KIPS Trans. Comp. and Comm. Sys.
Vol.12, No.6 pp.181~188
ISSN: 2287-5891 (Print), ISSN 2734-049X (Online)

https://doi.org/10.3745/KTCCS.2023.12.6.181

Post-Quantum Security Strength Evaluation through Implementation of Quantum Circuit for SIMECK

Song Gyeong Ju† · Jang Kyung Bae† · Sim Min Joo† · Seo Hwa Jeong††

ABSTRACT

Block cipher is not expected to be safe for quantum computer, as Grover's algorithm reduces the security strength by accelerating brute-force attacks on symmetric key ciphers. So it is necessary to check the post-quantum security strength by implementing quantum circuit for the target cipher. In this paper, we propose the optimal quantum circuit implementation result designed as a technique to minimize the use of quantum resources (qubits, quantum gates) for SIMECK lightweight cryptography, and explain the operation of each quantum circuit. The implemented SIMECK quantum circuit is used to check the estimation result of quantum resources and calculate the Grover attack cost. Finally, the post-quantum strength of SIMECK lightweight cryptography is evaluated. As a result of post-quantum security strength evaluation, all SIMECK family cipher failed to reach NIST security strength. Therefore, it is expected that the safety of SIMECK cipher is unclear when large-scale quantum computers appear. About this, it is judged that it would be appropriate to increase the block size, the number of rounds, and the key length to increase the security strength.

Keywords : SIMECK Quantum Circuit, Grover Algorithm, Quantum Computing, Quantum Security Strength

SIMEC 경량암호에 대한 양자회로 구현 및 Post-Quantum 보안 강도 평가

송 경 주† · 장 경 배† · 심 민 주† · 서 화 정††

요 약

Grover 양자 알고리즘은 brute-force attack 가속화로 대칭키 암호의 보안 강도를 크게 감소시키므로 기존 블록 암호가 양자 컴퓨터에 안전하지 않을 것이라 예상한다. 따라서 대상 암호에 대한 양자회로 구현을 통해 Post-quantum 보안 강도를 확인하여 대규모 양자 컴퓨터 시대에 대비할 수 있다. 본 논문에서는 모든 SIMECK 경량 암호군에 대해 양자 자원(큐비트, 양자 게이트)을 최소화 한 기법으로 설계된 최적의 양자회로 구현 결과를 제시하고 각 함수별 양자 회로 동작을 설명한다. 마지막으로 제안된 SIMECK 양자회로에 대한 양자자원 추정 결과를 SIMON 양자 회로 결과와 비교하고 Grover 공격 비용을 계산하여 SIMECK 경량암호의 Post-quantum 보안 강도를 평가한다. Post-quantum 보안 강도 평가 결과 모든 SIMECK 경량 암호군이 NIST 보안 강도에 도달하지 못했다. 따라서 대규모 양자 컴퓨터 등장 시 SIMECK 암호의 안전성이 불명확하다고 예상하며 이에 대해 본 논문에서는 보안 강도를 높이기 위한 방안으로 블록사이즈 및 라운드 수와 키 길이를 증가시키는 것이 적합하다고 판단한다.

키워드 : SIMECK 양자회로, 그루버 알고리즘, 양자 컴퓨팅, 양자 보안 강도

1. 서 론

양자 컴퓨터는 큐비트의 성질로 인해 특정 문제에 대해 기존 컴퓨터보다 빠른 계산 속도로 해결할 수 있다고 알려져 있으며 대규모 양자 컴퓨터의 등장은 기존 암호체계를 위협할 것이라 예상한다. Shor algorithm[1]은 1994년 Peter Shor에 의해 제안된 양자 알고리즘으로 기존 공개키 암호의 기반문제였던 인수분해, 이산로그 등의 문제를 다항시간 내에 해결할 수 있어 공개키 암호의 안전성을 위협한다. Grover algorithm[2]은 1996년 Lov Grover에 의해 제안된 양자 알고리즘으로 대칭키 암호에 대한 brute-force attack을 가속화 시켜 n-bit key 블록암호의 보안 강도를 $\sqrt{n}$-bit 수준으로 감소시킨다. 대규모 양자컴퓨터에 대비하기 위해서는 기존의 암호가 Post-quantum 시대에서도 안전한지 판단해야 하며, 안전하지 않다고 판단될 시 양자 컴퓨터에서의 보안 강도를 높이는 방법을 고안하거나 양자 내성 암호로의 교체가 필요하다. 블록 암호에 대한 post-quantum 강도를 평가

