CTU Journal of Innovation and Sustainable Development
ISSN 2588-1418 | e-ISSN 2815-6412

DOI:10.22144/ctujoisd.2024.317

Demonstration of Grover's algorithm for retrieving secret keys in a basic SPN block cipher

Vu Minh Thang[1], Nguyen Van Nghi[1*], Le Quoc Dat[2] and Do Quang Trung[1]

[1]*Academy of Cryptography Techniques, Viet Nam*

[2]*Institute of Cryptographic Science and Technology, Viet Nam*

**Corresponding author (nghinv@actvn.edu.vn)*

Article info.

Received 3 Jul 2024
Revised 4 Sep 2024
Accepted 8 Oct 2024

Keywords

Block cipher, Grover's algorithm, key searching, quantum algorithm

ABSTRACT

In this study, we present in detail the application of Grover's quantum algorithm to the searching problem of the secret key of a simple SPN (Substitution–permutation network) block cipher called Yo-yo. The main goal of the paper is to clarify the construction of the quantum circuit and the operation phases of Grover's algorithm to find the secret key with the condition of knowing at least 1 pair of plaintext-ciphertext. To achieve this goal, we consider 2 cases: the case where there is a unique key that satisfies and the case where there are 2 keys that satisfy at the same time. As a result, our implementation technique, implemented in the Qiskit programming language, requires only 17 qubits to find the key of the Yo-yo block cipher correctly. This technique can be effectively applied on IBM quantum computers for large-scale SPN block ciphers, such as AES and GOST R.34.10.2015, which are widely used today.

1. INTRODUCTION

Recently, there has been a lot of work focused on simulating quantum computers, as well as developing real quantum processors: in 2023, IBM announced its quantum computer chip and new Quantum System. According to IBM, this chip can serve as the building blocks for systems that are much larger and many times faster than traditional silicon supercomputers. IBM's new processor has 1,000 qubits. According to the company, shortly, they will focus on the problem of error correction of microprocessors, instead of racing to increase the number of qubits. In early 2024, Chinese scientists achieved a breakthrough in quantum simulation, when they successfully built the world's largest ion trap system. This is the largest ion trap quantum simulation project carried out to date, marking an important milestone in quantum science. In recent years, there have been many publications on applying Grover's algorithm to find cryptographic keys (Grassl et al., 2016; Kim et al., 2018; Denisenko, 2019; Jaques et al., 2020). Among them, the most prominent works can be found in two directions:

– Applying Grover in SPN block cipher key search as: in "Applying Grover's algorithm to AES: Quantum resource estimates" (Grassl et al., 2016) the author forces on the quantum resource estimates in applying Grover's algorithm to AES. In "Alternative Tower Field Construction for Quantum Implementation of the AES S-Box" (Chung et al., 2022), the authors describe how to build a quantum circuit for the AES S-Box. Kim et al. (2018) discussed time-space trade-offs for key search on block ciphers in general and used AES as an example. Jaques et al. (2020), described implementations of the full Grover oracle for key search on AES and LowMC in Q#, including full implementations of the block ciphers themselves.

