Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.34, NO.6, Dec. 2024 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2024.34.6.1189

Width 효율적 ASCON 양자 회로를 이용한 Grover 기반 양자 보안비도 분석*

오 진 섭,[1†] 최 찬 호,[2] 최 두 호[3‡]
[1,2,3]고려대학교 세종캠퍼스 (학생, 대학원생, 교수)

Grover-Based Quantum Security Analysis Using width Efficient Quantum Circuit of ASCON*

Jinseob Oh,[1†] Chanho Choi,[2] Dooho Choi[3‡]
[1,2,3]Korea University Sejong Campus (Student, Graduate student, Professor)

요 약

양자컴퓨팅의 발전에 따른 기존 암호화 시스템의 양자컴퓨터 상에서의 보안성 분석, 즉 양자보안성 분석의 필요성이 증가하고 있다. 본 논문에서는 Grover 키 탐색 알고리즘을 기반으로 NIST 경량 암호 ASCON의 보안비도 분석을 진행한다. 특히, Clifford+T 게이트 조합으로 ASCON-128의 양자 회로를 구현하는 동시에 보조 큐비트 값 초기화 문제를 해결하는 새로운 양자 회로 구현물을 제시한다. Grover 키 탐색 알고리즘 기반 보안비도 분석에 적합하도록 ASCON의 암호화 구조를 간략화하고 자원량을 측정한 결과 보조 큐비트 초기화 회로를 추가하였음에도 불구하고, 시-공간 복잡도와 관련된 비용인 $Td-M$과 $Fd-M$에서 각각 85.65%, 83.73% 감소를 보였다.

ABSTRACT

This paper discusses the need to reevaluate the security of existing cryptographic systems due to the advancement of quantum computing, and analyzes the security level of the NIST lightweight cipher ASCON based on the Grover key search algorithm. In particular, we present a novel quantum circuit implementation of ASCON-128 with a consist of clifford+T gates, which solves the problem of initializing the auxiliary qubit value. We simplified ASCON's cryptographic structure and measured the resource consumption to analyze the security level based on Grover's key discovery algorithm, and found that the cost associated with the space-time complexity, Td-M and Fd-M, was reduced by 85.65% and 83.73%, respectively, despite solving the secondary qubit initialization problem.

Keywords: Quantum Computing, Cryptographic engineering, Light weight cryptography

I. 서 론

양자컴퓨팅의 발전은 현존 암호화 시스템의 보안성에 의문을 제기한다[1]. 특히, Grover 키 탐색 알고리즘은 k비트의 키를 사용하는 암호화 알고리즘의 키 검색 시간 복잡도를 2^k에서 $2^{k/2}$로 감소시킨다[2]. 이에, 기존 암호 및 채택되는 알고리즘에 대

Received(10. 04. 2024), Modified(11. 25. 2024), Accepted(11. 26. 2024)
* 본 연구는 2024년도 한국정보보호학회 하계학술대회에 발표한 우수논문을 개선 및 확장한 것임.
* 본 연구는 정부(과학기술정보통신부)의 정보통신기술기획평가원(IITP) 과제(〈Q|Crypton〉, No.2024-0-00033)의 일부 지원과 과학기술정보통신부 과제의 양자컴퓨팅 기반 양자이득 도전연구 결과(RS-2024-00256221) 및 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터사업의 연구결과로 수행되었음(IITP-2024-RS-2022-00164800).
† 주저자, gnqorwptneh@korea.ac.kr
‡ 교신저자, doohochoi@korea.ac.kr(Corresponding author)

하여 Grover 키 탐색 알고리즘을 적용하였을 때, 암호가 지니는 보안성에 대한 철저한 재평가가 시급하다.

본 논문에서는 NIST 경량 암호 ASCON이 Grover 키 탐색 알고리즘에 대하여 지니는 보안비도를 측정하기 위한 회로를 설계한다.

기존의 ASCON에 대한 양자 회로 분석 연구는 Clifford+T 게이트 구성을 이용하지 않거나, 보조 큐비트의 상태를 초기화하지 않았다[3-4]. 이는, Clifford+T 게이트로 이루어진 기존 AES 암호분석 결과와의 공정한 비교를 어렵게 하고, 보조 큐비트의 상태가 초기화되지 않은 구성은 더 이상 이용되지 않는 값과의 얽힘 상태로 하여금 회로 결과의 신뢰성에 의문을 남긴다[5-6].

본 연구에서는 Clifford+T 게이트 조합으로 ASCON-128을 구현하는 동시에 보조 큐비트 값 초기화 문제를 해결하는 새로운 양자 회로 구현물을 제시한다. 그리고, Grover 키 탐색 알고리즘 기반 보안비도 분석에 적합하도록 ASCON의 암호화 과정을 간략화하고, 이에 대한 자원량을 측정한다.

상기 과정들을 통해 얻은 자원량을 바탕으로 NIST 양자 보안 평가 기준인 Grover Oracle의 비용을 계산하여 ASCON-128의 양자 보안비도 분석을 진행한다.

본 논문의 구성은 다음과 같다. II 장에서는 배경지식과 관련 연구를 서술하고, III 장에서는 양자 보안비도 분석에 적합한 ASCON 암호화 과정 간략화에 대하여 서술한다. IV 장에서는 이전 장에서 설계한 구조에 맞춰 양자 회로를 설계하고, V 장에서 IV 장의 회로를 바탕으로 보조 큐비트 상태 초기화 과정을 설명한다. 그리고, VI 장에서 이에 대한 Grover Oracle 양자 자원량을 측정하고, 마지막으로 VII 장에서 결론으로 마무리한다.

II. 배경지식 및 관련 연구

2.1 양자 논리 게이트

양자 논리 게이트는 정보 표현 단위의 상태만 반전시키는 고전 컴퓨터의 논리 게이트와 달리 큐비트의 상태를 반전하고, 위상을 조작하는 기능을 제공하는 양자 회로의 기본 논리 회로이다.

