정 보 보 호 학 회 지
제34권 제2호, 2024. 4

양자 컴퓨터를 통한 대칭키 AES 및 해시 함수 SHA-2/3 해킹 동향

장 경 배*, 오 유 진**, 서 화 정***

요 약

고전 컴퓨터에서 풀기 어려운 난제를 효율적으로 모델링하고 해결할 수 있는 양자 컴퓨터는 현재 암호들을 위협하고 있다. 특히, 공개키 암호에 해당하는 RSA와 Elliptic Curve Cryptography (ECC)는 Shor의 양자 알고리즘에 의해 해당 암호들의 안전성이 기반이 되는 난제들을 다항 시간 내에 해결하여 새로운 양자 내성 암호가 필요한 상황이다. 이에 NIST는 양자내성암호 표준화 공모전을 주최함으로써 현재까지 표준화 작업을 이어나가고 있다. 대칭키 암호의 경우, Grover의 양자 검색 알고리즘에 의해 고전 컴퓨터상에서 보장하던 보안 강도가 제곱근으로 감소되게 된다. 기존, 신규 암호 알고리즘 모두 양자 컴퓨터상에서의 보안 강도를 평가해야되는 상황이며, 이에 NIST는 양자 후 보안 강도 기준을 도입하였다. 양자 후 보안 강도는 레벨 1에서 5로 정의되며, 각 레벨에는 AES 및 SHA-2/3에 대한 양자 해킹 비용이 지정되어 있다. 본 논문에서는 이러한 암호 학계 상황에 따라, 대칭키 AES 및 해시 함수 SHA-2/3에 대한 해킹, 특히 양자 회로 구현 동향에 대해 살펴보고자 한다.

Ⅰ. 서 론

양자 컴퓨터의 발전은 현재 사용 중인 전통적인 암호 알고리즘들의 안전성에 대한 우려를 불러일으키고 있다. 특히, 대규모의 안정적인 양자 컴퓨터가 개발된다면, Shor의 알고리즘은[1] RSA 및 ECC와 같은 공개 키 암호의 안전성을 쉽게 붕괴시킬 수 있다. 대칭키 암호와 해시 함수의 경우에도 Grover의 검색 알고리즘이[2] 보안을 위협하는 요인으로 작용한다. Grover 알고리즘은 AES, SHA-2/3와 같은 알고리즘에서 검색 복잡도를 감소시켜, 검색 시간을 제곱근으로 줄일 수 있다. 이러한 양자 컴퓨팅의 발전은 암호학 분야에서 암호 알고리즘 및 시스템을 재평가하고 새로운 대응책을 모색할 필요성을 제기한다.

이에 미국 국립표준기술연구소(NIST)는 양자내성암호 공모전을 통해 양자 공격으로부터 안전한 알고리즘인 양자내성암호를 표준화하고 있다. 또한, NIST는 보안 강도 기준을 수립하여 양자 후 암호화 후보를 분류하고 있으며, 이는 양자 공격의 복잡성을 고려하여 회로 크기로 측정된다.

NIST는 레벨 1에서 5까지의 범위에서 양자 후 보안 강도를 정의하였다[3]. 여기서 레벨 1, 3 및 5는 AES-128, AES-192 및 AES-256에 대한 키를 찾는 데 Grover 알고리즘이 필요한 양자 회로 크기에 해당한다. 반면 레벨 2와 4는 SHA-2 및 SHA-3 해시 함수의 충돌 쌍 발견과 관련되며, 이에 대한 양자 회로 크기는 아직 정의되지 않았다. 이 경우에는 고전적인 회로 크기만이 보고되어 있다.

대칭키 암호 AES 그리고 해시 함수 SHA-2/3는 현재 가장 많이 활용되고 있는 대칭키 암호 알고리즘임에 따라, 다양한 최적화 연구들이 존재하며 이는 양자 컴퓨터상에서도 마찬가지이다. 최근 AES와 SHA-2/3에 대한 양자 회로를 구현하고 자원 및 공격 비용을 추정하는 다양한 연구들이 발표되고 있다. 이에 본 논

본 연구는 2024년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (<Q|Crypton>, No.2019-0-00033, 미래컴퓨팅 환경에 대비한 계산 복잡도 기반 암호 안전성 검증 기술개발, 50%) 그리고 본 연구는 2024년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥-센터의 지원을 받아 수행된 연구임 (No.2018-0-00264, IoT 융합형 블록체인 플랫폼 보안 원천기술 연구, 50%).