※ This work was supported by Institute for Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (〈Q|Crypton〉, No.2019-0-00033, Study on Quantum Security Evaluation of Cryptography based on Computational Quantum Complexity, 100%)..
※ 이 논문은 2022년 한국정보처리학회 ACK 2022의 우수논문으로 "SIMECK에 대한 양자회로 최적화 구현"의 제목으로 발표된 논문을 확장한 것임.
† 준 회 원 : 한성대학교 정보컴퓨터공학과 박사과정
†† 종신회원 : 한성대학교 융합보안학과 부교수
Manuscript Received : December 19, 2022
Accepted : January 26, 2023
* Corresponding Author : Seo Hwa Jeong(hwajeong84@gmail.com)

하기 위해서는 공격 대상 암호에 대한 양자 회로의 구현이 필요하며 Grover algorithm에 필요한 양자 자원을 추정하여 평가 할 수 있다. 현재의 양자컴퓨터는 양자회로 동작에 필요한 큐비트와 양자 게이트가 한정적이며 큰 Depth에 대해서는 오류로 인해 실질적인 동작이 어렵다. 따라서 양자 회로 동작에 필요한 양자 게이트와 Depth를 줄이기 위해 암호를 양자회로로 최적화 구현하고 양자 알고리즘 공격에 필요한 양자 자원을 추정하는 선행연구들이 많이 진행되었다[3-9].

본 논문에서는 기존 경량 암호 SIMON 과 SPECK 의 장점을 결합하여 설계된 SIMECK 경량암호에 대한 Post-quantum 보안 강도를 확인하기 위해 해당 암호에 대한 효율적인 양자회로를 최초로 제안한다. 제안하는 SIMECK 양자회로 구현에서는 양자 자원을 효율적으로 사용하기 위한 방안을 적용하여 사용하는 양자 자원의 줄였으며 이에 대해 SIMECK 양자회로 자원 추정 결과를 제시하고 비슷한 경량 암호군인 SIMON 과 비교하여 평가하였다. 또한, 제안하는 SIMECK 양자회로를 통해 Grover's algorithm 공격 비용을 추정하여 Post-quantum 보안 강도를 확인하고 결과를 바탕으로 추후 SIMECK 경량암호의 보안 강도를 높이는 방안을 고안하였다.

논문의 구성은 다음과 같다. Section 2에서는 논문을 이해를 돕기 위한 양자 컴퓨터, Grover algorithm, SIMECK 경량 암호에 대한 관련 연구를 작성하였으며 Section 3에서는 본 논문에서 제안하는 SIMECK 양자회로 구현에 대해 설명한다. Section 4는 제안하는 양자회로의 자원을 추정하고 추정 결과를 통해 SIMECK 경량암호의 보안강도를 확인한다. 마지막으로 Section 5에서 결론으로 논문을 마무리한다.

2. 관련 연구

2.1 양자 컴퓨터

양자컴퓨터는 큐비트의 양자역학적인 현상을 이용하여 데이터를 처리하는 컴퓨터이다. 큐비트의 중첩 및 얽힘 성질로 인해 n개의 큐비트로 2^n개의 데이터를 표현하고 한 번에 처리할 수 있어 일반적이 컴퓨터보다 훨씬 빠른 연산이 가능하다. 양자컴퓨터에서는 일반적인 컴퓨터에서 사용하는 논리 게이트와 유사한 양자 게이트를 사용하여 큐비트를 제어한다. 양자 게이트는 가역적인 특징을 가지기 때문에 역연산이 가능하다는 특징이 있다. 대표적인 양자게이트는 Fig. 1과 같다.

X gate는 하나의 입력 큐비트에 대해 상태를 반전시킨다. CNOT gate는 두 개의 입력 큐비트가 각각 control 큐비트, target 큐비트가 되며 control 큐비트가 1일 때만 target 큐비트의 상태가 반전된다. Toffoli gate는 세 개의 입력 큐비트 중 두 개의 큐비트가 control 큐비트, 한 개의 큐비트가 target 큐비트가 되며 두 개의 control 큐비트가 모두 1일 때만 target 큐비트가 반전된다. Swap gate는 두 큐비트의 위상을 서로 바꿔주며 양자 비용이 없는 게이트이다. 이와 같은 양자

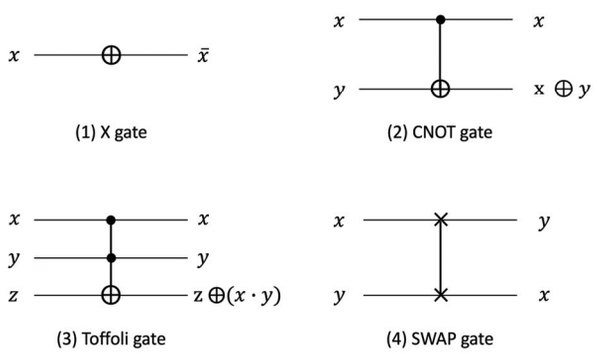

Fig. 1. Quantum Circuit

게이트와 큐비트로 구성된 회로를 양자회로라고 언급하며 양자회로에서는 양자 데이터 사이에서의 연산만 가능하다.

