SHA-256 해시함수의 Choice (Ch) 및 Majority (Maj) 프로세스 최적 양자 회로 설계

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

Optimal Quantum Circuit Design for the Choice (Ch) and Majority (Maj) Operations of the SHA-256 Hash Function

Yeonsong Suh, Younghoon Park*
Sookmyung Women's Univ.

요 약

양자컴퓨팅의 발전은 기존 해시 기반 보안 구조에 새로운 위협을 가하고 있다. 특히 Grover 알고리즘은 고전 컴퓨터보다 훨씬 적은 연산으로 해시 함수의 프리이미지 탐색이 가능해, 최근 연구들은 이를 이용한 해시 공격과 그 실현을 위한 양자 오라클 회로 설계에 집중하고 있다. 본 논문은 이러한 공격 연구 흐름을 따라 SHA-256 의 핵심 비선형 연산인 Choice(Ch)와 Majority(Maj)를 대상으로 진리표 기반의 행렬 연산 방식을 적용한 보조 큐빗 없는 양자 회로 구조를 제안한다. 제안된 회로는 CNOT 게이트 수와 회로 깊이를 동시에 줄여 SHA-2 기반 Grover 오라클의 자원 소모를 최소화하며, Grover 기반 프리이미지 공격의 실험적 구현 가능성과 평가 정확도를 향상시킨다.

Ⅰ. 서 론

양자컴퓨팅의 발전은 계산적인 성능 향상을 넘어 현재의 암호 체계를 근본적으로 재검토하게 하고 있다. Grover 알고리즘은 조건을 만족하는 값을 탐색할 때, 고전 컴퓨터가 평균 $O(2^{n-1})$ 회의 연산이 필요한 반면, 양자컴퓨터는 $O(\sqrt{2^n})$ 수준으로 낮출 수 있어 해시 함수에 대한 프리이미지 공격에 실질적인 위협이 된다 [1]. 이에 따라 최근 연구들은 Grover 알고리즘을 이용해 해시 함수를 공격하거나 그 과정에서 필요한 핵심 구성 요소인 양자 오라클 회로의 효율적 설계가 주요 연구 흐름으로 자리잡고 있다.

SHA-256 은 디지털 서명, 거래 검증, 블록체인 합의 등 다양한 보안 분야에서 표준 해시 함수로 널리 쓰이고 있다. 블록체인 시스템에서는 해시 함수가 블록 생성 및 작업증명, 트랜잭션 무결성 검증 등 핵심 보안 기능을 담당하고 있기 때문에 SHA-2 에 대한 양자 공격은 머지않아 블록체인 분야 전체에 영향을 미칠 수 있다. 기존 SHA-2 양자 회로 연구들은 주로 게이트 수와 회로 깊이를 줄이기 위한 구조적 최적화에 초점을 맞추어 왔다. 초기 연구에서는 순차적인 연산 구조로 인해 회로 깊이가 커지는 한계가 있었고, 이를 해결하기 위해 가역 연산을 이용한 구현이 제안되었다. 이후 Toffoli 게이트와 T-게이트 수를 줄이거나, 병렬 연산을 적용하는 방식으로 효율을 높이는 다양한 접근이 이루어졌다 [2]. 일부 연구에서는 전체 연산 구조를 분석하여 SHA-2 회로의 큐빗 수와 깊이를 정량적으로 제시하는 방법도 제안했다 [3]. 그러나 이러한 구현들은 대부분 보조 큐빗을 사용하거나 매 라운드마다 폐기하는 구조로 제안되어 큐빗 자원이 제한된 현재의 양자 하드웨어 환경에서는 실용성이 떨어지는 한계가 있었다.

본 논문에서는 이러한 문제를 해결하기 위해 SHA-256 의 Choice(Ch)와 Majority(Maj) 연산을 진리표 기반의 행렬 연산 방식으로 분석하고, 보조 큐빗을 사용하지 않는 양자 회로 설계 방법을 제안한다.

Ⅱ. 제안 방식

SHA-256 은 입력된 메시지를 512 비트 블록 단위로 나누어 처리하고, 각 라운드마다 여러 가지 연산을 반복해서 수행한다. 이 과정에는 비선형 함수, 모듈러 덧셈, 순환 시프트 등이 포함된다. 그 중 Choice(Ch) 와 Majority(Maj) 함수는 해시의 비선형성을 강화하여 복잡성과 보안성을 높인다. 두 함수는 내부 상태 값들을 서로 섞고 비교하여 예측이 어려운 출력을 만들어낸다. 하지만 해당 연산은 여러 개의 입력 비트가 동시에 서로에게 영향을 주는 구조로, 이를 양자 회로로 옮긴다면 게이트 수와 회로의 깊이가 모두 증가하는 문제가 발생한다. 따라서 이 두 함수의 효율적인 양자 회로 구현은 SHA-256 전체 회로의 성능을 좌우하게 된다.