* 한성대학교 정보컴퓨터공학과 (대학원생, starj1023@gmail.com)
** 한성대학교 융합보안학과 (대학원생, oyj0922@gmail.com)
*** 한성대학교 융합보안학과 (부교수, hwajeong84@gmail.com)

문에서는 AES와 SHA-2/3에 대한 양자 회로 구현 동향에 대해 살펴보고 구현 방법 및 필요 양자 자원들을 분석하고 비교하고자 한다.

Ⅱ. 관련 연구

2.1. 양자 컴퓨팅 및 양자 게이트

양자 컴퓨터의 가장 큰 특징은 Hadamard 게이트를 사용하여 데이터를 중첩 상태로 준비할 수 있다는 것이다. 고전 컴퓨터의 비트는 0 또는 1의 값만을 나타낼 수 있지만, 양자 컴퓨터의 양자 비트에 해당하는 큐비트는 0과 1이 확률적으로 중첩되어 존재할 수 있다. 이러한 특징을 활용하여 양자 컴퓨터는 고전 컴퓨터에서의 특정 난제들을 효율적으로 모델링하고 빠르게 해결할 수 있을 것으로 기대되고 있다. 양자 컴퓨터상에서의 암호 분석의 경우, 대상 암호 알고리즘의 양자 회로 구현물이 기본적으로 필요하다. Shor 그리고 Grover 알고리즘 모두 마찬가지로 해당 암호 알고리즘의 내부 연산 또는 암호화 양자 회로가 필요하다. 암호 알고리즘의 양자 회로의 경우, 고전 NOT, XOR, AND 연산들을 대체할 수 있는 양자 X, CNOT, Toffoli 게이트들을 효율적으로 조합함으로써 구현된다, 이 중에서도 Toffoli 게이트는 양자 컴퓨터상에서 높은 비용을 가지는 양자 게이트에 해당되기 때문에, 최근에는 Toffoli 게이트에 해당하는 양자 자원들을 최적화하는 방향으로 연구들이 다수 발표되고 있다.

2.2. Grover 알고리즘 [2]

Grover 알고리즘은 양자 컴퓨터에서 검색 문제를 빠르게 해결할 수 있는 양자 알고리즘이다. 검색 대상을 양자 중첩 상태로 준비하고, Grover 오라클에서 해당 검색 대상에 대한 솔루션을 찾아낸다. 해당 양자 알고리즘은 고전 컴퓨팅의 전주 소사의 검색 복잡도를 제곱근만큼 감소시킨다. 암호학 분야에서는 k-bit의 비밀 키를 사용하는 암호 알고리즘에 대한 전수조사의 고전 컴퓨팅 복잡도가 $O(2^k)$인 반면, Grover 알고리즘은 제곱근만큼 감소된 $O(\sqrt{2^k})$의 복잡도만을 가진다. 또한 Grover 알고리즘은 해시 함수에서 충돌을 찾는데 활용될 수 있다. 충돌은 서로 다른 입력이 동일한 출력 해시 값을 생성하는 것을 의미하며, Grover 알고리즘을 사용하면 이러한 충돌을 빠르게 찾아내어 해시 함수의 보안 강도를 감소시킬 수 있다. 하지만, 대칭키 암호에 대한 키 전수 조사와 비교하여 해시 함수에 대한 충돌 쌍 공격은 다양한 접근 방법이 존재하며 양자 컴퓨터가 고전 컴퓨터보다 공격 복잡도 측면에서 이점을 가지는지에 대한 논란이 존재한다는 점이 있다.