– Applying Grover's algorithm to find the key of Feistel architecture block cipher Denisenko (2019) presented in detail how to construct a quantum circuit for Grover's algorithm to find the key of small-sized Feistel block cipher system called SDES with only one pair of plain text and cipher text using Quipprer Quantum simulator. In the first direction, the authors only focus on building the optimal quantum circuit for Grover's algorithm in terms of quantum resources. The detailed presentation of the operation in Grover's algorithm is not clear because the quantum circuit for AES and LowMC block cipher algorithms is very large. Besides, for SPN cipher, no published work considers the case when there is more than 1 correct key. Thus, to clarify the details of the operation phases of Grover's algorithm in finding the key of the SPN block cipher system, similar to applying Grover's algorithm in finding the Feistel block cipher key such as SDES, it is necessary to apply this algorithm to a small-sized SPN block cipher. Therefore, in this paper, we will show how to apply Grover's algorithm to Yo-yo block cipher - a small block cipher with an 8-bit block length, and 8-bit key length, built on the SPN structure. The main goal of this paper is to show how to build a quantum circuit for Grover's algorithm, applied to the problem of finding the secret key of Yo-yo block cipher in the case of knowing at least 1 plaintext-cipher pair. We consider 2 cases: there is only one satisfying key, and there are 2 satisfying keys. In addition, our implementation technique has an optimal implementation for the S-box component of SPN block cipher in Qiskit programming language. It requires only 17 qubits, and this can be very useful when applied to large-size SPN block ciphers such as AES and GOST R 34.12- 2015 on a real IBM quantum computer. In section 2, we describe how Yo-yo block cipher works. In section 3, we describe Grover's algorithm and how to apply it to an arbitrary block cipher. In section 3, we describe in detail how to construct a complete quantum circuit for the key searching problem for Yo-yo block cipher. In section 4, we show some results when applying Grover's algorithm to search for the key of Yo-yo block cipher. We provide the source code of Yo-yo block cipher (written in C++), the source code of Grover's algorithm applied to the problem of finding the secret key of Yo-yo block cipher (written in Qiskit), and other necessary source codes for the testing process, which can be found at[1].

2. YO-YO BLOCK CIPHER DESCRIPTION

Yo-yo is a block cipher with a 2-round SPN structure. $E_{Yo-yo}: V_8 \times V_8 \to V_8$, where the master key K, plaintext and ciphertext are all 8 bits. (see Fig. 1).

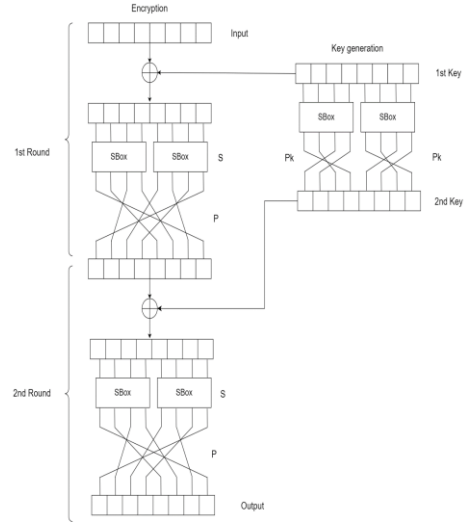

Fig. 1. Yo-yo block cipher

In which the Sbox used is a 4-bit Sbox:

Sbox	C 5 6 B 9 0 A D 3 E F 8 4 7 1 2

The round function of the Yo-yo block cipher is described as follows:

$$E_r(pt, k) = PSX_k(pt) \quad (1)$$

In which, X is a bitwise addition function:

$$X(pt, k) = pt \oplus k \quad (2)$$

The S function is described as follows:

Let $x = x_7x_6x_5x_4x_3x_2x_1x_0$; $x_l = x_7x_6x_5x_4$; $x_r = x_3x_2x_1x_0$. Then:

$$S(x) = Sbox(x_l)||Sbox(x_r) \quad (3),$$

where "||" is a bit concatenation operator.

P is a bit permutation function, which is described as follows:

$$P(x_7x_6x_5x_4x_3x_2x_1x_0) = (x_0x_5x_3x_1x_6x_4x_2x_7) \quad (4)$$

P_k is a bit permutation function too, which is described as follows:

$$P_k(k_3k_2k_1k_0) = (k_1k_0k_2k_3) \quad (5)$$

The key generation function of the Yo-yo block cipher is described as follows:

[1] https://github.com/thangvu97/Grover-Block-cipher

Let $k = k_7k_6k_5k_4k_3k_2k_1k_0$; $k_l = k_7k_6k_5k_4$; $k_r = k_3k_2k_1k_0$. Then:

$$k_{r1} = k = k_7k_6k_5k_4k_3k_2k_1k_0 \quad (6)$$

$$k_{r2} = P_k\big(Sbox(k_l)\big)||P_k\big(Sbox(k_r)\big) \quad (7)$$

Then, the encryption function of the Yo-yo block cipher is described as follows:

$$E_{yo-yo}(pt, k) = PSX_{k_{r2}}PSX_{k_{r1}}(pt) \quad (8)$$

3. GROVER'S ALGORITHM

Suppose having a set of $N = 2^n$ elements. We need to find at least 1 element that satisfies a certain search condition (the set of elements that satisfies the search condition is not empty and contains M elements, $M \leq N/2$) Define a Boolean function $f: V_n \to V_1$ as follows:

$f(x) = 1$ if and only if x satisfies search criteria.