2.2 Grover Algorithm

Grover algorithm은 1996년 Lov Grover가 제안한 양자 탐색 알고리즘이다. 일반적인 컴퓨터에서는 정렬되지 않은 N개의 데이터에서 특정 데이터를 찾는데 N번의 탐색이 필요하다. 하지만 양자 컴퓨터상에서 Grover algorithm을 사용하면 $\sqrt{N}$번의 탐색만으로 특정 데이터를 찾을 수 있다. 이러한 Grover algorithm을 대칭키 암호의 정답 key를 찾기 위한 brute-force attack에 사용하여 기존 n-bit 보안 레벨의 암호를 $\sqrt{n}$-bit 보안 레벨로 감소시킬 수 있다. Fig. 2는 4-bit 키를 사용하는 대칭키 암호에 대한 Grover algorithm의 동작을 보여준다.

Grover algorithm은 블록암호의 평문-암호문 쌍을 알고 있을 때 수행 할 수 있는 Known-Plaintext Attack(KPA)의 한 종류이며 크게 Oracle과 Diffusion operator로 동작한다. key는 Oracle에 입력되기 전에 Hadamard gate를 통해 중첩상태가 되어 Oracle에서 사용된다. Oracle 내부에는 암호화-복호화 양자회로가 위치하며 평문-암호문 쌍을 생성하는 정답 key를 찾는다. Diffusion operator는 Oracle에서 찾은 정답 key의 측정 확률을 높여준다. Grover algorithm은 약 $\left\lfloor \frac{\pi}{4}\sqrt{2^n} \right\rfloor$ 번의 반복으로 정답을 높은 확률로 찾을 수 있다.

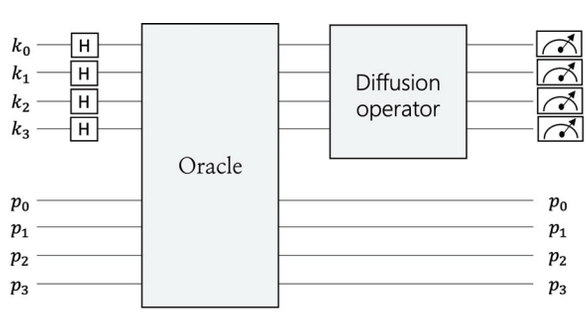

Fig. 2. Grover Algorithm (key size = 4)

2.3 SIMECK 경량 암호

SIMECK은 SIMON 과 SPECK 의 장점을 결합하여 설계된 경량암호이다[10]. SIMECK에서는 SIMON의 라운드 함수를 수정해서 사용하며 SPECK과 유사하게 키 스케줄 함수에서 재사용한다. 경량 암호군인 SIMECK은 SIMECK-$2n/mn$으로 표기되며, n은 word 크기를 나타내고 16, 24, 32 중 하나의 값을 가진다. 따라서 $2n/mn$은 (block size)/(key size)를 나타내며 Feistel 구조의 라운드 함수와 키 스케줄 함수 로 동작한다. Equation (1)은 SIMECK의 라운드 함수의 동작을 보여준다.

$$R_{k_i}(l_i, r_i) = (r_i \oplus f(l_i) \oplus k_i, l_i) \tag{1}$$

평문은 두 word l_0, r_0 로 나뉘며, 상위 n비트가 l_0이 되며 하위 n비트가 r_0가 된다. 두 word는 계속 나뉘어 동작하며 마지막 암호문 출력에서 합쳐진다. 라운드 함수의 내부 함수는 $f(x) = (x \odot (x \lll 5)) \oplus (x \lll 1)$로 정의되며 Fig. 3과 같다.

함수의 내부에서는 두 개의 입력 l_i, r_i중 첫 번째 입력 l_i의 rotation을 통한 AND 값을 두 번째 입력에 r_i에 XOR하는 연산이 수행된다. 키 스케줄에서 생성된 키 k_i는 라운드 함수의 두 번째 입력 r_i에 XOR된다. 키 스케줄 함수는 라운드 함수와 같은 내부함수로 동작하고 동작은 다음과 같다 :

$$\begin{cases} k_{i+1} = t_i \\ t_{j+3} = k_i \oplus f(t_i) \oplus C \oplus (z_j)_i \end{cases}$$

키 스케줄 함수에서 사용되는 C는 고정된 Constant 값이며 매 라운드 업데이트 된다.