먼저 Choice 함수는 SHA-256 의 입력 비트 중 하나인 e 의 값에 따라 두 입력 f 와 g 중 하나를 선택하는 역할을 한다. 수학적으로는 다음과 같이 정의된다.

$$Ch(e,f,g) = (e \wedge f) \oplus (\neg e \wedge g)$$

즉, $e = 1$ 일 때는 f 를, $e = 0$ 일 때는 g 를 출력으로 선택한다. 양자 회로에서는 모든 연산이 가역적이어야 하므로, 기존의 고전 논리 구조를 그대로 사용하면 보조 큐빗이 필요하거나 회로 깊이가 불필요하게 커지게 된다. 이러한 문제를 해결하기 위해 진리표 기반의 행렬 연산 방식을 적용했다. 입력 조합 (e,f,g) 의 진리표를 구성하고, 각 항의 논리 연산을 단위 행렬 I 과 $Pauli-X$ 행렬 X 의 곱으로 표현하였다. 전체 연산은 텐서곱($\otimes$)을 이용해 행렬 형태로 확장되며, Choice 함수는 다음과 같이 단순화된다.

$$D_{Ch} = D[I\ I\ I\ I\ I\ X\ X\ I] \cdot (I \otimes I \otimes CX)$$

해당 표현을 양자 게이트 수준으로 분해하면, 그림 1.과 같이 총 6 개의 CNOT 게이트와 5 개의 X 게이트로 구성되고 회로의 깊이는 5 가 된다. 이는 기존 Toffoli 기반 설계보다 게이트 수와 깊이를 모두 줄인 형태로, SHA-256 양자 회로 구현의 효율성을 향상시킨다.

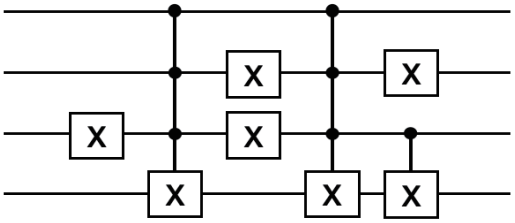

그림 1. Choice(Ch) 연산 최적 회로

Majority 함수는 입력 비트 a,b,c 중 다수의 값을 출력으로 결정하는 함수이다. 다수결의 원칙에 따라 세 비트 중 1 의 개수가 두 개 이상일 때 1 을 반환하고 그렇지 않으면 0 을 반환한다. 수학적으로는 다음과 같이 정의된다..

$$Maj(a,b,c) = (a \wedge b) \oplus (a \wedge c) \oplus (b \wedge c)$$

Choice 함수가 조건에 따라 입력 중 하나를 선택하는 구조라면, Majority 함수는 모든 입력을 동시에 고려하는 대칭적 구조를 가진다. 따라서 입력 간의 조합을 통해 직접 출력을 결정할 수 있어 Maj 는 병렬 연산에 적합하다. Maj 함수도 마찬가지로 진리표 기반으로 해석하여, 각 입력 조합을 행렬 형태로 구성하고 이를 단위 행렬 I과 $Pauli-X$ 행렬 X의 곱으로 변환하였다. 결과적으로 다음과 같은 연산 행렬로 표현된다.

$$D_{Maj} = (I \otimes I \otimes X) \cdot (I \otimes X \otimes I) \cdot (X \otimes I \otimes I)$$

해당 표현을 양자 게이트 수준으로 분해하면, 그림 2. 과 같이 총 7 개의 CNOT 게이트와 4 개의 X 게이트로 구성되고 회로의 깊이는 6 이 된다. 그리고 기존 연구와 본 논문에서 제안한 구조를 표 1 에서 정리했다.

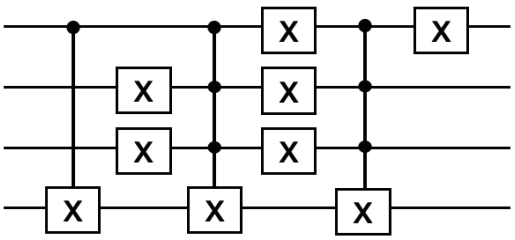

그림 2. Majority(Maj) 연산 최적 회로

표 1. 기존 Toffoli 기반 회로와의 게이트 구성 비교

Papers		Toffoli Gate	CNOT Gate	X Gate	Depth	Ancilla Qubit
Lee et. al. [2]	Ch	4	6	3	8	O
	Maj	3	5	3	7	
Proposed	Ch	0	6	5	5	X
	Maj	0	7	4	6	

Ⅲ. 결론

본 논문에서는 SHA-256 의 비선형 연산 블록인 Choice(Ch) 와 Majority(Maj) 함수를 대상으로 진리표 기반의 행렬 연산 접근법을 이용한 양자 회로 설계 방법을 제안한다. 제안된 방식은 각 함수의 논리식을 단위 행렬과 $Pauli-X$ 연산자의 조합으로 변환하여 복잡한 가역 변환이나 보조 큐빗의 사용 없이 입력 비트 간의 논리 관계를 직접 게이트 구조로 구현한다. 이를 통해 SHA-2 계열 해시 함수의 양자 오라클 구현에서 게이트 수와 회로 깊이를 효율적으로 줄일 수 있었다.

ACKNOWLEDGMENT

본 논문은 2025 년도 과학기술정보통신부 및 정보통신기획평가원의 'SW 중심대학사업' 지원을 받아 (제작,구축, 설치, 확보 등) 되었습니다. (2022-0-01087)

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] Lee, Jongheon, et al. "T-depth reduction method for efficient SHA-256 quantum circuit construction." IET Information Security17.1 (2023): 46-65.

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