양자 논리 게이트는 Fig. 1.과 같이 Clifford 게이트와 비-Clifford 게이트로 분류할 수 있으며, 각

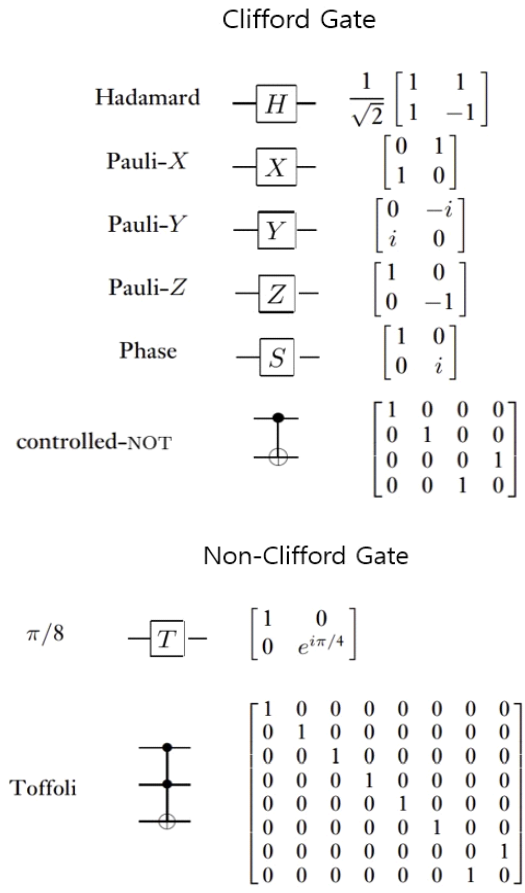

Fig. 1. Quantum Logic Gate

각은 고유한 특성에 따라 응용된다.

Clifford 게이트에는 pauli-X, Y, Z와 Hadamard 게이트, 위상-S 그리고 CX 게이트가 있으며, 이 중, pauli-X와 CX 게이트는 각각 암호화 알고리즘의 구현에 있어 주로 사용되는 연산인 NOT과 XOR의 기능을 양자컴퓨팅 환경에 구현하는데 사용된다.

특히, CX 게이트는 제어 큐비트의 상태에 따라 목표 큐비트의 위상을 변화시키기 때문에 양자상태의 일부 정보를 다른 양자비트로 전달할 수 있다. 이는 양자상태의 복제는 불가능하나 양자상태의 위상은 변형하는 것이 가능하다는 속성에 기인하여 양자비트의 복제 불가 정리를 극복할 수 있다[7-8].

하지만, Clifford 게이트만으로 구성된 회로는 양자 연산에 보편적이지 않기 때문에 Clifford 게이트가 아닌 다른 게이트와의 결합이 필요하다.

비-Clifford 게이트인 T 게이트는 Clifford 게이

트만으로는 달성할 수 없는 특정 위상의 연산을 가능하게 하여 양자 회로의 계산 범위를 확장한다. T 게이트와 Clifford 게이트들의 복합적인 활용은 다항식 곱셈과 같이 더 복잡한 논리 연산이 필요할 때 이용되는 Toffoli 게이트를 형성할 수 있게 한다. Toffoli 게이트는 양자 회로에서 일반적으로 AND라고 불리는 고전적인 논리 연산의 구현에 이용된다. 이는, Toffoli 게이트의 두 개의 제어 큐비트의 상태에 따라 하나의 목표 큐비트의 상태를 조정할 수 있는 특성에 기인한다.

2.2 ASCON

NIST 경량 암호화 표준에서 최종 채택된 ASCON은 컴퓨팅 자원이 제한된 환경에서 메모리 공간을 최소화하며 안전하고 효율적인 암호화를 제공하기 위해 설계된 경량 암호화 알고리즘이다.

ASCON AEAD의 암호화 과정은 초기화, 관련 데이터 처리, 암호문 생성, 최종화 단계로 구성되며 이는 보안성을 유지하며, 효율적인 구현을 위해 스펀지 구조로 구현된다.

스펀지 함수 내의 순열 연산은 확산을 용이하게 하고, 암호화 보안 강화에 기여한다. ASCON의 순열은 addition of constant, S-box, 그리고 linear diffusion layer로 구성되며, 특히 S-box 연산은 암호의 비선형성을 달성한다. ASCON의 S-box 연산은 입력 상태를 5개의 레지스터의 각 비트 슬라이스에 NOT, AND, 그리고 XOR 연산으로 구성된 5비트 S-box를 64회 병렬로 적용한다[9].

III. Grover 알고리즘 적용을 위한 ASCON 암호화 과정 간략화

Grover 알고리즘은 암호문을 출력하는 블랙박스 함수로부터 입력값에 해당하는 키를 찾는 것을 목적으로 한다. 본 연구에서는 Grover 키 탐색 알고리즘에 대한 ASCON-128의 양자 보안비도를 분석하기 위하여 단일 블록의 평문을 암호화하는 ASCON의 연산을 양자 회로로 구현한다.

ASCON의 암호화 체계는 초기화, 연관데이터 처리, 일반 텍스트 암호화, 최종화의 4단계로 구성된다. 그러나, Grover 알고리즘을 활용하여 암호문으로부터 비밀키를 찾는 경우 키 생성에 직접적으로 관여하는 단계만을 구현하는 것이 바람직하다.

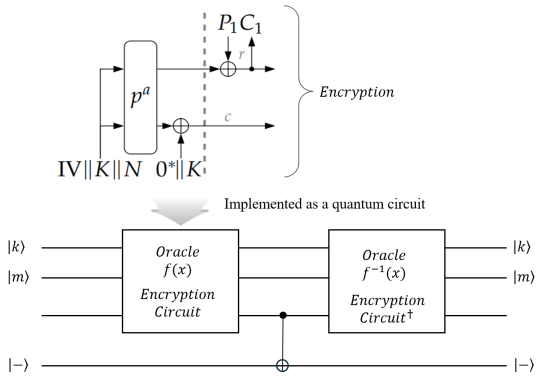

Fig. 2. Encrypt scheme of ASCON for Grover key search analysis.