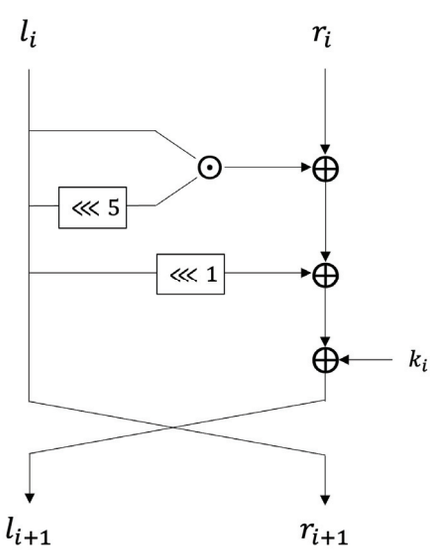

Fig. 3. SIMECK Round Function Operation

3. SIMECK 양자회로 구현

본 논문에서는 SIMECK 경량암호에 대한 양자회로 구현을 제시하고 암호 공격에 필요한 양자자원을 추정에 사용한다. 제안하는 양자회로는 사용 큐비트 수 및 양자자원을 줄이기 위한 방식을 사용하여 효율적인 양자회로를 설계하였다.

양자회로에서 큐비트의 임시 값을 저장하기 위해서는 temp 큐비트를 할당하여 사용해야 할 뿐만 아니라 temp 큐비트를 재사용하기 위해 inverse 연산이 추가되므로 양자자원 측면에서 매우 비효율적인 설계가 된다. 따라서 제시하는 양자회로에서는 처음 입력 메시지, key를 저장하기 위해 할당한 큐비트 이외에 추가 temp 큐비트를 사용하지 않도록 하여 양자자원 측면에서의 최적의 양자회로로 동작한다.

SIMECK-32/64는 입력 메시지 블록을 저장하기 위한 32 큐비트, key를 저장하기 위한 64 큐비트를 사용한다. SIMECK-48/96는 입력 메시지 블록을 저장하기 위한 48 큐비트, key를 저장하기 위한 96 큐비트를 사용하며 SIMECK-64/128에서는 메시지 블록을 저장하기 위한 64큐비트, key를 저장하기 위한 128 큐비트를 사용한다.

결과적으로 제안하는 SIMECK 양자회로는 Toffoli gate를 사용하여 덧셈 중간에 발생하는 temp 값을 따로 저장해두지 않고 바로 연산 대상 큐비트에 계산되도록 하였다. 이러한 방식은 temp 큐비트를 할당하지 않고 동작하기 때문에 큐비트 사용을 줄일 수 있다. 전체적인 SIMECK 양자회로의 구조는 Fig. 4와 같다. 내부는 Round function과 Key schedule의 반복으로 동작하며 Round 수 n만큼 두 함수를 반복한다. 이때, 마지막 라운드는 Key Schedule 함수를 제외하고 Round function만 동작한다. (SIMECK-32/48 : 32 라운드, SIMECK-48/96 : 36 라운드, SIMECK-64/128 : 44 라운드)

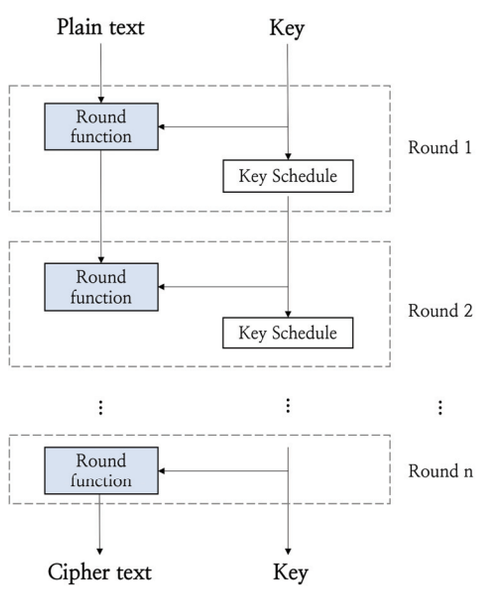

Fig. 4. SIMECK Quantum Circuit Structure

Algorithm 1. SIMECK quantum circuit for round function

Input : l_r, r_r
Output : l_r, r_r, k_r

1 : **for** i **in range**(length(r_r)):
2 : $r_r \leftarrow$ **Toffoli**($l_r[i]$, $l_r[(i \gg 11) \bmod n]$, $r_r[i]$)
3 : $r_r \leftarrow$ **CNOT**($l_r[(i \gg 15) \bmod n]$, $r_r[i]$)

