석사학위논문

ASCON 양자 구현 및 분석

ASCON 양자 회로 depth 최적 구현 및 분석

2024년

한성대학교 일반대학원

융합보안학과

융합보안전공

오 유 진

석사학위논문
지도교수 서화정

ASCON 양자 구현 및 분석

ASCON 양자 회로 depth 최적 구현 및 분석

Quantum Implementation and Analysis of ASCON

2024년 12월 10일

한성대학교 일반대학원

융 합 보 안 학 과

융 합 보 안 전 공

오 유 진

석사학위논문
지도교수 서화정

ASCON 양자 구현 및 분석

ASCON 양자 회로 depth 최적 구현 및 분석

Quantum Implementation and Analysis of ASCON

위 논문을 공학 석사학위 논문으로 제출함

2024년 12월 10일

한성대학교 일반대학원

융 합 보 안 학 과

융 합 보 안 전 공

오 유 진

오유진의 공학 석사학위 논문을 인준함

2024년 12월 10일

심사위원장 _____(인)

심 사 위 원 _____(인)

심 사 위 원 _____(인)

심 사 위 원 _____(인)

국 문 초 록

ASCON 양자 구현 및 분석

한 성 대 학 교 일 반 대 학 원
융 합 보 안 학 과
융 합 보 안 전 공
오 유 진

양자 컴퓨팅의 발전은 암호분야에서 보안 문제를 제기한다. 특히, Grover 알고리즘은 대칭 키 암호 및 해시 함수의 검색 복잡도 감소에 영향을 미치며, 최근 Grover 검색 복잡도를 추정하고 양자 후 보안을 평가하기 위한 연구가 이루어지고 있다. 본 논문에서는 NIST(국립표준기술연구소)의 경량 암호화 표준화의 일환으로, 대칭 키 암호화와 해시 함수를 모두 포함한 ASCON 양자 회로 구현 및 분석을 제안한다. 이전 연구와 비교하였을 때, ASCON-HASH의 양자 회로 구현은 Toffoli-depth 88.9%, 전체 회로 depth 80.5% 향상시켰다.

본 논문은 ASCON에 대한 depth 최적화된 양자 회로와 최적의 Grover 검색 비용을 제시한다. 또한, 관련 평가 기준과 최신 연구 동향을 바탕으로 ASCON의 양자 내성 보안 강도를 평가하기 위한 비용을 추정한다.

목 차

표 목 차

그 림 목 차

수 식 목 차

알 고 리 즘 목 차

제 1 장 서 론

양자 컴퓨터는 빠른 계산 속도와 향상된 처리 성능을 제공하며, 양자 상태의 특성을 활용해 암호화 문제를 효과적으로 해결할 수 있다. 고전 컴퓨터는 이진법을 사용하여 데이터를 0과 1로 처리하는 반면, 양자 컴퓨터는 중첩(superposition)과 얽힘(entanglement)을 활용하여 데이터를 처리한다. 양자 컴퓨터에서 기본 단위는 큐비트로, 고전 컴퓨터의 비트와 유사하지만 비트는 항상 0 또는 1의 상태를 가지는 반면 큐비트는 0과 1의 두 상태가 동시에 공존할 수 있다. 이러한 공존 상태를 중첩 상태라고 한다. 또한, 얽힘은 두 개 이상의 큐비트가 연결되어 있어, 한 큐비트의 상태가 다른 큐비트의 상태에 영향을 미치는 것을 말한다. 즉, 얽힘 관계에 있는 큐비트는 서로 멀리 떨어져 있어도 한 큐비트의 상태가 결정되면 다른 큐비트의 상태도 즉시 결정된다. 이로 인해 양자 컴퓨터는 복잡한 문제를 병렬적으로 처리하는데 성능이 뛰어나다.

하지만 이러한 이점은 기존 암호 시스템에 잠재적인 위협이 될 수 있으며, 암호 기술의 보안성을 재평가할 필요성을 제기한다. 이에 대응하기 위한 주요 과제 중 하나는 양자 내성 암호화의 필요성을 다루는 미국 국립표준기술연구소 (National Institute of Standards and Technology, NIST)의 양자 내성 암호 (Post-Quantum Cryptography, PQC) 표준화 프로세스이다. 이러한 필요성은 Shor 알고리즘이 인수분해와 이산 대수 문제를 효율적으로 해결할 수 있다는 점에서 비롯되었다.

암호와 관련된 또 다른 중요한 양자 알고리즘은 Grover 알고리즘이다. Grover 알고리즘은 데이터 검색을 가속화하여 대칭 키 암호의 검색 복잡도를 줄일 수 있다. 그러나 Grover 알고리즘이 보안 강도를 크게 낮출 수는 있으나 실제로 공격을 수행하기 위해서는 상당히 큰 규모의 양자 회로가 필요하다. 양자 공격은 필요한 양자 회로 크기에 따라 암호 알고리즘의 보안을 다르게 평가할 수 있음을 제시한다. 이러한 측면은 NIST의 양자 암호화 문서에서 다루고 있으며, 잠재적인 양자 공격에 필요한 양자 비용을 고려해 양자 후 보

안 강도를 평가한다. NIST는 AES-128, AES-192, AES-256에 대한 Grover 공격 비용을 추정하여 양자 후 보안 강도를 설정하였으며, 이 비용은 대상 암호 알고리즘에 대한 양자 회로 구현의 효율성에 따라 달라진다.

본 논문에서는 NIST 경량 암호 표준으로 선정된 ASCON AEAD 및 해시 함수에 최적화된 양자 회로를 제안한다. 본 연구의 주요 목표는 합리적인 수의 큐비트를 유지하면서 ASCON 양자 회로의 depth를 줄이는 것으로, 이는 Grover 공격 비용을 감소시키는 효율적인 접근법이다. 양자 회로의 depth는 회로 실행 시간에 직접적인 영향을 미치며, Grover 알고리즘은 검색 복잡도를 제곱근으로 줄일 수 있지만, 여전히 양자 회로 내에서 상당한 비용이 요구된다. 이러한 이유로 Grover 알고리즘을 통한 키 검색은 시간 소모적인 과정이 되며, NIST는 보안 평가 시 이러한 요소를 고려하고 있다. 따라서 대칭키 암호의 depth를 최소화하는 것은 Grover 공격 비용을 줄이기 위한 최적의 전략으로 간주된다. 본 논문에서는 제안된 ASCON 양자 회로를 바탕으로 Grover 공격 비용을 추정하고, NIST 기준에 따라 ASCON의 양자 후 보안 강도를 평가한다.

본 논문의 구성은 다음과 같다. 2장에서는 ASCON 양자 회로 구현을 위한 배경 지식에 대해 설명한다. 3장에서는 제안하는 ASCON 양자 회로 구현 기법에 대해 설명한다. 4장에서는 ASCON 양자 회로에 대한 양자 자원 비용과 Grover 공격 비용을 제시하고 양자 보안 강도를 평가한다. 마지막으로 5장에서는 결론과 향후 연구 방향에 대해 설명하며 마무리한다.

제 1 절 연구 기여

본 논문의 주요 기여는 다음과 같다. 첫째, ASCON-AEAD 및 해시 함수의 모든 파라미터에 대한 양자 회로를 구현한다. 둘째, 최적화된 ASCON 해시 함수의 양자 회로를 개선하고 이를 기존 연구와 비교한다. 본 논문의 주요 초점은 ASCON 양자 회로의 낮은 Toffoli-depth와 Full-depth를 달성하는 것이다. 이를 위해 병렬화, AND 게이트 등 다양한 최적화 기법을 활용하여 depth를 최소화하며, 합리적인 큐비트 수를 유지하기 위해 보조 큐비트를 재

사용하는 방법을 채택한다. 마지막으로, 구현된 ASCON 양자 회로를 바탕으로 Grover 공격 비용을 추정하여 ASCON 양자 내성 보안 강도를 평가한다. 해당 평가에서는 ASCON 양자 회로에 대해 추정된 Grover 검색 비용과 NIST에서 정의한 보안 레벨을 비교한다.

제 2 장 관련 연구

제 1 절 ASCON

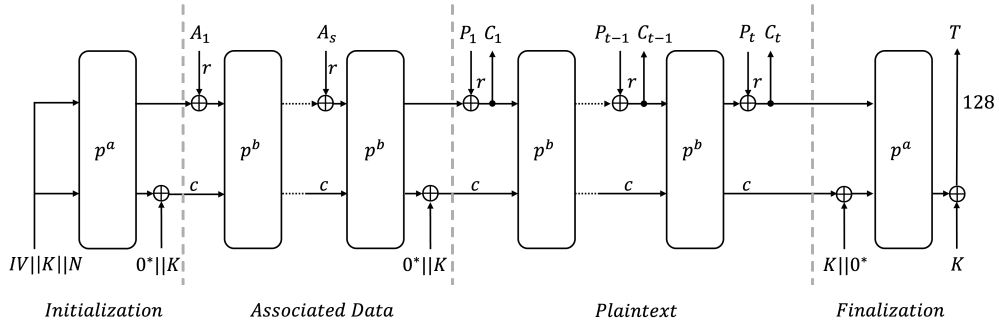
ASCON은 NIST 경량 암호 표준화에서 선정된 경량 암호 알고리즘이다. ASCON은 연관 데이터로 인증된 암호화 모드 (Authenticated Encryption with Associated Data, AEAD), 해시 함수, 그리고 양자 키 검색 공격에 대한 내성을 위해 설계된 변형인 Ascon-80pq로 구성된다.

