가역 양자 회로를 이용한 SHA-3 최적 설계

서연송, 박영훈*
숙명여자대학교 컴퓨터과학과, *숙명여자대학교 소프트웨어학부
yeonsongsuh@sookmyung.ac.kr, *yh.park@sookmyung.ac.kr

Implementation of Efficient Reversible Quantum Algorithm for SHA-3

Yeonsong Suh, Younghoon Park
Sookmyung Women's University

요 약

양자 컴퓨터의 발전은 기존의 해시 기반 보안 구조에 위협을 가하고 있다. 특히 Grover 알고리즘은 고전컴퓨터보다 훨씬 적은 수로 해시 함수의 프리이미지를 탐색할 수 있어, 해시 기반 구조의 양자에 대한 보안 대책이 필요하다. 기존 연구에서는 SHA-3 의 Keccak 기반의 오라클 회로를 구현하여 보조큐빗을 폐기하거나 역함수 없이 구성하여 효율성에 한계가 있었다. 본 논문에서는 SHA-3 의 핵심 연산인 θ 함수에 대해 역함수 θ^{-1}을 포함하는 가역적인 양자 회로를 제안하고, 보조큐빗을 다시 사용할 수 있는 구조를 구현했다. 제안된 회로는 기존에 제시된 연구 대비 CNOT 게이트 수를 줄이고 양자 회로의 깊이를 적절히 유지하고 있어 최적화된 Grover 알고리즘을 제공할 수 있다

Ⅰ. 서 론

양자컴퓨터의 등장으로 기존 통신 보안 체계의 흐름이 바뀌고 있다. 고전컴퓨터 기반의 암호 시스템은 주로 수학적 문제의 계산 복잡도를 전제로 보안성을 유지해 왔다. 그러나 Shor 나 Grover 과 같은 양자 알고리즘은 해당 문제를 고전컴퓨터보다 훨씬 빠르게 해결할 수 있는 가능성을 제시하여 암호 시스템의 안전성에 대한 재검토를 요구한다. 특히 Grover 알고리즘은 조건을 만족하는 값을 탐색할 때, 고전컴퓨터는 평균 $O(2^{n-1})$회의 연산이 필요하지만, 이를 $O(\sqrt{2^n})$으로 낮출 수 있어 해시 함수에 대한 프리이미지 공격에 실질적인 위협이 된다 [1]. 이로 인해 Grover 알고리즘 기반의 양자 오라클 회로 설계가 핵심 연구 주제로 떠오르고 있다.

Grover 알고리즘에서 요구되는 양자 오라클 회로는 함수 f와 역함수 f^{-1}로 구성되며, 전체 회로의 가역성을 보장하기 위해 두 연산의 구현이 모두 필요적이다 [2]. 그러나 기존 연구들은 함수 f 의 연산에서 θ 함수만 구현하거나, θ 연산을 위해 사용되는 보조큐빗을 매 연산마다 폐기하는 구조로 효율성과 확장성에서 한계를 보여주고 있다. 특히 θ연산은 SHA-3 해시 함수의 핵심 구성 요소인 Keccak 알고리즘에 포함되어 있으며, 해당 알고리즘은 보안 강화를 위해 24 라운드 이상 반복이 요구된다. 이러한 상황에서 매 라운드마다 큐빗을 버리는 구조는 큐빗 수가 제한적인 현재의 양자컴퓨터 환경에서는 매우 치명적이다.

이에 본 논문에서는 SHA-3 에서 θ 연산과 그 역함수를 포함하는 가역적인 양자 회로를 구현하여 매 연산마다 보조큐빗을 초기화하여 다음 연산에서 다시 사용할 수 있는 구조를 제안한다. 이를 통해 해시 함수의 프리이미지 공격을 위한 최적화된 Grover 알고리즘을 제공할 수 있다.

