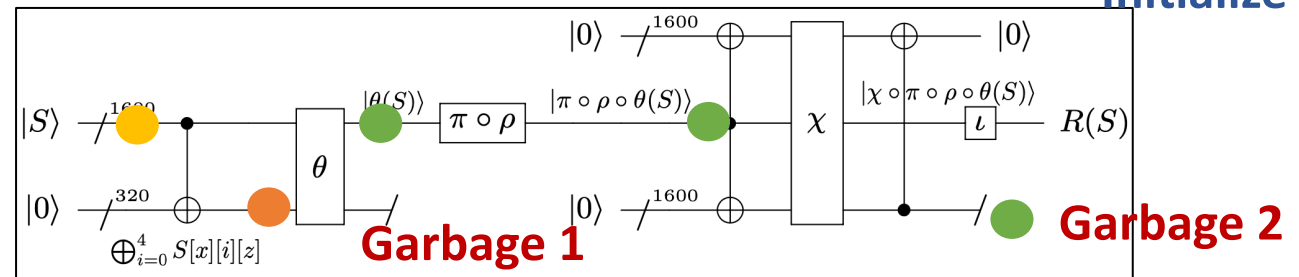
Note:

- Garbage 1 + Garbage2 + Initialize = **A** (3520 = 320 + 1600 + 1600)
- Garbage 1 + Garbage2 = **B** (1920 = 320 + 1600)
- Garbage2 = **C** (320)

Copy ■



Initialize



Quantum Circuit Implementation of SHA-3

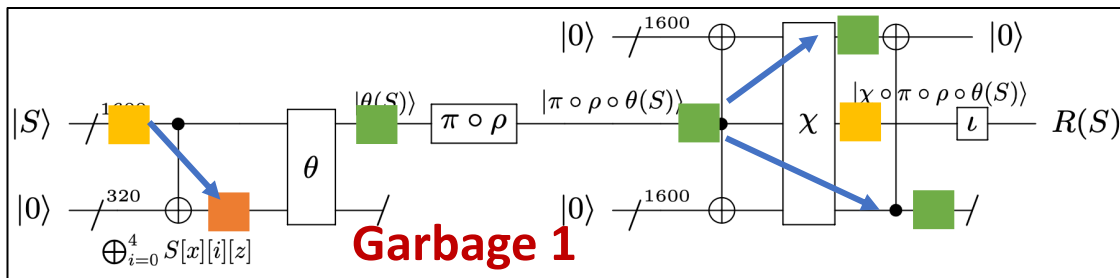
Case 2). 2 라운드 간격으로 Reverse를 수행하는 경우

- 첫 Reverse에서는 Garbage 1, 두번째 Reverse에서는 Garbage 1 + Garbage 2 + Initialize를 초기화할 수 있음 (320 qubits) → **C**와 **A**에 해당

Note:

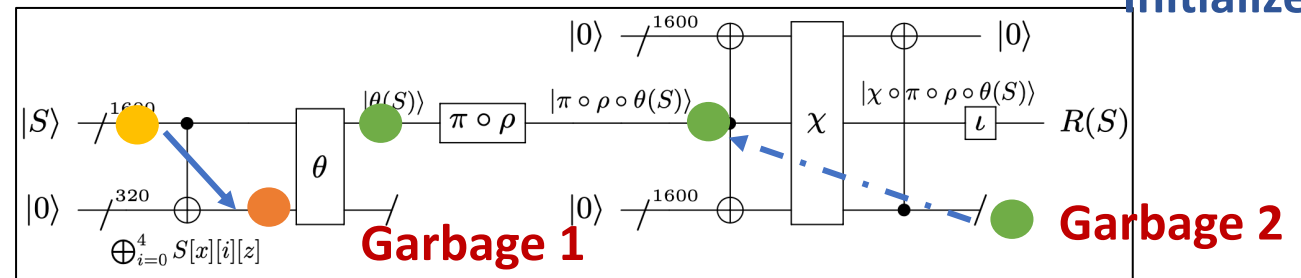
- Garbage 1 + Garbage2 + Initialize = **A** (3520 = 320 + 1600 + 1600)
- Garbage 1 + Garbage2 = **B** (1920 = 320 + 1600)
- Garbage2 = **C** (320)