본 절에서는 Fig. 2.처럼 암호문의 생성에 직접적으로 관여하지 않거나 보안성에 영향을 미치지 않는 연관데이터 처리와 최종화 단계를 생략하여 암호화 과정을 간략화했다.

3.1 연관 데이터 처리 과정 생략

ASCON 암호화 구조 중 연관 데이터 처리는 무결성과 인증을 보장하기 위하여 설계되었다. 그러나, 이는 평문 텍스트를 암호 텍스트로 암호화하는 암호화 프로세스와 보안 강도에 직접적인 영향을 미치지 않는다. 이러한 특수성은 0바이트의 연관데이터를 사용하여 8바이트 미만의 평문 텍스트를 암호화하는 실험 중 ASCON 암호화의 효율성과 효과를 보여주는 결과를 통해 나타난다[9]. 상기 결과는 8바이트 미만의 평문 텍스트를 암호화하는 경우 순열 함수 p^a를 호출하는 것으로 최소한의 계산 오버헤드와 안전한 암호화를 달성할 수 있음을 보인다. 또한, R. Ankele 등[10]이 진행한 실험에서 ASCON과 AES 암호 기반 시스템의 성능을 비교한 결과, 연관데이터를 사용하지 않아도 두 시스템 모두 보안비도가 유지된 상태로 동작할 수 있음을 확인하였다. 이는 연관 데이터 처리 과정 없이 ASCON의 암호화 구현이 가능함을 보인다.

3.2 최종화 과정 생략

ASCON의 암호화 구조 중 최종화는 암호문 C_1이 생성된 후 인증을 위한 태그를 생성하여 메시지와

연관데이터의 무결성을 입증한다.

그러나, Grover 키 탐색 알고리즘은 암호문에 대해 키를 전수조사(bruteforce) 하는 알고리즘으로, 평문 P_1과 암호문 C_1 만으로도 키를 찾아낼 수 있다. 따라서, 본 논문에서는 암호의 양자 저항성을 분석하기 위한 회로 구현에서 앞서 언급한 바와 같이 Grover 알고리즘 동작을 위한 입력이 모두 생성된 후에 동작하는 최종화를 제외한다.

IV. ASCON 양자 회로 구현

양자컴퓨팅 시스템은 고전 컴퓨터와는 다른 연산 구조로 동작한다. 고전 컴퓨터는 논리 게이트라고 불리는 연산을 통해 결과를 산출하는 반면, 양자 컴퓨터는 양자 게이트 연산을 이용하여 계산 결과를 출력한다. 또한, 양자 컴퓨터에는 고전 컴퓨터에는 존재하지 않는 위상(phase) 개념이 존재한다.

때문에, ASCON-128의 양자 보안비도를 분석하기 위해서는 암호화 구조를 Grover oracle에 들어갈 양자 회로로 구현하는 과정이 필요하다.

본 장에서는 Fig. 2.의 ASCON-128 암호화 과정 중 초기 연산인 p^a를 양자 회로로 구현한다.

ASCON 암호화 구조의 p^a는 ASCON에서 사용되는 순열 연산으로 순차적으로 Addition of Constants, S-box, 그리고 Linear Diffusion 연산을 a번 반복하는 연산이며, ASCON-128에서 a값은 12이다.

4.1 Addition of Constants

상수를 더하기 위한 양자 회로는 고전 논리 부호 NOT과 같이 정보의 상태 반전 기능을 양자컴퓨팅 환경에서 수행하는 Pauli-X 게이트를 활용해 구현할 수 있다. 상기 기술은 ASCON 상수의 이진 표현을 기반으로 하며, 상수의 이진 표현에서 비트 값이 '1'과 같은 위치의 큐비트에 Pauli-X 게이트가 입력된다. 이때, 각 라운드 r에 이용되는 상수는 수식(1)을 통하여 계산된다[9].

$$Constant = 0xF0 - r \times 0x10 + r \times 0x01 \qquad (1)$$

상기 수식에서 r은 라운드 인덱스를 의미하며, 본 논문의 순열 연산은 총 12번의 라운드가 수행된다. 따라서, r은 0에서 11까지의 값을 가진다.

수식의 $-r \times 0x10$과 $+r \times 0x01$은 각 라운드에서 상수 값을 조정하는 요소로 해당 과정은 비트 수준에서의 연산으로 이루어진다. 때문에, +와 -의 연산은 XOR 연산으로 해석할 수 있다.

4.2 S-box

본 논문은 ASCON의 S-box 연산을 구현하기 위해 두 가지 접근 방법을 적용하였다.

첫 번째 방법에서는 고전 논리 연산으로 구성된 S-box 연산을 양자 연산으로 변환하여 회로를 구현하였다. 이때, Toffoli 게이트 이용을 위해 보조 큐비트를 사용하였다.

두 번째 구현 모델에는 BS(Bidirectional Synthesis)가 사용되었다. BS는 양자 회로 설계에서 사용되는 기법으로, 가역 게이트(reversible gate)를 이용하여 입력과 출력 상태를 동시에 고려해 회로를 설계하는 알고리즘이다. BS는 구현 대상의 입력에 따른 출력 결과 테이블을 입력받은 후 회로의 입력 측 또는 출력 측에 가역 게이트를 추가하며, 주어진 결과 테이블과 동일한 결과가 나오는 양자 회로를 생성한다[11].

