# Grover on Simplified AES

Kyung-Bae Jang*, Gyeong-Ju Song*, Hyun-Ji Kim*, Hwa-Jeong Seo*
**IT Department, Hansung University, Seoul*
*{starj1023, thdrudwn98, khj1594012, hwajeong84}@gmail.com*

## Abstract

*NIST(National Institute of Standards and Technology) estimates the Grover key search cost required for symmetric key cryptography as the post-quantum security strength. The Grover search algorithm is applicable to key recovery in symmetric key cryptography, and for this, the target encryption process must be implemented as a quantum circuit. In this paper, we present an optimized implementation of Simplified AES as a quantum circuit. Substitution, Mix Columns, and Key Expansion are implemented efficiently, and as a result of resource analysis, qubits, quantum gates, and circuit depth are significantly reduced compared to the previous result.*

**Keywords:** Grover search algorithm, Simplified AES, Quantum circuit

## 1. Introduction

Quantum computers using quantum algorithms show greater computational power than classical computers in solving some problems. Grover's algorithm is a quantum algorithm that finds specific data with high probability among unsorted data [1]. The Grover algorithm, which can be used in various fields, can be used in a brute force attack to recover the key of symmetric key cryptography. To do this, first, the encryption of the target cipher must be implemented as a quantum circuit so that it can be operated in a quantum computer. According to this research motive, starting with the quantum circuit implementation of the widely used symmetric key cipher AES [2], researches on implementing various symmetric key ciphers into quantum circuits are being actively conducted [3]. In this paper, we efficiently implement Simplified AES as a quantum circuit. In terms of optimization on a quantum computer, there are three elements: qubits, quantum gates, and circuit depth. Since large-scale quantum computers have not yet been developed, the number of qubits required is related to when they actually work in quantum computers. Quantum gates and total depth are related to execution speed because they represent the complexity of the circuit.

The proposed Simplified AES quantum circuit uses only 32 qubits for 16-bit plaintext and 16-bit key. This is an optimized result to use the minimum number of qubits compared to the 72 qubits used in the previous result [4]. It is also optimized in terms of quantum gates and circuit depth. Finally, we perform quantum cryptanalysis by estimating the Grover key search cost based on the proposed Simplified AES quantum circuit.

## 2. Related Works

2.1 Simplified AES [5]

Simplified AES (S-AES) is an algorithm that has simplified the existing AES. It uses a 16-bit block plaintext and a 16-bit key and consists of a total of 2 rounds. Like AES, each round consists of Substitute nibble, Shift Rows, Mix Columns, and Add Roundkey, and Key Expansion for generating round keys is performed. The encryption structure of S-AES is shown in Figure 1.

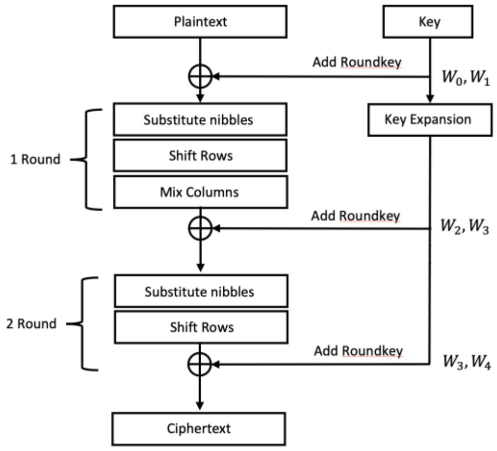

**Figure 1: Encryption structure of Simplified AES**

In Add Roundkey, a 16-bit round key is XORed into a 16-bit block. S-AES performs the following substitution in 4-bit units for 16-bit blocks. 4-bit ($b_0, b_1, b_2, b_3$) is expressed as a polynomial and converts it to an inversion of $GF(16)$ (filed polynomial = $x^4 + x + 1$). After that, the substitution is completed by performing matrix multiplication and vector addition (XOR) as shown in Figure 2. An S-box using a lookup table is shown in Table 1.

$$\begin{bmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

**Figure 2: Matrix multiplication and vector addition**

**Table 1: S-box look up table**

| $x$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| S-box(x) | 9 | 4 | A | B | D | 1 | 8 | 5 |
| $x$ | 8 | 9 | A | B | C | D | E | F |
| S-box(x) | 6 | 2 | 0 | 3 | C | E | F | 7 |

In Shift Rows, 4-bit $(b_4, b_5, b_6, b_7)$ and 4-bit $(b_{12}, b_{13}, b_{14}, b_{15})$ are interchanged. After Shift Rows, the Mix Columns in Figure 3 is performed on 16-bit blobk $B$.