A classical algorithm can solve this search problem with a complexity of $O(N/M)$. With Grover's algorithm, the complexity is reduced to $O\left(\sqrt{N/M}\right)$.

Grover's algorithm only works if the above function f can be implemented. In different problems, this function f will be different.

For any arbitrary block cipher, the key searching problem using Grover's algorithm is described as follows. Consider a block cipher with m-bit long input and n-bit long key: $E: V_n \times V_m \to V_m$. Suppose we obtain some plaintext-ciphertext pairs corresponding to an unknown key K: $C_i = E(K, P_i), i \in \overline{1,t}$. If there exist multiple keys that satisfy the same condition, to find a unique key, the number of plaintext-ciphertext pairs must be no less than $t = \lceil n/m \rceil$ (Shannon, 1949).

Then, the function $f: V_n \to V_1$ is defined as follows:

$$f(x) = \bigwedge_{i=1}^{t} \sigma(E(x, P_i) \oplus C_i) \quad (9)$$

In which:

$$\sigma: V_m \to V_1: \begin{cases} \sigma(x) = 1 \Leftrightarrow x = 0^m \\ \sigma(x) = 0, \quad otw \end{cases} \quad (10)$$

In this paper, we used only 1 plaintext-ciphertext pair. We consider two cases. In the first case, the plaintext-ciphertext pair only has 1 satisfied key. In the second case, the plaintext-ciphertext pair has more than 1 satisfied key. In these two cases, Grover's algorithm works similarly. The only difference is the number of Grover iterations, which is presented in the following section.

Grover's algorithm is described as follows (Lipton et al., 2021):

Input: a set $A = \{a_1, a_2, \dots, a_N\}$ of $N = 2^n$ elements. Boolean function $f: V_n \to V_1, f(x) = 1$ if and only if a_x satisfies the search criteria, in which x is the index of the element in the set A, $x \in V_n$.

Output: With probability $> 1/2$, an $a_{x'}$ that: $f(x') = 1$.

1. Initialization $n + 1$ qubit: $|\Psi_0\rangle = |0\rangle^{\otimes n}|1\rangle$. Other auxiliary qubits are initialized depending on the function f.
2. Apply Hadamard gates $H^{\otimes n+1}$:

$$|\Psi_1\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

3. Apply Grover's iteration $\frac{\pi}{4}\sqrt{N/M}$ times:

3.1. Apply Grover Oracle to change the sign of the amplitude of the target state: $|i\rangle \xrightarrow{O} (-1)^{f(i)}|i\rangle$

3.2. Apply Inversion about the mean:

- Apply $H^{\otimes n}$
- Apply $2|0\rangle\langle 0| - I$
- Apply $H^{\otimes n}$

4. Measurement of qubits. With probability $p > \frac{1}{2}$, we obtain an arbitrary x': $f(x') = 1$, from which we obtain an $a_{x'}$.

4. QUANTUM CIRCUIT FOR YO-YO BLOCK CIPHER AND QUANTUM CIRCUIT FOR GROVER'S ALGORITHM

4.1. Quantum circuit for key addition function

The key addition function can be implemented by using only CNOT gates.