4.2.1 고전 논리 연산 변환

ASCON의 S-box는 NOT, AND, 그리고 XOR 게이트로 동작하는 5비트 연산이다[9]. 따라서, 이와 동일한 기능을 양자컴퓨팅에서 제공하는

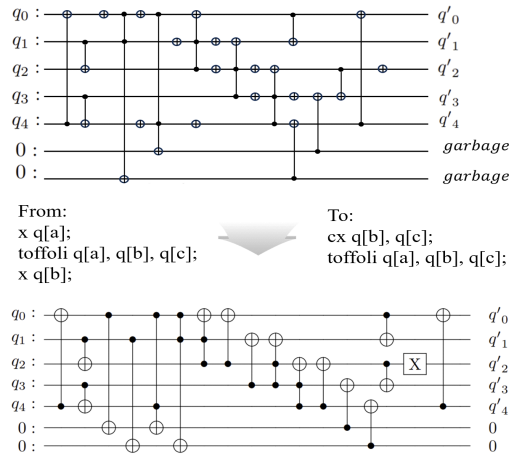

Fig. 3. Quantum circuit of ASCON S-box implemented using classical logic operation transformation technique and replace x q[a]; toffoli q[a], q[b], q[c]; x q[b]; sequence into cx q[b], q[c]; toffoli q[a], q[b], q[c];

Pauli-X, Toffoli, 그리고 CX의 3가지 양자 게이트를 사용하여 이를 대체할 수 있다.

Fig. 3.의 상단 그림은 두 개의 보조 큐비트를 사용한 ASCON의 S-box를 양자 회로로 구현한 결과이다. 보조 큐비트는 Toffoli 값의 저장을 위하여 이용되었다.

Fig. 3.의 하단 그림은 회로의 depth를 줄이기 위한 변환 작업을 추가한 결과이다. 이 과정에서 x q[a]; toffoli q[a], q[b], q[c]; x q[a];의 3 depth 회로는 cx q[b], q[c]; toffoli q[a], q[b], q[c];의 2 depth 회로로 변환되어 회로의 시간 자원량을 감소시켰다[14].

4.2.2 BS를 이용한 양자 회로 생성

BS 알고리즘은 입력 및 출력 상태 쌍으로 구성된 주어진 look up 테이블에 대해 각 쌍의 해밍 거리를 계산한다. 이를 통해 입력 상태에서 출력 상태로 전환하는 데 가장 적은 수의 상태 변경이 필요한 경로를 식별한다. 알고리즘은 출력 상태에 도달할 때까지 해밍 거리의 지속적인 계산에 따라 입력 또는 출력의 양쪽에서 양자 게이트를 점진적으로 적용한다[11].

그 후, Fig. 4.와 같이 생성된 게이트를 결합하여 ASCON의 S-box 양자 회로를 완성한다.

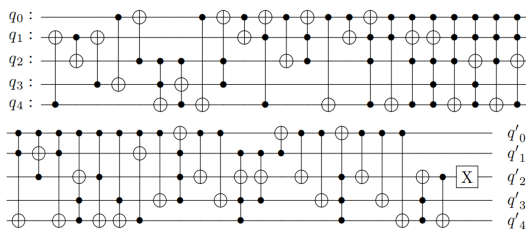

Fig. 4. Quantum circuit of ASCON S-box implemented using BS algorithm.

4.3 Linear Diffusion layer

ASCON의 LD(Linear Diffusion layer)는 x_0, x_1, x_2, x_3, x_4의 각 64비트의 5개 워드에 적용되는 XOR 및 우회전 연산으로 구성된다. LD는 320*320 이진 행렬로 효율적으로 표현할 수 있으며, 각 연산은 행렬 내의 특정 패턴에 해당한다. 본 연구에서는 수정된 XZLBZ 알고리즘을 사용하여 이를 효율적으로 구현한 결과를 활용하였다[15].

V. 보조 큐비트 상태 초기화

4.2.1의 방법과 같이 고전 논리 연산 변환을 이용하여 회로를 생성하면, 비교적 회로의 생성이 간단하다는 장점이 있지만 값의 저장을 위해 사용된 보조 큐비트 값이 초기화되지 않을 수 있다는 문제가 존재한다.

양자 회로에서 연산을 구현하기 위해 사용된 보조 큐비트 값이 초기화되지 않는 경우 일반 계산에 사용되는 큐비트의 신뢰성에도 영향을 미쳐 최종 연산 결과의 신뢰성에 의문을 남긴다.

이에 본 논문에서는 보조 큐비트의 상태를 초기화하는 알고리즘을 제안한다. 본 알고리즘은 최소한의 MCT(Multi Controlled Toffoli) 게이트를 이용하여 보조 큐비트의 상태를 최소화한다.

본 장에서는 ASCON-128의 큐비트 하나를 초기화하는 과정을 예시로 보조 큐비트 초기화 알고리즘을 서술한다.

(1) 알고리즘의 첫 단계에서는 보조 큐비트 a_0가 1로 설정되는 입력 큐비트 상태 집합을 식별한다. 이러한 상태는 정리 단계 시작 이전에 수행된 양자 연산을 분석하여 결정되며, 제어 큐비트 q_0, q_1, q_2, q_3, q_4의 모든 가능한 조합을 평가하여 $a_0 = 1$을 만드는 상태 집합을 찾는다. 이는 Table 1.의 (i)에 해당한다.

(2) 해당 입력 상태가 식별되면, 알고리즘은 다중 제어 Toffoli 게이트의 사용을 최소화하기 위한 경우를 탐색하는 과정을 거칩니다. 먼저 a_0를 1로 만드는 상태의 분포를 분석하여 가장 많이 나타나는 공통 값(예: $q_4 = 0$이 8번, $q_0 = 1$이 6번)을 순서대로 찾는다.

(3) (2)에서 발견한 공통 큐비트 패턴에 따라 MCT를 적용하여 a_0를 초기화한다. 이때, MCT는 최소한의 control 큐비트를 사용하도록 구성한다. Table 1의 경우 CCX q[0], q[4], a[0] 연산을 하였다.