$$\begin{bmatrix} B_0 & B_2 \\ B_1 & B_3 \end{bmatrix} = \begin{bmatrix} 1 & x^2 \\ x^2 & 1 \end{bmatrix} \begin{bmatrix} B_0 & B_2 \\ B_1 & B_3 \end{bmatrix} \bmod (x^4 + x + 1)$$

**Figure 3: Mix Columns**

The Key Expansion process is shown in Figure 4. In Swap, $(w_8, w_9, w_{10}, w_{11})$ and $(w_{12}, w_{13}, w_{14}, w_{15})$ are exchanged and substitution is performed for each 4-bit. 10000000 and 00110000 are round constants.

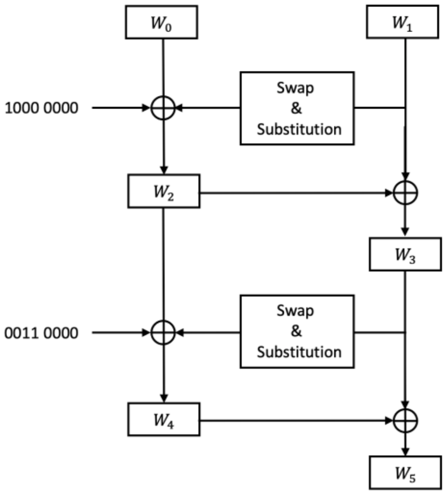

**Figure 4: Key Expansion**

2.2 Quantum Computing

Quantum computers are reversible for all operations except observation. In other words, it should be possible to restore the initial state again using only the output values. Figure 5 shows representative quantum gates with reversible characteristics that can replace logic gates of classical computers. The first row is the X gate and CNOT (CX) gate, which replace the NOT operation and the XOR operation, and the second row is the Swap gate and the Toffoli (CCX) gate, replacing the Swap operation and the AND operation. Quantum gates in Figure 5 can be used to implement the arithmetic required for cryptography.

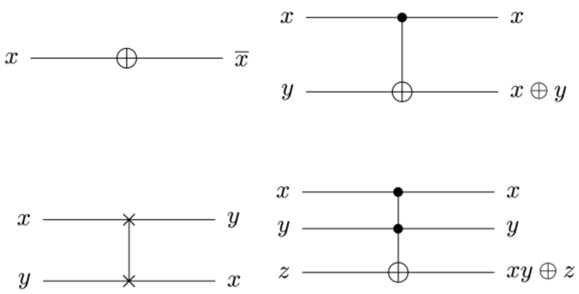

**Figure 5: Quantum gates**

2.3 Grover Search Algorithm

Grover search algorithm consists of oracle and diffusion operator. In Grover key search, oracle returns the key for known plaintext-ciphertext pairs. Because it operates in the superposition state, the diffusion operator amplifies the amplitude of the key returned by the oracle. Grover key search recovers the key with high probability by repeating the oracle and diffusion operator $\frac{\pi}{4}\sqrt{2^n}$ times for an $n$-bit key.

## 3. Proposed Method

Substitution, Mix Columns, and Key Expansion, which require a lot of quantum resources, are efficiently implemented in the proposed S-AES quantum circuit. Through this, only 32 (16+16) qubits for the plaintext and key were used, and quantum gates and circuit depth were also reduced.

3.1 Quantum circuit for Add Roundkey

Add Roundkey XORs the 16-bit round key to the 16-bit block $B$. The quantum circuit for Add Roundkey can be implemented with 16 CNOT gates, which is shown in Algorithm 1.

```
Algorithm 1: Quantum circuit for Add Roundkey
Input: 16-qubit Block $B(b_0, b_1, \dots, b_{15})$,
       16-qubit Roundkey $W(w_0, w_1, \dots, w_{15})$
Output: 16-qubit Block $B(b_0, b_1, \dots, b_{15})$
for $i = 0$ to 15
    CNOT $(w_i, b_i)$
return $B(b_0, b_1, \dots, b_{15})$
```

3.2 Quantum circuit for Substitution

Implementing an S-box using a lookup table on a classic computer is a common choice. However, using a lookup table in a quantum computer in a superposition state is quite complex and inefficient. Thus, implementing S-box operations in ANF(Algebraic Normal Form) is a common choice in quantum computers. In [4], Almazrooie et al. implemented a finite field inversion arithmetic of S-box with quantum gates for the S-AES quantum circuit, and a lot of resources were used. On the other hand, we choose the implementation method based on the lookup table of S-box. Using the LIGHTER-R tool, the S-box is efficiently implemented with few quantum gates and no additional qubits. LIGHTER-R generates a reversible ANF based on the input and output of the lookup table. Through this, it is possible to efficiently implement a quantum circuit for the S-box. LIGHTER-R is described in detail in [6]. Our quantum circuit for the S-box is shown in Figure 6, which generates the correct outputs for the S-box inputs of the S-AES.