ASCON은 ASCON-128과 ASCON-128a 두 가지 AEAD 모드를 제공한다. ASCON-128과 ASCON-128a의 파라미터는 [표 2-1]에 나와 있으며, 두 파라미터는 순열 함수 (p^b)의 라운드 수와 블록 사이즈만 다르다.

Name	Algorithms	Bit size				Rounds	
		Key	Nonce	Tag	block	p^a	p^b
ASCON-128	$\varepsilon, D_{128,64,12,6}$	128	128	128	64	12	6
ASCON-128a	$\varepsilon, D_{128,128,12,8}$	128	128	128	128	12	8

[표 2-1] ASCON AEAD 보안 파라미터

ASCON AEAD의 암호화 과정은 Initialization, Associated Data, Plaintext, Finalization 단계로 구성되며 [그림 2-1]과 같다.



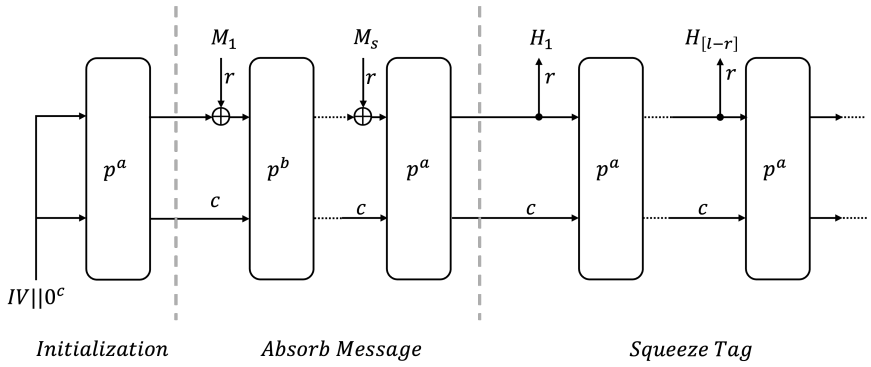
[그림 2-1] ASCON AEAD 암호화 과정

해시 함수의 경우, ASCON-HASH와 ASCON-XoF 두 가지 모드를 제공하며, 보안 파라미터는 [표 2-2]와 같다. ASCON-HASH는 해시 값이 256 비트이며 XoF는 임의의 길이를 가진다.

Name	Algorithms	Bit size		Rounds
		Hash	block	p^a
ASCON-Hash	$\chi_{256,64,12}$ with $l=256$	256	64	12
ASCON-XoF	$\chi_{0,64,12}$ with arbitrary l	l	64	12

[표 2-2] ASCON 해시함수 보안 파라미터

ASCON 해시 함수 암호화 과정은 Initialization, Absorb Message, Squeeze Tag로 구성되며 [그림 2-2]와 같다.



[그림 2-2] ASCON 해시함수 암호화 과정

모든 ASCON 체계에서 공통적으로 포함된 주요 구성 요소는 서로 다른 라운드 수(p^a 및 p^b)로 설정된 두 개의 320비트 순열이다. 계산을 위해 320비트는 다섯 개의 64비트 레지스터 워드 x_i로 나뉜다 ($S=x_0 \| x_1 \| x_2 \| x_3 \| x_4$, x_0는 최상위 워드, x_4는 최하위 워드). 순열 함수는 상수 덧셈, 5비트 S-box를 사용하는 치환 레이어, 그리고 64비트 확산 함수를 사용하는 선형 레이어로

구성된다.

제 2 절 양자 알고리즘과 양자 공격

1) Grover 알고리즘

Grover 알고리즘은 암호 해독 및 검색 문제를 효율적으로 해결할 수 있다. k-비트 키를 사용하는 암호 알고리즘의 경우, 고전적인 컴퓨터의 검색 복잡도는 $O(2^k)$인 반면, Grover 알고리즘의 검색 복잡도는 $O(2^{k/2})$로 감소한다. Grover 알고리즘은 총 세 단계로 이루어진다. 먼저 [수식 2-1]과 같이 하다마드 게이트를 사용하여 k-큐비트 키를 중첩 상태로 만든다. 이는 2^k개의 모든 키가 동일한 진폭을 갖게 한다.

$$H^{\otimes k}|0\rangle^{\otimes k} = |\psi\rangle = (\frac{|0\rangle + |1\rangle}{\sqrt{2}}) = \frac{1}{2^{k/2}} \sum_{x=0}^{2^k-1} |x\rangle$$

[수식 2-1] Grover 알고리즘 입력설정

다음은 오라클 단계이다. 오라클에서 해당 암호 알고리즘은 이전 단계에서 준비된 중첩상태의 키를 사용하여 알려진 평문을 중첩 상태에서 암호화하는 양자 회로로 구현된다. 이 과정에서 모든 가능한 키 값에 대한 암호문이 생성된다. 생성된 암호문(실제로는 중첩 상태의 하나의 암호문)은 알려진 암호문과 비교되며, 만약 일치하는 경우(즉, [수식 2-2]에서 f(x) = 1인 경우) 키 값의 부호가 반전된다 (즉, [수식 2-3]에서 $(-1)^{f(x)}$). 마지막으로, 구현된 양자 회로는 다음 반복을 위해 역연산되어 생성된 암호문을 알려진 평문으로 다시 변환한다.

$$f(x) = \begin{cases} 1 \text{ if } Enc_{key}(p) = c \\ 0 \text{ if } Enc_{key}(p) \neq c \end{cases}$$

[수식 2-2] Grover 오라클 연산자 1

$$U_f(|\psi\rangle|-\rangle) = \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle|-\rangle$$

[수식 2-3] Grover 오라클 연산자 2

오라클 단계 이후 확산 연산자는 오라클에서 반환된 솔루션 키의 진폭 (즉, 확률)을 증폭시킨다. 오라클은 부호를 변경하여 솔루션 키를 반환한다. 확산 연산자는 쉽게 구현될 수 있으며, 확산 연산자의 복잡도는 오라클에 비해 사소하기 때문에 일반적으로 Grover 공격 비용 추정에서는 무시된다. Grover 알고리즘은 솔루션 키의 진폭을 증폭하기 위해 오라클과 확산 연산을 수차례 반복 수행하며(약 $\sqrt{2^k}$ 번), 이를 통해 솔루션 키의 확률을 증가시킨다.

2) Grover 알고리즘을 이용한 양자 충돌 공격

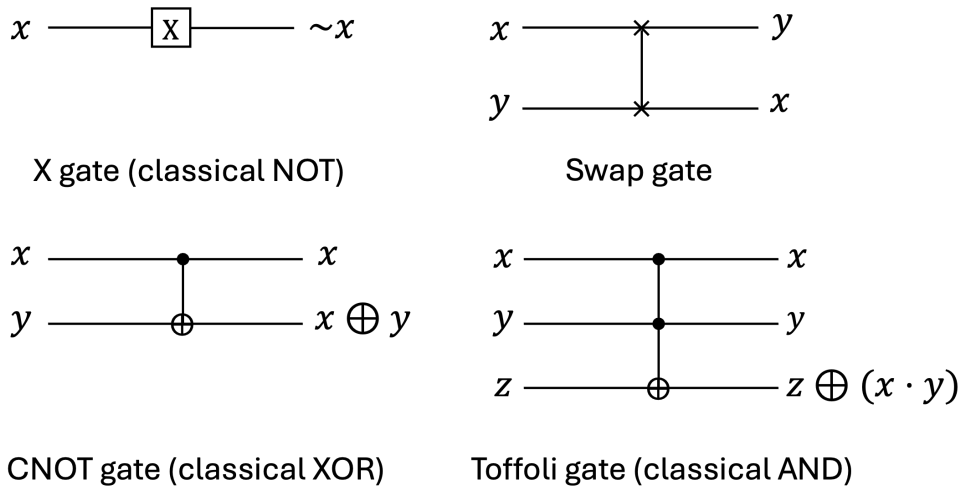
Grover 알고리즘은 블록 암호의 k-비트 키 또는 해시 함수의 n-비트 해시 출력의 프리이미지를 찾는 데 있어 간단하게 접근할 수 있다. 이는 고전 컴퓨터에서 검색 복잡도가 $O(n)$인 반면, 양자 컴퓨터에서는 $O(\sqrt{n})$으로 줄어들기 때문이다. 그러나 해시 함수에 대한 양자 충돌 검색은 더 복잡하며 여러 가지 방법으로 접근할 수 있다.