Copy ■



A인 경우

Initialize



C인 경우

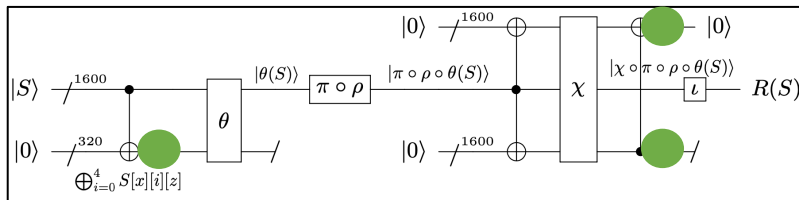
Quantum Circuit Implementation of SHA-3

Case 3). 3 라운드 이상의 간격으로 Reverse를 수행하는 경우

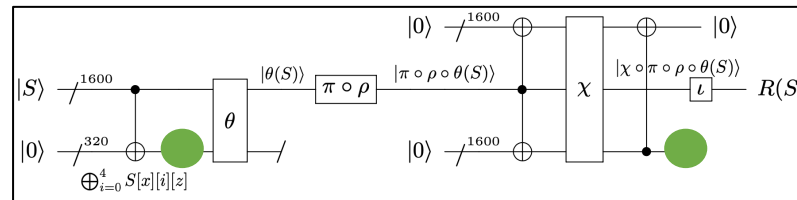
- 첫 Reverse에서는 Garbage 1, 중간 Reverse 에서는 Garbage 1 + Garbage 2를 초기화할 수 있음, 마지막 Reverse에서는 Garbage 1 + Garbage 2 + Intialize 초기화 가능 $\rightarrow \text{C} \rightarrow \text{B} \rightarrow \text{B} \dots \rightarrow \text{A}$

Note:

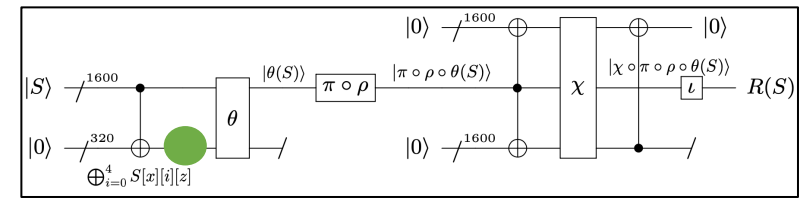
- Garbage 1 + Garbage2 + Initialize = **A** ($3520 = 320 + 1600 + 1600$)
- Garbage 1 + Garbage2 = **B** ($1920 = 320 + 1600$)
- Garbage2 = **C** (320)



A인 경우



B인 경우



C인 경우

Quantum Circuit Implementation of SHA-3

Case 2) 2 라운드 간격으로 Reverse (파란색: Round, 빨간색: Reverse)

A B C A

0 1 1 0 C A

2 3 3 2 C A

A B 4 5 5 4 C A

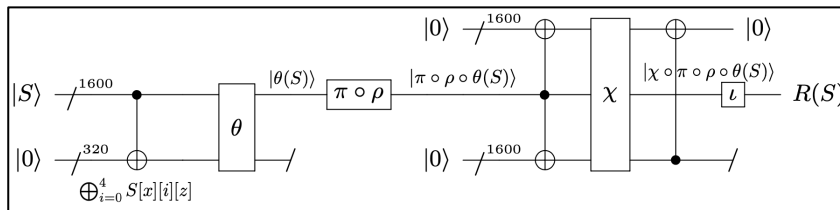
A B 6 7 7 6

A B 8 9

A B

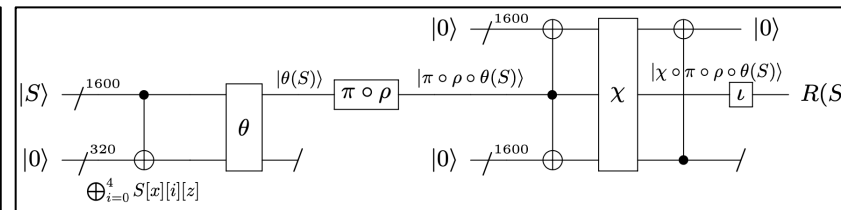
Note:

- Garbage 1 + Garbage2 + Initialize = **A** (3520 = 320 + 1600 + 1600)
- Garbage 1 + Garbage2 = **B** (1920 = 320 + 1600)
- Garbage2 = **C** (320)



A

A

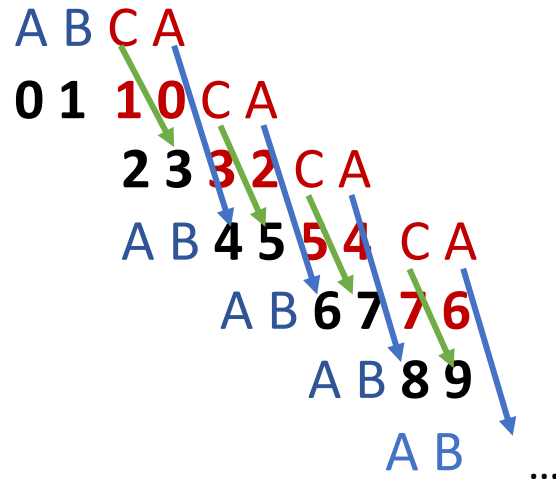


C

B

Quantum Circuit Implementation of SHA-3

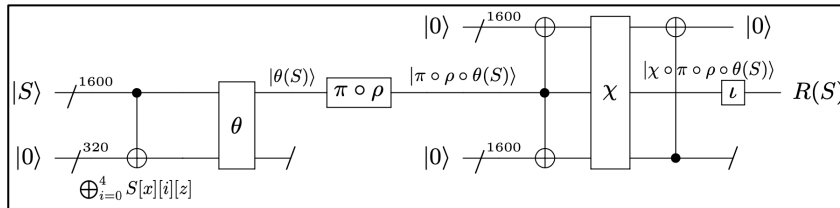
Case 2) 2 라운드 간격으로 Reverse (파란색: Round, 빨간색: Reverse)



Note:

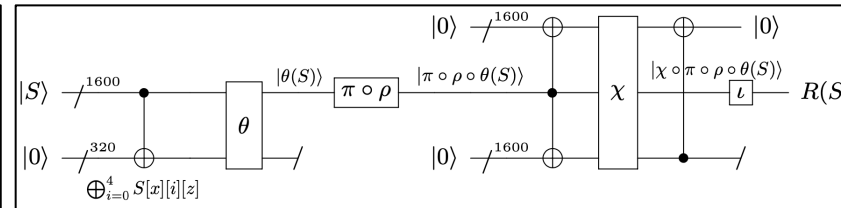
- Garbage 1 + Garbage2 + Initialize = **A** (3520 = 320 + 1600 + 1600)
- Garbage 1 + Garbage2 = **B** (1920 = 320 + 1600)
- Garbage2 = **C** (320)

$$A + B + A + (B-C) + (B-C) + (B-C).... \rightarrow 2A + B + 11(B-C)$$



A

A

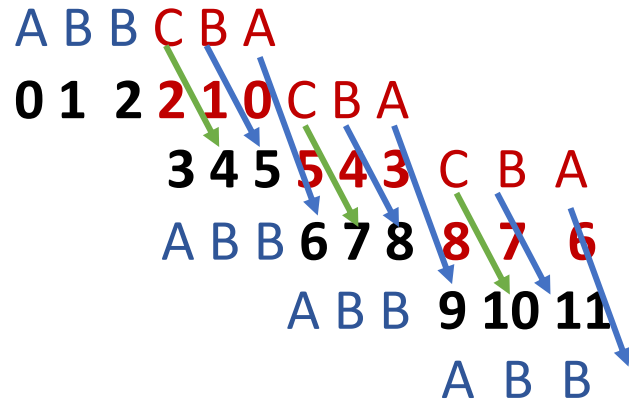


C

B

Quantum Circuit Implementation of SHA-3

Case 3) 3 라운드 이상 간격으로 Reverse (파란색: Round, 빨간색: Reverse)