2.3. NIST 양자 후 보안 강도 표준 [3]

NIST는 AES 및 SHA-2/3에 대한 공격 비용을 기준으로 양자 후 보안 강도를 추정하고, 이를 토대로 표 1과 같은 보안 레벨을 제안하였다. 해시함수 SHA-2/3에 해당하는 레벨 2 및 4에 대한 양자 공격 비용은 아직 정의되지 않았으며, 현재 고전적인 공격 비용만 정의되어 있는 상태이다. [표 1]에 제시되는 양자 공격 비용은 Grover 해킹에 필요한 총 양자 게이트 수와 회로의 depth를 곱하여 계산된다. 초기 2016년 문서에서는 Grassl et al.의 연구 [4]를 바탕으로 AES Grover 키 검색에 대한 추정을 기반으로 레벨 1, 3, 및 5를 정의하였다. 그러나 Grassl et al.의 구현은 최초인 만큼, 현 시점에서 평가해보았을 때 높은 양자 공격 비용이 제시되었다. 최근에는 AES 양자 회로를 개선한 연구들이 많이 발표되고 있는 추세이며, 2022년 최근,NIST는 Jaques et al. 의 연구 [6]의 감소된 양자 공격 비용을 기반으로 레벨 1, 3 및 5를 조정하였다 [3]. 최종적으로, 레벨 1, 3 및 5에서 정의된 Grover 공격 비용은 각각 2^{157}, 2^{221}, 2^{285}이다.

〔표 1〕 NIST 양자 후 보안 레벨

Security	Cipher	Cost (complexity)
Level 1	AES-128	$2^{170} \rightarrow 2^{157}$
Level 2	SHA-256/ SHA3-256	2^{146} classical gates
Level 3	AES-192	$2^{233} \rightarrow 2^{221}$
Level 4	SHA-384/ SHA3-384	2^{210} classical gates
Level 5	AES-256	$2^{198} \rightarrow 2^{285}$

Ⅲ. AES 암호 알고리즘에 대한 양자 회로 최적화 동향

본 장에서는, 네 가지의 AES 양자 회로 구현에 대해 살펴보고 그 특징들을 서술하고자 한다. [표 2]는 네 가지 AES 양자 회로 구현에 사용된 양자 자원들을 보여준다.

〔표 2〕 AES 양자 회로 구현 비용 비교

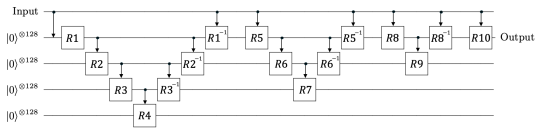
AES	Source	Qubits	Toffoli depth	Full depth
-128	Grassl etal. [4]	984	12,672	110,799
	Zou et al. [5]	512	2,016	-
	Jaques et al. [6]	5,088	114	1,612
	Jang et al. [7]	3,428	40	731
-192	Grassl etal. [4]	1,112	11,088	96,956
	Zou et al. [5]	640	2,022	-
	Jaques et al. [6]	5,664	138	1,936
	Jang et al. [7]	3,847	48	874
-256	Grassl etal. [4]	1,336	14,976	130,929
	Zou et al. [5]	768	2,292	-
	Jaques et al. [6]	6,240	162	2,264
	Jang et al. [7]	4,036	56	1,025

3.1. Grassl et al., Zou et al.의 AES 양자 회로 [4,5]

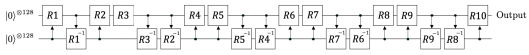
AES 양자 회로는 2016년 Grassl et al.에 의해 최초로 구현되었으며 구현된 양자 회로를 기반으로 Grover 해킹에 필요한 양자 자원들이 추정되었다. 최초의 구현 이였던 만큼 현 시점에서 해당 구현의 양자 회로 효율성을 비교한다면, 매우 비효율적인 구현이 제시되었다고 평가할 수 있다. AES의 양자 회로 구현의 경우, S-Box의 구현 효율성이 전체 양자 회로의 성능에 영향을 크게 끼친다. 해당 연구에서는 S-Box의 내부의 유한체상의 역연산 산술을 양자 회로 상에서 구현하였다. 양자 곱셈과 제곱 연산의 조합으로 구현되었으며, 이는 양자 구현에서 많은 비용을 차지함에 따라 높은 비용의 S-Box가 구현되었다. 하지만, 큐비트의 개수를 줄일 수 있는 [그림 1]의 Zig-zag 아키텍처가 제시되었는데, 해당 아키텍처를 기반으로 하여 현재까지 다양한 개선된 Zig-zag 아키텍처가 제시되고 있다.