현재, Grover의 알고리즘을 사용하는 다양한 양자 충돌 공격 알고리즘이 존재한다. 그 중 BHT 알고리즘은 복잡도가 $O(2^{n/3})$이다. 그러나 이 알고리즘은 상당히 큰 양자 메모리 ($O(2^{2n/3})$) 를 요구한다. 또한 Bernstein은 이 알고리즘이 논란의 여지가 있다고 지적하였다. 이러한 측면을 고려하여, 본 논문에서는 검색 복잡도가 $O(2^{2n/5})$이면서 $O(2^{n/5})$의 고전 메모리가 필요한 CNS 알고리즘을 채택한다. CNS 알고리즘은 검색 복잡도를 $O(2^{n/5})$으로 줄이기 위해 병렬화를 할 수 있다. 2^s개의 양자 인스턴스를 병렬로 활용함으로써, 충돌 검색 복잡도는 $O(2^{2n/5-3s/5})$로 줄어든다 ($s \leq n/4$). Jang et al. 은 SHA-2 및 SHA-3 해시 함수에서 충돌 공격에 필요한 양자 자원을 추정하기 위해 $s = n/6$로 정의하였다. 이 접근 방식을 따라, ASCON 해시 함수에서 충돌을

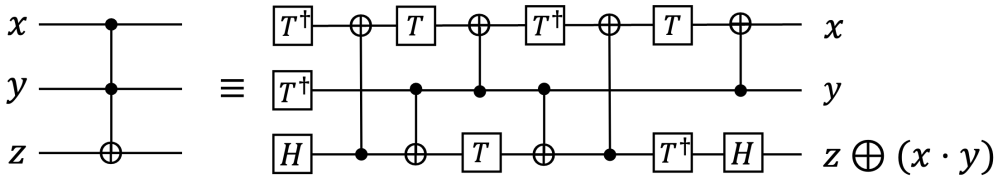
찾기 위해 $s=n/6$ 로 정의한다.

제 3 절 양자 게이트

본 절에서는 양자 회로를 구현하기 위한 양자 게이트를 설명한다. [그림 2-3]은 양자 회로 구현 시 자주 사용되는 게이트를 보여준다. X 게이트는 Pauli-X 게이트라고도 하며, 단일 큐비트에 작용한다. 이 게이트는 큐비트의 상태를 반전시켜 |0〉 상태를 |1〉로, |1〉 상태를 |0〉으로 변환한다. 이 연산은 고전 컴퓨터에서의 NOT 연산과 유사하다. Swap 게이트는 두 대상 큐비트의 상태를 교환한다. CNOT(Controlled-NOT) 게이트는 한 개의 제어 큐비트와 한 개의 대상 큐비트를 사용하며, 제어 큐비트가 |1〉 인 경우, 대상 큐비트에 NOT 연산을 수행한다. 제어 큐비트가 |0〉 인 경우, 대상 큐비트는 변화가 없다. 이는 고전 컴퓨터의 XOR 연산과 유사하다. Toffoli 게이트, 즉 CCNOT 게이트(Controlled-Controlled-NOT)는 두 개의 제어 큐비트와 하나의 대상 큐비트를 사용한다. Toffoli 게이트는 두 개의 제어 큐비트가 모두 |1〉 일 때만 대상 큐비트에 NOT 연산을 수행한다. 따라서 이는 고전컴퓨터의 AND 연산과 유사하다. 또한, [그림 2-4]와 같이 Toffoli 게이트는 H, CNOT 및 T 게이트와 같은 게이트의 조합으로 분해될 수 있다.



[그림 2-3] 양자 게이트



[그림 2-4] Toffoli 게이트 분해

제 4 절 NIST 보안 레벨

NIST는 양자 공격에 대한 양자 후 보안 레벨을 제공하며, 본 논문에서는 구현 평가 시 이를 참고한다. NIST는 AES 및 SHA-2/3 제품군에 대해 각각 Grover 키 검색과 충돌 검색 복잡도를 기반으로 보안 레벨을 정의하였으며, [표 2-3]은 해당 보안 레벨을 보여준다. 보안 레벨 1, 3, 5는 AES에 대한 Grover 키 검색의 복잡도에 해당하며, 레벨 2, 4는 SHA-2/3에 대한 충돌 검색 복잡도에 해당한다. 그러나 레벨 2, 4의 경우 양자 공격 비용은 아직 정의되지 않았으며, 고전적인 공격 비용만 정의되어있다.

보안 레벨	암호	비용(복잡도)
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	$2^{198} \rightarrow 2^{285}$

[표 2-3] NIST 양자 후 보안 레벨

Grover 알고리즘은 대칭 키 암호에 대한 주요 양자 공격 중 하나이며, NIST도 이를 고려하고 있다. 보안 레벨 1, 3, 5에서의 공격 복잡도는 각각 AES-128, 192, 256에 적용된 Grover의 키 검색 비용에 따라 달라진다. 이 비용은 Grover 키 검색 회로의 전체 게이트 수 × depth로 결정된다. NIST는 Grassl이 구현한 AES 양자 회로를 바탕으로 레벨 1, 3, 5에 대한 비용을 각각 2^{170}, 2^{233}, 2^{298}로 추정하였다. 그러나 최근 AES 양자 회로를 최적화하기 위한 다양한 연구가 진행되고 있으며, 특히 Jaques는 Eurocrypt 2020에서 AES의 depth 최적화된 양자 회로를 소개하여 AES에 대한 Grover 키 검색 비용을 감소시켰다. 따라서 NIST는 AES 제품군에 대한 Grover 키 검색 비용을 해당 연구 결과를 바탕으로 각각 2^{157}, 2^{221}, 2^{285}로 조정하였다.

보안 레벨 2, 4의 경우, NIST에서는 SHA-2 및 SHA-3 해시 함수 충돌 공격에 대한 양자 공격 비용은 아직 정의되지 않았다. 그러나 Jang et al.은 SHA-2/3 해시 함수 충돌 공격에 대한 레벨 2와 4에 대해 제안하였다. 이에 따라 본 논문에서는 Jang et al.이 제안한 보안 레벨과 함께 비교한다. Jang et al. 이 제안한 보안 레벨은 [표 2-4]와 같다.

Level	Cipher	Cost
Level 2	SHA-2/3 (256)	$2^{188}/2^{183}$
Level 4	SHA-2/3 (384)	$2^{266}/2^{260}$
Level 6 (Extension)	SHA-2/3 (512)	$2^{343}/2^{337}$

[표 2-4] Jang et al.이 정의한 양자 충돌 공격에 대한 보안 레벨

또한, NIST에서 정의한 MAXDEPTH를 고려해야 한다. MAXDEPTH는

양자 컴퓨터에서 실행 가능한 최대 회로 depth를 나타낸다. NIST는 양자 공격의 detph 제한(즉, MAXDEPTH)을 $2^{40} < 2^{64} < 2^{96}$과 같은 범위로 분류한다. 이는 회로의 depth가 너무 크면, Grover 알고리즘과 같은 양자 공격이 실용적으로 어려워질 수 있다는 점을 반영한다. 만약 지정된 depth 제한을 초과하게 된다면, Grover 검색을 병렬화하는 방안을 고려할 수 있다 .

Grover 알고리즘의 병렬화에 따라 양자 회로의 trade-off 메트릭이 회로 depth의 제곱으로 변경된다. 간단히 말해, 큐비트 수 × 회로 depth 메트릭은 큐비트 수 × 회로 depth의 제곱으로 대체된다. 본 논문에서는 큐비트 수, 전체 depth, Toffoli-depth, T-depth를 각각 M, FD, TD, Td로 표기한다. 또한, 양자 회로 평가를 위해 $FD-M, TD-M, Td-M$ 메트릭을 추정하며 Grover 병렬화에 대한 변경된 trade-off 메트릭 (FD^2-M, TD^2-M, Td^2-M)도 추정한다.

제 3 장 제안 기법

본 장에서는 ASCON AEAD와 ASCON 해시함수 양자 구현에 대해 설명한다. 특히, ASCON-128과 ASCON-HASH (256비트)를 예로 들어 설명한다.

Grover 알고리즘에서 최적의 성능을 위해 depth를 최소화하는 것을 우선시하는 설계 철학에 따라 ASCON-128 및 ASCON-HASH 양자 회로의 depth를 최적화하는 동시에 합리적인 수의 큐비트를 보장하는 데 중점을 둔다.

제 1 절 S-box 최적화

1) 병렬 구현을 통한 최적화

look-up 테이블 방식은 고전 컴퓨터에서 S-box를 구현할 때 흔히 사용되지만, 양자 컴퓨터에서는 연산의 가역적 특성 때문에 look-up 테이블을 사용할 수 없다. 또한, 주어진 문제의 구현을 찾는 양자 전용 도구들이 존재하지만, 해당 도구들은 5비트 S-box에서 작동하지 않는다. 따라서 S-box 양자 회로는 양자 게이트를 사용하여 부울 표현식을 기반으로 구현해야 한다.

