Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.33, NO.3, Jun. 2023 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2023.33.3.383

최적의 큐빗수를 만족하는 LED 블록암호에 대한 양자 회로 구현*

송 민 호,[1†] 장 경 배,[1] 송 경 주,[1] 김 원 웅,[1] 서 화 정[2‡]
[1,2]한성대학교 (대학원생, 교수)

Quantum Circuit Implementation of the LED Block Cipher with Compact Qubit*

Min-ho Song,[1†] Kyung-bae Jang,[1] Gyeong-ju Song,[1]
Won-woong Kim,[1] Hwa-Jeong Seo[2‡]
[1,2]Hansung University (Graduate student, Professor)

요 약

양자 컴퓨터의 발전 및 Shor 알고리즘, Grover 알고리즘과 같은 양자 알고리즘의 등장으로 인해 기존 암호의 안전성은 큰 위협을 받고 있다. 양자 알고리즘은 기존 컴퓨터에서 오랜 시간이 걸리는 수학적 작업을 효율적으로 할 수 있게 해준다. 이 특성은 수학적 문제에 의존하는 현대 암호 시스템이 깨지는 시간을 단축시킬 수 있다. 이러한 알고리즘을 기반으로 하는 양자 공격에 대비하기 위해서는 기존 암호를 양자회로로 구현해야 한다. 이미 많은 암호들은 양자회로로 구현되어 공격에 필요한 양자 자원을 분석하고 암호에 대한 양자 강도를 확인하였다. 본 논문에서는 LED 경량 블록암호에 대한 양자회로를 제시하고 양자회로의 각 함수에 대한 설명을 진행한다. 이후 LED 양자회로에 대한 자원을 추정하고 다른 경량 블록암호와 비교하여 평가해보도록 한다.

ABSTRACT

The development of quantum computers and the emergence of quantum algorithms such as Shor's algorithm and Grover's algorithm pose a significant threat to the security of existing cipher systems. Quantum algorithms can efficiently perform mathematical operations that take a long time on traditional computers. This characteristic can significantly reduce the time it takes to break modern cipher systems that rely on mathematical problems. To prepare for quantum attacks based on these algorithms, existing ciphers must be implemented as quantum circuits. Many ciphers have already been implemented as quantum circuits, analyzing quantum resources required for attacks and verifying the quantum strength of the cipher. In this paper, we present quantum circuits for LED lightweight block ciphers and explain each function of quantum circuits. Thereafter, the resources for the LED quantum circuit are estimated and evaluated by comparing them with other lightweight block ciphers.

Keywords: Quantum Computer, Lightweight Block Cipher, LED

Received(02. 23. 2023), Modified(04. 11. 2023), Accepted(04. 11. 2023)
* 본 논문은 2022년도 한국정보보호학회 동계학술대회에 발표한 우수논문을 개선 및 확장한 것임.

* This research was financially supported by Hansung University.
† 주저자, smino0906@gmail.com
‡ 교신저자, hwajeong84@gmail.com(Corresponding author)

I. 서 론

양자역학적인 현상을 이용하여 데이터를 처리하는 컴퓨터를 양자 컴퓨터라고 한다. 양자 컴퓨터는 기존의 컴퓨터보다 훨씬 빠른 계산 능력을 보여준다. 이러한 양자 컴퓨터의 개발은 기존 암호체계의 안전성에 위협이 될 것이라고 예상된다. 암호 공격에 필요한 양자 자원이 양자 컴퓨터의 가용 자원과 동일해졌을 때를 암호가 깨질 수 있는 시점으로 보고 있다.

또한, Shor 알고리즘과 Grover 알고리즘과 같은 양자 알고리즘의 등장은 기존의 암호 시스템을 깨는 시간을 단축시킨다. Shor 알고리즘은 고전 컴퓨터에서 계산이 오래 걸리는 인수 분해와 같은 연산을 효율적으로 수행한다[1]. 이 알고리즘은 RSA와 같이 큰 수를 소수로 분해하는 문제의 어려움을 기반으로 하는 알고리즘에 위협이 된다. Grover 알고리즘은 정렬되지 않은 N개의 데이터에 대하여 특정 데이터를 찾을 때, $O(N)$번이 아닌 $O(\sqrt{N})$번 만에 찾게 해주는 양자 알고리즘이다[2]. 이러한 Grover 알고리즘은 AES와 같은 대칭키 암호에 대한 Brute force 공격을 가속화시켜 암호화 시스템을 깨는 데 걸리는 시간을 단축시킬 수 있다.