Using 8 qubits corresponding to the plaintext, and 8 qubits corresponding to the key value, the quantum circuit for the key addition function is described as follows:

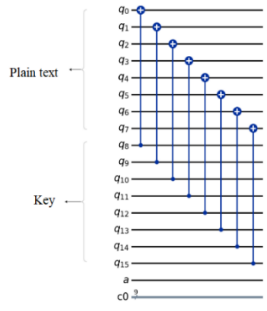

Fig. 2. Quantum circuit for key addition function

4.2. Quantum circuit for key addition function

Yo-yo block cipher uses 4-bit Sbox:

Sbox	C 5 6 B 9 0 A D 3 E F 8 4 7 1 2

The construction of a quantum circuit for a 4-bit Sbox using only basic NCT gates (NOT, CNOT, TOF) without auxiliary qubits can be done using the SAT Solver with some conditions (Chen et al., 2024). We have built a SAT Solver tool in python language to search for NCT quantum circuit for Sbox of Yo-yo block cipher. The source code can be found at https://github.com/thangvu97/Grover-Block-cipher.

The quantum circuit for the Sbox of the Yo-yo block cipher is described below:

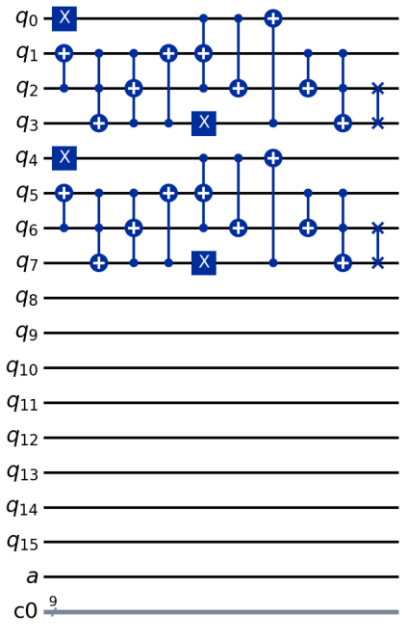

Fig. 3. Quantum Circuit for Sbox of Yo-yo block cipher

4.3. Quantum circuit for permutation P

The permutation P can be described as follows:

$$P = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 4 & 1 & 5 & 2 & 6 & 3 & 0 \end{pmatrix}$$
$$= (7 \quad 0)(6 \quad 3)(6 \quad 5)(4 \quad 2)(4 \quad 1)\,(11)$$

From this, it can be seen that the permutation P can be implemented using SWAP gates, to swap the positions of the qubits. The quantum circuit for the permutation P is described as follows:

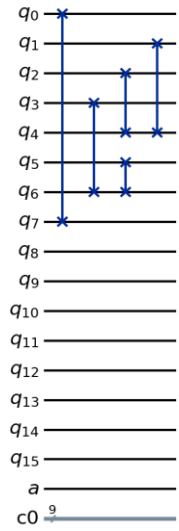

Fig. 4. Quantum Circuit for permutation *P*

4.4. Quantum circuit for key generation function

The key generation function of the Yo-yo block cipher is described as follows:

Put $k = k_7k_6k_5k_4k_3k_2k_1k_0$; $k_l = k_7k_6k_5k_4$; $k_r = k_3k_2k_1k_0$. Then:

$$k_{r1} = k = k_7k_6k_5k_4k_3k_2k_1k_0 \quad (12)$$

$$k_{r2} = P_k\big(Sbox(k_l)\big)||P_k\big(Sbox(k_r)\big) \quad (13)$$

The Sbox of the key generation function has been constructed in the above section. The quantum circuit for the permutation P_k is also easily constructed using SWAP gates.

Thus, the quantum circuit for the key generation function is described as follows:

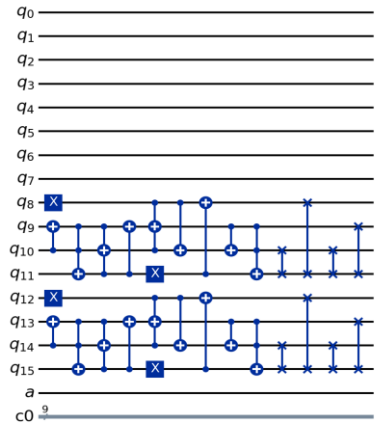

Fig. 5. Quantum circuit for key generation function

4.5. Quantum circuit for Grover's algorithm for finding the secret key of Yo-yo block cipher

Using quantum circuits in sections 4.1 to 4.4, we construct a quantum circuit for Grover's algorithm for finding the secret key of the Yo-yo block cipher.