Zig-zag 아키텍처는 4, 3, 2 라운드 간격으로 수행했던 라운드의 리버스 연산을 수행한 뒤, 다음 라운드들을 정상적으로 수행한다. 리버스 연산에서는 이전 라운드들에서 사용했던 보조 큐비트들을 초기화시키고, 다음 라운드들에서 해당 보조 큐비트들을 재사용한다. Zig-zag 아키텍처는 이와 같이, 큐비트 사용을 줄일 수 있지만, [그림 1]에서 알 수 있듯 과도한 리버스 연산으로 인해, 회로 Depth와 양자 게이트의 사용이 크게 증가한다.

2020년, Asiacrypt에서 Zou et al.은 Grassl et al.의 Zig-zag 아키텍처를 개선하여 큐비트 수 최적화된 AES 양자 회로 구현을 제시하였다. 기존 Zig-zag 아키텍처는 입력을 포함한 5개의 큐비트 라인을 사용하는 반면, [그림 2]의 개선된 Zig-zag 아키텍처는 입력을 포함하여 2개의 큐비트 라인만을 사용한다. 이는 출력 값으로부터 입력 값을 S-Box 양자 회로를 추가적으로 도입함으로써 달성될 수 있었다. 또한 해당 연구에서는 효율적인 S-Box 구현을 제시하였다. 사실, AES S-Box 양자 회로의 경우, 내부 유한체 역연산을 구현하는 것 보다는 기존 하드웨어를 대상으로 최적화 구현한 연구를 양자 컴퓨터상에서 구현하는 것이 훨씬 효율적이다. Zou et al.은 Boyer-Peralta의 S-Box 최적화 연구를 양자 컴퓨터상에서 구현함과 동시에, Temp 값의 사용을 줄일 수 있도록 수정하여



〔그림 1〕 Zig-Zag 아키텍처 AES 양자 회로 (Grassl et al.)



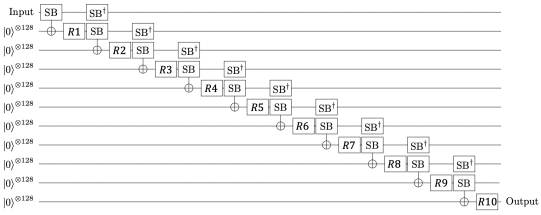
〔그림 2〕 개선된 Zig-Zag 아키텍처 AES 양자 회로 (Zou al.)

필요 큐비트 수를 줄인 양자 S-Box를 사용하여 크게 비용을 감소 시켰다.

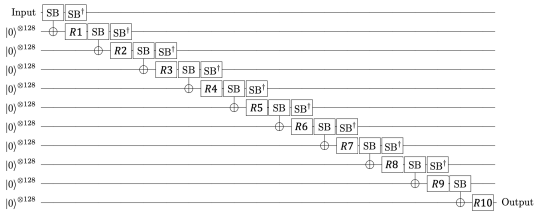
3.2. Jaques et al., Jang et al.의 AES 양자 회로 [6,7]

2020년 Jaques et al.은 Eurocrypt에 Depth 최적화된 AES 양자 회로 구현을 제시하였다. 해당 구현에는 [그림 3]의 기초적인 Pipeline 아키텍처가 제시되었다. Pipeline 아키텍처의 경우, 매 라운드마다 새로운 큐비트 라인을 사용하지만 리버스 연산을 수행하지 않기 때문에 Depth와 양자 게이트 수를 줄일 수 있다. 기존 구현들의 경우, 큐비트 최적화에 과도하게 초점을 맞춘 나머지, 이 외의 양자 자원들이 매우 높은 반면, 해당 연구에서는 큐비트의 사용을 적절히 늘림으로써 높은 성능의 AES 양자 회로 구현을 제시하였다. 해당 AES 양자 회로 구현을 기반으로 추정한 Grover 해킹 비용은 현재 NIST 양자 후 보안 레벨 1, 3, 5로 지정되어 있다.