이러한 양자 컴퓨팅의 발전 및 양자 알고리즘을 통한 공격에 대비하기 위해서는 새로운 양자 내성 암호 알고리즘을 개발하거나 기존 암호에 대한 새로운 양자 회로를 구현해야한다. 기존 암호의 양자 후 보안 강도 및 자원을 추정하기 위해서는 해당 암호의 암호화가 양자 회로로 구현되어야 한다. 이에 다양한 대칭키 암호들이 양자 회로로 최적화 구현이 진행되었다[3-7].

본 논문에서는 경량 블록암호 LED에 대한 양자 회로를 구현한다. 구현한 양자회로에 대해 자원을 추정하고 다른 암호들의 양자 후 자원량과 비교한다.

II. 관련 연구

2.1 양자 컴퓨터

양자 컴퓨터는 기존 컴퓨터와 달리 비트가 아닌 큐비트를 사용한다. 큐비트는 양자역학적인 개념인 양자 얽힘, 양자 중첩 등의 개념을 도입한 양자비트이다. 기존 컴퓨터의 비트는 0이나 1 둘 중 한 개의 상태로 결정되지만 큐비트는 0과 1 둘 다 동시에 가질 수 있으며, 이는 양자 중첩의 개념이다. 예를 들어 두 개의 비트를 사용할 경우엔 네 개의 가능한 값(00, 01, 10, 11)이 있지만 한 번에 하나의 값만 저장할 수 있다. 그러나 중첩 상태인 큐비트는 0, 1 또는 둘 다일 수 있으므로 네 개의 값을 동시에 나타낼 수 있다. 둘 다 동시에 가지고 있는 상태에서 관측되는 순간 큐비트의 상태가 결정된다.

양자 얽힘이란 한 큐비트가 관측 되어 상태가 결정되는 순간에 관측된 큐비트와 얽혀있던 큐비트의 상태도 같이 결정되는 개념이다. 이러한 개념은 효율적인 연산을 가능하게 한다. 기존의 컴퓨터는 비트를 0과 1로 표현하며 순차적으로 계산하여 많은 시간이 소요된다. 하지만 양자 컴퓨터는 양자 중첩과 얽힘이라는 성질을 이용하여 순차적으로 계산하는 것이 아닌 한 번에 계산하는 것을 가능하게 한다. 이러한 특성으로 양자 컴퓨터는 고전 컴퓨터보다 복잡한 계산을 효율적으로 할 수 있다.

2.2 양자 게이트

양자 회로를 이용하여 구현을 할 때에는 양자 게이트를 사용한다. 양자 게이트는 기존의 논리 연산과 동일한 역할을 수행한다. 대표적으로 X 게이트, CNOT 게이트, Toffoli 게이트, Swap 게이트가 존재한다. Fig.1.의 첫 번째 그림은 기존의 NOT 연산을 대체하는 X 게이트이다. X 게이트는 해당 큐비트의 기존 상태를 반전시킴으로써 NOT 연산을 수행한다. 두 번째 그림은 CNOT 게이트이다. CNOT 게이트는 두 개의 큐비트에 대하여 첫 번째 큐비트가 1인 상태라면 두 번째 큐비트의 상태를 반전시키고, 0인 상태라면 기존 큐비트의 상태를 반환한다. CNOT 게이트는 기존의 XOR 연산을 대체할

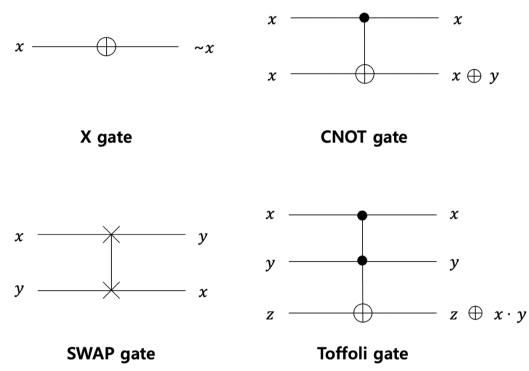

Fig. 1. Quantum gates

수 있다. 세 번째 그림은 Swap 게이트이다. Swap 게이트는 두 개의 큐비트에 대하여 서로의 상태를 반전시켜준다. 마지막 그림은 Toffoli 게이트이다. Toffoli 게이트는 앞의 게이트들과 달리 3개의 큐비트를 입력 받는다. 3개의 큐비트에 대하여 첫 번째 큐비트와 두 번째 큐비트가 모두 1인 경우에, 세 번째 큐비트의 상태를 반전시킨다. Toffoli 게이트는 기존의 AND 연산을 대체할 수 있다. 이러한 양자 게이트를 이용하여 다양한 암호 알고리즘에 사용되는 기존 연산을 구현할 수 있다.