(4) Table 1.의 (ii)와 같이 MCT 연산을 통해 오히려 a_0가 1이 되어버린 예외적인 경우를 처리하기 위한 추가 단계가 필요하다. 본 실험에서는 해당 경우 레지스터 q_0, q_1, q_2, q_4의 값이 동일함을 확인하여 C4X 게이트를 이용하여 $q_4 = 0$, $q_0 = 1$인 모든 경우

Table 1. Example of ancilla cleaup method: Cleaning up a_0 of quantum circuit for ASCON S-box

Input	(i)	(ii)	(iii)	Output
$q_0q_1q_2q_3q_4\ a_0a_1$	$q_0q_1q_2q_3q_4\ a_0a_1$	$q_0q_1q_2q_3q_4\ a_0a_1$	$q_0q_1q_2q_3q_4\ a_0a_1$	$q_0q_1q_2q_3q_4\ a_0a_1$
0: 00000 00	00000 00	00000 00	00000 00	00000 00
1: 00001 00	10101 00	10101 00	10101 00	10101 00
2: 00010 00	01011 00	01011 00	01011 00	01011 00
3: 00011 00	**1**100**0** 10	11000 00	11000 00	11000 00
4: 00100 00	10100 00	**101**0**0** 10	10100 00	10100 00
5: 00101 00	00001 00	00001 00	00001 00	00001 00
6: 00110 00	10111 00	10111 00	10111 00	10111 00
7: 00111 00	00100 10	00100 10	**001**0**0** 10	00100 00
8: 01000 00	01101 01	01101 01	01101 01	01101 01
9: 01001 00	11001 00	11001 00	11001 00	11001 00
10: 01010 00	01110 01	01110 01	01110 01	01110 01
11: 01011 00	**1**110**0** 10	11100 00	11100 00	11100 00
12: 01100 00	01001 01	01001 01	01001 01	01001 01
13: 01101 00	11101 00	11101 00	11101 00	11101 00
14: 01110 00	00010 01	00010 01	00010 01	00010 01
15: 01111 00	**1**000**0** 10	10000 00	10000 00	10000 00
16: 10000 00	**1**001**0** 10	10010 00	10010 00	10010 00
17: 10001 00	00101 00	00101 00	00101 00	00101 00
18: 10010 00	11011 00	11011 00	11011 00	11011 00
19: 10011 00	01010 00	01010 00	01010 00	01010 00
20: 10100 00	00110 10	00110 10	**001**1**0** 10	00110 00
21: 10101 00	10001 00	10001 00	10001 00	10001 00
22: 10110 00	00111 00	00111 00	00111 00	00111 00
23: 10111 00	10110 00	**101**1**0** 10	10110 00	10110 00
24: 11000 00	**1**111**0** 10	11110 00	11110 00	11110 00
25: 11001 00	01000 01	01000 01	01000 01	01000 01
26: 11010 00	11111 00	11111 00	11111 00	11111 00
27: 11011 00	01111 01	01111 01	01111 01	01111 01
28: 11100 00	**1**101**0** 10	11010 00	11010 00	11010 00
29: 11101 00	01100 01	01100 01	01100 01	01100 01
30: 11110 00	10011 00	10011 00	10011 00	10011 00
31: 11111 00	00011 01	00011 01	00011 01	00011 01

에 대해 a_0를 초기화했다.

(5) (4) 과정이 완료된 후 a_0가 1로 남아있는 값들의 경우에만 동작하는 MCT를 구성하여 a_0초기화를 완성한다. Table 1.의 경우 q_0, q_1, q_2, q_4의 값이 동일한 두 가지 경우가 남아있어 C4X 게이트를 이용하여 a_0 초기화를 완성하였다.

Fig. 5.는 Table 1.의 순서에 따라, a_0를 초기화하는 양자 회로이고, Fig. 6.은 상기 알고리즘을 통하여 ASCON S-box의 보조 큐비트를 초기화한 결과이다. 상기 과정을 통해 양자 자원을 보조 큐비트를 초기화하는 양자 회로가 생성된다.

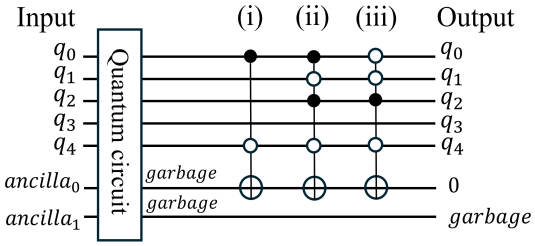

Fig. 5. Circuit for the function shown in Table 1.

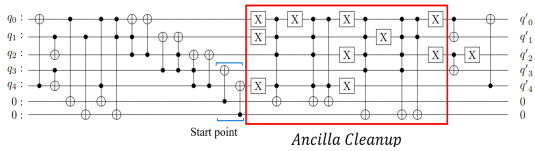

Fig. 6. Quantum circuit of ASCON s-box with ancilla qubit cleaned up

VI. 양자 자원량 측정

본 장에서는 앞서 구현된 ASCON-128 암호화 과정을 저수준(low level) 게이트 집합인 Clifford+T로 분해한 후, 양자 회로의 자원량과 Grover 키 탐색 알고리즘에 필요한 자원량을 측정한다. 양자 회로의 구현 및 시뮬레이션은 IBM의 qiskit 환경에서 진행되었다.

6.1 MCT 및 Toffoli 분해

고전 논리 연산 변환과 BS를 이용하여 생성한 양자 회로는 표준 양자 논리 게이트 모음에 포함되지 않는 C4X, C3X 게이트를 이용한다. 따라서, 우리는

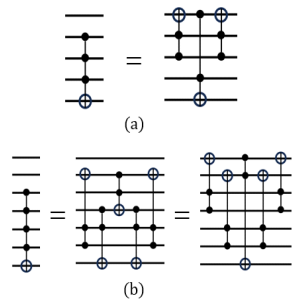

Fig. 7. MCT decomposition using Toffoli gate. (a) C3X decomposition (b) C4X decomposition

MCT 게이트를 Fig. 7.과 같이 분해하였다.