4 : **for** i **in range**(length(r_r)):
5 : $r_r \leftarrow$ **CNOT**($k_r[i]$, $r_r[i]$)

6 : **Swap**(l_r, r_r)

Algorithm 1. SIMECK Quantum Circuit for Round Function

Algorithm 2. SIMECK quantum circuit for key schedule

Input : key_0, key_1, key_2, key_3, constant
Output : key_0, key_1, key_2, key_3

1 : **for** i **in range**(length(key_1)) :
2 : $r_r \leftarrow$ **Toffoli**(key_1,$key_1[(i \gg 11) \bmod n]$, $key_0[i]$)
3 : $r_r \leftarrow$ **CNOT**($key_1[(i \gg 15) \bmod n]$, $key_0[i]$)

4 : **if** constant[i] == 1
5 : X (key_0)

6 : **Swap**(key_0, key_1)
7 : **Swap**(key_1, key_2)
8 : **Swap**(key_2, key_3)

Algorithm 2. SIMECK Quantum Circuit for Key Schedule

Algorithm 1은 SIMECK의 Round function에 대한 양자회로 동작을 보여준다. line 1~3 과 line 4~5의 반복문에서는 l_r의 값을 유지하며 r_r값만 업데이트 되도록 한다. Toffoli gate와 CNOT gate의 Target 큐비트를 r_r로 설정하여 l_r의 값이 중간에 변경 없이 계산되어 기존의 l_r을 저장하기 위한 temp 큐비트를 사용하지 않았다. 또한 line 1~3에서 l_r의 Shift 연산에 대해 Swap gate 사용 대신 반복문의 인덱스 변경을 통해 동작하여 양자회로 Depth를 줄인다.

Algorithm 2는 SIMECK의 Key schedule function을 보여준다. 클래식 컴퓨터에서는 라운드 함수와 키 스케줄 함수가 동일한 알고리즘으로 수행되지만 제안하는 양자회로는 사용 양자 자원을 줄이기 위해 키 스케줄 함수를 조금 변경하였다.

Algorithm 2 input의 key_0, key_1, key_2, key_3는 기존 n-bit key를 맨 앞 인덱스부터 n/4 크기 씩 4개의 key로 나눈 것이다. Constant는 정해진 상수 값이며 각 라운드마다 Equation (2)를 통해 업데이트 되어 키 스케줄 함수에서 사용된다.

$$\begin{aligned} Constant &= Constant \,\&\, \mathrm{0xFFFC} \\ Constant &= Sequence \,\&\, 1 \\ Sequence &= Sequence \gg 1 \end{aligned} \tag{2}$$

Equation (2)는 SIMECK32/48 기준으로 작성되었다. 초기 Constant는 (블록 사이즈)/(키 사이즈)에 따라 SIMECK SIMECK32/48 : 0xFFFC, SIMECK48/96 : 0xFFFFC, SIMECK64/128 : 0xFFFFFFFC 으로 고정되며 Constant 업데이트 수식에 사용되는 Sequence는 SIMECK32/48 와 SIMECK64/128는 0x9A42BB1F 로 동일하게 사용하며 SIMECK64/128는 0x938BCA3083F 로 고정된다. Constant 업데이터는 classic 데이터의 연산이므로 별로의 양자자원을 사용하지 않는다.

기존 SIMECK 암호 Key schedule function의 전체적인 동작은 Round function과 동일하다. 하지만 Round function은 〈Algorithm 1〉의 line 4~5와 같이 key와 메시지 블록 간의 CNOT gate 연산을 진행하지만 Key schedule function에서는 Key와 Constant 간의 CNOT gate 연산을 수행한다는 차이점이 있었다. 이에 대해 Round function은 두 연산 대상이 모두 quantum data 이므로 데이터 변환 없이 CNOT gate 연산이 진행된다. 반면 Key schedule function에서 두 데이터에 CNOT gate를 사용하기 위해서는 classic data인 Constant 값을 큐비트로 할당하여 진행해야하며 큐비트로 할당된 Constant의 업데이트 진행 또한 classic 데이터 연산에서 quantum 데이터 연산으로 변환되므로 매 라운드 Constant 업데이트 연산에 필요한 양자 자원을 사용해야 한다. 이것은 양자자원 측면에서 비효율적이므로 제안 양자회로에서는 Constant와 Key가 큐비트 간의 quantum to quantum 연산이 아닌 classic 상수 값 상태에 따른 classic to quantum 연산이 진행되도록 설계하였다. 해당 방식은 Constant 업데이트와 Key 업데이트에 사용되는 큐비트 및 양자 게이트를 줄일 수 있도록 한다. Constant는 이미 알려진 상수이므로 사전 연산 테이블에 매 라운드 별 Constant를 저장하고 각 라운드에서 Constant의 해당 인덱스 비트 값이 1인 부분과 동일한 Key 인텍스에 X gate가 동작하도록 하였다. 이러한 방법은 또한 CNOT gate 보다 더

저렴한 X gate 사용으로 대체할 수 있어 양자 자원 측면에서 매우 효율적이다.