Ⅱ. 제안 방식

본 논문에서는 Keccak 알고리즘의 θ 연산과 그 역함수인 θ^{-1} 을 모두 포함하고, 보조큐빗 $C[x][z]$ 을 폐기하지 않고 초기화하여 재사용할 수 있는 양자회로를 제안한다. 먼저 θ 연산은 $A[x][y][z]$의 열 방향 비트들을 XOR 하여 $C[x][z]$를 구한다. 이는 수식 (1)로 나타낼 수 있다.

$$C[x][z] \leftarrow \bigoplus_{y=0}^{4} A[x][y][z] \quad (1)$$

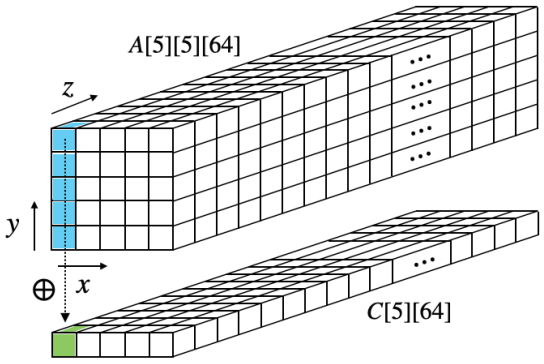

그림 1. Θ의 연산 구조 및 흐름

θ 의 연산 구조 및 흐름을 나타낸 그림 1 을 보면, 상단의 파란색 열은 고정된 x와 z에서 y방향으로 나열된 5 개의 $A[x][y][z]$ 비트를 의미하며, 이들을 XOR 한 결과가 하단 초록색의 보조큐빗 $C[x][z]$로 저장된다.

$$A'[x][y][z] \leftarrow A[x][y][z] \oplus C[x-1][z] \oplus C[x+1][z-1] \quad (2)$$

수식 (2)는 θ 연산의 두 번째 단계로, 기존 상태 $A[x][y][z]$ 에 대해 보조큐빗 C 를 활용해 새로운 상태 $A'[x][y][z]$를 계산하는 방식이다.

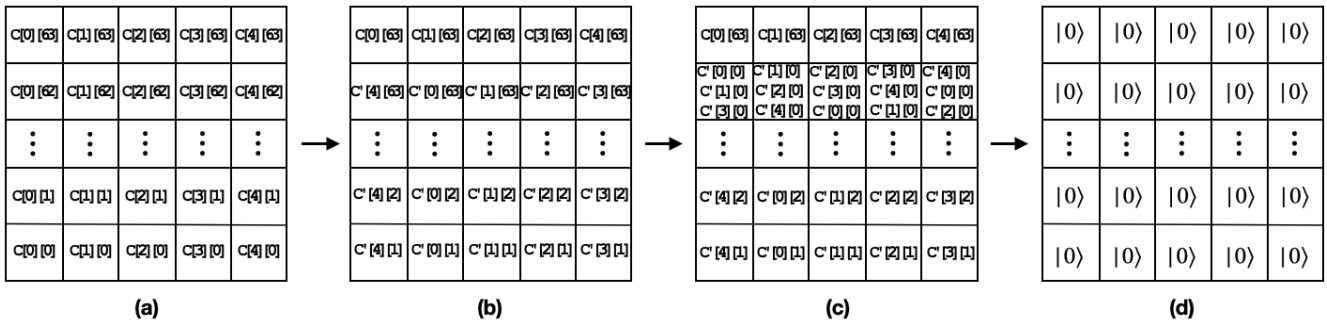

그림 2. θ 의 연산 구조 및 흐름

해당 연산은 각 비트에 대해 인접한 열의 정보를 반영하여 수직 및 대각선 방향으로 정보를 확산시키기 때문에 Keccak 전체 구조의 확산성을 강화하는 θ 연산의 특징을 확인할 있다. 따라서 위 수식을 통해 $A[x][y][z]$의 모든 비트는 주변 열들의 정보를 반영하여 업데이트 되고, θ 연산은 양자회로에서 4800개의 CNOT 게이트로 구현된다.

θ 연산이 완료된 이후에는 보조큐빗 $C[x][z]$를 다시 초기 상태로 복원해야 한다. 해당 과정이 역함수인 θ^{-1} 연산이며, θ 연산을 통해 업데이트 된 $A'[x][y][z]$로부터 $C[x][z]$를 복원하는 구조이다. $C'[x][z]$가 업데이트 된 $A'[x][y][z]$로 XOR 된 값이라 할 때, 수식 (2)를 변형한 수식 (3)을 통해 대부분의 $C[x][z]$를 되돌릴 수 있다.