회로의 분해 이후에는 하나 이상의 같은 파라미터를 공유하는 게이트가 존재하는 경우 보조 큐비트를 추가함을 통해 병렬성을 향상하여 양자컴퓨팅의 시간 자원을 감소시켰다[12].

하지만, 위 과정을 진행한 후에도 저수준 게이트 집합인 Clifford+T의 구성을 벗어난 Toffoli 게이트가 존재하기 때문에, 이를 Clifford+T로 분해하는 과정이 필요하다.

본 논문에서는 M. Amy 등[13]이 제안한 T-depth가 4이고, Full depth가 8인 Toffoli 분해 모델을 통해 저수준의 양자 자원량을 측정한다.

6.2 자원량 측정 결과 요약

Table 2.는 ASCON 암호화 과정 중 S-box 생성에 필요한 양자 자원 요구량이다. Table 2.의 Ours-Clean은 고전 논리 연산 변환을 수행 후 보조 큐비트 초기화 거쳐 생성된 S-box 회로를 의미

Table 2. Quantum resources required to implement the 5 bit S-box of ASCON

Source	Width	# Garbage qubits	#CX	#1qCliff	#T	T-depth	Full depth
Ours-BS	6	0	292	91	315	157	363
	7	0	282	87	301	138	319
	8	0	284	87	301	135	312
	9	0	290	87	301	125	294
Ours-Clean	8	0	183	63	189	89	211
	9	0	133	47	133	50	124
	10	0	137	48	133	48	118
	11	0	139	47	133	45	112
Y.Oh[4]	15	5	51	16	35	4	14

하고, Ours-BS는 BS 알고리즘을 기반으로 설계된 S-box 양자 회로를 의미한다.

Ours-Clean과 Ours-BS의 자원량을 비교하면 8큐비트와 9큐비트를 사용하는 각각의 모델에서 동일 큐비트를 이용하는 모델임에도 Our-Clean이 더 낮은 양자 자원량을 요구한다. 이는 Ours-BS에서 사용된 BS 알고리즘이 특정 입력으로부터 특정 결과를 출력하기 위한 알고리즘이고, 이 과정에서 더 적은 자원량을 사용하는 구성을 찾는 것은 고려하지 않아 많은 양의 MCT 게이트를 요구하기 때문이다. MCT 게이트는 6.1에서 설명한 바와 같이 다수의 Toffoli로 분해가 되는데 이는 Clifford+T에서 T-depth가 4, Full depth가 8로 분해된다. Ours-Clean 모델에서도 보조 큐비트 초기화를 위해 MCT를 이용하나 이는 Ours-BS보다 현저히 적은 수이다. 본 연구에서 Ours-Clean은 4개의 C4X 게이트만을 요구하였지만, Ours-BS는 2개의 C4X와 9개의 C3X 게이트를 사용하였다.

본 연구에서 생성된 S-box와 Y. Oh 등[4]이 제안한 S-box를 비교한 결과 큐비트 수가 최대 9개, 최소 4개 덜 사용되었다. 반면 depth 자원은 본 연구에서 가장 적은 depth 자원이 소요되는 S-box와 비교하여도 14에서 112로 700%증가하였다.

하지만, 기존 연구에서 제안한 S-box는 보조 큐비트 초기화 과정을 진행하지 않았기에, 본 연구의 양자 회로는 모든 큐비트가 재사용이 가능하지만 기존 연구는 5개의 큐비트가 재사용이 불가능한 상태로 남는다. 이는, ASCON과 같은 동일 연산이 다수 반복되는 스펀지 암호 구조에서 많은 양의 garbage 큐비트를 생성하고, 더 이상 이용되지 않는 값과의 얽힘 상태로 하여금 회로 결과의 신뢰성에 의문을 남긴다.

ASCON-128 암호화 과정의 구현에 필요한 양자 자원 요구량은 ASCON S-box 연산의 회로 구현 방법에 따라 분류되어 Table 3.에 제시되었다.

Ours-Clean은 설계에 최소 512개의 큐비트와 3,936의 depth가 필요하고, 이에 보조 큐비트를 추가하여 depth를 감소시키는 방법을 적용 시, 704개의 큐비트까지 유효한 감소가 지속되며 depth는 2,760까지 감소한다.

Ours-BS는 최소 384개의 큐비트와 5,657의 depth가 필요하고, 이에 보조 큐비트를 추가하여 depth를 감소시키는 방법을 적용 시, 576개의 큐비트까지 유효한 감소가 지속되며 depth는 4,829까지 감소한다.

Table 3.은 ASCON-128 암호화의 양자 회로 구현에 필요한 자원 요구량을 보여준다. 상기 결과를 ASCON-128의 암호화를 구현한 이전 결과와 비교하면, 게이트 수와 depth의 자원량이 증가하였지만 요구 큐비트 수가 현저히 감소함을 확인할 수 있다.

또한, 큐비트 수와 depth 간의 상충관계와 연관된 비용인 $Td-M, FD-M, TD^2-M$, 그리고 FD^2-M가 기존 연구 결과 대비 가장 많이 감소하였을 때(576큐비트로 구성된 Ours-Clean 모델), 각각 85.65%, 83.73%, 28.24%, 그리고 7.13% 감소한 결과를 확인할 수 있다.