2022년 Jang et al.은 Jaques et al.의 AES 양자 회로를 한 번 더 개선하여, 매우 높은 구현 성능을 달성하였다. 해당 연구에서는 새로운 S-Box, MixColumn 구현을 제시함과 동시에, [그림 4]의 개선된 Pipeline 아키텍처를 제시하였다. 기존 Pipeline 아키텍처의 경우, 라운드 내 S-Box들을 병렬로 동작시킨 후, 리버스 연산을 통해 S-Box 병렬 동작에 사용된 보조 큐비트들을 초기화시킨 뒤, 다음 라운드에서 재사용하였다. 기존 Pipeline 아키텍처에서는 다음 라운드가 이전 라운드의 S-Box 리버스 연산을 기다리는 오버헤드가 발생하였지만, 개선된 Pipeline 아키텍처에서는



〔그림 3〕 Pipeline 아키텍처 AES 양자 회로 (Jaques al.)



〔그림 4〕 개선된 Pipeline 아키텍처 AES 양자 회로 (Jang et al.)

홀수 라운드와 짝수 라운드를 구분하여 S-Box 병렬 동작을 위한 보조 큐비트들을 할당하였다. 즉 홀수 라운드가 S-Box의 리버스 연산을 수행할 때, 짝수 라운드는 정상적으로 S-Box 연산을 수행한다. 즉, 하나의 보조 큐비트 셋을 추가로 운용함으로써 회로의 완전 병렬성을 달성하였다. 그 결과, 현재 가장 낮은 AES 양자 회로 복잡도를 제공하고 있다. 최근, 2023년, Liu et al.은 개선된 Pipeline 아키텍처에서 활용하는 두 개의 보조 큐비트 셋을 서로 공유하는 기법을 제시함으로써 해당 구현의 결과에서 큐비트 수를 감소시켰다[8]. Jang et al.의 AES 양자 회로는 해당 구현 기법을 도입하고 새로운 S-Box, MixColumn 구현을 적용함으로써 구현 결과를 업데이트 하였다.

Ⅳ. SHA-2/3 해시 알고리즘에 대한 양자 회로 최적화 동향

본 장에서는 총 네 가지의 SHA-2/3 양자 회로 구현에 대해 살펴보고 그 특징들을 살펴보고자 한다. [표 3]은 네 가지 SHA-2/3 양자 회로 구현에 사용된 비용들을 보여준다.

〔표 3〕 SHA-2/3 양자 회로 구현 비용 비교

Hash function	Source	Qubits	Toffoli depth	Full depth
SHA-2	Amy et al. [9]	2,402	57,184	528,768
	Lee et al. [10]	962	4,418	-
SHA-3	Amy et al. [9]	3,200	264	10,128
	Meuli et al. [11]	44,798	24	-

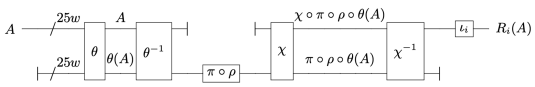
4.1. Amy et al., Lee et al.의 SHA-2 양자 회로 [9,10]

2016년, Amy et al.은 SHA-2/3에 대한 최초의 양자 회로 구현을 제시하였으며, 큐비트 수를 최적화하기 위해 In-place 방식의 SHA-2 양자 회로가 구현되었다. SHA-2의 경우, 키 스케줄 그리고 라운드 함수에 대해 많은 수의 덧셈 연산들이 수행된다. 암호에 대한 양자 회로 구현 시, 양자 덧셈은 많은 양자 자원을 필요로 하는 연산이다. 따라서, SHA-2 양자 회로는 이 많은 덧셈들을 어떠한 방식으로 구현하는지에 따라 양자 회로 성능이 결정되게 된다. 해당 논문에서는 구현 기법이 상세히 설명되어 있지는 않으나, 덧셈에 사용된 많은 보조 큐비트들을 초기화하기 위해 많은 리버스 연산들이 사용되었다. 그 결과, 하나의 라운드 내의 양자 덧셈 critical path가 14로 구현되었다. 최초의 SHA-2 양자 회로 구현인 만큼, 가장 낮은 성능을 제공하고 있다.