4. 양자자원 추정 및 평가

4.1 SIMECK 양자회로 양자자원 추정 결과

본 논문에서는 양자자원 측면에서 효율적인 SIMCEK 양자회로 구현을 제시하였다. 양자회로 설계에는 projectQ의 양자 프로그래밍 툴을 사용하여 해당 암호에 대한 양자회로를 구현하였으며 동작에 필요한 양자 자원을 추정했다.

Table 1은 SIMECK에서 제공하는 모든 (블록 크기)/(키 길이)에 대한 양자회로 자원 추정 결과이며 제시된 양자자원 추정 결과는 암호화가 한번 진행될 때 필요한 양자자원을 보여준다.

해당 논문은 SIMECK에 대한 첫 번째 양자회로 구현이므로 효율적인 양자회로에 대한 결과를 비교하기 위한 SIMECK 양자회로 선행 연구가 없다. 따라서 우리는 SIMECK과 비슷한 경량 암호군인 SIMON 경량암호의 양자회로 구현 결과와 비교하여 확인한다. Table 2은 [7]에서 제시한 SIMON 양자자원 추정 결과를 보여준다. SIMECK 과 동일한 (블록 사이즈)/(키 사이즈)를 가지는 SIMON의 양자 자원을 비교하였을 때, 양자 게이트 측면에서 SIMECK이 더 적은 X gate와 CNOT gate를 사용 하였으며 더 많은 Toffoli gate를 사용하였다. 양자회로 Depth 측면에서는 SIMECK 양자회로가 SIMON 양자회로 보다 훨씬 적은 Depth로 구현되었다.

Grover algorithm 동작은 Oracle과 Diffusion operator의 반복으로 동작하며 암호화 양자회로는 Oracle 내부에 위치한다. 한 번의 Oracle 동작에서는 암호화 및 복호화 양자회로가 동작하며 총 Grover algorithm 반복 횟수 $\left\lfloor \frac{\pi}{4}\sqrt{2^n} \right\rfloor$ 만큼 반복된다. 따라서 SIMECK에 대한 Grover 공격 비용은 〈Table 1〉$\times 2 \times \left\lfloor \frac{\pi}{4}\sqrt{2^n} \right\rfloor$ 로 계산된다. Table 3은 SIMECK에 대해 Grover algorithm을 적용하기 위해 필요한 양자자원 결과를 보여준다.

Table 1. Quantum Resource Estimation Results for SIMECK Quantum Circuit

Algorithm	Quantum resources			
	X	CNOT	Toffoli	Depth
SIMECK 32/64	434	1,520	1,008	193
SIMECK 48/96	770	2,568	1,704	325
SIMECK 64/128	1,290	4,192	2,784	355

Table 2. Quantum Resource Estimation Results for SIMON Quantum Circuit[7]

Algorithm	Quantum resources			
	X	CNOT	Toffoli	Depth
SIMON 32/64	448	2,816	512	946
SIMON 48/96	768	4,800	864	1,597
SIMON 64/128	1,216	7,396	1,408	2,643

Table 3. Quantum Resources Required for Grover Attack on SIMECK

Algorithm	Quantum resources			
	X	CNOT	Toffoli	Depth
SIMECK 32/64	1.7×2^{41}	1.48×2^{43}	1.97×2^{42}	1.51×2^{40}
SIMECK 48/96	1.5×2^{58}	1.25×2^{60}	1.66×2^{59}	1.27×2^{57}
SIMECK 64/128	1.6×2^{75}	1.02×2^{77}	1.36×2^{76}	1.39×2^{73}

Level 1	Block ciphers using 128-bit key (e.g. AES 128) require computational resources that are greater than or comparable to those required for key search.
Level 3	Block ciphers using 256-bit key (e.g. AES 256) require computational resources that are greater than or comparable to those required for key search.
Level 5	Block ciphers using 512-bit key (e.g. AES 512) require computational resources that are greater than or comparable to those required for key search.