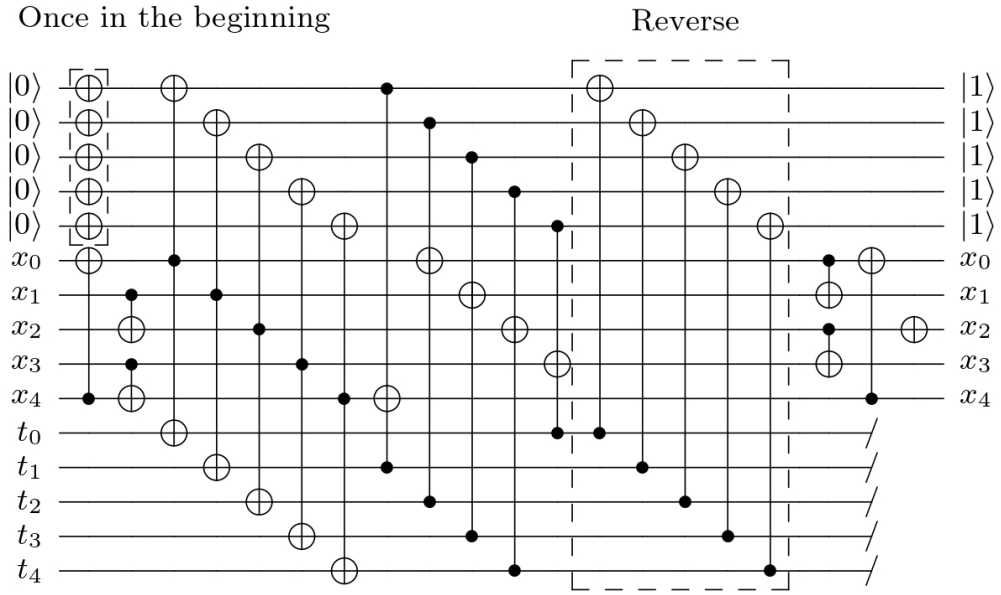
ASCON 양자 회로에서 S-box 구현은 가장 많은 자원을 요구한다. 5비트 ASCON S-박스는 [수식 3-1]과 같이 NOT (~) AND (·), 및 XOR (⊕) 게이트를 포함한 부울 연산을 통해 구현할 수 있다.

$$
\begin{aligned}
&x_0 = x_0 \oplus x_4,\ x_4 = x_4 \oplus x_3,\ x_2 = x_2 \oplus x_1 \\
&t_0 = x_0,\ t_1 = x_1,\ t_2 = x_2,\ t_3 = x_3,\ t_4 = x_4, \\
&t_0 = \sim t_0,\ t_1 = \sim t_1,\ t_2 = \sim t_2,\ t_3 = \sim t_3,\ t_4 = \sim t_4, \\
&t_0 = t_0 \cdot x_1,\ t_1 = t_1 \cdot x_2,\ t_2 = t_2 \cdot x_3,\ t_3 = t_3 \cdot x_4,\ t_4 = t_4 \cdot x_0, \\
&x_0 = x_0 \oplus t_1,\ x_1 = x_1 \oplus t_2,\ x_2 = x_2 \oplus t_3,\ x_3 = x_3 \oplus t_4,\ x_4 = x_4 \oplus t_0, \\
&x_1 = x_1 \oplus x_0,\ x_0 = x_0 \oplus x_4,\ x_3 = x_3 \oplus x_2,\ x_2 = \sim x_2
\end{aligned}
$$

[수식 3-1] ASCON S-box

이전 연구에서는 큐비트 수를 줄이기 위해 선형 레이어의 보조 큐비트를 활용하였다. 요약하자면, 치환 레이어와 선형 레이어는 보조 큐비트를 공유하며, 선형 레이어는 치환 레이어의 결과를 부분적으로 사용한다. 결과를 활용한 후, 치환 레이어에서 수행된 연산의 역연산을 통해 큐비트를 재사용한다. 이 아키텍처는 큐비트 수를 절약할 수 있지만, Toffoli 연산을 포함한 여러 번의 복잡한 역연산으로 인해 회로 depth가 증가하는 단점이 있다. 반면, 본 논문에서 제안된 접근 방식은 치환 레이어와 선형 레이어를 독립적으로 구현하여, 복잡한 역연산을 수행하지 않아도 된다. 비록 이전 연구보다 더 많은 큐비트를 사용하지만, 회로 depth를 크게 줄여 시간-공간 복잡성 측면에서 최적의 절충 성능을 달성할 수 있다.

수식 [3-1]을 보면 AND 연산과 XOR 연산을 결합해 중간 매개 변수를 계산하려면 보조 큐비트 t_0부터 t_4까지 총 5개가 필요하다. 따라서 각 S-box에 5개의 보조 큐비트를 할당해야 하며, 치환 레이어에서 총 64개의 S-box가 사용되므로, 매 라운드에서 치환 레이어를 실행할 때 총 320개(5 × 64)의 보조 큐비트가 필요하다. 그러나 이 경우, AND 연산을 위해 Toffoli 게이트가 순차적으로 실행되므로 Toffoli-depth가 증가하는 문제가 발생한다. 이를 해결하기 위해 본 논문에서는 Toffoli-depth를 1로 줄여 최적화하는 ASCON S-box 양자 회로를 제안한다.



[그림 3-1] ASCON S-box 양자 회로 (Toffoli depth 1)

그림 [3-1]은 ASCON S-box에 대해 제안된 양자 회로를 나타낸다. 이 회로에서는 보조 큐비트 세트를 추가적으로 할당하고, 해당 보조 큐비트를 역연산을 통해 반복적으로 재사용한다. 보조 큐비트 세트를 활용함으로써, Toffoli 게이트의 피연산자를 독립적으로 준비할 수 있게 된다. 그림 [3-1]과 같이, 모든 Toffoli 게이트는 병렬로 작동하여 Toffoli-depth를 1로 달성할 수 있다.

모든 Toffoli 게이트를 병렬로 연산하기 위해서는, t_0부터 t_4까지 할당된 320개의 큐비트와 마찬가지로 추가적으로 320개의 큐비트를 할당해야 한다. 그러나 큐비트 수는 양자 회로 최적화에서 매우 중요한 지표이다. 이를 고려하여, 역연산을 통해 사용된 보조 큐비트를 재사용함으로써 큐비트 수 증가로 인한 오버헤드를 효과적으로 해결할 수 있다. 이러한 최적화는 다음 제 3장 1절 2)에서 설명한다.

2) 역연산을 통한 보조 큐비트 재사용

치환 레이어 내에서 Toffoli 게이트를 병렬화한 결과, Toffoli-depth는 1

이 된다. 그러나 각 라운드마다 보조 큐비트 세트를 할당하면 큐비트 수 측면에서 높은 오버헤드가 발생한다. 양자 회로를 최적화하는 데 있어 depth 이외에도 큐비트 수는 중요한 지표이다. 이러한 오버헤드를 줄이기 위해 보조 큐비트 세트를 처음에 한 번만 할당한 후, 전체 과정에서 재사용한다.

이 경우, 보조 큐비트 세트를 재사용하기 때문에 치환 레이어의 각 라운드마다 새로운 보조 큐비트 세트를 할당할 필요가 없으며, 초기에 320개의 보조 큐비트만 할당하면 된다. 보조 큐비트 세트를 재사용하기 위해, Toffoli 게이트 연산 후 역연산을 수행한다 ([그림 3-1] 참조). 역연산 과정에서 CNOT 게이트의 수가 증가하지만, 이 역연산은 다른 연산의 양자 게이트와 동시에 수행되기 때문에 depth에 영향을 미치지 않는다. 또한, 역연산에서 X 게이트 연산은 생략한다. 보조 큐비트를 $|0\rangle$로 초기화하는 대신, X 게이트 연산을 생략하여 보조 큐비트를 반전 상태(즉, $|1\rangle$)로 남겨둔다. 이러한 방식은 다음 라운드에서 X 게이트 연산을 생략시켜 게이트 수를 줄인다. 구체적으로, 초기 라운드에서만 X 게이트 (NOT 연산)를 적용하고 역연산에서는 이를 생략함으로써 이후 라운드에서는 더 이상 X 게이트 (NOT 연산) 연산이 필요하지 않는다. 그 결과, 단일 치환 레이어에서 640(=320 × 2)개의 보조 큐비트를 사용하며, 추가적인 X 게이트 없이 320개의 보조 큐비트를 재사용한다.

요약하자면, 초기 보조 큐비트 세트 할당에 따른 오버헤드를 수용하고, 양자 게이트 수의 약간의 증가를 감수함으로써 Toffoli 게이트의 depth와 전체 회로 depth를 줄이는 이점을 얻을 수 있다. [표 3-1]에서는 이전 연구와 비교하여 ASCON S-box 양자 비용을 보여준다. 또한, 본 논문에서는 Stoffelen et al. 및 Lu et al. 의 ASCON 구현을 고전 컴퓨팅 환경에서 연구하고 이를 양자 회로에 적용한 결과를 조사하였으며, [표 3-1]에서 확인할 수 있다.