2.3 LED

LED는 2011년 CHES에서 제안된 AES와 같은 설계 원리에 기반을 두고 만들어진 경량 블록암호이다[8]. LED 알고리즘은 무선 센서 네트워크와 같은 제한된 환경에서의 효율적인 구현이 가능하도록 설계된 알고리즘이다. 블록의 길이는 64-bit이며, 64-bit, 80-bit, 96-bit, 128-bit의 키 길이를 지원한다. 키 길이가 64-bit일 경우에는 8라운드 연산을 통해 암호화를 진행하고 그 외에는 12라운드 연산을 통해 암호화를 진행한다. 64-bit 평문을 4-bit 단위로 나눠 4x4 배열을 만든 후 연산을 수행한다.

전체적인 구조는 Fig.2.와 같고 키 스케줄이 따로 없는 것이 특징이다. 평문과 키를 이용하여 AddRoundKey 연산을 수행한 후, $step$ 함수 연산을 수행한다. 이를 키 길이에 맞는 라운드 r만큼 연산을 반복 수행하고 마지막으로 AddRoundKey를 연산함으로써 암호화가 마무리된다.

$step$ 함수의 내부 연산은 Fig.3.과 같다. $step$ 함수의 내부는 AddConstants, SubCells, ShiftRows, MixColumnsSerial로 이루어져 있다. $step$ 함수는 4 라운드로 구성되어 있다. 내부의 4개의 함수들이 순차적으로 연산이 진행되는데, 그 과정을 4번 반복하는 것이 $one\,step$이다. 결과적으로 암호화가 진행되는 동안에 $step$ 함수는 $4 \times r$ 만큼 연산을 수행한다.

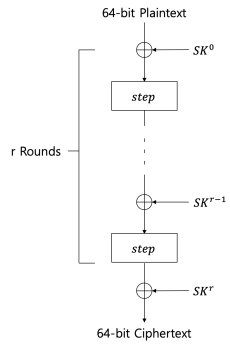

Fig. 2. LED structure

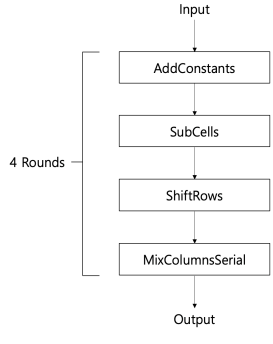

Fig. 3. $step$ Function

III. 구현 기법

3.1 AddRoundKey

AddRoundKey는 주어진 키를 사용하여 평문에 각각 XOR 연산을 해주는 과정이다. 본 논문에서 구현한 AddRoundKey 함수는 Fig. 4.와 같다. LED는 키 스케줄이 존재하지 않아 라운드 키가 아닌 초기 입력 키 값 K와 블록 B를 사용하여 XOR 연산을 수행한다. CNOT 게이트를 큐비트 수만큼 반복 사용해서 연산을 진행하며, 연산이 끝난 후 새로운 블록 값 B_{New}를 생성한다.

Algorithm :Quantum circuit for AddRoundKey of LED block cipher

Input : 64-qubit block $B(b_{63}, ..., b_0)$,
64-qubit key $K(k_{63}, ..., k_0)$
Output : 64-qubit block $B_{New}(b_{63}, ..., b_0)$
1: **for** i = 0 **to** 63 **do**
2: $b_i \leftarrow$ **CNOT** (k_i, b_i)
3: **end for**
4: **return** $B_{New}(b_{63}, ..., b_0)$

Fig. 4. Quantum circuit for AddRoundKey of LED block cipher

3.2 AddConstants

AddConstants는 주어진 Round Constants를 이용하여 XOR 연산을 수행한다. Fig.5.는 4x4 배열에서의 한 행 x에 대한 연산을 나타낸다. 주어진 Round Constants 값인 RC를 Shift 연산을 통해 각 주소의 상태가 0인지 1인지 판단한다. 해당 주소의 값이 1일 경우 x_i와 XOR 연산을 진행하면 상태가 반전된다. 이러한 점을 이용하여 상태가 1인 경우만 찾아내고, 해당하는 경우에만 X 게이트를 통해 연산을 수행한다. 처음부터 반복을 통해 CNOT