2023년, Lee et al.은 양자 덧셈의 critical path를 3으로 최적화함으로써, 매우 높은 SHA-2 양자 회로 성능 개선을 달성하였다. 수행하는 라운드와 다음 라운드덧셈 연산들의 연결성을 세부적으로 분석함으로써, 현 라운드의 일부 덧셈들이 다음 라운드의 덧셈들과 같이 병렬로 실행된다. 이를 위해, 기존 64 라운드가 아닌 65 라운드의 SHA-2 양자 회로 구조를 제시하였다. 총 11개의 덧셈에 대해 3의 critical path만을 달성하였기 때문에 기존 구현에 비해 매우 낮은 Depth 개선을 달성하였으며, 큐비트 개수 또한 훨씬 감소시켰다.

4.2. Amy et al., Meuli et al.의 SHA-3 양자 회로 [9,11]

2016년, Amy et al.은 SHA-2와 같이, SHA-3에 대한 양자 회로 구현 또한 최초로 제시하였다. SHA-2와 동일하게 큐비트 수를 최적화하기 위한 [그림 5]의 In-place 방식의 SHA-3 양자 회로가 구현되었다,



〔그림 5〕 In-place 구조의 SHA-3 양자 회로 (Amy et al.)

SHA-3의 경우, 선형 연산에 해당하는 θ (theta)와 비선형 연산인 χ (chi)를 얼마나 효율적으로 구현하는지에 따라 전체 회로 성능이 결정된다. 해당 구현에서는 θ의 연산 결과를 보조 큐비트 라인에 저장하고, 다시 연산 결과 값에 대한 리버스 θ를 통해, 연산 입력 값을 초기화 시켜 재사용한다. 리버스 θ의 경우, 출력 값에서 입력 값을 생성하는데 있어, 일반 θ보다 훨씬 더 많은 양자 비용이 소모되는 특징이 있다. χ 또한 앞서 초기화한 큐비트를 사용하며, χ의 결과 값과 리버스 χ를 통해, 입력 값을 0으로 초기화시키고 다음 라운드에서 재사용하는 특징이 있다. 그 결과, 총 3200 (=1600+1600)의 큐비트만이 사용되는 In-place 방식의 SHA-3 양자 회로가 구현되었으며, 병렬성이 낮고 많은 양자 게이트가 사용되는 특징이 있다.

Meuli et al.은 SHA-3 양자 회로 구현이 주는 아니지만, 내부 χ 연산에 해당되는 Xor-AND-Graph 연산을 양자 회로상에서 최적화할 수 있는 알고리즘을 제시함과 동시에, SHA-3 양자 회로 구현에 적용한 비용을 추정하였다. 구현 특징으로는, χ 연산을 구현하는데 있어, 많은 보조 큐비트들을 할당하여 모든 Toffoli (AND 연산에 해당) 연산들을 병렬로 수행한다. 또한 리버스 연산을 수행하지 않기 때문에 추가적인 양자 비용이 소모되지는 않지만, 보조 큐비트들이 매 라운드 할당됨으로써 회로 Depth는 낮지만, 매우 높은 큐비트 수의 양자 회로 구현이 제시되었다.

Ⅴ. 결 론

본 논문에서는, 양자 컴퓨터를 통한 AES와 SHA-2/3에 대한 해킹 동향에 대해 살펴보았다. AES에 대한 Grover 해킹 비용의 경우, NIST 양자 후 보안 강도를 추정하기 위한 Level 1, 3, 5에 활용되고 있다. SHA-2/3에 대한 Grover 해킹 비용의 경우, Level 2, 4에 지정되어 있다. AES는 현재 Jaques et al.의 연구 결과를 기반으로 공격 복잡도가 명시되어 있는 반면, SHA-2/3는 아직 구체적인 공격 복잡도가 명시되어 있지 않다. 그 이유는 SHA-2/3 연구의 경우, Grassl et al. Jaques et al.의 논문과는 다르게 구체적인 Grover 공격 비용을 추정하지 않았으며, 해시 함수에 대한 충돌 쌍 공격에 대한 Grover 공격을 명확하게 정의하고 추정하는데 어려움이 있기 때문이다. SHA-2/3에 대한 Grover 충돌 쌍 공격을 어떻게

정의하고 추정할지, 그리고 양자 회로 구현의 최적화 결과물에 따라 새로운 기준이 정립될 수 있을 것으로 사료된다. AES 또한 새로운 양자 회로 최적화 결과가 발표되어 복잡도가 감소될 수 있는지에 대해서도 지속적으로 살펴보아야 할 것이다.