Operation	Source	#CNOT	#1qCliff	#T	Toffoli depth	#Qubit (Reuse)	Full depth
Substitution	Stoffelen	4608	918	2240	2	1600	24
	Ours	**3264**	**1174**	**2240**	**1**	**960(320)**	**15**
	Luo	16,640	7808	15,680	7	5760	94
Substitution +Linear	LEE	4544	2070	3584	8	640	80
	Ours	**4224**	**1174**	**2240**	**1**	**1280(320)**	**18**
Linear	**Ours**	**960**	**0**	**0**	**0**	**640**	**3**

[표 3-1] ASCON 치환 레이어 양자 자원 비용 비교

제 2 절 선형 레이어 최적화

ASCON 선형 레이어는 320비트 상태에서 연산되며 [수식 3-2]와 같이 연산된다.

$$
\begin{aligned}
x_0 &\leftarrow \Sigma_0(x_0) = x_0 \oplus (x_0 \gg 19) \oplus (x_0 \gg 28),\\
x_1 &\leftarrow \Sigma_1(x_1) = x_1 \oplus (x_1 \gg 61) \oplus (x_1 \gg 39),\\
x_2 &\leftarrow \Sigma_2(x_2) = x_2 \oplus (x_2 \gg 1) \oplus (x_2 \gg 6),\\
x_3 &\leftarrow \Sigma_3(x_3) = x_3 \oplus (x_3 \gg 10) \oplus (x_3 \gg 17),\\
x_4 &\leftarrow \Sigma_4(x_4) = x_4 \oplus (x_4 \gg 7) \oplus (x_4 \gg 41),
\end{aligned}
$$

[수식 3-2] ASCON 선형 레이어

ASCON의 선형 레이어는 다섯 개의 32 × 32 이진 행렬에 대한 연산으로 간주될 수 있으며(x_0, x_1, x_2, x_3, x_4는 64 큐비트 배열), 궁극적으로 320 × 320 이진 행렬을 생성하게 된다. 이러한 선형 레이어 양자 회로를 구현할 때, out-of-place와 in-place 연산 모두 적용할 수 있다.

본 논문에서는 ASCON의 선형 레이어에 대한 이전 연구를 바탕으로, ASCON 선형 레이어의 다양한 구현 방법론을 평가하여 큐비트 수와 회로 depth 측면에서의 trade-off를 분석한다. 본 구현의 최적화 목표는 회로의 depth를 낮추는 것이며, 이를 위해 320개의 보조 큐비트를 각 라운드에 할당하여 선형 레이어의 출력을 저장하는 out-of-place 연산을 채택한다. 또한, 구현 과정에서 CNOT 게이트의 연산 순서가 회로 depth에 미치는 중요한 영향을 확인하고, ASCON 선형 레이어의 depth를 최적하기 위해 연산 순서를

전략적으로 배치한다. ASCON 선형 레이어에 대한 양자 자원 비교를 [표 3-2]에 제시하였으며, 본 논문의 구현은 640개의 큐비트를 사용하고(320 큐비트는 출력을 저장하는 데 사용됨), 960개의 CNOT 게이트를 사용하며, 가장 낮은 depth를 달성하였다.

Linear Layer	Source	#CNOT	#Qubit	Depth
Out-of-place	**Ours**	**960**	**640**	**3**
Naive(binary matrix)	Roy et al.	960	640	26
Gauss-Jordan	Roy et al.	2,413	320	358
PLU	Roy et al	2,413	320	288
XZLBZ	Roy et al.	1,595	320	119

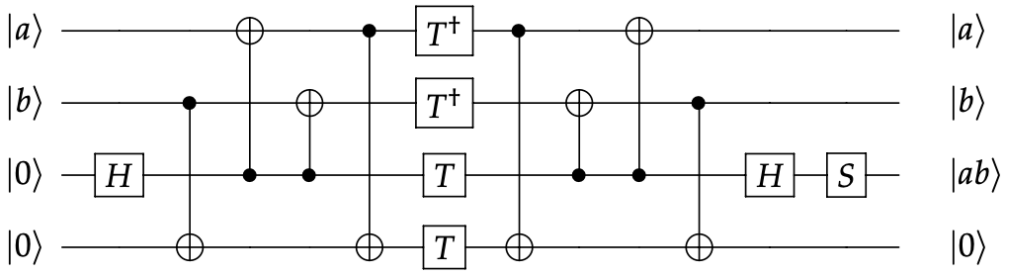
[표 3-2] ASCON 선형 레이어 양자 자원 비용 비교

제 3 절 AND 게이트를 통한 최적화

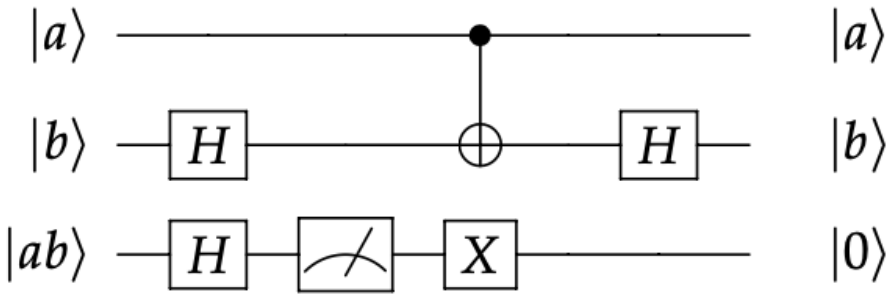
T-depth 또는 큐비트 수 최적화와 같은 목표에 따라, Toffoli 게이트를 분해하는 다양한 방법이 존재한다. 본 논문에서는 Amy et al. 이 제안한 기법을 채택하여 Toffoli 게이트를 8개의 Clifford 게이트 및 7개의 T 게이트로 분해한다. 이로 인해 T-depth는 4, 전체 depth는 8이 된다. 또한, Jaques et al.이 제안한 AND 게이트 방법도 적용한다. 이 방법은 Toffoli 게이트와 유사하게 동작하지만, 대상 큐비트가 clean(즉, $|0\rangle$) 상태여야 한다. AND 게이트는 11개의 Clifford 게이트, 4개의 T 게이트, 1개의 보조 큐비트로 구성되며, 그 결과 T-depth는 1, 전체 depth는 8이다 ([그림 3-2]). 이 때, AND 게이트에서 사용하는 보조 큐비트는 재사용 할 수 있다. 따라서, 치환 레이어에서 AND 게이트를 병렬로 처리하기 위해 320개(=5 × 64)의 보조 큐비트를 초기에 한번만 할당하면 된다. 그러나 본 구현에서는 보조 큐비트를 추가로 할당하지 않고 선형 레이어에서 사용할 보조 큐비트를 미리 선언하여 사용한다. 이에 따라 추가적인 보조 큐비트 할당은 필요하지 않으며, 320개의 큐비트 수를 아낄 수 있다.

또한, AND 게이트의 역연산인 AND† 게이트는 Measurement 게이트를 기반으로 하며, 5개의 Clifford 게이트와 1개의 Measurement 게이트로 구성

된다 ([그림 3-3]). 해당 게이트의 경우, depth는 4, T-depth는 0이다. 본 구현에서 Toffoli 게이트의 역연산이 사용되지 않기 때문에, AND† 게이트가 제공하는 자원 효율성의 이점을 활용하지 못한다. 그러나 Grover 오라클에서 AND† 게이트를 활용할 수 있다 (제 4장 2절에서 설명).



[그림 3-2] AND 게이트 양자 회로



[그림 3-3] AND† 게이트 양자 회로

제 4 절 ASCON 양자 회로 설계

1) ASCON AEAD 회로 설계

ASCON AEAD 양자 회로 구현은 [알고리즘 3-1]에 요약되어 있다. 순열 함수 (Permutation^a (*S*, *ancilla*))는 상수 덧셈, 치환 레이어 및 선형 레이어 회로로 구성되어 있다. 전체 회로에서 보조 큐비트 세트 ([알고리즘 3-1]에서 *ancilla*)는 제 3장 1절에 설명된 방법에 따라 재사용된다.

Initialization 단계에서는 320 큐비트 S 값과 128 큐비트 키 사이의 순열 연산과 비트 단위 XOR 연산이 수행된다. 이러한 XOR 연산에는 CNOT 게이트가 사용된다 (CNOT64는 CNOT 게이트가 64큐비트에서 작동함을 나타낸다). 키 값과 S (320비트)를 XOR하기 위해서는 키 값에 0을 패딩하는 작업이 수행된다. 그러나 0과의 XOR은 동작하지 않으므로 (결과 값이 변경되지 않음) 최하위 128 큐비트(x_3 및 x_4)에만 XOR 연산이 적용된다.

Associated Data와 Plaintext 단계에서는 입력 데이터가 각각 64비트 블록으로 처리되므로 64 큐비트 블록으로 분할하려면 패딩이 필요하다. 패딩은 단일 1과 최소 0을 추가한다. 1과의 XOR 연산은 NOT 연산을 적용하는 것과 동일한 결과이며, 따라서 알고리즘 1에서 x_0[31]로 식별된 큐비트에 대해 X 게이트로 표시되는 NOT 연산을 실행한다.