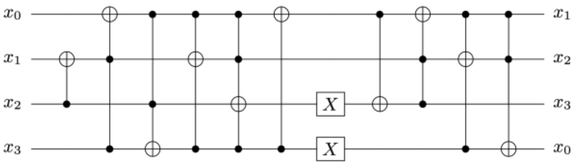

**Figure 6: S-box quantum circuit implemented using LIGHTER-R**

### 3.3 Quantum circuit for Mix Columns

In [4], 34(17 X 2) CNOT gates were used for Mix Columns. In this paper, only 16(8 X 2) CNOT gates are used by implementing a quantum circuit based on the final result of the Mix Columns. Below is the result after performing Mix Column to be implemented with quantum gates.

$$b_0 \oplus b_6,\ b_1 \oplus b_4 \oplus b_7,\ b_2 \oplus b_4 \oplus b_5,\ b_3 \oplus b_5,$$
$$b_2 \oplus b_4,\ b_0 \oplus b_3 \oplus b_5,\ b_0 \oplus b_1 \oplus b_6,\ b_1 \oplus b_7$$

We performed CNOT gates with each other in 8-qubit to generate Mix Columns result most efficiently. The quantum circuit for Mix Columns is shown in Algorithm 2. 16-qubit block is divided by 8-qubit to perform Mix Column (i.e. 32 CNOT = 2 ·16 CNOT).

Algorithm 2: Quantum circuit for Mix Columns

```
Input: 8-qubit Block $B(b_0, b_1, \ldots, b_7)$,
Output: 8-qubit Block $B(b_0, b_1, \ldots, b_7)$
CNOT $(b_0, b_6)$
CNOT $(b_5, b_3)$
CNOT $(b_4, b_2)$
CNOT $(b_1, b_7)$
CNOT $(b_7, b_4)$
CNOT $(b_2, b_5)$
CNOT $(b_3, b_0)$
CNOT $(b_6, b_1)$
return $B(b_0, b_1, \ldots, b_7)$
```

The proposed Mix Columns implementation method generates all result values correctly, but the index of the qubits changes during the optimization process. Therefore, after performing Algorithm 2, the index of the qubits must be changed using Swap gates. Swap gates are used for the convenience of implementation, but they are not measured as quantum resources because they can be replaced by relabeling qubits [7].

### 3.4 Quantum circuit for Shift Rows

Shift Rows can be simply implemented with only Swap gates. The quantum circuit for Shift Rows using Swap gates is shown below and is not measured as quantum resources.

$$\text{Swap}\ (x_4,\ x_{12}),\quad \text{Swap}\ (x_5,\ x_{13})$$
$$\text{Swap}\ (x_6,\ x_{14}),\quad \text{Swap}\ (x_7,\ x_{15})$$

### 3.4 Quantum circuit for Key Expansion

We do not allocate qubits for storing round keys in S-AES. Using the on-the-fly method, the input key is updated before Add Roundkey and used as a round key. Temporary values for $W_2$ and $W_4$ are computed in $W_1$ and $W_3$, and CNOT gates are performed to generate $W_2$ and $W_4$. Then, reverse operation is performed on $W_1$ and $W_3$ to return to the previous value. The returned $W_1$ and $W_3$ are changed to $W_3$ and $W_5$. Through this, we do not allocate additional qubits for the round key, and we also optimized the S-box used in Key Expansion. Finally, key expansion is performed without additional qubits.

For round constant addition, the constants are known in advance. Therefore, XORs are performed using X gates, which are more efficient than CNOT gates, according to the index in which the bit of the constant is 1. The proposed key schedule quantum circuit structure is shown in Figure 7.