Fig. 5. Security Strength Evaluation Criteria Presented by NIST[11]

4.2 SIMECK post-quantum 보안 강도 평가

본 논문에서는 SIMECK에 대한 양자게이트 및 양자회로 Depth의 종합적인 수치를 비교하기 위해 양자 Cost를 계산하여 SIMECK에 대한 post-quantum 보안 강도를 평가한다. 양자 자원에 대한 Cost 계산 결과는 SIMECK에 대한 post-quantum 보안 강도를 평가하는데 사용할 수 있으며 post-quantum 보안 강도 기준은 NIST에서 공개한 평가 기준에 따른다. NIST[11]에서 제시한 평가 기준은 Fig. 5와 같다.

블록암호는 총 3개의 카테고리로 구분된다. Level 1은 128-bit 키를 사용하는 블록암호(ex. AES-128)의 키 검색에 필요한 것과 같거나 더 많은 리소스가 필요하다. Level 2는 256-bit 키를 사용하는 블록암호(ex. AES-256)의 키 검색에 필요한 것과 같거나 더 많은 리소스가 필요하며 Level 3은 512-bit 키를 사용하는 블록암호(ex. AES-512)의 키 검색에 필요한 것과 같거나 더 많은 리소스가 필요하다.

SIMECK 경량암호를 해당 기준에 맞춰 평가하기 위해 우리는 우선 Table 3의 Grover 공격 비용 양자 게이트를 더 하위 레벨의 양자 게이트인 T+Clifford gate로 분해하였으며 Table 4와 같다.

Table 5는 T+Clifford로 분해된 결과를 통해 SIMECK에 대한 양자 Cost를 계산하고 Cost를 기준으로 Post-quantum 보안 강도를 평가한 결과를 보여준다.

SIMECK 경량암호에서 제공하는 모든 (블록 사이즈)/(키 사이즈)에 대해 보안 강도를 평가한 결과 모두 보안 레벨을 달성하지 못했다. 경량암호는 가용 자원이 제한된 저사양 디바이스에서 동작할 수 있도록 기존 암호화를 경량화 한 암호화 기법이다. 그 결과 일반 블록암호를 기준으로 제시된 보안 강도 평가 기준을 달성하기에 어려움이 있다는 것을 확인할 수 있다. 따라서 대규모 양자 컴퓨터가 등장하면 기존 경량암호의 보안에 위협이 될 것이라 예상되며 보안강도를 높이기 위한 방안을 고안하거나 다른 양자내성 암호로의 교체가 필요하다. 해당 암호에 대한 보안 강도를 높이기 위해서는 라운드 수 및 블록 사이즈를 증가시키거나 사용하는 키 길이를 증가시키는 방법을 고안 할 수 있다. 하지만 라운드 수 및 블록 사이즈를 증가시키는 것은 보안 강도에 크게 영향을 주지 않는다. 따라서 라운드 수 및 블록 사이즈를 증가시키는 동시에 키 길이를 증가시켜 Grover algorithm의 반복 횟수를 증가시키는 방법이 적합하다고 판단된다.

Table 4. Quantum Resources Required for Grover Attack on SIMECK (low level)

Algorithm	Quantum resources	
	T	Clifford
SIMECK 32/64	1.72×2^{45}	1.35×2^{46}
SIMECK 48/96	1.45×2^{62}	1.14×2^{63}
SIMECK 64/128	1.19×2^{79}	1.89×2^{79}

Table 5. Post-quantum Security Strength for SIMECK

Algorithm	Quantum resources		Quantum Cost	Level
	Total gates	Total Depth		
SIMECK 32/64	1.11×2^{47}	1.51×2^{40}	1.68×2^{87}	Not achieved
SIMECK 48/96	1.87×2^{63}	1.27×2^{57}	1.19×2^{121}	Not achieved
SIMECK 64/128	1.54×2^{80}	1.39×2^{73}	1.07×2^{154}	Not achieved