Algorithm : ASCON-128 양자 회로 구현

Input: $S = x_0 \| x_1 \| x_2 \| x_3 \| x_4$, pt, A, $\text{key} = \text{key}_0 \| \text{key}_1$, $ancilla$

Output: ct, T

1: $S \leftarrow \text{Permutation}^a\ (S,\ ancilla)$ #Inialization
2: $x_3 \leftarrow CNOT64\ (\text{key}_0,\ x_3)$
3: $x_4 \leftarrow CNOT64\ (\text{key}_1,\ x_4)$
5: $x_0[32:64] \leftarrow CNOT32\ (A,\ x_0[32:64])$ #Processing Associated Data
7: $x_0[31] \leftarrow \text{NOT}\ (\text{x}_0[31])$ $\#\ A\|1\|0^{r-1-(|A| \pmod r)}$XORed with x_0
9: $S \leftarrow \text{Permutation}^a\ (S,\ ancilla)$
11: $x_4[0] \leftarrow \text{NOT}\ (\text{x}_4[0])$ #Last bit of S XORed with 1
13: $x_0[32:64] \leftarrow CNOT32\ (pt,\ x_0[32:64])$ #Processing Plaintext
14: $ct \leftarrow$ allocate new 32 qubits
15: $ct \leftarrow x_0[32:64]$
17: $x_0[31] \leftarrow \text{NOT}\ (\text{x}_0[31])$ $\#\ pt\|1\|0^{r-1-(|pt| \pmod r)}$XORed with x_0
19: $x_1 \leftarrow CNOT64\ (\text{key}_0,\ x_1)$ #Finalization
20: $x_2 \leftarrow CNOT64\ (\text{key}_1,\ x_2)$
22: $S \leftarrow \text{Permutation}^a\ (S,\ ancilla)$
24: $x_3 \leftarrow CNOT64\ (\text{key}_0,\ x_3)$
25: $x_4 \leftarrow CNOT64\ (\text{key}_1,\ x_4)$
27: $T \leftarrow x_3 \| x_4$
28: **return** ct, T

[알고리즘 3-1] ASCON-128 양자 회로 구현 (AEAD 모드)

2) ASCON-HASH 회로 설계

[알고리즘 3-2]는 ASCON-HASH 양자 회로 구현을 보여준다. ASCON-HASH에서는 ASCON AEAD와 달리 p^b가 아닌 순열 p^a만 사용된다. 효율성을 높이기 위해, 각 인스턴스에 대해 초기 320비트 S를 사전에 계산할 수 있다. 이를 통해 X 게이트만 사용하여 ASCON-HASH의 Initialization을 구현한다. 간단히 말해서, S의 고전적인 값에 따라 X 게이트만 사용하여 S의 양자 상태를 설정한다.

Absorbing 단계에서 ASCON-HASH는 64비트 블록으로 메시지를 처리

한다. 메시지의 길이가 64비트의 배수가 되도록 단일 1과 최소 0을 추가하여 메시지에 패딩을 적용한다. 64비트의 각 메시지 블록은 S 값의 첫 번째 64비트 블록(즉, x_0)과 XOR 연산 후 S 값에 순열 함수를 적용한다.

Squeezing 단계는 256비트 해시 값을 생성한다. 해시 값은 64비트 블록 x_0에서 총 256비트 길이에 도달할 때까지 복사된다 ([알고리즘 3-2]의 8행). 각 복사 후 S 값은 순열 함수에 의해 값이 업데이트된다.

Algorithm : ASCON-HASH 양자 회로 구현

Input: $S = x_0 \| x_1 \| x_2 \| x_3 \| x_4$, *Message*, *ancilla*

Output: *Hash*

1: Inialization(S) #Only X gates are used
2: m_len = [*Message length*/64]
3: h_len = [*Hash length*/64]
4: **for** $0 \leqq i \leqq m\_len$ **do** #Absorbing
5: $x_0 \leftarrow CNOT64\ (Message[256-(64 \cdot (i+1)],\ x_0)$
6: $S \leftarrow \text{Permutation}^a\ (S,\ ancilla)$
7: **for** $0 \leqq i \leqq h\_len-1$ **do** #Squeezing
8: $Hash[64 \cdot i : 64 \cdot i+63] \leftarrow CNOT64\ (Hash[64 \cdot i : 64 \cdot i+63])$
9: $S \leftarrow \text{Permutation}^a\ (S,\ ancilla)$
10: **return** *Hash*

[알고리즘 3-2] ASCON-HASH 양자 회로 구현

제 4 장 성능 평가

제 1 절 양자 회로 비용 평가

본 절에서는 ASCON-AEAD 및 ASCON 해시함수의 모든 파라미터에 대한 양자 회로 자원 비용을 추정한다. ASCON-AEAD는 ASCON-128과 ASCON-128a가 있으며, ASCON 해시함수의 경우 256비트인 ASCON-HASH와 임의의 출력길이를 지정할 수 있는 XoF가 있다. 본 논문에서는 256비트의 ASCON-HASH와 XoF를 사용하여 384비트 512비트의 출력 길이를 가지는 ASCON 해시함수의 양자 회로 자원 비용을 추정한다. 양자 회로를 구현하고 시뮬레이션하기 위해 양자 프로그래밍 도구 ProjectQ를 사용한다. 구현의 정확성은 ProjectQ의 ClassicSimulator 라이브러리로 검증하여 확인하고, 양자 자원은 ResourceCounter로 분석하여 평가한다.

[표 4-1]은 ASCON 양자 회로 구현을 위해 요구되는 자원 비용 보여준다. 또한, [표 4-1]에 제시된 양자 자원은 Toffoli 게이트를 Clifford + T 게이트 (8개의 Clifford 게이트 + 7개의 T 게이트, T-depth 4, full depth 8)로 분해된 것을 기반으로 분석된다. 자원 추정을 위해, ASCON-AEAD의 경우 관련 데이터(AD)와 평문(P) 모두 32비트의 고정된 크기를 유지한다. ASCON 해시함수 자원 추정을 위한 입력 메시지 길이는 출력 길이와 동일하게 유지한다.

ASCON-HASH 구현은 이전 연구에 비해 Toffoli-depth와 Full-depth 측면에서 개선된 결과를 제공한다. 그러나 본 구현은 낮은 depth를 달성하는 대신 많은 수의 큐비트를 요구한다 (depth와 큐비트는 서로 trade-off 관계). 이러한 trade-off를 위해 [표 4-1]에 $TD-M$, $FD-M$, TD^2-M, FD^2-M 비용을 추정한다. TD 비용은 Toffoli-depth, FD는 Full depth, M은 큐비트 수를 나타낸다. 이러한 메트릭은 일반적으로 양자 회로의 trade-off 성능을 평가하는 데 사용된다. 해당 메트릭을 사용하여 이전 연구와 비교하였을 때, 본 구현은 최적화된 성능을 제공한다. 다음과 같이 추정된 양자 자원 비용을 사

용하여 ASCON에 대한 Grover의 키 검색 및 충돌 검색 비용을 추정하고 ASCON의 양자 후 보안을 평가한다.

Cipher		Source	#CNOT	#1qCliff	#T	Toffoli Depth (TD)	#Qubit (M)	Full Depth (FD)	TD−M	FD−M	TD^2-M	FD^2-M
ASCON-AEAD	ASCON-128	Ours	127,200	21,563	67,220	30	20,064	513	1.15×2^{19}	1.23×2^{23}	1.08×2^{24}	1.23×2^{32}
	ASCON-128a	Ours	135,648	22,979	71,680	32	21,344	547	1.30×2^{19}	1.39×2^{23}	1.30×2^{24}	1.49×2^{32}
ASCON hash function	ASCON-HASH (256)	Lee	491,008	208,018	387,072	864	35,136	8,427	1.81×2^{24}	1.10×2^{28}	1.53×2^{34}	1.13×2^{41}
		Ours	406,016	68,435	215,040	96	62,592	1,641	1.43×2^{22}	1.53×2^{26}	1.07×2^{29}	1.23×2^{37}
	ASCON-XoF (384)	Ours	609,024	102,419	322,560	144	93,568	2,461	1.61×2^{23}	1.72×2^{27}	1.81×2^{30}	1.03×2^{39}
	ASCON-XoF (512)	Ours	812,032	136,402	430,080	192	124,544	3,281	1.43×2^{24}	1.52×2^{28}	1.07×2^{32}	1.22×2^{40}

[표 4-1] ASCON 양자 회로 구현에 사용된 양자 자원 비용

제 2 절 Grover 공격 비용 평가

ASCON Grover 공격 비용을 추정하기 위해 제 2장 2절에 요약된 방법을 따른다. Grover 오라클에서는 ASCON 양자 회로와 역 회로가 순차적으로 실행된다. 첫 번째는 암호화 회로를 구성하고, 두 번째는 암호화 전 상태로 돌아가기 위해 암호화 회로를 역으로 연산한다. 이 과정에서 $\mathrm{AND}^\dagger$ 게이트는 역 회로에서 활용될 수 있다. [표 4-2]에 요약된 Grover 오라클 추정 비용에 따르면, AND 게이트를 사용하면 큐비트 수를 늘리지 않고 양자 자원 비용을 절감할 수 있다. 또한, 대부분의 양자 자원이 양자 회로에서 대상 암호를 구현하는 데 사용되므로 디퓨전 연산자의 오버헤드는 오라클에 비해 무시될 수 있다. 이러한 이유로 많은 연구에서 Grover 검색 비용은 오라클의 반복 비용으로 고려된다.

ASCON AEAD Grover 키 검색 공격은 대량의 ASCON 양자 회로를 순차적으로 반복해야 한다. k-비트 키를 사용하여 암호를 연속적으로 복구할

때마다 오라클 및 확산 연산자 세트를 $\left\lfloor \frac{\pi}{4}\sqrt{2^k} \right\rfloor$ 번 반복해야 한다. ASCON 해시함수의 충돌 공격 비용을 추정하기 위해 CNS 알고리즘을 사용한다. CNS 알고리즘은 $O(2^{2n/5-3s/5})$ $(s \leqq n/4)$의 복잡성을 가지고 있다. Jang et al.에 따르면, NIST 양자 후 보안 레벨에 적합한 기준을 정의하기 위해 $s=n/6$을 설정했으며, 본 논문 또한 해당 접근 방식을 따른다. 요약하자면, ASCON-AEAD 및 ASCON 해시함수에 대한 Grover 공격 비용은 다음과 같다 : [표 4-2] $\times \left\lfloor \frac{\pi}{4}\sqrt{2^k} \right\rfloor$ 및 [표 4-2] $\times \left\lfloor 2^{(\frac{2n}{5}-\frac{3s}{5})} \right\rfloor$.