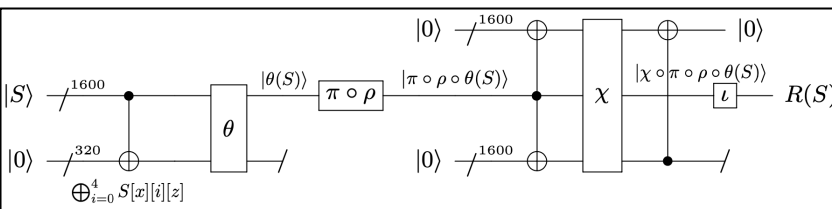


Note:

- Garbage 1 + Garbage2 + Initialize = **A** (3520 = 320 + 1600 + 1600)
- Garbage 1 + Garbage2 = **B** (1920 = 320 + 1600)
- Garbage2 = **C** (320)

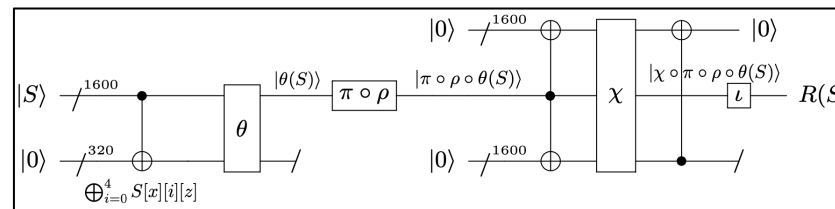
$$A + \mathbf{B} + \mathbf{B} + A + (\mathbf{B-C}) + (\mathbf{B-C}) + (\mathbf{B-C})... \rightarrow 2A + 2\mathbf{B} + 7(\mathbf{B-C})$$

...



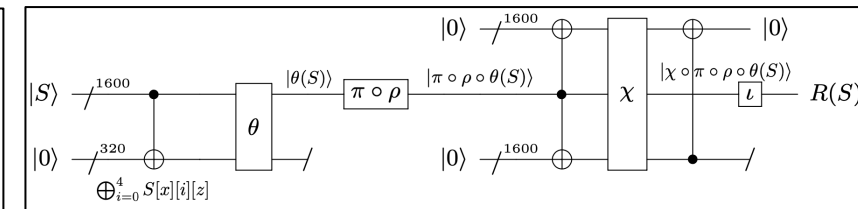
A

A



B

B



C

B

Quantum Circuit Implementation of SHA-3

- 라운드 간격 별, 필요 큐비트 수: $(2A + (B - C) \times (\frac{24}{n} - 1) + B \times (n - 1))$
 - 4 Round 간격일 때 가장 효율적 (20800)

Round		B-C	B	Total
2		17600	1920	26560
3		11200	3840	22080
4		8000	5760	20800
5		6080	7680	20800
6		4800	9600	21440
7		3885.71429	11520	22445.7143
8		3200	13440	23680
9		2666.66667	15360	25066.6667
10		2240	17280	26560
11		1890.90909	19200	28130.9091
12		1600	21120	29760

Results

- 가장 낮은 Depth를 가짐과 동시에, 가장 높은 트레이드오프 성능 달성

Hash function	Source	Architecture	#Qubit (M)	Toffoli depth (TD)	Full depth (FD)	TD-M	FD-M
SHA3-256	Amy et al. (2016)	in-place	3,200	264	10,128	844,800	3,2409,600
	Häner et al. (2022)	Out-of-place	46,400	24	-	1,113,600	
	Meuli et al. (2022)		44,798	24	-	1,075,152	
	Jang et al. (2024)		49,280	24	578	1,182,720	2,8483,840
	This work		22,400	24	578	537,600	1,2947,200



Thank you!