Algorithm : Quantum circuit for RoundConstants of LED block cipher

Input : 16-qubit input $x(x_{15}, ..., x_0)$, RC
Output : 16-qubit output $x(x_{15}, ..., x_0)$

```
for i = 0 to 15 do
  if (RC >> i) & 1 then
    x_i ← X (x_i)
  end if
end for
return x(x_15, ..., x_0)
```

Fig. 5. Quantum circuit for RoundConstants of LED block cipher

게이트를 사용하는 연산이 아닌 필요한 경우에만 X 게이트를 사용하여 양자비용을 줄일 수 있다.

3.3 SubCells

SubCells 함수는 Substitution 연산을 하는 과정이다. SPN(Substitution Permutation Network) 구조의 블록 암호를 양자 회로로 구현할 시, 대부분 이 연산 과정에서 가장 많은 자원을 소모한다. 따라서 S-box 양자 회로 구현에서 최적화를 통해 자원을 줄이는 것이 중요하다.

Algorithm : Quantum circuit for SBox of LED block cipher (C56B90AD3EF84712, using LIGHTER-R)

Input : 4-qubit input $x(x_3, x_2, x_1, x_0)$
Output : 4-qubit output $x(x_3, x_2, x_1, x_0)$

```
x_1 ← CNOT (x_2, x_1)
x_3 ← Toffoli (x_1, x_2, x_3)
x_2 ← Toffoli (x_3, x_1, x_2)
x_1 ← Toffoli (x_0, x_2, x_1)
x_2 ← CNOT (x_3, x_2)
x_3 ← X (x_3)
x_2 ← CNOT (x_1, x_2)
x_0 ← CNOT (x_3, x_0)
x_1 ← CNOT (x_0, x_1)
x_0 ← X (x_0)
x_3 ← Toffoli (x_1, x_2, x_3)
return x(x_1, x_3, x_2, x_0)
```

Fig. 6. Quantum circuit for SBox of LED block cipher (C56B90AD3EF84712, using LIGHTER-R)

본 논문에서는 4-bit S-box를 양자 회로로 구현하기 위해 LIGHTER-R을 사용하였다[9]. LIGHTER-R은 그래프 이론의 탐색 알고리즘인 MITM(Meet-in-the-middle)에 기반해서 4-bit 입력에 대한 출력을 계산하여 최적화된 S-box 양자 회로를 생성해주는 도구이다.

LED의 S-box 테이블은 C56B90AD3EF84712 이다. 이러한 테이블을 입력 값으로 사용하여 LIGHTER-R에 의해 만들어진 S-box의 양자 회로는 Fig.6.과 같다. 이 S-box는 2개의 X 게이트, 5개의 CNOT 게이트, 4개의 Toffoli 게이트로 이루어져 있다. 마지막에 값을 반환할 때에는 Swap 게이트가 사용된다. 하지만 실제 양자 구현에서는 Swap 게이트를 사용하지 않고 Logical Swap을 활용하였다. Logical Swap은 큐비트 간의 인덱스 순서를 변경하여 Swap 게이트의 연산을 대체하는 것을 의미한다. 실제 게이트를 사용하지 않으므로 양자 자원이 소비되지 않는다.

3.4 ShiftRows

ShiftRows 함수는 주어진 인덱스만큼 각 행의 성분에 대한 Rotation 연산을 수행한다. Fig.7.은 4x4 배열에서 두 번째 행에 대한 ShiftRows 양자 회로이다. 행의 한 성분은 4-큐비트로 이루어져 있기 때문에, 행의 성분에 대한 Rotation을 진행하기 위해서는 4-큐비트 단위로 연산을 해줘야 한다. 두 번째 행의 인덱스는 1이기에 Rotation 연산이 진행되면 총 4-큐비트만큼 Rotation된다. 연산은 양자

Algorithm : Quantum circuit for ShiftRows of LED block cipher

Input : 16-qubit input $b(b_{15}, ..., b_0)$
Output : 16-qubit output $b_{New}(b_{15}, ..., b_0)$

```
b_New = []
b_New(b_15, ..., b_12) ← b(b_3, ..., b_0)
b_New(b_11, ..., b_8) ← b(b_15, ..., b_12)
b_New(b_7, ..., b_4) ← b(b_11, ..., b_8)
b_New(b_3, ..., b_0) ← b(b_7, ..., b_4)
return b_New
```

Fig. 7. Quantum circuit for ShiftRows of LED block cipher

게이트를 사용하지 않고 Logical Swap을 이용하여 구현을 진행하였다. 이로 인해 양자 게이트로 인한 자원이 소비되지 않았다.