참 고 문 헌

[1] P. W. Shor, “Polynomial-Time Algorithmsfor Prime Factorization and Discrete Logarithms on a Quantum Computer” *SIAMreview*, Vol. 41. No. 2. 303-332. 1999.

[2] L.K. Grover, “A fast quantum mechanical algorithm for database search,” *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pp. 212–219, 1996.

[3] NIST, “Submission requirements and evaluation criteria for the post-quantum cryptography standardization process,” [internet], https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf.

[4] M. Grassl, B. Langenberg, M. Roetteler, and R. Steinwandt, “Applying Grover’s algorithm to AES: quantum resource estimates,” Post-Quantum Cryptography, *PQCrypto'16*, LNCS, 9606, pp. 29–43, 2016.

[5] J. Zou, Z. Wei, S. Sun, X. Liu, and W. Wu, “Quantum circuit implementations of AES with fewer qubits,” *International Conference on the Theory and Application of Cryptology and Information Security*, Springer, pp. 697-726, 2020.

[6] S. Jaques, M. Naehrig, M. Roetteler, and F. Virdia, “Implementing Grover oracles for quantum key search on AES and LowMC.” *Annual International Conference on the Theory and Applications of Cryptographic Techniques,* Springer, pp. 280–310, 2020.

[7] K. Jang, A. Baksi, H. Kim, G. Song, H. Seo, and A. Chattopadhyay “Quantum analysis of AES,” *Cryptology ePrint Archive*, Report 2022/683, 2022.

[8] Q. Liu, B. Preneel, Z. Zhao, and M. Wang, “Improved Quantum Circuits for AES: Reducing the Depth and the Number of Qubits,” *International Conference on the Theory and Application of Cryptology and Information Security*, Springer, pp. 67-98, 2023.

[9] M. Amy, O. Di Matteo, V. Gheorghiu, M. Mosca, A. Parent, and J. Schanck, “Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3,” *International Conference on Selected Areas in Cryptography*, Springer, pp. 317-337, 2016.

[10] J. Lee, S. Lee, YS. Lee, and D. Choi, “T depth reduction method for efficient SHA 256 quantum circuit construction,” *IET Information Security*, Vol. 17, No, 1, pp. 46-65, 2023.

[11] G. Meuli, M. Soeken, and G. D. Micheli, “Xor-and-inverter graphs for quantum compilation,” *npj Quantum Information*, Vol. 8, No. 1, 2022.

〈저 자 소 개〉

장 경 배 (Kyungbae Jang)

2019년 2월 : 한성대학교 IT응용시스템공학과 공학 학사
2021년 2월 : 한성대학교 IT융합공학과 석사과정
2021년 3월~현재 : 한성대학교 IT융합공학과 박사과정
<관심분야> 양자 컴퓨터, 정보보안

오 유 진 (Yujin Oh)

학생회원

2023년 2월 : 한성대학교 IT융합공학부 공학 학사
2023년 3월~현재 : 한성대학교 융합보안학과 석사과정
<관심분야> 양자 컴퓨터, 암호구현

서 화 정 (Hwa-Jeong Seo)

종신회원

2010년 2월 : 부산대학교 컴퓨터공학과 학사

2012년 2월 : 부산대학교 컴퓨터공학과 석사

2016년 1월 : 부산대학교 컴퓨터공학과 박사

2016년 1월~2017년 3월 : 싱가포르 과학기술청

2017년 4월~2023년 2월 : 한성대학교 IT 융합공학부 조교수

2023년 3월~현재 : 한성대학교 융합보안학과 부교수

<관심분야> 암호구현