[표 4-3]과 [표 4-4]는 Grover 알고리즘을 사용하여 ASCON-AEAD 및 ASCON 해시함수의 공격 비용을 보여준다. NIST의 문서에 따라, 본 논문에서는 $GF-D$ 비용을 추정하고 큐비트 수와 회로 depth 간의 trade-off에 대한 $Td-M$, $FD-M$, Td^2-M, FD^2-M 비용도 추정한다. 또한, MAXDEPTH를 고려하면, Toffoli-depth, T-depth 및 Full depth를 포함한 회로 depth와 관련된 메트릭은 중요한 요소이다. 이와 관련하여 depth 최적화된 구현은 이러한 메트릭에서 최적의 성능을 제공한다.

Cipher		Source	#CNOT	#1qCliff	#T	#Measure	T Depth (Td)	#Qubit (M)	Full Depth (FD)	Td−M	FD−M	Td^2-M	FD^2-M
ASCON-AEAD	ASCON-128	Ours	254,400	43,126	134,440	0	240	20,065	1,026	1.15×2^{22}	1.23×2^{24}	1.08×2^{30}	1.23×2^{34}
		Ours-AND	225,600	71,926	38,400	9,600	30	20,065	816	1.15×2^{19}	1.95×2^{23}	1.08×2^{24}	1.56×2^{33}
	ASCON-128a	Ours	271,296	45,958	143,360	0	256	21,355	1,094	1.30×2^{22}	1.40×2^{24}	1.30×2^{30}	1.49×2^{34}
		Ours-AND	240,576	76,678	40,960	10,240	32	21,355	872	1.30×2^{19}	1.11×2^{24}	1.30×2^{24}	1.89×2^{33}
ASCON hash function	ASCON-HASH (256)	Lee	982,016	416,036	774,144	0	6,912	35,137	16,854	1.81×2^{25}	1.10×2^{29}	1.53×2^{36}	1.13×2^{43}
		Ours	812,032	136,870	430,080	0	768	62,593	3,282	1.43×2^{25}	1.53×2^{27}	1.07×2^{35}	1.23×2^{39}
		Ours-AND	719,872	229,030	122,880	30,720	96	62,593	2,608	1.43×2^{22}	1.22×2^{27}	1.07×2^{29}	1.55×2^{38}
	ASCON-XoF (384)	Ours	1,218,048	204,838	645,120	0	1,152	93,569	4,922	1.61×2^{26}	1.72×2^{28}	1.81×2^{36}	1.03×2^{41}
		Ours-AND	1,079,808	343,076	184,320	46,080	144	93,569	3,904	1.61×2^{23}	1.36×2^{28}	1.81×2^{30}	1.55×2^{38}
	ASCON-XoF (512)	Ours	1,624,064	272,804	860,160	0	1,536	124,545	6,562	1.43×2^{27}	1.52×2^{29}	1.07×2^{38}	1.22×2^{42}
		Ours-AND	1,439,744	457,124	245,760	61,440	192	124,545	5,200	1.43×2^{24}	1.21×2^{29}	1.07×2^{32}	1.53×2^{41}

[표 4-2] ASCON Grover 오라클 양자 자원 비용

Cipher		Source	#Gate (G)	Full Depth (FD)	T Depth (Td)	#Qubit (M)	G−FD	FD−M	Td−M	FD^2-M	Td^2-M
ASCON-AEAD	ASCON-128	Ours	1.31×2^{82}	1.57×2^{73}	1.47×2^{71}	1.22×2^{14}	1.03×2^{156}	1.92×2^{87}	1.79×2^{85}	1.50×2^{161}	1.32×2^{157}
		Ours-AND	1.01×2^{82}	1.25×2^{73}	1.44×2^{68}	1.22×2^{14}	1.26×2^{155}	1.53×2^{87}	1.76×2^{82}	1.90×2^{160}	1.27×2^{151}
	ASCON-128a	Ours	1.39×2^{82}	1.68×2^{73}	1.57×2^{71}	1.30×2^{14}	1.17×2^{156}	1.10×2^{88}	1.02×2^{86}	1.83×2^{161}	1.60×2^{157}
		Ours-AND	1.10×2^{82}	1.34×2^{73}	1.56×2^{68}	1.30×2^{14}	1.47×2^{155}	1.74×2^{87}	1.01×2^{83}	1.17×2^{161}	1.58×2^{151}

[표 4-3] ASCON-AEAD Grover 공격 비용

Cipher		Source	#Gate (G)	Full Depth (FD)	T Depth (Td)	#Qubit (M)	G−FD	FD−M	Td−M	FD^2-M	Td^2-M
ASCON hash function	ASCON -HASH	Lee	1.42×2^{97}	1.40×2^{90}	1.15×2^{89}	1.70×2^{57}	1.99×2^{187}	1.19×2^{148}	1.96×2^{146}	1.68×2^{238}	1.13×2^{236}
		Ours	1.80×2^{96}	1.09×2^{88}	1.02×2^{86}	1.51×2^{58}	1.96×2^{184}	1.66×2^{146}	1.55×2^{144}	1.81×2^{234}	1.59×2^{230}
		Ours-AND	1.44×2^{96}	1.74×2^{87}	1.02×2^{83}	1.51×2^{58}	1.25×2^{184}	1.25×2^{146}	1.54×2^{141}	1.14×2^{234}	1.57×2^{224}
	ASCON -XoF (384)	Ours	1.78×2^{135}	1.08×2^{127}	1.01×2^{125}	1.42×2^{80}	1.92×2^{262}	1.54×2^{207}	1.44×2^{205}	1.67×2^{334}	1.46×2^{330}
		Ours-AND	1.42×2^{135}	1.67×2^{126}	1.01×2^{122}	1.42×2^{80}	1.19×2^{262}	1.19×2^{207}	1.44×2^{202}	1.00×2^{334}	1.46×2^{324}
	ASCON -XoF (512)	Ours	1.57×2^{174}	1.90×2^{165}	1.78×2^{163}	1.19×2^{102}	1.49×2^{340}	1.14×2^{268}	1.06×2^{266}	1.08×2^{434}	1.90×2^{429}
		Ours-AND	1.25×2^{174}	1.51×2^{165}	1.77×2^{160}	1.19×2^{102}	1.89×2^{339}	1.80×2^{267}	1.06×2^{263}	1.36×2^{433}	1.88×2^{423}

[표 4-4] ASCON 해시함수 Grover 양자 충돌 공격 비용

제 5 장 결 론

암호에 대한 양자 공격 비용 분석을 통해 암호의 양자 후 보안 강도를 평가할 수 있다. 이러한 맥락에서 NIST가 설정한 양자 후 보안 레벨을 고려하는 것이 중요하다. 2016년에 NIST는 AES 공격에 대한 예상 비용으로 양자 후 보안 레벨(레벨 1, 3, 5)을 도입했다. 그러나 AES에 대한 공격 비용이 감소함에 따라 NIST는 제 2장 2절에서 논의한 바와 같이 공격 비용 지표를 보안 수준에 맞게 수정하였다. [표 4-3]에 제공된 정보에 따르면 ASCON-128 및 ASCON-128a에 대해 가장 최적화된 양자 공격 비용은 1.26×2^{155}, 1.47×2^{155} 이다. 따라서 현재 표준에 따르면 ASCON-128과 ASCON-128a는 AES-128 (2^{157}) 공격 비용에 해당하는 양자 후 보안 레벨 1을 달성하는 데 미치지 못한다.

반면에 NIST는 SHA2/3-256 및 SHA2/3-384와 관련된 비용인 레벨 2와 4에 대해 클래식 비용만 제공하며 양자 비용을 제공하지 않는다. 따라서 이전 논문과의 비교에 초점을 맞추고, Jang et al. 이 제안한 2, 4 및 6 레벨 비용과 비교한다. ASCON-HASH (256 비트)와 ASCON-XoF (384, 512 비트)의 양자 충돌 공격 비용은 각각 1.25×2^{184}, 1.19×2^{262}, 1.89×2^{339} 이다. 본 구현은 이전연구에 비해 NIST가 제공하는 지표인 $GF-D$ 측면에서 더 높은 수준의 최적화를 보여준다. 또한, Jang et al. 은 SHA2/3와 관련된 공격 비용인 레벨 2, 4, 6의 비용을 $2^{188/183}$, $2^{266/260}$, $2^{343/337}$로 정의하였다 (제 2장 2절에서 설명). 이와 비교하면, ASCON 해시 함수는 SHA3와 관련된 공격 비용을 만족한다.