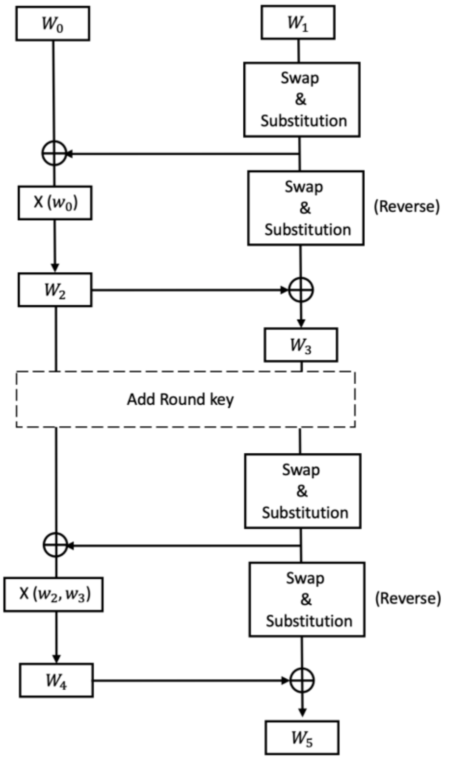

**Figure 7: Proposed Key Expansion structure**

## 4. Evaluation

To implement the proposed quantum circuit and evaluate quantum resources, the quantum programming tool ProjectQ provided by IBM was used, and the quantum resources required to implement S-AES are shown in Table 2. It saves more than two times the qubits compared to the previous result, and the quantum gates are also significantly reduced. Although the circuit depth is not specified in [4], but it will be higher than our circuit depth.

**Table 2: Quantum resources for S-AES quantum circuit**

| | Qubit | CX | CCX | CCCX | X | Depth |
|---|---|---|---|---|---|---|
| Key Expansion [4] | 40 | 568 | 192 | - | 10 | - |
| Encryption [4] | 32 | 512 | 384 | - | 16 | - |
| Total [4] | 72 | 1,080 | 576 | - | 26 | - |
| Key Expansion (Ours) | 16 | 56 | 48 | 8 | 19 | - |
| Encryption (Ours) | 16 | 88 | 48 | 8 | 16 | - |
| Total (Ours) | 32 | 144 | 96 | 16 | 35 | 47 |

We were able to lower the cost a lot by optimizing the S-box, Mix Columns and Key Expansion. S-AES using a 16-bit key can recover the key with only $\frac{\pi}{4}\sqrt{2^{16}}$ searches by applying Grover's algorithm. For estimating the attack cost of Grover key search, the quantum resources required for oracle are estimated. Because it is the main module in the Grover search algorithm, the attack cost is determined by oracle. In oracle, the encryption circuit is performed twice, including the reverse operation, and repeated $\frac{\pi}{4}\sqrt{2^{16}}$ times. Therefore, the final attack cost is calculated as Table $2 \times 2 \times \frac{\pi}{4}\sqrt{2^{16}}$ excluding qubits. The cost of Grover key search for symmetric key cryptography depends on how efficiently the encryption process implements it as a quantum circuit.

## 5. Conclusion

NIST estimates the Grover key search cost for symmetric key cryptography as the post-quantum security strength. In the Grover key search, the attack cost is determined by how efficiently the target encryption process is implemented. In this paper, Simplified AES is efficiently implemented as a quantum circuit, and the Grover key search cost is estimated based on this. As a result, the attack cost was significantly reduced compared to the previous result.

## 6. Acknowledgment

This work was partly supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) (No.2018-0-00264, Research on Blockchain Security Technology for IoT Services, 50%) and this work was partly 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, 50%).

## References

[1] Grover. L.K, “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.

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

[3] K. Jang, G. Song, H. Kim, H. Kwon, H. Kim, and H. Seo,“Efficient implementation of present and gift on quantum computers”, *Applied Sciences*, vol. 11, no. 11, 2021.

[4] Mishal Almazrooie, R. Abdullah, A. Samsudin, and K. N. Mutter, “Quantum Grover Attack on the Simplified-AES”, In *Proceedings of the 2018 7th International Conference on Software and Computer Applications*, pp. 204-211, 2018.

[5] M. A. Musa, E.F. Schaefer, and S. Wedig. A simplified AES algorithm and its linear and differential cryptanalysis. *Cryptologia*, Vol. XXVII (2), pp. 148-177, 2003.

[6] Dasu. V. A, Baksi. A, Sarkar. S, Chattopadhyay. A, “LIGHTER-R: Optimized Reversible Circuit Implementation For SBoxes”, *2019 32nd IEEE International System-on-Chip Conference (SOCC)*, pp. 260–265, 2019.

[7] M.ˇZnidariˇc, O. Giraud, and B. Georgeot, “Optimal number of controlled-not gates to generate a three-qubit state,” *Physical Review A*, vol. 77, no. 3, Mar 2008.