3.5 MixColumnsSerial

MixColumnsSerial은 주어진 matrix M을 이용하여 4x4 평문과 행렬곱을 수행한다. matrix M은 레퍼런스[8]에서 제공한다. XOR 연산을 통해 값을 구할 수 있으나, 연산 후 나온 값은 기존 크기의 4-bit 형태를 넘어간다. 유한체 상에서의 연산이므로 reduction을 통해 기존의 4-bit 형태로 크기를 맞춰줘야 한다. reduction을 위한 기약 다항식은 $X^4 + X + 1$이다[8]. 본 논문에서는 사전연산을 진행한 후, 결과 값을 이용하여 양자회로를 구현하였다. 첫 번째 cell에 대한 양자 회로는 Fig.8.과 같다. CNOT 게이트를 사용하여 구현하였으며, 사전연산을 통해 사용한 게이트의 수를 줄여 양자 자원의 소비를 줄였다.

Algorithm : Quantum circuit for MixColumnsSerial for first element of matrix in LED block cipher

Input : 4-qubit $x(x_3, x_2, x_1, x_0)$,
4-qubit input $y(y_3, y_2, y_1, y_0)$
Output : 4-qubit output $y(y_3, y_2, y_1, y_0)$
1: $y_0 \leftarrow$ **CNOT** $(x_2,\ y_0)$
2: $y_1 \leftarrow$ **CNOT** $(x_2,\ y_1)$
3: $y_1 \leftarrow$ **CNOT** $(x_3,\ y_1)$
4: $y_2 \leftarrow$ **CNOT** $(x_0,\ y_2)$
5: $y_2 \leftarrow$ **CNOT** $(x_3,\ y_2)$
6: $y_3 \leftarrow$ **CNOT** $(x_1,\ y_3)$
7: **return** $y(y_3, y_2, y_1, y_0)$

Fig. 8. Quantum circuit for MixColumnsSerial for first element of matrix in LED block cipher

IV. 비교분석

본 논문에서 제안하는 LED 암호화 양자 회로의 자원을 추정하고 다른 암호들과 비교한다. LED 암호화 과정에 필요한 양자 자원량과 다른 블록 암호들에 대한 자원량은 Table.1.과 같다[5]. Table.1에는 사용된 qubit의 수와 X, CNOT, Toffoli 게이트의 수, Depth가 있다.

Table 1. Quantum resources for LED and comparison with other cipher implementation

Algorithm	X gates	CNOT gates	Toffoli gates	Qubits	Depth
LED 64/64	1,438	19.008	2,048	142	810
PIPO 64/128	1,477	2,248	1,248	192	248
GIFT 64/128	3,261	1,792	1,792	192	308
SIMON 64/128	1,216	7,396	1,408	192	2,643

128-bit 키를 사용하는 다른 암호들과 달리 64-bit 키를 사용하는 LED의 qubit 수가 적은 것을 볼 수 있다. 그러나 다른 암호들에 비해 한 라운드에 많은 내부 연산이 수행되는 LED 특성 상, 적은 키를 사용함에도 불구하고 많은 양자 게이트가 사용되는 것을 확인할 수 있다.

V. 결 론

본 논문에서는 경량 블록 암호 LED에 대한 양자 회로의 구현 및 그에 필요한 양자 자원에 대해 알아보았다. 양자 회로를 통한 암호 구현에 있어서 가장 중요한 점은 양자 자원을 적게 사용하는 것이다. 이에 사전 연산, Logical Swap 등 다양한 방법을 통해 양자 자원을 적게 사용하는 방향으로 구현을 진행하였다. 양자 회로를 얼마나 효율적으로 구현함에 따라 필요한 양자 자원이 현저히 줄어든다.

이전과 다르게 양자 컴퓨터의 지속된 발전을 통해 암호체계는 계속 위협받고 있다. 양자 컴퓨터의 가용 자원이 계속 늘어나고 있고 이는 Grover 알고리즘 등을 통한 공격에 기존의 암호체계가 무너지는 순간이 앞당겨지고 있다는 뜻이다. 이에 암호에 대한 양자회로 구현 후 보안 강도를 확인해봐야 한다. NIST는 AES의 128-bit 키를 기준으로 대칭키 암호 공격 비용을 추정한 후, 양자 구현 이후 보안 레벨을 제시하고 있다. 그러나 128-bit보다 작은 키에 대한 보안 레벨은 존재하지 않는다. 본 논문은 작은 키를 사용한 LED에 대한 양자 회로의 구현이다. 이를 통해 작은 키에 대한 보안 레벨 분석에 도움이 될 수 있다.