Suppose we obtained a plaintext-ciphertext pair. plaintext = "11011011", ciphertext= "00100010";

First, set the input of the quantum circuit to the obtained plaintext. To do this, simply use the NOT gates. Consider an example where plaintext= "11011011":

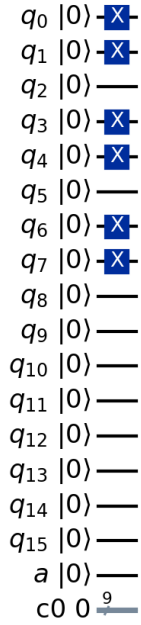

Fig. 6. Quantum circuit for plaintext "11011011"

Note, that the q_0 qubit is LSB (least significant bit) and q_7 is MSB (most significant bit).

Next, initialize the superposition of the key, and set up the auxiliary qubit a (See steps 1 and 2 of Grover's algorithm). The quantum circuit now becomes:

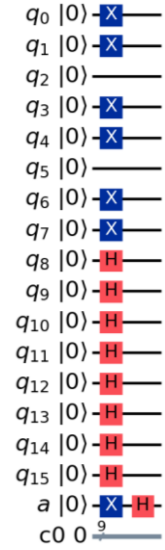

Fig. 7. Quantum circuit that implements steps 1 and 2 of Grover's algorithm

Now, apply Grover Oracle to change the sign of the amplitude:

$$|i\rangle \xrightarrow{O} (-1)^{f(i)}|i\rangle \qquad (14)$$

For the algorithm to find the secret key of a block cipher, the function f has been defined in the above section as follows:

$$f(x) = \bigwedge_{i=1}^{t} \sigma(E(x, P_i) \oplus C_i) \qquad (15)$$

Firstly, construct the circuit for the first round of the Yo-yo block cipher as follows:

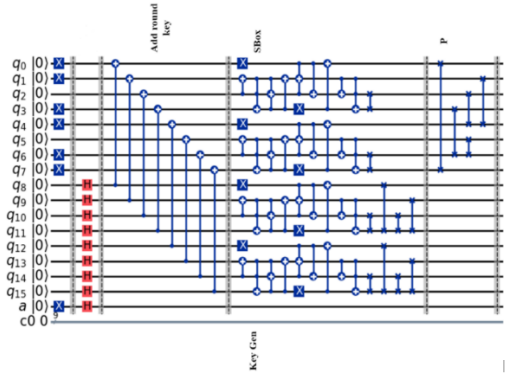

Fig. 8. The first part of the complete circuit: First round of Yo-yo block cipher

The second round of the Yo-yo block cipher is constructed similarly to the first round. Note that the key generation circuit is not needed in the second round because it has been implemented in the first round of the algorithm.

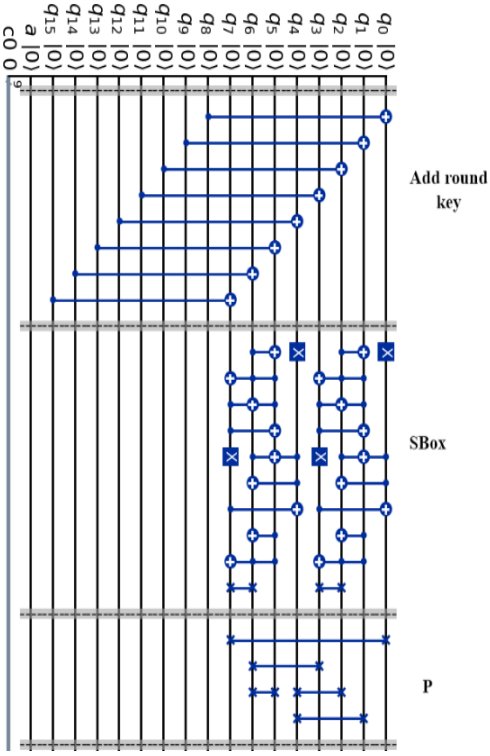

Fig. 9. The second part of the complete circuit: Second round of Yo-yo block cipher

Lastly, implement the function f defined as above:

$$f(x) = \bigwedge_{i=1}^{t} \sigma(E(x, P_i) \oplus C_i) \qquad (16)$$

In fact, this function $f(x)$ is responsible for checking the output after being encrypted. If the encrypted result matches the original ciphertext, the function $f(x)$ will give the result 1, otherwise it will give the result 0. This process can be done by using NOT gates and mcx gates (multi-controlled gates).