요약하면, 본 논문은 ASCON-AEAD 및 ASCON 해시함수의 최적화된 구현을 제시한다. 합리적인 큐비트 수를 보장하면서 Toffoli-depth와 Full depth를 최소화하기 위해 다양한 기술을 사용한다. depth에 최적화된 ASCON-AEAD 양자 회로는 양자 후 보안 레벨 1을 달성하지 못한다. 또한 ASCON-HASH의 양자 회로 구현은 이전 구현과 비교하여 80.5% 이상의

전체 depth 개선과 Toffoli-depth를 88.9% 이상 달성한다. 또한, Jang et al.이 정의한 해시 함수 양자 충돌 공격 비용과 비교하면 SHA3에 대한 공격 비용을 만족 하는 것을 알 수 있다.

ASCON의 저자들은 ASCON이 모든 양자 공격에 대한 저항을 가지지는 않을 것으로 예상하였다. 따라서, 추가로 160비트 더 긴 키 길이를 가진 ASCON-80pq를 제안하였다. 향후에는, 이를 기반으로 ASCON-80pq의 양자 회로를 구현하고 보안 강도를 평가할 예정이다.

참 고 문 헌

1. 국외문헌

Shor, P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Rev. 1999, 41, 303-332.

Grover, L.K. A fast quantum mechanical algorithm for database search. In Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, Philadelphia, PA, USA, 22-24 May 1996; pp. 212-219.

Dobraunig, C.; Eichlseder, M.; Mendel, F.; Schläffer, M. Ascon v1.2. Submission to NIST. 2019. Available online: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/ascon-spec-round2.pdf (accessed on 25 March 2024).

Bhattacharjee, D.; Chattopadhyay, A. Depth-optimal quantum circuit placement for arbitrary topologies. arXiv 2017, arXiv:1703.08540.

Grassl, M.; Langenberg, B.; Roetteler, M.; Steinwandt, R. Applying Grover's Algorithm to AES: Quantum Resource Estimates. In Post-Quantum Cryptography; Takagi, T., Ed.; Springer: Cham, Switzerland, 2016; pp. 29-43.

Jaques, S.; Naehrig, M.; Roetteler, M.; Virdia, F. Implementing Grover Oracles for Quantum Key Search on AES and LowMC. In Advances in Cryptology-EUROCRYPT 2020, Proceedings of the 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, 10-14 May 2020; Canteaut, A., Ishai, Y., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2020; Part II, Volume 12106, pp. 280-310.

Jang, K.; Baksi, A.; Kim, H.; Song, G.; Seo, H.; Chattopadhyay, A. Quantum Analysis of AES. Cryptology ePrint Archive, Paper 2022/683. 2022. Available online: https://eprint.iacr.org/2022/683 (accessed on 25 March 2024).

NIST. Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process. 2016. Available online: https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals- final-dec-2016.pdf (accessed on 25 March 2024).

NIST. Call for Additional Digital Signature Schemes for the Post-Quantum Cryptography Standardization Process. 2022. Available online: https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/call-for-proposals-dig-sig-sept-2022.pdf (accessed on 25 March 2024).

Kim, P.; Han, D.; Jeong, K.C. Time-space complexity of quantum search algorithms in symmetric cryptanalysis: Applying to AES and SHA-2. Quantum Inf. Process. 2018, 17, 339.

Lee, W.K.; Jang, K.; Song, G.; Kim, H.; Hwang, S.O.; Seo, H. Efficient implementation of lightweight hash functions on gpu and quantum computers for iot applications. IEEE Access 2022, 10, 59661-59674.

Stoffelen, K. Optimizing s-box implementations for several criteria using SAT solvers. In Proceedings of the International Conference on Fast Software Encryption, Bochum, Germany, 20-23 March 2016; pp. 140-160.

Lu, Z.; Wang, W.; Hu, K.; Fan, Y.; Wu, L.; Wang, M. Pushing the limits: Searching for implementations with the smallest area for lightweight s-boxes. In Progress in Cryptology-INDOCRYPT 2021, Proceedings of the 22nd International Conference on Cryptology in India,

Jaipur, India, 12–15 December 2021; Proceedings 22; Springer: Berlin/Heidelberg, Germany, 2021; pp. 159–178.
Feng, J.; Wei, Y.; Zhang, F.; Pasalic, E.; Zhou, Y. Novel Optimized Implementations of Lightweight Cryptographic S-Boxes via SAT Solvers. IEEE Trans. Circuits Syst. I Regul. Pap. 2023, 71, 334–347.
Dasu, V.A.; Baksi, A.; Sarkar, S.; Chattopadhyay, A. LIGHTER-R: Optimized Reversible Circuit Implementation For SBoxes. In Proceedings of the 32nd IEEE International System-on-Chip Conference, SOCC 2019, Singapore, 3–6 September 2019; pp. 260–265.
Chun, M.; Baksi, A.; Chattopadhyay, A. DORCIS: Depth Optimized Quantum Implementation of Substitution Boxes. Cryptology ePrint Archive, Paper 2023/286. 2023. Available online: https://eprint.iacr.org/2023/286 (accessed on 25 March 2024).
Chen, J.; Liu, Q.; Fan, Y.; Wu, L.; Li, B.; Wang, M. New SAT-based Model for Quantum Circuit Decision Problem: Searching for Low-Cost Quantum Implementation. IACR Commun. Cryptol. 2024, 1.
Lin, D.; Yang, C.; Xu, S.; Tian, S.; Sun, B. On the Construction of Quantum Circuits for S-Boxes with Different Criteria Based on the SAT Solver. Cryptology ePrint Archive, Paper 2024/565. 2024. Available online: https://eprint.iacr.org/2024/565 (accessed on 25 March 2024).
Amy, M.; Maslov, D.; Mosca, M.; Roetteler, M.; Roetteler, M. A Meet-in-the-Middle Algorithm for Fast Synthesis of Depth-Optimal Quantum Circuits. IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst. 2013, 32, 818–830.
Roy, S.; Baksi, A.; Chattopadhyay, A. Quantum Implementation of ASCON Linear Layer. Cryptology ePrint Archive, Paper 2023/617. 2023. Available online: https://eprint.iacr.org/2023/617 (accessed on 25 March 2024).
Xiang, Z.; Zeng, X.; Lin, D.; Bao, Z.; Zhang, S. Optimizing

Implementations of Linear Layers. IACR Trans. Symmetric Cryptol. 2020, 2020, 120–145.

Zheng, Y.; Luo, Q.; Li, Q.; Lv, Y. Quantum circuit implementations of lightweight authenticated encryption ASCON. J. Supercomput. 2024, 1–16.

Baksi, A.; Jang, K.; Song, G.; Seo, H.; Xiang, Z. Quantum Implementation and Resource Estimates for Rectangle and Knot. Quantum Inf. Process. 2021, 20, 395.

Anand, R.; Maitra, A.; Maitra, S.; Mukherjee, C.S.; Mukhopadhyay, S. Quantum Resource Estimation for FSR Based Symmetric Ciphers and Related Grover's Attacks. In Progress in Cryptology–INDOCRYPT 2021, Proceedings of the 22nd International Conference on Cryptology in India, Jaipur, India, 12–15 December 2021; Lecture Notes in Computer Science; Adhikari, A., Küsters, R., Preneel, B., Eds.; Springer: Berlin/Heidelberg, Germany, 2021; Volume 13143, pp. 179–198.

Huang, Z.; Sun, S. Synthesizing Quantum Circuits of AES with Lower T-depth and Less Qubits. In Advances in Cryptology– ASIACRYPT 2022, Proceedings of the 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, 5–9 December 2022; Lecture Notes in Computer Science; Agrawal, S., Lin, D., Eds.; Springer: Berlin/Heidelberg, Germany, 2022; Part III, Volume 13793, pp. 614–644.

Zou, J.; Wei, Z.; Sun, S.; Liu, X.; Wu, W. Quantum Circuit Implementations of AES with Fewer Qubits. In Advances in Cryptology–ASIACRYPT 2020, Proceedings of the 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, Republic of Korea, 7–11 December 2020; Moriai, S., Wang, H., Eds.; Springer: Cham, Switzerland, 2020; pp. 697–726.

Jang, K., Lim, S., Oh, Y., Kim, H., Baksi, A., Chakraborty, S., & Seo,

H. (2024). Quantum Implementation and Analysis of SHA-2 and SHA-3. Cryptology ePrint Archive.

ABSTRACT

Quantum Implementation and Analysis of ASCON

Oh, Yu-Jin

Major in Convergence Security

Dept. of Convergence Security

The Graduate School

Hansung University

The advancement of quantum computing poses security challenges in the field of cryptography. In particular, Grover's algorithm impacts the search complexity reduction of symmetric key ciphers and hash functions. Recent studies have focused on estimating Grover's search complexity and evaluating post-quantum security. This paper proposes the quantum circuit implementation and analysis of ASCON, which encompasses both symmetric key encryption and hash functions, as part of the lightweight cryptography standardization efforts by NIST (National Institute of Standards and Technology). Compared to previous research, the quantum circuit implementation of ASCON-HASH improves the Toffoli-depth by 88.9% and the overall circuit depth by 80.5%. The most effective approach to Grover's search is minimizing the circuit depth of the cipher. Thus, this paper presents a depth-optimized quantum circuit for ASCON and the optimal Grover search cost. Additionally, based on security levels and the latest research trends, it estimates the cost

required to evaluate the quantum-resistant security strength of ASCON.