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, Jun. 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, Jul. 1996

[3] M. GRASSL, B. Langenberg, M. Roetteler and R. Steinwandt, "Applying Grover's algorithm to AES: quantum resource estimates," Post-Quantum Cryptography: 7th International Workshop, PQCrypto 2016, Fukuoka, Japan, February 24-26, 2016, Proceedings 7, pp. 29-43, Feb. 2016

[4] Kyung-bae Jang, Gyeong-ju Song, Hyun-jun Kim, Hyeok-dong Kwon, Hyun-ji Kim and Hwa-jeong Seo, "Parallel quantum addition for Korean block ciphers," Quantum Information Processing, vol. 21, no. 11, pp. 373, Nov. 2022

[5] Kyung-bae Jang, Gyeong-ju Song, Hyeok-dong Kwon, Si-woo Uhm, Hyun-ji Kim, W.K. Lee and Hwa-jeong Seo, "Grover on PIPO," Electronics, vol. 10, no. 10, pp. 1194, May. 2021

[6] A. BAKSI, Kyung-bae Jang, Gyeong-ju Song, Hwa-jeong Seo and Z. Xiang, "Quantum implementation and resource estimates for rectangle and knot," Quantum Information Processing, vol. 20, pp. 1-24, Nov. 2021

[7] Kyung-bae Jang, Gyeong-ju Song, Hyun-jun Kim, Hyeok-dong Kwon, Hyun-ji Kim and Hwa-jeong Seo, "Efficient implementation of PRESENT and GIFT on quantum computers," Applied Sciences, vol. 11, no. 11, pp. 4776, May. 2021

[8] J. Guo, T. Peyrin, A. Poschmann and M. Robshaw, "The LED block cipher," Cryptographic Hardware and Embedded Systems - CHES 2011: 13th International Workshop, Nara, Japan, September 28 - October 1, 2011. Proceedings 13. pp. 326-341, Sept. 2011

[9] V.A. DASU, A. Baksi, S. Sarkar and A. Chattopadhyay, "LIGHTER-R: optimized reversible circuit implementation for sboxes," 2019 32nd IEEE International System-on-Chip Conference (SOCC), pp. 260-265, Sept. 2019

〈저자소개〉

송 민 호 (Min-ho Song) 학생회원
2023년 2월: 한성대학교 IT융합공학부 학사 졸업
2023년 3월~현재: 한성대학교 융합보안학과 석사과정
〈관심분야〉 암호구현, 정보보안

장 경 배 (Kyung-bae Jang) 학생회원
2019년 2월: 한성대학교 IT응용시스템공학과 학사 졸업
2021년 2월: 한성대학교 IT융합공학부 석사 졸업
2021년 3월~현재: 한성대학교 정보컴퓨터공학과 박사과정
〈관심분야〉 양자컴퓨터, 정보보안

송 경 주 (Gyeong-ju Song) 학생회원
2021년 2월: 한성대학교 IT융합공학부 학사 졸업
2023년 2월: 한성대학교 IT융합공학부 석사 졸업
2023년 3월~현재: 한성대학교 정보컴퓨터공학과 박사과정
〈관심분야〉 양자컴퓨터, 정보보안

김 원 웅 (Won-woong Kim) 학생회원
2022년 2월: 한성대학교 컴퓨터공학부 졸업
2022년 3월~현재: 한성대학교 IT융합공학부 석사과정
〈관심분야〉 인공지능, 블록체인

서 화 정 (Hwa-Jeong Seo) 종신회원
2010년 2월: 부산대학교 컴퓨터공학과 학사 졸업
2012년 2월: 부산대학교 컴퓨터공학과 석사 졸업
2015년 4월~5월: 싱가포르 난양공대 인턴쉽
2016년 2월: 부산대학교 컴퓨터공학과 박사 졸업
2017년 3월: 싱가포르 과학기술청 연구원
2017년 4월~2023년 2월: 한성대학교 IT융합공학부 조교수
2023년 3월~현재: 한성대학교 융합보안학과 부교수
〈관심분야〉 정보보호, 암호화 구현, IoT