After executing the function $f(x)$, it is necessary to bring the 8 qubits from q_0 to q_7 back to the initial plaintext state to be ready to perform the second Grover iteration. Similarly, it is necessary to bring the 8 qubits from q_8 to q_{15} back to the state before executing the key generation function. Because the quantum circuit is symmetric, to perform these processes, it is only necessary to take the symmetry of the entire circuit through the mcx gate.

The whole process is described as follows:

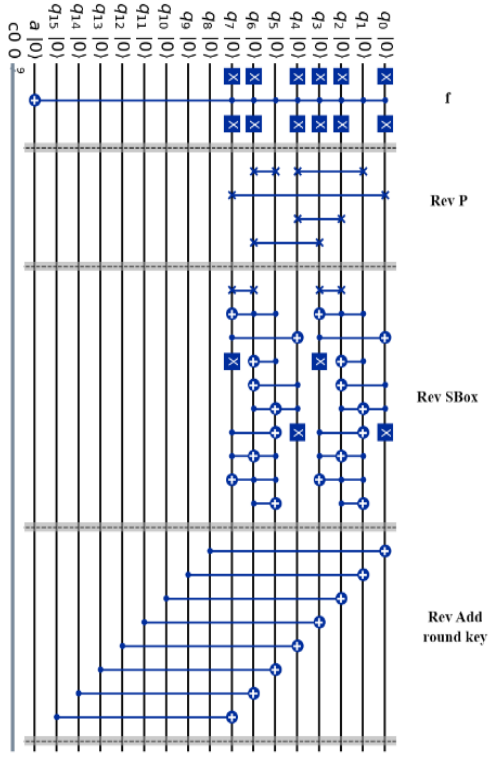

Fig. 10. Third part of the complete circuit: Check the output, and inversion circuit of the second round.

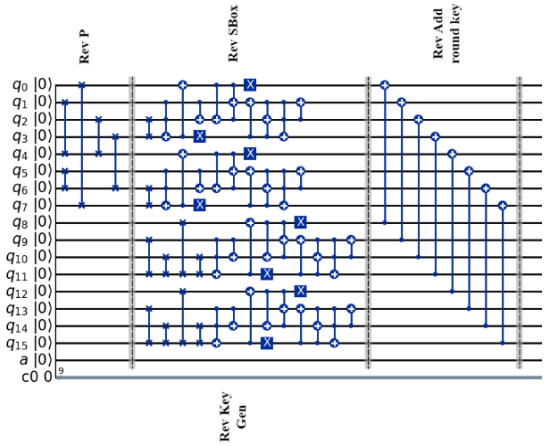

Fig. 11. The 4-th part of the complete circuit: Inversion of the first round and inversion of the key generation function

Finally, apply Inversion about the mean to the qubits that contain the key value. The process is described as follows:

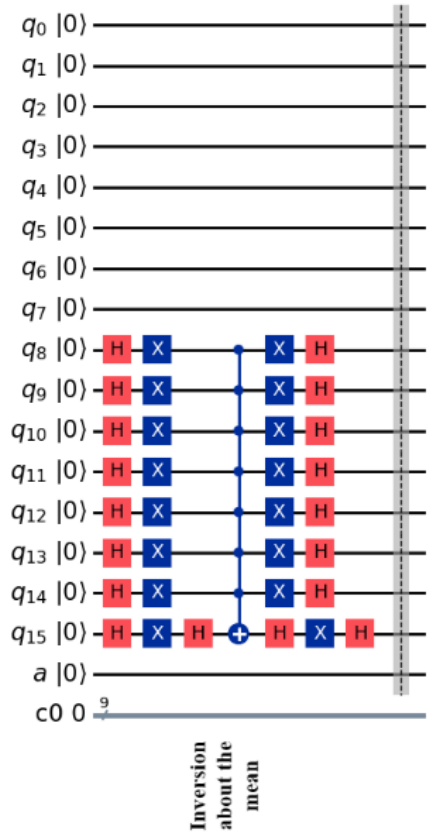

Fig. 12. The 5-th part of the complete circuit: Inversion about the mean

At this point, the first Grover iteration ends. The next Grover iteration performs the same as the first iteration. The number of Grover iterations needed to find the solution is $\approx R = \frac{\pi}{4}\sqrt{\frac{N}{M}}$ (Nielsen & Chuang, 2010). After R Grover iteration, perform a measurement on the qubits that contain the key value. The measurement will yield a correct value with probability $> \frac{1}{2}$.

The complete circuit of Grover's algorithm for Yo-yo block cipher's key searching problem is described as follows:

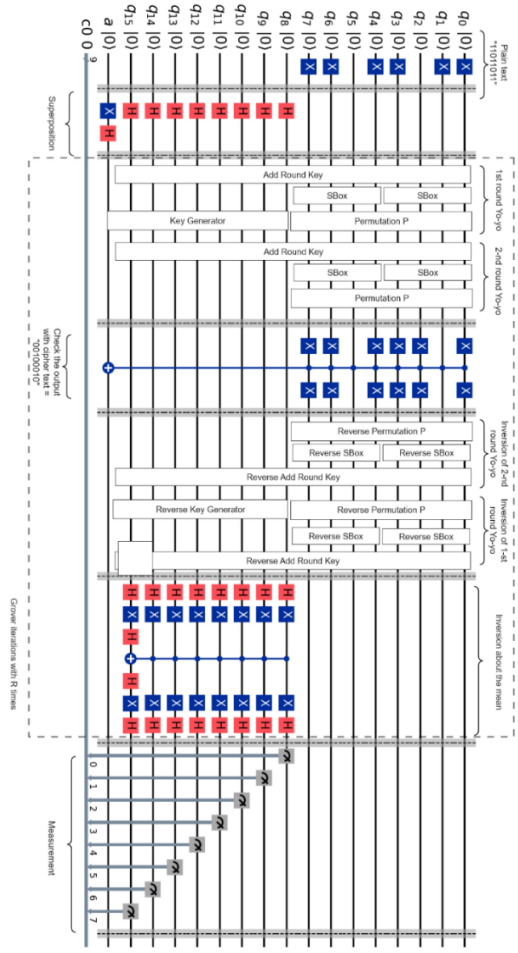

Fig. 13. The complete quantum circuit of Grover's algorithm for Yo-yo block cipher's key searching problem

5. RESULTS

5.1. First case: unique key exists

Consider the case where plaintext = "11011011"; ciphertext = "00100010". In this case, there exists a unique secret key $K \in V_8$ satisfy the condition $E_{yo-yo}(K, \text{plaintext}) = \text{ciphertext}$.

The corresponding number of Grover iterations is: $R = \frac{\pi}{4}\sqrt{\frac{N}{M}} = \frac{\pi}{4}\sqrt{\frac{2^8}{1}} \approx 12$.

After 12 Grover iterations, with 10.000.000 shots, Grover's algorithm successfully finds the correct secret key with probability $\approx 99{,}99501\%$. The probability distribution of the key values after the measurement is shown in Table 1.

Table 1. Probability distribution of key values after measurement in the first case

Yo-yo key	Probability after making the measurement
0000 0000	10^{-7}
0000 0001	2×10^{-7}
⋮	⋮
00010010	0,9999501
⋮	⋮
11111110	2×10^{-7}
11111111	3×10^{-7}

5.2. Second case: exist 2 keys

Consider the case where plaintext = "11001100"; ciphertext = "01011010". In this case, there are two secret keys $K_1, K_2 \in V_8$ that satisfy the condition $E_{yo-yo}(K_1, \text{PT}) = \text{CT}$, $E_{yo-yo}(K_2, \text{PT}) = \text{CT}$.