Table 4.는 위 결과를 바탕으로 NIST 양자 보안 기준에 따라 Grover 키 탐색 알고리즘에 필요한 자원량을 측정한 결과이다. Grover 키 탐색 알고리즘은 확률적으로 정확한 결과를 얻기 위하여 k비트 키에 대한 복구를 시도할 때마다 oracle 및 확산 연

Table 3. Quantum resources required to implement the encryption process of ASCON-128

Source	Width	#CX	#1qCliff	#T	T-depth	Full depth	Td-M	Fd-M	Td^2M	Fd^2M
Ours-BS	384	243,396	70,027	241,920	1,884	5,657	$1.38*2^{19}$	$1.04*2^{21}$	$1.27*2^{30}$	$1.43*2^{33}$
	448	235,716	66,955	231,168	1,656	5,129	$1.41*2^{19}$	$1.09*2^{21}$	$1.14*2^{30}$	$1.38*2^{33}$
	512	237,252	66,955	231,168	1,620	5,045	$1.58*2^{19}$	$1.23*2^{21}$	$1.25*2^{30}$	$1.52*2^{33}$
	576	241,860	66,955	231,168	1,500	4,829	$1.65*2^{19}$	$1.33*2^{21}$	$1.21*2^{30}$	$1.56*2^{33}$
Ours-Clean	512	159,684	48,523	145,152	1,044	3,936	$1.02*2^{19}$	$1.92*2^{20}$	$1.04*2^{29}$	$1.85*2^{32}$
	576	121,284	36,235	102,144	600	2,916	$1.32*2^{18}$	$1.60*2^{20}$	$1.55*2^{27}$	$1.14*2^{32}$
	640	124,356	37,003	102,144	576	2,844	$1.40*2^{18}$	$1.74*2^{20}$	$1.58*2^{27}$	$1.21*2^{32}$
	704	125,892	37,771	102,144	540	2,760	$1.45*2^{18}$	$1.85*2^{20}$	$1.53*2^{27}$	$1.25*2^{32}$
Y.Oh[4]	20,064	127,200	40,433	67,200	120	513	$1.15*2^{21}$	$1.23*2^{23}$	$1.08*2^{28}$	$1.23*2^{32}$

Table 4. Approximated cost of Grover key search for ASCON-128

Source	Width	#Gate	Full depth	T-depth	G-Fd	Fd-M	Td-M	Fd^2-M	Td^2-M
Ours-BS	385	$1.66*2^{83}$	$1.08*2^{77}$	$1.45*2^{75}$	$1.79*2^{160}$	$1.62*2^{85}$	$1.09*2^{84}$	$1.75*2^{162}$	$1.58*2^{159}$
	449	$1.60*2^{83}$	$1.97*2^{76}$	$1.27*2^{75}$	$1.58*2^{160}$	$1.73*2^{85}$	$1.11*2^{84}$	$1.70*2^{162}$	$1.41*2^{159}$
	513	$1.60*2^{83}$	$1.93*2^{76}$	$1.24*2^{75}$	$1.54*2^{160}$	$1.93*2^{85}$	$1.24*2^{84}$	$1.87*2^{162}$	$1.54*2^{159}$
	577	$1.62*2^{83}$	$1.85*2^{76}$	$1.15*2^{75}$	$1.50*2^{160}$	$1.04*2^{86}$	$1.30*2^{84}$	$1.93*2^{162}$	$1.49*2^{159}$
Ours -Clean	513	$1.06*2^{83}$	$1.51*2^{76}$	$1.60*2^{74}$	$1.60*2^{159}$	$1.51*2^{85}$	$1.60*2^{83}$	$1.14*2^{162}$	$1.28*2^{158}$
	577	$1.56*2^{82}$	$1.12*2^{76}$	$1.84*2^{73}$	$1.75*2^{158}$	$1.26*2^{85}$	$1.04*2^{83}$	$1.41*2^{161}$	$1.91*2^{156}$
	641	$1.58*2^{82}$	$1.09*2^{76}$	$1.77*2^{73}$	$1.72*2^{158}$	$1.36*2^{85}$	$1.11*2^{83}$	$1.49*2^{161}$	$1.96*2^{156}$
	705	$1.59*2^{82}$	$1.06*2^{76}$	$1.66*2^{73}$	$1.69*2^{158}$	$1.46*2^{85}$	$1.14*2^{83}$	$1.55*2^{161}$	$1.90*2^{156}$
Y.Oh[4]	20,065	$1.41*2^{82}$	$1.57*2^{73}$	$1.47*2^{71}$	$1.11*2^{156}$	$1.92*2^{87}$	$1.80*2^{85}$	$1.51*2^{161}$	$1.32*2^{157}$

산을 $\lfloor \pi/4 \times \sqrt{2^k} \rfloor$ 반복하여야 한다.

그러나, 확산 연산자의 오버헤드는 양자 회로 내에서 유의미한 자원량을 차지하지 않으므로 무시할 수 있다. 따라서, 본 논문에서는 Grover oracle의 반복에 필요한 비용만을 계산하였다. 반복 비용의 계산은 [4]의 $Table 2 \times 2 \times \lfloor \pi/4 \times \sqrt{2^k} \rfloor$ 계산식을 따라 산출하였다.

VII. 결 론

Grover 키 탐색 알고리즘에 대한 암호의 양자 보안비도 분석을 위해서는 암호화 구조를 양자 회로로 설계하는 과정이 필요하다. 본 논문에서는 키 탐색 알고리즘에 적합하도록 추가 데이터 처리와 최종화 과정을 생략하여 암호문 생성과 직접적으로 관련이 있는 부분만을 포함하도록 암호화 과정을 간략화하였다. 또한, Clifford+T 게이트 모음을 이용하지 않거나 보조 큐비트 상태를 초기화하지 않은 기존 논문들의 한계를 극복하는 새로운 ASCON 암호화 회로를 제시하였다. 본 연구에서 제시한 양자 회로는 크게 두 가지 과정으로 나뉘어 생성된다. 첫 번째 과정은 BS 혹은 고전 논리 연산 변환을 통한 양자 회로 생성이다. 상기 과정에서 BS의 경우에는 보조 큐비트를 이용하지 않는 알고리즘이기 때문에, 고전 논리 연산 변환을 통한 양자 회로 생성 결과물에만 MCT를 이용한 보조 큐비트 초기화 기법을 적용했다. 상기 과정을 완료한 후에는 회로의 자원 감소를 위해 선형 계층 변환과 보조 큐비트를 이용하는 단계를 거쳐 회로 최종 결과물을 생성하였다.