5. 결 론

본 논문에서는 SIMECK 경량암호를 위한 효율적인 양자회로를 처음으로 제안하였다. 제안하는 SIMECK 양자회로에서 사용되는 자원을 줄이기 위한 양자 자원(큐비트 수, 양자게이트) 측면에서의 최적화 방법들을 제시하고 양자회로 구현 결과를 수도 코드로 나타내었다. 구현된 양자회로를 통해 SIMECK의 모든 블록, 키 길이에 대한 양자 자원 추정을 통해 비슷한 경량 암호군인 SIMON 양자회로와 결과를 비교하였으며, Grover 공격 비용을 계산하였다. 마지막으로 NIST에서 제시한 평가 기준으로 SIMECK 경량암호에 대한 Post-quantum 강도를 평가하여 경량 암호가 Post-quantum 보안 강도를 충족하기 어렵다는 결과를 확인하였다. 따라서 본 논문에서는 해당 결과를 바탕으로 추후 SIMECK 암호에 대해 보안 강도를 높이는 방법을 고안하거나 다른 양자내성암호로의 교체가 필요하다고 판단하였다. 보안 강도를 높이는 방안으로 블록 사이즈 및 라운드 크기를 증가시키는 방법과 키 길이를 증가시키는 방법을 고려할 수 있지만 블록 사이즈 및 라운드 크기의 증가만으로 보안 강도에 크게 영향을 주지 않으므로 블록 사이즈 및 라운드 크기를 증가시키는 동시에 키 길이를 증가시키는 방안이 적절할 것이라 예상된다.

References

[1] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Review*, Vol.41, No.2, pp.303-332, 1999.

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

[3] G. Song, et al., "SPEEDY Quantum Circuit for Grover's Algorithm," *Applied Sciences*, Vol.12, No.14, pp.6870, 2022.

[4] A. Baksi, K. Jang, G. Song, H. Seo, and Z. Xiang, "Quantum implementation and resource estimates for rectangle and knot," *Quantum Information Processing*, Vol.20, No.12, pp.1-24, 2021.

[5] K. Jang, A. Baksi, H. Kim, G. Song, and H. Seo, "Quantum Analysis of AES," *Cryptology ePrint Archive*, 2022.

[6] A. K. Chauhan and S. K. Sanadhya, "Quantum resource estimates of Grover's key search on ARIA," *SPACE 2020: Security, Privacy, and Applied Cryptography Engineering*, pp.238-258, 2020.

[7] R. Anand, A. Maitra, and S. Mukhopadhyay, "Grover on SIMON," *Quantum Information Processing*, Vol.19, No.9, pp.1-17, 2020.

[8] M. Grassl, B. Langenberg, M. Roetteler, and R. Steinwandt, "Applying Grover's algorithm to AES: Quantum310 resource estimates," *Post-Quantum Cryptography,* Springer, pp.29-43, 2016.

[9] K. B. Jang, H. J. Kim, J. H. Park, G. J. Song, and H. J. Seo, "Optimization of LEA quantum circuits to apply Grover's algorithm," *KIPS Transactions on Computer and Communication Systems*, Vol.10, No.4, pp.101-106, 2021.

[10] G. Yang, B. Zhu, V. Suder, M. D. Aagaard, and G. Gong, "The simeck family of lightweight block ciphers," *International Workshop on Cryptographic Hardware and Embedded Systems*, Springer, Berlin, Heidelberg, 2015.

[11] NIST, Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography308 Standardization Process, 2016.

[12] S. G. Song, K. B. Jang, M. J. Sim, and H. J. Seo, "Implementation of quantum circuit optimization for SIMECK," *Proceedings of the Annual Conference of Korea Information Processing Society Conference (KIPS) 2022*, Vol.29, pp.97-99, 2022.

송 경 주

https://orcid.org/0000-0002-4337-1843
e-mail : thdrudwn98@gmail.com
2021년 한성대학교 IT융합공학부(학사)
2023년 한성대학교 IT융합공학부(석사)
2023년 ~ 현 재 한성대학교 정보컴퓨터공학과 박사과정
관심분야 : 양자 컴퓨팅, 암호보안, 인공지능

장 경 배

https://orcid.org/0000-0001-5963-7127
e-mail : starj1032@gmail.com
2019년 한성대학교 정보시스템공학부(학사)
2021년 한성대학교 IT융합공학부(석사)
2021년 ~ 현 재 한성대학교 정보컴퓨터공학과 박사과정
관심분야 : 양자 컴퓨팅, 정보보호, IoT

심 민 주

https://orcid.org/0000-0001-5242-214X
e-mail : minjoos9797@gmail.com
2021년 한성대학교 IT융합공학부(학사)
2023년 한성대학교 IT융합공학부(석사)
2023년 ~ 현 재 한성대학교 정보컴퓨터공학과 박사과정
관심분야 : 암호구현, 정보보안

서 화 정

https://orcid.org/0000-0003-0069-9061
e-mail : hwajeong84@gmail.com
2010년 부산대학교 컴퓨터공학과(학사)
2012년 부산대학교 컴퓨터공학과(석사)
2016년 부산대학교 컴퓨터공학과(박사)
2016년 ~ 2017년 싱가포르 과학기술청 연구원
2019년 ~ 현 재 한성대학교 융합보안학과 부교수
관심분야 : 정보보호, 암호화 구현, IoT