The corresponding number of Grover iterations is: $R = \frac{\pi}{4}\sqrt{\frac{N}{M}} = \frac{\pi}{4}\sqrt{\frac{2^8}{2}} \approx 8$.

After 8 Grover iterations, with 10.000.000 shots, Grover's algorithm successfully finds the correct secret key with probability $\approx 99{,}56376\%$. The probability distribution of the key values after the measurement is shown in Table 2.

Table 2. Probability distribution of key values after measurement in the second case

Yo-yo key	Probability after making the measurement
0000 0000	10^{-5}
0000 0001	2×10^{-5}
⋮	⋮
10111010	0,4976935
⋮	⋮
11001001	0, 4979432
⋮	⋮
11111110	10^{-5}
11111111	2×10^{-5}

6. CONCLUSIONS

In this paper, the authors presented a quantum circuit for Grover's algorithm, applied to the problem of finding the secret key of the Yo-yo block cipher. This quantum circuit uses a total of 17 qubits, of which 8 qubits are for the plaintext-ciphertext, 8 qubits are for the key, and 1 auxiliary qubit in the use of the phase-kickback technique. The authors presented 2 cases: when there is only 1 satisfying key, and when there are 2 satisfying keys. The required resources for the above quantum circuit are presented in the table below. It is observed that, in the case where only one key exists, 12 iterations of Grover's algorithm are required to obtain the correct key. If the circuit depth for one iteration is l, then 12 iterations result in a total depth of $12 \times l$. When two keys exist, only 8 iterations are needed, resulting in a circuit depth of $8 \times l$. Clearly, this reduces the depth, but in practice, the resources (number of quantum logic gates, number of qubits) effectively double. In practical implementations, this trade-off must be carefully considered to determine the most optimal attack strategy.

Table 3. Required resources for implementing Grover's algorithm on Yo-yo block cipher

Number of Grover iterations	Required resources						
	CNOT	NOT	TOF	SWAP	H gates	Mcx gates	Quantum depth
1	92	59	48	44	27	2	61
12	1104	631	576	528	225	24	699
8	736	389	384	352	153	16	467

ACKNOWLEDGMENT

This work has been supported by the Academy of Cryptography Techniques under Project/Lab.

REFERENCES

Chen, J., Liu, Q., Fan, Y., Wu, L., Li, B., & Wang, M. (2024). New Sat-based model for Quantum Circuit decision problem: Searching for low-cost quantum implementation. *IACR Communications in Cryptology*. https://doi.org/10.62056/anmmp-4c2h

Chung, D., Lee, S., Choi, D., & Lee, J. (2022). Alternative tower field construction for quantum implementation of the AES S-box. *IEEE Transactions on Computers*, *71*(10), 2553–2564.

Denisenko, D. V. (2019). Quantum circuits for S-box implementation without ancilla qubits. *Journal of Experimental and Theoretical Physics*, *128*(6), 847–855. https://doi.org/10.1134/s1063776119050108.

Grassl, M., Langenberg, B., Roetteler, M., & Steinwandt, R. (2016). Applying Grover's algorithm to AES: *Quantum Resource Estimates*. Lecture Notes in Computer Science, 29–43.

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing - STOC '96*, 212–219.

Jaques, S., Naehrig, M., Roetteler, M., & Virdia, F. (2020). Implementing Grover oracles for Quantum Key Search on AES and lowmc. *Lecture Notes in Computer Science*, 280–310.

Kim, P., Han, D., & Jeong, K. C. (2018). Time–space complexity of quantum search algorithms in symmetric cryptanalysis: Applying to AES and SHA-2. *Quantum Information Processing*, *17*(12).

Lipton, R. J., & Regan, K. W. (2021). *Introduction to quantum algorithms via linear algebra*. The MIT Press.

Nielsen, M., & Chuang, I. (2010). *Quantum Computation and Quantum Information Nielsen, Michael*. Cambridge University Press.

Shannon, C. E. (1949). Communication theory of secrecy systems. *The Bell system technical journal*, *28*(4), 656-715.