$$C'[x][z] = C[x][z] \oplus C[x-1][z] \oplus C[x+1][z-1] \tag{3}$$

그러나 $z = 63$과 같이 경계에 위치한 비트는 C' 값이 계산 불가능해 직접적인 복원이 어렵다. 이를 해결하기 위해 $C[x][63]$ 의 원래 정의였던 $A[x][0][63]$ 부터 $A[x][4][63]$까지 5 개의 비트를 XOR 하는 것을 바탕으로 복원 방식을 구현했다. $C'[0][63]$을 예시로 들면 다음과 같이 식을 전개하면 된다.

$$\begin{aligned} C'[63][0] = {} & C'[0][0] \oplus C'[1][0] \oplus C'[3][0] \oplus C'[0][1] \\ & \oplus C'[1][1] \oplus C'[2][1] \oplus C'[3][1] \\ & \oplus C'[2][2] \oplus \cdots \oplus C'[0][63] \oplus C'[2][63] \end{aligned} \tag{4}$$

그림 2 는 보조큐빗을 원래 상태로 되돌리는 과정을 단계별로 보여준다. (a) 는 θ 연산이 완료된 직후의 보조큐빗 $C[x][z]$ 상태이며, (b) 에서는 이를 기반으로 수식 (3)에 따라 역방향 연산을 수행하여 $C'[x][z]$ 값을 계산하는 단계이다. (c) 는 (4)의 $C'[0][63]$ 예시처럼, $C'[x][z]$에 포함된 항을 적절히 전개하고 일부 항을 한 번 더 XOR 해 원래의 $C[x][z]$를 소거하는 과정이다. 이때 해당 수식에는 총 171 개의 항이 포함되며, 자기 자신을 두 번 XOR 하면 0 이 되는 성질을 이용해 $C'[0][0]$, $C'[1][0]$, $C'[3][0]$을 제외한 항들을 한 번 더 XOR 해 중간 항들을 제거한다. 마지막으로 (d) 는 모든 보조큐빗을 초기 상태로 초기화한 결과를 보여주며, 이를 통해 양자 회로의 가역성과 보조큐빗의 완전한 복원이 되었음을 확인할 수 있다.

따라서 $z = 0$부터 $z = 62$까지는 수식 변형을 통해, $z = 63$은 논리 연산을 통해 보조큐빗 C를 모두 초기 상태로 되돌릴 수 있다. 결과적으로 제안된 θ^{-1} 연산은 총 3120 개의 CNOT 게이트를 사용하게 되고 양자 회로의 깊이는 318 이 된다. 기존 연구와 본 논문에서 제안한 구조를 표 1 에서 정리했다.

표 1. 성능 비교 결과

Papers	CNOT Gates		Qubits (Discarded)	Depth
	θ	θ^{-1}		
Amy et. al. [3]	17,600	1,360,000	3,200 (0)	300
Song et. al. [4]	24,000	N/A	3,200 (1,600)	79
Jang et. al. [5]	4,800	N/A	1,920 (320)	15
Proposed	4,800	3,120	1,920 (0)	318

IV. 결론

본 논문은 Keccak 알고리즘의 θ 연산에서 사용되는 보조큐빗을 폐기하지 않고 초기화하여 재사용 가능한 양자 회로를 제안한다. 기존 연구들은 θ^{-1} 연산을 생략하거나 보조큐빗을 폐기하는 구조로 반복 수행이 가능한 구조를 구현하였다. 결과적으로 회로 깊이는 기존과 유사하면서도 CNOT 게이트의 수를 적절히 유지했다.

참 고 문 헌

[1] Grover, Lov K. "A fast quantum mechanical algorithm for database search." Proceedings of the twenty-eighth annual ACM symposium on Theory of computing. 1996.

[2] Nielsen, Michael A., and Isaac L. Chuang. Quantum computation and quantum information. Cambridge university press, 2010.

[3] Amy, Matthew, et al. "Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3." International Conference on Selected Areas in Cryptography. Cham: Springer International Publishing, 2016.

[4] Song, Gyeongju, Kyungbae Jang, and Hwajeong Seo. "Improved low-depth SHA3 quantum circuit for fault-tolerant quantum computers." Applied Sciences 13.6 (2023): 3558.

[5] Jang, Kyungbae, et al. "Quantum implementation and analysis of SHA-2 and SHA-3." IEEE Transactions on Emerging Topics in Computing (2025)