회로 생성 후, 양자 자원량을 측정한 결과 기존의 논문과 비교하여 보조 큐비트 초기화를 진행했음에도 불구하고, 큐비트 수와 depth 간의 상충관계 관계와 관련된 시-공간 복잡도가 기존결과 대비 감소함을 확인할 수 있었다.

또한, Grover 키 탐색 알고리즘에 대한 자원량을 측정하여 NIST가 제시한 양자 보안비도의 정량적 측정 데이터를 제공하였다. NIST에서 제시한 암호의 Grover 키 탐색 알고리즘에 대한 보안비도는 양자 게이트 수와 depth를 곱한 G-FD 자원으로 평가되며, 기준에 따르면 본 연구에서 구현한 ASCON-128과 같은 128비트의 키 블록 암호는 G-FD 값이 2^{157}을 달성하여야 한다[16].

본 연구 결과에 따르면, 보조 큐비트 초기화가 수행된 결과 중 가장 작은 G-FD를 가지는 결과는 705큐비트를 이용하는 Ours-Clean이며, 상기 결과를 통해 ASCON이 NIST 보안비도 기준을 만족함을 재확인했다.

위와 같은 결과는 양자컴퓨팅 환경에서 ASCON의 양자 보안비도 분석에 도움이 될 것으로 기대한다.

References

[1] M. Njorbuenwu, B. Swar, and P. Zavarsky, "A survey on the impacts of quantum computers on information security," 2019 2nd International conference on data intelligence and security (ICDIS), IEEE, pp. 212-218, June. 2019.

[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, Jul. 1996.
[3] Y. Zheng, Q. Luo, Q. Li, and Y. Lv, "Quantum circuit implementations of lightweight authenticated encryption ASCON," The Journal of Supercomputing, pp. 1-16, Jan. 2024.
[4] Yujin Oh, Kyungbae Jang, Anubhab Baksi, and Hwajeong Seo, "Depth-Optimized Quantum Circuits for ASCON: AEAD and HASH," Mathematics 12, no. 9, p. 1337, Apr. 2024.
[5] Cryptology ePrint Archive: Kyungbae Jang, Anubhab Baksi, Hyunji Kim, Gyeongju Song, Hwajeong Seo, and Anupam Chattopadhyay, "Quantum analysis of AES," Cryptology ePrint 2022-683, May. 2022.
[6] V. Vedral, and M.B. Plenio, "Basics of quantum computation," Progress in quantum electronics 22, no. 1: pp. 1-39, Jan. 1998.
[7] W.K. Wootters, and Wojciech H. Zurek, "A single quantum cannot be cloned," Nature 299.5886: pp. 802-803, Oct. 1982.
[8] V. Bužek, and M. Hillery, "Quantum copying: Beyond the no-cloning theorem," Physical Review A 54.3: p. 1844, Sep. 1996.
[9] C. Dobraunig, Ma. Eichlseder, F. Mendel, and M. Schläffer, "Ascon v1. 2: Lightweight authenticated encryption and hashing," Journal of Cryptology 34: pp. 1-42, Jul. 2021.
[10] ICAR eprint archive: R. Ankele, and R. Ankele, "Software benchmarking of the 2nd round caesar candidates," IACR ePrint 2016-740, Oct. 2016.
[11] D.M Michael, D. Maslov, and G.W. Dueck, "A transformation based algorithm for reversible logic synthesis," Proceedings of the 40th annual Design Automation Conference, pp. 318-323. Jun. 2003.
[12] N. Abdessaied, R. Wille, M. Soeken, and R. Drechsler, "Reducing the depth of quantum circuits using additional circuit lines," In Reversible Computation: 5th International Conference, RC 2013, Victoria, BC, Canada, July 4-5, 2013. Proceedings 5, Springer Berlin Heidelberg, pp. 221 - 233, Jul. 2013.
[13] M. Amy, D. Maslov, M. Mosca, and M. Roetteler, "A meet-in-the-middle algorithm for fast synthesis of depth-optimal quantum circuits," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 32, no. 6: pp. 818-830, May. 2013.
[14] Jongheon Lee, Yousung Kang, You-Seok Lee, Boheung Chung, and Dooho Choi, "MPMCT gate decomposition method reducing T-depth quickly in proportion to the number of work qubits," Quantum Information Processing 22.10: p. 381, Oct. 2023.
[15] Cryptology ePrint Archive: S. Roy, A. Baksi, and A. Chattopadhyay, "Quantum implementation of ascon linear layer," Cryptology ePrint 2023-617, Apr. 2023.
[16] "Submission requirements and evaluation criteria for the post-quantum cryptography standardization process," NIST, CFP, 2016.

〈저자소개〉

오 진 섭 (Jinseob Oh) 학생회원
2021년 3월~현재: 고려대학교 세종캠퍼스 인공지능사이버보안학과 학사
〈관심분야〉 양자 회로 설계, 양자 컴퓨팅, 암호 엔지니어링, 무선 통신

최 찬 호 (Chanho Choi) 종신회원
2005년 2월: 충남대학교 컴퓨터공학 학사
2021년 1월~2023년 1월: (주)시스메이트 책임연구원
2023년 2월~2023년 12월: (주)이음소프트 대표이사
2024년 8월: 고려대학교 융합과학대학원 이학석사
2024년 1월~현재: 고려대학교 세종캠퍼스 산업기술연구소 연구원
〈관심분야〉 사이버 보안, 양자 암호 보안

최 두 호 (Dooho Choi) 종신회원
1994년 2월: 성균관대학교 수학과 졸업
1996년 2월: KAIST 수학과 석사
2002년 2월: KAIST 수학과 박사
2002년 1월~2021년 2월: 한국전자통신연구원 정보보호연구본부 실장
2021년 3월~현재: 고려대학교 세종 인공지능상비버보안학화 교수
〈관심분야〉 암호 양자분석, 부채널분석, IoT보안, 암호엔지니어링